Tenant-Region Management

Tenant-Region Management

Deploying Tenant Policies in Different Regions

Cisco Cloud APIC enforces ownership checks to prevent deployment of policies in the same tenant-region combination, done either intentionally or by mistake. For example, assume that one Cisco Cloud APIC (CAPIC1) is deployed in AWS account IA1 in the region R1, and you want to deploy a tenant in account TA1 in region R2. This tenant deployment (the account-region combination of TA1-R2) is now owned by IA1-R1 (CAPIC1). If another Cisco Cloud APIC (CAPIC2) attempts to manage the same tenant-region combination of TA1-R2 at some point in the future (for example, if CAPIC2 is deployed in AWS account IA2 in the region R3), this will not be allowed because the current owner for the deployment TA1-R2 is IA1-R1 (CAPIC1).

These restrictions are achieved using AWS Resource Groups. The following example provides several valid and invalid deployment combinations.

Cisco Cloud APIC	Tenant	Validity	Reason
IA1-R1 (CAPIC1)	TA1-R1	Valid	Tenant TA1-R1 is owned by IA1-R1 (CAPIC1)
IA1-R1 (CAPIC1)	TA1-R2	Valid	Tenant TA1-R2 is owned by IA1-R1 (CAPIC1)
IA1-R2 (CAPIC2)	TA1-R1	Invalid	Tenant TA1-R1 is already owned by IA1-R1 (CAPIC1)
IA1-R2 (CAPIC2)	TA1-R3	Valid	Tenant TA1-R3 is owned by IA1-R2 (CAPIC2)
IA2-R1 (CAPIC3)	TA1-R1	Invalid	Tenant TA1-R1 is already owned by IA1-R1 (CAPIC1)
IA2-R1 (CAPIC3)	TA1-R4	Valid	Tenant TA1-R4 is owned by IA2-R1 (CAPIC3)

Cisco Cloud APIC	Tenant	Validity	Reason
IA2-R1 (CAPIC3)	TA2-R4	Valid	Tenant TA2-R4 is owned by IA2-R1 (CAPIC3)

Deployment enforcement is done for the infra tenant as well as for user tenants. If CAPIC1 is deployed in the account IA1 in the region R1 and is also trying to manage the regions R2 and R3, another Cisco Cloud APIC (for example, CAPIC2) trying to manage the same account IA1 for regions R1, R2 and R3 would not be allowed.

The validation for the tenant-region ownership is done using AWS Resource Groups. For every tenant-region combination, a Resource Group is created using the syntax CloudAPIC_*TenantName_Region* (for example, the name CAPIC_TA1_R2 would be created if a tenant is deployed in account TA1 in region R2). It would also have an ownership tag of IA1_R1_TA1_R2, if the Cisco Cloud APIC is deployed in account IA1 in region R1.

Following are examples of situations where there might be an AciOwnerTag mismatch, where existing tenant-region deployments would fail:

- If a Cisco Cloud APIC was initially installed in one account, was then torn down and the Cisco Cloud APIC was installed in a different account. In this case, all existing tenant-region deployments would fail if you try to manage the same tenant-region combinations again.
- If a Cisco Cloud APIC was initially installed in one region, was then torn down and the Cisco Cloud APIC is installed in a different region. In this case, all existing tenant-region deployments would fail.
- If another Cisco Cloud APIC is managing the same tenant-region.

In ownership mismatch cases, Cisco Cloud APIC does not perform a retry of the tenant-region setup again. To resolve ownership mismatch cases, if you are positive that no other Cisco Cloud APIC is managing the same tenant-region combination, log in to the tenant's AWS account and manually remove the affected Resource Group (for example, `CAPIC_123456789012_us-east-2`). Then either reload the Cisco Cloud APIC instance or delete the tenant from the Cisco Cloud APIC and add it again.