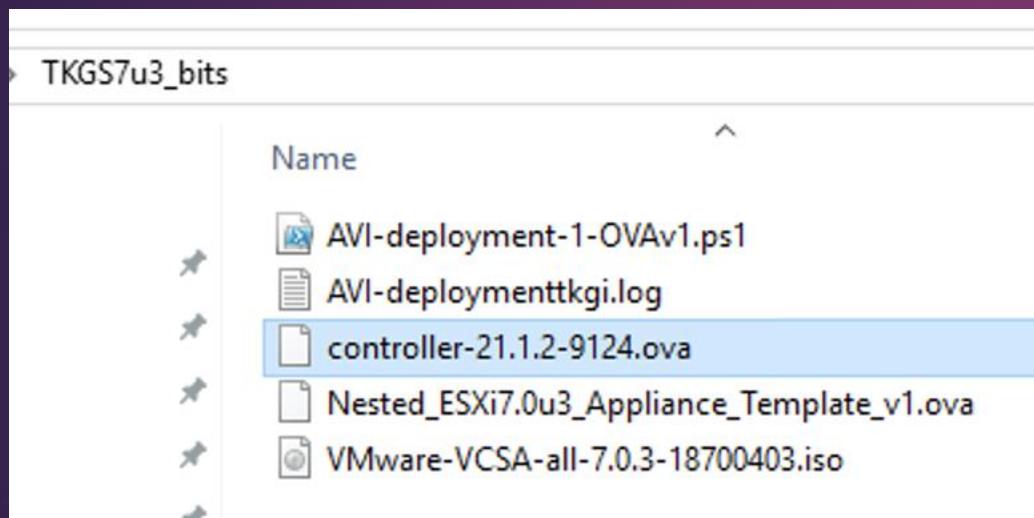


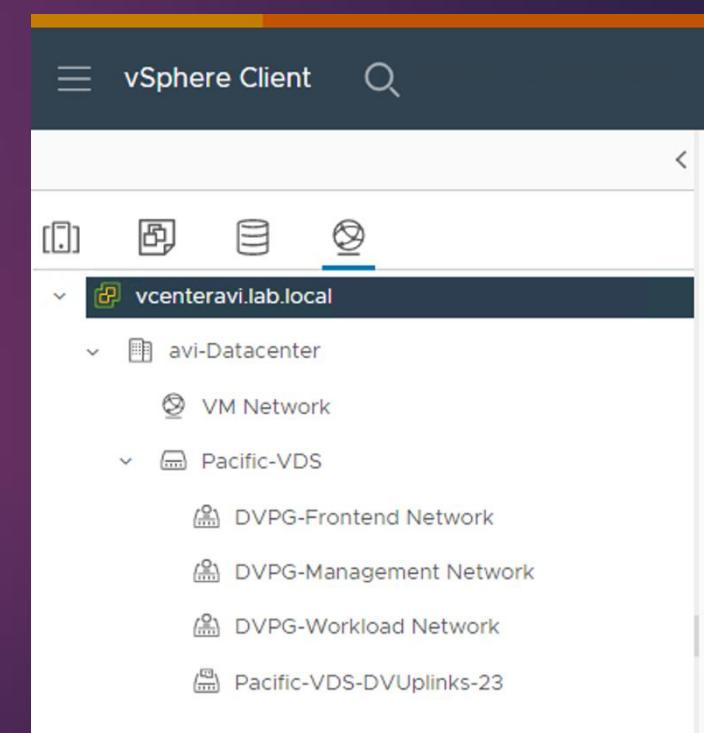
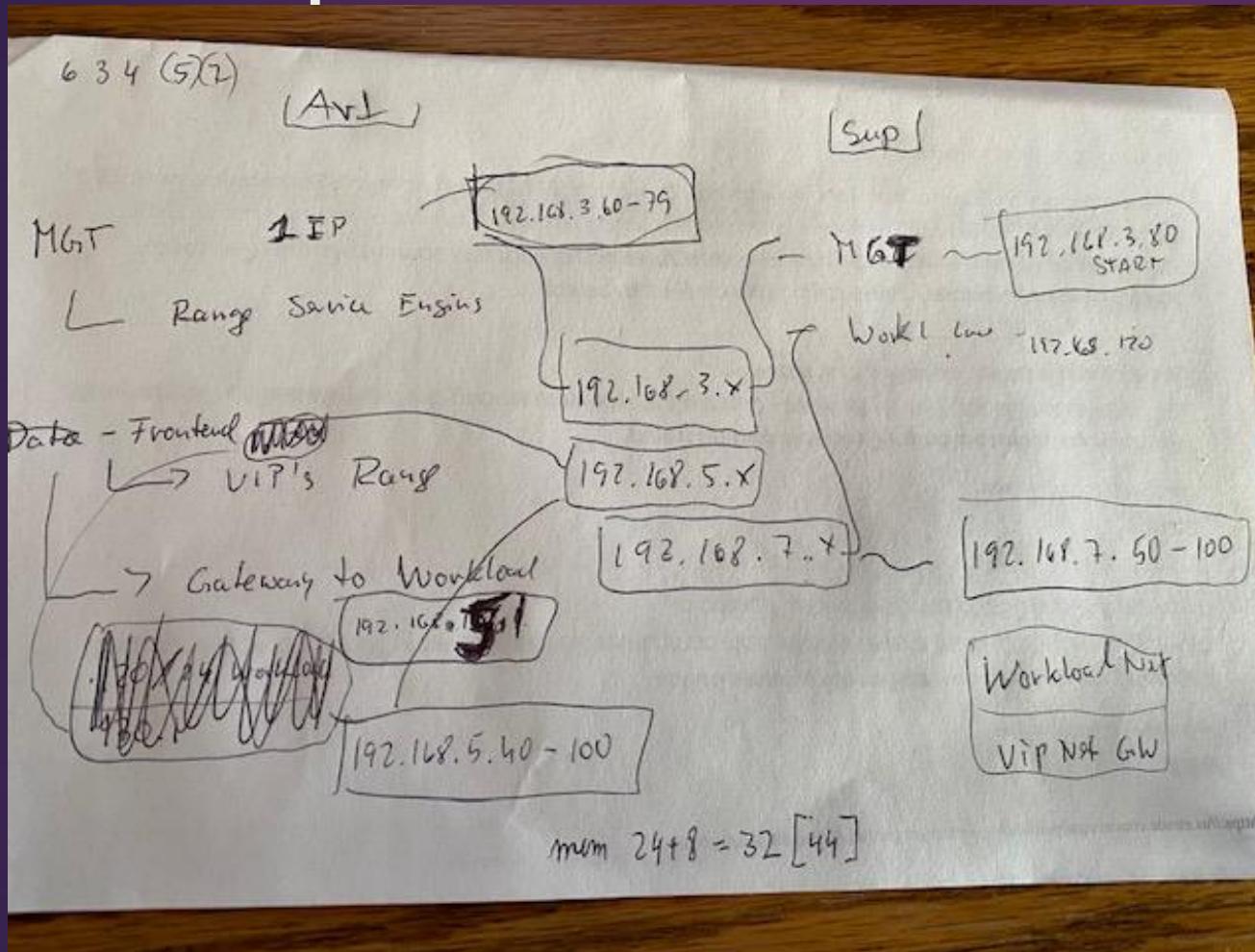
Deploy with AVI

VERSION 2

Versions used



Set up



My Network layout (.3)(.5)(.7)

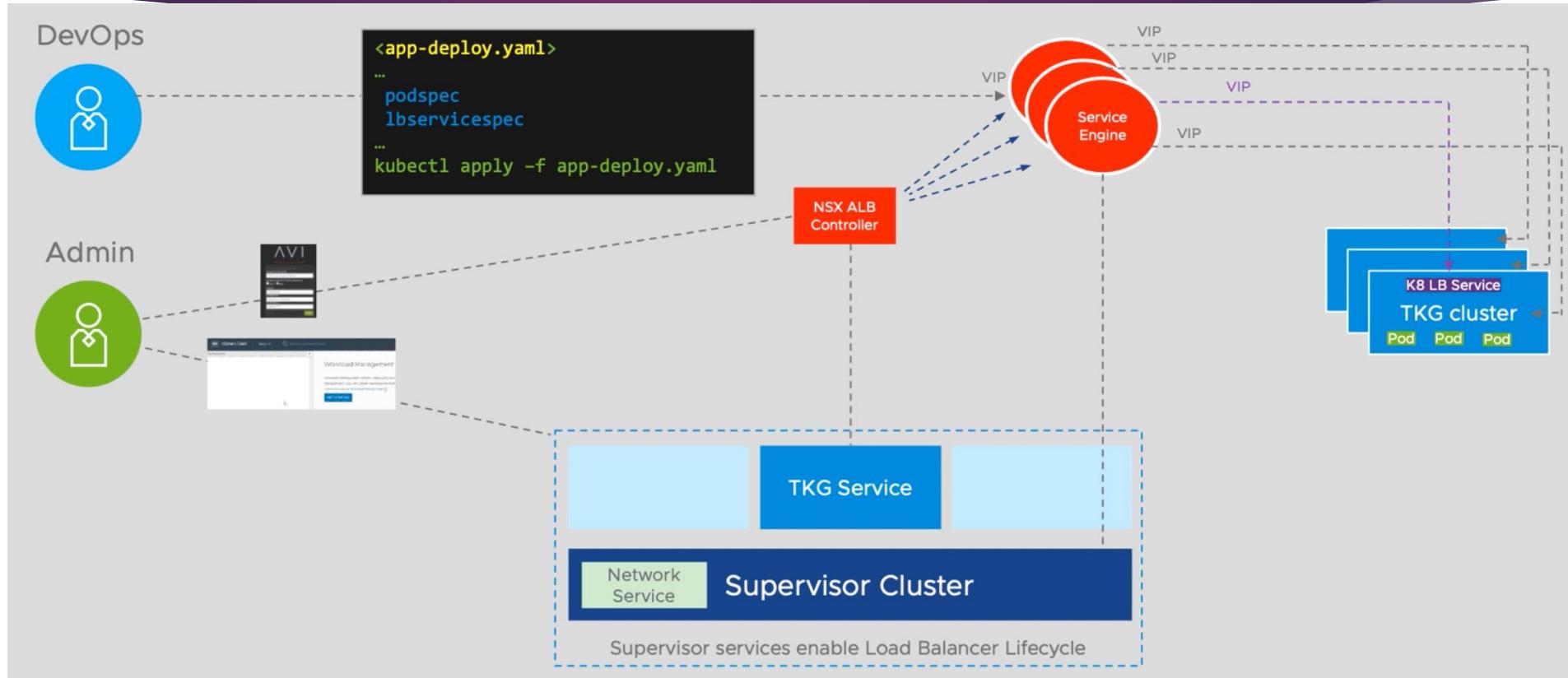
- ▶ **AVI** **Supervisor**
- ▶ 192.168.3.40 (AVI) 192.168.3.x MGT .50 vCenter .51-3 ESXi
- ▶ 192.168.3.60-79 MGT 192.168.3.80 (Start)
- ▶ 192.168.5.x Front
- ▶ 192.168.5.40-100 Front
- ▶ 192.168.7.x Workload
- ▶ Route 192.168.5.1 (192.168.7.0/24) Workload to frontend 192.168.7.50-100

Default AVI license after install

Displaying 2 items

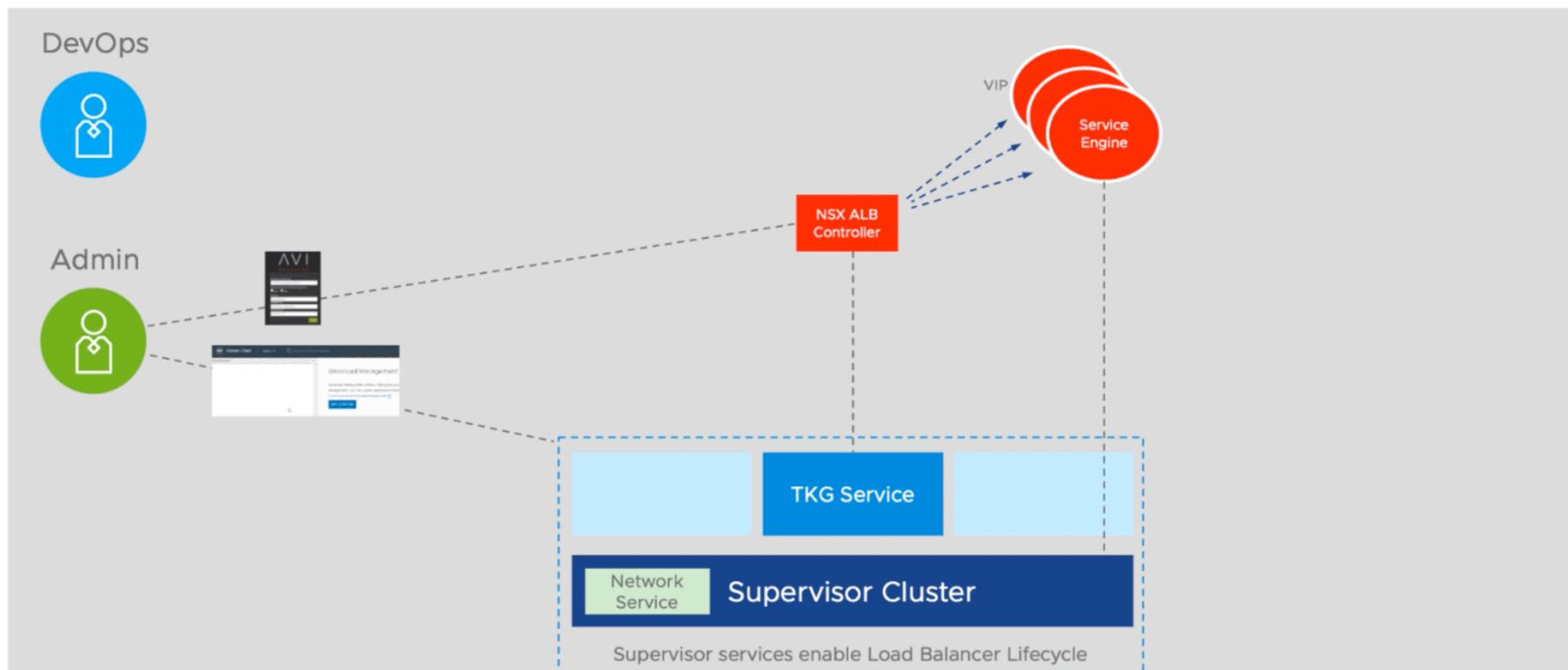
<input type="checkbox"/> <input type="button" value="▼"/>	Description	License ID	Tier	Service Cores	SE vCPUs	SE Sockets	Start Date	Expiry
<input type="checkbox"/>	Eval	Eval	ENTERPRISE	20	20	0	Oct 25, 2021	Nov 24, 2021
<input type="checkbox"/>	Trial	Trial	ENTERPRISE	2	2	0	Oct 25, 2021	Dec 31, 2034

AVI Layout



AVI Layout

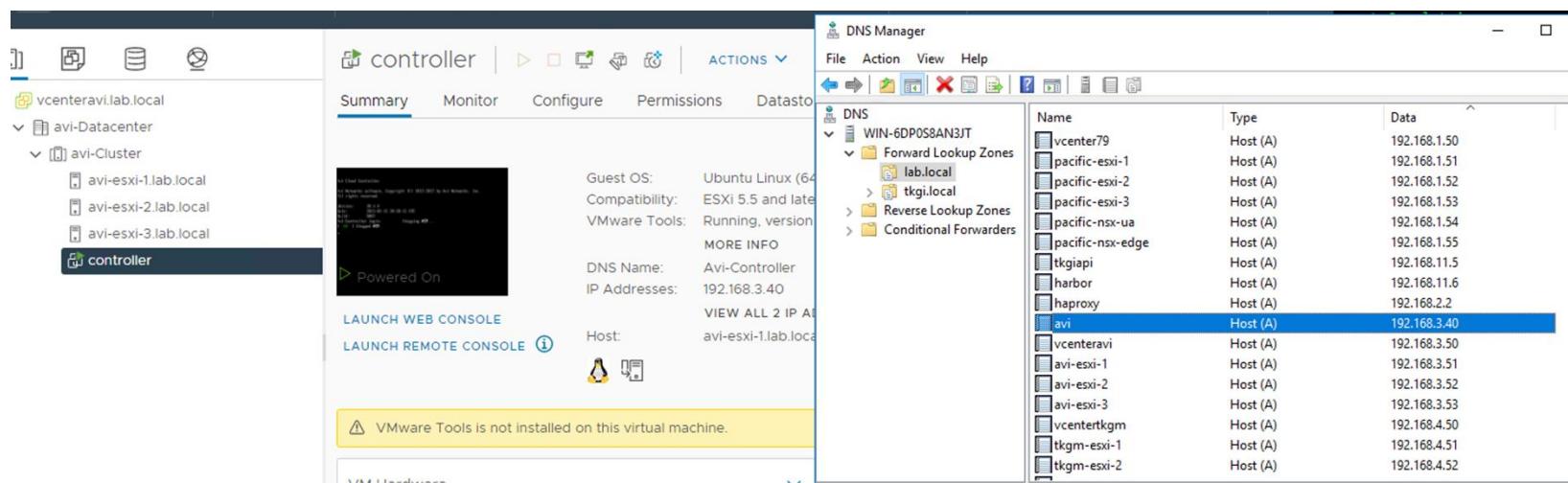
vSphere with Tanzu Integrated Load Balancing NSX Advanced Load Balancer Essentials Installation



Deploy

- ▶ Deploy Avi Controller OVA
- ▶ Deploy vCenter OVA
- ▶ Deploy ESXi hosts (vSAN)
- ▶ In my case all automated via William Lam's Powershell scripts

AVI 192.168.3.40 in DNS forward and reverse



AVI via Browser for final setup

- ▶ Open browser to <http://192.168.3.40>
- ▶ It may take a little bit before the GUI is up!

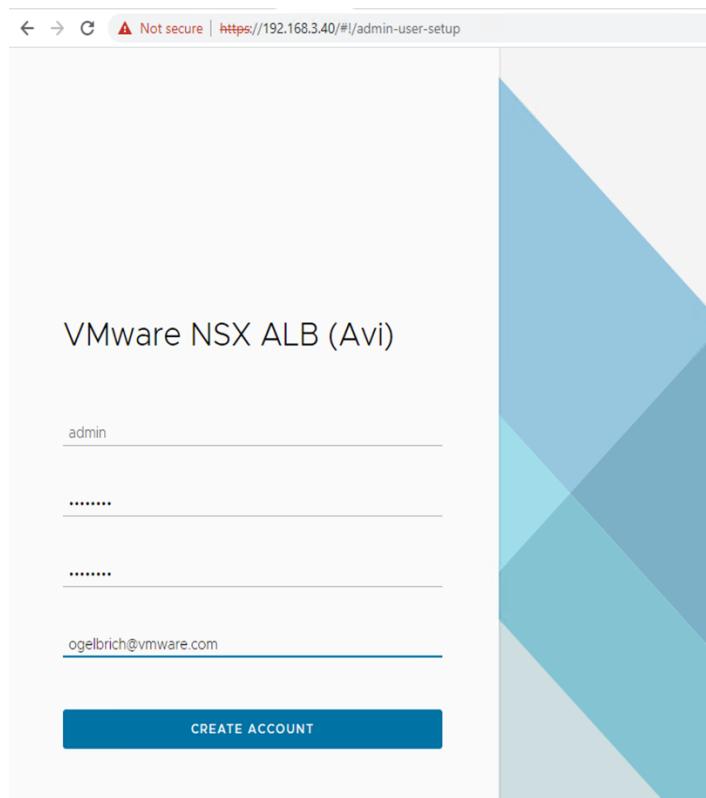
First time set up

VMware NSX ALB (Avi)

admin

ogelbrich@vmware.com

CREATE ACCOUNT



Welcome admin

System Settings Let's get started with some basic questions

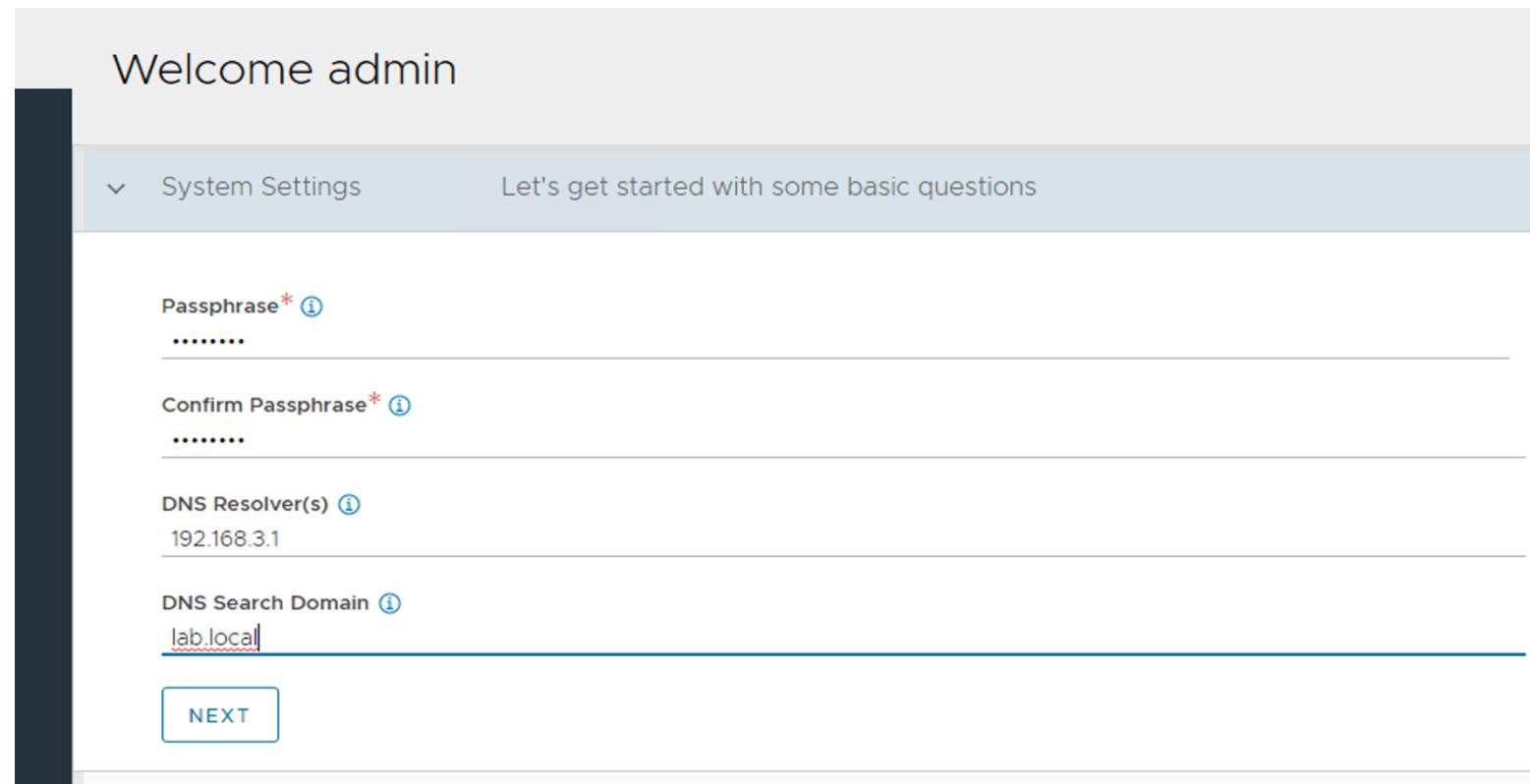
Passphrase* ⓘ
.....

Confirm Passphrase* ⓘ
.....

DNS Resolver(s) ⓘ
192.168.3.1

DNS Search Domain ⓘ
lab.local

NEXT



Frist time set up

▼ Email/SMTP

None Local Host SMTP Server Anonymous Server

From Address* 
admin@avicontroller.net

NEXT

▼ Multi-Tenant

IP Route Domain 
 Per tenant IP route domain Share IP route domain across tenants

Service Engines are managed within the 
 Tenant (Not shared across tenants) Provider (Shared across tenants)

Tenant Access to Service Engine
 Read Access No Access

Create Default Cloud

Not secure | https://192.168.3.40/#!/admin/infrastructure/cloud

NSX-ALB admin

Applications Operations Templates Infrastructure Administration

Displaying Past 6 Hours

Name	Type	Status	Actions
Default-Cloud	None	Green	

Edit Cloud: Default-Cloud

Infrastructure Data Center Network

Name*
Default-Cloud

Cloud Infrastructure Type

VMware VMware vCenter/vSphere ESX	openstack™	amazon web services™	Linux	Microsoft Azure	Google Cloud Platform	No Orchestrator
--------------------------------------	------------	----------------------	-------	-----------------	-----------------------	-----------------

Orchestrator: VMware vCenter/vSphere ESX

Default Cloud Data Center

The screenshot shows the vSphere Client interface with the 'Edit Cloud: Default-Cloud' dialog open. The left sidebar lists various hosts and controllers under the 'vcenteravi.lab.local' cluster. The 'avi-esxi-1.lab.local' host is selected. The main dialog has three tabs: Infrastructure, Data Center (selected), and Network. The 'Data Center' tab displays the 'avi-Datacenter' entry. The 'Network' tab contains sections for 'System IP Address Management Setting' and 'Virtual Service Placement Settings'. The 'Infrastructure' tab is partially visible.

vSphere Client

Edit Cloud: Default-Cloud

Infrastructure Data Center Network

• Select a Data Center •

Data Center

avi-Datacenter

• System IP Address Management Setting •

Default Network IP Address Management

DHCP Enabled IPv6 Auto Configuration

• Virtual Service Placement Settings •

Prefer Static Routes vs Directly Connected Network

Use Static Routes for Network Resolution of VIP

avi-esxi-1.lab.local

avi-esxi-2.lab.local

avi-esxi-3.lab.local

avi_controller

Default Cloud Networking

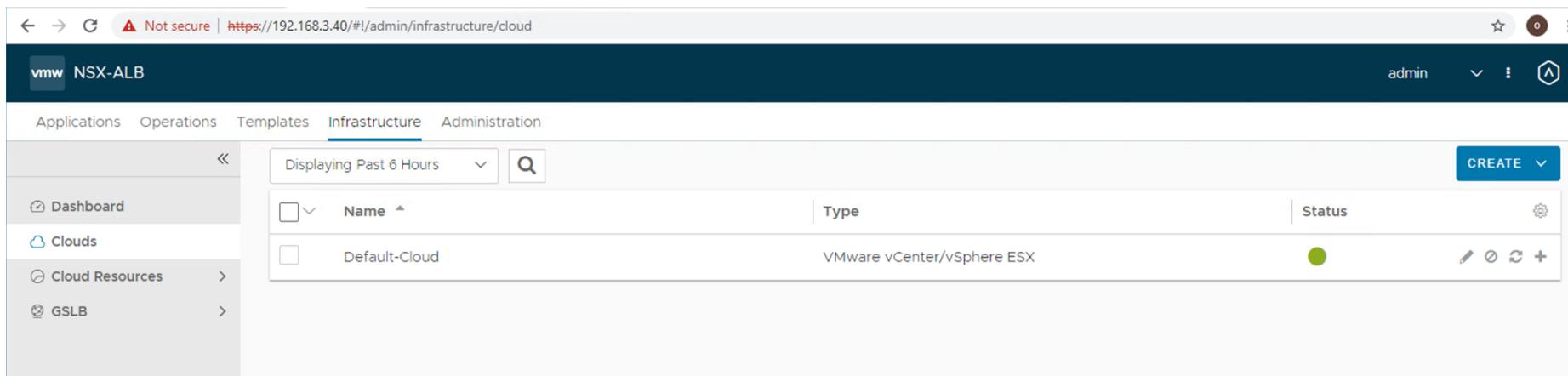
The screenshot shows the vSphere Client interface on the left and the 'Edit Cloud: Default-Cloud' configuration dialog on the right.

vSphere Client: The sidebar shows a selected connection named 'vcenteravi.lab.local'. Below it, under 'Pacific-VDS', there are three network configurations: 'DVPG-Frontend Network', 'DVPG-Management Network', and 'DVPG-Workload Network'. Other sections like 'avi-Datacenter' and 'VM Network' are also visible.

Edit Cloud: Default-Cloud Configuration:

- Management Network:** Set to 'DVPG-Management Network'.
- Service Engine:** Set to 'None'.
- IP Address Management for Management Network:**
 - DHCP Enabled
 - IPv6 Auto Configuration
- IP Subnet:** Set to '192.168.3.0/24'.
- Add Static IP Address Pool:** Contains the range '192.168.3.60-192.168.3.79'.
- Default Gateway:** Set to '192.168.3.1'.

Default Cloud is green



The screenshot shows the NSX-ALB web interface with the following details:

- Header:** vmw NSX-ALB, admin, Not secure | https://192.168.3.40/#/admin/infrastructure/cloud
- Navigation:** Applications, Operations, Templates, Infrastructure (selected), Administration
- Left Sidebar:** Dashboard, Clouds, Cloud Resources, GSLB
- Search Bar:** Displaying Past 6 Hours, Search icon
- Create Button:** CREATE
- Table Headers:** Name, Type, Status
- Table Data:** Default-Cloud (VMware vCenter/vSphere ESX, Green status)

Edit Cert (Pencil)

The screenshot shows the NSX ALB Administration interface. The URL in the address bar is <https://192.168.3.40/#/admin/administration/settings/systemaccess>. The page title is "System Access Settings". The left sidebar has a tree view with "Accounts", "Settings" (selected), "Authentication/Authorizat...", "Access Settings" (selected), "DNS/NTP", "Licensing", "Email/SMTP", "Tenancy Mode", "Upload HSM Packages", "DNS Service", "Pulse", "Controller", "System", and "User Credentials". The main content area displays various access mechanisms and their status:

- Access Mechanisms:
 - HTTP - Not Enabled
 - HTTPS - Not Enabled
 - Redirect HTTP to HTTPS - Not Enabled
 - Basic Authentication - Not Enabled
- Allowed Ciphers: None
- Allowed HMACs: None
- SNMP Community: None
- Management IP Access Control:
 - SSH Access: Any
 - CLI Shell Server Access: Any
 - API Access: Any
 - SNMP Access: Any
- Message of the Day:
- Login Banner:

Delete these two certs

Redirect HTTP to HTTPS

SSL Profile

SSL/TLS Certificate

Secure Channel SSL/TLS Certificate

• SNMP Setting

Create new Cert

Redirect HTTP to HTTPS

SSL Profile

System-Standard-Portal 

All

Allowe

aes12

Allowe

SSL/TLS Certificate 

Select SSL/TLS Certificate

Secure Channel SSL/TLS Certificate 

System-Default-Secure-Channel-Cert 

Allowe

allow

SSL/TLS Certificate

Select SSL/TLS Certificate 

Search 

System-Default-Portal-Cert

System-Default-Portal-Cert-EC256

System-Default-Secure-Channel-Cert

Create Certificate

SIM/MIP Version: 

Setting 

New cert with SAN

New Certificate (SSL/TLS): avi

General Certificate

General

Name*
avi

Type
Self Signed

Certificate

Common Name*
avi.lab.local

Subject Alternate Name (SAN) ⓘ

ADD

<input type="checkbox"/>	Name
<input type="checkbox"/>	192.168.3.40

SSL Profile

System-Standard-Portal

All

SSL/TLS Certificate ⓘ

All

Save of the cert for vCenter WCP enablement

The screenshot shows the NSX ALB interface with the following details:

- Header:** vmw NSX-ALB, admin, navigation icons.
- Menu:** Applications, Operations, **Templates**, Infrastructure, Administration.
- Left Sidebar:** Profiles, Policies, Groups, Security (selected), SSL/TLS Certificates (selected), SSL/TLS Profile.
- Table:** SSL/TLS Certificates. Columns: Name, Status, Common Name, Issuer Name, Algorithm, Self Signed, Valid Until. Data:

Name	Status	Common Name	Issuer Name	Algorithm	Self Signed	Valid Until
avi	●	avi.lab.local	avi.lab.local	RSA(2048 Bits)	Yes	2022-10-25 17:26:04
System-Default-Cert	●	System Default Cert	System Default Cert	RSA(2048 Bits)	Yes	2031-10-23 16:33:27
- Buttons:** CREATE, Copy to clipboard.
- Text:** Certificate content starting with -----BEGIN CERTIFICATE----- followed by a long base64 string.

Front end network (edit)

The screenshot shows the NSX-ALB web interface with the URL <https://192.168.3.40/#/admin/infrastructure/network/>. The page title is "Front end network (edit)". The top navigation bar includes links for Applications, Operations, Templates, Infrastructure (which is underlined), and Administration. The user is logged in as "admin". The left sidebar has sections for Dashboard, Clouds, Cloud Resources (with Service Engine and Service Engine Group options), Networks (with Routing), and GSLB. The main content area is titled "Default-Cloud" and displays a table of networks:

Name	Discovered Subnets	Configured Subnets	Static IP Pools
DVPG-Frontend Network	None	None	0
DVPG-Management Network	192.168.3.0/24	192.168.3.0/24 [20/20]	1
DVPG-Workload Network	None	None	0
Pacific-VDS-DVUplinks-23	None	None	0
VM Network	None	None	0

Front end network add subnet

Edit Network Settings: DVPG-Frontend Network

Name*
DVPG-Frontend Network

IP Address Management •

DHCP Enabled ⓘ IPv6 Auto Configuration ⓘ

+ Add Subnet

Network •

Displaying 0 items

IP Subnet Type

No items

Edit Network Settings: DVPG-Frontend Network

Name*

DVPG-Frontend Network

IP Address Management •

DHCP Enabled ⓘ IPv6 Auto Configuration ⓘ

Add/Modify Static IP Subnet •

IP Subnet * ⓘ

192.168.5.0/24

Static IP Address Pool

Result

The screenshot shows the NSX-ALB interface with the title "vmw NSX-ALB". The top navigation bar includes links for Applications, Operations, Templates, Infrastructure (which is underlined), and Administration. The user is logged in as "admin". The left sidebar has a "Clouds" section with "Default-Cloud" selected, and other sections like Dashboard, Cloud Resources (with Service Engine and Service Engine Group), Networks, Routing, and GSLB.

The main content area displays a table for "Cloud Resources" under "Default-Cloud". The table has columns for Name, Discovered Subnets, Configured Subnets, and Static IP Pools. The data is as follows:

Name	Discovered Subnets	Configured Subnets	Static IP Pools
DVPG-Frontend Network	None	192.168.5.0/24 [61/61]	1
DVPG-Management Network	192.168.3.0/24	192.168.3.0/24 [20/20]	1
DVPG-Workload Network	None	None	0
Pacific-VDS-DVUplinks-23	None	None	0
VM Network	None	None	0

Routing

The screenshot shows the NSX-ALB web interface with the following details:

- Header:** A red warning icon and the text "Not secure | https://192.168.3.40/#/admin/infrastructure/staticroute/".
- Logo:** "vmw NSX-ALB" logo.
- Navigation Bar:** Applications, Operations, Templates, Infrastructure (selected), Administration.
- Left Sidebar:** Dashboard, Clouds, Cloud Resources (Service Engine, Service Engine Group, Networks, Routing), GSLB.
- Current View:** Default-Cloud > Static Route.
- Sub-Menu:** Static Route (selected), BGP Peering, VRF Context, Gateway Monitor.
- Form Fields:** Prefix (dropdown menu), Next Hop.
- Message:** No items found.

Routing (work load to front)

Edit Static Route: 1

← → ⌂ Not secure | <https://192.168.3.40/#!/admin/infrastructure/staticroute/>

Gateway Subnet *

192.168.7.0/24

Next Hop *

192.168.5.1

vmw NSX-ALB

Applications Operations Templates Infrastructure Administration

Dashboard Clouds Cloud Resources Service Engine Service Engine Group Networks Routing GSLB

Default-Cloud

Static Route BGP Peering VRF Context Gateway Monitor

Prefix 192.168.7.0/24 Next Hop 192.168.5.1

The screenshot shows the NSX-ALB interface for editing a static route. The top navigation bar includes links for Applications, Operations, Templates, Infrastructure (which is selected), and Administration. The left sidebar has sections for Dashboard, Clouds, Cloud Resources (with sub-options like Service Engine, Service Engine Group, Networks, and Routing), and GSLB. The main content area is titled 'Default-Cloud' and contains tabs for Static Route, BGP Peering, VRF Context, and Gateway Monitor. Under the Static Route tab, there is a table with two rows. The first row has columns for 'Prefix' (with a dropdown menu) and 'Next Hop'. The second row shows '192.168.7.0/24' in the Prefix column and '192.168.5.1' in the Next Hop column. A red asterisk is present next to the 'Gateway Subnet' and 'Next Hop' fields, indicating they are required.

IPAM

The screenshot shows the NSX-ALB web interface at <https://192.168.3.40/#/admin/template/profile/ipam-profile>. The page title is "vmw NSX-ALB". The navigation bar includes links for Applications, Operations, Templates (which is the active tab), Infrastructure, and Administration. On the left, a sidebar under "Profiles" lists Application, TCP/UDP, Persistence, Health Monitors, Analytics, IPAM/DNS Profiles (which is highlighted), and Custom IPAM/DNS. The main content area features a search bar with a magnifying glass icon and a dropdown menu labeled "Name". A large blue "CREATE" button is visible, with "IPAM Profile" currently selected from a dropdown menu. A red callout box points to the "CREATE" button.

IPAM

Edit IPAM/DNS Profile: my-ipam

Name *  my-ipam

Type *  Avi Vantage IPAM

Allocate IP in VRF 

Avi Vantage IPAM Configuration

Cloud for Usable Network  Default-Cloud

Usable Network *  DVPG-Frontend Network 

+ Add Usable Network

← → ⌂  Not secure | <https://192.168.3.40/#/admin/template/profile/ipam-profile>

vmw NSX-ALB

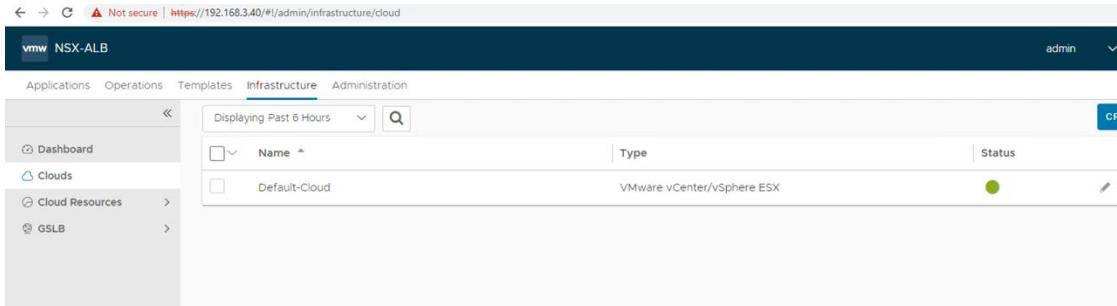
Applications Operations Templates Infrastructure Administration

Profiles

	Name	Type
<input type="checkbox"/>	my-ipam	Avi Vantage IPAM

Application
TCP/UDP
Persistence
Health Monitors
Analytics
IPAM/DNS Profiles
Custom IPAM/DNS
Traffic Clone

Default Cloud edit and add IPAM



The screenshot shows the NSX-ALB web interface. The top navigation bar includes links for Applications, Operations, Templates, Infrastructure (which is the active tab), and Administration. A user 'admin' is logged in. On the left, a sidebar lists Dashboard, Clouds (selected), Cloud Resources, and GSLB. The main content area displays a table titled 'Clouds' with one entry: 'Default-Cloud' of type 'VMware vCenter/vSphere ESX'. The status of this cloud is green. There are 'Edit' and 'Delete' icons next to the entry.

Name	Type	Status
Default-Cloud	VMware vCenter/vSphere ESX	Green (Healthy)

Default Cloud edit and add IPAM

The screenshot shows a user interface for managing IPAM profiles. At the top, there is a navigation bar with tabs: 'Cores' (which is active), 'IPAM Profile', 'DNS Resolver', and 'Cloud'. Below the navigation bar, there is a search bar labeled 'Search'. A list of IPAM profiles is displayed, with one profile highlighted in green: 'my-ipam'. This profile has a small icon next to it and the text 'STATE BASED DNS REGISTRATION'. The other profiles in the list are 'Select IPAM Profile' and 'ipam-profile'. The background of the interface is white, and there is a dark vertical sidebar on the left.

Cores

IPAM Profile ?

Select IPAM Profile

Search

my-ipam

STATE BASED DNS REGISTRATION

DNS Resolver ?

The screenshot shows the NSX ALB administration interface. The top navigation bar includes the VMW logo, the text "NSX-ALB", and a user dropdown for "admin". Below the navigation is a horizontal menu with tabs: Applications, Operations, Templates, Infrastructure, and Administration, with "Administration" being the active tab. On the left, a sidebar lists several categories: Accounts, Settings (which is currently selected), Authentication/Authorization, Access Settings, DNS/NTP, Licensing, Email/SMTP, and Tenancy Mode. The main content area is titled "System Access Settings" and contains the following information:

- Access Mechanisms:
 - HTTP - Not Enabled
 - HTTPS - Not Enabled
 - Redirect HTTP to HTTPS - Not Enabled
 - Basic Authentication - Not Enabled
- Allowed Ciphers:
 - None
- Allowed HMACs:
 - None
- SNMP Community:
 - None

A pencil icon in the top right corner of the main content area indicates that changes can be saved.

Default Cloud edit and add IPAM

Due to a bug in u3 make sure basic auth is enabled

Update System Access Settings

• System Access Settings •

HTTPS Access to System HTTP Access to System
HTTPS Port * ?
443

Redirect HTTP to HTTPS Allow Basic Authentication ?
HT
81
* I

SSL Profile
System-Standard-Portal

SSL/TLS Certificate ?
avi *

Secure Channel SSL/TLS Certificate ?
System-Default-Secure-Channel-Cert *

Allowed Ciphers ?
aes128-ctr, aes256-ctr

Allowed HMACs ?
hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etr

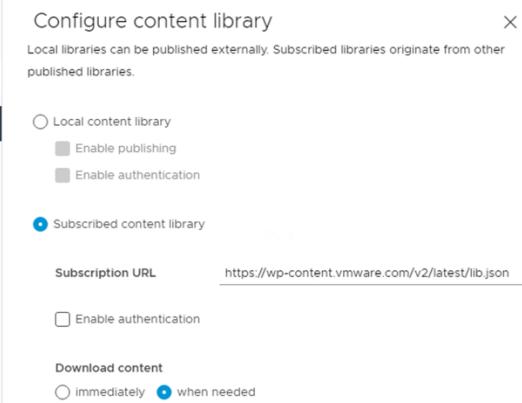
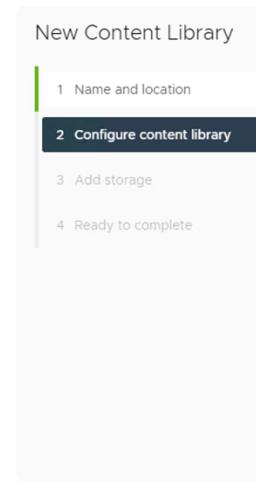
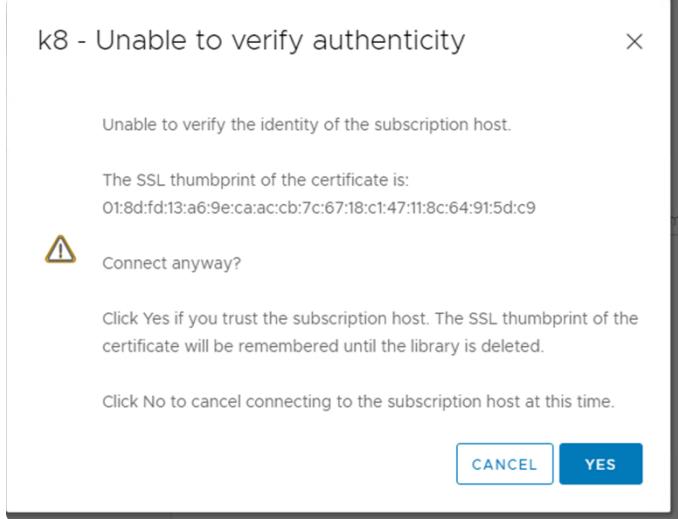


WCP enablement add content Lib

The screenshot shows the vSphere Client interface with the following details:

- Header:** Not secure | https://192.168.3.50/ui/app/content-libraries
- Left Sidebar:** Home, Shortcuts, Inventory, Content Libraries (selected), Workload Management, Global Inventory Lists, Policies and Profiles, Auto Deploy, Hybrid Cloud Services.
- Content Area:** Content Libraries. A modal window titled "New Content Library" is open, showing a step-by-step process:
 - Name and location** (selected)
 - Configure content library
 - Add storage
 - Ready to complete
- Modal Fields:**
 - Name:** k8
 - Notes:** (Empty text area)
 - vCenter Server:** vcenteravi.lab.local

Content lib subscription



New Content Library

1 Name and location

2 Configure content library

3 Apply security policy

Apply security policy

Applying security policy enforces strict validation while importing a synchronization of OVF library items.

Apply Security Policy

OVF default policy ▾

New Content Library

1 Name and location

2 Configure content library

3 Apply security policy

4 Add storage

5 Ready to complete

Add storage

Select a storage location for the library contents.

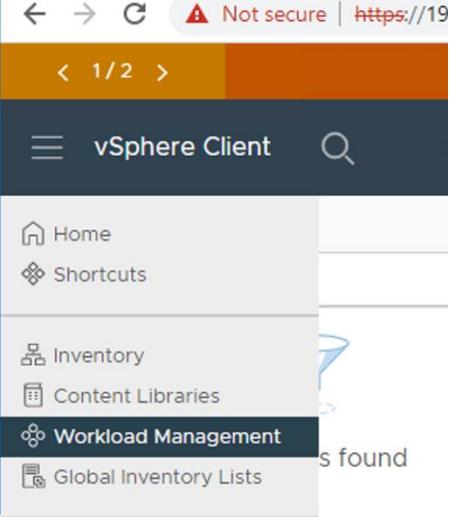
Filter

Name	Status	Type	Capacity	Free
avi-esxi...	Normal	VMFS 6	5.75 GB	3.91 GB
avi-esxi...	Normal	VMFS 6	5.75 GB	3.91 GB
vsanDat...	Normal	vSAN	899.98 GB	839.9 GB
avi-esxi...	Normal	VMFS 6	5.75 GB	4.34 GB

4 items

Content lib cont...

WCP enablement



The screenshot shows the vSphere Client interface. At the top, there's a header bar with navigation icons and a "Not secure | https://19" status message. Below the header is a dark blue navigation bar with the "vSphere Client" logo and a search icon. The main menu on the left includes "Home", "Shortcuts", "Inventory", "Content Libraries", "Workload Management" (which is highlighted in dark blue), and "Global Inventory Lists". A tooltip "s found" is visible near the "Workload Management" item. On the right side of the screen, there's a "Workload Management" configuration window with fields for basic information like First Name, Last Name, Work Email, Company, Country, State, and Zip Code.

Workload Management [Free Evaluation](#)

evaluation period.

Already have a Tanzu edition license?

[ADD LICENSE](#)

Basic Information

First Name	Orf
Last Name	Gelbrich
Work Email	ogelbrich@vmware.com
Company	VMware
Country	United States
State	Texas
Zip Code	76042

Regarding product and services, newsletters, invitation-only events (optional)

I have read and accept the VMware End User License Agreement

GET STARTED

Workload Management

Workload Management enables deploying and managing workloads across multiple clusters. By using Workload Management, you can leverage best practices for workload management. You can configure a vSphere cluster for Workload Management, and you can create namespaces that provide compute and storage resources for your Kubernetes applications. You can also configure resource consumption.

Learn more about Workload Management [↗](#)

GET STARTED

WCP Enablement cont...

Select the vCenter Server system that will host this Supervisor Cluster.

Select a vCenter Server system

VCENTERAVI.LAB.LOCAL

Select the networking stack that will provide connectivity to this Supervisor Cluster.

Select a networking stack



NSX
(Not Available)

Supports vSphere Pods and Tanzu Kubernetes clus!



vSphere Distributed Switch (VDS)

Supports Tanzu Kubernetes clusters.

NEXT

Workload Management

BACK

VIEW PRE

This vSphere cluster will be set up as a Supervisor Cluster. Select a vSphere cluster with enough space to support your Kubernetes workloads.

Cluster Name	Number of Hosts	Available CPU	Available Memory
avi-Cluster	3	63.59 GHz	139.73 GB

NEXT

WCP Enablement cont...

WCP Enablement cont...

Select a storage policy to be used for datastore placement of Kubernetes control plane VMs. The policy applies to the vSphere environment.

Control Plane Storage Policy

pacific-gold-storage-policy



[VIEW DATASTORES](#)

[NEXT](#)

WCP Enablement cont...

Workload Management

[BACK](#) [VIEW NETWORK TOPOLOGY](#)

Name i	avi
Load Balancer Type i	NSX Advanced Load Balancer v
If you have not yet configured HAProxy, VIEW OPTIONS	
NSX Advanced Load Balancer Controller IP i	192.168.3.40:443
Username i	admin
Password i @
Server Certificate i	<pre>s0+FHC1dE+9hvXF1ly7TsLzTGFt8TLCjjHqgU41W8t4Z2LPrU8Sx51UbrIeuU6Q/ OtDa5cc= -----END CERTIFICATE-----</pre>

[NEXT](#)

WCP Enablement cont...

Network Mode i	Static
Network i	DVPG-Management Network
Starting IP Address i	192.168.3.80
Subnet Mask i	255.255.255.0
Gateway i	192.168.3.1
DNS Server(s) i	10.197.79.7
DNS Search Domain(s) i	lab.local <small>Optional</small>
NTP Server(s) i	10.128.152.81

Port Group ①

Port Group	vSphere Distributed Switch
DVPG-Manage	Pacific-VDS
DVPG-Fronter	Pacific-VDS
DVPG-Worklo	Pacific-VDS

Network Name ① dvpg-workload network
You can edit this default setting

Layer 3 Routing Configuration

IP Address Range(s) ① 192.168.7.150-192.168.7.200

Subnet Mask ① 255.255.255.0

Gateway ① 192.168.7.1

VIEW NETWORK TOPOLOGY

Network Mode ① Static

Internal Network for Kubernetes Services ① 10.96.0.0/23

Port Group ①

Port Group	vSphere Distributed Switch
DVPG-Manage	Pacific-VDS
DVPG-Fronter	Pacific-VDS
DVPG-Worklo	Pacific-VDS

3 items

WCP Enablement cont...

WCP Enablement cont...

0 items

Network Name i !
Name must be DNS compliant.

Layer 3 Routing Configuration

IP Address Range(s) i

Subnet Mask i

Gateway i

DNS Server(s) i

NTP Server(s) i

NEXT

WCP Enablement cont...

The screenshot shows a configuration interface for a network named "dvpg-workload network". The interface includes fields for Layer 3 Routing Configuration, DNS Server(s), and NTP Server(s). A "NEXT" button is at the bottom.

Network Name	<input type="text" value="dvpg-workload network"/>
Layer 3 Routing Configuration	
IP Address Range(s)	<input type="text" value="192.168.7.150-192.168.7.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.7.1"/>
DNS Server(s)	<input type="text" value="10.197.79.7"/>
NTP Server(s)	<input type="text" value="10.128.152.81"/>

NEXT

WCP Enablement cont...

8. Review and Confirm

Review and confirm all details and default settings to start this Supervisor Cluster.

Advanced Settings

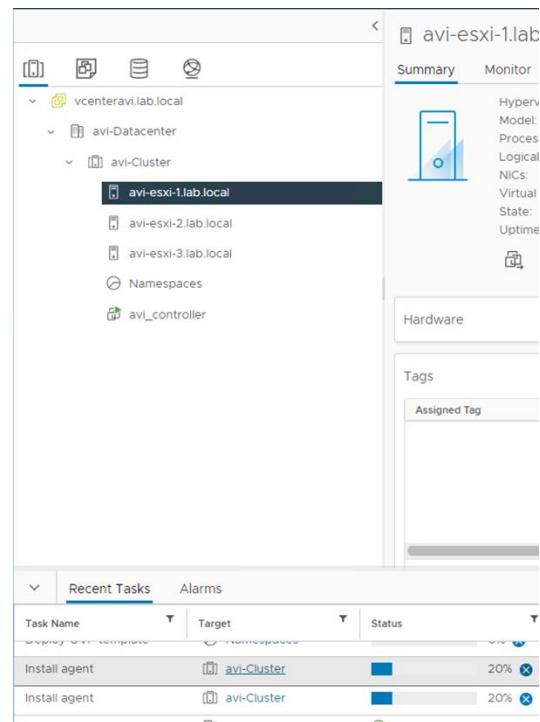
Control Plane Size (i) Small (Max # of pods: 2000, CPUs: 4, Memory: 16 GB, Storage: 32 GB) ▼
You can edit this default setting

API Server DNS Name(s) (i) E.g. domain.local
Optional

Review and confirm the steps above. Click Finish to start setting up avi-Cluster as a Supervisor Cluster.
You can view these configuration details in the cluster view under the Configure tab.

FINISH

WCP Enablement cont...



Did I fat finger the AVI password? Edit here:

The screenshot shows the vSphere Client interface with the following details:

- Left Panel:** Shows a tree view of the vSphere environment. At the top level is **vcenteravi.lab.local**, which contains **avi-Datacenter**, **avi-Cluster**, and **Namespaces**. **avi-Cluster** is selected and expanded, showing three ESXi hosts: **avi-esxi-1.lab.local**, **avi-esxi-2.lab.local**, and **avi-esxi-3.lab.local**. Under **Namespaces**, there are three Supervisor Control Plane VMs: **SupervisorControlPlaneVM (1)**, **SupervisorControlPlaneVM (2)**, and **SupervisorControlPlaneVM (3)**.
- Top Bar:** The title bar says **avi-Cluster**. Below it are tabs: **Summary**, **Monitor**, **Configure** (which is selected), **Permissions**, **Hosts**, **VMs**, **Namespaces**, and **Datastores**.
- Configure Tab Content:** The **Network** section displays network settings for namespaces. It includes a **Load Balancer** section.
 - Name:** avi
 - Load Balancer Type:** NSX Advanced Load Balancer
 - NSX Advanced Load Balancer:** Controller IP: 192.168.3.40:443
 - Username:** admin (with an **EDIT** button)
 - Password:** (Redacted with a red oval)
 - Server Certificate:** -----BEGIN CERTIFICATE-----

Did I fat finger the AVI password?

Config Status

X

Current Status: ○ Configuring

! Error (1) ! Warning (0) i Info (0)

Status Messages

- ! The control plane VM 4202aa30779d4936ec9a64301df0434b was unable to authenticate to the load balancer (Avi - http s://192.168.3.40:443/api/cluster) with the username 'admin ' and the supplied password. Validate the Supervisor cluster loa d balancer's authentication configuration.

1 item

OK

Still an issue... ssh to vCenter...

- ▶ ssh to vCenter ssh root@192.168.3.50
- ▶ shell
- ▶ /usr/lib/vmware-wcp/decryptK8Pwd.py
- ▶ ssh to IP and use password from above command
- ▶ kubectl get events -n vmware-system-ako -w
- ▶ kubectl get pods -A | grep ako
- ▶ kubectl logs -n vmware-system-ako pod/vmware-system-ako-ako-controller-manager-85bb7dd4-wnhrg
- ▶ kubectl get secrets -A | grep -i ako
- ▶ kubectl describe secrets/avi-secret -n vmware-system-ako
- ▶ kubectl get secret avi-secret -n vmware-system-ako -n vmware-system-ako -o jsonpath='{.data}'
- ▶ echo "Vk13YXJIMSE=" | base64 --decode

Well look what we have here user ID with a training space...

```
root@4202c1b4753322614d82535f07f425bd [ ~ ]# ^C
root@4202c1b4753322614d82535f07f425bd [ ~ ]# kubectl get secrets -A | grep -i ako
vmware-system-ako
    default-token-m5bb
    default-token-m5bb
    kube
    kubernetes.io/service-account-token
        Opaque
        kubernetes.io/service-account-token      3      122m
root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]# kubectl get secret avi-secret -n vmware-system-ako -n vmware-system-ako -o jsonpath='{.data}'
{"certificateAuthorityData": "LS0tLS1CRUdjT1BDRVJUSUZQdFURS0tLS0tCkJSUMwVENDQWtZ0f3SUJBZ01VUkdXeU5Tbk1Pb2JHSVhnZG5zDVZNEdidjRzd0RRWUpLb1pJaHzjTkFRRUwKQ1FBd0dERVdNQ1FHQTFRUF3d05ZWfpwTG14af1p
NXNiMk5oYkRBZU23MH1NVEV3TwPVeE56STJNRFJhRncweQpNakV3TwPVeE56STJNRFJhTUJneEZqQVVCZ05WQkFNTURXRjJhUzVzIwDjdWJH0WpZV3d3Z2dFaU1BMEdDU3FHC1NjYjNEUUVQVFVQUE0SUJEd0F3Z2dFS0FvSUJBURBZVFVbmzY0RHR31Fb
FBnMHNwZ01YdwipDN3h0K2UzUTIKedRZM29RbTRLbVExeFR3N0ZRwktXeG5hQkp0SkNCKzcxS1NFU1dNTVh2L3NkV1N0Y2x3TD82a011SDcxhEFzTQpxEfZNvys1NmdraVR2cdhW1Q2akXRLFRqNlZ1o3VlxFTV10aHJPNoSzR3NTcDJLQjJzdWFn1pEvj
dsZkhKCKh9z1UrATjol2UxYuowMG53R3F5QxFySWRkUVBuaHRmV09vREVIkuhUdDIdcmV6UE14N3ZhS2dRVnY5bVE0WkwKQjBKdXJQu19zUGU0aWJuaf13UVdVYkNuS2NHVjNrKytudHRUVF3WlhPNVA1WUh2ZF1LNTh2eW5hd2JC52sxbApjT0xJMUr4rdms
rUDJid0ZpmFVDTEkycGcybm5aaERNTkZVTUptNHbRz2wVEVKRmtsdzZkQwdNQkFBR2pfeKFskc180EdBMVvkRVFRSU1BYUhCTUWvQX1nd0RRWUpLb1pJaHzjTkFRRUxCUUFEZ2dFQkFc1dhTmVVZGJ0ky8wV1oKYo1axZSM0FW3d6K11Re1R4cXRNS2xs
e1d0YmJMy9zU1V6bEhYN0tTbEfZc3ppMC90t1FpZU8xd25GhGFhApIRzg1UmY3bTBZUk5TeE5RbD1CcXhXVytjdEVh0tKU3kz0W93ckdwExR0W11LzZyVjhiQzBWeRul0dLQTkwCnRuUe9BN09WcEpwU3juRH16SmRaRmJhBvd0em9MdhyZ25fREN0W
jRPUTJfb01LbhE1Q113RxkrSUJ15k1Q0FYKZehS0Qjg5YXlnNysxSnpPsN2c1NL1Bxu31EU1BIRjh0c2Q5SFJVZz1qN3Y0cUxGcWNiQ1dpWkp1aXpQbnV0bgpzTytGSENsZEUr0Wh2WEzpbhK3VHNW1RHZ1Q4VExDSpIcWdVNGxXOHOQ0WjJMUHJVOFN4NT
FVYnJJZXVN1EvCk90RGFTY2M9Ci0tLS0tRU5EIEFUJRK1DQVRFLS0tLS0=, "password": "VkJ13YXJ1MSE=", "username": "YWRtaW4g"}root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]# echo "VkJ13YXJ1MSE=" | base64 --decode
VMware1!root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]#
root@4202c1b4753322614d82535f07f425bd [ ~ ]# echo "YWRtaW4g" | base64 --decode
admin root@4202c1b4753322614d82535f07f425bd [ ~ ]#
```

Activate Windows
Go to Settings to activate Windows.

The system should update this user field but I have no time...

- ▶ echo -n '----BEGIN CERTIFICATE----'
- ▶ My cert here....OtDa\$cc=
- ▶ -----END CERTIFICATE-----' > ./certificateAuthorityData.txt
- ▶ echo -n 'VMware1!' > ./password.txt
- ▶ echo -n 'admin' > ./username.txt
- ▶ kubectl delete secret avi-secret -n vmware-system-ako
- ▶ kubectl create secret generic avi-secret -n vmware-system-ako --from-file=./certificateAuthorityData.txt --from-file=./password.txt --from-file=./username.txt
- ▶ kubectl edit secret avi-secret -n vmware-system-ako

Pod is running now...

- ▶ root@4202c1b4753322614d82535f07f425bd [~]# kubectl get pods -A | grep -i ako
- ▶ vmware-system-ako vmware-system-ako-ako-controller-
manager-684cc57587-k4pvv 1/1 Running 28 139m
- ▶ root@4202c1b4753322614d82535f07f425bd [~]#

Workload Management

Namespaces

Supervisor Clusters

Services

ADD CLUSTER

Supervisor Cluster

Names

avi-Cluster



0



vcenteravi.lab.local

avi-Datacenter

avi-Cluster

avi-esxi-1.lab.local

avi-esxi-2.lab.local

SE are running now...
and WCP green

Create namespace

Create Namespace X

Select a cluster where you would like to create this namespace.

Cluster i vcenteravi.lab.local

vcenteravi.lab.local
 avi-Datacenter
 avi-Cluster

Name i

Network i

Description

Add description for the namespace here (limit 180 characters)

CANCEL CREATE

Add permissions and storage

Permissions

Can view 0
No users have permission to only view namespaces.

Can edit 1
Administrator

Owner 0
No users are owners of this namespace.

[MANAGE PERMISSIONS](#)

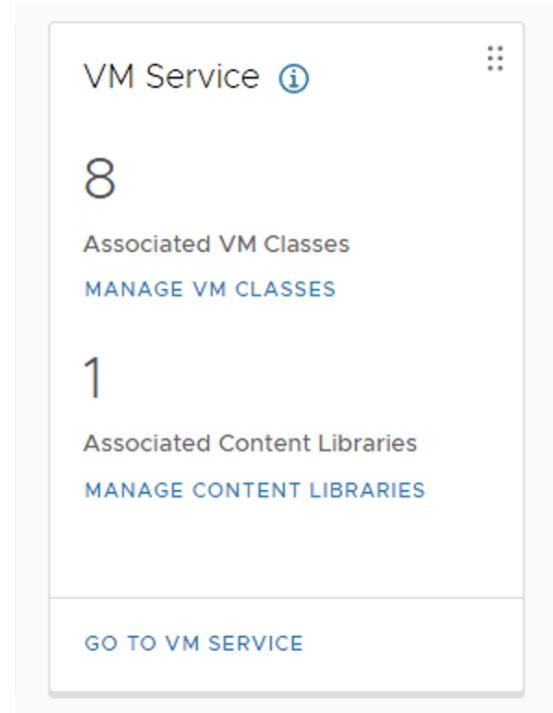
Storage

0 Persistent Volume Claims

Storage Policies 1 pacific-gold-storage-pol... | No limit

[EDIT STORAGE](#)

VM class and Content lib



```
[root@orfdns ~]# kubectl get virtualmachineclassbindings
NAME          VIRTUALMACHINECLASS   AGE
best-effort-2xlarge  best-effort-2xlarge  20m
best-effort-4xlarge  best-effort-4xlarge  20m
best-effort-8xlarge  best-effort-8xlarge  20m
best-effort-large   best-effort-large   20m
best-effort-medium  best-effort-medium  20m
best-effort-small   best-effort-small  20m
best-effort-xlarge  best-effort-xlarge  20m
best-effort-xsmall  best-effort-xsmall 20m
[root@orfdns ~]#
```

Logging on

- ▶ /usr/local/bin/kubectl-vsphere login --vsphere-username administrator@vsphere.local --server=https://192.168.5.40 --insecure-skip-tls-verify
- ▶ kubectl config use-context namespace1000
- ▶ [root@orfdns ~]# k get nodes
- ▶

NAME	STATUS	ROLES	AGE	VERSION
42025674cc72a310700121fadd8890a	Ready	control-plane,master	158m	v1.21.0+vmware.1-wcp
4202aa30779d4936ec9a64301df0434b	Ready	control-plane,master	158m	v1.21.0+vmware.1-wcp
4202c1b4753322614d82535f07f425bd	Ready	control-plane,master	164m	v1.21.0+vmware.1-wcp

Create Guest cluster

- ▶ `kubectl-vsphere login --vsphere-username administrator@vsphere.local --server=https://192.168.5.40 --insecure-skip-tls-verify`
- ▶ `kubectl config use-context namespace1000`
- ▶ `k apply -f ./7u3cluster_photon.yaml`

- ▶ `kubectl vsphere login --server 192.168.5.40 --vsphere-username administrator@vsphere.local --tanzu-kubernetes-cluster-namespace namespace1000 --tanzu-kubernetes-cluster-name workload-vsphere-tkg2 --insecure-skip-tls-verify`
- ▶ `k config use-context workload-vsphere-tkg2`
- ▶ `kubectl apply -f https://github.com/ogelbric/YAML/raw/master/authorize-psp-for-gc-service-accounts.yaml`
- ▶ `k apply -f /root/7u2a/google-nginx2.yaml`

Overall Help

- ▶ <https://github.com/ogelbric/YAML/blob/master/DemoScript.txt>

