



Protegrity Data Security Platform Upgrade Guide

Release 9.1.0.5

Created on: Nov 19, 2024

Copyright

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

Protegility products are protected by and subject to patent protections;

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

The Protegility logo is the trademark of Protegility 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

Copyright.....	2
Chapter 1 Introduction to this Guide.....	12
1.1 Sections Contained in this Guide.....	12
1.2 Accessing the Protegility documentation suite.....	13
1.2.1 Viewing product documentation.....	13
1.2.2 Downloading product documentation.....	13
Chapter 2 Data Security Platform Overview.....	15
2.1 Audience.....	15
2.2 Protegility Data Security Platform.....	15
2.2.1 Architecture.....	15
Chapter 3 General Enhancements in v9.1.0.5.....	17
3.1 Salient Features.....	17
3.2 ESA v9.1.0.5 Compatibility with Supported Protectors.....	17
Chapter 4 Upgrade Paths to ESA v9.1.0.5.....	18
Chapter 5 Upgrading to v9.1.0.x.....	21
5.1 Upgrading ESA from v7.2.1.....	21
5.1.1 Upgrade Process: Flow Diagram.....	23
5.1.2 Upgrade Process: Step-by-step Procedure.....	25
5.1.3 Installing ESA.....	28
5.1.4 Prerequisites.....	29
5.1.4.1 Accounts.....	29
5.1.4.2 Backup and Restore.....	29
5.1.4.3 Installations and Hardware Requirements.....	31
5.1.4.4 High Availability (HA).....	31
5.1.4.5 Trusted Appliances Cluster (TAC).....	31
5.1.4.6 Keys.....	32
5.1.4.7 ESA Settings.....	32
5.1.4.8 Creating a Metering Backup File.....	32
5.1.4.9 Customized Files (Configuration Files and Certificates).....	33
5.1.4.10 Logging, Reporting, and Certificates.....	33
5.1.4.11 License.....	34
5.1.5 Upgrading ESA to Pre-v9.0.0.0.....	34
5.1.6 Post Upgrade Steps on version Pre-v9.0.0.0.....	34
5.1.6.1 Restarting the ESA.....	34
5.1.6.2 Upgrade Logs.....	35
5.1.6.3 Restoring the Backup File of the Metering Logs.....	35
5.1.6.4 Verifying the Patch Installation.....	35
5.1.7 Migrating the ESA to v9.0.0.0.....	36
5.1.7.1 Exporting Data or Configurations to a Local File.....	36
5.1.7.2 Importing Data or Configurations from a File.....	37
5.1.8 Installing the ESA v9.1.0.x Patch.....	38
5.1.9 Restarting the ESA.....	38
5.1.10 Post Upgrade Steps on ESA v9.1.0.x.....	38
5.1.10.1 Verifying the ESA Patch Installation.....	39
5.1.10.2 Verifying the <i>cron-jobs</i> for the Analytics.....	39
5.1.11 Configuring Settings on v9.1.0.x.....	40
5.1.11.1 Configuring the ESA v9.1.0.x.....	40
5.1.11.2 Upgrading custom files to <i>python3</i>	41



5.1.11.3 Adding Permissions to the Existing Roles.....	42
5.1.11.4 Opening the Ports.....	42
5.1.11.5 Rotating Certificates on a Single Node Audit Store Cluster.....	43
5.1.12 Creating an Audit Store Cluster.....	48
5.1.12.1 Initializing the Audit Store Cluster on the ESA.....	48
5.1.12.2 Adding an ESA to the Audit Store Cluster.....	50
5.1.12.3 Refreshing the Audit Store Cluster.....	52
5.1.12.4 Configuring td-agent in the Audit Store Cluster.....	52
5.1.12.5 Verifying the Audit Store Cluster.....	53
5.1.13 Migrating DMS Logs and Metering Data.....	54
5.1.13.1 Setting the Audit Store.....	54
5.1.13.2 Migrating Logs.....	56
5.1.14 Restoring to the Previous Version of ESA.....	58
5.1.14.1 Restoring to the Previous Version of ESA On-premise.....	58
5.1.14.2 Restoring to the Previous Version of ESA from Snapshot.....	58
5.2 Upgrading from v9.x.0.0 to v9.1.0.x.....	61
5.2.1 Prerequisites.....	61
5.2.1.1 Accounts.....	61
5.2.1.2 Backup and Restore.....	61
5.2.1.3 Installations and Hardware Requirements.....	63
5.2.1.4 Disabling the Scheduled Tasks for a Cluster.....	64
5.2.1.5 Deleting a Scheduled Task.....	64
5.2.1.6 Removing Nodes from the Cluster.....	65
5.2.1.7 Keys.....	65
5.2.1.8 Disabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	65
5.2.1.9 Disabling <i>Rollover Index</i> Task.....	65
5.2.1.10 Configuring Local LDAP.....	66
5.2.1.11 Switching to the Protegility Soft HSM.....	66
5.2.1.12 Replacing the PSUs with the ESAs v9.1.0.x in the Audit Store Cluster.....	66
5.2.2 Installing the ESA v9.1.0.x Patch.....	74
5.2.3 Verifying the ESA Patch Installation.....	74
5.2.4 Post Upgrade Steps.....	75
5.2.4.1 Upgrade Logs.....	75
5.2.4.2 Restarting the System.....	75
5.2.4.3 Verifying the Local LDAP Settings.....	75
5.2.4.4 Verifying the <i>cron-jobs</i> for the Analytics.....	75
5.2.4.5 Restoring the Configuration File.....	76
5.2.4.6 Enabling the Scheduled Tasks for a Cluster.....	76
5.2.4.7 Updating the Priority IP List for Signature Verification.....	77
5.2.4.8 Enabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	77
5.2.4.9 Enabling <i>Rollover Index</i> Task.....	77
5.2.4.10 Optional: Configuring SMTP for Alerts.....	78
5.2.4.11 Configuring the GCP Key Store.....	79
5.2.4.12 Optional: Updating configuration for sending logs to the external SIEM.....	79
5.2.5 Restoring to the Previous Version of ESA.....	80
5.2.5.1 Restoring to the Previous Version of ESA On-premise.....	80
5.2.5.2 Restoring to the Previous Version of ESA from Snapshot.....	80
5.3 Upgrading from v9.1.0.x to v9.1.0.5.....	83
5.3.1 Prerequisites.....	83
5.3.1.1 Accounts.....	83
5.3.1.2 Backup and Restore.....	83
5.3.1.3 Installations and Hardware Requirements.....	85
5.3.1.4 Disabling the Scheduled Tasks for a Cluster.....	86
5.3.1.5 Keys.....	86
5.3.1.6 Disabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	86
5.3.1.7 Disabling <i>Rollover Index</i> Task.....	87
5.3.1.8 Switching to the Protegility Soft HSM.....	87
5.3.2 Installing the ESA v9.1.0.x Patch.....	87



5.3.3 Verifying the ESA Patch Installation.....	88
5.3.4 Post Upgrade Steps.....	88
5.3.4.1 Upgrade Logs.....	88
5.3.4.2 Restarting the System.....	89
5.3.4.3 Restoring the Configuration File.....	89
5.3.4.4 Enabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	89
5.3.4.5 Enabling <i>Rollover Index</i> Task.....	89
5.3.4.6 Enabling the Scheduled Tasks for a Cluster.....	90
5.3.4.7 Enabling the CloudWatch Service.....	90
5.3.4.8 Configuring the GCP Key Store.....	90
5.3.4.9 Optional: Updating configuration for sending logs to the external SIEM.....	91
5.3.5 Restoring to the Previous Version of ESA.....	91
5.3.5.1 Restoring to the Previous Version of ESA On-premise.....	91
5.3.5.2 Restoring to the Previous Version of ESA from Snapshot.....	92
5.4 Upgrading Protectors.....	94
5.4.1 Upgrading to Data Security Gateway (DSG) v3.1.0.x.....	95
5.4.1.1 Applying a DSG Patch.....	95
Chapter 6 Upgrading from v9.0.0.0 to v9.1.0.0.....	97
6.1 Prerequisites.....	97
6.1.1 Accounts.....	97
6.1.2 Backup and Restore.....	97
6.1.2.1 Full OS Backup.....	98
6.1.2.2 Exporting Data or Configuration to Remote Appliance.....	98
6.1.2.3 Creating a Snapshot for Cloud-based Services.....	99
6.1.2.4 Backing up the Configuration File.....	99
6.1.2.5 Validating Custom Configuration Files.....	99
6.1.3 Installations and Hardware Requirements.....	100
6.1.4 Keys.....	100
6.1.5 Disabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	100
6.1.6 Disabling <i>Rollover Index</i> Task.....	101
6.1.7 Disabling the ESA LDAP on the PSU.....	101
6.2 Upgrading to ESA v9.1.0.0.....	101
6.3 Upgrading PSU from v9.0.0.0 to v9.1.0.0.....	102
6.4 Verifying Patch Installation.....	103
6.4.1 Verifying the ESA Patch Installation.....	103
6.4.2 Verifying the PSU Patch Installation.....	104
6.5 Post Upgrade Steps.....	104
6.5.1 Upgrade Logs.....	104
6.5.2 Restarting the System.....	105
6.5.3 Restoring the Configuration File.....	105
6.5.4 Updating the Priority IP List for Signature Verification.....	105
6.5.5 Enabling <i>Update Audit Store Management Unicast Hosts</i> Task.....	105
6.5.6 Enabling <i>Rollover Index</i> Task.....	106
6.5.7 Enabling the ESA LDAP on the PSU.....	106
6.5.8 Optional: Configuring SMTP for Alerts.....	106
6.6 Restoring to the Previous Version of ESA.....	107
6.6.1 Restoring to the Previous Version of ESA On-premise.....	107
6.6.2 Restoring to the Previous Version of ESA from Snapshot.....	108
6.6.2.1 Restoring a Snapshot on AWS.....	108
6.6.2.2 Restoring from a snapshot on GCP.....	109
6.6.2.3 Restoring from a Snapshot on Azure.....	110
6.7 Upgrading Protectors.....	110
6.7.1 Upgrading Data Security Gateway (DSG).....	111
6.7.1.1 Upgrading the DSG from v3.0.0.0 to v3.1.0.0.....	111
Chapter 7 Upgrading from v8.1.0.1 to v9.0.0.0.....	113



7.1 Migrating ESA v8.1.0.1 to ESA v9.0.0.0.....	113
7.1.1 Upgrade Process: Flow Diagram.....	115
7.1.2 Upgrade Process: Step-by-step Procedure.....	121
7.2 Installing ESA.....	123
7.3 Prerequisites.....	124
7.3.1 Accounts.....	124
7.3.2 Backup and Restore.....	124
7.3.2.1 Full OS Backup.....	125
7.3.2.2 Exporting Data or Configuration to Remote Appliance.....	125
7.3.2.3 Creating a Snapshot for Cloud-based Services.....	126
7.3.3 Installations and Hardware Requirements.....	126
7.3.4 ESA Settings.....	126
7.3.5 Trusted Appliances Cluster (TAC).....	127
7.3.6 Two-factor Authentication.....	127
7.3.7 Keys.....	127
7.3.8 License.....	127
7.3.9 Customized Files (Configuration Files and Certificates).....	127
7.4 Installing the Pre-Patch on the PSU.....	128
7.5 Migrating the ESA to v9.0.0.0.....	129
7.6 Configuring the ESA v9.0.0.0.....	131
7.7 Upgrading custom files to <i>python3</i>	133
7.8 Rotating Certificates on a Single Node Audit Store Cluster.....	134
7.9 Installing the Protegility Storage Unit.....	139
7.9.1 Audit Store Clustering using the Protegility Storage Unit.....	139
7.9.1.1 Completing the Prerequisites.....	142
7.9.1.2 Initializing the Audit Store Cluster on the ESA.....	142
7.9.1.3 Adding an ESA to the Audit Store Cluster.....	143
7.9.1.4 Adding the Protegility Storage Unit to the Audit Store Cluster.....	146
7.9.1.5 Refreshing the Audit Store Cluster.....	148
7.9.1.6 Configuring td-agent in the Audit Store Cluster.....	149
7.9.1.7 Verifying the Audit Store Cluster.....	149
7.9.2 Optional: Using an External SIEM.....	150
7.10 Post Upgrade Steps.....	150
7.10.1 Migrating Configuration Settings and Logs.....	150
7.10.2 Migrating Reports and Indices.....	153
7.10.3 Updating the Priority IP List for Signature Verification.....	153
7.10.4 Configuring the Security Settings for Protectors.....	154
7.10.5 Optional: Configuring SMTP for Alerts.....	154
7.11 Restoring to the Previous Version of ESA.....	155
7.11.1 Restoring to the Previous Version of ESA On-premise.....	155
7.11.2 Restoring to the Previous Version of ESA from Snapshot.....	156
7.11.2.1 Restoring a Snapshot on AWS.....	156
7.11.2.2 Restoring from a snapshot on GCP.....	157
7.11.2.3 Restoring from a Snapshot on Azure.....	158
7.12 Upgrading Protectors.....	158
7.12.1 Upgrading Data Security Gateway (DSG).....	158
7.12.1.1 Applying a DSG Patch.....	159

Chapter 8 Upgrading from v7.2.1 to v9.0.0.0	160
8.1 Migrating ESA v7.2.1 to ESA v9.0.0.0.....	160
8.1.1 Upgrade Process: Flow Diagram.....	162
8.1.2 Upgrade Process: Step-by-step Procedure.....	169
8.2 Installing ESA.....	173
8.3 Prerequisites.....	173
8.3.1 Accounts.....	173
8.3.2 Backup and Restore.....	174
8.3.2.1 Full OS Backup.....	174
8.3.2.2 Exporting Data or Configuration to Remote Appliance.....	174



8.3.2.3 Creating a Snapshot for Cloud-based Services.....	175
8.3.3 Installations and Hardware Requirements.....	175
8.3.4 High Availability (HA).....	176
8.3.5 Trusted Appliances Cluster (TAC).....	176
8.3.6 Keys.....	176
8.3.7 ESA Settings.....	176
8.3.8 Creating a Metering Backup File.....	177
8.3.9 Customized Files (Configuration Files and Certificates).....	177
8.3.10 Logging, Reporting, and Certificates.....	178
8.3.11 License.....	178
8.4 Upgrading ESA to Pre-v9.0.0.0.....	178
8.5 Post Upgrade Steps on version Pre-v9.0.0.0.....	179
8.5.1 Restarting the ESA.....	179
8.5.2 Upgrade Logs.....	180
8.5.3 Restoring the Backup File of the Metering Logs.....	180
8.5.4 Verifying the Patch Installation.....	180
8.6 Migrating the ESA to v9.0.0.0.....	181
8.7 Configuring Settings on v9.0.0.0.....	183
8.7.1 Configuring the ESA v9.1.0.1.....	184
8.7.2 Upgrading custom files to <i>python3</i>	185
8.7.3 Adding Permissions to the Existing Roles.....	185
8.7.4 Opening the Ports.....	186
8.7.5 Rotating Certificates on a Single Node Audit Store Cluster.....	187
8.8 Installing the Protegility Storage Unit.....	192
8.8.1 Audit Store Clustering using the Protegility Storage Unit.....	192
8.8.1.1 Completing the Prerequisites.....	195
8.8.1.2 Initializing the Audit Store Cluster on the ESA.....	195
8.8.1.3 Adding an ESA to the Audit Store Cluster.....	196
8.8.1.4 Adding the Protegility Storage Unit to the Audit Store Cluster.....	199
8.8.1.5 Refreshing the Audit Store Cluster.....	201
8.8.1.6 Configuring td-agent in the Audit Store Cluster.....	202
8.8.1.7 Verifying the Audit Store Cluster.....	202
8.8.2 Optional: Using an External SIEM.....	203
8.9 Migrating DMS Logs and Metering Data.....	203
8.9.1 Setting the Audit Store.....	203
8.9.2 Migrating Logs.....	206
8.10 Restoring to the Previous Version of ESA.....	207
8.10.1 Restoring to the Previous Version of ESA On-premise.....	207
8.10.2 Restoring to the Previous Version of ESA from Snapshot.....	208
8.10.2.1 Restoring a Snapshot on AWS.....	208
8.10.2.2 Restoring from a snapshot on GCP.....	209
8.10.2.3 Restoring from a Snapshot on Azure.....	210
Chapter 9 Upgrading from v8.1.0.0 to v8.1.0.1.....	211
9.1 Prerequisites.....	211
9.1.1 Accounts.....	211
9.1.2 Backup and Restore.....	212
9.1.2.1 Full OS Backup.....	212
9.1.2.2 Exporting Data or Configuration to Remote Appliance.....	212
9.1.2.3 Creating a Snapshot for Cloud-based Services.....	213
9.1.3 Installations and Hardware Requirements.....	213
9.1.4 Keys.....	214
9.1.5 Customized Files (Configuration Files and Certificates).....	214
9.1.6 Configuring the External Elasticsearch with Open Distro.....	214
9.2 Upgrading ESA from v8.1.0.0 to v8.1.0.1.....	215
9.3 Upgrading PSU from v8.1.0.0 to v8.1.0.1.....	216
9.4 Verifying Patch Installation.....	217
9.4.1 Verifying the ESA Patch Installation.....	218



9.4.2 Verifying the PSU Patch Installation.....	218
9.5 Post Upgrade Steps.....	218
9.5.1 Upgrade Logs.....	219
9.5.2 Restarting the System.....	219
9.5.3 Updating the Priority IP List for Signature Verification.....	219
9.5.4 Optional: Configuring SMTP for Alerts.....	219
9.6 Restoring to the Previous Version of ESA.....	220
9.6.1 Restoring to the Previous Version of ESA On-premise.....	220
9.6.2 Restoring to the Previous Version of ESA from Snapshot.....	221
9.6.2.1 Restoring a Snapshot on AWS.....	221
9.6.2.2 Restoring from a snapshot on GCP.....	222
9.6.2.3 Restoring from a Snapshot on Azure.....	223
Chapter 10 Upgrading from v7.2.1 to v8.1.0.0.....	224
10.1 Upgrading to ESA v7.2.1 to ESA v8.1.0.0.....	224
10.1.1 Overview of the Upgrade from ESA v7.2.1 to ESA v8.1.0.0.....	224
10.1.1.1 Overview of upgrading ESA v7.2.1 to ESA v8.1.0.0.....	225
10.1.1.2 Upgrade Process: Flow Diagram.....	228
10.1.1.3 Upgrade Process: Step-by-step procedure.....	233
10.1.2 Prerequisites.....	237
10.1.2.1 Accounts.....	237
10.1.2.2 Backup and Restore.....	237
10.1.2.3 Installations and Hardware Requirements.....	239
10.1.2.4 High Availability (HA).....	240
10.1.2.5 Keys.....	240
10.1.2.6 Creating a Metering Backup File.....	240
10.1.2.7 Customized files (Configuration files, Certificates).....	241
10.1.2.8 Logging, Reporting, and Certificates.....	241
10.1.2.9 HSM.....	241
10.1.3 Upgrading ESA from v8.0.0.0 to v8.1.0.0.....	241
10.1.4 Completing the Upgrade.....	243
10.1.4.1 Upgrade Logs.....	243
10.1.4.2 Verifying the Patch Installation.....	244
10.1.4.3 Adding AppArmor Profiles.....	244
10.1.4.4 Restoring the Backup File of the Metering Logs.....	245
10.1.4.5 Restarting the System.....	245
10.1.4.6 Custom Certificates.....	245
10.1.4.7 Installing the Protegility Storage Unit.....	246
10.1.5 Configuring the Logging Database.....	246
10.1.5.1 Installing the Protegility Storage Unit.....	246
10.1.5.2 Optional: Using an External SIEM.....	256
10.1.6 Migrating DMS Logs and Metering Data.....	257
10.1.6.1 Metering Data.....	257
10.1.6.2 Migrating Logs.....	257
10.1.7 Post Upgrade Steps.....	258
10.1.7.1 Recreating Reports, Alerts, and Schedule Tasks.....	259
10.1.7.2 Removing the Reporting Server and DMS Components.....	259
10.1.7.3 Optional: Configuring SMTP for Alerts.....	260
10.1.8 Restoring to the Previous Version of ESA.....	261
10.1.8.1 Restoring to the Previous Version of ESA On-premise.....	261
10.1.8.2 Restoring to the Previous Version of ESA from Snapshot.....	262
10.2 Upgrading Protectors.....	264
10.2.1 Upgrading Application Protector.....	264
10.2.2 Upgrading Database Protector.....	265
10.2.3 Upgrading Data Security Gateway (DSG).....	265
Chapter 11 Upgrading from Big Data Protector v7.2 to Big Data Protector v8.1.0.0.....	266



Chapter 12 Upgrading from v7.2.1 to v8.0.0.0.....	267
12.1 Overview of the Upgrade to ESA v8.0.0.0.....	267
12.1.1 Upgrading a Standalone ESA.....	267
12.1.2 Upgrading ESA on a TAC Setup.....	268
12.2 Upgrading to ESA v8.0.0.0.....	272
12.2.1 Prerequisites.....	272
12.2.1.1 Accounts.....	272
12.2.1.2 Backup and Restore.....	272
12.2.1.3 Installations and Hardware Requirements.....	273
12.2.1.4 High Availability (HA).....	274
12.2.1.5 Trusted Appliances Cluster (TAC).....	274
12.2.1.6 Keys.....	274
12.2.1.7 Creating a Metering Backup File.....	274
12.2.1.8 Customized files (Configuration files, Certificates).....	275
12.2.1.9 DMS and Reporting Server.....	275
12.2.1.10 HSM.....	276
12.2.1.11 Kernel Mode.....	276
12.2.2 Upgrading ESA from v7.2.1 to v8.0.0.0.....	276
12.2.3 Upgrading to ESA v8.0.0.0 on Cloud-based Services.....	278
12.2.3.1 Upgrading from Existing ESA Instance of v8.0.0.0.....	279
12.2.4 Completing the Upgrade.....	279
12.2.4.1 Upgrade Logs.....	279
12.2.4.2 Verifying the Patch Installation.....	279
12.2.4.3 Adding AppArmor Profiles.....	280
12.2.4.4 Restoring the Backup File of the Metering Logs.....	280
12.2.4.5 Restarting the System.....	281
12.2.4.6 Custom Certificates.....	281
12.2.4.7 Installing the Protegility Storage Unit.....	282
12.2.5 Audit Store Clustering using the Protegility Storage Unit.....	282
12.2.5.1 Completing the Prerequisites.....	284
12.2.5.2 Initializing the Audit Store Cluster on the ESA.....	285
12.2.5.3 Adding an ESA to the Audit Store Cluster.....	286
12.2.5.4 Adding the Protegility Storage Unit to the Audit Store Cluster.....	289
12.2.5.5 Refreshing the Audit Store Cluster Settings	291
12.2.5.6 Configuring td-agent in the Audit Store Cluster.....	291
12.2.5.7 Verifying the Audit Store Cluster.....	292
12.2.6 Migrating DMS Logs and Metering Data.....	293
12.2.6.1 Metering Data.....	293
12.2.6.2 Migrating Logs.....	294
12.2.7 Post Upgrade Steps.....	295
12.2.7.1 Recreating Reports, Alerts, and Schedule Tasks.....	295
12.2.7.2 Removing the Reporting Server and DMS Components.....	296
12.2.7.3 Optional: Configuring SMTP for Alerts.....	296
12.2.8 Restoring to the Previous Version of ESA.....	297
12.2.8.1 Restoring to the Previous Version of ESA On-premise.....	297
12.2.8.2 Restoring to the Previous Version of ESA from Snapshot.....	298
12.3 Upgrading Protectors.....	300
12.3.1 Upgrading Application Protector.....	300
12.3.2 Upgrading Database Protector.....	301
12.3.3 Upgrading Data Security Gateway (DSG).....	301
12.3.4 Upgrading Big Data Protector.....	301
12.3.4.1 Upgrading Big Data Protector using CDH Native Installer.....	301
Chapter 13 Appendix A: System Hardware Requirements.....	311
13.1 Appendix A: System Hardware Requirements.....	311

Chapter 14 Appendix B: Protegility Products Compatibility Matrix.....	312
Chapter 15 Appendix C: Migrating Logs Using the DMS Exporter.....	315
15.1 Verifying the DMS Exporter Installation.....	315
15.2 Working with the DMS Exporter.....	316
15.2.1 Starting the DMS Exporter.....	316
15.2.2 Stopping the DMS Exporter.....	316
15.2.3 Viewing the DMS Exporter Status.....	317
15.2.4 Restarting the DMS Exporter.....	317
Chapter 16 Appendix D: Analytics Migration Tools.....	319
16.1 Migrating Analytics Configuration.....	319
16.2 Migrating Analytics Audits.....	322
16.2.1 Stopping the Migrate Analytics Audits Tool.....	325
16.3 Clear Analytics Migration Configuration.....	326
Chapter 17 Appendix E: Optional: Updating settings for External Databases.....	329
17.1 Configuring the External Elasticsearch with Open Distro.....	329
17.2 Upgrading the External Database Schemas.....	330
17.3 Migrating Logs on the External Elasticsearch with Open Distro.....	330

Chapter 1

Introduction to this Guide

1.1 Sections Contained in this Guide

1.2 Accessing the Protegility documentation suite

This guide provides information that you need to upgrade the Protegility products to v9.1.0.5.

1.1 Sections Contained in this Guide

The guide is broadly divided into the following sections:

- Section [*1 Introduction to this Guide*](#) defines the purpose and scope for this guide. In addition, it explains how information is organized in this guide.
- Section [*2 Data Security Platform Upgrade Overview*](#) provides an overview of the Data Security Platform Upgrade process. In addition, this section provides an overview of the Protegility Data Security Platform and its general architecture.
- Section [*3 General Enhancements in v9.1.0.5*](#) describes about the new features in v9.1.0.5. Additionally, this section also explains the ESA v9.1.0.5 compatibility with the supported protectors.
- Section [*4 Upgrade Paths to ESA v9.1.0.5*](#) contains references of the upgrade path to v9.1.0.5.
- Section [*5 Upgrading to ESA v 9.1.0.x*](#) describes the steps to upgrade the ESA to v9.1.0.5.
- Section [*6 Upgrading from v9.0.0.0 to v9.1.0.0*](#) describes the steps to upgrade the ESA from v9.0.0.0 to v9.1.0.0.
- Section [*7 Upgrading from v8.1.0.1 to v9.0.0.0*](#) describes the steps to upgrade the ESA from v8.1.0.1 to v9.0.0.0.
- Section [*8 Upgrading from v7.2.1 to v9.0.0.0*](#) describes the steps to upgrade the ESA from v7.2.1 to v9.0.0.0.
- Section [*9 Upgrading ESA from 8.1.0.0. to v8.1.0.1*](#) describes the steps to upgrade the ESA and protectors to v8.1.0.1.
- Section [*10 Upgrading ESA from 7.2.1 to v8.1.0.0*](#) describes the steps to upgrade the ESA and protectors from version v7.2.1 to v8.1.0.0.
- Section [*11 Upgrading from Big Data Protector v7.2 to Big Data Protector v8.1.0.0*](#) describes the steps to upgrade the Big Data Protector from version 7.2.0 to version 8.1.0.0.
- Section [*12 Upgrading to ESA v8.0.0.0*](#) describes the steps to upgrade the ESA and protectors to v8.0.0.0.
- Section [*13 Appendix A: System Hardware Requirements*](#) provides information about the compatibility settings for Protegility products.
- Section [*14 Appendix B: Protegility Products Compatibility Matrix*](#) contains tables that show the supported compatibility of Protegility products.
- Section [*15 Appendix C: Migrating Logs Using the DMS Exporter*](#) describes the required steps to migrate the logs using the DMS Exporter.
- Section [*16 Appendix D: Analytics Migration Tools*](#) describes the migration of analytics tools.
- Section [*17 Appendix E: Optional: Updating settings for External Databases*](#) describes the required steps to upgrade settings for external databases.



1.2 Accessing the Protegility documentation suite

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

1.2.1 Viewing product documentation

The **Product Documentation** section under **Resources** is a repository for Protegility product documentation. The documentation for the latest product release is displayed first. The documentation is available in the HTML format and can be viewed using your browser. You can also view and download the *.pdf* files of the required product documentation.

1. Log in to the [My.Protegility](#) portal.
2. Click **Resources > Product Documentation**.
3. Click a product version.
The documentation appears.

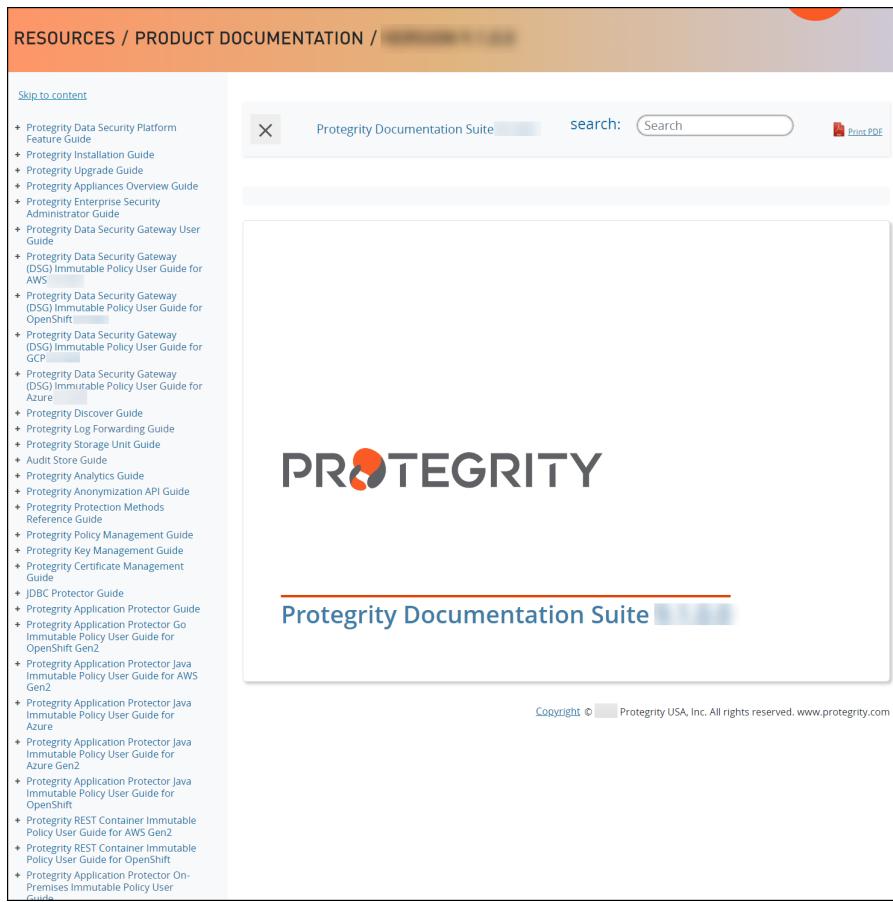


Figure 1-1: Documentation

4. Expand and click the link for the required documentation.
5. If required, then enter text in the **Search** field to search for keywords in the documentation.
The search is dynamic, and filters results while you type the text.
6. Click the **Print PDF** icon from the upper-right corner of the page.
The page with links for viewing and downloading the guides appears. You can view and print the guides that you require.

1.2.2 Downloading product documentation

This section explains the procedure to download the product documentation from the [My.Protegility](#) portal.

1. Click **Product Management > Explore Products**.
2. Select **Product Documentation**.
The **Explore Products** page is displayed. You can view the product documentation of various Protegility products as per their releases, containing an overview and other guidelines to use these products at ease.
3. Click **View Products** to advance to the product listing screen.
4. Click the **View** icon (⌚) from the **Action** column for the row marked **On-Prem** in the **Target Platform Details** column.
If you want to filter the list, then use the filters for: **OS**, **Target Platform**, and **Search** fields.
5. Click the icon for the action that you want to perform.

Chapter 2

Data Security Platform Overview

2.1 Audience

2.2 Protegility Data Security Platform

This section provides a general overview of the Protegility Data Security Platform and the intended audience of this guide.

2.1 Audience

This Upgrade Guide is intended for the following stakeholders:

- Security professionals such as security officers who are responsible for protecting business systems in organizations. They plan and ensure execution of security arrangement for their organization.
- System administrators and other technical personnel who are responsible for implementing data security solutions in their organization.
- System Architects who are responsible for providing expert guidance in designing, development and implementation of enterprise data security solution architecture for their business requirements.

2.2 Protegility Data Security Platform

The Protegility Data Security Platform is a comprehensive source of enterprise data protection solutions. Its design is based on a hub and spoke deployment architecture.

The Protegility Data Security Platform has following components:

Enterprise Security Administrator (ESA) Handles the management of policies, keys, monitoring, auditing, and reporting of protected systems in the enterprise.

Data Protectors – Protect sensitive data in the enterprise and deploy security policy for enforcement on each installed system. A policy is deployed from ESA to the Data Protectors and Audit Logs of all activity on sensitive data is forwarded to the appliances, such as, the ESA or external logging systems.

2.2.1 Architecture

The following diagram shows the general architecture of the Protegility Data Security Platform.

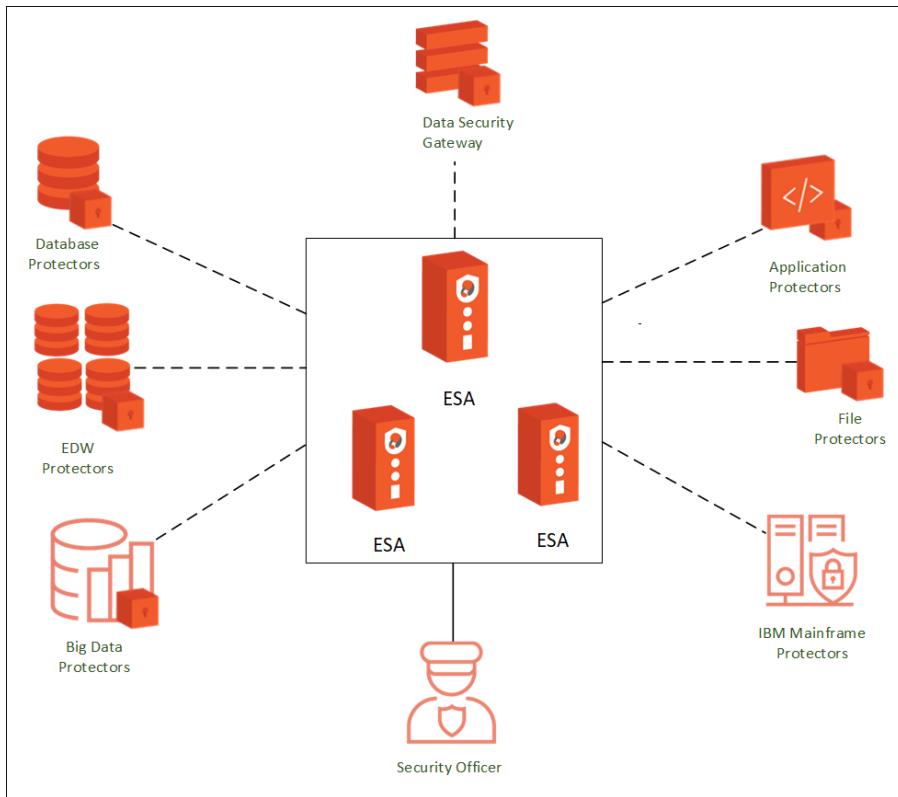


Figure 2-1: Protegility Data Security Platform

Chapter 3

General Enhancements in v9.1.0.5

3.1 Salient Features

3.2 ESA v9.1.0.5 Compatibility with Supported Protectors

This section describes the new features that are available in v9.1.0.x and the compatibility between the ESA v9.1.0.x and the supported protectors.

3.1 Salient Features

In the ESA v9.1.0.x, some new features have been added for enhancing the security of the Protegility appliance.

For more information about the new features added in this release, refer to the section *What's New* in the *Protegility Data Security Platform Feature Guide 9.1.0.5*.

3.2 ESA v9.1.0.5 Compatibility with Supported Protectors

This section explains the ESA v9.1.0.5 compatibility with the different versions of protectors.

The following table describes the compatibility matrix between the ESA v9.1.0.5 and the supported protectors.

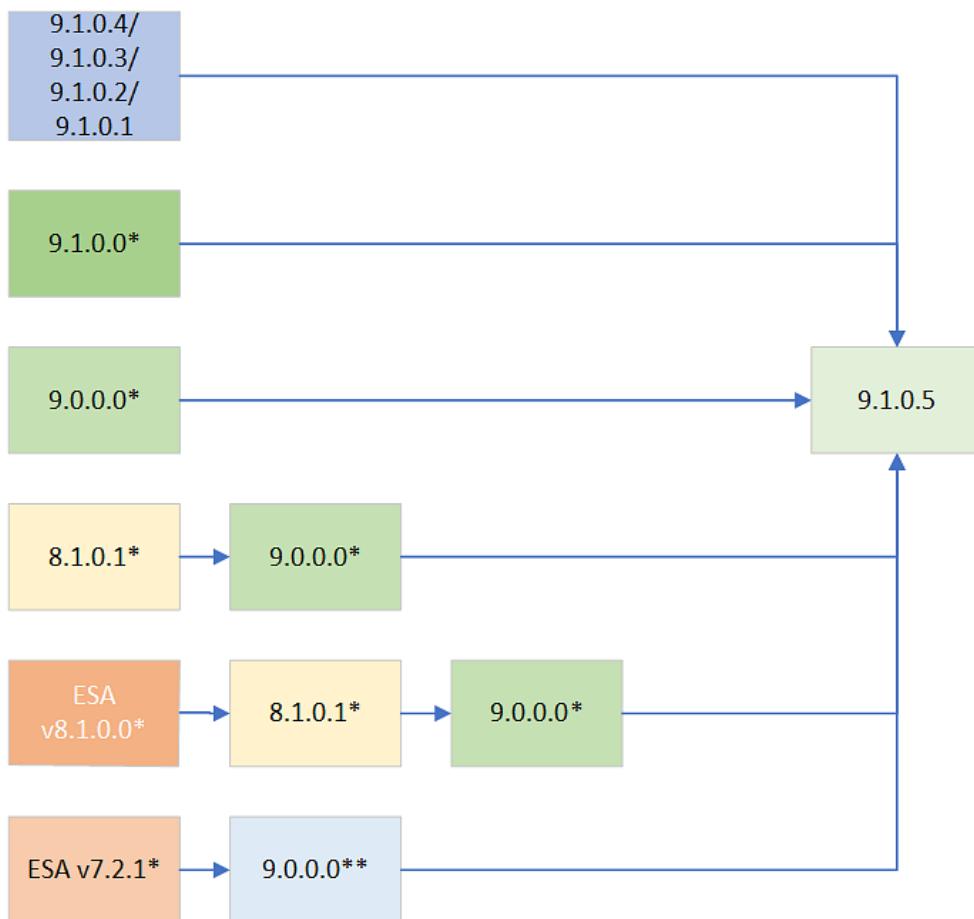
ESA Version	Supported Protector Versions
9.1.0.5	<ul style="list-style-type: none">• 9.1.0.0• 9.0.0.0• 8.1.0.0• 8.0.0.0

Chapter 4

Upgrade Paths to ESA v9.1.0.5

You can upgrade to the ESA v9.1.0.5 from any version, starting from v7.2.1 through v9.1.0.4. The following table provides the recommended upgrade paths to the ESA v9.1.0.5.

The following figure illustrates the supported paths for upgrading the ESA to v9.1.0.5.



Caution: * indicates all the available hotfix and security patches on the platform version.

** indicates the *pre-v9.0.0.0* patch. This is an intermediate step while migrating from v7.2.1 to v9.0.0.0. This *pre-v9.0.0.0* patch should not be used for upgrading to any other version.

Figure 4-1: Upgrade Paths to ESA v9.1.0.5

For example, to upgrade from the ESA v8.1.0.1 to the ESA v9.1.0.5, you must upgrade as follows:

1. ESA v8.1.0.1
2. ESA v9.0.0.0



3. ESA v9.1.0.5

Note: For more information about upgrading the ESA to v9.1.0.5, refer to the section [Upgrading to v9.1.0.x](#).

Note:

Before you install any patch, including Feature Enhancements (FE), Hot Fixes (HF), or Security Enhancements (SE), ensure to refer the [Release Notes](#) for the respective patch.

The specific requirements regarding the Trusted Appliances Cluster (TAC) and High Availability (HA) are listed in the respective [Release Notes](#) for the patch.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Table 4-1: Upgrade Path to the ESA v9.1.0.5

Current Version	Path to Upgrade the ESA to v9.1.0.5	Path to Upgrade the ESA to v9.1.0.5 (with the DSG installed)
9.1.0.4	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
9.1.0.3	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
9.1.0.2	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
9.1.0.1	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
9.1.0.0	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
9.0.0.0	Install the v9.1.0.5 patch	<ol style="list-style-type: none"> Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
8.1.0.1	<ol style="list-style-type: none"> Migrate to v9.0.0.0 Install the v9.1.0.5 patch 	<ol style="list-style-type: none"> Migrate to v9.0.0.0 Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
8.1.0.0	<ol style="list-style-type: none"> Install the v8.1.0.1 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch 	<ol style="list-style-type: none"> Install the v8.1.0.1 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch
7.2.1 Hotfix-x	<ol style="list-style-type: none"> Installing the pre-v9.0.0.0 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch 	<ol style="list-style-type: none"> Installing the pre-v9.0.0.0 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch
7.2.1 Dev-x	<ol style="list-style-type: none"> Installing the pre-v9.0.0.0 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch 	<ol style="list-style-type: none"> Installing the pre-v9.0.0.0 patch Migrate to v9.0.0.0 Install the v9.1.0.5 patch Install the DSG 3.1.0.5 patch



Current Version	Path to Upgrade the ESA to v9.1.0.5	Path to Upgrade the ESA to v9.1.0.5 (with the DSG installed)
7.2.1 SE-x		
7.2.1		

Note: On the ESA Web UI, navigate to **System > Information**, to view the current patch installed on the ESA. Navigate to the **About** page to view the current version of the ESA.

Chapter 5

Upgrading to v9.1.0.x

- [5.1 Upgrading ESA from v7.2.1](#)
- [5.2 Upgrading from v9.x.0.0 to v9.1.0.x](#)
- [5.3 Upgrading from v9.1.0.x to v9.1.0.5](#)
- [5.4 Upgrading Protectors](#)

This section describes the procedure to upgrade to the ESA v9.1.0.5, 9.1.0.4, 9.1.0.3, v9.1.0.2, and v9.1.0.1.

The list of available patches for the v9.1.0.x release is as follows.

Table 5-1: List of v9.1.0.x patches

Version	Patch
9.1.0.5	<i>ESA_PAP-ALL-64_x86-64_9.1.0.5.2242-UP.pty</i>
9.1.0.4	<i>ESA_PAP-ALL-64_x86-64_9.1.0.4.2204-UP.pty</i>
9.1.0.3	<i>ESA_PAP-ALL-64_x86-64_9.1.0.3.2168-UP.pty</i>
9.1.0.2	<i>ESA_PAP-ALL-64_x86-64_9.1.0.2.2164-UP.pty</i>
9.1.0.1	<i>ESA_PAP-ALL-64_x86-64_9.1.0.1.2162-UP.pty</i>

Note: If you are working with the certificates, then due to the security enhancement for the latest browser versions, the *KeyUsage* parameter must be configured. Ensure that *KeyUsage=Digital Signature* parameter is *Enabled* for the certificates.

5.1 Upgrading ESA from v7.2.1

This section describes the steps for upgrading the ESAs. In this upgrade process, an intermediate patch is applied on the ESA v7.2.1, then the configurations on the ESA are exported from v7.2.1 and imported on the ESA v9.0.0.0, which is then upgraded to the ESA v9.1.0.x.

The following figure illustrates a sample TAC environment on which the ESAs must be upgraded to v9.1.0.x.

Note: Ensure that at least two ESAs are in a TAC.

Ensure that you do not make any changes to configuration, policy, or CoP during the upgrade process.

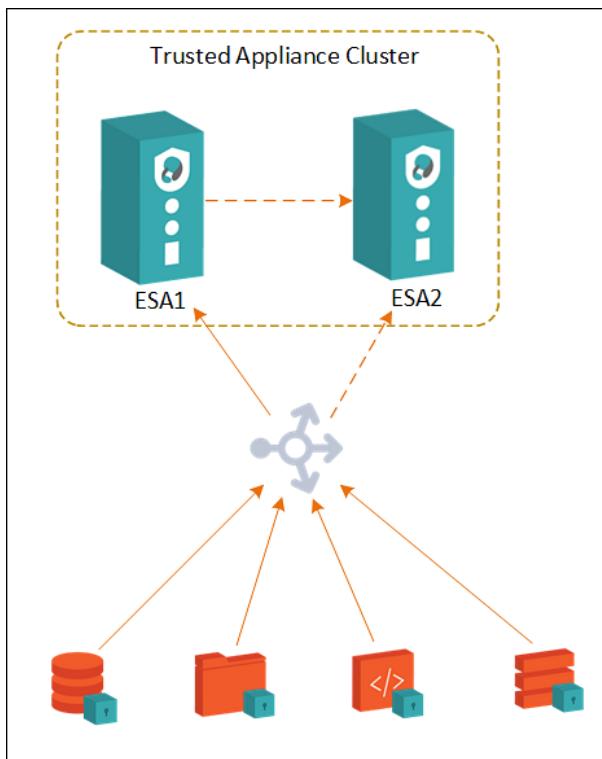


Figure 5-1: ESA v7.2.1 in a TAC

As shown in the setup,

1. The TAC contains an ESA 1 and ESA 2.

Note: Ensure that there is at least one server node in the TAC.
2. Data replication for policies, forensics, or DSG configurations takes place from the ESA 1 to the ESA 2.
3. Protectors communicate with the load balancer that balances the requests between the ESA 1 and the ESA 2.

The following figure illustrates the setup after the upgrade process is completed.

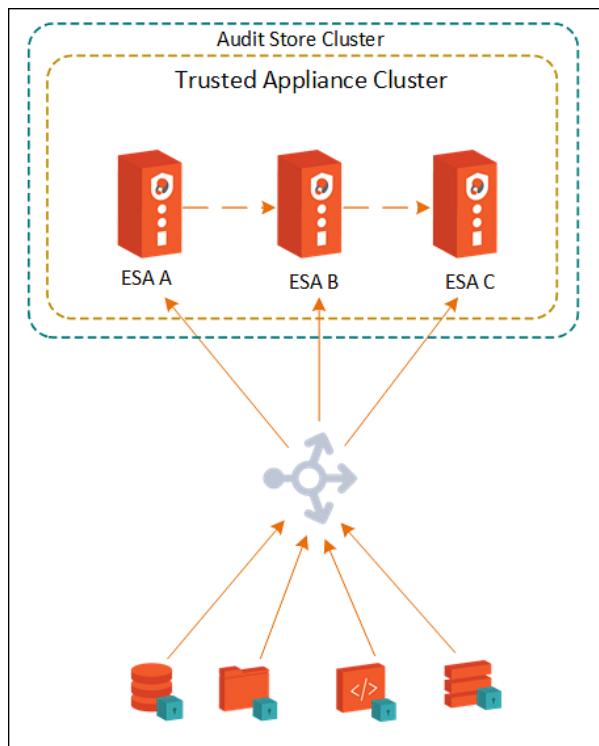


Figure 5-2: ESA v9.1.0.x in a TAC

1. The TAC is established between the ESA A, ESA B, and ESA C.
2. Data replication for policies, forensics, or DSG configurations take place from the ESA A to the ESA B and ESA C.
3. The Audit Store cluster is enabled for the ESAs.
4. Protectors communicate with the load balancer that balances the requests between the upgraded ESA A, ESA B, and ESA C.

5.1.1 Upgrade Process: Flow Diagram

The legend describes the elements used in the upgrade process.

Legend

Icon	Description	Version
	ESA Node appliance File System: Reiser FS	v7.2.1
	ESA Node appliance File System: Reiser FS	v7.2.1

Icon	Description	Version
 ESA Pre-v9.0.0.0	ESA Node appliance Updated to pre-v9.0.0.0 by applying the <i>ESA_PAP-ALL-64_x86-64_8.1.0.0.2095.UP-2.pty</i> patch	Pre-v9.0.0.0
 ESA A	ESA Node appliance (Server) File System: Ext4 FS	v9.1.0.x
 ESA B	ESA Node appliance File System: Ext4 FS	v9.1.0.x
 ESA C	ESA Node appliance File System: Ext4 FS	v9.1.0.x
	Trusted Appliances Cluster	<ul style="list-style-type: none"> • v7.2.1 • v9.1.0.x
	Audit Store Cluster	v9.1.0.x
	Protectors	<ul style="list-style-type: none"> • v7.2.1 • v9.1.0.x

Icon	Description	Version
	Load Balancer	N/A

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

5.1.2 Upgrade Process: Step-by-step Procedure

To upgrade the ESA appliances from v7.2.1 to v9.1.0.x, you must first install an intermediate patch on the v7.2.1 machine. After the pre-patch is successfully installed, you must export the configurations, rulesets, or settings to a file. These configurations, rulesets, or settings must be imported on the ESA v9.0.0.0. After the import is successfully completed, the ESA is upgraded to v9.1.0.x. Perform the required steps to complete the upgrade.

This section describes the procedure to upgrade the ESA v7.2.1 to v9.1.0.x.

Note:

Ensure that you perform the procedure in the prescribed sequence for a successful upgrade.

Before you begin

- At least two ESAs must be in a TAC on v7.2.1.
- The TAC must have at least one appliance as the *server* node.

For more information on the trusted appliance cluster, refer to the section *Trusted Appliances Cluster* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

- From the v7.2.1, the file system is changed from the *ReiserFS* to the *Ext4* file system, the *Buster OS* is upgraded, and *python2* is upgraded to *python3*. Therefore, install an additional ESA v9.0.0.0, that is, ESA A.

For more information on installing the v9.0.0.0 on a new machine, refer to the section *Installing ESA on-premise* in the [Protegility Installation Guide 9.0.0.0](#).

- Install two additional ESAs on v9.1.0.x, that is, ESA B and ESA C.

For more information on installing the v9.1.0.x on a new machine, refer to the section *Installing ESA on-premise* in the [Protegility Installation Guide 9.1.0.5](#).

- You must not make any changes to configuration, policy, or CoP on any appliance during the upgrade process.
- Ensure that the [Prerequisites](#) are met before beginning the upgrade process.

For more information on the prerequisites, refer to the section [Prerequisites](#).

- ▶ To upgrade the ESA to v9.1.0.x:

1. Ensure that the ESA 1 and ESA 2 in the TAC are in sync and have the latest policies and configurations.

Note: In the TAC, ensure that one *server* node remains in the cluster.

2. Create the ESA A on v9.0.0.0.

For more information on installing the v9.0.0.0 on a new machine, refer to the section *Installing ESA on-premise* in the [Protegility Installation Guide 9.0.0.0](#).

3. Delete the cluster scheduler tasks between the ESA 1 and the ESA 2.

For more information about deleting a cluster task, refer to the section *Scheduling Appliance Tasks* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

4. Remove the ESA 1 from the TAC.

Caution:

Before leaving the TAC, ensure that one *server* node remains in the cluster.

For more information about leaving a TAC, refer to section *Removing a Node from the Cluster using Web UI* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

5. To upgrade ESA 1 from v7.2.1 to pre-v9.0.0.0, perform the following steps on the ESA 1.

- a. Upgrade to the pre-v9.0.0.0 patch by installing the *ESA_PAP-ALL-64_x86-64_8.1.0.0.2095.UP-2.pty* patch.

For more information about installing the pre-v9.0.0.0 patch, refer to the section [Upgrading ESA to Pre-v9.0.0.0](#).

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the *Release Notes* of the respective patch.

- b. Complete the upgrade on the ESA 1.

For more information about the completing the upgrade, refer to the section [Post Upgrade Steps on version Pre-v9.0.0.0](#).

- c. Restart the ESA 1.

- d. From the ESA 1, export all the configurations, policy data, custom configurations, and so on, to a file using **Backup & Restore** functionality.

For more information on exporting a file, refer to the section [Migrating the ESA to v9.0.0.0](#).

Caution:

After the export is completed, you must not change any configurations on the ESA.

6. Transfer the exported file to the ESA A using your preferred method, such as, FTP, SCP, and so on.

Note:



If you are using the FTP or SCP, then ensure that the exported file is placed in the `/opt/product_exports` directory and permissions for the file are set to `755`.

7. Import the configurations, policy data, and custom configurations on the ESA A.
For more information about importing the configurations, policy data, and custom configurations, refer to the [Protegility Appliances Overview Guide 9.1.0.5](#).
8. After the file is successfully imported on the ESA A, configure the required settings on the ESA A.
For more information about configuring the required settings, refer to the section [Configuring the ESA v9.0.0.0](#).
9. Upgrade the custom files to `python3`.
10. On ESA A, open the ports `9200` and `9300`.
11. On ESA A, add the `ES Admin` and `Insight Admin` permissions to the `Security Administrator role`.
12. Upgrade the ESA A to v9.1.0.x patch by installing the 9.1.0.x patch.

Note: For more information about the 9.1.0.x patch, refer to the [Release Notes](#) of the respective release.

For more information about upgrading the ESA v9.0.0.0 to ESA v9.1.0.x, refer to the section [Installing the ESA v9.1.0.x Patch](#).

13. Restart the ESA A.
14. Rotate the Audit Store certificates on ESA A.
For more information about rotating the audit store certificates, refer to the section [Rotating Certificates on a Single Node Audit Store Cluster](#).
15. Create the ESA B and ESA C on v9.1.0.x.
For more information on installing the ESA v9.1.0.x on a new machine, refer to the [Protegility Installation Guide 9.1.0.5](#).
16. Join the ESA A, ESA B, and ESA C in a Trusted Appliance Cluster.
For more information on creating a TAC, refer to the section [Trusted Appliances Cluster \(TAC\)](#) in the [Protegility Appliances Overview Guide 9.1.0.5](#).
17. Configure the ESA v9.1.0.x to recreate the `local OS users`. Additionally, change the permissions of the files that are owned by `local OS users`.
18. To configure the Audit Store Cluster on the ESA A, ESA B, and ESA C, perform the following steps.
 1. Initialize the Audit Store Cluster on the ESA A.
For more information about initializing the Audit Store cluster on the ESA A, refer to the section [Initializing the Audit Store Cluster on the ESA](#).
 2. Add the ESA A, ESA B, and ESA C to the Audit Store Cluster.

Note:

Ensure that you add one appliance at a time. After adding the appliance, wait till the cluster becomes stable. The cluster is stable when the cluster status indicator turns green.

3. Configure the `td-agent` on the ESA A, ESA B, and ESA C in the Audit Store cluster.
For more information about configuring the `td-agent`, refer to the section [Configuring td-agent in the Audit Store Cluster](#).
19. Migrate the DMS logs to the Audit Store cluster from the ESA 1 to the ESA C.
20. After the migration is successfully completed, shut down the ESA 1.
21. Redirect the traffic from the ESA 2 to the ESA A, ESA B, and ESA C.
22. Upgrade the DSGs to their latest version.



23. Perform the following steps on the ESA 2.

- a. To migrate the DMS logs without upgrading the ESA 2 to pre-v9.0.0.0, you must install the *ESA_PAP-ALL-64_x86-64_7.2.1.1773.FE-1.pty* patch on the ESA 2.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

For more information about installing the patch, refer to the section [Upgrading ESA to Pre-v9.0.0.0](#).

- b. Configure the *td-agent* on the ESA 2 to point to ESA A.

For more information about configuring the *td-agent*, refer to the section [Configuring td-agent in the Audit Store Cluster](#).

- c. From the ESA 2, migrate the DMS logs to the Audit Store cluster.

For more information about migrating the DMS logs to the Audit Store cluster, refer to the section [Migrating Logs](#).

Important:

Ensure that the data migration is completed before proceeding to the next step.

24. After the migration is successfully completed, shut down the ESA 2.

5.1.3 Installing ESA

You can install the ESA on-premise or a cloud platform, such as, AWS, Azure, or GCP. When you upgrade from a previous version, the ESA is available as patch. The following are the different ways of installing the ESA:

- **ISO Installation:** This installation is performed for an on-premise environment where the ESA is installed on a local system using an ESA ISO is provided by Protegility. The installation of the ISO begins by installing the hardened version of Linux on your system, setting up the network, and configuring date/time. This is then followed by updating the location, setting up OS user accounts, and installing the ESA-related components.

For more information about installing the ESA using ISO, refer to the section [Installing the ESA On-Premise](#) in the [Protegility Installation Guide 9.1.0.5](#).

- **Cloud Platforms:** On Cloud platforms, such as, AWS, Azure, or GCP, the ESA images for the respective cloud are generated and provided by Protegility. In these images, the ESA is installed with specific components. You must obtain the image from Protegility and create an instance on the cloud platform. After creating the instance, you run certain steps for finalizing the installation.

For more information about installing the ESA on cloud platforms, refer to the section [Installing Appliances on Cloud Platforms](#) in the [Protegility Installation Guide 9.1.0.5](#).

Note: A temporary license is provided by default when you first install the Appliance and is valid for 30 days from the date of this installation. To continue using Protegility features, you have to obtain a validated license before your temporary license expires.

For more information about licensing, refer to [Protegility Data Security Platform Licensing Guide 9.0.0.0](#).

5.1.4 Prerequisites

This section describes the prerequisites which must be performed for upgrading the ESA from v7.2.1 to v9.1.0.x.

5.1.4.1 Accounts

The administrative account used for upgrading the ESA must be active.

Note:

Ensure to make a note of the required OS level user while moving from the ESA v7.2.1 to v9.1.0.x. These users are not exported as a part of the migration process. After moving to the ESA v9.1.0.x, you must create the OS level users.

For more information about the OS level users, refer to the section *OS Users in Appliances* in the *Protegility Appliances Overview Guide 9.1.0.5*.

5.1.4.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a backup of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

5.1.4.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

- To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

5.1.4.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

5.1.4.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before initiating the upgrade process.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)



- Microsoft Azure

For more information about creating the snapshots from the respective cloud platforms, refer to the [Protegility Appliances Overview Guide 9.1.0.5](#).

5.1.4.3 Installations and Hardware Requirements

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

- You must have at least one ESA on v9.0.0.0.
- You must have two ESAs on v9.1.0.x.

The used space in the OS(/) partition should not be more than 60%. If the used space is more than 60%, then you must clean up the OS(/) partition before proceeding with the patch installation process. For more information about cleaning up the OS(/) partition, refer to <https://my.protegility.com/knowledge/ka04W00000nSxJQAU/>.

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

Installation Requirements

- Two ESAs v7.2.1 must be available.
- The *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.pty* patch file is available.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

- The Pre-v9.0.0.0 *ESA_PAP-ALL-64_x86-64_8.1.0.0.2095.UP-2.pty* patch file is available.
- The *ESA_PAP-ALL-64_x86-64_7.2.1.1773.FE-1.pty* patch file is available.

5.1.4.4 High Availability (HA)

If you are upgrading an ESA appliance that is in an HA setup, then you must remove the HA services from the ESA appliance and then apply the upgrade patch.

For more information about removing the HA services, refer to the [Scalability and Availability Guide 7.2.1](#).

Note:

The HA services are not supported from version 8.0.0.0. If you continue using the HA services, then it might break the functionality of the system.

For more information about the alternate to HA services, refer to the [Fault Tolerance Guide 8.0.0.0](#) on the [My.Protegility](#) portal.

5.1.4.5 Trusted Appliances Cluster (TAC)

At least two ESAs must be in a Trusted Appliance Cluster.

For more information about the Trusted Appliances Cluster, refer to the section *Trusted Appliances Cluster* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

5.1.4.6 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the [Protegility Key Management Guide 9.1.0.0](#).

5.1.4.7 ESA Settings

Ensure to make a note of the required settings while moving from the ESA v7.2.1 to v9.1.0.x. These settings are not exported as a part of the migration process. After moving to the ESA v9.1.0.x, you must configure the following settings as a part of the post upgrade steps:

- SMTP Settings
- Scheduled tasks
- User notifications on dashboard, if any
- Local_admin permissions
- Service Account Passwords
- OS Users
- Add/Remove services
- SNMP configuration
- Preferences Settings
- Antivirus options and settings
- Open ports

5.1.4.8 Creating a Metering Backup File

Ensure that you create a backup file of the metering logs before performing the upgrade on the ESA v7.2.1.

► To create a backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility` directory using the following command.
`cd /opt/protegility/`
4. Create a temporary directory to save the metering logs using the following command.
`mkdir <directory_name>`

Note: Ensure that the temporary directory is accessible on the ESA v7.2.1. This directory must not be copied or moved to another location.

5. Add permissions to the temporary directory using the following command.
`chmod 755 <directory_name>`
6. Change the owner of the temporary directory to *service admin* using the following command.
`chown service_admin.service_admin <directory_name>`
7. Navigate to the temporary directory using the following command.
`cd <directory_name>`

8. Create the backup file of the metering logs using the following command.

```
/opt/protegility/repository/pim/pgsql/bin/pg_dump -h localhost -U admin -p 5211 --schema metering --format=c ADMINDB > /opt/protegility/<directory_name>/<backup_filename>.bak
```

5.1.4.9 Customized Files (Configuration Files and Certificates)

Exclude Files

The *exclude* file present in the */opt/ExportImport/filelist* directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section *Exporting Custom Files* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Custom files with python2 scripts

If you have modified any custom files, such as, *check_password.py*, *check_username.py*, *pty_get_username_from_certificate.py*, and so on, then these must be listed in the *customer.custom* file.

CloudWatch Files

To export the *CloudWatch* configurations, you must list the cloudwatch configurations in the *customer.custom* file to export the data in the upgraded ESA.

5.1.4.10 Logging, Reporting, and Certificates

If you are upgrading an ESA appliance that has scheduled tasks or cluster replication tasks created by the user, then ensure that DMS options, such as, *Log-Server Repository*, *Log-Server Configuration*, and *Log-Server Event Configuration*, reporting tasks, and certificates are disabled.

Note:

If a scheduled task has scheduled tasks or cluster replication tasks created by the user, such as, the *Logging*, *Reporting*, and *Certificates* components, then uncheck them and update the scheduled task.

If there are preconfigured scheduling tasks, such as, *100 DBIntegrity Logging-Repository Integrity Check (Once a week)*, then they are automatically disabled.

A notification will be displayed on the ESA Web UI dashboard.

The following scheduled tasks were disabled due to Log Server migration: [100]

Note:

The DMS, reporting server, and DMS2mail services are not supported from version 8.0.0.0 onwards.

5.1.4.11 License

Ensure that you have a valid license before upgrading.

Note:

After migration, if the license status is *invalid*, then contact *Protegility Support*.

5.1.5 Upgrading ESA to Pre-v9.0.0.0

This section describes the steps to upgrade from the ESA to Pre-v9.0.0.0.

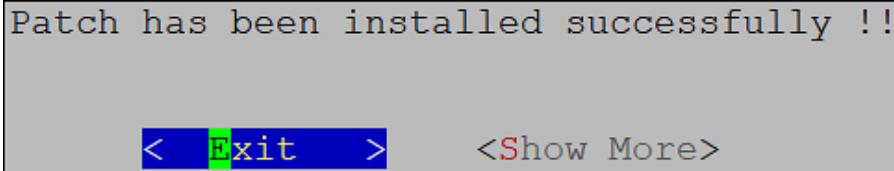
1. Login to the ESA CLI Manager with administrator credentials.
2. Navigate to **Administration > OS Console** to upload the patch.
3. Upload the patch to the `/products/uploads` directory using the FTP or SCP command.
4. Navigate to **Administration > Patch Management** to install the patch.
5. Enter the *root* password.
6. Select **Install a Patch**.
7. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.0.2095.UP-2.pty* patch file and select **Install**.

Note:

Ensure that you download the latest patch from the *My.Protegility* portal.

For more information about the latest build number and the patch details, refer to the *Release Notes* of the respective patch.

8. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the Pre-v9.0.0.0.

5.1.6 Post Upgrade Steps on version Pre-v9.0.0.0

This section describes the steps that must be performed on the ESA after successfully upgrading the ESA from v7.2.1 to version Pre-v9.0.0.0.

Note:

After installing the patch successfully, you must not change any configurations on the ESA.

5.1.6.1 Restarting the ESA

After you upgrade, restart the ESA to complete the upgrade.

► To restart the ESA:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Reboot and Shutdown > Reboot**.
The Reboot screen appears.
3. Type the reason and select **OK**.

5.1.6.2 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. `/var/log`
 - *Installation.log* - Provides the logs for all the installed components.
 - *syslog* - Provides collective information about the syslogs.
2. `/etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log`

5.1.6.3 Restoring the Backup File of the Metering Logs

A backup of the metering logs is required on the ESA Pre-v9.0.0.0 in the `/opt/protegility/` directory during the upgrade. This file is required for the migration of the metering logs.

Note: If the backup file of the metering logs is available in the directory, then skip this section.

For more information about the creating the backup file of the metering logs, refer to the section [Creating a Metering Backup File](#).

► To restore the backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility/` directory using the following command.
`cd /opt/protegility/`
4. Restore the backup file of the metering logs using the following command.
`cp <backup_filename>.bak /opt/protegility/hubcontroller/`

5.1.6.4 Verifying the Patch Installation

After upgrading to the ESA Pre-v9.0.0.0, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_8.1.0.0 UP-2* patch name appears.

Ensure to check the Logs to verify that there are no errors.

5.1.7 Migrating the ESA to v9.0.0.0

This section describes the procedure for migrating the data from the ESA Pre-v9.0.0.0 to ESA v9.0.0.0.

Caution: Ensure to export the configuration files from the CLI Manager only.

Note: Ensure that you perform the procedure in the prescribed sequence listed in the section [Upgrade Process: Step-by-step Procedure](#).

5.1.7.1 Exporting Data or Configurations to a Local File

This section describes the steps to export information from the ESA Pre-v9.0.0.0 to the ESA v9.0.0.0.

► To export information to the ESA v9.0.0.0:

1. Login to the CLI Manager.
2. Navigate to **Administration > Backup/Restore Center**.
3. Enter the *root* password.
The Backup Center dialog box appears.
4. From the menu, select the **Export data/configurations to a local file** option.
5. Select the packages to export.

Note:

It is recommended to select all the options while performing the export operation.

Note:

If you want to export the configuration for the DSG, then select the *Export Gateway Configuration Files* and perform the export operation.

6. Enter the desired Export Name.
7. Specify the password for the backup file.



8. Confirm the specified password.
9. If required, then enter description for the file.
10. Click **OK**.
11. You can optionally save the logs for the export operation when the export is done. Perform the following steps to save the logs for the export operation.
 - a. Click **More Details** button.
The export operation log will display.
 - b. Click **Save** button to save the export log.
 - c. In the following dialog box, enter the export log file name.
 - d. Click **OK**.
 - e. Click **Done** to exit the *More Details* screen.

Note: The newly created configuration file will be saved into */products/exports*. It can be accessed from the CLI Manager, **Exported Files and Logs** menu.

The export log file can be accessed from the from the CLI Manager, **Exported Files and Logs** menu.

5.1.7.2 Importing Data or Configurations from a File

Upload the exported file on the *ESA A* v9.0.0.0 using your preferred method, such as, FTP, SCP, and so on.

Before you begin

Note:

If you are using the SCP or FTP, then ensure that the exported file is placed in the */opt/product_exports* directory and permissions for the file are set to *755*.

Note:

When you import files or configurations, ensure that each component is selected individually.

► To import data configurations from file:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Backup/Restore Center**.
3. Enter the root password.
The Backup Center dialog box appears.
4. From the menu, select the **Import data/configurations from a file** option.
5. In the following dialog box, select a file from the list which will be used for the configuration import.
6. Press **OK**.
7. In the following dialog box, enter the password for this backup file.
8. Select Import method.
9. Press **OK**.
10. In the information dialog box, press **OK**.

The Backup Center screen appears.

5.1.8 Installing the ESA v9.1.0.x Patch

This section describes the steps to upgrade to the ESA to v9.1.0.x by installing the respective patch.

► To install the ESA v9.1.0.x patch:

1. Login to the ESA CLI Manager with administrator credentials.
2. Navigate to **Administration > OS Console** to upload the patch.
3. Upload the patch to the */products/uploads* directory using the FTP or SCP command.
4. Navigate to **Administration > Patch Management** to install the patch.
5. Enter the *root* password.
6. Select **Install a Patch**.
7. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.pty* patch file and select **Install**.

Note: Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

8. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the v9.1.0.x.

5.1.9 Restarting the ESA

After you upgrade, restart the ESA to complete the upgrade.

► To restart the ESA:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Reboot and Shutdown > Reboot**.
The Reboot screen appears.
3. Type the reason and select **OK**.

5.1.10 Post Upgrade Steps on ESA v9.1.0.x

Ensure that the following steps in the following sections are performed after the ESA upgrade is completed:

5.1.10.1 Verifying the ESA Patch Installation

After upgrading to the ESA v9.1.0.x, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_9.1.0.x* patch name appears.

Ensure that there are no errors in the logs.

5.1.10.2 Verifying the *cron-jobs* for the Analytics

After upgrading the ESA to the latest version, ensure that the *cron-jobs* for the Analytics are available.

► To verify the *cron-jobs* for the Analytics:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Check the *cron-jobs* entry in the */var/spool/cron/crontabs/root* file using the following command.

```
cat /var/spool/cron/crontabs/root
```

4. Verify that the following entry is available.
** * * * * source /opt/protegility/insight/analytics/analytcs_venv/bin/activate ; python /opt/protegility/insight/analytics/bin/cron/insight_cron_executor.pyc > /dev/null 2>&1*
5. If the entry mentioned in step 4 is unavailable, then perform the following steps.
 - a. Create a backup of the */var/spool/cron/crontabs/root* file.
 - b. Add the *cron-jobs* entry using the following command.

```
echo '* * * * * source /opt/protegility/insight/analytics/analytcs_venv/bin/activate ; python /opt/protegility/insight/analytics/bin/cron/insight_cron_executor.pyc > /dev/null 2>&1' >> /var/spool/cron/crontabs/root
```

- c. Verify the *cron-jobs* entry in the */var/spool/cron/crontabs/root* file using the following command.

```
cat /var/spool/cron/crontabs/root
```

- d. Restart the *cron* service using the following command.

```
/etc/init.d/cron restart
```

5.1.11 Configuring Settings on v9.1.0.x

The following sections describe the steps to complete the upgrade on v9.1.0.x.

5.1.11.1 Configuring the ESA v9.1.0.x

While migrating the ESA to v9.1.0.x, the following settings are not retained. You must configure the following settings after migrating to ESA v9.1.0.x.

SMTP Settings

You must set up an email server that supports the notification features.

For more information about configuring the SMTP settings, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Scheduled Tasks

Using **System > Task Scheduler** you can schedule appliance tasks to run automatically. You can create or manage tasks from the ESA Web UI.

For more information about configuring the scheduled tasks, refer to the section *Scheduling Appliance Tasks* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Grub Settings

To enhance security of the Protegility appliances on-premise, the GRUB menu can be protected by setting a username and password. It is recommended to secure the appliance using the GRUB settings.

For more information about securing the GRUB, refer to the section *Securing the GRand Unified Bootloader (GRUB)* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Local_admin permissions

By default, the *local_admin* user cannot login to the CLI Manager using SSH or log into the Web UI. However, you can configure this access using the tool, which changes the *local_admin* account permissions.

For more information about enabling the *local_admin* permissions, refer to the section *Changing the Local Admin Account Permission* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Service Account Passwords

Service Account users are *service_admin* and *service_viewer*. They are used for internal operations of components that do not support LDAP, such as Management Server internal users and Management Server Postgres database. You cannot log into the Appliance Web UI, Reports Management (for ESA), or CLI Manager using service accounts users.

For more information about changing the service accounts passwords, refer to the section *Changing Service Accounts Passwords* in the *Protegility Appliances Overview Guide 9.1.0.5*.

OS Users

You must configure the *OS Users* on the upgraded ESA.

For more information about OS Users, refer to the section *Managing Local OS Users* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Add/Remove services

Using the **Add/Remove Services** tool, you can install the necessary products or remove already installed ones. You must add or remove the services which were present on the ESA v7.2.1.

For more information about adding or removing service, refer to the section *Add/Remove Services* in the *Protegility Appliances Overview Guide 9.1.0.5*.

SNMP configuration

SNMP allows a remote machine to query different performance status of the Appliance, such as, start the service, set listening address, show or set community string, or refresh the service.

For more information about configuring SNMP, refer to the section *Configuring SNMP* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Preferences Settings

You must set up your console preferences using the **Preferences** menu.

For more information about preferences settings, refer to the section *Working with Preferences* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Antivirus options and settings

The AntiVirus program uses ClamAV, an open source and cross-platform antivirus engine designed to detect malicious trojan, virus, and malware threats. A single file or directory, or the whole system can be scanned. Infected file or files are logged and can be deleted or moved to a different location, as required.

For more information about configuring antivirus, refer to the section *Working with Preferences* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Firewall Settings

Protegility internal Firewall provides a way to allow or restrict inbound access from the outside to Protegility Appliances.

Using the **Rules List** option, you can view the available firewall rules. Alternatively, on the Web UI, navigate to **System > Information** to view the rules.

For more information about firewall settings, refer to the section *Managing Firewall Settings* in the *Protegility Appliances Overview Guide 9.1.0.5*.

The ports in a network are communication channels through which information flows from one system to another. A list of ports that must be configured in your environment to access the features and services on the Protegility appliances.

For more information about open ports, refer to the section *Open Listening Port* in the *Protegility Appliances Overview Guide 9.1.0.5*.

5.1.11.2 Upgrading custom files to *python3*

From v9.0.0.0, the support for *python2* is disabled.

Therefore, if you have modified any of the files in the previous version of the ESA including the following, then ensure that they are compatible with *python3*:

- */etc/ksa/check_password.py*
- */etc/ksa/check_username.py*
- */etc/ksa/pty_get_username_from_certificate.py*

You can run the following command to check if these files are *python3* compatible.

```
python3 -m compileall <path_to_file>
```



5.1.11.3 Adding Permissions to the Existing Roles

Analytics and the Audit Store have roles assigned for reading and displaying the logs. Grant the required permission to the roles using the steps provided in this section.

► To add permissions to the existing roles:

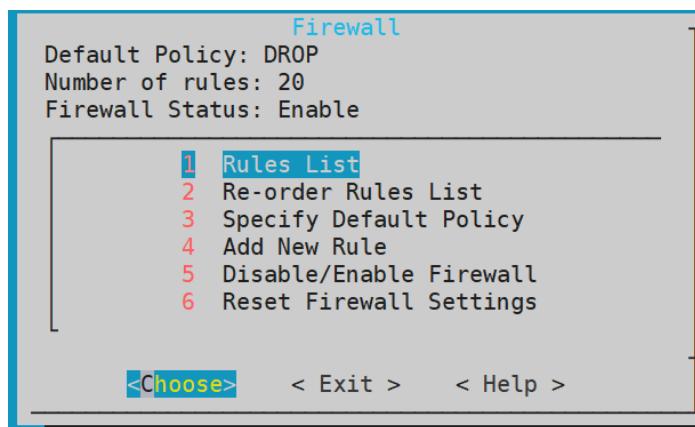
1. Login to the ESA A Web UI.
2. Navigate to **Settings > Users > Roles**.
3. Click the **Security Administrator** role.
The **Security Administrator** screen appears.
4. In the **Role Permissions and Privileges** section, select the following check boxes:
 - ES Admin
 - Insight Admin
5. Click the **Save** button.
6. Enter the password and select **OK**.
A confirmation message appears.

5.1.11.4 Opening the Ports

You must open the *9200* and *9300* ports. These ports are used by the Audit store service for the REST & cluster communications.

► To open the ports:

1. Login to the CLI Manager.
2. Navigate to **Networking > Network Firewall**.
3. Enter the *root* password.
The following screen appears.



4. Select **Add new rule**.
5. Select **Accept** and click **Next**.
6. Select **Audit Store** and click **Next**.
7. Select **ethMNG** and click **Next**.

8. Select **Any** and click **Next**.
9. Enter description and click **Confirm**.

Note:

From the **Rules List**, verify the added rule and ensure that the ports are mentioned in the allowed ports list.

5.1.11.5 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 Protegity certificate and keys. For rotating custom certificates, refer to the section *Updating Audit Store Custom Certificates* in the [Audit Store Guide 9.1.0.5](#).

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		Status	Mode	Actions
Misc						
	LDAP Server	Running	Automatic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	td-agent	Running	Automatic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Analytics	Running	Automatic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Figure 5-3: Stopping *td-agent*

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

System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Misc						
		LDAP Server		Running	Automatic	<input type="checkbox"/>
		Web-Services Engine		Running	Automatic	<input type="checkbox"/>
		Service Dispatcher		Running	Automatic	<input type="checkbox"/>
		td-agent		Stopped	Automatic	
		Analytics		Running	Automatic	<input type="checkbox"/>

Figure 5-4: Stopping Analytics

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

System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Audit Store						
		Audit Store Repository		Running	Automatic	<input type="checkbox"/>
		Audit Store Management		Running	Automatic	<input type="checkbox"/>

Figure 5-5: Stopping Audit Store Management

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

Services	Status	Mode	Actions
Audit Store Repository	Running	Automatic	[Stop] [Start]
Audit Store Management	Stopped	Automatic	[Start]

Figure 5-6: Stopping Audit Store Repository

10. Run the Rotate Audit Store Certificates tool on the system.

- 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 5-7: Rotating Certificates

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

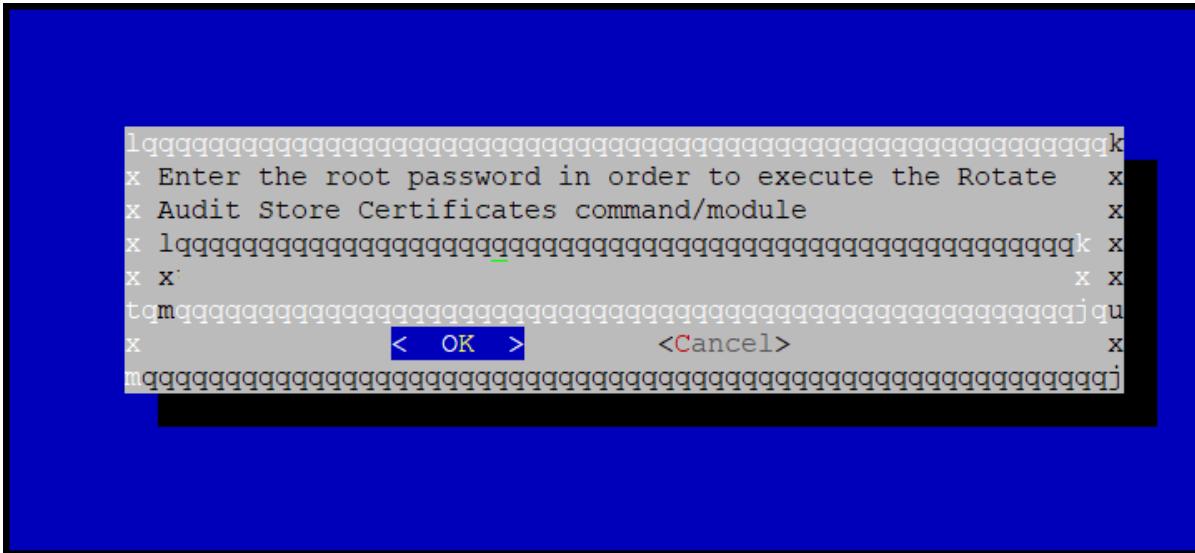


Figure 5-8: Root Password

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

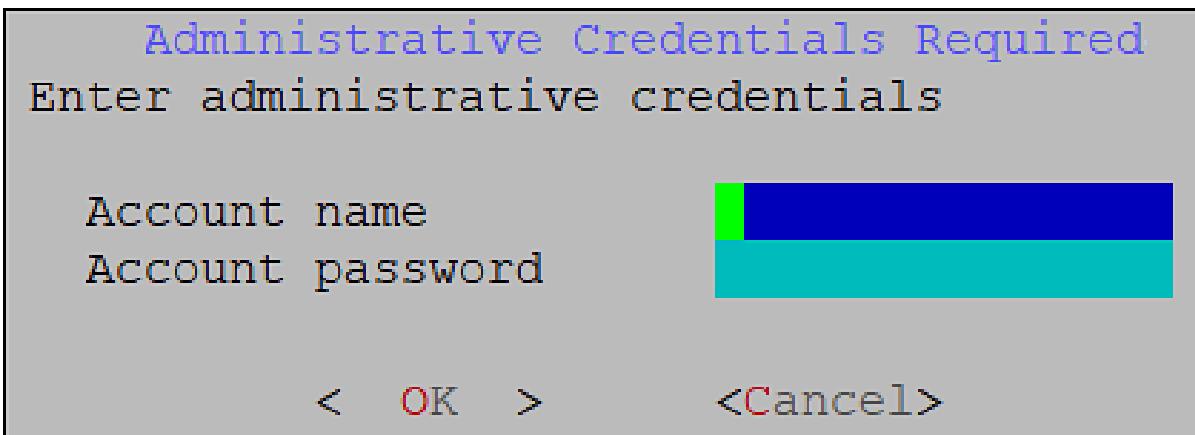


Figure 5-9: Admin Details

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

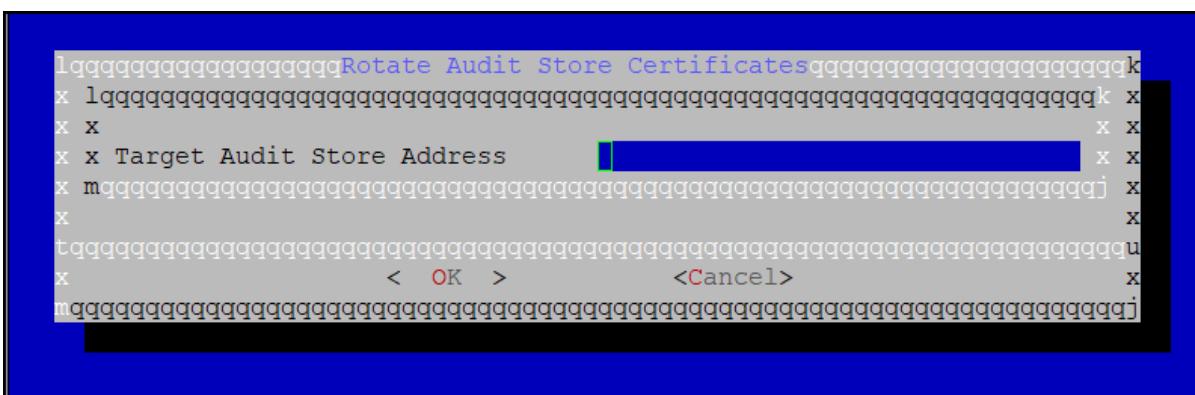


Figure 5-10: Target Audit Store Address

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

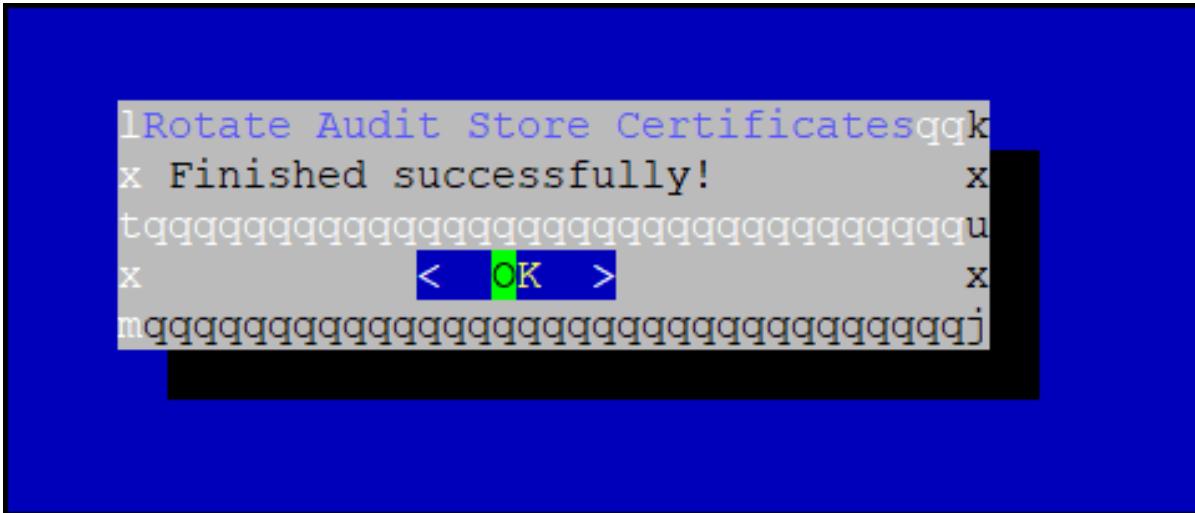


Figure 5-11: Rotation Complete

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 5-12: 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.

Figure 5-13: 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.

Figure 5-14: Services Started

5.1.12 Creating an Audit Store Cluster

The following sections describes the steps to create an Audit Store Cluster.

5.1.12.1 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, Protegility Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as,

td-agent, is started and Protegility 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.

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

The following screen appears.

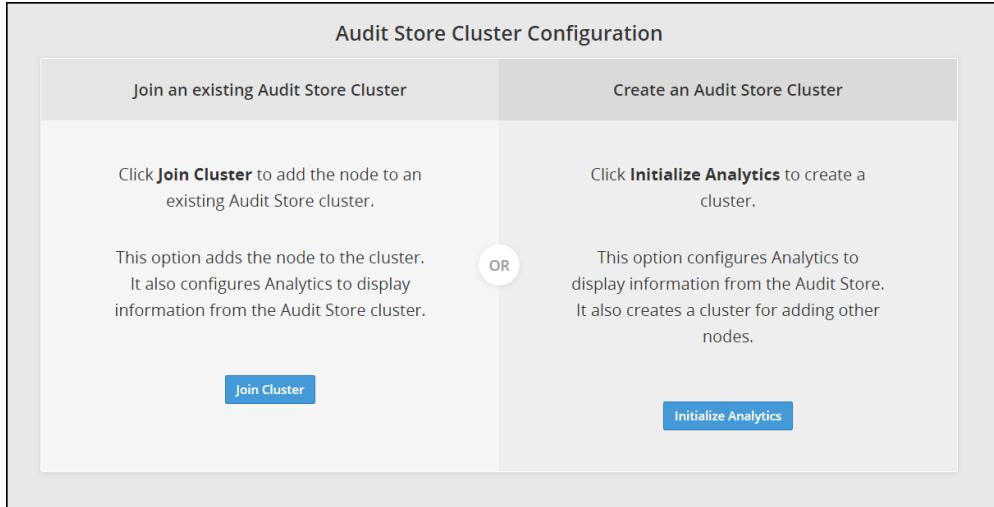


Figure 5-15: Analytics Screen

4. Click **Initialize Analytics**.

Protegility 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.

Protegility 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.

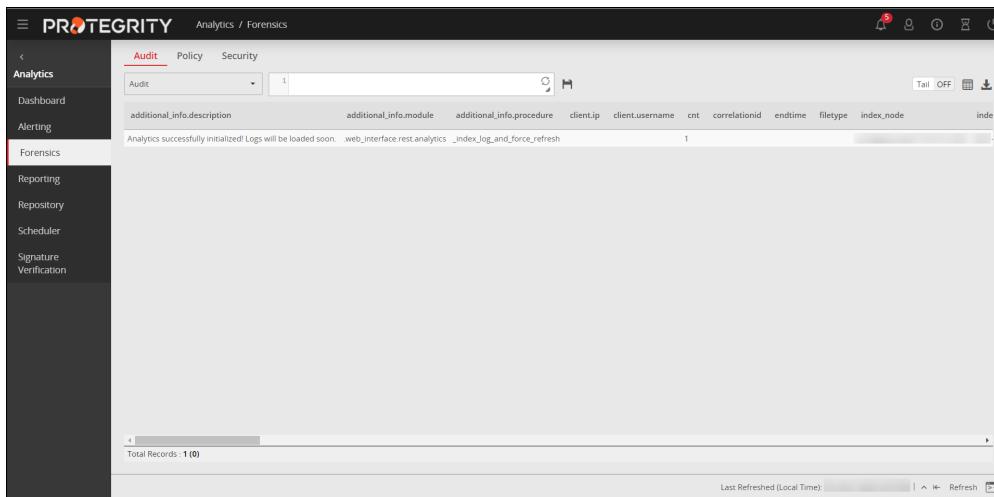


Figure 5-16: Forensics

5.1.12.2 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 [Protegility 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.



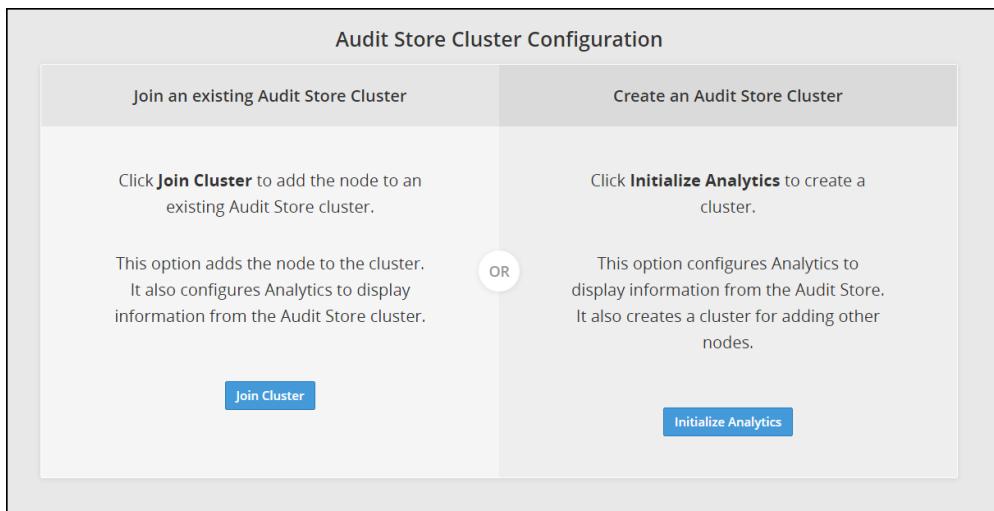


Figure 5-17: Analytics Screen

4. Click **Join Cluster**.

The following screen appears.

The dialog box is titled 'Join an existing Audit Store Cluster'. It contains fields for 'Node IP/Hostname', 'Username', and 'Password'. At the bottom, there is a checkbox for clearing cluster data and two buttons: 'Join Cluster' and 'Cancel'.

Figure 5-18: Joining an Audit Store Cluster

5. 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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](#).

6. 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.

7. 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.

Protegility 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.

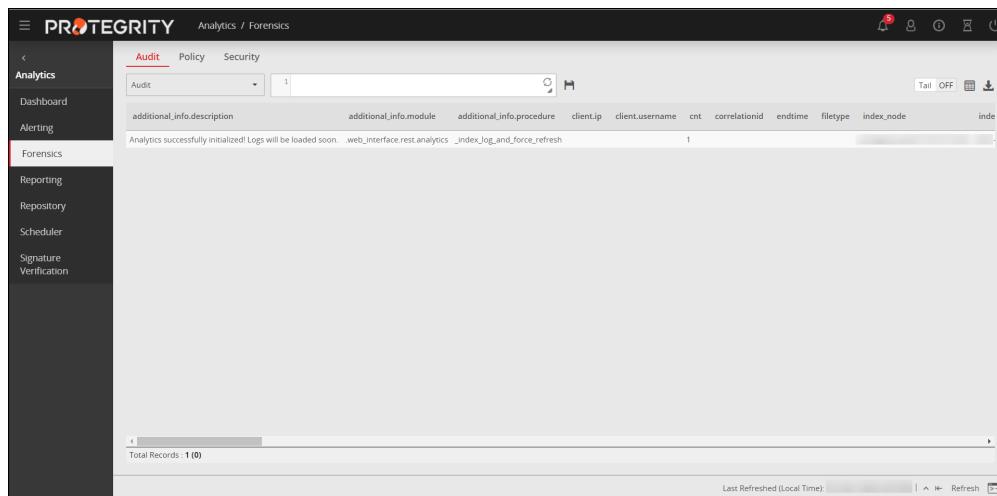


Figure 5-19: Protegility Analytics

5.1.12.3 Refreshing the Audit Store Cluster

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

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

5.1.12.4 Configuring td-agent in the Audit Store Cluster

Complete the following steps after adding the ESA node to the Audit Store cluster. This configuration is required for processing and storing the logs received by the Audit Store.

Note: This step must be performed on all the ESAs in the Audit Store cluster.

Before performing the steps provided here, verify that the Audit Store cluster health status is green on the **Audit Store Management** screen of the ESA Web UI.

1. Login to the CLI Manager of the *ESA* node.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
3. Enter the *root* password and select **OK**.
4. Enter the *username* and *password* for the administrative user, such as, *admin*.
5. Select **OK**.
6. In the *Setting ESA Communication* screen, select **OK**.
7. Specify the IP addresses of all the ESA machines in the cluster, separated by commas.



Figure 5-20: Forward Logs

8. Select **OK**.
9. Type *y* to fetch certificates for communicating with the ESA and select **OK**.

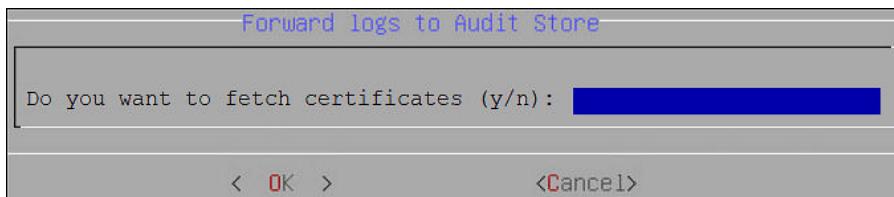


Figure 5-21: Fetch Certificates

10. Enter the *admin* username and password and select **OK**.

Repeat the steps provided in this section on all the ESAs in the Audit Store Cluster.

5.1.12.5 Verifying the Audit Store Cluster

View the Audit Store Management page to verify that the configurations that you performed were completed successfully using the steps provided here.

1. Login to the ESA Web UI.
2. Navigate to the **Audit Store Management** page.
3. Verify that the nodes are added to the cluster. The health of the nodes must be either green or yellow.
4. If you added additional ESAs for creating a TAC, then verify that the ESA has only the master role.

The screenshot shows a cluster named 'insight' with the following statistics:

- Number of Nodes:** 3
- Number of Data Nodes:** 2
- Active Primary Shards:** 17
- Active Shards:** 34
- Relocating Shards:** 0
- Initializing Shards:** 0
- Unassigned Shards:** 0
- OS Version:** 1.3.0
- Current Master:** [redacted]
- Indices Count:** 14
- Total Docs:** 212,995
- Number of Master Nodes:** 3
- Number of Ingest Nodes:** 2

The 'Nodes' tab is selected, showing a table of nodes with their IP addresses, roles (Master, Data, Ingest), and various metrics like Up Time, Disk Total, and RAM usage. One row's 'Master' column is highlighted with a red box.

Figure 5-22: Nodes Added to Cluster

5.1.13 Migrating DMS Logs and Metering Data

If your ESA is a part of the TAC setup, it is recommended to migrate your logs and metering data to Protegility Analytics to avoid data loss during upgrade. This section describes how to upgrade DMS logs and metering data from your current system to Protegility Analytics.

Note: Ensure that the backup of the metering logs is available on the ESA Pre-v9.0.0.0 in the `/opt/protegility/` directory.

If the backup file of the metering logs is unavailable, then you must restore the metering backup file.

For more information about the creating and restoring the backup file of the metering logs, refer to the sections [Creating a Metering Backup File](#) and [Restoring the Backup File of the Metering Logs](#).

5.1.13.1 Setting the Audit Store

Before you send the DMS logs to the ESA, you need to specify the Audit Store where the logs must be sent to, in this case, an ESA that is part of the Audit Store cluster in v9.1.0.x. Complete the following steps to set the Audit Store that must receive the logs.

Perform the following steps to forward logs.

1. Login to the CLI Manager on the Secondary ESA where the `ESA_PAP-ALL-64_x86-64_7.2.1.1773.FE-1.pty` patch is installed.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.

```
Tools:

Disk Management
Rotate Appliance OS Keys
-- Removable Media Management --
  Disable CD/DVD Drives
  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
```

Figure 5-23: Forwarding Logs

3. Enter the password for the `root` user and select **OK**.

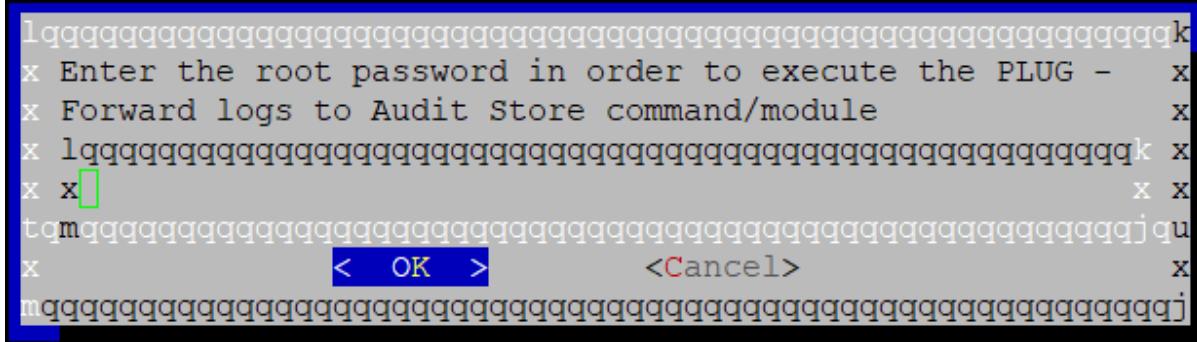


Figure 5-24: Root Password Screen

- Enter the username and password for the *admin* user and select **OK**.

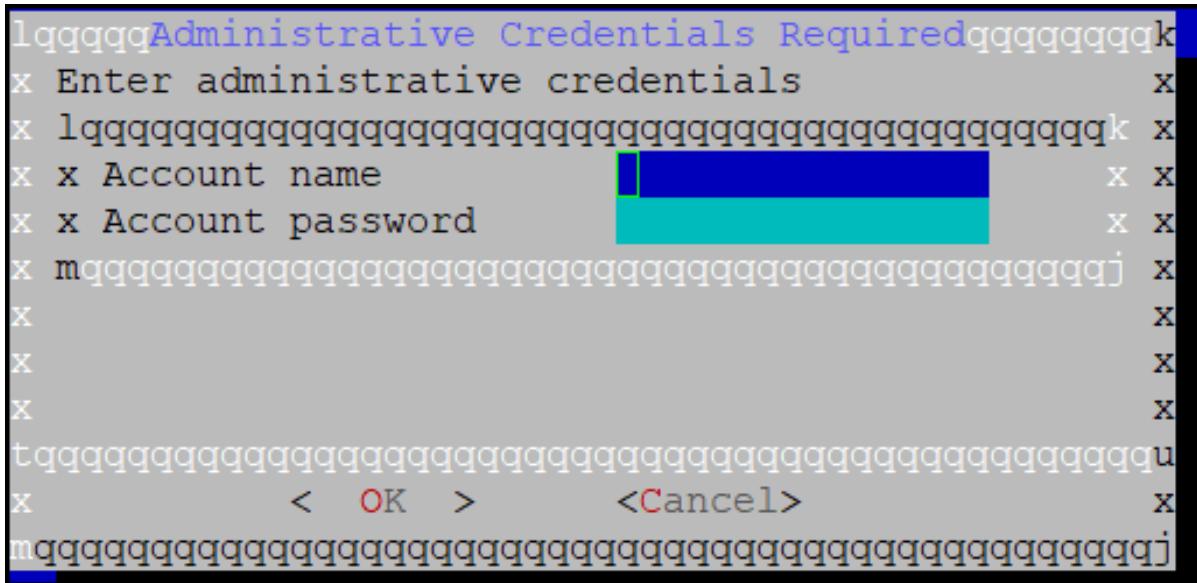


Figure 5-25: Admin Details Screen

- Select **OK**.

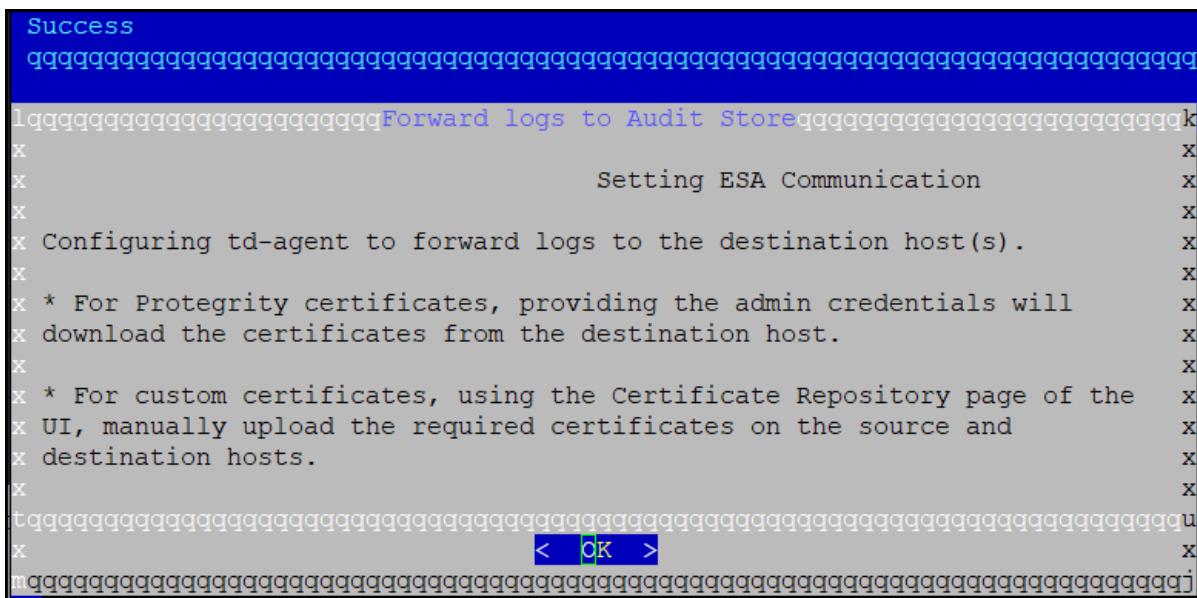


Figure 5-26: Certificates Information

- Enter the IP address of the ESA node that is a part of the Audit Store cluster of v9.0.0.0 and select **OK**.

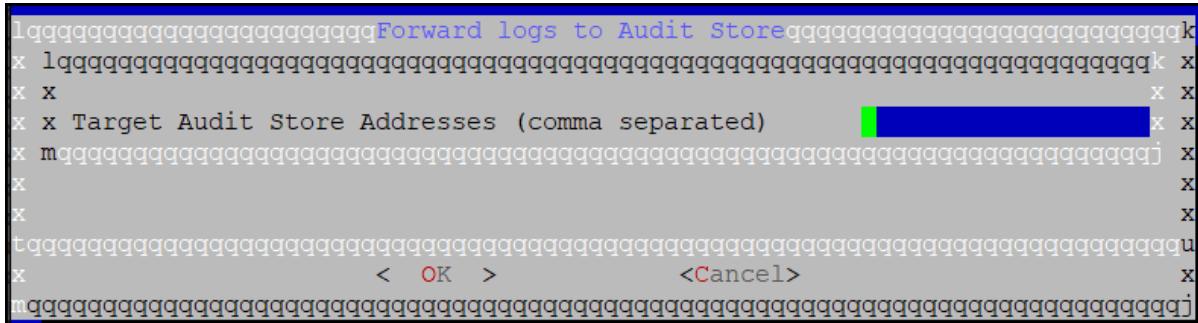


Figure 5-27: Audit Store Details

7. Enter **y** to fetch certificates and select **OK**.

Specifying `y` fetches `td-agent` certificates from target node. These certificates can then be used to validate and connect to the target node. They are required to authenticate with the Audit Store while forwarding logs to the target node.

If the certificates are already available on the system, you do not want to fetch the certificates, or you want to use custom certificates, then specify *n* on this screen.

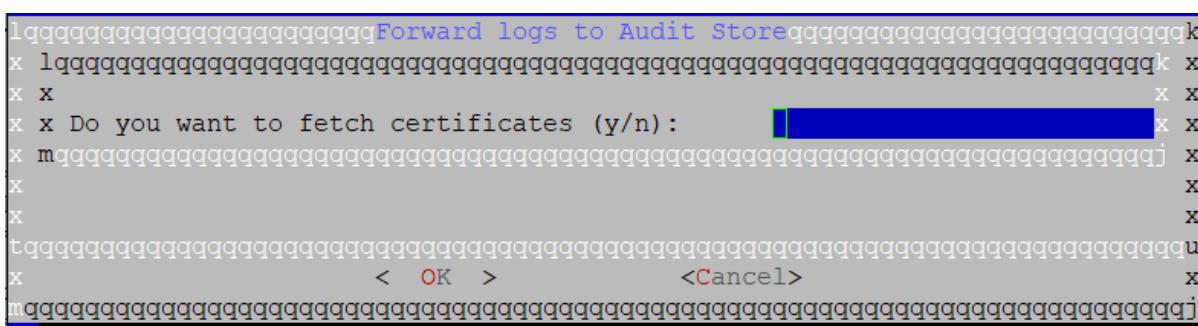


Figure 5-28: Audit Store Certificates

8. Enter the credentials for the admin user of the destination machine and select **OK**.

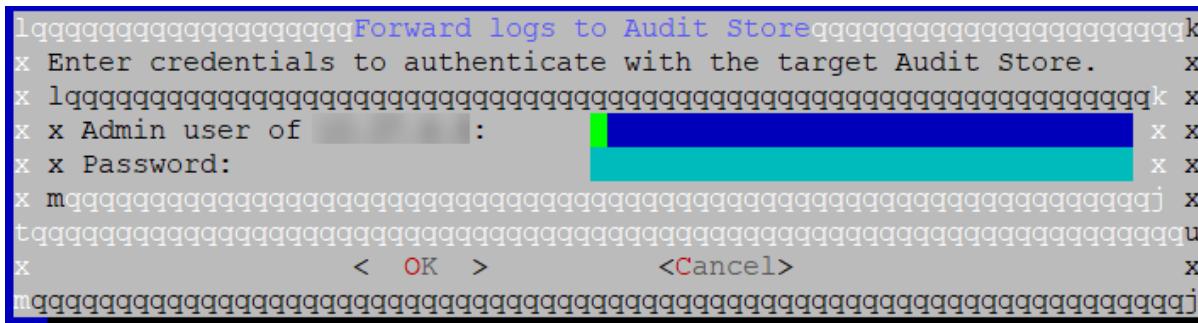


Figure 5-29: Admin User Details

The *td-agent* service is configured to send logs to the Audit Store and the CLI menu appears.

5.1.13.2 Migrating Logs

Migrate the logs from your current system to the Audit Store using the DMS Exporter. The logs are exported from the Postgres database to the Audit Store. Ensure that you import the logs that you require in the Audit Store to Postgres before you migrate the logs. Your existing archives would not be usable till they are exported to the Audit Store.

For more information about using the DMS Exporter, refer to the section [Appendix C: Migrating Logs Using the DMS Exporter](#).

Note:

It is recommended that all the logs are migrated from the current system using the DMS Exporter before performing any protect, unprotect, or reprotect operations.

Verify that the total hard disk space available is as per the following formula:

```
2 x (Total size of the Current used space + Size of the Upgrade patch)
```

For STA and LTA logs, import them back to Postgres before running the DMS Exporter. Ensure that the free space available on your system before importing STA and LTA logs is *2 times the space of the STA logs + LTA logs*. Contact Protegrity Services if you need help with migrating your STA and LTA logs.

Complete the following steps to migrate logs to the Audit Store.

1. Ensure that the steps in [Setting the Audit Store](#) are complete.
2. On the Secondary ESA where the *ESA_PAP-ALL-64_x86-64_7.2.1.1773.FE-1.pty* patch is installed, login to the CLI Manager as the root user.
3. Navigate to **Administrator > OS Console**.
4. Enter the *root* password and click **OK**.
5. Navigate to the */opt/protegrity/dms_exporter* directory.
6. Stop the DMS service using the following command:

```
dms stop
```

7. Run the following command for using the DMS Exporter.

```
python dms_exporter.pyc start
```

Note:

Use the command `python dms_exporter.pyc -h` or `python dms_exporter.pyc --help` to view the usage information for the command.

The DMS exporter sends logs in batches, where the exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store. Thus, if you have 4200000 rows, then the DMS Exporter will send rows in eight batches of 500000 rows and the ninth batch of the remaining 200000 rows.

Note:

If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the *last_imported_index* file in the */opt/protegrity/dms_exporter* directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics** in the ESA v9.0.0.0.

The logs are exported to the Audit Store. Verify that the export was successful by navigating to */var/log/dms_exporter* on the ESA and viewing the export status in the *dms_exporter.log* file.

Then, the logs can be seen on the **Forensics** tab in Protegrity Analytics of the ESA v9.0.0.0. These logs can then be used for further analysis.

5.1.14 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

5.1.14.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

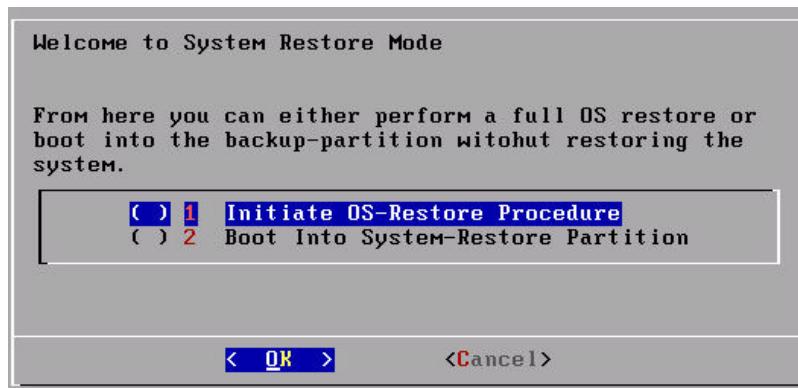
1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

5.1.14.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

5.1.14.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

5.1.14.2.2 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

5.1.14.2.3 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.



10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
 11. Enter the size of the disk in the **Size** text box.
 12. Click **Add Label** to add a label to the snapshot.
 13. Enter the label in the **Key** and **Value** text boxes.
 14. Click **Save**.
- The instance is updated with the new snapshot.

5.2 Upgrading from v9.x.0.0 to v9.1.0.x

This section describes the steps to upgrade the ESA to the latest compatible version.

Note: Ensure that you upgrade the ESA prior to upgrading the protectors.

Note: This section is applicable only if you are upgrading the ESA from v9.0.0.0 or v9.1.0.0 to the ESA v9.1.0.1, v9.1.0.2, 9.1.0.3, v9.1.0.4, or 9.1.0.5.

5.2.1 Prerequisites

The prerequisites for upgrading the ESA to the latest version must be performed.

5.2.1.1 Accounts

The *local admin* account used for upgrading the ESA must be active.

Ensure that the local administrator user has access to the CLI Manager and Web UI. Navigate to **Administration > Accounts And Passwords > Manage Passwords And Local-Accounts > Change OS 'local_admin' account permissions** to set the local administrator permissions.

5.2.1.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a back up of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

5.2.1.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

5.2.1.2.2 Exporting Data/Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration:

► To export data configurations to a remote appliance:

1. Log in to the CLI Manager
2. Navigate to **Administration > Backup/Restore Center**.
3. Enter the *root* password and select **OK**.
The Backup Center dialog box appears.
4. From the menu, select the **Export data/configurations to a remote appliance(s)** option and select **OK**.
5. From the **Select file/configuration to export** dialog box, select **Current (Active) Appliance Configuration package to export** and select **OK**.
6. In the following dialog box, **Select the packages to export** and select **OK**.
7. Select the **Import** method.
For more information on each import method, select **Help**.
8. Type the **IP address or hostname for the destination** appliance.
9. Type the administrative credentials of the remote appliance and select **Add**.
10. In the information dialog box, press **OK**.
The Backup Center screen appears.

Note: Do not import all network settings to another machine since it will create two machines with the same IP in your network. It is recommended to restart the appliance after receiving an appliance core configuration backup.

This item shows up only when exporting to a file.

5.2.1.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before upgrading to v9.1.0.5.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating snapshots of respective cloud platforms, refer to the *Protegility Appliances Overview Guide 9.1.0.5*.

5.2.1.2.4 Backing up the Configuration File

If you have updated the configuration file, then you need to backup the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the *root* password and select **OK**.
4. Navigate to the */opt/protegility/insight/analytics/config* directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```

5. Backup the *remote_cluster.json* file using the following command.

```
mv remote_cluster.json remote_cluster.json.backup
```
6. Repeat the step on all the other nodes in the Audit Store cluster.

5.2.1.2.5 Validating Custom Configuration Files

Complete the steps provided in this section if you modified any configuration files.

- Review the contents of any configuration files. Verify that the code in the configuration file is formatted properly. Ensure that there are no additional spaces, tabs, line breaks, or control characters in the configuration file.
- Validate that the backup files are created with the details appended to the extension, for example, *.conf_backup* or *.conf_bkup123*.
- Back up any custom configuration files or modified configuration files. If required, use the backup files to restore settings after the upgrade is complete.

5.2.1.3 Installations and Hardware Requirements

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have the at least one ESA on v9.0.0.0 or v9.1.0.0.

The used space in the OS(/) partition should not be more than 60%. If the used space is more than 60%, then you must clean up the OS(/) partition before proceeding with the patch installation process. For more information about cleaning up the OS(/) partition, refer to <https://my.protegility.com/knowledge/ka04W00000nSxJQAU/>.

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

Installation Requirements

The *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.pty* patch file is available.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Caution: If logs are forwarded to an external syslog server, then ensure that the syslog server is running during the upgrade.

5.2.1.4 Disabling the Scheduled Tasks for a Cluster

You must disable all the scheduled tasks for a cluster.

To disable the scheduled tasks for a cluster, perform the following steps.

1. From the ESA Web UI, navigate to **System > Task Scheduler**.
The **Scheduler** page displays the list of scheduled tasks for a cluster.
2. To edit a task, click **Edit**.
3. To disable the scheduled task for a cluster, clear the **Enable** check box.
4. Click **Save** and then click **Apply** after performing the required changes.
5. Enter the *root* password.
6. Click **OK**.

The Scheduled tasks for a cluster are disabled.

5.2.1.5 Deleting a Scheduled Task

This section explains the procedure to delete a scheduled task.

► To delete a scheduled task:

1. From the ESA Web UI, navigate to **System > Task Scheduler**.
The **Task Scheduler** screen appears.
2. Select the required task.
3. Select **Remove**.
A confirmation message to remove the scheduled task appears.
4. Select **Apply**.
5. Enter the *root* password and select **Ok**.
The task is deleted successfully.

5.2.1.6 Removing Nodes from the Cluster

This section describes the steps to remove a node from the cluster.

Note: This section is applicable only if you are upgrading the ESA from v9.0.0.0.

► To remove a node from the cluster:

1. On the Web UI of the node that you want to remove from the cluster, navigate to **System > Trusted Appliances Cluster**.
The screen displaying the cluster nodes appears
2. Navigate to **Management > Leave Cluster**.
A confirmation message appears
3. Select **Ok**.
The node is removed from the cluster

5.2.1.7 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the *Protegility Key Management Guide 9.1.0.4*.

5.2.1.8 Disabling *Update Audit Store Management Unicast Hosts* Task

You must disable the *Update Audit Store Management Unicast Hosts* task scheduled task on all the nodes in the *Audit Store* cluster.

► To disable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task.
4. Click **Run now** and then click **OK** in the confirmation box.
5. When the *Update Audit Store Management Unicast Hosts* task is completed successfully, then click **Edit**.
6. To disable the *Update Audit Store Management Unicast Hosts* task, clear the **Enable** checkbox.
7. Click **Save** and then click **Apply** after performing the required changes.
8. Enter the *root* password.
9. Click **OK**.
10. Repeat these steps on all the nodes in the *Audit Store* cluster.

5.2.1.9 Disabling *Rollover Index* Task

You must disable the *Rollover Index* task on the *Audit Store* cluster.

► To disable *Rollover Index* task:

1. Login to the Primary ESA Web UI.
2. Navigate to **Analytics > Scheduler > Tasks**.
3. Click the **Enabled** slider to disable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

5.2.1.10 Configuring Local LDAP

Ensure that the listener IP address of the LDAP is set to *127.0.0.1* or the *Management IP address* of the ESA.

If the listener IP address of the LDAP is not set, then navigate to **Administration > Configure local LDAP Settings**. Ensure that the value of the **LDAP Listener IP address** is set to *127.0.0.1*.

Note:

The Local LDAP configuration is required only when you are upgrading from v9.1.0.0 to v9.1.0.2.

5.2.1.11 Switching to the Protegility Soft HSM

If the Google Cloud Platform (GCP) Key Management Service (KMS) is configured as an external Key Store for the ESA v9.1.0.0, switch to the Protegility Soft HSM before upgrading. This is applicable for upgrading to the ESA v9.1.0.2, ESA v9.1.0.3, ESA v9.1.0.4, or ESA v9.1.0.5.

Note:

If you are upgrading to the ESA v9.1.0.1, then this step is not applicable.

For more information about the Key Store, refer to the section *Key Store* in the *Protegility Key Management Guide 9.1.0.5*.

For more information about switching to the Protegility Soft HSM, refer to the section *Switching from External Key Store to the Protegility Soft HSM* in the *Protegility Hardware Security Module (HSM) Integration Guide 9.1.0.0*.

For more information about the post upgrade steps, refer to the section *Configuring the GCP Key Store*.

5.2.1.12 Replacing the PSUs with the ESAs v9.1.0.x in the Audit Store Cluster

The Audit Store requires a minimum of 3 master-eligible role nodes because of the following scenarios:

- 1 master-eligible node: This scenario will result in total loss of service in case of a failure because no backup nodes are available.
- 2 master-eligible nodes: In this scenario, both nodes added will form the master Audit Store cluster. If one node fails, then the Audit Store cluster becomes unstable and inaccessible as it does not have the minimum required master-eligible nodes, that is two nodes.
- 3 master-eligible nodes and above: In this scenario, 2 master-eligible nodes will be used for the master Audit Store cluster. The remaining master-eligible nodes will be added as true Audit Store clustering nodes for expanding the capabilities of the system.

The Audit Store in your existing deployment might consist of 2 ESAs and 1 PSU or 1 ESA and 2 PSUs. It is recommended to replace the PSUs with ESAs due to the following reasons.



- **Capability:**

The ESA offers the capability of the PSU plus the ability to deploy policies and accept audit event traffic for legacy protection endpoints, such as, protector version 7.2.1.

- **Resilience:**

The ESA in an Audit Store cluster offers more resiliency. If the Primary ESA goes down in the cluster, the processing is continued by another ESA in the cluster. Hence, replacing the PSUs with ESAs increases the number of ESAs available in the case of machines crashing.

- **Ease of upgrade:**

Keeping an ESA and a PSU meant that separate upgrade steps are required. Keeping just ESAs in your Audit Store cluster reduces the need to download multiple upgrade files. One upgrade file can be downloaded and used to upgrade all the ESAs in the cluster.

- **Maintenance:**

The ESA and PSU are two different appliances. It required that you learn the architecture and use for both of them. Replacing PSUs frees up the time required to understand and master the PSU. This time can be better invested to understand the ESA and for other tasks.

- **Ease of installing security patches:**

Keeping just ESAs makes patch installation to secure your appliance faster and simpler to understand and implement. One security patch can be downloaded and installed on all the appliances. Additionally, to apply a security patch, you just need to apply the patch on the Primary ESA and then all of the secondary ESAs.

This section describes the steps for replacing a PSU with an ESA v9.1.0.x in the Audit Store cluster.

Note: Ensure that you add all the required ESAs v9.1.0.x in the Audit Store cluster before removing the PSUs.

If you are using custom certificates, then regenerate the certificates and add entries of the new ESA nodes that will be added to the cluster. Next, you rotate the certificates and then remove the PSU and replace it with an ESA. After all the PSUs are replaced, then remove the PSU entries from the certificates and rotate the certificates.

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

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

Complete the following steps for each PSU in the Audit Store cluster.

1. [Add the ESAs](#).
2. [Remove the PSUs](#).

5.2.1.12.1 Redirecting Protector Logs to the Audit Store on the ESA

If your Protectors are sending the logs to the PSU, then you must reconfigure the Log Forwarder to send the logs to the ESA. This section provides the steps for reconfiguring the Protectors to send the logs to the ESA.

Note: This section is only required for deployments where the Log Forwarder was configured to send logs to the PSU. Skip this section if the Log Forwarder is already configured to send logs to the ESA.

► To configure the Protector to send logs to the primary ESA:

1. Configure the Protector to send the logs from the PSU to the Primary ESA.

For more information about configuring the Protector, refer to the Protector documentation.

2. Restart *fluent-bit* on the Protector using the following commands.

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

3. If required, then complete the configurations on the remaining Protector machines.

5.2.1.12.2 Disabling the ESA LDAP on the PSU

Before you upgrade the PSU, you need to switch the LDAP connection of the PSU from the connected ESA to the local LDAP. You can revert the LDAP settings after you upgrade the PSU.

Note: This step is only required if you have PSUs in your architecture.

► To use local LDAP:

1. Login to the CLI Manager of the PSU that must be upgraded.
2. Navigate to **Administration > LDAP Tools > Specify LDAP server/s**.
3. Enter the root password and select **OK**.
4. Select **Reset LDAP Server settings** and select **OK**.
5. Enter the username and password for the administrator user and select **OK**.
6. Select **OK**.
7. Select **Generate a new random password** and select **OK**.
8. Select **OK**.

The LDAP is reset to the local LDAP server.

5.2.1.12.3 Updating Roles on the Primary ESA for the Audit Store Cluster

Complete the steps in this section to update the ESA roles for the Audit Store Cluster.

1. Login to the Primary ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Audit Store Management Update Unicast Hosts** task.
4. Click **Run now** and then click **OK** in the confirmation box.
5. Update the roles on the ESA using the following steps.

Note: This step must only be performed on the Primary ESA.

- a. Login to the Web UI of the system to change the role.
- b. Click **Audit Store Management** to open the Audit Store clustering page.
- c. Click **Edit Roles**.
- d. Ensure that the **Data** and **Ingest** check boxes are selected.
- e. Click **Update Roles**.

- f. Click **Dismiss** in the message box that appears after the role update.
6. Update the *td-agent* configuration using the following steps.
 - a. Login to the CLI Manager of the primary *ESA*.
 - b. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
 - c. Enter the *root* password and select **OK**.
 - d. Enter the username and password for the administrative user, such as, *admin*.
 - e. Select **OK**.
 - f. In the *Setting ESA Communication* screen, select **OK**.
 - g. Specify *localhost* in the *Target Audit Store Addresses* field.



Figure 5-30: Forward Logs

- h. Select **OK**.
- i. Type *y* to fetch certificates for communicating with the *ESA* and select **OK**.

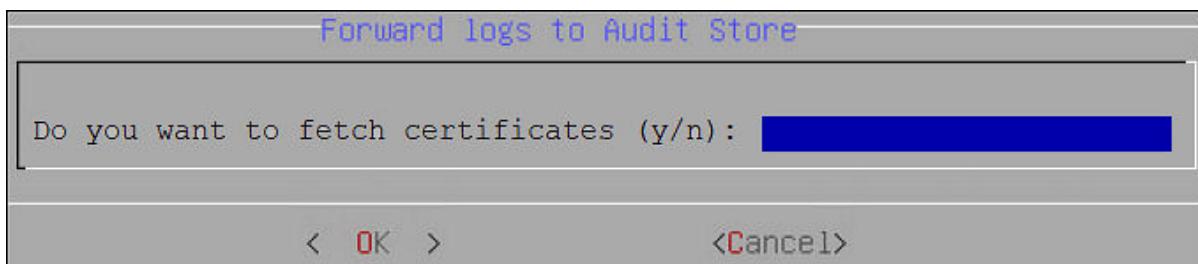


Figure 5-31: Fetch Certificates

- j. Enter the *admin* username and password and select **OK**.
 - k. Repeat the steps on the remaining *ESA* nodes, if you have multiple *ESAs*.
- Wait till the cluster status turns green and the clustering operation is complete.

5.2.1.12.4 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.

Note: Ensure that you add the latest *ESA* version to the Audit Store cluster.

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 *Protegility Appliances Overview Guide 9.1.0.5*.

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

The following screen appears.

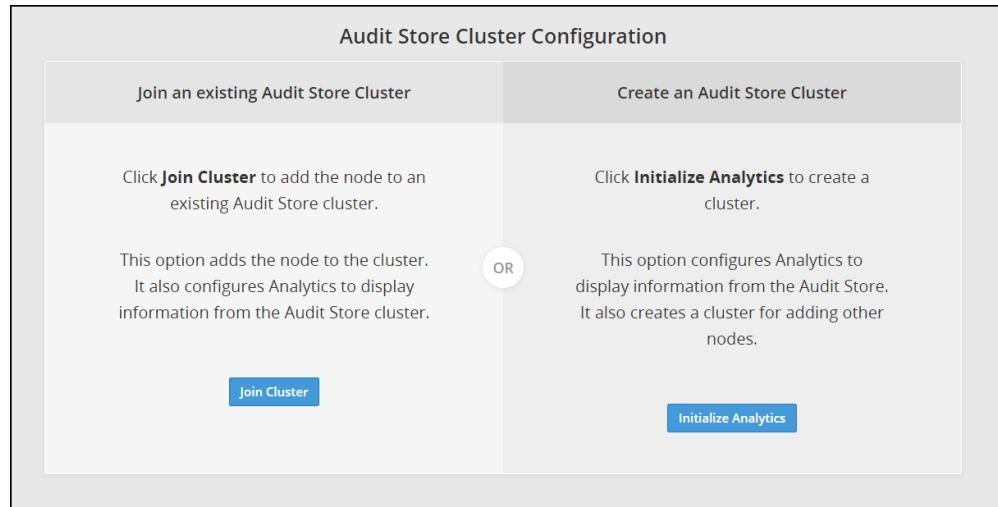


Figure 5-32: Analytics Screen

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 5-33: 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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.

Protegility 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.

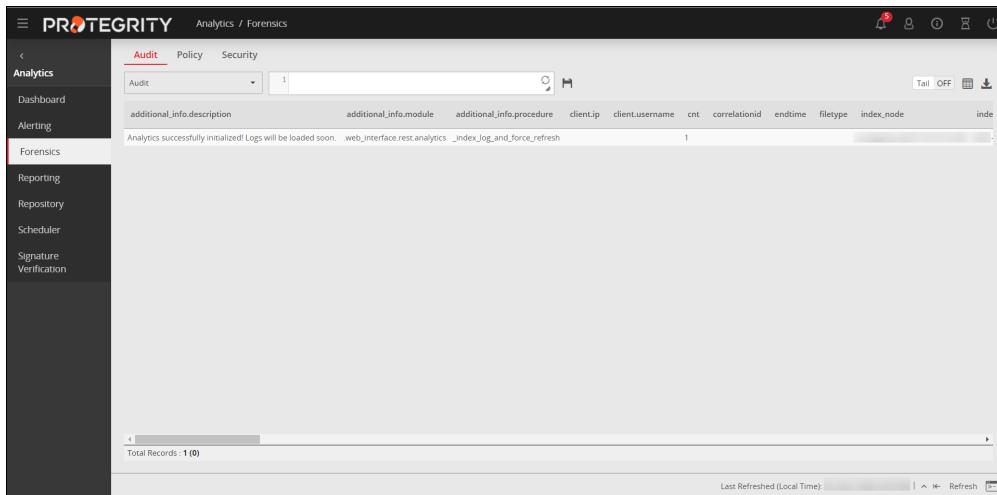


Figure 5-34: Protegility Analytics

8. Repeat the steps mentioned in this section to add the remaining ESAs as required.

Note: Ensure that you add one appliance at a time. After adding the appliance, wait till the cluster becomes stable. The cluster is stable when the cluster status indicator turns green.

5.2.1.12.5 Removing the PSUs from the Audit Store Cluster

Starting from v9.1.0.1 onwards, 3 ESAs are required for the Audit Store cluster. During the upgrade, the PSUs in the Audit Store cluster must be replaced with ESAs to make the cluster more robust. When you remove a node 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 a node:

1. Open the Audit Store clustering page.

The Cluster Overview screen appears.

The screenshot shows the 'Cluster Overview' screen for a cluster named 'insight'. At the top, there are buttons for 'Join Cluster' (disabled) and 'Leave Cluster'. A 'Cluster Status' indicator is green. Below the status, the cluster summary includes:

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
2	2	17	34	0

Below this, detailed shard information is shown:

Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count
0	0	1.3.0	[redacted]	14

At the bottom, a table lists nodes with their roles:

Node IP	Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
[redacted]	✓	✓	✓	Edit Roles	[redacted]	9h	39,502,524,416	7,035,338,752	32,467,185,664	16,6
[redacted]	✓	✓	✓	Edit Roles	[redacted]	3.4m	39,502,524,416	7,001,763,840	32,500,760,576	16,6

Figure 5-35: 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 to the Audit Store cluster at the same time using the ESA Web UI would lead to errors.

3. Click YES.

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

The screenshot shows the 'Cluster Overview' screen for the same cluster 'insight'. The 'Leave Cluster' button is now enabled (blue). The cluster summary shows:

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
1	1	17	17	0

Below this, detailed shard information is shown:

Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count
0	16	1.3.0	[redacted]	14

At the bottom, a table lists nodes with their roles. The first node is still present:

Node IP	Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
[redacted]	✓	✓	✓	Edit Roles	[redacted]	8.8h	39,502,524,416	7,033,622,528	32,468,901,888	16,6

Figure 5-36: Leaving a Cluster

Note: The process of removing a node from the cluster 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.

4. Repeat the steps mentioned in this section to remove the remaining PSUs.

Note: Ensure that you remove one appliance at a time. After removing the appliance, wait till the cluster becomes stable. The cluster is stable when the cluster status indicator turns green.

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, Protegity Analytics needs to be initialized on the node or the node needs to be added to another Audit Store cluster.

5.2.2 Installing the ESA v9.1.0.x Patch

This section describes the steps to upgrade to the ESA to v9.1.0.x by installing the respective patch.

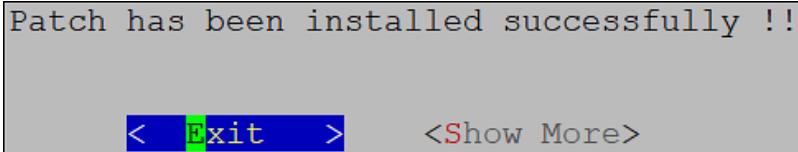
► To install the ESA v9.1.0.x patch:

1. Login to the ESA CLI Manager with administrator credentials.
2. Navigate to **Administration > OS Console** to upload the patch.
3. Upload the patch to the `/products/uploads` directory using the FTP or SCP command.
4. Navigate to **Administration > Patch Management** to install the patch.
5. Enter the `root` password.
6. Select **Install a Patch**.
7. Select the `ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.pty` patch file and select **Install**.

Note: Ensure that you download the latest patch from the [My.Protegity](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

8. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the v9.1.0.x.

5.2.3 Verifying the ESA Patch Installation

After upgrading to the ESA v9.1.0.x, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the `root` password.
4. Select **List installed patches**.

The `ESA_9.1.0.x` patch name appears.

Ensure that there are no errors in the logs.

5.2.4 Post Upgrade Steps

Ensure that the following steps in the following sections are performed after the ESA upgrade is completed:

5.2.4.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. `/var/log`
 - *Installation.log* - Provides the logs for all the installed components.
 - *syslog* - Provides collective information about the syslogs.
2. `/etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log`

5.2.4.2 Restarting the System

After the ESA patch is installed successfully, restart the ESA machine. This ensures that the updated configurations are reflected on the upgraded ESA.

5.2.4.3 Verifying the Local LDAP Settings

After restarting the instance, log in to the ESA to verify the local LDAP setting. Ensure that the listener IP address of the LDAP is set to *127.0.0.1* or the *Management IP address* of the ESA.

► To verify the local LDAP settings:

1. Login to the ESA CLI Manager using the local administrator credentials.
2. Navigate to **Administration > Configure local LDAP Settings**. Ensure that the value of the **LDAP Listener IP address** is set to *127.0.0.1*.

5.2.4.4 Verifying the *cron-jobs* for the Analytics

After upgrading the ESA to the latest version, ensure that the *cron-jobs* for the Analytics are available.

► To verify the *cron-jobs* for the Analytics:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.

3. Check the *cron-jobs* entry in the */var/spool/cron/crontabs/root* file using the following command.

```
cat /var/spool/cron/crontabs/root
```

4. Verify that the following entry is available.

```
* * * * * source /opt/protegility/insight/analytics/analytic_venv/bin/activate ;  
python /opt/protegility/insight/analytics/bin/cron/insight_cron_executor.py > /dev/null 2>&1
```

5. If the entry mentioned in step 4 is unavailable, then perform the following steps.

- a. Create a backup of the */var/spool/cron/crontabs/root* file.
- b. Add the *cron-jobs* entry using the following command.

```
echo '* * * * * source /opt/protegility/insight/analytics/analytic_venv/bin/activate ;  
python /opt/protegility/insight/analytics/bin/cron/insight_cron_executor.py > /dev/null  
2>&1' >> /var/spool/cron/crontabs/root
```

- c. Verify the *cron-jobs* entry in the */var/spool/cron/crontabs/root* file using the following command.

```
cat /var/spool/cron/crontabs/root
```

- d. Restart the *cron* service using the following command.

```
/etc/init.d/cron restart
```

5.2.4.5 Restoring the Configuration File

If you have updated the configuration file and backed it up before the upgrade, then you need to restore the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the *root* password and select **OK**.
4. Navigate to the */opt/protegility/insight/analytics/config* directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```

5. Restore the *remote_cluster.json* file using the following command.

```
cp remote_cluster.json.backup remote_cluster.json
```

6. Repeat these steps on all the other nodes in the Audit Store cluster.

5.2.4.6 Enabling the Scheduled Tasks for a Cluster

You must enable all the scheduled tasks for a cluster.

To enable the scheduled tasks for a cluster, perform the following steps.

1. From the ESA Web UI, navigate to **System > Task Scheduler**.
The **Scheduler** page displays the list of scheduled tasks for a cluster.
2. To edit a task, click **Edit**.
3. To enable the scheduled task for a cluster, select the **Enable** checkbox.

4. Click **Save** and then click **Apply** after performing the required changes.
5. Enter the *root* password.
6. Click **OK**.

The Scheduled tasks for a cluster are enabled.

5.2.4.7 Updating the Priority IP List for Signature Verification

Signature verification jobs run on the ESA and use the ESA's processing time. Ensure that you update the priority IP list for the default signature verification jobs after you set up the system. By default, the Primary ESA will be used for the priority IP. If you have multiple ESAs in the priority list, then additional ESAs are available to process the signature verifications jobs that must be processed. This frees up the Primary ESA's processor to handle other important tasks.

For example, if the maximum jobs to run on an ESA is set to 4 and 10 jobs are queued to run on 2 ESAs, then 4 jobs are started on the first ESA, 4 jobs are started on the second ESA, and 2 jobs will be queued to run till an ESA job slot is free to accept and run the queued job.

For more information about scheduling jobs, refer to the section *Using the Scheduler* in the [Protegility Analytics Guide 9.1.0.5](#).

For more information about signature verification jobs, refer to the section *Verifying Signatures* in the [Protegility Analytics Guide 9.1.0.5](#).

Use the steps provided in this section to update the priority IP list.

1. Login to the ESA Web UI.
2. Navigate to **Analytics > Scheduler**.
3. From the **Action** column, click the **Edit** icon () for the **Signature Verification** task.
4. Update the **Priority IPs** field with the list of the ESAs available separating the IPs using commas.
5. Click **Save**.

5.2.4.8 Enabling *Update Audit Store Management Unicast Hosts* Task

You must enable the *Update Audit Store Management Unicast Hosts* task on all the nodes.

► To enable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task and click **Edit**.
4. Click **Enable** for the *Update Audit Store Management Unicast Hosts* tasks.
5. Click **Save** and then click **Apply** after performing the required changes.
6. Enter the *root* password and select **OK**.
7. Repeat the steps on all the nodes in the *Audit Store* cluster.

5.2.4.9 Enabling *Rollover Index* Task

You must enable the *Rollover Index* task on any of the nodes in the *Audit Store* cluster.

► To enable *Rollover Index* task:

1. Login to the ESA Web UI on any of the nodes in the *Audit Store* cluster.
2. Navigate to **Analytics > Scheduler > Tasks**
3. Click the **Enabled** slider to enable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

5.2.4.10 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

Before you begin

Keep the following information handy before the setup process:

- SMTP server details
- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is **25**.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.
Protegility Reporting requires a full email address in the Username.
7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.
A message box appears.
14. Click **EXIT** to save the settings.



5.2.4.11 Configuring the GCP Key Store

After upgrading to the ESA v9.1.0.x, the Key Store configuration file is not migrated. You must configure the GCP Key Store for the ESA v9.1.0.2, ESA v9.1.0.3, ESA v9.1.0.4, or ESA v9.1.0.5. This is required because before upgrading, you had switched from the GCP Key Store to Protegility Soft HSM.

Note:

If you have upgraded to the ESA v9.1.0.1, then this step is not applicable.

For more information about configuring the GCP Key Store, refer to the section *Configuring a Key Store for GCP* in the [Google Cloud Platform \(GCP\) Key Management Service \(KMS\) Integration Guide for ESA 9.1.0.0](#).

5.2.4.12 Optional: Updating configuration for sending logs to the external SIEM

Complete the steps provided in this section to update the td-agent configuration. This improves the security of the appliance while sending logs to the external SIEM.

1. Open the OS Console on the Primary ESA.
 - a. Login to the CLI Manager of the Primary ESA.
 - b. Navigate to **Administration > OS Console**.
 - c. Enter the root password and select **OK**.
2. Update the configuration settings to improve the SSL/TLS server configuration on the system.
 - a. Navigate to the *config.d* directory using the following command.

```
cd /opt/protegility/td-agent/config.d
```

- b. Open the *INPUT_forward_external.conf* file using the following command.

```
vi INPUT_forward_external.conf
```

- c. Add the following content in bold to the file. Update and use the ciphers that you require.

```
<source>
  @type forward
  bind 0.0.0.0
  port 24284
  <transport tls>
    ca_path          /mnt/ramdisk/certificates/mng/CA.pem
    cert_path        /mnt/ramdisk/certificates/mng/server.pem
    private_key_path /mnt/ramdisk/certificates/mng/server.key
    ciphers "ALL:!
aNULL:!eNULL:!SSLv2:!SSLv3:DHE:!AES256-SHA:!CAMELLIA256-SHA:!AES128-SHA:!CAMELLIA128-
SHA:!TLS_RSA_WITH_RC4_128_MD5:!TLS_RSA_WITH_RC4_128_SHA:!TLS_RSA_WITH_3DES_EDE_CBC_SHA:!
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA:!TLS_RSA_WITH_SEED_CBC_SHA:!
TLS_DHE_RSA_WITH_SEED_CBC_SHA:!TLS_ECDHE_RSA_WITH_RC4_128_SHA:!
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA"
  </transport>
</source>
```

Ensure that you specify the entire line of code on a single line and retain the formatting of the file.

- d. Save and close the file.
3. Restart the *td-agent* service.
 - a. Login to the ESA Web UI.
 - b. Navigate to **System > Services > Misc > td-agent**,
 - c. Restart the **td-agent** service.



5.2.5 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

5.2.5.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

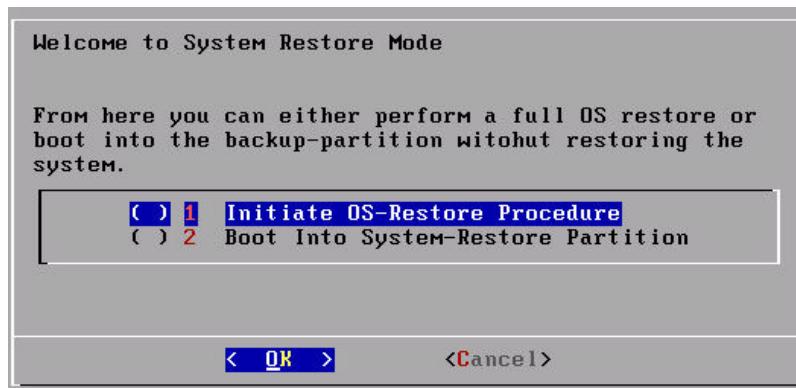
1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

5.2.5.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

5.2.5.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

5.2.5.2.2 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

5.2.5.2.3 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.

10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

5.3 Upgrading from v9.1.0.x to v9.1.0.5

This section describes the steps to upgrade the ESA and protectors to the latest compatible version.

Note: Ensure that you upgrade the ESA prior to upgrading the protectors.

Note: This section is applicable only if you are upgrading the ESA from the ESA v9.1.0.1, v9.1.0.2, 9.1.0.3, or 9.1.0.4 to the ESA v9.1.0.5.

5.3.1 Prerequisites

The prerequisites for upgrading the ESA to the latest version must be performed.

5.3.1.1 Accounts

The *local admin* account used for upgrading the ESA must be active.

Ensure that the local administrator user has access to the CLI Manager and Web UI. Navigate to **Administration > Accounts And Passwords > Manage Passwords And Local-Accounts > Change OS 'local_admin' account permissions** to set the local administrator permissions.

5.3.1.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a back up of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

5.3.1.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

5.3.1.2.2 Exporting Data/Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration:

► To export data configurations to a remote appliance:

1. Log in to the CLI Manager
2. Navigate to **Administration > Backup/Restore Center**.
3. Enter the *root* password and select **OK**.
The Backup Center dialog box appears.
4. From the menu, select the **Export data/configurations to a remote appliance(s)** option and select **OK**.
5. From the **Select file/configuration to export** dialog box, select **Current (Active) Appliance Configuration package to export** and select **OK**.
6. In the following dialog box, **Select the packages to export** and select **OK**.
7. Select the **Import** method.
For more information on each import method, select **Help**.
8. Type the **IP address or hostname for the destination** appliance.
9. Type the administrative credentials of the remote appliance and select **Add**.
10. In the information dialog box, press **OK**.
The Backup Center screen appears.

Note: Do not import all network settings to another machine since it will create two machines with the same IP in your network. It is recommended to restart the appliance after receiving an appliance core configuration backup.

This item shows up only when exporting to a file.

5.3.1.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before upgrading to v9.1.0.5.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating snapshots of respective cloud platforms, refer to the *Protegility Appliances Overview Guide 9.1.0.5*.

5.3.1.2.4 Backing up the Configuration File

If you have updated the configuration file, then you need to backup the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the *root* password and select **OK**.
4. Navigate to the */opt/protegility/insight/analytics/config* directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```

5. Backup the *remote_cluster.json* file using the following command.

```
mv remote_cluster.json remote_cluster.json.backup
```
6. Repeat the step on all the other nodes in the Audit Store cluster.

5.3.1.2.5 Validating Custom Configuration Files

Complete the steps provided in this section if you modified any configuration files.

- Review the contents of any configuration files. Verify that the code in the configuration file is formatted properly. Ensure that there are no additional spaces, tabs, line breaks, or control characters in the configuration file.
- Validate that the backup files are created with the details appended to the extension, for example, *.conf_backup* or *.conf_bkup123*.
- Back up any custom configuration files or modified configuration files. If required, use the backup files to restore settings after the upgrade is complete.

5.3.1.3 Installations and Hardware Requirements

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have the at least one ESA on previous v9.1.0.x.

The used space in the OS(/) partition should not be more than 60%. If the used space is more than 60%, then you must clean up the OS(/) partition before proceeding with the patch installation process. For more information about cleaning up the OS(/) partition, refer to <https://my.protegility.com/knowledge/ka04W00000nSxJQAU/>.

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

Installation Requirements

The *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx-UP.pty* patch file is available.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Caution: If logs are forwarded to an external syslog server, then ensure that the syslog server is running during the upgrade.

5.3.1.4 Disabling the Scheduled Tasks for a Cluster

You must disable all the scheduled tasks for a cluster.

To disable the scheduled tasks for a cluster, perform the following steps.

1. From the ESA Web UI, navigate to **System > Task Scheduler**.
The **Scheduler** page displays the list of scheduled tasks for a cluster.
2. To edit a task, click **Edit**.
3. To disable the scheduled task for a cluster, clear the **Enable** check box.
4. Click **Save** and then click **Apply** after performing the required changes.
5. Enter the *root* password.
6. Click **OK**.

The Scheduled tasks for a cluster are disabled.

5.3.1.5 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the [Protegility Key Management Guide 9.1.0.4](#).

5.3.1.6 Disabling *Update Audit Store Management Unicast Hosts* Task

You must disable the *Update Audit Store Management Unicast Hosts* task scheduled task on all the nodes in the *Audit Store* cluster.

► To disable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task.
4. Click **Run now** and then click **OK** in the confirmation box.



5. When the *Update Audit Store Management Unicast Hosts* task is completed successfully, then click **Edit**.
6. To disable the *Update Audit Store Management Unicast Hosts* task, clear the **Enable** checkbox.
7. Click **Save** and then click **Apply** after performing the required changes.
8. Enter the *root* password.
9. Click **OK**.
10. Repeat these steps on all the nodes in the *Audit Store* cluster.

5.3.1.7 Disabling Rollover Index Task

You must disable the *Rollover Index* task on the *Audit Store* cluster.

► To disable *Rollover Index* task:

1. Login to the Primary ESA Web UI.
2. Navigate to **Analytics > Scheduler > Tasks**.
3. Click the **Enabled** slider to disable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

5.3.1.8 Switching to the Protegility Soft HSM

If the Google Cloud Platform (GCP) Key Management Service (KMS) is configured as an external Key Store for the ESA v9.1.0.1, switch to the Protegility Soft HSM before upgrading. This is applicable for upgrading to the ESA v9.1.0.2, ESA v9.1.0.3, ESA v9.1.0.4, or ESA v9.1.0.5.

Note:

If you are upgrading to the ESA v9.1.0.5 from the ESA v9.1.0.2 or higher versions, then this step is not applicable.

For more information about the Key Store, refer to the section *Key Store* in the [Protegility Key Management Guide 9.1.0.5](#).

For more information about switching to the Protegility Soft HSM, refer to the section *Switching from External Key Store to the Protegility Soft HSM* in the [Protegility Hardware Security Module \(HSM\) Integration Guide 9.1.0.0](#).

For more information about the post upgrade steps, refer to the section [Configuring the GCP Key Store](#).

5.3.2 Installing the ESA v9.1.0.x Patch

This section describes the steps to upgrade to the ESA to v9.1.0.x by installing the respective patch.

► To install the ESA v9.1.0.x patch:

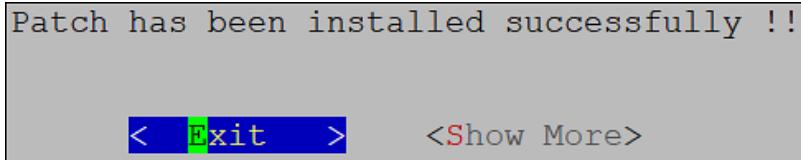
1. Login to the ESA CLI Manager with administrator credentials.
2. Navigate to **Administration > OS Console** to upload the patch.
3. Upload the patch to the */products/uploads* directory using the FTP or SCP command.
4. Navigate to **Administration > Patch Management** to install the patch.

5. Enter the *root* password.
6. Select **Install a Patch**.
7. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.pty* patch file and select **Install**.

Note: Ensure that you download the latest patch from the [My.Protegrity](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

8. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the v9.1.0.x.

5.3.3 Verifying the ESA Patch Installation

After upgrading to the ESA v9.1.0.x, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_9.1.0.x* patch name appears.

Ensure that there are no errors in the logs.

5.3.4 Post Upgrade Steps

Ensure that the following steps in the following sections are performed after the ESA upgrade is completed:

5.3.4.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. */var/log*
 - *Installation.log* - Provides the logs for all the installed components.

- *syslog* - Provides collective information about the syslogs.
2. */etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log*

5.3.4.2 Restarting the System

After the ESA patch is installed successfully, restart the ESA machine. This ensures that the updated configurations are reflected on the upgraded ESA.

5.3.4.3 Restoring the Configuration File

If you have updated the configuration file and backed it up before the upgrade, then you need to restore the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the *root* password and select **OK**.
4. Navigate to the */opt/protegility/insight/analytics/config* directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```

5. Restore the *remote_cluster.json* file using the following command.

```
cp remote_cluster.json.backup remote_cluster.json
```

6. Repeat these steps on all the other nodes in the Audit Store cluster.

5.3.4.4 Enabling *Update Audit Store Management Unicast Hosts* Task

You must enable the *Update Audit Store Management Unicast Hosts* task on all the nodes.

► To enable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task and click **Edit**.
4. Click **Enable** for the *Update Audit Store Management Unicast Hosts* tasks.
5. Click **Save** and then click **Apply** after performing the required changes.
6. Enter the *root* password and select **OK**.
7. Repeat the steps on all the nodes in the *Audit Store* cluster.

5.3.4.5 Enabling *Rollover Index* Task

You must enable the *Rollover Index* task on any of the nodes in the *Audit Store* cluster.

► To enable *Rollover Index* task:

1. Login to the ESA Web UI on any of the nodes in the *Audit Store* cluster.
2. Navigate to **Analytics > Scheduler > Tasks**
3. Click the **Enabled** slider to enable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

5.3.4.6 Enabling the Scheduled Tasks for a Cluster

You must enable all the scheduled tasks for a cluster.

To enable the scheduled tasks for a cluster, perform the following steps.

1. From the ESA Web UI, navigate to **System > Task Scheduler**.
The **Scheduler** page displays the list of scheduled tasks for a cluster.
2. To edit a task, click **Edit**.
3. To enable the scheduled task for a cluster, select the **Enable** checkbox.
4. Click **Save** and then click **Apply** after performing the required changes.
5. Enter the *root* password.
6. Click **OK**.

The Scheduled tasks for a cluster are enabled.

5.3.4.7 Enabling the CloudWatch Service

You must enable the CloudWatch service.

Note: This is applicable only if the CloudWatch service or the AWS tool is installed in the system.

► To enable the CloudWatch service, perform the following steps.

1. Login to the ESA Web UI.
2. Navigate to **System > Services** web page.
3. Under **Actions**, navigate to the **CloudWatch Service**.
4. Click the **Start** icon.

5.3.4.8 Configuring the GCP Key Store

After upgrading to the ESA v9.1.0.5, the Key Store configuration file is not migrated. You must configure the GCP Key Store for the ESA v9.1.0.5. This is required because before upgrading, you had switched from the GCP Key Store to Protegility Soft HSM.

Note:

If you are upgrading to the ESA v9.1.0.5 from the ESA v9.1.0.2 or higher versions, then this step is not applicable.

For more information about configuring the GCP Key Store, refer to the section *Configuring a Key Store for GCP* in the [Google Cloud Platform \(GCP\) Key Management Service \(KMS\) Integration Guide for ESA 9.1.0.0](#).

5.3.4.9 Optional: Updating configuration for sending logs to the external SIEM

Complete the steps provided in this section to update the td-agent configuration. This improves the security of the appliance while sending logs to the external SIEM.

1. Open the OS Console on the Primary ESA.
 - a. Login to the CLI Manager of the Primary ESA.
 - b. Navigate to **Administration > OS Console**.
 - c. Enter the root password and select **OK**.
2. Update the configuration settings to improve the SSL/TLS server configuration on the system.
 - a. Navigate to the *config.d* directory using the following command.

```
cd /opt/protegility/td-agent/config.d
```

- b. Open the *INPUT_forward_external.conf* file using the following command.

```
vi INPUT_forward_external.conf
```

- c. Add the following content in bold to the file. Update and use the ciphers that you require.

```
<source>
  @type forward
  bind 0.0.0.0
  port 24284
  <transport tls>
    ca_path          /mnt/ramdisk/certificates/mng/CA.pem
    cert_path        /mnt/ramdisk/certificates/mng/server.pem
    private_key_path /mnt/ramdisk/certificates/mng/server.key
    ciphers "ALL:!
aNULL:!eNULL:!SSLv2:!SSLv3:!DHE:!AES256-SHA:!CAMELLIA256-SHA:!AES128-SHA:!CAMELLIA128-
SHA:!TLS_RSA_WITH_RC4_128_MD5:!TLS_RSA_WITH_RC4_128_SHA:!TLS_RSA_WITH_3DES_EDE_CBC_SHA:!
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA:!TLS_RSA_WITH_SEED_CBC_SHA:!
TLS_DHE_RSA_WITH_SEED_CBC_SHA:!TLS_ECDHE_RSA_WITH_RC4_128_SHA:!
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA"
  </transport>
</source>
```

Ensure that you specify the entire line of code on a single line and retain the formatting of the file.

- d. Save and close the file.
3. Restart the *td-agent* service.
 - a. Login to the ESA Web UI.
 - b. Navigate to **System > Services > Misc > td-agent**,
 - c. Restart the **td-agent** service.

5.3.5 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

5.3.5.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

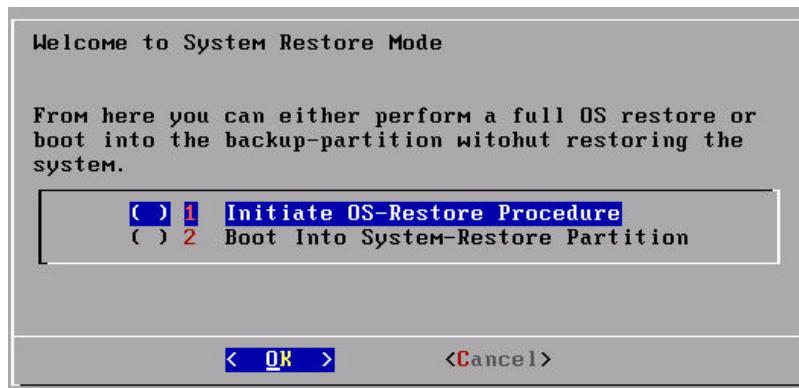
1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

5.3.5.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the *Protegility Appliances Overview Guide 9.1.0.5*.

5.3.5.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

5.3.5.2.2 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.



2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disks**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

5.3.5.2.3 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

5.4 Upgrading Protectors

If you are upgrading the Protectors to v9.1.0.x, then ensure that the ESA is at v9.1.0.x.

Note:

For more information about the compatible data elements for the different protector versions, refer to the table [Data Element Compatibility Matrix](#).

5.4.1 Upgrading to Data Security Gateway (DSG) v3.1.0.x

The Data Security Gateway (DSG) can be upgraded to the DSG v3.1.0.x. The upgrade process involves the following steps.

1. Upgrade the ESA to the version v9.1.0.x
2. Extend the ESA with the DSG Web UI by applying the DSG v3.1.0.x patch.

For information about extending the ESA with the DSG Web UI, refer to the section *Extending ESA with DSG Web UI* in the [Data Security Gateway User Guide 3.1.0.x](#).

3. Reimage the DSG nodes to v3.1.0.x.

The following is a list of patches available for the DSG v3.1.0.x release.

Table 5-2: List of the DSG v3.1.0.x patches

ESA version	Compatible DSG version	DSG patch on the ESA
9.1.0.5	3.1.0.5	<i>ESA_PAP-ALL-64_x86-64_9.1.0.5.2242.DSGUP.pty</i>
9.1.0.4	3.1.0.4	<i>ESA_PAP-ALL-64_x86-64_9.1.0.4.2204.DSGUP.pty</i>
9.1.0.3	3.1.0.3	<i>ESA_PAP-ALL-64_x86-64_9.1.0.3.2168.DSGUP.pty</i>
9.1.0.2	3.1.0.2	<i>ESA_PAP-ALL-64_x86-64_9.1.0.2.2164.DSGUP.pty</i>
9.1.0.1	3.1.0.1	<i>ESA_PAP-ALL-64_x86-64_9.1.0.1.2162.DSGUP.pty</i>

Note:

Ensure that you download the latest patch from the [My.Protegrity](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

For more information about upgrading the DSG to DSG v3.1.0.x, refer to the section *Upgrading to DSG v3.1.0.x* in the [Data Security Gateway User Guide 3.1.0.x](#).

5.4.1.1 Applying a DSG Patch

Apply the Data Security Gateway (DSG) patch on the ESA to extend its Web UI with the DSG menu. You must apply the *ESA_PAP-ALL-64_x86-64_9.1.0.x.xxxx.DSGUP.pty* patch on the ESA v9.1.0.x.

► To install the DSG patch on the ESA Web UI:

1. Login to the ESA Web UI.
2. Navigate to **Settings > System > File Upload**.
3. Click **Choose File** to upload the DSG patch file.
4. Select the file and click **Upload**.
The uploaded patch appears on the Web UI.
5. On the ESA CLI Manager, navigate to **Administration > Installation and Patches > Patch Management**.
6. Enter the *root* password.

7. Select **Install a Patch** and press **OK**.
8. Select the uploaded patch.
9. Press **Install**.

Note: After the patch is successfully installed, you may need to refresh the ESA Web UI to view the **Cloud Gateway** menu option. This will refresh the local copy (cache) of the ESA Web UI menu screen.

Chapter 6

Upgrading from v9.0.0.0 to v9.1.0.0

[6.1 Prerequisites](#)

[6.2 Upgrading to ESA v9.1.0.0](#)

[6.3 Upgrading PSU from v9.0.0.0 to v9.1.0.0](#)

[6.4 Verifying Patch Installation](#)

[6.5 Post Upgrade Steps](#)

[6.6 Restoring to the Previous Version of ESA](#)

[6.7 Upgrading Protectors](#)

This section describes the steps to upgrade the ESA, PSU, and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the PSU and protectors.

6.1 Prerequisites

The prerequisites for upgrading the ESA to v9.1.0.0 must be performed on the following components:

- Accounts
- Backup and Restore
- Installations and Hardware Requirements
- Keys
- Unicast host task
- Rollover index task
- ESA LDAP on the PSU

6.1.1 Accounts

The administrative account used for upgrading the ESA must be active.

6.1.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a backup of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

6.1.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

6.1.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.



- For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
 8. Type the admin user credentials of the remote appliance and select **Add**.
 9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

6.1.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before initiating the upgrade process.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating the snapshots from the respective cloud platforms, refer to the *Protegility Appliances Overview Guide 9.1.0.5*.

6.1.2.4 Backing up the Configuration File

If you have updated the configuration file, then you need to back up the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the root password and select **OK**.
4. Navigate to the `/opt/protegility/insight/analytics/config` directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```
5. Backup the `remote_cluster.json` file using the following command.

```
mv remote_cluster.json remote_cluster.json.backup
```
6. Repeat the step on all the other nodes in the Audit Store cluster.

6.1.2.5 Validating Custom Configuration Files

Complete the steps provided in this section if you modified any configuration files.

- Review the contents of any configuration files. Verify that the code in the configuration file is formatted properly. Ensure that there are no additional spaces, tabs, line breaks, or control characters in the configuration file.
- Validate that the backup files are created with the details appended to the extension, for example, `.conf_backup` or `.conf_bkup123`.
- Back up any custom configuration files or modified configuration files. If required, use the backup files to restore settings after the upgrade is complete.

6.1.3 Installations and Hardware Requirements

Installation Requirements

- An ESA v9.0.0.0 must be available to upgrade.
- The `ESA_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty` patch file is available.
- The minimum space available in the `/opt` directory should be more than twice the size of the patch files.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have the v9.0.0.0 platform release installed with at least the following components:

- 2 ESAs
- 2 Protegility Storage Units (PSUs)

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

6.1.4 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section [Working with Keys](#) in the [Protegility Key Management Guide 9.1.0.0](#).

6.1.5 Disabling *Update Audit Store Management Unicast Hosts* Task

You must disable the *Update Audit Store Management Unicast Hosts* task scheduled task on all the nodes in the *Audit Store* cluster.

► To disable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task.

4. Click **Run now** and then click **OK** in the confirmation box.
5. When the *Update Audit Store Management Unicast Hosts* task is completed successfully, then click **Edit**.
6. To disable the *Update Audit Store Management Unicast Hosts* task, clear the **Enable** checkbox.
7. Click **Save** and then click **Apply** after performing the required changes.
8. Enter the *root* password.
9. Click **OK**.
10. Repeat these steps on all the nodes in the *Audit Store* cluster.

6.1.6 Disabling *Rollover Index* Task

You must disable the *Rollover Index* task on the *Audit Store* cluster.

► To disable *Rollover Index* task:

1. Login to the Primary ESA Web UI.
2. Navigate to **Analytics > Scheduler > Tasks**.
3. Click the **Enabled** slider to disable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

6.1.7 Disabling the ESA LDAP on the PSU

Before you upgrade the PSU, you need to switch the LDAP connection of the PSU from the connected ESA to the local LDAP. You can revert the LDAP settings after you upgrade the PSU.

► To use local LDAP:

1. Login to the CLI Manager of the PSU that must be upgraded.
 2. Navigate to **Administration > LDAP Tools > Specify LDAP server/s**.
 3. Enter the root password and select **OK**.
 4. Select **Reset LDAP Server settings** and select **OK**.
 5. Enter the username and password for the administrator user and select **OK**.
 6. Select **OK**.
 7. Select **Generate a new random password** and select **OK**.
 8. Select **OK**.
- The LDAP is reset to the local LDAP server.

6.2 Upgrading to ESA v9.1.0.0

This section describes the steps to upgrade to the ESA v9.1.0.0.

► To install the ESA v9.1.0.0 patch:

1. Login to the ESA Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

The file upload is initiated.

Note:

Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the ESA CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the root password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty* patch file and select **Install**.
10. Select **OK**.
11. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the ESA v9.1.0.0.

6.3 Upgrading PSU from v9.0.0.0 to v9.1.0.0

This section describes the steps to upgrade from the PSU v9.0.0.0 to the PSU v9.1.0.0.

1. Login to the PSU Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *PSU_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty* file and click **Upload**.

- If the size of the file is less than the upload limit, then the file upload is initiated.
- If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

The file upload is initiated.

Note: Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the PSU CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the *root* password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *PSU_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty* patch file and select **Install**.
10. Select **Exit** on the following screen.

```
Patch has been installed successfully !!

< Exit >      <Show More>
```

The patch is installed and the PSU is upgraded to the PSU v9.1.0.0.

6.4 Verifying Patch Installation

After upgrading the ESA and PSUs to v9.1.0.0, you can verify the patch installation.

6.4.1 Verifying the ESA Patch Installation

After upgrading to the ESA v9.1.0.0, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_9.1.0.0* patch name appears.

5. Login to the ESA Web UI.
6. Navigate to the **System > Information** page.
The ESA is updated to v9.1.0.0 in the **Installed Patches** section.

Ensure that there are no errors in the logs.

6.4.2 Verifying the PSU Patch Installation

After upgrading to the PSU v9.1.0.0, you can verify the patch installation.

► To verify the patch installation:

1. Login to the PSU CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *PSU_9.1.0.0* patch name appears.

5. Login to the PSU Web UI.
6. Navigate to the **System > Information**.

The PSU is updated to v9.1.0.0 in the **Installed Patches** section.

Note: Ensure that there are no errors in the logs.

6.5 Post Upgrade Steps

Ensure that the following steps in the following sections are performed after the ESA upgrade is completed:

6.5.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. */var/log*
 - *Installation.log* - Provides the logs for all the installed components.
 - *syslog* - Provides collective information about the syslogs.
2. */etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log*

6.5.2 Restarting the System

After the ESA patch, *ESA_PAP-ALL-64_x86-64_9.1.0.0.x-UP.pty* is installed successfully, restart the ESA machine. This ensures that the updated configurations are reflected on the ESA v9.1.0.0.

6.5.3 Restoring the Configuration File

If you have updated the configuration file and backed it up before the upgrade, then you need to restore the file using the steps provided in this section.

1. Login to the CLI Manager of the Primary ESA.
2. Navigate to **Administration > OS Console**.
3. Enter the *root* password and select **OK**.
4. Navigate to the */opt/protegility/insight/analytics/config* directory using the following command.

```
cd /opt/protegility/insight/analytics/config
```

5. Restore the *remote_cluster.json* file using the following command.

```
cp remote_cluster.json.backup remote_cluster.json
```

6. Repeat these steps on all the other nodes in the Audit Store cluster.

6.5.4 Updating the Priority IP List for Signature Verification

Signature verification jobs can only run on the ESAs, they cannot run on the PSUs. Ensure that you update the priority IP list for the default signature verification jobs after you set up the system. By default, the Primary ESA will be used for the priority IP. If you have multiple ESAs in the priority list, then additional ESAs are available to process the signature verifications jobs that must be processed.

For example, if the maximum jobs to run on an ESA is set to 4 and 10 jobs are queued to run on 2 ESAs, then 4 jobs are started on the first ESA, 4 jobs are started on the second ESA, and 2 jobs will be queued to run till an ESA job slot is free to accept and run the queued job.

For more information about scheduling jobs, refer to the section *Using the Scheduler* in the *Protegility Analytics Guide 9.1.0.5*.

For more information about signature verification jobs, refer to the section *Verifying Signatures* in the *Protegility Analytics Guide 9.1.0.5*.

Use the steps provided in this section to update the priority IP list.

1. Login to the ESA Web UI.
2. Navigate to **Analytics > Scheduler**.
3. From the **Action** column, click the **Edit** icon () for the **Signature Verification** task.
4. Update the **Priority IPs** field with the list of the ESAs available separating the IPs using commas.
5. Click **Save**.

6.5.5 Enabling *Update Audit Store Management Unicast Hosts* Task

You must enable the *Update Audit Store Management Unicast Hosts* task on all the nodes.

► To enable *Update Audit Store Management Unicast Hosts* task:

1. Login to the ESA Web UI.
2. Navigate to **System > Task Scheduler**.
3. Click the **Update Audit Store Management Unicast Hosts** task and click **Edit**.
4. Click **Enable** for the *Update Audit Store Management Unicast Hosts* tasks.
5. Click **Save** and then click **Apply** after performing the required changes.
6. Enter the *root* password and select **OK**.
7. Repeat the steps on all the nodes in the *Audit Store* cluster.

6.5.6 Enabling *Rollover Index* Task

You must enable the *Rollover Index* task on any of the nodes in the *Audit Store* cluster.

► To enable *Rollover Index* task:

1. Login to the ESA Web UI on any of the nodes in the *Audit Store* cluster.
2. Navigate to **Analytics > Scheduler > Tasks**
3. Click the **Enabled** slider to enable the *Rollover Index* task.
4. Enter the *root* password and click **Submit**.

6.5.7 Enabling the ESA LDAP on the PSU

After you upgrade the PSU, you need to switch the LDAP connection of the PSU from the local LDAP to the Primary ESA.

► To use the ESA's LDAP:

1. Login to the CLI Manager of the PSU is upgraded.
 2. Navigate to **Tools > ESA Communication**.
 3. Enter the root password and select **OK**.
 4. Use the Spacebar to clear all the check boxes.
 5. Select **Local Appliance Directory Service** and select **Set Location Now**.
 6. Select the Primary ESA if it is found, else select **YES**, specify the IP address of the Primary ESA, and select **OK**.
 7. Specify the username and password for the administrative user.
 8. Select **OK**.
 9. Select **OK**.
- The LDAP is reset to the ESA's LDAP server.

6.5.8 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

Before you begin

Keep the following information handy before the setup process:

- SMTP server details
- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is *25*.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.
Protegility Reporting requires a full email address in the Username.
7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.
A message box appears.
14. Click **EXIT** to save the settings.

6.6 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

6.6.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

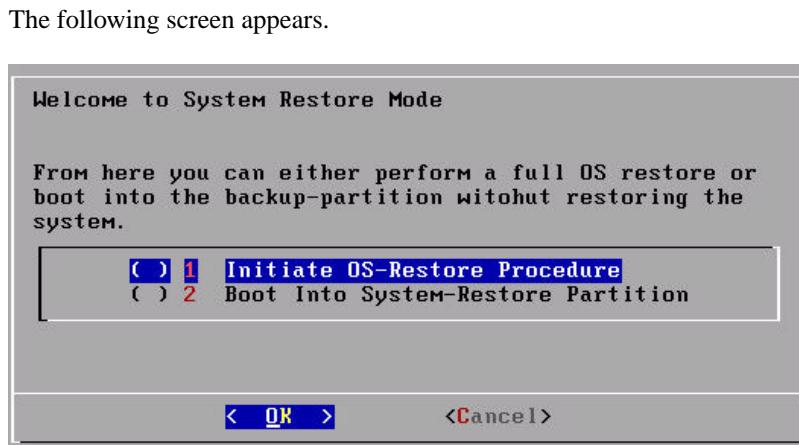
► To restore the system to the previous version:

1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

6.6.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

6.6.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

6.6.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.

3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

6.6.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

6.7 Upgrading Protectors

If you are upgrading the Protectors from v9.0.0.0 to v9.1.0.0, then ensure that the ESA is at v9.1.0.0.

Note:

For more information about the compatible data elements for the different protector versions, refer to the table [Data Element Compatibility Matrix](#).

6.7.1 Upgrading Data Security Gateway (DSG)

The Data Security Gateway (DSG) can be upgraded to the DSG v3.1.0.0. The upgrade process involves the following steps.

1. Upgrade the ESA to the version v9.1.0.0
2. Extend the ESA with the DSG Web UI by applying the *ESA_PAP-ALL-64_x86-64_9.1.0.0.2151.DSGUP-1.pty* patch.
For information about extending the ESA with the DSG Web UI, refer to the section *Extending ESA with DSG Web UI* in the [Data Security Gateway User Guide 3.1.0.0](#).
3. Reimage the DSG nodes to v3.1.0.0.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

For more information about upgrading the DSG to DSG v3.1.0.0, refer to the section *Upgrading to DSG v3.1.0.0* in the [Data Security Gateway User Guide 3.1.0.0](#).

6.7.1.1 Upgrading the DSG from v3.0.0.0 to v3.1.0.0

This section describes the steps to upgrade from the DSG v3.0.0.0 to the DSG v3.1.0.0 on the ESA.

Note:

Before upgrading to DSG v3.1.0.0, ensure that the *ESA_PAP-ALL-64_x86-64_9.0.0.0.2095-DSGUP-1.pty* patch is installed on the ESA v9.0.0.0.

For more information about applying the DSG 3.0.0.0 patch on the ESA, refer to the section [Install the DSG 3.0.0.0 patch](#).

► To install the DSG v3.1.0.0 patch on the ESA:

1. Login to the ESA Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.0.2151-DSGUP-1.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

The file upload is initiated.

Note:

Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the ESA CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the root password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *ESA_PAP-ALL-64_x86-64_9.1.0.0.2151-DSGUP-1.pty* patch file and select **Install**.
10. Select **OK**.
11. Select **Exit** on the following screen.

```
Patch has been installed successfully !!  
  
< Exit > <Show More>
```

The DSG patch is installed on the ESA and is upgraded to the DSG v3.1.0.0.

Chapter 7

Upgrading from v8.1.0.1 to v9.0.0.0

[7.1 Migrating ESA v8.1.0.1 to ESA v9.0.0.0](#)

[7.2 Installing ESA](#)

[7.3 Prerequisites](#)

[7.4 Installing the Pre-Patch on the PSU](#)

[7.5 Migrating the ESA to v9.0.0.0](#)

[7.6 Configuring the ESA v9.0.0.0](#)

[7.7 Upgrading custom files to python3](#)

[7.8 Rotating Certificates on a Single Node Audit Store Cluster](#)

[7.9 Installing the Protegility Storage Unit](#)

[7.10 Post Upgrade Steps](#)

[7.11 Restoring to the Previous Version of ESA](#)

[7.12 Upgrading Protectors](#)

This section describes the steps to upgrade the ESA, PSU, and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the PSU and protector.

7.1 Migrating ESA v8.1.0.1 to ESA v9.0.0.0

This section describes the steps for upgrading the ESAs from the v8.1.0.1 to v9.0.0.0. In this upgrade process, the configurations on the ESAs are exported from v8.1.0.1 and imported on v9.0.0.0. The following figure illustrates a sample TAC environment on which the ESAs must be upgraded to v9.0.0.0.

Note:

Ensure that at least two the ESAs are in a TAC.

Ensure that the ESA 1, ESA 2, PSU 1, and PSU 2 are in a Audit Store Cluster.

Ensure that you do not make any changes to configuration, policy, or CoP during the upgrade process.

Ensure that you install the pre-patch on PSU 1 or PSU 2.

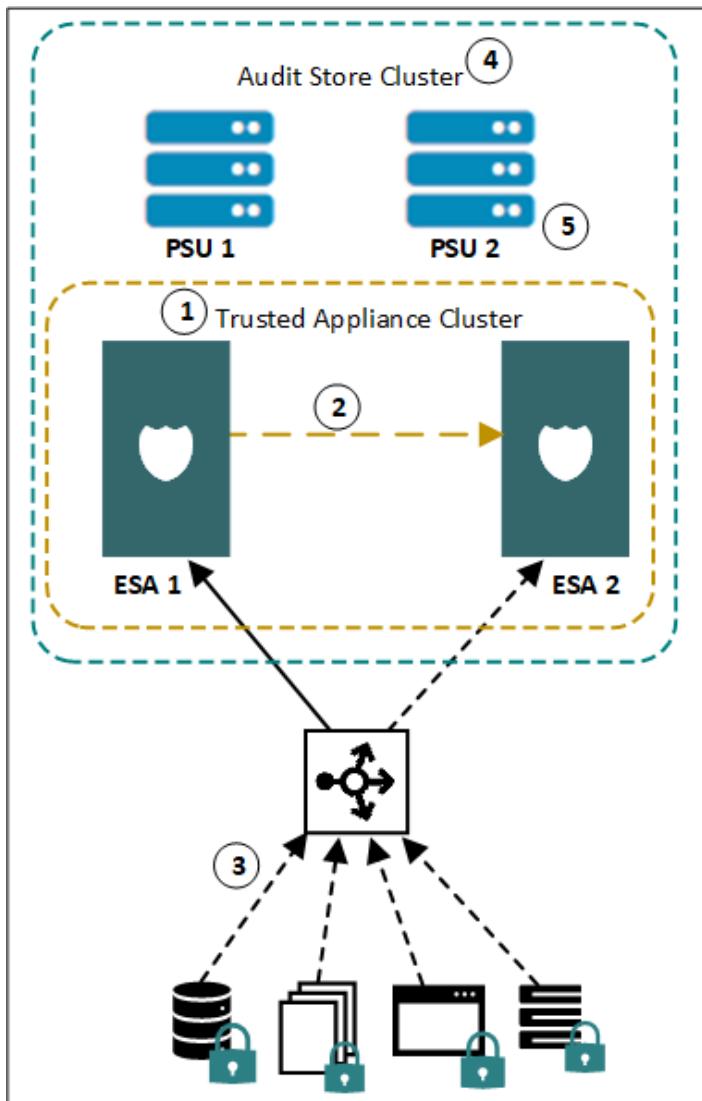


Figure 7-1: ESA v8.1.0.1 in a TAC

As shown in the setup,

1. The TAC is established between the primary appliance **ESA 1** and a stand-by appliance **ESA 2**.
2. Data replication for policies, forensics, or DSG configurations takes place from the **ESA 1** to the **ESA 2**.
3. Protectors communicate with the load balancer that balances the requests between the **ESA 1** and the **ESA 2**.
4. Audit Store cluster is enabled for the ESAs.
5. PSU 1 and PSU 2 are added as a part of the Audit Store cluster.

The following figure illustrates the v9.0.0.0 setup after the migration process is completed.

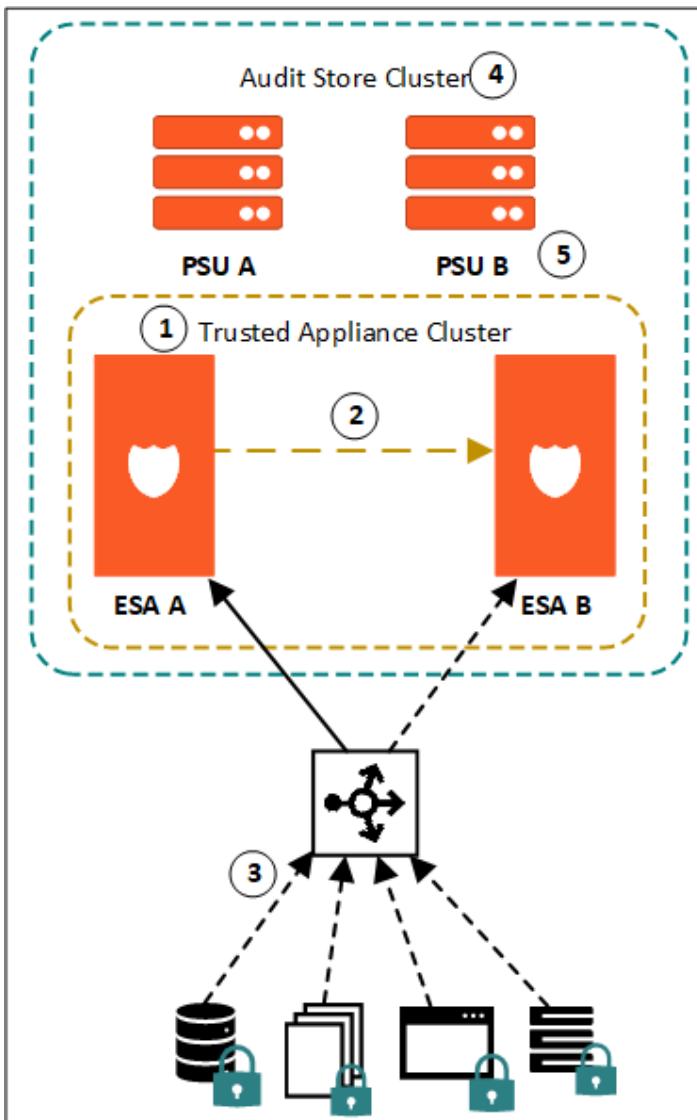


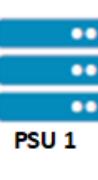
Figure 7-2: ESA v9.0.0.0

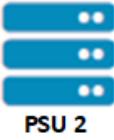
1. The TAC is established between the primary appliance **ESA A** and a stand-by appliance **ESA B**.
2. Data replication for policies, forensics, or DSG configurations takes place from the **ESA A** to the **ESA B**.
3. Protectors communicate with the load balancer that balances the requests between the upgraded **ESA A** and **ESA B**.
4. Audit Store cluster is enabled for the ESAs.
5. PSU A and PSU B are added as a part of the Audit Store cluster.

7.1.1 Upgrade Process: Flow Diagram

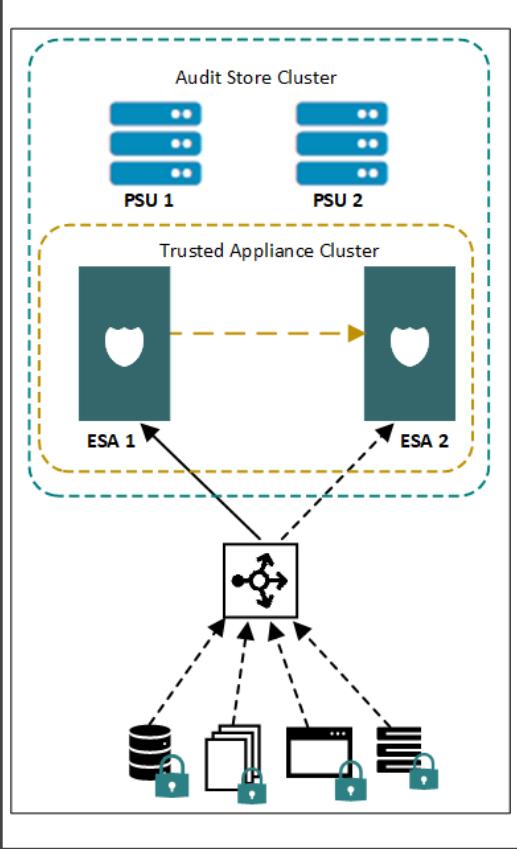
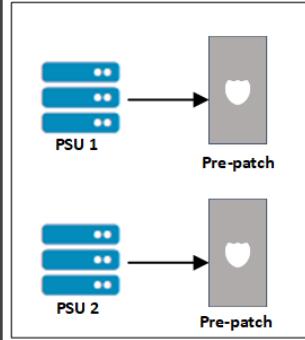
A diagrammatic representation of the upgrade process is provided in this section. The legend describes the elements used in the flow diagram.

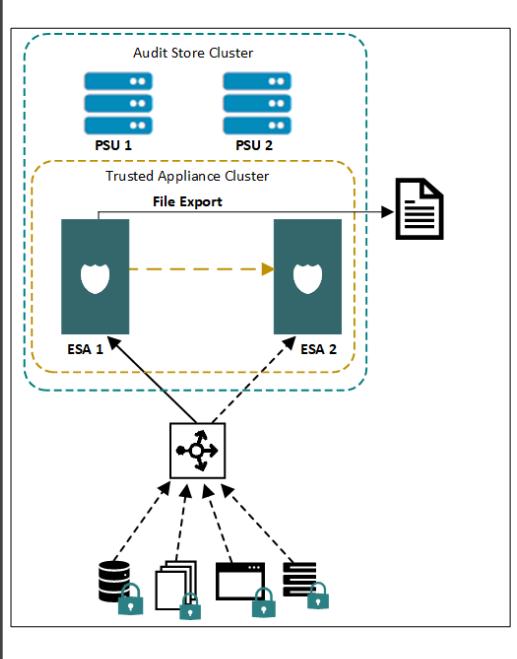
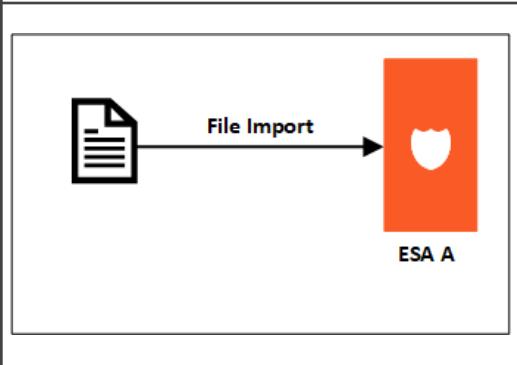
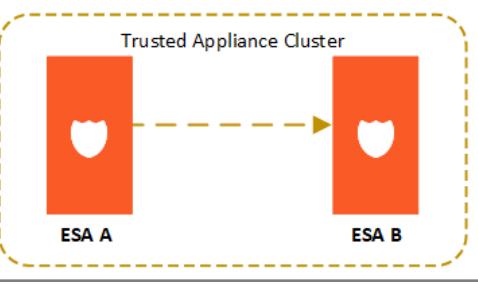
Legend

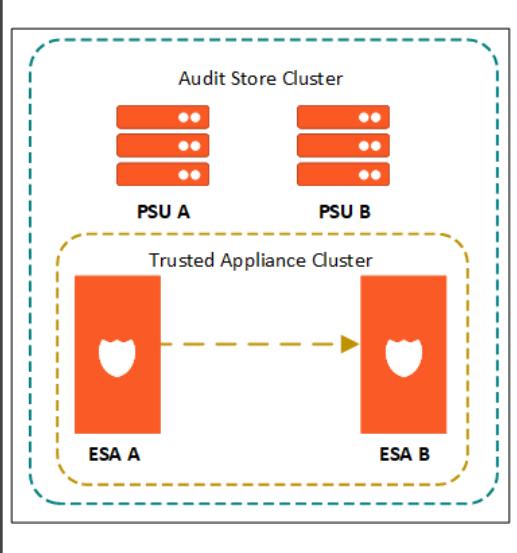
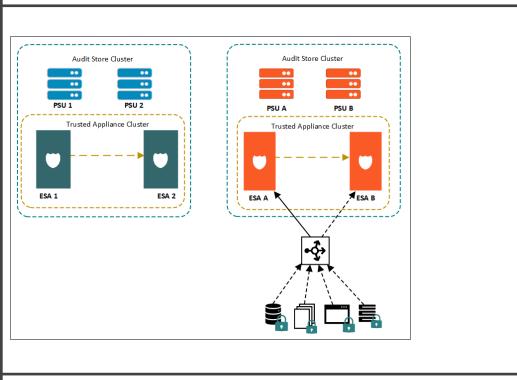
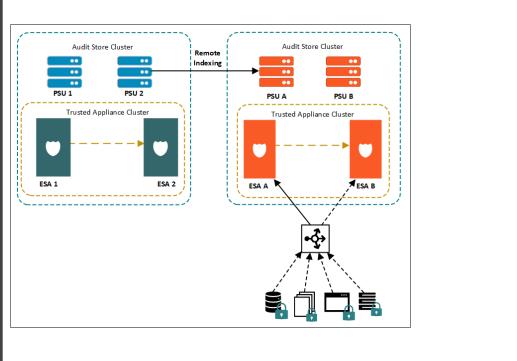
Icon	Description	Version
 ESA 1	ESA Node appliance (Server)	v8.1.0.1
 ESA 2	ESA Node appliance	v8.1.0.1
 ESA A	ESA Node appliance (Server)	v9.0.0.0
 ESA B	ESA Node appliance	v9.0.0.0
 ESA Pre-v9.0.0.0	Pre-patch for Protegility Storage Units (PSU) <i>PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty</i>	Pre-v9.0.0.0
 PSU 1	Protegility Storage Unit (PSU)	v8.1.0.1

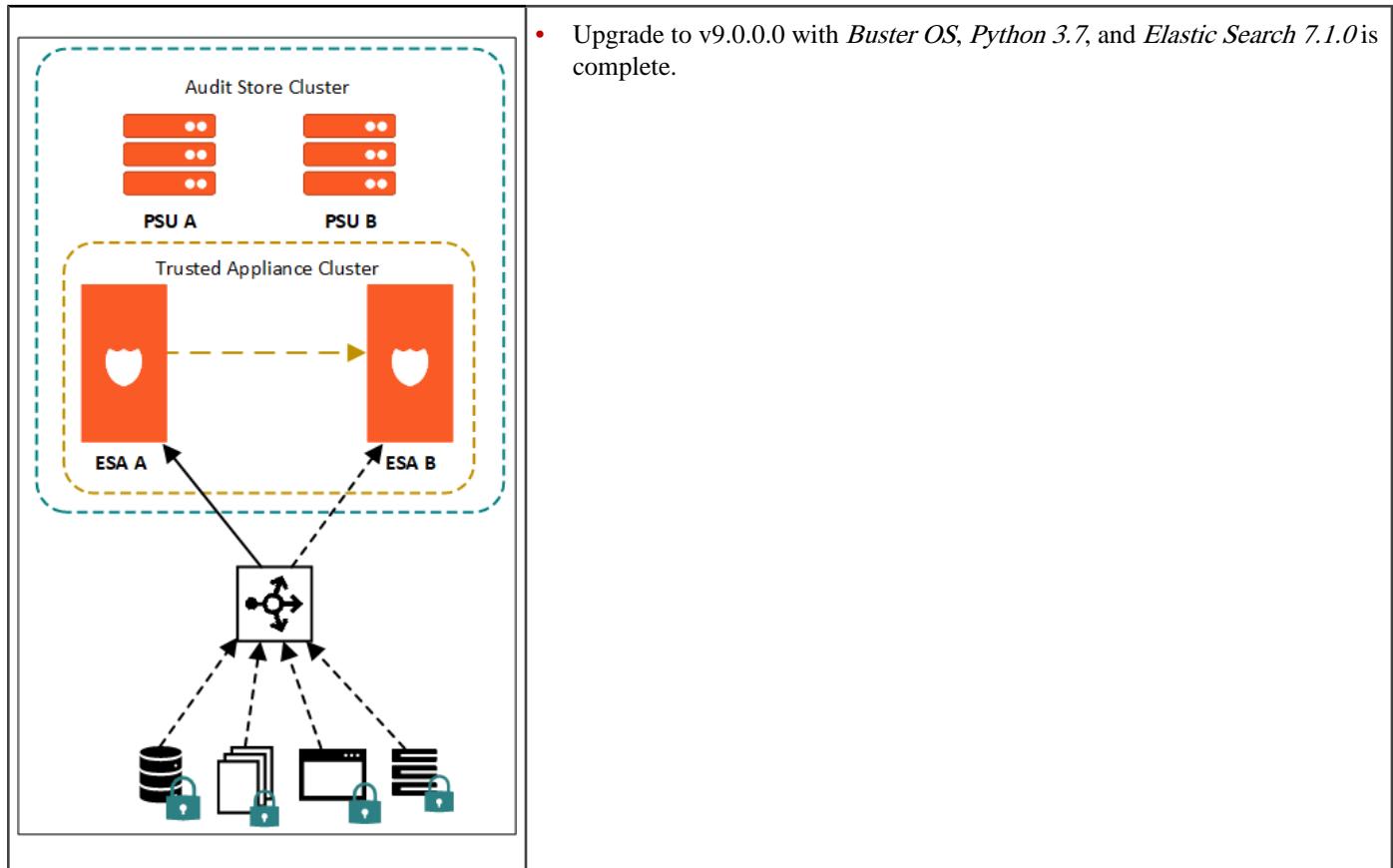
Icon	Description	Version
	Protegity Storage Unit (PSU)	v8.1.0.1
	Protegity Storage Unit (PSU)	v9.0.0.0
	Protegity Storage Unit (PSU)	v9.0.0.0
	Trusted Appliances Cluster	<ul style="list-style-type: none"> • v8.1.0.1 • v9.0.0.0
	Audit Store Cluster	<ul style="list-style-type: none"> • v8.1.0.1 • v9.0.0.0
	Protectors	<ul style="list-style-type: none"> • v8.1.0.1 • v9.0.0.0
	Load Balancer	N/A

The following is a diagrammatic representation of the overview of the upgrade process from v8.1.0.1 to v9.0.0.0.

	<ul style="list-style-type: none"> TAC contains a server node appliance ESA 1 and appliance ESA 2. Data replication for policies or DSG configurations take place from the ESA 1 to the ESA 2. Protectors communicate with the load balancer that routes the requests to the ESA 1 or ESA 2. Ensure that both ESA 1 and ESA 2 in the TAC are in sync and have the latest policies, configurations, DSG rulesets, and so on. The PSUs are in the Audit Store cluster.
 ESA A	<ul style="list-style-type: none"> Create the <i>ESA A</i> on v9.0.0.0. The ESA will have the <i>Ext4</i> file system, <i>Buster OS</i>, and <i>Python3</i> by default.
	<ul style="list-style-type: none"> Apply the pre-patch <i>PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty</i> on the PSU 1 and PSU 2.

	<ul style="list-style-type: none"> Export all the configurations, policy data, custom configurations, and so on, from the ESA 1 to a file using the Backup & Restore functionality. Transfer the exported file to the ESA A.
	<ul style="list-style-type: none"> Import the configurations, policy data, custom configurations on ESA A. Complete the post upgrade steps on ESA A.
 ESA A	<ul style="list-style-type: none"> Upgrade the scripts to <i>python3</i>. Rotate Audit Store certificates on ESA A.
	<ul style="list-style-type: none"> Create a ESA B. Join ESA A and ESA B in a Trusted Appliances Cluster.

	<ul style="list-style-type: none"> • Create two new PSUs (PSU A and PSU B) on v9.0.0.0. • Initialize Analytics on the ESA A. • Join the ESA A, ESA B, PSU A, and PSU B to create an Audit Store Cluster. • Configure <i>td-agent</i> on the ESA A and ESA B in the Audit store cluster. • Configure audit store roles on the ESA A and ESA B nodes. <p>Note: Ensure that the roles on the ESAs are changed to <i>Master</i>.</p>
	<ul style="list-style-type: none"> • Redirect the traffic from the ESA v8.1.0.1 to the ESA v9.0.0.0. • Update 8.1.0.1 protector configurations to point to the PSU v9.0.0.0. • Upgrade the DSGs to their latest version.
	<ul style="list-style-type: none"> • If you are using the PSUs, then initiate remote re-indexing to the PSU A. • After re-indexing is completed, shutdown ESA1, ESA 2, PSU1 and PSU2.



7.1.2 Upgrade Process: Step-by-step Procedure

To upgrade the ESA appliances from v8.1.0.1 to v9.0.0.0, you must first perform the export operation on the v8.1.0.1 machine. After the file is successfully exported, you must then import the file on the v9.0.0.0 machine. After the file is successfully imported on the ESA v9.0.0.0, perform the required steps to complete the upgrade.

This section describes the procedure to upgrade the ESA v8.1.0.1 to v9.0.0.0.

Note:

Ensure that you perform the procedure in the prescribed sequence for a successful upgrade.

Before you begin

- At least two ESAs must be in a TAC .
- The two ESAs and two PSUs must be in an Audit Store Cluster.

For more information on Audit Store Cluster, refer to the [Audit Store Guide 9.1.0.5](#).

- Install the ESA A and ESA B.

For more information on installing the ESA, refer to the [Protegility Enterprise Security Administrator Guide 9.1.0.5](#).

- If you are using the Protegility Storage Units, then install two PSUs, that is, PSU A and PSU B.

For more information on installing the PSU on a new machine, refer to the [Protegility Storage Unit Guide 9.1.0.0](#).

- You must not make any changes to configuration, policy, or CoP on any appliance during the upgrade process.
- All the [prerequisites](#) are met before beginning the upgrade process.

For more information on the prerequisites, refer to the section [Prerequisites](#).

► To upgrade to v9.0.0.0:

1. Ensure that the ESA 1 and ESA 2 in the TAC are in sync and have the latest policies and configurations.
2. If you are using the PSUs, then ensure that the ESA 1, ESA 2, PSU 1, and PSU 2 are in an Audit Store Cluster.
3. Create the ESA A on v9.0.0.0.

For more information on installing the ESA on v9.0.0.0, refer to the section [Installing ESA](#).

4. Install the *PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty* pre-patch on the PSU 1 or PSU 2.

For more information about installing the pre-patch, refer to the section [Installing the Pre-Patch on the PSU](#).

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

5. From the ESA 1, export all the configurations, policy data, custom configurations, and so on, to a file using **Backup & Restore** functionality.

For more information on exporting a file, refer to the section [Migrating the ESA to v9.0.0.0](#).

6. Transfer the exported file to the ESA A using your preferred method, such as, SCP, FTP, and so on.

Note:

If you are using the SCP or FTP, then ensure that the exported file is placed in the */opt/product_exports* directory and permissions for the file are set to *755*.

7. Import the configurations, policy data, custom configurations on the ESA A.

For more information on importing configurations, refer to the section [Migrating the ESA to v9.0.0.0](#).

8. Configure the required settings on the ESA A.

For more information about configuring the required settings, refer to the section [Configuring the ESA v9.0.0.0](#).

9. Update the scripts to *python3* on the ESA A.

For more information about upgrading the scripts to *python3*, refer to the section [Upgrading custom files to python3](#).

10. Rotate the Audit Store certificates on the ESA A.

For more information about rotating the audit store certificates, refer to the section [Rotating Certificates on a Single Node Audit Store Cluster](#).

11. Create the ESA B on v9.0.0.0.

For more information on installing the ESA on v9.0.0.0, refer to the section [Installing ESA](#).

12. Join the ESA A and the ESA B in a Trusted Appliance Cluster.

For more information on creating a TAC, refer to the section [Trusted Appliances Cluster \(TAC\)](#) in the [Appliances Overview Guide 9.0.0.0](#).

13. Configure the Audit Store Cluster on the ESA A, ESA B, PSU A, and PSU B.

Note:

Ensure that you add one appliance at a time.

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

14. Configure the *td-agent* on the ESA A and ESA B in the Audit Store cluster.

For more information about configuring the *td-agent*, refer to the section [Configuring td-agent in the Audit Store Cluster](#).

15. Change the roles on the ESA A and ESA B to *Master*.

Note:

Ensure that you add one appliance at a time.

For more information on changing roles in the ESA, refer to the section [Trusted Appliances Cluster](#) in the [Protegility Appliances Overview Guide 9.1.0.5](#).

16. Redirect the traffic from the ESA 2 to the ESA A and ESA B.

17. Update the v8.1.0.1 protector configurations to point to the PSU v9.0.0.0.

18. (Optional): Upgrade the DSGs to their latest version.

19. If you are using the PSUs, then initiate remote re-indexing to the ESA A.

For more information on initiating remote re-indexing, refer to the section [Migrating Configuration Settings and Logs](#).

20. After re-indexing is completed, shutdown the the ESA 1, ESA 2, PSU 1, and PSU 2.

21. The upgrade process is successfully completed.

7.2 Installing ESA

You can install the ESA on-premise or a cloud platform, such as, AWS, Azure, or GCP. When you upgrade from a previous version, the ESA is available as patch. The following are the different ways of installing the ESA:

- **ISO Installation:** This installation is performed for an on-premise environment where the ESA is installed on a local system using an ESA ISO is provided by Protegility. The installation of the ISO begins by installing the hardened version of Linux on your system, setting up the network, and configuring date/time. This is then followed by updating the location, setting up OS user accounts, and installing the ESA-related components.

For more information about installing the ESA using ISO, refer to the section [Installing the ESA On-Premise](#) in the [Protegility Installation Guide 9.1.0.5](#).

- **Cloud Platforms:** On Cloud platforms, such as, AWS, Azure, or GCP, the ESA images for the respective cloud are generated and provided by Protegility. In these images, the ESA is installed with specific components. You must obtain the image from Protegility and create an instance on the cloud platform. After creating the instance, you run certain steps for finalizing the installation.

For more information about installing the ESA on cloud platforms, refer to the section [Installing Appliances on Cloud Platforms](#) in the [Protegility Installation Guide 9.1.0.5](#).

Note: A temporary license is provided by default when you first install the Appliance and is valid for 30 days from the date of this installation. To continue using Protegility features, you have to obtain a validated license before your temporary license expires.

For more information about licensing, refer to [Protegility Data Security Platform Licensing Guide 9.0.0.0](#).

7.3 Prerequisites

The prerequisites for upgrading the ESA must be preformed on the following components:

- Accounts
- Backup and Restore
- Installations and Hardware Requirements
- Trusted Appliances Cluster (TAC)
- Keys
- Customized files (Configuration files, Certificates)
- Install the pre-patch on a PSU in the v8.1.0.1 Audit Store cluster

Note: If you are using an external SIEM, then complete the steps from the section [Appendix E: Optional: Updating settings for External Databases](#).

7.3.1 Accounts

The administrative account used for upgrading the ESA must be active.

Note:

Ensure to make a note of the required OS level user before upgrading the ESA. These users are not exported as a part of the migration process. After moving to the upgraded ESA, you must create the OS level users.

For more information about the OS level users, refer to the Protegility Appliances Overview Guide 9.1.0.0.

7.3.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section [Working with Backup and Restore](#) in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a backup of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

7.3.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

7.3.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

7.3.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before initiating the upgrade process.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating the snapshots from the respective cloud platforms, refer to the [Protegility Appliances Overview Guide 9.1.0.5](#).

7.3.3 Installations and Hardware Requirements

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have the at least the following components:

- On platform v8.1.0.1:
 - 2 ESAs
 - 2 Protegility Storage Units (PSUs)
- On platform v9.0.0.0:
 - 2 ESAs
 - If you are using the Protegility Storage Units, then 2 PSUs

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

Installation Requirements

- An ESA v8.1.0.1 must be available to perform the *Export/Import* operation.
- Ensure that the ESA v9.0.0.0, the **Max File Upload Size** is more than the size of the exported file. You can navigate to **Settings > Network > Web Settings** to modify the **Max File Upload Size**.

7.3.4 ESA Settings

Ensure to make a note of the required settings while moving from the ESA v8.1.0.1 to v9.0.0.0. These settings are not exported as a part of the migration process. After moving to the ESA v9.0.0.0, you must configure the following settings as a part of the post upgrade steps:

- SMTP Settings
- Scheduled tasks
- Grub Settings
- User notifications on dashboard, if any
- Local_admin permissions



- Service Account Passwords
- OS Users
- Add/Remove services
- SNMP configuration
- Preferences Settings
- Antivirus options and settings
- Firewall Settings
- Open ports
- Two-Factor Authentication

7.3.5 Trusted Appliances Cluster (TAC)

At least two ESAs must be in a Trusted Appliance Cluster.

For more information about the Trusted Appliances Cluster, refer to the section *Trusted Appliances Cluster* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

7.3.6 Two-factor Authentication

If you have two-factor authentication enabled with per-user shared-secret, then you must revoke the shared secrets for all the users. After successfully revoking the shared secrets, you must disable the two-factor authentication.

To revoke the shared secrets, perform the following steps.

1. From the Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. From the **Settings**, change the **Storage** type to **Local file-system**.
3. From the OS Console, remove the file containing shared secret for each user using the following command:

```
rm /opt/protegility/.OS/users/<username>/2FA.vcode
```

7.3.7 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the [Protegility Key Management Guide 9.1.0.0](#).

7.3.8 License

Ensure that you have a valid license before upgrading.

Note:

After migration, if the license status is *invalid*, then contact [Protegility Support](#).

7.3.9 Customized Files (Configuration Files and Certificates)

Exclude Files

The *exclude* file present in the */opt/ExportImport/filelist* directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section *Exporting Custom Files* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Custom files with python2 scripts

If you have modified any custom files, such as, *check_password.py*, *check_username.py*, *pty_get_username_from_certificate.py*, and so on, then these must be listed in the *customer.custom* file.

CloudWatch Files

To export the *CloudWatch* configurations, you must list the cloudwatch configurations in the *customer.custom* file to export the data in the upgraded ESA.

7.4 Installing the Pre-Patch on the PSU

The pre-patch must be installed on any *one* PSU in the Audit Store cluster during the upgrade process. Upload the pre-patch using the PSU Web UI and then install it using the CLI Manager. The steps to install the pre-patch on the existing PSU v8.1.0.1 is provided in this section.

1. Login to the PSU Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the pre-patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the **PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty** file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the *Release Notes* of the respective patch.

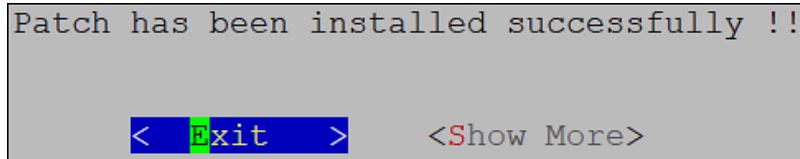
The file upload is initiated.

5. Wait till the **PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty** file appears in the **Uploaded Files** list.

Note: Do not click **Install**, you must install the pre-patch from the CLI Manager.

6. Login to the PSU CLI Manager with administrator credentials.
7. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.

8. Enter the *root* password.
The patch management screen appears.
9. Select **Install a Patch**.
10. Select the *PSU_PAP-ALL-64_x86-64_8.1.0.1.x.FE-1.pty* pre-patch file and select **Install**.
11. Select **Exit** on the following screen.



The pre-patch is installed.

7.5 Migrating the ESA to v9.0.0.0

This section describes the steps to upgrade to the ESA v9.0.0.0.

► To upgrade to the ESA v9.0.0.0:

1. On the current version of the ESA (*ESA 1*), login to the WebUI using the *administrative* credentials.
2. Navigate to **System > Backup & Restore > Export**.
3. From the **Export type** field, select the **To file** option.
4. From the **Data To export** field, select the required options.

Note:

It is recommended to select all the options while performing the export operation.

Note:

If you want to export the configuration for the DSG, then select the *Export Gateway Configuration Files* and perform the export operation.

5. Click **Export**.

The following screen appears.

Output File

Export Name	<input type="text"/>
<input type="checkbox"/> Overwrite existing file (if exists)	
Password	<input type="password"/> Please input password
<input type="password"/> Please confirm password	
Export Description(optional)	<input type="text"/>
Confirm Cancel	

6. Enter the information in the **Export Name**, **Password**, and **Export Description** fields and select **Confirm**.
7. Download the exported file.
8. Upload the exported file on the *ESA A* v9.0.0.0 using your preferred method, such as, SCP, FTP, and so on.

Note:

If you are using the SCP or FTP, then ensure that the exported file is placed in the */opt/product_exports* directory and permissions for the file are set to *755*.

Note:

Ensure that the **Max File Upload Size** is more than the size of the exported file. You can navigate to **Settings > Network > Web Settings** to modify the **Max File Upload Size**.

9. Login to the *ESA A* v9.0.0.0 WebUI using the *administrative* credentials.
10. Navigate to **System > Backup & Restore > Import**.

Note: If you are importing the configuration for the DSG appliance, then ensure to apply the DSG patch on the ESA before importing the configurations.

For more information about applying the DSG patch on the ESA, refer to the section [Install the DSG 3.0.0.0 patch](#).

The following screen appears.

Import

Select an exported file...	Please select one file to show more information
<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>	

11. Select the exported file and click **Import**.

Import	
<input type="file"/>	Size: [REDACTED] Creation Time: [REDACTED] Description: [REDACTED]
Delete Import Download	This file provides the following import options: - OS configuration - Web settings - SSH settings - SSH server configuration and Keys - Certificates - Management and WebService Certificates - Firewall settings - Appliance Authentication Settings - Appliance JWT Configuration - Appliance SSO Configuration - Time-zone and NTP settings - OS Services Status - Appliance FIM Policies and Settings - User custom list of files - LDAP Server - Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery - Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster - Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster - Import policy manager web ui settings

12. Select the required options except **Appliance Configuration (ALL)** and **Certificates**.

Title	Description																												
Component: OS v 8.0.1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input type="checkbox"/> Appliance Configuration (ALL)</td><td style="padding: 2px;">OS configuration more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Web Settings</td><td style="padding: 2px;">Web settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> SSH Settings</td><td style="padding: 2px;">SSH settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Server Identity</td><td style="padding: 2px;">SSH server configuration and Keys more...</td></tr> <tr><td style="padding: 2px;"><input type="checkbox"/> Certificates</td><td style="padding: 2px;">Certificates more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Management and WebService Certificates</td><td style="padding: 2px;">Management and WebService Certificates more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Firewall Settings</td><td style="padding: 2px;">Firewall settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Authentication Settings</td><td style="padding: 2px;">Appliance Authentication Settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> JWT Configuration</td><td style="padding: 2px;">Appliance JWT Configuration more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> SSO Configuration</td><td style="padding: 2px;">Appliance SSO Configuration more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Timezone And NTP</td><td style="padding: 2px;">Time-zone and NTP settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Services Status</td><td style="padding: 2px;">OS Services Status more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> FIM Policies and Settings</td><td style="padding: 2px;">Appliance FIM Policies and Settings more...</td></tr> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Custom Files and folders</td><td style="padding: 2px;">User custom list of files more...</td></tr> </table>		<input type="checkbox"/> Appliance Configuration (ALL)	OS configuration more...	<input checked="" type="checkbox"/> Web Settings	Web settings more...	<input checked="" type="checkbox"/> SSH Settings	SSH settings more...	<input checked="" type="checkbox"/> Server Identity	SSH server configuration and Keys more...	<input type="checkbox"/> Certificates	Certificates more...	<input checked="" type="checkbox"/> Management and WebService Certificates	Management and WebService Certificates more...	<input checked="" type="checkbox"/> Firewall Settings	Firewall settings more...	<input checked="" type="checkbox"/> Authentication Settings	Appliance Authentication Settings more...	<input checked="" type="checkbox"/> JWT Configuration	Appliance JWT Configuration more...	<input checked="" type="checkbox"/> SSO Configuration	Appliance SSO Configuration more...	<input checked="" type="checkbox"/> Timezone And NTP	Time-zone and NTP settings more...	<input checked="" type="checkbox"/> Services Status	OS Services Status more...	<input checked="" type="checkbox"/> FIM Policies and Settings	Appliance FIM Policies and Settings more...	<input checked="" type="checkbox"/> Custom Files and folders	User custom list of files more...
<input type="checkbox"/> Appliance Configuration (ALL)	OS configuration more...																												
<input checked="" type="checkbox"/> Web Settings	Web settings more...																												
<input checked="" type="checkbox"/> SSH Settings	SSH settings more...																												
<input checked="" type="checkbox"/> Server Identity	SSH server configuration and Keys more...																												
<input type="checkbox"/> Certificates	Certificates more...																												
<input checked="" type="checkbox"/> Management and WebService Certificates	Management and WebService Certificates more...																												
<input checked="" type="checkbox"/> Firewall Settings	Firewall settings more...																												
<input checked="" type="checkbox"/> Authentication Settings	Appliance Authentication Settings more...																												
<input checked="" type="checkbox"/> JWT Configuration	Appliance JWT Configuration more...																												
<input checked="" type="checkbox"/> SSO Configuration	Appliance SSO Configuration more...																												
<input checked="" type="checkbox"/> Timezone And NTP	Time-zone and NTP settings more...																												
<input checked="" type="checkbox"/> Services Status	OS Services Status more...																												
<input checked="" type="checkbox"/> FIM Policies and Settings	Appliance FIM Policies and Settings more...																												
<input checked="" type="checkbox"/> Custom Files and folders	User custom list of files more...																												
Component: LDAP v 7.1.2 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> LDAP Server</td><td style="padding: 2px;">LDAP Server</td></tr> </table>		<input checked="" type="checkbox"/> LDAP Server	LDAP Server																										
<input checked="" type="checkbox"/> LDAP Server	LDAP Server																												
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data</td><td style="padding: 2px;">Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery more...</td></tr> </table>		<input checked="" type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data	Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery more...																										
<input checked="" type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data	Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery more...																												
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data</td><td style="padding: 2px;">Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster more...</td></tr> </table>		<input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data	Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster more...																										
<input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data	Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster more...																												
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs, Data without HSM</td><td style="padding: 2px;">Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster more...</td></tr> </table>		<input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs, Data without HSM	Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster more...																										
<input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs, Data without HSM	Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster more...																												
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;"><input checked="" type="checkbox"/> Policy Manager Web UI Settings</td><td style="padding: 2px;">Import policy manager web ui settings more...</td></tr> </table>		<input checked="" type="checkbox"/> Policy Manager Web UI Settings	Import policy manager web ui settings more...																										
<input checked="" type="checkbox"/> Policy Manager Web UI Settings	Import policy manager web ui settings more...																												
Password: <input type="password"/> Import Cancel																													

13. Click **Import**.

A message on the screen is displayed once the file is successfully imported.

7.6 Configuring the ESA v9.0.0.0

While migrating the ESA to v9.0.0.0, the following settings are not retained. You must configure the following settings after migrating to the ESA v9.0.0.0.

SMTP Settings

You must set up an email server that supports the notification features.

For more information about configuring the SMTP settings, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Scheduled Tasks

Using **System > Task Scheduler** you can schedule appliance tasks to run automatically. You can create or manage tasks from the ESA Web UI.

For more information about configuring the scheduled tasks, refer to the section *Scheduling Appliance Tasks* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Grub Settings

To enhance security of the Protegility appliances on-premise, the GRUB menu can be protected by setting a username and password. It is recommended to secure the appliance using the GRUB settings.

For more information about securing the GRUB, refer to the section *Securing the GRand Unified Bootloader (GRUB)* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Local_admin permissions

By default, the *local_admin* user cannot log into the CLI Manager using SSH or log into the Web UI. However, you can configure this access using the tool, which changes the *local_admin* account permissions.

For more information about enabling the *local_admin* permissions, refer to the section *Changing the Local Admin Account Permission* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Service Account Passwords

Service Account users are *service_admin* and *service_viewer*. They are used for internal operations of components that do not support LDAP, such as Management Server internal users and Management Server Postgres database. You cannot log into the Appliance Web UI, Reports Management (for the ESA), or CLI Manager using service accounts users.

For more information about changing the service accounts passwords, refer to the section *Changing Service Accounts Passwords* in the *Protegility Appliances Overview Guide 9.1.0.5*.

OS Users

You must configure the *OS Users* on the ESA v9.0.0.0.

For more information about OS Users, refer to the section *Managing Local OS Users* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Add/Remove services

Using Add/Remove Services tool, you can install the necessary products or remove already installed ones. You must add or remove the services which were present on the ESA v7.2.1.

For more information about adding or removing service, refer to the section *Add/Remove Services* in the *Protegility Appliances Overview Guide 9.1.0.5*.

SNMP configuration

SNMP allows a remote machine to query different performance status of the Appliance, such as, start the service, set listening address, show or set community string, or refresh the service.

For more information about configuring SNMP, refer to the section *Configuring SNMP* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Preferences Settings

You must set up your console preferences using the Preferences menu.

For more information about preferences settings, refer to the section *Working with Preferences* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Antivirus options and settings

The AntiVirus program uses ClamAV, an open source and cross-platform antivirus engine designed to detect malicious trojan, virus, and malware threats. A single file or directory, or the whole system can be scanned. Infected files are logged and can be deleted or moved to a different location, as required.

For more information about configuring antivirus, refer to the section *Working with Preferences* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Open ports

The ports in a network are communication channels through which information flows from one system to another. A list of ports that must be configured in your environment to access the features and services on the Protegility appliances.

For more information about open ports, refer to the section *Open Listening Ports* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Two-Factor Authentication

The two factor authentication is a verification process where two recognized factors are used to identify you before granting you access to a system or website. In addition to your password, you must correctly enter a different numeric one-time passcode or the verification code to finish the login process. This provides an extra layer of security to the traditional authentication method.

Note:

The appliance must be configured to local LDAP to support Two-Factor Authentication.

For more information about two-factor authentication, refer to the section *Configuring Appliance Two Factor Authentication* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

7.7 Upgrading custom files to python3

From v9.0.0.0, the support for *python2* is disabled.

Therefore, if you have modified any of the files in the previous version of the ESA including the following, then ensure that they are compatible with *python3*:

- */etc/ksa/check_password.py*
- */etc/ksa/check_username.py*
- */etc/ksa/pty_get_username_from_certificate.py*

You can run the following command to check if these files are *python3* compatible.

```
python3 -m compileall <path_to_file>
```

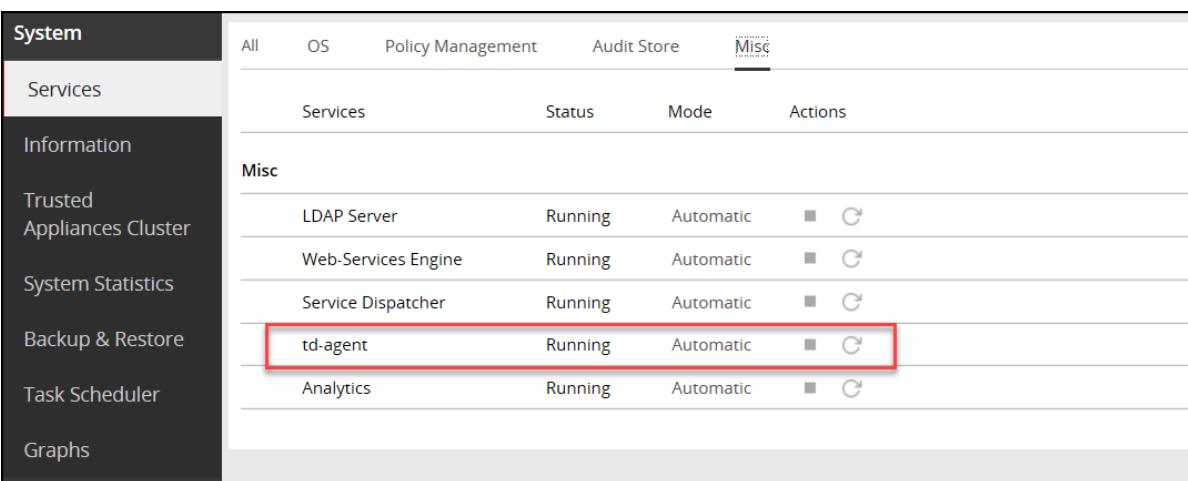
7.8 Rotating Certificates on a Single Node Audit Store Cluster

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 Protegity certificate and keys. For rotating custom certificates, refer to the section *Updating Audit Store Custom Certificates* in the *Audit Store Guide 9.1.0.5*.

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

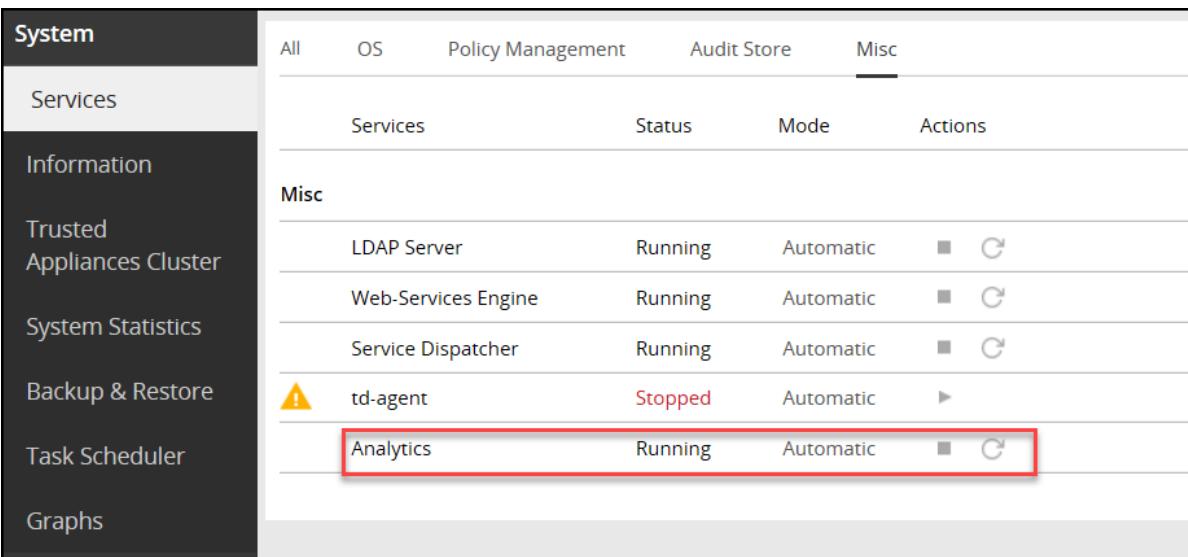
Note: Skip this step if *Analytics* is not initialized.



System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Misc						
	LDAP Server	Running	Automatic	<input type="checkbox"/>		
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>		
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>		
	td-agent	Running	Automatic	<input type="checkbox"/>		
	Analytics	Running	Automatic	<input type="checkbox"/>		

Figure 7-3: Stopping *td-agent*

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



System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Misc						
	LDAP Server	Running	Automatic	<input type="checkbox"/>		
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>		
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>		
	td-agent	Stopped	Automatic	<input type="checkbox"/>		
	Analytics	Running	Automatic	<input type="checkbox"/>		

Figure 7-4: Stopping *Analytics*

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



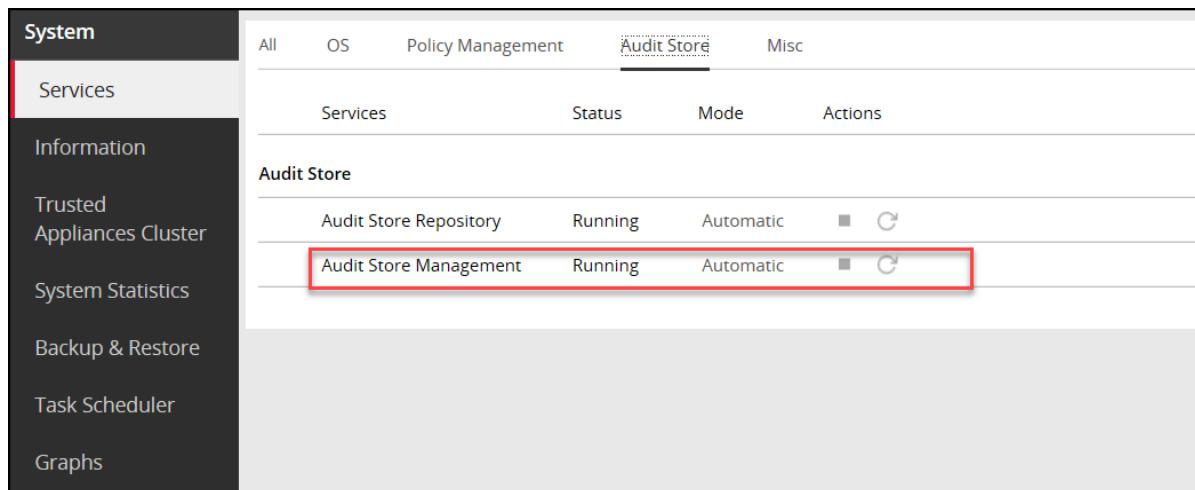


Figure 7-5: Stopping Audit Store Management

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

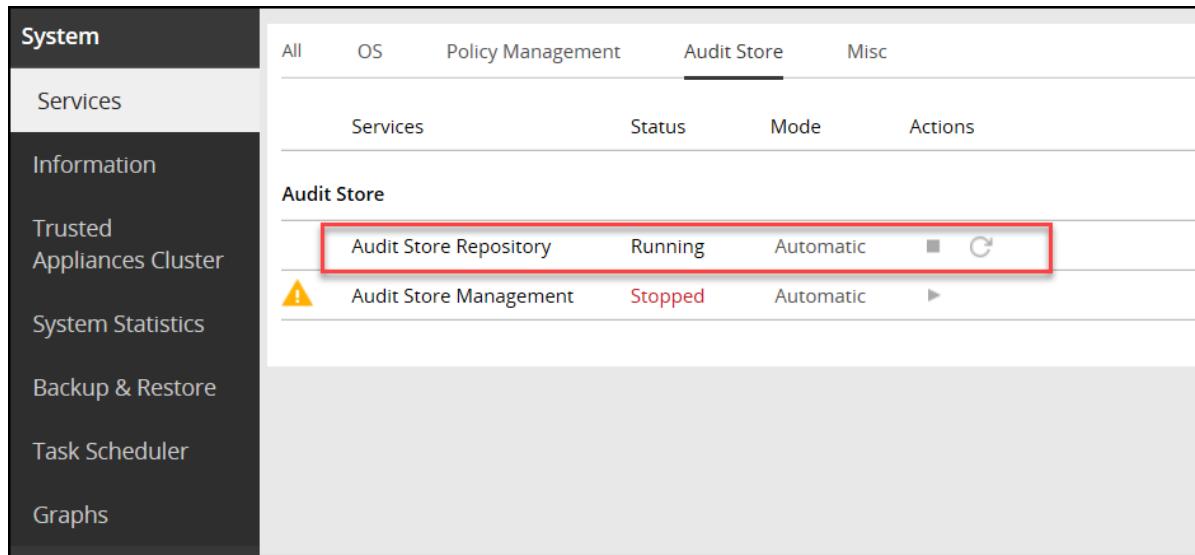


Figure 7-6: Stopping Audit Store Repository

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 7-7: Rotating Certificates

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

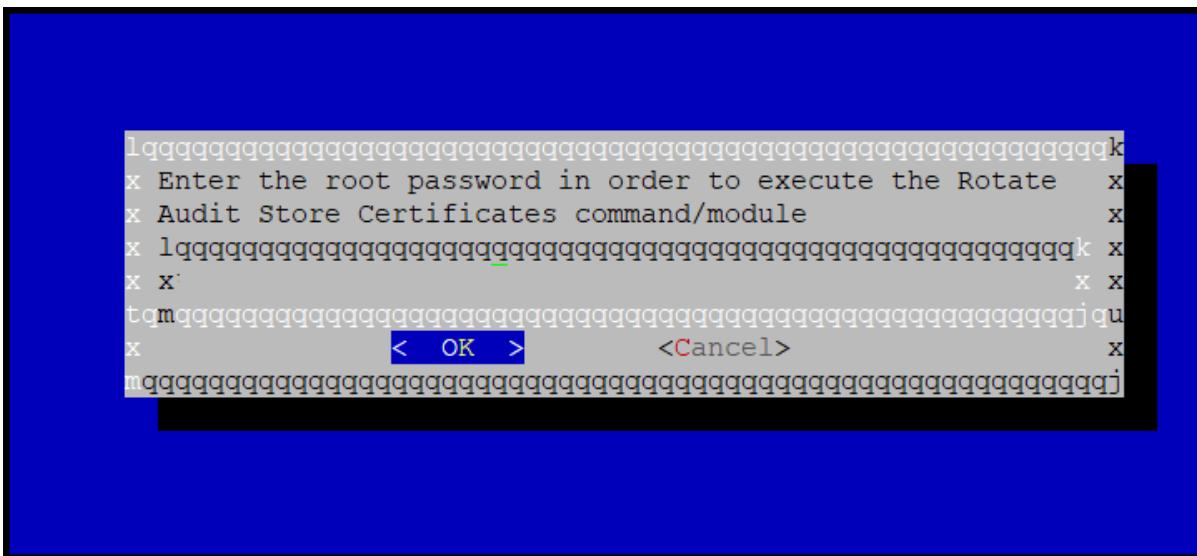


Figure 7-8: Root Password

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

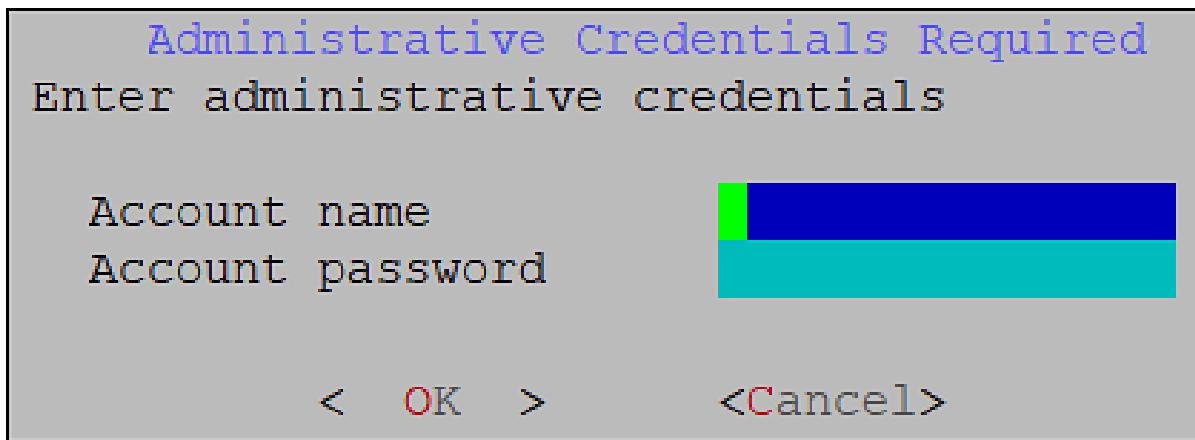


Figure 7-9: Admin Details

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

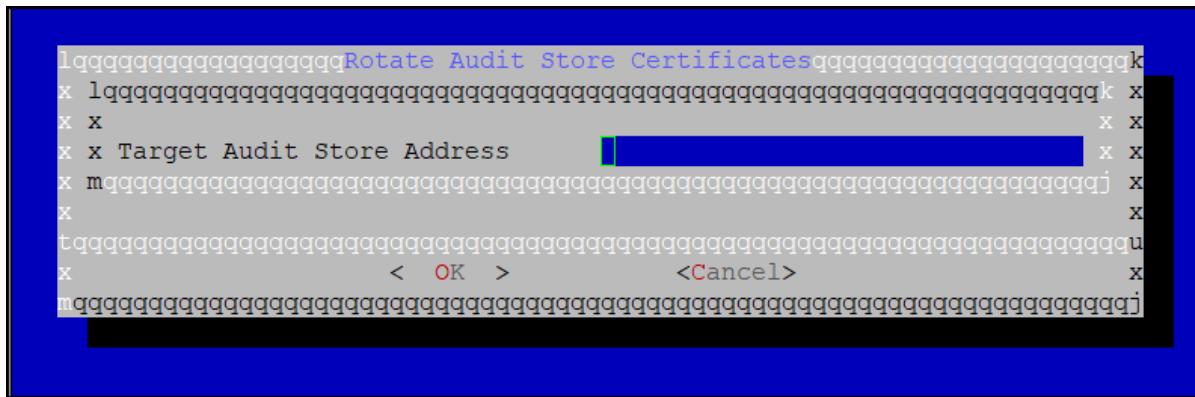


Figure 7-10: Target Audit Store Address

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

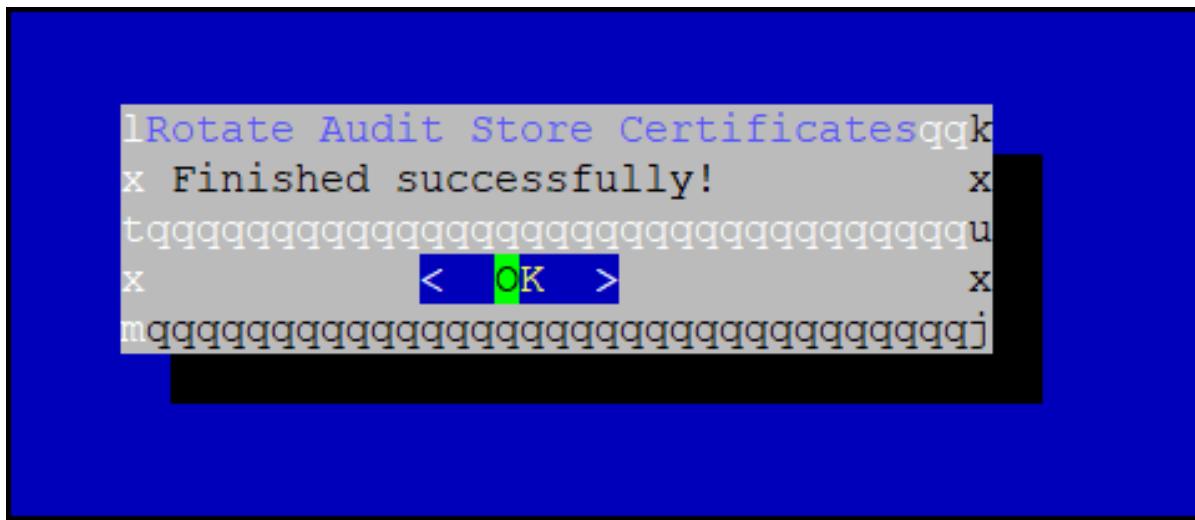


Figure 7-11: Rotation Complete

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 7-12: 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.

The screenshot shows the 'Join, View, or Leave Cluster' interface. At the top right are 'Join Cluster' and 'Leave Cluster' buttons. Below them is a 'Cluster Status' indicator with a green dot. The main area displays cluster statistics:

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
1	1	17	17	0

Below this are sections for 'Initializing Shards' (0), 'Unassigned Shards' (16), 'OS Version' (1.3.0), 'Current Master' (redacted), and 'Indices Count' (14). Further down are 'Total Docs' (190,430) and 'Number of Master Nodes' (1), 'Number of Ingest Nodes' (1).

At the bottom, there are tabs for 'Nodes' (selected) and 'Indices'. The 'Nodes' tab shows a table with columns: Node IP, Roles (Master, Data, Ingest), Action, Name, Up Time, Disk Total (Bytes), Disk Used (Bytes), Disk Avail (Bytes), and RAM. One node entry is visible with a redacted IP address, showing it has all three roles assigned.

Figure 7-13: 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.

System	Logfacade	Running	Automatic	<input type="checkbox"/>
Services	Logfacade Legacy	Running	Automatic	<input type="checkbox"/>
Audit Store				
	Audit Store Repository	Running	Automatic	<input type="checkbox"/>
	Audit Store Management	Running	Automatic	<input checked="" type="checkbox"/>
Misc				
	LDAP Server	Running	Automatic	<input type="checkbox"/>
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>
	td-agent	Running	Automatic	<input checked="" type="checkbox"/>
	Analytics	Running	Automatic	<input type="checkbox"/>

Figure 7-14: Services Started

7.9 Installing the Protegility Storage Unit

The Protegility Storage Unit consists of the *td-agent* and the Audit Store installed on the Appliance. It is a hardened appliance that is used to scale the Audit Store cluster with the logging capability of a Protegility appliance. After installing the ESA, you can add additional Protegility Storage Units to the setup.

As a basic requirement of the Audit Store Cluster, you must have at least 2 ESAs and 2 PSUs installed.

For more information about installing the Protegility Storage Unit, refer to the section *Installing the Protegility Storage Unit* in the [Protegility Storage Unit Guide 9.0.0.0](#).

7.9.1 Audit Store Clustering using the Protegility Storage Unit

Clustering is a powerful way to increase the capability of your system. You can add nodes to expand the cluster. Expanding the cluster using the Protegility Storage Unit provides an advantage by increasing the storage space available.

A basic setup is shown in the following figure.

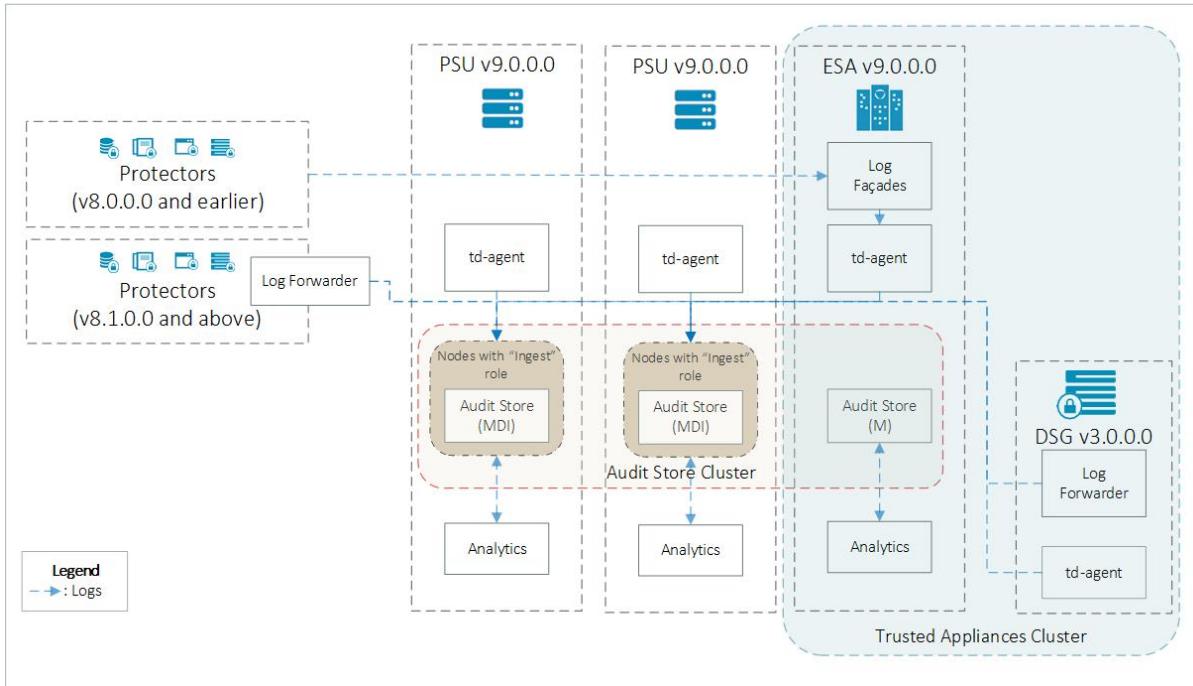


Figure 7-15: Basic Audit Store Cluster

In the figure, the arrows show the log flow direction. The basic setup consists of three systems. Here the systems consist of 1 ESA and 2 Protegility Storage Unit. The Protegility Storage Unit forms a part of the Audit Store cluster where the Audit Stores on all the nodes are linked together to form the storage unit. The logs received by the ESA are stored in the Audit Store cluster, the data would be stored on the local node or any node that is a part of the Audit Store cluster with the *ingest* role.

The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

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

The basic setup when Trusted Appliance Cluster (TAC) is implemented consists of 2 ESAs and 2 Protegility Storage Units as shown in the following figure.

Note: The Audit Store cluster is different from the TAC in the ESA. A TAC is used for grouping and managing multiple ESAs together. In the Audit Store cluster, the Audit Store nodes are grouped together to form the storage unit. The Audit Stores in the Audit Store cluster might be a part of the ESA or the Protegility Storage Unit. The Protegility Storage Unit may or may not be a part of the TAC.

For more information about the TAC, refer to the section *Trusted Appliances Cluster (TAC)* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

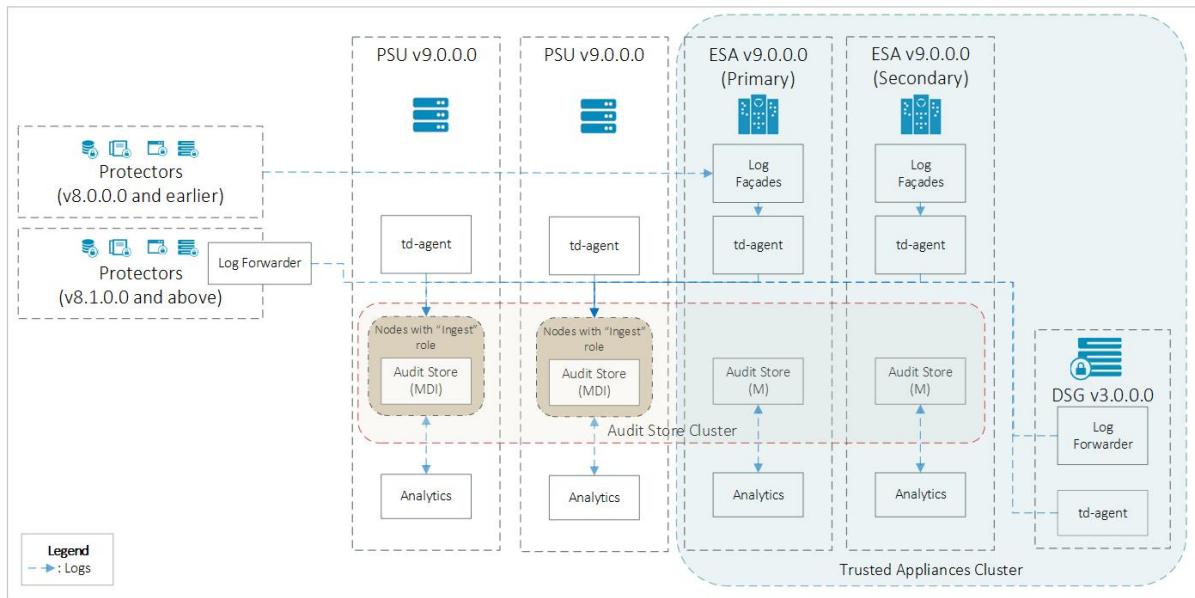


Figure 7-16: Basic Audit Store Cluster in TAC

The Audit Store cluster is flexible and nodes can be added and removed from the Audit Store cluster based on your requirements. Thus, multiple nodes can be added to the Audit Store cluster as shown in the following figure.

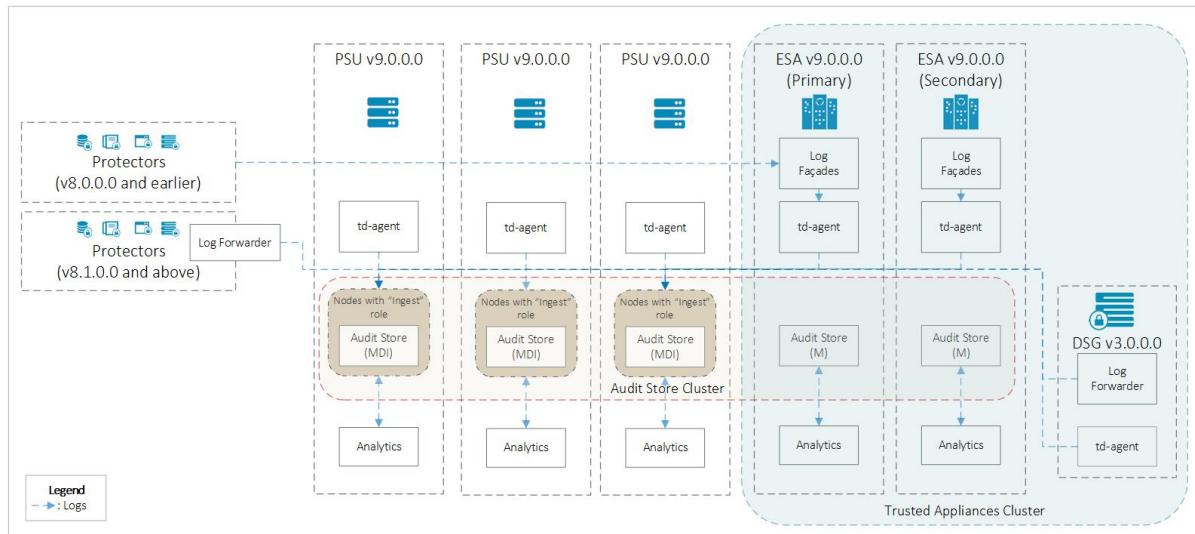


Figure 7-17: Multi-Node Cluster

Note: The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

If any node is not required, then the node can be removed from the Audit Store cluster. When the node is removed from a cluster, the indexes and internal configurations, such as, the td-agent and Analytics settings are reset. In this case, the Protegility Storage Unit remains uninitialized and needs to be added to another Audit Store cluster before it can be used again.

7.9.1.1 Completing the Prerequisites

Ensure that the following prerequisites are met before configuring the Audit Store Cluster. Protegility recommends that the Audit Store Cluster has a minimum of 1 ESA and 2 PSUs or 2 ESAs and 1 PSU for creating a highly-available multi-node Audit Store cluster.

1. Install and set up the first ESA. This will be the Primary ESA if you set up a TAC.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

2. If you require TAC, then install and set up the second ESA. This will be the Secondary ESA in a TAC. Skip this step if TAC is not required.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

3. Install and set up the first PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

4. Install and set up the second PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

7.9.1.2 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, Protegility Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as, *td-agent*, is started and Protegility 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.

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

The following screen appears.

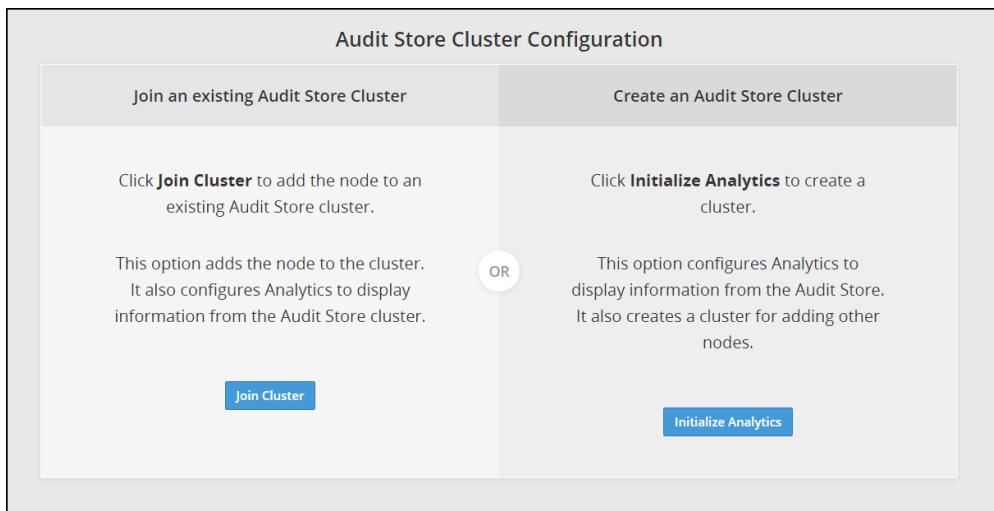


Figure 7-18: Analytics Screen

4. Click **Initialize Analytics**.

Protegility 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.

Protegility 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.

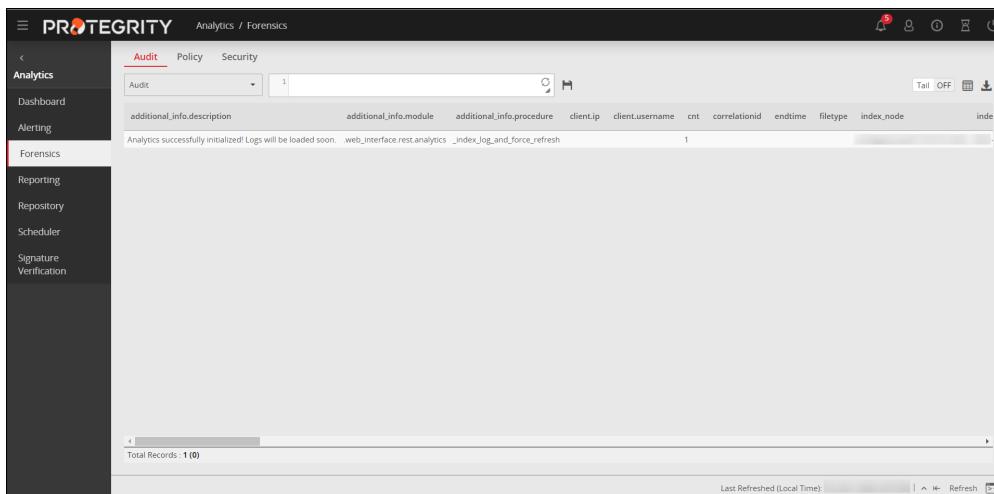


Figure 7-19: Forensics

7.9.1.3 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 *Protegility 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.

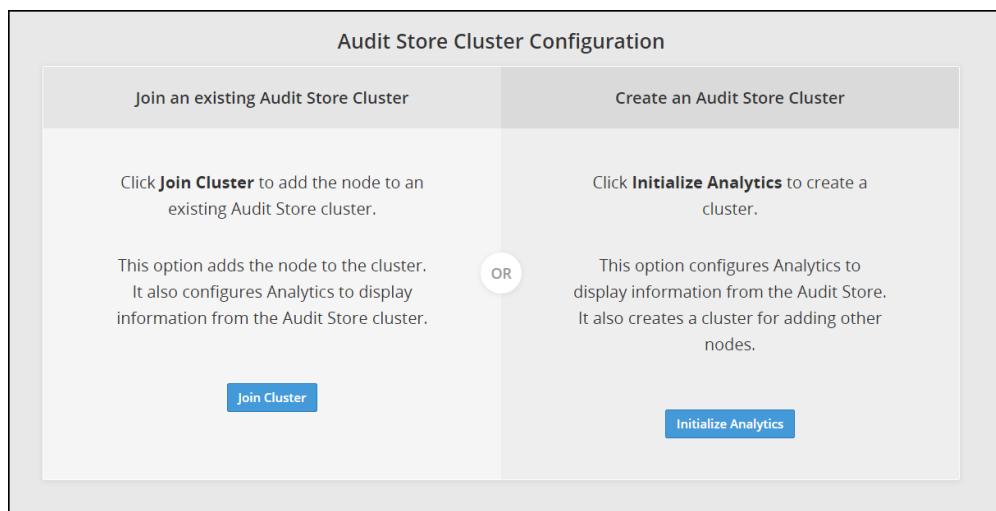


Figure 7-20: Analytics Screen

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.

Figure 7-21: 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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.

Protegility 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.

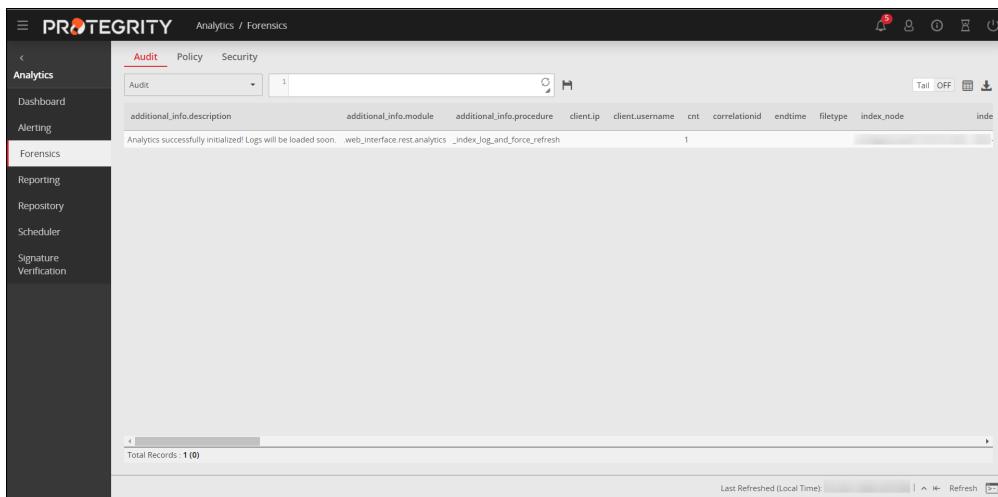


Figure 7-22: Protegility Analytics

7.9.1.4 Adding the Protegility Storage Unit to the Audit Store Cluster

Add the Protegility Storage Unit to the Audit Store Cluster that is initialized on the ESA. You need to specify the IP address of the Audit Store cluster that you want to join with the username and password of the admin user for authorization.

Before you begin

Ensure that the Audit Store services are running on the ESA Web UI by navigating to **System > Services > Audit Store**.

Note: 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 PSU Web UI would make the cluster information inconsistent, make the Audit Store cluster unstable, and would lead to errors.

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 *Protegility Appliances Overview Guide 9.1.0.5*.

► To join the Audit Store cluster:

1. Log in to the Web UI of the Protegility Storage Unit.
2. Open the **Audit Store Management** screen.
The **Cluster Overview** screen appears.

The screenshot shows the 'Cluster Overview' screen. At the top, there are buttons for 'Join Cluster' and 'Leave Cluster'. Below that, the 'Cluster Name' is set to 'insight'. The main area displays various cluster metrics:

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	[redacted]	14

Total Docs	Number of Master Nodes	Number of Ingest Nodes
190,528	1	1

Below these tables, there are two tabs: 'Nodes' (selected) and 'Indices'. Under 'Nodes', there is a table titled 'Details' showing one node's configuration:

Node IP	Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
[redacted]	✓	✓	✓	Edit Roles	[redacted]	8.8h	39,502,524,416	7,033,622,528	32,468,901,888	16.6

Figure 7-23: Cluster Overview Screen

3. Click **Join Cluster**.

The **Join Cluster** screen appears.

Note: The **Join Cluster** button is disabled if a node is already a part of the Audit Store cluster.

The dialog box has a title 'Join an existing Audit Store Cluster'. It contains fields for 'Target node IP/Hostname*', 'Username*', and 'Password*'. There is also a checkbox for clearing cluster data and a note about backing up data. At the bottom are 'Join Cluster' and 'Cancel' buttons.

Target node IP/Hostname*	
<input type="text" value="Node IP/Hostname"/>	
Username*	
<input type="text" value="Username"/>	
Password*	
<input type="password" value="Password"/>	
<input type="checkbox"/>	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 7-24: Join Cluster Dialog Box

4. Specify the following details for the node that you want to connect.

- **Target node IP/Hostname:** This is the IP address or hostname of the node that you want to connect to.

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

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

For more information about creating an Audit Store cluster, refer to the section *Creating a Local Cluster* in the [Protegility Analytics Guide 9.1.0.5](#).

- **Username:** This is the administrator user name to connect to the target machine. For example, admin.
- **Password:** This is the password for the user.

5. Click **Join Cluster**.

Note: The **Join Cluster** button in this dialog box is enabled after you specify the required information in all the fields and select the check box.

The Audit Store data on the node is cleared . The node is then added to the Audit Store cluster. The Cluster Overview screen appears with the updated Audit Store cluster information. The **Join Cluster** button is disabled and the **Leave Cluster** button is now enabled.

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
2	2	17	34	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
192,494	2	2

Nodes		Indices		Details					
Node IP	Master	Roles	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
192.168.1.100	✓	✓ ✓	Edit Roles	node1	9h	39,502,524,416	7,035,338,752	32,467,185,664	16,6
192.168.1.101	✓	✓ ✓	Edit Roles	node2	3.4m	39,502,524,416	7,001,763,840	32,500,760,576	16,6

Figure 7-25: Node Added to Cluster

Repeat the steps provided in this section to add the remaining Protegility Storage Units you installed to the Audit Store Cluster.

7.9.1.5 Refreshing the Audit Store Cluster

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

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

7.9.1.6 Configuring td-agent in the Audit Store Cluster

Complete the following steps after adding the Protegility Storage Unit to the Audit Store cluster. This configuration is required for processing and storing the logs received by the Audit Store.

Note: This step must be performed on all the ESAs in the Audit Store cluster.

Before performing the steps provided here, verify that the Audit Store cluster health status is green on the **Audit Store Management** screen of the ESA Web UI.

1. Login to the CLI Manager of the *ESA* node.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
3. Enter the root password and select **OK**.
4. Enter the username and password for the administrative user, such as, admin.
5. Select **OK**.
6. In the *Setting ESA Communication* screen, select **OK**.
7. Specify the IP addresses of all the Protegility Storage Unit machines in the cluster, separated by commas.



Figure 7-26: Forward Logs

8. Select **OK**.
9. Type *y* to fetch certificates for communicating with the ESA and select **OK**.

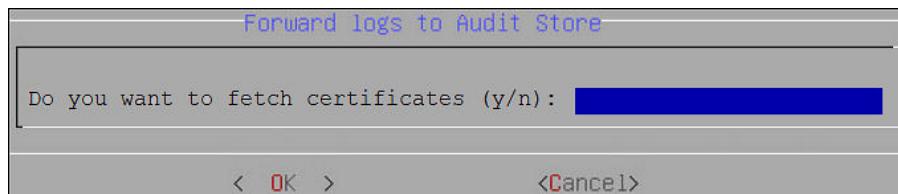


Figure 7-27: Fetch Certificates

10. Enter the admin username and password and select **OK**.
- Repeat the steps provided in this section on all the ESAs in the Audit Store Cluster.

7.9.1.7 Verifying the Audit Store Cluster

View the Audit Store Management page to verify that the configurations that you performed were completed successfully using the steps provided here.

1. Login to the ESA Web UI.
2. Navigate to the **Audit Store Management** page.
3. Verify that the nodes are added to the cluster. The health of the nodes must be either green or yellow.
4. If you added additional ESAs for creating a TAC, then verify that the ESA has only the master role.

The screenshot shows a cluster named 'insight' with the following statistics:

- Number of Nodes:** 3
- Number of Data Nodes:** 2
- Active Primary Shards:** 17
- Active Shards:** 34
- Relocating Shards:** 0
- Initializing Shards:** 0
- Unassigned Shards:** 0
- OS Version:** 1.3.0
- Current Master:** [redacted]
- Indices Count:** 14
- Total Docs:** 212,995
- Number of Master Nodes:** 3
- Number of Ingest Nodes:** 2

The 'Nodes' tab is selected, showing a table of nodes with their IP addresses, roles (Master, Data, Ingest), and other metrics like Up Time and Disk Usage. One row's 'Roles' column is highlighted with a red box.

Node IP	Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAN
[redacted]	✓	✓	✓	Edit Roles	[redacted]	19s	39,502,524,416	6,955,266,048	32,547,258,368	6,44
[redacted]	✓	✓	✓	Edit Roles	[redacted]	2.5h	39,502,524,416	7,021,211,648	32,481,312,768	16,6
[redacted]	✓	✓	✓	Edit Roles	[redacted]	4.9m	45,709,819,904	5,415,325,696	40,294,494,208	28,3
[redacted]					[redacted]					

Figure 7-28: Nodes Added to Cluster

7.9.2 Optional: Using an External SIEM

If you have an external SIEM for storing your logs, then you can configure the ESA and Protectors to sent the logs to your SIEM. You can use just your SIEM with the Protegility Audit Store and Protegility Storage Unit for storing logs.

For more information about configuring an external SIEM, refer to the section *Sending Logs to an External Location* in the [Audit Store Guide 9.1.0.5](#).

7.10 Post Upgrade Steps

Ensure that the following steps are performed after the ESA upgrade is completed:

7.10.1 Migrating Configuration Settings and Logs

After setting up the Audit Store cluster by installing the ESAs and PSUs. Migrate settings and the logs to v9.0.0.0 using the steps provided here.

Before you begin

Ensure that the following is complete:

- The pre-patch is installed on any one PSU of the v8.1.0.1 Audit Store cluster.

For more information about installing the pre-patch, refer to the section [Installing the Pre-Patch on the PSU](#).

- The Audit Store cluster for v9.0.0.0 is set up and running.
- The Analytics in the ESA is initialized.

- Login to any PSU on the v9.0.0.0 Audit Store cluster.
- Migrate the configuration to the v9.0.0.0 Audit Store cluster using the following steps.
 - Navigate to **Tools**.
 - Run **Migrate Analytics Configuration**.

```
Tools:

    Rotate Appliance OS Keys
    -- Removable Media Management --
        Disable CD/DVD Drives
        Disable USB Flash Drives
    Web-Services Tuning
    Service Dispatcher Tuning
    AntiVirus
    PLUG - Forward logs to Audit Store
    -- Audit Store Tools --
        Rotate Audit Store Certificates
        Apply Audit Store Security Configs
    -- Analytics Tools --
        Migrate Analytics Configuration
        Migrate Analytics Audits
        Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.

(Q)uit (U)p (T)op

(100%)
```

Figure 7-29: Migrate Analytics Configuration Setting

For more information about the *Migrate Analytics Configuration* tool, refer to the section [Migrating Analytics Configuration](#).

- c. Enter the *root* password and select **OK**.
- d. Enter the *admin* username and password and select **OK**.
- e. Enter the address, port, and credentials of the source PSU of the v8.1.0.1 cluster where the pre-patch is installed and select **OK**.

The *Migration Logs* saved query is available in Forensics to view the migration logs. You can delete this saved query after successfully migrating the Analytics configuration and audit logs.

To view the query, login to the ESA Web UI and navigate to **Analytics > Forensics > Audit > Migration Logs**.

Note: When the reports are migrated to v9.1.0.5, only custom reports that you modified or created are moved to v9.1.0.5. The ESA v9.1.0.5 has its own set of reports that display log info for v9.1.0.5-related protectors. Hence, the system-generated reports available in v8.1.0.1 are not migrated to v9.1.0.5.

3. Migrate the logs to the v9.0.0.0 Audit Store cluster using the following steps.
 - a. Navigate to **Tools**.
 - b. Run **Migrate Analytics Audits**.

```
Tools:
  Rotate Appliance OS Keys
  -- Removable Media Management --
    Disable CD/DVD Drives
    Disable USB Flash Drives
  Web-Services Tuning
  Service Dispatcher Tuning
  AntiVirus
  PLUG - Forward logs to Audit Store
  -- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
  -- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op
(100%)
```

Figure 7-30: Migrate Analytics Audits Setting

For more information about the *Migrate Analytics Audits* tool, refer to the section [Migrating Analytics Audits](#).

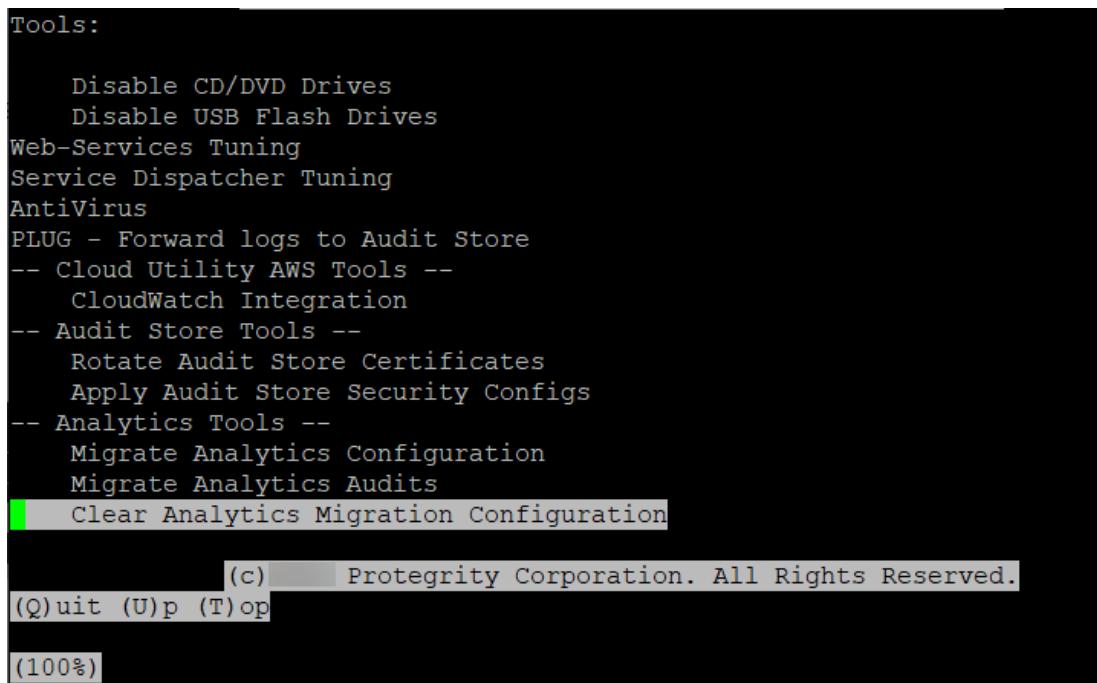
- c. Enter the root password and select **OK**.
 - d. Enter the *admin* username and password and select **OK**.
 - e. Enter the address, port, and credentials of the source PSU of the v81.0.1 cluster where the pre-patch is installed and select **OK**.
The *Migrate Analytics Audits started successfully!* message appears. The migration process runs in the background. You can view the migration status using the *Migration Logs* saved query in Forensics.
 - f. Select **Exit** to go to the CLI menu screen.
4. Removing all the temporary indexes and configuration created during the migration using the following steps.

Note: Ensure that you run this step only after successfully migrating all the configuration and logs.

To verify that the migration is complete, login to the ESA Web UI, navigate to **Analytics > Forensics > Audit > Migration Logs**, and verify that the following messages appear in the logs:

- *Migration of all audit indices from source Audit Store cluster to destination Audit Store cluster is completed.*
- *Migrate Analytics Configuration is completed. The Migration Logs saved query is available in Forensics to track progress and status. Delete that saved query after successfully migrating the Analytics configuration and audit logs.*

- a. Navigate to **Tools**.
- b. Run **Clear Analytics Migration Configuration**.



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

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op
(100%)
```

Figure 7-31: Clear Analytics Migration Configuration Setting

For more information about the *Clear Analytics Migration Configuration* tool, refer to the section [Clear Analytics Migration Configuration](#).

- c. Enter the *root* password and select **OK**.
 - d. Enter the *admin* username and password and select **OK**.
- After the migration cleanup is complete, the CLI menu screen appears.

7.10.2 Migrating Reports and Indices

While working with the ESA v8.1.0.1, you might have downloaded the reports generated and archived indices on the ESA or the PSU. When you upgrade, ensure that you migrate these reports and indices to v9.0.0.0 using the steps provided here.

1. Login to the CLI Manager of the ESA v8.1.0.1 or PSU v8.1.0.1.
2. Navigate to **Administration > OS Console**.
3. Enter the root password.
4. Navigate to the */opt/protegility/insight/archive* directory using the following command.

```
cd /opt/protegility/insight/archive
```
5. Copy the files from the *archive* directory to the PSU v9.0.0.0 retaining the directory structure and permissions.
6. Navigate to the */opt/protegility/insight/reports* directory using the following command.

```
cd /opt/protegility/insight/reports
```
7. Copy the files from the *reports* directory to the PSU v9.0.0.0 retaining the directory structure and permissions.
8. Repeat the steps on the remaining ESA v8.1.0.1 or PSU v8.1.0.1 where the reports and indices might be saved.

7.10.3 Updating the Priority IP List for Signature Verification

Signature verification jobs can only run on the ESAs, they cannot run on the PSUs. Ensure that you update the priority IP list for the default signature verification jobs after you set up the system. By default, the Primary ESA will be used for the priority IP. If

you have multiple ESAs in the priority list, then additional ESAs are available to process the signature verifications jobs that must be processed.

For example, if the maximum jobs to run on an ESA is set to 4 and 10 jobs are queued to run on 2 ESAs, then 4 jobs are started on the first ESA, 4 jobs are started on the second ESA, and 2 jobs will be queued to run till an ESA job slot is free to accept and run the queued job.

For more information about scheduling jobs, refer to the section *Using the Scheduler* in the *Protegility Analytics Guide 9.1.0.5*.

For more information about signature verification jobs, refer to the section *Verifying Signatures* in the *Protegility Analytics Guide 9.1.0.5*.

Use the steps provided in this section to update the priority IP list.

1. Login to the ESA Web UI.
2. Navigate to **Analytics > Scheduler**.
3. From the **Action** column, click the **Edit** icon () for the **Signature Verification** task.
4. Update the **Priority IPs** field with the list of the ESAs available separating the IPs using commas.
5. Click **Save**.

7.10.4 Configuring the Security Settings for Protectors

During upgrade, the security configuration files for communication between the Log Forwarder on the Protectors and the Audit Store communication are analyzed. If the default settings are used, then the upgrade is performed and the configurations are applied.

However, if you have modified or updated the security configuration for communication between the Log Forwarder and the Audit Store to use Basic Authentication or Certificate-based Authentication, then the configuration files that you modified are backed up to the `/SECURITY_CONFIG_DIR/_backup_v1.2` directory. The files are then overwritten to use the default security configuration. In this case, you need to reapply the security configurations.

Note: The security settings available in the configuration files have changed. You need to reconfigure the security configuration. Use the back up files only as a reference. Using the backup files as-is will result in errors in configuration and the Audit Store will not be able to receive logs from the Log Forwarder.

For more information about updating the security configurations for the Log Forwarder to Audit Store communication, refer to the section *Configuring Security for the Log Forwarder* in the *Audit Store Guide 9.1.0.5*.

7.10.5 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

Before you begin

Keep the following information handy before the setup process:

- SMTP server details
- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is **25**.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.
Protegility Reporting requires a full email address in the Username.
7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.
A message box appears.
14. Click **EXIT** to save the settings.

7.11 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

7.11.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

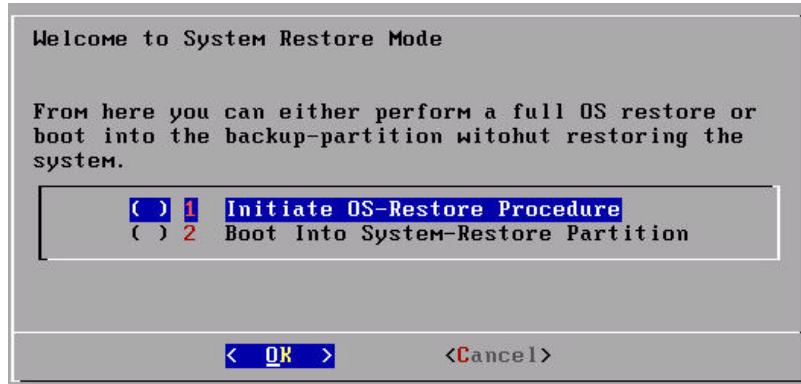
1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system.
A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

7.11.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the *Protegility Appliances Overview Guide 9.1.0.5*.

7.11.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

- To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

7.11.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot

8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

7.11.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

7.12 Upgrading Protectors

If you are upgrading the Protectors from v8.1.0.1 to v9.0.0.0, then ensure that the ESA is at v9.0.0.0.

Note:

For more information about the compatible data elements for the different protector versions, refer to the table [Data Element Compatibility Matrix](#).

7.12.1 Upgrading Data Security Gateway (DSG)

The Data Security Gateway (DSG) can be upgraded to the DSG v3.0.0.0. The upgrade process involves the following steps.

1. Upgrade the ESA to the version v9.0.0.0
2. Extend the ESA with the DSG Web UI by applying the *ESA_PAP-ALL-64_x86-64_9.0.0.0.2095-DSGUP-1.pty* patch.



For information about extending the ESA with the DSG Web UI, refer to the section *Extending ESA with DSG Web UI* in the [Data Security Gateway User Guide 3.0.0.0](#).

3. Reimage the DSG nodes to v3.0.0.0.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

For more information about upgrading the DSG to DSG v3.0.0.0, refer to the section *Upgrading to DSG v3.0.0.0* in the [Data Security Gateway User Guide 3.0.0.0](#).

7.12.1.1 Applying a DSG Patch

Apply the Data Security Gateway (DSG) patch on the ESA to extend its Web UI with the DSG menu. You must apply the *ESA_PAP-ALL-64_x86-64_9.0.0.0.2095-DSGUP-1.pty* patch on the ESA v9.0.0.0.

► To install the DSG patch on the ESA Web UI:

1. Login to the ESA Web UI.
2. Navigate to **Settings > System > File Upload**.
3. Click **Choose File** to upload the DSG patch file.
4. Select the file and click **Upload**.
The uploaded patch appears on the Web UI.
5. On the ESA CLI Manager, navigate to **Administration > Installation and Patches > Patch Management**.
6. Enter the *root* password.
7. Select **Install a Patch** and press **OK**.
8. Select the uploaded patch.
9. Press **Install**.

Note: After the patch is successfully installed, you may need to refresh the ESA Web UI to view the **Cloud Gateway** menu option. This will refresh the local copy (cache) of the ESA Web UI menu screen.

Chapter 8

Upgrading from v7.2.1 to v9.0.0.0

[8.1 Migrating ESA v7.2.1 to ESA v9.0.0.0](#)

[8.2 Installing ESA](#)

[8.3 Prerequisites](#)

[8.4 Upgrading ESA to Pre-v9.0.0.0](#)

[8.5 Post Upgrade Steps on version Pre-v9.0.0.0](#)

[8.6 Migrating the ESA to v9.0.0.0](#)

[8.7 Configuring Settings on v9.0.0.0](#)

[8.8 Installing the Protegility Storage Unit](#)

[8.9 Migrating DMS Logs and Metering Data](#)

[8.10 Restoring to the Previous Version of ESA](#)

This section describes the steps to upgrade the ESA v7.2.1 to ESA v9.0.0.0, and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the protectors.

8.1 Migrating ESA v7.2.1 to ESA v9.0.0.0

This section describes the steps for upgrading the ESAs. In this upgrade process, an intermediate patch is applied on the ESA v7.2.1, then the configurations on the ESAs is exported from v7.2.1 and imported on the v9.0.0.0. The following figure illustrates a sample TAC environment on which the ESAs must be upgraded to v9.0.0.0.

Note:

Ensure that at least two ESAs are in a TAC.

Ensure that you do not make any changes to configuration, policy, or CoP during the upgrade process.

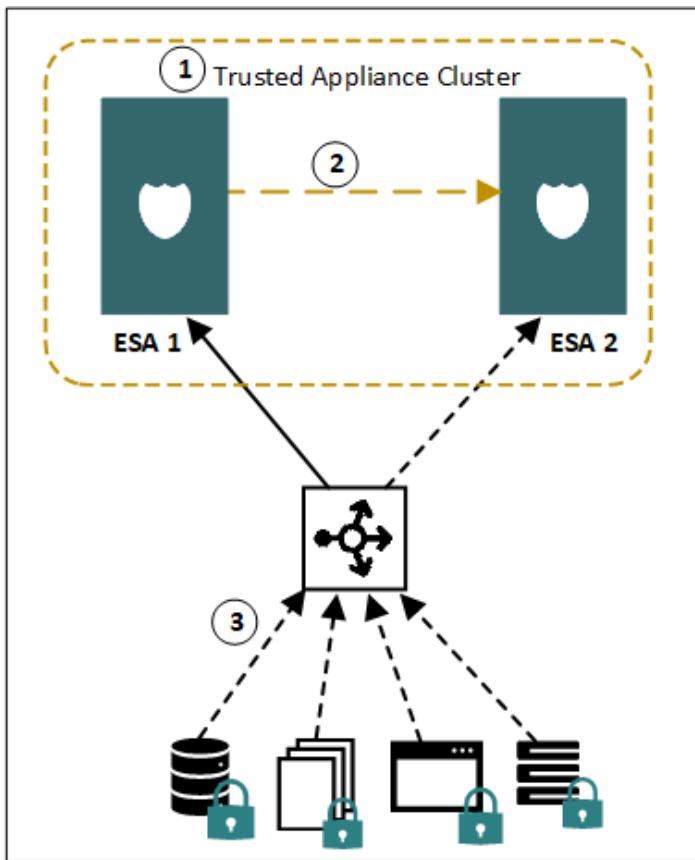


Figure 8-1: ESA v7.2.1 in a TAC

As shown in the setup,

1. The TAC contains a server node appliance the ESA 1 and a client node appliance the ESA 2.
2. Data replication for policies, forensics, or DSG configurations takes place from the ESA 1 to the ESA 2.
3. Protectors communicate with the load balancer that balances the requests between the ESA 1 and the ESA 2.

The following figure illustrates the TAC setup after the upgrade process is completed.

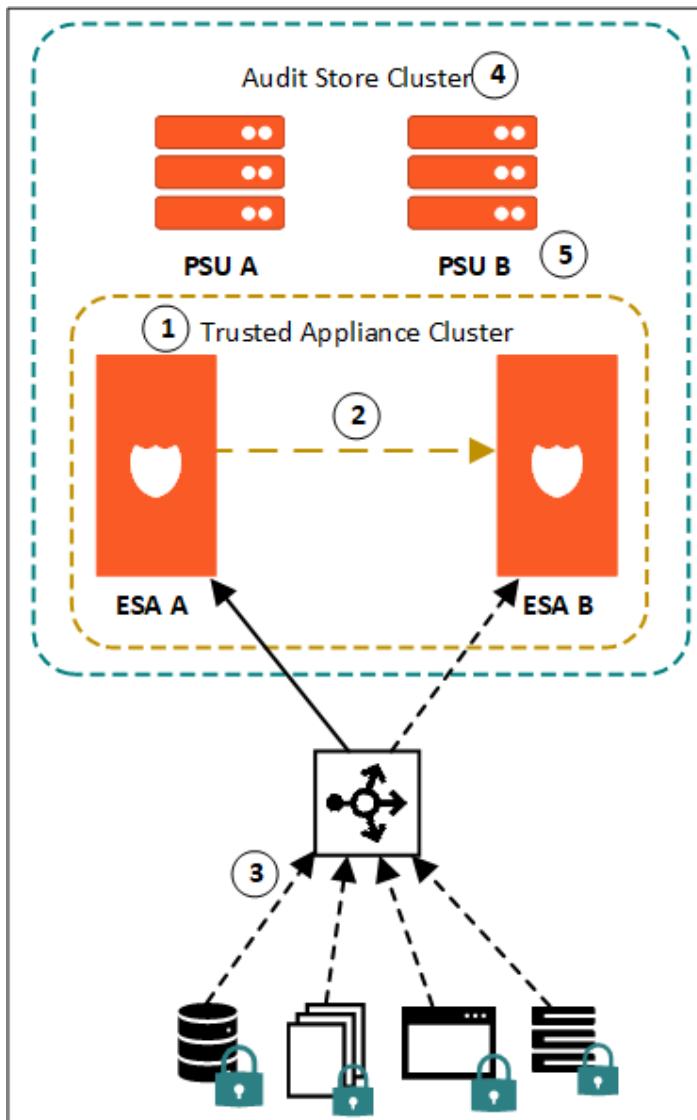


Figure 8-2: ESA v9.0.0.0 in a TAC

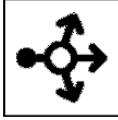
1. The TAC is established between the ESA A and ESA B.
2. Data replication for policies, forensics, or DSG configurations take place from the ESA A to the ESA B.
3. Protectors communicate with the load balancer that balances the requests between the upgraded ESA A and ESA B.
4. Audit Store cluster is enabled for the ESAs.
5. The PSU A and PSU B are added as a part of the Audit Store cluster.

8.1.1 Upgrade Process: Flow Diagram

A diagrammatic representation of the upgrade process is provided in this section. The legend describes the elements used in the flow diagram.

Legend

Icon	Description	Version	File System
 ESA 1	ESA appliance node	v7.2.1	Reiser FS
 ESA 2	ESA Node appliance	v7.2.1	Reiser FS
 ESA Pre-v9.0.0.0	ESA Node appliance Updated to pre-v9.0.0.0 by applying the <i>ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-2.pty</i> patch	Pre-v9.0.0.0	
 ESA v7.2.1 FE-1	ESA Node appliance Still remains on v7.2.1 by applying the <i>ESA_PAP-ALL-64_x86-64_7.2.1.x.FE-1.pty</i> patch	v7.2.1	
 ESA A	ESA Node appliance (Server)	v9.0.0.0	Ext4 FS
 ESA B	ESA Node appliance	v9.0.0.0	Ext4 FS

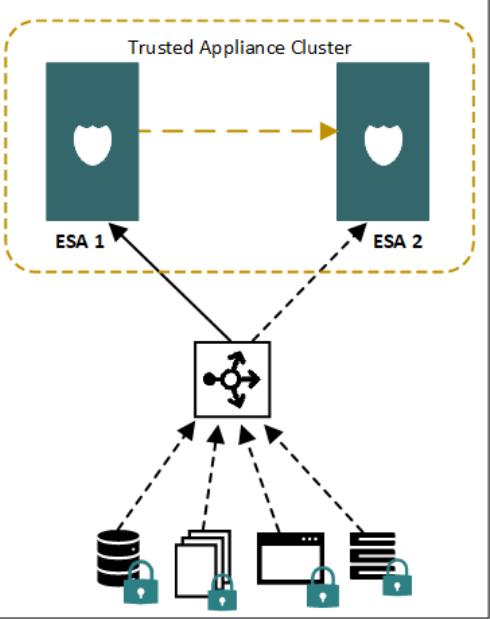
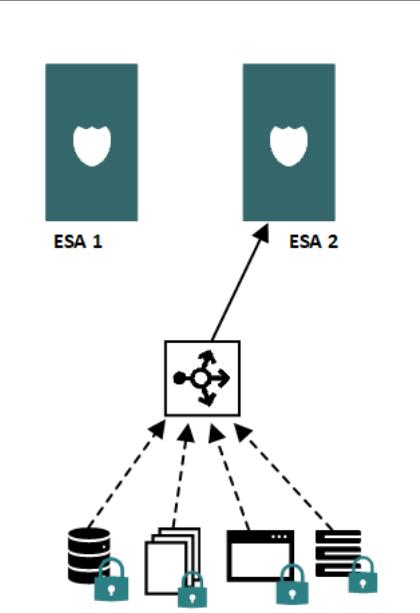
Icon	Description	Version	File System
	Protegility Storage Unit (PSU)	v9.0.0.0	Ext4 FS
	Protegility Storage Unit (PSU)	v9.0.0.0	Ext4 FS
	Trusted Appliances Cluster	<ul style="list-style-type: none"> • v7.2.1 • v9.0.0.0 	N/A
	Audit Store Cluster	v9.0.0.0	N/A
	Protectors	<ul style="list-style-type: none"> • v7.2.1 • v9.0.0.0 	N/A
	Load Balancer	N/A	N/A

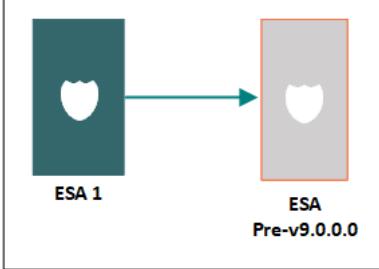
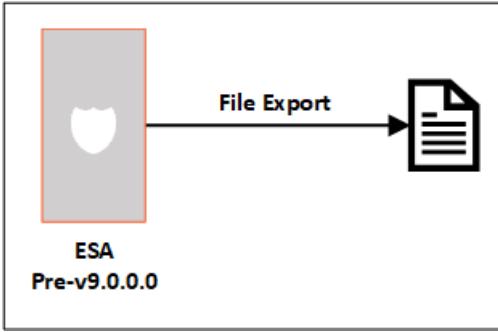
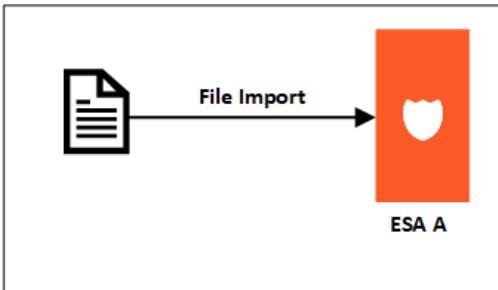
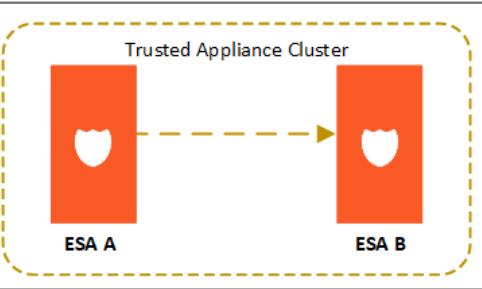
Note:

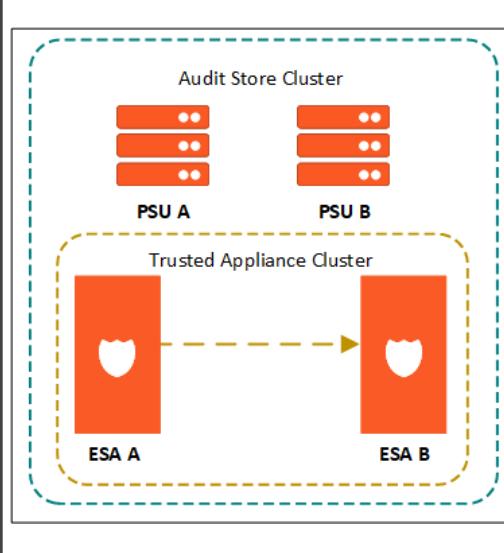
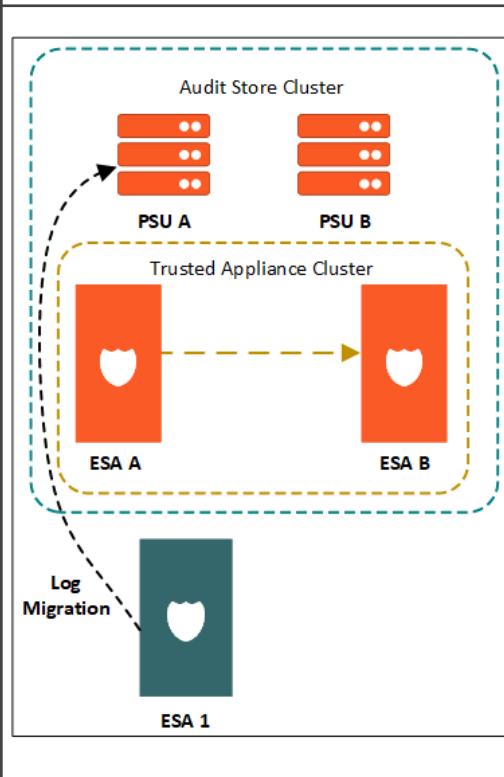
Ensure that you download the latest patch from the [My.Protegility](#) portal.

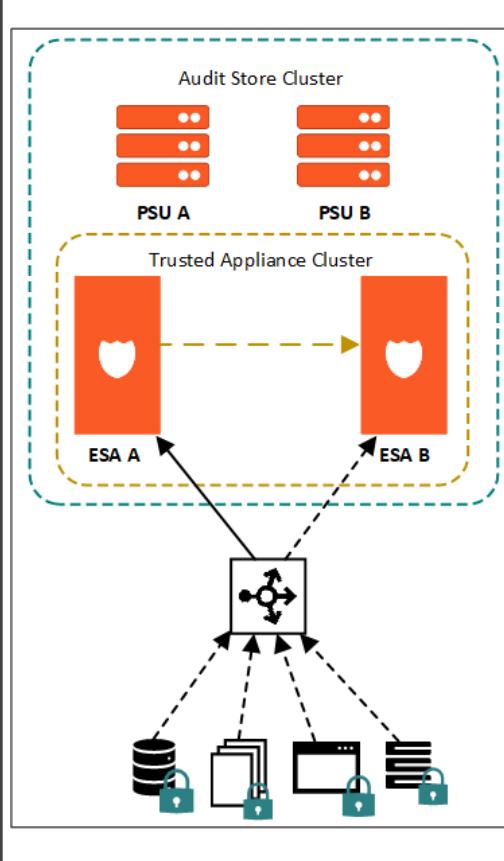
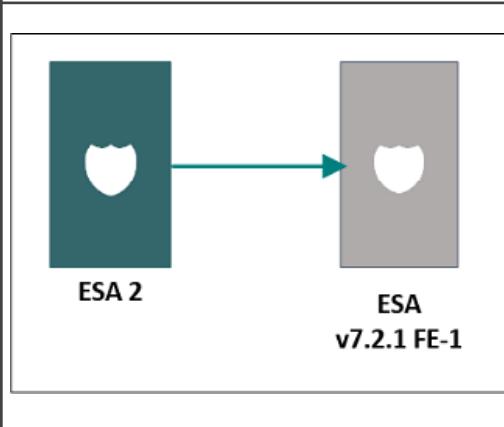
For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

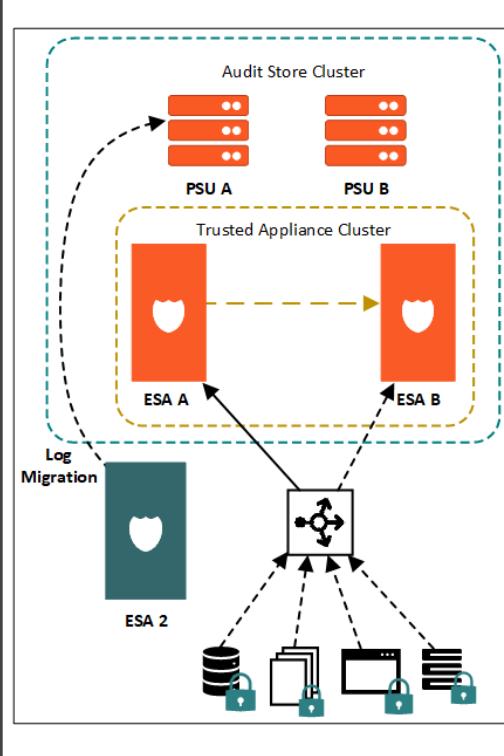
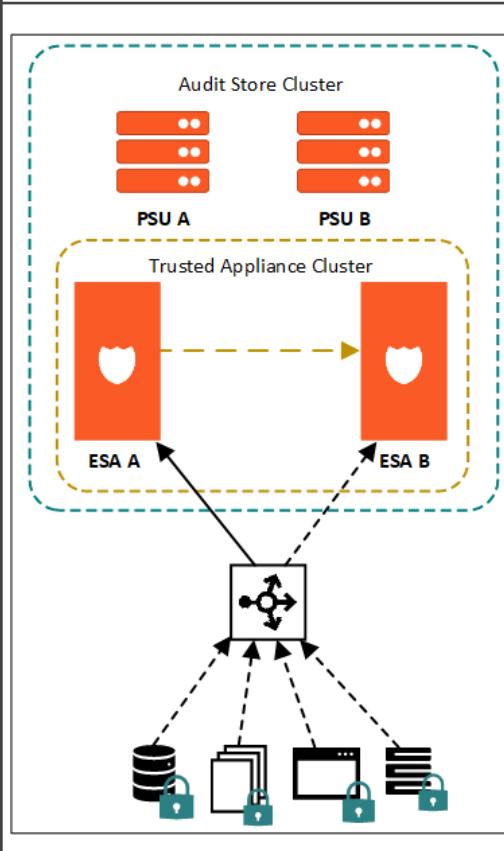
The following is a diagrammatic representation of the overview of the upgrade process from v7.2.1 to v9.0.0.0.

	<ul style="list-style-type: none"> TAC contains a server node appliance ESA 1 and appliance ESA 2. Data replication for policies or DSG configurations takes place from the ESA 1 to the ESA 2. Protectors communicate with the load balancer that routes the requests to the ESA 1 or ESA 2. Ensure that the ESA 1 and ESA 2 in the TAC are in sync and have the latest policies, configurations, DSG rulesets, and so on.
 ESA A	<ul style="list-style-type: none"> Create <i>ESA A</i> on v9.0.0.0. The ESA will have the <i>Ext4</i> file system, <i>Buster OS</i>, and <i>Python3</i> by default.
	<ul style="list-style-type: none"> Delete the cluster scheduler tasks between the ESA 1 and the ESA 2. Break the TAC. All traffic is routed to the ESA 2.

	<ul style="list-style-type: none"> Upgrade the ESA 1 to pre-v9.0.0.0 by applying the <i>ESA_PAP-ALL-64_x86-64_8.1.0.0.x_UP-2.pty</i> patch Complete the upgrade on the ESA pre-v9.0.0.0 <p>Note: This is an intermediate step while migrating from v7.2.1 to v9.0.0.0. This should not be used for upgrading to any other release version.</p>
	<ul style="list-style-type: none"> Export all the configurations, policy data, custom configurations, and so on, from ESA 1 (version Pre-9.0.0.0) to a file using the Backup & Restore functionality. Transfer the exported file to ESA A using your preferred method, such as, SCP, FTP, and so on. <p>Caution: After the export is completed, you must not change any configurations on the ESA.</p>
	<ul style="list-style-type: none"> Import the configurations, policy data, custom configurations on the ESA A. Complete the post upgrade steps on the ESA A.
	<ul style="list-style-type: none"> Upgrade the scripts to <i>python3</i>. Open the ports 9200 and 9300. Add permissions to the existing roles. Rotate the Audit Store certificates on the ESA A.
	<ul style="list-style-type: none"> Create a ESA B. Join the ESA A and the ESA B in a Trusted Appliances Cluster.

	<ul style="list-style-type: none"> • Create two new PSUs (PSU A and PSU B). • Initialize Analytics on the ESA A. • Join the ESA A, ESA B, PSU A, and PSU B to create an Audit Store Cluster. • Configure <i>td-agent</i> on the ESA A and ESA B in the Audit store cluster. • Configure the audit store roles on the ESA A and ESA B nodes. <p>Note: Ensure that the roles on the ESAs are changed to <i>Master</i>.</p>
	<ul style="list-style-type: none"> • Configure the <i>td-agent</i> on ESA 1 to point to the PSU A. • Migrate the DMS logs and metering logs using the migration scripts from ESA 1 to the PSUs. Wait till the migration is complete. • After the migration is successfully completed, shut down ESA 1.

	<ul style="list-style-type: none"> • Redirect the traffic from ESA 1 to ESA A. • Upgrade the DSG to the latest version. • Upgrade any other protectors. • After the migration is successfully completed, shut down ESA 1.
	<ul style="list-style-type: none"> • To migrate the DMS logs without upgrading the ESA 2 to pre-v9.0.0.0, you must install the <i>ESA_PAP-ALL-64_x86-64_7.2.1.x.FE-1.pty</i> patch on the ESA 2. <div data-bbox="931 1100 1538 1326" style="background-color: #e0f2e0; padding: 10px;"> <p>Note: If you want to migrate the metering logs and the DMS logs from the ESA 2, then apply the <i>ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-2.pty</i> patch on the ESA 2.</p> </div> <ul style="list-style-type: none"> • Complete the installation on the ESA 2.

	<ul style="list-style-type: none"> Configure the <i>td-agent</i> on the ESA 2 to point to the PSUs. Migrate the DMS logs and metering logs using the migration scripts from ESA 2 to the PSUs. Wait till the migration is complete. After the migration is successfully completed, shut down ESA 2.
	<ul style="list-style-type: none"> Upgrade to v9.0.0.0 with <i>Buster OS</i>, <i>Python 3.7</i>, and <i>Elastic Search 7.1.0</i> is complete.

8.1.2 Upgrade Process: Step-by-step Procedure

To upgrade the ESA appliances from v7.2.1 to v9.0.0.0, you must first install an intermediate patch on the v7.2.1 machine. After the pre-patch is successfully installed, you must export the configurations, rulesets, or settings. These configurations, rulesets, or settings must be imported on the v9.0.0.0 machine. After the import is successfully completed, the logs are then migrated to the PSUs. Perform the required steps to complete the upgrade.

This section describes the procedure to upgrade the ESA v7.2.1 to v9.0.0.0.

Note:

Ensure that you perform the procedure in the prescribed sequence for a successful upgrade.

Before you begin

- At least two ESAs must be in a TAC on v7.2.1.
- The TAC must have at least one appliance as the *server* node.

For more information on the trusted appliance cluster, refer to the section *Trusted Appliances Cluster* in the *Protegility Appliances Overview Guide 9.0.0.0*.

- From the v7.2.1, the file system is changed from the *ReiserFS* to the *Ext4* file system, the *Buster OS* is upgraded, and *python2* is upgraded to *Python3*. Therefore, install two additional ESAs v9.0.0.0, that is, ESA A and ESA B.

For more information on installing the v9.0.0.0 on a new machine, refer to the section *Installing ESA on-premise* in the *Protegility Installation Guide 9.0.0.0*.

- Install two PSUs, that is, PSU A and PSU B.

For more information on installing the PSU v9.0.0.0 on a new machine, refer to the *Protegility Storage Unit Guide 9.0.0.0*.

- You must not make any changes to configuration, policy, or CoP on any appliance during the upgrade process.
- All the *Prerequisites* are met before beginning the upgrade process.

For more information on the prerequisites, refer to the section *Prerequisites*.

To upgrade the ESA to v9.0.0.0:

1. Ensure that the ESA 1 and ESA 2 in the TAC are in sync and have the latest policies and configurations.

Note: In the TAC, ensure that the ESA 1 is a *server* node.

2. Create the ESA A on v9.0.0.0.

For more information on installing the ESA on v9.0.0.0, refer to the section *Installing ESA*.

3. Delete the cluster scheduler tasks between the ESA 1 and the ESA 2.

For more information about deleting a cluster task, refer to the section *Scheduling Appliance Tasks* in the *Protegility Appliances Overview Guide 9.1.0.5*.

4. Remove the ESA 1 from the TAC.

Caution:

Before leaving the TAC, ensure that the ESA 1 is the *server* node.

For more information about leaving a TAC, refer to section *Removing a Node from the Cluster using Web UI* in the *Protegility Appliances Overview Guide 9.0.0.0*.

5. Perform the following steps on the ESA 1.

- a. Upgrade to the pre-v9.0.0.0 patch by installing the *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-2.pty* patch.

For more information about installing the pre-v9.0.0.0 patch, refer to the section [Migrating the ESA to v9.0.0.0](#).

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

- b. Complete the upgrade on the ESA 1.

For more information about the completing the upgrade, refer to the section [Post Upgrade Steps on version Pre-v9.0.0.0](#).

- c. From the ESA 1, export all the configurations, policy data, custom configurations, and so on, to a file using **Backup & Restore** functionality.

For more information on exporting a file, refer to the section [Migrating the ESA to v9.0.0.0](#).

Caution:

After the export is completed, you must not change any configurations on the ESA.

Important:

If you have installed the v7.2.1 SE-8 patch on the ESA v7.2.1, then export the configuration files from the CLI Manager only.

6. Transfer the exported file to the ESA A using your preferred method, such as, SCP, FTP, and so on.

Note:

If you are using the SCP or FTP, then ensure that the exported file is placed in the `/opt/product_exports` directory and permissions for the file are set to `755`.

7. Import the configurations, policy data, custom configurations on the ESA A.

For more information on importing configurations, refer to the section [Migrating the ESA to v9.0.0.0](#).

8. After the file is successfully imported on the ESA A, configure the required settings on the ESA A.

For more information about configuring the required settings, refer to the section [Configuring the ESA v9.0.0.0](#).

9. Upgrade the custom files to `python3`.

10. On ESA A, open the `9200` and `9300` ports.

11. On ESA A, add permissions to the existing roles.

12. Rotate the Audit Store certificates on ESA A.

For more information about rotating the audit store certificates, refer to the section [Rotating Certificates on a Single Node Audit Store Cluster](#).

13. Create the ESA B on v9.0.0.0.

For more information on installing the ESA on v9.0.0.0, refer to the section [Installing ESA](#).

14. Join the ESA A and the ESA B in a Trusted Appliance Cluster.

For more information on creating a TAC, refer to the section [Trusted Appliances Cluster \(TAC\)](#) in the [Appliances Overview Guide 9.0.0.0](#).

15. Create the PSU A and PSU B on v9.0.0.0.
16. Configure the Audit Store Cluster on the ESA A, ESA B, PSU A, and PSU B.

Note:

Ensure that you add one appliance at a time.

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

17. Configure the *td-agent* on the ESA A and the ESA B in the Audit Store cluster.

For more information about configuring the *td-agent*, refer to the section [Configuring td-agent in the Audit Store Cluster](#).

18. Change the roles on the ESA A and the ESA B to *Master*.

Note:

Ensure that you add one appliance at a time.

For more information on changing roles in the ESA, refer to the section in the [Protegility Appliances Overview Guide 9.1.0.5](#).

19. Migrate the DMS logs to Audit Store cluster from the ESA 1 to the PSU A.

For more information about migrating the DMS logs to the Audit Store Cluster, refer to the section [Migrating Logs](#).

20. Shut down the ESA 1.

21. Redirect the traffic from the ESA 2 to the ESA A and ESA B.

22. Update the protector configurations to point to the PSU v9.0.0.0.

23. (Optional): Upgrade the DSGs to their latest version.

24. Perform the following steps on the ESA 2.

- a. To migrate the DMS logs without upgrading the ESA 2 to pre-v9.0.0.0, you must install the *ESA_PAP-ALL-64_x86-64_7.2.1.x.FE-1.pty* patch on the ESA 2.

Note:

If you want to migrate the metering logs and the DMS logs from the ESA 2, then apply the *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-2.pty* patch on the ESA 2.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

For more information about installing the patch, refer to the section [Migrating the ESA to v9.0.0.0](#).

- b. Complete the upgrade on the ESA 2.

For more information about completing the upgrade, refer to the section [Configuring Settings on v9.0.0.0](#).

- c. From the ESA 2, migrate the DMS logs to Audit Store cluster.

For more information about migrating the DMS logs to the Audit Store cluster, refer to the section [Migrating Logs](#).

Important:

Ensure that the data migration is completed before proceeding to the next step.

- d. Complete the post upgrade steps.

For more information about completing the post upgrade steps, refer to the section [Migrating the ESA to v9.0.0.0](#).

25. After the migration is successfully completed, shut down the ESA 2.

For more information about leaving an audit store cluster, refer to the [Protegility Storage Unit Guide 9.0.0.0](#).

8.2 Installing ESA

You can install the ESA on-premise or a cloud platform, such as, AWS, Azure, or GCP. When you upgrade from a previous version, the ESA is available as patch. The following are the different ways of installing the ESA:

- **ISO Installation:** This installation is performed for an on-premise environment where the ESA is installed on a local system using an ESA ISO is provided by Protegility. The installation of the ISO begins by installing the hardened version of Linux on your system, setting up the network, and configuring date/time. This is then followed by updating the location, setting up OS user accounts, and installing the ESA-related components.

For more information about installing the ESA using ISO, refer to the section *Installing the ESA On-Premise* in the [Protegility Installation Guide 9.1.0.5](#).

- **Cloud Platforms:** On Cloud platforms, such as, AWS, Azure, or GCP, the ESA images for the respective cloud are generated and provided by Protegility. In these images, the ESA is installed with specific components. You must obtain the image from Protegility and create an instance on the cloud platform. After creating the instance, you run certain steps for finalizing the installation.

For more information about installing the ESA on cloud platforms, refer to the section *Installing Appliances on Cloud Platforms* in the [Protegility Installation Guide 9.1.0.5](#).

Note: A temporary license is provided by default when you first install the Appliance and is valid for 30 days from the date of this installation. To continue using Protegility features, you have to obtain a validated license before your temporary license expires.

For more information about licensing, refer to [Protegility Data Security Platform Licensing Guide 9.0.0.0](#).

8.3 Prerequisites

This section describes the prerequisites which must be performed for upgrading the ESA to v9.0.0.0.

8.3.1 Accounts

The administrative account used for upgrading the ESA must be active.

Note:



Ensure to make a note of the required OS level user while moving from the ESA v7.2.1 to v9.0.0.0. These users are not exported as a part of the migration process. After moving to the ESA v9.0.0.0, you must create the OS level users.

For more information about the OS level users, refer to the [Protegility Appliances Overview Guide 9.1.0.5](#).

8.3.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a backup of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

8.3.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

8.3.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

8.3.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before initiating the upgrade process.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating the snapshots from the respective cloud platforms, refer to the *Protegility Appliances Overview Guide 9.1.0.5*.

8.3.3 Installations and Hardware Requirements

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have at least two ESAs and two PSUs on v9.0.0.0.

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

Installation Requirements

- Two ESAs v7.2.1 must be available.
- The *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-2.pty* patch file is available.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

8.3.4 High Availability (HA)

If you are upgrading an ESA appliance that is in an HA setup, then you must remove the HA services from the ESA appliance and then apply the upgrade patch.

For more information about removing the HA services, refer to the [Scalability and Availability Guide 7.2.1](#).

Note:

The HA services are not supported from version 8.0.0.0. If you continue using the HA services, then it might break the functionality of the system.

For more information about the alternate to HA services, refer to the [Fault Tolerance Guide 8.0.0.0](#) on the [My.Protegility](#) portal.

8.3.5 Trusted Appliances Cluster (TAC)

At least two ESAs must be in a Trusted Appliance Cluster.

For more information about the Trusted Appliances Cluster, refer to the section *Trusted Appliances Cluster* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

8.3.6 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the [Protegility Key Management Guide 9.1.0.0](#).

8.3.7 ESA Settings

Ensure to make a note of the required settings while moving from the ESA v7.2.1 to v9.0.0.0. These settings are not exported as a part of the migration process. After moving to the ESA v9.0.0.0, you must configure these settings as a part of the post upgrade steps.

- SMTP Settings
- Scheduled tasks



- User notifications on dashboard, if any
- Local_admin permissions
- Service Account Passwords
- OS Users
- Add/Remove services
- SNMP configuration
- Preferences Settings
- Antivirus options and settings
- Open ports

8.3.8 Creating a Metering Backup File

Ensure that you create a backup file of the metering logs before performing the upgrade on the ESA v7.2.1.

► To create a backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility` directory using the following command.
`cd /opt/protegility`
4. Create a temporary directory to save the metering logs using the following command.
`mkdir <directory_name>`

Note: Ensure that the temporary directory is accessible on the ESA v7.2.1. This directory must not be copied or moved to another location.
5. Add permissions to the temporary directory using the following command.
`chmod 755 <directory_name>`
6. Change the owner of the temporary directory to *service admin* using the following command.
`chown service_admin.service_admin <directory_name>`
7. Navigate to the temporary directory using the following command.
`cd <directory_name>`
8. Create the backup file of the metering logs using the following command.
`/opt/protegility/repository/pim/pgsql/bin/pg_dump -h localhost -U admin -p 5211 --schema metering --format=c ADMINDB > /opt/protegility/<directory_name>/<backup_filename>.bak`

8.3.9 Customized Files (Configuration Files and Certificates)

Exclude Files

The *exclude* file present in the `/opt/ExportImport/filelist` directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section *Exporting Custom Files* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Custom files with python2 scripts

If you have modified any custom files, such as, *check_password.py*, *check_username.py*, *pty_get_username_from_certificate.py*, and so on, then these must be listed in the *customer.custom* file.

CloudWatch Files

To export the *CloudWatch* configurations, you must list the cloudwatch configurations in the *customer.custom* file to export the data in the upgraded ESA.

8.3.10 Logging, Reporting, and Certificates

If you are upgrading an ESA appliance that has scheduled tasks or cluster replication tasks created by the user, then ensure that DMS options, such as, *Log-Server Repository*, *Log-Server Configuration*, and *Log-Server Event Configuration*, reporting tasks, and certificates are disabled.

Note:

If a scheduled task has scheduled tasks or cluster replication tasks created by the user, such as, the *Logging*, *Reporting*, and *Certificates* components, then uncheck them and update the scheduled task.

If there are preconfigured scheduling tasks, such as, *100 DBIntegrity Logging-Repository Integrity Check (Once a week)*, then they are automatically disabled.

A notification will be displayed on the ESA Web UI dashboard.

The following scheduled tasks were disabled due to Log Server migration: [100]

Note:

The DMS, reporting server, and DMS2mail services are not supported from version 8.0.0.0 onwards.

8.3.11 License

Ensure that you have a valid license before upgrading.

Note:

After migration, if the license status is *invalid*, then contact [Protegility Support](#).

8.4 Upgrading ESA to Pre-v9.0.0.0

This section describes the steps to upgrade from the ESA to Pre-v9.0.0.0.



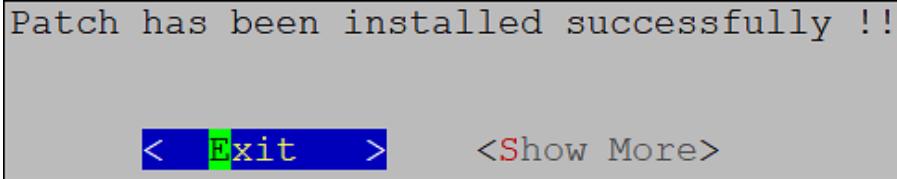
1. Login to the ESA CLI Manager with administrator credentials.
2. Navigate to **Administration > OS Console** to upload the patch.
3. Upload the patch to the */products/uploads* directory using the FTP or SCP command.
4. Navigate to **Administration > Patch Management** to install the patch.
5. Enter the *root* password.
6. Select **Install a Patch**.
7. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.0.2095.UP-2.pty* patch file and select **Install**.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

8. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the Pre-v9.0.0.0.

8.5 Post Upgrade Steps on version Pre-v9.0.0.0

This section describes the steps that must be performed on the ESA after successfully upgrading the ESA from v7.2.1 to version Pre-v9.0.0.0.

Note:

After installing the patch successfully, you must not change any configurations on the ESA.

8.5.1 Restarting the ESA

After you upgrade, restart the ESA to complete the upgrade.

► To restart the ESA:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Reboot and Shutdown > Reboot**.
The Reboot screen appears.
3. Type the reason and select **OK**.

8.5.2 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. `/var/log`
 - *Installation.log* - Provides the logs for all the installed components.
 - *syslog* - Provides collective information about the syslogs.

2. `/etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log`

8.5.3 Restoring the Backup File of the Metering Logs

A backup of the metering logs is required on the ESA Pre-v9.0.0.0 in the `/opt/protegility/` directory during the upgrade. This file is required for the migration of the metering logs.

Note: If the backup file of the metering logs is available in the directory, then skip this section.

For more information about the creating the backup file of the metering logs, refer to the section [Creating a Metering Backup File](#).

- To restore the backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility/` directory using the following command.
`cd /opt/protegility/`
4. Restore the backup file of the metering logs using the following command.
`cp <backup_filename>.bak /opt/protegility/hubcontroller/`

8.5.4 Verifying the Patch Installation

After upgrading to the ESA Pre-v9.0.0.0, you can verify the patch installation.

- To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_8.1.0.0 UP-2* patch name appears.

Ensure to check the Logs to verify that there are no errors.

8.6 Migrating the ESA to v9.0.0.0

Caution: Ensure to export the configuration files from the CLI Manager only.

Note: Ensure that you perform the procedure in the prescribed sequence listed in the section [Upgrade Process: Step-by-step Procedure](#).

This section describes the steps to migrate information from the ESA Pre-v9.0.0.0 to the ESA v9.0.0.0.

► To migrate information to the ESA v9.0.0.0:

1. On the current version of ESA (*ESA 1*), login to the WebUI using the *administrative* credentials.
2. Navigate to **System > Backup & Restore > Export**.
3. From the **Export type** field, select the **To file** option.
4. From the **Data To export** field, select the required options.

Note:

It is recommended to select all the options while performing the export operation.

Note:

If you want to export the configuration for the DSG, then select the *Export Gateway Configuration Files* and perform the export operation.

5. Click **Export**.

The following screen appears.

Output File

Export Name	<input type="text"/>
<input type="checkbox"/> Overwrite existing file (if exists)	
Password	<input type="password"/> Please input password
<input type="password"/> Please confirm password	
Export Description(optional)	<input type="text"/>
Confirm Cancel	

6. Enter the information in the **Export Name**, **Password**, and **Export Description** fields and select **Confirm**.
7. Download the exported file.
8. Upload the exported file on the *ESA A* v9.0.0.0 using your preferred method, such as, SCP, FTP, and so on.

Note:

If you are using the SCP or FTP, then ensure that the exported file is placed in the */opt/product_exports* directory and permissions for the file are set to *755*.

9. Login to the *ESA A* v9.0.0.0 WebUI using the *administrative* credentials.
10. Navigate to **System > Backup & Restore > Import**.

Note: If you are importing the configuration for the DSG appliance, then ensure to apply the DSG patch on the ESA before importing the configurations.

For more information about applying the DSG patch on the ESA, refer to the section [Install the DSG 3.0.0.0 patch](#).

The following screen appears.

Import

Select an exported file...	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>	Please select one file to show more information
----------------------------	--	---

11. Select the exported file and click **Import**.

Import	
<input type="file" value="File to Import"/>	Size: [REDACTED] Creation Time: [REDACTED] Description: [REDACTED]
Delete Import Download	This file provides the following import options: - OS configuration - Web settings - SSH settings - SSH server configuration and Keys - Certificates - Management and WebService Certificates - Firewall settings - Appliance Authentication Settings - Appliance JWT Configuration - Appliance SSO Configuration - Time-zone and NTP settings - OS Services Status - Appliance FIM Policies and Settings - User custom list of files - LDAP Server - Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery - Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster - Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster - Import policy manager web ui settings

12. Select the required options except **Appliance Configuration (ALL)** and **Certificates**.

Title	Description
Component: OS v 8.0.1 <input type="checkbox"/> Appliance Configuration (ALL) OS configuration more... <input checked="" type="checkbox"/> Web Settings Web settings more... <input checked="" type="checkbox"/> SSH Settings SSH settings more... <input checked="" type="checkbox"/> Server Identity SSH server configuration and Keys more... <input type="checkbox"/> Certificates Certificate more... <input checked="" type="checkbox"/> Management and WebService Certificates Management and WebService Certificates more... <input checked="" type="checkbox"/> Firewall Settings Firewall settings more... <input checked="" type="checkbox"/> Authentication Settings Appliance Authentication Settings more... <input checked="" type="checkbox"/> JWT Configuration Appliance JWT Configuration more... <input checked="" type="checkbox"/> SSO Configuration Appliance SSO Configuration more... <input checked="" type="checkbox"/> Timezone And NTP Time-zone and NTP settings more... <input checked="" type="checkbox"/> Services Status OS Services Status more... <input checked="" type="checkbox"/> FIM Policies and Settings Appliance FIM Policies and Settings more... <input checked="" type="checkbox"/> Custom Files and folders User custom list of files more...	
Component: LDAP v 7.1.2 <input checked="" type="checkbox"/> LDAP Server LDAP Server	
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <input checked="" type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data Import All Policy-Management Configs, Keys, Certs and Data for disaster recovery more...	
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs and Data Import All Policy-Management Configs, Keys, Certs and Data for Trusted Appliance Cluster more...	
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <input type="checkbox"/> Import All Policy-Management Configs, Keys, Certs, Data without HSM Import All Policy-Management Configs, Keys, Certs, Data but without HSM files for Trusted Appliance Cluster more...	
Component: Data Protection System v 1.4.0+10.gfa535.1.4 <input checked="" type="checkbox"/> Policy Manager Web UI Settings Import policy manager web ui settings more...	
Password: <input type="password"/> Import Cancel	

13. Click **Import**.

A message on the screen is displayed after the file is successfully imported.

8.7 Configuring Settings on v9.0.0.0

The following sections describe the steps to complete the upgrade.

8.7.1 Configuring the ESA v9.1.0.1

While migrating the ESA to v9.1.0.1, the following settings are not retained. You must configure the following settings after migrating to ESA v9.1.0.1.

SMTP Settings

You must set up an email server that supports the notification features.

For more information about configuring the SMTP settings, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Scheduled Tasks

Using **System > Task Scheduler** you can schedule appliance tasks to run automatically. You can create or manage tasks from the ESA Web UI.

For more information about configuring the scheduled tasks, refer to the section *Scheduling Appliance Tasks* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Grub Settings

To enhance security of the Protegility appliances on-premise, the GRUB menu can be protected by setting a username and password. It is recommended to secure the appliance using the GRUB settings.

For more information about securing the GRUB, refer to the section *Securing the GRand Unified Bootloader (GRUB)* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Local_admin permissions

By default, the *local_admin* user cannot login to the CLI Manager using SSH or log into the Web UI. However, you can configure this access using the tool, which changes the *local_admin* account permissions.

For more information about enabling the *local_admin* permissions, refer to the section *Changing the Local Admin Account Permission* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Service Account Passwords

Service Account users are *service_admin* and *service_viewer*. They are used for internal operations of components that do not support LDAP, such as Management Server internal users and Management Server Postgres database. You cannot log into the Appliance Web UI, Reports Management (for ESA), or CLI Manager using service accounts users.

For more information about changing the service accounts passwords, refer to the section *Changing Service Accounts Passwords* in the *Protegility Appliances Overview Guide 9.1.0.5*.

OS Users

You must configure the *OS Users* on the upgraded ESA.

For more information about OS Users, refer to the section *Managing Local OS Users* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Add/Remove services

Using the **Add/Remove Services** tool, you can install the necessary products or remove already installed ones. You must add or remove the services which were present on the ESA v7.2.1.

For more information about adding or removing service, refer to the section *Add/Remove Services* in the *Protegility Appliances Overview Guide 9.1.0.5*.

SNMP configuration

SNMP allows a remote machine to query different performance status of the Appliance, such as, start the service, set listening address, show or set community string, or refresh the service.

For more information about configuring SNMP, refer to the section *Configuring SNMP* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Preferences Settings



You must set up your console preferences using the **Preferences** menu.

For more information about preferences settings, refer to the section *Working with Preferences* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Antivirus options and settings

The AntiVirus program uses ClamAV, an open source and cross-platform antivirus engine designed to detect malicious trojan, virus, and malware threats. A single file or directory, or the whole system can be scanned. Infected file or files are logged and can be deleted or moved to a different location, as required.

For more information about configuring antivirus, refer to the section *Working with Preferences* in the *Protegility Appliances Overview Guide 9.1.0.5*.

Firewall Settings

Protegility internal Firewall provides a way to allow or restrict inbound access from the outside to Protegility Appliances.

Using the **Rules List** option, you can view the available firewall rules. Alternatively, on the Web UI, navigate to **System > Information** to view the rules.

For more information about firewall settings, refer to the section *Managing Firewall Settings* in the *Protegility Appliances Overview Guide 9.1.0.5*.

The ports in a network are communication channels through which information flows from one system to another. A list of ports that must be configured in your environment to access the features and services on the Protegility appliances.

For more information about open ports, refer to the section *Open Listening Port* in the *Protegility Appliances Overview Guide 9.1.0.5*.

8.7.2 Upgrading custom files to *python3*

From v9.0.0.0, the support for *python2* is disabled.

Therefore, if you have modified any of the files in the previous version of the ESA including the following, then ensure that they are compatible with *python3*:

- */etc/ksa/check_password.py*
- */etc/ksa/check_username.py*
- */etc/ksa/pty_get_username_from_certificate.py*

You can run the following command to check if these files are *python3* compatible.

```
python3 -m compileall <path_to_file>
```

8.7.3 Adding Permissions to the Existing Roles

Analytics and the Audit Store have roles assigned for reading and displaying the logs. Grant the required permission to the roles using the steps provided in this section.

► To add permissions to the existing roles:

1. Login to the ESA A Web UI.
2. Navigate to **Settings > Users > Roles**.

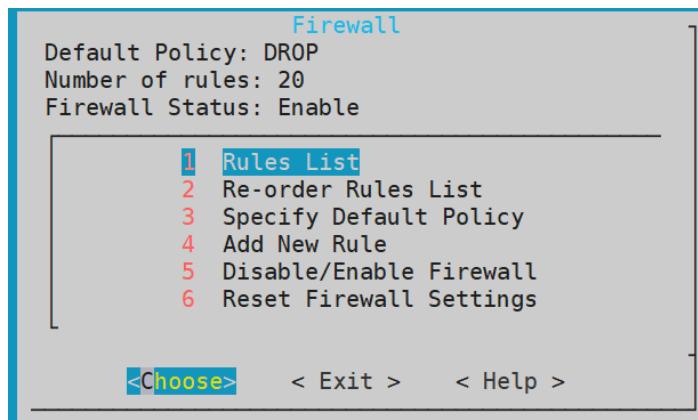
3. Click the **Security Administrator** role.
The **Security Administrator** screen appears.
4. In the **Role Permissions and Privileges** section, select the following check boxes:
 - ES Admin
 - Insight Admin
5. Click the **Save** button.
6. Enter the password and select **OK**.
A confirmation message appears.

8.7.4 Opening the Ports

You must open the *9200* and *9300* ports. These ports are used by the Audit store service for the REST & cluster communications.

► To open the ports:

1. Login to the CLI Manager.
2. Navigate to **Networking > Network Firewall**.
3. Enter the *root* password.
The following screen appears.



4. Select **Add new rule**.
5. Select **Accept** and click **Next**.
6. Select **Audit Store** and click **Next**.
7. Select **ethMNG** and click **Next**.
8. Select **Any** and click **Next**.
9. Enter description and click **Confirm**.

Note:

From the **Rules List**, verify the added rule and ensure that the ports are mentioned in the allowed ports list.

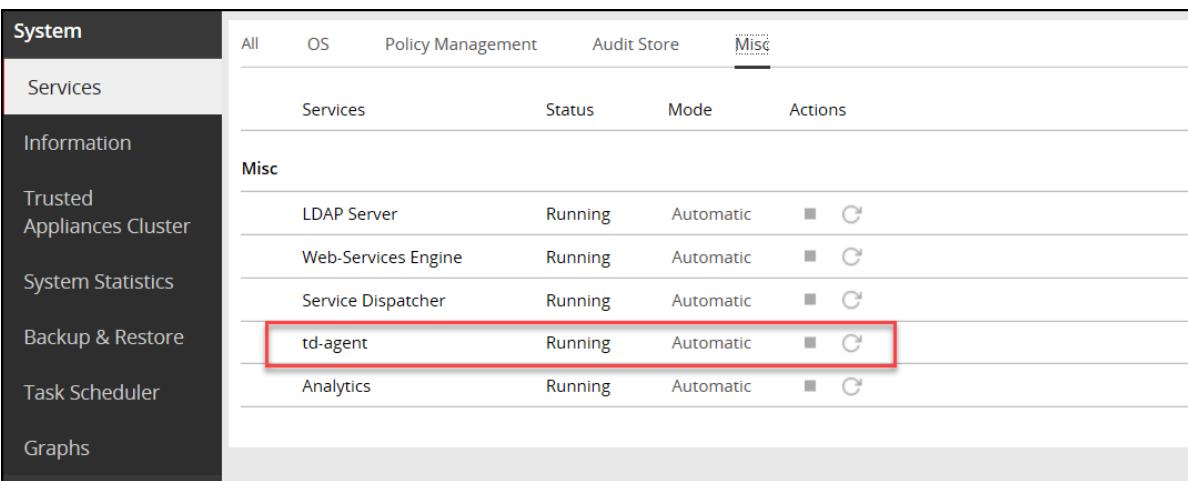
8.7.5 Rotating Certificates on a Single Node Audit Store Cluster

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 Protegity certificate and keys. For rotating custom certificates, refer to the section *Updating Audit Store Custom Certificates* in the [Audit Store Guide 9.1.0.5](#).

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

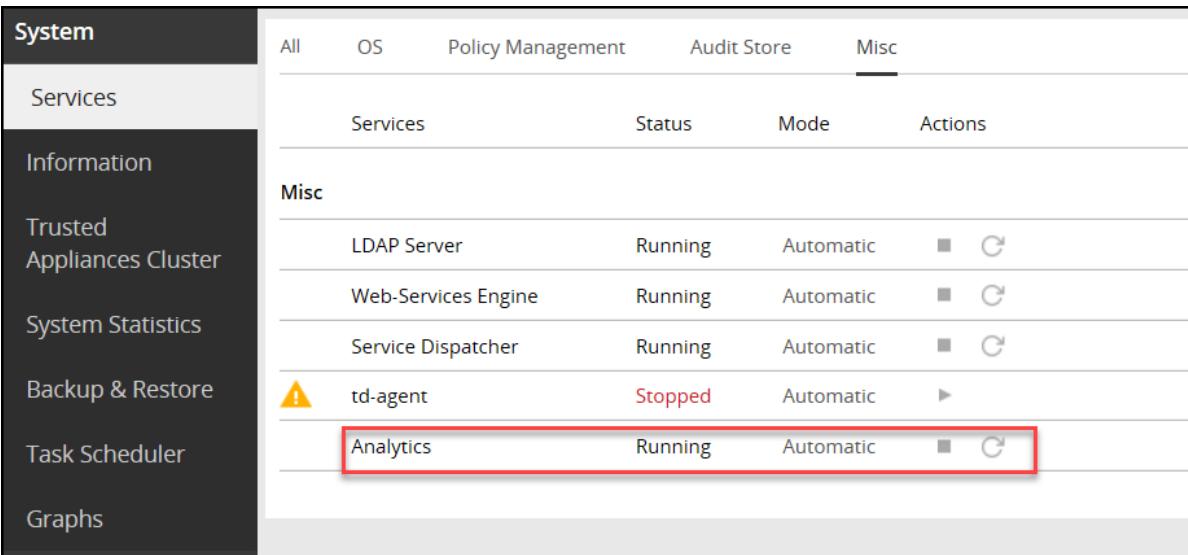
Note: Skip this step if *Analytics* is not initialized.



System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Misc						
	LDAP Server	Running	Automatic	<input type="checkbox"/>		
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>		
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>		
	td-agent	Running	Automatic	<input type="checkbox"/>		
	Analytics	Running	Automatic	<input type="checkbox"/>		

Figure 8-3: Stopping *td-agent*

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



System		All	OS	Policy Management	Audit Store	Misc
		Services		Status	Mode	Actions
Misc						
	LDAP Server	Running	Automatic	<input type="checkbox"/>		
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>		
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>		
	td-agent	Stopped	Automatic	<input type="checkbox"/>		
	Analytics	Running	Automatic	<input type="checkbox"/>		

Figure 8-4: Stopping *Analytics*

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



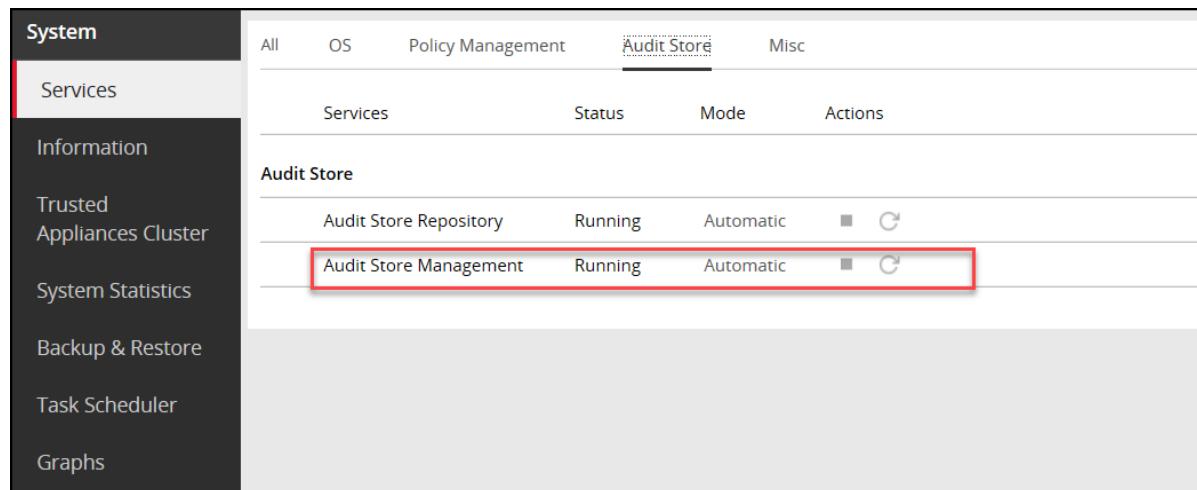


Figure 8-5: Stopping Audit Store Management

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

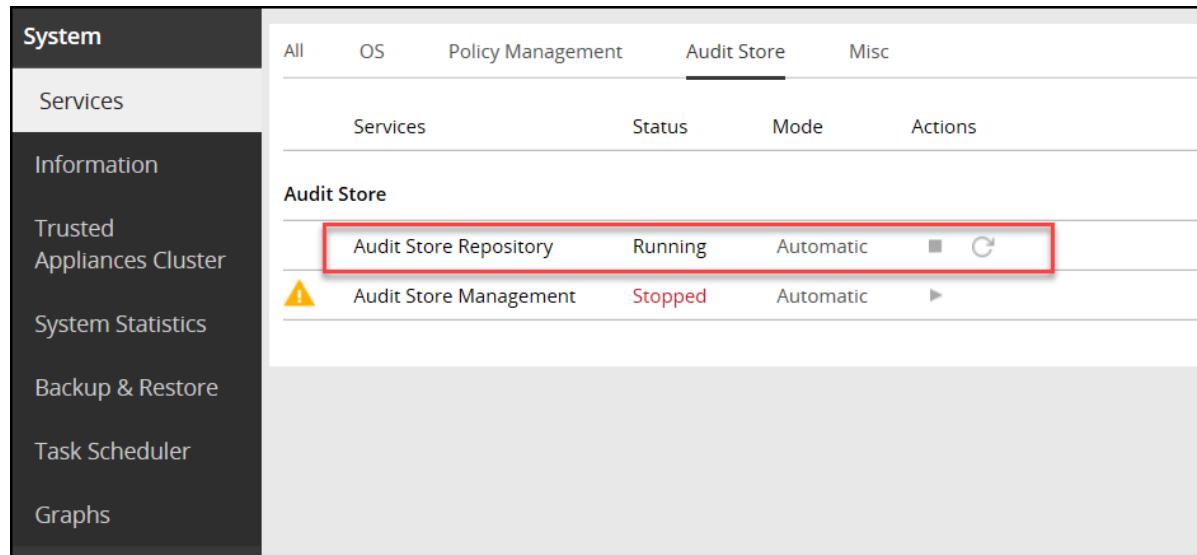


Figure 8-6: Stopping Audit Store Repository

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 8-7: Rotating Certificates

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

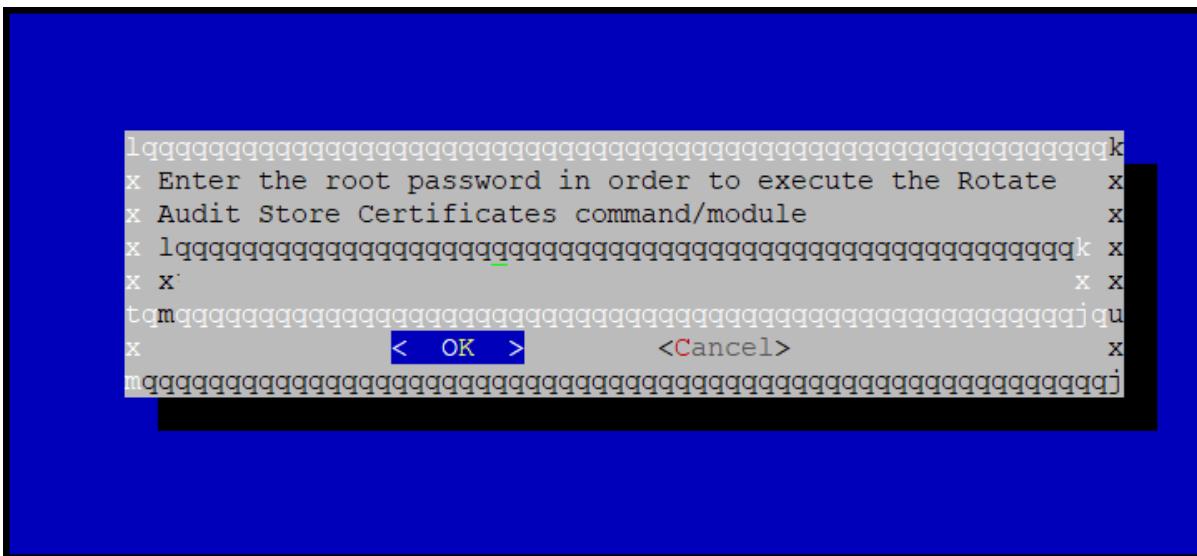


Figure 8-8: Root Password

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

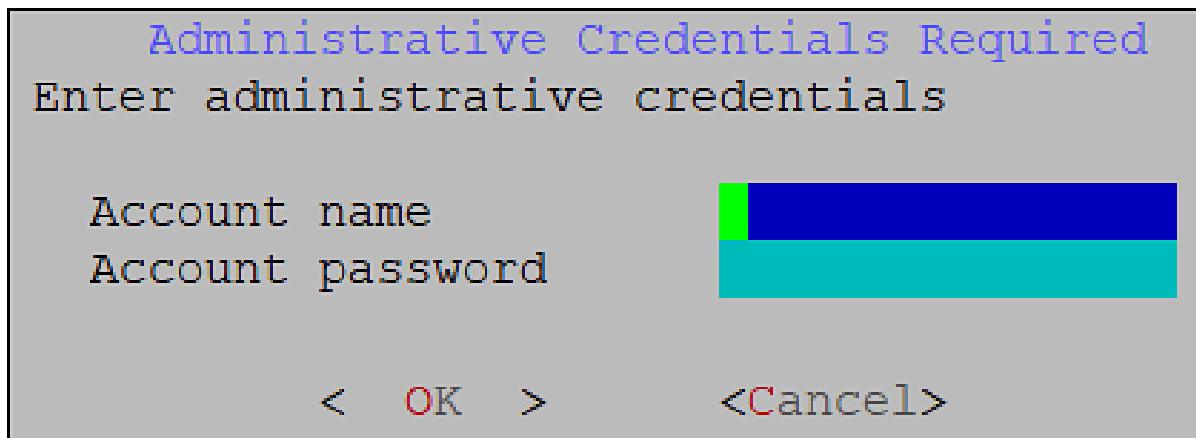


Figure 8-9: Admin Details

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

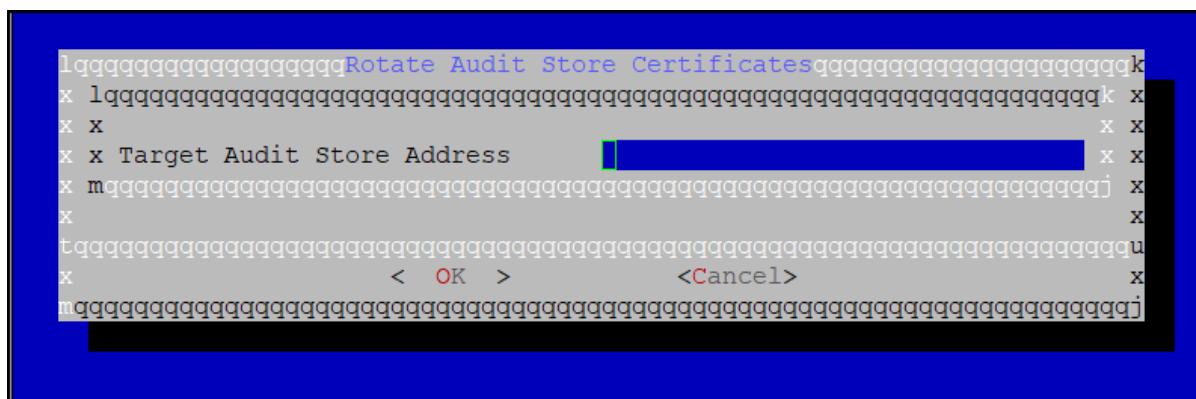


Figure 8-10: Target Audit Store Address

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

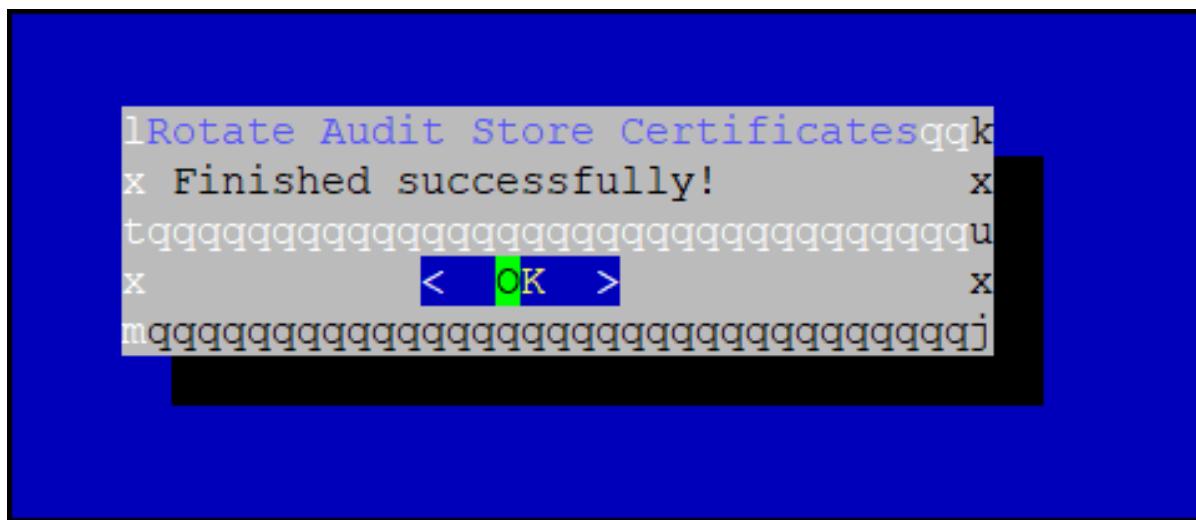


Figure 8-11: Rotation Complete

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 8-12: 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.

The screenshot shows the 'Join, View, or Leave Cluster' interface. At the top right are 'Join Cluster' and 'Leave Cluster' buttons. Below them is a 'Cluster Status' indicator with a green dot. The main area displays cluster statistics:

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
1	1	17	17	0

Below this are sections for 'Initializing Shards' (0), 'Unassigned Shards' (16), 'OS Version' (1.3.0), 'Current Master' (redacted), and 'Indices Count' (14). Further down are 'Total Docs' (190,430) and 'Number of Master Nodes' (1), 'Number of Ingest Nodes' (1).

At the bottom, there are tabs for 'Nodes' (selected) and 'Indices'. The 'Nodes' tab shows a table with columns: Node IP, Roles (Master, Data, Ingest), Action, Name, Up Time, Disk Total (Bytes), Disk Used (Bytes), Disk Avail (Bytes), and RAM. One node entry is visible with a redacted IP address, marked as a Master and Data node, with ingest checked, and an 'Edit Roles' button.

Figure 8-13: 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.

System	Logfacade	Running	Automatic	<input type="checkbox"/>
Services	Logfacade Legacy	Running	Automatic	<input type="checkbox"/>
Audit Store				
	Audit Store Repository	Running	Automatic	<input type="checkbox"/>
	Audit Store Management	Running	Automatic	<input checked="" type="checkbox"/>
Misc				
	LDAP Server	Running	Automatic	<input type="checkbox"/>
	Web-Services Engine	Running	Automatic	<input type="checkbox"/>
	Service Dispatcher	Running	Automatic	<input type="checkbox"/>
	td-agent	Running	Automatic	<input checked="" type="checkbox"/>
	Analytics	Running	Automatic	<input type="checkbox"/>

Figure 8-14: Services Started

8.8 Installing the Protegility Storage Unit

The Protegility Storage Unit consists of the *td-agent* and the Audit Store installed on the Appliance. It is a hardened appliance that is used to scale the Audit Store cluster with the logging capability of a Protegility appliance. After installing the ESA, you can add additional Protegility Storage Units to the setup.

As a basic requirement of the Audit Store Cluster, you must have at least 2 ESAs and 2 PSUs installed.

For more information about installing the Protegility Storage Unit, refer to the section *Installing the Protegility Storage Unit* in the [Protegility Storage Unit Guide 9.0.0.0](#).

8.8.1 Audit Store Clustering using the Protegility Storage Unit

Clustering is a powerful way to increase the capability of your system. You can add nodes to expand the cluster. Expanding the cluster using the Protegility Storage Unit provides an advantage by increasing the storage space available.

A basic setup is shown in the following figure.

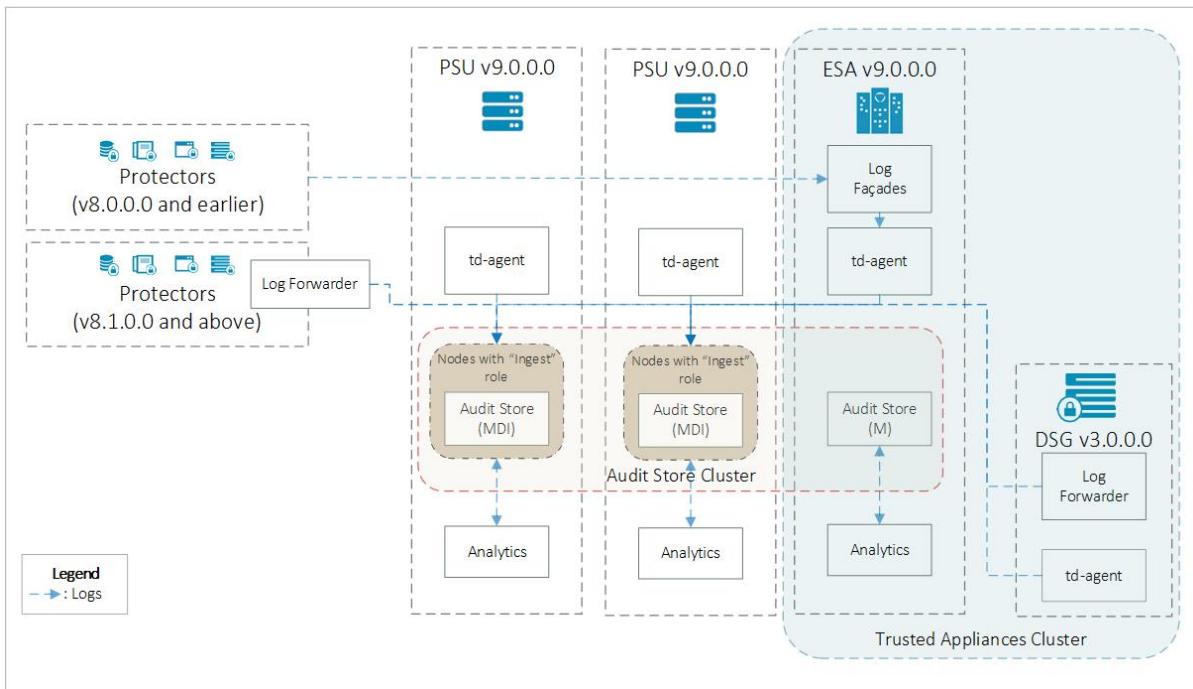


Figure 8-15: Basic Audit Store Cluster

In the figure, the arrows show the log flow direction. The basic setup consists of three systems. Here the systems consist of 1 ESA and 2 Protegility Storage Unit. The Protegility Storage Unit forms a part of the Audit Store cluster where the Audit Stores on all the nodes are linked together to form the storage unit. The logs received by the ESA are stored in the Audit Store cluster, the data would be stored on the local node or any node that is a part of the Audit Store cluster with the *ingest* role.

The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

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

The basic setup when Trusted Appliance Cluster (TAC) is implemented consists of 2 ESAs and 2 Protegility Storage Units as shown in the following figure.

Note: The Audit Store cluster is different from the TAC in the ESA. A TAC is used for grouping and managing multiple ESAs together. In the Audit Store cluster, the Audit Store nodes are grouped together to form the storage unit. The Audit Stores in the Audit Store cluster might be a part of the ESA or the Protegility Storage Unit. The Protegility Storage Unit may or may not be a part of the TAC.

For more information about the TAC, refer to the section *Trusted Appliances Cluster (TAC)* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

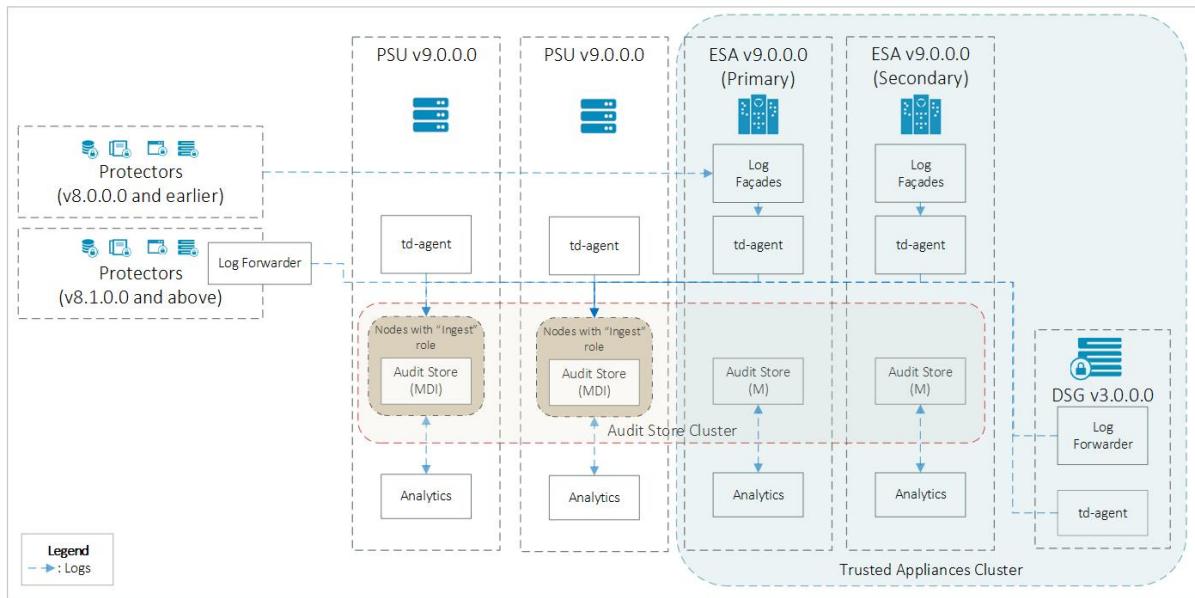


Figure 8-16: Basic Audit Store Cluster in TAC

The Audit Store cluster is flexible and nodes can be added and removed from the Audit Store cluster based on your requirements. Thus, multiple nodes can be added to the Audit Store cluster as shown in the following figure.

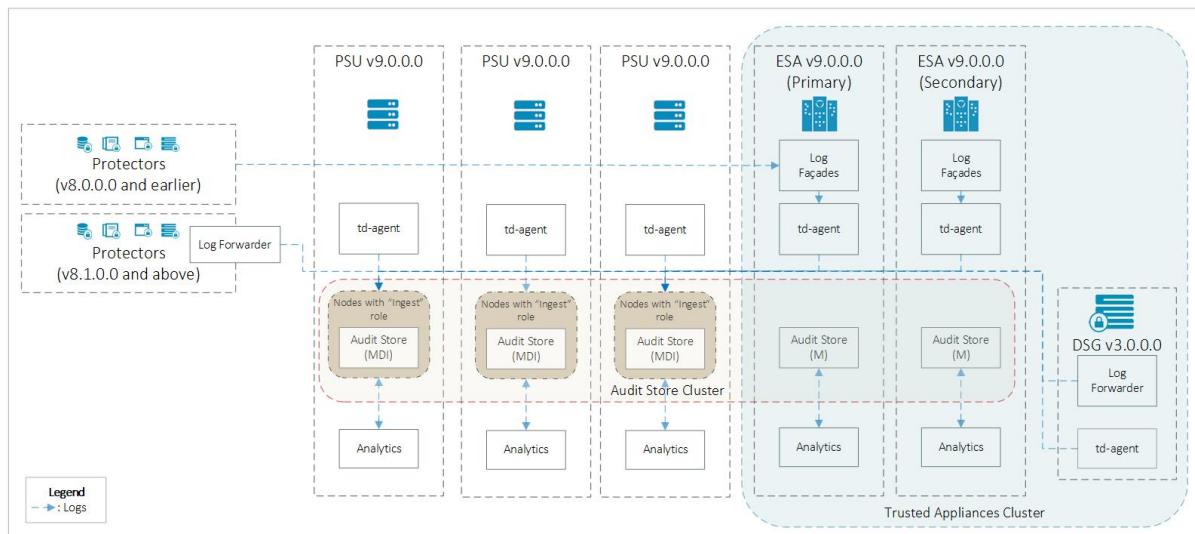


Figure 8-17: Multi-Node Cluster

Note: The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

If any node is not required, then the node can be removed from the Audit Store cluster. When the node is removed from a cluster, the indexes and internal configurations, such as, the td-agent and Analytics settings are reset. In this case, the Protegility Storage Unit remains uninitialized and needs to be added to another Audit Store cluster before it can be used again.

8.8.1.1 Completing the Prerequisites

Ensure that the following prerequisites are met before configuring the Audit Store Cluster. Protegility recommends that the Audit Store Cluster has a minimum of 1 ESA and 2 PSUs or 2 ESAs and 1 PSU for creating a highly-available multi-node Audit Store cluster.

1. Install and set up the first ESA. This will be the Primary ESA if you set up a TAC.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

2. If you require TAC, then install and set up the second ESA. This will be the Secondary ESA in a TAC. Skip this step if TAC is not required.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

3. Install and set up the first PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

4. Install and set up the second PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

8.8.1.2 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, Protegility Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as, *td-agent*, is started and Protegility 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.

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

The following screen appears.

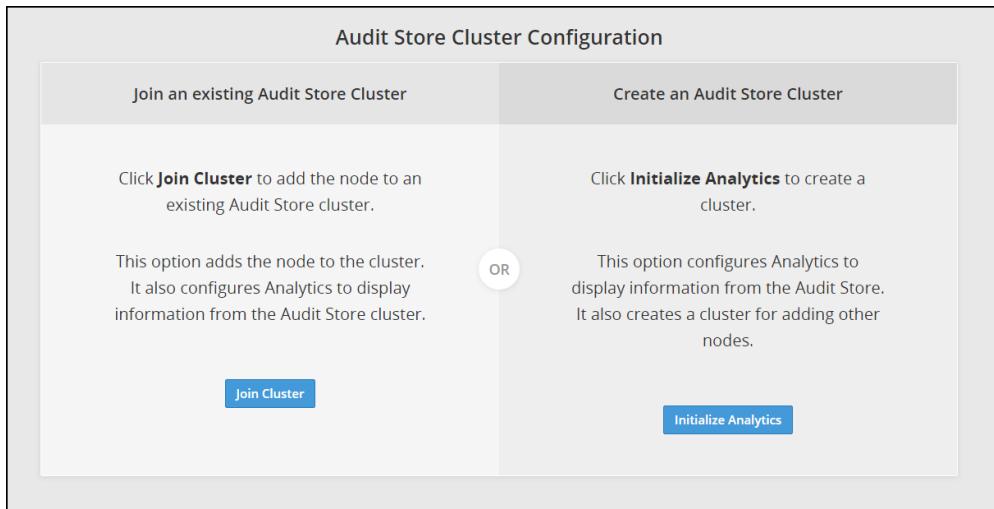


Figure 8-18: Analytics Screen

4. Click **Initialize Analytics**.

Protegility 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.

Protegility 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.

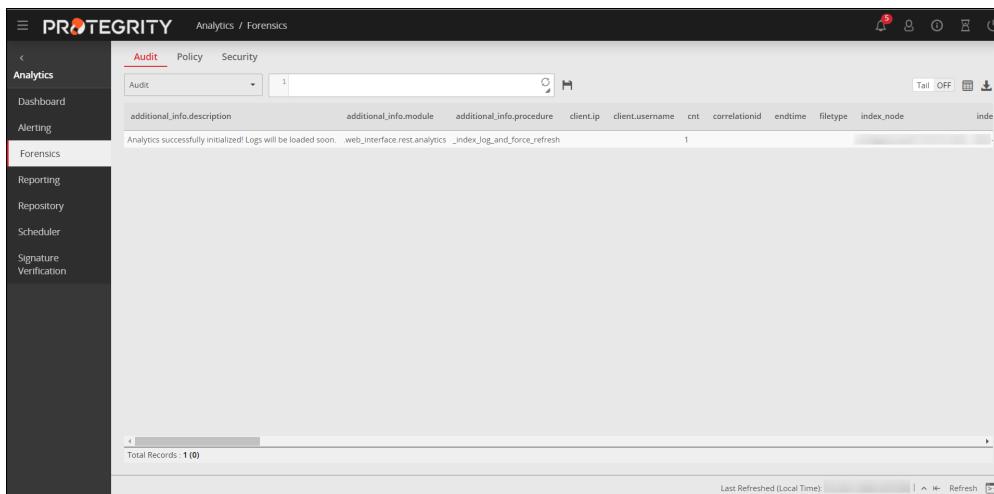


Figure 8-19: Forensics

8.8.1.3 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 *Protegility 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.

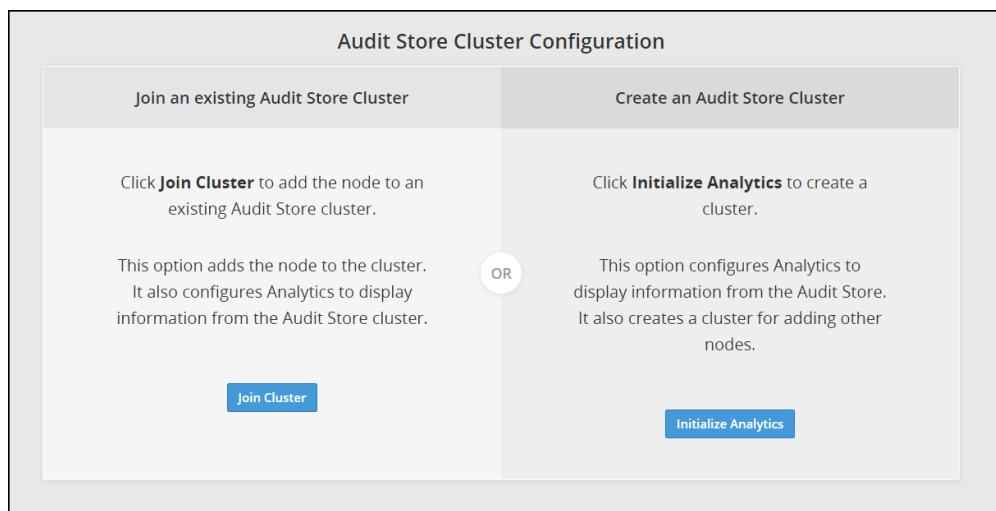


Figure 8-20: Analytics Screen

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**

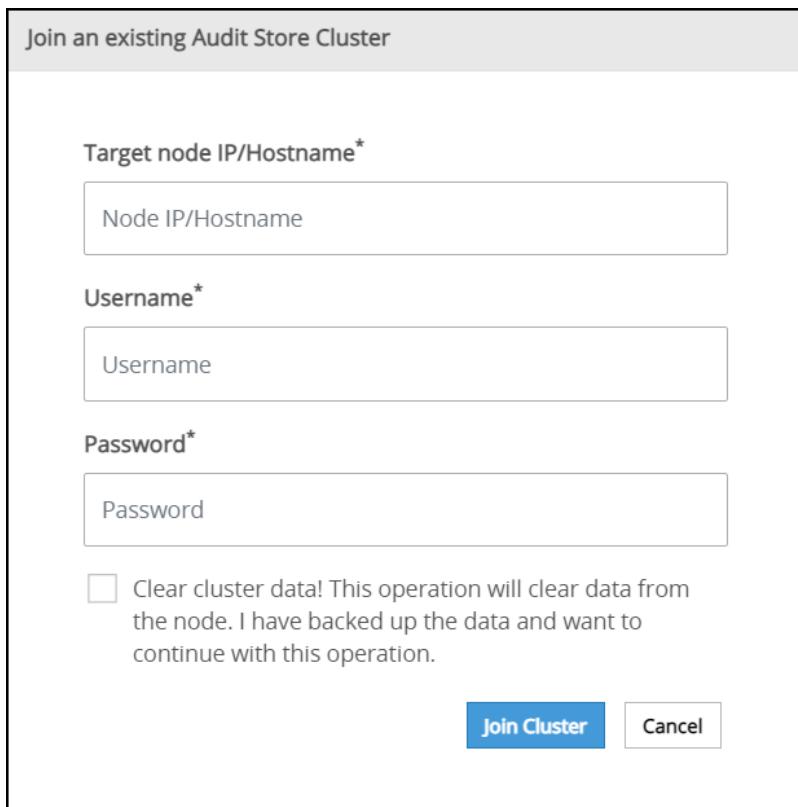


Figure 8-21: Joining an Audit Store Cluster

- 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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.

Protegility 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.

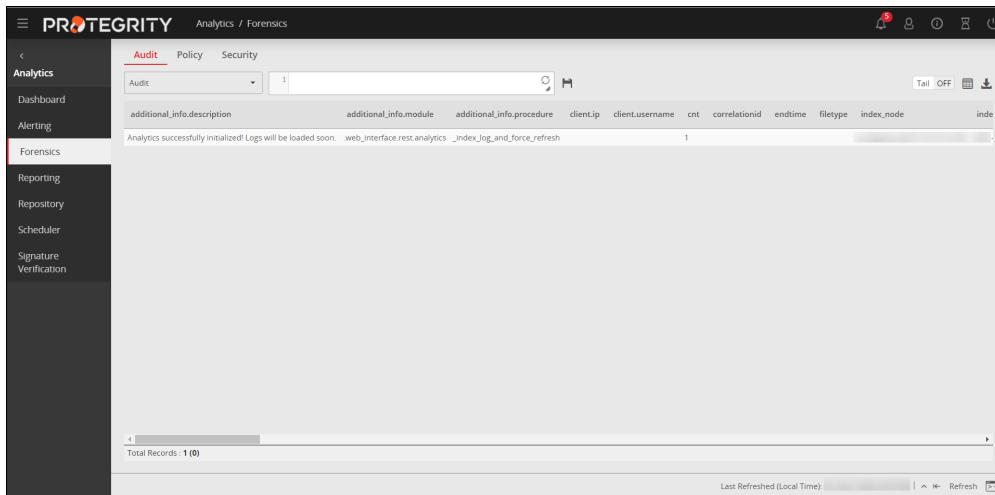


Figure 8-22: Protegility Analytics

8.8.1.4 Adding the Protegility Storage Unit to the Audit Store Cluster

Add the Protegility Storage Unit to the Audit Store Cluster that is initialized on the ESA. You need to specify the IP address of the Audit Store cluster that you want to join with the username and password of the admin user for authorization.

Before you begin

Ensure that the Audit Store services are running on the ESA Web UI by navigating to **System > Services > Audit Store**.

Note: 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 PSU Web UI would make the cluster information inconsistent, make the Audit Store cluster unstable, and would lead to errors.

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 *Protegility Appliances Overview Guide 9.1.0.5*.

► To join the Audit Store cluster:

1. Log in to the Web UI of the Protegility Storage Unit.
2. Open the **Audit Store Management** screen.
The **Cluster Overview** screen appears.

The screenshot shows the 'Cluster Overview' screen. At the top, there are buttons for 'Join Cluster' (highlighted in blue) and 'Leave Cluster'. Below this, the 'Cluster Name' is listed as 'insight'. The main area displays various cluster metrics in a grid format:

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		
190,528	1	1		

Below the metrics, there are two tabs: 'Nodes' (selected) and 'Indices'. Under 'Nodes', a table provides detailed information for a single node:

Node IP	Master	Roles	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
192.168.1.100	✓	Master, Data, Ingest	Edit Roles	node-1	8.8h	39,502,524,416	7,033,622,528	32,468,901,888	16.6

Figure 8-23: Cluster Overview Screen

3. Click **Join Cluster**.

The **Join Cluster** screen appears.

Note: The **Join Cluster** button is disabled if a node is already a part of the Audit Store cluster.

The dialog box has a title bar 'Join an existing Audit Store Cluster'. It contains fields for 'Target node IP/Hostname*', 'Username*', and 'Password*'. There is also a checkbox for clearing cluster data and a note about backing up data. At the bottom are 'Join Cluster' and 'Cancel' buttons.

Target node IP/Hostname*	
<input type="text" value="Node IP/Hostname"/>	
Username*	
<input type="text" value="Username"/>	
Password*	
<input type="password" value="Password"/>	
<input type="checkbox"/>	Clear cluster data! This operation will clear data from the node. I have backed up the data and want to continue with this operation.
<input type="button" value="Join Cluster"/> <input type="button" value="Cancel"/>	

Figure 8-24: Join Cluster Dialog Box

4. Specify the following details for the node that you want to connect.

- **Target node IP/Hostname:** This is the IP address or hostname of the node that you want to connect to.

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

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

For more information about creating an Audit Store cluster, refer to the section *Creating a Local Cluster* in the [Protegility Analytics Guide 9.1.0.5](#).

- **Username:** This is the administrator user name to connect to the target machine. For example, admin.

- **Password:** This is the password for the user.

5. Click **Join Cluster**.

Note: The **Join Cluster** button in this dialog box is enabled after you specify the required information in all the fields and select the check box.

The Audit Store data on the node is cleared . The node is then added to the Audit Store cluster. The Cluster Overview screen appears with the updated Audit Store cluster information. The **Join Cluster** button is disabled and the **Leave Cluster** button is now enabled.

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
2	2	17	34	0

Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count
0	0	1.3.0	[redacted]	14

Total Docs	Number of Master Nodes	Number of Ingest Nodes
192,494	2	2

Nodes		Indices		Details									
Node IP		Roles		Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
[redacted]		✓	✓	✓	[Edit Roles]			[redacted]	9h	39,502,524,416	7,035,338,752	32,467,185,664	16,6
[redacted]		✓	✓	✓	[Edit Roles]			[redacted]	3.4m	39,502,524,416	7,001,763,840	32,500,760,576	16,6

Figure 8-25: Node Added to Cluster

Repeat the steps provided in this section to add the remaining Protegility Storage Units you installed to the Audit Store Cluster.

8.8.1.5 Refreshing the Audit Store Cluster

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

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

8.8.1.6 Configuring td-agent in the Audit Store Cluster

Complete the following steps after adding the Protegility Storage Unit to the Audit Store cluster. This configuration is required for processing and storing the logs received by the Audit Store.

Note: This step must be performed on all the ESAs in the Audit Store cluster.

Before performing the steps provided here, verify that the Audit Store cluster health status is green on the **Audit Store Management** screen of the ESA Web UI.

1. Login to the CLI Manager of the *ESA* node.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
3. Enter the root password and select **OK**.
4. Enter the username and password for the administrative user, such as, admin.
5. Select **OK**.
6. In the *Setting ESA Communication* screen, select **OK**.
7. Specify the IP addresses of all the Protegility Storage Unit machines in the cluster, separated by commas.



Figure 8-26: Forward Logs

8. Select **OK**.
9. Type *y* to fetch certificates for communicating with the ESA and select **OK**.

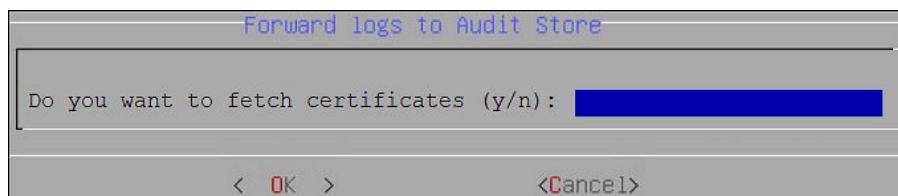


Figure 8-27: Fetch Certificates

10. Enter the admin username and password and select **OK**.
- Repeat the steps provided in this section on all the ESAs in the Audit Store Cluster.

8.8.1.7 Verifying the Audit Store Cluster

View the Audit Store Management page to verify that the configurations that you performed were completed successfully using the steps provided here.

1. Login to the ESA Web UI.
2. Navigate to the **Audit Store Management** page.
3. Verify that the nodes are added to the cluster. The health of the nodes must be either green or yellow.
4. If you added additional ESAs for creating a TAC, then verify that the ESA has only the master role.

The screenshot shows a cluster named 'insight' with the following statistics:

- Number of Nodes: 3
- Number of Data Nodes: 2
- Active Primary Shards: 17
- Active Shards: 34
- Relocating Shards: 0
- Initializing Shards: 0
- Unassigned Shards: 0
- OS Version: 1.3.0
- Current Master: [redacted]
- Indices Count: 14
- Total Docs: 212,995
- Number of Master Nodes: 3
- Number of Ingest Nodes: 2

The 'Nodes' tab is selected, showing a table of nodes with their IP addresses, roles (Master, Data, Ingest), and various metrics like Up Time, Disk Total, and RAM usage. One row's 'Roles' column is highlighted with a red box.

Figure 8-28: Nodes Added to Cluster

8.8.2 Optional: Using an External SIEM

If you have an external SIEM for storing your logs, then you can configure the ESA and Protectors to sent the logs to your SIEM. You can use just your SIEM with the Protegility Audit Store and Protegility Storage Unit for storing logs.

For more information about configuring an external SIEM, refer to the section *Sending Logs to an External Location* in the [Audit Store Guide 9.1.0.5](#).

8.9 Migrating DMS Logs and Metering Data

If your ESA is a part of the TAC setup, it is recommended to migrate your logs and metering data to Protegility Analytics to avoid data loss during upgrade. This section describes how to upgrade DMS logs and metering data from your current system to Protegility Analytics.

Note: Ensure that the backup of the metering logs is available on the ESA Pre-v9.0.0.0 in the `/opt/protegility/` directory.

If the backup file of the metering logs is unavailable, then you must restore the metering backup file.

For more information about the creating and restoring the backup file of the metering logs, refer to the sections [Creating a Metering Backup File](#) and [Restoring the Backup File of the Metering Logs](#).

8.9.1 Setting the Audit Store

Before you send the DMS logs to the PSU, you need to specify the Audit Store where the logs must be sent to, in this case, a PSU that is part of the Audit Store cluster in v9.0.0.0. Complete the following steps to set the Audit Store that must receive the logs.

Perform the following steps to forward logs.

1. Login to the CLI Manager on the Secondary ESA where the `ESA_PAP-ALL-64_x86-64_7.2.1.x.FE-1.pty` patch is installed.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.

Tools:

```
Disk Management
Rotate Appliance OS Keys
-- Removable Media Management --
  Disable CD/DVD Drives
  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
```

Figure 8-29: Forwarding Logs

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

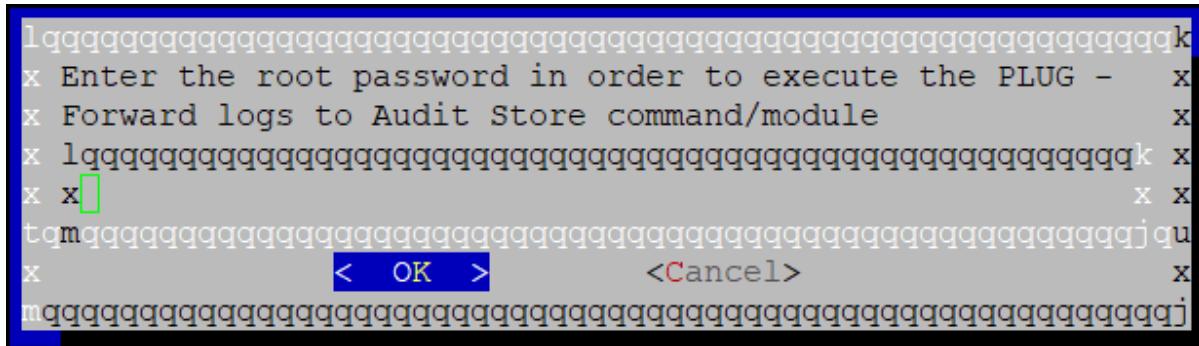


Figure 8-30: Root Password Screen

4. Enter the username and password for the admin user and select **OK**.

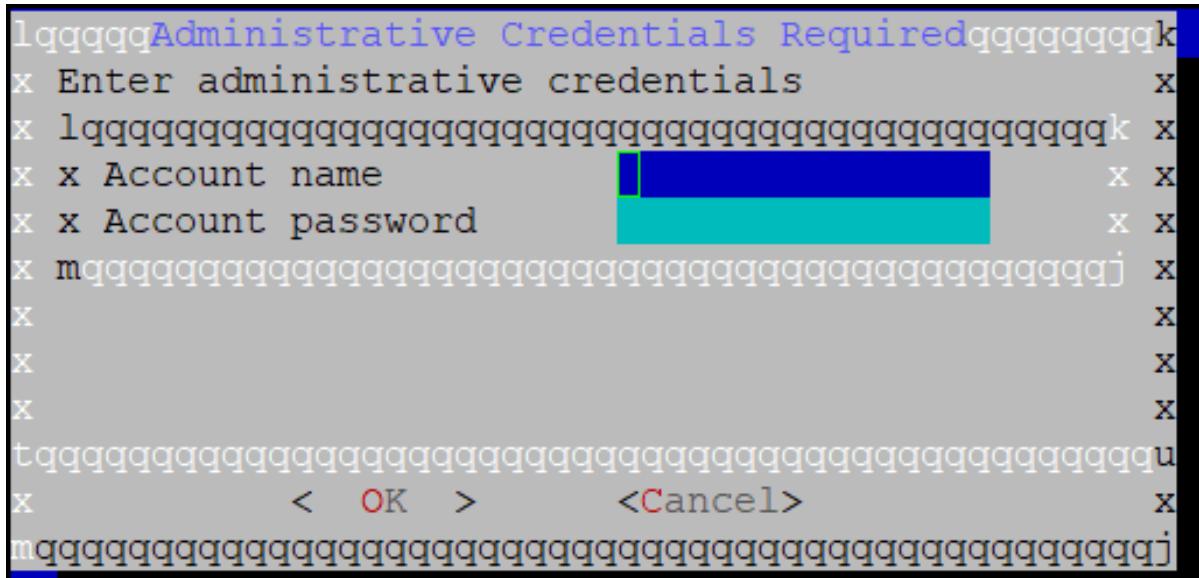


Figure 8-31: Admin Details Screen

5. Select **OK**.

Figure 8-32: Certificates Information

6. Enter the IP address of the PSU node that is a part of the Audit Store cluster of v9.0.0.0 and select **OK**.

Figure 8-33: Audit Store Details

7. Enter *y* to fetch certificates and select **OK**.

Specifying `y` fetches `td-agent` certificates from target node. These certificates can then be used to validate and connect to the target node. They are required to authenticate with the Audit Store while forwarding logs to the target node.

If the certificates are already available on the system, you do not want to fetch the certificates, or you want to use custom certificates, then specify n in this screen.

Figure 8-34: Audit Store Certificates

8. Enter the credentials for the admin user of the destination machine and select **OK**.

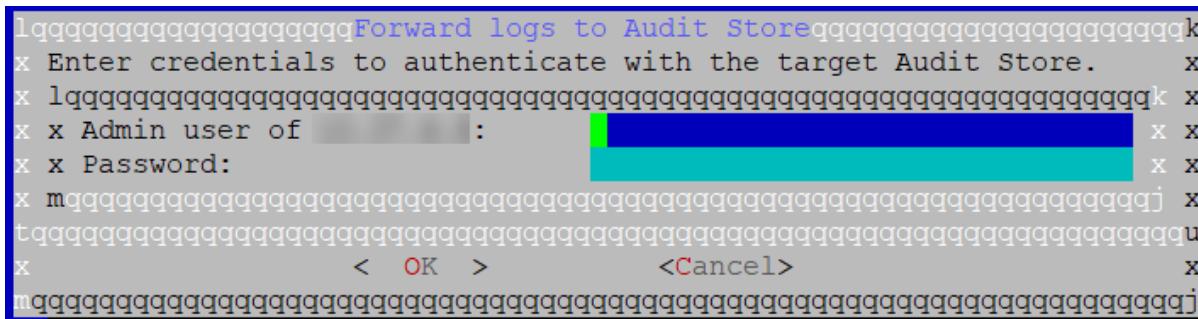


Figure 8-35: Admin User Details

The *td-agent* service is configured to send logs to the Audit Store and the CLI menu appears.

8.9.2 Migrating Logs

Migrate the logs from your current system to the Audit Store using the DMS Exporter. The logs are exported from the Postgres database to the Audit Store. Ensure that you import the logs that you require in the Audit Store to Postgres before you migrate the logs. Your existing archives would not be usable till they are exported to the Audit Store.

For more information about using the DMS Exporter, refer to the section [Appendix C: Migrating Logs Using the DMS Exporter](#).

Note:

It is recommended that all the logs are migrated from the current system using the DMS Exporter before performing any protect, unprotect, or reprotect operations.

Verify that the total hard disk space available is as per the following formula:

```
2 x (Total size of the Current used space + Size of the Upgrade patch)
```

For STA and LTA logs, import them back to Postgres before running the DMS Exporter. Ensure that the free space available on your system before importing STA and LTA logs is *2 times the space of the STA logs + LTA logs*. Contact Protegility Services if you need help with migrating your STA and LTA logs.

Complete the following steps to migrate logs to the Audit Store.

1. Ensure that the steps in [Setting the Audit Store](#) are complete.
2. On the Secondary ESA where the *ESA_PAP-ALL-64_x86-64_7.2.1.1773.FE-1.pty* patch is installed, login to the CLI Manager as the root user.
3. Navigate to **Administrator > OS Console**.
4. Enter the *root* password and click **OK**.
5. Navigate to the */opt/protegility/dms_exporter* directory.
6. Stop the DMS service using the following command:

```
dms stop
```

7. Run the following command for using the DMS Exporter.

```
python dms_exporter.py start
```

Note:

Use the command `python dms_exporter.py -h` or `python dms_exporter.py --help` to view the usage information for the command.

The DMS exporter sends logs in batches, where the exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store. Thus, if you have 4200000 rows, then the DMS Exporter will send rows in eight batches of 500000 rows and the ninth batch of the remaining 200000 rows.

Note:

If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the `last_imported_index` file in the `/opt/protegility/dms_exporter` directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics** in the ESA v9.0.0.0.

The logs are exported to the Audit Store. Verify that the export was successful by navigating to `/var/log/dms_exporter` on the ESA and viewing the export status in the `dms_exporter.log` file.

Then, the logs can be seen on the **Forensics** tab in Protegility Analytics of the ESA v9.0.0.0. These logs can then be used for further analysis.

8.10 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

8.10.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

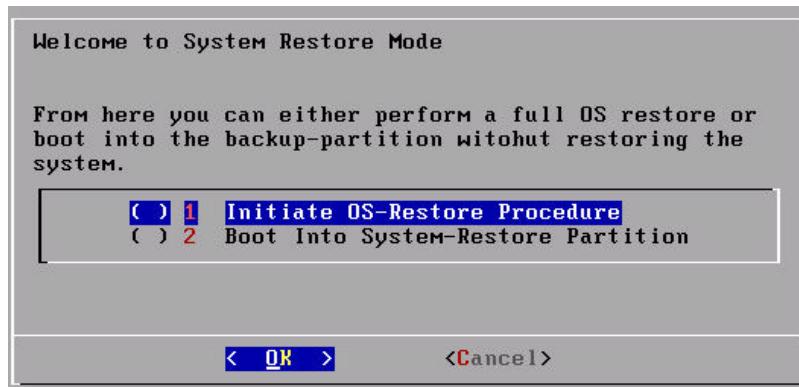
► To restore the system to the previous version:

1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the `root` password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.
The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

8.10.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

8.10.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.

4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

8.10.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.

13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

8.10.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

Chapter 9

Upgrading from v8.1.0.0 to v8.1.0.1

[9.1 Prerequisites](#)

[9.2 Upgrading ESA from v8.1.0.0 to v8.1.0.1](#)

[9.3 Upgrading PSU from v8.1.0.0 to v8.1.0.1](#)

[9.4 Verifying Patch Installation](#)

[9.5 Post Upgrade Steps](#)

[9.6 Restoring to the Previous Version of ESA](#)

This section describes the steps to upgrade the ESA, PSU, and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the PSU and protector.

9.1 Prerequisites

The prerequisites for upgrading the ESA must be preformed on the following components:

- Accounts
- Backup and Restore
- Installations and Hardware Requirements
- Trusted Appliances Cluster (TAC)
- Keys
- Customized files (Configuration files, Certificates)
- Install the pre-patch on a PSU in the v8.1.0.1 Audit Store cluster

Note: If you are using an external SIEM, then complete the steps from the section [Appendix E: Optional: Updating settings for External Databases](#).

9.1.1 Accounts

The administrative account used for upgrading the ESA must be active.

Note:

Ensure to make a note of the required OS level user before upgrading the ESA. These users are not exported as a part of the migration process. After moving to the upgraded ESA, you must create the OS level users.

For more information about the OS level users, refer to the [Protegility Appliances Overview Guide 9.1.0.0](#).

9.1.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *Working with Backup and Restore* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a backup of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* option and perform the export operation.

9.1.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

9.1.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

9.1.2.3 Creating a Snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before initiating the upgrade process.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating the snapshots from the respective cloud platforms, refer to the *Protegility Appliances Overview Guide 9.1.0.5*.

9.1.3 Installations and Hardware Requirements

Installation Requirements

- An ESA v8.1.0.0 must be available to upgrade to the v8.1.0.1.
- The *ESA_PAP-ALL-64_x86-64_8.1.0.1.1984.UP-1.pty* patch file is available.
- The minimum space available in the */opt* directory should be more than twice the size of the patch files.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must have the v8.1.0.0 platform release installed with at least the following components:

- 2 ESAs
- 2 Protegility Storage Units (PSUs)

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

9.1.4 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section [Working with Keys](#) in the [Protegility Key Management Guide 9.1.0.0](#).

9.1.5 Customized Files (Configuration Files and Certificates)

Exclude Files

The *exclude* file present in the */opt/ExportImport/filelist* directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section [Exporting Custom Files](#) in the [Protegility Appliances Overview Guide 9.1.0.5](#).

Custom files with python2 scripts

If you have modified any custom files, such as, *check_password.py*, *check_username.py*, *pty_get_username_from_certificate.py*, and so on, then these must be listed in the *customer.custom* file.

CloudWatch Files

To export the *CloudWatch* configurations, you must list the cloudwatch configurations in the *customer.custom* file to export the data in the upgraded ESA.

9.1.6 Configuring the External Elasticsearch with Open Distro

If you are using an external Elasticsearch database with Open Distro with Protegility Analytics, then you need to complete the configurations provided here before upgrading the ESA. The configurations provided here must be completed on your external Elasticsearch.

Before you begin

Ensure that you take a backup of your Elasticsearch before completing the following steps.

► To configure the external Elasticsearch with Open Distro:

1. Login to the system where the external Elasticsearch with Open Distro is installed.

Caution: You must complete these steps only if you have an external Elasticsearch with Open Distro configured with Protegility Analytics, else skip the steps provided in this section.

2. Navigate to the `/usr/share/elasticsearch/plugins/opendistro_security` directory using the following command.

```
cd /usr/share/elasticsearch/plugins/opendistro_security
```

3. Create a copy of the `roles.yml` file.

```
cp roles.yml roles.yml.bkup
```

4. Open the `roles.yml` file.

```
vi roles.yml
```

5. Add the code marked in bold to the file.

```
insight_analytics:  
  readonly: true  
  cluster:  
  .: <existing configuration>  
  .:  
    # upgrade  
    - "indices:admin/template/get"  
    - "indices:admin/template/delete"  
  .: <existing configuration>  
  .:  
    indices:  
      'pty_insight_*':  
        '*':  
  .: <existing configuration>  
  .:  
    # misc  
    - "indices:monitor/settings/get"  
  .: <existing configuration>  
  .:
```

6. Save and close the file.

9.2 Upgrading ESA from v8.1.0.0 to v8.1.0.1

This section describes the steps to upgrade from the ESA v8.1.0.0 to the ESA v8.1.0.1.

► To install the ESA v8.1.0.1 patch:

1. Login to the ESA Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.1.1984.UP-1.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

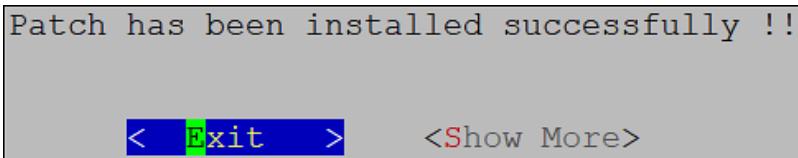
For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

The file upload is initiated.

Note:

Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the ESA CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the root password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.1.1984.UP-1.pty* patch file and select **Install**.
10. Select **Exit** on the following screen.



The patch is installed and the ESA is upgraded to the ESA v8.1.0.1.

9.3 Upgrading PSU from v8.1.0.0 to v8.1.0.1

This section describes the steps to upgrade from the PSU v8.1.0.0 to the PSU v8.1.0.1.

1. Login to the PSU Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *PSU_PAP-ALL-64_x86-64_8.1.0.1.77.UP-1.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.

- If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

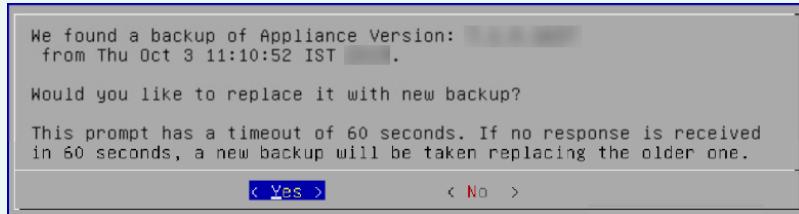
For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

The file upload is initiated.

Note: Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the PSU CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the *root* password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *PSU_PAP-ALL-64_x86-64_8.1.0.1.77.UP-1.pty* patch file and select **Install**.

Note: If a backup operation is performed before upgrading to the PSU v8.1.0.1, then the following message to replace the existing backup appears.



You can select **Yes** to overwrite the existing backup. Alternatively, you can select **No** to retain the existing backup and continue the upgrade operation.

10. Select **Exit** on the following screen.



The patch is installed and the PSU is upgraded to the PSU v8.1.0.1.

9.4 Verifying Patch Installation

After upgrading the ESA and PSUs to v9.1.0.0, you can verify the patch installation.

9.4.1 Verifying the ESA Patch Installation

After upgrading to the ESA v8.1.0.1, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_8.1.0.1* patch name appears.

5. Login to the ESA Web UI.
6. Navigate to the **System > Information** page.

The ESA is updated to v8.1.0.1 in the **Installed Patches** section.

Ensure that there are no errors in the logs.

9.4.2 Verifying the PSU Patch Installation

After upgrading to the PSU v8.1.0.1, you can verify the patch installation.

► To verify the patch installation:

1. Login to the PSU CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *PSU_8.1.0.1* patch name appears.

5. Login to the PSU Web UI.
6. Navigate to the **System > Information**.

The PSU is updated to v8.1.0.1 in the **Installed Patches** section.

Note: Ensure that there are no errors in the logs.

9.5 Post Upgrade Steps

Ensure that the following steps are performed after the ESA upgrade is completed:

9.5.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. `/var/log`

- *Installation.log* - Provides the logs for all the installed components.
- *syslog* - Provides collective information about the syslogs.

2. `/etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log`

9.5.2 Restarting the System

After the ESA patch, *ESA_PAP-ALL-64_x86-64_8.1.0.1.1984.UP-1.pty* is installed successfully, restart the ESA machine. This ensures the configuration files of the Linux Kernel are upgraded.

9.5.3 Updating the Priority IP List for Signature Verification

Signature verification jobs can only run on the ESAs, they cannot run on the PSUs. Ensure that you update the priority IP list for the default signature verification jobs after you set up the system. By default, the Primary ESA will be used for the priority IP. If you have multiple ESAs in the priority list, then additional ESAs are available to process the signature verifications jobs that must be processed.

For example, if the maximum jobs to run on an ESA is set to 4 and 10 jobs are queued to run on 2 ESAs, then 4 jobs are started on the first ESA, 4 jobs are started on the second ESA, and 2 jobs will be queued to run till an ESA job slot is free to accept and run the queued job.

For more information about scheduling jobs, refer to the section *Using the Scheduler* in the *Protegility Analytics Guide 9.1.0.5*.

For more information about signature verification jobs, refer to the section *Verifying Signatures* in the *Protegility Analytics Guide 9.1.0.5*.

Use the steps provided in this section to update the priority IP list.

1. Login to the ESA Web UI.
2. Navigate to **Analytics > Scheduler**.



3. From the **Action** column, click the **Edit** icon () for the **Signature Verification** task.
4. Update the **Priority IPs** field with the list of the ESAs available separating the IPs using commas.
5. Click **Save**.

9.5.4 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

Before you begin

Keep the following information handy before the setup process:

- SMTP server details

- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is **25**.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.
Protegility Reporting requires a full email address in the Username.
7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.
A message box appears.
14. Click **EXIT** to save the settings.

9.6 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

9.6.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system.
A screen to enter the reason for restart appears.

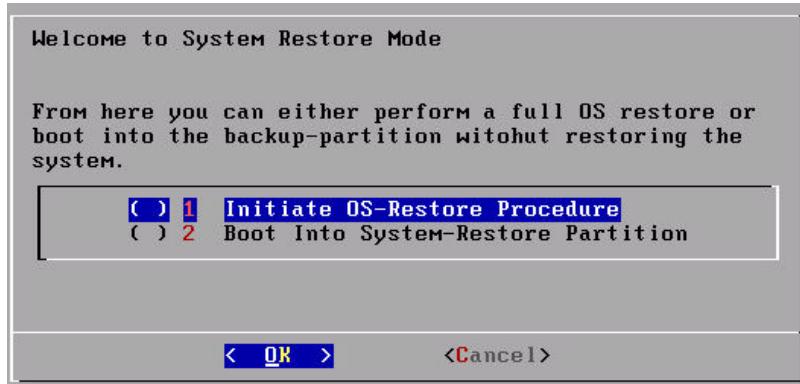
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

9.6.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

9.6.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

9.6.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.

7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

9.6.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disks**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

Chapter 10

Upgrading from v7.2.1 to v8.1.0.0

[10.1 Upgrading to ESA v7.2.1 to ESA v8.1.0.0](#)

[10.2 Upgrading Protectors](#)

This section describes the steps to upgrade the ESA v7.2.1 to the ESA v8.1.0.0 and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the protector.

10.1 Upgrading to ESA v7.2.1 to ESA v8.1.0.0

This section describes the steps to upgrade the ESA v7.2.1 to ESA v8.1.0.0.

10.1.1 Overview of the Upgrade from ESA v7.2.1 to ESA v8.1.0.0

The upgrading of your ESA involves completing the prerequisites, installing the patch, verifying the upgrade, configuring settings, and so on. During this process, it is important that data integrity is upheld and carried over to the upgraded version. This calls for a step-by-step approach to ensure a smooth transition of system to the latest version.

In this release, the *ReiserFS* file system is replaced by the *Ext4* file systems. The *ReiserFS* is amongst the oldest file system supported on Linux, however, there is no active support for it. Additionally, the *ReiserFS* can not handle multicore processors because of the restraint in its architecture. It can support only a few operations at a given point in time. Due to this, *ReiserFS* may or may not provide optimal support for the current features or operations.

This led to the change in file system to *Ext4*. The *Ext4* is a recent file system, and includes some major improvements over the existing *Ext3* file system.

The following are the advantages of using the *Ext4* file system:

- It is based on the *Ext3* file system, which is amongst the most stable file system available.
- Active support is available for *Ext4*.
- Supports features, such as, nanosecond timestamps, verifying journals using checksums, and so on.
- It is compatible with previous versions, such as, *Ext2* and *Ext3*.

Due to this change in the file system in v8.1.0.0, additional hardware with the *Ext4* file system is required to upgrade the appliances on v7.2.1 to v8.1.0.0.

The following sections provide a walk through of the procedures that you must follow to upgrade the ESA v7.2.1 to ESA v8.1.0.0.

10.1.1.1 Overview of upgrading ESA v7.2.1 to ESA v8.1.0.0

This section describes the steps for upgrading the ESAs. In this upgrade process, the ESAs in a cluster are upgraded one at a time. It involves removing ESA from the TAC, upgrading them, connecting to the audit store, and then re-building the TAC. The following figure illustrates a sample TAC environment on which the ESAs must be upgraded to v8.1.0.0.

Note:

Ensure that at least two ESAs are in a TAC.

Ensure that you do not make any changes to configuration, policy, or CoP during the upgrade process.

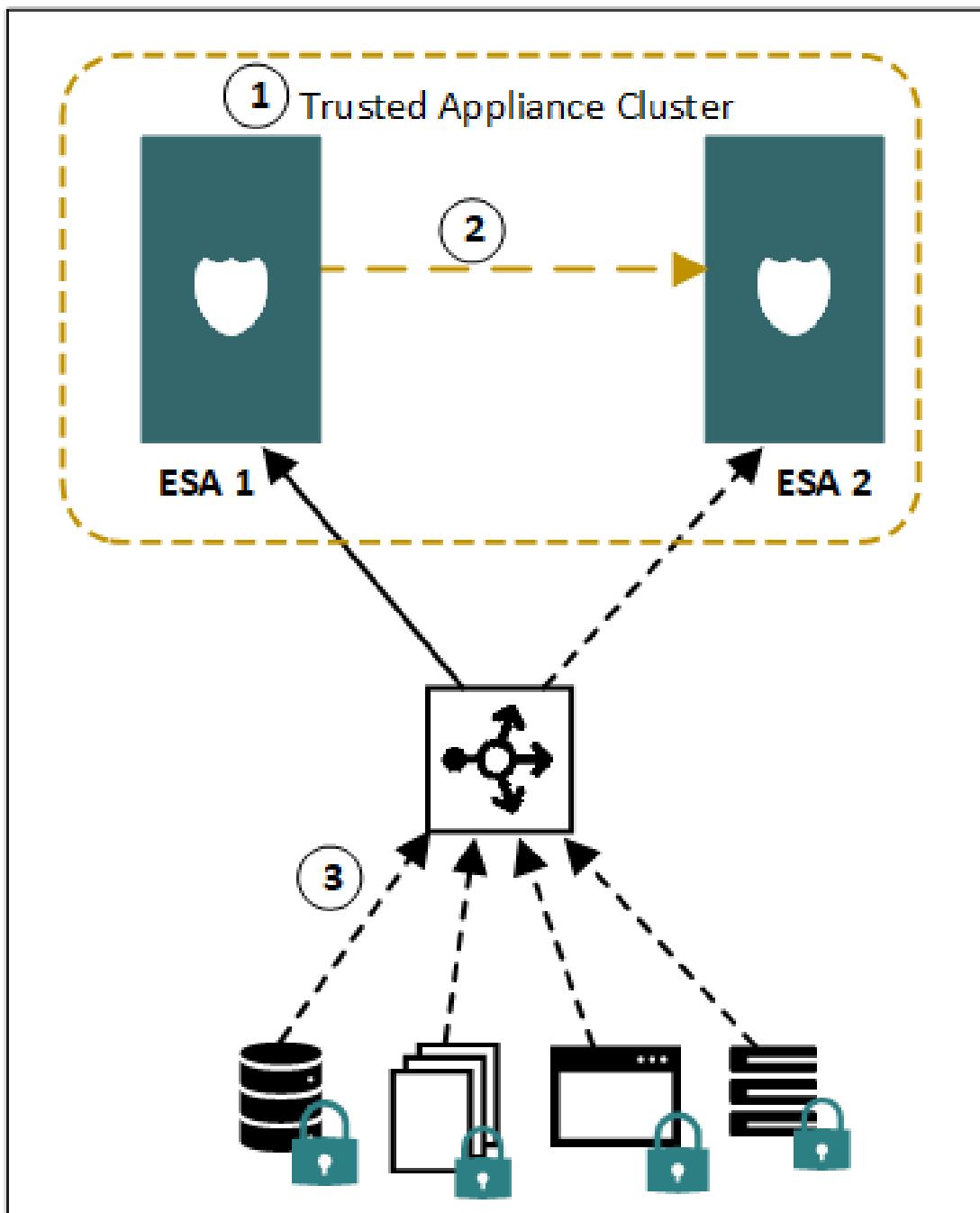


Figure 10-1: ESA v7.2.1 in a TAC

As shown in the setup,

1. The TAC contains a server node appliance ESA 1 and a client node appliance ESA 2
2. Data replication for policies, forensics, or DSG configuration operate from the ESA 1 to the ESA 2
3. Protectors communicate with the load balancer that balances the requests between the ESA 1 and the ESA 2

The following figure illustrates the TAC setup after the upgrade process is completed.

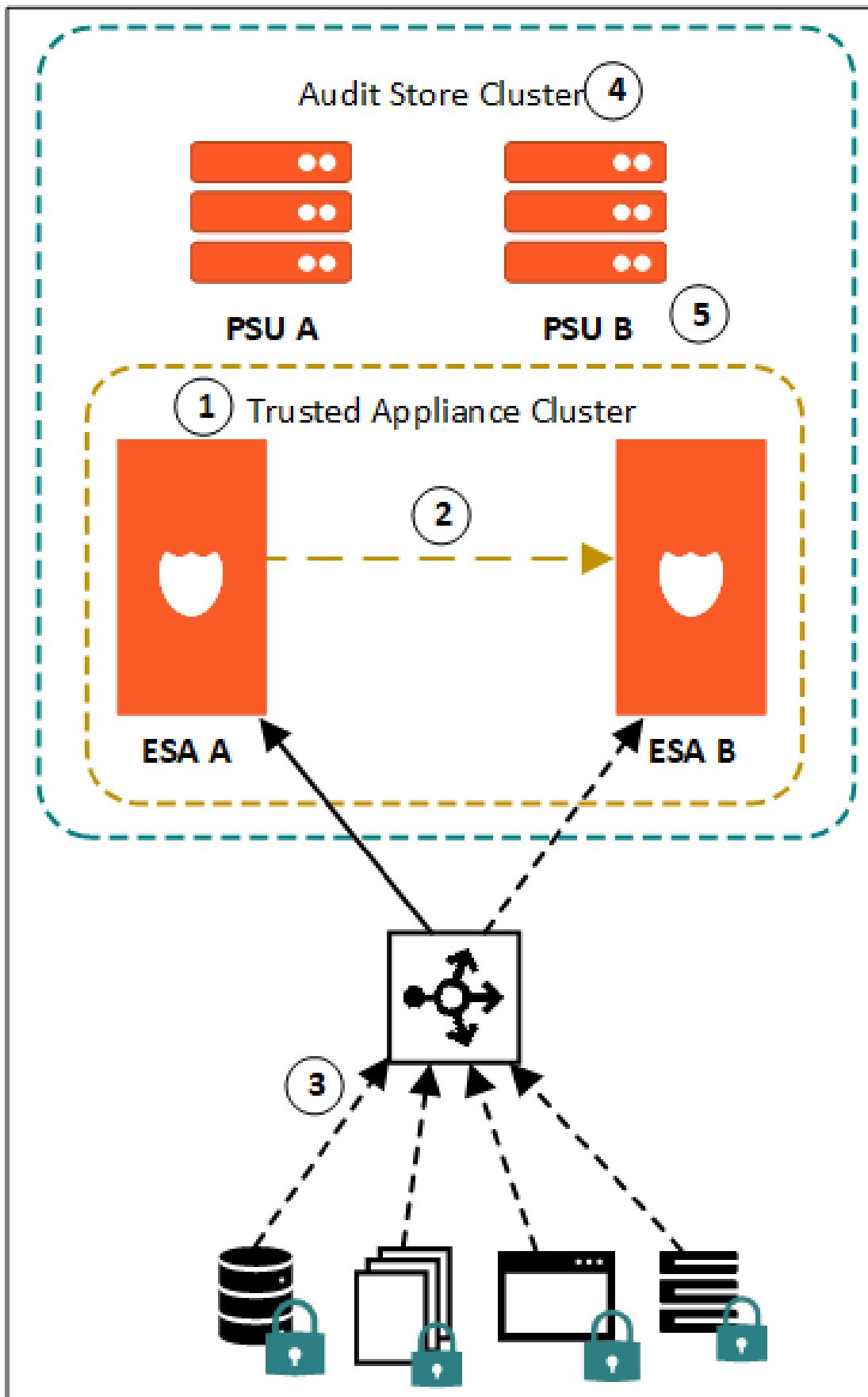


Figure 10-2: ESA v8.1.0.0 in a TAC

1. The TAC is established between the primary appliance ESA A and a stand-by appliance ESA B

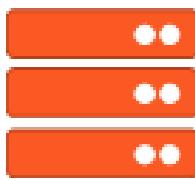
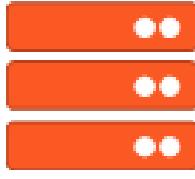
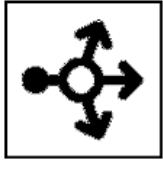
2. Data replication for policies, forensics, or DSG configuration operate from the ESA A to the ESA B
3. Protectors communicate with the load balancer that balances the requests between the upgraded ESA A and ESA B
4. Audit Store cluster is enabled for the ESAs
5. Protegility Storage Unit (PSU) is added as a part of the Audit Store Cluster

10.1.1.2 Upgrade Process: Flow Diagram

A diagrammatic representation of the upgrade process is provided in this section. The legend describes the elements used in the flow diagram.

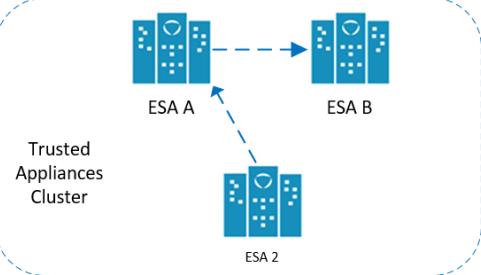
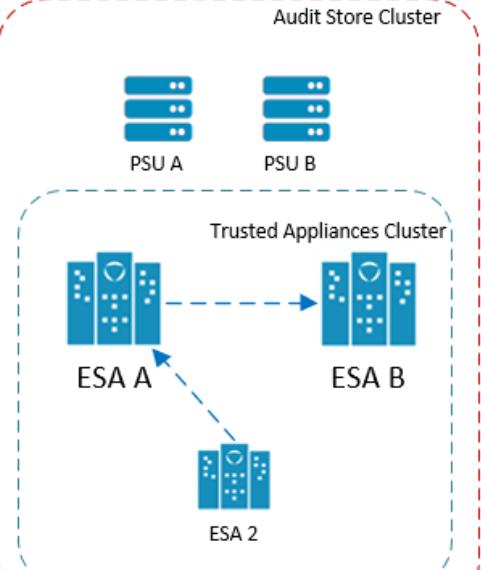
Legend

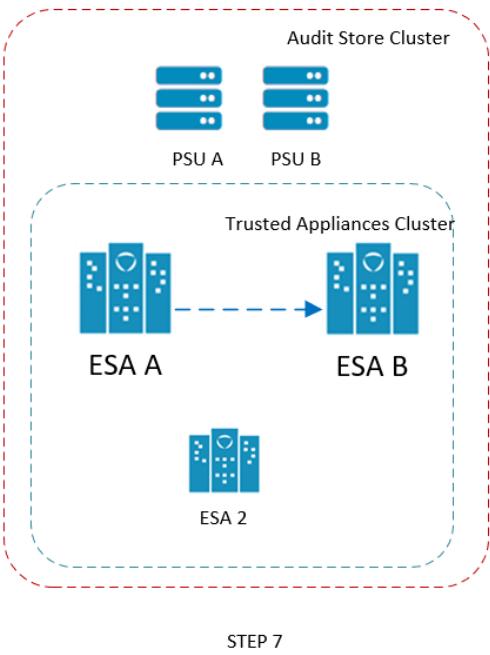
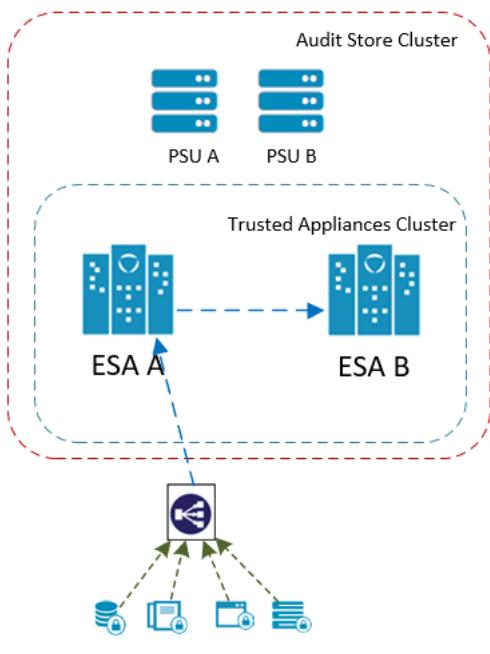
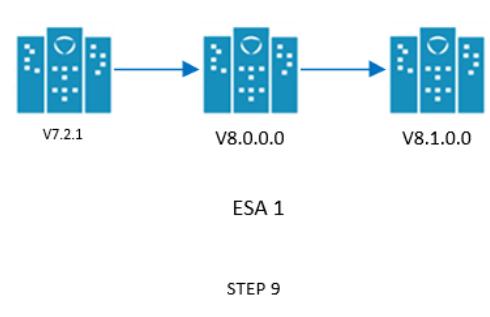
Icon	Description	Version	File System
 ESA 1	Server Node appliance	v7.2.1	Reiser FS
 ESA 2	Appliance Node	v7.2.1	Reiser FS
 ESA A	Server Node appliance	v8.1.0.0	Ext4 FS

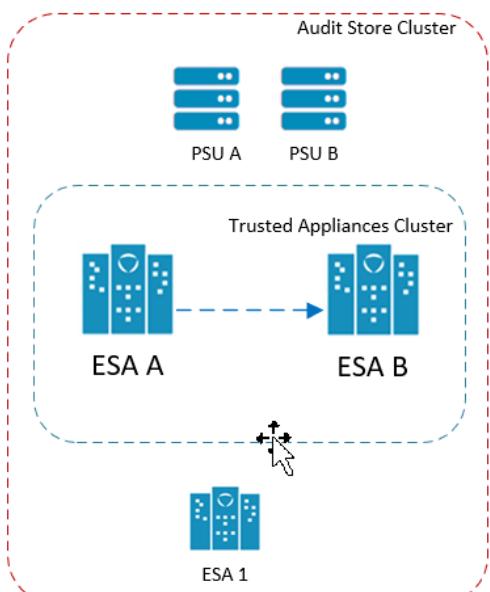
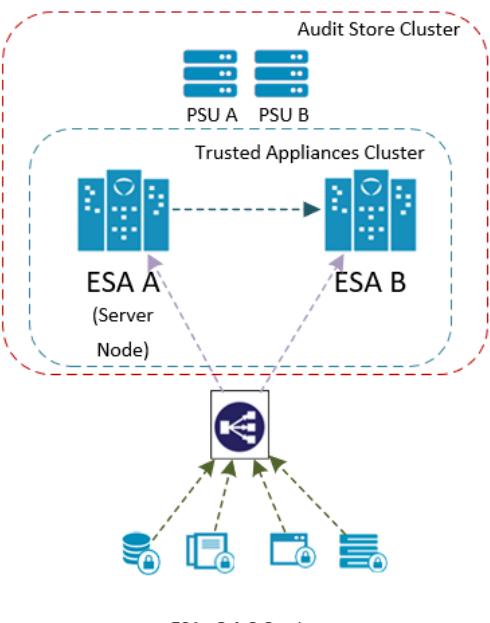
Icon	Description	Version	File System
 ESA B	Appliance Node	v8.1.0.0	Ext4 FS
 PSU A	Protegility Storage Unit (PSU)	v8.1.0.0	Ext4 FS
 PSU B	Protegility Storage Unit	v8.1.0.0	Ext4 FS
	Trusted Appliances Cluster	<ul style="list-style-type: none"> • v7.2.1 • v8.1.0.0 	N/A
	Audit Store Cluster	v8.1.0.0	N/A
	Protectors	<ul style="list-style-type: none"> • v7.2.1 • v8.1.0.0 	N/A
	Load Balancer	N/A	N/A

The following is a diagrammatic representation of the overview of the upgrade process from v7.2.1 to v8.1.0.0.

	<ul style="list-style-type: none"> • TAC contains a server node appliance ESA 1 and appliance ESA 2. • Data replication for policies or DSG configuration operate from ESA 1 to ESA 2. • Protectors communicate with the load balancer that routes the requests to ESA 1 or ESA 2. • Ensure that both ESA 1 and ESA 2 in the TAC are in sync and have the latest policies, configurations, DSG rulesets, and so on.
	<ul style="list-style-type: none"> • Disable the cluster scheduler tasks between ESA 1 and ESA 2. • Break the TAC. • All traffic is routed to ESA1.
	<ul style="list-style-type: none"> • Upgrade ESA2 to v8.0.0.0 <ul style="list-style-type: none"> • Apply the v8.0.0.0 patch • Complete the upgrade on v8.0.0.0 • Reboot to apply the kernel changes • Upgrade ESA2 to v8.1.0.0 <ul style="list-style-type: none"> • Apply the v8.1.0.0 patch • Complete the upgrade on v8.1.0.0 • Reboot to apply the kernel changes

 <p>STEP 4</p>	<ul style="list-style-type: none"> Spawn 2 brand new ESAs on v8.1.0.0. These will have the <i>ext4</i> file system by default.
 <p>STEP 5</p>	<ul style="list-style-type: none"> Join ESA 2, ESA A, and ESA B in a Trusted Appliances Cluster. Create a scheduler task to replicate policies, configuration etc. from ESA 2 to ESA A. Create a scheduler task to replicate policies, configurations from ESA A to ESA B. Ensure that all 3 ESAs are in sync.
 <p>STEP 6</p>	<ul style="list-style-type: none"> Spawn 2 new PSUs. Initialize Analytics on ESA2. Join ESA A, ESA B, PSU A, and PSU B to create an Audit Store Cluster of 5 nodes with ESA 2. Configure td-agent on ESA2, ESA A, and ESA B in Audit store cluster. Configure audit store roles on the ESA2, ESA A, and ESA B nodes. Migrate the DMS logs and metering logs using the migration scripts from ESA 2 to the PSUs. Wait till the migration is complete.

 <p>STEP 7</p>	<ul style="list-style-type: none"> • Delete the cluster scheduler task between ESA 2 and ESA A. • Remove ESA 2 from the Audit store cluster and the TAC. • Shut down ESA 2.
 <p>STEP 8</p>	<ul style="list-style-type: none"> • Redirect the traffic from ESA 1 to ESA A. • Upgrade DSG to v2.6.0
 <p>STEP 9</p>	<ul style="list-style-type: none"> • Upgrade ESA 1 to v8.0.0.0 <ul style="list-style-type: none"> • Apply the v8.0.0.0 patch • Complete the upgrade on v8.0.0.0 • Reboot to apply the kernel changes • Upgrade ESA 1 to v8.1.0.0 <ul style="list-style-type: none"> • Apply the v8.1.0.0 patch • Complete the upgrade on v8.1.0.0 • Reboot to apply the kernel changes

 <p>STEP 10</p>	<ul style="list-style-type: none"> • Add the ESA 1 to the Audit Store cluster with ESA A. • From ESA 1, migrate the Metering data and DMS logs to Protegility Analytics cluster • After the migration is successfully completed, remove ESA 1 from the Audit store cluster. • Shut down ESA 1.
 <p>ESAs v8.1.0.0 setup</p>	<ul style="list-style-type: none"> • Upgrade is complete to v8.1.0.0 with new file system.

10.1.1.3 Upgrade Process: Step-by-step procedure

To upgrade the ESA appliances from v7.2.1 to v8.1.0.0, you must first install the v8.0.0.0 patch on the v7.2.1 machine. After the 8.0.0.0 patch is successfully installed, you must then install the v8.1.0.0 patch. Complete the upgrade by verifying the installed patch and restarting the ESA appliance. After the 8.1.0.0 patch is successfully installed on the ESA, perform the required steps to complete the upgrade.

This section describes the procedure to upgrade the ESA v7.2.1 to v8.1.0.0.

Before you begin

- At least two ESAs must be in a TAC.
- The TAC must have at least one appliance as the *server* node.

For more information on the trusted appliance cluster, refer to the section *Trusted Appliances Cluster* in the [Appliances Overview Guide 8.1.0.0](#).

- From the v8.1.0.0, the file system is changed from the *ReiserFS* to the *Ext4* file system. Therefore, install two additional ESAs v8.1.0.0, that is, ESA A and ESA B.

For more information on installing the v8.1.0.0 on a new machine, refer to the section *Installing ESA on-premise* in the [Installation Guide 8.1.0.0](#).

- Install two PSUs, that is, PSU A and PSU B.

For more information on installing the PSU v8.1.0.0 on a new machine, refer to the [Protegility Storage Unit Guide 8.1.0.0](#).

- You must not make any changes to configuration, policy, or CoP on any appliance during the upgrade process.
- All the [prerequisites](#) are met before beginning the upgrade process.

For more information on the prerequisites, refer to the [Prerequisites](#).

► To upgrade to v8.1.0.0:

1. Ensure that the ESA 1 and ESA 2 in the TAC are in sync and have the latest policies and configurations.

2. Delete the cluster scheduler tasks between ESA 1 and ESA 2.

For more information about deleting a cluster task, refer to the section *Disabling Cluster Tasks* in the [Installation Guide 8.1.0.0](#).

3. Remove ESA 2 from the TAC.

Caution:

Before leaving the TAC, ensure that ESA 1 is the *server* node.

For more information about leaving a TAC, refer to section *Removing a Node from the Cluster using Web UI* in the [Appliances Overview Guide 8.1.0.0](#).

4. Perform the following steps on ESA 2.

- a. Upgrade to v8.0.0.0 by installing the v8.0.0.0 patch.

For more information about installing the v8.0.0.0 patch, refer to the section [Upgrading ESA from v7.2.1 to v8.0.0.0](#).

- b. Complete the upgrade on ESA 2.

For more information about the completing the upgrade, refer to the section [Completing the Upgrade](#).

- c. Upgrade to v8.1.0.0 by installing the v8.1.0.0 patch.

For more information about installing the v8.1.0.0 patch, refer to the section [Upgrading ESA from v8.0.0.0 to v8.1.0.0](#).

- d. Complete.

For more information about completing the upgrade, refer to the section [Completing the Upgrade](#).

- e. Create a TAC between ESA 2, ESA A, and ESA B.



For more information on creating a TAC, refer to the section *Trusted Appliances Cluster (TAC)* in the [Appliances Overview Guide 8.1.0.0](#).

Note:

Ensure that you add one appliance at a time.

- f. If you have the DSG installed, then apply the DSG 2.6.0.0 patch.

Important: This step applies if you are upgrading an ESA with the DSG component installed.

For more information about applying the DSG patch, refer to the section [Applying a DSG Patch](#).

- g. Create a scheduler task to replicate policies, configuration, DSG rulesets, and so on, from ESA 2 to ESA A.
- h. Create another scheduler task to replicate policies, configuration, DSG rulesets, and so on, from ESA A to ESA B.

For more information about creating a cluster task, refer to the section *Scheduling Configuration Export to Cluster Tasks* in the [Appliances Overview Guide 8.1.0.0](#).

- i. If you have any custom files to be replicated from ESA 2 to ESA A and ESA B, then it must be listed in the *customer.custom* file.

For more information about exporting custom files, refer to the section *Exporting Custom Files* in the [Appliances Overview Guide 8.1.0.0](#).

- j. Initialize Analytics on the ESA 2 to create an Audit Store cluster.

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

- k. Join ESA A, ESA B, PSU A and PSU B to the Audit Store cluster with ESA 2.

Note:

Ensure that you add one appliance at a time.

- l. Configure the td-agent on ESA 2, ESA A, and ESA B in the Audit Store cluster.

For more information about configuring the td-agent, refer to the section [Configuring td-agent in the Audit Store Cluster](#).

- m. Configure the Audit Store roles on the ESA2, ESA A, and ESA B nodes..

For more information about configuring the Audit Store cluster roles, refer to the section [Refreshing the Audit Store Cluster](#).

- n. Verify the Audit Store cluster..

For more information about verifying the Audit Store cluster, refer to the section [Verifying the Audit Store Cluster](#).

- o. From ESA 2, migrate the Metering data to Audit Store cluster..

For more information about migrating the metering data, refer to the section [Metering Data](#).

- p. From ESA 2, migrate the DMS logs to Audit Store cluster.

For more information about migrating the DMS logs to the Audit Store Cluster, refer to the section [Migrating Logs](#).

Note:

Before performing the upgrade, if the DMS logs were replicated between ESA 1 and ESA 2, then it is not recommended to perform this step.

Important:

Ensure that the logs or the data migration is completed before proceeding to the next step.

- q. Complete the post upgrade steps..

For more information about completing the post upgrade steps, refer to the section [Post Upgrade Steps](#).

- r. Delete the cluster scheduler task created in *step g*.

5. After the migration is completed, remove ESA 2 from the Audit store cluster and the TAC.

For more information about leaving an audit store cluster, refer to the [Protegility Storage Unit Guide 8.1.0.0](#).

For more information about leaving a TAC, refer to the section [5.12 Removing a Node from the Cluster using Web UI](#) in the [Appliances Overview Guide 8.1.0.0](#).

6. Shut down ESA 2.

7. Redirect the traffic from ESA 1 to ESA A.

8. Perform the following steps on ESA 1.

- a. Upgrade the ESA1 to v8.0.0.0 by installing the v8.0.0.0 patch.

For more information about installing the v8.0.0.0 patch, refer to the section [Upgrading ESA from v7.2.1 to v8.0.0.0](#).

- b. Complete the upgrade on ESA 1.

For more information about completing the upgrade, refer to the section [Completing the Upgrade](#).

- c. Upgrade to v8.1.0.0 by installing the v8.1.0.0 patch.

For more information about installing the v8.1.0.0 patch, refer to the section [Upgrading ESA from v8.0.0.0 to v8.1.0.0](#).

- d. Complete the upgrade on ESA 1.

For more information about completing the upgrade, refer to the section [Completing the Upgrade](#).

- e. Add the ESA 1 to the Audit Store cluster with ESA A.

For more information joining the ESA to the Audit Store cluster, refer to the section [Adding an ESA to the Audit Store Cluster](#).

- f. From ESA 1, migrate the Metering data to Audit Store cluster.

For more information about migrating data to Audit Store cluster, refer to the section [Metering Data](#).

- g. From ESA 1, migrate the DMS logs to Audit Store cluster.

For more information about migrating the DMS logs to the Audit Store cluster, refer to the section [Migrating Logs](#).

Important:

Ensure that the data migration is completed before proceeding to the next step.

- h. Complete the post upgrade steps.

For more information about completing the post upgrade steps, refer to the section [Post Upgrade Steps](#).

9. After the migration is successfully completed, remove ESA 1 from the Audit store cluster.

For more information about leaving an audit store cluster, refer to the [Protegility Storage Unit Guide 8.1.0.0](#).

10. Shut down ESA 1.

10.1.2 Prerequisites

The prerequisites for upgrading the ESA to v8.1.0.0 must be preformed on the following components:

- Accounts
- Backup and Restore
- Installations and Hardware Requirements
- High Availability (HA)
- Trusted Appliance Cluster (TAC)
- Keys
- Customized files (Configuration files, Certificates)
- Logging, Reporting, and Certificates
- HSM

10.1.2.1 Accounts

The administrative account used for upgrading the ESA must be active.

For more information about Accounts and Password Management, refer to the [Appliance Overview Guide 8.1.0.0](#).

10.1.2.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

Note:

After upgrading to 8.0.0.0, if you take the backup of the ESA v8.0.0.0, then it will overwrite the backup of the ESA v7.2.1. Therefore, ensure that you take the backup of the ESA v7.2.1. Ensure that the backup is available on a different server.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section [3.4.4 Working with Backup and Restore](#) in the [Appliances Overview Guide 8.1.0.0](#).

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a back up of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* and perform the export operation.

10.1.2.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

10.1.2.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

10.1.2.2.3 Creating a snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before upgrading to v8.1.0.0.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating snapshots for respective cloud platforms, refer to the [Appliance Overview Guide 8.1.0.0](#).

10.1.2.3 Installations and Hardware Requirements

Installation Requirements

- The *ESA_PAP-ALL-64_x86-64_8.0.0.0.x.UP-1.pty* patch file is available.
- The *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-1.pty* patch file is available.
- The minimum space available in the */opt* directory should be more than twice the size of the patch files.

Note:

Ensure that you download the latest patch from the [My.Protegrity](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

You must provide at least the following additional hardware for the upgrade:

- 2 ESAs
- 2 Protegrity Storage Units (PSUs)

For more information about the detailed hardware requirements, refer to the section [System Hardware Requirements](#).

10.1.2.4 High Availability (HA)

If you are upgrading an ESA appliance that is in an HA setup, then you must remove the HA services from the ESA appliance and then apply the upgrade patch.

For more information about removing the HA services, refer to the [Scalability and Availability Guide 7.2.1](#).

Note:

The HA services are not supported from version 8.0.0.0. If you continue using the HA services, then it might break the functionality of the system.

For more information about the alternate to HA services, refer to the [Fault Tolerance Guide 8.0.0.0](#) on the [My.Protegility](#) portal.

10.1.2.5 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section *Working with Keys* in the [Protegility Key Management Guide 9.1.0.0](#).

10.1.2.6 Creating a Metering Backup File

Ensure that you create a backup file of the metering logs before performing the upgrade on the ESA v7.2.1.

► To create a backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility`/directory using the following command.
`cd /opt/protegility`
4. Create a temporary directory to save the metering logs using the following command.
`mkdir <directory_name>`

Note: Ensure that the temporary directory is accessible on the ESA v7.2.1. This directory must not be copied or moved to another location.

5. Add permissions to the temporary directory using the following command.
`chmod 755 <directory_name>`
6. Change the owner of the temporary directory to *service admin* using the following command.
`chown service_admin.service_admin <directory_name>`
7. Navigate to the temporary directory using the following command.
`cd <directory_name>`
8. Create the backup file of the metering logs using the following command.
`/opt/protegility/repository/pim/pgsql/bin/pg_dump -h localhost -U admin -p 5211 --schema metering --format=c ADMINDB > /opt/protegility/<directory_name>/<backup_filename>.bak`

10.1.2.7 Customized files (Configuration files, Certificates)

The *exclude* file present in the */opt/ExportImport/filelist* directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section *Exporting Custom Files* in the [Appliance Overview Guide 8.1.0.0](#).

10.1.2.8 Logging, Reporting, and Certificates

If you are upgrading an ESA appliance that has scheduled tasks or cluster replication tasks created by the user, then ensure that DMS options, such as, *Log-Server Repository*, *Log-Server Configuration*, and *Log-Server Event Configuration*, reporting tasks, and certificates are disabled.

Note:

If a scheduled task has scheduled tasks or cluster replication tasks created by the user, such as, the *Logging*, *Reporting*, and *Certificates* components, then uncheck them and update the scheduled task.

If there are preconfigured scheduling tasks, such as, *100 DBIntegrity Logging-Repository Integrity Check (Once a week)*, then they are automatically disabled.

A notification will be displayed on the ESA Web UI dashboard.

The following scheduled tasks were disabled due to Log Server migration: [100]

Note:

The DMS, reporting server, and DMS2mail services are not supported from version 8.0.0.0 onwards.

10.1.2.9 HSM

If you are working with HSM vendor apart from Safenet HSM, Futurex HSM, or Utimaco HSM and are planning to continue working with this HSM solution post upgrade, then you must switch to the soft HSM prior to upgrading the ESA version 7.2.1 to version 8.1.0.0. Post upgrade, you must switch from the soft HSM to the HSM to continue using the HSM solution.

For more information about switching from the soft HSM to the required external HSM, refer to the section *Switching from the external HSM to the Soft HSM* in the [Key Management Guide 8.1.0.0](#).

10.1.3 Upgrading ESA from v8.0.0.0 to v8.1.0.0

This section describes the steps to upgrade from the ESA v8.0.0.0 to ESA v8.1.0.0.



► To install the ESA v8.1.0.0 patch:

1. Login to the ESA Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-1.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

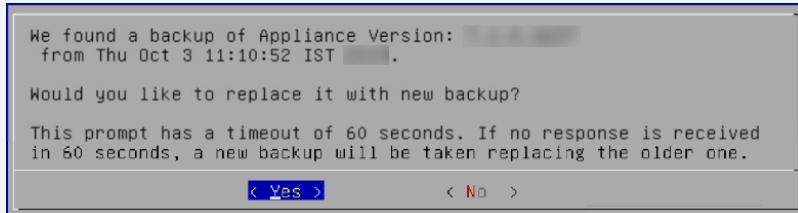
The file upload is initiated.

Note:

Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the ESA CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the root password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-1.pty* patch file and select **Install**.

Note: If a backup operation is performed before upgrading to the ESA v8.0.0.0, then the following message to replace the existing backup appears.



You can select **Yes** to overwrite the existing backup. Alternatively, you can select **No** to retain the existing backup and continue the upgrade operation.

If no existing backup is available in the system, then it will initiate the back up process automatically.

It is recommended to select **No** during this step. If you take the backup of the ESA v8.0.0.0, then it will overwrite the backup of the ESA v7.2.1.

For more information about backup and restore, refer to the section [Exporting Data or Configuration to Remote Appliance](#).

The backup is initiated.

- After the backup is completed, the upgrade process begins. During upgrade for the ESA on-premise, a screen to update the TLS version appears. On the ESA, TLSv1.3 is updated in v8.1.0.0. The SSL Protocol is updated from *TLSv1.2* to *ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1* in the earlier versions of the appliances.

The following screen appears.

To enhance the security of the product, the support to
TLS version 1.3 is added.
The cipher suite is updated to provide additional
ciphers to strengthen the security.

< **OK** >

Note:

The timeout of this screen is 60 seconds.

Note:

This screen is not displayed while performing the upgrade on the cloud instances.

- Select **OK**.
- Select **Exit** on the following screen.

Patch has been installed successfully !!

< **Exit** > <Show More>

The patch is installed and ESA is upgraded to ESA v8.1.0.0.

10.1.4 Completing the Upgrade

After installing the patch, you must verify the patch installation, check the upgrade logs, add AppArmor profiles, configure certificates, and install the PSU to complete the upgrade. The following sections describe the steps to complete the upgrade.

10.1.4.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

- `/var/log`
 - Installation.log* - Provides the logs for all the installed components.

- *syslog* - Provides collective information about the syslogs.
2. */etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log*

10.1.4.2 Verifying the Patch Installation

After upgrading to the ESA v8.0.0.0, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_8.0.0.0* patch name appears.

5. Login to the ESA Web UI.
6. Navigate to the **System > Information page**.

The ESA is updated to v8.0.0.0 in the **Installed Patches** section.

Ensure to check the Logs to verify that there are no errors.

10.1.4.3 Adding AppArmor Profiles

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

In ESA v8.0.0.0, the AppArmor is enabled as part of the ESA installation to protect the different appliance capabilities, such as, antivirus, trusted appliances cluster, firewall, NTP services, web services, and two factor authentication. Thus, after installing ESA, you must add permissions to the *usr.sbin.apache2* profile for enabling features, such as Proxy Authentication, Import/Export, and Cluster operation to function without AppArmor restricting them.

Complete the following steps to add permissions to the profile.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the */etc/apparmor.d/custom* directory.
4. Edit the *usr.sbin.apache2* profile.
5. Insert the following lines.

```
/opt/ldap/** rix,  
/usr/lib/sftp-server ix,  
/lib/bridge-utils/ifupdown.sh rix,  
/usr/lib/rabbitmq/lib/rabbitmq_server-0.0.0/sbin/rabbitmq-server rix,  
/lib/bridge-utils/ifupdown.sh rix,  
/lib/bridge-utils/ifupdown.sh rix,  
/usr/sbin/sshd Ux,
```

6. Edit the *etc.opt.Cluster.cluster_helper* profile.



7. Insert the following lines.

```
/usr/local/sbin/tcping rix,  
/usr/local/sbin/Log rix,  
/usr/bin/sudo rix,  
/usr/local/lib/python2.7/dist-packages/** rw,
```

8. Restart the AppArmor service using the following command.

```
/etc/init.d/apparmor restart
```

The permissions are applied to the profile and you can run the features without AppArmor denial logs.

For more information about AppArmor, refer to the [Appliances Overview Guide 8.0.0.0](#).

10.1.4.4 Restoring the Backup File of the Metering Logs

A backup of the metering logs is required on the ESA Pre-v9.0.0.0 in the `/opt/protegility/` directory during the upgrade. This file is required for the migration of the metering logs.

Note: If the backup file of the metering logs is available in the directory, then skip this section.

For more information about the creating the backup file of the metering logs, refer to the section [Creating a Metering Backup File](#).

► To restore the backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility/` directory using the following command.
`cd /opt/protegility/`
4. Restore the backup file of the metering logs using the following command.
`cp <backup_filename>.bak /opt/protegility/hubcontroller/`

10.1.4.5 Restarting the System

After the ESA patch, `ESA_PAP-ALL-64_x86-64_8.0.0.0.x.UP-1.pty` is installed successfully, restart the ESA machine. This ensures the configuration files of the Linux Kernel are upgraded.

10.1.4.6 Custom Certificates

If you are upgrading from an earlier version to ESA 8.0.0.0 and use custom certificates, then run the following step after the upgrade is complete and custom certificates are applied for td-agent, Audit Store, and Analytics, if installed.

After the upgrade is complete, the *Audit Store Repository* service will be in the stopped state till the security is set up. Additionally, errors might be displayed in the logs related to the certificates. Complete the following steps to configure the custom certificates.

1. From the ESA Web UI, navigate to **System > Services > Audit Store**.
2. Ensure that the **Audit Store Repository** service is not running. If the service is running, then stop the service.

3. Configure the custom certificates and upload it to the Certificate Repository.

Note:

For more information about configuring custom certificates, refer to the section *Using Custom Certificates in the Audit Store* in the [Certificate Management Guide 8.0.0.0](#).

4. Set the custom certificates for the PLUG components as *Active*.

Note:

For more information about marking certificates as active, refer to the section *To change certificates* in the [Certificate Management Guide 8.0.0.0](#).

5. From the ESA Web UI, navigate to **System > Services > Audit Store**.
6. Start the **Audit Store Repository** service.
7. Open the ESA CLI.
8. Navigate to **Tools**.
9. Run **Apply Audit Store Security Configs**.

10.1.4.7 Installing the Protegility Storage Unit

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

The Protegility Storage Unit consists of the *td-agent* and the Audit Store installed on the Appliance. It is a hardened appliance that is used to scale the Audit Store cluster with the enhanced security of a Protegility appliance. After installing the ESA, you can add additional Protegility Storage Units to the setup.

The Audit Store cluster requires a minimum of 3 nodes in the Audit Store Cluster. If you require more nodes, then add Protegility Storage Units as nodes to the Audit Store cluster.

As a basic requirement, you must install 2 PSUs to create the Audit Store Cluster.

For more information about installing the Protegility Storage Unit, refer to the section *Installing the Protegility Storage Unit* in the [Protegility Storage Unit Guide 8.0.0.0](#).

10.1.5 Configuring the Logging Database

The logs are stored in a database. From the database, the logs can be used by Analytics to monitor the system. Additionally, the logs in the database can also be used for forensics and for locating any breach or issues in the system. The ESA stores the logs in the Audit Store and the Protegility Storage Unit. Additionally, you can use your own Security Information and Event Management (SIEM) for capturing and storing logs.

Note: For more information about upgrading the appliance from v9.0.0.0 to v9.1.0.0, refer to the [Protegility Upgrade Guide 9.1.0.5](#).

10.1.5.1 Installing the Protegility Storage Unit

The Protegility Storage Unit consists of the *td-agent* and the Audit Store installed on the Appliance. It is a hardened appliance that is used to scale the Audit Store cluster with the logging capability of a Protegility appliance. After installing the ESA, you can add additional Protegility Storage Units to the setup.

As a basic requirement of the Audit Store Cluster, you must have at least 2 ESAs and 2 PSUs installed.

For more information about installing the Protegility Storage Unit, refer to the section *Installing the Protegility Storage Unit* in the [Protegility Storage Unit Guide 9.0.0.0](#).

10.1.5.1.1 Audit Store Clustering using the Protegility Storage Unit

Clustering is a powerful way to increase the capability of your system. You can add nodes to expand the cluster. Expanding the cluster using the Protegility Storage Unit provides an advantage by increasing the storage space available.

A basic setup is shown in the following figure.

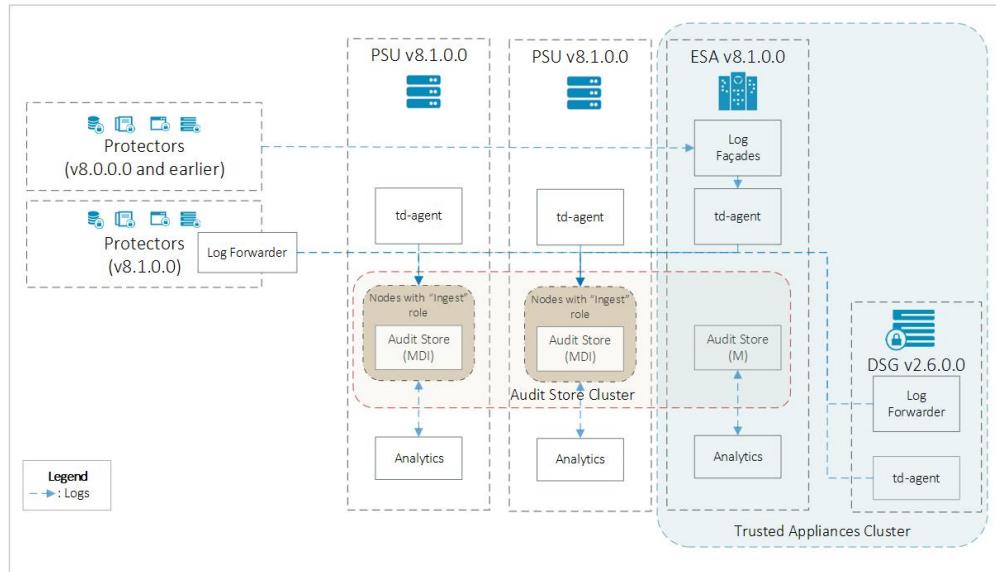


Figure 10-3: Basic Audit Store Cluster

In the figure, the arrows show the log flow direction. The basic setup consists of three systems. Here the systems consist of 1 ESA and 2 Protegility Storage Unit. The Protegility Storage Unit forms a part of the Audit Store cluster where the Audit Stores on all the nodes are linked together to form the storage unit. The logs received by the ESA are stored in the Audit Store cluster, the data would be stored on the local node or any node that is a part of the Audit Store cluster with the *ingest* role.

The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

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

The basic setup when Trusted Appliance Cluster (TAC) is implemented consists of 2 ESAs and 2 Protegility Storage Units as shown in the following figure.

Note: The Audit Store cluster is different from the TAC in the ESA. A TAC is used for grouping and managing multiple ESAs together. In the Audit Store cluster, the Audit Store nodes are grouped together to form the storage unit. The Audit Stores in the Audit Store cluster might be a part of the ESA or the Protegility Storage Unit. The Protegility Storage Unit may or may not be a part of the TAC.

For more information about the TAC, refer to the section *Trusted Appliances Cluster (TAC)* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

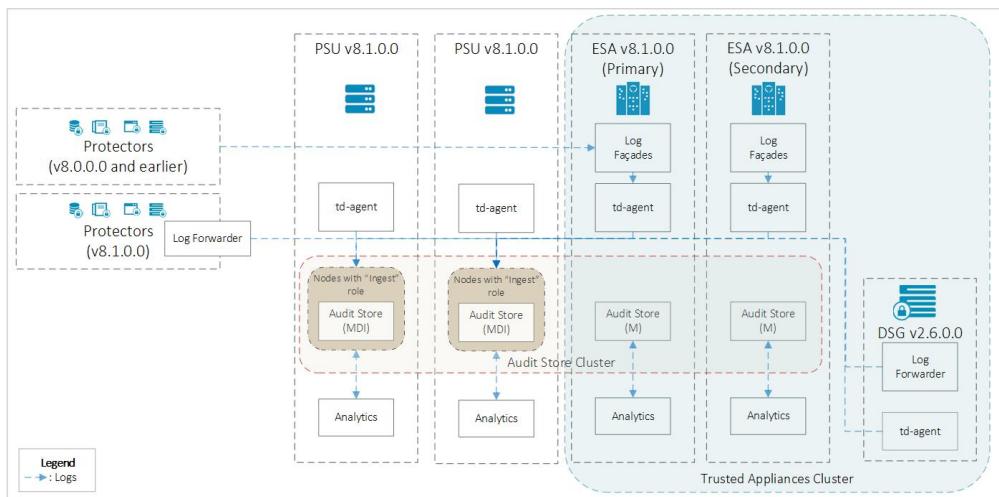


Figure 10-4: Basic Audit Store Cluster in TAC

The Audit Store cluster is flexible and nodes can be added and removed from the Audit Store cluster based on your requirements. Thus, multiple nodes can be added to the Audit Store cluster as shown in the following figure.

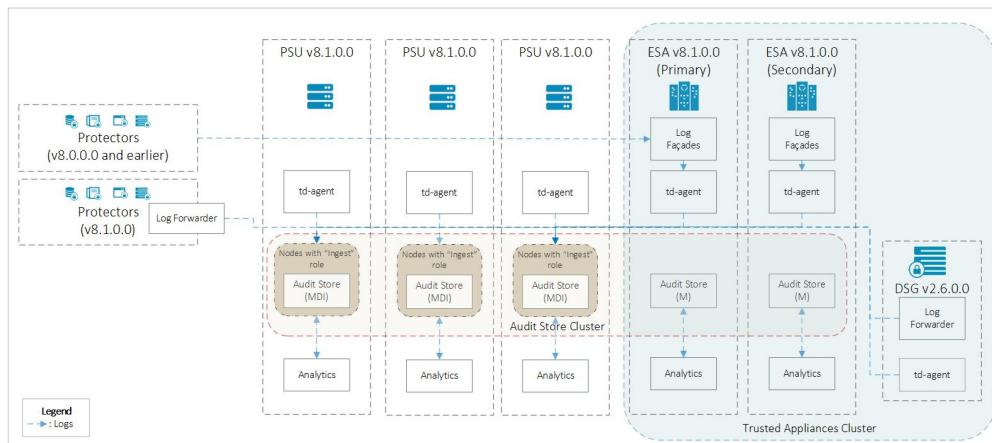


Figure 10-5: Multi-Node Cluster

Note: The ESA must have the *master-eligible* role and the PSUs must have all the three roles, the *master-eligible*, *data*, and *ingest* roles.

If any node is not required, then the node can be removed from the Audit Store cluster. When the node is removed from a cluster, the indexes and internal configurations, such as, the td-agent and Analytics settings are reset. In this case, the Protegility Storage Unit remains uninitialized and needs to be added to another Audit Store cluster before it can be used again.

10.1.5.1.1 Completing the Prerequisites

Ensure that the following prerequisites are met before configuring the Audit Store Cluster. Protegility recommends that the Audit Store Cluster has a minimum of 1 ESA and 2 PSUs or 2 ESAs and 1 PSU for creating a highly-available multi-node Audit Store cluster.

1. Install and set up the first ESA. This will be the Primary ESA if you set up a TAC.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

2. If you require TAC, then install and set up the second ESA. This will be the Secondary ESA in a TAC. Skip this step if TAC is not required.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

3. Install and set up the first PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

4. Install and set up the second PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

10.1.5.1.1.2 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, Protegility Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as, *td-agent*, is started and Protegility 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.

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

The following screen appears.

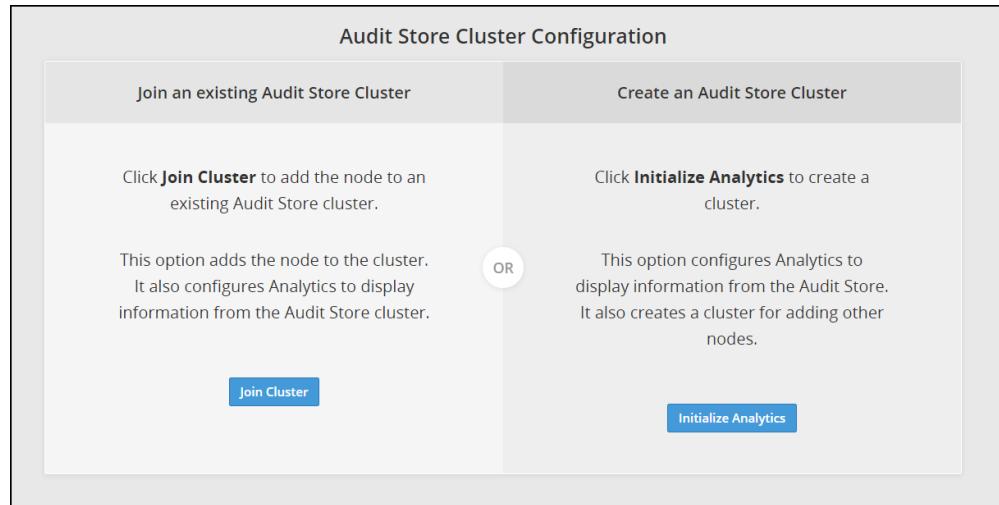


Figure 10-6: Analytics Screen

4. Click **Initialize Analytics**.

Protegility 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.

Protegility 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.

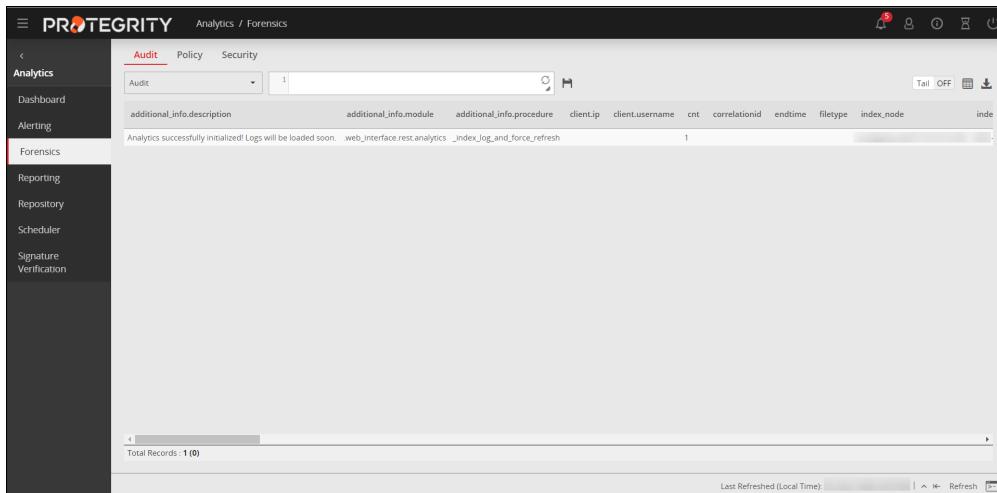


Figure 10-7: Forensics

10.1.5.1.1.3 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 [Protegility 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.

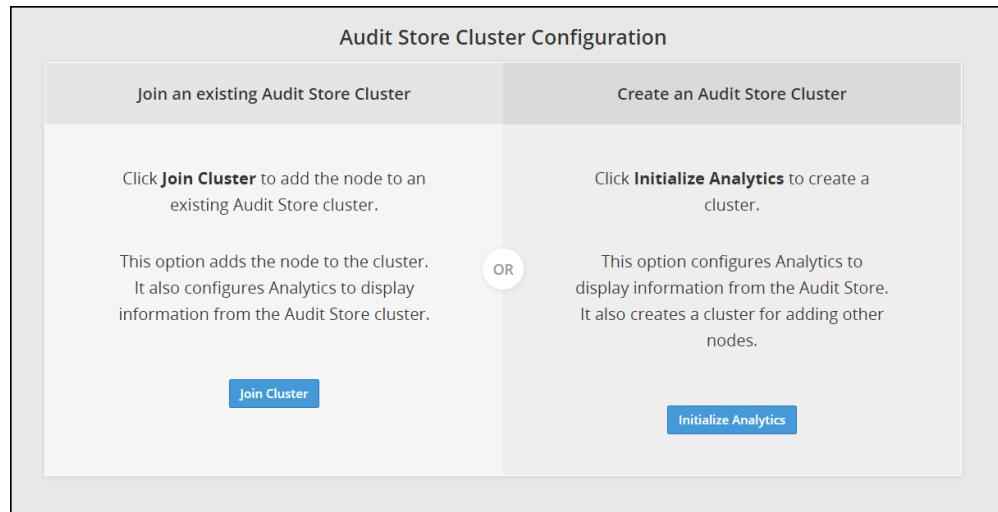


Figure 10-8: Analytics Screen

4. Click **Join Cluster**.

The following screen appears.

The screenshot shows the 'Join an existing Audit Store Cluster' dialog box. It contains fields for 'Node IP/Hostname', 'Username', and 'Password'. There is also a checkbox for clearing cluster data and a 'Join Cluster' button.

Join an existing Audit Store Cluster	
Target node IP/Hostname*	
<input type="text" value="Node IP/Hostname"/>	
Username*	
<input type="text" value="Username"/>	
Password*	
<input type="password" value="Password"/>	
<input type="checkbox"/> 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 10-9: Joining an Audit Store Cluster

5. 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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](#).

6. 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.

7. 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.

Protegility 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.

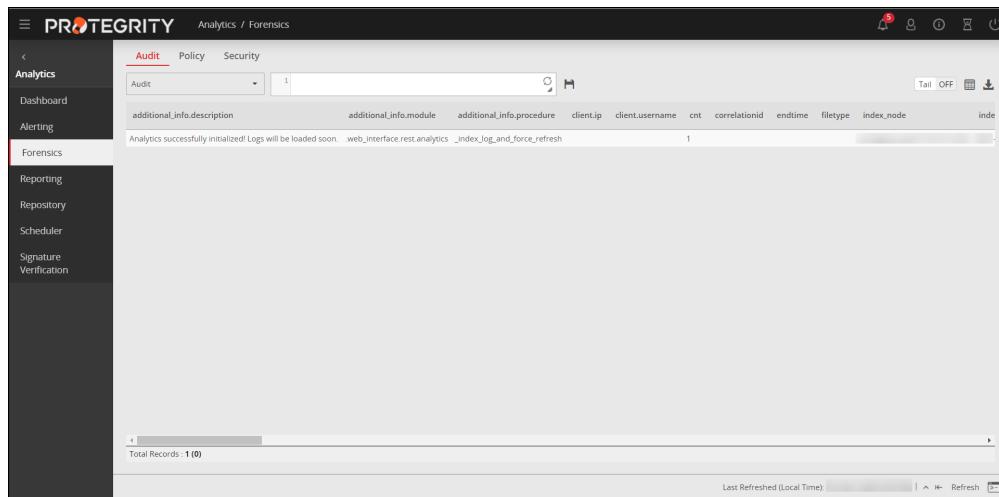


Figure 10-10: Protegility Analytics

10.1.5.1.1.4 Adding the Protegility Storage Unit to the Audit Store Cluster

Add the Protegility Storage Unit to the Audit Store Cluster that is initialized on the ESA. You need to specify the IP address of the Audit Store cluster that you want to join with the username and password of the admin user for authorization.

Before you begin

Ensure that the Audit Store services are running on the ESA Web UI by navigating to **System > Services > Audit Store**.

Note: 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 PSU Web UI would make the cluster information inconsistent, make the Audit Store cluster unstable, and would lead to errors.

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 [Protegility Appliances Overview Guide 9.1.0.5](#).

► To join the Audit Store cluster:

1. Log in to the Web UI of the Protegility Storage Unit.
2. Open the **Audit Store Management** screen.

The **Cluster Overview** screen appears.

The screenshot shows the 'Cluster Overview' screen with the following data:

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
190,528	1	1

Below the tables, there are two tabs: **Nodes** (selected) and **Indices**. Under the **Nodes** tab, there is a table titled 'Details' showing node configuration:

Node IP	Roles			Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
	Master	Data	Ingest						
192.168.1.100	✓	✓	✓	Node 1	8.8h	39,502,524,416	7,033,622,528	32,468,901,888	16.6

Figure 10-11: Cluster Overview Screen

3. Click **Join Cluster**.

The **Join Cluster** screen appears.

Note: The **Join Cluster** button is disabled if a node is already a part of the Audit Store cluster.

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**

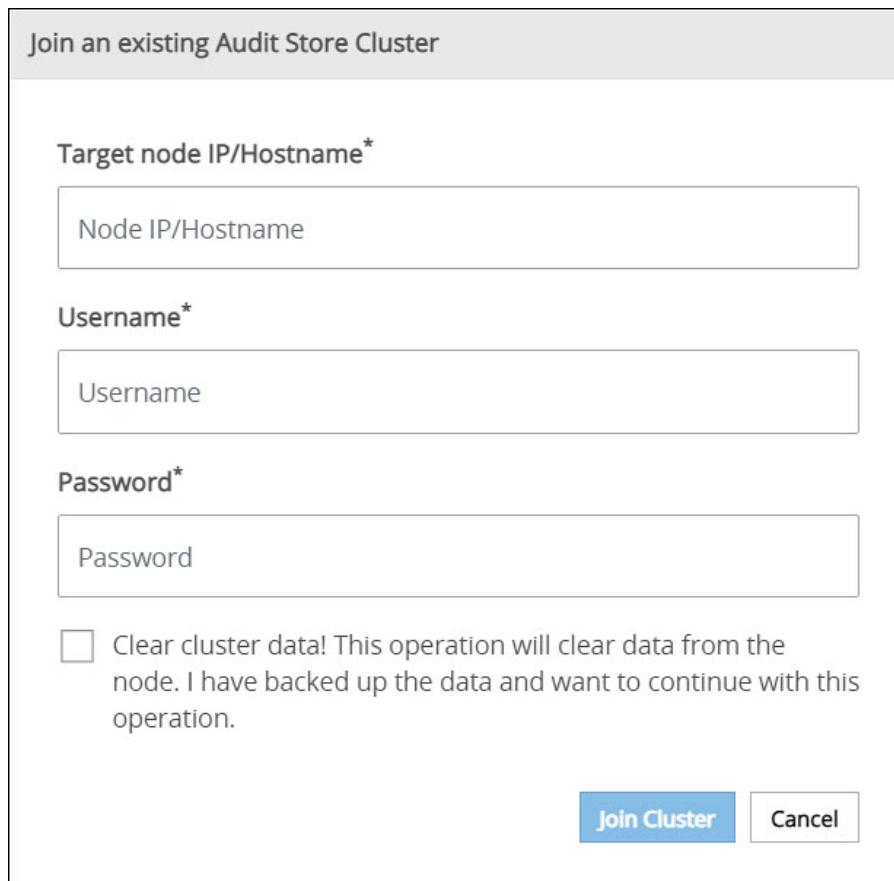


Figure 10-12: Join Cluster Dialog Box

4. Specify the following details for the node that you want to connect.

- **Target node IP/Hostname:** This is the IP address or hostname of the node that you want to connect to.

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

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

For more information about creating an Audit Store cluster, refer to the section *Creating a Local Cluster* in the [Protegility Analytics Guide 9.1.0.5](#).

- **Username:** This is the administrator user name to connect to the target machine. For example, admin.
- **Password:** This is the password for the user.

5. Click **Join Cluster**.

Note: The **Join Cluster** button in this dialog box is enabled after you specify the required information in all the fields and select the check box.

The Audit Store data on the node is cleared . The node is then added to the Audit Store cluster. The Cluster Overview screen appears with the updated Audit Store cluster information. The **Join Cluster** button is disabled and the **Leave Cluster** button is now enabled.

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
2	2	17	34	0

Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count
0	0	1.3.0	[redacted]	14

Total Docs	Number of Master Nodes	Number of Ingest Nodes
192,494	2	2

Nodes		Indices		Details							
Node IP		Master	Data	Ingest	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
[redacted]	[redacted]	✓	✓	✓	Edit Roles	[redacted]	9h	39,502,524,416	7,035,338,752	32,467,185,664	16,6
[redacted]	[redacted]	✓	✓	✓	Edit Roles	[redacted]	3.4m	39,502,524,416	7,001,763,840	32,500,760,576	16,6

Figure 10-13: Node Added to Cluster

Repeat the steps provided in this section to add the remaining Protegility Storage Units you installed to the Audit Store Cluster.

10.1.5.1.1.5 Refreshing the Audit Store Cluster

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

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

10.1.5.1.1.6 Configuring td-agent in the Audit Store Cluster

Complete the following steps after adding the Protegility Storage Unit to the Audit Store cluster. This configuration is required for processing and storing the logs received by the Audit Store.

Note: This step must be performed on all the ESAs in the Audit Store cluster.

Before performing the steps provided here, verify that the Audit Store cluster health status is green on the **Audit Store Management** screen of the ESA Web UI.

1. Login to the CLI Manager of the *ESA* node.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
3. Enter the root password and select **OK**.
4. Enter the username and password for the administrative user, such as, admin.
5. Select **OK**.
6. In the *Setting ESA Communication* screen, select **OK**.
7. Specify the IP addresses of all the Protegility Storage Unit machines in the cluster, separated by commas.

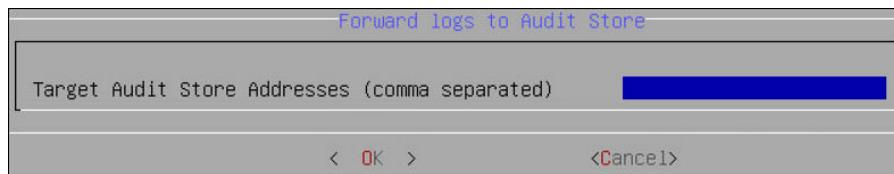


Figure 10-14: Forward Logs

8. Select **OK**.
9. Type *y* to fetch certificates for communicating with the ESA and select **OK**.

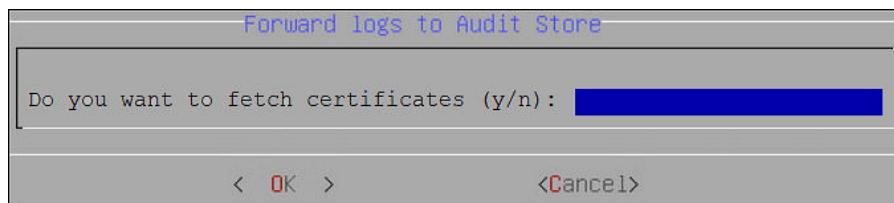


Figure 10-15: Fetch Certificates

10. Enter the admin username and password and select **OK**.

Repeat the steps provided in this section on all the ESAs in the Audit Store Cluster.

10.1.5.1.1.7 Verifying the Audit Store Cluster

View the Audit Store Management page to verify that the configurations that you performed were completed successfully using the steps provided here.

1. Login to the ESA Web UI.
2. Navigate to the **Audit Store Management** page.
3. Verify that the nodes are added to the cluster. The health of the nodes must be either green or yellow.
4. If you added additional ESAs for creating a TAC, then verify that the ESA has only the master role.

Node IP	Roles	Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
192.168.1.101	✓ ✓ ✓	Edit Roles		19s	39,502,524,416	6,995,266,048	32,547,258,368	6,44
192.168.1.102	✓ ✓ ✓	Edit Roles		2.5h	39,502,524,416	7,021,211,648	32,481,312,768	16,6
192.168.1.103	✓ ✓ ✓	Edit Roles		4.9m	45,709,819,904	5,415,325,696	40,294,494,208	28,3

Figure 10-16: Nodes Added to Cluster

10.1.5.2 Optional: Using an External SIEM

If you have an external SIEM for storing your logs, then you can configure the ESA and Protectors to sent the logs to your SIEM. You can use just your SIEM with the Protegility Audit Store and Protegility Storage Unit for storing logs.

For more information about configuring an external SIEM, refer to the section *Sending Logs to an External Location* in the [Audit Store Guide 9.1.0.5](#).

10.1.6 Migrating DMS Logs and Metering Data

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

If your ESA is a part of the TAC setup, it is recommended to migrate your logs and metering data to Protegility Analytics to avoid data loss during upgrade. This section describes how to upgrade DMS logs and metering data from your current system to Protegility Analytics.

10.1.6.1 Metering Data

The metering data is displayed on Protegility Analytics. Post the upgrade, you must execute the *Metering Upgrade* script to ensure that the metering data is exported to Protegility Analytics.

The following command must be executed to run the *Metering Upgrade* script from the `/etc/init.d` directory after performing the steps specified in the section [Setting the Audit Store](#).

```
/etc/init.d/dps_meteringupgrade
```

Note:

The *Metering Upgrade* service is uninstalled after the execution is complete.

Note:

If you have configured an Audit Store cluster, then ensure that the cluster configuration is completed successfully prior to executing the *Metering Upgrade* script.

For more information about configuring an Audit Store cluster, refer to section *Configuring the Audit Store Cluster* in the [Audit Store Guide 9.0.0.0](#).

For more information about the metering data displayed on Protegility Analytics, refer to section *Viewing the Metering Information* in the [Protegility Analytics Guide 9.0.0.0](#).

10.1.6.2 Migrating Logs

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

Migrate the logs from your current system to the Audit Store using the DMS Exporter. The logs are exported from the Postgres database to the Audit Store. Ensure that you import the logs that you require in the Audit Store to Postgres before you migrate the logs. Your existing archives would not be usable till they are exported to the Audit Store.

For more information about using the DMS Exporter, refer to [Appendix C: Migrating Logs Using the DMS Exporter](#).

Note:

It is recommended that all the logs are migrated from the current system using the DMS Exporter before performing any protect, unprotect, or reprotect operations.

Verify that the total hard disk space available is as per the following formula:

```
2 x (Total size of the Current used space + Size of the Upgrade patch)
```

For STA and LTA logs, import them back to Postgres before running the DMS Exporter. Ensure that the free space available on your system before importing STA and LTA logs is *2 times the space of the STA logs + LTA logs*. Contact Protegility Services if you need help with migrating your STA and LTA logs.

Complete the following steps to migrate logs to the Audit Store.

1. On the ESA, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegility/dms_exporter` directory.
5. Stop the DMS service using the following command:

```
dms stop
```

6. Run the following command for using the DMS Exporter.

```
python dms_exporter.py start
```

Note:

Use the command `python dms_exporter.py -h` or `python dms_exporter.py --help` to view the usage information for the command.

The DMS exporter sends logs in batches, where the exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store. Thus, if you have 4200000 rows, then the DMS Exporter will send rows in eight batches of 500000 rows and the ninth batch of the remaining 200000 rows.

Note:

If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the `last_imported_index` file in the `/opt/protegility/dms_exporter` directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics**.

The logs are exported to the Audit Store. Verify that the export was successful by navigating to `/var/log/dms_exporter` on the ESA and viewing the export status in the `dms_exporter.log` file.

Then, the logs can be seen on the **Forensics** tab in Protegility Analytics. These logs can then be used for further analysis.

10.1.7 Post Upgrade Steps

Ensure that the following steps are performed in the order given here after the upgrade to the ESA 8.1.0.0 is completed:

Note:

The export and import feature to migrate data from previous versions of the ESA to the ESA 8.1.0.0 is not supported.

1. Recreate reports, alerts, and schedule tasks



2. Remove the Reporting server and DMS components

Important: It is recommended to use ILM to export the logs from the main index and import them back in the secondary index everyday. This improves the ingestion rate of the logs into the Audit Store by periodically reducing the size of the main index.

For more information about ILM, refer to the section *Information Lifecycle Management (ILM)* in the [Protegility Analytics Guide 8.1.0.0](#).

10.1.7.1 Recreating Reports, Alerts, and Schedule Tasks

The Reporting Server and DMS Components are deprecated in the ESA 8.0.0.0. The rules, events, and alerts that were created in the ESA 7.2.1 or previous releases are available in the read-only mode after upgrading to the ESA 8.1.0.0. These must be recreated in the ESA 8.1.0.0 using the *Alerting* option in Protegility Analytics. The reports must be recreated after the upgrade to the ESA 8.1.0.0 is completed.

Similarly, the scheduled tasks that were created in the ESA 7.2.1 must be reviewed after upgrading to the ESA version 8.1.0.0. Ensure that the tasks referring to DMS components and Reporting Server in the ESA 7.2.1 are deleted, updated, or recreated in the ESA 8.1.0.0.

Note:

The reporting, alerting, and scheduling system in the ESA 8.0.0.0 is different from previous releases of the ESA, do not use the export and import feature to port the data from previous versions of the ESA to the ESA 8.0.0.0.

Create reports, alerts, and scheduled tasks in the ESA 8.1.0.0 using the following information:

- Create the reports that you require using Protegility Analytics.

For more information about creating reports, refer to the section *Working with Reports* in the [Protegility Analytics Guide 8.1.0.0](#).

- Create the alerts that you require for monitoring the system using Protegility Analytics.

For more information about creating alerts, refer to the section *Working with Alerts* in the [Protegility Analytics Guide 8.1.0.0](#).

- Create the scheduled tasks for automating the regularly performed tasks using Protegility Analytics.

For more information about the scheduler, refer to the section *Using the Scheduler* in the [Protegility Analytics Guide 8.1.0.0](#).

10.1.7.2 Removing the Reporting Server and DMS Components

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

The Reporting Server and the DMS Components are deprecated and available in the read-only mode in the ESA 8.0.0.0. Uninstall these services after completing all the upgrade steps to the ESA 8.0.0.0.

Caution:

Ensure that you have successfully migrated all the logs and metering data and that you have recreated the reports, alerts, and scheduled tasks that you require in the ESA 8.0.0.0 before uninstalling the services.

Complete the following steps to uninstall the services.



1. Login to the ESA CLI.
2. Navigate to **Administration > Add/Remove Services**.
3. Enter the root password and select **OK**.
4. Select *Remove already installed applications* and select **OK**.
5. Use the **SPACEBAR** to select the **Reporting Server v8.0.0** and the **Logging v8.0.0** products.

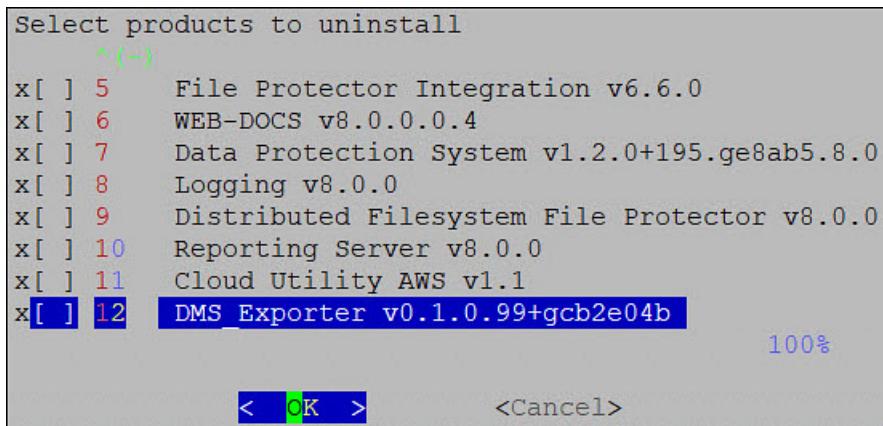


Figure 10-17: Uninstalling Services

6. Select **OK**.

The services are uninstalled and the ESA CLI Manager screen appears.

10.1.7.3 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

Before you begin

Keep the following information handy before the setup process:

- SMTP server details
- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is **25**.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.

Protegility Reporting requires a full email address in the Username.

7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user. SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.
A message box appears.
14. Click **EXIT** to save the settings.

10.1.8 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

10.1.8.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

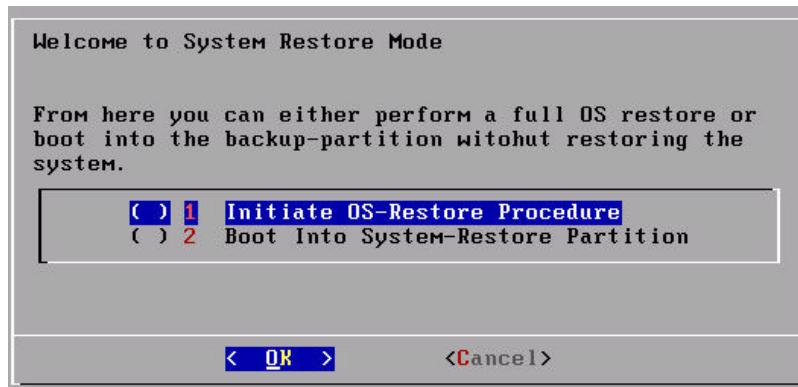
1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system. A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.
3. Enter the *root* password and select **OK**.

Note:

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

10.1.8.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

10.1.8.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.

4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

10.1.8.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.

13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

10.1.8.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

► To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

10.2 Upgrading Protectors

If you are upgrading the Protectors from v7.2.1 to v8.1.0.0, then ensure that the ESA is at v8.1.0.0.

Note:

For more information about the compatible data elements for the different protector versions, refer to the table [Data Element Compatibility Matrix](#).

10.2.1 Upgrading Application Protector

You must uninstall the earlier version of the Application Protector and install the Application Protector v8.1.0.0.

For more information about installing the Application Protector v8.1.0.0 protector, refer to the section *Installing and Uninstalling Application Protectors* in the [Installation Guide 8.1.0.0](#).

Note: The ESA v8.1.0.0 is not compatible with AP Lite version 6.6.5.

10.2.2 Upgrading Database Protector

You must uninstall the previous version of the Database Protector and then install the v8.1.0.0 protector.

For more information about installing the v8.1.0.0 protector, refer to the section [*Installing and Uninstalling Database Protectors*](#) in the [*Installation Guide 8.1.0.0*](#).

10.2.3 Upgrading Data Security Gateway (DSG)

The Data Security Gateway (DSG) can be upgraded to the DSG v2.6.0.0, which is compatible with the ESA v8.1.0.0. You must apply the *ESA_PAP-ALL-64_x86-64_8.1.0.0.1962.FE-1.pty* patch on the ESA v8.1.0.0 and reimage the DSG nodes to DSG v2.6.0.0.

For more information about upgrading the DSG to DSG v2.6.0.0, refer to the section *Upgrading to DSG v2.6.0.0* in the [*Data Security Gateway User Guide 2.6.0.0*](#).

Chapter 11

Upgrading from Big Data Protector v7.2 to Big Data Protector v8.1.0.0

You must uninstall the earlier version of the Big Data Protector and then install the Big Data Protector v8.1.0.0.

For more information about installing the Big Data Protector v8.1.0.0 protector, refer to the section *13.6.1 Installing Big Data Protector using CDP Private Cloud Base (CDP-PVC-Base) Native Installer* in the *Installation Guide 8.1.0.0*.

Note: If you are performing a rolling upgrade of the CDP-PVC-Base distribution, then you need to uninstall Big Data Protector before starting the rolling upgrade. After the rolling upgrade of the CDP-PVC-Base distribution is completed, you need to install the Big Data Protector version that is compatible with the updated version of the CDP-PVC-Base distribution.

Note: Ensure that you upgrade the ESA prior to upgrading the protector.

Chapter 12

Upgrading from v7.2.1 to v8.0.0.0

[12.1 Overview of the Upgrade to ESA v8.0.0.0](#)

[12.2 Upgrading to ESA v8.0.0.0](#)

[12.3 Upgrading Protectors](#)

This section describes the steps to upgrade the ESA v7.2.1 to ESA v8.0.0.0 and protectors to the latest compatible versions.

Note: Ensure that you upgrade the ESA prior to upgrading the protector.

Important:

If you are upgrading from the ESA v7.2.1 or earlier to ESA v8.1.0.0, then you do not require to perform all the steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0.

For more information about upgrading the ESA v7.2.1 to ESA 8.1.0.0, refer to the [Upgrade Process: Step-by-step procedure](#).

12.1 Overview of the Upgrade to ESA v8.0.0.0

The upgrading of your ESA involves completing the prerequisites, installing the patch, verifying the upgrade, configuring settings, and so on. During this process, it is important that data integrity is upheld and carried over to the upgraded version. This calls for a step-by-step approach to ensure a smooth transition of system to the latest version. Based on whether the ESA is a standalone system or set up in a Trusted Appliances Cluster (TAC), different steps must be performed to finalize the upgrade successfully. The following sections provides a walkthrough of the different procedures that you must follow to upgrade ESA to v8.0.0.0.

12.1.1 Upgrading a Standalone ESA

When you are upgrading a standalone ESA v7.2.1 to 8.0.0.0, then complete the following steps.

1. Ensure that the Prerequisites for upgrading the ESA are met.
2. [Upgrade to v8.0.0.0 by installing the patch](#).
3. [Complete the upgrade on the standalone system](#)
4. [Initialize Analytics on the upgraded ESA to create a single node audit store cluster](#).
5. [Add two Protegility Storage Units \(PSUs\) to the Audit Store cluster](#).
6. [Configure the td-agent in the Audit Store cluster](#).
7. [Configure ESA for the Audit Store cluster](#).
8. [Verify the Audit Store cluster](#).



9. *Migrate DMS logs and metering data to the Audit Store.*
10. *Perform the required post upgrade steps.*
11. Configure the load balancer used by the protectors to point to the upgraded ESA.

12.1.2 Upgrading ESA on a TAC Setup

This section describes the steps for upgrading the ESAs that are in a TAC. In this upgrade process, the ESAs in a cluster are upgraded one at a time. It involves removing ESA from the TAC, upgrading them, connecting to audit store, and then re-building the TAC. The following figure illustrates a sample TAC environment on which the ESAs must be upgraded to v8.0.0.0.

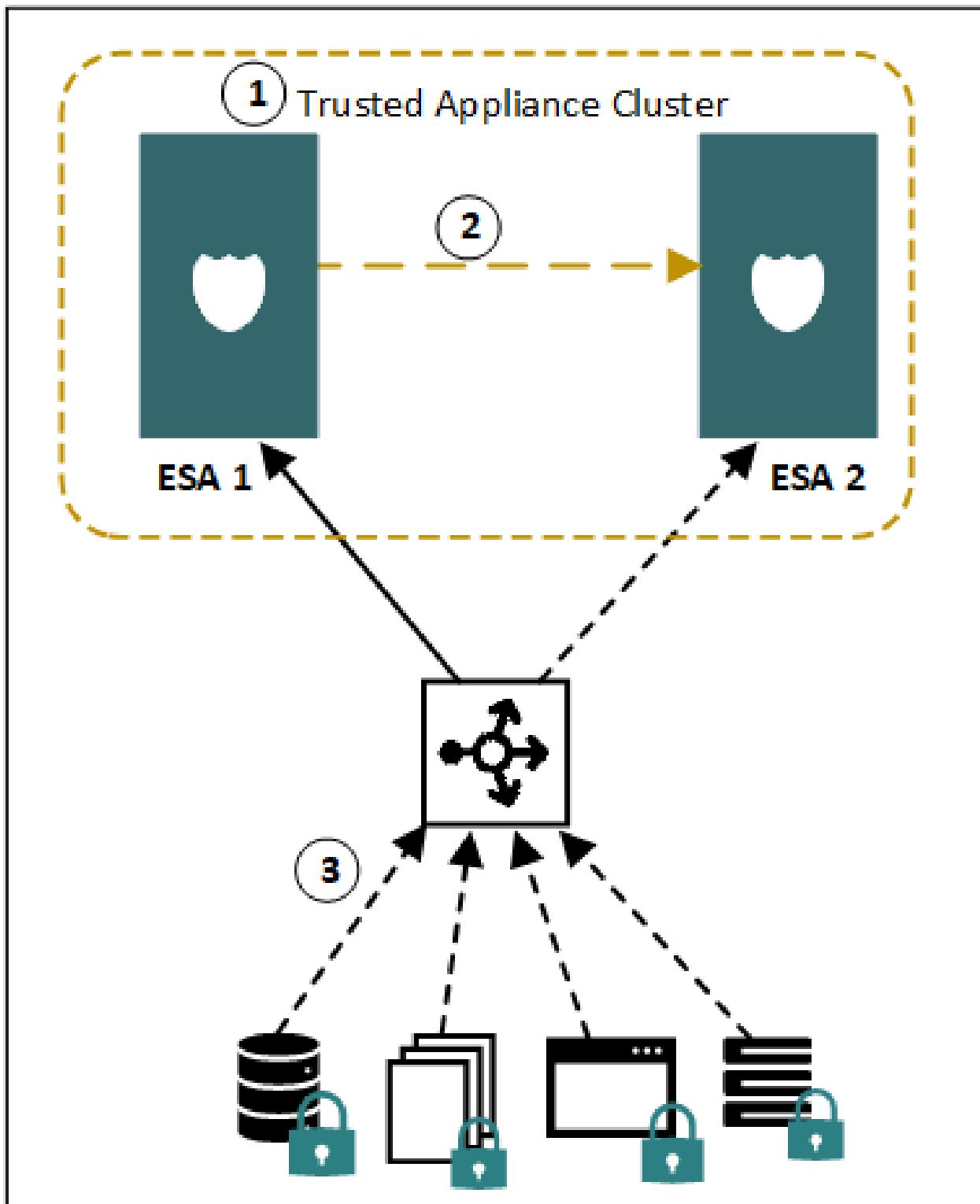


Figure 12-1: ESA v7.2.1 in a TAC

The following table illustrates the figure.

Table 12-1: TAC Setup

Callout	Description
1	TAC contains a primary appliance ESA 1 and a stand-by appliance ESA 2
2	Data replication for policies, forensics, or DSG configuration operate from ESA 1 to ESA 2

Callout	Description
3	Protectors communicate with the load balancer that balances the requests between ESA 1 and ESA 2

In this setup, you must perform the following steps to upgrade the appliances.

Note:

Ensure that you upgrade the Primary ESA only after upgrading all the stand-by ESAs.

1. Disable the scheduler tasks between ESA 1 and ESA 2.
2. Remove the secondary appliance ESA 2 from the TAC.
3. *Upgrade ESA 2 to v8.0.0.0 by installing the patch.*
4. Perform the following steps on ESA 2.
 - a. *Complete the upgrade on the ESA 2*
 - b. *Initialize Analytics on the upgraded ESA to create an Audit Store cluster.*
 - c. *Add two Protegility Storage Units (PSUs) to the Audit Store cluster.*
 - d. *Configure the td-agent in the Audit Store cluster.*
 - e. *Configure ESA for the Audit Store cluster.*
 - f. *Verify the Audit Store cluster.*
 - g. *Migrate the Metering data to Protegility Analytics cluster.*
 - h. *Migrate the DMS logs to Protegility Analytics cluster.*

Important:

Before upgrade, if the DMS logs were replicated between ESA 1 and ESA 2, then it is recommended to not perform this step.

- i. *Perform the required post upgrade steps on ESA 2.*
5. Configure the load balancer to point to ESA 2.
6. Remove ESA 1 from the TAC.
7. *Upgrade ESA 1 to v8.0.0.0 by installing the patch.*
8. Complete the following steps on ESA 1.
 - a. *Complete the upgrade on the ESA 1*
 - b. *Perform the required post upgrade steps on ESA 1.*
 - c. *Add ESA1 to the audit store cluster.*
 - d. *Configure the td-agent in the Audit Store cluster.*
 - e. *Configure ESA for the Audit Store cluster.*
 - f. *Verify the Audit Store cluster.*
 - g. *Migrate the Metering data to Protegility Analytics cluster.*
 - h. *Migrate the DMS logs to Protegility Analytics cluster.*
 - i. *Perform the required post upgrade steps on ESA 1.*
9. Create a TAC on ESA1.
For more information about creating a TAC, refer to the *Appliances Overview Guide 8.0.0.0*.
10. Join ESA 2 to the TAC created on ESA1.



For more information about joining a TAC, refer to the [Appliances Overview Guide 8.0.0.0](#).

11. Enable the scheduler tasks between ESA 1 and ESA 2.

For more information about replication tasks, refer to section [Working with Backup and Restore](#) in the [Appliances Overview Guide 8.0.0.0](#).

The following figure illustrates the upgraded TAC setup.

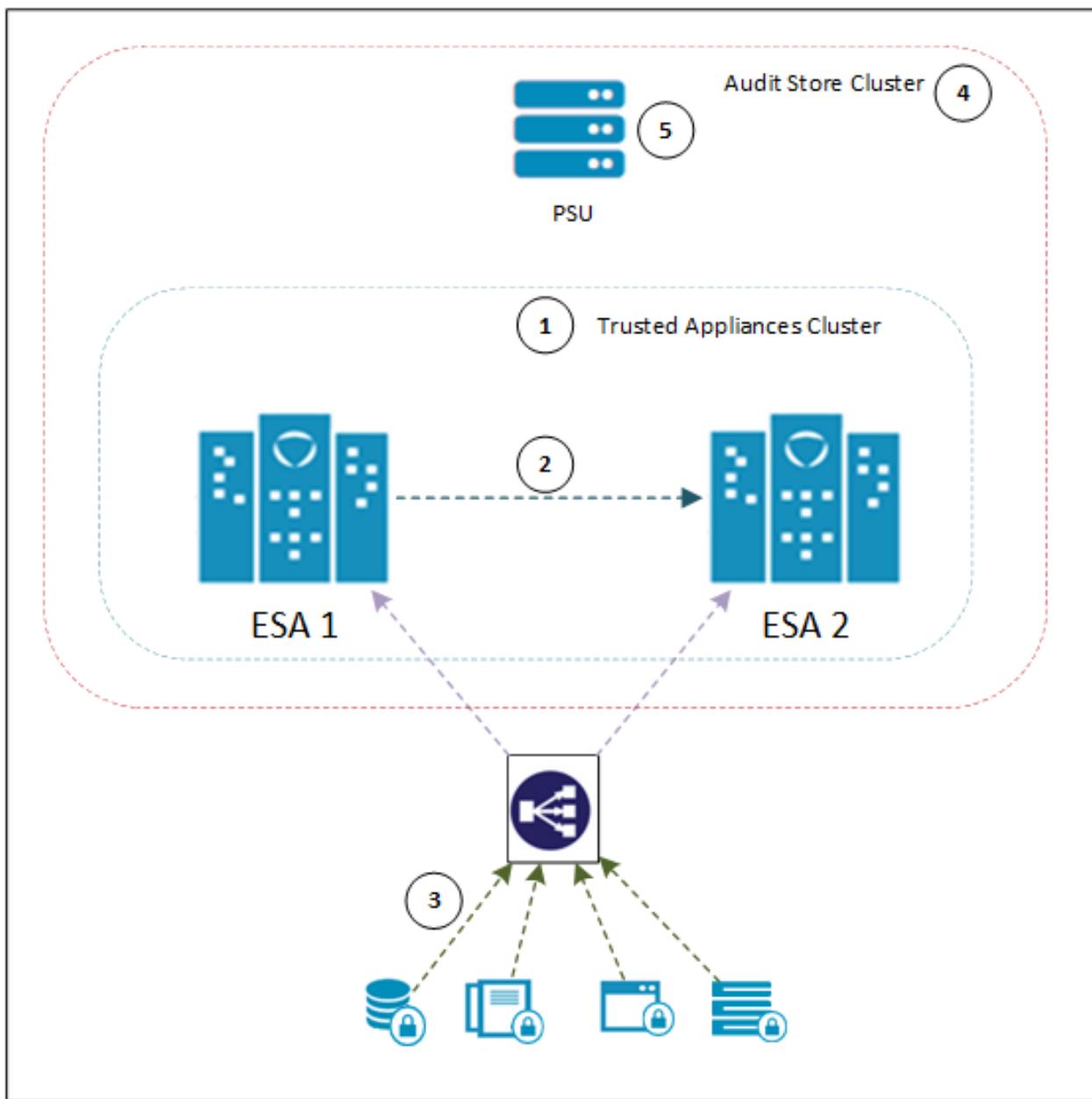


Figure 12-2: ESA v8.0.0.0 in a TAC

Table 12-2: Upgraded TAC Setup

Callout	Description
1	TAC is established between primary appliance ESA 1 and a stand-by appliance ESA 2. For more information about TAC, refer to section Trusted Appliances Cluster (TAC) in the Appliances Overview Guide 8.0.0.0 .

Callout	Description
2	Data replication for policies, forensics, or DSG configuration operate from ESA 1 to ESA 2. For more information about replication tasks, refer to section Working with Backup and Restore in the Appliances Overview Guide 8.0.0.0 .
3	Protectors communicate with the load balancer that balances the requests between the upgraded ESA 1 and ESA 2
4	Audit Store cluster is enabled for the ESAs. For more information about enabling Audit Store Cluster, refer to section Trusted Appliances Cluster (TAC) in the Appliances Overview Guide 8.0.0.0 .
5	PSUs are added to the Audit Store Cluster

12.2 Upgrading to ESA v8.0.0.0

This section describes the steps to upgrade the ESA to v8.0.0.0. In this release, the Linux kernel-related configuration files for v4.19.100 are updated. In addition, the OS packages are updated to their latest versions.

The information about the OS packages and their versions is available in the *Contractual.htm* file. Navigate to **Settings > System > Files > Downloads - Other files** to download the *Contractual.htm* file.

12.2.1 Prerequisites

The following are the prerequisites for upgrading the ESA to the latest version:

- Accounts
- Backup and Restore
- Installations and Hardware Requirements
- High Availability (HA)
- Keys
- Customized files (Configuration files, Certificates)
- HSM

12.2.1.1 Accounts

The administrative account used for upgrading the ESA must be active.

For more information about Accounts and Password Management, refer to the [Appliance Overview Guide 8.1.0.0](#).

12.2.1.2 Backup and Restore

The OS backup procedure is performed to backup files, OS settings, policy information, and user information. Ensure that you have the latest backup before upgrading to the latest version.

Note:

After upgrading to 8.0.0.0, if you take the backup of the ESA v8.0.0.0, then it will overwrite the backup of the ESA v7.2.1. Therefore, ensure that you take the backup of the ESA v7.2.1. Ensure that the backup is available on a different server.

If the patch installation fails, then you can revert the changes to a previous version. Ensure that you backup the complete OS or export the required files before initiating the patch installation process.

For more information about backup and restore, refer to the section *3.4.4 Working with Backup and Restore* in the [Appliances Overview Guide 8.1.0.0](#).

Note:

You can backup specific components of your appliance using the **File Export** option. Ensure that you create a back up of the Policy Management data, Directory Server settings, Appliance OS Configuration, Export Gateway Configuration Files, and so on.

Note: If you are upgrading an ESA with the DSG installed, then select the *Export Gateway Configuration Files* and perform the export operation.

12.2.1.2.1 Full OS Backup

You must backup the complete OS. This prevents loss of data and ensures that you can revert to a previous stable configuration in case of a failure during patch installation.

Note:

This option is available only for the on-premise deployments.

► To backup the full OS configuration:

1. Login to the ESA Web UI.
2. Navigate to **System > Backup & Restore > OS Full**, to backup the full OS.
3. Click **Backup**.
The backup process is initiated. After the OS Backup process is completed, a notification message appears on the ESA Web UI Dashboard.

12.2.1.2.2 Creating a snapshot for Cloud-based Services

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup and restore information in case of failures. Ensure that you have the latest snapshot before upgrading to v8.0.0.0.

You can create a snapshot of an instance or a disk on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating snapshots for respective cloud platforms, refer to the [Appliance Overview Guide 8.0.0.0](#).

12.2.1.3 Installations and Hardware Requirements

Installation Requirements

- The *ESA_PAP-ALL-64_x86-64_8.0.0.0.x_UP-1.pty* patch file is installed.
- The minimum space available in the */opt* directory should be more than twice the size of the patch file.

For example, if the size of the patch is 2 GB, then the minimum space available in the `/opt` directory should be more than 4 GB.

Note:

Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

Hardware Requirements

Ensure that the hardware requirements are met before you upgrade the appliance.

For more information about the hardware requirements, refer to section [System Hardware Requirements](#).

12.2.1.4 High Availability (HA)

If you are upgrading an ESA appliance that is in an HA setup, then you must remove the HA services from the ESA appliance and then apply the upgrade patch.

For more information about removing the HA services, refer to the [Scalability and Availability Guide 7.2.1](#).

Note:

The HA services are not supported from version 8.0.0.0. If you continue using the HA services, then it might break the functionality of the system.

For more information about the alternate to HA services, refer to the [Fault Tolerance Guide 8.0.0.0](#) on the [My.Protegility](#) portal.

12.2.1.5 Trusted Appliances Cluster (TAC)

If the ESA you want to upgrade is a part of the Trusted Appliances Cluster (TAC), ensure that all the replication tasks are disabled.

12.2.1.6 Keys

If the security keys, such as, master key or repository key have expired or are due to expire within 30 days, then the upgrade fails. Thus, you must rotate the keys before performing the upgrade.

For more information about rotating keys, refer to section [Working with Keys](#) in the [Protegility Key Management Guide 9.1.0.0](#).

12.2.1.7 Creating a Metering Backup File

Ensure that you create a backup file of the metering logs before performing the upgrade on the ESA v7.2.1.

► To create a backup file of the metering logs:

1. Login to the ESA CLI Manager.

2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility`/directory using the following command.
`cd /opt/protegility/`
4. Create a temporary directory to save the metering logs using the following command.
`mkdir <directory_name>`

Note: Ensure that the temporary directory is accessible on the ESA v7.2.1. This directory must not be copied or moved to another location.

5. Add permissions to the temporary directory using the following command.
`chmod 755 <directory_name>`
6. Change the owner of the temporary directory to *service admin* using the following command.
`chown service_admin.service_admin <directory_name>`
7. Navigate to the temporary directory using the following command.
`cd <directory_name>`
8. Create the backup file of the metering logs using the following command.
`/opt/protegility/repository/pim/pgsql/bin/pg_dump -h localhost -U admin -p 5211 --schema metering --format=c ADMINDB > /opt/protegility/<directory_name>/<backup_filename>.bak`

12.2.1.8 Customized files (Configuration files, Certificates)

The following is the prerequisite for upgrading the ESA to the latest version:

- The *exclude* file present in the `/opt/ExportImport/filelist` directory contains the list of system files and directories that you do not want to export. If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

Note:

If a file or directory is present in the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

Note: Ensure that you do not remove the files or directories that are listed in the *customer.custom* file from the system.

For more information about including custom files in the *customer.custom* file and editing the *exclude* file, refer to the section *Exporting Custom Files* in the *Appliance Overview Guide 8.0.0.0*.

12.2.1.9 DMS and Reporting Server

If you are upgrading an ESA appliance that has cluster replication tasks created by the users, then ensure that DMS options, such as, *Log-Server Repository*, *Log-Server Configuration*, and *Log-Server Event Configuration* are disabled.

If there are preconfigured scheduling tasks, such as, *100 DBIntegrity Logging-Repository Integrity Check (Once a week)*, then they will be automatically disabled.

A notification will be displayed on the ESA Web UI dashboard.

The following scheduled tasks were disabled due to Log Server migration: [100]

Note:



The DMS, reporting server, and DMS2mail services are not supported in version 8.0.0.0.

12.2.1.10 HSM

If you are working with HSM vendor apart from Safenet HSM, Futurex HSM, or Utimaco HSM and are planning to continue working with this HSM solution post upgrade, then you must switch to the soft HSM prior to upgrading the ESA version 7.2.1 to version 8.1.0.0. Post upgrade, you must switch from the soft HSM to the HSM to continue using the HSM solution.

For more information about switching from the soft HSM to the required external HSM, refer to the section *Switching from the external HSM to the Soft HSM* in the [Key Management Guide 8.1.0.0](#).

12.2.1.11 Kernel Mode

The v7.2.1 release supports switching kernel modes. You can switch the kernel between generic and audit mode. The audit mode is used for running audits related to the kernel. The v8.0.0.0 release supports a unified kernel mode that also includes the audits related to kernel. Before updating ESA v7.2.1 to ESA v8.0.0.0, you must select the generic mode of the kernel. Retaining the kernel mode as audit and upgrading to v8.0.0 might cause issues in the upgrade leading to the Web UI not being accessible.

You can check the mode of the kernel using the following command.

```
uname -r
```

Ensure that the mode of the kernel is **generic-4.9.194**. If the kernel is in **audit-4.9.194**, switch it to the generic mode by performing the following steps:

1. Log in the ESA CLI Manager as an administrative user.
2. Navigate to **Administration > OS Console**.
3. Run the following command:

```
/etc/opt/scripts/support/kernel_mng.py
```

4. Select **generic-4.9.194**.
5. Type **YES** to restart the system.

12.2.2 Upgrading ESA from v7.2.1 to v8.0.0.0

This section describes the steps to upgrade from the ESA v7.2.1 to ESA v8.0.0.0.

► To install the ESA v8.0.0.0 patch:

1. Login to the ESA Web UI with administrator credentials.
2. Navigate to **Settings > System > File Upload** to upload the patch.
3. On the **File Selection** screen, click **Choose File**.
4. Select the *ESA_PAP-ALL-64_x86-64_8.0.0.0.x.UP-1.pty* file and click **Upload**.
 - If the size of the file is less than the upload limit, then the file upload is initiated.
 - If the size of the file exceeds the upload limit, then a prompt to enter the administrator credentials appears. Enter the administrator credentials to initiate the file upload.

Note:



Ensure that you download the latest patch from the [My.Protegility](#) portal.

For more information about the latest build number and the patch details, refer to the [Release Notes](#) of the respective patch.

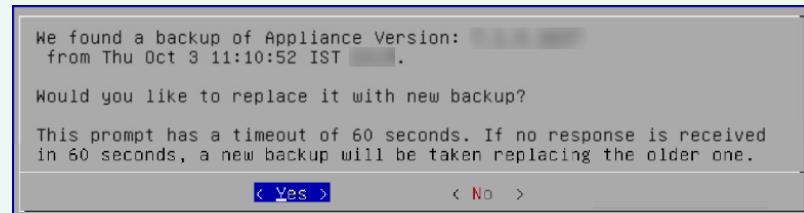
The file upload is initiated.

Note:

Ensure that the file upload is completed before proceeding to the CLI Manager.

5. Login to the ESA CLI Manager with administrator credentials.
6. Navigate to **Administration > Patch Management** to install the patch.
A prompt to enter the root credentials appears.
7. Enter the root password.
The patch management screen appears.
8. Select **Install a Patch**.
9. Select the *ESA_PAP-ALL-64_x86-64_8.0.0.0.x.UP-1.pty* patch file and select **Install**.

Note: If a backup operation is performed before upgrading to the ESA v8.0.0.0, then the following message to replace the existing backup appears.

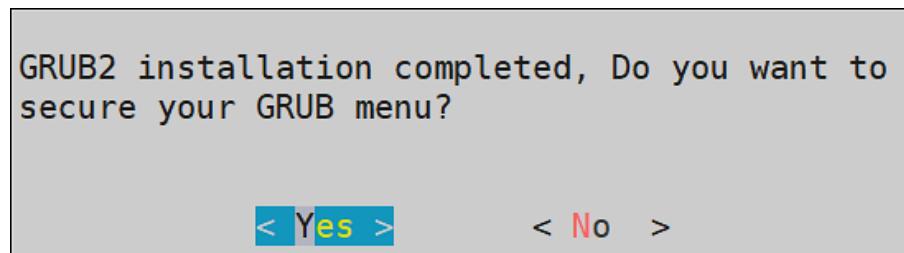


You can select **Yes** to overwrite the existing backup. Alternatively, you can select **No** to retain the existing backup and continue the upgrade operation.

The backup is initiated.

10. After the backup is completed, the upgrade process begins. During upgrade for the ESA on-premise, a screen to configure GRUB credentials appears. In Protegility appliances, GRUB2 is packaged with v8.0.0.0. This replaces GRUB1 that is present in the earlier versions of the appliances. If you want to protect the boot configurations, you can secure it by enforcing a username and password combination for the GRUB menu. While upgrading to v8.0.0.0, you can secure the GRUB menu by creating a username and setting password as shown in the following figure.

The following screen appears.



Note:

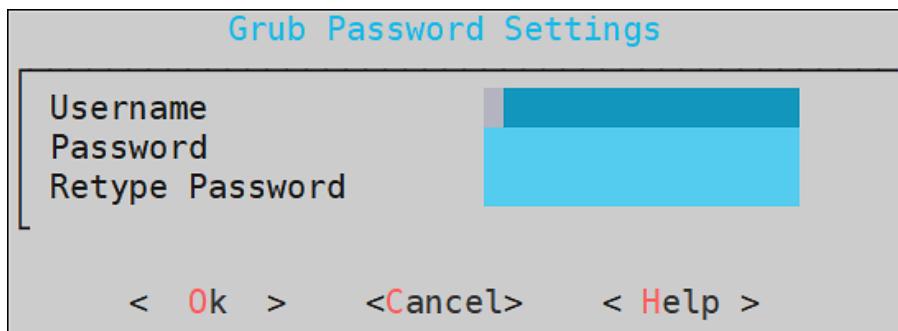
The timeout of this screen is 60 seconds. If you do not initiate the action within 60 seconds, then the security for the GRUB menu is disabled. If required, you can enable this feature from the CLI Manager after the patch installation is completed.

For more information about GRUB2, refer to GRUB in the *Appliances Overview Guide 8.0.0.0*.

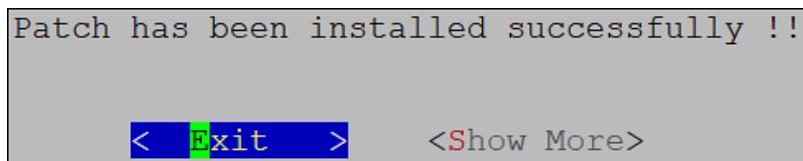
Note:

This screen is not displayed while performing the upgrade on the cloud instances.

11. Select **Yes** to secure the GRUB menu. Alternatively, you can select **No** to continue the upgrade process without securing GRUB menu.
12. Enter the information in the **Username**, **Password**, and **Retype Password** textboxes on the following screen.



13. Select **Exit** on the following screen.



The patch is installed and ESA is upgraded to ESA v8.0.0.

12.2.3 Upgrading to ESA v8.0.0.0 on Cloud-based Services

On Cloud-based services, such as AWS, Azure, or GCP, you can upgrade to the ESA v8.0.0.0. Ensure that the latest snapshot of the instance is created before the upgrade.

For more information about creating a snapshot of the respective cloud instances, refer to the *Appliances Overview Guide 8.0.0.0*.

You can then upgrade your appliance deployed in the instance to the ESA v8.0.0.0.

Note:

After the upgrade is completed, *Azure Tools* is installed on the Azure Cloud Platform.

For more information about the installed products on the ESA, refer to the *Appliances Overview Guide 8.0.0.0*.

For more information about upgrading to the ESA v8.0.0.0, refer to section [Upgrading ESA from v7.2.1 to v8.0.0.0](#).

12.2.3.1 Upgrading from Existing ESA Instance of v8.0.0.0

On Cloud Based services, such as AWS, Azure, or GCP, you can upgrade from the ESA v8.0.0.0 versions to the ESA v8.1.0.0.

You must install the *ESA_PAP-ALL-64_x86-64_8.1.0.0.x.UP-1.pty* patch provided on the existing ESA v8.0.0.0 instance.

Note:

Ensure that the snapshot for the instance is taken before upgrade.

For more information about creating a snapshot for the respective Cloud instances, refer to the *Appliance Overview Guide 8.1.0.0*.

For more information about upgrading to the ESA v8.1.0.0, refer to [Upgrading ESA from v7.2.1 to v8.0.0.0](#).

12.2.4 Completing the Upgrade

After installing the patch, you must verify the patch installation, check the upgrade logs, add AppArmor profiles, configure certificates, and install the PSU to complete the upgrade. The following sections describe the steps to complete the upgrade.

12.2.4.1 Upgrade Logs

During the upgrade process, logs describe the status of the upgrade process. The logs describe the services that are initiated, restarted, or the errors generated.

To view the logs under the following directories from the CLI Manager, navigate to **CLI Manager > Administration > OS console**.

1. */var/log*
 - *Installation.log* - Provides the logs for all the installed components.
 - *syslog* - Provides collective information about the syslogs.
2. */etc/opt/PatchManagement/installed_patches/<PATCH_NAME>/patchdata/patch.log*

12.2.4.2 Verifying the Patch Installation

After upgrading to the ESA v8.0.0.0, you can verify the patch installation.

► To verify the patch installation:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Select **List installed patches**.

The *ESA_8.0.0.0* patch name appears.

5. Login to the ESA Web UI.

6. Navigate to the **System > Information** page.

The ESA is updated to v8.0.0.0 in the **Installed Patches** section.

Ensure to check the Logs to verify that there are no errors.

12.2.4.3 Adding AppArmor Profiles

Note: If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

In ESA v8.0.0.0, the AppArmor is enabled as part of the ESA installation to protect the different appliance capabilities, such as, antivirus, trusted appliances cluster, firewall, NTP services, web services, and two factor authentication. Thus, after installing ESA, you must add permissions to the *usr.sbin.apache2* profile for enabling features, such as Proxy Authentication, Import/Export, and Cluster operation to function without AppArmor restricting them.

Complete the following steps to add permissions to the profile.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the */etc/apparmor.d/custom* directory.
4. Edit the *usr.sbin.apache2* profile.
5. Insert the following lines.

```
/opt/ldap/** rix,  
/usr/lib/sftp-server ix,  
/lib/bridge-utils/ifupdown.sh rix,  
/usr/lib/rabbitmq/lib/rabbitmq_server-0.0.0/sbin/rabbitmq-server rix,  
/lib/bridge-utils/ifupdown.sh rix,  
/lib/bridge-utils/ifupdown.sh rix,  
/usr/sbin/sshd Ux,
```

6. Edit the *etc.opt.Cluster.cluster_helper* profile.
 7. Insert the following lines.
- ```
/usr/local/sbin/tcping rix,
/usr/local/sbin/Log rix,
/usr/bin/sudo rix,
/usr/local/lib/python2.7/dist-packages/** rw,
```
8. Restart the AppArmor service using the following command.

```
/etc/init.d/apparmor restart
```

The permissions are applied to the profile and you can run the features without AppArmor denial logs.

For more information about AppArmor, refer to the [Appliances Overview Guide 8.0.0.0](#).

### 12.2.4.4 Restoring the Backup File of the Metering Logs

A backup of the metering logs is required on the ESA Pre-v9.0.0.0 in the */opt/protegility/* directory during the upgrade. This file is required for the migration of the metering logs.

**Note:** If the backup file of the metering logs is available in the directory, then skip this section.

For more information about the creating the backup file of the metering logs, refer to the section [Creating a Metering Backup File](#).

► To restore the backup file of the metering logs:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/opt/protegility` directory using the following command.

```
cd /opt/protegility/
```

4. Restore the backup file of the metering logs using the following command.  
`cp <backup_filename>.bak /opt/protegility/hubcontroller/`

#### 12.2.4.5 Restarting the System

After the ESA patch, `ESA_PAP-ALL-64_x86-64_8.0.0.0.x.UP-1.pty` is installed successfully, restart the ESA machine. This ensures the configuration files of the Linux Kernel are upgraded.

#### 12.2.4.6 Custom Certificates

If you are upgrading from an earlier version to ESA 8.0.0.0 and use custom certificates, then run the following step after the upgrade is complete and custom certificates are applied for td-agent, Audit Store, and Analytics, if installed.

After the upgrade is complete, the *Audit Store Repository* service will be in the stopped state till the security is set up. Additionally, errors might be displayed in the logs related to the certificates. Complete the following steps to configure the custom certificates.

1. From the ESA Web UI, navigate to **System > Services > Audit Store**.
2. Ensure that the **Audit Store Repository** service is not running. If the service is running, then stop the service.
3. Configure the custom certificates and upload it to the Certificate Repository.

**Note:**

For more information about configuring custom certificates, refer to the section *Using Custom Certificates in the Audit Store* in the [Certificate Management Guide 8.0.0.0](#).

4. Set the custom certificates for the PLUG components as *Active*.

**Note:**

For more information about marking certificates as active, refer to the section *To change certificates* in the [Certificate Management Guide 8.0.0.0](#).

5. From the ESA Web UI, navigate to **System > Services > Audit Store**.
6. Start the **Audit Store Repository** service.
7. Open the ESA CLI.
8. Navigate to **Tools**.
9. Run **Apply Audit Store Security Configs**.

## 12.2.4.7 Installing the Protegility Storage Unit

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

The Protegility Storage Unit consists of the *td-agent* and the Audit Store installed on the Appliance. It is a hardened appliance that is used to scale the Audit Store cluster with the enhanced security of a Protegility appliance. After installing the ESA, you can add additional Protegility Storage Units to the setup.

The Audit Store cluster requires a minimum of 3 nodes in the Audit Store Cluster. If you require more nodes, then add Protegility Storage Units as nodes to the Audit Store cluster.

As a basic requirement, you must install 2 PSUs to create the Audit Store Cluster.

For more information about installing the Protegility Storage Unit, refer to the section *Installing the Protegility Storage Unit* in the [\*Protegility Storage Unit Guide 8.0.0.0\*](#).

## 12.2.5 Audit Store Clustering using the Protegility Storage Unit

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

Clustering is a powerful way to increase the capability of your system. You can add nodes to expand the cluster. Expanding the cluster using the Protegility Storage Unit provides an advantage by increasing the storage space available.

When adding Protegility Storage Unit nodes for expanding the Audit Store cluster, ensure that you create the Audit Store cluster of an odd number of nodes with 3 nodes and above. A minimum of 3 nodes are required because of the following scenarios:

- 1 node: This scenario will result in total loss of service in case of a failure because no backup nodes are available.
- 2 nodes: In this scenario, both nodes added will form the master Audit Store cluster. If one node fails, then the Audit Store cluster becomes unstable and inaccessible as it does not have the minimum required master nodes, that is two nodes.
- 3 nodes and above: In this scenario, 2 nodes will be used for the master Audit Store cluster. The remaining nodes will be added as true Audit Store clustering nodes for expanding the capabilities of the system.

A basic setup is shown in the following figure.

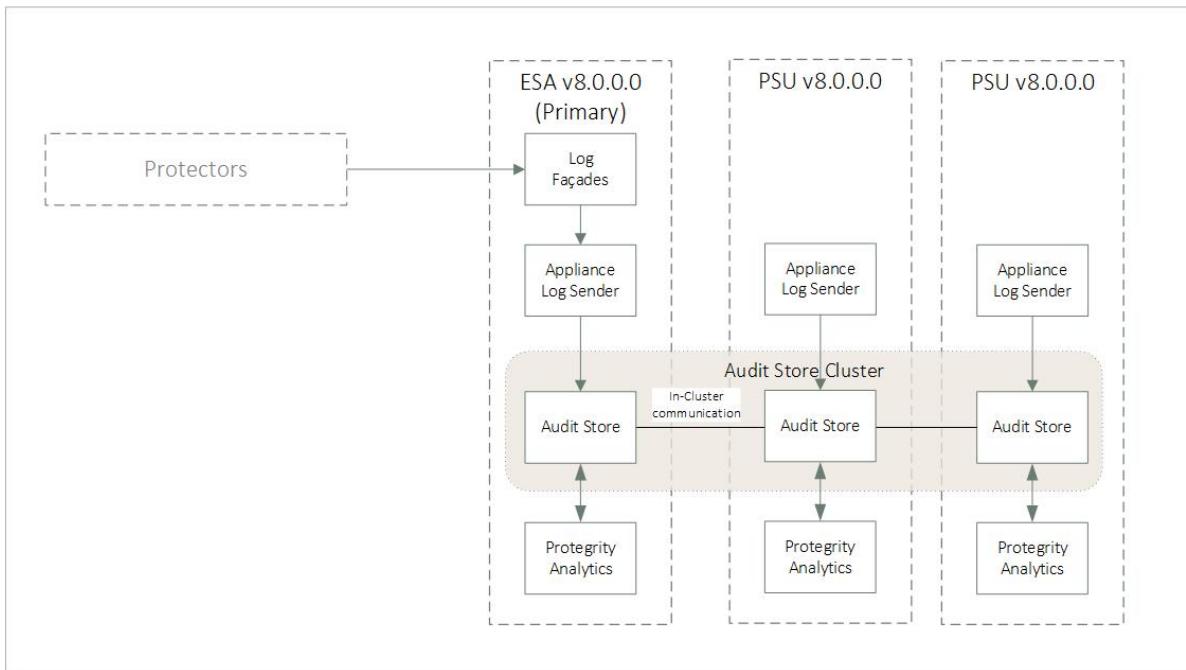


Figure 12-3: Basic Audit Store Cluster

In the figure, the arrows show the log flow direction. The basic setup consists of three systems. Here the systems consist of 1 ESA and 2 Protegility Storage Unit. The Protegility Storage Unit forms a part of the Audit Store cluster where the Audit Stores on all the nodes are linked together to form the storage unit. The logs received by the ESA are stored in the Audit Store cluster, the data would be stored on the local node or any node that is a part of the Audit Store cluster with the *ingest* role.

For more information about the various node roles, refer to the section *Configuring Roles for the Audit Store Cluster* in the [Audit Store Guide 8.1.0.0](#).

The basic setup when Trusted Appliance Cluster (TAC) is implemented consists of 2 ESAs and 2 Protegility Storage Units as shown in the following figure.

**Note:** The Audit Store cluster is different from the TAC in the ESA. A TAC is used for grouping and managing multiple ESAs together. In the Audit Store cluster, the Audit Store nodes are grouped together to form the storage unit. The Audit Stores in the Audit Store cluster might be a part of the ESA or the Protegility Storage Unit. The Protegility Storage Unit may or may not be a part of the TAC.

For more information about the TAC, refer to the section *Trusted Appliances Cluster (TAC)* in the [Appliances Overview Guide 8.1.0.0](#).

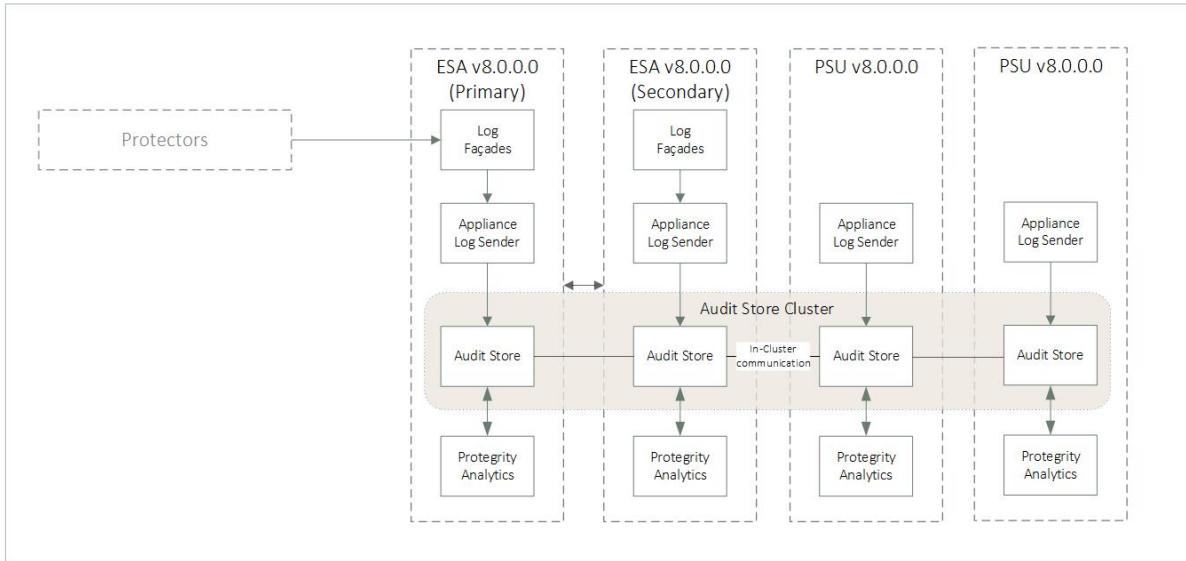


Figure 12-4: Basic Audit Store Cluster in TAC

The Audit Store cluster is flexible and nodes can be added and removed from the Audit Store cluster based on your requirements. Thus, multiple nodes can be added to the Audit Store cluster as shown in the following figure.

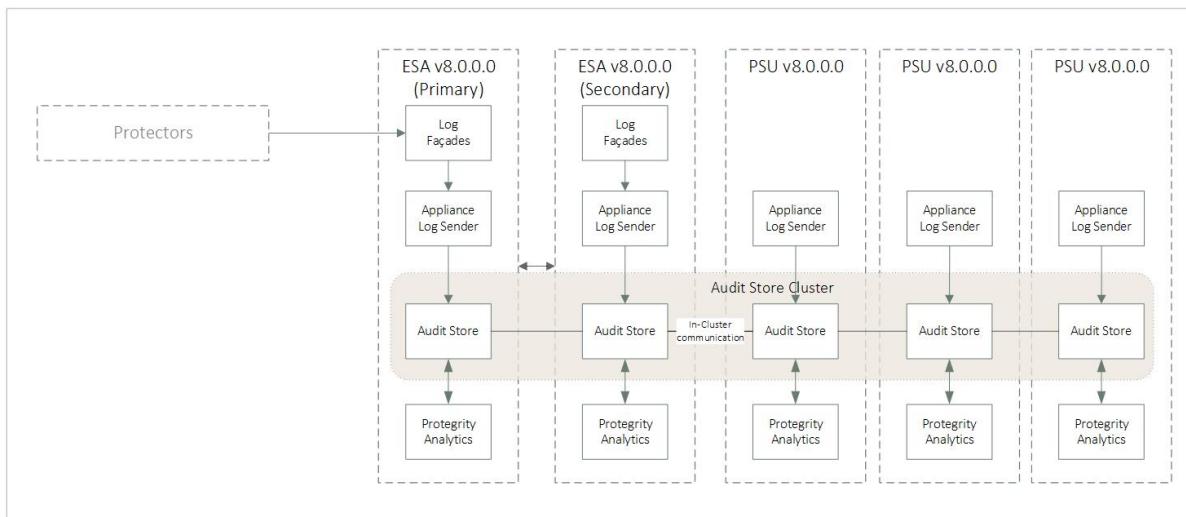


Figure 12-5: Multi-Node Cluster

**Note:** When you add nodes to the Audit Store cluster using the ESAs or Protegility Storage Unit, it is recommended that the number of nodes are odd in number to make the cluster more resilient.

If any node is not required, then the node can be removed from the Audit Store cluster. When the node is removed from a cluster, the indexes and internal configurations, such as, the td-agent and Analytics settings are reset. In this case, the Protegility Storage Unit remains uninitialized and needs to be added to another Audit Store cluster before it can be used again.

### 12.2.5.1 Completing the Prerequisites

Ensure that the following prerequisites are met before configuring the Audit Store Cluster. Protegility recommends that the Audit Store Cluster has a minimum of 1 ESA and 2 PSUs or 2 ESAs and 1 PSU for creating a highly-available multi-node Audit Store cluster.

1. Install and set up the first ESA. This will be the Primary ESA if you set up a TAC.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

2. If you require TAC, then install and set up the second ESA. This will be the Secondary ESA in a TAC. Skip this step if TAC is not required.

For more information about installing the ESA, refer to the section [Installing the ESA On-Premise](#) or [Installing Appliances on Cloud Platforms](#).

3. Install and set up the first PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

4. Install and set up the second PSU.

For more information about installing the PSU, refer to the section [Installing the Protegility Storage Unit](#) in the [Protegility Storage Unit Guide 9.1.0.0](#).

### 12.2.5.2 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, Protegility Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as, *td-agent*, is started and Protegility 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.

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

The following screen appears.

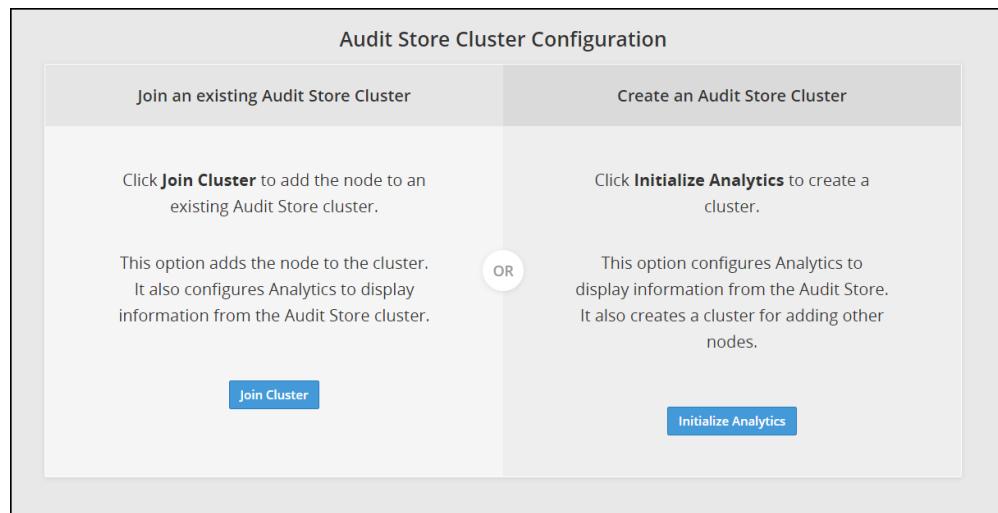


Figure 12-6: Analytics Screen

4. Click **Initialize Analytics**.

Protegility 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.

Protegility 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.

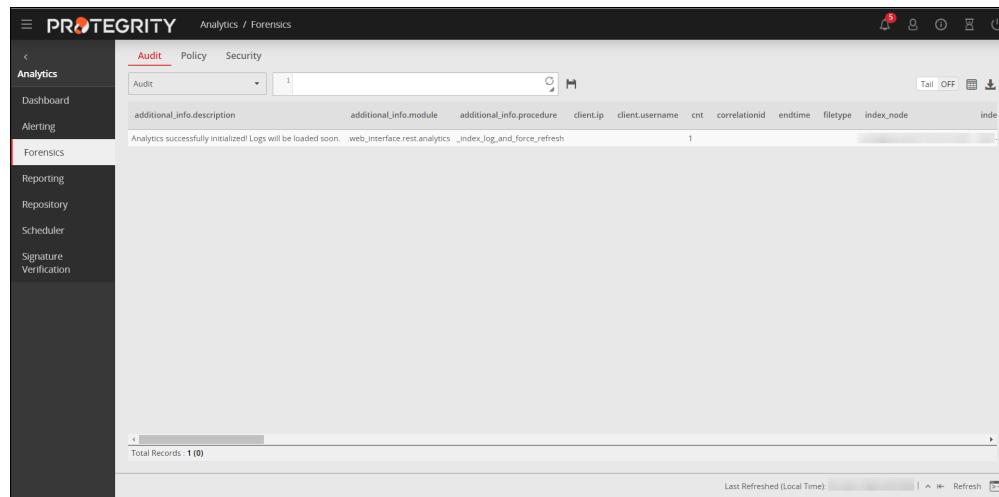


Figure 12-7: Forensics

### 12.2.5.3 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 [Protegility 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.

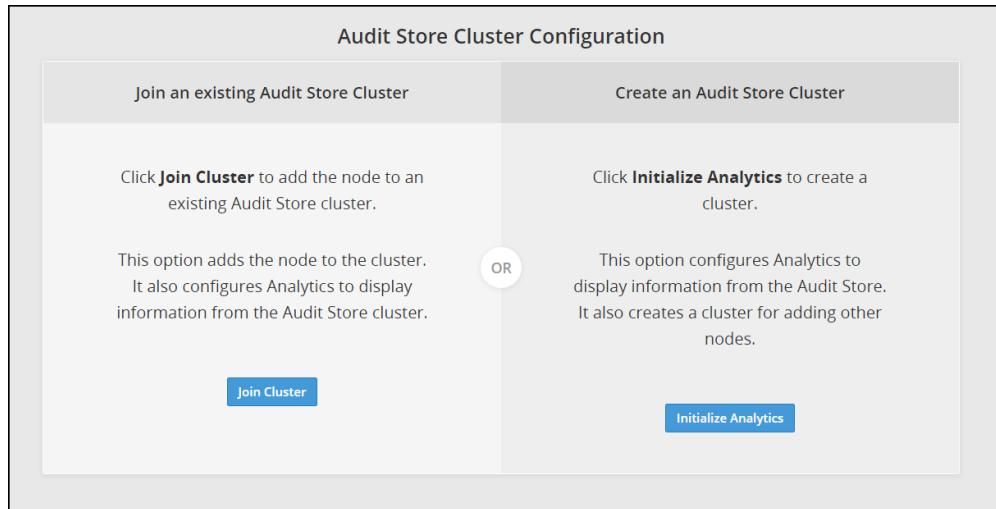


Figure 12-8: Analytics Screen

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 12-9: 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 Protegility Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegility 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.

Protegility 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.

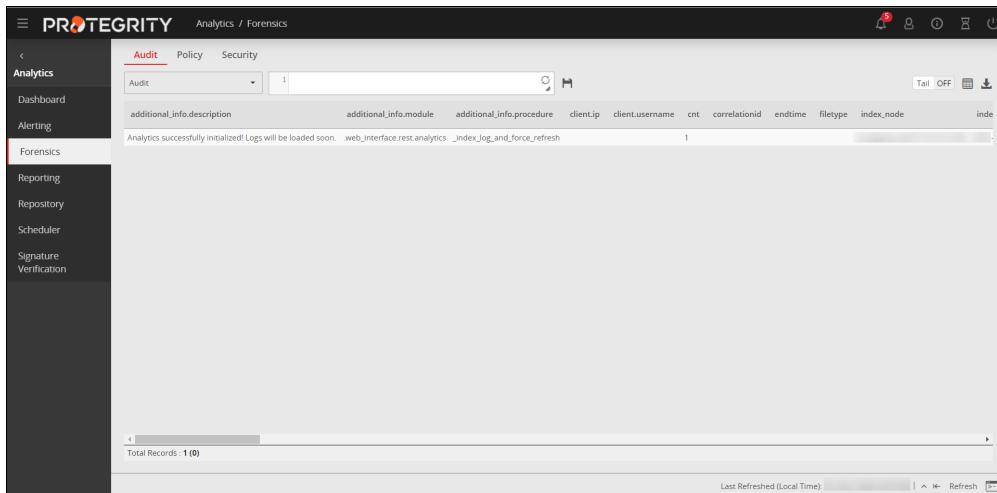


Figure 12-10: Protegility Analytics

#### 12.2.5.4 Adding the Protegility Storage Unit to the Audit Store Cluster

Add the Protegility Storage Unit to the Audit Store Cluster that is initialized on the ESA. You need to specify the IP address of the Audit Store cluster that you want to join with the username and password of the admin user for authorization.

##### Before you begin

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 Web UI of the node, click **Audit Store Management**, and view the **Cluster Status** from the upper-right corner of the screen.

Ensure that the Audit Store services are running on the ESA Web UI by navigating to **System > Services > Audit Store**.

**Note:** 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 PSU Web UI would make the cluster information inconsistent, make the Audit Store cluster unstable, and would lead to errors.

**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 *Protegility Appliances Overview Guide 9.1.0.5*.

##### ► To join the Audit Store cluster:

1. Log in to the Web UI of the Protegility Storage Unit.
2. Open the **Audit Store Management** screen.  
The **Cluster Overview** screen appears.

The screenshot shows the 'Join, View, or Leave Cluster' interface. At the top, it displays the cluster name 'insight'. Below this, there are two tabs: 'Nodes' (selected) and 'Indices'. The 'Nodes' tab provides a summary of cluster metrics: 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, and Indices Count (14). It also shows Total Docs (190,528) and Number of Master Nodes (1), Number of Ingest Nodes (1). The 'Indices' tab is currently inactive. Below the summary, a table lists node details: Node IP, Roles (Master, Data, Ingest), Action (Edit Roles), Name, Up Time, Disk Total (Bytes), Disk Used (Bytes), Disk Avail (Bytes), and RAM. One node entry is shown with a checked 'Master' role.

Figure 12-11: Cluster Overview Screen

### 3. Click Join Cluster.

The **Join Cluster** screen appears.

**Note:** The **Join Cluster** button is disabled if a node is already a part of the Audit Store cluster.

The dialog box is titled 'Join an existing Audit Store Cluster'. It contains three input fields: 'Target node IP/Hostname\*' (Node IP/Hostname), 'Username\*' (Username), and 'Password\*' (Password). Below these fields is a checkbox labeled 'Clear cluster data! This operation will clear data from the node. I have backed up the data and want to continue with this operation.' At the bottom right are two buttons: 'Join Cluster' (blue background) and 'Cancel'.

Figure 12-12: Join Cluster Dialog Box

### 4. Specify the following details for the node that you want to connect.

- **Target node IP/Hostname:** This is the IP address or hostname of the node that you want to connect to.

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

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

For more information about creating an Audit Store cluster, refer to the section *Creating a Local Cluster* in the [Protegility Analytics Guide 9.1.0.5](#).

- **Username:** This is the administrator user name to connect to the target machine. For example, admin.
- **Password:** This is the password for the user.

## 5. Click **Join Cluster**.

**Note:** The **Join Cluster** button in this dialog box is enabled after you specify the required information in all the fields and select the check box.

The Audit Store data on the node is cleared . The node is then added to the Audit Store cluster. The Cluster Overview screen appears with the updated Audit Store cluster information. The **Join Cluster** button is disabled and the **Leave Cluster** button is now enabled.

| Number of Nodes | Number of Data Nodes | Active Primary Shards | Active Shards | Relocating Shards |
|-----------------|----------------------|-----------------------|---------------|-------------------|
| 2               | 2                    | 17                    | 34            | 0                 |

| Initializing Shards | Unassigned Shards | OS Version | Current Master | Indices Count |
|---------------------|-------------------|------------|----------------|---------------|
| 0                   | 0                 | 1.3.0      | [redacted]     | 14            |

| Total Docs | Number of Master Nodes | Number of Ingest Nodes |
|------------|------------------------|------------------------|
| 192,494    | 2                      | 2                      |

**Nodes** [selected] **Indices**

**Details**

| Node IP    | Master | Data | Ingest | Action    | Name       | Up Time | Disk Total (Bytes) | Disk Used (Bytes) | Disk Avail (Bytes) | RAM  |
|------------|--------|------|--------|-----------|------------|---------|--------------------|-------------------|--------------------|------|
| [redacted] | ✓      | ✓    | ✓      | Edit Node | [redacted] | 9h      | 39,502,524,416     | 7,035,338,752     | 32,467,185,664     | 16,6 |
| [redacted] | ✓      | ✓    | ✓      | Edit Node | [redacted] | 3.4m    | 39,502,524,416     | 7,001,763,840     | 32,500,760,576     | 16,6 |

Figure 12-13: Node Added to Cluster

Repeat the steps provided in this section to add the remaining Protegility Storage Units you installed to the Audit Store Cluster. While installing the additional nodes, the target node can be any node in the Audit Store cluster having the *Master* role. It is recommended to use the first initialized node, such as, the Primary ESA, as the target node.

**Note:** To check the role of the node, login to Web UI of the node, click **Audit Store Management**, and view the **Roles** from the **Nodes** tab.

### 12.2.5.5 Refreshing the Audit Store Cluster Settings

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

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

### 12.2.5.6 Configuring td-agent in the Audit Store Cluster

Complete the following steps after adding the Protegility Storage Unit to the Audit Store cluster. This configuration is required for processing and storing the logs received by the Audit Store.

**Note:** This step must be performed on all the ESAs in the Audit Store cluster.

Before performing the steps provided here, verify that the Audit Store cluster health status is green on the **Audit Store Management** screen of the ESA Web UI.

1. Login to the CLI Manager of the *ESA* node.
2. Navigate to **Tools > PLUG - Forward logs to Audit Store**.
3. Enter the root password and select **OK**.
4. Enter the username and password for the administrative user, such as, admin.
5. Select **OK**.
6. In the *Setting ESA Communication* screen, select **OK**.
7. Specify the IP addresses of all the Protegility Storage Unit machines in the cluster, separated by commas.



Figure 12-14: Forward Logs

8. Select **OK**.
9. Type *y* to fetch certificates for communicating with the ESA and select **OK**.

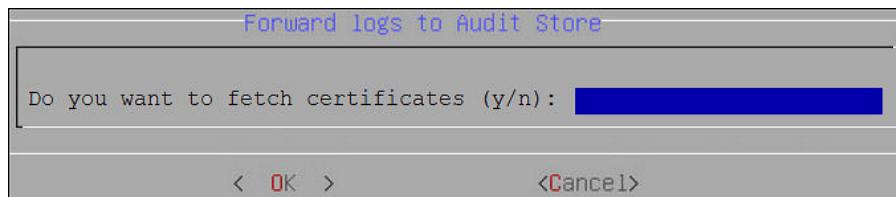


Figure 12-15: Fetch Certificates

10. Enter the admin username and password and select **OK**.

Repeat the steps provided in this section on all the ESAs in the Audit Store Cluster.

### 12.2.5.7 Verifying the Audit Store Cluster

View the Audit Store Management page to verify that the configurations that you performed were completed successfully using the steps provided here.

1. Login to the ESA Web UI.
2. Navigate to the **Audit Store Management** page.
3. Verify that the nodes are added to the cluster. The health of the nodes must be either green or yellow.
4. If you added additional ESAs for creating a TAC, then verify that the ESA has only the master role.

The screenshot shows a cluster named 'insight' with the following statistics:

- Number of Nodes:** 3
- Number of Data Nodes:** 2
- Active Primary Shards:** 17
- Active Shards:** 34
- Relocating Shards:** 0
- Initializing Shards:** 0
- Unassigned Shards:** 0
- OS Version:** 1.3.0
- Current Master:** [redacted]
- Indices Count:** 14
- Total Docs:** 212,995
- Number of Master Nodes:** 3
- Number of Ingest Nodes:** 2

The 'Nodes' tab is selected, showing a table of nodes with their IP addresses, roles (Master, Data, Ingest), and status. One row has three checkmarks in the roles column, which is highlighted with a red box.

| Node IP    | Master | Data | Ingest | Action                     | Name       | Up Time | Disk Total (Bytes) | Disk Used (Bytes) | Disk Avail (Bytes) | RAM  |
|------------|--------|------|--------|----------------------------|------------|---------|--------------------|-------------------|--------------------|------|
| [redacted] | ✓      | ✓    | ✓      | <a href="#">Edit Roles</a> | [redacted] | 19s     | 39,502,524,416     | 6,955,266,048     | 32,547,258,368     | 6,44 |
| [redacted] | ✓      | ✓    | ✓      | <a href="#">Edit Roles</a> | [redacted] | 2.5h    | 39,502,524,416     | 7,021,211,648     | 32,481,312,768     | 16,6 |
| [redacted] | ✓      | ✓    | ✓      | <a href="#">Edit Roles</a> | [redacted] | 4.9m    | 45,709,819,904     | 5,415,325,696     | 40,294,494,208     | 28,3 |

Figure 12-16: Nodes Added to Cluster

## 12.2.6 Migrating DMS Logs and Metering Data

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

If your ESA is a part of the TAC setup, it is recommended to migrate your logs and metering data to Protegility Analytics to avoid data loss during upgrade. This section describes how to upgrade DMS logs and metering data from your current system to Protegility Analytics.

### 12.2.6.1 Metering Data

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

Starting from the ESA version 8.0.0.0, the metering data is displayed on Protegility Analytics. Post the upgrade, you must execute the *Metering Upgrade* script to ensure that the metering data is exported to Protegility Analytics.

The following command must be executed to run the *Metering Upgrade* script from the */etc/init.d* directory.

```
/etc/init.d/dps_meteringupgrade
```

**Note:**

The *Metering Upgrade* service is uninstalled after the execution is complete.

**Note:**

If you have configured an Audit Store cluster, then ensure that the cluster configuration is completed successfully prior to executing the *Metering Upgrade* script.

For more information about configuring an Audit Store cluster, refer to section *Configuring the Audit Store Cluster* in the *Audit Store Guide 8.0.0.0*.

For more information about the metering data displayed on Protegility Analytics, refer to section *Viewing the Metering Information* in the *Protegility Analytics Guide 8.0.0.0*.

## 12.2.6.2 Migrating Logs

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

Migrate the logs from your current system to the Audit Store using the DMS Exporter. The logs are exported from the Postgres database to the Audit Store. Ensure that you import the logs that you require in the Audit Store to Postgres before you migrate the logs. Your existing archives would not be usable till they are exported to the Audit Store.

For more information about using the DMS Exporter, refer to [Appendix C: Migrating Logs Using the DMS Exporter](#).

**Note:**

It is recommended that all the logs are migrated from the current system using the DMS Exporter before performing any protect, unprotect, or reprotect operations.

Verify that the total hard disk space available is as per the following formula:

```
2 x (Total size of the Current used space + Size of the Upgrade patch)
```

For STA and LTA logs, import them back to Postgres before running the DMS Exporter. Ensure that the free space available on your system before importing STA and LTA logs is *2 times the space of the STA logs + LTA logs*. Contact Protegity Services if you need help with migrating your STA and LTA logs.

Complete the following steps to migrate logs to the Audit Store.

1. On the ESA, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegity/dms_exporter` directory.
5. Stop the DMS service using the following command:

```
dms stop
```

6. Run the following command for using the DMS Exporter.

```
python dms_exporter.pyc start
```

**Note:**

Use the command `python dms_exporter.pyc -h` or `python dms_exporter.pyc --help` to view the usage information for the command.

The DMS exporter sends logs in batches, where the exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store. Thus, if you have 4200000 rows, then the DMS Exporter will send rows in eight batches of 500000 rows and the ninth batch of the remaining 200000 rows.

**Note:**

If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the `last_imported_index` file in the `/opt/protegity/dms_exporter` directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics**.

The logs are exported to the Audit Store. Verify that the export was successful by navigating to `/var/log/dms_exporter` on the ESA and viewing the export status in the `dms_exporter.log` file.

Then, the logs can be seen on the **Forensics** tab in Protegility Analytics. These logs can then be used for further analysis.

## 12.2.7 Post Upgrade Steps

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

Ensure that the following steps are performed in the order given here after the upgrade to the ESA 8.0.0.0 is completed:

**Note:**

The export and import feature to migrate data from previous versions of the ESA to the ESA 8.0.0.0 is not supported.

1. Migrate logs
2. Migrate metering data
3. Recreate reports, alerts, and schedule tasks
4. Remove the Reporting server and DMS components

### 12.2.7.1 Recreating Reports, Alerts, and Schedule Tasks

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

The Reporting Server and DMS Components are deprecated in the ESA 8.0.0.0. The rules, events, and alerts that were created in the ESA 7.2.1 are available in the read-only mode after upgrading to the ESA 8.0.0.0. These must be recreated in the ESA 8.0.0.0 using the *Alerting* option in Protegility Analytics. The reports must be recreated after the upgrade to the ESA 8.0.0.0 is completed.

Similarly, the scheduled tasks that were created in the ESA 7.2.1 must be reviewed after upgrading to the ESA version 8.0.0.0. Ensure that the tasks referring to DMS components and Reporting Server in the ESA 7.2.1 are deleted, updated, or recreated in the ESA 8.0.0.0.

**Note:**

The reporting, alerting, and scheduling system in the ESA 8.0.0.0 is different from previous releases of the ESA, do not use the export and import feature to port the data from previous versions of the ESA to the ESA 8.0.0.0.

Create reports, alerts, and scheduled tasks in the ESA 8.0.0.0 using the following information:

- Create the reports that you require using Protegility Analytics.

For more information about creating reports, refer to the section *Working with Reports* in the *Protegility Analytics Guide 8.1.0.0*.

- Create the alerts that you require for monitoring the system using Protegility Analytics.

For more information about creating alerts, refer to the section *Working with Alerts* in the *Protegility Analytics Guide 8.1.0.0*.

- Create the scheduled tasks for automating the regularly performed tasks using Protegility Analytics.



For more information about the scheduler, refer to the section *Using the Scheduler* in the *Protegility Analytics Guide 8.1.0.0*.

### 12.2.7.2 Removing the Reporting Server and DMS Components

**Note:** If you are upgrading to ESA v8.1.0.0, then you must not perform these steps on the ESA v8.0.0.0. You will be performing these steps after the configuration of the ESA v8.1.0.0 upgrade.

The Reporting Server and the DMS Components are deprecated and available in the read-only mode in the ESA 8.0.0.0. Uninstall these services after completing all the upgrade steps to the ESA 8.0.0.0.

**Caution:**

Ensure that you have successfully migrated all the logs and metering data and that you have recreated the reports, alerts, and scheduled tasks that you require in the ESA 8.0.0.0 before uninstalling the services.

Complete the following steps to uninstall the services.

1. Login to the ESA CLI.
2. Navigate to **Administration > Add/Remove Services**.
3. Enter the root password and select **OK**.
4. Select *Remove already installed applications* and select **OK**.
5. Use the **SPACEBAR** to select the **Reporting Server v8.0.0** and the **Logging v8.0.0** products.

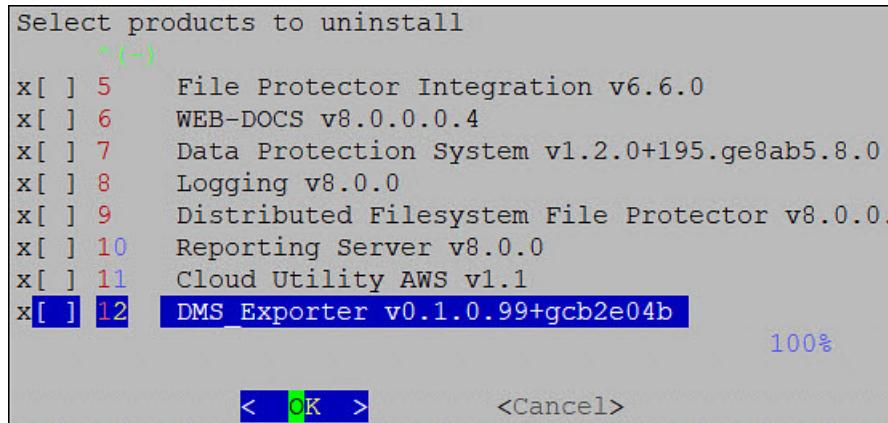


Figure 12-17: Uninstalling Services

6. Select **OK**.

The services are uninstalled and the ESA CLI Manager screen appears.

### 12.2.7.3 Optional: Configuring SMTP for Alerts

If you have alerts configured with the destination type set as **Email**, then you need to configure SMTP on the ESA after the upgrade. Complete the steps provided in this section to configure SMTP.

**Before you begin**

Keep the following information handy before the setup process:

- SMTP server details

- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

**Note:** Ensure that you save the email settings before you exit the Email Setup tool.

For more information about the SMTP tool, refer to the section *Setting Up the Email Server* in the *Protegility Appliances Overview Guide 9.1.0.5*.

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > Email (SMTP) Settings**.  
The Protegility Appliance Email Setup wizard appears.
3. Enter the *root* password and select **OK**.
4. Select **OK**.
5. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.  
For SMTP Server, the default port is **25**.
6. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.  
Protegility Reporting requires a full email address in the Username.
7. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.  
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
8. In the Contact address field, type the email recipient address.
9. In the Host identification field, type the name of the computer hosting the mail server.
10. Select **OK**.  
The tool tests the connectivity and then the next Secured SMTP screen appears.
11. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
12. Select **OK**.
13. Select **Save**.  
A message box appears.
14. Click **EXIT** to save the settings.

## 12.2.8 Restoring to the Previous Version of ESA

If you want to roll back your system to the previous version of the ESA, in cases, such as, upgrade failure, then you can restore it through the OS backup or by importing the backed up files.

### 12.2.8.1 Restoring to the Previous Version of ESA On-premise

If you want to roll back your system to the previous version, in case of an upgrade failure, then you can restore the system.

► To restore the system to the previous version:

1. On the CLI Manager navigate to **Administration > Reboot And Shutdown > Reboot**, to restart your system.  
A screen to enter the reason for restart appears.
2. Enter the reason and select **OK**.

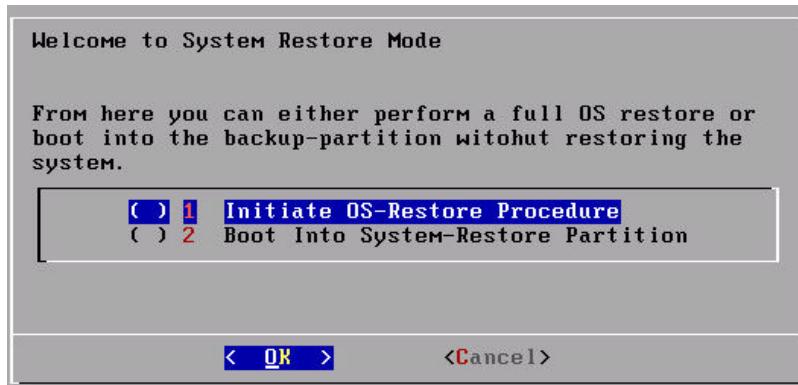
3. Enter the *root* password and select **OK**.

**Note:**

The screen is available for 10 seconds only.

4. Select **System-Restore** and press **ENTER**.

The following screen appears.



5. Select **Initiate OS-Restore Procedure** and select **OK**.

The restore procedure is initiated.

After the OS-Restore procedure is completed, the login screen appears.

### 12.2.8.2 Restoring to the Previous Version of ESA from Snapshot

If you want to roll back your system to the previous version, then you can restore through the backed-up snapshot.

You can restore to the previous version of ESA using a snapshot on the following platforms:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

For more information about creating a snapshot of the respective cloud environments, refer to the section *Installing Protegility Appliances on Cloud Platforms* in the [Protegility Appliances Overview Guide 9.1.0.5](#).

#### 12.2.8.2.1 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

**Note:**

Ensure that the status of the instance is **Stopped**.

**Note:**

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.  
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.  
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

**Note:**

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.  
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.  
The pop-up menu appears.
10. Select **Attach Volume**.  
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter */dev/xvda* in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.  
The snapshot is added to the EC2 instance as a volume.

### 12.2.8.2.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

**Note:** Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.  
The *VM instances* screen appears.
2. Select the required instance.  
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.

7. Enter information in the following text boxes:
  - Name - Name of the snapshot
  - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.  
The instance is updated with the new snapshot.

### 12.2.8.2.3 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

**Note:**

Ensure that the snapshot of the machine is taken.

- To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.  
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.  
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.  
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.  
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

## 12.3 Upgrading Protectors

If you are upgrading the Protectors from v7.2.1 to v8.1.0.0, then ensure that the ESA is at v8.1.0.0.

**Note:**

For more information about the compatible data elements for the different protector versions, refer to the table *Data Element Compatibility Matrix*.

### 12.3.1 Upgrading Application Protector

You must uninstall the earlier version of the Application Protector and install the Application Protector v8.0.0.0.

For more information about installing the Application Protector v8.0.0.0 protector, refer to the section *Installing and Uninstalling Application Protectors* in the [Installation Guide 8.0.0.0](#).

**Note:** The ESA v8.0.0.0 is not compatible with AP Lite, versions 6.6.5 and lower.

### 12.3.2 Upgrading Database Protector

You must uninstall the previous version of the Database Protector and then install the v8.0.0.0 protector.

For more information about installing the v8.0.0.0 protector, refer to the section *Installing and Uninstalling Database Protectors* in the [Installation Guide 8.0.0.0](#).

### 12.3.3 Upgrading Data Security Gateway (DSG)

The Data Security Gateway (DSG) can be upgraded to the DSG v2.5.0.0, which is compatible with the ESA v8.0.0.0. You must apply the patch on the ESA and the DSG nodes to upgrade the DSG version to the required release.

For more information about upgrading the DSG to DSG v2.5.0.0, refer to the section *Upgrading to DSG v2.5.0.0* in the [Data Security Gateway User Guide 2.5.0.0](#).

### 12.3.4 Upgrading Big Data Protector

If you are using Big Data Protector v7.2.1, which was installed using the CDH Native Installer, then you can upgrade to Big Data Protector v8.0.0.0 using the respective Big Data Protector v8.0.0.0 parcels.

**Note:** If you are performing a rolling upgrade of the CDH distribution, then you need to uninstall Big Data Protector before starting the rolling upgrade. After the rolling upgrade of the CDH distribution is completed, you need to install the Big Data Protector version that is compatible with the updated version of the CDH distribution.

**Note:** If you need to upgrade the CDH or HDP distributions, then refer to section *Guidelines for Upgrading CDH and HDP Distributions* in the [Big Data Protector Guide 8.0.0.0](#).

#### 12.3.4.1 Upgrading Big Data Protector using CDH Native Installer

Perform the following steps to upgrade Big Data Protector from v7.2.1 to v8.0.0.0 using the respective parcels for the Big Data Protector v8.0.0.0 release.

**Note:**

Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated.

If you are using HDFSFP with an older version of Big Data Protector and are upgrading to Big Data Protector 8.0.0.0, then ensure that you stop and uninstall the HDFSFP-related services and ensure that you do not add these after Big Data Protector 8.0.0.0 is installed.

**Note:** Ensure that you are logged in as the required user with the relevant privileges for installing Big Data Protector and managing the Cloudera SCM Server.

**Note:** The *cloudera-scm* user is the default user for running the Cloudera management services.

**Note:** This section considers the *cloudera-scm* user as the default user for installing Big Data Protector and running the Cloudera management services.

After receiving the Big Data Protector v8.0.0.0 installation package from Protegity, copy it to any user defined directory on any node that has ESA connectivity.

#### 12.3.4.1.1 Extracting the Big Data Protector Package

You must extract the Big Data Protector package to access the Big Data Protector Configurator script to generate the Big Data Protector parcels and CSDs required for the installation of Big Data Protector on the nodes in the Hadoop cluster, which are managed by Cloudera Manager.

► To extract the files from the installation package:

1. Login to the CLI on the Master node node that has connectivity to the ESA.
2. Copy the Big Data Protector package *BigDataProtector\_Linux-ALL-64\_x86-64\_CDH-6.2-64\_9.1.0.0.x.tgz* to a directory, such as the */opt/bigdata* directory.
3. To extract the *BDPConfigurator\_CDH-6.2\_9.1.0.0.x.sh* file from the Big Data Protector installation package, run the following command.

```
tar -xvf BigDataProtector_Linux-ALL-64_x86-64_CDH-6.2-64_9.1.0.0.x.tgz
```

4. Press ENTER.

The command extracts the *BDPConfigurator\_CDH-6.2\_9.1.0.0.x.sh* file from the Big Data Protector installation package.

#### 12.3.4.1.2 Running the Big Data Protector Configurator Script

You must run the Big Data Protector configurator script to download certificates from the ESA, and create the parcels and CSDs for Big Data Protector.

► To generate the Big Data Protector Parcels and CSDs:

1. Run the *BDPConfigurator\_CDH-6.2\_9.1.0.0.x.sh* script from the directory where it is extracted.

A prompt to continue the configuration of Big Data Protector appears.

```
./BDPConfigurator_CDH-6.2_9.1.0.0.x.sh

Welcome to the Big Data Protector Configurator Wizard

```

```
This will setup the Big Data Protector Installation Files for CDH.
```

```
Do you want to continue? [yes or no]
```

2. To start the configuration of Big Data Protector, type *yes*.

3. Press ENTER.

The prompt to select the type of the installation appears.

```

```

```
Welcome to the Big Data Protector Configurator Wizard
```

```

```

```
This will setup the Big Data Protector Installation Files for CDH.
```

```
Do you want to continue? [yes or no]
```

```
yes
```

```
Big Data Protector Configurator started...
```

```
Unpacking...
```

```
Extracting files...
```

```
Please select the type of Installation files you want to generate?
```

```
[1: Create All] : Creates entire Big Data Protector CSDs and Parcels.
```

```
[2: Update PTY_CERT] : Creates new PTY_CERT parcel with an incremented patch version.
Use this if you have updated the ESA certificates.
```

```
[3: Update PTY_FLUENTBIT_CONF]
: Creates new PTY_FLUENTBIT_CONF parcel with an incremented patch
version.
Use this if you want to set Custom Fluent-Bit configuration
files to
forward logs to an External Audit Store.
```

```
[1, 2 or 3]:
```

4. To create the Big Data Protector parcels and CSDs, type *1*.

5. To update the *PTY\_CERT* parcels with an incremented patch version, type *2*.

For more information about updating the *PTY\_CERT* parcel, refer to section [Updating the Certificates Parcel](#).

6. To update the *PTY\_FLUENTBIT\_CONF* parcel with an incremented patch version, type *3*.

For more information about updating the *PTY\_FLUENTBIT\_CONF* parcel, refer to section [Updating the Fluent Bit Parcel](#).

7. Press ENTER.

The prompt to select the operating system appears.

```
Please select the OS version for Cloudera Manager Parcel.
```

```
This will be used as the OS Distro suffix in the Parcel name.
```

```
[1: el6] : RHEL 6 and clones (CentOS, Scientific Linux, etc)
```

```
[2: el7] : RHEL 7 and clones (CentOS, Scientific Linux, etc)
```

```
[3: sles12] : SuSE Linux Enterprise Server 12.x
```

```
Please enter the no.:
```

8. Depending on the requirements, type *1*, *2*, or *3* to select the operating system version for the Big Data Protector parcels.

9. Press ENTER.

The prompt to enter the ESA Hostname or IP address appears.

```
Please enter the ESA Host or IP Address[]:
```

10. Enter the ESA Hostname or IP address.

11. Press ENTER.

The prompt to enter the listening port for the ESA appears.

```
Enter ESA host listening port [8443]:
```

12. If you want to use the default value of the ESA host listening port, which is *8443*, then press ENTER.
13. If you have configured an external proxy having connectivity with the ESA to download the certificates from the ESA, then enter the external Proxy listening port.
14. Press ENTER.  
The prompt to enter the ESA user name appears.

```
Enter ESA User name :
```

15. Enter the ESA user name.

16. Press ENTER.  
The prompt to enter the password for the ESA appears.

```
Fetching Certificates from ESA....
```

```
Enter host password for user '<username>':
```

17. Enter the ESA administrator password.
18. Press ENTER.

The certificates are downloaded from the ESA and the prompt to create the *PTY\_FLUENTBIT\_CONF* parcel containing the custom Fluent Bit configuration file(s) for an external audit store.

```
Do you want to package any custom Fluent-Bit configuration files for External Audit Store?
[yes] : Create a PTY_FLUENTBIT_CONF parcel containing configuration files to be used
with External Audit Store.
[no] : Skip this step.
```

```
[yes or no] :
```

19. To include the Fluent Bit configuration file(s) for an external audit store, type *yes*

20. Press *ENTER*.

The prompt to enter the directory to store the configuration files for Fluent Bit appears.

```
Do you want to package any custom Fluent-Bit configuration files for External Audit
Store?
[yes] : Create a PTY_FLUENTBIT_CONF parcel containing configuration files to be used
with External Audit Store.
[no] : Skip this step.
[yes or no] : yes
Creation of PTY_FLUENTBIT_CONF parcel is enabled.
Enter the local directory path on this machine that stores the Fluent-Bit configuration
files for External Audit Store:
```

**Note:** The *PTY\_FLUENTBIT\_CONF* parcel is used to package any custom Fluent Bit configuration files that the user provides and can be distributed across CDP nodes through Cloudera Manager. Ensure that you name the custom Fluent Bit configuration file(s) for the external audit store with the *\*.conf* extension.

If you type *no* at the prompt to create the *PTY\_FLUENTBIT\_CONF* parcel, then the installer will skip the creation of the Fluent Bit parcel and proceed to generate the installation files.

```
Do you want to package any custom Fluent-Bit configuration files for External Audit
Store?
```

```
[yes] : Create a PTY_FLUENTBIT_CONF parcel containing configuration files to be used
with External Audit Store.
[no] : Skip this step.
```

```
[yes or no] : no
```

```
Creation of PTY_FLUENTBIT_CONF parcel is skipped.
```

```
Generating Installation files...
```

```
Big Data Protector parcels & CSDs are generated in ./Installation_Files/ directory.
```

**NOTE:**

Copy Big Data Protector CSDs (jars) to Cloudera Manager local csd repository.  
 Copy Big Data Protector parcels (\*.parcel and \*.sha files) to Cloudera Manager local parcel repository.

21. Enter the local directory path that contains the Fluent Bit configuration files.

22. Press *ENTER*.

```
Enter the local directory path on this machine that stores the Fluent-Bit configuration
files for External Audit Store: /root/fluentbit_file_output
```

Generating Installation files...

Big Data Protector parcels & CSDs are generated in ./Installation\_Files/ directory.

**NOTE:**

Copy Big Data Protector CSDs (jars) to Cloudera Manager local csd repository.  
 Copy Big Data Protector parcels (\*.parcel and \*.sha files) to Cloudera Manager local parcel repository.

The following Big Data Protector parcels and CSDs are generated in the *Installation\_Files/* directory:

- *BDP\_PEP-9.1.0.0.x.jar*
- *PTY\_BDP-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel*
- *PTY\_BDP-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel.sha*
- *PTY\_CERT-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel*
- *PTY\_CERT-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel.sha*
- *PTY\_FLUENTBIT\_CONF-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel*
- *PTY\_FLUENTBIT\_CONF-9.1.0.0.x\_CDH6.2.p0-<OS\_Version>.parcel.sha*
- *PTY\_PROXY-9.1.0.0.x.jar*

#### **12.3.4.1.3 Setting up the Big Data Protector Parcels and CSDs**

After the Big Data Protector parcels and CSDs are copied to the respective local Cloudera repository directories, you need to restart the Cloudera SCM server to ensure that Cloudera Manager identifies the new CSD files and display the Big Data Protector services in the Add Services section in Cloudera Manager.

► To set up the Big Data Protector Parcels and CSDs:

1. Copy the Big Data Protector parcels with the *.parcel* extension and respective checksum files with the *.sha* extension to the local parcel repository of Cloudera Manager.

The default local parcel repository for Cloudera Manager is located in the */opt/cloudera/parcel-repo/* directory.

2. Copy the Big Data Protector CSD files with the *.jar* extension to the local CSD repository.

The default local CSD repository for Cloudera Manager is located in the */opt/cloudera/csd/* directory.

3. Navigate to the local parcel repository directory.

**Note:** The local parcel repository is stored in the */opt/cloudera/parcel-repo/* directory.

4. To assign the ownership permissions for the *Cloudera SCM* user to the Protegility Big Data Protector parcels and checksum files, run the following command.

```
chown cloudera-scm:cloudera-scm *
```

5. Press *ENTER*.
6. To set 640 permissions to the parcel files, run the following command.

```
chmod 640 *
```

7. Navigate to the local CSD repository directory.

**Note:** The local CSD repository is located in the `/opt/cloudera/csd` directory.

8. To assign the ownership permissions for the Cloudera SCM user to the Big Data Protector CSD files, run the following command.

```
chown cloudera-scm:cloudera-scm *
```

9. Press *ENTER*.

10. To set 640 permissions to the CSD files, run the following command.

```
chmod 640 *
```

11. To restart the Cloudera SCM server and load the Big Data Protector CSD files in the Cloudera Manager, run the following command.

```
service cloudera-scm-server restart
```

12. Press *ENTER*.

The new parcels in the local parcel repository are detected by Cloudera Manager.

**Note:** You must restart the Cloudera SCM server to ensure that the Big Data Protector services are listed on the **Add Services** screen in Cloudera Manager.

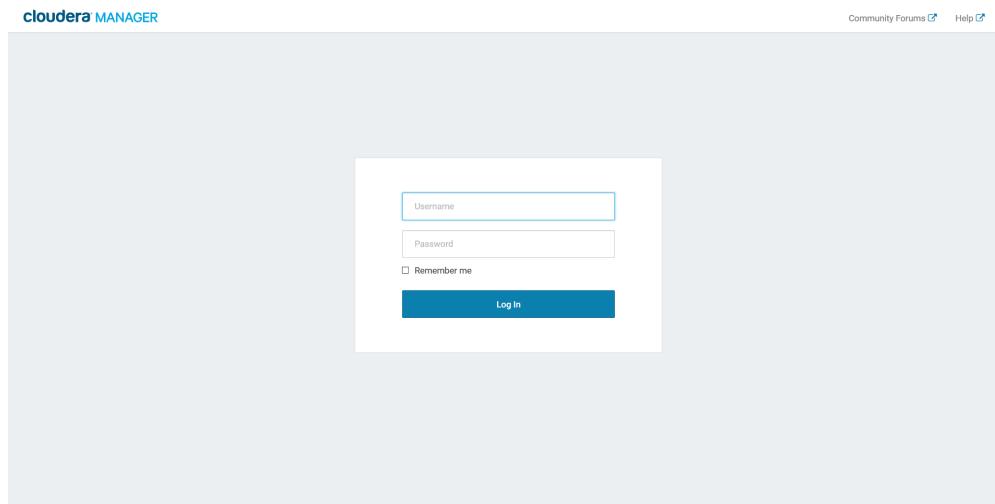
#### 12.3.4.1.4 Distributing Big Data Protector Parcels to the Nodes

You need to distribute the following Big Data Protector parcels to the cluster nodes before installing or activating them on the nodes:

- Big Data Protector parcel: `PTY_BDP`
- Certificates parcel: `PTY_CERT`

► To distribute the Big Data Protector Parcels to the Nodes in the Cluster:

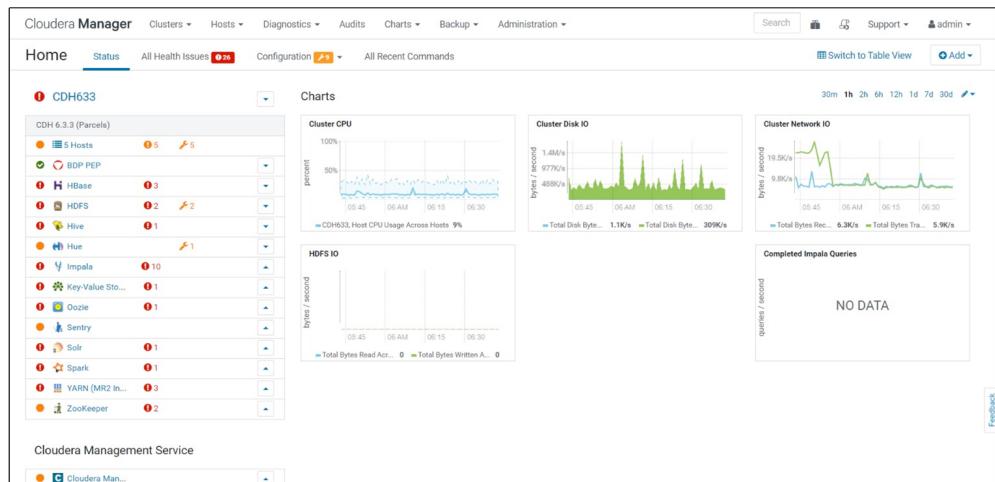
1. Using a browser, navigate to the Cloudera Manager screen.



*Figure 12-18: Cloudera Manager screen*

2. Enter the required user name for logging in to Cloudera Manager.
3. Enter the required password for logging in to Cloudera Manager.
4. Click **Log In**.

The Cloudera Manager Home screen appears.



*Figure 12-19: Cloudera Manager Home screen*

5. Navigate to **Administration > Settings**.

The Settings screen appears.

6. Ensure that the check box beside the *Create Users and Groups, and Apply File Permissions for Parcels* option is selected.



*Figure 12-20: Options on the Settings screen*

7. Click  on the Cloudera Manager screen.

The Cloudera Manager Parcels screen appears listing the Big Data Protector v7.2.1 and v8.0.0.0 parcels.

The screenshot shows the Cloudera Manager interface with the 'Parcels' tab selected. On the left, there are filters for Location (CDH633), Error Status (Error: 1), Parcel Name (PTY\_BDP: 2, PTY\_CERT: 2, SPARK: 13), and Status (Distributed: 3, Other: 13). The main table lists parcels with their versions and statuses. The 'PTY\_BDP' parcel is highlighted with version 7.2.1.1\_CDH6.3.p0 and status Distributed, Activated. Other parcels listed include ACCUMULO, CDH 5, CDH 6, KAFKA, KUDU, PTY\_BDP, PTY\_CERT, SPARK, SQOOP\_NETEZZA\_CONNECTOR, SQOOP\_TERADATA\_CONNECTOR, and mkl.

Figure 12-21: Cloudera Manager Parcels screen

8. Ensure that the following Protegility v8.0.0.0 parcels appear on the Parcels screen.
  - **PTY\_BDP:** Big Data Protector parcel, with version *8.0.0.0.x\_CDH6.x.p0*
  - **PTY\_CERT:** Certificates parcel, with version *8.0.0.0.x\_CDH6.x.p0*

This screenshot shows a subset of the parcels from Figure 12-21, specifically focusing on the PROTEGILITY\_BDP and PROTEGILITY\_CERT parcels. The PROTEGILITY\_BDP parcel is listed with version 7.2.1.1\_CDH6.3.p0 and status Distributed, Activated. The PROTEGILITY\_CERT parcel is also listed with version 7.2.1.1\_CDH6.3.p0 and status Distributed, Activated.

Figure 12-22: Protegility Big Data Protector Parcels for v7.2.1 and v8.0.0.0

9. Click the **Distribute** button beside the *PTY\_BDP* parcel with version *8.0.0.0.x\_CDH6.x.p0*, to distribute the Big Data Protector parcel.
- The distribution of the Big Data Protector parcel starts.

A modal dialog box titled 'Distributing 0% Details' shows the progress of distributing the PROTEGILITY\_BDP parcel. It lists two items: 'PTY\_BDP' (status Downloaded) and '7.2.1.1\_CDH6.3.p0' (status Distributed, Activated). Buttons for 'Cancel' and 'Deactivate' are visible.

Figure 12-23: Distribution of the Big Data Protector Parcel

10. Click the **Distribute** button beside the *PTY\_CERT* parcel with version *8.0.0.0.x\_CDH6.x.p0*, to distribute the Certificates parcel.
- The distribution of the Certificates parcel starts.

A modal dialog box titled 'Distributing 0% Details' shows the progress of distributing the PROTEGILITY\_CERT parcel. It lists two items: 'PTY\_CERT' (status Downloaded) and '7.2.1.1\_CDH6.3.p0' (status Distributed, Activated). Buttons for 'Cancel' and 'Deactivate' are visible.

Figure 12-24: Distribution of the Certificates Parcel

After the Protegility parcels are distributed to the nodes, their status on the Parcels screen is updated to *Distributed* as the parcels are distributed on the nodes.

|          |                     |                        |                             |
|----------|---------------------|------------------------|-----------------------------|
| PTY_BDP  | 8.0.0.0.2_CDH6.3.p0 | Distributed            | <button>Activate</button>   |
|          | 7.2.1.1_CDH6.3.p0   | Distributed, Activated | <button>Deactivate</button> |
| PTY_CERT | 8.0.0.0.2_CDH6.3.p0 | Distributed            | <button>Activate</button>   |
|          | 7.2.1.1_CDH6.3.p0   | Distributed, Activated | <button>Deactivate</button> |

Figure 12-25: Protegility Big Data Protector v8.0.0.0 Parcels Distributed

11. After the Protegility parcels are distributed to the nodes, click *Activate* to activate the Big Data Protector parcels. A dialog box to confirm the activation of the parcel and restart of the dependent services appears.



Figure 12-26: Confirmation Dialog Box for Activating the PTY\_BDP Parcel

You can restart the dependent services later too, but it is recommended to restart the dependent services immediately.

12. Select the *Restart* option to restart the Hadoop services, which are dependent on the parcel that needs to be activated. Alternatively, to just activate the parcel, select the *Activate Only* option.
13. Click **OK** to activate the Big Data Protector parcel.  
Alternatively, to terminate activation, click **Cancel** button.

The Big Data Protector parcel is activated.

14. Click the **Activate** button beside the *PTY\_CERT* parcel to activate the Certificates parcel. A dialog box to confirm the activation of the parcel appears.

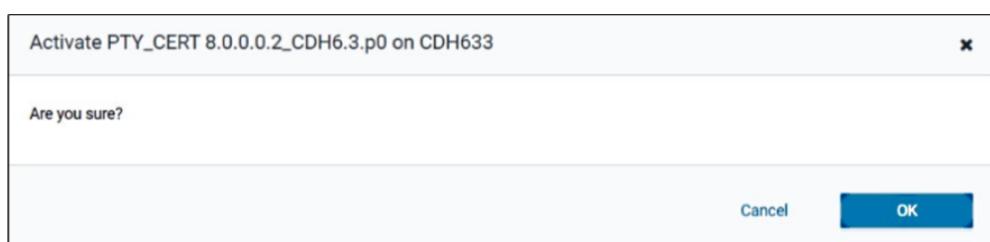


Figure 12-27: Confirmation Dialog Box for Activating the PTY\_CERT Parcel

15. Click **OK** to activate the *PTY\_CERT* parcel.

After the Protegility parcels are activated on the nodes, their status on the Parcels screen is updated to *Distributed, Activated*, and the **Deactivate** button appears.

|          |                     |                        |                             |
|----------|---------------------|------------------------|-----------------------------|
| PTY_BDP  | 8.0.0.0.2_CDH6.3.p0 | Distributed, Activated | <button>Deactivate</button> |
|          | 7.2.1.1_CDH6.3.p0   | Distributed            | <button>Activate</button>   |
| PTY_CERT | 8.0.0.0.2_CDH6.3.p0 | Distributed, Activated | <button>Deactivate</button> |
|          | 7.2.1.1_CDH6.3.p0   | Distributed            | <button>Activate</button>   |

Figure 12-28: Protegility Parcels Activated

16. Remove the Big Data Protector v7.2.1 parcels from all the nodes.

For more information about removing the Big Data Protector v7.2.1 parcels, refer to section *Removing the Big Data Protector Parcels from all Nodes* in the [\*Installation Guide 8.0.0.0\*](#).

17. Delete the Big Data Protector v7.2.1 parcels from the local Cloudera Manager repository.

For more information about deleting the Big Data Protector v7.2.1 parcels, refer to section *Deleting the Big Data Protector Parcels from the Repository* in the [\*Installation Guide 8.0.0.0\*](#).

# Chapter 13

## Appendix A: System Hardware Requirements

### *13.1 Appendix A: System Hardware Requirements*

---

This section describes the hardware requirements for the ESA components.

### 13.1 Appendix A: System Hardware Requirements

The compatibility settings for your products to run smoothly are listed in the following table.

*Table 13-1: Compatibility of Appliances Components*

| Component             | Compatibility                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Protocols | HTTP 1.0, HTTP 1.1, SSL/TLS                                                                                                                                                                                                                                              |
| WebServices           | SOAP 1.1 and WSDL 1.1                                                                                                                                                                                                                                                    |
| Web Browsers          | Minimum version supported for the Web Browser is as follows: <ul style="list-style-type: none"><li>• Google Chrome version 121.0.6167.161 (64-bit)</li><li>• Mozilla Firefox version 122.0.1 (64-bit)</li><li>• Microsoft Edge version 121.0.2277.112 (64-bit)</li></ul> |

The minimum hardware configuration recommended is as follows:

| Hardware Components | Configuration                            |
|---------------------|------------------------------------------|
| CPU                 | Multicore Processor, with minimum 8 CPUs |
| RAM                 | 32 GB                                    |
| Hard Disk           | 320 GB                                   |
| CPU Architecture    | x86                                      |

# Chapter 14

## Appendix B: Protegility Products Compatibility Matrix

This section describes the compatibility matrix between different Protegility products and the data element compatibility based on the different versions of protectors.

The following requirements should be met to work with the Protegility products:

- The version of the ESA must be same or greater than the protectors.
- The ESA must be upgraded, before you upgrade the protectors.
- The data element compatibility must be known, that is, data elements supported by later versions cannot be used with earlier versions of protectors.

For more information about the compatible data elements for the different protector versions, refer to the table [Data Element Compatibility Matrix](#).

The following table shows the supported compatibility between the ESA and the protectors along with the data elements that are compatible with the different protector versions. If you upgrade ESA, then make sure the other Protegility products are compatible with the upgraded version of ESA.

**Note:** The versions listed in the tables below can be fresh installations or upgraded versions. Products listed in tables below are: Application Protector (AP), Big Data Protector (BDP), Database Protector (DBP), File Protector (FP), FPVE Core, FUSE FP, and z/OS Protector (z/OS).

**Note:** The ESA v8.1.0.0 is not compatible with protectors v7.0.

**Note:**

Mainframe current version, 7.0.1 has been supported past the 4 years End of Support (EOS) Policy. Currently there is no version to replace it. For this reason, Protegility offers extended End of Support for it, with no additional charge, to customers until further notice.

Extended support at no additional charge is offered when the product is past the 4-year support life cycle, but the next version is not yet available.

Table 14-1: Data Element Compatibility Matrix

| ESA     | AP      | BDP     | DBP     | FP      | FPVE Core | FUSE FP | z/OS | Supported Data Element Properties |
|---------|---------|---------|---------|---------|-----------|---------|------|-----------------------------------|
| 9.1.0.0 | 9.1.0.0 | 9.1.0.0 | 9.1.0.0 | none    | none      | none    | none |                                   |
|         | 9.0.0.0 | 9.0.0.0 | 9.0.0.0 | 9.0.0.0 | 9.0.0.0   | none    | none |                                   |
|         | 8.1.0.0 | 8.1.0.0 | 8.1.0.0 | 8.1.0.0 | none      | none    | none |                                   |
|         | 8.0.0.0 | 8.0.0.0 | 8.0.0.0 | 8.0.0.0 | none      | 8.0.0.0 | none |                                   |
|         | 7.2.1   | 7.2.1   | 7.2.1   | none    | none      | none    | none |                                   |
|         | 7.2.0   | 7.2.0   | 7.2.0   | none    | 7.2.0     | none    | none |                                   |



| ESA     | AP      | BDP                   | DBP     | FP      | FPVE Core | FUSE FP | z/OS | Supported Data Element Properties                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|---------|-----------------------|---------|---------|-----------|---------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.0.0.0 | 9.0.0.0 | 9.0.0.0               | 9.0.0.0 | 9.0.0.0 | 9.0.0.0   | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|         | 8.1.0.0 | 8.1.0.0               | 8.1.0.0 | 8.1.0.0 | none      | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|         | 8.0.0.0 | 8.0.0.0               | 8.0.0.0 | 8.0.0.0 | none      | 8.0.0.0 | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|         | 7.2.1   | 7.2.1                 | 7.2.1   | none    | none      | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|         | 7.2.0   | 7.2.0                 | 7.2.0   | none    | 7.2.0     | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 8.1.0.0 | 8.1.0.0 | 8.1.0.0               | 8.1.0.0 | 8.1.0.0 | none      | none    | none | The <b>Unicode Base64</b> , <b>Unicode Gen2</b> , <b>Monitor</b> , and <b>Masking</b> data elements are introduced in the release 8.1.0.0. These data elements will not be deployed in protectors older than 8.1.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|         | 8.0.0.0 | 8.0.0.0* <sup>2</sup> | 8.0.0.0 | 8.0.0.0 | none      | 8.0.0.0 | none | <p><b>Note:</b> *<sup>1</sup>The Big Data Protector v7.2 and v8.1.0.0 are available for the CDP-PVC-Base distribution. If you are using Big Data Protector v7.2, which was installed using the CDP-PVC-Base Native Installer, then you can upgrade to Big Data Protector v8.1.0.0 using the respective Big Data Protector v8.1.0.0 parcels.</p> <p><b>Note:</b> *<sup>2</sup>The Big Data Protector v8.0.0.0 is not available for the HDP distribution. If you are using Big Data Protector v7.2.1, which was installed using the HDP Native Installer, then you can upgrade to Big Data Protector v8.1.0.0 using the respective Big Data Protector v8.1.0.0 parcels.</p> |
|         | 7.2.1   | 7.2.1                 | 7.2.1   | none    | none      | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|         | 7.2.0   | 7.2.0* <sup>1</sup>   | 7.2.0   | none    | 7.2.0     | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 8.0.0.0 | 8.0.0.0 | 8.0.0.0               | 8.0.0.0 | 8.0.0.0 | none      | 8.0.0.0 | none | The additional tokenization properties for case-preservation and position-preservation are introduced in the release version 8.0.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|         | 7.2.1   | 7.2.1                 | 7.2.1   | none    | none      | none    | none | The short data tokenization property for the Unicode data elements is available starting from the release version 7.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|         | 7.2.0   | 7.2.0                 | 7.2.0   | none    | 7.2.0     | none    | none |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 7.2.1   | 7.2.1   | 7.2.1                 | 7.2.1   | none    | none      | none    | none | The short data tokenization property for the Unicode data elements is available starting from the release version 7.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|         | 7.2.0   | 7.2.0                 | 7.2.0   | none    | 7.2.0     | none    | none | In the case of FP, the feature of "managing the dfpshell for LDAP users" will not be available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 7.2.0   | 7.2.0   | 7.2.0                 | 7.2.0   | 7.2.0   | 7.2.0     | 7.2.0   | none | In the case of FP, the feature of "managing the dfpshell for LDAP users" will not be available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

The following table describes the compatibility matrix between DSG and ESA.

| DSG                                                                           | Compatible ESA |
|-------------------------------------------------------------------------------|----------------|
| 2.4.0                                                                         | 7.2.1          |
| 2.4.1, 2.4.1 HF-1, 2.4.1 SE-1, 2.4.1 FE-2, 2.4.2                              | 7.2.1          |
| 2.5.0.0                                                                       | 8.0.0.0        |
| 2.6.0.0, 2.6.0.0 HF-1, 2.6.0.0 SE-1, 2.6.0.0 HF-3, 2.6.0.0 SE-2, 2.6.0.0 HF-4 | 8.1.0.0        |
| 2.6.0.1, 2.6.0.1 HF-1, 2.6.0.1 SE-1, 2.6.0.1 HF-2, 2.6.0.1 SE-2, 2.6.0.1 HF-4 | 8.1.0.1        |
| 3.0.0.0, 3.0.0.0 HF-1, 3.0.0.0 HF-2, 3.0.0.0 SE-2, 3.0.0.0 HF-3               | 9.0.0.0        |



| DSG                                                                                                                                                                             | Compatible ESA |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 3.1.0.0, 3.1.0.0 FE-1, 3.1.0.0 HF-1, 3.1.0.0 HF-2, 3.1.0.0 SE-1, 3.1.0.0 FE-2, 3.1.0.0 HF-3, 3.1.0.0 SE-2, 3.1.0.0 HF-4, 3.1.0.0 SE-3, 3.1.0.0 FE-3, 3.1.0.0 SE-4, 3.1.0.0 HF-5 | 9.1.0.0        |
| 3.1.0.1, 3.1.0.1 SE-1, 3.1.0.1 HF-1                                                                                                                                             | 9.1.0.1        |
| 3.1.0.2, 3.1.0.2 HF-1, 3.1.0.2 FE-1, 3.1.0.2 HF-2, 3.1.0.2 HF-3, 3.1.0.2 SE-1, 3.1.0.2 HF-4                                                                                     | 9.1.0.2        |
| 3.1.0.3, 3.1.0.3 HF-1                                                                                                                                                           | 9.1.0.3        |
| 3.1.0.4, 3.1.0.4 HF-2                                                                                                                                                           | 9.1.0.4        |
| 3.1.0.5                                                                                                                                                                         | 9.1.0.5        |

The following table describes the compatibility matrix between the ESA and the container-based protectors.

| ESA     | IAP Java               | REST Container         | Additional Information                                                                                                                                                                                                                                                                       |
|---------|------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.1.0.0 | 9.1.0.0 Gen2           | 9.1.0.0 Gen2           | <b>Important:</b> * <sup>1</sup> If you have generated the policy package using the Immutable Service Export API, then you cannot use the policy with the 7.1 MR4 container-based protectors. However, you can use the Get ESA Policy container to retrieve the policy from the ESA 9.1.0.0. |
|         | 9.0.0.0 Gen2           | 9.0.0.0 Gen2           |                                                                                                                                                                                                                                                                                              |
|         | 7.1 MR4 * <sup>1</sup> | 7.1 MR4 * <sup>1</sup> |                                                                                                                                                                                                                                                                                              |
| 9.0.0.0 | 9.0.0.0 Gen2           | 9.0.0.0 Gen2           | <b>Important:</b> * <sup>1</sup> If you have generated the policy package using the Immutable Service Export API, then you cannot use the policy with the 7.1 MR4 container-based protectors. However, you can use the Get ESA Policy container to retrieve the policy from the ESA 9.0.0.0. |
|         | 7.1 MR4 * <sup>1</sup> | 7.1 MR4 * <sup>1</sup> |                                                                                                                                                                                                                                                                                              |

# Chapter 15

## Appendix C: Migrating Logs Using the DMS Exporter

### [15.1 Verifying the DMS Exporter Installation](#)

### [15.2 Working with the DMS Exporter](#)

In previous releases, logs were processed by the DMS. From the ESA 8.0.0.0, logs are stored in the Audit Store. The DMS Exporter is a utility for upgrading from legacy versions of the ESAs to the ESA 8.1.0.0. The DMS Exporter tool sends logs from the old DMS to the Audit Store. The logs can then be used for analysis, further study, and Forensics in Protegility Analytics.

The DMS Exporter is included as a part of the ESA 8.1.0.0 upgrade patch and is installed in the `/opt/protegility/dms_exporter` directory. The following file is available as part of the DMS Exporter:

- `dms_exporter.py`

The logs are exported from the Postgres database to the Audit Store. Ensure that you import the logs that you require in the Audit Store to Postgres before you migrate the logs. Your existing archives would not be usable until they are exported to the Audit Store.

**Note:** If the number of logs to import is large and it is not feasible to import all your archives to Postgres, then contact Protegility Services for help with migrating your logs.

### 15.1 Verifying the DMS Exporter Installation

Verify that the DMS Exporter provided as part of the ESA 8.1.0.0 upgrade is installed on your system using one of the two steps provided here.

1. Verify that the DMS Exporter is installed from the CLI.
  - a. Login to the ESA CLI Manager as an admin.
  - b. Navigate to **Administration > Patch Management > List installed patches**.
  - c. Verify that the DMS Exporter is present in the list of installed items.
2. Verify that the DMS Exporter is installed from the ESA Web UI.
  - a. Login to the ESA Web UI as an admin.
  - b. Click the **information** icon.
  - c. Click **About**.
  - d. Verify that the DMS Exporter feature is installed.

## 15.2 Working with the DMS Exporter

Use the `dms_exporter` script to start, stop, restart, or view the status of the DMS Exporter. You can run only one instance of the DMS Exporter. You must stop the DMS service before running the DMS Exporter tool.

**Note:** Verify that the total hard disk space available is as per the following formula:

```
2 x (Total size of the Current used space + Size of the Upgrade patch)
```

For STA and LTA logs, import them back to Postgres before running the DMS Exported. Ensure that the free space available on your system before importing STA and LTA logs is *2 times the space of the STA logs + LTA logs*. Contact Protegrity Services if you need help with migrating your STA and LTA logs.

### 15.2.1 Starting the DMS Exporter

Use the `start` switch to start the DMS Exporter. When the DMS Exporter starts, it sends the existing logs to the Audit Store.

1. On the ESA 8.1.0.0, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegrity/dms_exporter` directory.
5. Stop the DMS service using the following command.

```
dms stop
```

6. Run the following command for using the DMS Exporter.

```
python dms_exporter.py start
```

**Note:** Use the command `python dms_exporter.py -h` or `python dms_exporter.py --help` to view the usage information for the command.

The DMS exporter sends logs in batches, where the DMS exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store. Thus, if you have 4200000 rows, then the DMS Exporter will send rows in eight batches of 500000 rows and the ninth batch of the remaining 200000 rows.

**Note:** If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the `last_imported_index` file in the `/opt/protegrity/dms_exporter` directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics**.

The logs are exported to the Audit Store. Verify that the export was successful by navigating to `/var/log/dms_exporter` on the ESA and viewing the export status in the `dms_exporter.log` file.

Then, the logs can be seen on the **Forensics** tab in Protegrity Analytics. These logs can then be used for further analysis.

### 15.2.2 Stopping the DMS Exporter

Use the `stop` switch to stop the DMS Exporter while it is running. This stops the export process from the DMS to the Audit Store. The DMS Exporter saves the ID of the last exported log in the `last_imported_index` file in the `/opt/protegrity/dms_exporter` directory. This file is used when the DMS Exporter tool is run again to continue the export process.



1. On the ESA 8.1.0.0, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegility/dms_exporter` directory.
5. Run the following command to stop the DMS Exporter.

```
python dms_exporter.py stop
```

The DMS Exporter is stopped and the ID of the last exported log is saved in the `last_imported_index` file in the `/opt/protegility/dms_exporter` directory.

**Note:** A `dms_exporter.pid` file is visible in the `/opt/protegility/plug/dms_exporter` directory if the export process crashes or is terminated. This file is automatically removed when the export process completes or is stopped using a `dms_exporter` switch.

### 15.2.3 Viewing the DMS Exporter Status

Use the `status` switch to the view current status of the DMS Exporter.

1. On the ESA 8.1.0.0, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegility/plug/dms_exporter` directory.
5. Run the following command to view the status of the DMS Exporter.

```
python dms_exporter.py status
```

The current status of the DMS Exporter, that is, stopped or running, appears.

### 15.2.4 Restarting the DMS Exporter

Use the `restart` switch to restart the DMS Exporter. The working of the restart switch is similar to the `start` switch. Hence, you need to stop the DMS service before running the DMS Exporter. Restarting, recalculates the end value of the logs to be sent to include fresh logs that might have been generated after the DMS Exporter was last run.

1. On the ESA 8.1.0.0, login to the CLI Manager as the root user.
2. Navigate to **Administrator > OS Console**.
3. Enter the root password and click **OK**.
4. Navigate to the `/opt/protegility/dms_exporter` directory.
5. Stop the DMS service using the following command if the DMS service is running.

```
dms stop
```



- Run the following command for restarting the DMS Exporter.

```
python dms_exporter.pyc restart
```

**Note:** Use the command `python dms_exporter.pyc -h` or `python dms_exporter.pyc --help` to view the usage information for the command.

The DMS exporter continues to send logs in batches, where the DMS exporter queries logs from the current system in batches of 500000 rows and sends 100000 rows at a time to the Audit Store.

The DMS exporter continues sending the logs to the Audit Store. Verify that the export was successful by navigating to `/var/log/dms_exporter` on the ESA and viewing the export status in the `dms_exporter.log` file. You can now use the logs for further analysis in Protegility Analytics.

**Note:** If the DMS Exporter crashes while it is running or stops unexpectedly, then the DMS Exporter enters an inconsistent state. You need to update the `last_imported_index` file in the `/opt/protegility/dms_exporter` directory with the last imported log id and then run the DMS Exporter again. You can obtain the entry for the last log imported from **Analytics > Forensics**.

# Chapter 16

## Appendix D: Analytics Migration Tools

[\*16.1 Migrating Analytics Configuration\*](#)

[\*16.2 Migrating Analytics Audits\*](#)

[\*16.3 Clear Analytics Migration Configuration\*](#)

The Analytics migration tools can be accessed by logging in the ESA or the Protegity Storage Unit CLI and navigating to the **Tools** menu. These tools are used for migrating Analytic data, such as, audit logs and configurations, during the upgrade from version 8.1.0.1 to 9.0.0.0. The following tools are available in the CLI for working with Analytics.

- **Migrate Analytics Configuration**
- **Migrate Analytics Audits**
- **Clear Analytics Migration Configuration**

**Caution:** Running these tools overwrite the configurations from the 8.1.0.1 cluster to the 9.0.0.0 cluster. If you create or customized any of the following features in the 9.0.0.0 cluster and run these tools, you will lose your changes. Ensure that you run these tools before you create or customize the following Analytics features in 9.0.0.0:

- Saved queries in Forensics
- Reports
- Scheduled tasks in Scheduler

### 16.1 Migrating Analytics Configuration

The **Migrate Analytics Configuration** tool is available for migrating Analytic configuration data.

1. Login to the CLI Manager of the destination PSU.
2. Navigate to **Tools**.
3. Run **Migrate Analytics Configuration**.

```
Tools:

Rotate Appliance OS Keys
-- Removable Media Management --
 Disable CD/DVD Drives
 Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Audit Store Tools --
 Rotate Audit Store Certificates
 Apply Audit Store Security Configs
-- Analytics Tools --
 Migrate Analytics Configuration
 Migrate Analytics Audits
 Clear Analytics Migration Configuration

 (c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op

(100%)
```

Figure 16-1: Migrate Analytics Configuration Setting

4. Enter the root password and select **OK**.

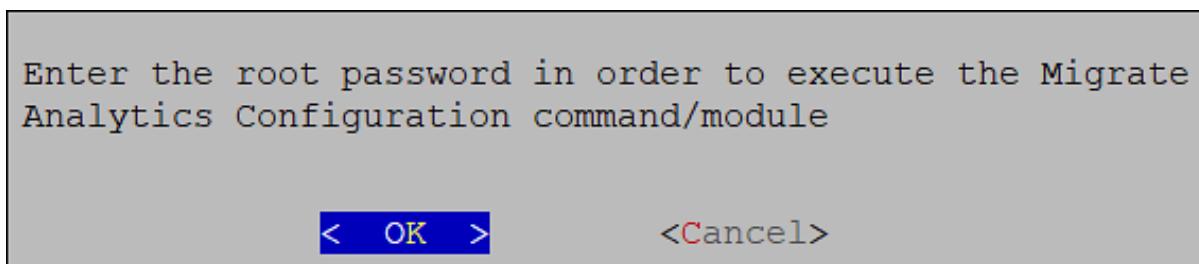


Figure 16-2: Root Password

5. Enter the *admin* username and password and select **OK**.

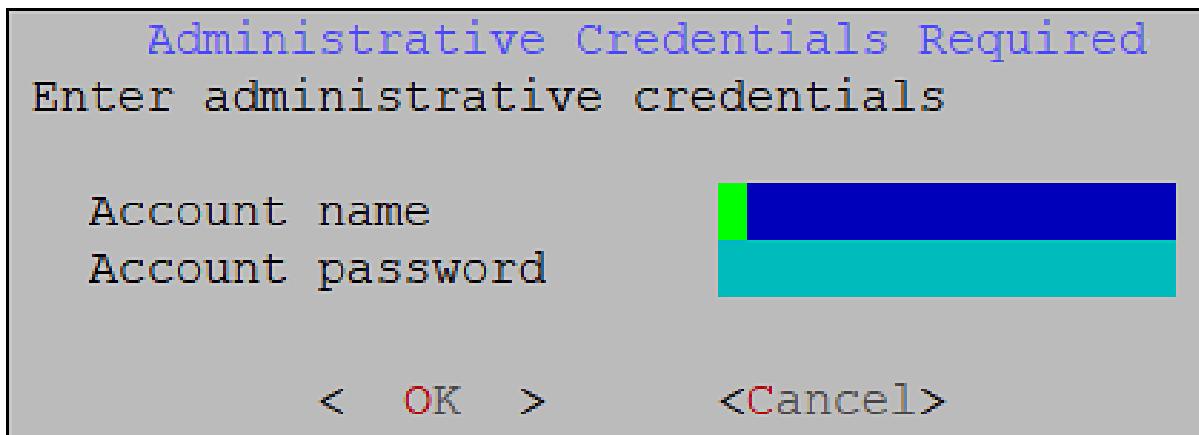


Figure 16-3: Admin Details

6. Enter the address, port, and credentials of the source PSU from where you want to obtain the configurations and select **OK**.

**Note:** Ensure that the pre-patch is installed on the source PSU.

For more information about the pre-patch, refer to [Installing the Pre-Patch on the PSU](#).

- **Source PSU Address:** This is the address of the source PSU where the pre-patch is installed.
- **Source PSU HTTP Port:** This is the port used by the Audit Store on the source PSU for HTTP communication.
- **Administrator Account Username:** This is the username of the administrator account on the source PSU, such as, `admin`.
- **Administrator Account Password:** This is the password of the administrator account on the source PSU.

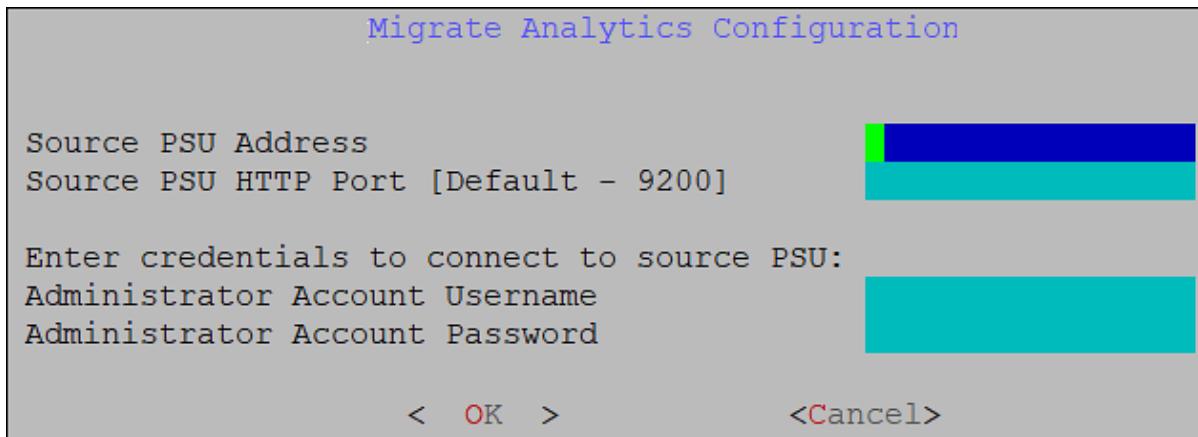


Figure 16-4: Source PSU Details

7. After the migration is completed without errors, the *Migrate Analytics Configuration completed successfully!* message appears. Select **Exit** to go to the CLI menu screen.

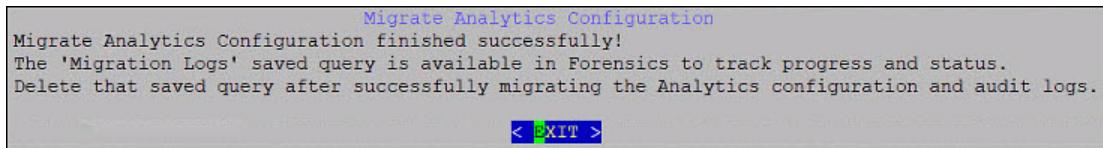
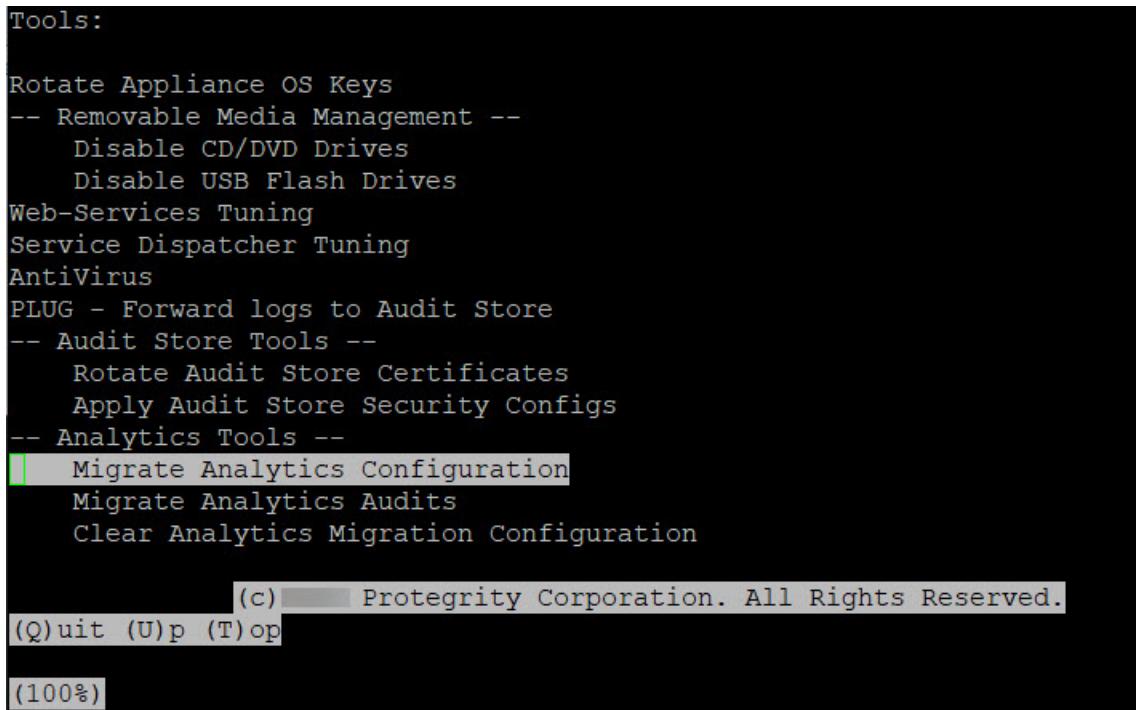


Figure 16-5: Success Message

The CLI screen appears.



```
Tools:
 Rotate Appliance OS Keys
 -- Removable Media Management --
 Disable CD/DVD Drives
 Disable USB Flash Drives
 Web-Services Tuning
 Service Dispatcher Tuning
 AntiVirus
 PLUG - Forward logs to Audit Store
 -- Audit Store Tools --
 Rotate Audit Store Certificates
 Apply Audit Store Security Configs
 -- Analytics Tools --
 Migrate Analytics Configuration
 Migrate Analytics Audits
 Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op
(100%)
```

Figure 16-6: Configurations Migrated

8. The *Migration Logs* saved query is available in Forensics to view the migration logs. You can delete this saved query after successfully migrating the Analytics configuration and audit logs.

For more information about working with saved queries, refer to the section *Working with Saved Queries* in the [Protegility Analytics Guide 9.1.0.5](#).

**Note:** The temporary indexes appear in Forensics with the *\_temp* suffix. These are created by the migration tool and are automatically deleted after running the cleanup tool.

For more information about using the cleanup tool, refer to the section [Clear Analytics Migration Configuration](#).

You can verify that all the logs are migrated by checking the **Total Docs** count on the **Audit Store Management** page of Protegility Analytics.

## 16.2 Migrating Analytics Audits

The **Migrate Analytics Audits** tool is available for migrating Analytic audit logs to version 9.1.0.5.

1. Login to the CLI Manager of the destination PSU.
2. Navigate to **Tools**.
3. Run **Migrate Analytics Audits**.

```

Tools:
 Rotate Appliance OS Keys
 -- Removable Media Management --
 Disable CD/DVD Drives
 Disable USB Flash Drives
 Web-Services Tuning
 Service Dispatcher Tuning
 AntiVirus
 PLUG - Forward logs to Audit Store
 -- Audit Store Tools --
 Rotate Audit Store Certificates
 Apply Audit Store Security Configs
 -- Analytics Tools --
 Migrate Analytics Configuration
 [M] Migrate Analytics Audits
 Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op
(100%)

```

Figure 16-7: Migrate Analytics Audits Setting

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

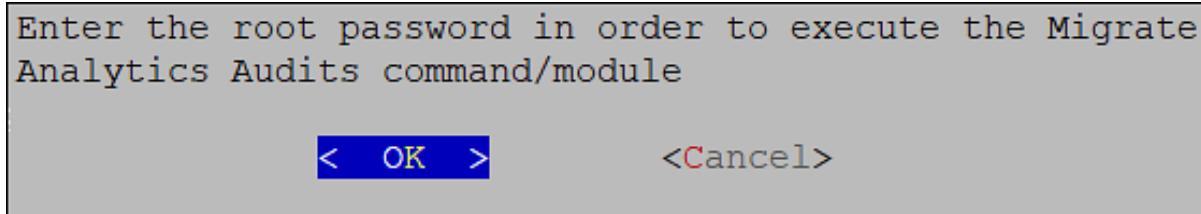


Figure 16-8: Root Password

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

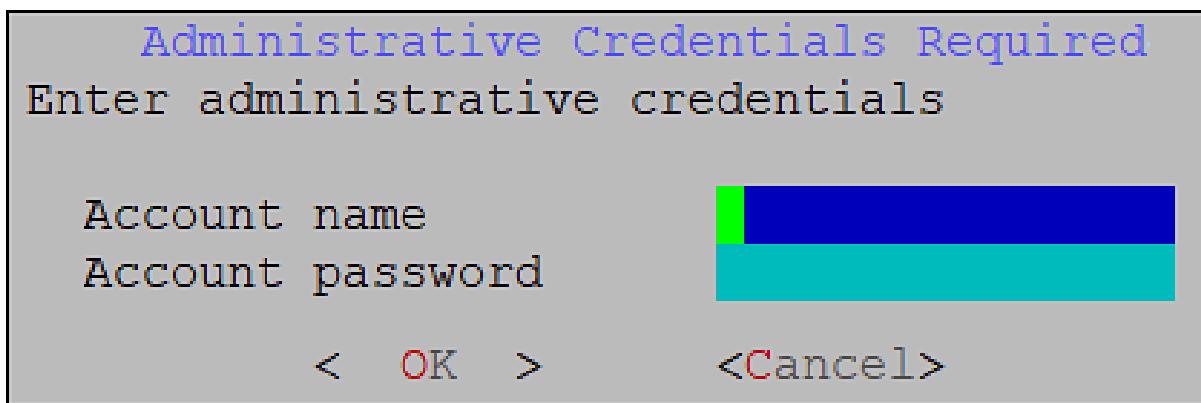


Figure 16-9: Admin Details

- Enter the address, port, and credentials of the source PSU from where you want to obtain the logs and select **OK**.

**Note:** Ensure that the pre-patch is installed on the source PSU.

For more information about the pre-patch, refer to [Installing the Pre-Patch on the PSU](#).

- Source PSU Address:** This is the address of the source PSU where the pre-patch is installed.

- **Source PSU HTTP Port:** This is the port used by the Audit Store on the source PSU for HTTP communication.
- **Administrator Account Username:** This is the username of the administrator account on the source PSU, such as, *admin*.
- **Administrator Account Password:** This is the password of the administrator account on the source PSU.

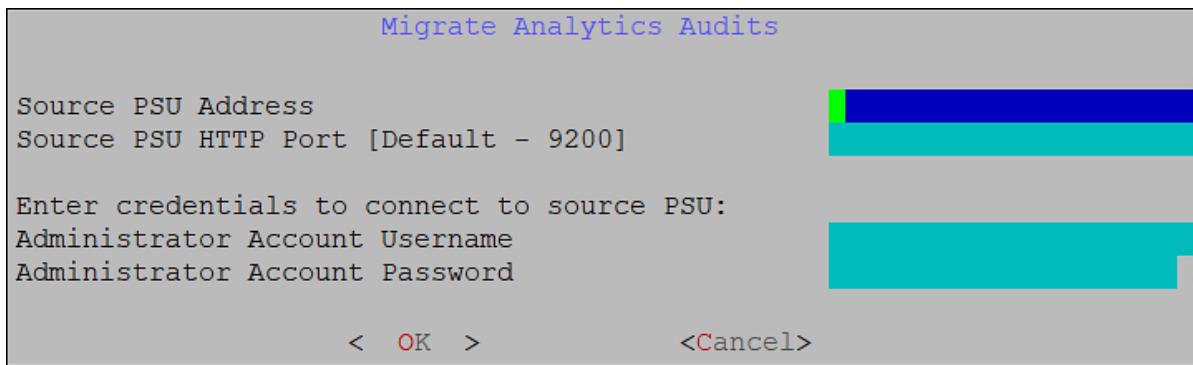


Figure 16-10: Source PSU Details

7. The *Migrate Analytics Audits started successfully!* message appears. The migration process runs in the background. You can view the migration status using the *Migration Logs* saved query in Forensics. Select **Exit** to go to the CLI menu screen. For more information about working with saved queries, refer to the section *Working with Saved Queries* in the *Protegility Analytics Guide 9.1.0.5*.

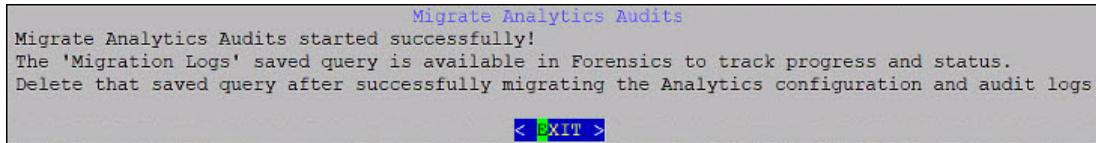


Figure 16-11: Migration Started Message

The CLI screen appears.

```
Tools:

Rotate Appliance OS Keys
-- Removable Media Management --
 Disable CD/DVD Drives
 Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Audit Store Tools --
 Rotate Audit Store Certificates
 Apply Audit Store Security Configs
-- Analytics Tools --
 Migrate Analytics Configuration
 Migrate Analytics Audits
 Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.

(Q)uit (U)p (T)op

(100%)
```

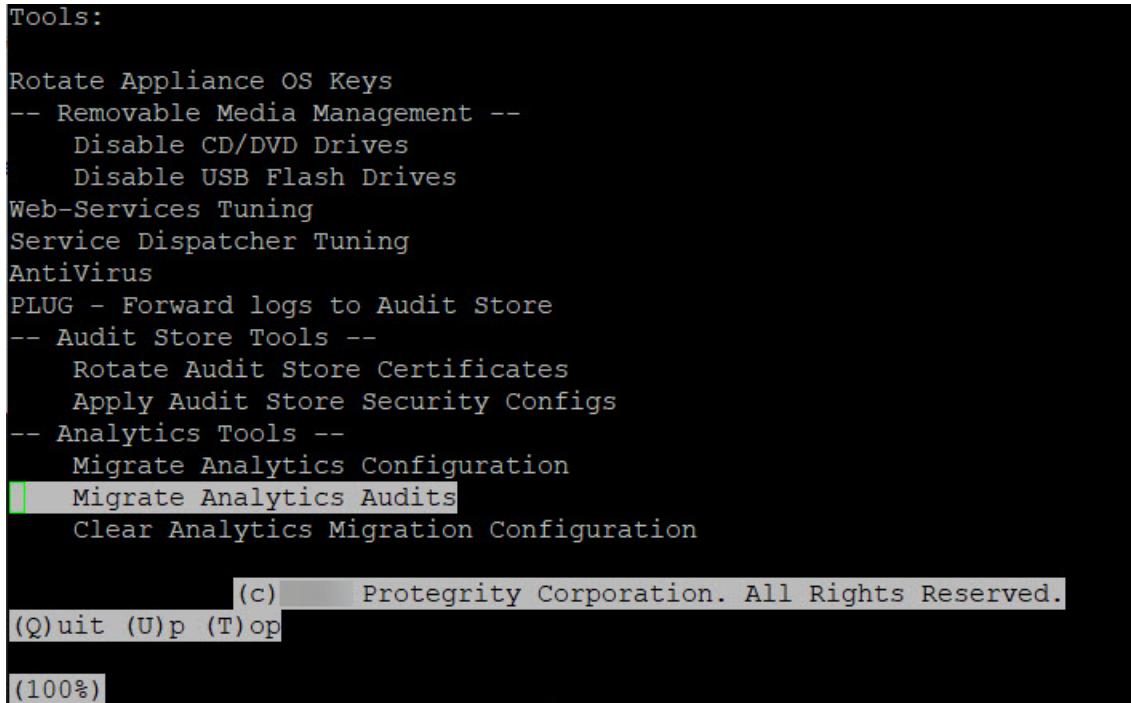
Figure 16-12: Logs Migrated

8. After the migration is completed without errors, the *Migrate Analytics Audits completed successfully!* message appears in the Audit logs.

## 16.2.1 Stopping the Migrate Analytics Audits Tool

The **Migrate Analytics Audits** tool is available for migrating Analytic audit logs to version 9.1.0.5. This migration might take a lot of time if you have a lot of logs that need to migrated. After it is started, the migration tool runs in the background. You can stop the migration tool, if you need to prioritize processing on some task other than migration. Stopping the migration tool pauses the migration activity. The migration can be continued from the last log migrated at a later time by starting the migration tool again.

1. Login to the CLI Manager of the destination PSU.
2. Navigate to **Tools**.
3. Run **Migrate Analytics Audits**.



```
Tools:
Rotate Appliance OS Keys
-- Removable Media Management --
 Disable CD/DVD Drives
 Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Audit Store Tools --
 Rotate Audit Store Certificates
 Apply Audit Store Security Configs
-- Analytics Tools --
 Migrate Analytics Configuration
Migrate Analytics Audits
 Clear Analytics Migration Configuration

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op
(100%)
```

Figure 16-13: Migrate Analytics Audits Setting

4. Enter the root password and select **OK**.

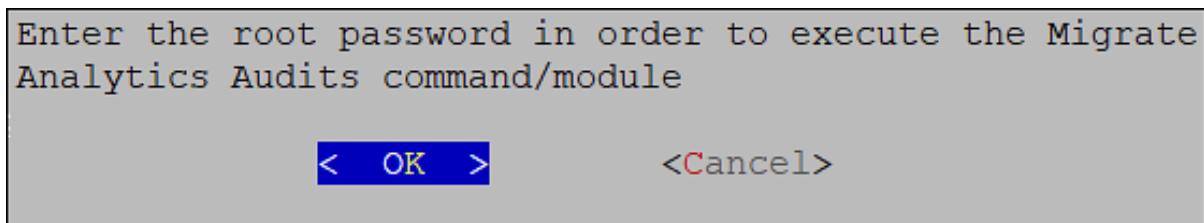


Figure 16-14: Root Password

5. Enter the *admin* username and password and select **OK**.

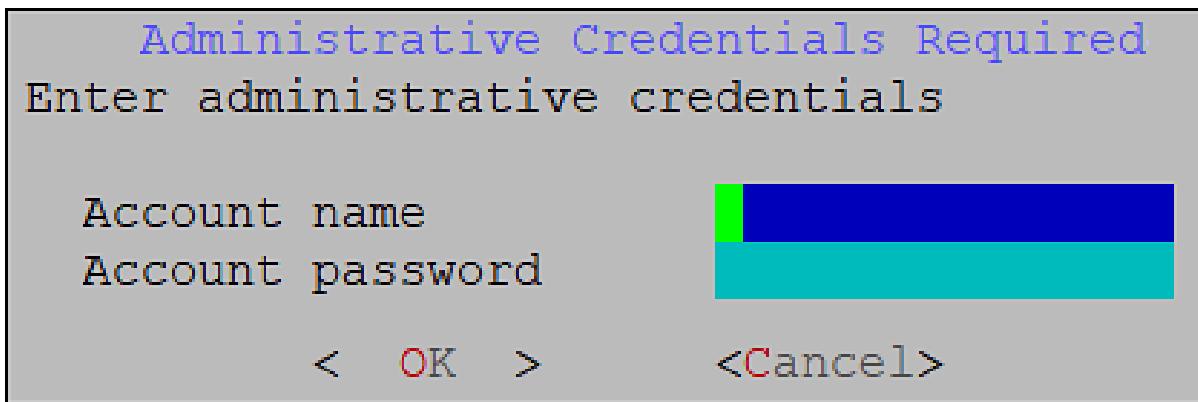
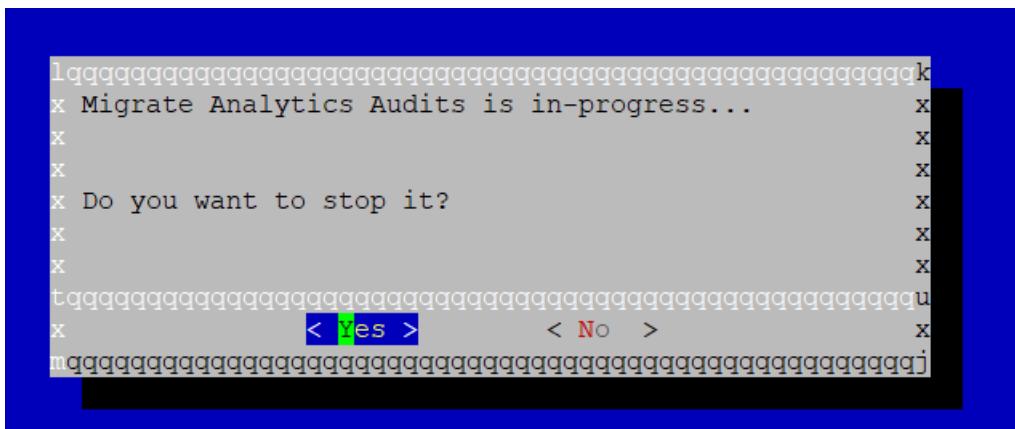
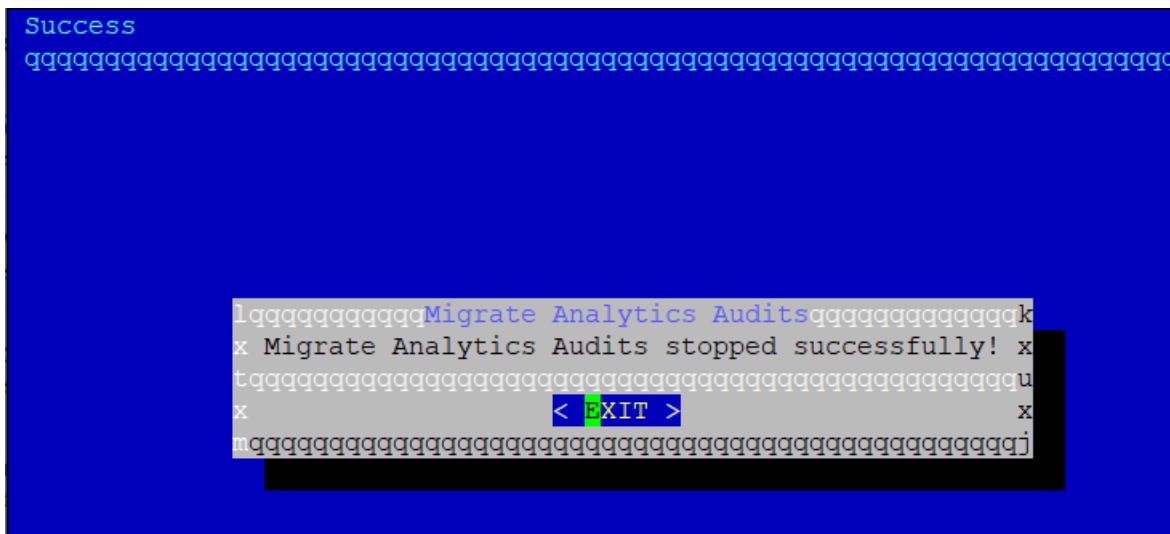


Figure 16-15: Admin Details

6. If the tool is running in the background, then the migration in-progress message appears. Select **Yes** to stop the migration tool.



7. Select **EXIT** to go back to the CLI Manager.



You can run the migration tool again to continue the log migration.

## 16.3 Clear Analytics Migration Configuration

The **Clear Analytics Migration Configuration** tool is available for removing all the temporary indexes and configuration created during the Analytics migration.

1. Login to the CLI Manager of the destination appliance.
2. Navigate to **Tools**.
3. Run **Clear Analytics Migration Configuration**.

**Note:** Ensure that you run this step only after successfully migrating all the configuration and logs.

To verify that the migration is complete, login to the ESA Web UI, navigate to **Analytics > Forensics > Audit > Migration Logs**, and verify that the following messages appear in the logs:

- *Migration of all audit indices from source Audit Store cluster to destination Audit Store cluster is completed.*
- *Migrate Analytics Configuration is completed. The Migration Logs saved query is available in Forensics to track progress and status. Delete that saved query after successfully migrating the Analytics configuration and audit logs.*

Tools:

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

(c) Protegility Corporation. All Rights Reserved.
(Q)uit (U)p (T)op

(100%)
```

Figure 16-16: Clear Analytics Migration Configuration Setting

4. Enter the root password and select **OK**.

Enter the root password in order to execute the Clear Analytics Migration Configuration command/module

< OK > <Cancel>

Figure 16-17: Root Password

5. Enter the *admin* username and password and select **OK**.

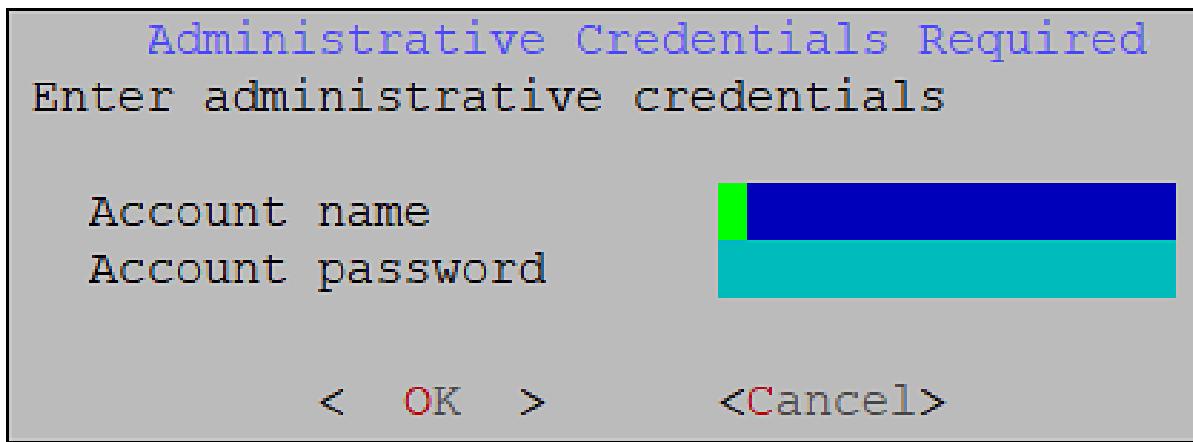


Figure 16-18: Admin Details

6. After the migration cleanup is complete the CLI menu screen appears.

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

 (c) Protegrity Corporation. All Rights Reserved.
(Q)uit (U)p (T)op

(100%)
```

The screenshot shows a terminal window with a black background and white text. It displays a menu of tools and specific configuration options. The option "Clear Analytics Migration Configuration" is highlighted with a green rectangular selection bar. At the bottom, there is copyright information "(c) Protegrity Corporation. All Rights Reserved." and command-line navigation keys "(Q)uit (U)p (T)op". A progress bar at the bottom indicates "(100%)".

Figure 16-19: Clearing Migration Configurations

# Chapter 17

## Appendix E: Optional: Updating settings for External Databases

[17.1 Configuring the External Elasticsearch with Open Distro](#)

[17.2 Upgrading the External Database Schemas](#)

[17.3 Migrating Logs on the External Elasticsearch with Open Distro](#)

Before upgrading, complete the steps in this section that are applicable for your environment. You need to perform these steps to prepare your external database for processing logs.

**Caution:** You must complete these steps only if you have an external database configured with Protegity Analytics. If you are using the PSU for storing logs, then skip the steps provided in this section.

### 17.1 Configuring the External Elasticsearch with Open Distro

If you are using an external Elasticsearch database with Open Distro with Protegity Analytics, then you need to complete the configurations provided here before upgrading the ESA. The configurations provided here must be completed on your external Elasticsearch.

#### Before you begin

Ensure that you take a backup of your Elasticsearch before completing the following steps.

► To configure the external Elasticsearch with Open Distro:

1. Login to the system where the external Elasticsearch with Open Distro is installed.

**Caution:** You must complete these steps only if you have an external Elasticsearch with Open Distro configured with Protegity Analytics, else skip the steps provided in this section.

2. Navigate to the `/usr/share/elasticsearch/plugins/opendistro_security` directory using the following command.

```
cd /usr/share/elasticsearch/plugins/opendistro_security
```

3. Create a copy of the `roles.yml` file.

```
cp roles.yml roles.yml.bkup
```

4. Open the `roles.yml` file.

```
vi roles.yml
```

- Add the code marked in bold to the file.

```

insight_analytics:
 readonly: true
 cluster:
 .
 : <existing configuration>
 .
 # upgrade
 - "indices:admin/template/get"
 - "indices:admin/template/delete"

 .
 : <existing configuration>
 .
 indices:
 'pty_insight_*':
 '*':
 .
 : <existing configuration>
 .
 # misc
 - "indices:monitor/settings/get"
 .
 : <existing configuration>
 .

```

- Save and close the file.

## 17.2 Upgrading the External Database Schemas

A feature enhancement included with the current release includes log ingestion information. When multiple nodes are available in the Audit Store cluster, then any of nodes with the ingest role might process the logs that are received. With this upgrade, the node IP that ingested a log is added to the log message. This makes it easy to identify which node received the log in case there is any issue. Complete the steps in this section to update the database schema to add the additional columns for tracking information about the ingest node.

**Caution:** You must complete these steps only if you have an external Elasticsearch with Protegility Analytics, else skip the steps provided in this section.

- Login to a machine that can access the ESA and the Elasticsearch machine.
- Using a file transfer utility, copy the *ingest-protegility* file. The file is located in the */usr/share/elasticsearch/plugins* directory of the ESA.
- Using a file transfer utility, paste the *ingest-protegility* file in the */usr/share/elasticsearch/plugins* directory of the Elasticsearch machine.
- Restart Elasticsearch.
- Repeat this step on all the Elasticsearch machines in the cluster.

## 17.3 Migrating Logs on the External Elasticsearch with Open Distro

Complete the steps provided here to migrate logs from your External Elasticsearch with Open Distro connected to ESA v8.1.0.1 to the External Elasticsearch with Open Distro connected to ESA v9.0.0.0.

**Caution:** You must complete these steps only if you have an external Elasticsearch with Open Distro and Protegility Analytics, else skip the steps provided in this section.

The External Elasticsearch with Open Distro connected to ESA v9.0.0.0 must be of the version 7.10.2.

1. Preparing the systems for migration.

- a. Login to the CLI Manger of the ESA v8.1.0.1 and navigate to the `/etc/ksa/certificates/ian/` directory.
- b. Copy the `CA.pem`, `client.key`, and `client.pem` certificate files to a system.
- c. Login to the system where the external Elasticsearch 7.10.2 with Open Distro is installed.
- d. Open a command prompt.
- e. Navigate to the `/etc/elasticsearch/` directory.
- f. Create a directory that is named `certmig` in the `elasticsearch` directory.
- g. Copy the certificate files from your system to the `/etc/elasticsearch/certmig` directory that you created.
- h. From the `/etc/elasticsearch/` directory, open the `elasticsearch.yml` file.
- i. Add the following code in the `elasticsearch.yml` file.

```
reindex.remote.whitelist: "<IP_of_Elasticsearch_6.8.1>:9200"
reindex.ssl.certificateAuthorities: /etc/elasticsearch/certmig/CA.pem
reindex.ssl.certificate: /etc/elasticsearch/certmig/client.pem
reindex.ssl.key: /etc/elasticsearch/certmig/client.key
```

- j. Save and close the file.
- k. Login to the CLI Manger of the ESA v9.0.0.0 and navigate to the `/etc/elasticsearch/` directory.
- l. Create a directory that is named `certmig` in the `elasticsearch` directory.
- m. Copy the certificate files from your system to the `/etc/elasticsearch/certmig` directory that you created.
- n. Restart the `Elasticsearch` service on the system where the Elasticsearch 7.10.2 with Open Distro is installed.

2. Migrate the configuration to the Elasticsearch 7.10.2 with Open Distro using the following steps.

- a. Login to the CLI Manager of the ESA v9.0.0.0.
- b. Navigate to **Tools**.
- c. Run **Migrate Analytics Configuration**.

For more information about the *Migrate Analytics Configuration* tool, refer to the section [Migrating Analytics Configuration](#).

- d. Enter the root password and select **OK**.
- e. Enter the `admin` username and password and select **OK**.
- f. Enter the IP address of the Elasticsearch 6.8.1 with Open Distro, the port as `9200`, and select **OK**.

**Note:** Leave the credential fields empty.

3. Migrate the logs to the Elasticsearch 7.10.2 with Open Distro using the following steps.

- a. Login to the CLI Manager of the ESA v9.0.0.0.
- b. Navigate to **Tools**.
- c. Run **Migrate Analytics Audits**.

For more information about the *Migrate Analytics Audits* tool, refer to the section [Migrating Analytics Audits](#).

- d. Enter the root password and select **OK**.
- e. Enter the `admin` username and password and select **OK**.
- f. Enter the IP address of the Elasticsearch 6.8.1 with Open Distro, the port as `9200`, and select **OK**.

**Note:** Leave the credential fields empty.

4. Remove all the temporary indexes and configuration created during the migration using the following steps.

- Note:** Ensure that you run this step only after successfully migrating all the configuration and logs.

- a. Login to the CLI Manager of the ESA v9.0.0.0.
- b. Navigate to **Tools**.
- c. Run **Clear Analytics Migration Configuration**.

For more information about the *Clear Analytics Migration Configuration* tool, refer to the section [\*Clear Analytics Migration Configuration\*](#).

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

After the migration cleanup is complete the CLI menu screen appears.