Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform

Software Version: 2.20

Release Notes

October 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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

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 2.20

ArcSight Data Platform (ADP) 2.20 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 2.20 components include:

- **ArcMC 2.70:**ArcSight Management Center provides one centralized view for end-to-end monitoring and simplified processing of bulk operations.
- **Event Broker 2.10:** Event Broker centralizes event processing and opens up ArcSight data to a variety of data consumers.
- **Logger 6.50:** Logger is a log management solution that is optimized for high event throughput, efficient long-term storage, and rapid data analysis.
- **Smart Connectors 7.7.0:** More than 350 pre-built connectors help customers easily extend their data collection sources without manual customization.
- **Load Balancer 1.2:**SmartConnector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of SmartConnectors.

ArcMC 2.70

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 2.70 Features and Enhancements

This version of ArcMC includes the following features and enhancements:

- **Instant Connector Deployment:** Deploy connectors and Collectors directly in the Deployment View where needed with just a few clicks, using the new Deployment Templates feature.
- **Deployment View:** The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations. Use the deployment view to model subsystems, and quickly trace issues and drill down on details.
- **Connectors in Event Broker (CEB):** ArcMC now includes the alpha Connectors in Event Broker (CEB) feature, **for non-production public alpha testing and evaluation**, which collects raw data through a source topic in Event Broker. Raw events are sent to this source topic from a Collector device. CEBs enable event normalization and processing to be moved directly to Event Broker. For restrictions on the alpha feature, see "CEB and Collectors: For Testing and Evaluation Only" below.
- **ArcSight Secure Data Add-On Integration:** Deploy the ArcSight Secure Data Add-On encryption client to connectors and Collectors as part of Instant Connector Deployment. Events will be displayed in encrypted format in Logger and the ESM console.

For information about ArcMC 2.70 features and functionality, refer to the Release Notes, Administrator's Guide, and other ArcMC 2.70 documentation, available from the ArcSight Product Documentation Community.

CEB and Collectors: For Testing and Evaluation Only

Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features.** These features are provided for your testing and evaluation only and should not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future.

Consult the ArcMC Admin Guide, and directions from the ArcMC product team, for best practices and guidance on how to use these features.

CEB and Collectors must not in any circumstances be used in a production environment.

We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ArcMC product team at adp-ceb-alpha@hpe.com.

Logger 6.50

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 6.50 Features and Enhancements

ArcSight Logger 6.50 introduces the following new features and enhancements.

Documentation

Logger Cheat sheets are now available for quick reference.

Licensing

ADP Logger has an option to disable ArcMC license management. Both, ADP Logger license and the capacity can be applied in Logger.

Reporting Enhancements

The new features bring more advantages to the reporting tool, including:

- Logger filters and saved searches can be used to create reports.
- Charts rendered on reports can be saved as images (SVG, PNG & JPEG).
- Reports can be embedded in emails.

Security Enhancements

The upgrade from SHA-1 to SHA-2 algorithm strengthens the communication between:

- Connectors and receivers.
- Event Broker and receivers.
- Forwarders and ESM.
- Forwarders and connectors.
- Logger when managed by ArcMC back and forth.

TLS 1.2 protection improves communication privacy:

- Between peers.
- On board Connector forwarders in fips and non-fips mode.
- In Loggers peered with ESM in fips and non-fips mode.

Logger installer upgrade to JRE 1.8.0_141 fixes previous JRE known vulnerabilities

SHA-2 algorithm also improves datafiles integrity protection.

Storage Enhancements

Archived events created in Logger 6.5 are automatically indexed.

System Administration Enhancements

Scheduling Report Rights can be limited to one category of reports.

User Interface

Logger has now a feature in which users can switch between light and dark theme.

For information about Logger 6.50 features and functionality, refer to the Release Notes, Administrator's Guide, and other Logger 6.50 documentation, available from the ArcSight Product Documentation Community.

Event Broker 2.10

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 2.10 Features and Enhancements

Event Broker 2.1 includes the following new features and enhancements.

- **TLS 1.2:** Event Broker 2.1 only accepts the TLS 1.2 protocol. Note that any consumers or producers that connect to Kafka must use TLS 1.2. TLS v1 and v1.1 can be used for other communication.
- **Confluent Platform Upgrade:** Event Broker now uses Confluent Platform 3.3.0, which includes Kafka 0.11.0.0.
- **CEB (Evalulation Only):** Event Broker includes support for Connectors in Event Broker (CEB). This new functionality moves the security event normalization, categorization, and enrichment of connectors processing to the Docker containers environment of Event Broker, while reducing the work done by the system component left outside of Event Broker to collection of raw data (the new Collector). For more information, see "CEB and Collectors: For Testing and Evaluation Only" on page 5

For information about Event Broker 2.10 features and functionality, refer to the Release Notes, Administrator's Guide, and other Event Broker 2.20 documentation, available from the ArcSight Product Documentation Community.

SmartConnector Release 7.7.0

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 7.7.0.

For more information in this release, including resolved issues, refer to the SmartConnector Release Notes for 7.7.0, 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 2.20)

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!