Micro Focus Security ArcSight ESM

Software Version: 7.0 Patch 1

Checklist: Installing and Configuring ESM with Distributed Correlation

Document Release Date: August 16, 2018

Software Release Date: August 16, 2018

MICRO FOCUS®

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

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.

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

Node Installation

This document applies to the installation of ESM with Distributed Correlation, containing a cluster of nodes.

Purpose:

The purpose of this document is to aid you in tracking the progress of your installation and configuration tasks at a high level. This document does not provide details. You are expected to refer to the main user's guides for specific steps and command syntax as needed.

The example uses the most basic cluster, called **Small Configuration** in the installation guide. Feel free to expand based on your needs.

Requirements:

You must have planned your cluster environment and completed all system prerequisites as documented. You will need:

- *ESM Installation Guide*
- *ESM Administrator's Guide*

Scenarios:

This checklist assumes a basic distributed correlation cluster consisting of **3** nodes:

- **Node 1:** Is the persistor (Manager is installed here) node. It contains one message bus control, and one repository service.
- **Node 2:** Contains one correlator, one aggregator, one message bus control, one message bus data, and one repository service.
- **Node 3:** Contains one correlator, one aggregator, one message bus control, one message bus data, and one repository service.

Node 1, the Persistor Node

Node 1 Tasks

Step #	Task	Done
1	See the *ESM Installation Guide*. Complete all system requirements and cluster planning. **Topics in Chapter 3, Installing Software ESM:** Preparing to Install, Starting the Installer, Using the Configuration Wizard in Distributed Correlation Mode > Persistor Node Installation	☐
2	Follow instructions to download the ESM installation package and then prepare the system. Note the required open ports.	☐
3	Run the installer: Console or GUI mode, your choice, and reply to the initial prompts, such as license agreement acceptance, and so on. Refer to the guide for specific settings. Continue through the configuration prompts until you see the dialog for Installation Mode.	☐
4	Enter settings relevant to distributed correlation: • Installation mode = **Distributed** • Cluster setup = **Starting a new cluster** **Note:** For `Starting a new cluster`, the Wizard follows a different logical path as opposed to `Add to existing` cluster, so make sure you're picking the correct option here. • ESM server ports = Refer to the installation guide for guidelines on lowest and highest	☐
5	Enter the **Certificate Administrator Password** Record the password here, you will use this information later for setting up the other nodes: _____ Refer to the *ESM Administrator's Guide* later for information on the `certadmin` command.	☐
6	Continue with the steps to configure ESM for CORR-Engine password, storage, notifications, and so on. Enter host information in the **Manager Information** dialog. Record the **server hostname or IP address** here, you will need this information later to identify this persistor on this node to the other nodes. _____ Continue till you see the Selection of Services dialog, which refer to distributed correlation services.	☐
7	In **Selection of Services**, do not select any of the presented the options, since you are only installing the persistor service on Node 1.	☐

Node 1 Tasks, continued

Step #	Task	Done
8	Complete the configuration on Node 1 and notice the reminder to set up required services. Exit.	☐
9	Complete the final step in the install guide to log in as **root** and run the `setup_services.sh` command. This sets up the installed services in Node 1. At the end of Node 1 installation, it is automatically configured with the repository service, and this service is available. **Note:** Not all services will be available or cannot be started at this time until the entire cluster has been configured.	☐
10	Proceed with Node 2 installation and configuration.	☐

Node 2, One Correlator and One Aggregator

The message bus and repository service on this node are installed later as part of Concluding Tasks.

Node 2 Tasks

Step #	Task	Done
1	See the *ESM Installation Guide*. Complete all system requirements. **Topics in Chapter 3, Installing Software ESM:** Preparing to Install, Starting the Installer, Using the Configuration Wizard in Distributed Correlation Mode > Add Nodes to a Cluster - Further Node Installation, Post Cluster Creation Configuration	☐
2	Follow instructions in the installation guide to download the ESM installation package and then prepare the system. Note the required open ports.	☐
3	Run the installer: Console or GUI mode, your choice, and reply to the initial prompts, such as license agreement acceptance, and so on. Refer to the guide for specific settings. Continue through the configuration prompts until you see the dialog for Installation Mode.	☐
4	Enter settings relevant to distributed correlation: Installation mode = **Distributed** Cluster setup = **Adding to an existing cluster**	☐
5	Enter persistor (Node 1) **IP address or hostname**, whatever you used to configure Node 1, as the location of the persistor.	☐

Node 2 Tasks, continued

Step #	Task	Done
6	In the Selection of Services dialog: **Correlation** **Related options:** Service type = **correlator** Configuration type = **Add/configure an instance** **Add new instance**, then name this correlator service: _____ **Host name** of the server for Node 2 (this node): _____	☐
7	Configure additional settings, such as Java heap memory, your preferred key pair certificate options, SSL keystore password, and so on, as applicable. Continue until your correlator instance is saved.	☐
8	Select another service type. Service type = **aggregator** Configuration type = **Add/configure an instance** Select **Add new instance**, then name this aggregator service: _____ **Host name** of the server for Node 2 (this node): _____	☐
9	Because you have set up in a previous step, keep settings for Java heap memory. For preferred key pair certificate options, choose **Do not change anything**.	☐
10	Continue until your aggregator instance is saved. Choose **I am done with my changes.**	☐
11	Complete the final step in the install guide to log in as **root** and run the setup_services.sh command. This sets up the installed services in Node 2. You are done with Node 2. At this time, the aggregator and correlator services are installed but not yet started. Proceed with Node 3 installation.	☐

Node 3, One Correlator and One Aggregator

The message bus and repository service on this node are installed later as part of Concluding Tasks.

Node 3 Tasks

Step #	Task	Done
1	See the *ESM Installation Guide*. Complete all system requirements. **Topics in Chapter 3, Installing Software ESM:** Preparing to Install, Starting the Installer, Using the Configuration Wizard in Distributed Correlation Mode > Add Nodes to a Cluster - Further Node Installation, Post Cluster Creation Configuration	☐
2	Follow instructions in the installation guide to download the ESM installation package and then prepare the system. Note the required open ports.	☐
3	Run the installer: Console or GUI mode, your choice, and reply to the initial prompts, such as license agreement acceptance, and so on. Refer to the guide for specific settings. Continue through the configuration prompts until you see the dialog for Installation Mode.	☐
4	Enter settings relevant to distributed correlation: Installation mode = **Distributed** Cluster setup = **Adding to an existing cluster**	☐
5	Enter persistor (Node 1) **IP address or hostname**, whatever you used to configure Node 1, as the location of the persistor	☐
6	In the Selection of Services dialog: **Correlation** **Related options:** Service type = **correlator** Configuration type = **Add/configure an instance** **Add new instance**, then name this correlator service: _____ **Host name** of the server for Node 3 (this node): _____	☐
7	Configure additional settings, such as Java heap memory, your preferred key pair certificate options, SSL keystore password, and so on, as applicable. Continue until your correlator instance is saved.	☐
8	Select another service type. Service type = **aggregator** Configuration type = **Add/configure an instance** Select **Add new instance**, then name this aggregator service: _____ **Host name** of the server for Node 3 (this node): _____	☐

Node 3 Tasks, continued

Step #	Task	Done
9	Because you have set up in a previous step, keep settings for Java heap memory. For preferred key pair certificate options, choose **Do not change anything**.	☐
10	Continue until your aggregator instance is saved. Choose **I am done with my changes.**	☐
11	Complete the final step in the install guide to log in as **root** and run the `setup_services.sh` command. This sets up the installed services in Node 3. You are done with Node 3. At this time, the aggregator and correlator services are installed but not yet started. Proceed with Concluding Tasks.	☐

Concluding Tasks, Node 1 Only: Message Bus Controller and Repository Services

At this stage, you should now be able to see the configured services in all the nodes in the cluster with the `arcsight_services status` command. Refer to the *Administrator's Guide* for details on this command.

You perform the remaining configurations from the persistor node (Node 1), which are then applied to the entire cluster.

Concluding tasks in Node 1

Step #	Task	Done
1	Make sure the *ESM Installation Guide* and *ESM Administrator's Guide* are available. **Install guide topics in Chapter 3:** Post Cluster Creation Configuration, Setting Up Key-Based Passwordless SSH - Distributed Correlation Mode Only **Admin guide topics:** Configuring and Managing Distributed Correlation and all subtopics.	☐
2	Follow the steps in the install guide to set up **passwordless SSH** in the cluster with the `arcsight_services sshSetup` command. In the *Installation Guide*, see the topics on Post Cluster Creation Configuration, Setting Up Key-Based Passwordless SSH - Distributed Correlation Mode Only. See also the *ESM Administrator's Guide*, topic on "ESM ArcSight Commands," for details on the `arcsight_services` command.	☐

Concluding tasks in Node 1, continued

Step #	Task	Done
3	Use /opt/arcsight/manager/bin/arcsight certadmin -approveall to approve all certificates on the nodes. See the *ESM Installation Guide*. **Note:** Use the password configured for the certificate administrator during Node 1 (persistor) installation. See also the *ESM Administrator's Guide*, topic on "ESM ArcSight Commands," for details on the certadmin command.	☐
4	Make sure all services are stopped, except the repo service. Follow instructions in the *ESM Administrator's Guide*, topic on Configuring Services in a Distributed Correlation Cluster > Configuring Message Bus Control and Message Bus Data: Configure **Message Bus (mbus) services** with the arcsight mbussetup command. Choose **I want to add, delete, or change Message Bus instances** Specify the number of mbus_data and mbus_control instances in each node on the cluster. The nodes are identified by their host names. See the cluster guidelines in the *ESM Installation Guide*.	☐
5	Make sure all services are stopped, except the repo service. Follow instructions in the *ESM Administrator's Guide*, topic on Configuring Services in a Distributed Correlation Cluster > Configuring a Repository: Configure **Repository (repo) services** with the arcsight reposetup command. Choose **Change the list of information Repository instances**. The host where the repo instance is running is marked with an asterisk and pre-selected. Specify the remaining unselected repo hosts to provide redundant services to the cluster.	☐
6	Exit the configuration and start all services with /etc.init.d/arcsight_services start all Verify that all services are running with /etc/init.d/arcsight_services status or /etc/init.d/arcsight_services statusByNode	☐
7	This completes the installation of ESM Manager configured with Distributed Correlation. Try accessing the ArcSight Command Center from a client, or continue with ArcSight Console installation and access the Manager from the Console.	☐

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 Checklist: Installing and Configuring ESM with Distributed Correlation (ESM 7.0 Patch 1)

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!