Protegrity Troubleshooting Guide 9.2.0.0

Created on: Aug 8, 2024

Copyright

Table of Contents

Chapter 1

Introduction to this Guide

This guide provides a first-level support to Protegrity customers. It includes a description of error codes that you may encounter while working with different Protegrity products.

This Guide is intended to make the communication with Protegrity support effective and quick. It instructs you how to collect and analyse the necessary information in case of system errors.

The Guide also answers the most frequently asked questions. It includes references to the other Protegrity user guides which may answer the questions you have.

1.1 Sections contained in this Guide

The guide is broadly divided into the following sections:

> **Note:** The File Protector is certified for version 6.6.4.

- Section *Introduction to this Guide* defines the purpose and scope for this guide. In addition, it explains how information is organized in this guide.
- Section *Customer Support* describes how you can access Protegrity Support and what information you need to collect before contacting support.
- Section *Logging Level Configuration* provides information about the logging level configuration of each Policy Management DPS Server.
- Section *HDFSFP Logging Level Configuration* describes the logging level configuration for HDFSFP.
- Section *Protegrity Products Error Handling* explains the common errors and problems users might encounter while working with Protegrity products.
- Section *Troubleshooting of Special Environments* provides information about the common cluster related issues that you may face.
- Section *Renewing Certificates in the ESA v8.1.0.0 for 6.6.x Protectors* provides you with the steps to recreate certificates to ensure the backward compatibility of the ESA v8.0.0.0 with the v6.6.x protectors using the renewed certificates.
- Section *Resetting Administrator Password* provides information to reset the administrator password.
- Section *Special Utilities* provides information about the special utilities that are provided with Protegrity products.
- Section *Frequently Asked Questions* provides answers for the common questions that users might have while working with Protegrity products.

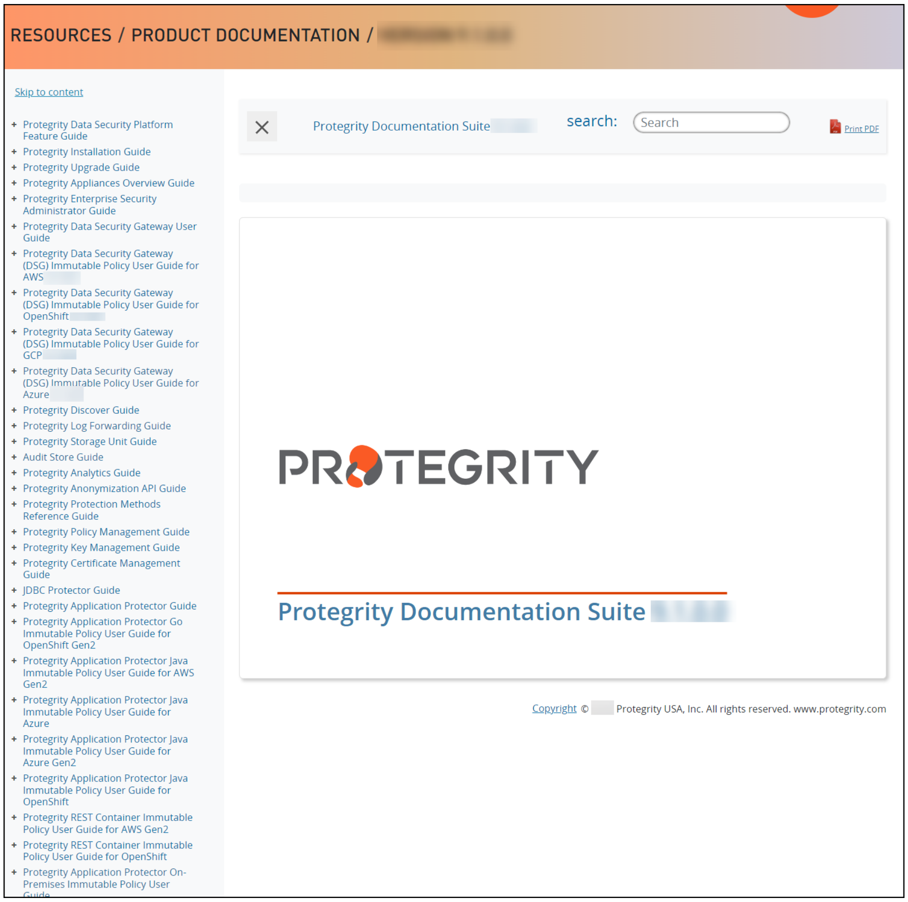
1.2 Accessing the Protegrity documentation suite

This section describes the methods to access the *Protegrity Documentation Suite* using the *My.Protegrity* portal.

1.2.1 Viewing product documentation

The **Product Documentation** section under **Resources** is a repository for Protegrity 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.Protegrity* portal.
2. Click **Resources** > **Product Documentation**.
3. Click a product version.
   The documentation appears.



RESOURCES / PRODUCT DOCUMENTATION /

Skip to content

- + Protegrity Data Security Platform Feature Guide
- + Protegrity Installation Guide
- + Protegrity Upgrade Guide
- + Protegrity Appliances Overview Guide
- + Protegrity Enterprise Security Administrator Guide
- + Protegrity Data Security Gateway User Guide
- + Protegrity Data Security Gateway (DSG) Immutable Policy User Guide for AWS
- + Protegrity Data Security Gateway (DSG) Immutable Policy User Guide for OpenShift
- + Protegrity Data Security Gateway (DSG) Immutable Policy User Guide for GCP
- + Protegrity Data Security Gateway (DSG) Immutable Policy User Guide for Azure
- + Protegrity Discover Guide
- + Protegrity Log Forwarding Guide
- + Protegrity Storage Unit Guide
- + Audit Store Guide
- + Protegrity Analytics Guide
- + Protegrity Anonymization API Guide
- + Protegrity Protection Methods Reference Guide
- + Protegrity Policy Management Guide
- + Protegrity Key Management Guide
- + Protegrity Certificate Management Guide
- + JDBC Protector Guide
- + Protegrity Application Protector Guide
- + Protegrity Application Protector Go Immutable Policy User Guide for OpenShift Gen2
- + Protegrity Application Protector Java Immutable Policy User Guide for AWS Gen2
- + Protegrity Application Protector Java Immutable Policy User Guide for Azure
- + Protegrity Application Protector Java Immutable Policy User Guide for Azure Gen2
- + Protegrity Application Protector Java Immutable Policy User Guide for OpenShift
- + Protegrity REST Container Immutable Policy User Guide for AWS Gen2
- + Protegrity REST Container Immutable Policy User Guide for OpenShift
- + Protegrity Application Protector On-Premises Immutable Policy User Guide

Protegrity Documentation Suite
search:
Search
Print PDF
PROTEGRITY
Protegrity Documentation Suite

Copyright © Protegrity USA, Inc. All rights reserved. www.protegrity.com

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.Protegrity* 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 Protegrity 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

Customer Support

The purpose of Protegrity Customer Support is to provide the technical resources required for successful usage of our software products.

This section explains how you can access Protegrity Support and what information you need to collect before contacting support.

2.1 Access Protegrity Support

You may access Protegrity support services in several ways:

Support Type	
Telephone	+1.203.326.7200 Option 2
Internet	*http://www.protegrity.com* • Using Customer Portal • Through live chat
E-mail	*support@protegrity.com*

Preferred communication methods are accessing Customer Portal and live chat.

2.1.1 Accessing Protegrity Support via Live Chat

➤ To access Protegrity Support via Live Chat:

1. Using your browser (Chrome, Internet Explorer, or Mozilla), enter *http://www.protegrity.com* into the address bar.
2. Select **Customer Support** on the top of the Web page (refer to *Figure 2-1 Customer Support tab*).

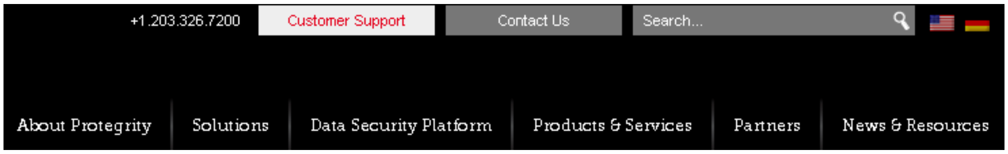


Figure 2-1: Customer Support tab

3. In the page that displays, select **Chat Online**. The Protegrity chat dialog opens in the right bottom corner of the screen (refer to *Live Chat dialog box*).

Jovany E.

Thank you for contacting us. How may I help you?.

Figure 2-2: Live Chat dialog box

2.2 Information Required from Customers

It is always advisable to keep the following information handy before you contact Protegrity support.

> **Note:** The File Protector (FP) is certified for version 6.6.5.

Table 2-1: Handy Information for Protegrity Support

	Before contacting Protegrity support, answer the following questions:
1.	Define the problem severity. Select one of the following: Crash situation Critical Medium Minor
2.	What version of Enterprise Security Administrator (ESA) are you using? Provide the exact version name and release number. My ESA is of the following version x.x.x.xxxx .
3.	What kind of Protector are you using? Database Protector Application Protector File Protector Row Level Protector Big Data Protector
4.	What are the exact names of Protectors packages? What are the exact names for: Operating System and bit level? x.x.x.x ___________ 32bit 64bit 86bit Database? x.x.x.x ____________ Type of Application protector? x.x.x.x ___________ Product versions? x.x.x.x ___________
5.	Are you using any specific environments for your Protegrity appliance? If yes, then review the following environments, and select the appropriate check box. Xen Server MS HyperV HP Dell for ESA? Xen Server MS HyperV HP Dell for DSG?

	Before contacting Protegrity support, answer the following questions:
6.	Are you using High Availability for your Protegrity appliance? Active-Passive Node environment for ESA?
7.	Are you using a clustered environment for ESA or other Protegrity appliances? ESA cluster Number of nodes ____ DSG cluster Number of nodes ____
8.	Provide all products logs with related error messages.
9.	Provide samples of SQL queries or API calls, resulting in errors.
10.	Provide any other information describing a problem.
11.	Explain the business impact of the problem.
12.	Provide information for two persons who can be contacted: a primary contact and an alternative contact, if any: Name and Surname Job position Email Personal mobile phone/office telephone Skype
13.	Provide your communication preference information.

2.2.1 FUSE FP Customer Required Information

If you have an error situation while using your FUSE FP, then before contacting Protegrity Technical Support, you need to collect system information. FUSE FP provides a script that will gather the necessary system information and output the result as a log file.

The script will gather the following information:

- Current date time
- Booting information
- System name
- Kernel version
- Machine model
- Memory statistics
- Volume/disk/cluster statistics
- Mounted file systems
- Loaded kernel modules
- Running processes list
- Installed software packages
- Installed database information
- SELinux Configuration

The following table explains how to run the gather script on Windows and Linux, and where the output log file will be saved:

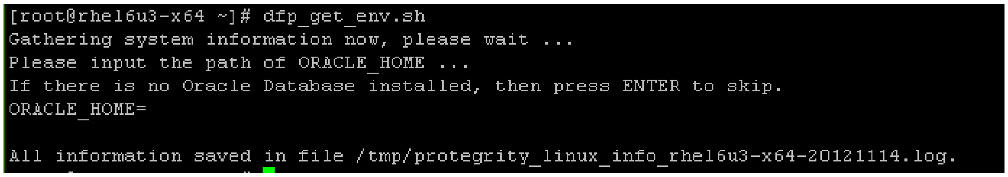
Platform	Gather Script Location	Output Log File
Windows	*C:\Program: Files\Protegrity\Defiance File Protector\bin\dfp_get_env.bat*	*C:\Program Files\Protegrity\Defiance File Protector\bin\systeminformation.txt*
Linux	*/opt/protegrity/fileprotector/bin/dfp_get_env.sh*	Location of the mount point log files */opt/protegrity/fileprotector/fuse/data* Location of the FUSE FP log files: */var/protegrity/dfplogd/log* Location of the system logs(dmesg and message): */var/log/* */tmp* The file name includes platform information and current date.

The following table depicts the location of the FUSE FP log, mount log, and system log files:

Table 2-2: Location of the FUSE FP Log, Mount Log, and System Log Files

Protector	Location of the FUSE FP log files	Location of the mount point log files	Location of the system logs
FUSE FP	*/opt/protegrity/fileprote ctor/fuse/data*	*/var/protegrity/dfplogd/log*	*/var/log/*

When running the gather script on Linux with Oracle Database installed, enter the ORACLE_HOME path:



```
[root@rhel6u3-x64 ~]# dfp_get_env.sh
Gathering system information now, please wait ...
Please input the path of ORACLE_HOME ...
If there is no Oracle Database installed, then press ENTER to skip.
ORACLE_HOME=

All information saved in file /tmp/protegrity_linux_info_rhel6u3-x64-20121114.log.
```

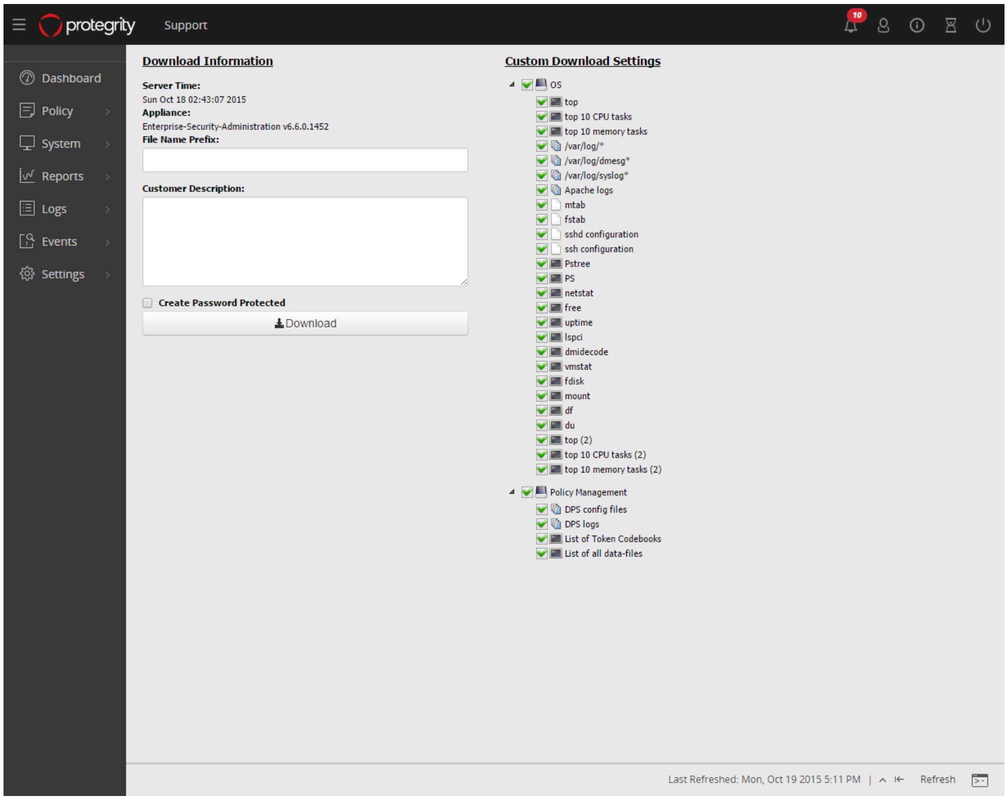
For FUSE FP, run the ***dfpshell dfpadmin status*** command to display the following information on terminal.

- Product components information
- Available policies
- FUSE FP license status
- Service information
- The file encryption krotate list

2.2.2 Downloaded Files and Product Logs

Many times, you are required by Protegrity Services to provide files and product logs to help with troubleshooting. To help you provide the correct information, go to the ESA Web interface, **Help icon (i)** > **Support**. You can select the files to download, zip the files, and send in an email to Protegrity. For more information, refer to *Protegrity Appliance Overview Guide*.

If you are unable to download the support files when you click **Download**, then click **Refresh**. You can then click Download to download the support files.



Download Information

Server Time:
Sun Oct 18 02:43:07 2015
Appliance:
Enterprise-Security-Administration v6.6.0.1452
File Name Prefix:

Customer Description:

□ Create Password Protected

Custom Download Settings

- ☑ OS
  - ☑ top
  - ☑ top 10 CPU tasks
  - ☑ top 10 memory tasks
  - ☑ /var/log/*
  - ☑ /var/log/dmesg*
  - ☑ /var/log/syslog*
  - ☑ Apache logs
  - ☑ mtab
  - ☑ fstab
  - ☑ sshd configuration
  - ☑ ssh configuration
  - ☑ Pstree
  - ☑ PS
  - ☑ netstat
  - ☑ free
  - ☑ uptime
  - ☑ lspci
  - ☑ dmidecode
  - ☑ vmstat
  - ☑ fdisk
  - ☑ mount
  - ☑ df
  - ☑ du
  - ☑ top (2)
  - ☑ top 10 CPU tasks (2)
  - ☑ top 10 memory tasks (2)
- ☑ Policy Management
  - ☑ DPS config files
  - ☑ DPS logs
  - ☑ List of Token Codebooks
  - ☑ List of all data-files

Figure 2-3: Support Page for Customers in Protegrity Appliance

Chapter 3

Logging Level Configuration

3.1 PEP Server Logging Level

PEP Server logging level is defined in *pepserver.cfg* file which is available on the machine where PEP Server is installed.

To configure the most detailed logging level for PEP Server:

1. Open for editing *pepserver.cfg* file. Change the default logging level *WARNING* to *ALL*.

    ```
    [logging]
    # level must be set to one of: OFF - No logging, SEVERE, WARNING, INFO, CONFIG, ALL
    level = ALL
    ```

2. Save the file and restart the PEP Server.

Chapter 4

HDFSFP Logging Level Configuration

Note:

Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated. The HDFSFP-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.

4.1 DFS Cache Refresh Logging Level Configuration

The logging level configuration for the DFS Cache Refresh service is defined in its configuration file *dfscacherefresh.cfg*, which can be viewed and edited from the ESA Web UI at **Settings** > **System** under the **Distributed Filesystem File Protector - Configuration Files** section.

Note: The File Protector is certified for version 6.6.4.

If you need to change the logging level, then open the *dfscacherefresh.cfg* file and modify the logging level.

```
# ---------------------------------
# Logging configuration,
# Write application log to file as trace
# ---------------------------------
[logging]
# level must be set to one of: OFF - No logging, SEVERE, WARNING, INFO, CONFIG, ALL
level =ALL
```

Save the changes and restart the Cache Refresh daemon to ensure that the modifications are reflected.

4.2 DFS Cache Monitor Logging Level Configuration

The logging level configuration for the DFS cache monitor is defined in its configuration file, *dfscachemonitor.cfg*, which can be viewed and edited by logging to the Name node through SSH. The configuration file is located in the `/var/log/protegrity` directory.

If you need to change the logging level, then open the *dfscachemonitor.cfg* file and modify the logging level.

```
# ---------------------------------
# Logging configuration,
# Write application log to file as trace
# ---------------------------------
[logging]
# level must be set to one of: OFF - No logging, SEVERE, WARNING, INFO, CONFIG, ALL
level = WARNING
```

Save the changes and restart the Cache Monitor daemon to ensure that the modifications are reflected.

The default directory path of the *dfscachemonitor.log* file is `/var/log/protegrity`.

For more information on the DFS Cache Monitor logging level configuration, refer to section *6.5.1.3.2 Ùpdating the HDFSFP Service Parameters* in the *Installation Guide 8.0.0.0*.

4.3 Beuler Logs

The default logging level for Beuler logs is *INFO*, which collects all *INFO, WARNING, and ERROR* logs. The Beuler log file is generated on the Lead node in the `/var/log/protegrity/beuler.log` file.

Chapter 5

Protegrity Products Error Handling

The High-level architecture of Protegrity products is reflected in the following picture:

> **Note:** The File Protector (FP) is certified for version 6.6.5.

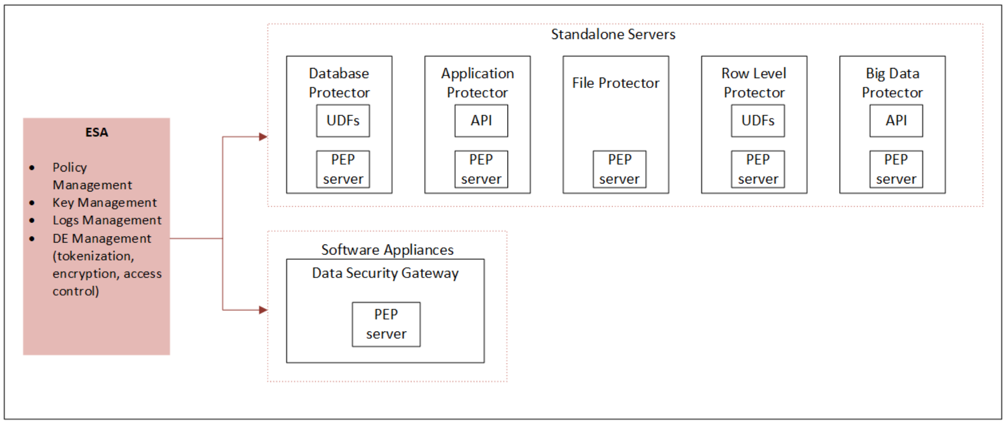


Figure 5-1: Protegrity Products High-Level Architecture

Protegrity products have their own logs. It is recommended to monitor logs on a regular basis to ensure all products function as expected. The first step in troubleshooting of possible problems should also be checking the logs of the corresponding product.

Table 5-1: List of Logs

Product	Log File and its Location	Log Description
Enterprise Security Administrator (ESA)	ESA Web Interface, **System Information** > **Appliance Logs**	Shows the appliance-specific logs: • Users logging into/out of Web Interface and the IP from which the users logged

Product	Log File and its Location	Log Description
		• Users logging into/out of CLI Manager • License status warnings • Operations in the internal LDAP: users/ groups adding/editing/removing, password changes • Network configuration changes • System Data and Time changes • System Configuration (OS level, disk space problem) logs • Starting/stopping of the services
PEP Server	PEP Server, OS console: *`defiance_dps/data/pepserver.log`*	Shows PEP Server internal specific logs: • Shared-memory related events • Token tables related events • Policy status related events • Policy changes related events • License status related events • Internal server processes related events • and other logs
Protectors	ESA Web Interface, **Protegrity Analytics** > **Forensics**	The *security* logs in ESA Forensics that are identified by codes 1-46, provide the details of protection operation events and are explained in section *5.4 Protectors Security Logs*.
DPS Servers	ESA Web Interface, **Protegrity Analytics** > **Forensics**	The *audit* logs in ESA Forensics that are identified by codes 50-159 log the policy related events, are explained in section *5.5 DPS Servers Internal Audit Logs*.

5.1 Policy Management in ESA Error Handling

This section explains the main Policy management connection errors, permission restrictions, policy creation and deployment problems users may encounter while working with Policy management in ESA.

Table 5-2: Policy management ESA Server Connection Errors

Error /Problem	This may happen because…	Recovery
Communication Error. Failed to connect to host <ESA IP> at port <host number>.	The entered ESA host and port information is incorrect. The ESA host and port information has changed. The ESA is down for some reason. The ESA default gateway is configured incorrectly.	Contact your ESA administrator and verify the correct host/port settings and the availability of ESA.
Session Timeout. The client automatically logs out the user after 15 minutes of inactivity.	15 minutes of inactivity passed.	Re-login into Policy management in ESA.

Error /Problem	This may happen because…	Recovery
Login failed. Authentication Failed.	User name and/or password submitted is incorrect.	Re-login with the correct credentials. Verify if CAPSLOCK is on/off if you fail to login again.
An error occurs, when you navigate to the Policy Management dashboard, create a data element, create a policy, deploy a data store, perform any policy operations.	The Hubcontroller service are stopped.	Perform the following steps. 1. Navigate to **System** > **Services**. 2. Restart the **HubController** service.
If you are create a short data token in a policy with settings as *Allow Short Data=Yes* or *Allow Short Data=No, return input as it is* and then deploy the policy, the Forensics displays a policy deployment warning indicating that the data element has unsupported settings.	n/a	Note the following: • For protectors v6.6.x, the warning indicates that short data tokens are not supported and data elements cannot be deployed. The policy is deployed without the short data tokens. • For protectors v7.x.x, the warning appears as a cautionary and can be ignored. The policy along with the short data tokens is deployed successfully.

Table 5-3: ESA Licensing and Policy Deployment Errors

Error /Problem	This may happen because…	Recovery
`License is expired` message displays on the bottom pane. Security Officer permissions are reduced to the permissions of viewer.	Your current license has expired.	The ESA administrator must request a new license and then activate it. When the license is activated, the Security Officer users will have full administrative permissions.
`License does not support that many protectors`.	You have limited number of protectors that can be used by your license type.	You can delete one of the data stores that you have been using (unless there are policies deployed to this data store!), and only then create a new data store. If you need more protectors to be enabled by the license, then the Security Administrator should request a new Protegrity license.
`License is invalid`	Login has been disabled due to an invalid license.	The ESA administrator must request a new license and then activate it. When the license is activated, the Security Officer users will have full administrative permissions.
Error creating a data element. Data Element with that name already exists. Data element names must be unique.	Data element names cannot be repeated, that is data element for application protection cannot be created if data element with the same name already exists for database protection.	Use unique name for new data element, or rename existing data element by using *Edit* button on the *Manage Data Elements* dialog.
Error creating a data store, data element, policy.	Names for policy data (data stores, data elements, policies) in the Policy management in ESA MUST NOT:	Verify that the Name field of the policy data you are creating is correct (you can also refer to *Policy Management Guide 8.0.0.0* for additional details):

Error /Problem	This may happen because…	Recovery
Datastore with that name already exist. Datastore names must be unique.	1. Contain spaces 2. Contain special symbols (except, “_”, “-”) 3. Start with the digital values, “-”, or “_”. 4. Be more than 65 characters in length.	1. If you have two words as a name of a data store, then you do not have space as a separator. For example: *PolicyName*, *Policy-Name*, “or *Policy_Name* can be used instead of *Policy Name* 2. You do not have special symbols in the names of the policy data. For example: *DateAndTime* can be used instead of *Date@time* as the name of the data element. 3. Your policy data does not contain digital values at the beginning of the name. For example: *Policy1* or *Policy_1* can be used as a policy name, instead of *1_Policy*.
Error deploying a policy. "Policy <Policy Name> failed to be deployed.	The data store connectivity settings are incorrect.	Check the data store connectivity settings in Data Stores workspace
Name: <Server type>, Hostname: <Server host>, Port: <Server port>. Reason: Failed to connect to <Server host>:<Server port>. Failed!(0)”	The server you are trying to deploy the policy to, is not accessible.	Verify that the PEP Server is up and running. If you are using PEP Sever on Data Security Gateway (DSG), then verify that the Pepserver Service is up and running. In case of a recurring error, try to restart it.
	The server you are trying to deploy the policy to, is bound to a specific NIC.	Verify the PEP server is not bound to a specific NIC by reviewing the *pepserver.log*. If the PEP server is bound to a specific NIC, then verify it is bound to the correct NIC. If the server is bound to the incorrect IP, then the log file has a record: (SEVERE) Error binding to 6.6.6:15710 - Host not found (SEVERE) Failed to create listener (Code=-12 : Unreachable!)
Error creating a policy. *A policy with that name already exists, please enter another name for this policy.*	Policy with the same name already exists.	Enter a policy name that is unique, and not used by any other policy.

The following section provides information about the resultant errors when trying to fetch the members from a member source.

Table 5-4: Member Source Service Errors

Error/Problem	This may happen because...	Recovery
The following error is observed in the logs when fetching the groups from an LDAP source. • HubController log - *`"Failed to send member request to Member Source Service","no GROUPs were found"`* • Member Source service log - *`LDAP error: {"lde_message":"No Such Object","lde_dn":null,"memberType":"GROUP"}`*	Member Source connectivity information provided during creation of this member source is incorrect.	Ensure that the provided *Group Base DN* attribute information is correct for the member source. Ensure that the Member Source service is up and running by navigating to **ESA Web UI** > **System** > **Services**. In case of a recurring error, try to restart it.
The following error is observed in the logs when fetching the users from an LDAP source. • HubController log - *`"Failed to send member request to Member Source Service","no USERs were found"`* • Member Source service log - *`LDAP error: {"lde_message":"No Such Object","lde_dn":null,"memberType":"USER"}`*	Member Source connectivity information provided during creation of this member source is incorrect	Ensure that the provided *User Base DN* attribute information is correct for the member source. Ensure that the Member Source service is up and running by navigating to **ESA Web UI** > **System** > **Services**. In case of a recurring error, try to restart it.
The following connection timeout error occurs when connecting to an LDAP source. • HubController log - *`"Failed to send member request to Member Source Service","connect ETIMEDOUT <host>:<port>"`* • Member Source service log - *`Failed to connect to LDAP server: connect ETIMEDOUT <host>:<port>`*	The host and port information provided during the creation of this member source is incorrect.	Ensure that the provided *host* and *port* attribute information is correct for the member source. Ensure that the Member Source service is up and running by navigating to **ESA Web UI** > **System** > **Services**. In case of a recurring error, try to restart it.
The following error is observed in the logs when fetching the users or groups from an LDAP source. • HubController log - *`"Failed to send member request to Member Source Service","no such attribute: user1"`*	The user or group attribute does not exists.	Ensure that the *user* or *group* attribute information exists in the LDAP source.

Error/Problem	This may happen because...	Recovery
- Member Source service log - `LDAP error: {"name":"ClientError","statusCode":400`		
The following error is observed in the logs when working with an LDAP source. - HubController log - `"Failed to send member request to Member Source Service","Invalid Credentials"` - Member Source service log - `Failed to bind: Invalid Credentials, LDAP error: {"lde_message":"Invalid Credentials","lde_dn":null,"isConnected":true}`	The credentials provided for connecting to the LDAP source is incorrect.	Ensure that the *username* or *password* information for the LDAP source is correct.
The following connection timeout error occurs when connecting to an AD source. - HubController log - `"Failed to send member request to Member Source Service","connection timeout"` - Member Source service log - `Timeout connecting to AD server: connection timeout`	The host and port information provided during the creation of this member source is incorrect.	Ensure that the provided *host* and *port* attribute information is correct for the member source. Ensure that the Member Source service is up and running by navigating to **ESA Web UI** > **System** > **Services**. In case of a recurring error, try to restart it.
The following error is observed in the logs when working with an AD source. - HubController log - `"Failed to send member request to Member Source Service","Base DN is invalid"` - Member Source service log - `LDAP error: {"lde_message":"0000202B: RefErr: DSID-031007EF, data 0, 1 access points\\n\\tref 1: 'example.com'\\n\\u0000","lde_dn":null,"memberType":"USER"}`	The *Base DN* information provided during creation of this member source is invalid.	Ensure that the provided *Base DN* attribute information is correct for the member source.
When working with the member source on the ESA Web UI, a connection timeout error is observed while fetching the members or syncing a group in a role. If you get a connection timeout error, then check the *hubcontroller.log* and the *mbs.log* files to check for error messages.	The timeout period exceeds the default values specified for the following parameters: - PTY_ROLE_MBS_REQUEST_TIMEOUT - PTY_MEMBERSOURCESERVER_REQUEST_TIMEOUT	Perform the following steps to fix the timeout error. 1. To check the error message in the *mbs.log* and the *hubcontroller.log* files, on the CLI Manager, navigate to **Administration** > **OS Console**.

Error/Problem	This may happen because...	Recovery
- HubController log - *`"Failed to synchronize 'auto_role' member 'MBSTest50001-100000' [Caused by: PIM MBS returned error: Failed to send request to upstream PIM MBS service: The timeout period of 30000ms has been exceeded while executing POST /api/v1/members for server localhost:25800]", "POST /dps/v1/management/roles/60/members/sync | 500 | 127.0.0.1 | admin | 30sec | 1 of 1 members could not be synchronized"`* - Member Source Service log - *`"Failed to query group members | causedBy=Get "https://graph.microsoft.com/v1.0/groups/transitiveMembers?": net/http: request canceled (Client.Timeout exceeded while awaiting headers)"`* - Web UI error message - *`Failed to synchronize member. 1 of 1 members could not be synchronized.`*	- PTY_MANAGEMENT_MBS_REQUEST_TIMEOUT	2. If the error is related to connection or request timeout, then add the following parameters in the *hubcontroller.env* file with the required timespan: - PTY_ROLE_MBS_REQUEST_TIMEOUT=<timespan> - PTY_MEMBERSOURCESERVER_REQUEST_TIMEOUT=<timespan> - PTY_MANAGEMENT_MBS_REQUEST_TIMEOUT=<timespan> 3. Login to the ESA Web UI. 4. Navigate to **System** > **Services**. 5. Restart the **HubController** service.
When working with the member source using the DevOps API, a connection timeout error is observed in the DevOps API while fetching members or syncing a group in a role. If you get a connection timeout error, then check the *devops.log* file to check for the error message. DevOps log - *`"GET /api/v2/sources/11/members | 500 | 127.0.0.1 | admin | 30sec | com.protegrity.framework.exception.DpsException: PIM MBS returned error [Caused by: PIM MBS returned error: Failed to send request to upstream PIM MBS service: The timeout period of 30000ms has been exceeded while executing POST /api/v1/members f or server localhost:25800]"`*	The timeout period exceeds the default values specified for the following parameters: - PTY_ROLE_MBS_REQUEST_TIMEOUT - PTY_MEMBERSOURCESERVER_REQUEST_TIMEOUT - PTY_MANAGEMENT_MBS_REQUEST_TIMEOUT - PTY_HUBCONTROLLER_REQUEST_TIMEOUT	Perform the following steps to fix the timeout error: 1. To check the error message in the *devops.log*, *mbs.log*, and the *hubcontroller.log* files, on the CLI Manager, navigate to **Administration** > **OS Console**. 2. Add the following parameters in the *hubcontroller.env* file and add the required timespan: - PTY_ROLE_MBS_REQUEST_TIMEOUT=<timespan> - PTY_MEMBERSOURCESERVER_REQUEST_TIMEOUT=<timespan> - PTY_MANAGEMENT_MBS_REQUEST_TIMEOUT=<timespan> 3. Add the parameter PTY_HUBCONTROLLER_REQUEST_TIMEOUT=<timespan> in the *devops.env* file and add the required timespan: 4. Login to the ESA Web UI. 5. Navigate to **System** > **Services**.

Error/Problem	This may happen because...	Recovery
		6. Restart the **HubController** and the **DevOps** services.

5.2 ESA Error Handling

ESA appliance collects all logs that come from different Protegrity Servers. The following section explains the logs that you may find on ESA and the errors that you may encounter on the ESA.

Table 5-5: Common ESA Logs

Log type	Details	Logs Description
Appliance logs ESA Web Interface, **System Information** > **Appliance Logs**	Here you can view appliance system logs. These logs are saved for two weeks, and then they are automatically deleted.	The ESA appliance logs the appliance-specific system events: • Users logging into/out of Web Interface and the IP from which the users logged • Users logging into/out of CLI Manager • License status warnings • Operations in the internal LDAP: users/groups adding/editing/removing, password changes • System Data and Time changes • System Configuration (OS level, disk space problem) logs • Network configuration changes • Starting/stopping of the services.
Data Management Server (DMS) logs ESA Web Interface, **Logging & Reporting** > **Logs**	Here you can view DMS system related logs: • Startup • WatchDog • Database Access layer • Database Engine	System logs related to monitoring and maintenance of the Logging Repository (DMS).

Table 5-6: ESA Common Errors

Error /Problem	This may happen because…	Recovery Actions
High severity audit log files with title “Failed to import some users” is created in ESA Forensics.	The high severity audit log files are a result of the following conditions: • Blank lines in the file which lists the ESA users. • User names are exceeding 36 characters in length.	Ensure that the user names which are specified in the list of ESA users are less than or equal to 36 characters in length and are created or imported in the ESA.
When a Trusted Appliance Cluster is created between an HA ESA primary and other appliances, a permission denied error is generated when you try to add a node to the cluster.	Incorrect file permissions, 640, for the ssh_known_hosts file on the any of the HA nodes.	Perform the following steps: a. In the ESA CLI web interface of the HA nodes, navigate to the following file. /etc/ssh/ssh_known_hosts a. Edit the permission to 644.

Error /Problem	This may happen because…	Recovery Actions
In an environment where the TAC and HA co-exist, the LDAP fails when the cluster export tasks are executed after a primary switchover occurs. **Note:** The cluster export task contains the appliance authentication and LDAP server settings.	The password for the *ldap_bind* user is not updated in the new Primary ESA after a switchover occurs.	Perform the following steps: 1. Login to the Secondary ESA using the *local_admin* credentials. 2. In the OS console navigate to the */etc/ksa/conf* directory. 3. Open the *self.xml* file in edit mode. 4. Note the value of the *LDAP_BINDPW* attribute. 5. Login to the Primary ESA using the local_admin credentials. 6. In the CLI Manager, navigate to **Administration** > **Specify LDAP Server** > **Protegrity LDAP Server**. 7. Type the value of the *LDAP_BINDPW* attribute in the *Bind Password* textbox. 8. Select *Test*. 9. Select *Ok*. 10. Select *Ok*. 11. Login to the ESA Web UI of the Primary ESA. 12. Navigate to **System** > **Services**. 13. Restart the **External Group Sync Service**.
In the ESA CLI, when you copy files to home directories (*`/home/service_admin, /home/local_admin, or /home/service_viewer`*) using the *Put Files* for the option under Trusted Appliance Cluster, a following traceback error appears. *`Permission denied:`*	The user does not have the permission to copy the file to the target directory.	Perform the following steps to copy the files to the home directory: 1. From the ESA CLI, navigate to**Tools** > **Trusted Appliance Cluster** > **Cluster Operations: Execute Commands/Deploy files** > **Put Files**. 2. Select the required files from the source directory. 3. Select Next. 4. In the **Target Path** screen, choose **Select Target Directory**. 5. Navigate to the required target directory. 6. A message to enter the directory manually appears. 7. Select **Yes**. 8. Type the path for the target directory and select **OK**. 9. Select the required target nodes in the **Target Node** screen and select **OK**. The files are deployed to the target node.
When you run a cluster export task, the following message appears for all the target nodes: *`Host Denied`*		Perform the following steps: 1. Login to the CLI Manager of the target node. 2. Navigate to **> > Tools** > **SSH Configuration** > **Known Hosts: Hosts I can connect to**. 3. Select **Add Host**. 4. Enter *127.0.0.1* and select **Done**. On the Web UI, refresh the trusted appliance cluster screen.
When exporting or importing custom files, the export import process fails.	The file that is exported does not exist.	You can perform one of following options: • Remove the file path in the *customer.custom* file. • Remove the file path in the exclude file. • Perform the following steps:

Error /Problem	This may happen because…	Recovery Actions
		1. In the Web UI, navigate to **Settings** > **System** > **Files**. 2. Click **Edit** corresponding to the *customer.custom*. 3. Add the prefix, *optional*, to the required file paths and save the changes. Run the export process.

While uploading a file from the Web UI the following error appears:
`Proxy Error`
`Reason: Error reading from remote server`
	The file is not uploaded to the server.	Perform one of the following methods..
		- Perform the following steps to increase the session timeout for the service dispatcher:
		1. In the OS Console, navigate to the `/etc/ksa/service_dispatcher/proxies/mng` directory.
		2. Run the following command to create a file.
		`# vi apache.mng.UploadFile`
		3. Type the following configuration changes.
		ProxyPass/Management/Upload File http://0.0.0.0:2443/Management/UploadFile/ retry=0 timeout=3600
		ProxyPassReverse/Management/Upload File http://0.0.0.0:2443/Management/UploadFile
		4. Save the changes.
		5. Run the following command to restart the service dispatcher service.
		`# /etc/init.d/service_dispatcher restart`
		- Upload the file using the following *scp* command:
		1. In the CLI Manager, navigate to the OS Console.
		2. Run the following command to transfer files between the source and target directories.
		`# scp -r user@host:directory/<Source directory> <Target directory>`

A failure occurs while extending the OS or logs partition.		- Perform the following steps to fix the errors:
		1. Boot the system from the ISO.
		2. In the OS Console, run the following command to enable LVM mapping.
		`# lvchange -ay PTYVG`
		3. Run the following command to fix the errors in the file system for the required volume group.
		For example,
		`# reiserfsck --fix-fixable /dev/mapper/PTYVG-OS`
		4. Run the following command to mount the required volume.

Error /Problem	This may happen because…	Recovery Actions

		For example,
		`# mount /dev/mapper/PTYVG-OS /TARGET`
		- If the above step fails, perform the following steps:
		1. Run the following command to format the partition.
		For example,
		`# mkfs.reiserfs /dev/mapper/PTYVG-OS`
		- Restart the appliance in the *System-Restore Mode* and restore the backup data.

While extending the OS partition, the following message appears: Couldn't find device with uuid <ID> Cannot change VG <volume group> while PVs are missing		Run the following command and press **ENTER**: `#vgreduce –removemisssing <volumegroup>`
When a role is deleted, the users associated with the role are not updated. The deleted role appears on user list in the **User Management** screen. For example, role name appears in the following format: *<Role name><Random number>*		Delete the user from the **User Management** screen. If required, add a user with the same name and credentials.
When you are importing a file from **System** > **Backup & Restore** > **Import**, the following error appears: `Bad Gateway The proxy server received an invalid response from an upstream server`	The size of the file is more than the value in the **Max File Upload Size**.	Perform the following steps to increase the file upload size: 1. On the Web UI, navigate to **Settings** > **Network** > **Web Settings**. 2. Under General Settings, increase the size of the file from the **Max File Upload Size** slider. 3. Select **Update**.
The Linux Host ID does not change in an ESA or a DSG instance created on the AWS cloud platform.	The Linux Host ID and the Protegrity Host ID are generated after an ESA or DSG instance is created on the AWS cloud platform. As per the expected behaviour of the appliance, only the Protegrity Host ID is modified after running the appliance rotation tool on the ESA or the DSG instance.	Perform the following steps to modify the Linux Host ID: 1. Launch an ESA or DSG instance on the AWS cloud platform. 2. On the CLI of the ESA or DSG instance, navigate to **Administration** > **OS Console**.

Error /Problem	This may happen because…	Recovery Actions

		3. Run the following command to change the Linux Host ID:
		`echo -ne \\x$11\\x$22\\x$22\\x$11`
		`> /etc/hostid`
		In this example, parameters like `x$11` and `x$22` are sample values for the Linux Host ID. You must enter actual values for `x$11` and `x$22`.
		4. Run the following command to check the Linux Host ID:
		`# hostid`
		`11222211`

The SSH session is terminated during the creation of a bond on the ethMNG interface.		Restart the session after the NIC bond on the ethMNG NIC is created.
The slave NICs do not have an IP assigned, but the following message appears during creating a bond: *`NIC Bonding is not available`*	The NICs might be on the DHCP mode.	Convert the NICs to Static mode.
The Web UI is not accessible after the NICs are bonded.		Reset the Network Bonding from the CLI Manager and bond the NICs again. For more information about resetting the NIC bonding, refer to the *Appliance Overview Guide*.
During binding NICs, the following message appears. *`Unknown Error`*	This might occur if the network is slow.	Restart the appliance queues using the following command: `/etc/init.d/appliance-queues server restart`
When you enable Two-Factor Authentication and export data from one ESA to another, the export process fails.		You must create two separate scheduler tasks to export data. First you must export the LDAP settings. Then, you must export the OS settings.
When you remove an appliance from the cluster is removed, a warning that the appliance is the last leader of the server of the cluster appears.	The appliance that is the last server of the cluster cannot be removed as all the clients are connected to it for receiving cluster-related information. Removing the last server from the cluster might de-stabilize the cluster.	NA
You cannot add an appliance to the cluster.	Certificates are not valid.	Ensure that you assign a valid server and CA certificates on the appliance. For more information about validating certificates, refer the *Certificate Management Guide.*
When you join an appliance to the cluster, the process is not completed, and a	The Consul service is not available.	Perform the following steps to remove the Consul labels for the appliance:

Error /Problem	This may happen because…	Recovery Actions
following error appears in the logs: *`Error: [WARNING] No Consul node is available as join target!`*		1. On the CLI Manager, navigate to **Tools** > **Trusted Appliances Cluster** > **Update Cluster Information**. 2. Remove **Consul Client** or **Consul Server** label from the **Label** textbox. 3. Select **OK**. 4. Login to the Web UI and remove the appliance from the cluster.
When you simultaneously remove multiple appliances from a cluster, the following error appears in the logs: *`Failed To Update KV Store.`*		Remove the appliances separately from the cluster and refresh the Trusted Appliances Cluster screen.
When you remove a node from the cluster the following error appears on the screen: *`RunNow error: [object Object] errorThrown: error`*		Perform the following steps to remove the Consul labels for the appliance: 1. On the CLI Manager, navigate to **Tools** > **Trusted Appliances Cluster** > **Update Cluster Information**. 2. Remove Consul Client or Consul Server label from the Label textbox. 3. Select **OK**. 4. Login to the Web UI and remove the appliance from the cluster.
When you create a cluster, the following error appears on the screen: *`Failed to join. Error: “Cannot get/parse target cluster config file. Please make sure the target node’s cluster is enabled.`*	The SSH configuration on the target machine is incorrect.	Ensure that the Authentication Type on the SSH configuration manager screen is set to **Password + PublicKey**. Perform the following steps: 1. On the Web UI, navigate to **Settings** > **Network** > **SSH**. 2. Select **Password + PublicKey** from the Authentication Type drop-down list. 3. Click **Apply**.
The following error is observed in the logs: *`/dev/shm/ heardbeat/servers File Doesn't exists`*	When a Set ESA Communication is established, the heartbeat service checks for the ESA's that are available. If the heartbeat is not established, the file is not generated, and the error appears.	There is no functional impact on the appliance. This error can be ignored.
In the System File page, when you modify, upload, or reset a file, the ownership of the file changes from local user such as, *service_admin* user to the *root* user. The ownership of the files in the following file groups change:		Perform the following commands to change the ownership of the file 1. In the CLI Manager, navigate to **Administration** > **OS Console**. 2. Run the following command to change the ownership. `chown service_admin:service_admin <directory of file>`

Error /Problem	This may happen because…	Recovery Actions
- Logging Configuration Files - Policy Management Files		For example, to change the ownership of the *DMS.cfg* file, run the following command. `chown service_admin:service_admin /opt/protegrity/DefianceEnterprise/Config/DMS.cfg`

In the System File page, when you modify, upload, or reset a file, the ownership of the file changes from local user such as, *www-data* user to the *root* user.
The ownership of the files in the following file group changes:
- Cloud Gateway
		Perform the following commands to change the ownership of the file:
		1. In the CLI Manager, navigate to the **Administration** > **OS Console**.
		2. Run the following command to change the ownership.
		`chown www-data:www-data <directory of file>`
		For example, to change the ownership of the *gateway.json* file, run the following command.
		`chown www-data:www-data /opt/protegrity/alliance/config/gateway.json`

On the ESA Web UI, run the the export-import procedure to a file or a cluster by selecting the **Log-Repository Server** option. The following error appears on the **Forensics** screen:
`Internal Error: Invalid input provided`
		Perform the following steps:
		1. In the CLI Manager, navigate to the **Administration** > **OS Console**.
		2. Create a *recover-emsdb.sh* file using the vi editor and insert the following script:
		`#!/bin/sh -e`
		`PGSQL_DIR="/opt/protegrity/DefianceEnterprise/database/pgsql"`
		`DUMPFILE=/root/pgdumpall.sql.$$`
		
		`echo "Press ENTER to recover the logging database or CTRL+C to cancel"`
		`read`
		
		``SERVICE_ADMIN_PASSWORD=`python -m ksa.acl --get-credentials | grep SERVICE_ADMIN_PASSWORD | cut -d= -f2` ``
		`test -z "$SERVICE_ADMIN_PASSWORD" && { echo "Failed to obtain service-admin password" ; exit 1 ; }`
		`export PGPASSWORD=$SERVICE_ADMIN_PASSWORD`
		
		`echo "Resetting xlog..."`
		
		`# su dmsuser -c  "$PGSQL_DIR/bin/pg_resetxlog  /opt/protegrity/DefianceEnterprise/database/data/"`
		`# su dmsuser -c  "$PGSQL_DIR/bin/pg_resetxlog  -f /opt/protegrity/DefianceEnterprise/database/data/"`
		
		`echo "Reindex database..."`
		`$PGSQL_DIR/bin/reindexdb -U admin    -a -h 127.0.0.1 -p 5433`
		
		`echo "Dumping to file $DUMPFILE"`
		`$PGSQL_DIR/bin/pg_dumpall  -U admin -h 127.0.0.1 -p 5433  --clean > $DUMPFILE`

Error /Problem	This may happen because…	Recovery Actions

		`echo "restore (MUST stop DMS)..."`
		`dms stop`
		`$PGSQL_DIR/bin/psql -h 127.0.0.1`
		`-p 5433 -U admin -d postgres < $DUMPFILE`
		`rm /root/pgdumpall.sql.$$`
		`echo "Restarting services"`
		`dms_postgres restart`
		`dms restart`
		3. Save the file.
		4. Assign execute permissions to the *recover-emsdb.sh* file using the following command.
		`chmod 700 recover-emsdb.sh`
		5. Run the *recover-emsdb.sh* script.
		6. Press **ENTER**.
		7. Enter the your administrative credentials on the screen and press **ENTER**.

When you upload a patch on the Web UI, the following message appears on the Web UI. *`The file cannot be uploaded as it may be infected`*		- This is a false positive message that appears on the Web UI. Select **Yes** to continue uploading the file. - Ensure that the minimum space available in the */opt* directory is more than twice the size of the patch. For example, if the size of the patch is 2 GB, the minimum space available in the */opt* directory is more than 4 GB.
The update of the antivirus database fails.		Complete the following steps: 1. On the CLI Manager, navigate to **Administration** > **OS Console** 2. Run the following command: `rm /var/lib/clamav/*.c?d` 3. On the Web UI, navigate to **Settings** > **Security** > **Antivirus.** 4. Select **Database Update** to update the antivirus database. A warning message appears. You can ignore the warning message. The antivirus database is updated.
The Proxy Authentication service is not visible on the Services screen.		Complete the following steps: 1. On the ESA Web UI, navigate to **Settings** > **Users** > **Advanced** 2. Click **Save**. 3. Logout from the ESA Web UI and login again. 4. Navigate to **System** > **Services.** Ensure that the required services are running.
When you export a report, the following error appears. *`Error Message There was an error on the server. Try again or contact site administrators.`*		Complete the following steps: 1. On the CLI Manager, navigate to **Administration** > **OS Console**. 2. Run the following command: ***`sed -i '/^assistive_technologies/s/^/# /g' /etc/java-8-openjdk/accessibility.properties`***

Error /Problem	This may happen because…	Recovery Actions
or *`Internal server error occurred. Please contact your system administrator`*. *`Details: Handler processing failed; nested exception is java.lang.NoClassDefFoundError: Could not initialize class org.apache.batik.bridge.CursorManager`*		3. Login to the ESA Web UI and navigate to **System** > **Services**. 4. Restart the **Reporting Server** service.
The following error appears on the logs or the error is observed when you add a new user. *`LDAP Failure: {'info': 'operation restricted', 'desc': Server is unwilling to perform'}`*	The OS backup procedure was interrupted or not completed.	Restart the OS backup operation by running the following command from the OS Console: `/etc/opt/scripts/after-backup.sh`
When you add an appliance to the cluster and remove them immediately from the cluster, the following error appears on the screen. *`/etc/init.d/appliance-queues-server: Exception while calling -.-().Serialize(args=['<ESA IP Address>', '<username>', '<password>', [u'<ESA IP Address>', u'<hostname>']],kwargs={}) :#012Traceback (most recent call last):#012 File "/usr/local/lib/python/dist-`*	The status of the nodes are not updated after you immediately add a remove an appliance from the cluster.	When you add or remove a node from a cluster, the updates are propagated across all appliances in the cluster. The wait time for this process is approximately one minute. You must wait for a minute before performing any action on the cluster.

Error /Problem	This may happen because…	Recovery Actions
`packages/ksa/backend/server.py", line 232, in call_function#012 File "/usr/local/lib/python/dist-packages/ksa/backend/server.py", line 120, in call_serialized_function#012 File "<string>", line 1, in <module>#012 File "/opt/cluster/cluster_operations.py", line 144, in _join#012 password=target_password, comm_methods=communication_methods)#012 File "/etc/opt/Cluster/clustermgr.py", line 1066, in JoinCluster#012 File "/etc/opt/Cluster/clustermgr.py", line 1400, in _JoinCluster#012ClusterException: Failed to add the requested cluster-node: Node id gZ68G4kWoOdMoWxj already exists`		
After performing a delete operation from the **Files** screen, you are unable to reset the following files: • *gateway.json* • *alliance.conf* • *exampleusers.txt* • *examplegroups.txt*		When you delete a file from the Files screen, the files are backed up in the */etc/configuration-files-backup* directory. You can restore them by copying the files from the backup directory to the original directory. In the OS Console of the CLI Manager, run the *copy* or *move* command to restore the file from the backup directory to the original directory. The original directory of the files are as follows: • *gateway.json* - */opt/protegrity/alliance/config/gateway.json* • *alliance.conf* - */opt/protegrity/alliance/config/rsyslog/alliance.conf* • *exampleusers.txt* - */opt/protegrity/mbs/users/exampleusers.txt* • *examplegroups.txt* - */opt/protegrity/mbs/groups/examplegroups.txt*

Error /Problem	This may happen because…	Recovery Actions
After you upgrade the ESA to v7.2.0, the following configuration files are listed in the File Integrity Module (FIM) on the ESA Web UI after the upgrade. - */opt/protegrity/hubcontroller/conf/hubcontroller.conf* - */opt/protegrity/defiance_dps/bin/adminserver* - */opt/protegrity/defiance_dps/bin/membersourceserver.env* - */opt/protegrity/hubcontroller/membersources/users/exampleusers.txt* - */opt/protegrity/hubcontroller/membersources/groups/examplegroups.txt*	These configuration files are either no longer present from v7.2.0 or contain changes in the file path from v7.2.0.	You must perform the following steps to address the file modifications: 1. On the ESA Web UI, navigate to **Settings** > **File Integrity**. 2. Click **Check** to see the file modifications. 3. Select the required files and then click **Accept**. 4. Enter a comment in the dialog box and then click **Ok**.
When the Appliance OS keys rotation process is run, the following error appears. `Failed to set admin password. Error : LDAP Error: {'desc': Invalid credentials'}` and `Failed to set viewer password. Error : LDAP Error: {'desc': Invalid credentials'}`	The appliance keys are rotated after the Set ESA communication process is performed.	Perform the following steps: 1. On the screen, select **OK**. 2. Run the Set ESA communication process again.
On the Web UI, when you navigate **Settings** > **Network** > **Web Settings** and click **Update** under the **SSL Cipher Settings** tab, the following error appears. `Fail to update Cipher Settings, please check events`	The **DES-CBC3-SHA** cipher suite is not supported	Perform one of the following steps: - In the **SSLCipherSuite** text box, remove the **DES-CBC3-SHA** cipher suite from the list - In the **SSLCipherSuite** text box, append an exclamation (!) before **DES-CBC3-SHA** to disable the cipher suite
During the reinitialization of the finalization an instance, the following message is displayed.	During the finalization an instance, if the session was interrupted, then the instance will become unstable.	NA

Error /Problem	This may happen because…	Recovery Actions
`Finalization is already in progress.` However, the finalization of the instance is not completed.	If you reinitialize the finalization on the same instance, the system will not be able to process the finalization process.	
While restoring a VM using the 'Creating a new virtual machine' procedure, the following error is observed: `UserErrorInvalidManagedDiskOperation`	While restoring a virtual machine using recovery services vaults, the Instance size of VM inherits the Instance Size that is specified while creating the instance from which backup is taken. If this instance size that is used to create the instance is insufficient, the error is displayed.	- Clear the resources for this instance before creating the VM - Create a new VM from the existing disk
After a TAC is created, an status **`Unknown`** is displayed.	The **Authentication type** on the **SSH** screen is set to **Password**.	Set the **Authentication Type** to **Password + PublicKey** or **Public key**

On the ESA Web UI, navigate to **System** > **Files**. When you edit `exampleusers.txt` the or `examplegroups.txt` files, the following error appears.
`Failed to retrieve product file from the server`
	The files might contain a |*U* character	1. On the CLI manager, navigate to **Administration** > **OS Console**
		2. Run the following command.
		`vi /opt/protegrity/mbs/users/exampleusers.txt`
		or
		`vi /opt/protegrity/mbs/users/examplegroups.txt`
		3. Remove the |*U* character and save the changes.
		4. On the ESA Web UI,navigate to **System** > **Files** and edit the files.
		5. The files can be edited.

On the Web UI, reset password for the *ldap_bind_user* account. When you refresh the User Management screen, the following message appears: `No Users available` Also, an LDAP user cannot log in to the appliance from the CLI Manager or Web UI.		Perform the following steps: 1. Log in to the CLI Manager with the *local_admin* user. 2. Navigate to **Administration** > **Specify LDAP server/s**. 3. Enter the root credentials. 4. Select **Set Proxy Authentication**. 5. In the **Bind Password** text box, enter the password that you specified for *ldap_bind_user* while resetting it from the Web UI 6. Save the changes. 7. Log in to the CLI manager or Web UI with any LDAP user. The LDAP user can log in to the appliance. On the **User Management** screen, the users are visible.
In a Primary ESA of a TAC, when you navigate to External Groups screen, the following message appears. Failed to fetch data from External Groups. Try refreshing the page	The following JSON files in */opt/externallookup/data* whose size are 0 KB: - *ESA_Policy_Admins.json* - *BankDataAccess.json* - *ESA_Admins.json* - *ESA_Developers.json*	Delete the mentioned files. This issue mainly occurs if the size the */opt* partition is full. Ensure that you maintain the required space in the */opt* partition by keeping only the relevant files in it.

Error /Problem	This may happen because…	Recovery Actions
When you run the Full OS Backup operation from the Web UI, the following message appears. Unauthorised User		Perform the following steps: 1. Click **Done**. 2. Click **OS Full**. 3. Wait till the notification Backup has been initiated appears. 4. Click Ok.
When removing a remote node from the cluster, uninstalling the cluster services, or performing a leave cluster operation on the Web UI, the following message appears. Error! Failed to leave cluster: LeaveCluster <IP address>: The node cannot leave the cluster as it has existing associated tasks.		Delete all the tasks associated with the node before removing the node from the cluster.
On the Azure and the GCP instances, when you reset the password from the CLI manager for a user, you get the following error message: Login failure - 'failed to authenticate user: Insufficient privileges'		Azure and GCP instances do not support reset password in the CLI manager. You must reset passwords only from the Web UI.
When the listening address of the SNMPD port is changed, the following error appears on the Web UI: SNMP Service started failed	The assigned port is already configured for SNMPTRAPD.	It is recommended to not use the listening address which is already assigned and configured for other ports.
When the listening address of the SNMPD port is set as an invalid value (example: abcd), the following error appears on the Web UI: SNMP Service started failed		It is recommended to not set invalid listening address for the ports.
When the cluster node label is updated in the CLI Manager under **Tools** > **TAC** > **Node Management** > **Update Cluster Information**, the Appliance logs on the Web UI show the following traceback:*/etc/init.d/appliance-cluster-status: Cluster-AutoUpdate:Exception while updating cluster-status: (<type 'exceptions.ValueError'>, ValueError('list.remove: x*		To remove the traceback from the Appliance logs, remove the custom labels added for the cluster nodes. To update the cluster node label, perform the following steps: 1. In the CLI Manager of the node hosting the cluster, navigate to **Tools** > **TAC** > **Node Management** > **Update Cluster Information**. The **Update Cluster Information** screen appears. 2. Update the label of the node in the *custom:<your label>* format. 3. Select **OK**. The label for the cluster node is updated.

Error /Problem	This may happen because…	Recovery Actions
not in list',), <traceback object at 0x7f26293a5d40>		

When you try to revoke Two-Factor Authentication shared secret for per user shared secret setting, the operation fails	This may happen if the *username* contains special characters.	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/protegrity/.OS/users/<username>/`
		`2FA.vcode`

The *logrotate* task fails intermittently with the following error.
`Cloud gateway`
`logrotate`
`failed with`
`error: error`
`renaming`
`temp state`
`file /var/lib/`
`logrotate/`
`status.tmp`
However, the logs are rotated successfully.
	The *logrotate* task maintains a temporary file which is common for all logrotate operations.
	When the *logrotate* script is executed, it updates the temporary file, renames the temporary file, and rotates the logs successfully. Simultaneously, if another *logrotate* operation is triggered, then it is unable to find the temporary file as it was updated and renamed during the previous *logrotate* operation. This results in the *logrotate* task failure.
		To resolve the *logrotate* task fail error, perform the following steps.
		1. Copy the */etc/cron.d/ksa* file.
		2. Edit the */etc/cron.d/ksa* file.
		3. Update the following lines.
		`*/10 * * * * root /usr/sbin/`
		`logrotate  /etc/ksa/logrotate.conf`
		`2-59/10 * * * * root /usr/`
		`sbin/logrotate -s /var/lib/logrotate/`
		`status1.tmp /var/webservices/logrotate.conf`
		`4-59/10 * * * * root /usr/sbin/logrotate`
		`-s /var/lib/logrotate/status2.tmp /etc/ksa/`
		`service_dispatcher/logrotate.conf`
		4. Save the */etc/cron.d/ksa* file.

When you access Help from the CLI Manager, you are not able to exit from the CLI Help menu.		To exit from the CLI Manager Help menu, you can: • Close/restart the SSH session. • Restart the ESA.

When you log in to the ESA instance in either AWS or GCP, the following error appears.
`WARNING: Failed`
`to find a`
`usable hardware`
`address from`
`the network`
`interfaces;`
`using random`
`bytes:`
`1b:1f:ff:64:9b:b`
`6:ea:ce`
	The licenses generated are not locked to the MAC address of the ESA machine.	You must contact Protegrity support to generate a license file that is linked to the MAC address of the ESA machine.

When you execute the Antivirus daily update, a high severity log event is generated, and the following error message appears.
`Anti-Virus`
`database update`
`has failed.`
	The Anti-virus program connects to the *clamav* web and check for updates. If there are no update available for download, then the task is executed and a high severity log event is generated.	Run the task manually.
		Perform the following steps:
		1. Navigate to **Tools** > **AntiVirus**.
		2. Select **Options** and press **Enter**.

Error /Problem	This may happen because…	Recovery Actions

On ESA or appliance based product, after you reboot the system, the service dispatcher stops. It does not starts even after performing the operation manually.
The status of */etc/init.d/service_dispatcher* shows *running* on *OS Console*. However, if you navigate to **Administration** > **Services** from the *CLI Manager*, then the status appears as *stopped*.
	This might occur when the *"/usr/local/pty-apache/var/run/apache2/httpd.pid"* file is present.	Perform the following steps:
		1. Verify if the *"/usr/local/pty-apache/var/run/apache2/httpd.pid"* file is present.
		2. If the file is present, then remove the *"/usr/local/pty-apache/var/run/apache2/httpd.pid"* file using the following command:
		`rm /usr/local/pty-apache/var/run/apache2/httpd.pid`
		3. Restart the service dispatcher using the following command.
		`/etc/init.d/service_dispatcher restart`

When you rotate the appliance OS keys, no error log event is generated, however, the following error message appears on the screen.
`Failed to apply all the changes.`
`Please accept all the changes from the Web UI`
		Perform the following steps:
		1. Login to ESA CLI using the *administrative user* credentials.
		2. Navigate to **Administration** > **OS Console**.
		3. Enter *root* password.
		4. In the VI editor, edit the */var/lib/samhain/samhain_file* file.
		5. Add the following line in the file
		`[SOF]`
		and save the file.
		6. Quit and exit from the console.
		7. Navigate to **Tools** > **Rotate Appliance OS Keys**.
		8. Enter *root* password.
		9. Select **Yes** and enter *admin* credentials.
		10. Set new passwords for the required users and click **Apply**.
		11. After the credentials are successfully updated, exit from the CLI Manager.
		12. Login to the CLI Manager using the updated passwords.

After creating the backup of the system, if you modify the the authorized keys, then the ESA overwrites the updated keys while performing the import operation. However, after creating the backup of the system, if you add new users and their authorized keys, then the ESA will include them in the system after you perform the import operation. By default, the ESA will append the new users and their corresponding keys.		Delete the new users and their corresponding keys from the system, if they are not required. For more information about deleting keys, refer to *Deleting an Authorized Key* in the *Protegrity Appliance Overview Guide 9.1.0.0*.

Error /Problem	This may happen because…	Recovery Actions
On the Azure and GCP cloud platforms, if a new machine is created using a snapshot of the disk, then the machine is not reachable.	When you create a machine using a snapshot of the disk, then the routing tables are not updated.	To resolve this issue, restart the network settings for the new machine. To restart the network settings, perform the following steps: 1. Login to the CLI Manager. 2. Navigate to **Administration** > **OS Console**. 3. Enter the *root* password. 4. To restart the networking settings, run the following command. `/etc/init.d/networking restart`
Unable to export the information while executing the cluster task using the *IP address* of the node.	This might occur if the task is executed using the *IP address* of the cluster task instead of the *Hostname*.	To resolve this issue, ensure that the *IP address* of the cluster node is replaced with the *Hostname* in the task. For more information about executing the cluster task, refer to *Scheduling Configuration Export to Cluster Tasks* in the *Protegrity Appliance Overview Guide 9.2.0.0*.

> **Note:** Users of Active Directory group **Domain Users** will not be fetched as we do not support searching for Primary group ID.

The following section provides information about errors that are related to external HSM implementation with ESA.

Table 5-7: External HSM and Key Store Errors

Error/Problem	This may happen because…	Recovery

Error creating a data store after configuring ESA 7.0.1 with external HSM.
`Failed to create Data Store. sun.security.pkcs11.wrapper`
`.PKCS11Exception: CKR_DEVICE_ERROR or timeout occurs.`
	This occurs if ESA was previously in suspended state. When resuming from suspended state, this behavior is observed.	Restart ESA if it is in suspended state.

If you are using an external HSM to generate and manage keys, and try to create a Data Store and related policy, a connectivity timeout error is displayed. *`Failed to create Data Store.nextByte() failed`*		You must restart the Hubcontroller service, and then try to create a Data Store. Perform the following steps: 1. Click **System** > **Services**. 2. Restart the **HubController** service under Policy Management area.
When you are using an external HSM, the following error is displayed. `SEVERE: Failed to start key verticle : (RECIPIENT_FAILURE,0) load failed: CKR_PIN_INCORRECT`		Ensure that the following points are considered: • The Crypto Officer (CO) input password and pin provided in ESA is incorrect • Partition Officer (PO), Crypto Officer (CO), and Crypto User (CU) are not initialized.

Error/Problem	This may happen because…	Recovery
When you are using an external HSM, the following error is displayed. `SEVERE: Failed to start key verticle : (RECIPIENT_FAILURE,0) PKCS11 not found: no such algorithm: PKCS11 for provider SunPKCS11-hsm`		Ensure that the following points are considered: • Keys are not present in the external HSM • Keys created are not being used by external HSM Policies • External systems are unable to view keys due to incorrect user assignments for accessing keys. • HubController is unable to read external HSM certificates since Third-Party system does not have permission to access the certificates.
When you are using an external HSM, the following error is displayed. `SEVERE: Crypto operation using PKCS11 failed: java.io.IOException: load failed`		The same key label is present for multiple keys.
When you are using an external HSM, the following error is displayed. `(SEVERE) Failed to decrypt repository key. (Code=-206 : No hardware token available!)`		Ensure that the following points are considered: • The external HSM-related configuration settings are accurate. • The external HSM connection is not broken.
When you try to switch to an external HSM the switch fails.	The external HSM does not support or allow the type of key that is used.	Verify that the external HSM supports creating secret keys with the following attributes: • CKA_PRIVATE: TRUE • CKA_SENSITIVE: TRUE • CKA_EXTRACTABLE: FALSE • CKA_ENCRYPT: TRUE • CKA_DECRYPT: TRUE • CKA_MODIFIABLE: FALSE • CKA_WRAP: TRUE • CKA_UNWRAP: TRUE • CKA_DERIVE: FALSE • CKA_SIGN: FALSE • CKA_VERIFY: FALSE
In a TAC, the source ESA is configured with Key Store and the target ESA is configured with soft HSM. When you export the policy management settings from the source ESA to the target ESA with the *Backup Policy-Management for Trusted Appliances Cluster without Key Store* option selected, then the *HubController* service on the target ESA stops with the following error: `[SEVERE ] Failed to start HubController [Caused by: Failed to start Key verticle: Failed to decrypt key: Cannot open session to Key`		The following steps must be followed on the target ESA to address this issue: 1. On the target ESA, configure the Key Store setup by following the steps 1 through 13 from the section *Switching from Soft HSM to Key Store* in the *Key Management Guide*. 2. In the ESA CLI manager, navigate to **Administration** > **OS Console**. 3. Enter the **root** password 4. Navigate to the */opt/protegrity/keystore/external* directory.

Error/Problem	This may happen because…	Recovery
`Store since there's no user pin]`		5. Copy the HSM *userpin.bin* file from the */opt/protegrity/keystore/external* directory in the source ESA to the */opt/protegrity/keystore/external* directory in the target ESA. **Note:** The file permission for the *userpin.bin* file must be changed to *640*. Also, ensure that the file owner is *service_admin*. 6. Restart the *Key Management Gateway* service by navigating to **ESA Web UI** > **System** > **Services**. 7. Restart the *HubController* service by navigating to **ESA Web UI** > **System** > **Services**.

5.3 Troubleshooting Components Related to Logging

These sections describe the problems that you might face while working with logging-related components and the solutions or workarounds to resolve those problems.

5.3.1 Known issues for the td-agent

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

- **Known Issue:** The **Buffer overflow** error appears in the */var/log/td-agent/td-agent.log* file.

  Description: When the total size of the files in *td-agent* buffer */opt/protegrity/td-agent/es_buffer* directory reaches the default maximum limit of 64 GB, then the **Buffer overflow** error appears.

  Resolution:

  Add the *total_limit_size* parameter to increase the buffer limit in the *OUTPUT.conf* file using the following steps.

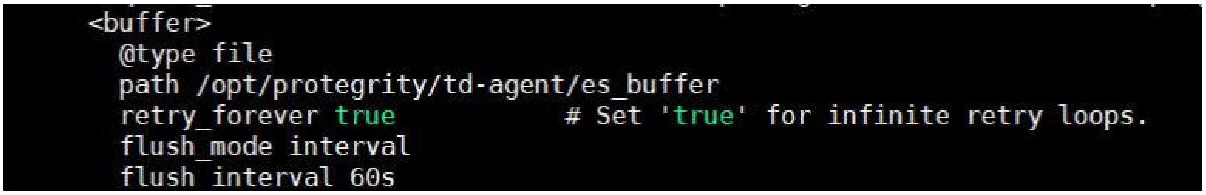
  1. Login to the CLI Manager of the ESA node.
  2. Navigate to **Administration** > **OS Console**.
  3. Stop the *td-agent* service using the following command:

     ```
     /etc/init.d/td-agent stop
     ```

     Note: You can also stop the service by logging into the ESA Web UI, navigating to **System** > **Services**, and stopping the **td-agent** service under **Misc**.

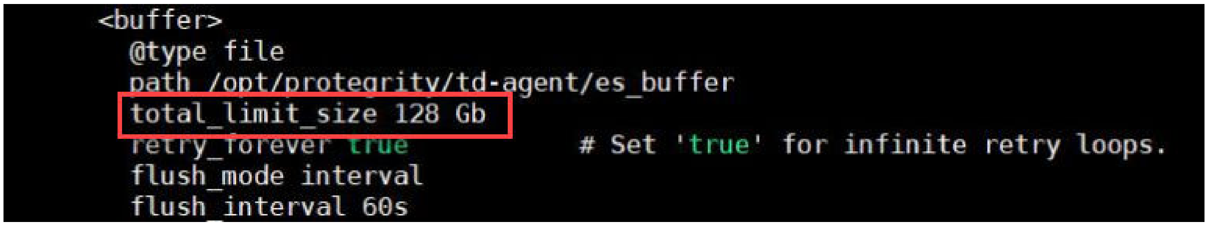
  4. Navigate to the `/opt/protegrity/td-agent/config.d` directory.
  5. Open the `OUTPUT.conf` file.
  6. Add the *total_limit_size* parameter in the buffer section of the `OUTPUT.conf` file.

In this example, the *total_limit_size* is doubled to **128 GB**.



```
    <buffer>
      @type file
      path /opt/protegrity/td-agent/es_buffer
      retry_forever true           # Set 'true' for infinite retry loops.
      flush_mode interval
      flush_interval 60s
```

Figure 5-2: Before Update



```
    <buffer>
      @type file
      path /opt/protegrity/td-agent/es_buffer
      total_limit_size 128 Gb
      retry_forever true           # Set 'true' for infinite retry loops.
      flush_mode interval
      flush_interval 60s
```

Figure 5-3: Updated `OUTPUT.conf` *File*

7. Save the file.
8. Start the *td-agent* service using the following command:

```
/etc/init.d/td-agent start
```

> **Note:** You can also start the service by logging into the ESA Web UI, navigating to **System** > **Services**, and starting the **td-agent** service under **Misc**.

- **Known Issue:** The **Too many open files** error appears in the */var/log/td-agent/td-agent.log* file.

  Description: When the total number of files in the *td-agent* buffer */opt/protegrity/td-agent/es_buffer* directory reaches the maximum limit, then the **Too many open files** error appears.

  Resolution:

  Change the limit for the maximum number of open files for the *td-agent* service in the */etc/init.d/td-agent* file using the following steps.

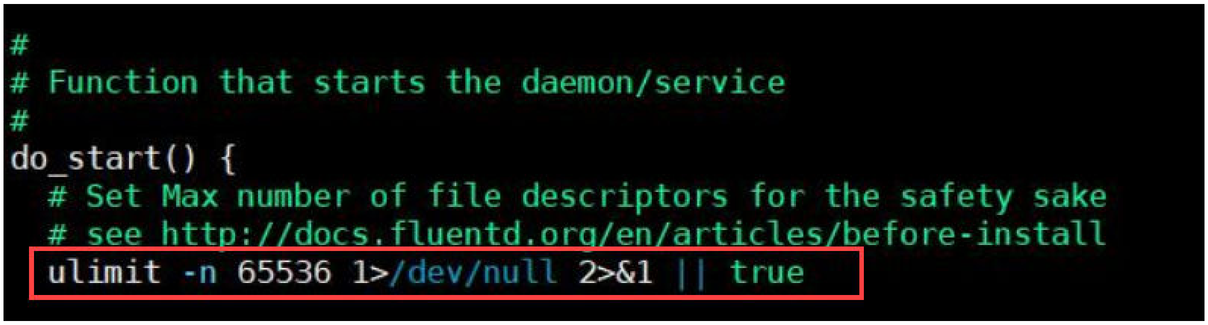
  1. Login to the CLI Manager of the ESA node.
  2. Navigate to **Administration** > **OS Console**.
  3. Stop the *td-agent* service using the following command:

  ```
  /etc/init.d/td-agent stop
  ```

  > **Note:** You can also stop the service by logging into the ESA Web UI, navigating to **System** > **Services**, and stopping the **td-agent** service under **Misc**.

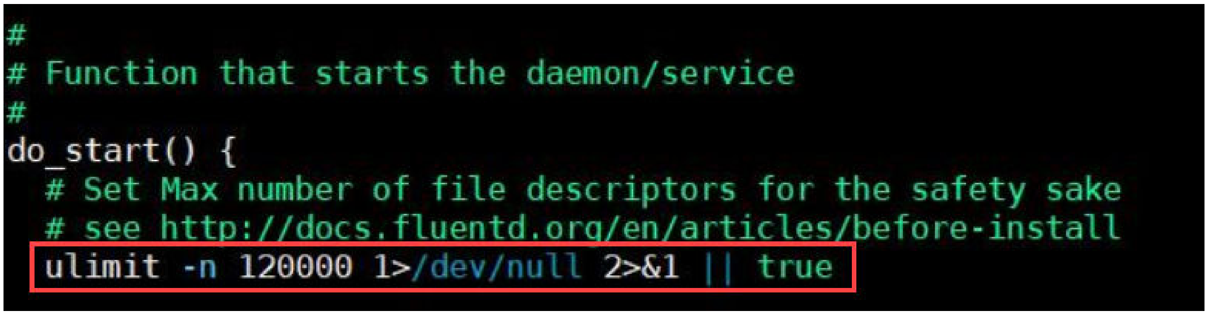
  4. Navigate to the `/etc/init.d` directory.
  5. Open the `td-agent` file.
  6. Change the *ulimit*.

     In this example, the *ulimit* is increased to **120000**.



```
#
# Function that starts the daemon/service
#
do_start() {
  # Set Max number of file descriptors for the safety sake
  # see http://docs.fluentd.org/en/articles/before-install
  ulimit -n 65536 1>/dev/null 2>&1 || true
```

Figure 5-4: Before Update



```
#
# Function that starts the daemon/service
#
do_start() {
  # Set Max number of file descriptors for the safety sake
  # see http://docs.fluentd.org/en/articles/before-install
  ulimit -n 120000 1>/dev/null 2>&1 || true
```

Figure 5-5: Updated `td-agent` *File*

7. Save the file.
8. Start the *td-agent* service using the following command:

```
/etc/init.d/td-agent start
```

> **Note:** You can also start the service by logging into the ESA Web UI, navigating to **System** > **Services**, and starting the **td-agent** service under **Misc**.

5.3.2 Known Issues for the Log Forwarder

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

Known Issue: The Protector is unable to reconnect to a Log Forwarder after it is restarted.

Description: This issue occurs whenever you have a Proxy server between a Protector and a Log Forwarder. When the Log Forwarder is stopped, the connection between the Protector and the Proxy server is still open, even though the connection between the Proxy server and the Log Forwarder is closed. As a result, the Protector continues sending audit files to the Proxy server. This results in loss of the audit files. Whenever the Log Forwarder is restarted, the Protector is unable to reconnect to the Log Forwarder.

This issue is applicable to all the Protectors where the Log Forwarder is not running on the local host machine. For example, this issue is applicable to AIX or z/OS protectors because the Log Forwarder is not running on the same machine where the Protectors have been installed. This issue also occurs if you have a Load Balancer or a Firewall between the Protector and the Log Forwarder, instead of a Proxy server.

Resolution: Remove the Proxy server or ensure that you configure the Proxy server in a way that the connection between the Protector and the Proxy server is stopped as soon as the Log Forwarder is stopped. This ensures that whenever the Log Forwarder is restarted, the Protector reconnects with the Log Forwarder and continues to send the audits to the Log Forwarder without any data loss.

For more information about configuring the Proxy server, contact your IT administrator.

5.3.3 Known issues for the Audit Store

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

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

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

  Workaround

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

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

  Issue:

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

  Resolution:

  Perform one of the following steps to resolve the issue:

  - Delete old indices that are not required using ILM in Analytics.
  - Increase the disk space on all nodes.
  - Add new nodes to the cluster.

- **Known Issue**: The *Upgrade cannot continue as the cluster health status is red. Check out the Troubleshooting Guide for info on how to proceed.* error message appears.

  Issue: A cluster status in red color means that at least one primary shard and its replicas are not allocated to a node, that is, there are indices with the index health status in red color in the Audit Store cluster.

  Workaround

  Complete the following steps to resolve the cluster health with the red status.

  a. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.
  b. Ensure that the **Audit Store Repository** service is running.
  c. Login to the CLI Manager of the ESA.
  d. Navigate to **Administration** > **OS Console**.
  e. Enter the *root* password.
  f. Identify the indices with the health status as *red* using the following command:

  ```
  wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
  certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
  client.key -O - https://<Appliance_IP>:9200/_cat/indices | grep red
  ```

Ensure that you update the variables before running the command. An example of the command is provided here.

```
wget -q --ca-cert=/etc/ksa/certificates/as_cluster/CA.pem --certificate=/etc/ksa/
certificates/as_cluster/client.pem --private-key=/etc/ksa/certificates/as_cluster/
client.key -O - https://ESA_IP:9200/_cat/indices | grep red
```

A list of indices containing the health status as red appears as shown in the following example.

```
red    open   pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014
dxmEWom8RheqOhnaFeM3sw   1   1
```

In the example, *pty_insight_audit_vx.x-xxxx.xx.xx-000014* is the index having a red index health status where the index's primary shard and replicas are not available or allocated to any node in the cluster.

g. Identify the reason for unassigned shards using the following command.

```
wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
client.key -O - https://<Appliance_IP>:9200/_cat/shards?
h=index,shard,prirep,state,unassigned.reason | grep UNASSIGNED
```

Ensure that you update the variables before running the command. An example of the command is provided here.

```
wget -q --ca-cert=/etc/ksa/certificates/as_cluster/CA.pem
--certificate=/etc/ksa/certificates/as_cluster/client.pem --private-key=/etc/ksa/
certificates/as_cluster/client.key -O - https://ESA_IP:9200/_cat/shards?
h=index,shard,prirep,state,unassigned.reason | grep UNASSIGNED
```

The reasons for the shards being unassigned appear. This example shows one of the reasons for the unassigned shard.

```
    `pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014             0 p UNASSIGNED
NODE_LEFT`

    `pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014             0 r UNASSIGNED
NODE_LEFT`
```

In the example, the *0*th *p* and *r* shards of the *pty_insight_analytics_audit_ vx.x-xxxx.xx.xx-000014* index are unassigned due to the *NODE_LEFT* reason, that is, because the node left the Audit Store cluster. The *p* indicates a primary shard and the *r* indicates a replica shard.

h. Retrieve the details for the shard being unassigned using the following command.

```
wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
client.key --header='Content-Type:application/json' --method=GET --body-
data='{ "index": "<Index_name>", "shard": <Shard_ID>, "primary":<true or false> }' -O -
https://<Appliance_IP>:9200/_cluster/allocation/explain?pretty
```

Ensure that you update the variables before running the command. An example of the command with the index name as *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014*, shard ID as 0, and primary shard as true is provided here.

```
wget -q --ca-cert=/etc/ksa/certificates/as_cluster/CA.pem --certificate=/etc/ksa/
certificates/as_cluster/client.pem --private-key=/etc/ksa/certificates/as_cluster/
client.key --header='Content-Type:application/json' --method=GET --body-
data='{ "index": "pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014", "shard": 0,
"primary": true }' -O - https://ESA_IP:9200/_cluster/allocation/explain?pretty
```

The details of the unassigned shard appears. This example shows one of the reasons for the unassigned shard.

```
{
        "index": "pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014",
        "shard": 0,
        "primary": true,
        "current_state": "unassigned",
        "unassigned_info": {
            "reason": "NODE_LEFT",
            "at": "2022-03-28T05:05:25.631Z",
            "details": "node_left [gJ38FzlDSEmTAPcP0yw57w]",
            "last_allocation_status": "no_valid_shard_copy"
        },
        "can_allocate": "no_valid_shard_copy",
        "allocate_explanation": "cannot allocate because all found copies of the shard
are either stale or corrupt",
        "node_allocation_decisions": [
            {
                "node_id": "3KXS1w9HTOeMH1KbDShGIQ",
                "node_name": "ESA1",
                "transport_address": "xx.xx.xx.xx:9300",
                "node_attributes": {
                    "shard_indexing_pressure_enabled": "true"
                },
                "node_decision": "no",
                "store": {
                    "in_sync": false,
                    "allocation_id": "HraOWSZlT3KNXxOHDhZL5Q"
                }
            }
        ]
    }
```

In this example, the shard is not allocated because *all found copies of the shard are either stale or corrupt*. There are no valid shard copies that can be allocated for this index. This is a *data loss scenario*, where the data is unavailable because the node or nodes that had the data have disconnected from the cluster. In such a scenario, if the disconnected nodes are brought back in the cluster, then the cluster can reconstruct itself and become healthy again. If bringing the nodes back is not possible, then deleting indices with the red index health status is the only way to fix a red cluster health status.

i. Complete one of the following two steps to stabilize the cluster.

   - **Troubleshoot the cluster:**

     i. Verify that the Audit Store services are running. Restart any Audit Store service that is in the stopped state.

     ii. Ensure that the disconnected nodes are running.

     iii. Try to add any disconnected nodes back to the cluster.

     iv. Restart the system or restore the system from a backup..

   - **Delete the index:**

     Delete the indices with the index health status as red using the following command. Execute the command from any one node of Audit Store node which is running.

     ```
     wget -q --ca-cert=<Path_to_CA_certificate>/
     CA.pem --certificate=<Path_to_client_certificate>/client.pem --private-
     key=<Path_to_client_key>/client.key --header='Content-Type:application/json' --
     method=DELETE -O - https://<Appliance_IP>:9200/<Index_name>
     ```

     Ensure that you update the variables before running the command. An example of the command to delete the *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014* index is provided here.

     ```
     wget -q --ca-cert=/etc/ksa/certificates/as_cluster/CA.pem --certificate=/etc/ksa/
     certificates/as_cluster/client.pem --private-key=/etc/ksa/certificates/as_cluster/
     client.key --header='Content-Type:application/json' --method=DELETE -O - https://
     ESA_IP:9200/pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014
     ```

     > **Caution:** This command deletes the index and must be used carefully.

- **Known Issue:** High memory usage on the ESA.

  Issue:

When using the Audit Store, the memory usage is high on the ESA.

Workaround:

Reduce the memory usage by updating the memory allocated to the Audit Store on the ESA to **4** GB using the **Set Audit Store Repository Total Memory** CLI option.

For more information about the **Set Audit Store Repository Total Memory** CLI option, refer to the section *Setting the Total Memory for the Audit Store Repository* in the *Audit Store Guide 9.2.0.0*.

- **Known Issue:** The *FATAL: Failed to apply security configs to Audit Store Repository, exitcode=6.* message appears in the **Notifications** on the dashboard of the ESA..

  Issue:

  The *exitcode=6*, indicates that there was an issue while applying the Audit Store security configuration.

  Workaround:

  Try to apply the Audit Store security configurations using the following steps:

  1. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.
  2. Ensure that the **Audit Store Repository** service is running.
  3. Login to the CLI Manager of the ESA.
  4. Navigate to **Administration** > **OS Console**.
  5. Enter the *root* password.
  6. Run the following command:

     ```
     /opt/protegrity/auditstore/management/scripts/apply_security_configs.sh --first-install
     ```

  If the issue still persists after running the command, then contact Protegrity Support.

- **Known Issue:** The *Unable to connect to the Audit Store: security is not initialized. Refer to the Protegrity Troubleshooting Guide to resolve this issue.* message appears on the **Audit Store** > **Cluster Management** page.

  Issue:

  The message appears after installing the ESA, when the user navigates to the **Cluster Management** page.

  Workaround:

  Try to apply the Audit Store security configurations using the following steps:

  1. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.
  2. Ensure that the **Audit Store Repository** service is running.
  3. Login to the CLI Manager of the ESA.
  4. Navigate to **Administration** > **OS Console**.
  5. Enter the *root* password.
  6. Run the following command:

     ```
     /opt/protegrity/auditstore/management/scripts/apply_security_configs.sh --first-install
     ```

  If the issue still persists after running the command, then contact Protegrity Support.

- **Known Issue:** The *Failed to join <IP_address> node cluster! Audit Store Repository client is unavailable. Unable to connect to the Audit Store: security is not initialized. Refer to the Protegrity Troubleshooting Guide to resolve this issue.* message appears on the **Audit Store** > **Cluster Management** page.

  Issue:

The issue occurs when there is an issue with the certificate, such as, the node is unavailable, certificate exception, or certificate information is incomplete. The message is displayed when the user navigates to the **Cluster Management** page.

Workaround:

Try to apply the Audit Store security configurations using the following steps:

1. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.
2. Ensure that the **Audit Store Repository** service is running.
3. Navigate to **Logs** > **Appliance**, select **auditstore** from the list.
4. Search for any certificate-related error messages, such as, *CertificateException*. For example, *Caused by: java.security.cert.CertificateException: No subject alternative DNS name matching ip-192-168-0-10.protegrity.comp found*. If any certificate-related errors are displayed, then complete the following steps before continuing:
    a. Fix the certificate by re-creating the certificate with the correct configuration.
    b. Update the certificate on the target node, that is, the node that the joining node tried to connect.

       For more information about certificates, refer to the section *Audit Store Certificates* in the *Protegrity Certificate Management Guide 9.2.0.0*.

    c. Rotate the certificate on the joining node, using the target node address for the input while rotating the certificate.

       For more information about rotating certificates, refer to the section *Updating Audit Store custom certificates* in the *Audit Store Guide 9.2.0.0*.

    d. Verify that the **Cluster Management** page loads with the following *Failed to join <IP_address> node cluster! Audit Store Repository client is unavailable.* notification.
    e. Dismiss the notification.
    f. Verify that the node is part of the cluster from the **Nodes** tab.
5. Remove the node from the Audit Store cluster.
6. Add the node again to the Audit Store cluster for the internal cluster operations to complete successfully.

If the issue still persists after running the command, then contact Protegrity Support.

5.3.4 Resolving Logging-Related Issues During an Upgrade

This section details the issues and resolutions for errors that might appear during the upgrade.

- **Known Issue**: The *Timeout reached while waiting for cluster health status to be green.* error message is displayed.

  Issue: This issue appears when the timeout set for verifying the Audit Store cluster health status to be green is reached.

  Workaround

  Wait for the cluster health status to turn green.
- **Known Issue**: The *Timeout reached while waiting for shard initialization/relocation to complete.* error message is displayed.

  Issue: This issue appears when the shard initialization and allocation process takes time and the timeout set for verifying the process is reached.

  Workaround

  Wait for the shard allocation process to complete.
- **Known Issue**: The *Upgrade cannot continue as the cluster shard allocation is not enabled for all shards. Check out the Troubleshooting Guide for info on how to proceed.* error message is displayed.

  Issue: This issue appears when the *cluster.routing.allocation.enable* configuration is not set to *all* and therefore there are unassigned shards in the cluster.

Workaround

Set the configuration value to *all* using the following steps.

a. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.

b. Ensure that the **Audit Store Repository** service is running.

c. Login to the CLI Manager of the Appliance.

d. Navigate to **Administration** > **OS Console**.

e. Run the following command to update the configuration:

```
wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
client.key --header='Content-Type:application/json' --method=PUT --body-data
'{  "persistent": {    "cluster.routing.allocation.enable": null  }}' -O - https://
<Appliance_IP>:9200/_cluster/settings
```

Note: Ensure that you update the variables before running the command. An example of the command is provided here.

```
wget -q --ca-cert=/etc/ksa/certificates/es_rest/CA.pem --certificate=/etc/ksa/
certificates/es_rest/client.pem --private-key=/etc/ksa/certificates/es_rest/
client.key --header='Content-Type:application/json' --method=PUT --body-data
'{  "persistent": {    "cluster.routing.allocation.enable": null  }}' -O - https://
ESA_IP:9200/_cluster/settings
```

- **Known Issue**: The *Upgrade cannot continue as there are only {master_node_count} master-eligible nodes available in the cluster including the current node. Add one or more master-eligible nodes to proceed with the upgrade.* error message appears.

  Issue: This issue appears when number of master-eligible nodes in the Audit Store cluster is insufficient.

  ### Workaround

  Add additional ESA nodes to the Audit Store cluster and continue the upgrade.

  For more information about understanding about the Audit Store clustering and adding nodes to the cluster, refer to the section *Adding an ESA to the Audit Store Cluster* in the *Protegrity Installation Guide 9.2.0.0*.

- **Known Issue**: The *Upgrade cannot continue as current node is the only data node available in the cluster. Add one or more data nodes to proceed with the upgrade.* error message appears.

  Issue: This issue appears when number of Data nodes in the Audit Store cluster is insufficient.

  ### Workaround

  Add additional ESA nodes to the Audit Store cluster and continue the upgrade.

  For more information about understanding about the Audit Store clustering and adding nodes to the cluster, refer to the section *Adding an ESA to the Audit Store Cluster* in the *Protegrity Installation Guide 9.2.0.0*.

- **Known Issue**: The *Upgrade cannot continue as the cluster health status is red. Check out the Troubleshooting Guide for info on how to proceed.* error message appears.

  Issue: A cluster status in red color means that at least one primary shard and its replicas are not allocated to a node, that is, there are indices with the index health status in red color in the Audit Store cluster.

  ### Workaround

  Complete the following steps to resolve the cluster health with the red status.

  a. From the Web UI of the Appliance, navigate to **System** > **Services** > **Audit Store**.

b. Ensure that the **Audit Store Repository** service is running.

c. Login to the CLI Manager of the Appliance.

d. Navigate to **Administration** > **OS Console**.

e. Identify the indices with the health status as *red* using the following command:

   ```
   wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
   certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
   client.key -O - https://<Appliance_IP>:9200/_cat/indices | grep red
   ```

   Ensure that you update the variables before running the command. An example of the command is provided here.

   ```
   wget -q --ca-cert=/etc/ksa/certificates/es_cluster/CA.pem --certificate=/etc/ksa/
   certificates/es_cluster/client.pem --private-key=/etc/ksa/certificates/es_cluster/
   client.key -O - https://ESA_IP:9200/_cat/indices | grep red
   ```

   A list of indices containing the health status as red appears as shown in the following example.

   ```
   `red    open   pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014
   dxmEWom8RheqOhnaFeM3sw   1   1
   ```

   In the example, *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014* is the index having a red index health status where the index's primary shard and replicas are not available or allocated to any node in the cluster.

f. Identify the reason for unassigned shards using the following command.

   ```
   wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
   certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
   client.key -O - https://<Appliance_IP>:9200/_cat/shards?
   h=index,shard,prirep,state,unassigned.reason | grep UNASSIGNED
   ```

   Ensure that you update the variables before running the command. An example of the command is provided here.

   ```
   wget -q --ca-cert=/etc/ksa/certificates/es_cluster/CA.pem
   --certificate=/etc/ksa/certificates/es_cluster/client.pem --private-key=/etc/ksa/
   certificates/es_cluster/client.key -O - https://ESA_IP:9200/_cat/shards?
   h=index,shard,prirep,state,unassigned.reason | grep UNASSIGNED
   ```

   The reasons for the shards being unassigned appear. This example shows one of the reasons for the unassigned shard.

   ```
       `pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014             0 p UNASSIGNED
   NODE_LEFT`

       `pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014             0 r UNASSIGNED
   NODE_LEFT`
   ```

   In the example, the *0*th *p* and *r* shards of the *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014* index are unassigned due to the *NODE_LEFT* reason, that is, because the node left the Audit Store cluster. The *p* indicates a primary shard and the *r* indicates a replica shard.

g. Retrieve the details for the shard being unassigned using the following command.

   ```
   wget -q --ca-cert=<Path_to_CA_certificate>/CA.pem --
   certificate=<Path_to_client_certificate>/client.pem --private-key=<Path_to_client_key>/
   client.key --header='Content-Type:application/json' --method=GET --body-
   data='{ "index": "<Index_name>", "shard": <Shard_ID>, "primary":<true or false> }' -O -
   https://<Appliance_IP>:9200/_cluster/allocation/explain?pretty
   ```

   Ensure that you update the variables before running the command. An example of the command with the index name as *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014*, shard ID as 0, and primary shard as true is provided here.

   ```
   wget -q --ca-cert=/etc/ksa/certificates/es_cluster/CA.pem --certificate=/etc/ksa/
   certificates/es_cluster/client.pem --private-key=/etc/ksa/certificates/es_cluster/
   client.key --header='Content-Type:application/json' --method=GET --body-
   ```

```
data='{ "index": "pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014", "shard": 0,
"primary": true }' -O - https://ESA_IP:9200/_cluster/allocation/explain?pretty
```

The details of the unassigned shard appears. This example shows one of the reasons for the unassigned shard.

```
{
        "index": "pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014",
        "shard": 0,
        "primary": true,
        "current_state": "unassigned",
        "unassigned_info": {
            "reason": "NODE_LEFT",
            "at": "2022-03-28T05:05:25.631Z",
            "details": "node_left [gJ38FzlDSEmTAPcP0yw57w]",
            "last_allocation_status": "no_valid_shard_copy"
        },
        "can_allocate": "no_valid_shard_copy",
        "allocate_explanation": "cannot allocate because all found copies of the shard
are either stale or corrupt",
        "node_allocation_decisions": [
            {
                "node_id": "3KXS1w9HTOeMH1KbDShGIQ",
                "node_name": "PSU1",
                "transport_address": "xx.xx.xx.xx:9300",
                "node_attributes": {
                    "shard_indexing_pressure_enabled": "true"
                },
                "node_decision": "no",
                "store": {
                    "in_sync": false,
                    "allocation_id": "HraOWSZlT3KNXxOHDhZL5Q"
                }
            }
        ]
    }
```

In this example, the shard is not allocated because *all found copies of the shard are either stale or corrupt*. There are no valid shard copies that can be allocated for this index. This is a *data loss scenario*, where the data is unavailable because the node or nodes that had the data have disconnected from the cluster. In such a scenario, if the disconnected nodes are brought back in the cluster, then the cluster can reconstruct itself and become healthy again. If bringing the nodes back is not possible, then deleting indices with the red index health status is the only way to fix a red cluster health status.

h. Complete one of the following two steps to stabilize the cluster.

- Try to bring the disconnected nodes back up and wait for the cluster health status to become non-red by adding the disconnected nodes back to the cluster, restarting the system, or restoring the system from a backup.
- Delete the indices with the index health status as red using the following command.

  ```
  wget -q --ca-cert=<Path_to_CA_certificate>/
  CA.pem --certificate=<Path_to_client_certificate>/client.pem --private-
  key=<Path_to_client_key>/client.key --header='Content-Type:application/json' --
  method=DELETE -O - https://<Appliance_IP>:9200/<Index_name>
  ```

  Ensure that you update the variables before running the command. An example of the command to delete the *pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014* index is provided here.

  ```
  wget -q --ca-cert=/etc/ksa/certificates/es_cluster/CA.pem --certificate=/etc/ksa/
  certificates/es_cluster/client.pem --private-key=/etc/ksa/certificates/es_cluster/
  client.key --header='Content-Type:application/json' --method=DELETE -O - https://
  ESA_IP:9200/pty_insight_analytics_audit_vx.x-xxxx.xx.xx-000014
  ```

  Caution: This command deletes the index and must be used carefully.

5.4 PEP Server Common Errors (Database, Application and Big Data Protectors)

PEP Server logs its operations in pepserver.log file on the machine where PEP Server is installed. This file reports about version of PEP Server and time left till the license will expire. When in some cases PEP Server does not start, you can examine this file for details.

This section explains the common errors and problems users may encounter while working with Database, Application, and Big Data Protectors.

Table 5-8: PEP Common Errors

Error /Problem	This may happen because…	Recovery
Fail to deploy policy to the machine where PEP Server is running.	ESA host name or IP address was not specified during PEP Server installation. *pepserver.log* has the following record: (WARNING) Failed to connect to localhost:15500 (Code=-4 : Timeout!)	Change the host to the ESA IP address in *ESA connectivity information* section in *pepserver.cfg* and restart the PEP Server.
	PEP Server has no certificates or the wrong certificates of the ESA from which the policy is being deployed.	Verify that the PEP Server machine has certificates of the correct ESA.
Failure to start PEP Server.	Required keys and certificates can be missing. Any edited parameters in *pepserver.cfg* may have incorrect settings.	Check the *pepserver.log* for Warnings or Errors (set logging level to ALL), fix the problem indicated in the log and start the PEP Server.
	Any edited parameters in *pepserver.cfg* may have errors in syntax.	Run PEP Server in verbose mode (using -verbose parameter) to display errors preventing PEP Server start.
Newly added user is not able to protect/ unprotect data.	User is added to the External Source but not yet synchronized with ESA.	If your role is automatic, then wait until role members are synchronized automatically from the external source to ESA (default synchronization interval is 1 hour). The updated policy is deployed automatically after the synchronization. If your role is semi-automatic, then synchronize members manually using the **Synchronize** button in Roles under Policy management in ESA. If your role is manual, then directly add new members by updating the role, and re-deploy the policy. For more information about role refresh mode types, refer to section *Role Mode Types* in the *Policy Management Guide 8.0.0.0*. If your role failed to synchronize using the **Synchronize** button in Roles under Policy management in ESA, then you need to verify whether your configuration of the External Source in Policy management in ESA is still valid.

Error /Problem	This may happen because…	Recovery
	User is synchronized with ESA but not yet synchronized with PEP Server.	For automatic role type, wait until role members are synchronized automatically from ESA to PEP Server (default synchronization interval is 24h, configurable in pepserver.cfg). For more information about other role refresh mode types, refer to section *Role Mode Types* in the *Policy Management Guide 8.0.0.0*. For immediate synchronization of members from ESA to PEP Server, re-deploy the policy. If the role failed to get synchronized after the required time interval or after re-deploying the policy, then check the pepserver.log for errors and ensure the ESA communication parameter in pepserver.cfg points to the valid ESA host. Check network connectivity and make sure that the traffic from PEP Server to ESA is not blocked by network, for example, by firewall rules.
Policy is locked due to an expired license.	The current date is past the end date of your license.	Request a license from Protegrity by generating a license request and providing it to Protegrity (for details refer to Protegrity Data Security Platform Licensing document). Make sure that the time is correct on the machine where the PEP Server is installed. If not, then change it to the correct time and restart the PEP Server.
Policy is locked due to an invalid license.	ESA was activated with the wrong license file or a tampered license file.	Ensure that ESA has a valid license (request a new license if needed). Ensure that the machine where the PEP Server is installed has a valid date and time (in sync with the ESA date and time). Restart the PEP Server and re-deploy the policy with the valid license.
Audit records are not sent to ESA.	Log Server host/port is incorrect, or not reachable by network (for example, blocked by Firewall blocking traffic, etc.).	Specify the correct Log Server host/port, and restart the PEP Server.
	PEP Server does not recognize the cash file pepserverb1.dat due to connectivity or other issues.	Stop the PEP Server, delete the *pepserverloginfo.dat* and restart the PEP Server.
License expiration date is not accurate in ESA.	The date and time of the PEP servers and ESA are out of sync.	Ensure that the time zone, date and time set up in the ESA and the PEP servers are accurate according to their locations and restart the services.
PEP Server starts with an empty repository (with no policy deployed).	The PEP Server repository (*pepserver.db*) has been compromised.	Check for any unauthorised access to the machine where PEP Server is installed.

Error /Problem	This may happen because…	Recovery
Policy is compromised log is available in ESA Forensics.		Review pepserver.log for details. Redeploy the policy.
AP Client fails to open a session.	By default, XC listener ports are disabled in *pepserver.cfg*. On attempt to use AP Client, you will have the following error: XCOpenSession failed: Failed to connect to server.	Uncomment the XC listener ports (TCP or/and SSL) in *pepserver.cfg* and restart the PEP Server.
Failure to execute multiple queries when using multiple data elements.	When using multiple data elements, there is a limitation on the number of queries that can be executed in an instance.	1. If you are using multiple data elements, then ensure the queries are sent in batches of 50, at most. 2. If additional queries are to be sent, then perform the following steps. a. Log out of the database. b. Re-login to the database. c. Insert the next batch of queries. **Note:** This limitation persists in Oracle 12c versions prior to version 12.1.2.0.
If you are using the pepsrvctl utility, which is located in the `<PROTEGRITY_DIR>/defiance_dps/bin/` directory, then all the running PEP server instances are stopped on executing the following command. `pepsrvctl stop all`	The stop all parameter provided for the *pepsrvctl* utility iteratively kills all the PEP server instances that are running on the node.	This issue has no recovery action as it is expected behavior. If you need to stop a specific PEP server instance, then navigate to the `<PROTEGRITY_DIR>/defiance_dps/bin/` directory on the required PEP server to be stopped, and run the following command. `pepsrvctl stop`
If you have entered wrong combination of cases for policy user names, then the following error message is displayed in the Logs tab under Forensics in ESA GUI. *`The username could not be found in the policy in shared memory.`*	Policy user names are case sensitive as a default. You might have entered incorrect user name or incorrect combination of cases.	Enable the case insensitive user name in the PEP Server: 1. Navigate to the `opt/protegrity/defiance_dps/data/` directory of the protector. 2. Open the *pepserver.cfg* file in a text editor. 3. Under the [member] section, uncomment the case-sensitive parameter and set the value as *no*. case-sensitive = no 4. Restart the PEP Server.
The following exception appears when high volume of queries is run on SQL Server Management Studio (SSMS):	The memory allocation in SSMS for large results is insufficient.	It is recommended to use the sqlcmd utility to run queries.

Error /Problem	This may happen because…	Recovery
`Exception of type System.OutOfMemoryException was thrown`		
If you are performing bulk deletion of policy management components, such as data elements, masks, data stores, or Trusted Applications in one instance, then a single Audit Log is generated. The Audit Log description captures the first deleted component and the extended information captures all the deletions, except the first component that is deleted. For instance, if the data elements DE1, DE2, DE3, and DE4 are deleted, then the Audit Log description captures the deletion of the data elements DE1 and the extended information captures the deletion of the data elements DE2, DE3, and DE4 only.	This is a limitation of the way in which current Audit Logs are captured for data elements, masks, data stores, and Trusted Applications.	This issue has no recovery action as it is expected behavior.
When trying to restart or shutdown the PEP Server in a windows platform, we get the following error: *`Error 1503: The service did not respond to the start or control request in a timely fashion`*.	If a policy download is in progress during the PEP Server shutdown, then it results in this error.	Check for the policy download status from the PEP Server logs. Once the policy download is successful, you must then restart or shutdown the PEP Server.
Connection timeout error stating ‘Failed to send request to Pep Server: Connection timed out’ occurs.	When running the hubcontroller service within a vCloud system, persistent connection requests results in a timeout error.	Perform the following steps. 1. From the OS Console, navigate to `/opt/protegrity/hubcontroller/conf` directory. 2. In the pepserver settings field, set the *idle_timeout* (hidden) configuration parameter to a time interval for which the persistent connection should remain active. If you set *idle_timeout* configuration parameter to 0, the timeout is disabled. The specified timeout must be less than the vCloud connection dropout time, which is 60 minutes.
PEP Server sends the error ‘Integrity check failed on metering file’ to the ESA when you rotate and then destroy the data store key (DSK) after stopping the PEP Server.	The PEP Server stores the *metering.json* file, which is also signed with the data store key (DSK) on the disk. If you stop the PEP Server now, rotate and destroy this DSK on the ESA, and then start the PEP Server, the PEP Server considers the *metering.json* file to be tampered; it sends "Integrity check failed on metering file" log message to the ESA.	Perform the following steps: 1. Stop the PEP Server. 2. Delete the *metering.json* file. 3. Start the PEP Server.
The policy download fails when you rotate and destroy the data store key (DSK) and then start the PEP Server again.	If you perform security operations on the PEP Server and then stop the PEP Server, it records the forensics for the performed security operations locally in an audit (*.*dat*)	Perform the following steps: 1. Stop the PEP Server.

Error /Problem	This may happen because…	Recovery
	file. This file is encrypted by the data store key (DSK) and the *metering.json* file is also signed with this DSK. Now, if you rotate and destroy this DSK on the ESA and then start the PEP Server, the PEP Server considers the metering.json file to be tampered; it sends "Integrity check failed on metering file" log message to the ESA. The PEP Server is also unable to decrypt the audit (**.dat*) file, since the DSK that is used to encrypt the audit file is destroyed. Hence, the PEP Server ceases to download the policy.	2. Delete the *metering.json* file. 3. Start the PEP Server. It will now automatically convert the *.dat* file to *.elf* (error log file) file.
After the Teradata Database Protector is provisioned with a new ESA, an *Unknown* connectivity status appears on the ESA dashboard for the Database Protector and the following warning message appears in the *pepserver.log* file. `Failed to post message to ESA: https://<ESA IP>/dps/v1/deployment/nodes, Unauthorized`	Incorrect *CN* attribute of the *client certificate*	When you create a *CA-signed client certificate* to use with an ESA, it is mandatory to keep the *CN* attribute of the *client certificate* as *Protegrity Client*. For more information about the certificate management in ESA, refer to *Certificate Management Guide*.
Observing inconsistent results while tokenizing and detokenizing data on the Oracle database. If you try to insert a clear text data and the update the column using the *upd_varchar2()* UDF, then the data element is supposed to leave last 4 digit in clear text, but it is not working in the expected way.	This may happen because if you are using the preserved length data type and the data inserted is less than the length of the data type defined. While storing the data in the database, the Oracle would append additional character set.	• Change the datatype to varchar2. • Use *trim()* with the *char()* datatype.
If you are using AP Java and trying to reprotect bulk data, and the reprotect operation fails for each data item passed in the bulk call, then an audit log is generated for each data item, instead of a single audit log for the bulk data.	This is a limitation in the way audit logs are generated for bulk data.	This issue has no recovery action as it is expected behavior.
When you are using AP Java and trying to protect, unprotect, or reprotect data, an audit log is not generated in ESA, and the following error message is displayed on the console: `Input is null or not within allowed limits.`	The length of the data element name exceeds 55 characters.	Ensure that the data element name does not exceed 55 characters.

The PEP server application stops on a Linux-based OS. The following error occurs.
`(SEVERE) Failed to create shared memory of size 402653184 bytes: Invalid argument (Code=-1 : Invalid parameter!)`
	This issue may occur due to insufficient shared memory size.	The following snippet displays the steps to increase the maximum size in bytes for the shared memory segment. It increases the SHMMAX value to 500MB.
		`SHMMAX= cat /proc/sys/kernel/shmmax`
		`echo "kernel.shmmax=$SHMMAX" >> /etc/sysctl.conf`
		`echo 500000000 > /proc/sys/kernel/shmmax`

Error /Problem	This may happen because…	Recovery
		`sysctl -w kernel.shmmax=500000000` Start the PEP server.
When deploying policies that contain a large number of token elements, the PEP server stops abruptly. In addition, issues related to exceeding the disk space or failure in creating a request log record occur.	This issue may occur if large number of token elements are part of a policy. When the PEP server downloads the policy, the token element size exceeds the shared memory size.	Perform the following steps: • Consider increasing the disk size or allocate free space on the disk. • Redeploy the policy by removing all the token elements from the policy. You must then add the amount of token elements to the policy that can load successfully and redeploy.

Table 5-9: Common Tokenization Errors

Error /Problem	This may happen because…	Recovery
Tokenization fails with `Tokenization is disabled` message.	Tokenization is disabled in *pepserver.cfg* file.	Enable tokenization in *pepserver.cfg* file by setting: tokenproc = pep Restart the PEP Server.
Protect, unprotect, and reprotect operations fail with `Invalid parameter` error.	Length of the data element name, which is passed as a parameter to the Protect, Unprotect, or Reprotect API, exceeds 55 characters.	Ensure that the data element name does not exceed 55 characters.

5.5 Protectors Security Logs

All protectors log the results of the protection operations.

The security logging level can be configured when a data security policy is created in the Policy management in ESA. If logging level is set to *audit successful* and *audit failed*, then both successful and failed Unprotect/Protect/Reprotect/Delete operations will be logged.

You can define the server where these security audit logs will be sent to. You can do that by modifying the Log Server configuration section in *pepserver.cfg* file.

If you configure to send protector security logs to ESA, you will be able view them in the ESA Web Interface, **Protegrity Analytics** > **Forensics**. The following table displays the logs sent by protectors.

Table 5-10: PEP Return Codes

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
0	S	Internal ID when audit record should not be generated.	-	-	-	-	-	-	XC_LOG_NONE	No action is required.

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
1	W	The username could not be found in the policy.	No such user	URPD	1	01H01 or U0001	20101	38821	XC_LOG_USER_NOT_FOUND	Verify that the user that calls a PTY function is in the policy. Ensure that your policy is synchronized across all Teradata nodes. Make sure that the ESA connectivity information is correct in the *pepserver.cfg* file.
2	W	The data element could not be found in the policy.	No such data element	URPD	2	U0002	20102	38822	XC_LOG_DATA_ELEMENT_NOT_FOUND	Verify that you are calling a PTY function with data element that exists in the policy.
3	W	The user does not have the appropriate permissions to perform the requested operation.	Permission denied	URPD	3	01H03 or U0003	20103	38823	XC_LOG_PERMISSION_DENIED	Verify that you are calling a PTY function with a user having access permissions to perform this operation according to the policy.
4	E	Tweak is null.	Tweak null	URPD	4	01H04 or U0004	20104	38824	XC_LOG_TWEAK_NULL	Ensure that the tweak is not a null value.

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
5	W	Integrity check failed.	Integrity check failed	U---	5	U0005	20105	38825	XC_LOG_INTEGRITY_CHECK_FAILED	Check that you use the correct data element to decrypt. Check that your data was not corrupted, restore data from the backup.
6	S	Data protect operation was successful.	<empty>	-RP-	6	U0006	20106	38826	XC_LOG_PROTECT_SUCCESS	No action is required.
7	W	Data protect operation failed.	<multiple messages>	-RP-	7	U0007	20107	38827	XC_LOG_PROTECT_FAILED	Failed to create Key ID crypto context. Verify that your data is not corrupted and you use valid combination of input data and data element to encrypt.
8	S	Data unprotect operation was successful. If mask was applied to the DE, then the appropriate record is added to the audit log description.	<empty>	U---	8	U0008	20108	38828	XC_LOG_UNPROTECT_SUCCESS	No action is required.
9	W	Data unprotect	<multiple messages>	U---	9	U0009	20109	38829	XC_LOG_UNPROTE	Failure to decrypt

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
		operation failed.							CT_FAILED	data with Key ID by data element without Key ID. Verify that your data is not corrupted and you use valid combination of input data and data element to decrypt.
10	S	The User has appropriate permissions to perform the requested operation but no data has been protected/ unprotected.	<empty>	---D	10	U0010	20110	38830	XC_LOG_OK_ACCESS	No action is required. Successful DELETE operation was performed.
11	W	Data unprotect operation was successful with use of an inactive keyid.	<empty>	U---	11	U0011	20111	38831	XC_LOG_INACTIVE_KEYID_USED	No action is required. Successful UNPROTECT operation was performed.
12	E	Input is null or not within allowed limits.	<multiple messages>	URPD	12	U0012	20112	38832	XC_LOG_INVALID_PARAM	Verify the input parameters are correct.
13	E	Internal error occurring in a function call after the Provider has been opened.	<multiple messages>	URPD	13	U0013	20113	38833	XC_LOG_INTERNAL_ERROR	Restart PEP Server and re-deploy the policy.

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
		For instance: - *`unexpected null parameter in internal (private) functions`* - *`uninitialized provider`*								
14	W	Failed to load data encryption key	Failed to load data encryption key - Cache is full, or Failed to load data encryption key - No such key, or Failed to load data encryption key - Internal error.	URP-	14	U0014	20114	38834	XC_LOG_LOAD_KEY_FAILED	If return message is ‘Cache is full’, then logoff and logon again, clear the session and cache. For all other return messages restart PEP Server and re-deploy the policy.
17	E	Failed to initialize the PEP - This is a fatal error	<multiple messages>	URPD	17	U0017	20117	38837	XC_LOG_INIT_FAILED	Re-install the protector, re-deploy policy.
20	E	Failed to allocate memory.		URPD	20	U0020	20120	38840	XC_LOG_OUT_OF_MEMORY	Check what uses the memory on the server.
21	W	Input or output buffer is too small.	Buffer too small	URPD	21	U0021	20121	38841	XC_LOG_BUFFER_TOO_SMALL	Token specific error about

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
										supplied buffers. Data expands too much, using non-length preserving Token element. Check return message for specific error, and verify you use correct combination of data type (encoding), and token element. Verify supported data types according to *Protegrity Protection Methods Reference 7.2.1*.
22	W	Data is too short to be protected or unprotected. For example, too few characters were provided when tokenizing with a length-preserving token element.	Input too short	URPD	22	U0022	20122	38842	XC_LOG_INPUT_TOO_SHORT	Provide the longer input data.
23	W	Data is too long to be protected	Input too long	URPD	23	U0023	20123	38843	XC_LOG_INPUT_T	Provide the shorter input data.

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
		or unprotected. For example, too many characters were provided.							OO_LONG	
25	W	Username too long.	Username too long.	UPRD	-	U0025	-	-		Run query by user with Username up to 255 characters long.
26	E	Unsupported algorithm or unsupported action for the specific data element. For example, unprotect using HMAC data element.	<multiple>	URPD	26	U0026	20126	38846	XC_LOG_UNSUPPORTED	Check the data elements used for the crypto operation. Note that HMAC data elements cannot be used for decrypt and re-encrypt operations.
31	E	Policy not available	Policy not available	URPD	31	U0031	20131	38851	XC_LOG_EMPTY_POLICY	No policy is deployed on PEP Server.
40	E	No valid license or current date is beyond the license expiration date.	License expired	-RP-	40	U0040	20140	38860	XC_LOG_LICENSE_EXPIRED	ESA System Administrator should request and obtain a new license. Re-deploy policy with renewed license.
41	E	The use of the protection method is restricted by license.	Protection method restricted by license.	URPD	41	U0041	20141	38861	XC_LOG_METHOD_RESTRICTED	Perform the protection operation with the protection

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
										method that is not restricted by the license. Request license with desired protection method enabled.
42	E	Invalid license or time is before licensestart.	License is invalid.	URPD	42	U0042	20142	38862	XC_LOG_LICENSE_INVALID	ESA System Administrator should request and obtain a new license. Re-deploy policy with renewed license.
44	W	The content of the input data is not valid. (e.g. for Tokenization) E.g. Input is alphabetic when it is supposed to be numeric.	Invalid format	-RP-	44	U0044	20144	38864	XC_LOG_INVALID_FORMAT	Verify the input data is of the supported alphabet for specified type of token element.
46	E	Used for z/OS Query Default Data element when policy name is not found.	No policy. Cannot Continue.		46	n/a	n/a	n/a	XC_LOG_INVALID_POLICY	Specify the valid policy. Policy name is case sensitive.
50	S	Data reprotect	<empty>	-R-	n/a	n/a	n/a	n/a		No action is required.

Log Code	Severity	Description	Error Message	DB / AP Operations	MSSQL	Teradata	Oracle	DB2	XC API Definitions	Recovery Actions
		operation was successful.								Successful REPROTECT operation was performed.

The *Severity* column lists W, S, and E corresponding to **W**arning, **S**uccess, and **E**rror severity.

The **DB/AP Operations** column lists URPD operations corresponding to **U**nprotect/**P**rotect/**R**eprotect/**D**elete operations. Delete operation is applicable only on database protectors.

Caution:

After the Log Forwarder service is restarted, any data security operation, such as, protect or unprotect, may result in loss of the first data security operation audit. Subsequent data security operation counts are displayed accurately in the *Forensics*.

Note:

If the protect, unprotect, or reprotect operations fail, then the logs for *protection.operation* parameter appears as *Unknown* in the *Forensics*.

If the user does not have the permissions to perform the protect, unprotect, and reprotect operations, then the logs for *protection.operation* parameter appears as *Protect*, *Unprotect*, or *Reprotect* in the *Forensics*.

5.6 Internal Audit Logs

The following table explains internal audit logs that are sent to ESA, and can be viewed in the ESA Web Interface, **Protegrity Analytics** > **Forensics** navigation menu.

Table 5-11: Audit Log Codes

Log Code	Log Description	Description of the event
50	Policy created	Generated when a new policy was created in Policy management in ESA.
51	Policy updated	Generated when a new policy was updated in Policy management in ESA.
52	Policy deleted	Generated when an existing policy was deleted from Policy management in ESA.
56	Policy role created	Generated when a new policy role was created in Policy management in ESA.
71	Policy deployed	Generated when a policy was sent for deployment to a PEP Server.
75	Policy data store added	Generated when a new data store was added to a policy.
76	Policy changed state	Generated when a policy has changed its state to Ready to Deploy, or Deployed.
78	Key created	Generated when new key was created for the Data Element.

Log Code	Log Description	Description of the event
80	Policy deploy failed	Generated when a policy failed to be deployed.
83	Token deploy failed	Generated when the token failed to be deployed.
84	Token deployed successfully	Generated when the token deployed successfully.
85	Data Element Key(s) exported	Generated when export keys API executes successfully. Lists each Data Element that was successfully exported.
86	Policy deploy warning	Generated when the Policy deploy operation fails.
100	Password changed	Generated when the password of the admin user was changed.
101	Data store created	Generated when a new data store was created.
102	Data store updated	Generated when a new data store was updated.
103	Data store deleted	Generated when a data store was deleted.
107	Mask created	Generated when a new mask was created.
108	Mask deleted	Generated when any mask was deleted.
109	Security coordinate deleted	Generated when an existing security coordinate was deleted.
110	Security coordinate created	Generated when a new security coordinate is created.
111	Role created	Generated when a new role is created in Policy management in ESA.
112	Role deleted	Generated when any role was deleted from Policy management in ESA.
113	Member source created	Generated when a new external source is created in Policy management in ESA.
114	Member source updated	Generated when a new member source is updated in Policy management in ESA.
115	Member source deleted	Generated when any external source was deleted from Policy management in ESA.
116	All roles resolved	Generated when the members in the automatic roles are synchronized.
117	Role resolved	Generated when it has fetched all members from a certain role into the policy.
118	Role group member resolved	Generated when it has fetched all group members from a role into the policy.
119	Trusted application created	Generated when a new trusted application is created in Policy management in ESA.
120	Trusted application deleted	Generated when a new trusted application is deleted in Policy management in ESA.
121	Trusted application updated	Generated when a new trusted application is updated in Policy management in ESA.
126	Mask updated	Generated when a mask is updated in Policy management in ESA.
127	Role updated	Generated when a role is updated in Policy management in ESA.
129	Node registered	Generated when a node is registered with ESA.

Log Code	Log Description	Description of the event
130	Node updated	Generated when a node is updated.
131	Node unregistered	Generated when a node is not registered with ESA.
140	Disk full alert	Generated when the disk is full.
141	Disk full warning	Generated to warn the IT administrator that the disk is almost full.
144	Login success	Generated when Security Officer logs into Policy management in ESA.
145	Login failed	Generated when Security Officer failed to log into Policy management in ESA.
146	Logout success	Generated when Security Officer logs out from Policy management in ESA.
149	Data element key updated	Generated when a data element with a key is updated in Policy management in ESA.
150	Data element key created	Generated when a new data element with a key is created in Policy management in ESA.
151	Data element key deleted	Generated when a data element (and its key) was deleted from Policy management in ESA.
152	Too many keys created	Generated when the number of data element key IDs has reached its maximum.
153	License expire warning	Generated once per day and upon HubController restart when less than 30 days are left before license expiration.
154	License has expired	Generated when the license becomes expired.
155	License is invalid	Generated when the license becomes invalid.
156	Policy is compromised	Generated when integrity of *pepserver.db* has been compromised.
157	Failed to import some users	Generated when users having names longer than 255 characters were not fetched from an external source.
158	Policy successfully imported	Generated when the policy is successfully retrieved from the *pepserver.imp* file (configured in *pepserver.cfg*), imported and decrypted.
159	Failed to import policy	Generated when the policy fails to be imported from the *pepserver.imp* file (configured in *pepserver.cfg*).
170	Data store key exported	Generated when the Data store key is exported.
171	Key updated	Generated when the key rotation is successful.
172	Key deleted	Generated when the key is deleted.
173	Datastore key has expired	Generated when the Data store key expires.
174	Datastore key expire warning	Generated when the Data store key is about to expire.
176	Datastore key rotated	Generated when the Data store key is rotated.
177	Master key has expired	Generated when the Master key expires.
178	Master key expire warning	Generated when the Master key is about to expire.
179	Master key rotated	Generated when the Master key is rotated.

Log Code	Log Description	Description of the event
180	New external HSM Configured	Generated when a new external HSM configuration is created.
181	Repository key has expired.	Generated when the Repository Key has expired.
182	Repository key expiry warning.	Generated when the Repository Key is on the verge of expiry. The warning message mentions the number of days left for the Repository Key expiry.
183	Repository key rotated.	Generated when the Repository Key has been rotated.

5.7 Error Codes

The following table displays the common error codes.

Table 5-12: Common Error Codes

Log Code	Error Code	Description	Recovery Actions
1	P_SUCCESS	OK.	
0	P_FAILED	Failed.	
-1	P_INVALID_PARAMETER	Invalid parameter encountered.	
-2	P_EOF	Reached the end of the file.	
-3	P_BUSY	Operation already in progress or object already locked.	
-4	P_TIMEOUT	There was a time-out waiting for response or the operation took too long.	Ensure that the server is available and the configuration is as required.
	P_ALREADY_EXISTS	Object such as file or shared memory segment already exists.	
-6	P_ACCESS_DENIED	No permissions to access the object or file.	
-7	P_PARSE_ERROR	Error when parsing contents of the file or user supplied data.	Verify the format of the file or user supplied data.
-8	P_NOT_FOUND	The search did not return any results. File not found. ”Failed to Load Master Key. –8” Master key file not found. “Failed to load plm.” – plm file not found. “Certificate not found”	Ensure that the file exists in the required directory and the configuration file is as required.
-9	P_NOT_SUPPORTED	The operation is not supported.	
-10	P_CONNECTION_REFUSED	The connection was refused.	
-11	P_DISCONNECTED	Disconnected.	
-12	P_UNREACHABLE	Net or host is unreachable.	Ensure that the network is functional as required.

Log Code	Error Code	Description	Recovery Actions
-13	P_ADDRESS_IN_USE	The IP Address or port is in use. An instance of server is already started.	Shutdown the server or use another port.
-14	P_OUT_OF_MEMORY	Out of memory.	Verify the memory on the Check memory on server. Restart server.
-15	P_CRC_ERROR	CRC check failed	
-16	P_BUFFER_TOO_SMALL	Buffer is too small	
-17	P_BAD_REQUEST	A malformed message was received	Check for a mismatch in the DPS versions.
-18	P_INVALID_STRING_LENGTH	Input string too long.	
-19	P_INVALID_TYPE	Wrong type used. For instance, trying to use Communication id other than 44, on MainFrames.	
-20	P_READONLY_OBJECT	Not able to write to object.	
-201	P_CRYPT_KEY_DATA_ILLEGAL	Invalid key data specified.	
-202	P_CRYPT_INTEGRITY_ERROR	Data integrity check failure.	
-203	P_CRYPT_DATA_LEN_ILLEGAL	Invalid data length specified.	For example: wrong format of kekup.bin file used. Old (pre .4.3) format used with 4.3.
-205	P_CRYPT_CONTEXT_IN_USE	Attempt to close key in use.	
-207	P_CRYPT_OBJECT_EXISTS	Object to create already exists. Key already exists.	Delete the old key or use the existing key.
-221	P_X509_SET_DATA	Set data in object failed.	Ensure that the required certificates are used.
-222	P_X509_GET_DATA	Get data from object failed.	Ensure that the required certificates are used.
-223	P_X509_SIGN_OBJECT	Sign operation failed for object.	Ensure that the required certificates are used.
-224	P_X509_VERIFY_OBJECT	Verification failed for object.	Ensure that the required certificates are used.
-231	P_SSL_CERT_EXPIRED	Certificate has expired.	Ensure that the required certificates are used.
-232	P_SSL_CERT_REVOKED	Certificate has been revoked.	Ensure that the required certificates are used.
-233	P_SSL_CERT_UNKNOWN	No trusted certificate founds.	Ensure that the required certificates are used.

Log Code	Error Code	Description	Recovery Actions
-234	P_SSL_CERT_VERIFY_FAILED	Certificate couldn't be verified.	Ensure that the required certificates are used.
-235	P_SSL_FAILED	General SSL error.	Ensure that the required certificates are used.
-241	P_KEY_ID_FORMAT_ERROR	Invalid format on Key id.	
-242	P_KEY_CLASS_FORMAT_ERROR	Invalid format on KeyClass.	
-243	P_KEY_EXPIRED	Key expired.	

5.8 Application Protectors API Return Codes

When you develop an application using the API of the Protegrity AP C, AP Go, AP Java, AP NodeJS, AP .Net, and AP Python, you may encounter the errors described in this section.

5.8.1 AP C Error Return Codes

This section includes the list of error return codes for Application Protector C.

Error Number	Error Code	Code Definition
0	XC_FAILED	General fail with no detailed description.
1	XC_SUCCESS	Function call is successfully executed and return values are created.
100	XC_INVALID_PARAMETER	A parameter specified in a function call was invalid, or not within valid limits. An example would be when a null parameter is used when not null is expected. All parameters have to be initialized before a call. For instance, output parameters need to be initialized to a value, null, or zero if nothing else is specified.
101	XC_TIMEOUT	The operation timed out before a result was returned. A timeout can occur when you try to connect to a server and the server does not exist.
102	XC_ACCESS_DENIED	If you do not have the permissions to access an object or a file then you will receive a return code that the access is denied.
103	XC_NOT_SUPPORTED	The requested operation is not supported.
104	XC_SESSION_REFUSED	The remote peer did not accept the session request. Check if the server that you are trying to connect to is running.
105	XC_DISCONNECTED	The session was terminated. If you do not have a session and you try to use the session, then you will receive a return code that you are disconnected.
106	XC_UNREACHABLE	The host could not be reached or is not able to be contacted. If you cannot connect to the server, then try to start the server or change the parameters for the connection.
107	XC_SESSION_IN_USE	The session is already in use. You are trying to use a session that is already used.
108	XC_EOF	If you get an end of file that is unexpected, such as an empty key file, then you will receive a return code that an unexpected end of file is reached.
109	XC_NOT_FOUND	Error returned when a file required to complete an operation is not found.
110	XC_BUFFER_TOO_SMALL	If you try to encrypt, decrypt, or re-encrypt and the output buffer size is too small, then you will receive this return code.
111	XC_NOT_DEFINED	A property or setting has not been set or defined.
112	XC_POLICY_LOCKED	The policy is locked so no operations are allowed.
113	XC_PROTOCOL_ERROR	This can be caused by an invalid frame or similar, or formatting errors in the protocol message structure.
114	XC_COMMUNICATION_ERROR	This can happen when sending or receiving data over an SSL or TCP socket.
115	XC_THROW_EXCEPTION	Used when an operation should throw an exception.

Error Number	Error Code	Code Definition
116	XC_INVALID_FORMAT	Either the length or the contents of the provided input data are not in a valid format.

5.8.2 AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API Return Codes

When you develop an application using the Application Protector (AP) Java APIs, AP Python APIs, AP NodeJS APIs, AP .Net APIs, or AP Go APIs, you may encounter the errors described in this section. You can avoid most of the errors if you use the API correctly.

For more information, refer to the *Protegrity Application Protector Guide 9.1.0.0*.

5.8.2.1 AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API Log Return Error Codes

This section lists the log return error codes returned by the AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API as a result of policy exceptions. Audits are generated in the ESA for these errors.

Table 5-13: AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API Log Return Codes

Code	Error Message	Error Description
1	1, The username could not be found in the policy in shared memory.	The user name could not be found in the policy residing in the shared memory.
2	2, The data element could not be found in the policy in shared memory.	The data element could not be found in the policy residing in the shared memory.
3	3, The user does not have the appropriate permissions to perform the requested operation.	The user does not have the required permissions to perform the requested operation.
5	5, Integrity check failed.	The data integrity check failed when decrypting using a Data Element with CRC enabled.
6	6, Data protection was successful.	The operation to protect the data was successful.
7	7, Data protection failed.	The operation to protect the data failed.
8	8, Data unprotect operation was successful.	The operation to unprotect the data was successful.
9	9, Data unprotect operation failed.	The operation to unprotect the data failed.
10	10, The user has the appropriate permissions to perform the requested operation. This is just a policy check and no data has been protected or unprotected.	The user has the required permissions to perform the requested operation. This return code ensures a verification and no data is protected or unprotected.
11	11, Data unprotect operation was successful with use of an inactive keyid.	The operation to unprotect the data was successful using an inactive Key ID.
12	12, Input is null or not within allowed limits.	Input parameters are either NULL or not within allowed limits.
13	13, An internal error occured in a function call after the PEP provider is started.	Internal error occurring in a function call after the PEP provider has been opened. For example: - `failed to get mutex / semaphore, - unexpected null param`.
14	14, Failed to load the data encryption key	A key for a data element could not be loaded from shared memory into the Crypto engine.
15	15, Tweak input is too long.	Tweak input is too long.
16	16, External IV is not supported in this version	External IV is not supported in this version.
17	17, Failed to initialize the PEP - This is a fatal error	The PEP server failed to initialize, which is a fatal error.
19	19, Unsupported tweak action for the specified fpe dataelement	The external tweak is not supported for the specified FPE data element.
20	20, Failed to allocate memory.	Failed to allocate memory.
21	21, Input or output buffer is too small.	The input or output buffer is very small.

Code	Error Message	Error Description
22	22, Data is too short to be protected/unprotected.	The data is too short to be protected or unprotected.
23	23, Data is too long to be protected/unprotected.	The data is too long to be protected or unprotected.
25	25, Username too long.	The user name is longer than the maximum supported length of the user name that can be used for protect or unprotect operations.
26	26, Unsupported algorithm or unsupported action for the specific data element.	The algorithm or action for the specific data element is unsupported.
27	27, Application has been authorized.	The application is authorized.
28	28, Application has not been authorized.	The application is not authorized.
31	31, The policy in shared memory is empty.	The policy residing in the shared memory is empty.
39	39, The policy in shared memory is locked. This can be caused by a disk full alert.	The policy residing in the shared memory is locked. This error can be caused by a *Disk Full* alert.
40	40, No valid license or current date is beyond the license expiration date.	The license is invalid or the current date is beyond the license expiry date.
41	41, The use of the protection method is restricted by license.	The use of the Protection method is restricted by the license.
42	42, Invalid license or time is before licensestart.	The license, or the time, is invalid prior to the start of the license tenure.
44	44, The content of the input data is not valid.	The content of the input data is invalid.
49	49, Unsupported input encoding for the specific data element.	The input encoding for the specific data element is not supported.
50	50, Data reprotect operation was successful.	The operation to reprotect the data was successful.

5.8.2.2 AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API PEP Result Codes

This section lists the PEP result codes returned by AP Java, AP Python, AP NodeJS, AP .Net, and AP Go APIs as a result of system exceptions. Audits are not generated in the ESA for these errors.

Table 5-14: AP Java, AP Python, AP NodeJS, AP .Net, and AP Go API PEP Result Codes

Code	Error Message	Error Description
-1	-1, Invalid parameter	The parameter is invalid.
-7	-7, Error when parsing contents, e.g.	The error occurred when the contents were parsed.
-8	-8, Not found!	The search operation was not successful.
-16	-16, Buffer is too small	The buffer size is very small.
-26	-26, Policy not available	The policy is not available.
-43	-43, Invalid format	The format is invalid.
-46	-46, Requesting service/function on an object that is not initialized	The service requested or function is performed on an object that is not initialized.
-47	-47, Policy locked for some reason	The Policy is locked.

5.9 Protector Error Handling

This section explains the common errors and problems users may encounter while working with Database, z/OS, Data Security Gateway, and Big Data Protectors.

5.9.1 Configuring the application log for Protectors

The user needs to perform the following steps to configure the application log in order to generate the logs to the *applogs.txt* file in the Log Forwarder.

➤ To enable the application log:

1. From the OS Console, navigate to the ***/opt/protegrity/fluent-bit/data/config.d*** directory.
2. Open the *out_applog_file.conf* file.

```
cat out_applog_file.conf
[FILTER]
    Name          rewrite_tag
    Match         logdata
    Rule          $logtype ^(Application)$ applog true
    Emitter_Name  re_emitted

[FILTER]
    Name lua
    Match applog
    call restructure
    code function restructure(tag, timestamp, record) new_record = {} currtime
= os.date('%Y-%m-%d %H:%M:%S', record["origin"]["time_utc"]) new_record["level"] =
record["level"] new_record["currenttime"] = currtime new_record["description"] =
record["additional_info"]["description"] return 2, timestamp, new_record end

[OUTPUT]
    Name file
    Match applog
    Path /opt/protegrity/fluent-bit/data/
    File applogs.txt
    Format template
    Template {currenttime} ({level}) {description}
    storage.total_limit_size  5M
```

3. Rename the *out_applog_file.disabled* file to *out_applog_file.conf* file within the directory.

```
ls
in_tail.conf
in_tcp.conf
out_applog_file.disabled
out_elastic.conf
upstream_es.cfg
```

```
mv out_applog_file.disabled out_applog_file.conf
```

```
ls
in_tail.conf
in_tcp.conf
out_applog_file.conf
out_elastic.conf
upstream_es.cfg
```

4. Restart the Log Forwarder using the following commands.

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

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

5. The log data is written to the *applogs.txt* file in the ***/opt/protegrity/fluent-bit/data*** folder.

```
applogs.txt
buffer
config.d
logforwarder.conf
logforwarder.log
logforwarder.pos
logforwarder.pos-shm
logforwarder.pos-wal
parser.d
```

6. To verify the application log configuration, run the following command.

   ```
   /opt/protegrity/defiance_dps/bin/pepserver -dir /opt/protegirty/defiance_dps/data
   -verbose
   ```

   The policy is loaded successfully.

   ```
   2023-06-14 12:18:38 (INFO) Application starting, pid=11957
   2023-06-14 12:18:38 (INFO) Starting Protegrity PEP Server
   2023-06-14 12:18:38 (INFO) Version: 1.2.1+10.gd214f8.1.2
   2023-06-14 12:18:38 (INFO) Platform: Linux_x64
   2023-06-14 12:18:38 (INFO) Hostname: rhel74base
   2023-06-14 12:18:38 (INFO) IP Address: xx.xx.x.xxx
   2023-06-14 12:18:38 (CONFIG) Policy will be downloaded from https://xx.xx.x.x:xxxx
   2023-06-14 12:18:38 (CONFIG) Policy refresh interval: 80 seconds
   2023-06-14 12:18:38 (INFO) Key handler loaded: internal
   2023-06-14 12:18:38 (CONFIG) Communication id: 0
   2023-06-14 12:18:38 (CONFIG) Semaphore resources: 4000
   2023-06-14 12:18:38 (INFO) Shared memory GID: -1
   2023-06-14 12:18:38 (CONFIG) Is shared memory worldreadable: yes
   ```

The Log Forwarder is configured with an enabled application log configuration file.

5.9.2 Big Data Protector Error Handling

This section explains the common errors, permission restrictions, and problems users may encounter while working with the Big Data Protector.

> **Note:**
>
> Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated. The HDFSFP-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.

> **Note:**
>
> The HDFSFP-related components in the CDH Native installer (such as the *PTY_HDFSFP* parcel, *BDP_HDFSFP* CSD, and the *BDP HDFSFP* service) will not be available starting from the Big Data Protector 7.2.0 release, as the HDFS File Protector (HDFSFP) is deprecated.

> **Note:**
>
> The HDFSFP-related components in the Shell-based installer (such as the *PepHdfsFp_Setup* shell script, *XCPep2Jni_Setup* shell script, Protegrity Cache Control (*cluster_cachesrvctl.sh*) utility, Recover utility, and the Talend-related files) will not be available starting from the Big Data Protector 7.2.0 release, as the HDFS File Protector (HDFSFP) is deprecated.

Table 5-15: Big Data Protector Common Errors

Error /Problem	This may happen because…	Recovery Actions
Failed to download certificates or password binaries from the ESA when the Big Data Protector configurator script is run.	• The ESA is not connected. • The ESA IP address is incorrect. • The Admin user is not present in the ESA.	Check the IP address entered for the ESA.

Error /Problem	This may happen because…	Recovery Actions
	The user name and password for the ESA is incorrect.	Check the user name and password entered for the ESA.
If you are using either the `hadoop fs, ptyfs - get, or ptyfs -put` command, then the following error message appears: *`WARN hdfs.DFSClient: DFSInputStream has been closed already`*.	This is a known issue in HDP, version 2.3 containing Hadoop, version 2.7.1.	This known issue is fixed in Hadoop, version 2.7.2.

After installation of Big Data Protector, the Oozie workflow fails and the following exception appears. *`java.lang.ClassNotFoundException: Class com.protegrity.hadoop.fileprotector.crypto.codec.PtyCryptoCodec not found`*	The Oozie workflow is not able to find the Protegrity codec in its classpath.	Perform the following steps to resolve the issue.
		1. Navigate to the <OOZIE_HOME> directory.
		2. If you are using the CDH native installer, then execute the following commands.
		`ln -s /opt/cloudera/parcels/PTY_HDFSFP/hdfsfp/hdfsfp-1.1.2.jar`
		`ln -s /opt/cloudera/parcels/PTY_HDFSFP/hdfsfp/jedis-2.1.0.jar`
		`ln -s /opt/cloudera/parcels/PTY_HDFSFP/defiance_xc/java/lib/xcpep2jni.jar`
		3. If you are using the Ambari native installer, then execute the following commands.
		`ln -s <PROTEGRITY_DIR>/7.0.1.x/hdfsfp/hdfsfp-1.1.2.jar .`
		`ln -s <PROTEGRITY_DIR>/7.0.1.x/hdfsfp/jedis-2.1.0.jar .`
		`ln -s <PROTEGRITY_DIR>/7.0.1.x/defiance_xc/java/lib/xcpep2jni.jar`
		4. Restart the Oozie service.

The installation of the Big Data Protector failed on one or more nodes in the Hadoop cluster. Depending on the status of the AUTOCREATE_PROTEGRITY_IT_USR parameter, which was specified in the BDP.config file during the installation of Big Data Protector, one of the following exception appears. If the AUTOCREATE_PROTEGRITY_IT_USR parameter is set to no, then the following exception appears. *`*** Some of the node(s) in the cluster is not reachable.`*	- Some nodes in the cluster are powered off. - The IP addresses or host names of some nodes in the cluster are incorrectly specified in the hosts file. - Some nodes in the cluster are unreachable due to network issues. - The password for the *ADMINISTRATOR*, which is the *sudoer* user account for	Perform the following steps, as required. - Ensure that all the nodes in the cluster are running. - Ensure that the required IP addresses or host names of the required nodes are added to the hosts file. - Resolve the network issues so that the nodes are reachable. - Ensure that the password for the *ADMINISTRATOR* is consistent across all the nodes in the cluster.

Error /Problem	This may happen because…	Recovery Actions

`***Please check the log file for failure status: /opt/protegrity/logs/bdp_setup.log Exiting...`
If the *AUTOCREATE_PROTEGRITY_IT_USR* parameter is set to yes, then the following exception appears.
`Failed to create protegrity service user: <PROTEGRITY_IT_USR> on some node(s)`
	installing Big Data Protector, is not consistent across all the nodes in the cluster.	

User unable to create data store with the *dfsdatastore* utility for HDFSFP.	The Protegrity Cache server on the Lead node is not running.	Verify if the Protegrity Cache server on the Lead node is running using the command **`service ptycache status`**. If it is not running, then start it.
If HDFSFP is installed and you are working with Hive tables, then the following exception appears in the hive-server2.log file. `Caused by: com.protegrity.hadoop.fileprotector.acl.AclAccessException: redis.clients.jedis.exceptions.JedisConnectionException: java.net.SocketException: Broken pipe at com.protegrity.hadoop.fileprotector.acl.redis.RedisAccessControlAdapterImpl.isPathExists(Unknown Source) at com.protegrity.hadoop.fileprotector.crypto.codec.PtyCodecManagerImpl.isProtctedPath(Unknown Source) ... 25 more Caused by: redis.clients.jedis.exceptions.JedisConnectionException: java.net.SocketException: Broken pipe at redis.clients.jedis.Connection.flush(Connection.java:66) at redis.clients.jedis.Connection.getIntegerReply(Connection.java:186) at redis.clients.jedis.Jedis.exists(Jedis.java:93) ... 27 more`	This is a known issue when HDFSP is used with Hive.	This issue does not have any recovery action.
If HDFSFP is installed and you are using Hive, then an exception is not generated in any of the following conditions: • You are using Hive to write data to an HDFSFP protected ACL path and the data is written in clear text format. • You are using Hive to read data from an HDFSFP protected ACL path and the data is read in protected (encrypted) format.	The Protegrity Cache Server is not running on the node, which is processing the data.	Ensure that the Protegrity Cache server is running on the node using the command **`service ptycache status`**. If it is not running, then start it.

Error /Problem	This may happen because…	Recovery Actions

User unable to connect to the ACL data store and the following exception appears in the *dfscacherefresh.log* file.
`SEVERE) Distcache event error (Code=0 : Failed!)`
`(SEVERE) Distcache event error (Code=0 : Failed!)`
`(SEVERE) Failed to Connect to Protegrity Cache Server ... Retrying :<Datastore name> (Code=504 : Unknown)`
	The Protegrity Cache server on the Lead node is not running.	Verify if the Protegrity Cache server on the Lead node is running using the command `service ptycache status`. If it is not running, then start it.

Data store added successfully but does not reflect on the *Active* list for HDFSFP.	The *dfscacherefresh* daemon is not running.	Restart the *dfscacherefresh* daemon using the ESA Web UI.
Unable to create ACL entry for HDFSFP.	The Protegrity Cache server on the Lead node is not running.	Verify if the Protegrity Cache server on the Lead node is up and running. If it is not running, then start it.

ACL entry remains in locked state.	The ESA transitioned from the hibernation state to the running state.	Perform the following steps to restart (stop/start) the DfsCacheRefresh Server/Service.
		1. Login to the ESA Web UI.
		2. Stop the *DfsCacheRefresh* service.
		3. Start the *DfsCacheRefresh* service.
		4. Alternatively, you can restart the *DfsCacheRefresh* service by running the following commands from ESA CLI Manager.
		`<PROTEGRITY_DIR>/dfs/cacherefresh/bin: ./cacherefsrvctrl stop all`
		`<PROTEGRITY_DIR>/dfs/cacherefresh/bin: ./cacherefsrvctrl start`

ACL entry remains in locked state after it is activated for HDFSFP.	The PEP server is not running on the Lead node.	Verify if the Lead node PEP server is up and running and the required policy are deployed. For more information, refer to section 5.3 PEP Server Common Errors (Database, Application and Big Data Protectors).
	The user *ptyitusr* does not have the protect permission.	Check policy. The user *ptyitusr* should have protect access on ACL data element for that time of point. Verify the *beuler.log* file in the `/var/log/protegrity/` directory for any exception stack trace.
	The user *ptyitusr* does not have the write permissions for the local directory `/tmp/hadoop-ptyitusr`.	Ensure that the user *ptyitusr* has the write permissions to the local directory `/tmp/hadoop-ptyitusr`.

Error /Problem	This may happen because…	Recovery Actions
		If the user *ptyitusr* does not have write permissions for the local directory `/tmp/hadoop-ptyitusr`, then perform the following steps. 1. Provide write permissions to the ingestion user for local directory `/tmp/hadoop-ptyitusr`. 2. Login to the Lead node. 3. If you are using the CDH native installer, then navigate to the `/opt/cloudera/parcels/PTY_HDFSFP/hdfsfp/ptyitusr/` directory. 4. If you are using the Ambari native installer, then navigate to the `<PROTEGRITY_DIR>/7.0.1.x/hdfsfp/ptyitusr/` directory. 5. Run the **`beuler.sh`** script. The following is a sample beuler.sh script command. **`sh beuler.sh -path /user/root -datastore -datastore <datastore_name> -activationid <activation_ID> -beulerjobid <beuler_job_ID>`**
	The user *ptyitusr* does not have the write permission on the directory path in HDFS.	1. Ensure that the user *ptyitusr* has write permissions on the directory path in HDFS. 2. Login to the Lead node and run the **`bueler.sh`** script. The following is a sample **`bueler.sh`** script command. **`sh beuler.sh -path /user/root -datastore <datastore_name> -activationid <activation_ID> -beulerjobid <beuler_job_ID>`**
	The Protegrity Cache server on the Lead node is not running.	Verify if the Protegrity Cache server on the Lead node is up and running.
	The *dfscacherefresh* daemon is not running.	Start the *dfscacherefresh* daemon using the ESA Web UI.
	The ACL activation process was not completed successfully.	Monitor the *beuler.log* file, which is located in the `/var/log/Protegrity` directory, for details about any exceptions by performing the following steps. 1. Login to the Lead node with root permissions. 2. If you are using the CDH native installer, then navigate to the `/opt/cloudera/parcels/PTY_HDFSFP/hdfsfp/ptyitusr` directory. 3. If you are using the Ambari native installer, then navigate to the `<PROTEGRITY_DIR>/7.0.1.x/hdfsfp` directory. 4. After the ACL is activated, monitor the beuler.log file for any exceptions.

Error /Problem	This may happen because…	Recovery Actions
		5. If any exception occurs, then resolve the exception as required. 6. Run the `beuler.sh` script using the following command. `sh beuler.sh -path /user/root -datastore <datastore_name> -activationid <activation_ID> -beulerjobid <beuler_job_ID>`
	An incorrect data element name was specified initially during ACL creation.	Perform the following steps to resolve the issue, only if the entire path is unprotected. 1. From the ESA Web UI, stop the *dfscacherefresh* service. 2. Login to the ESA OS Console. 3. Open the `/opt/protegrity/dfs/dfsadmin/data/<Datastore-name>ActiveList.xml` file. **Note:** It is recommended to take a backup of the `/opt/protegrity/dfs/dfsadmin/data/<Datastore-name>ActiveList.xml` file before you proceed. 4. Remove the ACL entry, which was created with the incorrect data element. 5. Save the file. 6. From the ESA Web UI, start the *dfscacherefresh* service.
ACL entry remains in locked state after it is activated for HDFSFP and the beuler.log file is not generated.	The configuration updates for the *BDPHDFSFP* service are not set in the Ambari UI.	Ensure that the required HDFSFP-related configuration updates for MapReduce, HDFSFP, and Yarn services are set accurately in the Ambari UI. Alternatively, set the HDFSFP configuration to the recommended values using the **Set Recommended** option in the Ambari UI.
MapReduce job failed when trying to read protected data in HDFSFP.	The MapReduce configuration is incorrect.	Verify the configuration of MapReduce. For more information, refer to *Big Data Protector Guide 7.2.0*.
	The PEP servers on data nodes are not running.	Ensure that the PEP servers on the data nodes are up and running.
	There are issues with the policy.	Ensure that the policy is loaded on all the PEP servers in the Hadoop cluster. In addition, verify if the user who running the MapReduce job has the required read permissions.
MapReduce job failed when trying to write protected data in HDFSFP.	The MapReduce configuration is incorrect.	Verify the configuration of MapReduce.

Error /Problem	This may happen because…	Recovery Actions
		For more information, refer to *Big Data Protector Guide 7.2.0*.
	The PEP servers on data nodes are not running.	Ensure that the PEP servers on the data nodes are up and running.
	There are issues with the policy.	Ensure that the policy is loaded on all the PEP servers in the Hadoop cluster. In addition, verify if the user who running the MapReduce job has the required write permissions.
MapReduce job is successful but the output in the protected zone is in clear form in HDFSFP.	The MapReduce configuration is incorrect.	Verify if the MapReduce configuration has the following parameter values as *true*: `mapred.output.compress (MRv1)` `Mapreduce.output.fileoutputformat.compress` (MRv2)
After installation of Big Data Protector, the MapReduce API, Hive UDF, or Pig UDF is not working and displays the `ClassNotFound` exception.	The required protector jar file is not present in the Hadoop classpath.	Restart the Hadoop services for the required protector.
HDFSFP, MapReduce API or Hive UDF used with HDFSFP fails due to the XCPep2JNI call failure exception and the following exception appears: `Caused by: com.protegrity.xc.XCExceptionJni: Call failure at com.protegrity.xc.XCPepJni.protect(Unknown Source) ... 24 more`	The PEP server is not started on any of the nodes of the Hadoop cluster.	Start all the stopped PEP servers on the required nodes.
	The policy is not deployed.	Check the ESA audit logs and deploy the policy.
	The data element used is not found in the policy.	Check the ESA audit logs and use the required data element name in the API.
	The License is expired.	Check the ESA audit logs and contact Protegrity support for a new license.
The MapReduce API, Hive UDF, or Pig UDF fails due to the *InvocationTarget* exception.	The protector is not able to load the *jpeplite.plm* file.	Check the *jpeplite.plm* file, which is configured in the Hadoop classpath.
	The protector is not able to load the *jpeplite.properties* property file.	Check the *jpeplite.properties* property file, which is configured in Hadoop classpath.
Function not found error appears when using the Protegrity UDF.	The UDF is not defined in the *.hiverc* file for the user	Check the *.hiverc* file and ensure that the missing UDF definition is added to the *.hiverc* file. In addition, define the function before using it in the Hive query.
	The UDF is not defined in the Pig Latin script.	Define the UDF before using it in the Pig Latin script.
The Protegrity UDF failed due to permissions for the Hadoop directory in the Hive warehouse.	The user does not have the required permissions for the Hadoop directory in the Hive warehouse.	Ensure that the required Read, Write, or Delete permissions are configured for the Hadoop directory in the Hive warehouse for the user.
The Hive Unprotect UDF does not return the original clear text data.	The data element used for protecting data is the encryption data element.	The Hive protector does not support encryption data element. For more information, refer to *Protection Methods Reference Guide 7.1*.
A join query does not show any records or fails and the unauthorized user hive appears in ESA Forensics in one of the following conditions:	The *hive.auto.convert.join*	Depending on the requirements, perform one of the following tasks:

Error /Problem	This may happen because…	Recovery Actions

- When you run the join query using Hive UDFs on a HDFSFP protected Hive table.
- When you run the join query between a Hive internal or external table protected with HDFSFP and an internal or external unprotected or protected table.
	property is not set at session level.	- If you are using join queries with the Hive protector UDFs, then ensure that the *hive.auto.convert.join* property is set to false at the session level using the following command.
		`set hive.auto.convert.join=false;`
		- If you are using join queries between Hive internal table protected with HDFSFP and an internal or external unprotected table, then ensue that the *hive.auto.convert.join* property is set to true at the session level using the following command.
		`set hive.auto.convert.join=true;`

In a Hive shell, if one table is protected with the Protegrity codec and another table is protected with the Gzip codec, then the *join* operation for the two tables does not function if it is executed after a set of other queries are executed.	The Hive system is unable to ascertain the accurate input path of the respective tables to perform the *join* operation.	Ensure that you perform any one of the following actions: - After running the insert query on the protected table, set the value of the *hive.exec.compress.output* parameter to False. - Execute the load and join operations for the respective tables in two different Hive consoles. Alternatively, you can use Beeline instead of Hive shell.

After running a command in MapReduce, Pig, the following error appears:
`Output directory already exists`
	The output directories were created by using the sample commands previously.	Clean up the output directories for the protected and unprotected data by using the following commands:
		MapReduce:
		`hadoop fs -rm -r /tmp/basic_sample/<MapReduce Protected output_directory>`
		`hadoop fs -rm -r /tmp/basic_sample/<MapReduce Unprotected output_directory>`
		Pig:
		`hadoop fs –rm –r /tmp/basic_sample/basic_sample_protected`

If you are using the HBase protector, then duplicate *Audit success* logs appear per operation.	This is a known issue with the HBase protector.	This issue does not have any recovery action.
If you are using Hive UDFs on Spark SQL, then duplicate *Audit success* logs appear per task.	This is a known issue when you are using Hive UDFs with Spark SQL.	This issue does not have any recovery action.
After running a query, which involves the Protegrity UDFs for Impala, the following error appears: `Operation not supported for the datatype`	The encryption method is not supported for the datatype.	- Ensure that the data to be protected is from one of the following data types: - STRING - INT - DOUBLE - FLOAT - Ensure that the data element used is not *Binary*.

Error /Problem	This may happen because…	Recovery Actions

After running a query, which involves the Protegrity UDFs for Impala, the following error appears:
`AnalysisException: default.<UDF_Name>() unknown`
	• The *createobjects.sql* script was not executed.
	• If the *catalogd* process is restarted, then all the Protegrity UDFs for the Impala protector should be reloaded.
		If you are not using a Kerberos-enabled Hadoop cluster, then execute the *createobjects.sql* script to load the Protegrity UDFs for the Impala protector.
		`impala-shell -i <IP address of any Impala slave node> -f /opt/cloudera/parcels/PTY_BDP/pepimpala/sqlscripts/createobjects.sql`
		If you are using a Kerberos-enabled Hadoop cluster, then execute the *createobjects.sql* script to load the Protegrity UDFs for the Impala protector.
		`impala-shell -i <IP address of any Impala slave node> -f /opt/cloudera/parcels/PTY_BDP/pepimpala/sqlscripts/createobjects.sql -k`
		For more information, refer to *Big Data Protector Guide 7.1*.

After running a query, which involves the Protegrity UDFs for Impala, the following error appears:
`Socket error 104: Connection reset by peer`
`Error connecting: TTransportException, Could not connect to node1:21000`
	The Impala daemon is not running.	Verify if the Impala daemon specified in the error is up and running.
		If the Impala daemon is not running, then start it.

	The Impala daemon automatically restarts as the memory consumed by Impala UDFs is higher than the *Impala Daemon Memory Limit* parameter in the Cloudera Manager UI.	Ensure that you increase the *Impala Daemon Memory Limit* parameter in the Cloudera Manager UI, as required.
If the protect or unprotect operations using the Impala protector fail, then multiple audit failure logs are generated in the ESA.	Cloudera Impala does not abort the execution of the query on the first failure, resulting in audit failure logs in the ESA for each protect or unprotect operation failure.	This is a limitation of Cloudera Impala.
If you are performing protect or unprotect operations using the Impala protector UDFs in the insert query by specifying the limit clause <= 1024, then the following issues occur: • Empty values are inserted in the column where the Impala UDFs were applied. • Depending on the number of records, multiple audit failure logs are generated in the ESA. If the number of records are larger than 1024, then 1024 audit failure logs are generated in the ESA.	Cloudera Impala does not abort the execution of the query on the first failure, resulting in empty values inserted in the columns and multiple audit failure logs in the ESA.	This is a limitation of Cloudera Impala.

Error /Problem	This may happen because…	Recovery Actions
If you are performing protect or unprotect operations using the Impala protector UDFs in the select query by specifying the limit clause <=1024, then the following issues occur: - Empty values are inserted in the column where the Impala UDFs were applied. - Depending on the number of records, multiple audit failure logs are generated in the ESA. If the number of records are larger than 1024, then 1024 audit failure logs are generated in the ESA.	Cloudera Impala does not abort the execution of the query on the first failure, resulting in empty values inserted in the columns and multiple audit failure logs in the ESA.	Depending on the CDH version, one of the following resolutions is applicable: - This limitation is fixed by Cloudera in Impala, version 2.3 with CDH, version 5.5. - If you are using a version other than CDH, version 5.5, then this limitation has no recovery action.
The error messages do not appear in the Impala shell due to one of the following conditions: - When failures occur during protect or unprotect operations with simple Impala protector UDFs calls without the use of tables or views. - When failures occur while performing unprotect operations using views.	This is a limitation of Cloudera Impala.	This limitation is fixed by Cloudera in Impala, version 2.3 with CDH, version 5.5.
The ACL Activation Job Progress information shows a failure status.	This occurs due to several reasons, such as incorrectly set permissions for the user *ptyitusr*, missing data element, and so on. The errors or exceptions are logged in the *beuler.log* file.	Monitor the beuler.log file for any errors or exceptions and take the required corrective action. For more information about monitoring the beuler.log file, refer to *Big Data Protector Guide 7.1*. If the *beuler.log* file does not contain any errors or exceptions, then verify the Job History server against the Application ID for any additional details.
During the ACL operations (*Protect/Reprotect/ Unprotect/Update*), the following exception appears: `java.io.IOException: Processed: 2 Skipped: 0 Failed: 2 at com.protegrity.hadoop.fileprotector.crypto.dist.CryptoFilesMapper.close(Unknown Source) at org.apache.hadoop.mapred.MapRunner.run(MapRunner.java:61) ...`	- The sticky bit was set for the HDFS directory, on which the ACL operations (*Protect/ Reprotect/Unprotect/ Update*) need to be performed. - The user *ptyitusr* does not have read/ write permissions for the HDFS directory, on which the ACL operations (*Protect/ Reprotect/Unprotect/ Update*) need to be performed.	Depending on the issue, one of the following resolutions is applicable: - Remove the sticky bit set for the HDFS directory. If required, then the user can set the sticky bit again for the HDFS directory after performing the ACL operations. - Set the read/write permissions for the user *ptyitusr* for the HDFS directory.
If an unauthorized user, with no privileges to unprotect data in the security policy, and the output value set to NULL, attempts to unprotect the protected data of Numeric type data containing Short, Int, Float, Long, Double, and Decimal format values using the respective Spark SQL UDFs, then the output is 0.	The null value output returned by the UDF is stored as 0, as per the Null handling behavior of the Scala environment.	This issue has no recovery action as it is expected behavior.
If a NULL value is protected using the Spark SQL protector Numeric UDFs, working with Short, Int, Long, Float, Double, and Decimal format values, then	- If you are using Spark, version 1.6	If NULL values are to be protected, then utilize the *ptyProtectStr()* UDF to protect the NULL data.

Error /Problem	This may happen because…	Recovery Actions
the protected output is either null or non-null, and an Audit log is not generated in ESA.	and protecting NULL value, then the Protegrity Spark UDFs are not invoked, and the null value is provided as output. As the Spark SQL protector UDF is not invoked, Audit logs are not generated in the ESA. • If you are using Spark, version lower than 1.6 and protecting NULL value, then the NULL value is internally converted to 0/0.0 and the 0/0.0 value is protected. As a result, on unprotecting the protected data, the original NULL value is not returned as the output. This is the known behavior as per the Scala environment semantics.	In this case, Audit logs will also be generated in the ESA.
If you are protecting, unprotecting, or reprotecting data using the same data element, then an audit success log is generated in ESA Forensics, in one of the following conditions: • In multiple columns of the table in the same query, when using Hive, Pig, or Impala. • In subsequent steps as part of the same MapReduce or Spark job.	This is a limitation of the Spark SQL UDFs.	This issue has no recovery action as it is expected behavior.
The Big Data Protector configurator script terminates when the certificates are downloaded from the ESA.	• The ESA is either not working, or is unreachable due to firewall or network-related issues. • The credentials for the Administrative user of the ESA, specified at the time of running the Big Data Protector configurator script, are incorrect.	Depending on the issue, one of the following resolutions is applicable: • Ensure that the ESA is up and running, and any firewall or network-related issues are resolved. • Ensure that the credentials for the Administrative user of the ESA, specified at the time of running the Big Data Protector configurator script, are accurate.
The Big Data Protector services are not visible on the Cloudera Manager Parcels screen.	• The Cloudera SCM server service is not restarted after the Big Data Protector	Depending on the issue, one of the following resolutions is applicable:

Error /Problem	This may happen because…	Recovery Actions
	CSD files are loaded in Cloudera Manager. - The ownership permissions for the Big Data Protector CSD files are not assigned to the *Cloudera SCM* user.	- Ensure that the Cloudera SCM server service is restarted after the Big Data Protector CSD files are loaded in Cloudera Manager and verify the status of the Cloudera SCM server service. For more information about restarting the Cloudera SCM server service, refer to *Installation Guide 7.1*. - Ensure that the ownership permissions for the Big Data Protector CSD files are assigned to the *Cloudera SCM* user. For more information about assigning the permissions for the CSD files, refer to *Installation Guide 7.2.0*.
The Big Data Protector PEP service (*BDP PEP*) is not visible on the Cluster Services screen in Cloudera Manager.	The Big Data Protector parcel (*PTY_BDP*) is not activated on the nodes.	Ensure that the Big Data Protector parcel (*PTY_BDP*) is activated before starting the Big Data Protector PEP service (*BDP PEP*) on the nodes.
The Big Data Protector PEP service (*BDP PEP*) is started in Cloudera Manager but the Big Data Protector service is not functional.	The Certificates parcel (*PTY_CERT*) is not activated on the nodes before starting the Big Data Protector service (*BDP PEP*) on the nodes.	Ensure that the Certificates parcel (*PTY_CERT*) is activated before starting the Big Data Protector PEP service (*BDP PEP*) on the nodes.
The HDFSFP service (*BDP HDFSFP*) is not visible on the Cluster Services screen in Cloudera Manager.	The HDFSFP parcel (*PTY_HDFSFP*) is not activated on the nodes.	Ensure that the HDFSFP parcel (*PTY_HDFSFP*) is activated before starting the HDFSFP service (*BDP HDFSFP*) on the nodes.
The HDFSFP service (*BDP HDFSFP*) is started in Cloudera Manager but the HDFSFP service is not functional.	The Certificates parcel (*PTY_CERT*) is not activated on the nodes before starting the HDFSFP service (*BDP HDFSFP*) on the nodes.	Ensure that the Certificates parcel (*PTY_CERT*) is activated before starting the HDFSFP service (*BDP HDFSFP*) on the nodes.
The HDFSFP service (*BDP HDFSFP*) is started in Cloudera Manager but the HDFSFP service is not functional.	The hosts assigned as *HDFSFP Cache Master* and *HDFSFP Cache Slave* are the same.	Ensure that the hosts assigned for *HDFSFP Cache Master* and *HDFSFP Cache Slave* are different.

Big Data Protector does not work on a Kerberos-enabled cluster using the Ambari UI.	The Kerberos services are not running.	Ensure that the Kerberos services are up and running.
		Execute the following commands to verify the status of Kerberos services.
		`service krb5kdc status`
		`service kadmin status`
		Execute the following commands to start the Kerberos services.
		`Service krb5kdc start`
		`service kadmin start`

Error /Problem	This may happen because…	Recovery Actions
The Big Data Protector services are not visible in the **Add Service** wizard on the Ambari UI.	The Ambari server is not restarted after the Big Data Protector management packs are installed in Ambari.	Ensure that the Ambari server is restarted after the Big Data Protector management packs are installed in Ambari and verify the status of the Ambari server. For more information about restarting the Ambari service, refer to *Installation Guide 7.2.0*.

If you have used the Ambari Native installer to install the Big Data Protector, and a MapReduce job fails and one of the following exception appears.
`java.lang.ClassNotFoundException: com.protegrity.hadoop.mapreduce.ptyMapRedProtectorException`
OR
`Exception in thread "main" com.protegrity.hadoop.mapreduce.ptyMapRedProtectorException: 0, Init library failed, no jpeplite in java.library.path`
	The Big Data Protector jar files required for MapReduce jobs are not configured, as required, on the Ambari UI.	Perform the following steps from the Ambari UI to resolve the issue:
		1. Verify if the following configuration parameter entries appear in the hadoop-env template configuration of the HDFS service.
		export HADOOP_CLASSPATH=${HADOOP_CLASSPATH}:/<PROTEGRITY_DIR>/7.0.1.<x>/pepmapreduce/lib/*
		export JAVA_LIBRARY_PATH=${JAVA_LIBRARY_PATH}:/<PROTEGRITY_DIR>/7.0.1.<x>/jpeplite/lib
		2. If the required configuration parameter entries are present, then the exception is caused due to some other issue that needs to be investigated.
		3. If the required configuration parameter entries are not present, then set the recommended configuration value for the hadoop-env template parameters of the HDFS service for the Big Data Protector by clicking on the ↻ icon beside the required parameter.
		4. Ensure that the following configuration parameter entries appear in the hadoop-env template configuration of the HDFS service.
		export HADOOP_CLASSPATH=${HADOOP_CLASSPATH}:/<PROTEGRITY_DIR>/7.0.1.<x>/pepmapreduce/lib/*
		export JAVA_LIBRARY_PATH=${JAVA_LIBRARY_PATH}:/<PROTEGRITY_DIR>/7.0.1.<x>/jpeplite/lib
		5. Restart the required Hadoop services.

If you have used the Ambari Native installer to install and configure the BDPPEP service, with the BDPHDFSFP service not installed, and an import job using Sqoop fails to load data in a Hive table and the following exception appears.
`hive.exec.pre.hooks Class not`
`found:com.protegrity.hive.PtyHiveUserPreHook`
FAILED: Hive Internal Error:
`java.lang.ClassNotFoundException(com.protegrity.hive.PtyHiveUserPreHook)`
	The Big Data Protector jar files required for Hive are not configured, as required, on the Ambari UI.	Perform the following steps from the Ambari UI to resolve the issue:
		1. In the hadoop-env template configuration of the HDFS service, set the following configuration parameter entries.
		export HADOOP_CLASSPATH=${HADOOP_CLASSPATH}:/<PROTEGRITY_DIR>/7.0.1.<X>/pephive/lib/*
		where <x> is the required build version of the Big Data Protector.
		2. Restart the required Hadoop services.

Error /Problem	This may happen because…	Recovery Actions
…. *at org.apache.sqoop.Sqoop.runSqoop(Sqoop.java:183)* *at org.apache.sqoop.Sqoop.runTool(Sqoop.java:225)* *at org.apache.sqoop.Sqoop.runTool(Sqoop.java:234)* *at org.apache.sqoop.Sqoop.main(Sqoop.java:243)*		

5.9.3 Database Protector Error Handling

This section explains the common errors, permission restrictions, and problems users may encounter while working with the Database Protector.

Table 5-16: Database Protector Common Errors

Error/Problem	This may happen because…	Recovery Actions
Incomplete error message appears while performing security operations using DB2 Database Protector.	The error message is too long.	No action is required. This is a limitation of DB2 Database Protector that truncates some text of long error messages. Incomplete error message is observed in the protector, but complete and expected error message is displayed in the ESA Forensics.

5.9.4 Mainframe z/OS Error Handling

5.9.4.1 z/OS Protector Common Errors

Error /Problem	This may happen because…	Recovery Actions
During initial PEP Server start up, the following error message displays: *`<date time> (SEVERE) Error binding to :15700 – EDC8116l Address not available`*	• Localhost is not found in `/etc/hosts` on the system. • Localhost in the DNS server is defined by the default TCP/IP definition present in the system	• Define localhost in `/etc/hosts`. • Remove localhost from DNS. **Note:** For AIX - modify the TCP/IP DATA located in `/etc/netsvc.conf` to specify *LOOKUP LOCAL DNS* so that the local definition in `/etc/hosts` is used first and the DNS definition is ignored.

Error /Problem	This may happen because…	Recovery Actions
The z/OS UDFs fail with *SQLCODE=-430/ SQLSTATE 38503* The following error message appears: `FUNCTION <UDF-name> (SPECIFIC NAME <UDF-name>) HAS ABNORMALLY TERMINATED`	The *Communication ID* specified in the UDF does not match with the *Communication ID* specified in the *pepserver.cfg*.	The *Communication ID* specified in the UDF should match with the *Communication ID* specified in the *pepserver.cfg*.
Unpredictable behavior is observed when unprotect operation is performed using data element or algorithm on the data, which is protected with different data element or algorithm.	The protected data has no memory of the data element or algorithm with which the data is protected.	Use the same data element or algorithm to unprotect the data with which it is protected.

5.9.4.2 Error Codes on z/OS Mainframes

The PTYCSRV may issue several messages that should be monitored by system automation. The following table describes these messages. These messages are Cryptographic Services server messages and are not specific to any single protector.

Table 5-17: PTYCSRV Messages

Message ID	Definition	Issued when…	Recovery Actions
PTY009E	Invalid Startup parameter value.	The startup parameter contains an invalid value. Valid values are AUTO, WARM, or COLD.	Correct the startup parameter value and restart the Cryptographic Services server.
PTY010E	Invalid Startup parameter value.	The startup parameter *PEPS_MONITOR_WAIT_INTERVAL* is not specified or has an invalid value.	Correct the startup parameter value and restart the Cryptographic Services server.
PTY011E	Maximum number of parameters exceeded.	The number of parameters specified in the START command or in the startup parameters file exceeds the maximum allowed parameters.	Check the number of startup parameter and restart the Cryptographic Services server.
PTY013E	Already started.	The Cryptographic Services server is already started.	No action is required. If you need to start the Cryptographic Services server with new parameter values, then stop the server and then restart it.
PTY014E	Parameter value is not numeric.	The Startup parameter value contains non-numeric characters.	Provide the required numeric value and restart the Cryptographic Services server.
PTY015E	Parameter value contains too many digits.	The Startup parameter value contains more than the maximum 15 digits.	Provide the required value and restart the Cryptographic Services server.
PTY030W	Parameter is repeated.	The Startup parameter is repeated. Only the last specification is effective.	No action is required.
PTY031I	Protegrity DPS policy updated.	The security policy is loaded and available for use. Once this message is issued, ciphering operations can begin.	No action is required. If not received within the configuration file timeout period, then the PEP Server did not

Message ID	Definition	Issued when…	Recovery Actions
			initialize properly. Refer to PTY045I. If your LPAR is short of CPU cycles, then you may need to increase the timeout period in the configuration file PTYPARM1.
PTY038E	Unbalanced quotes in the Startup parameter.	The parameters specified in the START command or in the startup parameters file contain unbalanced quotes.	Provide the required quotes and restart the Cryptographic Services server.
PTY039E	Unbalanced parenthesis in the Startup parameter.	The parameters specified in the START command or in the startup parameters file contain unbalanced parentheses.	Provide the required quotes and restart the Cryptographic Services server.
PTY045S	Protegrity PEP Server startup timed out.	The handshake between the Open MVS PEP Server and PTYCSRV fails. This means that the security policy is not loaded and ciphering cannot happen.	Review…`/defiance_dps/data/pepserver.log` to find out why the PEP Server did not initialize properly. You may also need to check the PTYSPEPS and system logs for failures.
PTY046S	Protegrity Cryptographic Service Task startup timed out.	Job PTYCST is started by PTYCSRV. PTYCSRV monitors the startup of PTYCST through a system timer. The timer expired and PTYCST has not started.	This is normally due to system load. Try starting PTYCSRV after some of the system load has let up.
PTY048E	Misplaced parenthesis in the Startup parameter.	The parameters specified in the START command or in the startup parameters file contain misplaced parentheses.	Provide the required parentheses and restart the Cryptographic Services server.
PTY049E	Invalid sub parameter	The Username parameter provided is invalid.	Only USERID and/or GROUPNAME are allowed for the USERNAME startup parameter. Correct the parameter and restart.
PTY051S	Stall condition detected. Forcing termination.	The number of log records written to log buffer remain unchanged.	A deadlock in either the use of the logging dataspace or the logging shared memory is detected. Check for error messages in the PTYCSRV job log and the pepserver.log in the …`/defiance_dps/data` sub-directory.
PTY052I	The maximum number of allowed buffer queue blocks specified on the LOGMQB start-up parameter has been reached. Log records may be lost.	The last LOGQBS buffer is allocated. Normally this means that for some reason the Open MVS PEP Server is not sending log records at all or quickly enough to the ESA appliance. Check the pepserver.log in the PEP Server data sub-directory.	Check whether ESA communication is operating properly and check `.../defiance_dps/data/pepserver.log` file for logging issues. Note that if you are only doing failure logging, then you may have a breach in progress or you may have a batch job that is failing policy for some reason.

Message ID	Definition	Issued when…	Recovery Actions
PTY053I	Log records have been lost due to insufficient buffer queue storage. This message may precede or follow PTY052I. If it precedes PTY052I by several seconds, then increase LOGQBS in PTYPARM before the next restart of PTYCSRV.	A log message buffer is completely full and another log record is created by PTYCSRV can allocate another buffer or the maximum number of buffers has been reached.	Refer to PTY052I for possible issues.
PTY065E	Access denied.	The specified data element is not found in the policy or the current user is not authorized for the data element.	Check the policy for the data element and users defined and redeploy the policy.
PTY066E	The data protector is not active.	The Cryptographic Services server or Pep Server is not started.	Start the Cryptographic Services server or Pep Server.
PTY080W	The security policy has been locked by the PEP Server because logging disk space has been exhausted. Cryptographic services are suspended until the policy is unlocked. Refer to the pepserver.log for details.	The diskfullalert value in the Open MVS PEP Server *pepserver.cfg* is reached. No further ciphering can take place until PTY081I message is issued. There is mostly likely an issue with the PEP Server sending log records to the ESA appliance.	Refer to PTY052I for possible issues. You may also need to increase the amount of space available to the `.../defiance_dps/data` directory.
PTY082W	The disk space available to the PEP Server for logging is less than the specified minimum. Refer to the *pepserver.log* file for details. If available disk space is exhausted, then the policy may be locked or logging may be suspended.	The threshold value the Open MVS PEP Server *pepserver.cfg* is reached. Further logging will still occur, but the reasons why the threshold has been reached should be investigated. If nothing is done, then the diskfullalert may be reached and this can cause ciphering problems as mentioned in PTY080W.	Refer to PTY080W for possible issues.
PTY083I	The disk space shortage for PEP Server logging has been relieved. Refer to the *pepserver.log* file for details.	Disk space becomes available for continued logging.	No action is required. Message notifies you that the condition noted by PTY082W is resolved.
PTY084W	The disk space available to the PEP Server for logging has been exhausted. Refer to the *pepserver.log* file for details. Logging is suspended until sufficient disk space is available. Refer to the message PTY080W.	The diskfullalert value is reached. The diskfullaction parameter in pepserver.cfg determines whether this message or PTY080W will be issued when the diskfullalert value is reached.	Refer to PTY080W for possible issues.
PTY085I	The disk space shortage for PEP Server logging has been relieved. Refer to the pepserver.log for details. Logging is resumed.	The disk space problem for the Open MVS PEP Server is resolved. It is the inverse of PTY084W.	No action is required. Message notifies you that the condition noted by PTY084W is resolved.
PTY086E	Invalid parameter value.	The parameter for Monitor Wait Interval, Peps Startup Wait Interval or Peps Monitor Wait Interval has invalid value.	Provide the required value and restart the Cryptographic Services Server.

Message ID	Definition	Issued when…	Recovery Actions
PTY087E	Conflicting wait intervals.	Conflicting startup parameters are specified: *MONITOR_WAIT_INTERVAL (default: &MONITOR_WAIT_INTERVAL) must be <= PEPS_MONITOR_WAIT_INTERVAL (default: &PEPS_MONITOR_WAIT_INTERVAL), which must be <=PEPS_STARTUP_WAIT_INTERVAL (default: &PEPS_STARTUP_WAIT_INTERVAL).*	Provide the required value and restart the Cryptographic Services Server.
PTY088E	Parameter value less than the minimum required value.	The Startup parameter value is less than the required minimum value.	Provide an updated value which is equal to or greater than required minimum value.
PTY089E	Parameter value greater than the maximum required value.	The Startup parameter value is greater than the required maximum value.	Provide an updated value which is equal to or less than required maximum value.
PTY090E	Invalid value for Log buffer queue block size in megabytes and Maximum allowed log buffer queue blocks.	The product of the LOGQBS X 1MB and LOGMQB startup parameters exceeds the 2GB maximum for buffer queue storage.	Provide the required value and restart the Cryptographic Services Server.
PTY102W	Tokenproc is disabled.	Token data element found, but tokenproc value is not PEP in *pepserver.cfg*.	If you want to use tokens, then change the Tokenproc value in *pepserver.cfg* to TOKENPROC=PEP.
PTY103W	Policy License Expired.	The security policy has been locked by the PEP Server due to license expiration. Only unprotection is available. No additional data may be protected.	Please renew the license for your ESA and Cryptographic Services Server.
PTY104W	Policy License Audit only.	Encryption and Token data elements are not allowed due to the audit only license.	Please procure a new license for your ESA with the required permissions.
PTY113W	Conversion not supported.	Unicode Conversion Service FROM Codepage provided is not supported. Character conversion will be done using Static tables.	Use static conversion tables.
PTY114W	Conversion not supported.	Unicode Conversion Service TO Codepage provided is not supported. Character conversion will be done using Static tables.	Use static conversion tables.
PTY115W	Conversion not supported.	Unicode Conversion Service FROM and TO Codepage provided is not supported. Character conversion will be done using Static tables.	Use static conversion tables.
PTY116W	Conversion failed.	Unicode Conversion Service Failed. Character conversion will be done using Static tables.	Use static conversion tables.
PTY120W	Message PTY120W is returned every 24 hours until the policy in shared memory is updated.	1. The policy that exists in the shared memory has not been updated in 24 hours.	1. Configure the PepServer listener socket to update the policy timestamp. 2. Power on the ESA machine.

Message ID	Definition	Issued when…	Recovery Actions
		2. When ESA is suspended, or powered off.	
PTY121E	NOCST is disabled in v6.5.2 and later versions, due to which software encryption or decryption for 3DES is disabled.	Software encryption or decryption for 3DES is not supported with PTYPFPS.	Set the CSTPROC=PTYCST statement in the PTYPARM file to start the Cryptographic Service Task (CST) startup procedure, and then comment out or remove the NOCST statement.
PTY128E	Attempt to read the *pepserver.log* file failed	The *pepserver.log* file is unavailable or the path to the *pepserver.log* file is incorrect.	Provide the entire path of the *pepserver.log* file in the *PEGLOPATH* parameter. For example, `"PEPLOGPATH =../defiance_dps/data/pepserver.log` Restart the Cryptographic Services server.

The following table describes the abend, or abort, codes that the Application Protector interfaces can issue.

Table 5-18: Abend Codes

Abend Code	Hex value	Decimal value	Applicable interfaces		
			CSL/CSI	CXL/CXI	SLL/SLI
CSI_PARMLIST_ADDRESS_NULL	X'001'	1	√		√
CXI_PARMLIST_ADDRESS_NULL	X'001'	1		√	
CSI_RETURN_CODE_ADDRESS_NULL	X'002'	2	√		√
CXI_RETURN_CODE_ADDRESS_NULL	X'002'	2		√	
CSI_REASON_CODE_ADDRESS_NULL	X'003'	3	√		√
CXI_REASON_CODE_ADDRESS_NULL	X'003'	3		√	
CSI_ESTAEX_FAILURE	X'004'	4	√		√
CXI_ESTAEX_FAILURE	X'004'	4		√	
CSI_RETURN_CODE_PARM_OMITTED	X'005'	5	√		√
CXI_RETURN_CODE_PARM_OMITTED	X'005'	5		√	
CSI_REASON_CODE_PARM_OMITTED	X'006'	6	√		√
CXI_REASON_CODE_PARM_OMITTED	X'006'	6		√	

Note: The various interface reason codes are broken into multiple pieces. Each code is only one byte in length and all the four bytes might not be used at any time. The right-most byte contains the reason code. The initial three bytes might contain an application specific value.

The following table lists the Return and Reason codes of the Application Protector solutions on z/OS.

Table 5-19: Application Protector Solutions on z/OS - Return and Reason Codes

Error Description	z/OS API Return Code	z/OS API Reason Code	ESA Log Code	Log Message – ESA Forensics
The data element was found, and the user has the appropriate permissions for the operation. Data protection was successful.	4	0	6	Authorized Data protection was successful

Error Description	z/OS API Return Code	z/OS API Reason Code	ESA Log Code	Log Message – ESA Forensics
The data element was found, and the user has the appropriate permissions for the operation. Data unprotect operation was successful. If mask was applied to the data element, then the appropriate record is added to the audit log description.	4	0	8	Authorized Data unprotection was successful
Policy check OK. The data element was found, and the user has the appropriate permissions for the operation. NO protection operation is done.	NA	NA	10	Authorized The User has appropriate permissions to perform the requested operation but no data has been protected/ unprotected.
The username could not be found in the policy in shared memory.	4	X'01'	1	UnAuthorized The username could not be found in the policy in shared memory.
The data element could not be found in the policy in shared memory.	4	X'02'	2	UnAuthorized The data element could not be found in the policy in shared memory.
The data element was found, but the user does not have the appropriate permissions to perform the requested operation.	4	X'03'	3	UnAuthorized The user does not have the appropriate permissions to perform the requested operation.
The data element was found, but the user does not have the appropriate permissions to perform the requested operation at this point in time.	4	X'04'	4	UnAuthorized The user does not have the appropriate permissions to perform the requested operation at this point of time
Data is too short to be protected or unprotected. For example, too few characters were provided when tokenizing with a length-preserving token element.	4	0001442838	22	Data is too short to be protected/unprotected.
Data is too long to be protected or unprotected. For example, too many characters were provided.	4	0001508375	23	Data is too long to be protected/unprotected.
Supplied input or output buffer is too small.	4	0001377301	21	Input or output buffer is too small.
Content of the input data to protect is not valid (e.g. for Tokenization). For example: • Invalid Date • Invalid Email address • Invalid Credit Card input • Invalid input for the Decimal token type • Invalid input size for Integer token type	4	2884652	44	The content of the input data is not valid.
The data element was found, and the user has the appropriate permissions for the operation. Data unprotect operation was successful with use of an inactive key ID.	4	0	11	Authorized Data unprotect operation was successful with use of an inactive keyid.
Used for z/OS Query Default Data Element when policy name is not found.	12	X'2E'	46	Used for z/OS Query Default Data element when policy name is not found
The data element was found, and the user has the appropriate permissions for the operation. Algorithm is NOT supported.	12	X'58'	7	UnAuthorized Data protection failed.
The data element was found, and the user has the appropriate permissions for the operation. Algorithm is unknown.	12	X'5D'	9	UnAuthorized Data unprotect operation failed.
No valid license or current date is beyond the license expiration date.	12	X'2C'	40	No valid license or current date is beyond the license expiration date.

5.9.5 Data Security Gateway (DSG) Error Handling

This section explains the common errors, permission restrictions, and problems you might encounter while working with Protegrity Data Security Gateway (DSG).

Table 5-20: DSG Common Errors

Error /Problem	This may happen because…	Recovery Actions
The following error appears in the browser when the SaaS is accessed through the Gateway: *`HTTP Response Code 599: Unknown.`*	The SaaS server certificate is invalid.	Perform one of the following steps: • Ensure that the forwarding address is correct. • Add the SaaS server certificate to the gateway's trusted store.
	The system time on the DSG nodes is not in sync with the ESA.	Perform one of the following steps: • Synchronize the system time for all the DSG nodes performing the following steps. 1. From the CLI Manager, navigate to **Tools** > **ESA Communication**. 2. Select **Use ESA's NTP** to synchronize the system time of the node with ESA. • Consider using an NTP server for system time across all DSG nodes and the ESA.
	The DNS configuration might be incorrect.	Perform one of the following steps: • Verify that the DNS configuration for the DSG node is set as required. • Verify that the hostname addresses mentioned in the service configuration are accessible by the DSG node.
The SaaS web interface is not accessible through the browser. The following error appears on the browser: *`HTTP Response Code 500: Internal Server Error.`*	The DSG node is not configured to service the requested host name.	Verify if the Cloud Gateway profiles and services are configured to accept and serve the requested hostname.
The following error message appears on the client application while accessing DSG. *`<h1>404 : Not Found<h1>`*	The HTTP Extract Message rule configured on the DSG node cannot be invoked.	Perform one of the following steps: 1. Ensure that you have sent the request to the URI configured on the DSG. If the request is sent to the incorrect URI, then the request will not be processed. 2. Verify the HTTP Method in the HTTP request.
A clustering error indicating that the host name is denied appears.	SSH key mismatch.	Perform the following steps on all nodes. 1. Navigate to **CLI** > **Tools** > **SSH Config** > **Known Hosts**. 2. Remove the host name or the host IP address that appears in the error message.

Error /Problem	This may happen because…	Recovery Actions
		3. Add the same host name or the host IP address to the cluster.
Clustering TCP communication failure occurred.	The node is not accessible.	Navigate to **Cloud Gateway** > **Cluster** and verify that the node IP address is accessible.
The Learn mode is not working.	The Learn mode is not enabled.	Perform one of the following steps: - Enable the Learn Mode for the required service. - Configure the following Learn Mode settings in the service creation screen: - Mention the contents to be included in the **includeResource** and the **includeContentType** parameters. For example, you can include the following resources and content types: *"includeResource": "\\.(css|png|gif|jpg|ico|woff|ttf|svg|eot)(\\?|\\b)",* *"includeContentType": "\\bcss|image|video|svg\\b",* - Mention the contents to be excluded in the **excludeResource** and the **excludeContentType** parameters. For example, you can exclude the following resources and content types: *"excludeResource": "\\.(css|png|gif|jpg|ico|woff|ttf|svg|eot)(\\?|\\b)",* *"excludeContentType": "\\bcss|image|video|svg\\b",*
The following message appears in the log: *`WarningPolicy;missing_host_key;Unknown ssh-rsa host key for <Host IP address>: f1b2e0bde5d34244ba104bab1ce66f96`*	The gateway issues an outbound request to an SFTP server.	The functionality of the DSG node is not affected. No action is required.
The following message appears in the log: *`raise ValueError("unknown cipher")#012ValueError: unknown cipher`*	An unsupported cipher is used in the Cipher field for SFTP Advanced Settings.	Use the list of ciphers supported for SFTP Inbound Settings. For more information about the list of supported ciphers, refer to the section *SFTP Inbound Settings*.
The following message appears in the gateway logs: *`protegrity-cg606 gateway.pyc: PCPG:20210415090809989914;18840;Error;Gateway;loadServic`*	The *default_80* HTTP tunnel created for the service is disabled.	To access the service, you must enable the *default_80* HTTP tunnel. To enable the *default_80* HTTP tunnel, on the ESA Web UI, navigate to **Cloud Gateway** > **Transport**, and click the **Tunnels** tab. Select the *default_80* HTTP tunnel and click **Edit**.

Error /Problem	This may happen because…	Recovery Actions
`es;restapi service cannot be associated with tunnel default_80. Tunnel default_80 is not loaded`		After the *default_80* tunnel is enabled, you must restart the gateway. On the **Tunnels** tab, click **Deploy to All Nodes** to restart the gateway.
When the data security operation request fails, the following message appears in the gateway logs : `protegrity-cg354 gateway.pyc: PCPG:20210416081619774574;40456;Error;RestRequestHandler;display_error;default_443 REST API Examples 10.10.3.16 POST /protect/csv 500 Failed to send logs to log processor.`	The **LogForwarder Service** is stopped.	To start the service, login to DSG Web UI, navigate to **System** > **Services** , and start the **LogForwarder Service**.
When the data security operation is performed, the following message appears in the gateway logs: `protegrity-cg591 gateway.pyc: PCPG:20210527114559844907;55080;Error;RestStreamRequestHandler;display_error;default_443 REST API Examples 10.242.2.3 POST /protect/csv 500 signature key and export value not loaded`		Perform one of the following options: 1. Ensure to perform the **Deploy** or **Deploy to Node Groups** operation from the *Cluster* screen on the ESA Web UI. a. Login to the ESA Web UI. b. Navigate to **Cloud Gateway** > **Cluster**. c. Select the **Refresh** drop down menu and click **Deploy** or **Deploy to Node Groups**. 2. If the DSG node is not in the cluster, then ensure to perform the *ESA Communication*.
When you enter the invalid **XPath** value in the *XML with ToT Extract Rule*, the rule is disabled and the following message appears in the gateway logs : `protegrity-cg852 gateway.pyc: PCPG:20210412113311375180;9869;Error;ExtensibleMarkupLanguageToT;_init_;Invalid XPath given for XPath option in rule : xml tot message extract no profile reference protegrity-cg852 gateway.pyc: PCPG:20210412113311375276;9869;Error;ExtensibleMarkupLanguageToT;_init_;Disabling rule xml tot message extract no profile reference due to XPath option error: Invalid expression`		Ensure that you enter the correct value in the **XPath** field and deploy the configuration to enable the rule.

Error /Problem	This may happen because…	Recovery Actions
An SSL error appears when the browser connects to the ESA Web UI.	The SSL handshake between the web browser and the ESA is not completed.	Update your web browser to the latest version (Internet Explorer, Google Chrome, or Microsoft Edge). Alternatively, perform the following steps. 1. In the Web UI, navigate to **Cloud Gateway** > **Transport** > **Tunnels**. 2. Select the *default_443* tunnel. 3. In the **OpenSSLCipherList** text box, check the version of SSL that is not allowed, for example, SSLv2 or SSLv3. 4. Configure the Cipher list to allow the SSL version. 5. Restart the DSG process. **Note:** If the Cloud Gateway menu is not available on the ESA Web UI, then login again to the ESA Web UI.
The Cloud Gateway nodes are stopped after patch is installed from the ESA Web UI.	More than one SSH Keys is assigned to the node added in the cluster.	Perform the following steps. 1. Delete the cluster from the *Trusted Appliance Cluster* screen. 2. In the ESA Web UI, navigate to **Settings** > **Network** > **SSH** > **Known Hosts** 3. Delete all the host names under known hosts. 4. Re-create a new cluster from the *Trusted Appliance Cluster* screen. 5. Add a node to the cluster from the *Cluster Monitoring* screen.
A connection timed out error occurs for an outbound request.	The outbound timeout limit is set to 20 seconds.	Perform the following steps. 1. Click **Cloud Gateway** > **RuleSet**. 2. Click the service that requires edits for the outbound timeout limit. 3. In the **Outbound Transport Settings** field, type the following code to increase the timeout limit. `{"connect_timeout": 30,"request_timeout": 180}`
In the *Log Viewer* screen, if you try to search for a time stamp, the search fails. If you searched for 2016-07-18T07: 41:15.429350 timestamp as seen in the table, the search fails.	The search field accepts numerical values.	Ensure that you remove the date and time separators from the timestamp that appears on the screen before you perform a search. For example, if you want to search for logs that occurred on 2016-07-18T07: 41:15.429350 timestamp, you must remove

Error /Problem	This may happen because…	Recovery Actions
		the date and time separators, and then search for 20160718074115429350. You can also search for a subset of the given timestamp. For ex, you can search for date by searching “20160718” in the search field.
When two or more DSG appliances are in a cluster, the following error message appears in Forensics. *`The clock on at least 3 nodes is out of sync.`*	The system time on some or all the nodes in the cluster is out of sync.	Ensure that the system time is synced manually on each of the affected nodes in the cluster. Perform the following steps: • Synchronize the system time for all the DSG nodes performing the following steps. 1. From the CLI Manager, navigate to **Tools** > **ESA Communication**. 2. Select Use *ESA’s NTP* to synchronize the system time of the node with ESA. 3. Perform the same steps on all DSG nodes. • Consider using an NTP server for system time across all DSG nodes and the ESA.
The following error appears in the *Log Viewer* screen or the gateway.log file when working with the S3 tunnel: *`An error occurred (RequestTimeTooSkewed) when calling the ListObjects operation: The difference between the request time and the current time is too large.`*	The system time on the DSG nodes is not in sync with the ESA.	Perform one of the following steps: • Synchronize the system time for all the DSG nodes performing the following steps. 1. From the CLI Manager, navigate to **Tools** > **ESA Communication**. 2. Select Use *ESA’s NTP* to synchronize the system time of the node with ESA. Consider using an NTP server for system time across all DSG nodes and the ESA.
The SSH session is terminated during the creation of a bond on the ethMNG interface.		Restart the session after the NIC bond on the ethMNG NIC is created.
A bond is created on both the network interfaces. While testing the fail over scenario by disconnecting the network, the gateway will be lost on both the interfaces. As a result, both the network interfaces will be unreachable.		Log in to the popout console and provide the gateway for both the interfaces if they are in the same network. After adding a gateway, check if the IP addresses are provided or acquired to the network interfaces. For more information about adding a default gateway to the Management NIC and Service NIC, refer to the section *Configuring Default Gateway for Network Interfaces*
The slave NICs do not have an IP assigned, but the following message appears during creating a bond: **`NIC Bonding is not available`**	The NICs might be on the DHCP mode.	Convert the NICs to Static mode.
The Web UI is not accessible after the NICs are bonded.		Reset the Network Bonding from the CLI Manager and bond the NICs again.

Error /Problem	This may happen because…	Recovery Actions
		For more information about resetting the NIC bonding, refer to the section *NIC Bonding*.
During binding NICs, the following message appears: `Unknown Error`	This might occur if the network is slow.	Restart the appliance queues using the following command: `/etc/init.d/appliance-queues server restart`
A bond is created (mode:1) on both the Network Interfaces using the DHCP mode. If you reboot the system, the MAC address and the IP address are changed.		To check if bonds are intact after a reboot on mode: 1, we recommend using Static IP for the Network Interfaces.
The `Join Cloud Gateway Cluster` operation fails.	The ESA administrator username, password, or both are incorrect.	Perform the following steps to mitigate the issue: - Ensure that the correct ESA administrator username and password is provided.

If an SFTP service is configured with public key authentication and the SSH public and private key are uploaded to the DSG, the following error is observed in the *gateway.log* when the SFTP tunnel is deployed.
`Error;SftpService;loadUserAu`
`thConfig;Service`
`SFTP_tunnel. Exception not`
`a valid RSA private`
` key file in processing`
`private key file /opt/`
`protegrity/alliance/config/`
`resources/`
`sftp_ssh_outbound_push_priva`
`te_key`
`Oct 23 16:34:41 protegrity-`
`cg874 gateway.pyc:`
`PCPG:20191023110441600085;41`
`133;Error;`
`Gateway;loadServices;service`
` initialization /opt/`
`protegrity/alliance/config/`
`services`
`/sftptunnel/sftptunnel.json`
`failed with message not a`
`valid RSA private key file`
	The SSH private key uploaded to the DSG is a not valid RSA key.	Ensure that the SSH private key is a valid RSA key. The DSG supports only RSA keys for SFTP.

After the DSG is installed, an error appears in startup log in the *gateway* log.
`PCPG:20200507012905113945;22`
`372;Error;Gateway;loadServic`
`es;service initialization`
`/opt/protegrity/alliance/`
`config/services/restapi/`
`<rule_name> failed with`
`message Blocked python`
`method '<module/method`
`name>' called in UDF`
	The module or method used in the custom code for UDF payload includes a blocked method or module.	Ensure that the module or method is not listed in the blocked method and modules. The vulnerable blocked method and modules are configured as part of the *gateway.json* file. It is recommended that these modules or methods are not removed from the list as a security best practice.
		You can either remove the module or method from the blocked list, or override the blocked module at the rule level.
		Note:
		You can only override modules at the rule level.

Error /Problem	This may happen because…	Recovery Actions
		For more information about the list of blocked modules and methods, refer to the section *Blocked Modules and Methods in UDF*. For more information about overriding modules, refer to the section *Advanced Rule Settings in UDFs*.
The following error message appears in the log while trying to process a file using SFTP. `PCPG:20190901205649639207 ;56920;Error; StubServer ;check_auth_publickey;<ip_address:port> backend connection to <ip_address:port> has failed, [Errno 110] Connection timed out`	- Network connectivity issues - SFTP server not reachable	Check the following list to mitigate the issue: - Check the network connection for the SFTP server. - Check the SFTP server is reachable.
When you access the Tokenization Portal, the **DSG Node** drop down does not display any node. All the other field s appear empty too.	It can occur due to following reasons: - Policy is synced across all ESA nodes in the cluster - Policy is not deployed to the nodes in the cluster - Nodes in the TAC are unhealthy - Nodes on the Cluster screen are unhealthy	Perform the steps provided for resolving the probable reasons: **Policy is synced across all ESA nodes in the cluster** Solution: Ensure that the policy on ESA is in sync with the policy on any other ESA in the cluster. **Policy is not deployed to the nodes in the cluster** Solution: Ensure that the policy is deployed to all the DSG nodes in the cluster. **Nodes in the TAC are unhealthy** Solution: On the ESA Web UI, navigate to **System** > **Trusted Appliances Cluster** to verify the node health. **Nodes on the Cluster screen are unhealthy** Solution: On the ESA Web UI, navigate to **Cloud Gateway** > **Cluster** > **Monitoring** to verify the node health.
The following message is displayed. `No enabled service to process request from <IP address>`	It can occur due to following reasons: - Hostname or IP address in a reque st is not mapped to any service in the Ruleset - Tunnel is not loaded in the DSG - Service is not loaded in the DSG	Perform the steps provided for resolving the probable reasons: **Hostname or IP address is not mapped to any service** Ensure that the hostname defined in the */etc/hosts* file is used to raise a request as well as is defined in the service at the Ruleset level. If the hostname is not defined in the *hosts* file and IP address is used, then ensure that the service IP address is used to raise a request and is defined in the service at the Ruleset level. **Tunnel is not loaded in the DSG**

Error /Problem	This may happen because…	Recovery Actions

		Perform the following steps based on the protocol used:
		1. Login to the DSG CLI manager.
		2. Navigate to **Administration** > **OS Console**.
		3. For HTTP, SFTP, or SMTP tunnels, execute the following command.
		`netstat -nap|grep <tunnel_port>`
		Check if the port mapped to the service IP is same as defined in the tunnel configuration.
		Note: If the command does not return the expected output, then navigate to the */var/log* directory and check the *gateway.log* for any exceptions during startup.
		4. For CIFS/NFS tunnel, execute the following command.
		`df -h`
		Check if the tunnel is mounted.
		Note: If the command does not return the expected output, then navigate to the */var/log* directory and check the *gateway.log* for any exceptions during startup.
		5. For an S3 tunnel, navigate to the */var/log* directory and check the *gateway.log* for any exceptions during start up.
		Service is not loaded in the DSG
		1. Login to the DSG CLI manager.
		2. Navigate to **Administration** > **OS Console**.
		3. Navigate to the */var/log* directory and check the *gateway.log* for any exceptions during startup.

The following error messages appear in *gateway.json*.
`PCPG:20200630071506415715;16`
`643;Error;ProtegrityDataProt`
`ection;transformProtect`
`;IV can't be used with this`
`token element (returnCode`
`0) filter Data Protection`
`PCPG:20200630071506415810;16`
	An Alpha-Numeric (0-9, a-z, A-Z) token type is used, with the case-preserving and position-preserving property enabled, in the Transform rule to transform sensitive data.	Ensure that you disable the case-preserving and position-preserving property in the Alpha-Numeric (0-9, a-z, A-Z) token type in order to use External IV property.

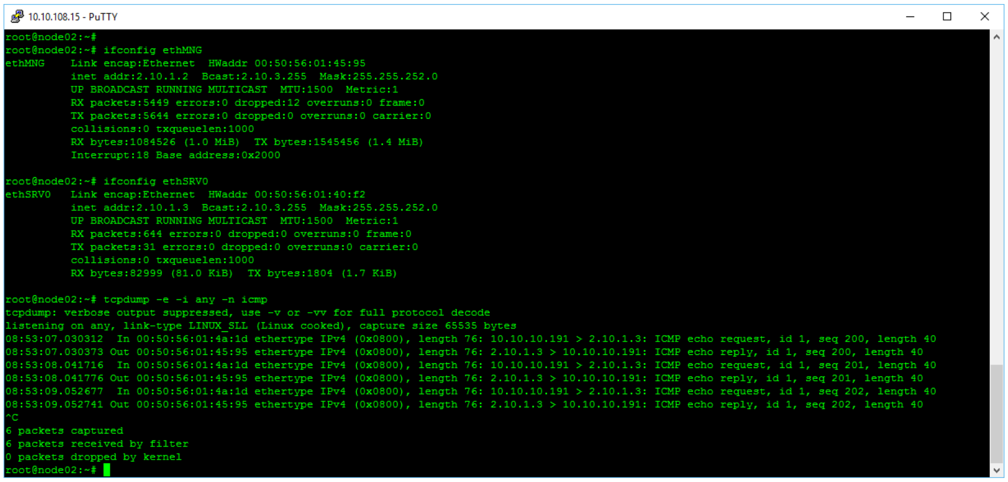
Error /Problem	This may happen because…	Recovery Actions
`643;Error;ProtegrityDataProtection;transform;Failed to transform. Rule Data Protection Err IV can't be used with this token element PCPG:2020063007150641995 0;16643;Error;RestRequestHandler;log_exception;IV can't be used with this token element (returnCode 0)`		
When CSV input with non-ASCII or Unicode data is processed using the *CSV* extract rule, the following error appears. `File "rule/extract/cCharacterSeparatedValues.pyx", line 520, in extract UnicodeDecodeError: 'ascii' codec can't decode byte 0xc3 in position 31: ordinal not in range(128)`	n/a	Ensure that the *Binary* extract rule is used before using the *CSV* extract rule.

When using SFTP service, the following error appears.
`Aug 30 22:10:18 DSG-1 gateway.pyc: PCPG:20200830164018867619;65345;Verbose; SFTPServer;_log;    raise IOError(text)`
`Aug 30 22:10:18 DSG-1 gateway.pyc: PCPG:20200830164018867666;65345;Verbose; SFTPServer;_log;IOError: SETSTAT unsupported`
	The SFTP client is trying to upload a file through the DSG to the *AWS Transfer for SFTP* server.	Check the following list to mitigate the issue.
		• Ensure that the *enable_setstat* parameter is set to `False`.
		• Verify that the value set for the *enable_setstat* parameter is a *boolean* value.

5.9.5.1 Static Routing Configuration

When both the NICs of a gateway appliance are part of the same network, it is recommended that static routing is enabled and configured. In absence of static routing, it might happen that a request is sent from one NIC, while the reply is received on the other NIC.

To understand a situation when static routing is not implemented, consider the following image.



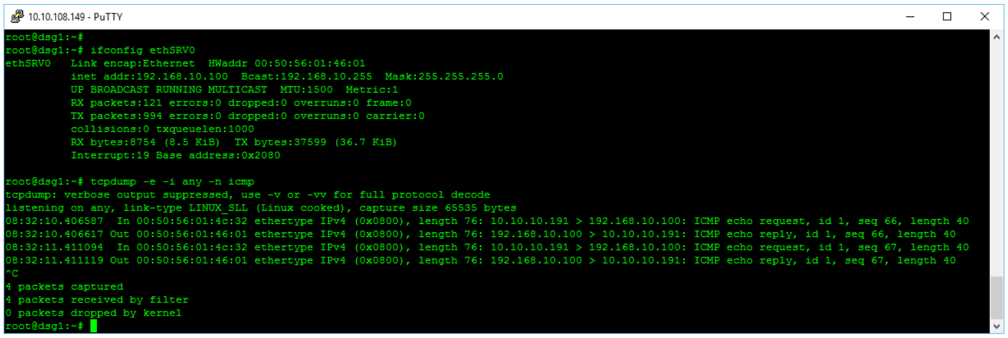
```
root@node02:~#
root@node02:~# ifconfig ethMNG
ethMNG    Link encap:Ethernet  HWaddr 00:50:56:01:45:95
          inet addr:2.10.1.2  Bcast:2.10.3.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5449 errors:0 dropped:12 overruns:0 frame:0
          TX packets:5644 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1084526 (1.0 MiB)  TX bytes:1545456 (1.4 MiB)
          Interrupt:18 Base address:0x2000

root@node02:~# ifconfig ethSRV0
ethSRV0   Link encap:Ethernet  HWaddr 00:50:56:01:40:f2
          inet addr:2.10.1.3  Bcast:2.10.3.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82999 (81.0 KiB)  TX bytes:1804 (1.7 KiB)

root@node02:~# tcpdump -e -i any -n icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
08:53:07.030312  In 00:50:56:01:4a:1d ethertype IPv4 (0x0800), length 76: 10.10.10.191 > 2.10.1.3: ICMP echo request, id 1, seq 200, length 40
08:53:07.030373 Out 00:50:56:01:45:95 ethertype IPv4 (0x0800), length 76: 2.10.1.3 > 10.10.10.191: ICMP echo reply, id 1, seq 200, length 40
08:53:08.041716  In 00:50:56:01:4a:1d ethertype IPv4 (0x0800), length 76: 10.10.10.191 > 2.10.1.3: ICMP echo request, id 1, seq 201, length 40
08:53:08.041776 Out 00:50:56:01:45:95 ethertype IPv4 (0x0800), length 76: 2.10.1.3 > 10.10.10.191: ICMP echo reply, id 1, seq 201, length 40
08:53:09.052677  In 00:50:56:01:4a:1d ethertype IPv4 (0x0800), length 76: 10.10.10.191 > 2.10.1.3: ICMP echo request, id 1, seq 202, length 40
08:53:09.052741 Out 00:50:56:01:45:95 ethertype IPv4 (0x0800), length 76: 2.10.1.3 > 10.10.10.191: ICMP echo reply, id 1, seq 202, length 40
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@node02:~#
```

As seen in the image, though a request is raised from the client IP to a DSG node associated with the NIC 2 (ethSRV0), the reply is directed towards the second NIC (ethMNG). This can be seen by the reply request, which points to the HW address of the second NIC.

The following image shows the expected behavior when static routing is implemented.



```
root@dsg1:~#
root@dsg1:~# ifconfig ethSRV0
ethSRV0   Link encap:Ethernet  HWaddr 00:50:56:01:46:01
          inet addr:192.168.10.100  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:994 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8754 (8.5 KiB)  TX bytes:37599 (36.7 KiB)
          Interrupt:19 Base address:0x2080

root@dsg1:~# tcpdump -e -i any -n icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
08:32:10.406587  In 00:50:56:01:4c:32 ethertype IPv4 (0x0800), length 76: 10.10.10.191 > 192.168.10.100: ICMP echo request, id 1, seq 66, length 40
08:32:10.406617 Out 00:50:56:01:46:01 ethertype IPv4 (0x0800), length 76: 192.168.10.100 > 10.10.10.191: ICMP echo reply, id 1, seq 66, length 40
08:32:11.411094  In 00:50:56:01:4c:32 ethertype IPv4 (0x0800), length 76: 10.10.10.191 > 192.168.10.100: ICMP echo request, id 1, seq 67, length 40
08:32:11.411119 Out 00:50:56:01:46:01 ethertype IPv4 (0x0800), length 76: 192.168.10.100 > 10.10.10.191: ICMP echo reply, id 1, seq 67, length 40
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@dsg1:~#
```

In this case, when the request is raised from the client to a DSG node associated with NIC 1(ethSRV0), the reply is also received at the same NIC. This can be seen by the reply request, which points to the HW address of the same NIC.

Static routing ensures that routing in the network operates smoothly.

5.9.5.1.1 Configuring Static Routing

Before you begin

Before you can configure static routing, ensure that after DSG v1.0.1 installation, a system reboot is performed. The system reboot upgrades the Linux kernel version to *4.1.27generic*, which is required for configuring static routing.

Execute the following command to verify the kernel version.

```
uname -r
```

➤ To configure static routing:

1. From the CLI Manager, navigate to **Tools** > **OS Console**.
2. Execute the following set of commands.

```
# ip route add 2.10.0.0/22 dev ethMNG table 1 //2.10.0.0 is the network of first
NIC (ethMNG).

# ip route add default via 2.10.1.1 table 1

# ip route add 192.168.10.0/24 dev ethSRV0 table 2 //192.168.10.0 is the network of
second NIC (ethSRV0).

# ip route add default via 192.168.10.1 table 2

# ip rule add from 2.10.1.5/22 table 1 priority 100

# ip rule add from 192.168.10.100/24 table 2 priority 200
# ip route flush cache
```

Chapter 6

Troubleshooting of Special Environments

6.1 Trusted Appliance Cluster

In ESA, you can configure the *customer.custom* file to export or import custom files from one node to another. You can validate the export import process by running the *validate_export.py* script. You can fix the errors that are occur based on the logs generated by running this script.

➤ To run the export_validate.py file

1. In the CLI Manager, navigate to the **Administration** > **OS Console**.
2. Navigate to the `/opt/ExportImport/filelist/` directory.
3. Run the following command:

   ./validate_export.py

   > **Note:** You can view the logs related to the export and import of custom files under `/var/log/ExportImport.log` and `/var/log/syslog` directories.

6.2 Paravirtualization FAQ and Troubleshooting

This section lists some Paravirtualization Frequently Asked Questions and Answers.

Frequently Asked Questions	Answers
Why are XenTools not provided with the appliance?	In addition to the distribution issues, the XenTools depends on the exact version of your XenServer.
I cannot boot the virtual machine in PVM mode.	Ensure that no CD/DVD (ISO image) is inserted to the machine. Eject all CD/DVDs, and then reboot. Make sure that PVM is enabled on the hypervisor itself. For more information about PVM, refer to section *Manual Configuration of Xen Server*. The last resort would be to use a Live-CD, for example, Knoppix, in order modify the appliance files.

Frequently Asked Questions	**Answers**
I cannot initialize High-Availability.	Probably you have installed the XenTools but you have not rebooted the system after the XenTools installation. Reboot the system and retry.

I need to set up a cloned virtual machine as soon as possible.	Currently cloning a virtual appliance is a risk which is not recommended.
	Perform the following steps. 1. 2.
	1. Clone a machine.
	2. Log onto to the cloned machine.
	3. Modify the hostname and the IP address.
	4. Manually execute the following scripts:
	`#/etc/opt/scripts/first-boot/5_mk_ssh_keys.sh`
	`#/etc/opt/scripts/first-boot/5_mk_web_certificate.sh`

After switching to PVM mode, I cannot use the XenCenter.	Close the XenCenter and open a new instance.

Chapter 7

Renewing Certificates in the ESA v8.1.0.0 for 6.6.x Protectors

Before you begin
Consider a scenario where you are working with the ESA v8.1.0.0 that is operating with a v6.6.x protector. If the v6.6.x protector-specific certificates are expired, then you must renew the certificates to continue operating with the ESA v8.1.0.0. This ensures the backward compatibility of the ESA v8.1.0.0 with the v6.6.x protectors using the renewed certificates.

➤ To renew certificates:

1. Navigate to the **ESA Web UI** > **System** > **Services**.
2. In the *Policy Management* area, stop the *HubController* service.
3. On the ESA CLI Manager, navigate to the **Administration** > **OS Console**.
4. Execute the following command.

   ```
   wget -O- --method=POST http://localhost:25300/api/v1/certificates/dps/renew
   ```

5. Navigate to the **ESA Web UI** > **System** > **Services**.
6. In the *Policy Management* area, start the *HubController* service.
7. In the *Policy Management* area, restart the *Logfacade Legacy* service.
8. Execute the following commands on all the PEP Servers with the expired certificates.

   ```
   cd /opt/protegrity/defiance_dps/data
   ../bin/GetCertificates ESA [host] [username]
   tar zxvf esacerts.tgz
   ```

   The renewed certificates are downloaded from the ESA to all the PEP Servers.

9. Restart all the PEP Servers.

   ```
   [/opt/protegrity/defiance_dps/bin]# pepsrvctrl start
   ```

Chapter 8

Resetting Administrator Password

If your administrator password is unavailable, perform the following steps to reset the administrator password. You need to update the LDAP server after the password is reset.

➤ To reset the administrator password:

1. Boot the appliance.

   The splash screen appears.
2. Select **Normal**.
3. Press **E** to edit the entry.
4. Set the value of the *kernel line* parameter to *single*.
   a. Navigate to the end of the following line.

      .....audit_backlog_limit=8192

   b. Type the following text.

      <SPACE>S
5. Press **F10** to start the appliance.

   The screen to enter the root password appears.
6. Type the root password and press **ENTER**.
7. Run the following command.

   ```
   slapcat -l /tmp/dump.ldif
   ```
8. Run the following command to edit the *dump.ldif* file.

   ```
   vi /tmp/dump.ldif
   ```
9. Search the *userPassword*:: attribute for the following entries:
   - *dn: cn=admin*
   - *dn: cn=ldap_bind_user*
10. Edit the *userPassword:: <old password>* to *userPassword: <new password>*.

    > **Note:**
    > Ensure that the *userPassword* attribute contains a single colon.
    >
    > If a user account is locked due to multiple login failure, delete the *pwdFailureTime:* attribute to unlock the user.
11. Save the file.
12. Exit the editor.

13. Run the following commands:

```
rm -rf /opt/ldap/db.bak
cp -aR /opt/ldap/db /opt/ldap/db.bak
rm -rf /opt/ldap/db/*
cp -aR /opt/ldap/db.bak/DB_CONFIG /opt/ldap/db/
slapadd -l /tmp/dump.ldif
chown -R openldap:openldap /opt/ldap/db
```

14. Restart the machine.

15. If the password for the *ldap_bind_user* is changed in step 12, LDAP users cannot login to the appliance. To ensure that LDAP users can login to the appliance, perform the following steps.

    a. Login to the appliance as *local_admin* user.

    b. navigate to **Administration** > **Specify LDAP server/s** > **Protegrity LDAP server/s**.

    c. Specify the password provided for *ldap_bind_user* in step 10 in the **Bind Password** text box.

    d. Select **Ok** to save the changes.

Chapter 9

Special Utilities

9.1 DPS Admin

The PEP Server is supplied with a special utility, called DPS Admin that helps you analyse your protection operations, troubleshoot the possible errors, etc.

> **Note:** In fact, all DPS Servers have this tool and capability. The functions vary by server. The common functionality is that all servers have the function to alter log level. This is helpful when troubleshooting. Thus, for example, using this tool you can increase the log level without restarting the server.

Start DPS Admin from the PEP Server, from the *`opt/protegrity/defiance_dps/data`* directory:

```
[root@protegrity-ps:/opt/protegrity/defiance_dps/data ] # ../bin/dpsadmin
Enter admin user password :

dpsadmin 7.0.0.4
Type help for usage.
Type quit to exit the application.
>>> help
getversion: Returns the DPS version information.
getloglevel: Returns the current application log level.
setloglevel: Sets the application log level.
login: Login to the server.
help: Returns this help text.
getpolicyheader: Returns information about the policy in shared memory.
getdataelements: Returns a list of data elements in shared memory.
getpolicyusers: Returns a list of users in shared memory.
getuserdeaccess: Returns access list of a user in shared memory.
gettrustedapplications: Returns a list of trusted applications in shared memory.
getpolicydataelements: Returns a list of data elements for a specific policy type.
getpolicyinfoheader: Returns information about the policy INFO in shared memory.
getlicense: Returns the license in XML format.
getlicensestatus: Returns the current license status ('OK', 'Expired', or 'Invalid').
getlicenseremainingdays: Returns the number of remaining days ('none', 'unlimited', or a
number).
gettokenelements: Returns a list of token elements in shared memory.
sendlog: Send XML log file to ESA
getjsonpolicyroles: Returns a list of users and roles in json format.
getdownloadinfo: Returns information about registration, download and status.
```

The following table explains the commands which you can run using the DPS Admin tool available on PEP Server:

You can	Using command
View the current application version	***`print(getversion())`***

You can	Using command
View the application log level	`print(getloglevel())`
Set the application log level when the server is running. Once restarted, it will use the setting from the *cfg* file.	`print(setloglevel())`
Login to the server	`login(‘masteruser’, ‘masterpassword’)`
View information about the policy in shared memory	`print(getpolicyheader())`
View a list of data elements in shared memory	`print(getdataelements())`
View a list of policy users for a specific policy type	`print(getpolicyusers())`
View a list of data elements for a specific policy type	`print(getpolicydataelements())`
View a list of data elements for unstructured policies	`print(getpolicydataelements('unstructured'))`
View a list of data elements for structured policies	`print(getpolicydataelements('structured'))`
View information about the policy information in shared memory	`print(getpolicyinfoheader())`
View the license in XML format	`print(getlicense())`
View the current license status ('OK', 'Expired', or 'Invalid')	`print(getlicensestatus())`
View the number of remaining days ('none', 'unlimited', or a number)	`print(getlicenseremainingdays())`
View a list of token elements in shared memory	`print(gettokenelements())`
Send XML log file to ESA	`sendlog`
View help	`help`

The sample result of running `>>>print(getpolicyusers())` command follows:

```
1;PolicyUser;171552018
[A:URP-] [T:URPD] [S:URP-] [F:URP-] [M:<none>          ] [O:CLEAR    ]
[A:URP-] [T:URPD] [S:URP-] [F:URP-] [M:C 6 / C 4 / Ch=*] [O:MASK     ]
[A:URP-] [T:URPD] [S:URP-] [F:URP-] [M:M 3 / M 2 / Ch=#] [O:MASK     ]
[A:URP-] [T:URPD] [S:URP-] [F:URP-] [M:M 0 / M 5 / Ch=*] [O:MASK     ]
[A:--P-] [T:URPD] [S:URP-] [F:URP-] [M:<none>          ] [O:NULL     ]
[A:--P-] [T:URPD] [S:URP-] [F:URP-] [M:<none>          ] [O:ENCDDATA ]
[A:--P-] [T:URPD] [S:URP-] [F:URP-] [M:<none>          ] [O:EXCEPTION]
[A:URP-] [T:URPD] [S:----] [F:URP-] [M:<none>          ] [O:CLEAR    ]
[A:--P-] [T:----] [S:URP-] [F:URP-] [M:<none>          ] [O:EXCEPTION]
```

The columns above define the following security details for each data element for a specific user:

- **A**: Access permissions for the data element (**U**nprotect/**R**eprotect/**P**rotect/**D**elete)
- **T**: Time permissions (operations permissions for **U**nprotect/**R**eprotect/**P**rotect/**D**elete at the current time, i.e. when the DPS is)
- **S**: Success audit for **U**nprotect/**R**eprotect/**P**rotect/**D**elete operations
- **F**: Failed audit for **U**nprotect/**R**eprotect/**P**rotect/**D**elete operations
- **M**: Masks (none if applied or details of the mask applied)
- **O**: Output (null, mask, encrypted value, exception).

Chapter 10

Frequently Asked Questions

Note: The File Protector (FP) is certified for version 6.6.5.

10.1 Common FAQ

Questions	Answers
What should I do if I encounter a problem with my Protegrity products?	First, refer to your Protegrity documentation package. *Master Index Document* includes a high level explanation of product specific guides. It can help you understand which guide has the information about the features that you need help with. If Protegrity documentation does not help, then refer to this guide for error handling and troubleshooting steps. Finally, you can contact Protegrity Services as suggested in section *2.1 Access Protegrity Support* of this guide.
Which protection methods are supported for my protector?	Refer to *Protection Methods Reference Guide* document for detailed information on protection methods to be used by Database protectors, Application protectors, and File protectors.

10.2 Policy Management FAQ

Questions	Answers
I am trying to create a policy to be deployed to a database protector. I cannot view the Select/Update /Insert/Delete permissions in Policy management.	To view the deleted option, set *dbpolicy = 1 in /var/www/Management/SecurityManager/private/sm.cfg* file.

10.3 Appliance FAQ

Questions	Answers
How do I ensure my ESA is installed/ upgraded correctly?	Review the appliance installation log to ensure smooth installation/ upgrade of your ESA Appliance. You can do that using the appliance Web Interface (**System Information** > **Appliance Logs**) or the CLI Manager (**Status and Logs Appliance** > **Logs**).
What should I do if I cannot login to my appliance with the *admin* user account?	Use the local_admin user account to login to ESA CLI to troubleshoot and fix problems related to LDAP or the admin user account. If the appliance System Administrator has not changed the default credentials, then the password of local_admin is the same as the password of the admin user.
My ESA Appliance has two factor authentication enabled. I am the admin user and I need to log onto appliance Web Interface immediately. However I do not have the hand-held device with the Authenticator app with me. Is there any way to access the appliance now?	If it is not possible for you to generate the verification code to login to Protegrity appliance, then you can use the local_admin user account to login. This user is kept out of the list of users using the two factor authentication. By default, as a local_admin, you can login only from the local console, and you can enable both SSH and web-access.
How can I disable the appliance two factor authentication?	If you have enabled the *local_admin* user access to the Web Interface, then you can simply login to the Web Interface and disable the appliance two factor authentication. If the *local_admin* cannot login to the Web Interface, which is the default, then you can login as the *local_admin* from the local console, switch to O.S console and execute `#/etc/opt/2FA/2fa.sh -disable`.
My ESA Appliance has two factor authentication enabled. I can login to Protegrity Reports using only my current username and password, and I am not asked to enter the verification code.	Protegrity Reports is currently not included in appliance two factor authentication. As a user, you can login with your username and password.
How can I access my appliance CLI Manager?	You can access the CLI Manager via the appliance Web Interface by navigating to **System Configuration** > **CLI Manager**. Alternatively, you can access the CLI Manager using an SSH client, for example PuTTy.
Upon trying to log into the CLI Manager via the appliance Web Interface using the IE browser, whatever I type for admin credentials, is not even displayed. What should I do?	You need to change the Compatibility View by clicking on the blue icon displayed to the right in the address bar, in the SSH login dialog. Alternately, you can use Firefox Mozilla or Google Chrome browsers.
How should I monitor my ESA appliance on a regular basis?	Use real-time graphs (**System Information** > **Graphs**) and system information (**System Information** > **Services & Status** > **Information tab**tab) in the appliance Web Interface. Use appliance System Monitor, accessible via appliance CLI Manager (**Status and Logs Appliance** > **System Monitor**).

Questions	Answers
	If you are using an appliance cluster, then you can monitor the cluster status via the appliance Web Interface (**System Information** > **High Availability**). Check current event appliance logs. You can do that using the appliance Web Interface (**System Information** > **Appliance Logs**) or the CLI Manager (**Status and Logs Appliance** > **Logs**). Set up alerts for specific events (refer to *Protegrity Enterprise Security Administrator Guide*).
What is the best way to back up my appliance?	6.6.x and 7.x.x appliances support clustering with scheduled replications of nodes within an appliance cluster. On-demand backups can be created by saving data to files, remote appliances, or cluster nodes. For details on backup and restore, refer to *Protegrity Appliances Overview Guide*.
How should I troubleshoot any issues related to the appliance internal LDAP?	Use LDAP Monitor tool available in the appliance CLI Manager (**Appliance Administration** > **LDAP Management** > **Local LDAP Monitor**) and LDAP monitor in the appliance Web Interface (**LDAP** > **Management** > **Monitor**).
How do I configure a Firewall on my appliance?	Starting with the 6.6.x Release, the appliance has a rule-based Firewall for incoming connections. Standard rules can be managed using the CLI Manager (**Networking** > **Network Firewall** tool). Manual/complex rules can be applied in the script files. Required ports are by default opened for installed products.
How can I check that another appliance/server is reachable by my appliance?	You can ping your server using the Ping tool, available in the appliance CLI Manager, **Networking** > **Network Troubleshooting Tools**.
What clustering options are available for Protegrity appliances?	From v6.6.x onwards, release appliances support High Availability (active-passive) cluster between two appliances, and a trusted network (active-active) between multiple appliances. For details, refer to *Appliances Overview Guide 8.0.0.0* and *Scalability and Availability Guide 7.0.1*.

How to fix the error that occurs while importing a user from external LDAP?	The following error occurs if you try to import a user where the username in local LDAP and External LDAP are same.
	`Failed (err=-1): #1: Error: LDAP Failure: {'desc': 'Already exists'}`
	`#2: Error: Failed (err=-1) to add user 'XXXXX' role(s) '['Allow_SSH_Access', 'XXXXXX_XXX_Administrator', 'Appliance_web_manager', 'XXXX_XXXX']' by 'cn=XXXXX,ou=people,dc=esa,dc=protegrity,dc=com'`
	Workaround:

Questions	Answers
	1. Delete the user from the Local LDAP. 2. Import User

10.4 Database Protector FAQ

Questions	Answers
How can I check whether my Database Protector is working or not?	You can easily check the state of your Database Protector by inspecting *pepserver.log* for any warnings or errors. If pepserver.log does not show any errors but you still want to check the policy state on your Protector, then use the DPS Admin tool to inspect the policy state, deployed data elements and users in the policy. Refer to section 7.1 DPS Admin of this document for guidance on using `dpsadmin`. To verify whether UDFs are working you can execute the following functions: whoami() getversion()

Encryption fails for data with input length nearing 500 bytes.	Depending on the database and the non-length preserving encryption algorithms used—AES-128, AES-256, and 3DES—encryption is successful for data with input length of up to around 490 bytes.
	The following error messages are returned.
	• For length of the input data beyond this successful length and up to 500 bytes:
	`Failure 7509 Result Exceeded maximum length`
	• For length of input data more than 500 bytes:
	`Failure 7504 in <UDF/XSP/UDM>`
	The input length of data can be changed for certain databases. Refer to the next troubleshooting question in this table to improve Teradata database performance.

When I check the version number of Teradata DB protector with pty_getversion(), after upgrading to the latest protector version, I am able to view the older version number and not the correct one.	This happens because the cache that has been brought forward with the upgrade continues to retain the older version number. From the three workarounds provided here, follow one before you begin a task in the upgraded protector: • Reboot the host • Restart the database • Install the UDFs in a path that is different from the earlier installation
I cannot view the SQL Director of a Database Protector. What should I do?	The SQL Director is no longer supported for all the Database Protectors. As an alternative to the SQL Director, you should use

Questions	Answers
	the sample scripts that are available in the installation package of the Database Protector. After the protector is installed, run the *sample* scripts that are available in the `/defiance_dps/pep/sqlscripts/<DB Name>` directory. The *sample* script shows how the user-defined function can be used to implement data protection (both encryption and tokenization).
Are there any restrictions for bulk protect, unprotect, or reprotect operations with Oracle database platforms?	There are no limitations from the product side but restrictions from the database platform side. The utility [sqlplus] provided by Oracle supports only 2499 characters in a single line. If data larger than 2499 has to be inserted in a column, then the delimiter "|" has to be used.

10.5 Application Protector FAQ

Questions	Answers
How can I check whether Application Protector is working or not?	You can easily check the state of your Application Protector by inspecting the pepserver.log for any warnings or errors. If pepserver.log does not show any errors but you still want to check the policy state on your Protector, then use the DPS Admin tool to inspect policy state, deployed data elements and users in the policy. Refer to the section DPS Admin of this document for guidance on using **`dpsadmin`**.
How can I check whether AP Standard, AP Client, AP Lite, AP Java are working or not?	A simple program can be compiled and run, using samples provided as a part of the Application Protector installation package.
I perform bulk operations. How many audit logs should I expect?	You should expect one most severe audit log for each request. In addition, if you have *logcallouts* parameter set to Yes in *pepserver.cfg*, then you will also get one audit log with code "45" for each data item processed in a batch.
When using AP Java with multiple threads, a core dump is generated or "Out of Swap space" message is generated.	You can resolve this by increasing the kernel limits for memory and virtual memory.

Whenever a policy is deployed with token element of type Printable, the token element of type Printable is not generated.	In Scenarios where policy with only one element (token type printable) or policy with more than one element (at least one element is token printable and others are different types of token elements) are deployed, tokens get generated except for type Printable.
	At the first level of resolving, the system file `/etc/security/limits.conf` have been modified as below to make stack and data memory unlimited:
	default:
	fsize=-1
	core=2097151
	cpu=-1
	data=-1

Questions	Answers

	rss=-1
	stack=-1
	nofiles = 2000
	root:
	cpu=-1
	data=-1
	rss=-1
	stack=-1
	stack_hard=-1
	fsize=-1
	For 32bit AIX programs:
	An AIX application can allocate many chunks of native heap memory from a single 256MB segment. An application can also map multiple chunks of memory in a single segment. However, when AIX attaches a shared memory set, it reserves an entire 256MB segment regardless of the size of the set. This is only true for 32-bit applications; AIX 64-bit applications only need enough space to fit the set.
	Therefore, when a 32-bit application attaches a 10K shared memory set, AIX must reserve an entire 256MB segment, even though 255.99MB are unused.
	Uniquely, AIX allows 32-bit applications to use the shmctl() function to resize a shared memory set up to the 256MB segment size. There is a workaround to overriding the memory model at runtime.
	Use an environment variable command to start a single application with a different memory model (in bash):
	export LDR_CNTRL=MAXDATA=0x50000000
	This will allow the pepserver to use 5 segments of 256MB. With this setting, you can deploy a Printable token element.
	Since a 32bit application can address 4GB which can have a maximum of 16 segments. Our build machine has 2GB so it can have a maximum of 8 segments, but the pepserver wouldn't start with that. It got other resource limits then. 5 segments are enough for a Printable token element.

10.6 FUSE FP FAQ

Questions	Answers
Do FUSE FP protection and encryption change the file size?	The protection that the Access Control function provides doesn't change the file size. However, the encryption that the File Encryption function provides will increase the file size 8k.
What if I forget the policy password?	The FUSE FP uses policy which is deployed from ESA. If you forget the policy password, then you can reset it in ESA, and redeploy the policy to FUSE FP. To update the policy password cache in File Protector database file, run the following command. `dfpadmin database –o update-policy-password <policy> <password>`
What if I forget which files/folders are FE encrypted?	Run the following command to list the FE encrypted files/folders located in the specified path. `find <path> -exec dfp file stat {} \; | grep "<?>"`
Can I manually protect or encrypt all the files under a directory?	Yes. The following commands show how to protect or encrypt all files under a directory with a data element: • `dfp ac protect [-f] [-I] [-r] -d <data element> <folder>` • `dfp file protect -noac [-r] -d <data element> <folder>`
How much space should I prepare for file encryption?	File size will increase 8KB after it is encrypted. If your folder has n sub files/folders, then you need to prepare additional n*8KB space for the encrypted file. The File Protector will require a temporary space (2*file size + 8KB) in the current mount point for encrypting an existing file. For example: if you have a 10GB single file that needs to be encrypted, then you will need additional 10GB+8KB free space for the encryption apart from the base file size.After the 10GB file encryption ends, this temporary space will free up again.
Do the user or process can create a clear text file in an FE protected folder without loading a policy or data element?	No, FUSE FP returns `Permission Denied` error message.
How to protect the source path using FUSE FP?	You can protect the source path in case of AC and AC+FE protection. In case of FE protection, the source path protection is not available.
How do I get the protection/encryption status of a directory tree?	The following example shows how to find all directories' protection/ encryption status within a directory called hard_plus: • `dfp ac status` • `dfp file stat -r hard_plus`

Questions	Answers
How do I force a task to have no data element loaded while the current process has data elements loaded?	Use `dfp start -n` to launch a new process without data elements. The following example shows the protection status of the current directory with no policy loaded. `dfp start -n dfp ac stat /`

How to check whether FUSE FP is working or not?	Run the following command to check all the FUSE FP modules are live and operational.
	`dfpadmin module status`
	Run the following command to check all the FUSE FP services are running.
	`dfpadmin service status`

How do we prove the file is encrypted?	When you open an encrypted file without loading the required policy, the following scenarios can occur: • You can view the encrypted file with cipher text outside the mount point. • you can get a `permission denied` error message within the mount point. **Note:** If a file is encrypted with a data element where there is no read permission and output setting is set cipher, then you can view the encrypted file with cipher text within the mount point.
Does FUSE FP have any limitation on the data element algorithm?	Yes. For now, FUSE FP Encryption only supports AES (128 and 256 bit) and 3DES encryption algorithms.
What kind of applications does FUSE FP support to delegate?	For Linux, FP supports all executable applications delegation.
How can we prevent some folders from protecting/encrypting?	You can add the folders absolute path to the `/opt/protegrity/fileprotector/data/ac_disallow.conf` and `/opt/protegrity/fileprotector/data/disallow.conf` to force them not to be protected and encrypted.
Does File Encryption have access control?	No. File Encryption has no access control since it is provided by the Access Control functionality. If you want to apply the AC and FE protection (file protection) on files and directories, then you must run the *file protect* command. The following command shows how to encrypt a file and protect it with access control: `dfp file protect -d <data element> <file>` The following command shows how to encrypt a folder and protect it with access control:

Questions	Answers
	`dfp file protect [-f] [-r] -d <data element> <folder>`
Can we delegate a user?	Yes. FUSE FP supports user delegation. Use this command to delegate a user: `dfp delegate [-f] –u <username> <role>@<policy> [<password>]`
Does FUSE FP depend on the Kernel version?	The Enhanced Security (*es*) modules of FUSE FP are introduced to protect the access for the source path. These modules depend upon the kernel version. If the FUSE FP is installed with the *es* modules, then the kernel version must be compatible with the FUSE FP *es* modules.

10.7 File Protector Gateway FAQ

Queations	Answers
Can the size of an encrypted loopback device be increased when FPV is installed on FPG Server?	Yes. From File Protector Gateway 6.5 Release, we can increase the loopback device size by running some Unix system command, such as `losetup, dd, resize2fs, cryptsetup`, etc.
Does FPV installation on FPG have any limitation on the data element algorithm?	Yes. For now, FPV only supports AES (128 and 256 bit) and 3DES encryption algorithms.
What kind of volumes can be encrypted on FPG Server?	Loopback devices (e.g., `/dev/loop1`) and storage devices (e.g., `/dev/sdb1`).
What protocols are supported by FPG?	FPG supports NFS/CIFS/iSCSI/FTP/WebDAV protocols for mounting storage and service shares. FPG supports SFTP/SCP/CP/HDFS/HDFS FP protocols in Extract and Load tab of ETL Toolkit, for extracting source files from remote/local server and loading output files onto remote/local target server.
Is FPG Server compatible with ETL Gateway?	No
Is upgrade supported by FPG Server?	Yes. You can upgrade from FPG V6.5.2 SP2 patch 4 to FPG 6.6.2. If you are upgrading a 6.5.2 SP2 Patch 4 to v6.6.2 with FPV-add-on, then the old FPV add-on is overwritten by FPV v6.6.2, rather than a real upgrade.
What browsers are supported by FPG Server?	FPG supports IE 10, Mozilla FireFox 24.x, and Google Chrome 26.x or higher version.
Does FPG change the source directory structure tree?	The FPG keeps the same source directory tree in all modes, except the many-to-one flat file mode. For example, the tree will have as many layers in the output folder as the source folder has.
Is it mandatory to create tasks under the /output folder?	Though for folder activities related to FPG the files must be under the /output folder, for ETL specific task creations, the files can be present under the `/opt/protegrity/fpg/etl/tasks` folder.
Can FPG keep the number of source files?	Yes. You will have as many output files as source files.
Can FPG support LDAP and Active Directory authentication?	Yes. FPG supports Protegrity LDAP servers and Active Directory authentication.
What kind of files does FPG support for encryption or tokenization?	Delimited, Fixed, XML and Custom Data type data structure files. For example, text file with these suffixes txt, xml, html, htm, csv, etc.

Queations	Answers
Is there any limitation on supported type file size?	For both Flat file and Custom Data files there is no limitation on the supported file size. For now, XMLReplace file size supports the maximum size of 200 MB.
Does FPG support PGP encryption and decryption?	Yes. FPG supports PGP decryption/encryption.
Can FPG schedule when to execute a task?	Yes. FPG can configure task execution when input directory is updated and specify the time to execute the task.
Can FPG backup/restore the task configuration files?	Yes. FPG supports task configuration files backup and restore. Thus, you can export your task configuration files or import your existing task configuration files.
What kind of protection types does FPG support?	FPG supports protection, tokenization, unprotection, detokenization, and hashing.
Can we just protect/encrypt simple data or message without configuring a task?	Yes. FPG provides Data Protection function to preview and test your configured task execution, and protect/unprotect the simple sensitive data/message without configuring a task.
Can FPG log the operations?	Yes. FPG has the Task Log and Audit function.
Does Automatic Setting of FPG task monitor the updates of the specified input directory of a remote server?	No. FPG only supports monitoring the local directory only on the FPG machine.
Can FPG HDFS/HDFS FP extract and load settings support connection to more than one Hadoop cluster at the same time?	No. FPG HDFS/HDFS FP extract and load settings can only support connection to one Hadoop cluster at a time. This connection is also a global setting for all ETL tasks in this FPG. **Note:** Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated. The HDFSFP-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.
Is it mandatory to install FPV v6.6.2 before upgrading FPG v6.6.3 to FPG v6.6.4?	Yes. If you want to use FPV v6.6.4 that is packaged with FPG v6.6.4, you must install FPV v6.6.2 that is packaged with FPG v6.6.3 before upgrading FPG v6.6.3 to v6.6.4.