Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

Cloud CEF Implementation Standard

Technical Note

May 16, 2016

Technical Note: Cloud CEF Implementation Standard

May 16, 2016

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 Package Enterprise Development LP shall not be liable for technical or editorial 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. Hewlett Package Enterprise Development LP 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 Development LP 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.

Follow this link to see a complete statement of Hewlett Package Enterprise Development LP copyrights, trademarks and acknowledgements: http://www.hpenterprisesecurity.com/copyright.

Revision History

Date	Description
05/16/2016	Added information regarding the ArcSight CEF Implementation Standard.
02//02/2016	Generally available.
08/14/2016	Initial release of this specification

Contents

Overview

ArcSight Common Event Format (CEF) Standard

The **Common Event Format (CEF) Standard**, developed by ArcSight, lets vendors and their customers quickly integrate their product information into ESM. CEF is an open log management standard that simplifies log management, letting third parties create their own device schemas that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, for later analysis by an enterprise management system.

The *ArcSight Common Event Format (CEF) Guide*, also known as "Implementing ArcSight Common Event Format (CEF)" defines the CEF protocol and provides details about how to implement the standard. It details the header and predefined extensions used within the standard as well as how to create user defined extensions. It also includes a list of CEF mappings as well as supported date formats.

To access this standard, go to https://www.protect724.hpe.com/docs/DOC-1072

ArcSight Cloud CEF Implementation Standard

The **ArcSight Cloud CEF Implementation Standard** specifies the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

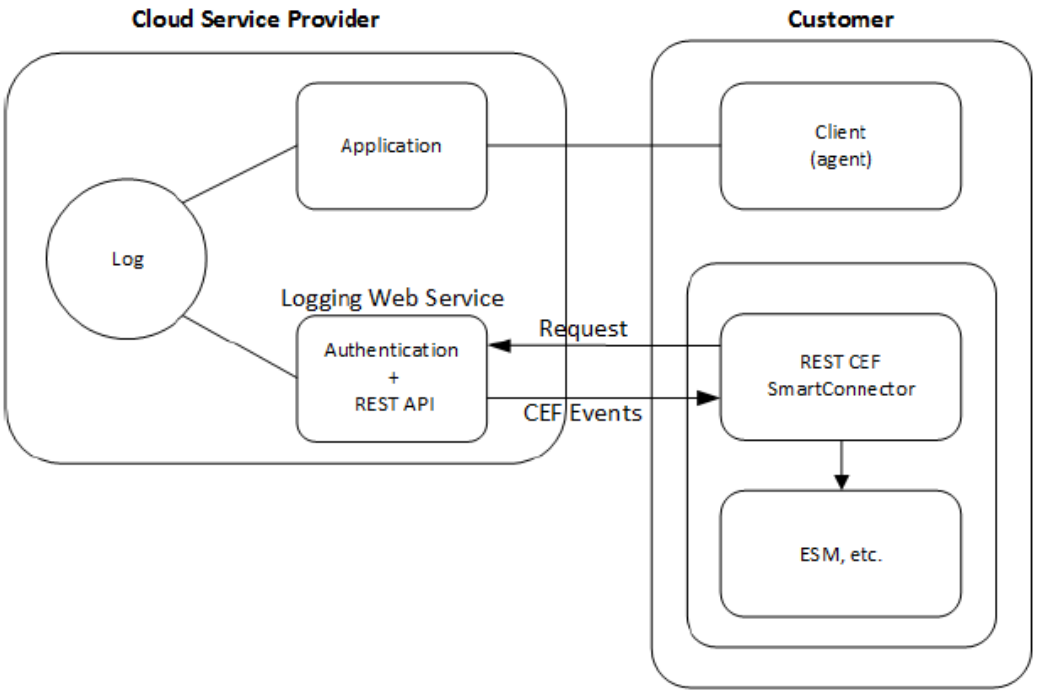
ArcSight SmartConnector technology addresses the core challenge of log collection by providing an effective and highly scalable infrastructure to simplify and optimize the aggregation and normalization of logs across thousands of devices and hundreds of locations.

Historically, ArcSight connectors were designed to run within an enterprise IT environment using a syslog-based standard, with all devices contained on the customer premises. Increasingly, enterprises around the world are adopting cloud-based services that have different characteristics and requirements than on premise devices and applications.

The ArcSight Cloud CEF Implementation Standard addresses these challenges by specifying the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

ArcSight CEF for the Cloud

The SmartConnector for ArcSight Common Event Format REST (or REST CEF SmartConnector) is the device that customers of ArcSight and the cloud-based service provider will use to retrieve events. This is based on the following model:



Cloud service provider customers (“Client” in the diagram) interact with applications typically using a web browser or other user interface. The cloud-based application creates log entries as a by-product of these interactions. The particular log entries are application dependent.

The cloud service provider must provide a logging web service component. The logging web service retrieves the log entries and includes a REST API, support for authentication, and ArcSight Cloud CEF as the event format.

As an open log management standard, Cloud CEF improves the interoperability of security-related information by reducing various message syntaxes to one matching the ArcSight schema. This API must use ArcSight Cloud CEF as the event format.

There are three main elements to the Cloud CEF solution:

1. The REST CEF SmartConnector retrieves events through a REST API exposed by the cloud service provider.
2. Events are retrieved in ArcSight CEF format and transported over HTTPS (which may require an access token).
3. Once the connector retrieves the events from the cloud service provider, it sends the information to ArcSight products, such as ArcSight Enterprise Security Manager (ESM).

Challenges to Cloud Event Collection

Enabling log event collection between a cloud service provider and a customer running ArcSight security products differs significantly from traditional log collection processes. These differences include:

- Network architecture– The architecture of cloud technologies differs from the network architecture on which traditional ArcSight devices operate.
- Event generation– Security events generated by devices in the cloud differ from events generated by traditional security devices in content, format, and transport mechanism.

- Security – Log collection for cloud-based services involves securely importing events from outside to inside the customer's environment.
- Scalability – Each cloud application changes rapidly and the volume continues to grow, making it challenging to keep current with traditional log collection processes.

To address the challenges these differences pose, ArcSight has developed standards for:

- Event retrieval from cloud vendors that can be re-used across many different types of cloud service providers.
- Use of standard HTTPS for security and support of strong authentication and access control.
- The overall transport format for a retrieved batch of events using JSON.
- Common format for event content called ArcSight Common Event Format (CEF).

Supported Industry Standards

The Cloud CEF Implementation Standard supports the following industry standards:

- REST Web Service APIs
- OAuth 2.0 or Basic authentication
- JSON event transport format
- ArcSight Common Event Format

The ArcSight Cloud CEF Implementation Standard provides the development toolkit to integrate with the cloud service providers using these standards.

SmartConnector for ArcSight Common Event Format REST

The SmartConnector for ArcSight Common Event Format REST (REST CEF SmartConnector) is the connector installed to retrieve CEF events from cloud service providers. The configuration guide for this connector is available on the ArcSight Protect 724 website at the following link https://www.protect724.hpe.com/docs/DOC-12848 .

This connector lets customers configure an authentication method and the REST API URLs for event retrieval. The connector is typically located on customer premises (although it can be run on the service provider platform), where it attempts to retrieve the latest events as reported by the cloud service provider REST APIs.

To make sure these conditions are met, the Cloud CEF Implementation Standard mandates that the cloud service provider adhere to the following conditions for authentication and event retrieval, by implementing an authentication mechanism and event retrieval APIs as described in the following sections.

Authentication

Authentication is generally required to gain access to the cloud server containing the event data. Each cloud service provider defines the authentication method used for its servers. The REST CEF SmartConnector provides flexible authentication support. Initially the two authentication methods supported are OAuth 2.0 and Basic authentication. The REST CEF SmartConnector user chooses the authentication method at connector installation time based on the capabilities of the cloud service provider.

OAuth 2.0 Authentication

The OAuth 2.0 standard is defined by IETF RFC 649. With OAuth 2.0, a third party application (in this case, the REST CEF SmartConnector) can be allowed access to server resources without disclosing the credentials of the resource owner.

To achieve this, the cloud service provider implementation of OAuth 2.0 must support:

- Callback URLs for the local host, so that the connector can access the authentication code and complete the OAuth authentication.
- HTTPS for local host URLs

  For example, `https://localhost:8080/oauth2callback` is an example of a supported callback URL, known as a `redirect_uri` in the OAuth 2.0 specification.
- Provisions for maintaining a valid refresh token without human intervention. If refresh tokens are used, there must be a mechanism for automatically extending the refresh token expiration date.

  For example, if the refresh token is initially valid for 14 days and is used to acquire a new access token, the expiration date is extended for 14more days.

Basic Authentication

The other option is Basic authentication, where the client provides an identifier (a username) and a shared secret (a password). Basic authentication is defined by RFC 2617. This authentication method uses TLS protocol, in which both the identifier and shared secret are encrypted. A client certificate may also be required by the vendor to verify the client's identity.

Event Retrieval APIs

The REST CEF SmartConnector retrieves events using REST API calls over secure transport (HTTPS). It expects CEF events in JSON format.

The API endpoint URL is comprised of several elements:

- The base URL
- The CEF events endpoint
- One or more event query arguments

Each of these elements are described in the following sections.

Base URL

The API endpoint base URL is specific to the cloud service provider, and includes the host name and path designation.

The base URL can be static or dynamic, although static URLs are recommended. If Dynamic URLs are used, the vendor must provide the means to get the dynamic portion of the URLs.

- Static URLs, such as **`https://api.abc.com/1.0/auditEvents`**, are the same for any user.
- Dynamic URLs, such as **`https://<SomeUserSpecificValue>.api.abc.com/1.0/auditEvents`**, include a value (**`<SomeUserSpecificValue>`** in this example) derived from the authenticated user using OAuth.

CEF Events Endpoint

The CEF events component of the path denotes a service that conforms to the REST CEF SmartConnector standard.

For example, a base URL of `https://www.acmeapis.com/admin/reports` contains the hostname `www.acmeapis.com`, and the path specification `/admin/reports`.

When combined with the `cef-events` endpoint, the event retrieval URL becomes:

`https://www.acmeapis.com/admin/reports/cef-events`

Event Query Arguments

The following query parameters are defined:

- `startTime=<timestamp>`

  where **`<timestamp>`** follows the form **`yyyy-MM-dd'T'HH:mm:ss.SSSZ`**.

  Example: `2012-05-15T00:01:02.345-08:00`

  The timestamp components after **`yyyy-MM-dd'T'HH:mm:ss`** are optional. The time zone designator is **`Z`** or **`+hh:mm`** or **`-hh:mm`**. If the **`startTime`** is not specified, events are retrieved beginning with the earliest available event.

- `maxResults=<number>`

  where **`<number>`** is an integer. This specifies that nomore than **`<number>`** events should be returned in the response. If **`maxResults`** is not specified, the number of events produced is determined by the cloud service provider.

- `eventType=<event type list>`

  The **`<event type list>`** is a comma-separated list of the event types to retrieve. The individual event type names are specific to the cloud service provider. If **`eventType`** is not specified, events of all types are retrieved.

The REST CEF SmartConnector periodically requests new events from the server. The polling period has a default value of 30 seconds, which is user-configurable. If a request to the server for events produces some events, the connector immediately makes another request using the continuation capability. This process continues until a request for events produces no events, after which the connector reverts to the configured polling period.

Retrieved Response Format

The server returns the response in an HTML document. The content type is **`application/JSON`**, as defined by RFC 4627.Containedwithin the document is a collection of CEF-formatted event data. The document content is formatted as follows:

```
{
"format" : "cef",
"version" : "1.0",
"timestamp" : <timestamp in standard format>,"count" : <number>,
"events" :[
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]",
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]",
.
```

```
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]"
],
"links" : [
{
"rel": "next",
"href": URL
}
]
```

"version" defines the ArcSight REST CEF SmartConnector version number (which may change as new versions are defined)

"timestamp" defines the date and time at which this collection of events was produced. The time stamp is in standard format, with Greenwich Mean Time (GMT) as the default time zone.

"count" defines the number of CEF events returned in the response. If **maxResults** was specified in the request, **"count"** should not exceed this value.

"events" defines an array of CEF events. Each CEF event is a string whose content conforms to ArcSight's CEF event format.

"links" defines an array of links. The "links" array contains a single element with "href" property indicating the URL used to retrieve next set of events. The "links" array is never empty and should always contain URL to retrieve the next set of events.

Continuation

When the connector starts up, it makes a first request to the server using the Events URL provided in the setup configuration to get the first set of events, and uses the URL contained in the "links" array of the response for each subsequent request.

Whenever the server has more events than can be contained in a single response, the connector immediately makes additional requests to retrieve more events using the URL from links array contained in the response. If there are no events in the response, the connector waits for the configured polling period to retrieve more events using the URL from the links array contained in the response.

CEF Mappings

The ArcSight Common Event Format is defined in *Implementing ArcSight Common Event Format (CEF)*, posted on the ArcSight Protect 724 website as *ArcSight Common Event Format (CEF) Guide* at https://www.protect724.hpe.com/docs/DOC-1072. Cloud service providers should use this document to map native event fields to the appropriate CEF key value.

Summary

If a cloud service provider supports OAuth 2.0 or Basic authentication, and exposes REST APIs for event retrieval in ArcSight CEF (over JSON) format, ArcSight and cloud service providers customers can monitor their applications on the service provider's cloud platform.

Send Documentation Feedback

If you have comments about this document, you can contact the documentationteam by email. If an email client is configured on this system, click the link above and an email window opens with the subject already filled in. 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 webmail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!

Support

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