Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform

Software Version: 2.0.1

Release Notes

November 28, 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 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 2.0.1

ArcSight Data Platform (ADP) 2.0.1 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 2.0.1 components include:

- **Event Broker 1.0:** The new Kafka-based Event Broker enables the consumption of up to 1 million events per second.
- **ArcMC 2.5.1:** ArcSight Management Center provides one centralized view for end-to-end monitoring and simplified processing of bulk operations.
- **Logger 6.3.1:** Logger is a log management solution that is optimized for high event throughput, efficient long-term storage, and rapid data analysis.
- **SmartConnector Release 7.3.0:** 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.

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 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 LoggerAr, Apache Hadoop, or your own consumer.

ArcMC 2.5.1

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.

What's New in ArcMC 2.5.1

The ArcSight Management Center (ArcMC) 2.5.1 release provides the same functionality as ArcMC 2.5, introduces fixes for a number of bugs, and includes the following security updates.

- New RHEL 6.8 and 7.2 Operating System upgrades address the Linux kernel vulnerability, CVE-2016-5195: Kernel Local Privilege Escalation "Dirty COW". For details, see https://access.redhat.com/security/cve/cve-2016-6304.
- The version of OpenSSL has been upgraded to 1.0.2j to address multiple vulnerabilities including CVE-2016-6304. For details, see https://www.openssl.org/news/secadv/20160926.txt.

Additionally, a new bulk license installer tool is included with your download. Use this tool if you need to update or install more than one license at a time from ArcMC. The tool and a readme that explains how to use it are included in the package bulk-license-installer.zip.

For more information about this release, including resolved issues, refer to the ArcSight Management Center 2.5.1 Release Notes, available from the ArcSight Product Documentation Community on Protect 724.

ArcMC 2.5 Features and Enhancements

The following features and enhancements were introduced in ArcMC 2.5 and are included in this release. For more information about the ArcMC 2.5 features and functionality, refer to the ArcMC 2.5 Release Notes, Administrator's Guide, and other ArcMC documentation, available from the ArcSight Product Documentation Community on Protect 724.

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 6.3.1

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 6.3.1

The HPE Security ArcSight Logger 6.3.1 release provides the same functionality as Logger 6.3, introduces fixes for a number of bugs, and includes the following security updates.

- Logger included a change that impacted the GB per day event ingestion and could trigger the 5-day license violation feature lockout erroneously. This release fixes that error.
- New RHEL 6.8 and 7.2 Operating System upgrades address the Linux kernel vulnerability, CVE-2016-5195: Kernel Local Privilege Escalation "Dirty COW." For details, see https://access.redhat.com/security/cve/cve-2016-6304.
- The version of OpenSSL has been upgraded to 1.0.2j to address multiple vulnerabilities including CVE-2016-6304. For details, see https://www.openssl.org/news/secadv/20160926.txt.

For more information about this release, including resolved issues, refer to the Logger6.3.1 Release Notes, available from the ArcSight Product Documentation Community on Protect 724.

Logger 6.3 Features and Enhancements

The following features and enhancements were introduced in Logger 6.3 and are included in this release. For information about Logger 6.3 features and functionality, refer to the Release Notes, Administrator's Guide, and other Logger 6.3 documentation, available from the ArcSight Product Documentation Community on Protect 724.

Search Improvements

- Enhanced Logger peer search capabilities and support:
  - Up to 100 peers,
  - Up 100 concurrent peer searches,
  - Improved peer search performance.

Refer to the Configuration chapter of the Logger Administrator's Guide for more information.

- Search fields are now color coded for easy identification and index status.

A New Approach to ArcSight Data Platform Licenses

- Independent license support for ArcSight Data Platform Loggers and standalone ArcSight Loggers.
- All new and upgraded Loggers include a trial license. After installing or upgrading to Logger 6.3, you must apply the production license to enable full access.

Updated User Interface

- A new License Volume page for ArcSight Data Platform Loggers.
- Updated License Volume page for standalone ArcSight Loggers.
- Improved usability and updated look and feel.

New and Enhanced ArcSight Data Platform Receivers

- New Event Broker receiver enables support for ArcSight Data Platform Logger.
- For Logger Appliances, an automatic firewall configuration script makes updating the firewall fast and easy. See Firewall Rules for more information.

Updated Trial Logger

- Trial license valid for 90 days.
- Storage Capacity 90 GB.
- Daily Data Ingestion 5 GB per day.
- A fresh installation is no longer required when you want a full Logger; just apply the new license.
- Only Reporting features are disabled.

Other New Features and Capabilities

- Capacity pooling support for ArcSight Data Platform Loggers 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 Logger over HTTPS.
- Digital signature support for Logger reports is now available on reports configured with this option.

SmartConnector Release 7.3.0

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 7.3.0.7886.

For more information in this release, including resolved issues, refer to the SmartConnector Release Notes for 7.3.0.7886, available from the ArcSight Product Documentation Community on Protect 724.

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 Product Documentation 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 (ArcSight Data Platform 2.0.1)

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!