Integration with Exabeam

Implementation Guide

About Exabeam

Exabeam delivers next-generation Security Management technology that enables organizations to protect their most valuable information. The Exabeam Security Management Platform combines unlimited log data collection, advanced behavioral analytics, and automated incident response, all supported by Exabeam's patented Smart Timelines technology that uses machine learning to track identity and behavior over time.

This guide describes how to configure CyberArk Enterprise Password Vault (EPV) and Privileged Threat Analytics (PTA) to send syslog messages to Exabeam SIEM solution, and how to configure Exabeam to be able to receive and process these messages.

The guide is based on CyberArk EPV Version 9.95, CyberArk PTA Version 3.6 and Exabeam Advanced Analytics i48.

CyberArk PTA - Exabeam Integration

PTA can send detected incidents as syslog messages to a SIEM solution. This section describes how to configure integration of PTA with Exabeam SIEM solution.

When PTA detects an event, it sends a syslog record to Exabeam SIEM solution in real time using CEF/LEEF format. The Syslog integration is controlled by **syslog_outbound** parameter in PTA **systemparm.properties** file located in

Configure CyberArk PTA to send incidents to Exabeam:

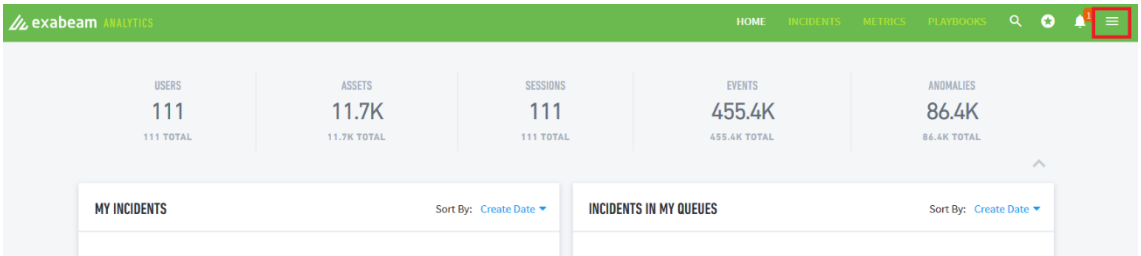
1. Log on to PTA as root
2. Open **/opt/tomcat/diamond-resources/local/systemparm.properties** add the following line

```
syslog_outbound=[{"host": "<ip of Exabeam server>", "port": 514, "format":
"CEF", "protocol": "UDP", "siem":"HP ArcSight"}]
```

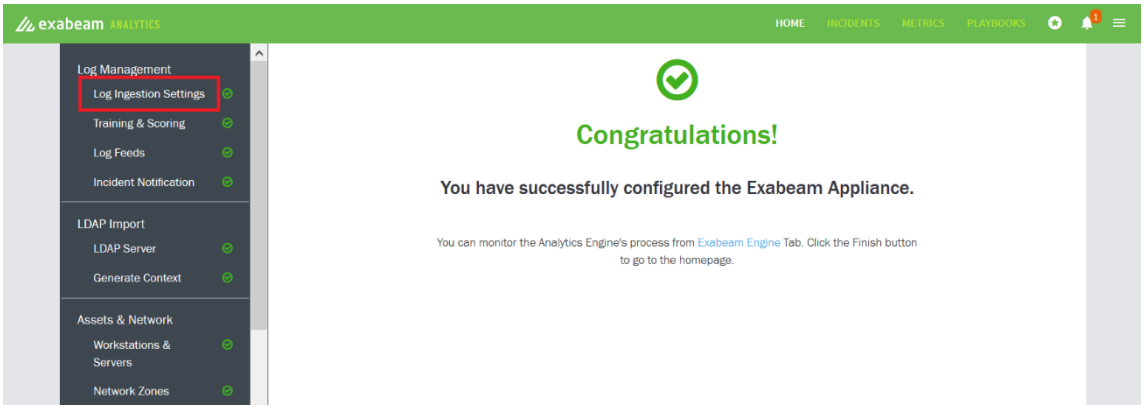
3. Save the configuration file and close it**.**
4. Restart PTA

Configure Exabeam to receive incidents from CyberArk PTA:

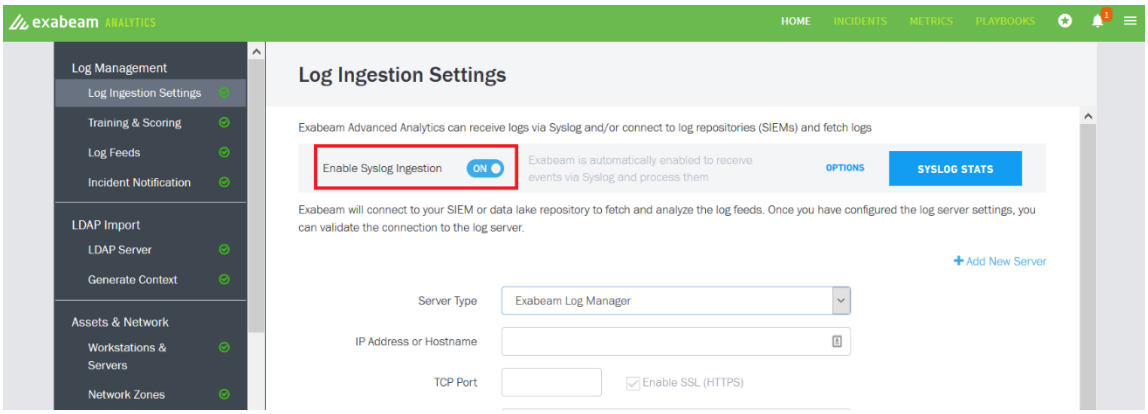
1. Log into Exabeam as Admin
2. Click on the  icon in the upper right-hand corner



3. Click on Log Ingestion Settings



4. Click on Enable Syslog Ingestion



CyberArk EPV - Exabeam Integration

CyberArk EPV can send audit logs to Exabeam through the Syslog protocol and create a complete audit picture of privileged account activities in the Exabeam solution.

These audit logs include privilege users, accounts, and safes activities, which are reported by the Vault to Exabeam.

Some of the benefits of the integration include:

- Multi-layer correlation between log data and alerts from PTA, allow clients to perform in depth analysis.
- Behavioral analysis identifying suspicious privileged user activity.
- Scores to particular threat – so that customers can decide which incident poses the biggest threat.
- PTA alerts to be included in dashboards and reporting.
- PTA alerts to be included in the general alerting and incident handling

Forward of Syslog is controlled by the following parameters in DBParm.ini. For complete instructions about configuring Syslog servers, **see Integrating with SIEM Applications** in the *Privileged Account Security Implementation Guide.*

Configure the CyberArk Vault to forward events to Exabeam:

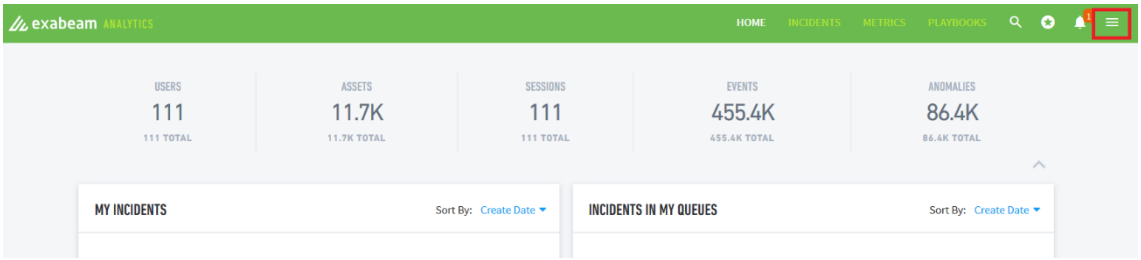
1. If there is a custom translator file, download it from the CyberArk Marketplace or it might be bundled in the Exabeam installation package. Copy it to the **Syslog** folder of the Vault installation folder. By default, the location is: **C:\Program Files (x86)\PrivateArk\Server\Syslog.** Otherwise a standard translator is provided in that folder. Make a copy of it and add it to the **SyslogTranslatorFile** parameter in the DBPARM.ini file (see step 2 for example).
2. In the same server installation folder,by default **C:\Program Files (x86)\PrivateArk\Server**, open dbparm.ini and add the following lines:

```
[SYSLOG]
SyslogServerIP=<ip of Exabeam server>
SyslogServerProtocol=UDP
SyslogServerPort=<Port used to send syslog to Exabeam>
SyslogMessageCodeFilter=295,308,7,24,31,428,361,372,373,359,436,412,411,300,302
,294,427,57,416,385,386,471,472
SyslogTranslatorFile=Syslog\Exabeam.xsl
UseLegacySyslogFormat=no
```

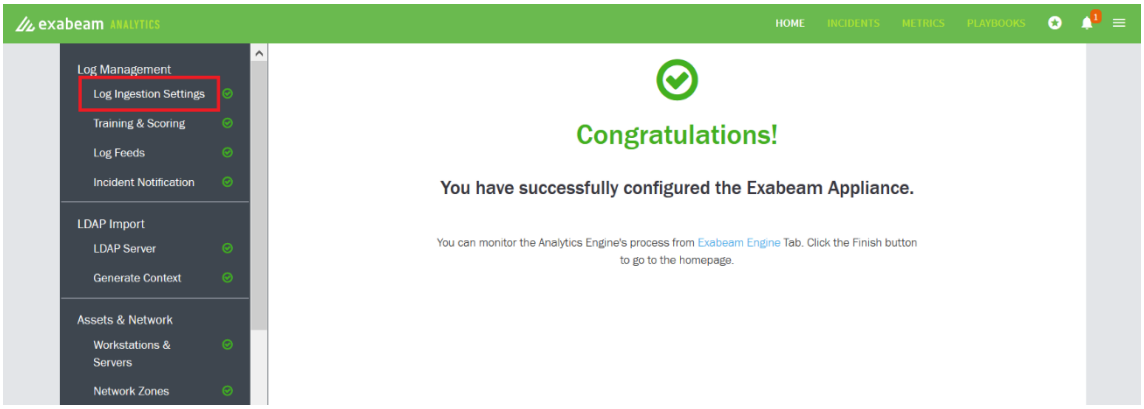
3. Save the file and close it.
4. Restart the Vault start the PrivateArk Server Service

Configure Exabeam to receive CyberArk Vault events:

1. Log into Exabeam as Admin
2. Click on the  icon in the upper right-hand corner



3. Click on Log Ingestion Settings



4. Click on Enable Syslog Ingestion