SUPPORT NOTICE
Intel® Enterprise Edition for Lustre* Software
High Performance Data Division

Intel® Manager for Lustre* Software
Generating new certificates using SHA-256 encryption

March 16, 2017

Overview

The Intel® Manager for Lustre* Software is made up of many components which work together to manage a Lustre file system. These components rely on certificates to establish a handshake when communicating between nodes. It is important that the certificates are generated using a strong encryption algorithm. If the certificate is generated with a weak algorithm, the system is vulnerable to collision attacks. This link provides additional reference: (https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html)

Intel® Manager for Lustre* Software currently uses a SHA-1 encryption algorithm to generate certificates. Both Firefox and Google Chrome are in the process of sunsetting support for SHA-1 encryption, and blocking users from accessing sites that rely on certificates that were generated using this type of encryption:

- https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html
- https://blog.mozilla.org/security/2017/02/23/the-end-of-sha-1-on-the-public-web/

Regenerating certificates using a stronger encryption algorithm (SHA-256) is required to prevent interruption of the monitoring and management functions of the Intel® Manager for Lustre* Software for your file system(s). File systems that are not being managed or monitored by Intel® Manager for Lustre* Software are unaffected.

Intel has provided a script that will automatically regenerate new certificates using SHA-256 encryption on your manager node, and on all Lustre servers associated with it. Running this script will upgrade your certificates to the stronger encryption algorithm and ensure that any Lustre file system monitored/managed by Intel® Manager for Lustre* Software will remain accessible.

Determine your current encryption standard

Before migrating to SHA-256, let's first check that it is not already in use. Perform the following steps:

1. ssh into the manager node.
2. Run the following command:

```
 openssl x509 -noout -text -in /var/lib/chroma/<file>.crt | grep
"Signature Algorithm”
```

This command will print out the signature algorithm being used (sha-1 or sha-256). If the output contains “sha1” in the text, an update is required. There may be more than one file in the /var/lib/chroma directory, so check both. The following example shows the output for a server that is vulnerable:

```
[root@ct7-adm ~]# for i in /var/lib/chroma/*.crt; do
> openssl x509 -noout -text -in $i | grep  "Signature Algorithm"
> done
    Signature Algorithm: sha1WithRSAEncryption
    Signature Algorithm: sha1WithRSAEncryption
    Signature Algorithm: sha1WithRSAEncryption
    Signature Algorithm: sha1WithRSAEncryption
```

Generate certificates using SHA-256 encryption

The script will first generate a certificate on your manager node. Then the script will determine all of the servers that Intel® Manager for Lustre* Software currently monitors or manages, regenerate their certificates, restart the agent on each server, and finally, restart the manager node.

Running the script is simple. Enter the followng commands:

1. Users of Intel* EE for Lustre* Software, version 2.4.x, enter:
   ```
   scp sha-256-browser-migration-2.4.x.v1.tar.gz
   root@my_manager_domain.com:~
   ```
2. Users of Intel* EE for Lustre* Software, version 3.x.x,, enter:
   ```
   scp sha-256-browser-migration- 3.x.x.v1.tar.gz
   root@my_manager_domain.com:~
   ```
3. ssh into the node running the Intel® Manager for Lustre* Software Dashboard.
4. Enter: `cd sha-256-migration`
5. Enter: `./main`

Following is example out:

```
[root@lotus-30vm13 sha]# ./main

/usr/lib/python2.6/site-packages/kombu/utils/__init__.py:407: UserWarning:
Module scripts was already imported from /usr/share/chroma-
manager/scripts/__init__.pyc, but /usr/lib/python2.6/site-packages is being
added to sys.path

  from pkg_resources import iter_entry_points


Creating manager certificates:

    - Backing up certificates and pem files to
/var/lib/chroma/backup_1489176035

    - Generated Private Key: /var/lib/chroma/authority.pem

    - Created Authority Certificate using sha256:
/var/lib/chroma/authority.crt

    - Generated Private Key: /var/lib/chroma/manager.pem

    - Created Manager Certificate using sha256: /var/lib/chroma/manager.crt

    - Updating /usr/share/chroma-
manager/chroma_core/services/http_agent/crypto.py on manager node.

    - Updating /usr/share/chroma-manager/chroma_agent_comms/views.py on
manager node.


Migrating certificates to lotus-30vm15:

    - Backing up certificates on lotus-30vm15

    - Uploading /var/lib/chroma/authority.crt to lotus-
30vm15:/var/lib/chroma/authority.crt

    - Generating private key on lotus-30vm15

    - Creating new certificate on lotus-30vm15

    - Restarting Agent on lotus-30vm15


Migrating certificates to lotus-30vm16:

    - Backing up certificates on lotus-30vm16

    - Uploading /var/lib/chroma/authority.crt to lotus-
30vm16:/var/lib/chroma/authority.crt

    - Generating private key on lotus-30vm16

    - Creating new certificate on lotus-30vm16

    - Restarting Agent on lotus-30vm16


Migrating certificates to lotus-30vm17:

    - Backing up certificates on lotus-30vm17
    - Uploading /var/lib/chroma/authority.crt to lotus-
30vm17:/var/lib/chroma/authority.crt
    - Generating private key on lotus-30vm17
    - Creating new certificate on lotus-30vm17
    - Restarting Agent on lotus-30vm17

Restarting Manager:
Stopping daemons
Starting daemons
```

At this point, the customer can run the following command to verify that their certificate has been updated:

```
openssl x509 -noout -text -in /var/lib/chroma/manager.crt | grep "Signature
Algorithm"
```

The process is complete.

Disclaimer

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.

Copies of documents referenced in this document, or other Intel® literature, may be obtained by calling 1-800-548-4725, or visiting: http://www.intel.com/design/literature.htm.

Intel® and the Intel® logo are trademarks of Intel® Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.