# ACI BCS MultiPod POD1 User5

This ACI AutoPod is offered as an IaaS (Infrastructure-as-a-Service) pod, meaning that it will remain static and **is not intended for break-fix\rebuilt testing**. If you require break-fix testing, please consider booking out other ACI AutoPods. Bookable tenants will be used for testing customer use-cases, learning etc.

# User-5 Topology

A picture containing indoor, table, photo, man

Description automatically generated

# Device Details

|  | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | | **Model** | | **Serial No.** | | **OOB IP** | |
| N77-C7706 / N77-C7706\_IPN | | N77-C7706 | | FXS1851Q084 | | 10.77.7.136 | |
| **APICs** | | | | | | | |
| **APIC Name** | **Model** | | **Pod ID** | **Node ID** | **Serial No.** | | **OOB IP** |
| APIC1 | APIC-SERVER-M3 | | 1 | 1 | WZP233006BV | | 10.77.7.150/27 |
| APIC2 | APIC-SERVER-M3 | | 1 | 2 | WZP233006BU | | 10.77.7.151/27 |
| APIC3 | APIC-SERVER-M3 | | 2 | 3 | WZP233006BF | | 10.77.7.152/27 |

| **Spine Switches** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Spine Name** | **Model** | **Pod ID** | **Node ID** | **Serial No.** | **OOB IP** |
| pod1-spine201 | N9K-C9504 | 1 | 201 | FOX2332P927 | 10.77.7.130/27 |
| pod2-spine202 | N9K-C9504 | 2 | 202 | FOX2330PAWN | 10.77.7.131/27 |
| **Leaf Switches** | | | | | |
| **Leaf Name** | **Model** | **Pod ID** | **Node ID** | **Serial No.** | **OOB IP** |
| pod1-leaf101 | N9K-C93180YC-FX | 1 | 101 | FDO23340AE5 | 10.77.7.132/27 |
| pod1-leaf102 | N9K-C93180YC-EX | 1 | 102 | FDO22181C46 | 10.77.7.133/27 |
| pod2-leaf103 | N9K-C93180YC-EX | 2 | 103 | FDO22182UKC | 10.77.7.134/27 |
| pod2-leaf104 | N9K-C93180YC-EX | 2 | 104 | FDO22181BU5 | 10.77.7.135/27 |

# RBAC and Priviledge Restriction

This AutoPod has been preconfigured with ACI Security Domains. UserX will have full access rights to specifically its Tenant and Interface Profiles. As this AutoPod/Fabric is non-breakfix and is a shared resource, users will only have **read only access** to the fabric and access policies. This fabric is an IaaS pod meaning you consume the pod in a similar manner to a cloud based service, i.e. you can modify your own tenancy space without disrupting the overall cloud. If you require the ability to modify any of the fabric or access policies, please consider booking an alternative break-fix AutoPod where the whole fabric/infrastructure is assigned “as a whole” to a user.

# User Logical Policy

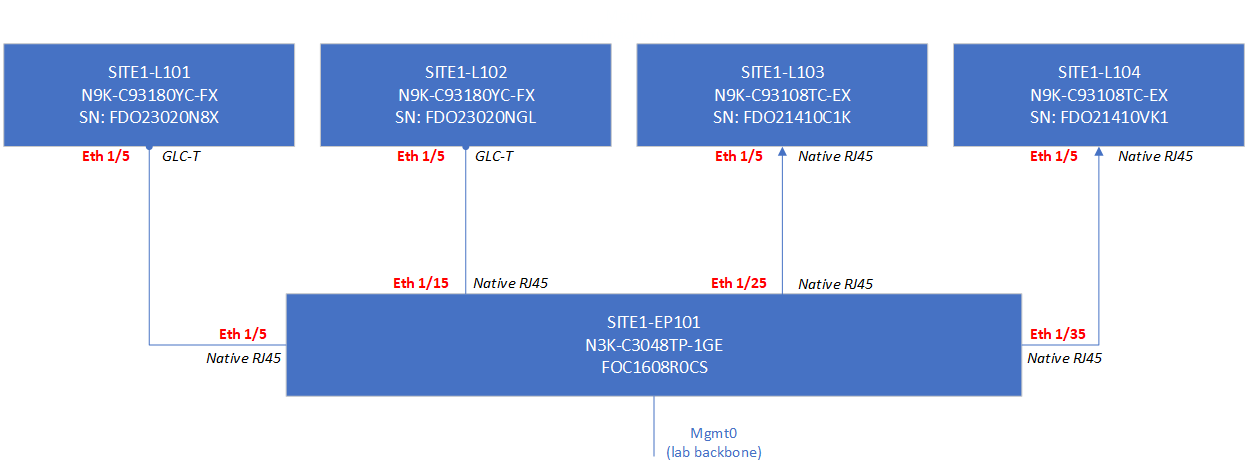
| **User ID** | **Endpoints Available** | **IP Address Space** | | **VLAN Allocations** | **Leaf and Endpoint Switch Port Allocations** |
| --- | --- | --- | --- | --- | --- |
| User5 | Physical and Virtual | 100.105.0.0/17 (100.105.0.0 - 100.105.127.255) | | 1280 - 1294 (Pod 1) 1295 - 1309 (Pod 2) | POD1-LF101:Eth1/5 POD2-LF102:Eth1/5 |
| **ACI and NX-OS Policy Constructs** | | |
| **Tenant:** user5 **Security Domain:** user5 **VLAN Pool:** user5 **Phydom:** user5 **L3.ExtDom:** user5 **AAEP:** user5 **IPGs:** user5-<speed>-<port-type> | | |

# Physical Endpoint Connectivity

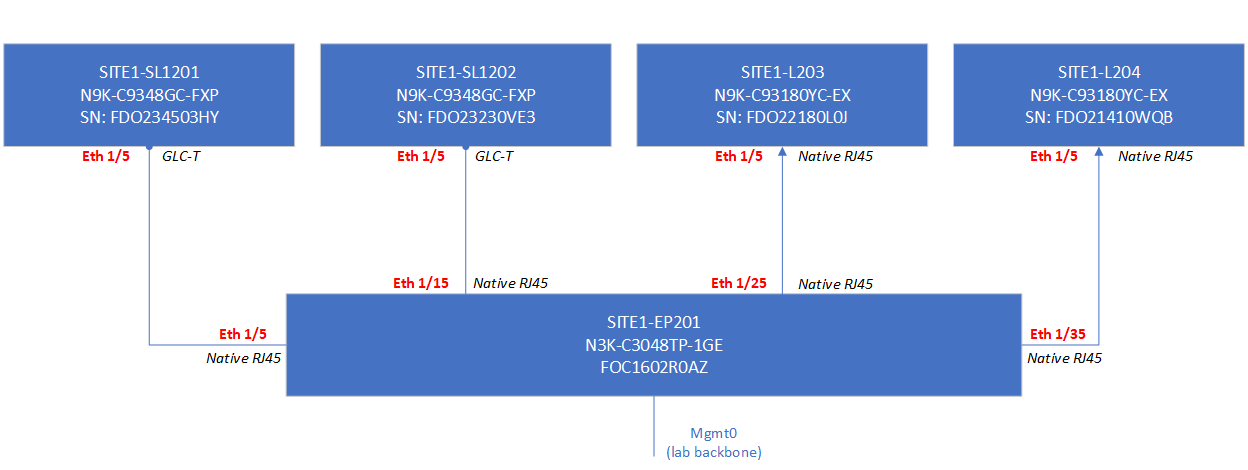
Each user account can connect their ACI tenant to the external Nexus 7706 series switches (POD1-EP1 and POD1-EP2) in each pod to test physical endpoint connectivity or connectivity to external L2/L3 domains using their allocated VLANs. There are a total of two endpoint switches deployed in this AutoPod.

* User5 gets two interfaces: Eth1/5 and Eth1/15 on each endpoint switch:
  + This will allow a single access port or VPC connectiity to ACI leaf switches in the AutoPod.
* Each user has 1x VRF created:
  + Users should create interfaces in the VRF using the IP address space that they have been allocated.
* Each user has 30 VLANs that can be used for Phydom connectivity:
  + There are 15 VLANs per pod - **DO NOT CONSUME VLANS or VRFs BELONGING TO ANOTHER USER**
* Assign your physical routed interface or SVI to your VRF

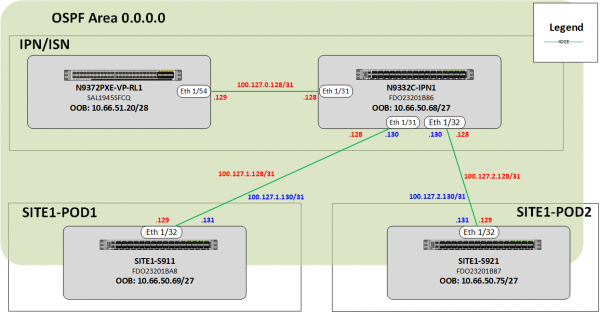
##### POD1-EP101 - User5



##### POD1-EP201 - User5

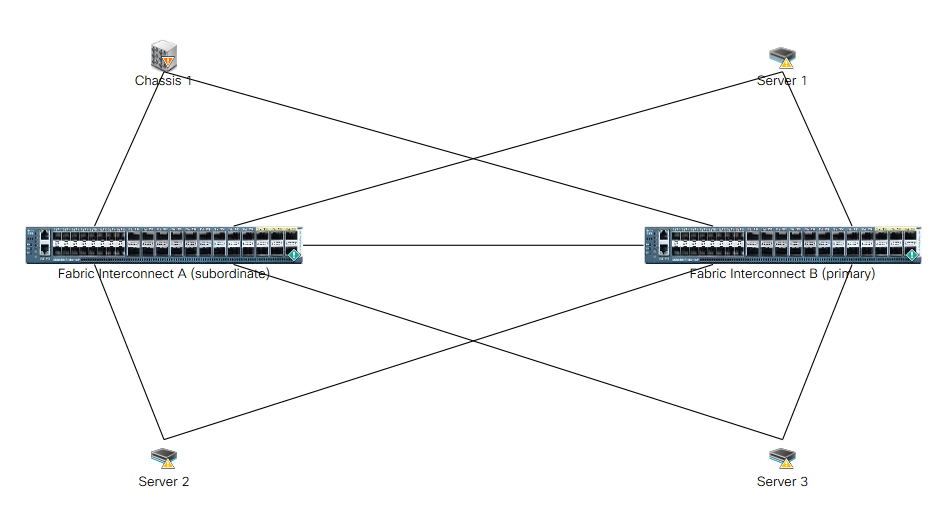


## IPN-ISN Design

[](https://calo-docs.cisco.com/lib/exe/fetch.php?media=external:sites:syd:autopods:ipn-site1.png)

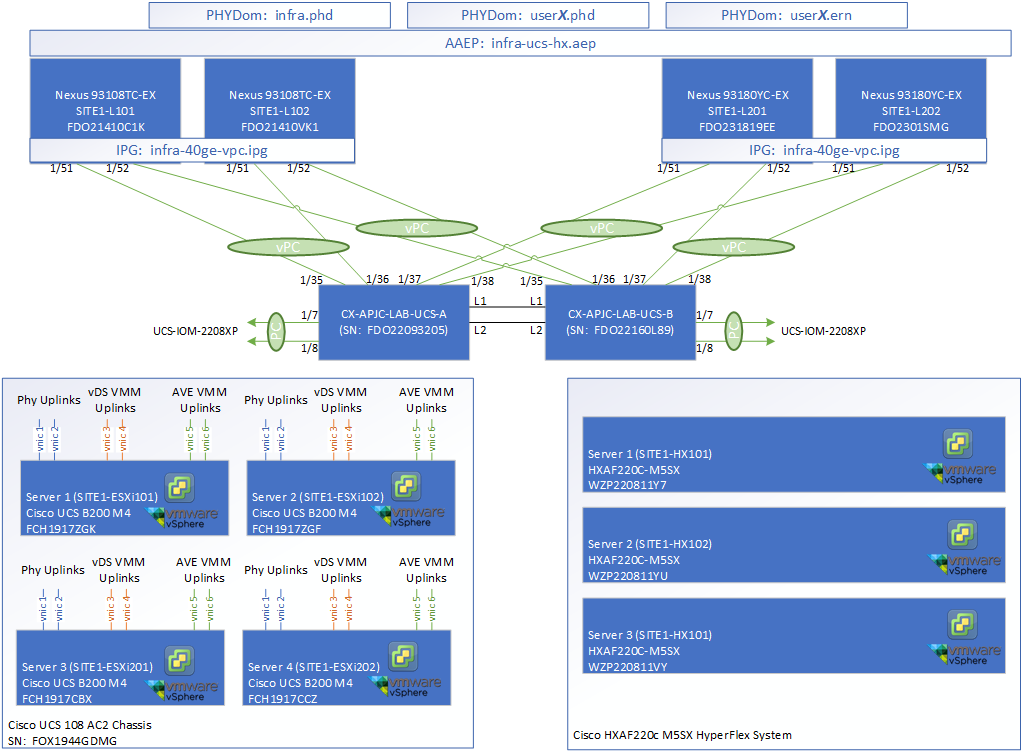
## UCS Connectivity Design

**AutoPod users have read-only access to UCSM.**

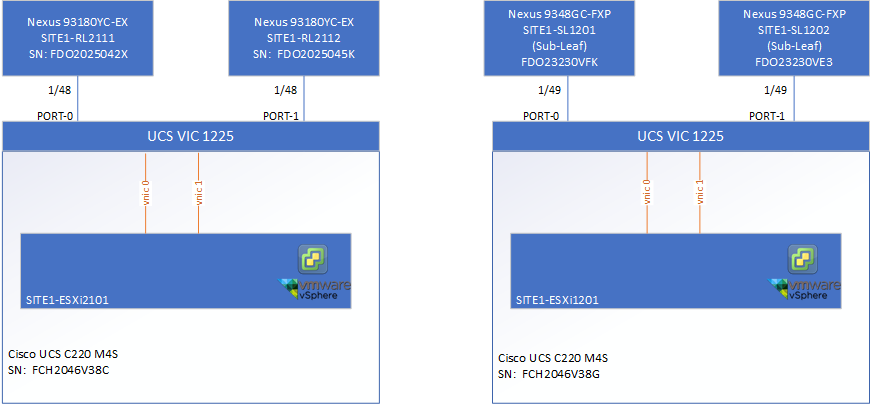
A single UCS system is shared by all ACI pods. The following design considerations apply:

* A pair of UCS 6332-16UP are deployed
* UCS connect up to the ACI leaf switches in each of the pods via 40GE links - port-channelled
* The UCS FIs connect to the 2208XP in the UCS 5108 chassis using a pair of 40GE links configured as a port-channel
* There are 8x UCSB-200M4 blades deployed in the 5108 chassis
* There are 3x HXAF220C-M5SX nodes deployed for CCP

### POD1 - UCS-B-Series and HX Connectivity



### POD1 and COLO UCS C-Series Connectivity



## VM Deployments

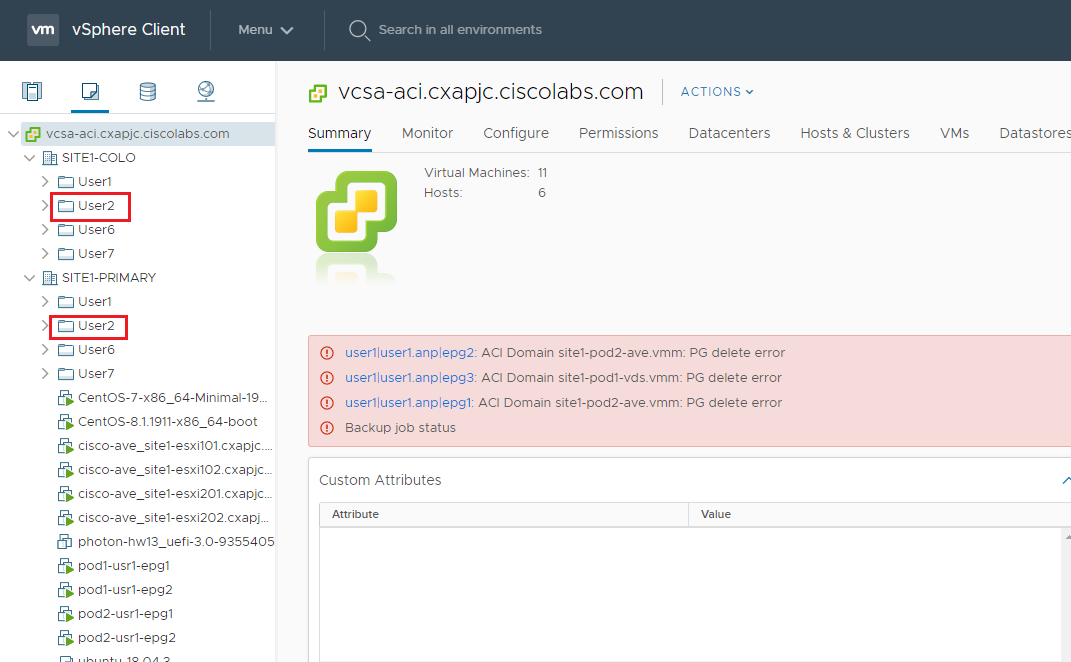
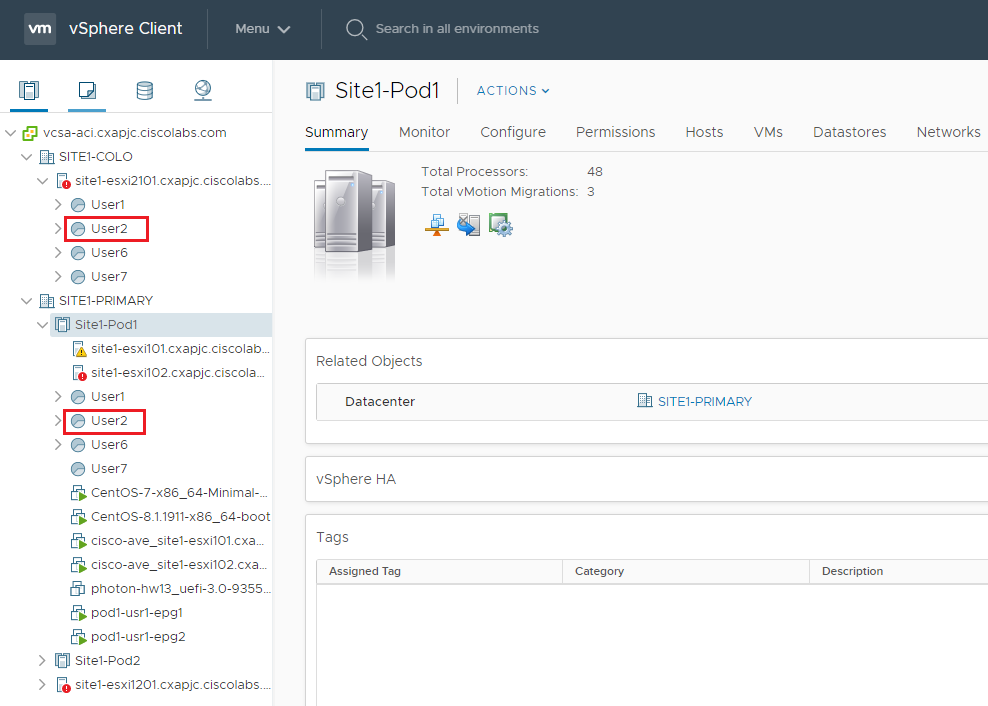
* User VMs can be deployed into either pod using the pre-configured VMM Domain Infrastructure (VDS or AVE)
* User VMs allocated to the VMM domain infrastrucutre willb e dynamically allocated VLANs from the dynamic VLAN pools
* Users are only granted the necessary vCenter permissions to deploy VMs for testing purposes
* Users are given a Resource Pool and VM folder where tehy have permission to deploy VMs into.
* Users are given permission to the appropriate datastores for their VMs. **Please use thin provisioning for all VM disk type.**
* Users must provision EPGs in their User tenant in ACI and attach the appropriate VMM domain.
* Users can attach networks to their VMs from either the VDS or AVE virtual switches managed by the APIC.
* Users have access to the Content Library where they will find VM templates and ISOs available for use. Alternatively they can upload their own OVA templates when creating a VM.
* **User VMs are not backed up or kept in vCenter when a booking has finished.** If there is configuration needed in the future, please backup the config or export the VM.

#### POD1 VMM Domains

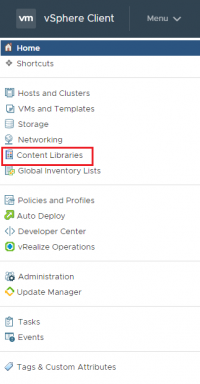
A screenshot of a cell phone

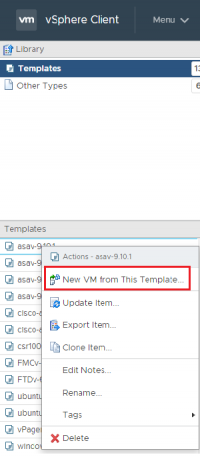
Description automatically generated

#### Example User

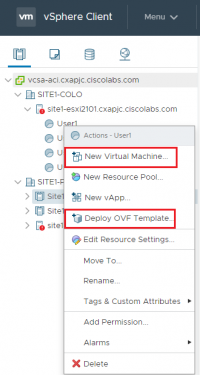


### VM ISOs and Templates

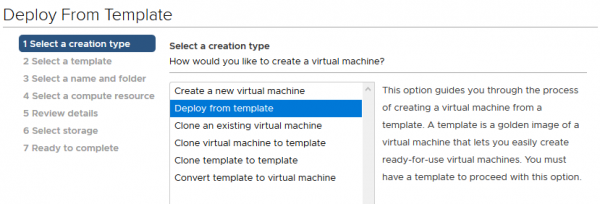
The Content library is used to store VM templates and ISOs. Access is via the Home menu in vCenter.

Right-click any template and select “New VM from this Template” to start the deploy VM wizard.

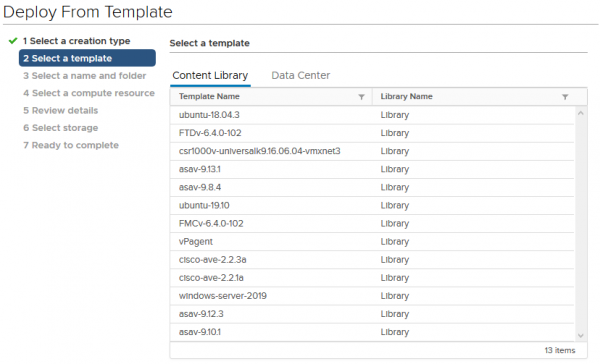
Users can also deploy VMs by right-clicking their Resource Pool or VM folder and select **“New Virtual Machine”** or **“Deploy OVF Template”** from the menu. The former will allow a user to deploy form existing VM templates in vCenter, the latter will allow a user to deploy from existing VM templates



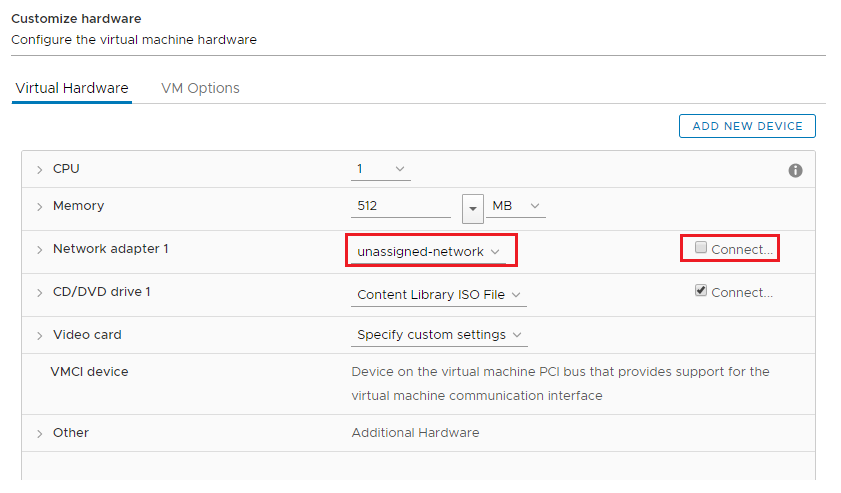
Choose **“Deploy from template”**



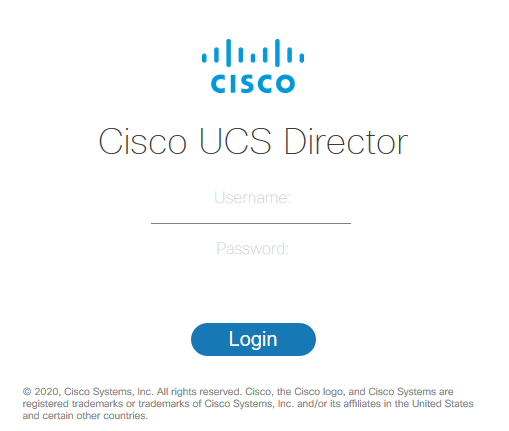
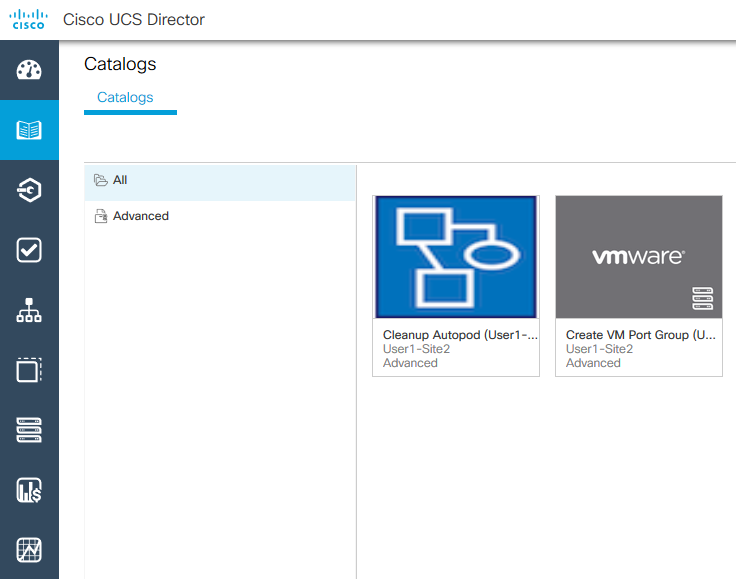
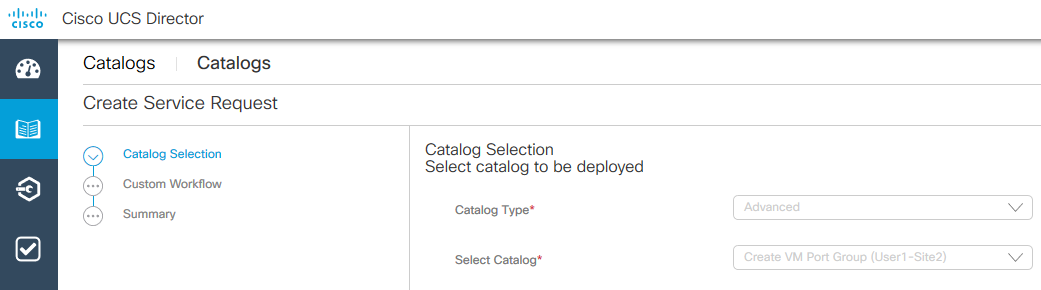
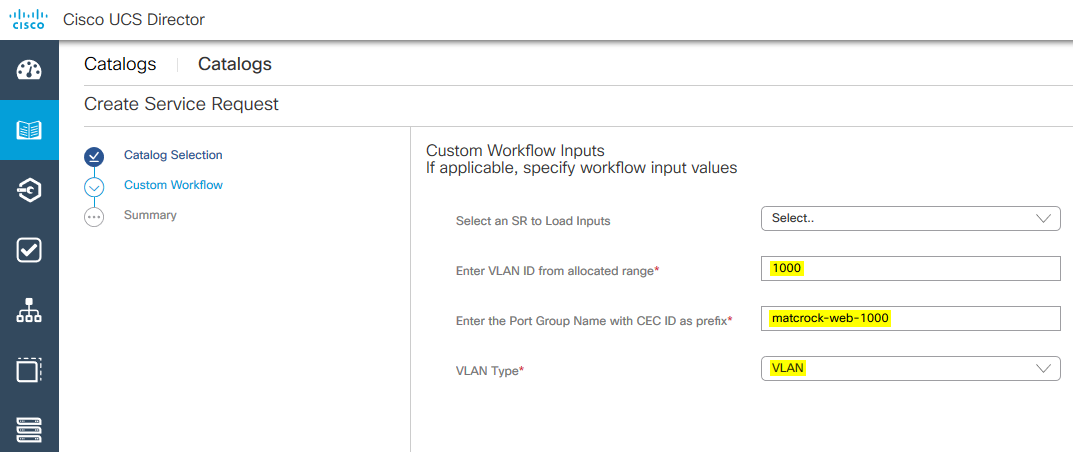
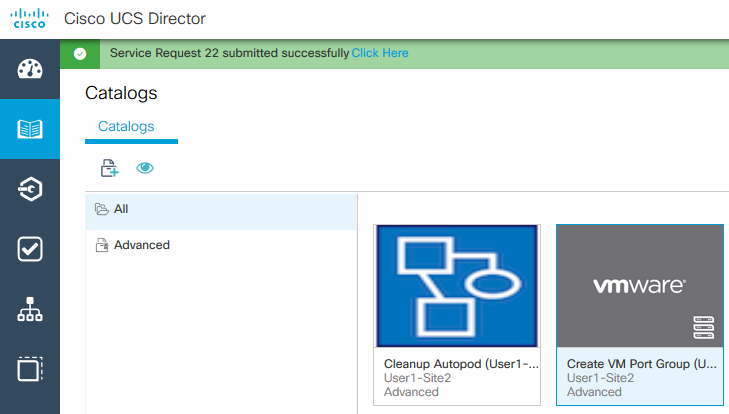
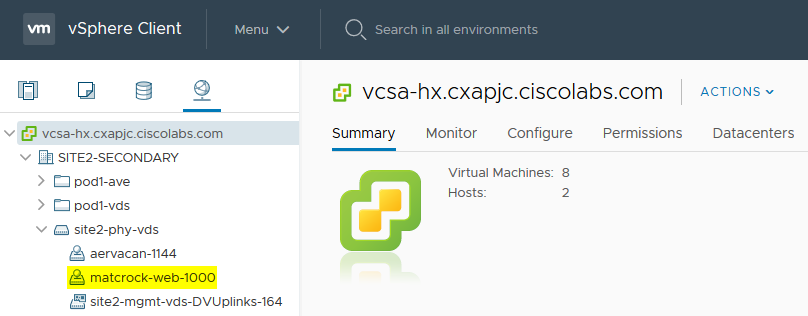
A user can now choose any of the VM templates contained in the Content Library. Alternatively, if a user wants to deploy their own OVA template that is not available in the library, they can choose **“Deploy OVF Template”** from the initial menu.



After deploying your VM, remember to **Edit Settings** and ensure you connect the VM to your desired network.



### Create VM Port Group

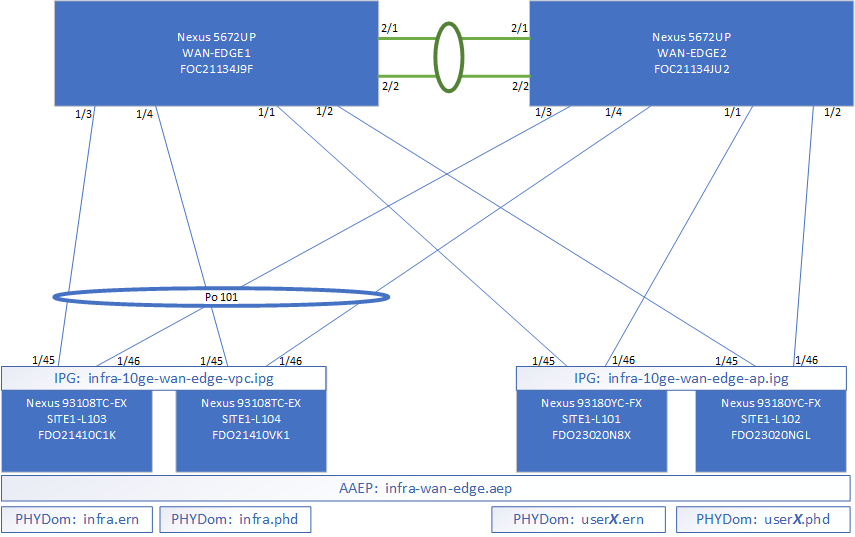
1. Login to the UCS Director portal (<https://portal.cxapjc.ciscolabs.com/>) with your AutoPod User credentials.2. To create a VM Port Group to be used for User Tenant static path bindings (non-VMM domain), launch the **Create VM Port Group Service** Service Request from the catalog.3. Click Next to commence the Service Request.4. Enter in a VLAN ID from the allocated range to your AutoPod User. Please ensure you include your CEC ID prefix into the Port Group Name.5. Submit the Service Request and ensure it was successful.6. Login to vCenter and under Networking, the new Port Group will be created.

## WAN Connectivity

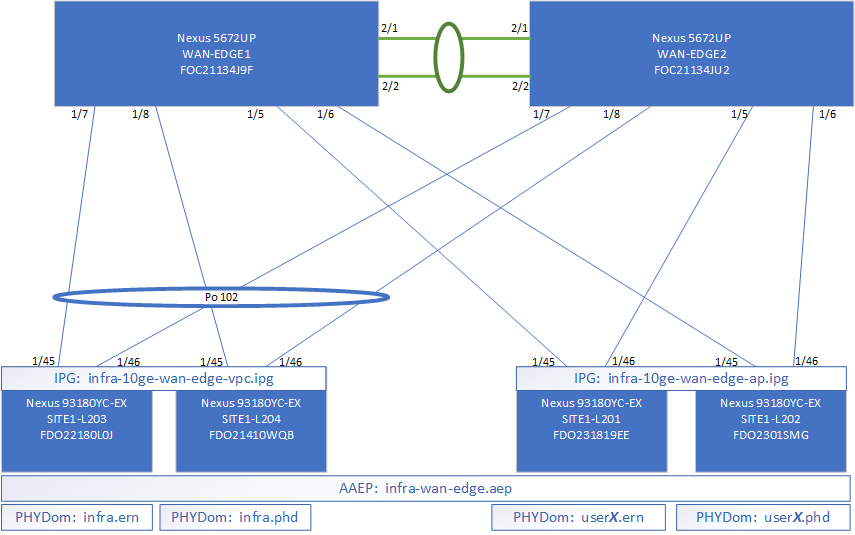
The WAN Edge switching is comprised of 2x Nexus 5672UP series switches. They provide connectivity to:

* **The border leaf switches in each pod:**
  + 2 connectivity models are offered - L3 pt-pt using routeable sub-interfaces and vPC using SVI
* **The UCS Fabric Interconnects:**
  + Used to build HX
  + Used for DMZ subnet
* **The Lab backbone:**
  + Extends the VLAN used for perimeter firewall

#### POD1/Pod1 Connectivity

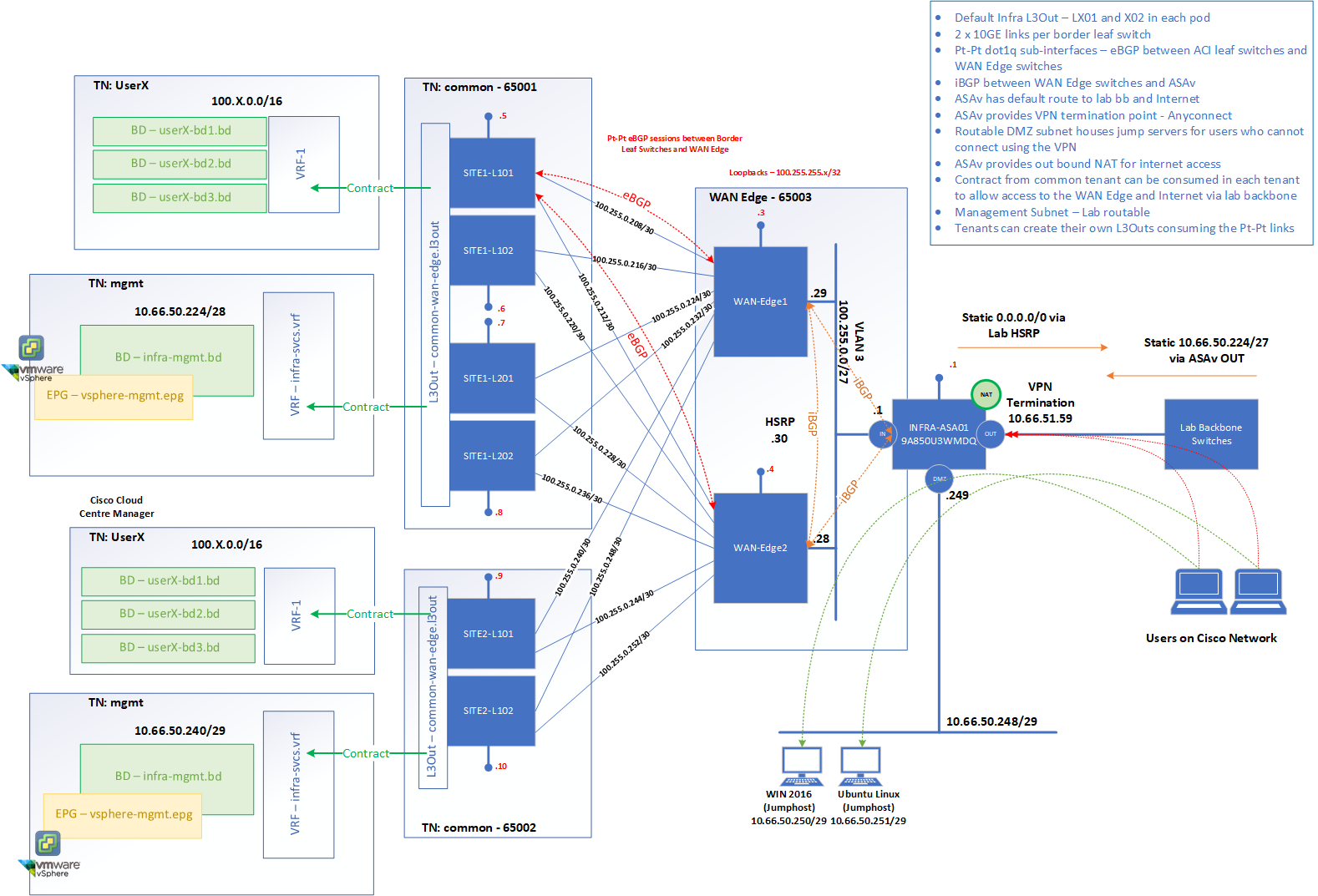


#### POD1/Pod2 Connectivity



### Logical Connectivity

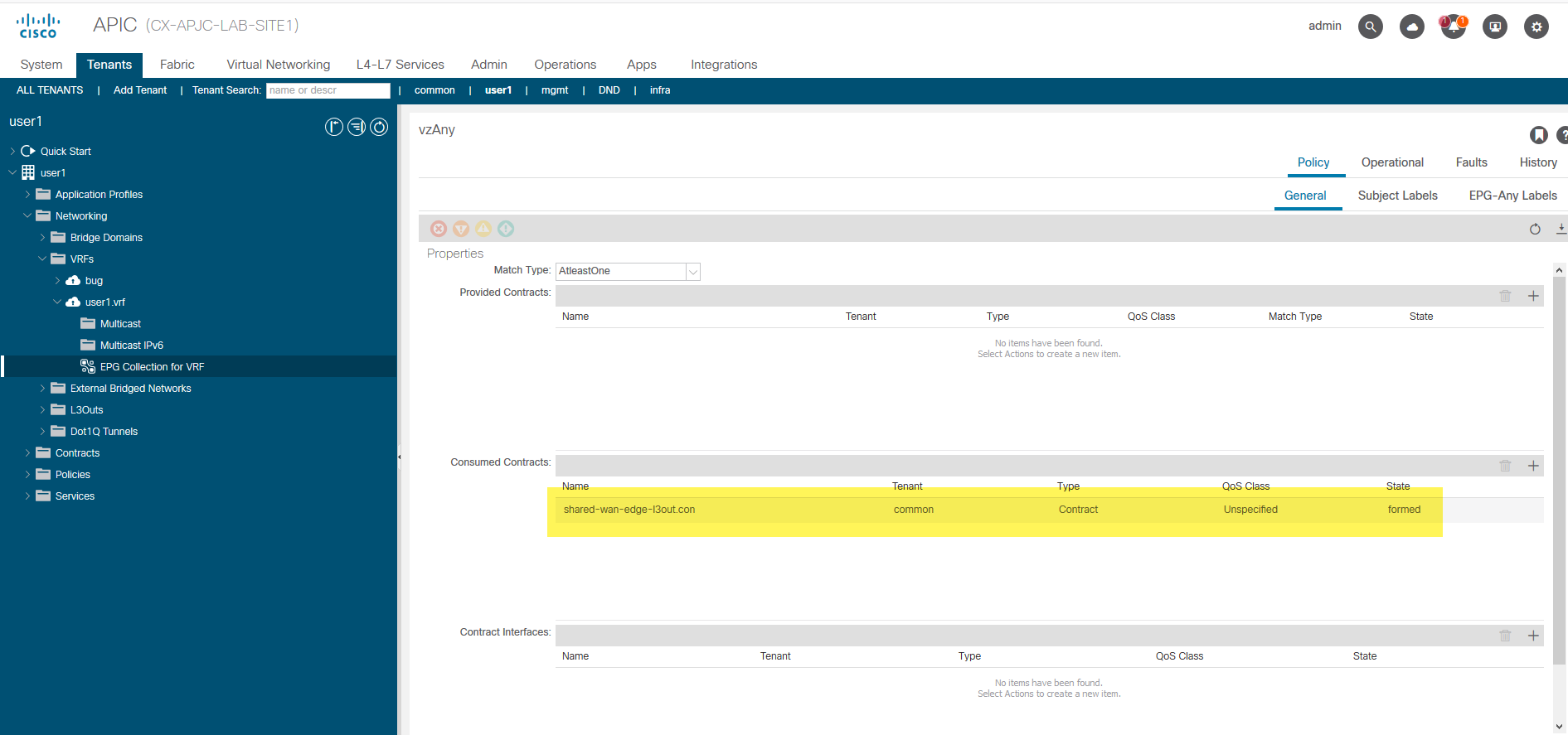
#### Common L3Out

[](https://calo-docs.cisco.com/lib/exe/fetch.php?media=external:sites:syd:autopods:wan-edge-logical.png)

### Internet Access for VMs

To gain internet access for your VMs, you can do one of two things:

**1. Consume the L3Out form the Common Tenant (Simple and Preferred)** - This can be done by consuming the contract provided by the Common L3Out in your user VRF:

[](https://calo-docs.cisco.com/lib/exe/fetch.php?media=external:sites:syd:autopods:wan-connectivity-l3out.png)

The ASAv in the WAN Edge block provides an outbout NAT for the subnets allocated to each user account. So for User x, if you leverage the 100.10x.0.0/16 in your user tenant, you will automatically be NAT'ed on egress to the WAN Edge and as such be able to access the internet.

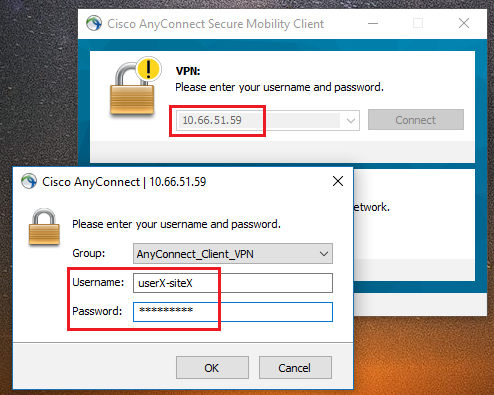
**2. Create your own L3Out** - If your design requires you to create your own L3Out in your user tenant, it can be done using the L3 (pt-pt) or L2 (vPC) connectivity between the leaf switches and the WAN Edge Switches. You will need to consume the L3Ext Domain and VLAN pool for your tenant and configure the WAN Edge switch accordingly.

* You will not have access to the ASAv to influence the outbound NAT, as such or User x, if you leverage the 100.10x.0.0/16 in your user tenant, you will automatically be NAT'ed on egress to the WAN Edge and as such be able to access the internet.
* **Please DO NOT modify the existing configuration on the WAN Edge Switching as this is shared infrastructure**

### External Access to your tenant

External access to your VMs can be achieved by connecting to the WAN Edge block in one of 2 ways:

**1. Anyconnect Access to the ASAv Instance in the WAN Edge:**

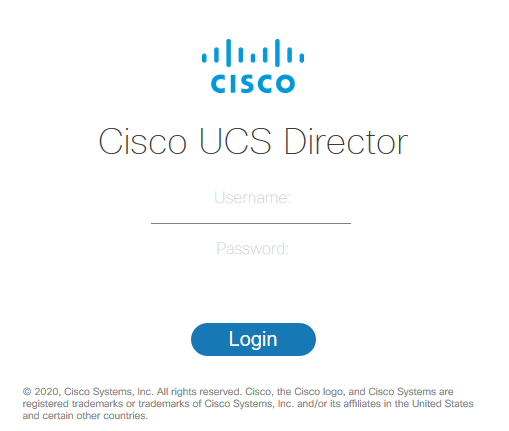
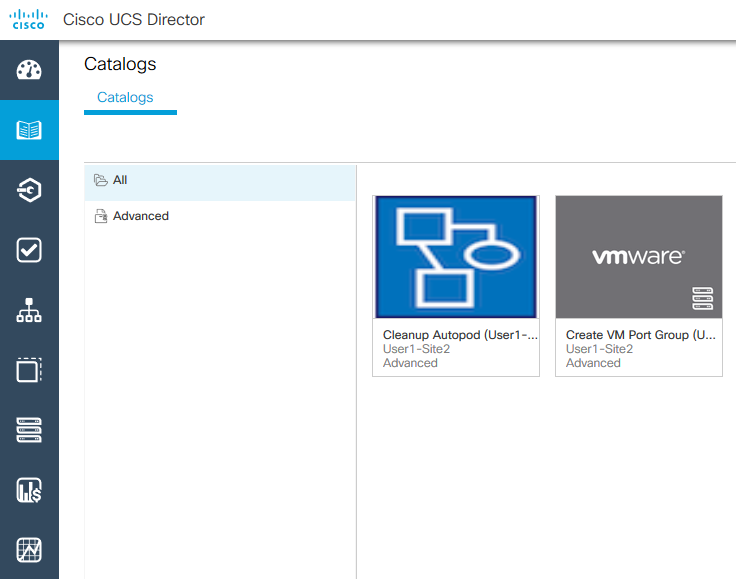
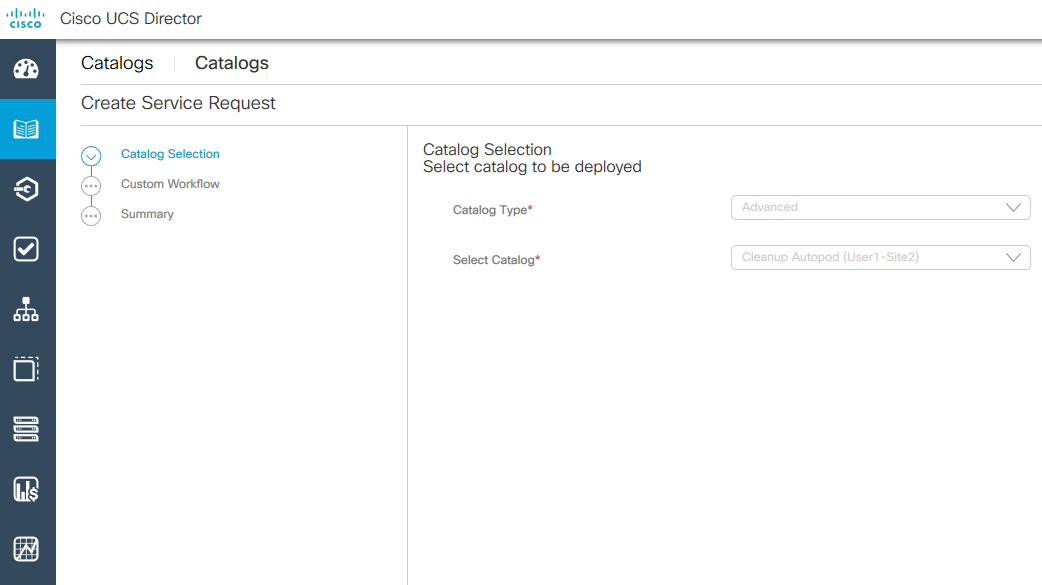
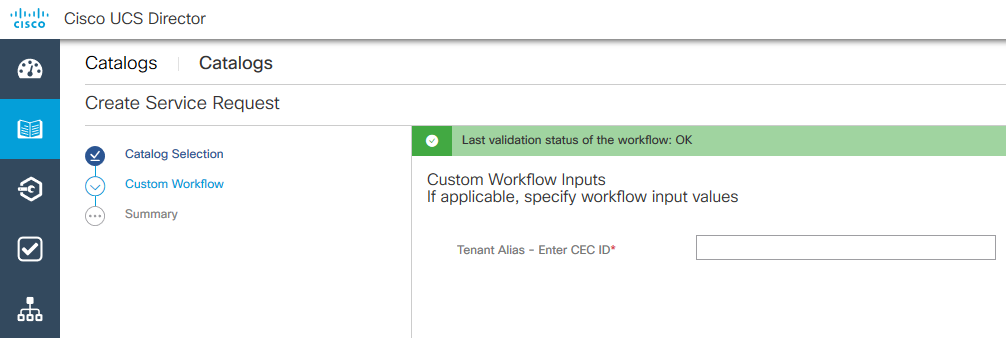
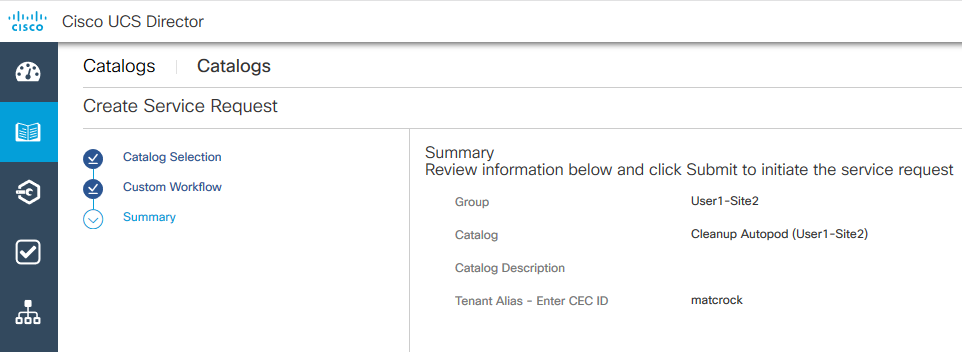


**2. RDP to Windows Jumphost:**

A screenshot of a cell phone

Description automatically generated

## AutoPod Cleanup

1. Login to the UCS Director portal (<https://portal.cxapjc.ciscolabs.com/>) with your AutoPod User credentials2. To cleanup the AutoPod for the user, launch the **Cleanup AutoPod** Service Request from the catalog.3. Click Next to commence the Service Request4. Enter in your CEC ID when prompted. Your CEC ID will be added as the tenant alias in ACI for identification.5. Click next to proceed with the cleanup of the AutoPod for the user.6. A new Service Request should successfully be raised as below.A screenshot of a cell phone

Description automatically generated7. You can now login to the APIC and verify the User tenant has been recreated using your CEC ID as the alias.A screenshot of a cell phone

Description automatically generated

* The cleanup tasks only include deleting/recreating the ACI tenant and deleting all VMs for the user.
* Access Policies for the User will also need to be alterted manually.
* Cleanup tasks for Endpoint and WAN Edge switches (NX-OS) will need to be performed manually.