Hewlett Packard
Enterprise

HPE ArcSight Logger Brute Force Attack Detection

Software Version: 1.0

Security Use Case Guide

January 20, 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:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

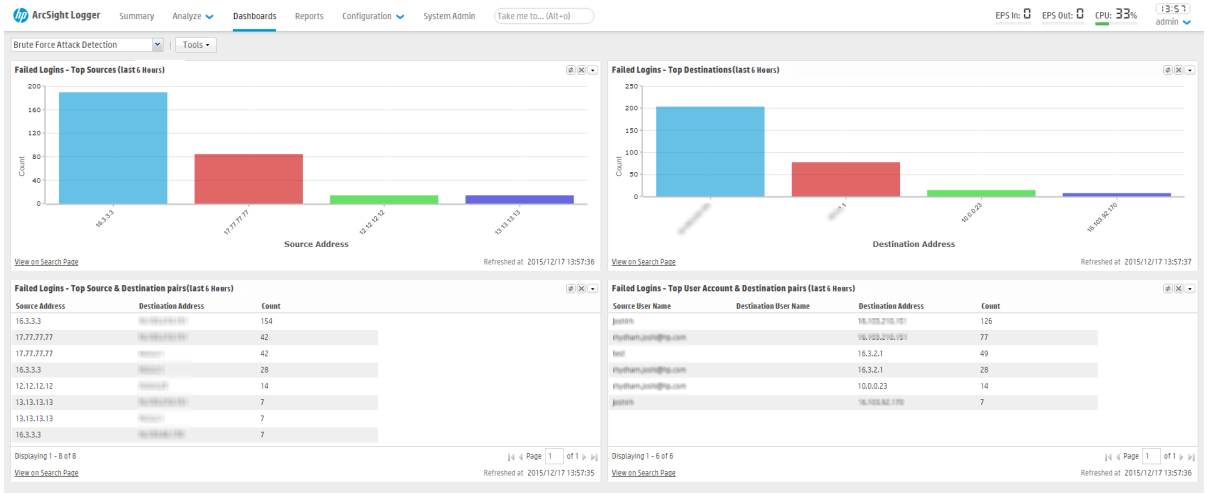
Phone	A list of phone numbers is available on the HPE ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Overview

Brute force attacks apply trial-and-error methods to hack into a system and obtain encrypted information such as passwords and personal identification numbers (PINs). A brute force program generates a massive number of automated consecutive login attempts.

The HPE ArcSight Logger Brute Force Attack Detection Security Use Case helps you identify potential brute force attempts using HPE ArcSight Logger. After identification of a threat, you can take action to investigate the activity and protect your assets.



Parameters

The Brute Force Attack Detection Security Use Case tracks the following parameters related to brute force attack detection.

- **Count:** The number of login attempts made during a given interval. A count includes both successful and unsuccessful logins. A high count may indicate a possible brute force attack.
- **Source:** The system from which a possible brute force attack originated.
- **Destination:** The target system subject to a possible brute force attack.
- **User Account:** User account associated with the possible brute force attack, used by the source to log in to the destination.

These parameters are tracked in two ways: through dashboards and reports.

Dashboards

The Brute Force Attack Detection *dashboards* display a count of failed logins for each of the following for the past 6 hours:

- Top sources of failed logins
- Top destinations of failed logins
- Top source destination pairs
- Top user account and destination pairs

For more information, see "Brute Force Attack Detection Dashboards" on page 7.

Reports

As part of the Logger Brute Force Attack Detection Security Use Case, these reports are available in Logger. Reports enable you to track failed login trends over any period and are highly customizable to meet your needs. The included reports track information on counts, sources, and trends. For more information, see "Brute Force Attack Detection Reports" on page 9.

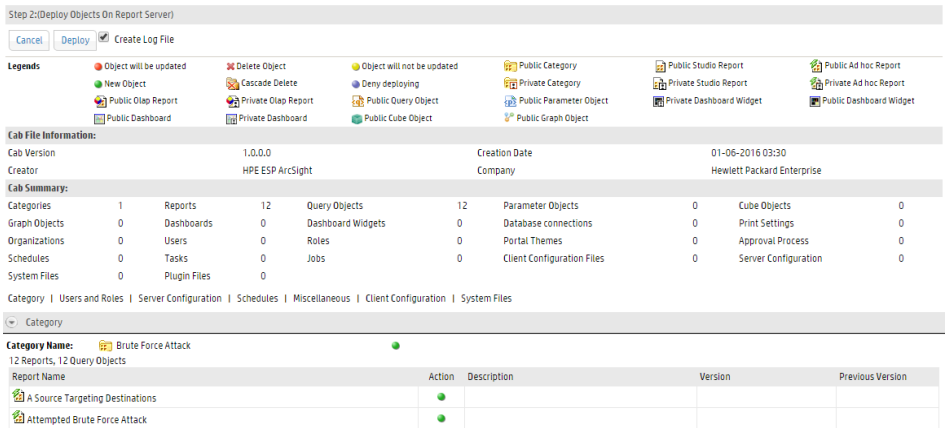
Installation

Installation of the Logger Brute Force Detection Security Use Case is accomplished with the installer file downloaded from the HPE ArcSight Marketplace. You must separately install the use case content (the fieldset, dashboard, and filters).

The Logger Brute Force Detection Security Use Case is supported on Logger v6.0 and later versions.

To install the Logger Brute Force Detection Security Use Case package:

1. In Logger, on the main menu, click **Reports**.
2. Click **Deploy Report Bundle.**
3. Under **Step 1: Upload and View Cab Information**, browse to the `*.cab` file containing the Logger Brute Force package, then click **Upload**.
4. Under **Step 2: Deploy Objects on Report Server**, review the objects that will be deployed to your report server. Then click **Deploy**. The objects are added to your server.

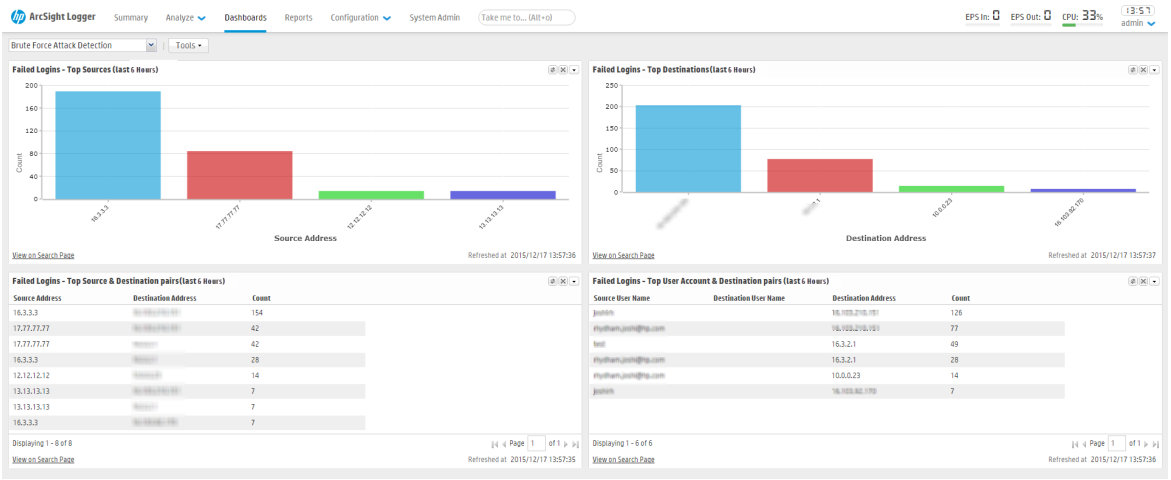


To install the Logger Brute Force Detection Security Use Case content:

1. In Logger, on the main menu, click **Configuration**.
2. Under **Advanced**, click **Import Content.**
3. Click **Choose File.** Select the *.gz file containing the fieldset content. Click **Import**.
4. Repeat Step 3 for the file containing the dashboard content.
5. Repeat Step 3 for the file containing the filter content.

Brute Force Attack Detection Dashboards

Four dashboards are available as part of the Logger Brute Force Attack Security Use Case. Dashboards give a snapshot of current activity for the defined interval (by default, the interval is 6 hours).



To view the Brute Force Attack Detection dashboard:

1. In the Logger main menu, click **Dashboards**.
2. In the dashboard drop-down list, select *Brute Force Attack Detection*.
3. The dashboard displays with four panels displaying data on failed logins:

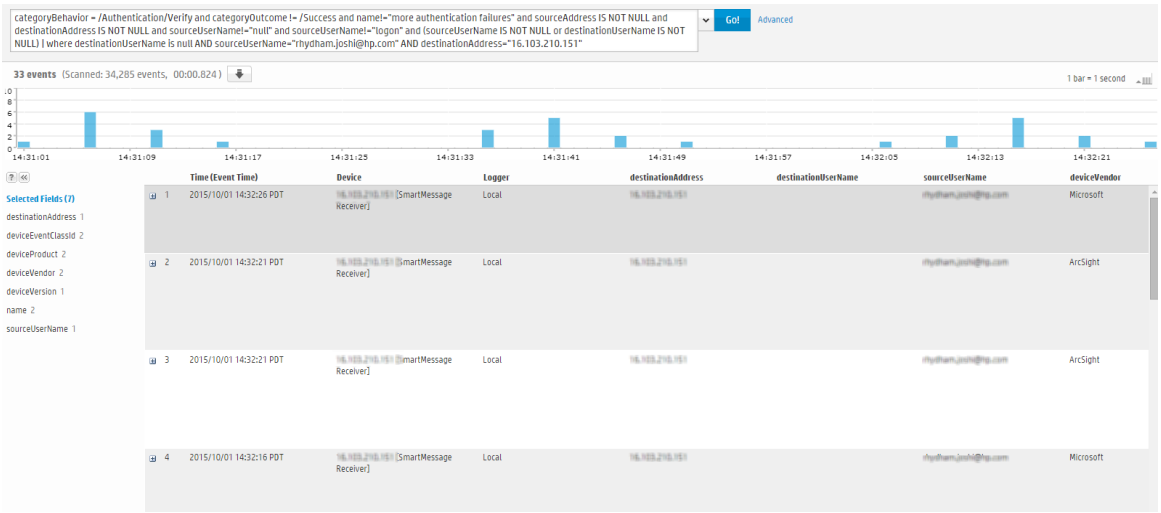
- **Failed Logins - Top Sources:** displays a bar graph of the 10 sources with the highest count of login attempts for the last 6 hours.
- **Failed Logins - Top Destinations:** displays a bar graph of the 10 destinations with the highest count of login attempts for the last 6 hours.
- **Failed Logins - Top Source & Destination Pairs:** displays a table of the 10 source-destination pairs with the highest count of login attempts from the last 6 hours.
- **Failed Logins - Top User Account and Destination Pairs:** displays a table of the 10 user account-destination pairs with the highest count of login attempts from the last 6 hours.

Hover your pointer over any colored portion of a graph to display the overall details, including the count of login attempts.

Click **View on Search Page** to display the panel in its own page, including the Saved Search details.

Drilling Down

To drill down on the data in a dashboard graph and review details of the data displayed, click the colored portion of any graph. While the graphs displays the 10 items with the highest count, the drill-down page shows the 100 items with the highest count.



At the top of the page is a graph with local time as the x-axis, showing groups of events across time as bars. Click any bar shown on the graph to view the details of all events that took place at the indicated time.

The Saved Search used to filter data for the dashboard is displayed at the top of the page. The filter can be used as-is, or may be customized by the filter tools. For details on how to modify a filter, consult the Logger Administrator's Guide.

To export the dashboard data, click **Export**. Then, on the **Export Options** page, select the details of the export.

Modifying the Default Dashboard Settings

You can modify the default dashboard settings by editing the panel display or by editing the Saved Search used to compile the dashboard. For more information on modifying a dashboard layout, panels, or a Saved Search, see the *Logger Administrator's Guide*.

Brute Force Attack Detection Reports

By running and reviewing the reports included in the Brute Force Attack Detection Security Use Case, you can easily determine trends over time and that could be brute force attacks.

Before running a report, verify that the report's period (start and end date) is for the desired time frame. Period can be retained from previously run reports.

To access a Brute Force Attack Detection report:

1. On the Logger main menu, click **Reports**.
2. In the navigation menu, click **Report Explorer.**
3. Select **Brute Force Attack.**
4. Select a report to run.
5. Under **Actions**, select an action to take with the report, such as **Run with Default Options.**

You can run reports, customize, copy or take other actions with any of these reports as you would with other Logger reports. For detailed instructions on how to run, edit, and manage Logger reports, see the *Logger Administrator's Guide*.

Brute Force Attack Reports

Brute force attacks show possible brute force attacks by source, user account, and destination. You should run these reports as often as possible (preferably daily) to spot possible brute force attacks early. Alternatively, you can schedule these reports to run automatically in Logger under **Scheduled Reports** in the navigation menu.

Report	Description
Attempted Brute Force Attack	Shows source, user account, and destination involved in an attempted brute force attack. An attempted brute force attack is defined as one where the number of failed login attempts exceeds the report query's threshold (by default, 50 failed attempts per day).
Successful Brute Force Attack	Shows source, user account, and destination involved in an attempted brute force attack, which resulted in one or more successful logins.

Source Reports

Source reports display information on the sources of possible brute force attacks.

Report	Description
A Source Targeting Destinations	Shows a list, sorted by count, of the top 100 sources targeting multiple destinations with failed logins. You can customize the report to isolate one or more sources or destinations.
Exploit Attempts of User Accounts by Sources	Shows a list, sorted by count, of the top 100 user accounts that failed to log in to any destination. You can customize the report to isolate one or more user accounts, sources, or destinations.

Failed Login Counts Reports

Failed login counts reports show the trends of the count of failed logins, grouped by different parameters. Using failed login counts reports will let you spot possible trends and other issues.

Report	Description
Failed Login Counts by Days	Groups failed login events by day of occurrence.
Failed Login Counts by Destinations	Groups the top 100 (by count) destinations for failed login events.
Failed Login Counts by Sources	Groups the top 100 (by count) sources for failed login events.
Failed Login Counts by User Accounts	Groups the top 100 (by count)user accounts for failed login events.
Failed Login Counts by Weeks	Groups failed login events by the week in which they occurred.

Failed Login Statistics Reports

Failed login statistics reports show the statistics of all failed logins, each by different parameters.

Report	Description
Failed Login Statistics by a Destination	Shows statistics of all failed login events associated with a destination.
Failed Login Statistics by a Source	Shows statistics of all failed login events associated with a source.
Failed Login Statistics by a User Account	Shows statistics of all failed login events associated with a user account.

Additional Information

The dashboard and reports included in the Brute Force Security Use Case make use of the following queries, filters, and fieldset.

Queries

The Logger Brute Force Detection Attack Security Use Case includes queries for each report discussed under "Brute Force Attack Detection Reports" on page 9 You can view or edit the query details as needed.

To view or edit query details:

1. In the main menu, click **Reports**.
2. In the left navigation menu, click **Query Explorer.**
3. Select **Brute Force Attack** in the first column.
4. In the second column, double-click the query you wish to view or edit.

For complete details on editing or managing queries, see the Logger Administrator's Guide.

Filters

These filters are part of the Logger Brute Force Detection Attack Security Use Case.

- Brute Force Attack - Failed Login Events
- Brute Force Attack - Successful Login Events

To view or edit filter details:

1. On the main menu, click **Configuration**.
2. Under **Search**, click **Filters**.
3. The Brute Force filters are displayed in the list. Click any filter to display its details.

For complete details on editing or managing filters, see the Logger Administrator's Guide.

Fieldset

A single fieldset is part of the Security Use Case.

- Brute Force Attack Detection

To view or edit fieldset details:

1. On the main menu, click **Configuration**.
2. Under **Search**, click **Fieldsets**.
3. The Brute Force fieldset is displayed in the list, with details.

For complete details on editing or managing fieldsets, see the Logger Administrator's Guide.

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 Security Use Case Guide (Logger Brute Force Attack Detection 1.0)

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!