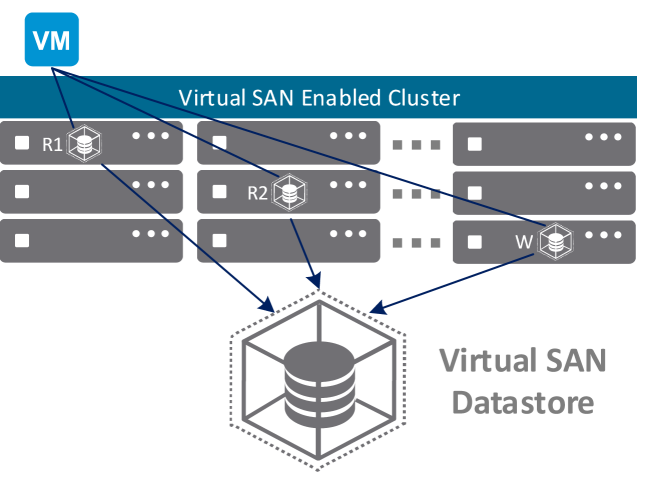
# **1. Introduction to vSAN:**

vSAN is a software-defined storage solution that is fully integrated with vSphere. vSAN aggregates locally attached disks in a vSphere cluster to create a storage solution. It is an example of a hypervisor-converged platform—that is, a solution in which storage and compute for virtual machines are combined into a single device, with storage being provided within the hypervisor itself as opposed to through a storage virtual machine running alongside other virtual machines.



# **2. vSAN 2-Node Implementation:**

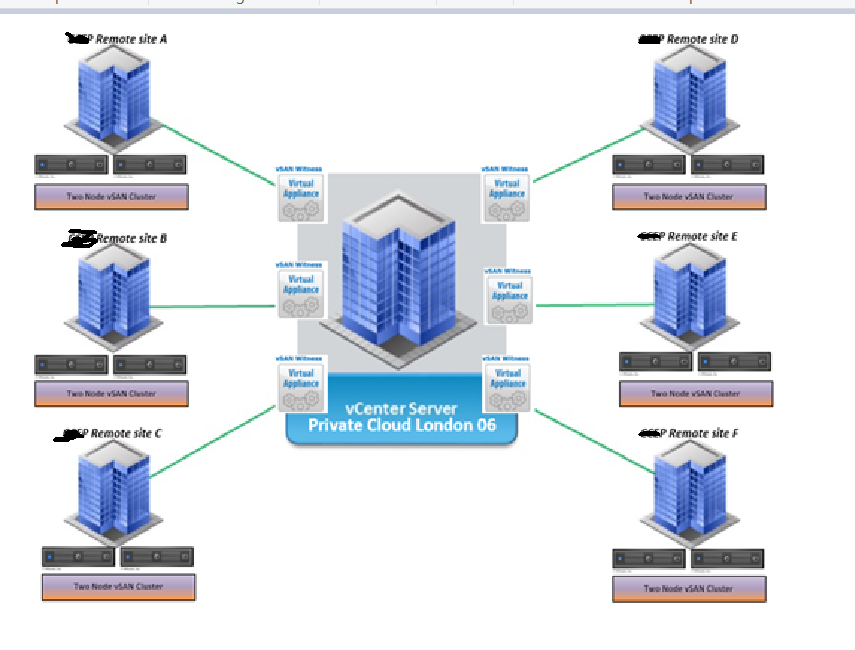
vSAN Two-Node Architecture Overview As of vSAN 6.1, a new type of two-node solution has been supported, typically referred to as Remote Office/Branch Office (ROBO) environments. This solution architecture allows small office implementations to benefit from shared storage, while also minimizing cost.

The two-node vSAN architecture builds on the concept of Fault Domains, first introduced in vSAN 6.0. Each of the two VMware ESXi™ hosts, located on the tenant’s premises, represent a single Fault Domain. In vSAN architecture, the objects that make up a virtual machine are typically stored in a redundant mirror across two Fault Domains, assuming the Number of Failures to Tolerate is equal to 1. As a result of this, in a scenario where one of the hosts goes offline, the virtual machines can continue to run, or be restarted, on the alternate node. To achieve this, a Witness is required to act as a tiebreaker, to achieve a quorum, and enable the surviving nodes in the cluster to restart the affected virtual machines. However, unlike a traditional vSAN enabled cluster, where the witness objects are local to the configured cluster hosts, in a two-node architecture, the witness objects are located externally at a second site on a dedicated virtual appliance specifically configured to store metadata, and to provide the required quorum services for a host failure.

# 3.Multi-Site vSAN 2-Node high level overview:

Each of the CCEP site has a vSAN cluster with 2 vSphere ESXi nodes. Witness appliance will be installed at IBM private Cloud London vCenter. There is a dedicated vCenter Appliance installed at Private Cloud London which manages all the remote site’s vSAN vSphere clusters.

Fig. below shows the high-level overview of 2-Node vSAN infrastructure for CCEP remote sites.



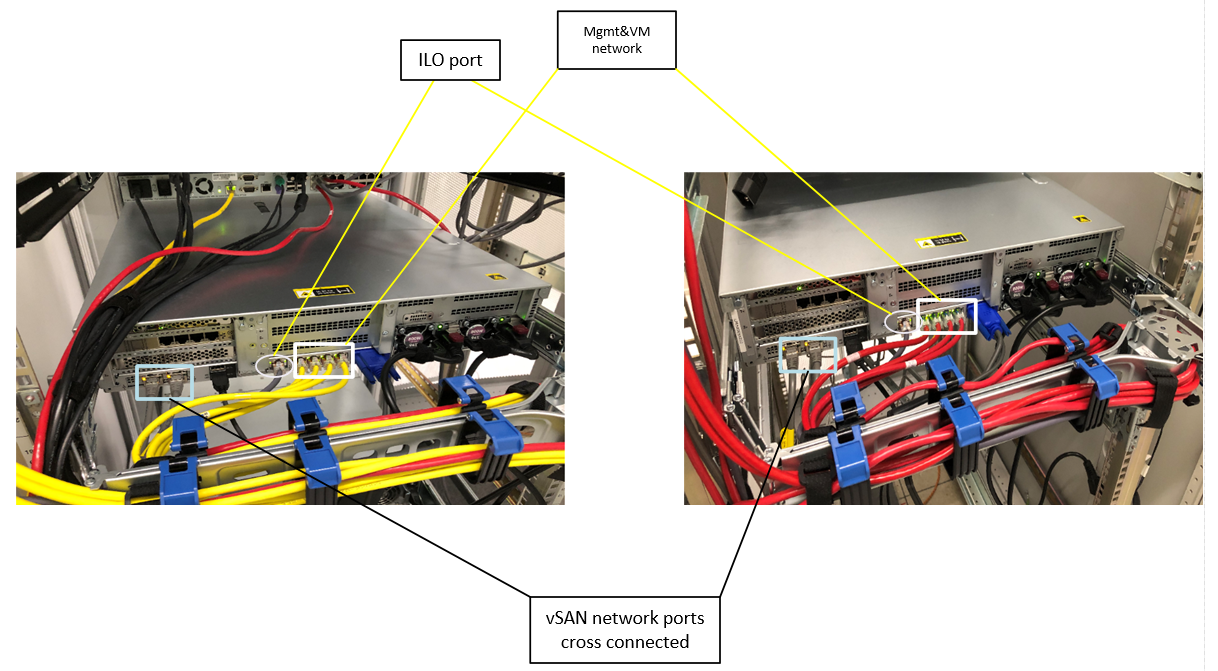
# 4.Installation and Configuration of 2 Node vSAN cluster on Remote Site

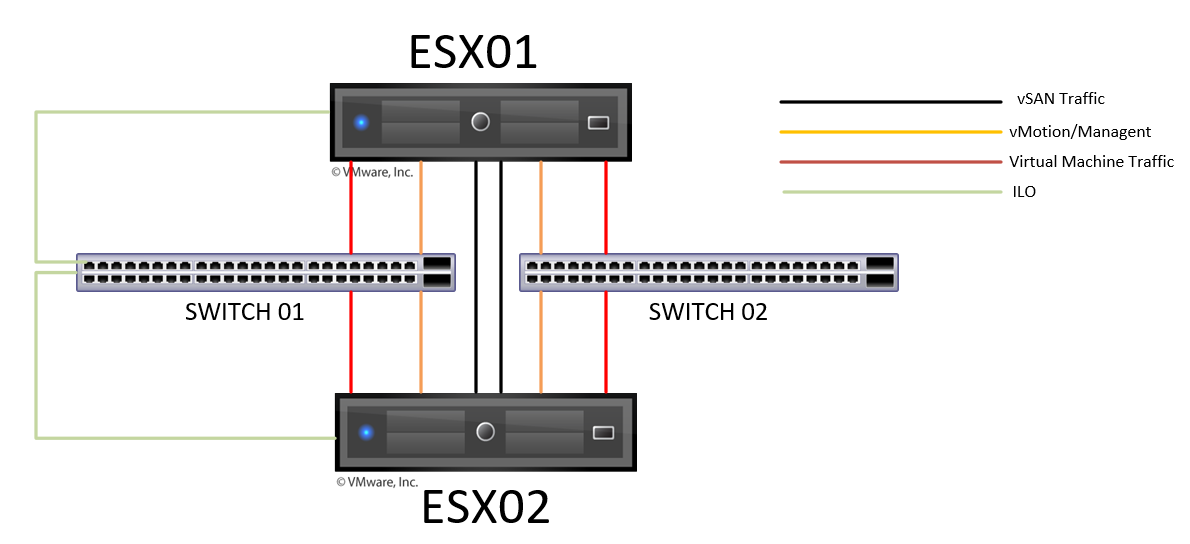
Each remote site is installed with pair of HP DL380 Gen10 servers configured for vSAN 2 Node Cluster. This cluster is managed by a vCenter Server appliance installed at Private Cloud London 06. This solution is using VMware vSphere 7.0

## 4.1 Physical cabling:

In each host there are 7 network ports will be cabled. two 10gig network ports on each host will be used for vSAN traffic. They will be cross connected using crossover cables. Four n/w ports will be cabled for Virtual machine traffic and ESXi Management traffic. They will be placed on VLAN 900. One port from each sever is used for ILO.

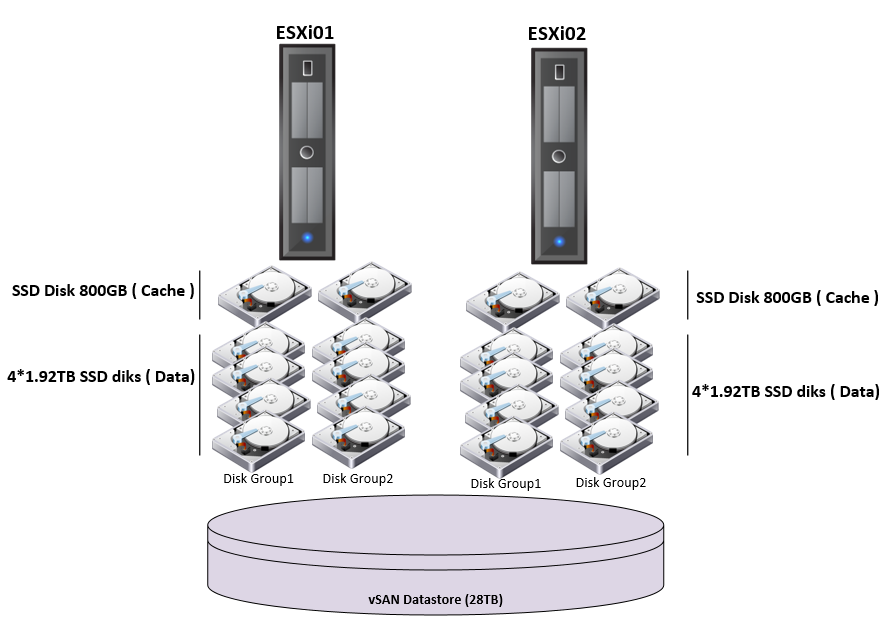
Physical cabling done on one of the sites is shown below.

****

****

## 4.2 vSAN Disk Groups Configuration:

Each host will have two vSAN disk groups.

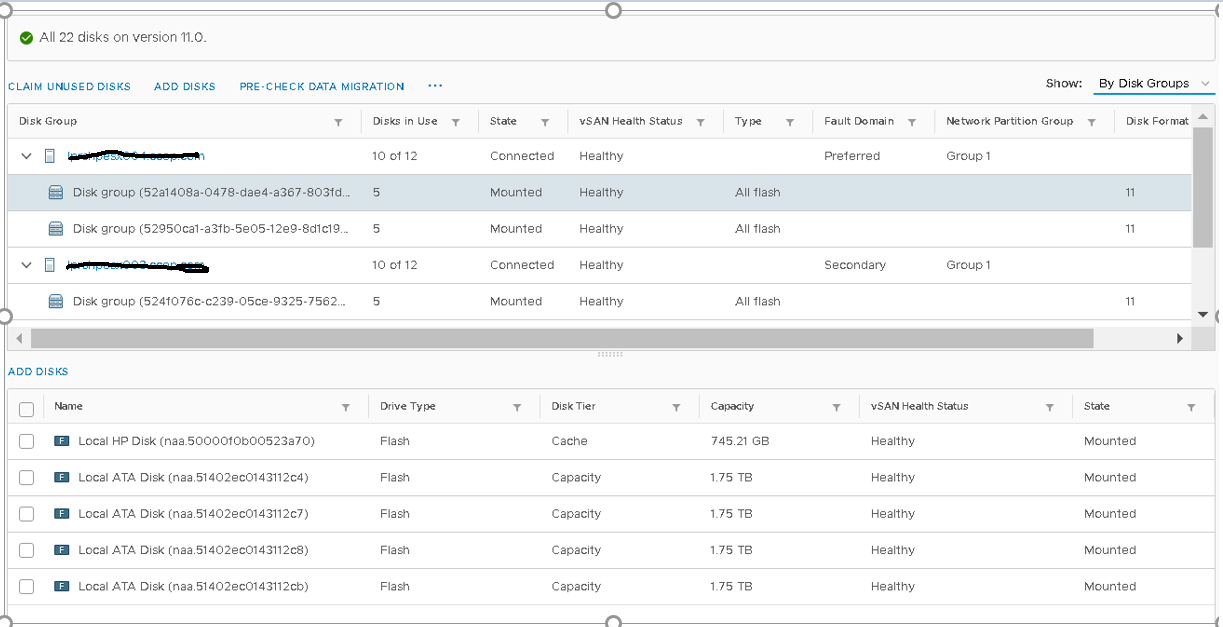


HPE Smart Array P408i-a SR Gen10 is where all the disks for VSAN are connected.   
We will have 2 disk groups for the data with 4 disks and one Cache disk for each group  
We have reserved in each host: one unallocated spare disk for OS Raid, Cache and for Data disk group.

The total amount of disks per server for VSAN are:

3\* HPE 800GB SAS MU SFF SC SSD for Cache volume (includes one spare 800GB)

9\* HPE 1.92Tbyte SATA MU SFF SC DS SSD for Data Volume (includes one spare 1.92TB)



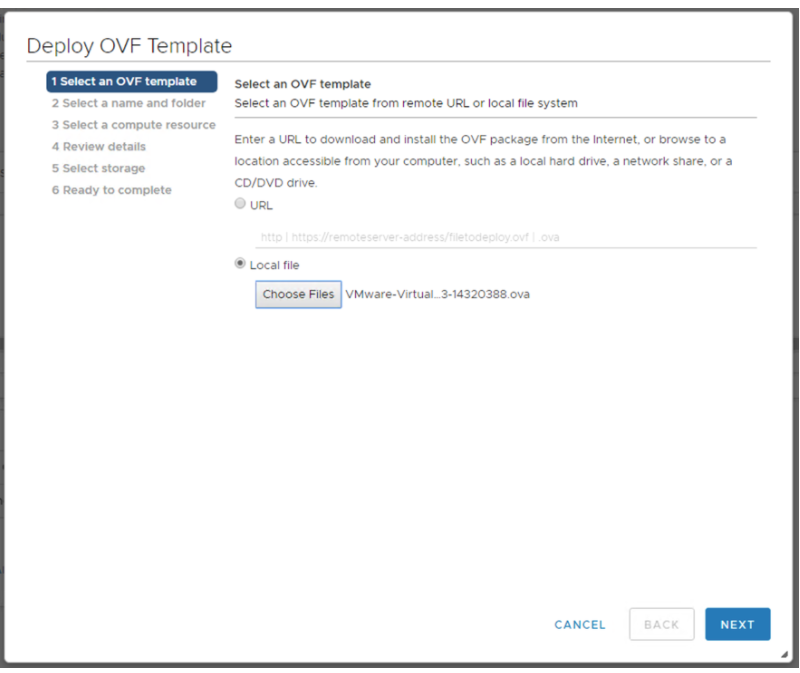
## 4.3Installation steps for vSAN Cluster

Installation vSAN requires following steps.

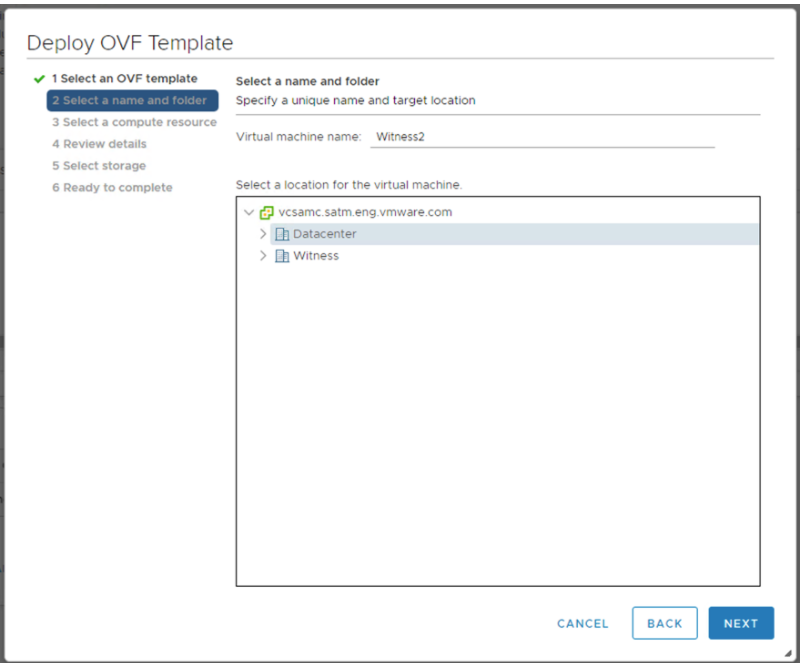
4.3.1 Installation of ESXi servers: This step can be skipped since HP hardware shipped is already installed with ESXi.

4.3.2 Installation of vCenter: We already have a vCenter 7.0 installed in Private Cloud. vCenter Server Name <https://pvislpvvc001.cokecce.com/> . All the future sites will use this vCenter for configuring the vSAN cluster.

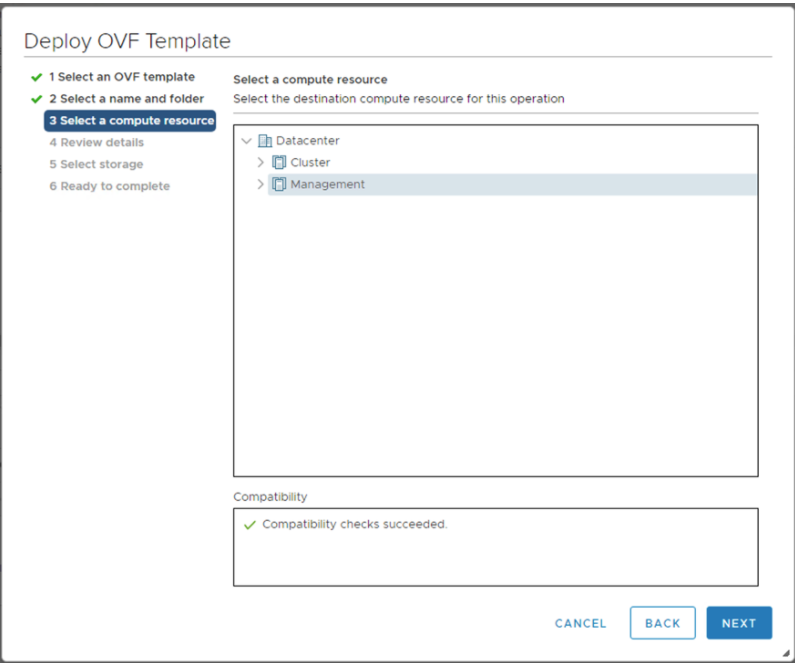
4.3.2 Installation if vSAN Witness appliance: Witness appliance for each remote site will be deployed in Private Cloud Lon06 VMware infrastructure. Download the Witness appliance from VMware portal and follow the below instructions to deploy the appliance.



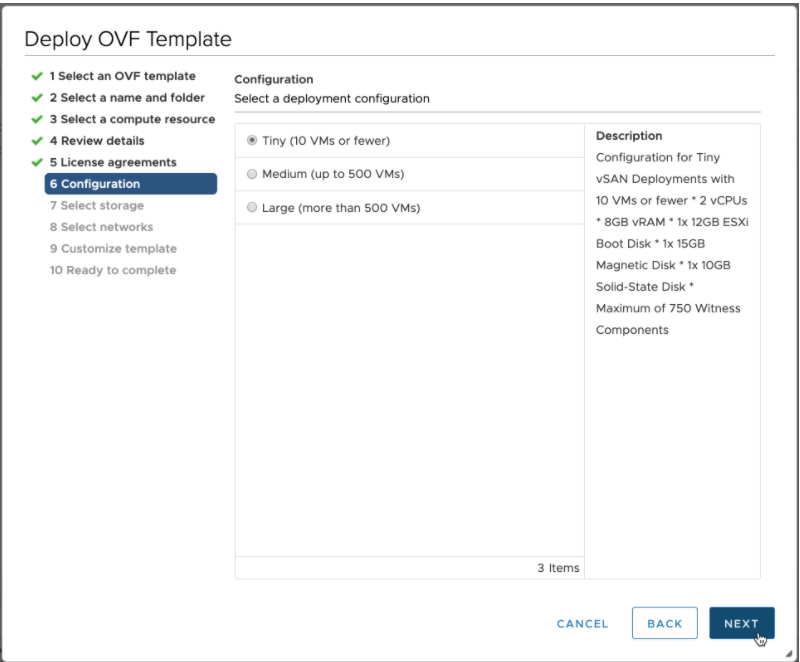
Select a Datacenter for the vSAN Witness Appliance to be deployed to and provide a name

****

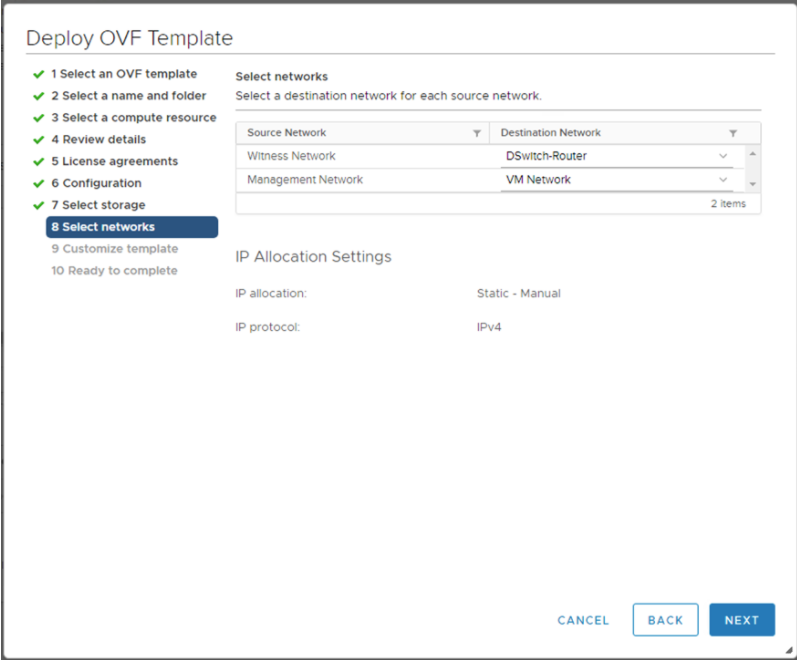
Select a cluster for the vSAN Witness Appliance to reside on. Select Cluster 1 in private Cloud.



Select size of the witness appliance. Select as “Tiny”.



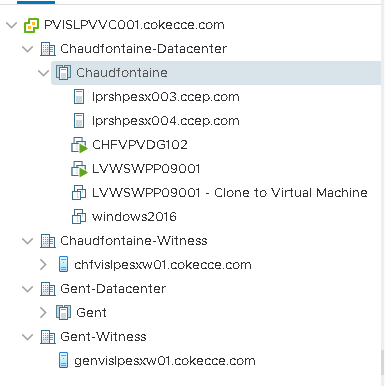
Select a network for the Management Network and for the Witness Network. You may select a single network for both. After the deployment you can remove the one virtual nic from the witness appliance.



Once the Witness appliance is deployed, go to appliance console and configure the management IP address for the ESXi host appliance. Follow the standard ESXi install procedure to complete this step.

### 4.3.3 Create Clusters for vSAN hosts and witness appliance:

You need to create two datacenters for each location within vCenter <https://pvislpvvc001.cokecce.com/> . One DC for vSAN cluster and another DC for witness appliance. As shown in the below figure.



Add the witness appliance to the Witness datacenter. Create a cluster for vSAN under the first datacenter and add the two vSAN hosts to the cluster. Do not enable HA and DRS until configure vSAN service.

### 4.3.4 Enable vSAN service on cluster.

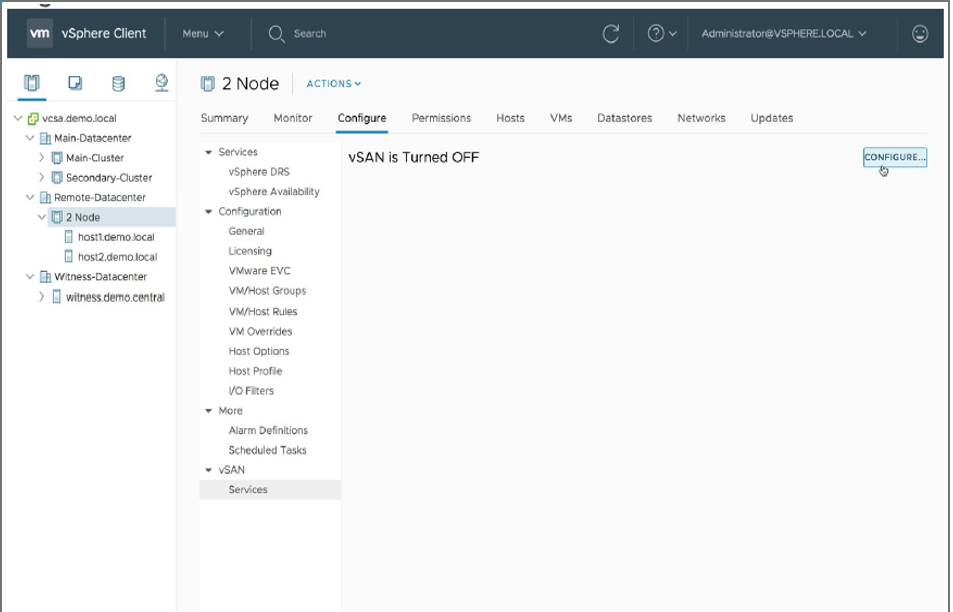
Before you enable the vSAN service on the cluster, create virtual switches and VMkernel port groups for vMotion and vSAN traffic on each of the host.

vSwitch0 🡪 vmnic0, vmnic1 🡪 Enable management network, vMotion

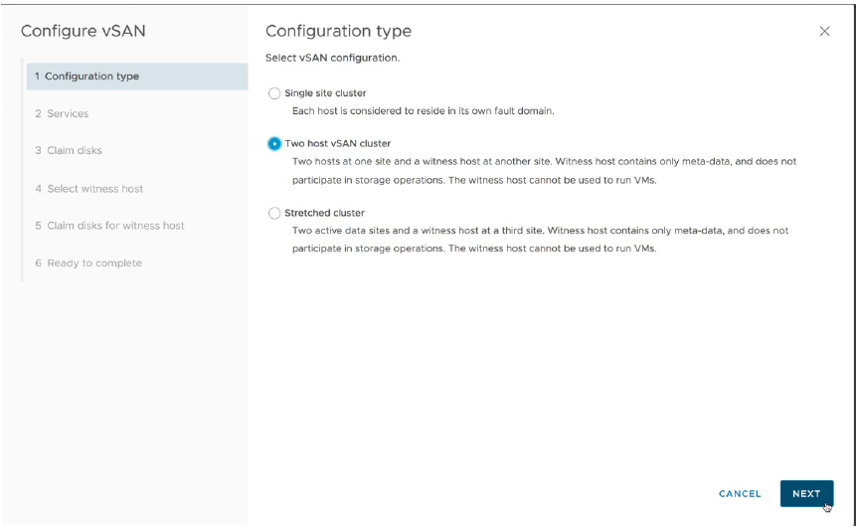
vSwitch1 🡪vmnic4, vmnic5 🡪Create a vmkernel port group for vSAN and enable vSAN service. Make sure these two nics are of 10Gig speed. Set MTU as 9000 on the port group.

vSwitch3 🡪 vmnic2, vmnic3 🡪 Create virtual machine port group and TAG vlan 900.

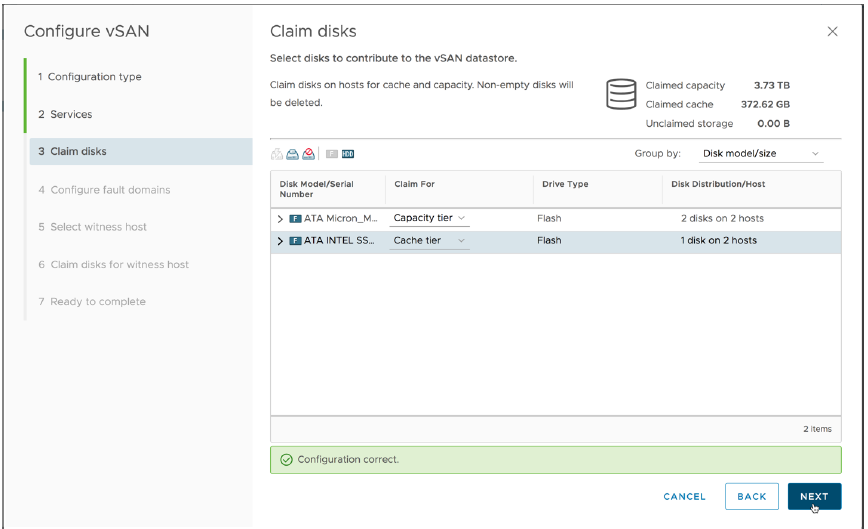
Now click on cluster > Configure - > vSAN >Services. Click on Turn on vSAN



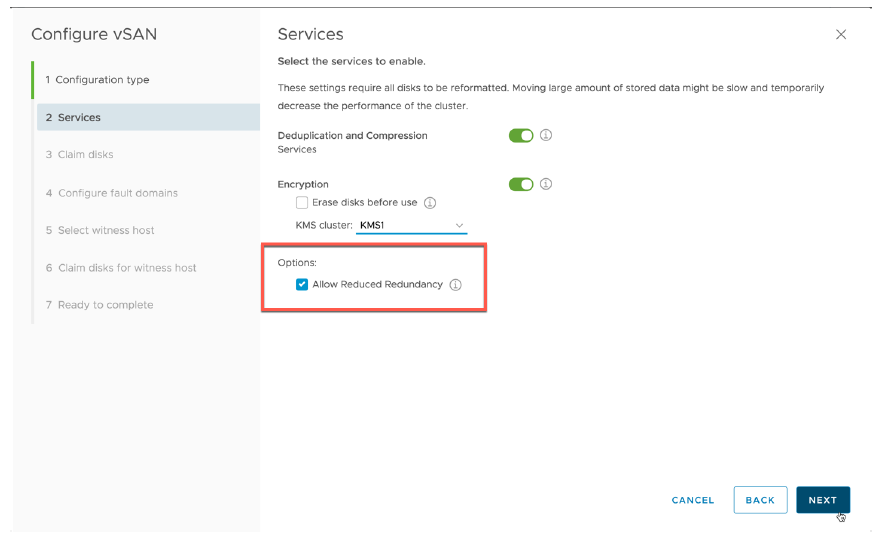
Select Two host vSAN Cluster and Next.



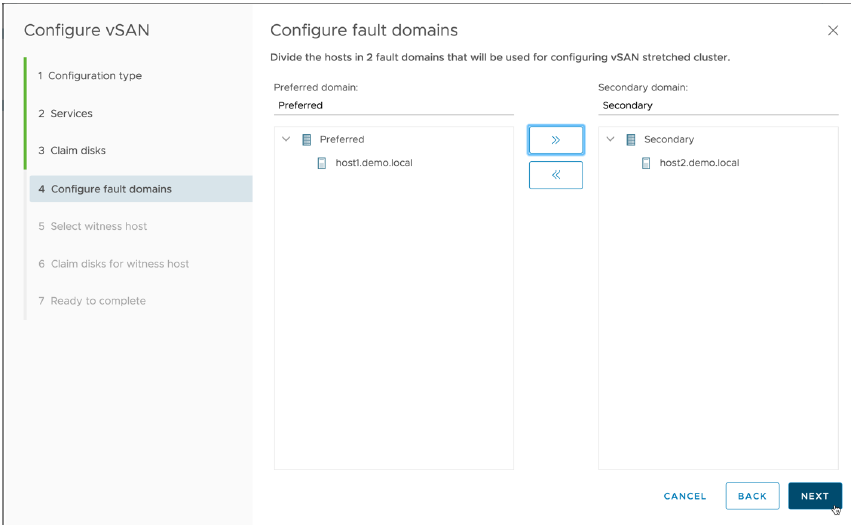
Claim disks for vSAN, make sure you do not claim all the disks as there spare disks. Refer 4.2 , to understand the disk groups structure.



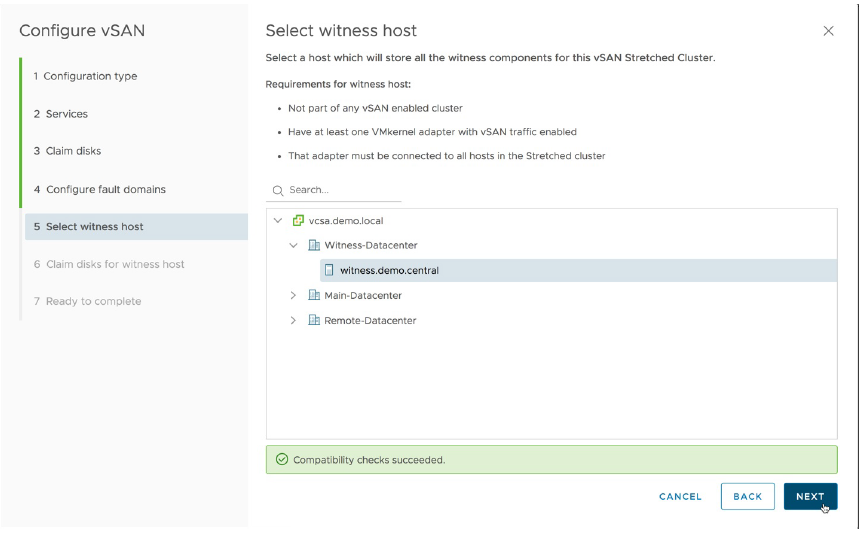
**Disable deduplication and compression.**



Now under the fault domain, keep the each host on its own fault domain.



Select the witness host.



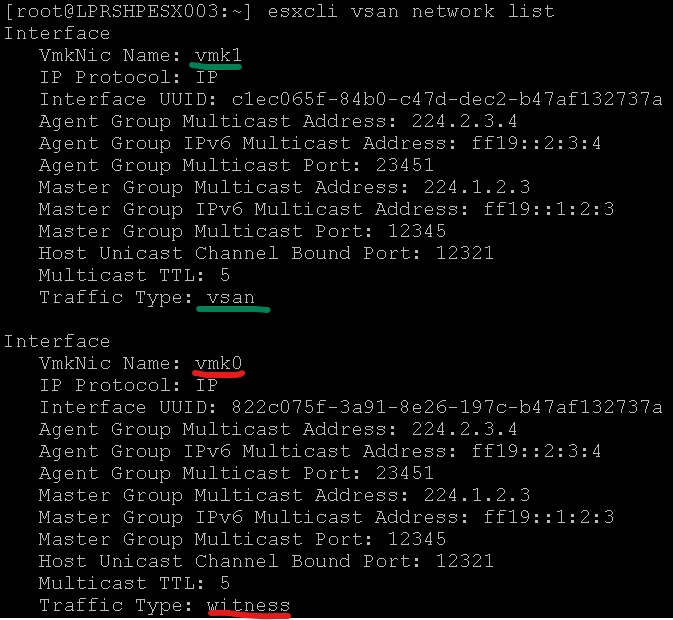
Next screen claims the disks for witness host and click finish.

**Important:** By default, Witness traffic flows through the vSAN interface. Since the witness appliance is in Private cloud Layer3 communication is required from remote site for witness traffic. Since vSAN network is configured using cross over cables and it is non-routable, witness communication fails and cluster gets partitioned. To resolve this issue after the vSAN service is enabled on the cluster, run the below command to tag the witness traffic to vmk0 which has layer 3 connectivity.

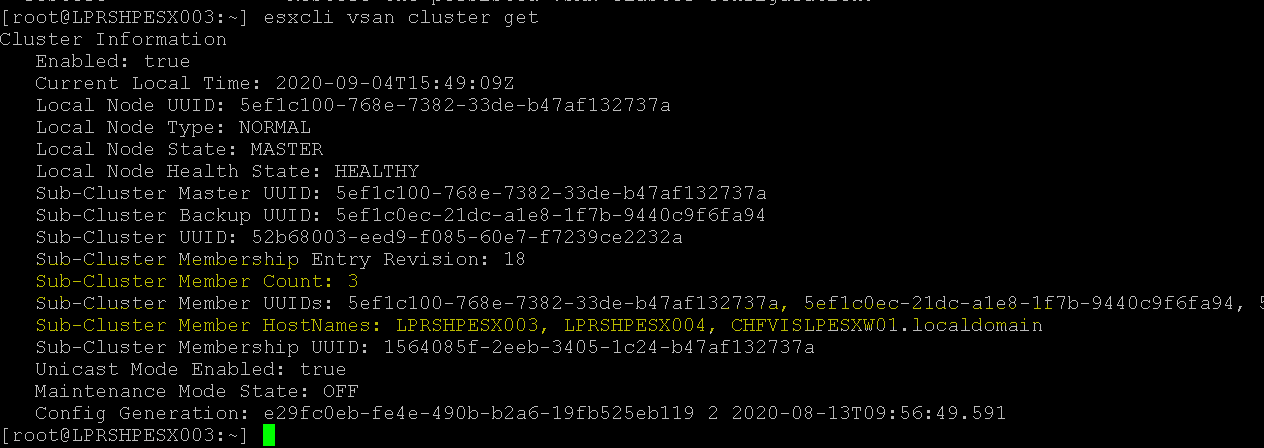
esxcli vsan network ip add -i vmk0 -T=witness

### 4.3.5 Validate vSAN cluster

Logon to each esxi host and run ***esxcli vsan network list****.* Make sure that vmk0 is used for witness and vmk1 is used for vsan traffic.



Run *esxcli vsan cluster get*, validate sub-cluster member count is 3 and you should see all the three host names under sub-cluster member hostnames.



\*\*END OF DOCUMENT \*\*