HPE ArcSight ADP

Software Version: 2.0

Release Notes

September 27, 2016

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 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 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 (ADP) 3

Event Broker 1.0 4

ArcMC 2.5 4

What's New in ArcMC 2.5 4

Logger 6.3 5

What's New in Logger 6.3 5

SmartConnector Load Balancer 1.2 6

What's New in SmartConnector LoadBalancer 1.2 6

For More Information 6

Send Documentation Feedback 7

About ArcSight Data Platform (ADP)

ArcSight Data Platform (ADP) 2.0 delivers the industry's first open security architecture that seamlessly connects to third-party platforms, including Hadoop. ADP 2.0 components include:

- **Event Broker 1.0:** The new Kafka-based Event Broker allows for the consumption of up to 1 million events per second.
- **ArcMC 2.5:** ArcSight Management Center provides one centralized view for end-to-end monitoring and simplified processing of bulk operations.
- **Logger 6.3:** Logger 6.3 is a log management solution that is optimized for high event throughput, efficient long-term storage, and rapid data analysis.
- **SmartConnectors 7.3.0:** 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.

ArcSight Data Platform transforms the data collection process, and simplifies administrative tasks, making organizations more effective in their monitoring capabilities.

Event Broker 1.0

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 ArcSight environment, and opens up ArcSight 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, Apache Hadoop, or your own consumer.

ArcMC 2.5

ArcSight Management Center 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

What's New in ArcMC 2.5

Monitoring

- **Dashboard Improvements:** The monitoring dashboard has been enhanced with new color displays, dials, and graphs, showing vital metrics that let you review the health and topology of your network at a glance.

Connector Management

- **Bulk Framework and Parser Upgrades:** Perform connector framework and parser upgrades in bulk with a single click, in conjunction with an account on the ArcSight Marketplace.
- **Bulk Restart:** Restart all connectors in a container in bulk,with a single click.
- **Event Broker:** CEF Kafka connector destinations are now supported.

General

- **License Server and Tracking:** ArcMC can be enabled as an ADP license server for managed ADP Loggers and ADP Connectors, tracking usage and reporting on data ingestion.
- **ArcSight Marketplace Content Updates:** ArcMC relies on the ArcSight Marketplace to download and install connector parser updates. An ArcSight Marketplace administrative account is required.

Logger 6.3

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.

What's New in Logger 6.3

Search Improvements

- Enhanced peer search capabilities and support:
  - Up to 100 peers,
  - Up 100 concurrent peer searches,
  - Improved peer search performance.
- Search fields are now color coded for easy identification and index status.

A New Approach to Licenses

- Independent license support for ADP Loggers and standalone Loggers.
- Updated User Interface
- A new License Volume page for Loggers.
- Updated License Volume page for standalone Loggers
- Updated Trial Logger with trial license valid for 90 days

New and Enhanced Receivers

- New receiver enables support for Event Broker.
- For Appliances, an automatic firewall configuration script makes updating the firewall fast and easy.

Other New Features and Capabilities

- Capacity pooling support for s is now available to help redistribute and manage the total capacity of your environment.
- Users can now use HTTP Strict Transport Security Protocol (HSTS) to ensure that their browsers always connect to over HTTPS.
- Digital signature support for reports is now available on reports configured with this option.

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.

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 support community on Protect 724.

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 (ADP 2.0)

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!