

RSA NetWitness Platform

Event Source Log Configuration Guide



Palo Alto Prisma Cloud

Last Modified: Monday, April 5, 2021

Event Source Product Information:

Vendor: Palo Alto

Event Source: Prisma Cloud

Versions: 21.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: prismacloud_audit

Collection Method: syslog

Event Source Class.Subclass: Cloud

Introduction

Prisma™ Cloud is a cloud native security platform that enables cloud security posture management (CSPM) and cloud workload protection platform (CWPP) for comprehensive visibility and threat detection across your organization's hybrid, multi-cloud infrastructure.

Prisma Cloud taps into the cloud providers' APIs for read-only access to your network traffic, user activity, and configuration of systems and services. It correlates these disparate data sets to help the cloud compliance and security analytics teams prioritize risks and quickly respond to issues. It also uses an agent-based approach to secure your host, container, and serverless computing environments against vulnerabilities, malware, and compliance violations.

Prisma Cloud software consists of two components: Console and Defender.

- **Console**- Console is Prisma Cloud's management interface. It lets you define policy and monitor your environment.
- **Defender**- Defender protects your environment according to the policies set in Console. There are a number of Defender types, each designed to protect a specific resource type.

Prisma Cloud can be configured to send audit events to syslog and/or stdout. Both Console and Defender emit messages. Console syslog messages are tagged as Twistlock-Console and Defender syslog messages are tagged as Twistlock-Defender in the logs.

Note: RSA Netwitness supports Console and Defender audit events collected from Prisma Cloud.

Forward Palo Alto Prisma Cloud logs

- I. Configure Syslog Settings for Palo Alto Prisma Cloud
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Settings for Palo Alto Prisma Cloud

Follow the below steps to configure Syslog Settings for Palo Alto Prisma Cloud:

1. Log into **Console**.
2. Go to **Manage > Alerts > Logging**.
3. Set **Syslog** to **Enabled**.
4. In '**Send syslog messages over the network to**', click '**Edit**', and then specify a destination. Enter the IP address or hostname of the RSA NetWitness Log Decoder or Remote Log Collector.

Additional Resources and Troubleshooting

For additional information refer

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/logging.html>

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma/prisma-cloud/prisma-cloud-admin-compute/prisma-cloud-admin-compute.pdf

Configure Syslog Event Sources on the NetWitness Platform

Perform the below steps on the RSA NetWitness Platform to configure Syslog Event Source

- Enable the required parser
- Configure Syslog Collection

Enable the required parser

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Enable the parser for your event source



1. In the NetWitness menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the Config Value field for your event source is selected.

Note: The required parser is `prismacloud_audit`.

Configuring Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness. You must configure the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the NetWitness menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu. The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**. The Available Event Source Types dialog is displayed.

5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar. The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary. Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without any further configuration in Netwitness.

© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.