Registration troubleshooting

After Initializing the enclave like so:

```

Copy SCRT_ENCLAVE_DIR=/usr/libsecretdinit-enclave

```

(orSCRT_ENCLAVE_DIR=/usr/lib secretd init-enclave | grep -Po 'isvEnclaveQuoteStatus":".+?"')

An outtput like this should be generated:

```

Copy INFO [wasmi_runtime_enclave::registration::attestation] Attestation report: {"id":"183845695958032083367610248637243990718","timestamp":"2020-07-12T09:43:12.297820","version":4,"advisoryURL":"https://security-center.intel.com","advisoryIDs":["INTEL-SA-00334"],"isvEnclaveQuoteStatus":"SW_HARDENING_NEEDED","isvEnclaveQuoteBody":"AgAAAMYLAAALAAoAAAAAABf93MlHcUSizYTifNzpi+QD9Lqdmd+k62/B9e4nOc4sDw8DBf+ABgAAAAAAAA

```

(orisvEnclaveQuoteStatus":"SW_HARDENING_NEEDED")

Where the important fields areisvEnclaveQuoteStatus andadvisoryIDs . This is are fields that mark the trust level of our platform. The acceptable values for theisvEnclaveQuoteStatus field are:

- OK
- SW_HARDENING_NEEDED
-

With the following value accepted fortestnet only :

- GROUP_OUT_OF_DATE
-

For the statusCONFIGURATION_AND_SW_HARDENING_NEEDED we perform a deeper inspection of the exact vulnerabilities that remain. The acceptable valuesfor mainnet are:

- "INTEL-SA-00334"
- "INTEL-SA-00219"
-

Consult with theIntel API for more on these values.

If you do not see such an output, look for a file calledattestation_cert.der which should have been created in yourHOME directory. You can then use the commandsecretd parse to check the result a successful result should be a 64 byte hex string (e.g.0x9efe0dc689447514d6514c05d1161cea15c461c62e6d72a2efabcc6b85ed953b .

What to do if this didn't work?

1. Runningsecretd init-enclave
2. should have created a file calledattestation_cert.der
3. . This file contains the attestation report from above.
4. Contact us on the proper channels onscrt.network/discord
5. The details we will need to investigate will include:
6.
    - Hardware specs
7.
    - SGX PSW/driver versions
8.
    - BIOS versions
9.
    - The fileattestation_cert.der
10. *
11.

Troubleshooting

Output is:

```

Copy secretd init-enclave 2020-07-12 13:21:31,864 ERROR [go_cosmwasm] Error :( ERROR: failed to initialize enclave: Error calling the VM: SGX_ERROR_ENCLAVE_FILE_ACCESS

```

Make sure you have the environment variableSCRT_ENCLAVE_DIR=/usr/lib set before you runsecretd .

Output is:

```

Copy secretd init-enclave ERROR [wasmi_runtime_enclave::crypto::key_manager] Error sealing registration key ERROR [wasmi_runtime_enclave::registration::offchain] Failed to create registration key 2020-07-12 13:37:26,690 ERROR [go_cosmwasm] Error :( ERROR: failed to initialize enclave: Error calling the VM: SGX_ERROR_UNEXPECTED

```

Make sure the directory~/.sgx_secrets/ is created. If that still doesn't work, try to create/root/.sgx_secrets

Output is:

```

Copy secretd init-enclave ERROR [wasmi_runtime_enclave::registration::attestation] Error in create_attestation_report: SGX_ERROR_SERVICE_UNAVAILABLE ERROR [wasmi_runtime_enclave::registration::offchain] Error in create_attestation_certificate: SGX_ERROR_SERVICE_UNAVAILABLE ERROR: failed to create attestation report: Error calling the VM: SGX_ERROR_SERVICE_UNAVAILABLE

```

Make sure theaesmd-service is runningsystemctl status aesmd.service

Output is:

```

Copy secretd init-enclave Creating new enclave registration key 2021-07-27 02:37:24,017 INFO [cosmwasm_sgx_vm::seed] Initializing enclave.. 2021-07-27 02:37:25,962 INFO [cosmwasm_sgx_vm::seed] Initialized enclave successfully! ERROR [wasmi_runtime_enclave::registration::cert] Platform is updated but requires further BIOS configuration ERROR [wasmi_runtime_enclave::registration::cert] The following vulnerabilities must be mitigated: ["INTEL-SA-00161", "You must disable hyperthreading in the BIOS", "INTEL-SA-00289", "You must disable overclocking/undervolting in the BIOS"] Platform status is SW_HARDENING_AND_CONFIGURATION_NEEDED. This means is updated but requires further BIOS configuration

```

Please disable hyperthreading and overclocking/undervolting (Turboboost) in your BIOS.

I'm seeing CONFIGURATION_AND_SW_HARDENING_NEEDED in the isvEnclaveQuoteStatus field, but with more advisories than what is allowed

This could mean a number of different things related to the configuration of the machine. Most common are:

- ["INTEL-SA-00161", "INTEL-SA-00233"] - Hyper-threading must be disabled in the BIOS
- ["INTEL-SA-00289"] - Overclocking/undervolting must be disabled by the BIOS (sometimes known as Turboboost)
- ["INTEL-SA-00219"] - Integrated graphics should be disabled in the BIOS - we recommend performing this step if you can, though it isn't required
-

If you are still having trouble getting rid of INTEL-SA-00219 and INTEL-SA-00289, here are some possible settings to look for outside of the CPU settings:

- Primary Display = 'PCI Express'
- IGPU Multi-Monitor = Disabled
- Onboard VGA = Disabled
-

I'm seeing SGX_ERROR_DEVICE_BUSY

Most likely you tried reinstalling the driver and rerunning the enclave - restarting should solve the problem