Resolve "default Keyring certificate is invalid, reason: expired" Error on Firepower 9300/4100

Contents

Issue

An error message is displayed on FXOS: "default Keyring certificate is invalid, reason: expired". This issue is observed on Cisco Firepower 9300 appliances.

Environment

- Product: Cisco Secure Firewall Firepower
- Appliance Model: Firepower 9300/4100
- Platform: FXOS

Resolution

To resolve the "default Keyring certificate is invalid, reason: expired." error, the default keyring certificate must be regenerated on the affected Firepower 9300/4100 chassis. This workflow details the steps required to regenerate the certificate and clear the fault.

1. Scope to the security context - Access the security scope in FXOS CLI to begin managing keyring certificates.

```
scope security
```

2. Scope to the default keyring - Navigate to the default keyring context.

```
scope keyring default
```

3. Regenerate the certificate - Set the system to regenerate the default keyring certificate.

```
set regenerate yes
```

4. Commit the changes - Apply the regeneration operation by committing the changes.

```
commit-buffer
```

The aforementioned procedure must be performed on each Firepower 9300/4100 chassis where the error is reported.

After successfully regenerating the default keyring certificate, the error is cleared and the certificate is renewed. The system reports a resolved state for the major fault previously associated with the expired keyring certificate.

Cause

The root cause of the issue is the expiration of the default keyring certificate on the FXOS platform after an upgrade of the firewall system. The expired certificate triggered a major fault and the corresponding error message. Regenerating the certificate restores normal operation.

Related Content

- Regenerating the Default Key Ring