Micro Focus Security ArcSight ESM

Software Version: 7.4

SSL/TLS Key Pairs on ESM Distributed Nodes

Document Release Date: November 2020
Software Release Date: November 2020

Legal Notices

Copyright Notice

Trademark Notices

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

SSL/TLS Key Pairs on ESM Distributed Nodes

Overview

This document describes the SSL/TLS key pairs that distributed correlation nodes use for inter-node communication within an ESM cluster.

Prerequisites

This document applies only to ESM 7.0 and later in distributed mode.

Prior to using this document, review the following documentation:

- *ESM 101*
- *ESM Installation Guide*
- *ESM Administrator's Guide*
  - *Chapter 3: Configuring and Managing Distributed Correlation*
  - *Chapter 4: SSL Authentication*

Cluster Node Client Key

Correlators and Aggregators connect to the ESM Manager as SSL clients, with the ESM Manager acting as an SSL server. This communication is secured using a key pair dedicated for this purpose. The private key is stored in the client keystore on the distributed node where the Correlator or Aggregator is running. All of the Correlators and Aggregators on a given node share the same key.

The private key uses the alias `myclusternodeclientkey`.

To examine the contents of this keystore, open an ssh client to one of the **distributed nodes** in your cluster and execute the following commands:

```
cd /opt/arcsight/manager/bin
./arcsight keytool -store clientkeys -list -alias myclusternodeclientkey
```

The output should contain something like this:

```
myclusternodeclientkey, Oct 22, 2019, PrivateKeyEntry,
Certificate fingerprint (SHA1):
41:2A:41:47:F6:FA:BF:9D:58:47:D4:30:00:36:9D:62:44:C0:B4:EF
```

To view more details about the private key, you can add the option `-v` to the command. The output with this option might look like this:

SSL/TLS Key Pairs on ESM Distributed Nodes

```
Alias name: myclusternodeclientkey
Creation date: Oct 22, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=arcsightclusteruser, OU=ArcSight, O=MicroFocus, L=Sunnyvale, ST=CA,
C=US
Issuer: CN=arcsightclusteruser, OU=ArcSight, O=MicroFocus, L=Sunnyvale,
ST=CA, C=US
Serial number: 20000016df735a367
Valid from: Mon Oct 21 23:02:30 PDT 2019 until: Tue Oct 22 23:02:30 PDT 2024
Certificate fingerprints:

MD5: 3E:55:76:F2:E6:28:57:71:05:B4:52:98:35:BC:7D:07
SHA1: 41:2A:41:47:F6:FA:BF:9D:58:47:D4:30:00:36:9D:62:44:C0:B4:EF
SHA256:
A4:61:23:B8:A2:A7:76:78:24:40:41:46:F9:B0:C4:92:5F:97:05:F9:9B:5F:EE:D7:B8:0A
:F0:50:05:95:34:7C

Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Note: The actual file in which the key is stored depends on whether you are using ESM in FIPS mode or not. The keytool command and options are the same. The option `-store clientkeys` is an alias that resolves to the correct keystore file based on your configuration (FIPS or non-FIPS).

Cluster Node SSL Certificate

The private key is half of the key pair. For it to be useful, other processes must trust the associated SSL certificate. To do this, share the SSL certificate containing the public key with other parts of the ESM cluster.

To use this key to communicate with the ESM Manager, the associated SSL certificate must exist in the ESM Manager SSL truststore. This occurs as part of the installation process. Installing a distributed correlation node generates the key pair and uploads the associated SSL certificate to the ESM Information Repository (Repo).

Note: Only the public certificate is uploaded. The private key is not copied anywhere.

Use the arcsight certadmin tool to examine and approve all uploaded certificates. Only approved certificates are copied to the various truststores of the ESM cluster.

To see the certificate associated with the above private key in the truststore of the ESM Manager, open an ssh client to the **ESM Manager** host and run the following command:

SSL/TLS Key Pairs on ESM Distributed Nodes

```
cd /opt/arcsight/manager/bin
./arcsight keytool -store managercerts -list
```

This lists all currently trusted certificates for clients. The alias for cluster node client certificates begins with `esm-client-`, followed by the distributed node host name and a timestamp.

Note: You can positively identify the certificate by comparing the certificate fingerprint with the fingerprint of the private key, but the alias `esm-client-<host name>-<timestamp>` is usually enough to locate a particular certificate.

The ESM Manager truststore should contain a client certificate for all distributed correlation nodes in the cluster. For example, the ESM Manager truststore in this case might contain the following:

```
esm-client-hostname5-20191022.230230, Oct 23, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
41:2A:41:47:F6:FA:BF:9D:58:47:D4:30:00:36:9D:62:44:C0:B4:EF
esm-client-hostname2-20191022.230501, Oct 23, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
A8:E8:67:83:06:04:5B:8B:53:19:53:AA:48:B7:8F:BD:B4:3E:1B:00
esm-client-hostname4-20191022.230324, Oct 23, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
A8:39:14:1D:40:F2:06:52:F7:EB:80:54:C1:AF:33:8D:70:62:A0:58
esm-client-hostname3-20191022.230409, Oct 23, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
0F:C4:E5:13:D3:18:BA:E4:E9:98:FB:26:98:4D:56:E0:17:76:3D:36
```

Note that the SHA1 fingerprint of the first certificate matches the SHA1 fingerprint of the private key from `hostname5`.

You can examine the details of any certificate using the `-v` option of the keytool command:

```
./arcsight keytool -store managercerts -list -alias esm-client-hostname5-
20191022.230230 -v
```

Note: The `-alias` option is optional and limist the output to just one certificate. Without it, you see the details of all certificates in the truststore. You can pipe the output to a command such as `less` to scroll through the output.

The certificate details might appear as follows:

```
Alias name: esm-client-hostname5-20191022.230230
Creation date: Oct 23, 2019
Entry type: trustedCertEntry

Owner: CN=arcsightclusteruser, OU=ArcSight, O=MicroFocus, L=Sunnyvale, ST=CA,
```

SSL/TLS Key Pairs on ESM Distributed Nodes

```
C=US
Issuer: CN=arcsightclusteruser, OU=ArcSight, O=MicroFocus, L=Sunnyvale,
ST=CA, C=US
Serial number: 20000016df735a367
Valid from: Mon Oct 21 23:02:30 PDT 2019 until: Tue Oct 22 23:02:30 PDT 2024
Certificate fingerprints:

MD5: 3E:55:76:F2:E6:28:57:71:05:B4:52:98:35:BC:7D:07
SHA1: 41:2A:41:47:F6:FA:BF:9D:58:47:D4:30:00:36:9D:62:44:C0:B4:EF
SHA256:
A4:61:23:B8:A2:A7:76:78:24:40:41:46:F9:B0:C4:92:5F:97:05:F9:9B:5F:EE:D7:B8:0A
:F0:50:05:95:34:7C

Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Manually Replacing the Cluster Node Client Certificate

You should not need to replace the cluster node client certificate, but some organizations have a policy requiring all SSL certificates to be signed by a Certificate Authority (CA).

A CA-signed certificate is no more secure than the self-signed certificate the cluster node normally uses. A cluster node only connects to one SSL server, the ESM Manager, and that SSL server has an explicit trust relationship with each cluster node by virtue of keeping a copy of each certificate.

If your organization requires a CA-signed certificate, use the following procedures to replace the self-signed certificate with a CA-signed certificate.

Generate Certificate Signing Requests

Open an ssh client to each distributed correlation node in turn and generate a certificate signing request as follows:

```
cd /opt/arcsight/manager/bin

./arcsight keytool -store clientkeys -alias myclusternodeclientkey -certreq -
file /<full working directory to>/<your filename>.csr
```

This does not generate a new key-pair for each node, as the certificate owner information (CN=arcsightclusteruser) needs to stay the same to guarantee communication with the Persistor node.

SSL/TLS Key Pairs on ESM Distributed Nodes

You must do this for each distributed node. Send all of the `.csr` files to your chosen CA. The CA uses its private key to electronically sign and replies with a certification response that contains the signed certificate (a file with a `.cer` or `.crt` file extension).

(Conditional) If the extension is something other than `.cer` or `.crt`, use a text editor to copy and paste the encoded certificate to a separate file. The encoded certificate looks like this:

```
-----BEGIN CERTIFICATE-----
MIICjTCCAfagAwIBAgIDWnWvMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJaQTEiMCAGA1UEC
BMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMUVGhhd3RlIENlcnRpZmljYXRpb2
4xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4
XDTAyMDkyNzIzMzI0MVoXDTAyMTAxODIZMzI0MVowaDELMAkGA1UEBhMCrVMxDTALBgNVBAgTBGJs
YWgxDTALBgNVBAcTBGJsYWgxDTALBgNVBAoTBGJsYWgxDTALBgNVBAsTBGJsYWgxHTAbBgNVBAMTF
HppZXIuc3YuYXJjc2lnaHQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b
+BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vwN4JViC
CSBkDpiqVF7K11Sx4ZVSXX4+VQ6k4gT5G0kDNvQeN05wWkzEMygMB+ZBnYqPA/XtWRZtjxvH
MoqS+JEqHruiMLITC6q0reUB/txby6+S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHSUEDDAKBggrB
gEFBQcDATAMBgNVHRMBAg8EAjAAMA0GCSqGSIb3DQEBBAUAA4GBAFY37E60+P4b3zTLnaG7EVM57G
tkED6PwCIilB6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQVQxnpABjzTalRfYgjNFJ6ltI6ZKjBO5kim
9UBeCnKiNNzhIyDyFwbHXOPB/JaLIV+jGugYNS7hf/ay0BXKlfueO07EgjhhB/mQFs2JB
-----END CERTIFICATE-----
```

Ensure the following:

- Include the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`
- There are no extra spaces before or after the string

Once you have all of the CA-signed certificates, import them to the client keystore on each distributed node.

Stop the ESM Cluster

(Conditional) If you have not already done so, stop the ESM cluster at this point using the command `/etc/init.d/arcsight_services stop` from the Persistor node.

Backing Up Client Keystores and Truststores

Note: Before proceeding to the next step, take a backup copy of the client keystore and truststore on each node.

The exact files to copy depends on whether you are using FIPS mode or not. You can positively identify the file by looking at the output of the keytool command when using the options `-store clientkeys` and `-store clientcerts`. For example:

```
./arcsight keytool -store clientkeys -list
Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/manager/jre
```

SSL/TLS Key Pairs on ESM Distributed Nodes

```
ArcSight Keytool Wrapper starting...

ArcSight Keytool Wrapper 7.0.0.2605.2
keytool -list -alias myclusternodeclientkey -keystore
/opt/arcsight/manager/config/keystore.client.bcfks -storetype BCFKS -
storepass ******** -keypass ********
...
```

Note: The line `-keystore /opt/arcsight/manager/config/keystore.client.bcfks` is the client keystore in this example. Note your client keystore and copy that file to a safe location in case you need to restore it.

Run the command again with the option `-store clientcerts`.

```
./arcsight keytool -store clientcerts -list
Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/manager/jre

ArcSight Keytool Wrapper starting...

ArcSight Keytool Wrapper 7.0.0.2605.2
keytool -list -keystore /opt/arcsight/manager/config/keystore.client.bcfks -
storetype BCFKS -storepass ******** -keypass ********
Keystore type: BCFKS
Keystore provider: BCFIPS...
```

Note: The line `-keystore /opt/arcsight/manager/config/keystore.client.bcfks` is the client truststore. In this example, it is the same as the client keystore because the system is configured for FIPS mode. It might be a different file in your environment. Note the truststore file and copy that file to a safe location in case you need to restore it.

Import CA-Signed Certificates into Client Keystores

Import the CA-signed certificate for each cluster node into the client keystore on each node. Open an ssh client to each cluster node and execute the following command:

```
./arcsight keytool -store clientkeys -alias myclusternodeclientkey -
importcert -file /<full working directory to>/<your client certificate file>
```

Ensure you import the correct certificate into each keystore. Each node uses a different certificate.

Import CA Root and Intermediate Certificates to Cluster Node Client Truststores

The CA provides a procedure for downloading their root certificate and/or intermediate certificates. Import each of these into the client truststore.

SSL/TLS Key Pairs on ESM Distributed Nodes

Open an ssh client to each cluster node and execute the following command for each root and intermediate certificate:

```
./arcsight -store clientcerts -importcert -file /<full working directory
to>/<CA certificate file> -alias <alias name>
```

The `<alias name>` can be any string you wish to use as long as it is not the same as other aliases in the truststore.

Back Up the ESM Manager Truststore

Open an ssh client to the ESM Manager host. Take a backup copy of the ESM Manager truststore in case you need to restore it. You can positively identify the truststore file using the keytool command with the option `-store managercerts`. For example:

```
./arcsight keytool -store managercerts -list

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/manager/jre

ArcSight Keytool Wrapper starting...

ArcSight Keytool Wrapper 7.0.0.2605.2
keytool -list -keystore /opt/arcsight/manager/config/jetty/keystore.bcfks -
storetype BCFKS -storepass ******** -keypass ********
Keystore type: BCFKS
Keystore provider: BCFIPS

Your keystore contains 5 entries
...
```

Note: The line `-keystore /opt/arcsight/manager/config/jetty/keystore.bcfks` is the manager keystore in this example. Note your manager keystore and copy that file to a safe location in case you need to restore it.

Import CA Root and Intermediate Certificates to ESM Manager Truststore

The CA provides a procedure for downloading their root certificate and/or intermediate certificates. You must import each of these into the ESM Manager truststore before the newly signed cluster node certificates will be trusted.

For each CA root and intermediate certificate, execute the following command:

```
./arcsight -store managercerts -importcert -file /<full working directory
to>/<CA certificate file> -alias <alias name>
```

SSL/TLS Key Pairs on ESM Distributed Nodes

The `<alias name>` can be any string you wish to use as long as it is not the same as other aliases in the truststore.

Restart the ESM cluster to start using these new certificates.

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 SSL/TLS Key Pairs on ESM Distributed Nodes (ESM 7.4)

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!