Below are the SAN details and our proposed approach.

**Current SAN Requirements**

According to IBM’s documentation for EEM and EGW, the required SANs are:

|  |  |
| --- | --- |
| **Subsystem** | **Subject Alternative Names** |
| Events Endpoint Manager | manager-ibm-eem-manager |
| manager-ibm-eem-manager.eemnp |
| manager-ibm-eem-manager.eemnp.svc |
| manager-ibm-eem-manager.eemnp.svc.cluster.local |
| manager-ibm-eem-apic-eemnp.api.integrationocpnp.afs1-sit.aws-za.example.cloud |
| manager-ibm-eem-gateway-eemnp.api.integrationocpnp.afs1-sit.aws-za.example.cloud |
| manager-ibm-eem-manager-eemnp.api.integrationocpnp.afs1-sit.aws-za.example.cloud |
| manager-ibm-eem-admin-eemnp.api.integrationocpnp.afs1-sit.aws-za.example.cloud |
| DEV Events Gateway | dev-events-gateway-ibm-egw-svc |
| dev-events-gateway-ibm-egw-svc.eemnp |
| dev-events-gateway-ibm-egw-svc.eemnp.svc |
| dev-events-gateway-ibm-egw-svc.eemnp.svc.cluster.local |
| dev-events-gateway-ibm-egw-rt-eemnp.api.integrationocpnp.afs1-sit.aws-za.example.cloud |

**Alternate approach**

We can create a subdomain called **\*.eemnp.example.com** which can easily be delegate through AWS Route53.

Although SAN's through this approach are much shorter, they still have those hardcoded "ibm" names.

|  |  |
| --- | --- |
| **Subsystem** | **Subject Alternative Names** |
| Events Endpoint Manager | manager-ibm-eem-manager |
| manager-ibm-eem-manager.eemnp |
| manager-ibm-eem-manager.eemnp.svc |
| manager-ibm-eem-manager.eemnp.svc.cluster.local |
| manager-ibm-eem-apic-eemnp.example.com |
| manager-ibm-eem-gateway-eemnp.example.com |
| manager-ibm-eem-manager-eemnp.example.com |
| manager-ibm-eem-admin-eemnp.example.com |
| DEV Events Gateway | dev-events-gateway-ibm-egw-svc |
| dev-events-gateway-ibm-egw-svc.eemnp |
| dev-events-gateway-ibm-egw-svc.eemnp.svc |
| dev-events-gateway-ibm-egw-svc.eemnp.svc.cluster.local |
| dev-events-gateway-ibm-egw-rt-eemnp.example.com |

Ideally, we would like to simplify the SAN's used in the certificate which can cover various internal and external endpoints used by EEM.

If we drop the SAN requirement of **${MANAGER\_NAME}-ibm-eem-manager** (for the Manager) and **${GATEWAY\_NAME}-ibm-egw-svc** (for the Gateway) we could achieve much simpler SAN's.

|  |  |  |
| --- | --- | --- |
| **Subsystem** | **Subject Alternative Names** | Notes |
| Events Endpoint Manager | \*.emmnp |  |
| \*.emmnp.svc |  |
| \*.emmnp.svc.cluster.local |  |
| \*-emmnp.example.com |  |
| ${MANAGER\_NAME}-ibm-eem-apic-emmnp.example.com | Can be shortened |
| ${MANAGER\_NAME}-ibm-eem-gateway-emmnp.example.com | Can be shortened |
| ${MANAGER\_NAME}-ibm-eem-admin-emmnp.example.com | Can be shortened |
| Events Gateway | \*.emmnp | covered above |
| \*.emmnp.svc | covered above |
| \*.emmnp.svc.cluster.local | covered above |
| ${GATEWAY\_NAME}-ibm-egw-rt-emmnp.example.com | Can be shortened |

Below is a list of API Connect and Event Streams endpoints we use. We've simplified certificate management for each of these endpoints by using a custom wildcard certificate. All API Connect Endpoints are secured through one certificate. We use a certificate with the CN and SAN of "**\*.apinp.example.com**" for each of the API Connect endpoints.

Similarly for Event Streams, we have one custom certificate which secures all endpoints with a CN and SAN of "**\*.rtsnp.example.com**".

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clusters** | **NAME** | **HOST/PORT** | **PATH** | **SERVICES** |
| API Connect | analytics-ai-endpoint | analytics-ai.apinp.example.com |  | analytics-mtls-gw |
| api-gatewaynp-gateway | api-gatewaynp.apinp.example.com |  | api-gatewaynp-datapower |
| api-gatewaynp-gateway-manager | api-gatewaynp-manager.apinp.example.com |  | api-gatewaynp-datapower |
| dev-gateway-gateway | dev-gateway.apinp.example.com |  | dev-gateway-datapower |
| dev-gateway-gateway-manager | dev-gateway-manager.apinp.example.com |  | dev-gateway-datapower |
| management-admin | cloud-manager.apinp.example.com |  | management-juhu |
| management-api-manager | manager.apinp.example.com |  | management-juhu |
| management-compliance-api | platform-api.apinp.example.com | /governance | management-juhu |
| management-consumer-api | consumer-api.apinp.example.com |  | management-juhu |
| management-consumer-catalog | consumer-catalog.apinp.example.com |  | management-juhu |
| management-hub | hub.apinp.example.com |  | management-atm-api |
| management-platform-api | platform-api.apinp.example.com |  | management-juhu |
| management-turnstile | turnstile.apinp.example.com |  | management-turnstile |
| portal-portal-director | portal-admin.apinp.example.com |  | portal-nginx |
| portal-portal-web | portal.apinp.example.com |  | portal-de2aaf37-www |
| route-bootcamp-portal-web | bootcamp-portal.apinp.example.com |  | portal-de2aaf37-www |
| route-dev-portal-web | dev-portal.apinp.example.com |  | portal-de2aaf37-www |
| route-developernp-portal-web | developernp.example.com |  | portal-de2aaf37-www |
| route-sit-portal-web | sit-portal.apinp.example.com |  | portal-de2aaf37-www |
| sit-gateway-gateway | sit-gateway.apinp.example.com |  | sit-gateway-datapower |
| sit-gateway-gateway-manager | sit-gateway-manager.apinp.example.com |  | sit-gateway-datapower |
| Event Streams | es-cluster-2-ibm-es-ac-reg-apicurio | apicurio.es-cluster-2.rtsnp.example.com |  | es-cluster-2-ibm-es-ac-reg-external |
| es-cluster-2-ibm-es-admapi-admin-api | admin-api.es-cluster-2.rtsnp.example.com |  | es-cluster-2-ibm-es-admapi-external |
| es-cluster-2-ibm-es-recapi-rest-producer | rest-producer.es-cluster-2.rtsnp.example.com |  | es-cluster-2-ibm-es-recapi-external |
| es-cluster-2-ibm-es-ui-admin-ui | admin-ui.es-cluster-2.rtsnp.example.com |  | es-cluster-2-ibm-es-ui-external |
| es-cluster-2-kafka-extscram-0 | broker-0.extscram.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-extscram-0 |
| es-cluster-2-kafka-extscram-1 | broker-1.extscram.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-extscram-1 |
| es-cluster-2-kafka-extscram-2 | broker-2.extscram.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-extscram-2 |
| es-cluster-2-kafka-extscram-bootstrap | bootstrap.extscram.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-extscram-bootstrap |
| es-cluster-2-kafka-exttls-0 | broker-0.exttls.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-exttls-0 |
| es-cluster-2-kafka-exttls-1 | broker-1.exttls.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-exttls-1 |
| es-cluster-2-kafka-exttls-2 | broker-2.exttls.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-exttls-2 |
| es-cluster-2-kafka-exttls-bootstrap | bootstrap.exttls.es-cluster-2.rtsnp.example.com |  | es-cluster-2-kafka-exttls-bootstrap |

It would be a lot easier if EEM also allowed for its endpoints to be secured in this manner. Following this structure keeps certificate management simpler and endpoint names cleaner/prettier.