
Micro Focus Security ArcSight Logger

Software Version: 6.7

Data Migration Guide

Document Release Date: November, 2020

Software Release Date: May, 2019



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

© Copyright 2019 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Support

Contact Information

| | |
|---------------------------------------|---|
| Phone | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| Support Web Site | https://softwaresupport.softwaregrp.com/ |
| ArcSight Product Documentation | https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

Contents

- Data Migration Between Loggers 4
 - Summary 4
- The Data Migration Process 5
- Supported Migration Paths 6
- Prerequisites for Migration 7
- Migrating Data Between Loggers 9
 - What is Migrated from a Logger Appliance 9
 - Data Migration Steps 10
 - Prepare Source and Target Loggers for Migration 11
 - Run the Setup Script 12
 - Run the Data Migration Utility 13
 - Finish the Data Migration 16
- Migrating Event Archive Settings Separately 18
 - Event Archive Migration Steps 18
- After the Migration 25
- Troubleshooting 26
- Send Documentation Feedback 27

Data Migration Between Loggers

This document explains how to migrate data and event archive settings between supported Micro Focus Security ArcSight Loggers. The information in this guide applies to ArcSight Data Platform (ADP) Logger, standalone ArcSight Logger, version 6.7 (L8242) and the Logger Data Migration Utility 6.7 (DM6.7-D1116).

Note: Where there are no specific differences, all types of Logger are called *Logger* in this document.

Summary

Data migration between Loggers may be required for situations like these:

- You want to move data to a Logger with higher storage capacity.
- You want to move data from an old Logger model to a current model.
- You want to move data from a Logger Appliance to a Software Logger.
- You want to move data from a Software Logger on RHEL 6.10 to a Software Logger on RHEL 7.5 .

Event data on a Logger Appliance can be migrated to the following devices:

- Another Logger Appliance of equal or higher capacity.
- A Software Logger installed on a supported operating system.

This capability applies to both storage-area network (SAN) and non-SAN Loggers.

The Data Migration Process

Micro Focus Security ArcSight offers a data migration utility for migrating data between two Loggers. The utility consists of two scripts, one for the source Logger and the other one for the target Logger. The scripts need to be run in parallel on the source and target Loggers, as described in ["Data Migration Steps " on page 10.](#)

Both the source and the target Logger must be up and running for data migration to work. You cannot use the data migration process to migrate data from a non-functional, down Logger, or for migrating data from Logger's local storage to NFS storage.

The utility copies data from the source to the target Logger. Therefore, data on the source Logger is preserved after a successful migration. The target Logger should not have any data on it before migration.

The existing configuration and event data on a target Logger is overwritten by this utility. If there is any existing data on a target Logger appliance, Micro Focus Security ArcSight recommends that you restore the appliance to its original factory settings before beginning the migration.

The data migration stops all Logger processes except for the Logger and the PostgreSQL servers. Therefore, neither Logger can receive events during this phase; however, SSH access to both Loggers is still available.

Scheduled tasks on the source Logger are also suspended during the migration, but the tasks resume as scheduled on the source after the migration is complete. Scheduled task information is not migrated over to the target Logger, as described in ["Migrating Data Between Loggers" on page 9.](#) Therefore, scheduled tasks will not run on the target Logger until explicitly configured after the migration.

Supported Migration Paths

Migration times vary, and may take from 5 to 18 hours or more. The time required to migrate data depends on the connectivity between the two Loggers, the amount of data migrated, the event data size, the form factor of each Logger, and the migration options you select.

You can migrate data between Loggers over a high-speed local area network (LAN) connection that can provide at least 1 Gbps dedicated network bandwidth. Network speed and traffic will affect data migration speed.

Note: Micro Focus Security ArcSight **does not** recommend using a wide area network (WAN) link for the migration. We strongly recommend using a cross-over cable between Logger Appliances to eliminate network latency delays.

The paths in the table below are supported for data migration between two Loggers.

| Migration Path | Source / From | Version | Target / To | Version |
|------------------------------------|---------------|---------|--------------------------------|---------|
| Appliance to Appliance | Lx500 | 6.7 | L7600 | 6.7 |
| Appliance to Software | Lx500 | 6.7 | Software Logger on OS RHEL 7.5 | 6.7 |
| SAN Appliance to Non-SAN Appliance | L7500-SAN | 6.7 | L7600 | 6.7 |
| SAN Appliance to Software | L7500-SAN | 6.7 | Software Logger on OS RHEL 7.5 | 6.7 |
| Software to Software | RHEL 6.10 | 6.7 | RHEL 7.5 | 6.7 |

Data migration tools and services for older versions of Logger may be available through Micro Focus Professional Services.

Prerequisites for Migration

Ensure that the following prerequisites are met before beginning the data migration process.

| Area | Prerequisite |
|----------------|---|
| Source Logger | <ul style="list-style-type: none">• It may be a Logger Appliance or a Software Logger• Software Logger on RHEL 7.5 |
| Target Logger | <ul style="list-style-type: none">• Must be of equal or higher capacity than the source Logger.• Must be either a brand-new Logger with only the configuration described in this section or, for Logger Appliances, an existing Logger that has been restored to its original factory settings. For details about restoring a Logger to its factory settings, see the <i>Logger Administrator's Guide</i>.• The storage volume on the target Logger must be at least as large as the storage volume of the source Logger. After installing the target Logger software and before migrating the data, ensure that the storage volume is at least as large as that on the source Logger. <p>For target Software Loggers:</p> <ul style="list-style-type: none">• Installation as user "root" is required.• The unique identifier (UID) and group identifier (GID) for the <i>non</i>-root user must be 1500 and 750, respectively, to match the UID and GID of the same user on the source Logger. |
| Logger Version | <p>Both Loggers must be running a supported Logger version for migration:</p> <ul style="list-style-type: none">• All other source Loggers must be running Logger version 6.7.• All target Loggers must be running Logger version 6.7. <p>Note: Upgrade your appliance to the appropriate version before the migration.</p> |
| Time settings | <p>Time settings (timestamp and time zone) must be identical on both Loggers.</p> |
| Storage Groups | <p>The target Logger can be configured with either the default storage groups or any additional ones.</p> <p>Caution:</p> <ul style="list-style-type: none">• The target Logger's storage group configuration is overwritten with the source Logger's information. Therefore, after the migration, only the storage groups that existed on the source Logger will be available on the target.• A 100% pre-allocation of space is performed automatically on the storage volume on the target Logger during the data migration process. If any pre-allocated space exists on the target, it is overwritten. |

| Area | Prerequisite |
|---------------------|--|
| NFS/CIFS Mount Name | <p>The remote mount points on the source and target Loggers must match.</p> <div data-bbox="477 310 1406 405" style="background-color: #f0f0f0; padding: 5px;"> <p>Caution: If the mount point is not correctly set up on the target Logger before data migration begins, the process will fail.</p> </div> <p>To configure mount points:</p> <ul style="list-style-type: none"> • Logger Appliance targets—use Logger’s System Admin interface. • Software Logger targets—set the mount points manually as appropriate for your operating system: <ol style="list-style-type: none"> a. Make sure the mount point directory belongs to the Logger installation non-root username (usually name=arcsight, group name=arcsight, groupid=750, userid=1500). b. Use the following mount command to proceed: mount NFSS_IP:<shared directory> <logger mountpoint> . For example: mount 192.0.2.0:/opt/export /opt/mnt/SL_NFS c. Confirm that the NFS server in the /etc/exports shared directory includes this parameter: no_root_squash. For example: /opt/export *(rw,sync,no_subtree_check,no_root_squash) <p>Confirm that all storage groups are added in the target system. See, "Adding Storage Groups" in the Admin Guide.</p> <p>Verify that all of the following configuration parameters exist and are identical on the source and target Loggers:</p> <ul style="list-style-type: none"> • The number of mounts • Mount name • Mount path • Hostname |
| Event Archive | <p>If an event archive is loaded on the source Logger, make sure it is unloaded before you begin the data migration process. See, "Loading and Unloading Archives" in the Admin Guide,</p> |
| Archive Settings | <p>If you archive events to an NFS or CIFS server, make sure the mount point is configured on the target Logger, and the server is up and reachable from the target Logger.</p> <ul style="list-style-type: none"> • To ensure the ensure the previous statement follow these steps: <ol style="list-style-type: none"> 1. Go to System Admin > Remote File Systems 2. Copy the information from the source into the target field. <p>When setting the mount point:</p> <ul style="list-style-type: none"> • Logger Appliance targets—use Logger’s System Admin interface. • Software Logger targets—set the mount points manually as appropriate for your operating system. |

Migrating Data Between Loggers

You can migrate event data in live storage, archived event settings, and some Logger configuration data to another Logger of a supported type.

What is Migrated from a Logger Appliance

The following event and configuration data can be migrated from a Logger Appliance using the data migration script. For examples of data types that are not migrated, see ["Data Not Migrated from Logger Appliance" on the next page](#).

Data Migrated from Logger Appliance

- Custom schema fields
- Devices
- Global ID settings
- Event archive *settings* (archive configuration metadata and mappings)

Caution: If you skip archive migration during the data migration process, your archive configuration metadata and mappings will not be migrated. After the migration, you will not be able to access any of your archives until you migrate your archives. See ["Migrating Event Archive Settings Separately" on page 18](#) for more information.

- Event data and its metadata
- Global summary data (**Summary** menu option)

Note: Global Summary Persistence was disabled in Logger 5.3 SP1, however, any existing global summary data will still be migrated.

- Indexing information
- Lookup files

Note: A known issue with data migration prevents lookup files from being properly migrated if the path to the data migration file on the target Logger is different from the one on the source Logger. See ["Migrating Event Archive Settings Separately" on page 18](#) for how to handle data that is not migrated.

- Parser definitions
- Receivers
- Retention information

- Source type information
- Storage groups
- Superindexing information

Data Not Migrated from Logger Appliance

- Alerts
- All scheduled jobs
- Archived events data (migrating event archive *settings* allow you to see and access your event archive *data*)
- Configuration backup settings
- Daily archive settings
- Dashboards
- Device groups
- ESM destinations
- Filters, including system filters, user-defined filters, and PCI/SOX package filters
- Forwarders
- Peer configuration
- Reports (including published reports)
- Saved searches
- Storage rules

Caution: Do not use the configuration backup and restore feature in an attempt to move data that is not migrated to the target Logger. See ["Migrating Event Archive Settings Separately" on page 18](#) for how to handle data that is not migrated.

Data Migration Steps

Perform these steps to migrate data from one Logger to another.

Note: Be sure to start the **target** Logger script before the **source** Logger script; otherwise, the data migration process will not proceed as expected.

If data migration fails at any point, refer to ["Troubleshooting" on page 26](#).

Prepare Source and Target Loggers for Migration

| steps | On the Source Logger.. | On the Target Logger.. |
|-------|---|---|
| 1 | Make sure that the source and target Loggers meet the requirements listed in "Prerequisites for Migration" on page 7 before continuing. | |
| 2 | Reboot the Source Logger. | |
| 3 | <p>Copy</p> <p>datamigration-6.7-D1116.tar.gz</p> <p>to: /opt/arcsight/logger.</p> <p>This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.</p> <ul style="list-style-type: none"> On Software Loggers, use the directory path where Logger was installed. The default is: /opt/current/arcsight/logger <p>This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.</p> | <p>Copy</p> <p>datamigration-6.7-D1116.tar.gz</p> <p>to the following directory:</p> <ul style="list-style-type: none"> On Logger Appliances: /opt/arcsight/logger On Software Loggers, use the directory path where Logger was installed. The default is: /opt/current/arcsight/logger <p>This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.</p> |
| 4 | SSH to the Logger and log in as user "root" | SSH to the Logger and log in as user "root" |
| 5 | <p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME= /opt/arcsight/logger</pre> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME= <LoggerInstallDirectory>/current /arcsight/logger</pre> <p>By default this is: /opt/current/arcsight/logger</p> | <p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME= /opt/arcsight/logger</pre> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME= <LoggerInstallDirectory>/current /arcsight/logger</pre> <p>By default this is: /opt/current/arcsight/logger</p> |
| 6 | <p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre> | <p>Enter this command to navigate to the Logger home directory:</p> <pre>cd \$ARCSIGHT_HOME</pre> |
| 7 | <p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> | <p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> |

Run the Setup Script

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|---|
| 1 | Enter this command to run the setup script: <pre>bin/scripts/dataMigrationSource_rsh_setup.sh</pre> | Enter this command to run the setup script: <pre>bin/scripts/dataMigrationTarget_rsh_setup.sh</pre> |
| 2 | | <p>The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location.</p> <p>If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory.</p> <p>After you enter the directory, the script prompts you to confirm the location you entered. Enter 'y' to confirm or 'n' to re-enter the location.</p> |
| 3 | | You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not. |
| 4 | | Edit the /etc/hosts.deny file to add the following information: <pre>in.rlogind: all in.rshd: all</pre> |
| 5 | | Edit the /etc/hosts.allow file to add the following: <pre>all: <source_IPAddress></pre> <p>where <source_IPAddress> is the IP address of the source Logger, unless you are using a crossover cable.</p> <div data-bbox="857 1360 1406 1486" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached.</p> </div> |
| 6 | | Create the following files if they are not present: <ul style="list-style-type: none"> • /etc/hosts.equiv • /root/.rhosts Edit the files to add the following information: <pre><source_IPAddress> root</pre> <p>where <source_IPAddress> is the IP address of the source Logger, unless you are using a crossover cable.</p> <div data-bbox="857 1808 1406 1892" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: When using a crossover cable, enter the IP address of the NIC to which the cable is attached.</p> </div> |

Run the Data Migration Utility

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|--|
| 1 | | <p>Enter this command to run the Data Migration utility:</p> <pre>bin/scripts/dataMigrationTarget.sh</pre> <p>Tip: Press Ctrl+C to exit the script at any time.</p> |
| 2 | | <p>On software Logger, you may be asked if the non-root user is "arcsight." If so, enter 'y'. If not, enter the non-root user name used when installing Logger.</p> <p>After you enter the user name, the script prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the user name.</p> |
| 3 | | <p>A message telling you to run the data migration script on the source Logger is displayed.</p> |
| 4 | <p>Enter one of the following commands to run the Data Migration utility:</p> <pre>bin/scripts/dataMigrationSource.sh</pre> <pre>bin/scripts/dataMigrationSource.sh -force_checksum</pre> <p>Tip: Using the <code>-force_checksum</code> option can take significantly longer to migrate data. However, this command provides an additional check to ensure that each file has been reliably copied from the source to the target Logger.</p> <p>Logger prompts you to confirm whether or not to reboot the source Logger before running data migration scripts. Enter [y/n] or Ctrl - C to terminate the script.</p> | |
| 5 | <p>The utility prompts you to confirm the ARCSIGHT_HOME location. Enter 'y' to confirm or 'n' to re-enter the location.</p> <p>The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>Tip: Press Ctrl+C to exit the script at any time.</p> | |

| Steps | On the Source Logger... | On the Target Logger... |
|-------|--|-------------------------|
| 6 | <p>The utility prompts you to enter the IP address of the target Logger.</p> <p>After you enter the IP address, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the IP address.</p> | |
| 7 | <p>The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'n', the utility prompts you to enter the ARCSIGHT_HOME of the target machine. (The utility assumes the ARCSIGHT_HOME for Logger Appliances.)</p> <p>After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.</p> | |
| 8 | <p>The utility now prompts you to consider how you want to handle archive migration.</p> <p>Option 1: Default archive migration: The data migration script fails and exits if the archive check fails. If the scripts exits because the archive check failed, restore the missing archives and run the script again.</p> <p>Option 2: Ignore archive check: Data migration continues even if the archive check fails. Event archive settings (archive configuration metadata and mappings) are migrated and any missing archives will be accessible if you restore them to their original location.</p> <p>Option 3: Skip archive migration: No archive configuration metadata is migrated. You will not be able to access any of your archives until after you run the Archive Migration Utility. See "Migrating Event Archive Settings Separately" on page 18 for more information.</p> <p>Answer the following prompts in accordance with the migration option you select.</p> | |
| 9 | <p>The utility asks if you would like to migrate your archives only after the archive check passes.</p> <ul style="list-style-type: none"> • Option 1: Enter 'y'. Go to "12" on the next page. • Option 2: Enter 'n'. Continue to the next step. • Option 3: Enter 'n'. Continue to the next step. | |
| 10 | <p>If you entered 'n', the utility asks you if you would like to migrate the archive configuration metadata even if some archives are missing.</p> <ul style="list-style-type: none"> • Option 2: Enter 'y'. Go to "12" on the next page. • Option 3: Enter 'n'. Continue to the next step. | |

| Steps | On the Source Logger... | On the Target Logger... |
|-------|--|-------------------------|
| 11 | <p>If you entered 'n', the utility asks you if you are sure you want to skip archive migration.</p> <ul style="list-style-type: none">Option 3: Enter 'y'. Go to "12" below. <div data-bbox="321 426 829 648" style="border: 1px solid #ccc; padding: 5px;"><p>Caution: If you confirm this option, you will not be able to access any of your archives after the migration until after you run the Archive Migration Utility. See "Migrating Event Archive Settings Separately" on page 18 for instructions.</p></div> <ul style="list-style-type: none">If you enter 'n' to all three options, the utility returns to "8" on the previous page, or press Ctrl+C to exit the script. | |
| 12 | <p>The utility prompts you to confirm the location of the source and target Loggers' data directories. Enter 'y' to confirm or 'n' to exit the without migrating the data.</p> | |

| Steps | On the Source Logger... | On the Target Logger... |
|-------|--|---|
| | <p>The data migration utility starts to migrate the data.</p> <p>Note: During the migration process, the utility checks if there is sufficient space on the source Logger to perform the dump. If sufficient space is not found, a message indicating the amount of space required is displayed and the utility exits on both Loggers, the source and target. You must free up the indicated amount of space before restarting the utility. When you restart the data migration utility, make sure that you start it on the target Logger first, and then the source Logger.</p> <p>You can check the progress of the migration in <code>user/logger/dataMigrationSource.out</code> and <code>user/logger/dataMigrationTarget.out</code>.</p> | |
| 13 | <p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <pre>source: Source box is done! source: Please make sure data migration has completed on the target logger before rebooting this logger.</pre> <p>Caution: Wait for both Loggers to complete this step before going on to the next step.</p> | <p>If the migration script completes successfully, the following messages are displayed on the target Logger.</p> <pre>target: Data migration successfully completed! target: Please reboot target box!</pre> <p>Caution: Wait for both Loggers to complete this step before going on to the next step.</p> |
| 14 | <p>Reboot the Logger now or later, depending upon the event archiving choice you made in "8" on page 14.</p> <ul style="list-style-type: none"> Option 1 and 2: Data and event archive migrations are complete. Reboot now. Option 3: If you are not going to migrate your event archives immediately, reboot now. Option 3: If you are going to migrate your event archives immediately, you can wait to reboot until after you migrate the archives. | <p>Reboot the Logger now or later, depending upon the event archiving choice you made in "8" on page 14.</p> <ul style="list-style-type: none"> Option 1 and 2: Data and event archive migrations are complete. Reboot/restart now. Option 3: If you are not going to migrate your event archives immediately, reboot/restart now. Option 3: If you are going to migrate your event archives immediately, you can wait to reboot/restart until after you migrate the archives. |

Finish the Data Migration

Follow these steps to finish the data migration process, depending upon the event archiving choice you made in ["8" on page 14](#):

- Option 1 and 2: complete these steps now.
- Option 3: If you are not going to migrate your event archives immediately, complete these steps now.
- Option 3: If you are going to migrate your event archives immediately, you can wait to complete these steps until after you migrate the archives.

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|--|
| 1 | | <p>Configure the target Logger to make it match the source Logger.</p> <p>See "Migrating Data Between Loggers" on page 9 and "After the Migration" on page 25 for more information.</p> |
| 2 | | <p>Edit these files:</p> <ul style="list-style-type: none"> • /etc/hosts.equiv • /root/.rhosts <p>Remove the following line:</p> <pre><source_IPAddress> root</pre> <p>where <source_IPAddress> is the IP address of the source Logger.</p> |
| 3 | <p>After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 11.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/ dataMigrationSource_rsh_cleanup.sh</pre> | <p>After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 11.</p> <p>Enter this command to clean up the RSH files:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/ dataMigrationTarget_rsh_cleanup.sh</pre> |
| 4 | <p>Create a gzip file of log files created during the data migration process. To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/ dataMigrationClean.sh</pre> <p>A file similar to dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory.</p> <p>Copy this new file to another location to preserve the log files.</p> | <p>Create a gzip file of log files created during the data migration process. To do so, enter this command:</p> <pre>\$ARCSIGHT_HOME/bin/scripts/ dataMigrationClean.sh</pre> <p>A file similar to dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory.</p> <p>Copy this new file to another location to preserve the log files.</p> |
| 5 | <p>Remove the original data migration utility files. To do so, enter this command:</p> <pre>rm -f \$ARCSIGHT_HOME/ datamigration*.tar.gz</pre> <p>Note: This may delete the gzip of the log files created in "4" above. To preserve this file, copy it to another location.</p> | <p>Remove the original data migration utility files. To do so, enter this command:</p> <pre>rm -f \$ARCSIGHT_HOME/ datamigration*.tar.gz</pre> <p>Note: This mayl delete the gzip of the log files created in "4" above. To preserve this file, copy it to another location.</p> |

Migrating Event Archive Settings Separately

The event archive settings consist of the archive configuration metadata and mappings. If you choose to skip archive migration during data migration, the data that tells Logger how to find the event archives is not migrated. Therefore, when you look at your Event Archive list in Logger, the archives will not be displayed.

The Archive Migration Utility migrates these event archive settings. After archive migration is complete, you will be able to see and access your event archives from your Logger UI, provided they exist in the expected locations.

Note: The archives themselves are not moved. They stay in their original locations, but you will be able to access them from the target Logger.

The archive mapping migration process is very similar to the data migration process and has the same requirements. Like the Data Migration Utility, the Archive Migration Utility consists of two scripts, one for the source Logger and the other one for the target Logger. The scripts need to be run in parallel on the source and target Loggers.

Event Archive Migration Steps

Migrating your event archives separately is only required if you chose to skip archive migration (Option 3 in "[Data Migration Steps](#)" on page 10.) If you chose the first or second option and migrated your archives, *do not run these scripts*.

Perform these steps to migrate event archive settings from one Logger to another.

Note: Be sure to start the **target** Logger script before the **source** Logger script; otherwise, the data migration process will not proceed as expected.

If archive migration fails at any point, refer to "[Troubleshooting](#)" on page 26.

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|---|---|
| 1 | Make sure that you have completed the data migration process through at least " 13 " on page 16 of Data Migration Between Loggers before starting archive migration. | |
| 2 | Enable SSH access to the appliance if it is not already enabled. <ul style="list-style-type: none">On the System Admin page, under System, click SSH. The SSH configuration page opens. Click Enable. | Enable SSH access to the target Logger if it is not already enabled. On Logger appliances: <ul style="list-style-type: none">On the System Admin page, under System, click |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|---|
| | | <p>SSH. The SSH configuration page opens. Click Enable.</p> <p>On Software Loggers:</p> <ul style="list-style-type: none"> Verify that the system on which Logger is installed is reachable through SSH. |
| 3 | <p>Copy datamigration-6.7-D1116.tar.gz</p> <p>to: /opt/arcsight/logger.</p> <p>This is the Logger home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.</p> <p>On Software Loggers, use the directory path where was installed. The default is:</p> <p>/opt/current/arcsight/logger This is the home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.</p> <p>Note: Skip this step if you did not remove the Data Migration files as described in Step 5 on page 1.</p> | <p>Copy datamigration-6.7-D1116.tar.gz</p> <p>On Logger Appliances:</p> <p>to /opt/arcsight/logger.</p> <p>This is the Logger home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.</p> <p>On Software Loggers, use the directory path where was installed. The default is</p> <p>: /opt/current/arcsight/logger</p> <p>This is the home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.</p> <p>Note: Skip this step if you did not remove the Data Migration files as described in Step 5 on page 1.</p> |
| 4 | SSH to the Logger and log in as user “root.” | SSH to the Logger and log in as user “root.” |
| 5 | <p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre> <p>Note: Skip this step if you did not reset the ARCSIGHT_HOME environment variable and run the cleanup script in "3" on page 17.</p> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME=<Logger_install_directory>/current/arcsight/logger</pre> <p>By default this is:</p> <pre>/opt/current/arcsight/Logger</pre> | <p>Set the ARCSIGHT_HOME environment variable, using the following command:</p> <pre>export ARCSIGHT_HOME=/opt/arcsight/logger</pre> <p>Note: Skip this step if you did not reset the ARCSIGHT_HOME environment variable and run the cleanup script in "3" on page 17.</p> <p>To set the environment variable on Software Loggers, issue the following command:</p> <pre>export ARCSIGHT_HOME=<Logger_install_directory>/current/arcsight/logger</pre> <p>By default this is:</p> <pre>/opt/current/arcsight/Logger</pre> |
| 6 | Enter this command to navigate to the Logger home directory: | Enter this command to navigate to the Logger home directory: |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|---|
| | cd \$ARCSIGHT_HOME | cd \$ARCSIGHT_HOME |
| 7 | <p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> <p>Note: Skip this step if you did not run the cleanup script in "3" on page 17.</p> | <p>Enter this command to extract the compressed files:</p> <pre>tar xzvf datamigration*.tar.gz</pre> <p>Note: Skip this step if you did not run the cleanup script in "3" on page 17.</p> |
| 8 | <p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationSource_rsh_setup.sh</pre> | <p>Enter this command to run the setup script:</p> <pre>bin/scripts/dataMigrationTarget_rsh_setup.sh</pre> |
| 9 | | <p>The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location.</p> <p>If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory.</p> <p>After you enter the directory, the script prompts you to confirm the location you entered. Enter 'y' to confirm or 'n' to re-enter the location.</p> |
| 10 | | <p>You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not.</p> |
| 11 | | <p>Edit the /etc/hosts.deny file to add the following information:</p> <pre>in.rlogind: all in.rshd: all</pre> <p>Note: Skip this step if you added this information earlier, as described in "4" on page 12.</p> |
| 12 | | <p>Edit the /etc/hosts.allow file to add the following:</p> <pre>all: <source_IPAddress></pre> <p>where <sourceIPAddress> is the IP address of the source Logger.</p> <p>Note:</p> <ul style="list-style-type: none"> • When using a cross-over cable, enter the IP address of the Network Interface Card (NIC) to which the cable is attached. • You can skip this step if you edited the files as described in "2" on page 17. |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|--|
| 13 | | <p>Edit the <code>/etc/hosts.equiv</code> and <code>/root/.rhosts</code> files to add the following information:</p> <pre><source_IPAddress> root</pre> <p>where <code><source_IPAddress></code> is the IP address of the source Logger.</p> <div data-bbox="878 541 1406 800" style="background-color: #f0f0f0; padding: 5px;"> <p>Note:</p> <ul style="list-style-type: none"> • When using a cross-over cable, enter the IP address of the NIC to which the cable is attached. • You can skip this step if you edited the files as described in "2" on page 17. </div> |
| 14 | | <p>Enter this command to run the Archive Migration utility:</p> <pre>bin/scripts/dataMigrationTarget_Archive_Only.sh</pre> <p>On software Logger targets, you may be asked if the non-root user is "arcsight". If so, enter 'y'. If not, enter the non-root user name that was used when installing Logger.</p> <p>After you enter the user name, the script prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the user name.</p> |
| 15 | | <p>A message telling you to run the Archive Migration utility on the source Logger is displayed.</p> <div data-bbox="878 1339 1406 1402" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Press Ctrl+C to exit the script at any time.</p> </div> |
| 16 | <p>Enter this command to run the Archive Migration utility:</p> <pre>bin/scripts/dataMigrationSource_Archive_Only.sh</pre> | |
| | <p>The utility prompts you to confirm the ARCSIGHT_HOME location. Enter 'y' to confirm or 'n' to re-enter the location.</p> <p>The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <div data-bbox="326 1787 849 1850" style="background-color: #f0f0f0; padding: 5px;"> <p>Tip: Press Ctrl+C to exit the script at any time.</p> </div> | |
| 17 | <p>The utility prompts you to enter the IP address of</p> | |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|------------------------|
| | <p>the target Logger.</p> <p>After you enter the IP address, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the IP address.</p> | |
| 18 | <p>The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not.</p> <p>If you entered 'n', the utility prompts you to enter the ARCSIGHT_HOME of the target machine. (The utility assumes the ARCSIGHT_HOME for Logger Appliances.)</p> <p>After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.</p> | |
| 19 | <p>If you migrated the archive event settings when performing the Data Migration You cannot run this script, and the script will display the following warning: "You did not choose to skip archive migration last time, thus You cannot migrate archive separately."</p> | |
| 20 | <p>Otherwise, the utility prompts you to consider how you want to handle archive migration:</p> <p>Option 1: Default archive migration: The Archive Migration script fails and exits if the archive check fails. If the scripts exits because the archive check failed, restore the missing archives and run the script again.</p> <p>Option 2: Ignore archive check: Archive Migration continues even if the archive check fails. Event archive settings (archive configuration metadata and mappings) are migrated and any missing archives will be accessible if you restore them to their original location.</p> <p>Answer the following prompts in accordance with the migration option you select.</p> | |
| 21 | <p>The utility then asks if you would like to migrate your archives only after the archive check passes. Enter 'y' if so. Enter 'n' if not.</p> <ul style="list-style-type: none"> • Option 1: Enter 'y'. Go to "23" on the next page. • Option 2: Enter 'n'. Continue to the next step. | |
| 22 | <p>If you entered 'n', the utility asks you if you would like to migrate the archive configuration metadata</p> | |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|--|--|
| | <p>even if some archives are missing?</p> <p>Enter 'y' and continue to the next step.</p> | |
| 23 | <p>The utility prompts you to confirm the settings. Enter 'y' to proceed or 'n' to enter the settings again.</p> | |
| 24 | <p>The utility asks if you want to migrate the event archive settings now. Enter 'y' to confirm or 'n' to exit the without migrating the event archive settings.</p> | |
| 25 | <p>The Archive Migration utility starts to migrate the settings.</p> <p>During the migration process, the utility checks if there is sufficient space on the source Logger to perform the dump. If sufficient space is not found, a message indicating the amount of space required is displayed and the utility exits on both Loggers, the source and target. You must free up the indicated amount of space before restarting the utility.</p> <p>Note: When you restart the utility, make sure that you start it on the target Logger first and then the source Logger.</p> <p>You can check the progress of the migration in: user/Logger/dataMigrationSourceArchiveOnly.out and user/Logger/dataMigrationTargetArchiveOnly.out</p> | |
| 26 | <p>If the migration script completes successfully, the following messages are displayed on the source Logger.</p> <pre>source: Source box is done! source: Please make sure Archive Migration has completed on the target logger before rebooting this logger.</pre> <p>Caution: Wait for both Loggers to complete this step before going on to the next step.</p> | <p>If the migration script completes successfully, the following messages are displayed on the target Logger.</p> <pre>target: Archive Migration successfully completed! target: Please reboot target box!</pre> <p>Caution: Wait for both Loggers to complete this step before going on to the next step.</p> |
| 27 | <p>Reboot the Logger.</p> | <p>Reboot the Logger Appliance or restart the Software Logger.</p> |
| 28 | | <p>Configure the target Logger to make it match the source Logger. See "Migrating Data Between Loggers" on page 9 and "After the Migration" on page 25 for more information.</p> <p>Note: Skip this step if you configured your Logger before performing the event archive migration, as described in "1" on page 17.</p> |
| 29 | | <p>Edit the /etc/hosts.equiv and /root/.rhosts files to remove the following</p> |

| Steps | On the Source Logger.. | On the Target Logger.. |
|-------|---|---|
| | | information: source_IPAddress> root where <source_IPAddress> is the IP address of the source Logger. |
| 30 | After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 19. Enter this command to clean up the RSH files: <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationSource_rsh_cleanup.sh</pre> | After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 19. Enter this command to clean up the RSH files: <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationTarget_rsh_cleanup.sh</pre> |
| 31 | Enter this command to create a gzip file of log files created during the migration process: <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> A file such as dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory. | Enter this command to create a gzip file of log files created during the migration process: <pre>\$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh</pre> A file such as dataMigrationLog.2016-01-11PST164827.tar.gz is created in the ARCSIGHT_HOME directory. |
| 32 | Enter this command to remove the original Data Migration utility files: <pre>rm -f \$ARCSIGHT_HOME/datamigration*.tar.gz</pre> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: This will delete the gzip of the log files created in "31" above. To preserve this file, copy it to another location.</p> </div> | Enter this command to remove the original Data Migration utility files: <pre>rm -f \$ARCSIGHT_HOME/datamigration*.tar.gz</pre> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: This will delete the gzip of the log files created in "31" above. To preserve this file, copy it to another location.</p> </div> |

After the Migration

Once data migration has completed successfully, do the following:

1. If file receivers were configured on the source Logger, add appropriate NFS mounts for them on the target Logger and configure the receivers to use those mount points. The NFS mount points need to be the same as the one on the source Logger.

When setting the mount point on Logger Appliance targets, use Logger's System Admin interface. For Software Logger targets, set the mount points manually as appropriate for your operating system.

2. Create data and perform configuration that is not migrated (as listed in ["Migrating Data Between Loggers" on page 9](#)) on the target Logger:
 - a. Use the Configuration Backup and Restore feature, described in Logger Administrator's Guide, to back up **only the report content** from the source Logger and restore it to the target Logger. (To back up only the report content, select **Report Content only** from the Backup Content field.)
 - b. Use the Content Import/Export capability of Logger, described in Logger Administrator's Guide, to export alerts and filters from the Source Logger and import it into the Target Logger.

Note: You may need to add destination information to imported alerts.

- c. Manually re-create all other data.
3. If the source Logger had Compliance Insight Packages for PCI, SOX, or IT Governance deployed, reload those packages to the target Logger. If the SOX filters on your source Logger were loaded using the `soxfilters-1188.enc` file, the file is available from Micro Focus ArcSight Customer Support upon request.
 4. If look-up files were not migrated properly, delete the look-up files on the target Logger, and upload those files that are on the source Logger.

Troubleshooting

- If the data migration utility fails during the migration process, press **Ctrl+C** to terminate the utility on both (source and target) Loggers. Once you have exited, re-run the data migration scripts from "1" on [page 12](#), and the archive migration scripts from "14" on [page 21](#).

Note: When re-running the utility, make sure you start the target Logger script before the source Logger script.

- If the migration process is interrupted, the operation restarts from the beginning when the script is re-run on the source and target Loggers.
- If the data migration process fails with an error message similar to the following message:

```
source: event archive checking failed!
```

ensure that the remote mount points (that match the source Logger's mount points) are set up on the target Logger, or consider selecting a different Archive Migration option.

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Data Migration Guide (Logger 6.7)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!