Hewlett Packard
Enterprise

HPE Security ArcSight ESM: Antivirus Monitoring

Software Version: 1.0

Security Use Case Guide

April 3, 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

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

Chapter 1: Overview

Monitoring antivirus activity is a network security information-gathering activity that scans for virus activities in your enterprise. Computer viruses are malicious programs that, when installed in assets such as servers, desktops, and laptops, can damage files and applications. Computer viruses can also spread across systems, therefore increasing the scope of damage.

To protect critical assets, enterprises would invest in antivirus protection packages covering installations of antivirus programs (called agents) in their assets. These agents are being managed by antivirus servers. The antivirus server hosts also contain antivirus agents for their own protection. In that scenario, there would be regular communications between the servers and agents to ensure that the agents are up and running to monitor and resolve virus attacks at all times.

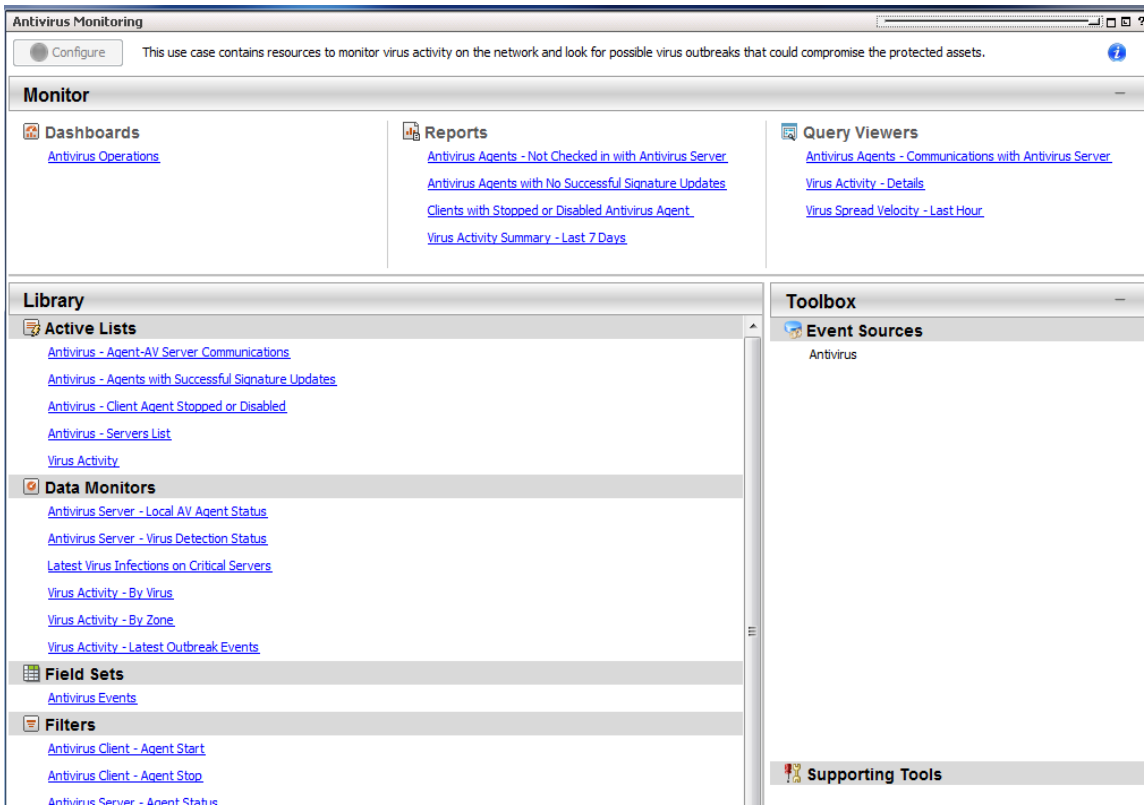
Antivirus servers not only send regular signature updates to the agents, but also take proper action if viruses are detected. Antivirus servers:

- Quarantine the virus (move the virus to a separate location so that the it cannot cause harm); or
- Delete the virus so that it no longer exists in the file system.

The Antivirus Monitoring Security Use Case monitors such activities and displays them on data monitors and a query viewer, which you access from the dashboard. The information collected by the use case helps you investigate, then take actions on virus outbreaks, infected critical assets, and antivirus agents that are stopped.

The Antivirus Monitoring Security Use Case provides rules that can create cases and send notifications if certain conditions are met. By default, the rule actions are disabled but you can customize and then enable as required.

The Antivirus Monitoring use case contains the following resources, partially shown:



- A **dashboard** (Antivirus Operations) is your starting point to monitor antivirus activities. The dashboard provides access to the data monitors that show latest virus infections on critical servers, the latest virus outbreak events, the velocity at which viruses have spread in the last hour, viruses detected by the antivirus server but not deleted, and antivirus agent status. See "Getting Started with the Antivirus Operations Dashboard" on page 11 for details.
- **Reports** show various historical events on antivirus-related activities. See "Running Reports" on page 31 for details.
- **Query viewers** show data queried from active lists that are, in turn, populated by triggered rules. See "Monitoring Query Viewers" on page 23 for details.
- **Rules**. The following rules are designed to perform actions, for example, create cases, send notifications, or both. These actions are disabled by default, and you can enable them as required:
  - Antivirus Servers - AV Client Agent Stopped
  - Critical Asset - Virus Infected
  - Virus Outbreak - by Virus
  - Virus Outbreak - by Zone

  See "Refining the Antivirus Monitoring Use Case Rules" on page 33 for details.

Access the Antivirus Monitoring use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard, reports, and query viewers used to monitor and investigate antivirus activities.

The Library section of the use case lists all supporting resources that help collect information that goes on the dashboard, reports, and query viewers. Aside from the rules described in "Refining the Antivirus Monitoring Use Case Rules" on page 33, you are not expected to configure resources in the Library section of the use case.

This document describes how to install, configure, and use the Antivirus Monitoring use case and is designed for security professionals who have a basic understanding of ArcSight ESM and are familiar with the ArcSight Console. For detailed information about using ArcSight ESM, see the ArcSight ESM help system from the ArcSight Console **Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

Chapter 2: Installation

To install the Antivirus Monitoring use case, perform the following tasks in the following sequence:

1. Download the Antivirus Monitoring use case zip file into the ArcSight Console system where you plan to install the use case, then extract the zip file.

   The zip file includes the package, the accompanying Readme file, and the *Downloads_Groups_1.0.arb* package.
2. Log into the ArcSight Console as administrator.

   Note: During the package installation process, do not use the same administrator account to start another Console or Command Center session simultaneously. This login is locked until the package installation is completed.
3. Verify if you have a previous version of the use case package you want to install. If so, uninstall and delete this previous version:
   a. On the **Packages** tab of the Navigator panel, right-click the package and select **Uninstall Package**. The package icon is gray when it is uninstalled.
   b. Right-click the package and select **Delete Package**.
4. On the Packages tab, verify if **Downloads Groups** is already installed. If you see packages in `/All Packages/Downloads/Downloads Groups`, then ignore this step.

   If the Downloads Groups package is not present, import and install the *Downloads_Groups_1.0.arb* package. See "Importing and Installing a Package" on the next page for details.
5. Import and install the Antivirus Monitoring use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Antivirus Monitoring resources. See "Assigning User Permissions" on page 9 for details.

No configuration is required for the Antivirus Monitoring use case. However, before using the Antivirus Monitoring use case, make sure that you have populated your ESM network and asset models. A network model keeps track of the network nodes participating in the event traffic. Assets provide more granular attributes of the nodes, such as descriptions of critical servers. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

Importing and Installing a Package

Follow the steps below to import and install the package(s). This assumes you have downloaded the zip file and extracted the contents into the ArcSight Console system.

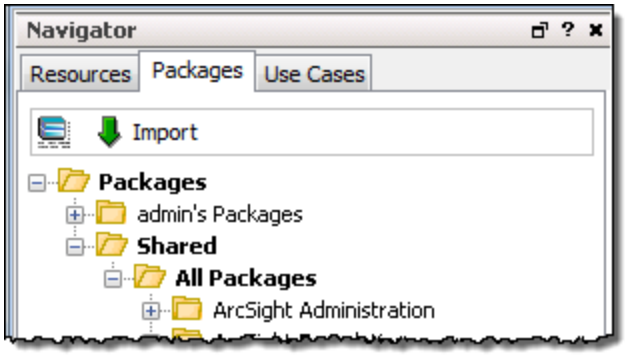
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the **Antivirus Monitoring** use case package.

  Note: The Downloads Groups package contains the groups used by the resources in the security use case; you must import and install this package first.

- If the Downloads Groups package is already installed, follow the steps to import and install the Antivirus Monitoring use case package only.

To import and install a package:

1. Log into the ArcSight Console as administrator. In the Navigator panel, click the **Packages** tab.



2. Click **Import**.
3. In the Open dialog, browse and select the package file (`*.arb`) you want to import, then click **Open**.
   The Importing Packages dialog shows how the package import is being verified for any resource conflicts.
4. In the Packages for Installation dialog, make sure that the check box is selected next to the name of the package you want to install and click **Next**.
   The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the summary report.
5. In the Installing Packages dialog, click **OK**. In the Importing Packages dialog, click **OK**.
6. On the **Packages** tab of the Navigator panel, expand the package group in `/All Packages/Downloads/` to verify that the package group is populated and that installation is successful.

Assigning User Permissions

By default, users in the `Administrators` and `Default User Groups/Analyzer Administrators` user groups can view and edit the resources. Users in the `Default User Groups` (and any custom user group under this group) can only view Antivirus Monitoring resources. Depending on how you set up user access controls within your organization, you might need to adjust those controls to make sure the resources are accessible to the right users.

Note: By default, the `Default User Groups/Analyzer Administrators` user group does not have edit permissions for archived reports in the Downloads group.

The following procedure assumes that you have logged into the ArcSight Console as administrator, and that you have set up the required user groups with the right users.

To assign user permissions:

1. In the Navigator panel, open the **Resources** tab.
2. For each of the resource types provided in the use case, navigate to `Downloads/Antivirus Monitoring`.
3. Right-click the `Antivirus Monitoring` group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
4. Select the user groups for which you want to grant permissions and click **OK**.

Required ESM Configurations

The Antivirus Monitoring use case itself does not require configurations, however, you need ESM configurations before you can be operational in your environment:

- **SmartConnectors:** Install the appropriate ArcSight SmartConnectors to receive relevant events from your antivirus servers. SmartConnector examples are SmartConnector for McAfee ePolicy Orchestrator DB and SmartConnector for Symantec Endpoint Protection DB.
  - Refer to the applicable SmartConnector guide for installation instructions.
  - Refer to the *ArcSight Console User's Guide* for instructions to register SmartConnectors in ESM.
- Manually categorize all internal assets (assets inside the company network), or the zones to which the assets belong, with the **Protected** asset category. This category is located in `/All Asset Categories/Site Asset Categories/Address Spaces/Protected`. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as Web servers) as **Protected**.

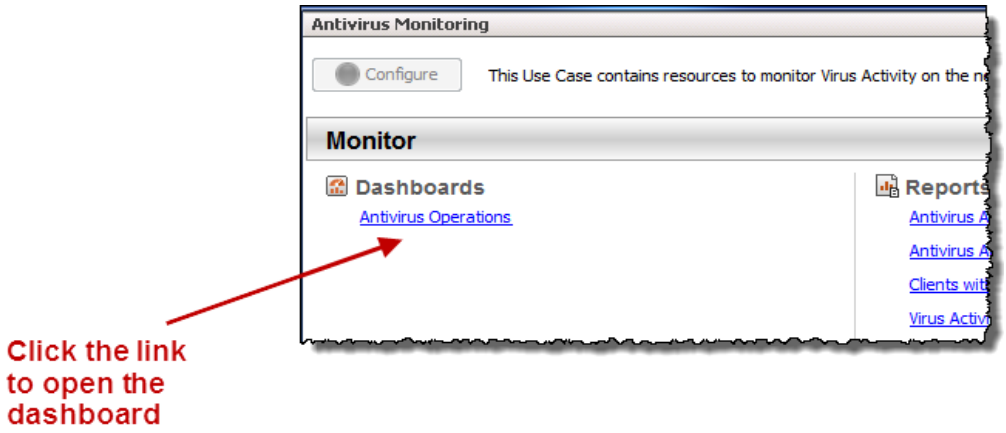
In addition, configure which protected assets belong to either `/All Asset Categories/System Asset Categories/Criticality/`**`Very High`** or `/All Asset Categories/System Asset Categories/Criticality/`**`High`**.

Refer to the topic, "Managing Asset Categories," in the *ArcSight Console User's Guide*.

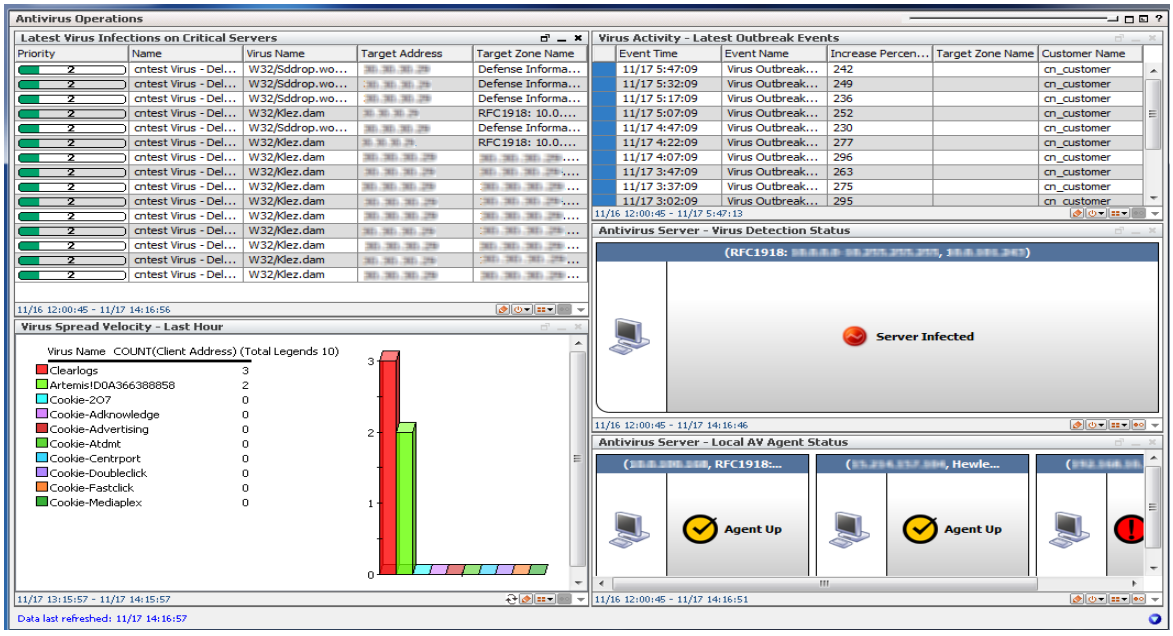
Chapter 3: Getting Started with the *Antivirus Operations* Dashboard

The Antivirus Monitoring use case provides the Antivirus Monitoring dashboard to help you detect antivirus activities. Use this dashboard as a starting point.

To open the dashboard, click the link to the dashboard in the Antivirus Monitoring use case.



The dashboard opens in the Viewer panel of the ArcSight Console. An example of the dashboard is shown below.



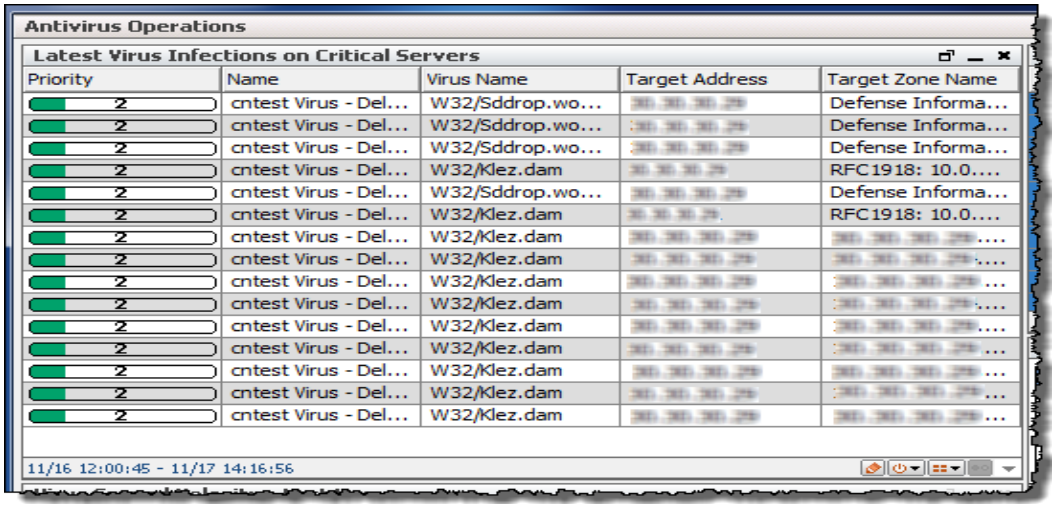
The Antivirus Operations dashboard includes the following elements, from top left, clockwise:

- **Latest Virus Infections on Critical Servers Data Monitor**, described in "Using the Latest Virus Infections on Critical Servers Data Monitor" below.
- **Virus Activity - Latest Outbreak Events Data Monitor**, described in "Using the Virus Activity - Latest Outbreak Events Data Monitor" on page 14.
- **Antivirus Server - Virus Detection Status Data Monitor**, described in "Using the Antivirus Server - Virus Detection Status Data Monitor" on page 15.
- **Antivirus Server - Local AV Agent Status Data Monitor**, described in "Using the Antivirus Server - Local AV Agent Status Data Monitor" on page 17.
- **Virus Spread Velocity - Last Hour Query Viewer**, described in "Using the Virus Spread Velocity - Last Hour Query Viewer" on page 19.

Using the *Latest Virus Infections on Critical Servers* Data Monitor

The *Latest Virus Infections on Critical Servers* data monitor displays the most recent 15 virus infections that affected assets categorized with High or Very High criticality. Any attempts to delete or quarantine the virus have failed. The data monitor is updated every 30 seconds, and older data is removed as new information comes in.

Use this data monitor to identify assets that require immediate attention. Following is an example of the data monitor:



To benefit from this data monitor, make sure you have defined your asset model and categorized your assets accordingly.

To view the *Latest Virus Infections on Critical Servers* data monitor:

- On the Antivirus Monitoring use case's Dashboards section, click the link to the dashboard, **Antivirus Operations**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboards/Downloads/Antivirus`
  b. Right-click **Antivirus Operations** and select **Show Dashboard**.

The *Latest Virus Infections on Critical Servers* data monitor is displayed on the top left of the dashboard.

To interpret the *Latest Virus Infections on Critical Servers* data monitor:

The data monitor displays the most recent data in a table format, showing event priority, event name, virus name, the infected host's address, and the infected host's ArcSight network zone. Use this data monitor to identify infected critical servers.

Further investigations on the *Latest Virus Infections on Critical Servers* data monitor:

Right-click a row and select **Show Event Details**. The Event Inspector panel on the right of the Console displays additional details beyond what the data monitor displays.

Right-click a row, select **Investigate**, and create a channel.

Refer to the following topics in the *ArcSight Console User's Guide* :

- The "Reference Guide" section for descriptions of the different categories displayed on the active channel
- The "Investigating Views" topic for various ways to use the right-click **Investigate** option

To fine tune the *Latest Virus Infections on Critical Servers* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor.

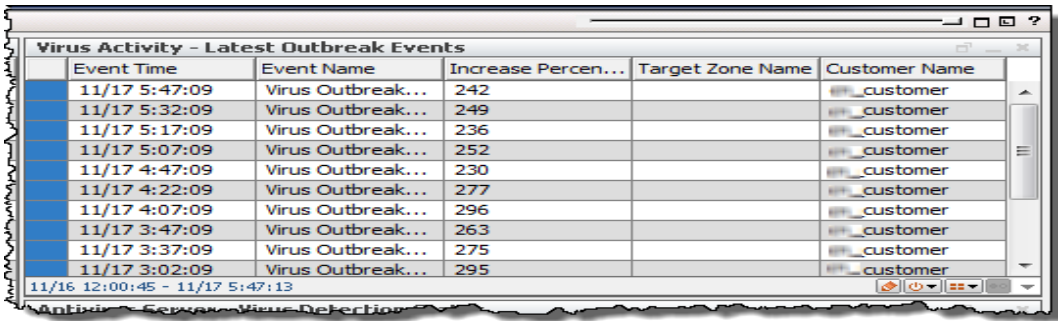
Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	**Availability Interval:** Default is 30 seconds in which the data monitor is updated. If the number of events has reached the limit of 15, then the oldest data is removed as new ones are added. You can increase or reduce this number. To edit the data monitor, click the pencil icon ( ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Last N Events Data Monitor."
Filter used by the data monitor	Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Antivirus/Critical Assets - Virus Infected`. **Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter. Refer to the *ArcSight Console User's Guide*'s topic on "Filtering Events" for details.

Using the *Virus Activity - Latest Outbreak Events* Data Monitor

The *Virus Activity - Latest Outbreak Events* data monitor shows the last 15 events on virus outbreaks and the percentage increase of such activity, by virus outbreak and by network zone. The outbreaks are detected by correlation data monitors. The*Virus Activity - Latest Outbreak Events* data monitor is updated every 30 seconds, replacing the oldest data as new events come in.

Following is a closeup of the data monitor.



To view the *Virus Activity - Latest Outbreak Events* data monitor:

- On the Antivirus Monitoring use case's Dashboards section, click the link to the dashboard, **Antivirus Operations**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboards/Downloads/Antivirus/Antivirus Operations`.
  b. Right-click **Antivirus Operations** and select **Show Dashboard**.

The *Virus Activity - Latest Outbreak Events* data monitor is displayed on the top right of the Antivirus Operations dashboard.

To interpret the *Virus Activity - Latest Outbreak Events* data monitor:

The data monitor displays the most recent data in a table format, showing event time, event name, percent increase of virus activity events, the target zone name where the outbreak is taking place, and the customer name. Implement any business policies to prevent spreading of viruses further.

Further investigations on the *Virus Activity - Latest Outbreak Events* data monitor:

Right-click a row and choose **Show Event Details**. The Event Inspector panel on the right of the Console displays additional details on the selected row beyond what the data monitor displays.

Right-click a row, choose **Investigate**, and create a channel for that specific event.

Refer to the following topics in the *ArcSight Console User's Guide* :

- The "Reference Guide" section for descriptions of the different categories displayed on the active channel
- The "Investigating Views" topic for various ways to use the right-click **Investigate** option

To fine tune the *Virus Activity - Latest Outbreak Events* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

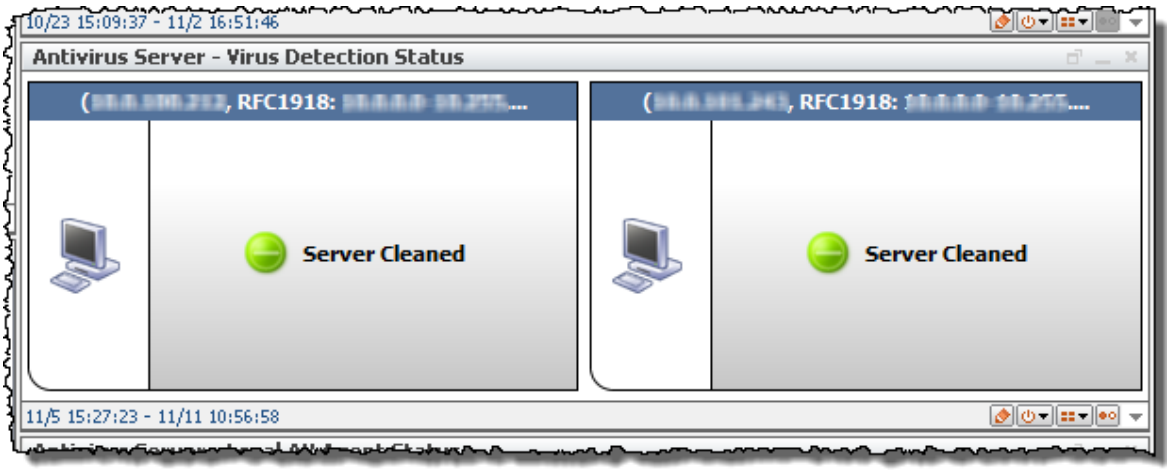
Data monitor	**Availability Interval:** Default is 30 seconds in which the data monitor is updated. If the number of events has reached the limit of 15, then the oldest data isremoved as new ones are added. You can increase or reduce this number. To edit the data monitor, click the pencil icon ( ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Last N Events Data Monitor."
Filter used by the data monitor	Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Antivirus/Virus Outbreak - Events`. **Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter. Refer to the *ArcSight Console User's Guide*'s topic on "Filtering Events" for details.

Using the *Antivirus Server - Virus Detection Status* Data Monitor

The antivirus server polls and updates antivirus agents that are installed in multiple clients.

The *Antivirus Server - Virus Detection Status* data monitor indicates the status of a virus found on the antivirus server, whether the virus has been deleted or not. The data monitor is refreshed every 30 seconds.

Following is a closeup of the data monitor.



Each reported server is presented in a tile that includes a green or red circle. A green circle represents the status, `Server Cleaned`, meaning the antivirus agent has deleted or quarantined the virus. A red circle represents the status, `Server Infected`. Regardless of a green or red circle, you should know that the server machine itself has been infected by a virus and it is still potentially vulnerable. Make sure to implement all the necessary measures to protect the server from virus attacks.

The data monitor does not display anything if no virus infection was found on the antivirus server.

To view the *Antivirus Server - Virus Detection Status* data monitor:

- On the Antivirus Monitoring use case's Dashboards section, click the link to the dashboard, **Antivirus Operations**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboards/Downloads/Antivirus/Antivirus Operations`.
  b. Right-click **Antivirus Operations** and select **Show Dashboard**.

The *Antivirus Server - Virus Detection Status* data monitor is displayed on the middle right of the Antivirus Operations dashboard.

Further investigations on the *Antivirus Server - Virus Detection Status* data monitor:

- Right-click a tile representing a server, choose **Investigate,** then choose a data field to open a channel on that field.

- Click the **View As** icon () on the lower right of the data monitor to change from Tile to Table view. The Table view shows more information than the simplified Tile view.

Refer to the subtopic, "Options for Table and Tile Views" in the discussion on the Last State Data Monitor in the *ArcSight Console User's Guide*.

To fine tune the *Antivirus Server - Virus Detection Status* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

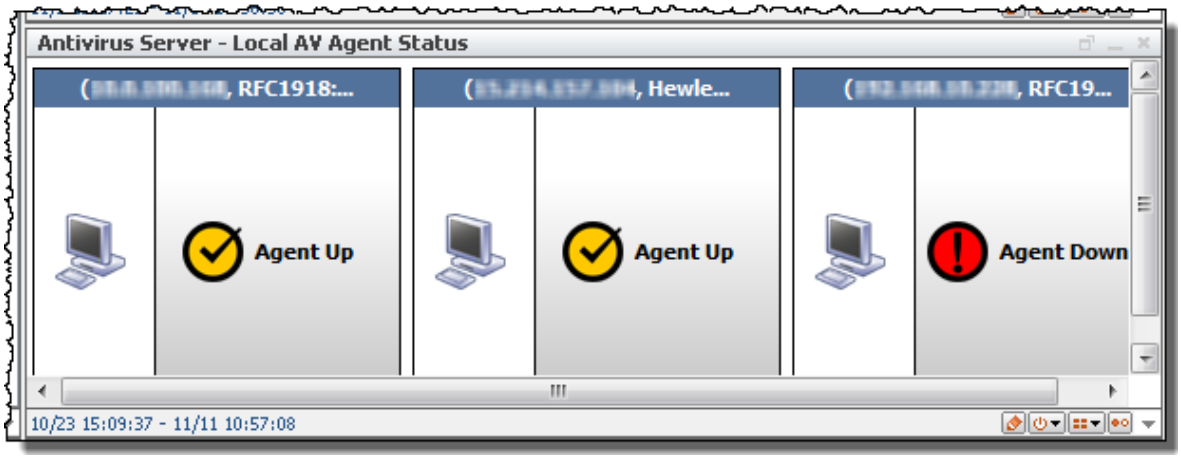
Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	**Availability Interval:** Default is 30 seconds in which the data monitor is updated. It displays a maximum number of indicators, set to 20. You can increase or reduce this number. To edit the data monitor, click the pencil icon () on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Last State Data Monitor."
Filter used by the data monitor	Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Antivirus/Antivirus Servers - Virus Infections`. **Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter. Refer to the *ArcSight Console User's Guide*'s topic on "Filtering Events" for details.

Using the *Antivirus Server - Local AV Agent Status* Data Monitor

The *Antivirus Server - Local AV Agent Status* data monitor indicates the status of the antivirus agent installed in the antivirus server itself. The status indicates whether the agent is running or not. The data monitor is refreshed every 30 seconds and the data is purged every 48 hours.

Following is a closeup of the data monitor.



Each reported agent in a server is presented in a tile that includes a yellow or red circle. A yellow circle with a check mark represents the status, `Agent UP`. The `Agent Up` status means the antivirus server has received the local antivirus agent's startup event.

A red circle with exclamation point represents the status, `Agent Down`. The `Agent Down` status means the antivirus server has received the local antivirus agent's stop event. Make sure to restart antivirus agents reported as `Agent Down`.

To view the *Antivirus Server - Local AV Agent Status* data monitor:

- On the Antivirus Monitoring use case's Dashboards section, click the link to the dashboard, **Antivirus Operations**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboards/Downloads/Antivirus/Antivirus Operations`.
  b. Right-click **Antivirus Operations** and select **Show Dashboard**.

The *Antivirus Server - Local AV Agent Status* data monitor is displayed on the bottom right of the Antivirus Operations dashboard.

Further investigations on the *Antivirus Server - Local AV Agent Status* data monitor:

- Right-click a tile representing an agent in an antivirus server, select **Investigate,** then choose a data field to open a channel on that agent.
- Click the **View As** icon ( ) on the lower right of the data monitor to change the view from Tile to Table. The Table view shows more information than the simplified Tile view.

Refer to the subtopic, "Options for Table and Tile Views" in the discussion on the Last State Data Monitor in the *ArcSight Console User's Guide*.

To fine tune the *Antivirus Server - Local AV Agent Status* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

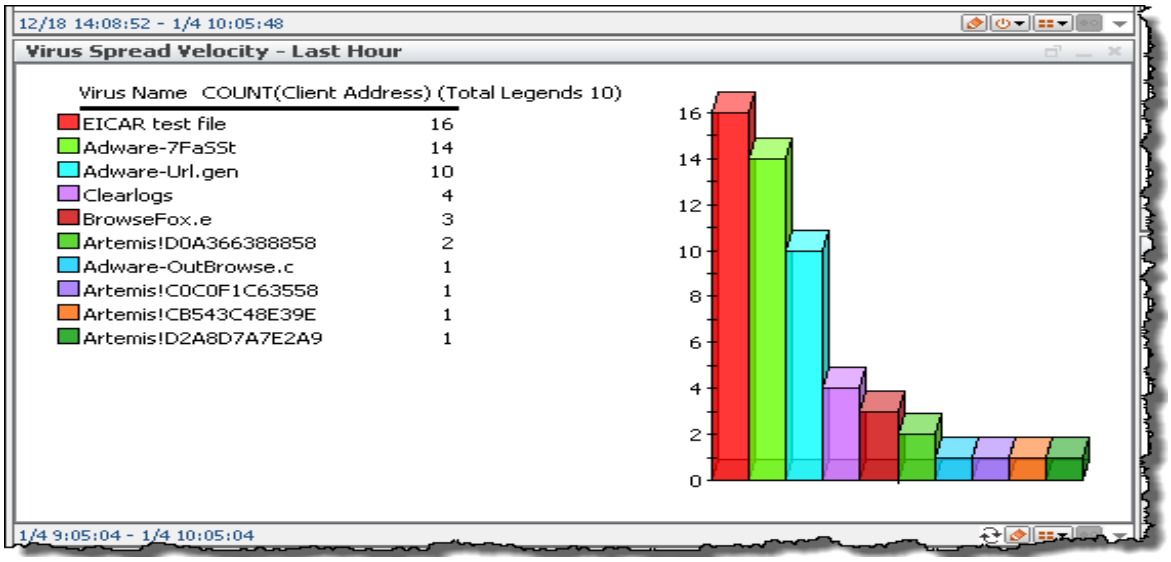
Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	**Availability Interval:** Default is 30 seconds in which the data monitor is updated. It displays a maximum number of indicators, set to 20. You can increase or reduce this number. To edit the data monitor, click the pencil icon () on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Last State Data Monitor."
Filter used by the data monitor	Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Antivirus/Antivirus Server - Agent Status`. **Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter. Refer to the *ArcSight Console User's Guide*'s topic on "Filtering Events" for details.

Using the *Virus Spread Velocity - Last Hour* Query Viewer

The *Virus Spread Velocity - Last Hour* query viewer displays the spread of virus infections across clients in the last hour. It shows how many clients have been infected by a specific virus, ordered by the number of infected clients. The most aggressively-spreading virus infections appear at the top. The data is refreshed every minute.

Following is a closeup of the query viewer:



The query viewer displayed on the dashboard does not include the header information. Header information is only available if you

To view the *Virus Spread Velocity - Last Hour* query viewer on the dashboard:

- On the Antivirus Monitoring use case's Dashboards section, click the link to the dashboard, **Antivirus Operations**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboards/Downloads/Antivirus`.
  b. Right-click **Antivirus Operations** and select **Show Dashboard**.

The *Virus Spread Velocity - last Hour* query viewer is displayed on the bottom left of the Antivirus Operations dashboard. Query viewers displayed on the dashboard do not include the standard query viewer header.

To access the *Virus Spread Velocity - Last Hour* query viewer directly:

On the Navigator > Resources panel:

1. Go to `/All Query Viewers/Downloads/Antivirus`.
2. Right-click **Virus Spread Velocity - Last Hour**, select **View Data As**, then select your preferred display format. Refer to the *ArcSight Console User's Guide*'s topic, "Running Queries and Viewing Results" for an explanation of display formats.

The query viewer results are displayed on the Viewer panel.

The query viewer header displays some attributes of the query viewer. For example, the top line shows the name of the query that contains the event fields defined for this query viewer.

Further investigations on the *Virus Spread - Last Hour* query viewer:

This query viewer has an associated drilldown, the *Virus Activity - Details* query viewer.

- Double-click a row to open the associated drilldown.

  Or

- Select **Drilldown > Virus Activity - Details**.

The drilldown displays results specific to the selected row, in this case, a specific virus.

Click the **Refresh** icon (⟳) below the query viewer to update the results.

To fine tune the *Virus Spread Velocity - Last Hour* query viewer:

ArcSight ESM provides queries to refine the data returned by the query viewer. The query viewer itself has default parameters.

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Query viewer	**Refresh Data After:** Default is one minute in which the query viewer runs its query to get new data. **Query Time Out:** Default is no time out, which actually defaults to 5 minutes. Enter a time in seconds or minutes if you want. To edit the query viewer, click the pencil icon () on the bottom toolbar of the query viewer. This opens the query viewer's Edit panel. Or, on the Navigator > Resources panel, go to `/All Query Viewers/Downloads/Antivirus/Virus Spread Velocity - Last Hour`. Right-click and select **Edit Query Viewer**. The data fields in the query viewer's Fields tab are inherited from its base query, described next. You can select or deselect the fields brought in by the query, so that the query viewer results includes only the fields you are interested in. Query viewer attributes are described in the *ArcSight Console User's Guide*'s topic on "Defining Query Viewer Settings."
Query used by the query viewer	Change the query to suit your business requirements. To edit the query: • On the query viewer results header, click the query name, or • On the Navigator > Resources panel, go to **Reports > Queries** tab. Then go to `/Queries/Downloads/Antivirus/Virus Spread Velocity - Last Hour`. Right-cick then select **Edit Query**. • If you are adding fields to the query, these added fields do not automatically show up as selected in the query viewer's Fields tab. In that case, edit the query viewer and select the new fields if you want to include their values in the query viewer results. **Caution:** Before modifying any query, verify if this query is being used by other resources. Changes to query settings such as fields may affect the expected results in all resources using that query. Refer to the *ArcSight Console User's Guide*'s topic on "Building Queries" for details.

Chapter 4: Monitoring Query Viewers

The Antivirus Monitoring use case provides query viewers to help you detect antivirus activities. The data displayed by these query viewers come from active lists that are populated by rules.

To display query viewer results from the Antivirus Monitoring use case, click one of the links under the Monitors section:

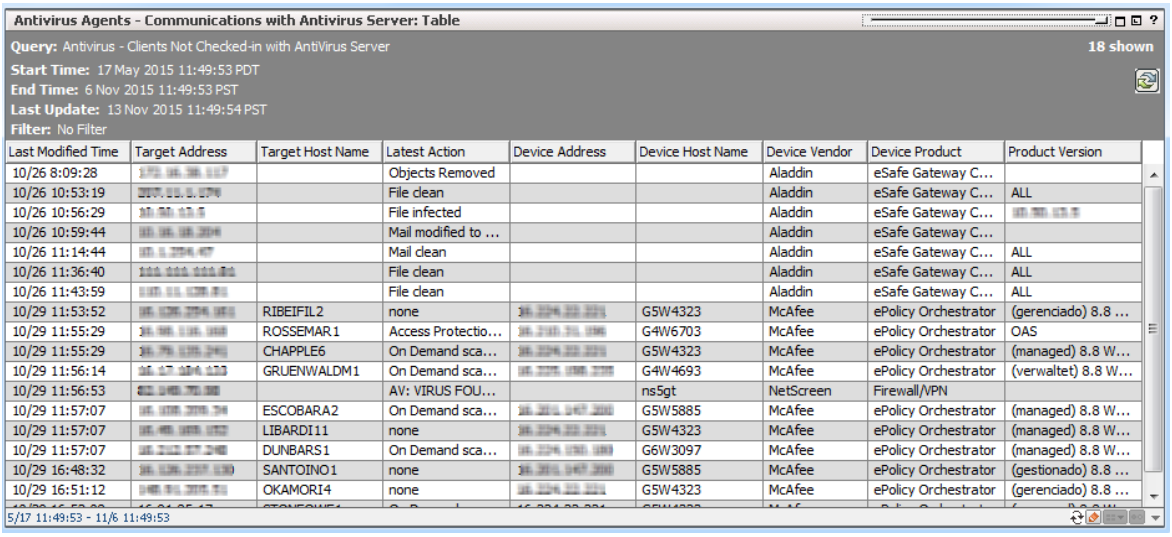
The query viewers listed on the use case are:

- Antivirus Agents - Communications with Antivirus Server
- Virus Activity - Details
- Virus Spread Velocity - Last Hour

Using the *Antivirus Agents - Communications with Antivirus Server* Query Viewer

Antivirus servers and antivirus agents are expected to communicate with each other regularly, so that the server knows which agents are running. The *Antivirus Agents - Communications with Antivirus Server* query viewer displays those agents that have not contacted the server for at least seven days (the default setting). The query viewer displays the results in a table format.

Following is a closeup of the query viewer results:



The query viewer header displays some attributes of the query viewer. For example, the top line shows the name of the query that contains the event fields defined for this query viewer.

To view the *Antivirus Agents - Communications with Antivirus Server* query viewer:

- On the Antivirus Monitoring use case, click the link to the query viewer, **Antivirus Agents - Communications with Antivirus Server**.

  or

- On the Navigator > Resources panel:
  a. Go to `/All Query Viewers/Downloads/Antivirus`.
  b. Right-click **Antivirus Agents - Communications with Antivirus Server** and select **View Data as > Table**.

The Console displays the query viewer results on the Viewer panel.

Note: If nothing is displayed by the query viewer, this means there has been communications between agents and server within the last 7-day period.

To interpret the *Antivirus Agents - Communications with Antivirus Server* query viewer:

The first column contains the last date when there was communication between the server and the agents, sorted by the oldest date at the top. Additionally, each row provides communication details.

You should manually check the agents identified on the query viewer and fix the problem as soon as possible.

To fine tune the *Antivirus Agents - Communications with Antivirus Server* query viewer:

ArcSight ESM provides queries to refine the data returned by the query viewer. The query viewer itself has default parameters.

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

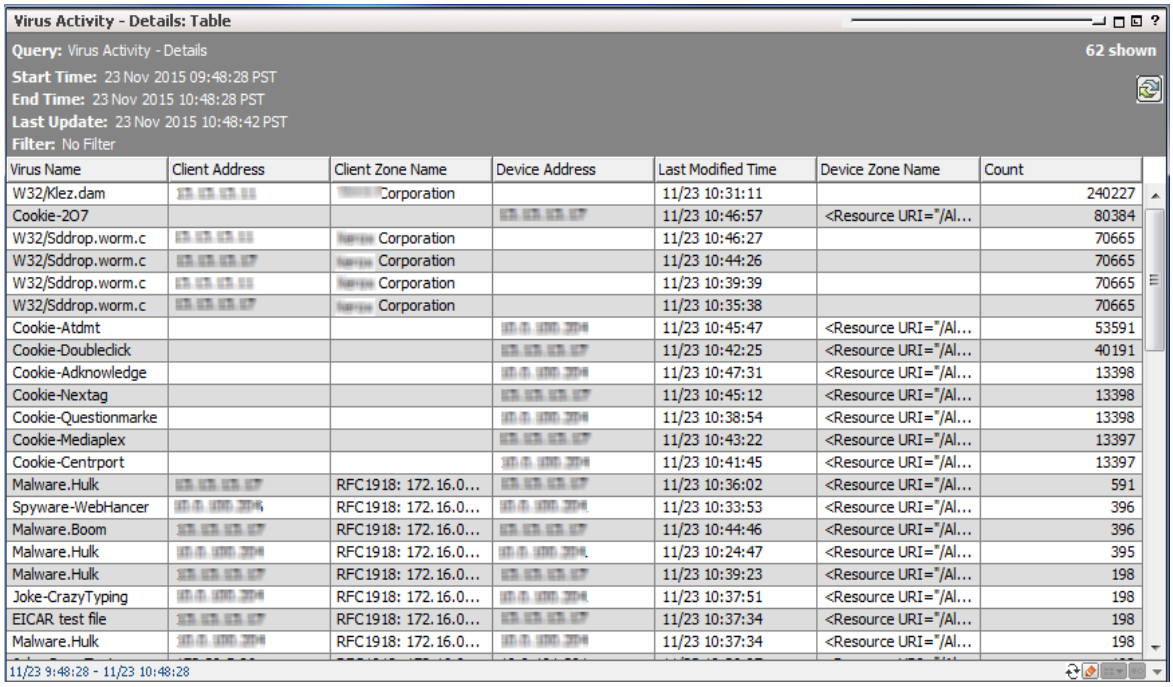
Query viewer	**Refresh Data After:** Default is 15 minutes in which the query viewer runs its query to get new data. **Query Time Out:** Default is no time out, which actually defaults to 5 minutes. Change the time in seconds or minutes if you want. To edit the query viewer, click the pencil icon ( ) on the bottom toolbar of the query viewer. This opens the query viewer's Edit panel. Or, on the Navigator > Resources panel, go to `/All Query Viewers/Downloads/Antivirus`. Right-click **Antivirus Agents - Communications with Antivirus Server** and select **Edit Query Viewer**. The data fields in the query viewer's Fields tab are inherited from its base query, described next. You can select or deselect the fields brought in by the query, so that the query viewer results includes only the fields you are interested in. Query viewer attributes are described in the *ArcSight Console User's Guide*'s topic on "Defining Query Viewer Settings."
Query used by the query viewer	Change the query to suit your business requirements. To edit the query: • On the query viewer results header, click the query name. • On the Navigator > Resources panel, go to **Reports > Queries** tab. Then go to `/All Queries/Downloads/Antivirus`. Right-cick **Antivirus - Clients Not Checked In with Antivirus Server** then select **Edit Query**. • If you are adding fields to the query, these added fields do not automatically show up as selected in the query viewer's Fields tab. In that case, edit the query viewer and select the new fields if you want to include their values in the query viewer results. **Caution:** Before modifying any query, verify if this query is being used by other resources. Changes to query settings such as fields may affect the expected results in all resources using that query. Refer to the *ArcSight Console User's Guide*'s topic on "Building Queries" for details.

Using the *Virus Activity - Details* Query Viewer

The *Virus Activity - Details* query viewer displays antivirus agents that have been infected with a specific virus. This query viewer is also used as a drilldown from the *Virus Spread Velocity - Last Hour* query viewer. See "Using the Virus Spread Velocity - Last Hour Query Viewer" on page 19 for related information.

For more information about drilldowns, refer to the topic, "Managing Drilldowns from a Query Viewer," in the *ArcSight Console User's Guide*.

Following is a closeup of the query viewer.



The query viewer header displays some attributes of the query viewer. For example, the top line shows the name of the query that contains the event fields defined for this query viewer.

The example shows details about all virus activities, including virus names, client address, zones where the clients are located, and so on. You can access the query viewer directly if you want to see activities in all viruses found; or you can drilldown from a specific virus for more focused information.

To view the *Virus Activity - Details* query viewer:

- On the Antivirus Monitoring use case, click the link to the query viewer, **Virus Activity - Details**.

  or

- On the Navigator > Resources panel:
  a. Go to `/All Query Viewers/Downloads/Antivirus`.
  b. Right-click **Virus Activity - Details** and select **View Data as > Table**.

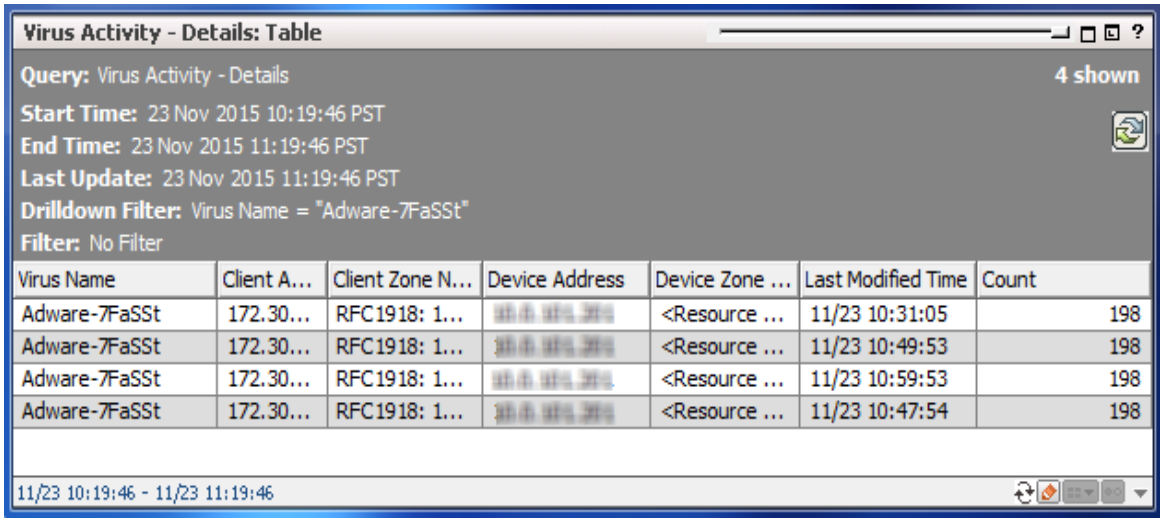
The results display activities concerning all viruses.

To view the *Virus Activity - Details* query viewer as a drilldown:

1. View the *Virus Spread Velocity - Last Hour* query viewer according to the instructions in "Monitoring Query Viewers" on page 23.

2. Right-click a row corresponding to a specific virus of interest, and select **Drilldown > Virus Activity - Details**.

The results display activities pertaining to the virus you selected, for example:



To fine tune the *Virus Activity - Details* query viewer:

ArcSight ESM provides queries to refine the data returned by the query viewer. The query viewer itself has default parameters.

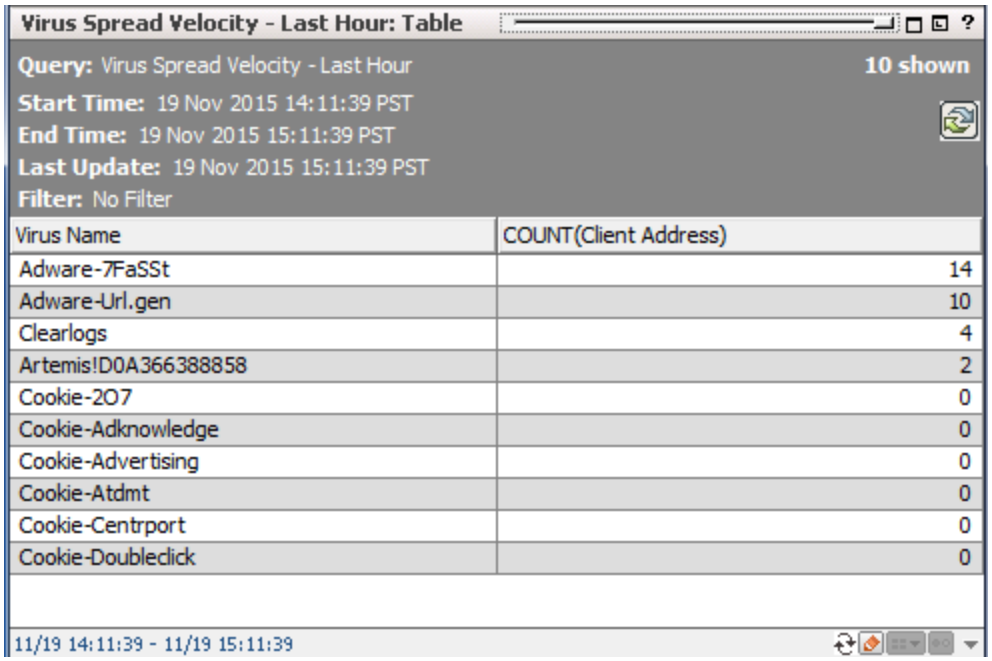
Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Query viewer	**Refresh Data After:** Default is two minutes in which the query viewer runs its query to get new data. **Query Time Out:** Default is no time out, which actually defaults to 5 minutes. Change the time in seconds or minutes if you want. To edit the query viewer, click the pencil icon () on the bottom toolbar of the query viewer. This opens the query viewer's Edit panel. Or, on the Navigator > Resources panel, go to `/All Query Viewers/Downloads/Antivirus`. Right-click **Virus Activity - Details** and select **Edit Query Viewer**. The data fields in the query viewer's Fields tab are inherited from its base query, described next. You can select or deselect the fields brought in by the query, so that the query viewer results includes only the fields you are interested in. Query viewer attributes are described in the *ArcSight Console User's Guide*'s topic on "Defining Query Viewer Settings."
Query used by the query viewer	Change the query to suit your business requirements. To edit the query: • On the query viewer results header, click the query name. • On the Navigator > Resources panel, go to **Reports > Queries** tab. Then go to `/All Queries/Downloads/Antivirus`. Right-cick **Virus Activity - Details** then select **Edit Query**. • If you are adding fields to the query, these added fields do not automatically show up as selected in the query viewer's Fields tab. In that case, edit the query viewer and select the new fields if you want to include their values in the query viewer results. **Caution:** Before modifying any query, verify if this query is being used by other resources. Changes to query settings such as fields may affect the expected results in all resources using that query. Refer to the *ArcSight Console User's Guide*'s topic on "Building Queries" for details.

Using the *Virus Spread Velocity - Last Hour* Query Viewer

The query viewer shows how many client machines have been infected with viruses in the last hour. It provides the virus name and the number of infected machines. The results are refreshed every minute. The query viewer displays the results in a table of up to 10 rows.

Following is a closeup of the query viewer results:



Virus Spread Velocity - Last Hour: Table

Query: Virus Spread Velocity - Last Hour **10 shown**
Start Time: 19 Nov 2015 14:11:39 PST
End Time: 19 Nov 2015 15:11:39 PST
Last Update: 19 Nov 2015 15:11:39 PST
Filter: No Filter

Virus Name	COUNT(Client Address)
Adware-7FaSSt	14
Adware-Url.gen	10
Clearlogs	4
Artemis!D0A366388858	2
Cookie-2O7	0
Cookie-Adknowledge	0
Cookie-Advertising	0
Cookie-Atdmt	0
Cookie-Centrport	0
Cookie-Doubleclick	0

11/19 14:11:39 - 11/19 15:11:39

The query viewer header displays some attributes of the query viewer. For example, the top line shows the name of the query that contains the event fields defined for this query viewer.

To view the *Virus Spread Velocity - Last Hour* query viewer:

- On the Antivirus Monitoring use case, click the link to the query viewer, **Virus Spread Velocity - Last Hour**.

  or

- On the Navigator > Resources panel:
  a. Go to `/All Query Viewers/Downloads/Antivirus`.
  b. Right-click **Virus Spread Velocity - Last Hour** and select **View Data as > Table**.

The Console displays the query viewer results on the Viewer panel.

Note: If nothing is displayed by the query viewer, this means there has been no virus infections in the last hour.

To interpret the *Virus Spread Velocity - Last Hour* query viewer:

The first column contains the virus name and the second column contains the corresponding number of infected machines.

Further investigations on the *Virus Spread Velocity - Last Hour* query viewer:

Right-click on a table row and

- Use the query viewer results to create a baseline or compare the results to an existing baseline.
- Select **Drilldown > Virus Activity Details**. The Virus Activity Details query viewer displays results specific to the selected row, in this case, a specific virus.

To fine tune the *Virus Spread Velocity - Last Hour* query viewer:

ArcSight ESM provides queries to refine the data returned by the query viewer. The query viewer itself has default parameters.

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Query viewer	**Refresh Data After:** Default is one minute in which the query viewer runs its query to get new data. **Query Time Out:** Default is no time out, which actually defaults to 5 minutes. Change the time in seconds or minutes if you want. To edit the query viewer, click the pencil icon () on the bottom toolbar of the query viewer. This opens the query viewer's Edit panel. Or, on the Navigator > Resources panel, go to `/All Query Viewers/Downloads/Antivirus`. Right-click **Virus Spread Velocity - Last Hour** and select **Edit Query Viewer**. The data fields in the query viewer's Fields tab are inherited from its base query, described next. You can select or deselect the fields brought in by the query, so that the query viewer results includes only the fields you are interested in. Query viewer attributes are described in the *ArcSight Console User's Guide*'s topic on "Defining Query Viewer Settings."
Query used by the query viewer	Change the query to suit your business requirements. To edit the query: • On the query viewer results header, click the query name, or • On the Navigator > Resources panel, go to **Reports > Queries** tab. Then go to `/All Queries/Downloads/Antivirus`. Right-cick **Virus Spread Velocity - Last Hour** then select **Edit Query**. • If you are adding fields to the query, these added fields do not automatically show up as selected in the query viewer's Fields tab. In that case, edit the query viewer and select the new fields if you want to include their values in the query viewer results. **Caution:** Before modifying any query, verify if this query is being used by other resources. Changes to query settings such as fields may affect the expected results in all resources using that query. Refer to the *ArcSight Console User's Guide*'s topic on "Building Queries" for details.

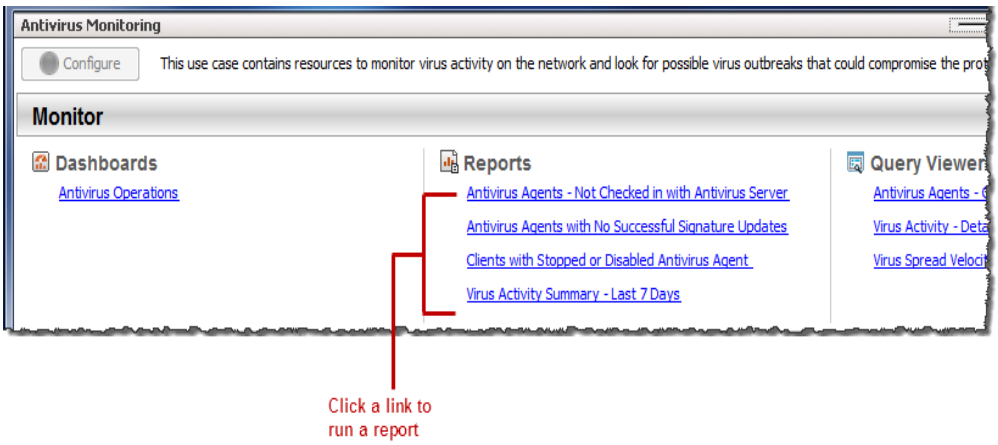
Chapter 5: Running Reports

The Antivirus Monitoring use case provides four reports that you can run to see events on antivirus agents.

The reports have different start and end times which you can change for shorter- or longer-term analysis when you run the report.

To run a report:

1. Click the link for the report in the Antivirus Monitoring use case.



2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The use case provides the following reports:

- The **Antivirus Agents - Not Checked In with Antivirus Server** report shows antivirus clients that have not communicated with the antivirus server in the last seven days. Antivirus agents regularly contact the antivirus server to indicate that the agents are up and running. The report shows a list of the agent address, the last connection time, last action performed by the agent, antivirus server address, the device product, and product version.
- The **Antivirus Agents with No Successful Signature Updates** report shows antivirus agents that have a failed signature update, and then have not had any successful signature updates after that. The information is within the last 7 to 30 days. The report shows a list of antivirus agent addresses, agent hostnames, antivirus product, antivirus server address, and antivirus server hostname.
- The **Clients with Stopped or Disabled Antivirus Agents** report shows events with stopped or disabled clients without any subsequent agent restarts. The report has no start and end dates. The

events are based on when you run the report. The information shows event time, antivirus agent address, antivirus agent host name, antivirus agent zone, and device product.

- The **Virus Activity Summary - Last 7 Days** report shows the top occurrences of virus infections throughout the network as well as on different machines. The report lists the viruses and number of times they were detected.

Run these reports so that you can identify any patterns of virus infections across the network.

Following is a sample report:

10-31-2015-14:36:18 to 11-23-2015-14:36:18

Antivirus Agents with No Successful Signature Updates

Antivirus Agent Address	Antivirus Agent Host Name	Antivirus Product	Antivirus Server Address	Antivirus Server Host Name
[redacted]	NAVSAZTMDR1	AntiVirus Corporate Edition		
[redacted]	RCSDMN1000XYZ6N	AntiVirus Corporate Edition		NAVSAZTMDR1
[redacted]	DTC0D0006F53E5C	AntiVirus Corporate Edition		NAVSAZTMDR1
[redacted]	DTC02005AB22791	AntiVirus Corporate Edition		NAVSAZTMDR1
[redacted]	WELLS-140ECE662	AntiVirus Corporate Edition		NAVSAZTMDR1
[redacted]	K02223-3232	AntiVirus Corporate Edition		HSCC
[redacted]	HQIA2301	AntiVirus Corporate Edition		HSYmC
[redacted]	ADBSK	AntiVirus Corporate Edition		HRTHDEC
[redacted]	HADJHFC	AntiVirus Corporate Edition		
[redacted]	HSKLSKLC	AntiVirus Corporate Edition		
[redacted]	SC	AntiVirus Corporate Edition		SAVSYS
[redacted]	PNYG43GK71	AntiVirus Corporate Edition		hostAV02
[redacted]	BF-04-075402	AntiVirus Corporate Edition		NSVMUC7L
[redacted]	BK-04-014236	AntiVirus Corporate Edition		NSVMUC7L
[redacted]	WHMWS01	AntiVirus Corporate Edition		WHMSVR01
[redacted]	cn-tgt-10.10.1.27	cn Product		
[redacted]	cn-tgt-10.10.1.37	cn Product		
[redacted]	EXCHSRV	MOVE Antivirus		EXCHSRV
[redacted]	MOON	AntiVirus Corporate Edition		ZHONGDENG
[redacted]	ARCSIGHT-PC	ePolicy Orchestrator	[redacted]	WIN-OJ4V173FK06
[redacted]	n150-h087	Endpoint Protection		N150-H086
[redacted]	SZ0A0002	AntiVirus Corporate Edition		MOTOSOC
[redacted]	EPO-VIRUSSCAN	ePolicy Orchestrator	[redacted]	EPO36
[redacted]	scmgateway	Email Gateway		

Page 1 of 10

Chapter 6: Refining the *Antivirus Monitoring* Use Case Rules

The Antivirus Monitoring use case provide multiple rules, and four of them are designed to create cases and send notifications:

By default, these actions are disabled. Refer to the topics in this chapter for instructions on how to fine tune these rules to suit your business requirements.

Below are the rules described in this topic:

- Antivirus Servers - AV Client Agent Stopped
- Critical Asset - Virus Infected
- Virus Outbreak - By Virus
- Virus Outbreak - By Zone

Refining the *Antivirus Servers - AV Client Agent Stopped* Rule

This rule tracks "stop" or "disable" actions on antivirus agents installed in antivirus servers. Stopped or disabled antivirus agents require immediate attention because this means their hosts are unprotected from infections.

The rule's Send Notification action is disabled by default. If enabled, the action:

- Sends this default notification message:

  Antivirus client agent stopped on antivirus server `$targetAddress`
- Sends the notification about the affected host to the default destination, `/All Destinations/SOC Operators/`.
  - If you want to enable this rule with the default destination, make sure to configure that destination by adding users to the appropriate destination levels.
  - If you want to enable this rule action and you are not using the default destination `SOC Operators`, make sure you first define your own destination resource.

  Refer to the "Managing Notification Destinations" topic in the *ArcSight Console User's Guide*.

To customize rule actions:

Tip: Refer to the *ArcSight Console User's Guide*'s topic on "Rule Actions Reference" for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Access the rule in one of two ways:
   - Go to `/All Rules/Downloads/Antivirus`, right-click **Antivirus Servers - AV Client Agent Stopped** and choose **Edit Rule**, or
   - On the Antivirus Monitoring use case's Library section under Rules, click **Antivirus Servers - AV Client Agent Stopped**.

   This opens the rule's Edit panel.
3. Go to the **Actions** tab.
   a. Click the disabled action, **Send Notifications**.
   b. Right-click and select **Enable Action**.
   c. If you want to further modify the rule action, right-click that particular action and select **Edit**. For example, select a different destination group or customize the notification message.

   > **Caution:** If you want to edit the notification message, make sure not to change the Velocity expression, `$targetAddress`, because the value is dynamically supplied by the rule.

Refining the *Critical Asset - Virus Infected* Rule

This rule looks for virus infection events on critical assets (high or very high), as defined by your asset model. The following actions are disabled by default:

- Create a case in `/All Cases/Downloads/Antivirus` with the following features:
  - The case name is dynamically derived as `Failure to clean or quarantine in critical asset $targetAddress`
  - Include the base events related to the case.

> **Note:** If the case does not yet exist, the rule first creates the case with the dynamically-configured name then adds the base events to it. When the rule is triggered in the future, new base events are added to the case.

- Send this default notification message:

  The `$deviceCustomString1` virus in critical asset `$targetAddress` not cleaned or quarantined.

  > **Note:** The message is a template using variables. The variables will be populated with actual event values when the rule triggers.

- Send notification about the scan to the default destination, `/All Destinations/SOC Operators/`.
  - If you want to enable this rule with the default destination, make sure to configure it by adding users to the appropriate destination levels.

- If you want to enable this rule action and you are not using the default destination `SOC Operators`, make sure you first define your own destination resource.

Refer to the "Managing Notification Destinations" topic in the *ArcSight Console User's Guide*.

To customize rule actions:

Tip: Refer to the *ArcSight Console User's Guide*'s topic on "Rule Actions Reference" for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Access the rule in one of two ways:
   - Go to `/All Rules/Downloads/Antivirus`, right-click **Critical Asset - Virus Infected** and select **Edit Rule**, or
   - On the Antivirus Monitoring use case's Library section, under Rules, click **Critical Asset - Virus Infected**.

   This opens the rule's Edit panel.
3. Go the **Actions** tab.
   a. Click the disabled rule action, **Add To Existing Case**.
   b. Right-click **Add To Existing Case** and select **Enable Action**.
   c. If you want to further modify the rule action, right-click again and select **Edit**.
   For example, change the URI if you have previously created a custom case group for tracking antivirus activity.
4. Click the disabled rule action, **Send Notification**.
   a. Right-click **Send Notification** and select **Enable Action**.
   b. If you want to further modify the rule action, right-click that particular action and select **Edit**.
   For example, select a different destination group or customize the notification message.

   Caution: If you want to edit the notification message, make sure not to change the Velocity expressions, `$targetAddress` and `$deviceCustomString1`, because the values are dynamically supplied by the rule.

Refining the *Virus Outbreak - By Virus* Rule

This rule looks for virus outbreak events generated by an increase in a specific virus activity, as detected by a data monitor. The following rule actions are disabled by default:

- Send this default notification message:

  `$deviceCustomString1` virus had a possible outbreak detected by device `$deviceHostName - $deviceAddress`

The notification message is sent to the default destination, `/All Destinations/SOC Operators/`.

- If you want to enable this rule action and you are not using the default destination, `SOC Operators`, make sure you first define your own destination resource.

  Refer to the "Managing Notification Destinations" topic in the *ArcSight Console User's Guide*.
- If you want to enable this rule with the default destination, make sure to configure it by adding users to the appropriate destination levels.

- Set an event field with:
  - Name = Virus Outbreak - `$deviceCustomString1`, and
  - Priority = 9
- Create a case in `/All Cases/Downloads/Antivirus` with the following features:
  - The case name is dynamically derived as

    Virus outbreak was detected - `$deviceCustomString1`
  - Include the base events related to the case.

    Note: If the case does not yet exist, the rule first creates the case with the dynamically-configured name then adds the base events to it. When the rule is triggered in the future, new base events are added to the case.

To customize rule actions:

Tip: Refer to the *ArcSight Console User's Guide*'s topic on "Rule Actions Reference for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Access the rule in one of two ways:
   - Go to `/All Rules/Downloads/Antivirus`, right-click **Virus Outbreak - By Virus** and select **Edit Rule**, or
   - On the Antivirus Monitoring use case's Library section under Rules, click **Virus Outbreak - By Virus**.

   This opens the rule's Edit panel.
3. Go to the **Actions** tab.
4. Click the disabled rule action, **Send Notification**.
   a. Right-click and select **Enable Action**.
   b. If you want to further modify the rule action, right-click that particular action and select **Edit**.
   For example, choose a different destination group or customize the notification message.

   Caution: If you want to edit the notification message, make sure not to change the

Velocity expressions `$deviceCustomString1`, `$deviceHostName`, and `$deviceAddress` because the values are dynamically supplied by the rule.

5. Click the disabled **Set Event Field Actions** action. Right-click, then select **Enable Action**.
6. Click the disabled **Add To Existing Case** action.
   a. Right-click **Add To Existing Case** and select **Enable Action**.
   b. If you want to further modify the rule action, right-click again and select **Edit**.
      For example, change the URI if you have previously created a custom case group for tracking antivirus activity.

Refining the *Virus Outbreak - By Zone* Rule

This rule looks for correlation events generated when a virus outbreak in a zone is detected by a data monitor. The following rule actions are disabled by default:

- Send this default notification message:
  A possible virus outbreak was detected on zone `$targetZoneResource`
- Send notification about the scan to the default destination, `/All Destinations/SOC Operators/`.
  - If you want to enable this rule with the default destination, make sure to configure it by adding users to the appropriate destination levels.
  - If you want to enable this rule action and you are not using the default destination `SOC Operators`, make sure you first define your own destination resource.

  Refer to the "Managing Notification Destinations" topic in the *ArcSight Console User's Guide*.
- Set event fields with:
  - Name = Virus Outbreak in Zone - `$targetZoneResource`, and
  - Priority = 9
- Create a case in `/All Cases/Downloads/Antivirus` with the following features:
  - The case name is dynamically derived as
    Virus outbreak was detected in zone, `$targetZoneResource`
  - Include the base events related to the case.

Note: If the case does not yet exist, the rule first creates the case with the dynamically-configured name then adds the base events to it. When the rule is triggered in the future, new base events are added to the case.

To customize rule actions:

Tip: Refer to the *ArcSight Console User's Guide*'s topic on "Rule Actions Reference" for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Access the rule in one of two ways:
   - Go to `/All Rules/Downloads/Antivirus`, right-click **Virus Outbreak - By Zone** and select **Edit Rule**, or
   - On the Antivirus Monitoring use case's Library section under Rules, click **Virus Outbreak - By Zone**.

   This opens the rule's Edit panel.
3. Go to the **Actions** tab.
4. Click the disabled rule action, **Send Notification**.
   a. Right-click and select **Enable Action**.
   b. If you want to further modify the rule action, right-click that particular action and select **Edit**.
   For example, choose a different destination group or customize the notification message.

   Caution: If you want to edit the notification message, make sure not to change the Velocity expression, `$targetZoneResource`, because the value is dynamically supplied by the rule.
5. Click the disabled **Set Event Field Actions** action. Right-click, then select **Enable Action**.
6. Click the disabled **Add To Existing Case** action.
   a. Right-click **Add To Existing Case** and select **Enable Action**.
   b. If you want to further modify the rule action, right-click again and select **Edit**.
   For example, change the URI if you have previously created a custom case group for tracking antivirus activity.

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 (ESM: Antivirus Monitoring 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!