Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform

Software Version: 2.11

Release Notes

June 20, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

About ArcSight Data Platform 2.11

ArcSight Data Platform (ADP) 2.11 delivers open security architecture that seamlessly connects to third-party platforms, including Hadoop. ADP transforms the data collection process, and simplifies administrative tasks, making organizations more effective in their monitoring capabilities.

ADP 2.11 components include:

- **Event Broker 2.01:** Event Broker centralizes event processing and opens up ArcSight data to a variety of data consumers.
- **ArcMC 2.6:** ArcSight Management Center provides one centralized view for end-to-end monitoring and simplified processing of bulk operations.
- **Logger 6.4:** Logger is a log management solution that is optimized for high event throughput, efficient long-term storage, and rapid data analysis.
- **SmartConnector Release 7.6.0:** More than 350 pre-built connectors help customers easily extend their data collection sources without manual customization.
- **SmartConnector Load Balancer 1.2:** SmartConnector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of SmartConnectors.

ArcMC 2.6

ArcSight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective way. ArcMC offers these key capabilities:

- **Management and Monitoring:** deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Loggers, Connectors, Connector Appliances, and other ArcMCs.
- **SmartConnector Hosting:** for the hardware appliance, as a platform to host and execute SmartConnectors.

ArcMC 2.6 Features and Enhancements

The following features and enhancements were introduced in ArcMC 2.6 and are included in this release. For more information about the ArcMC 2.6 features and functionality, refer to the ArcMC 2.6 Release Notes, Administrator's Guide, and other ArcMC documentation, available from the ArcSight Product Documentation Community.

This version of ArcMC includes the following new features and enhancements:

- **Event Broker Management:** ArcSight Event Broker management includes route and topic creation, as well as health and status parameter monitoring. Monitored parameters for Event Broker include CPU Usage, Memory, Disk Usage, Event Broker Throughput, Total EPS In, Event Parsing Error, Stream Processing EPS, and Stream Processing Lag.
- **Improved Node Management Interface:** The Node Management interface has been improved for clarity and ease of use.
- **Improvements to Topology View:** The Topology View now includes many improvements, including time-out settings, to age out inactive devices and remove them from management.
- **Improved Import Hosts Process:** Importing hosts from a CSV will take less time than formerly, as jobs run in parallel.
- **Improved License Consumption Report:** The License Consumption report can now be run for a specified time interval, instead of an entire year.
- **New Rules:** Several additional monitoring rules have been enabled by default. These can be edited or deleted as preferred.

Logger 6.4

Logger is a log management solution that is optimized for high event throughput, efficient long-term storage, and rapid data analysis. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events. Logger compresses raw data, but can always retrieve unmodified data on demand for forensics-quality litigation data.

Logger 6.4 Features and Enhancements

The following features and enhancements were introduced in Logger 6.4 and are included in this release. For information about Logger 6.4 features and functionality, refer to the Release Notes, Administrator's Guide, and other Logger 6.4 documentation, available from the ArcSight Product Documentation Community.

Search Improvements

Improved Search capabilities and updated search interface enable users to do the following:

- Search for IPv6 data.
- Index the requestURL field.
- Run multiple searches in the same browser session.
- View and access searches from the Active Search list on the Search main page.
- Administrators can set the number of concurrent searches and the search expiry time value.

Reporting Improvements

The integration of new features provides a greatly improved reporting experience, including the following improvements:

- Open up to ten Report tabs, so you can move easily from screen to screen as you create, manage, and generate concurrent reports.
- Create Smart reports that can support multiple queries, offer new chart types, and create Smart dashboards.
- Create Smart dashboards that display the results of multiple queries on one dashboard, as well as rich text, slide show, and web page widgets.
- Create new report chart types, including Sunburst, Funnel, Pyramid, Tree maps, Counter, Gauge, and Packed circles.

Other Updates

- Updated Event Broker receiver adds support for Event Broker 2.0, including TLS Client Authentication.
- Logger can now send and receive data in CEF v0.1, v1.0 and raw data formats. CEF 1.0 enables Logger to send and receive IPv6 data.
- Incorporated FIPS Bouncy Castle libraries provide improved security and enables support for TLS 1.2.
- Updated localization for supported languages (Japanese, Traditional Chinese and Simplified Chinese).

Event Broker 2.01

This release introduces HPE Security ArcSight Data Platform Event Broker (ADP Event Broker.) The ADP Event Broker centralizes event processing, helps you to scale your environment, and opens up events to third party solutions. It enables you to take advantage of scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data.

The ADP Event Broker provides a packaged version of Apache Kafka. After you install and configure an Event Broker Kafka broker or cluster of brokers, you can use ADP SmartConnectors to publish data, and subscribe to that data with ADP Logger, ArcSight ESM, ArcSight Investigate, Apache Hadoop, or your own consumer.

Event Broker 2.01 Features and Enhancements

The following features and enhancements are included in this release. For more information about the Event Broker 2.01 features and functionality, refer to the Event Broker 2.01 Release Notes, Administrator's Guide, and other ArcMC documentation, available from the ArcSight Product Documentation Community.

This version of Event Broker includes the following new features and enhancements:

- **New Data Format Support:** In addition to ArcSight Logger, new consumer types can now be configured to operate with Event Broker and process new data formats, including:
  - ArcSight Investigate 1.0 (via Vertica): Avro format
  - ArcSight ESM 6.11.0: Binary format
  - Third-party products, such as Hadoop
  - Customer-created applications that can read CEF.
- **ArcMC Management:** Event Broker can now be managed and monitored by ArcSight Management Center (ArcMC). ArcSight Event Broker management includes route and topic creation, as well as health and status parameter monitoring. Monitored parameters for Event Broker include CPU Usage, Memory, Disk Usage, Event Broker Throughput, Total EPS In, Event Parsing Error, Stream Processing EPS, and Stream Processing Lag.
- **Kafka Upgrade:** Event Broker 2.01 uses an upgraded version of Kafka (0.10.1.1)

SmartConnector Release 7.6.0

ArcSight SmartConnectors collect raw events from security devices, process them into ArcSight security events, and transport them to destination devices, such as ArcSight ESM and ArcSight Logger. Connectors are the interface between the chosen destination and the network devices that generate destination related relevant data on your network.

Each SmartConnector release provides new version support, enhancements, and fixed issues for individual SmartConnectors. The SmartConnector release supported with this ADP release is 7.6.0.8009.

For more information in this release, including resolved issues, refer to the SmartConnector Release Notes for 7.5.0.8009, available from the ArcSight Product Documentation Community.

SmartConnector Load Balancer 1.2

SmartConnector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of SmartConnectors. Currently it supports two types of event sources and SmartConnectors. One distributes the syslog input stream to syslog connectors using TCP or UDP protocol, and the other downloads files from a remote server and distributes them to the file-based connectors.

No updates were made to Load Balancer for this ADP release.

What's New in SmartConnector LoadBalancer 1.2

- Prepended remote IP address or hostname on incoming syslog messages.
- Expressions that can be used to more accurately determine the load on SmartConnectors globally or per destination.

For More Information

For detailed information about ADP component product features and functionality, including technical requirements, fixed, and open issues, refer to the product documentation, available from the ArcSight Product Documentation Community.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (ArcSight Data Platform 2.11)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!