Developer Days
Automation

cisco
The bridge to possible

Granular Role-Based Access Control

Crosswork Network Controller 6.0

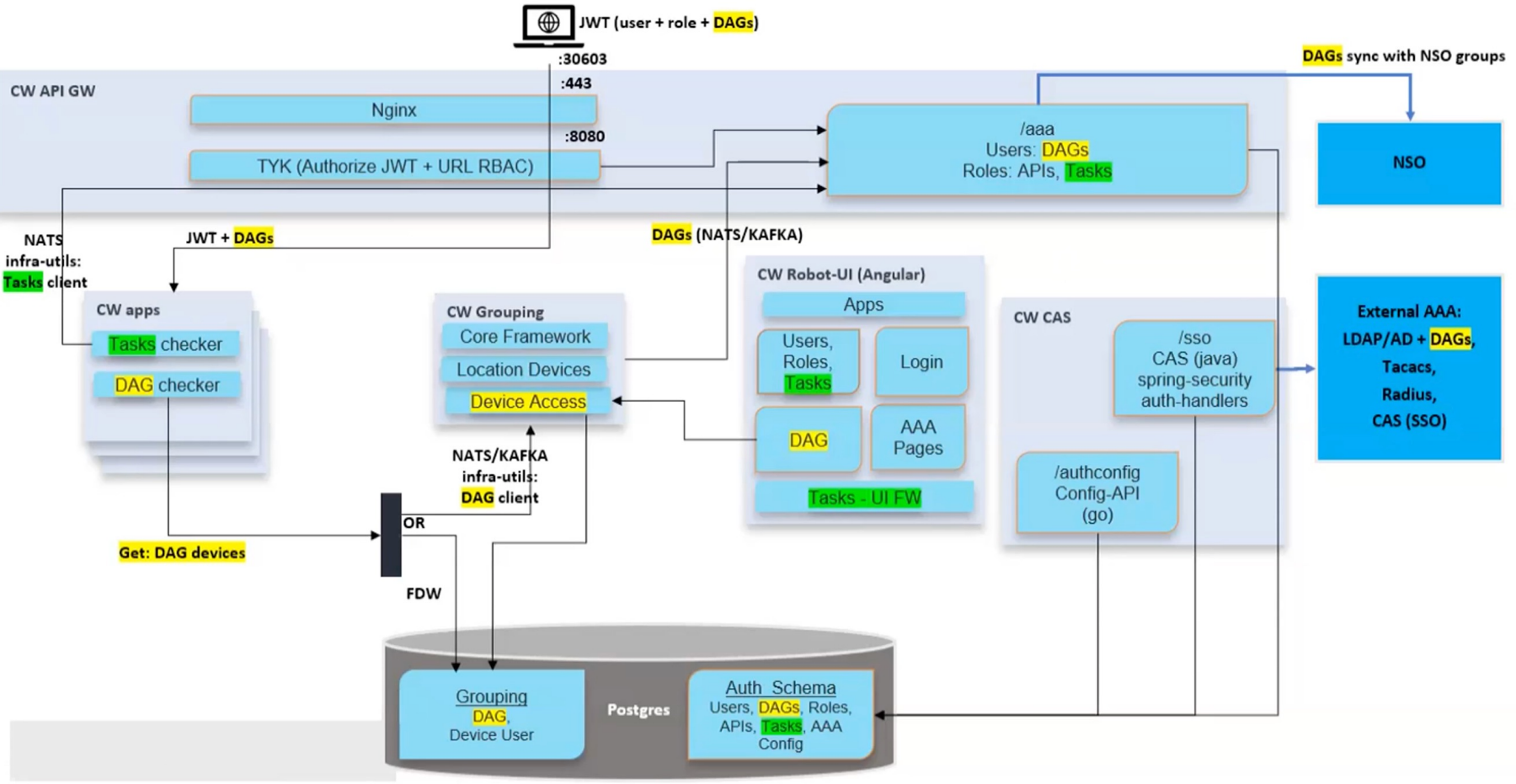
Michael Maddern
Krishnan Thirukonda
Dec 6, 2023

Role-Based Access Control Feature Overview

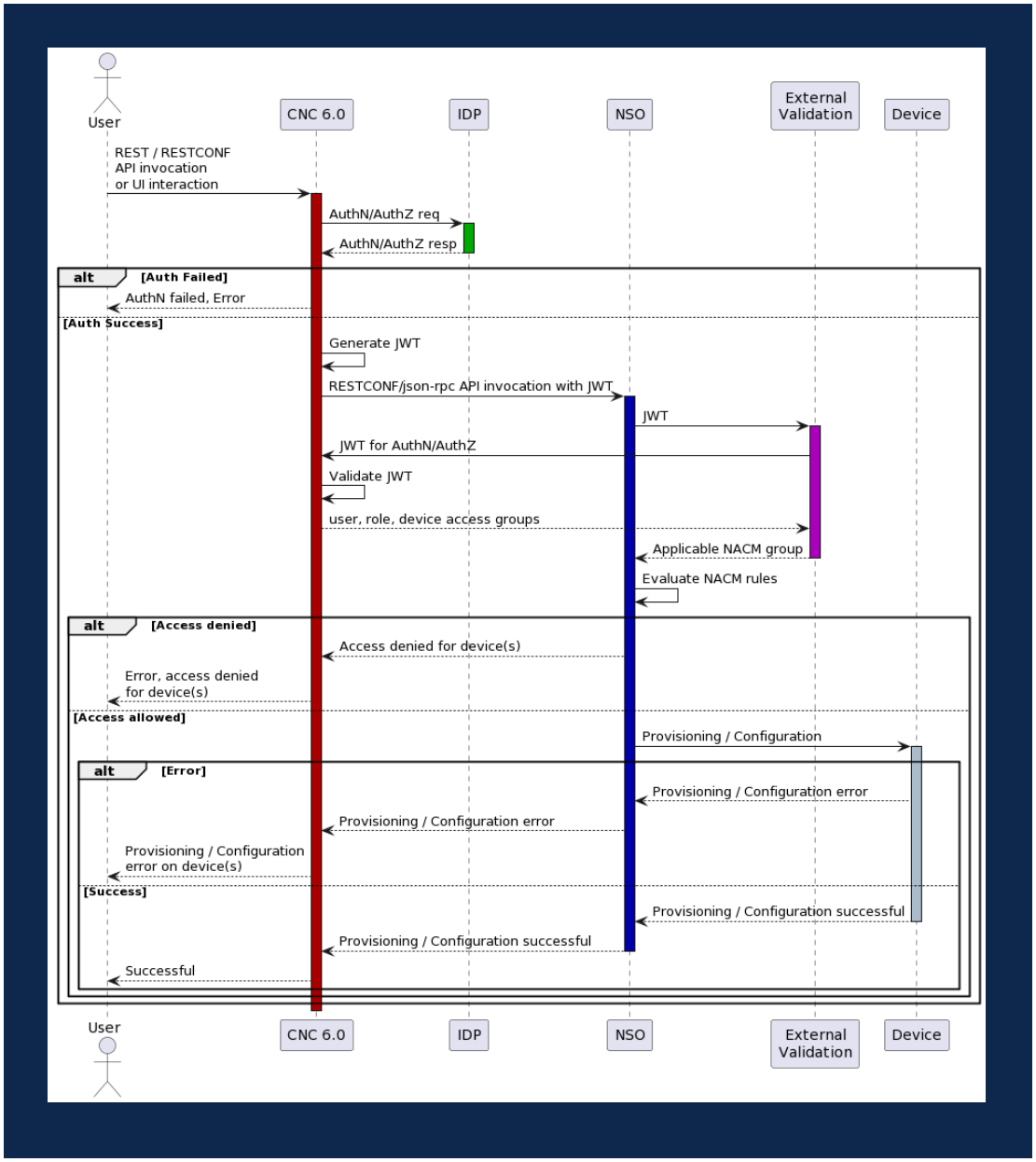
Granularity: Tasks and Device Access Groups

- Tasks: Logical grouping of functions that constitute an established workflow for a CNC user
- Device Access Group: Group of devices with the same access control policy

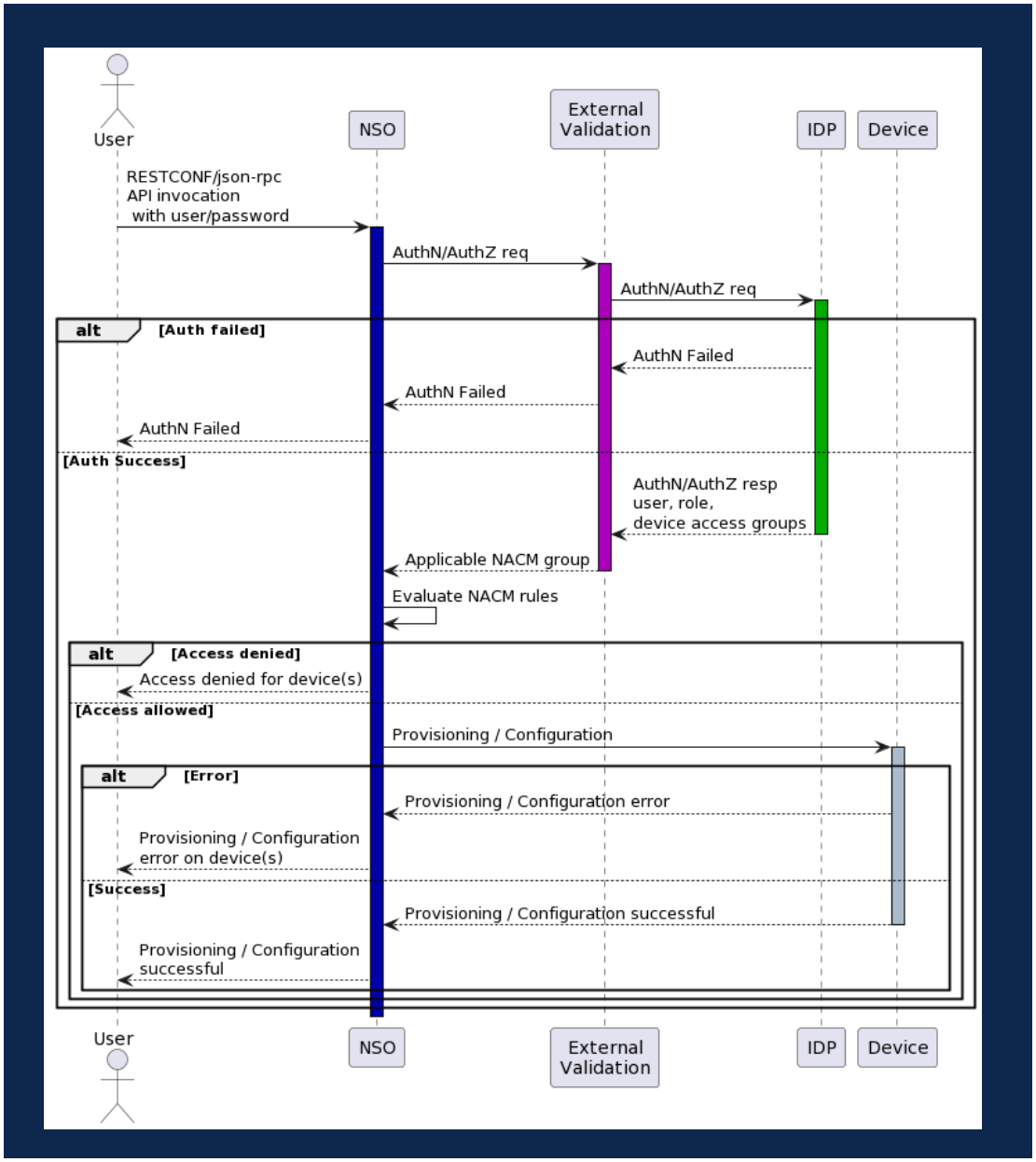
DAG and Tasks in AAA architecture



CNC – NSO – Device Authorization Flow



1. RESTCONF/json-rpc API invocations from CNC will include a JWT for auth.
2. The external validation script within NSO sends the JWT back to CNC to assess validity and authorization.
3. CNC responds with <user, role, device-access-groups>, if the token is valid.
4. The external validation script formulates the applicable NACM group based on <role + device-access-groups>.
5. NSO evaluates the applicable NACM rules to determine if it can proceed with the requested action.



1. User authenticates to NSO with username and password.
2. If this is a remote user, the external validation script connects to the Identity Provider for authentication and authorization.
3. The Identity Provider returns the applicable <user, role, device-access-groups>.
4. The external validation script formulates the applicable NACM group based on <role + device-access-groups>.
5. NSO evaluates the applicable NACM rules to determine if it can proceed with the requested action.
6. If this is local NSO user, the appropriate <user to NACM group> mapping will need to be done manually during user creation (or user management).

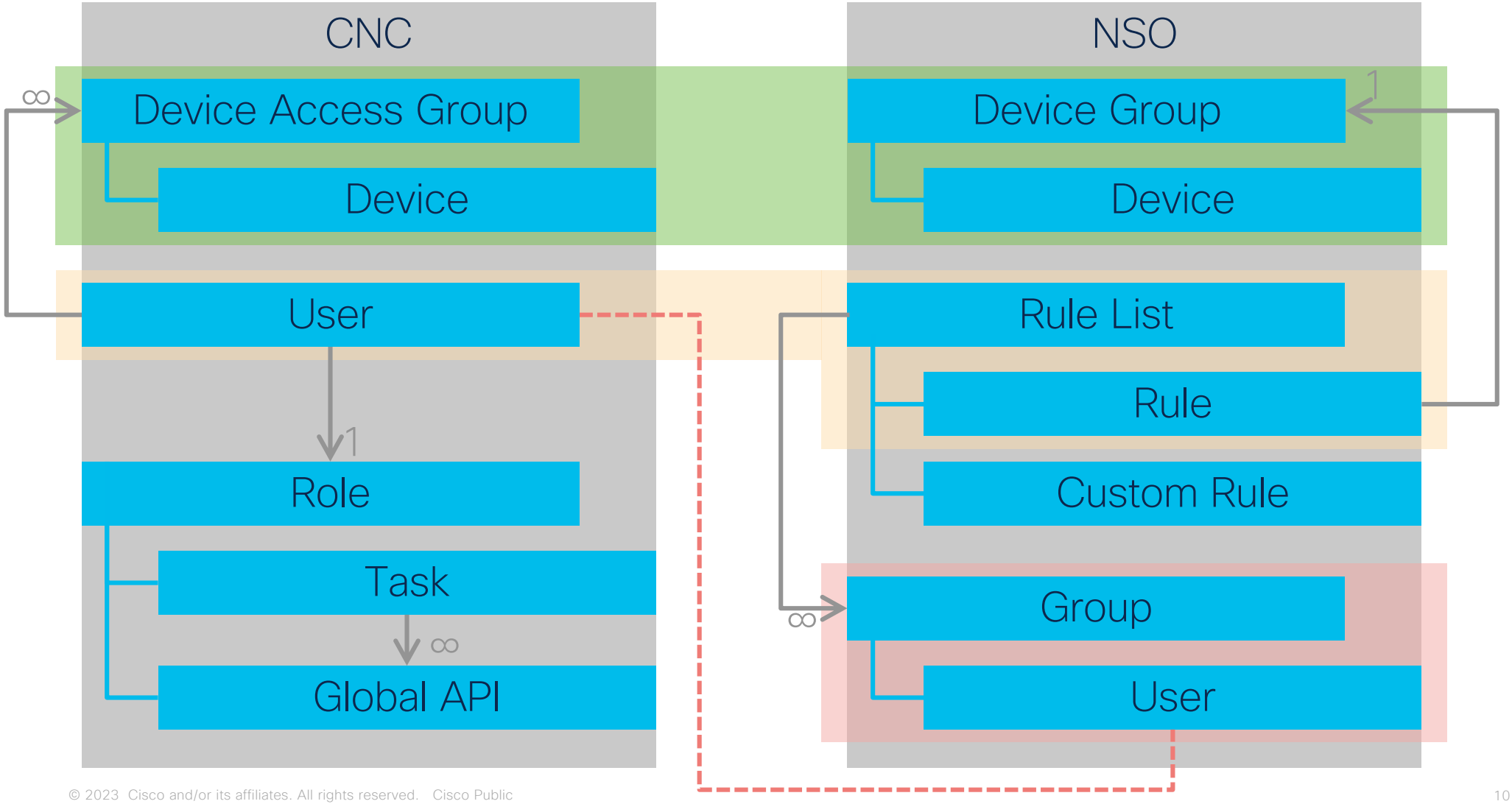
CNC – NSO Integration

Device Access Groups (DAG)

- A Device Access Group is a logical grouping of devices used to control who administer a network segment
- By default, all the devices in the setup belong to the ALL-ACCESS DAG
- When a DAG is created in CNC, an equivalent device-group will be created in NSO

Tasks

- A group of functions that are part of a preestablished workflow
- Task permissions are part of a “role” configuration and are assigned to individual users as part of the user configuration
- Global API permissions are associated to Task Permissions and can’t be edited for tasks enabled in the Task Permissions section



NSO Configuration Overview

Enable authentication package `cisco-cfp-jwt-auth`

Enforce NACM on services

Per user:

- NACM rule-list creation (generated by CNC)
- NACM group creation (for mapping local users)

Enable cisco-cfp-jwt-auth on NSO

1. Add cisco-cfp-jwt-auth package to NSO
2. Add package-authentication entry in ncf.conf

```
<aaa>
  <package-authentication>
    <enabled>true</enabled>
    <packages>
      <package>cisco-cfp-jwt-auth</package>
    </packages>
  </package-authentication>
</aaa>
```

Enable cisco-cfp-jwt-auth on NSO

3. Bootstrap configuration – CNC and certificate

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <jwt-auth xmlns="http://cisco.com/ns/nso/cfp/cisco-cfp-jwt-auth">
    <cnc-host>172.18.116.150</cnc-host>
    <port>30603</port>
    <pem-key-path>/home/nso/crosswork.pem</pem-key-path>
  </jwt-auth>
</config>
```

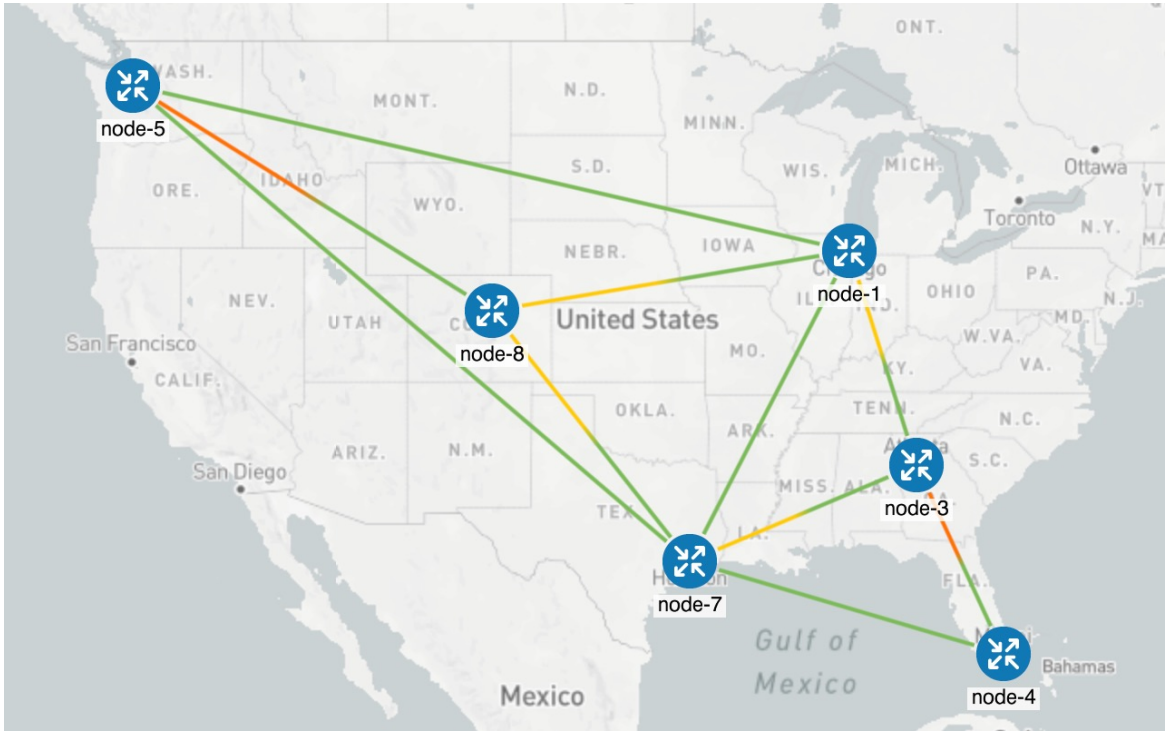
4. Enforce NACM on services

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <enforce-nacm-on-services xmlns="http://tail-f.com/yang/ncs-acm">
      true</enforce-nacm-on-services>
  </nacm>
</config>
```

Demo

Network Topology

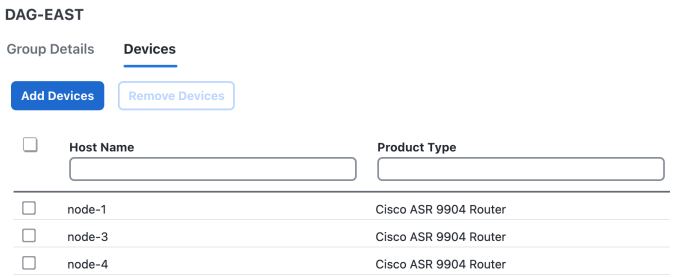
Network topology used to demonstrate Granular RBAC feature



DAG configuration

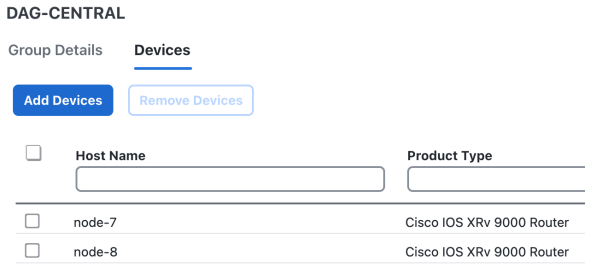
DAG-EAST

Node-1
Node-3
Node-4



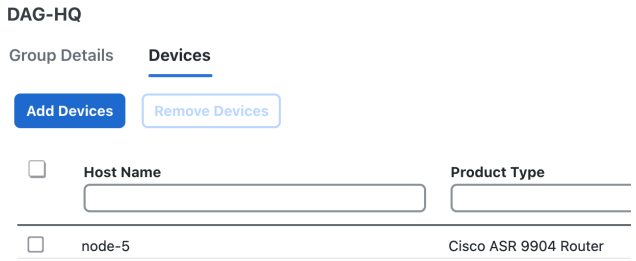
DAG-CENTRAL

Node-7
Node-8



DAG-HQ

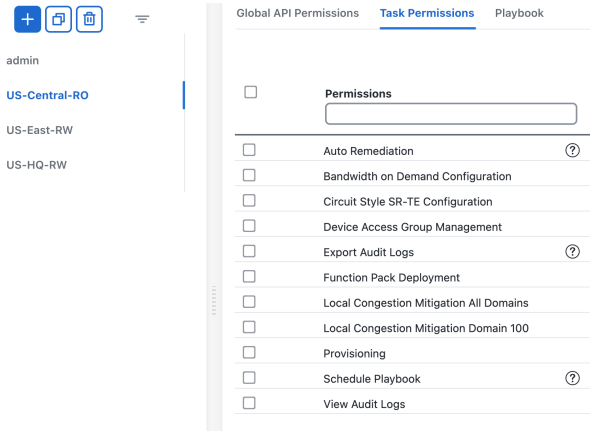
Node-5



Role configuration

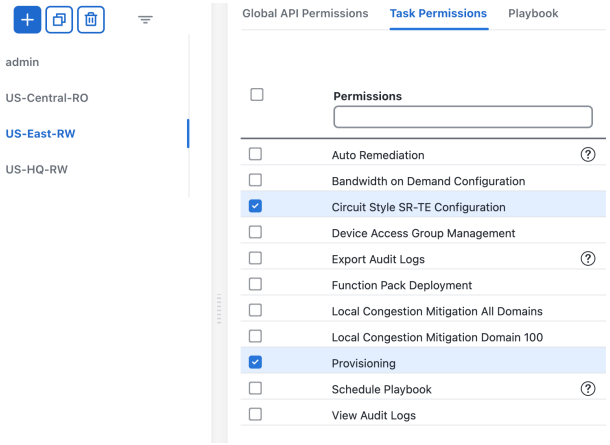
US-Central-RO

- None



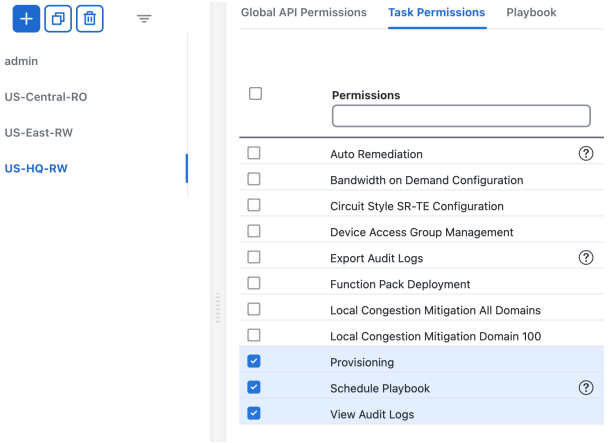
US-East-RW

- Provisioning
- Circuit Style SR-TE Configuration



US-HQ-RW

- Provisioning
- Schedule Playbook
- View Audit Logs



User configuration

centraluser

Role:
- US-Central-RO

DAG:
- DAG-CENTRAL

eastuser

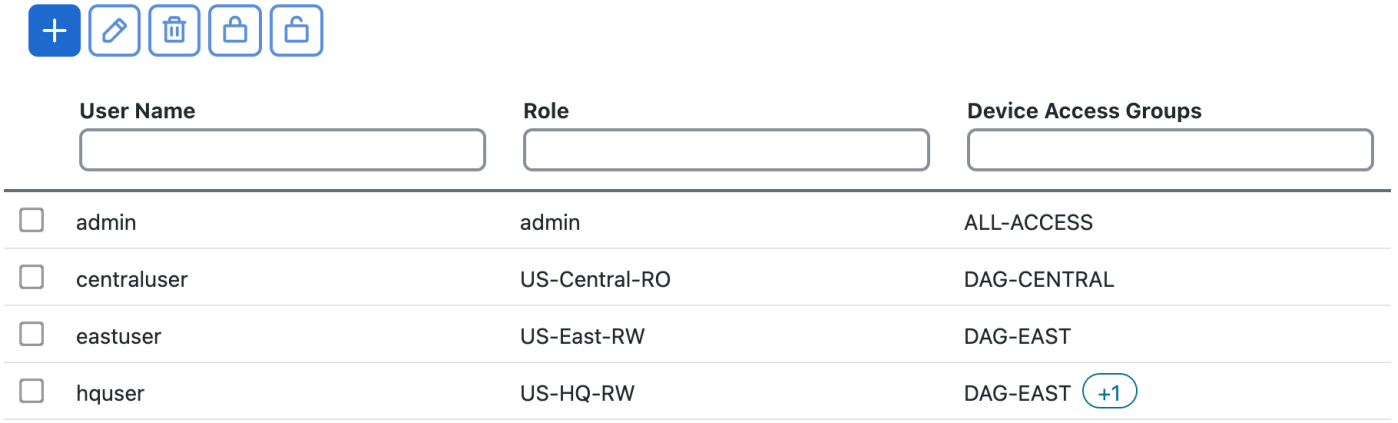
Role:
- US-East-RW

DAG:
- DAG-EAST

hquser

Role:
- US-HQ-RW

DAG:
- DAG-HQ
- DAG-EAST



User Name	Role	Device Access Groups
admin	admin	ALL-ACCESS
centraluser	US-Central-RO	DAG-CENTRAL
eastuser	US-East-RW	DAG-EAST
hquser	US-HQ-RW	DAG-EAST +1

The bridge to possible