Micro Focus Security ArcSight Logger

Data Migration Guide

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

© Copyright 2023 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S.Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

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.

Documentation Updates

The title page of this document home page of this Help contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

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://www.microfocus.com/documentation/arcsight/

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 ADP Logger, standalone ArcSight Logger version 7.3 (L8422) and the Logger Data Migration Utility DM720-D1143.

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 on the following situations:

- 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 7.9 to a Software Logger on RHEL 8.6

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 PostgreSQL and 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 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.

IMPORTANT: The L7600 Logger Appliance models are no longer supported. All Appliance sections refer to L7700 models specifically.

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	L7600 (RHEL 7.9)	7.2.2	L7700 (RHEL 7.9)	7.3
Appliance to Software	L7600 (RHEL 7.9)	7.2.2	Software Logger on OS RHEL 8.6	7.3
Software to Software	RHEL 7.9	7.2.2	RHEL 8.6	7.3

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	• It may be a Logger Appliance or a Software
Target Logger	• 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 ArcSight Logger 7.3 Administrator's Guide. • 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. For target Software Loggers: • The unique identifier (UID) and group identifier (GID) for the *non*-root user must be `1500` and `750`, respectively, to match the UID and GID of the same user on the source Logger.
Logger Version	Both Loggers must be running a supported Logger version for migration: • All other source Loggers must be running Logger version 7.3. • All target Loggers must be running Logger version 7.3. **Note:** Upgrade your appliance to the appropriate version before the migration.
Time settings	Time settings (timestamp and time zone) must be identical on both Loggers.
Storage Groups	**Caution:** • 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	The remote mount points on the source and target Loggers must match.
	Caution: If the mount point is not correctly set up on the target Logger before data migration begins, the process will fail.
	To configure mount points:
	• Logger Appliance targets—use Logger's System Admin interface.
	• Software Logger targets—set the mount points manually as appropriate for your operating system:
	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 mount point>`
	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)`
	Verify that all of the following configuration parameters exist and are identical on the source and target Loggers:
	• The number of mounts
	• Mount name
	• Mount path
	• Hostname

Event Archive	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 ArcSight Logger 7.3 Administrator's Guide.
Archive Settings	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. • To ensure the previous statement, follow these steps: 1. Go to **System Admin** > **Remote File Systems** 2. Copy the information from the source into the target field. When setting the mount point: • 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

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" on the next page.

Data Migrated from Logger

- 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 21 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 21 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

- 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 "After the Migration" on page 27 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 28.

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	Copy
	datamigration-7.2-D1143.tar.gz
	to:
	`/opt/arcsight/logger`
	This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.
	• On Software Loggers, use the directory path where Logger was installed. The default is:
	`/opt/current/arcsight/logger`
	This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.
		Copy
		datamigration-7.2-D1143.tar.gz
		to the following directory:
		• On Logger Appliances:
		`/opt/arcsight/logger`
		On Software Loggers, use the directory path where Logger was installed. The default is:
		`/opt/current/arcsight/logger`
		This is the Logger home directory, referred to by the Data Migration utility as ARCSIGHT_HOME.

4	SSH to the Logger and log in as user “root”	SSH to the Logger and log in as user “root”

5	Set the ARCSIGHT_HOME environment variable, using the following command:
	`export ARCSIGHT_HOME=/opt/arcsight/logger`
	To set the environment variable on Software Loggers, issue the following command:
	`export ARCSIGHT_ HOME=< Logger InstallDirectory>/current/arcsight/logger`
	By default this is:
	`/opt/current/arcsight/logger`
		Set the ARCSIGHT_HOME environment variable, using the following command:
		`export ARCSIGHT_HOME=/opt/arcsight/logger`
		To set the environment variable on Software Loggers, issue the following command:
		`export ARCSIGHT_ HOME=< Logger InstallDirectory>/current/arcsight/logger`
		By default this is:
		`/opt/current/arcsight/logger`

6	Enter this command to navigate to the Logger home directory: `cd $ARCSIGHT_HOME`	Enter this command to navigate to the Logger home directory: `cd $ARCSIGHT_HOME`
7	Enter this command to extract the compressed files: `tar xzvf datamigration*.tar.gz`	Enter this command to extract the compressed files: `tar xzvf datamigration*.tar.gz`

Run the Setup Script

Steps	On the Source Logger...	On the Target Logger...

1	Enter this command to run the setup script:
	`bin/scripts/dataMigrationSource_ssh_setup.sh`
		Run the following command:
		`mkdir /root/.ssh`
		Enter this command to run the setup script:
		`bin/scripts/dataMigrationTarget_ssh_setup.sh`
		The setup script above installs rsync in the target Logger. If you wish to verify its presence, execute this command:
		`rpm -qa | grep rsync`

2		The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location. If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory. 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.
3		You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not.

If the SSH connection is lost, the ARCSIGHT_HOME needs to be reset, see "Trying to run a script returns a not found error:" on page 30

Run the Data Migration Utility

Steps	On the Source Logger...	On the Target Logger...

1		(Conditional - For non-root Software Logger installations only) Execute the following command:
		`chown root:root ARCSIGHT_HOME/current/local/monit/watchdog/monitrc`
		Enter this command to run the Data Migration utility:
		`bin/scripts/dataMigrationTarget.sh`
		Tip: Press Ctrl+C to exit the script at any time.

2		On Software Logger, you may be asked if the non-root user is “arcsight.” If so, enter ‘y’. If not, enter the non-root username used when installing Logger. After you enter the username, the script prompts you to confirm it. Enter ‘y’ to confirm or ‘n’ to re-enter the username.
3		A message telling you to run the data migration script on the source Logger is displayed.

Steps	On the Source Logger...	On the Target Logger...

4	Enter one of the following commands to run the Data Migration utility:
	`bin/scripts/dataMigrationSource.sh`
	`bin/scripts/dataMigrationSource.sh -force_checksum`
	`bin/scripts/dataMigrationSource.sh -use_rsync`
	Tip: Using the `-force_checksum` 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.
	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.
	Using the `-use_rsync` option bypasses the use of `Ftran` entirely, and forces the use of `Rsync` for the live data transfer instead. See "The target Logger is stuck displaying either of these messages:" on page 28	

5	The utility prompts you to confirm the `ARCSIGHT_HOME` location. Enter 'y' to confirm or 'n' to re-enter the location. The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not. **Tip:** Press Ctrl+C to exit the script at any time.	
6	The utility prompts you to enter the IP address of the target Logger. 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.	
7	The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not. 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. After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.	

Steps	On the Source Logger...	On the Target Logger...
8	The utility now prompts you to consider how you want to handle archive migration. **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. **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. **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 21 for more information. **Option 4: Archive migration.** The latest unarchived live data since the last daily archive execution on Logger Target will be migrated while the archives in Logger source will no longer be accessed. **Caution:** Make sure the daily archive is enabled prior the archive migration. Otherwise, Logger will automatically migrate the last daily archive job executed as it will not find any records of live data. Answer the following prompts in accordance with the migration option you select.	
9	The utility asks if you would like to migrate your archives only after the archive check passes. • 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. • Option 4: Enter 'n'. Continue to the next step.	
10	If you entered ‘n’, the utility asks you if you would like to migrate the archive configuration metadata even if some archives are missing. • 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	If you entered ‘n’, the utility asks you if you are sure you want to skip archive migration. • Option 3: Enter 'y'. Go to step "12" below. **Caution:** If you confirm this option, you will not be able to access any of your archives after the migration until you run the Archive Migration Utility. See "Migrating Event Archive Settings Separately" on page 21 for instructions. • Option 4: Enter 'y'. Go to step "12" below. **Caution:** If you confirm this option, you can only access the archives and the latest unarchived live data since the last automatic daily archive execution. All archives references will be removed on the source after the archive migration. **Note:** You can manually create archives. However, the live data will come from the last automatic daily archive execution. • If you entered ‘n’, the utility will ask you to confirm the Archive Migration. • 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	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.	

Steps	On the Source Logger...	On the Target Logger...

	The data migration utility starts to migrate the data.
	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.
	You can check the progress of the migration in
	`user/logger/dataMigrationSource.out`
	and:
	`user/logger/dataMigrationTarget.out`	

13	If the migration script completes successfully, the following messages are displayed on the source Logger.
	`source: Source box is done!`
	`source: Please make sure data migration has completed on the target logger before rebooting this logger.`
	Caution: Wait for both Loggers to complete this step before going on to the next step.
		If the migration script completes successfully, the following messages are displayed on the target Logger.
		`target: Data migration successfully completed!`
		`target: Please reboot target box!`
		Caution: Wait for both Loggers to complete this step before going on to the next step.

14	Reboot the Logger now or later, depending upon the event archiving choice you made in "8" on page 15. • 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. • Option 4: The event archive migration is complete. Reboot now.	Reboot the Logger now or later, depending upon the event archiving choice you made in "8" on page 15. • 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. • Option 4: The event archive migration is complete. Reboot now.

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 15:

- 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.
- Option 4: Complete these steps now.

Steps	On the Source Logger...	On the Target Logger...
Step 1		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 27 for more information.
Step 2	After reboot, reset the `ARCSIGHT_HOME` environment variable, as described in "5" on page 11. Enter this command to clean up the SSH files: `$ARCSIGHT_HOME/bin/scripts/dataMigrationSource_ssh_cleanup.sh`	After reboot, reset the `ARCSIGHT_HOME` environment variable, as described in "5" on page 11. Enter this command to clean up the SSH files: `$ARCSIGHT_HOME/bin/scripts/dataMigrationTarget_ssh_cleanup.sh`
Step 3	Create a gzip file of log files created during the data migration process. To do so, enter this command: `$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh` A file similar to `dataMigrationLog.2016-01-11PST164827.tar.gz` is created in the `ARCSIGHT_HOME` directory. Copy this new file to another location to preserve the log files.	Create a gzip file of log files created during the data migration process. To do so, enter this command: `$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh` A file similar to `dataMigrationLog.2016-01-11PST164827.tar.gz` is created in the `ARCSIGHT_HOME` directory. Copy this new file to another location to preserve the log files.

Steps	On the Source Logger...	On the Target Logger...
Step 4	Remove the original data migration utility files. To do so, enter this command: `rm -f $ARCSIGHT_HOME/datamigration*.tar.gz` **Note:** This may delete the gzip of the log files created in "Step 3" on the previous page. To preserve this file, copy it to another location.	Remove the original data migration utility files. To do so, enter this command: `rm -f $ARCSIGHT_HOME/datamigration*.tar.gz` **Note:** This may delete the gzip of the log files created in "Step 3" on the previous page. To preserve this file, copy it to another location.

Step 5 (conditional)		For non-root Software Logger installations, the migrated archives may no be accessible to the Target Logger due to permissions.
		To solve this issue, execute the following commands:
		1. Generate a list of the archive data files stored in the remote archive server:
		`ls -l <NFS Mount Point>`
		Where `<NFS Mount Point>` is the path in the Target Logger where the remote archive NFS server is mounted, for example `/opt/mnt/archives`.
		This list captures the current permissions and ownership. Save this list and have it handy (it might be needed in case of a rollback).
		2. Change the permissions of the archive files stored in the remote archive server in such a way that the new Target Logger - deployed as non-root - is able to access those files:
		`chmod 755 <NFS Mount point> -R`
		`chown 500:500 <NFS Mount Point> -R`
		Note: After the permissions change, the archives will no longer be accessible to the Source Logger. If for any reason the data migration must be rolled back, or if the migration gets aborted, the permissions must change back to their original value. Use the list obtained in step 1 of this procedure to restore archive access to the Source Logger.

Step 6 (conditi		To finish the process, undo the conditional command performed in step 1 of "Run the Data Migration Utility" on page 13.

Steps	On the Source Logger...	On the Target Logger...
onal)		On the Target Logger (logged in as root), run the following command to revert back to the original permissions: `chown arcsight:arcsight <LoggerInstallDir>/current/local/monit/watchdog/monitrc`

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 "8" on page 15 in "Run the Data Migration Utility" on page 13) . 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 28.

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 17 of Data Migration Between Loggers before starting archive migration.	
2	Enable SSH access to the appliance if it is not already enabled. • 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:

Steps	On the Source Logger...	On the Target Logger...
		• On the System Admin page, under System, click **SSH**. The SSH configuration page opens. Click **Enable**. On Software Loggers: • Verify that the system on which Logger is installed is reachable through SSH.

3	Copy datamigration-7.2-D1143.tar.gz to:
	`/opt/arcsight/logger`
	This is the Logger home directory, referred to by the Archive Migration utility as `ARCSIGHT_HOME`.
	On Software Loggers, use the directory path where it was installed. The default is:
	`/opt/current/arcsight/logger`
	This is the home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.
	Note: Skip this step if you did not remove the Data Migration files as described in "Finish the Data Migration" on page 17.
		Copy datamigration-7.2-D1143.tar.gz
		On Logger Appliances:
		`/opt/arcsight/logger`
		This is the Logger home directory, referred to by the Archive Migration utility as `ARCSIGHT_HOME`.
		On Software Loggers, use the directory path where it was installed. The default is:
		`/opt/current/arcsight/logger`
		This is the home directory, referred to by the Archive Migration utility as ARCSIGHT_HOME.
		Note: Skip this step if you did not remove the Data Migration files as described in "Finish the Data Migration" on page 17.

4	SSH to the Logger and log in as user "`root`."	SSH to the Logger and log in as user "`root`."

5	Set the ARCSIGHT_HOME environment variable, using the following command:
	`export ARCSIGHT_HOME=/opt/arcsight/logger`
	Note: Skip this step if you did not reset the ARCSIGHT_HOME environment variable and run the cleanup script in "Step 2" on page 18.
	To set the environment variable on Software Loggers, issue the following command:
	`export ARCSIGHT_HOME=<Logger_install_directory>/current/arcsight/logger`
	By default this is:
	`/opt/current/arcsight/Logger`
		Set the ARCSIGHT_HOME environment variable, using the following command:
		`export ARCSIGHT_HOME=/opt/arcsight/logger`
		Note: Skip this step if you did not reset the ARCSIGHT_ HOME environment variable and run the cleanup script in "Step 2" on page 18.
		To set the environment variable on Software Loggers, issue the following command:
		`export ARCSIGHT_HOME=<Logger_install_directory>/current/arcsight/logger`

Steps	On the Source Logger...	On the Target Logger...
		By default this is: `/opt/current/arcsight/Logger`
6	Enter this command to navigate to the Logger home directory: `cd $ARCSIGHT_HOME`	Enter this command to navigate to the Logger home directory: `cd $ARCSIGHT_HOME`

7	Enter this command to extract the compressed files:
	`tar xzvf datamigration*.tar.gz`
	Note: Skip this step if you did not run the cleanup script in "Step 2" on page 18.
		Run the following command:
		`mkdir/root/.ssh`
		Enter this command to extract the compressed files:
		`tar xzvf datamigration*.tar.gz`
		Note: Skip this step if you did not run the cleanup script in "Step 2" on page 18.

8	Enter this command to run the setup script: `bin/scripts/dataMigrationSource_ssh_setup.sh`	Enter this command to run the setup script: `bin/scripts/dataMigrationTarget_ssh_setup.sh`
9		The script prompts you to confirm the ARCSIGHT_HOME directory. Enter 'y' to confirm or 'n' to enter the location. If you entered 'n', the script prompts you to enter the correct ARCSIGHT_HOME directory. 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.
10		You are asked if this is an appliance. Enter 'y' if so. Enter 'n' if not.
11		Enter this command to run the Archive Migration utility: `bin/scripts/dataMigrationTarget_Archive_Only.sh` 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 username that was used when installing Logger.

Steps	On the Source Logger...	On the Target Logger...
		After you enter the username, the script prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the username.
12		A message telling you to run the Archive Migration utility on the source Logger is displayed. **Note:** Press Ctrl+C to exit the script at any time.
13	Enter this command to run the Archive Migration utility: `bin/scripts/dataMigrationSource_Archive_Only.sh`	
14	The utility prompts you to confirm the ARCSIGHT_HOME location. Enter 'y' to confirm or 'n' to re-enter the location. The utility asks you if this Logger is an appliance. Enter 'y' if so. Enter 'n' if not. **Tip:** Press Ctrl+C to exit the script at any time.	
15	The utility prompts you to enter the IP address of the target Logger. 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.	
16	The utility asks you if the target Logger is an appliance. Enter 'y' if so. Enter 'n' if not. 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. After you enter the directory, the utility prompts you to confirm it. Enter 'y' to confirm or 'n' to re-enter the location.	
17	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 archives separately."	
18	Otherwise, the utility prompts you to consider how you want to handle archive migration: **Option 1: Default archive migration:** The Archive Migration script fails and exits if the archive check fails. If the script exits because the archive check failed, restore the missing archives and run the script again. **Option 2: Ignore archive check:** Archive Migration continues	

Steps	On the Source Logger...	On the Target Logger...
	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. Answer the following prompts in accordance with the migration option you select.	
19	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. • Option 1: Enter 'y'. Go to "21" below. • Option 2: Enter 'n'. Continue to the next step.	
20	If you entered ‘n’, the utility asks you if you would like to migrate the archive configuration metadata even if some archives are missing. Enter ‘y’ and continue to the next step.	
21	The utility prompts you to confirm the settings. Enter ‘y’ to proceed or ‘n’ to enter the settings again.	
22	The utility asks if you want to migrate the event archive settings now. Enter ‘y’ to confirm or ‘n’ to exit without migrating the event archive settings.	

23	The Archive Migration utility starts to migrate the settings.
	
	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.
	
	Note: When you restart the utility, make sure that you start it on the target Logger first and then the source Logger.
	
	You can check the progress of the migration in:
	
	`user/Logger/dataMigrationSourceArchiveOnly.out`
	
	and:
	
	`user/Logger/dataMigrationTargetArchiveOnly.out`	

24	If the migration script completes successfully, the following messages are displayed on the source Logger.
	
	`source: Source box is done!`
	`source: Please make sure Archive Migration has completed on the target logger before rebooting this logger.`
	
	Caution: Wait for both Loggers to complete this step before going on to the next step.
		If the migration script completes successfully, the following messages are displayed on the target Logger.
		
		`target: Archive Migration successfully completed!`
		`target: Please reboot target box!`

Steps	On the Source Logger...	On the Target Logger...
		Caution: Wait for both Loggers to complete this step before going on to the next step.
25	Reboot the Logger.	Reboot the Logger Appliance or restart the Software Logger.
26		Configure the target Logger to make it match the source Logger. See "Migrating Data Between Loggers" on page 9 and "After the Migration" on the next page for more information. **Note:** Skip this step if you configured your Logger before performing the event archive migration, as described in "Step 1" on page 18.
27	After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 22. Enter this command to clean up the SSH files: `$ARCSIGHT_HOME/bin/scripts/dataMigrationSource_ssh_cleanup.sh`	After reboot, reset the ARCSIGHT_HOME environment variable, as described in "5" on page 22. Enter this command to clean up the SSH files: `$ARCSIGHT_HOME/bin/scripts/dataMigrationTarget_ssh_cleanup.sh`
28	Enter this command to create a gzip file of log files created during the migration process: `$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh` A file such as `dataMigrationLog.2016-01-11PST164827.tar.gz` is created in the `ARCSIGHT_HOME` directory.	Enter this command to create a gzip file of log files created during the migration process: `$ARCSIGHT_HOME/bin/scripts/dataMigrationClean.sh` A file such as `dataMigrationLog.2016-01-11PST164827.tar.gz` is created in the `ARCSIGHT_HOME` directory.
29	Enter this command to remove the original Data Migration utility files: `rm -f $ARCSIGHT_HOME/datamigration*.tar.gz` **Note:** This will delete the gzip of the log files created in "28" above. To preserve this file, copy it to another location.	Enter this command to remove the original Data Migration utility files: `rm -f $ARCSIGHT_HOME/datamigration*.tar.gz` **Note:** This will delete the gzip of the log files created in "28" above. To preserve this file, copy it to another location.

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:
   - Use the **Configuration Backup and Restore** feature, described in ArcSight Logger 7.3 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.
   - Use the **Content Import/Export** capability of Logger, described in ArcSight Logger 7.3 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.
   - 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. File receivers or folder follower receivers path are not migrated in the Logger target. Manually update the file receiver path or follower folder receiver with the proper path in the target. For instance, if you migrate from an appliance to a software logger, you must update the Apache URL Access Error Log receiver with the path `<logger_install_path>/userdata/logs/apache`.
5. All setting configurations in Logger Source (storage group settings and event archives) will be deleted after performing the archive migration. To get the daily archives, configure the archive storage settings once data migration is completed.

Troubleshooting

If the first data migration attempt fails, and the target Logger is an appliance, apply a Factory Restore procedure to the target Logger before retrying the data migration.

- 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 "11" on page 23.

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

- If the data migration process has failed in the target with the following error message:

  ```
  obsolete processes (dataMigrationDB or ftran) found, data migration failed
  ```

  Make sure to reboot the Logger target to terminate the processes appropriately.
- 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.
- The target Logger is stuck displaying either of these messages:

  ```
  waiting for data files copying from source box
  ```

  or

  ```
  Data file copy failed, retrying count: 11
  ```

  Check the `<ARCSIGHT_HOME>/user/dmc_ftran.log` file, and look for the following messages:

  ```
  Copying: Arcsight_Data_* unable to connect.
  ```

  If the file contains multiple instances of the message, this indicates that the `Ftran` client in the source Logger cannot establish a connection with the `Ftran` server in the target Logger. To bypass the use of `Ftran` entirely, and force the use of `Rsync` for the live data transfer instead (using port 22), apply the following steps:

a. (Conditional) If the target is an appliance, manually remove the pre-allocated data files in the target Logger using the following command:

```
rm -f /opt/data/logger/*
```

b. Follow the data migration procedure, and at step 4 of the Run the Data Migration Utility section, add the `-use_rsync` option when running the `dataMigrationSource.sh` script in the source Logger, like this:

```
bin/scripts/dataMigrationSource.sh -use_rsync
```

During execution, the data migration tool in the source Logger might stop printing messages for a while, since the `Rsync` process takes time to prepare internally before beginning the actual transfer of the files. This is normal, and does not indicate that the process has stopped.

c. (Optional) Reduce the `Rsync` transfer time and increase verbosity.

Open the following file on the source Logger with a text editor:

For Appliance:

```
/opt/arcsight/logger/bin/scripts/dataMigrationSource_fc_rsync.sh
```

For Software:

```
<LoggerInstallDirectory>/current/arcsight/logger/bin/scripts/dataMigrat
ionSource_fc_rsync.sh
```

Replace the following line:

```
/usr/bin/rsync -ac --out-format="[`/bin/date`] source: %n transfered
%''b" --delete-after -e "$SSH_OPTS" $SOURCE_DATAFILE_HOME/ $TARGET_
MACHINE:$TARGET_DATAFILE_HOME/ | grep 'Arcsight_Data_' | sed
s/deleting/"[`/bin/date`] source: Removing"/g
```

with this one:

```
/usr/bin/rsync -av --progress  --delete-after -e "$SSH_OPTS" $SOURCE_
DATAFILE_HOME/ $TARGET_MACHINE:$TARGET_DATAFILE_HOME/
```

This change will reduce the number of times `Rsync` calculates the checksum of all the data files from 2 to 1, speeding up the process. As well, the progress and transfer rate of the files will be detailed onscreen.

- The `DataMigrationSource.sh` script asks for the target Logger's password at every step.

  The target Logger's password should not be requested by the source Logger after running the `SSH` setup script, so this indicates that the script did not work properly. Follow these steps to remedy the issue:

a. Run this command on the source Logger:

```
ssh-keygen -R <Target Logger's IP>
```

b. Make sure that the `/root/.ssh` directory exists on the target Logger.

c. Run the `dataMigrationTarget_ssh_setup.sh` script on the target Logger before running the `dataMigrationSource_ssh_setup.sh` script on the source Logger.

d. If prompted, select to overwrite `/root/.ssh/id_rsa`.

e. Continue with the "Run the Data Migration Utility" on page 13 process.

- Trying to run a script returns a **not found** error:

```
/bin/scripts/<script name>.sh: No such file or directory
```

This is caused by the `ARCSIGHT_HOME` variable not having been set, or having been lost at the end of an SSH session. Just run the next command and try again.

For Appliances:

```
export ARCSIGHT_HOME=/opt/arcsight/logger
```

For Software:

```
export ARCSIGHT_HOME=<LoggerInstallDirectory>/current/arcsight/logger
```

- After an appliance-to-software data migration, the archives migrated from the source appliance cannot be loaded in the target software Logger because of the **Events are not in local storage** error.

Migrating the archives separately from a source appliance to a target software Logger using the `archive_only` script causes the remote archive settings to be migrated incorrectly. To fix the mount path in the software Logger, the values of the `mount` column from `alg_eventarchivemount` must be set to null with the following command:

```
<LoggerInstallDirectory>/current/arcsight/bin/psql rwdb web -c "update
alg_eventarchivemount set mount=null"
```

Restoring Archives

After migrating the archives to the Target Logger, the archive metadata can be restored using a configured and operating mount. By running the archive restore tool with the correspondent details (base or root installation of the Logger, mount name, archive path, archive IP), the mount path will be checked and the archives will be scanned and allocated to the storage group of your selection.

The restored archives will move to generated folders with the following prefix:

`External_Archive_IP_WHERE_ARCHIVES_COME_FROM_ $ OLD_STORAGE_GROUP`

However, corrupted or empty archives (XML without datafiles and CSV) will be moved to the folder with the prefix:

`Archive_Not_Imported_ $ IP_WHERE_ARCHIVES_COME_FROM`.

Prerequisites for restoring archives

Ensure that the following prerequisites are met before beginning the archive restore process.

- The mount point must be configured and set on the target Logger. Go to **System Admin > Remote File Systems** and fill the correspondent fields.
- Make sure an RFS mount contains the archives that you want to restore in the target Logger.

  You are responsible for moving the data from one mount to a new one.
- Setup the RFS mount on the Logger and make sure that the server is up and reachable.
- If no directory has been created, a directory will be created automatically.
- Go to the **Configuration > Storage > Archive Storage Settings** and make sure the storage group is related to a mount and archive path. Otherwise, the restored archives will be allocated to the file where the file was restored.

Archive Restore Tool

The archive metadata can be restored through a mount and a series of steps described in this section.

1. Confirm RFS mount on the Logger and make sure that the server is up and reachable.
2. From the `restoreArchive.sh`, run the archive restore tool:

```
./restoreArchive.sh INSTALL_DIR_PATH [Logger directory path] ARCHIVE_MOUNT
[mount name] ARCHIVE_FOLDER [archive folder name]IP_WHERE_ARCHIVES_COME_
FROM [source IP]"
```

3. The archive restore will confirm the data. Type `[Y/N]` as needed.
4. Relate the restore archive folder to the available storage group.
5. Go to the **Configuration > Storage > Archive Storage Settings**. The restored archives will be labeled as **External Logger Archive**.
6. Try to load, sanitize and unload the restored archives.

Publication Status

Released: May 31, 2023

Updated: Wednesday, October 25, 2023

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 7.3)

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 documentation-feedback@microfocus.com.

We appreciate your feedback!