Virtualized SAP HANA on FlexPod Datacenter: Design Considerations and Best Practices
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Purpose of this document</td>
<td>3</td>
</tr>
<tr>
<td>Audience</td>
<td>3</td>
</tr>
<tr>
<td>Document reference</td>
<td>3</td>
</tr>
<tr>
<td>Reference architecture</td>
<td>3</td>
</tr>
<tr>
<td>Network layer</td>
<td>5</td>
</tr>
<tr>
<td>Storage layer</td>
<td>6</td>
</tr>
<tr>
<td>Computing layer</td>
<td>10</td>
</tr>
<tr>
<td>Virtual machine and OS layers</td>
<td>18</td>
</tr>
<tr>
<td>Configuration example for a virtualized SAP HANA scale-up system</td>
<td>20</td>
</tr>
<tr>
<td>Post-OS installation configuration</td>
<td>21</td>
</tr>
<tr>
<td>Sizing</td>
<td>22</td>
</tr>
<tr>
<td>Computing</td>
<td>22</td>
</tr>
<tr>
<td>Storage</td>
<td>22</td>
</tr>
<tr>
<td>Appendix: Cisco Application Centric Infrastructure (ACI) based solution configuration</td>
<td>23</td>
</tr>
<tr>
<td>Cisco ACI virtual machine management (VMM)</td>
<td>24</td>
</tr>
<tr>
<td>For more information</td>
<td>25</td>
</tr>
<tr>
<td>Certified SAP HANA Hardware Directory</td>
<td>25</td>
</tr>
<tr>
<td>SAP HANA TDI documentation</td>
<td>25</td>
</tr>
<tr>
<td>SAP Notes</td>
<td>25</td>
</tr>
<tr>
<td>Additional references</td>
<td>26</td>
</tr>
</tbody>
</table>

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
Introduction
Support for running SAP HANA virtualized and Tailored Datacenter Integration (TDI) option enable customers to align established data center processes and reuse existing infrastructure while implementing SAP HANA.

SAP supports VMware vSphere 6.5 and 6.7 for virtual deployments in production scenarios of SAP HANA on certified appliances and TDI verified hardware configurations. Customers thus can gain the benefits of virtualization for their SAP HANA environments and optimize costs through more efficient resource utilization. With Intel® Broadwell (running SAP HANA 1.0 SPS 12) and Intel Skylake processors (with SAP HANA 1.0 SPS 12 Revision 122.19, or with SAP HANA 2.0, recommended), virtual machines with up to 128 virtual CPUs (vCPUs) and 4 to 6 terabytes (TB) of main memory are possible.

The main use case for SAP HANA on VMware is within the TDI framework. Virtualized SAP HANA systems implemented by the customer using existing hardware listed in the Certified and Supported SAP HANA Hardware Directory should be verified with the SAP HANA Hardware Configuration Check Tool (HWCCT) to be sure that they qualify for SAP support. Increasing numbers of customers are taking advantage of the enhanced flexibility achieved by running SAP HANA TDI.

IDC confirmed in a recent survey (IDC US42198216) that Cisco is the leading vendor for SAP HANA infrastructure. In line with the current trend toward converged infrastructure to further simplify and support multitenant workload deployments, Cisco and NetApp have partnered to deliver FlexPod Datacenter as a platform for a variety of SAP workloads, including fully virtualized workloads. FlexPod uses best-in-class server and network components integrated with Cisco Unified Computing System™ (Cisco UCS®) programmability features and backed by high-performance all-flash storage from NetApp. Using the Cisco UCS servers and NetApp AFF all-flash arrays listed in the SAP HANA Hardware Directory’s Certified Appliances and Certified Enterprise Storage sections, respectively, FlexPod provides an optimized platform for SAP HANA TDI.

Purpose of this document
This document provides configuration guidelines for implementing a virtualized SAP HANA on FlexPod Datacenter solution. It describes the best practices to be followed while configuring the storage, server, network, virtualization, and operating system layers for optimal operation.

Audience
This document is intended for IT architects, engineers, and administrators who are responsible for configuring and deploying the SAP HANA platform in a VMware virtualization environment. It assumes that the reader has a basic knowledge of FlexPod, Cisco UCS, NetApp Storage, VMware vSphere, Linux, and SAP HANA TDI scenarios.

Document reference
The Cisco® Validated Design document FlexPod Datacenter with VMware vSphere 6.5, published in June 2017, provides the foundation design for this solution. This document builds on that foundation, focusing on preparation of the infrastructure to support an application tenant: that is, a virtualized SAP HANA system. It describes the steps that need to be performed for the various layers of the architecture.

Reference architecture
Figure 1 shows the various layers of architecture, from the storage layer to the application layer. It shows the possible constituents of each layer of FlexPod Datacenter.

NetApp AFF A-Series arrays form the storage base layer, Cisco Nexus® 9000 Series Switches provide the network backbone, and Cisco UCS C-Series Rack Servers and B-Series Blade Servers make up the computing layers. SAP HANA is installed in virtual machines running either the SUSE Linux Enterprise Server (SLES) or Red Hat Enterprise Linux (RHEL) operating system hosted on the VMware ESXi virtualization platform.
Virtualized SAP HANA implementations use the Network File System (NFS) and Internet Small Computer System Interface over IP (iSCSI) storage protocols. The ESXi hosts boot through iSCSI, and the SAP HANA virtual machines have their OS installed on the VMware NFS datastore.

Figure 2. OS boot mechanism
For each SAP HANA node in a virtual machine, a data volume; a log volume; and a volume for executable files, configurations, and application logs are configured. The persistence volumes for the SAP HANA system are directly mounted on the provisioned guest OS using the dedicated network connection to the storage.

The storage configuration and sizing for virtualized SAP HANA is identical to that for bare-metal servers. The existing SAP HANA storage requirements for the partitioning, configuration, and sizing of data, log, and binary volumes remain valid for virtualization scenarios.

The configuration flow starts with the definition of VLANs specific to SAP HANA that correspond to the various networks required by the system.

**Network layer**

SAP categorizes the SAP HANA system networks into three logical communication zones (Figure 3):

- **Client zone:** External communication networks consisting of application server and client connectivity networks
- **Internal zone:** Internal communication networks consisting of the internode communication network in a scale-out system and the replication network for traffic in a distributed configuration
- **Storage zone:** All storage-related networks consisting of the NFS-based /hana/shared, data, and log file system access network along with the dedicated backup network

*Figure 3.  SAP HANA TDI network requirements (source: SAP SE)*
The system also includes a management zone consisting of the ESXi host boot (iSCSI) and administration network, SAP HANA virtual machine boot (NFS) and access network, and VMware vMotion network, at minimum. The configuration steps are presented in the Cisco Validated Design.

1. Create the SAP HANA system-specific VLANs on the Cisco Nexus switch pair:
   vlan <<var_hanadata_vlan_id>>
   name HANA-NFS-Data

   vlan <<var_hanalog_vlan_id>>
   name HANA-NFS-Log

   vlan <<var_admin_vlan_id>>
   name HANA-VM-Management

   vlan <<var_internal_vlan_id>>
   name HANA-Internal

   vlan <<var_backup_vlan_id>>
   name HANA-Backup

   vlan <<var_client_vlan_id>>
   name HANA-Client

   vlan <<var_appserver_vlan_id>>
   name HANA-AppServer

   vlan <<var_datasource_vlan_id>>
   name HANA-DataSource

   vlan <<var_replication_vlan_id>>
   name HANA-Replication

Note: The configuration variables in double parentheses above and in the subsequent chapters are placeholders for customer specific parameter settings. Also, naming conventions followed here are only suggestive and could be altered based on customer requirement.

2. Verify that the defined VLANs are allowed on the Cisco UCS port channels and the virtual port channel (vPC) peer link and the storage zone VLANs, specifically on the storage port channels.

Storage layer
For the NetApp array, use the following steps to adapt the base configuration to host the virtualized SAP HANA system.

1. Modify the infrastructure storage virtual machine (SVM) configuration to accommodate the SAP HANA system tenant. Figure 4 below shows the existing infrastructure SVM components in the Cisco Validated Design.
a. In preparation to adding the SAP HANA application tenant, create two more broadcast domains apart from the existing NFS, iSCSI-A, and iSCSI-B domains: one for SAP HANA data and one for the SAP HANA log.

b. Create two more VLANs, one for SAP HANA data and one for the SAP HANA log, and add them to their respective broadcast domains:

network port vlan create -node <clusternname>-01 -vlan-name a0a-<data-vlan-id>
network port vlan create -node <clusternname>-02 -vlan-name a0a-<data-vlan-id>

broadcast-domain add-ports -broadcast-domain NFS-Data -ports <clusternname>-01:a0a-<data-vlan-id>, <clusternname>-02:a0a-<data-vlan-id>

network port vlan create -node <clusternname>-01 -vlan-name a0a-<log-vlan-id>
network port vlan create -node <clusternname>-02 -vlan-name a0a-<log-vlan-id>

broadcast-domain add-ports -broadcast-domain NFS-Log -ports,<clusternname>-01:a0a-<log-vlan-id>, <clusternname>-02:a0a-<log-vlan-id>
Create the application-specific SVM configuration. Figure 6 below shows the SAP HANA SVM with all the required storage objects (volumes, export policies, and logical interfaces [LIFs]) to be configured.

**Figure 6.** Overview of SAP HANA SVM components

![Diagram of SAP HANA SVM components](image)

a. To create the SVM for SAP HANA volumes, follow these steps.

   1. Run the `vserver create` command:

      ```
      vserver create -vserver hana-svm -rootvolume hana_rootvol -aggregate aggr01 -rootvolume-security-style unix
      ```

   2. Select the SVM data protocols that you want to configure, keeping iSCSI and NFS:

      ```
      vserver remove-protocols -vserver hana-svm -protocols fcp,cifs,ndmp
      ```

   3. Add the two data aggregates to the infrastructure SVM aggregate list for the NetApp Virtual Storage Console (VSC):

      ```
      vserver modify -vserver hana-svm -aggr-list aggr01,aggr02
      ```

   4. Enable and run the NFS protocol in the infrastructure SVM:

      ```
      nfs create -vserver hana-svm -udp disabled
      ```

   5. Enable a large NFS transfer size:

      ```
      set advanced
      nfs create -vserver hana-svm -tcp max-transfer-size 1048576
      ```

   6. Initialize the mirroring relationship:

      ```
      snapmirror initialize -ls -set -source-path hana-svm:hana_rootvol
      ```

b. To create a load-sharing mirror of an SVM root volume, complete the following steps.

   1. Create a volume to be the load-sharing mirror of the SAP HANA SVM root volume on each node:

      ```
      volume create -vserver hana-svm -volume hana_rootvol_m01 -aggregate aggr01 -size 1GB -type DP
      volume create -vserver hana-svm -volume hana_rootvol_m02 -aggregate aggr02 -size 1GB -type DP
      ```

   2. Create the mirroring relationships:

      ```
      snapmirror create -source-path hana-svm:hana_rootvol -destination-path hana-svm:hana_rootvol_m01 -type LS -schedule 15min
      ```

      ```
      snapmirror create -source-path hana-svm:hana_rootvol -destination-path hana-svm:hana_rootvol_m02 -type LS -schedule 15min
      ```

   3. Initialize the mirroring relationship:

      ```
      snapmirror initialize -ls-set -source-path hana-svm:hana_rootvol
      ```
c. To configure the NFS export policies on the SVM, complete the following steps.

Create a new rule for the infrastructure NFS subnet in the default export policy:

```
vserver export-policy rule create -vserver hana-svm -policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule sys -rwrule sys -superuser sys -allow-suid true -anon 0
```

Assign the FlexPod export policy to the infrastructure SVM root volume:

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

d. To add the SAP HANA SVM administrator and SVM administration LIF in the out-of-band management network, complete the following steps.

```
network interface create -vserver hana-svm -lif hana-svm-mgmt -role data -data-protocol none -home-node <clustername>-02 -home-port e0c -address <hana-svm-ip> -netmask <hana-svm-netmask> -status admin up -failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-revert true
```

**Note:** The SVM management IP address in this step should be in the same subnet as the storage cluster management IP address.

Create a default route to allow the SVM management interface to reach the outside world:

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

Set a password for the SVM vsadmin user and unlock the user:

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

e. Create export policies for the SAP HANA SVM.

Create a new export policy for the SAP HANA data and log subnet:

```
vserver export-policy create -vserver hana-svm -policyname hana-vm
```

Create a rule for this policy:

```
vserver export-policy rule create -vserver hana-svm -policyname hana-vm -clientmatch <data-cidr>,<log-cidr> -rorule sys -rwrule sys -allow-suid true -allow-dev true -ruleindex 1 -anon 0 -protocol nfs -superuser sys
```

f. Create NFS LiFs for the SAP HANA data and SAP HANA log.

To create the NFS LiFs for the SAP HANA data, run the following commands:

```
network interface create -vserver hana-svm -lif data-lif01 -role data -data-protocol nfs -home-node <clustername>-01 -home-port a0a -address <data-vlan-id> -netmask <data-netmask> -status admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true
```

```
network interface create -vserver hana-svm -lif data-lif02 -role data -data-protocol nfs -home-node <clustername>-02 -home-port a0a -address <data-vlan-id> -netmask <data-netmask> -status admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true
```

```
security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```

```
vserver hana
admin up
```

```
volume modify -vserver hana-svm -volume hana_rootvol -policy default
```

```
network route create -vserver hana-svm -destination 0.0.0.0/0 -gateway <hana-svm-gateway>
```

```
security login password -username vsadmin -vserver hana-svm
Enter a new password: <password>
Enter it again: <password>

security login unlock -username vsadmin -vserver hana-svm
```
To create the NFS LIF for the SAP HANA log, run the following commands:

```
network interface create -vserver hana-svm -lif log_lif01 -role data -data-protocol nfs -home-node <clusternam>e-01 -home-port a0a-<log-vlan-id> -address <node01-log_lif01-ip> -netmask <log-netmask> -status-admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true

network interface create -vserver hana-svm -lif log_lif02 -role data -data-protocol nfs -home-node <clusternam>e-02 -home-port a0a-<log-vlan-id> -address <node02-log_lif02-ip> -netmask <log-netmask> -status-admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true
```

**Note:** The data and log persistence partitions are accessed by the host through the IP address assigned to the LIFs created previously: `<node02-data_lif01-ip>`, `<node02-log_lif01-ip>`, `<node01-data_lif01-ip>`, and `<node01-log_lif01-ip>`.

**Computing layer**

In Cisco UCS, one approach to setting up a tenant’s virtualized SAP HANA system is to dedicate a VMware ESXi cluster with a set of Cisco UCS servers for each tenant.

1. Create the SAP HANA VLANs in Cisco UCS under the LAN cloud:
2. Create additional virtual network interface card (vNIC) templates for the SAP HANA traffic, creating each on Fabrics A and B. For instance, create vNICs for virtualized SAP HANA system storage access, client access, and access for the application server:

Create vNIC Template

Name: VHAHA_NA
Description: vNIC Template for the VFI Network Trunk
Fabric ID: Fabric A
Redundancy: No Redundancy

Target
- Adapter
- VM

Warning
If VM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten.

VLANs

Select | Name | Native VLAN
--- | --- | ---
Access | 0
Backup | 0
DataSource | 0
ESXi-Motion | 0
HMC-MGMT | 0
Infra-RFS | 0
ISCSEI-A-VLAN | 0
ISCSEI-B-VLAN | 0
Native-VLAN | 0
NFS_Data | 0
NFS_Log | 0
Server | 0
SysDep | 0
Application | 0

Create VLAN

CDK Source: vNIC_Name
MTU: 9000
MAC Pool: MAC-Pool-VHAHA_NA
QoS Policy: <not set>
Network Control Policy: Enable-CDP-LLDP
Pin Group: <not set>
State Threshold Policy: default
Connection Polices:
- Dynamic vNIC: 0
- vNIC: 0
- VMI: 0

Dynamic vNIC Connection Policy: <not set>
Create vNIC Template

Name: vHA_B
Description: vNIC Template for VM Network Trunk
Fabric ID: Fabric B
Failover

Redundancy
Redundancy Type: No Redundancy
Peer Redundancy Template: vHA_A

Target
Adapter
VM

Warning
If VM is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten.

Template Type: Initial Template

VLANs

Select Name Native VLAN
Access
Application
Backup
DataSource

Create VLAN

CDN Source: vNIC Name: User Defined
MTU: 9000
MAC Pool: MAC-Pool-1[64/64]
QoS Policy: <not set>
Network Control Policy: enable-CDP-LLDP
FQ Group: <not set>
State Threshold Policy: default
Connection Policies:
Dynamic vNIC, vNIC, vNIC
Dynamic vNIC Connection Policy: <not set>
3. Add vNICs, based on the vNIC templates created earlier, to the service profile template:

The vNICs in the service profile template will be listed:

<table>
<thead>
<tr>
<th>Name</th>
<th>MAC Address</th>
<th>Fabric ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNIC 05-vHANA-B</td>
<td>Derived</td>
<td>B A</td>
</tr>
<tr>
<td>vNIC 09-Infra-A</td>
<td>Derived</td>
<td>A B</td>
</tr>
<tr>
<td>vNIC 01-Infra-B</td>
<td>Derived</td>
<td>B A</td>
</tr>
<tr>
<td>vNIC 02-iSCSI-A</td>
<td>Derived</td>
<td>A</td>
</tr>
<tr>
<td>vNIC 03-iSCSI-B</td>
<td>Derived</td>
<td>B</td>
</tr>
<tr>
<td>vNIC 04-vHANA-A</td>
<td>Derived</td>
<td>A B</td>
</tr>
</tbody>
</table>
4. Correlate the vNICs from Cisco UCS Manager with the vmnics at the ESXi web client for the hosts:

<table>
<thead>
<tr>
<th>Name</th>
<th>MAC Address</th>
<th>Desired Order</th>
<th>Actual Order</th>
<th>Fabric ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNIC 01-Infra-B</td>
<td>00:25:B5:08:00:31</td>
<td>1</td>
<td>1</td>
<td>B A</td>
</tr>
<tr>
<td>vNIC 02-ISCSI-A</td>
<td>00:25:B5:0A:00:10</td>
<td>2</td>
<td>2</td>
<td>A B</td>
</tr>
<tr>
<td>vNIC 03-ISCSI-B</td>
<td>00:25:B5:0A:00:6E</td>
<td>3</td>
<td>3</td>
<td>A B</td>
</tr>
<tr>
<td>vNIC 00-Infra-A</td>
<td>00:25:B5:0A:00:07</td>
<td>4</td>
<td>4</td>
<td>B</td>
</tr>
<tr>
<td>vNIC 04-vHANA-A</td>
<td>00:25:B5:0A:00:01</td>
<td>5</td>
<td>5</td>
<td>A B</td>
</tr>
<tr>
<td>vNIC 05-vHANA-B</td>
<td>00:25:B5:0B:00:30</td>
<td>2</td>
<td>6</td>
<td>B A</td>
</tr>
</tbody>
</table>

5. The solution has existing two standard virtual switches (vSwitches) at the host—one for the infrastructure port groups (vMotion, infra-nfs, etc.) and one for iSCSIBootvSwitch exclusively for the iSCSI networks. Now add another vSwitch, vHANA, for the SAP HANA networks:
6. Add VMkernel NICs depending on the defined networks selected while creating the vNIC template earlier: for example, the application server network, data-source network, NFS data, and log.

The application server network port group is shown here:
7. Replicate the SAP HANA network port groups on the VMware vCenter server, by configuring them either in the existing distributed switch after increasing the uplink ports from the initial two to four or as part of another distributed switch specific to SAP HANA. It helps to create another VMware vSphere Distributed Switch (vDS) exclusively for SAP HANA virtual machine networks because they use completely different uplink vnics and are also pinned to specific fabrics depending on bandwidth requirements:
8. While adding hosts to manage the virtual networking under vCenter vDS-fp-HANA, initially assign the Fabric B path vmnic (vmnic2 in the example) as the uplink to the uplink port group:

![Uplink Configuration](image1.png)

9. Map the VMkernel network adapters to the exact same port groups you created earlier on the vDS, selecting the “Assign port group” option:

![Port Group Assignment](image2.png)
10. After the distributed switch reconfiguration is complete, in vCenter remove the vHANA virtual switch so that it releases the Fabric A path vmnic that was assigned to it at the host level. Assign the available Fabric A path vmnic to the vDS-fp-vHANA:

![Uplink Ports](image)

Now the SAP HANA vDS has two redundant uplinks. These are used by the SAP HANA network port groups in active-standby mode to help pin traffic to a fabric.

**Virtual machine and OS layers**

This section presents best practices for the virtual machine and OS layers.

**Virtual machine configuration**

The recommended approach is to configure the cores per socket to match the actual hardware configuration. For example, configure 22 cores per socket for Intel® Xeon® processor E7-8880 v4, 24 cores per socket for Intel Xeon processor E7-8890 v4, and 28 cores per socket for Intel Xeon Platinum 8180 and 8176 processors:

![Virtual Machine Configuration](image)
Reserve CPU and, especially, memory resources for production virtual machines. Select the “Reserve all guest memory (All locked)” option:

<table>
<thead>
<tr>
<th>Virtual Hardware</th>
<th>VM Options</th>
<th>SDRS Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling Affinity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>512 GB</td>
<td></td>
</tr>
<tr>
<td>Reservation</td>
<td>1024 MB</td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Unlimited MB</td>
<td></td>
</tr>
<tr>
<td>Shares</td>
<td>Normal 10240</td>
<td></td>
</tr>
</tbody>
</table>

Use VMXNET 3 type vNICs to configure the network interfaces for all the networks defined:

Refer to **Best Practices of Virtualized SAP HANA for Skylake-Based Server Host Systems** and **SAP HANA on VMware vSphere Best Practices Guide** for comprehensive guidelines for configuring the virtual machines for SAP HANA.

**Operating system installation**

To configure optimal settings for running SAP HANA on SLES or RHEL, follow the respective SAP notes that provide the SAP HANA database recommended OS settings as you would do for bare-metal implementations. See the “For more information” section of this document for all relevant SAP Notes.
ESXi has its own I/O scheduling mechanisms that not only make guest OS I/O scheduling redundant but also adds unnecessary overhead. The recommended approach is to disable I/O scheduling at the virtual machine level. Append `elevator=noop` to the kernel boot arguments.

**Configuration example for a virtualized SAP HANA scale-up system**

The following examples show an SAP HANA database with SID=VHA and a server RAM size of 512 GB. For different server RAM sizes, the required volume sizes are different.

For a detailed description of the capacity requirements for SAP HANA, see the SAP HANA Storage Requirements white paper.

Figure 7 below shows the volumes that must be created on the storage nodes and the network paths used.

*Figure 7. Configuration example for an SAP HANA single-host system*

Create SAP HANA persistence volumes on the storage nodes

Run the following command to create data volume vhana01_data in the aggregate agrgr_hana01 with a size of 512 GB:

```
volume create -vserver hana_svm -volume vhana01_data -aggregate agrgr_hana01 -size 256GB -state online -policy hana-vm -junction-path /vhana01_data -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
```

Run the following command to create log volume vhana01_log in the aggregate agrgr_hana02 with a size of 256 GB:

```
volume create -vserver hana_svm -volume vhana01_log -aggregate agrgr_hana02 -size 256GB -state online -policy hana-vm -junction-path /vhana01_log -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
```

Run the following command to create shared volume vhana01_sapexe in the aggregate agrgr_hana02 with a size of 512 GB:

```
volume create -vserver hana_svm -volume vhana01_sapexe -aggregate agrgr_hana02 -size 512GB -state online -policy hana-vm -junction-path /vhana01_sapexe -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none.
```
**Post-OS installation configuration**

To create the required mount-point directories, run the following commands:

```bash
mkdir -p /hana/data/VHA/mnt00001
mkdir -p /hana/log/VHA/mnt00001
mkdir -p /hana/shared
mkdir -p /usr/sap/VHA

chmod 777 -R /hana/log/VHA
chmod 777 -R /hana/data/VHA
chmod 777 -R /hana/shared
chmod 777 -R /usr/sap/VHA
```

The mount options are identical for all file systems that are mounted on the host:

- `/hana/data/VHA/mnt00001`
- `/hana/log/VHA/mnt00001`
- `/hana/shared`
- `/usr/sap/VHA`

Table 1 shows the required mount options.

For NFS Version 3 (NFSv3), you must switch off NFS locking to enable failover capabilities in multiple-host installations. Also, in single-host setups, NFS locking must be switched off to avoid NFS lock cleanup operations in the event of a software or server failure.

With NetApp ONTAP 9, you can configure the NFS transfer size with a value up to 1 MB. With 40 Gigabit Ethernet connections to the storage system, you must set the transfer size to 1 MB to achieve the expected throughput values.

<table>
<thead>
<tr>
<th>Common parameter</th>
<th>NFSv3</th>
<th>NFS transfer size with ONTAP 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>rw, bg, hard, timeo=600, intr, noatime</td>
<td>vers=3, nolock</td>
<td>rsiz=1048576, wsize=1048576</td>
</tr>
</tbody>
</table>

To mount the file systems during system boot using the `/etc/fstab` configuration file, complete the following steps.

**Note:** The following example shows an SAP HANA database with SID=VHA using NFSv3 and an NFS transfer size of 1 MB.

a. Add the file systems to the `/etc/fstab` configuration file:

```bash
cat /etc/fstab

<node02-data_lif01-ip>:/vhana01_data /hana/data/VHA/mnt00001 nfs
rw,bg,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
<node02-log_lif01-ip>:/vhana01-log_/hana/log/VHA/mnt00001 nfs
rw,bg,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
<node01-data_lif01-ip>:/vhana01_sapexe/usr-sap /usr/sap/VHA nfs
rw,bg,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
<node01-data_lif01-ip>:/vhana01_sapexe/shared /hana/shared nfs
rw,bg,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
```

b. Run `mount -a` on each host to mount the file systems and verify the mounts with the `df -h` command.
Sizing
This section provides sizing guidelines based on the virtual machine memory-to-vCPU ratio and the number of virtualized SAP HANA instances and hosts supported by by NetApp storage systems.

Computing
The generation of the CPU platform and SAP’s guidelines for the memory range supported for a socket count are the basis for sizing virtualized SAP HANA instances. The vCPU and virtual RAM (vRAM) maximums for a specific vSphere ESXi version also influence the sizing. Additionally, some memory overhead should be considered because ESXi needs some for its own kernel and for hosting virtual machine memory pages. Refer to the VMware documentation for more information.

With the Intel Xeon Platinum platform, SAP allows memory configurations of 128 GB to 3 TB on four-way server systems for SAP Business Warehouse on HANA (BWoH). It allows up to 6 TB for SAP Suite on HANA (SoH) workloads. With SAP HANA TDI Phase 5, SAP extends the support for Intel E7 CPUs to include all Intel Broadwell E7 and Skylake (Platinum, Gold and Silver) with 8 or more cores per socket. This makes a wide range of CPUs available for customers to choose from, for their specific workload.

The matrix in Table 2 provides a reference for technically feasible virtual machine configurations with the current top bin Intel Xeon Platinum platform (supported only on Cisco UCS M5 servers) and previous Intel Xeon processor generations.

Table 2. Virtual machine sizing: vCPU and vRAM with processor platform matrix

<table>
<thead>
<tr>
<th>vCPU (with hyperthreading on)</th>
<th>vRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Xeon E7 v4 8880</td>
<td></td>
</tr>
<tr>
<td>BWoH</td>
<td>SoH</td>
</tr>
<tr>
<td>≤SPS10</td>
<td>≥SPS11</td>
</tr>
<tr>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>66</td>
<td>66</td>
</tr>
<tr>
<td>88</td>
<td>88</td>
</tr>
<tr>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>120</td>
<td>120</td>
</tr>
</tbody>
</table>

Storage
NetApp recommends storing data for SAP HANA systems in NetApp FlexVol volumes connected through the NFS protocol. You should also mount these volumes directly on the guest operating systems because doing so offers greater flexibility and simplified management in heterogeneous landscapes.

Each SAP HANA host, either bare metal or VMware virtual machine, has two network interfaces connected to the storage network. One network interface is used to mount the log volumes, and the second interface is used to mount the data volumes for SAP HANA. The data and log volumes of the SAP HANA systems must be distributed equally to the storage nodes.

SAP requires KPIs for storage throughput to be fulfilled for productive SAP HANA systems. As this number of SAP HANA hosts differs for different storage systems, the optimum storage systems to SAP HANA nodes ratio will be determined during the sizing
process. Nonproduction SAP HANA systems though need not fulfill the storage throughput KPIs, it is a good practice to include them in the sizing process to achieve the expected performance.

Appendix: Cisco Application Centric Infrastructure (ACI) based solution configuration

This section provides a network layer configuration for a Cisco Application Centric Infrastructure (Cisco ACI™) solution. The Cisco Validated Design FlexPod for SAP Solution with Cisco ACI is the reference for this section.

The fabric access policies define the connectivity and prepare the infrastructure platform for implementing a virtualized SAP HANA system.

1. Create a pool of VLANS that virtualized SAP HANA systems can use:

   - VLAN Pool - vHANA-VLANs (Dynamic Allocation)

     **Properties**
     - Name: vHANA-VLANs
     - Description: vHANA-VLANs
     - Allocation Mode: Dynamic Allocation
     - VLAN Range: 100-500

2. For the application tenant configuration, the existing endpoint groups (EPGs) HANA-T01-Mgmt and HANA-T01-Mgmt-External serve as ESXi-Mgmt and vCenter-Mgmt entities in the virtual scenario. The iSCSI Initiator and Target EPGs enable ESXi hosts to boot through iSCSI. HANA Data and Log EPGs provide persistence endpoint access:

<table>
<thead>
<tr>
<th>Application EPG</th>
<th>Bridge Domain</th>
<th>Physical Domain</th>
<th>Paths</th>
<th>Port Encap</th>
</tr>
</thead>
<tbody>
<tr>
<td>HANA-T01-HANA Data</td>
<td>HANA-T01/HANA-T01-Storage</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-Netapp-control-a</td>
<td>vlan-&lt;&lt;var_storage_data_vlan_id_a&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-Node-Data</td>
<td>HANA-T01/HANA-T01-Storage</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-Netapp-control-b</td>
<td>vlan-&lt;&lt;var_storage_data_vlan_id_b&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-HANA-Log</td>
<td>HANA-T01/HANA-T01-Storage</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-11</td>
<td>vlan-&lt;&lt;var_storage_log_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-Node-Log</td>
<td>HANA-T01/HANA-T01-Storage</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-12</td>
<td>vlan-&lt;&lt;var_storage_log_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-Mgmt</td>
<td>HANA-T01/HANA-T01-Mgmt</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-11</td>
<td>vlan-&lt;&lt;var_admin_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-ESXi-Mgmt</td>
<td>HANA-T01/HANA-T01-Mgmt</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-12</td>
<td>vlan-&lt;&lt;var_admin_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-Mgmt-External / HANA-T01-vCenter</td>
<td>HANA-T01/HANA-T01-Mgmt</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-ESXMT-Port</td>
<td>vlan-&lt;&lt;var_admin_vlan_id_mgmt&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-iscsi-InitiatorA</td>
<td>HANA-T01/HANA-T01-iscsiA</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-11</td>
<td>&lt;&lt;iscsi_vlan_id_a&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-iscsi-TargetA</td>
<td>HANA-T01/HANA-T01-iscsiA</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-Netapp-control-a</td>
<td>&lt;&lt;iscsi_vlan_id_a&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-iscsi-InitiatorB</td>
<td>HANA-T01/HANA-T01-iscsiB</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-FIB-12</td>
<td>&lt;&lt;iscsi_vlan_id_b&gt;&gt;</td>
</tr>
<tr>
<td>HANA-T01-iscsi-TargetB</td>
<td>HANA-T01/HANA-T01-iscsiB</td>
<td>HANA</td>
<td>Host 1/Node 1/Node 101-102/VPC-Netapp-control-b</td>
<td>&lt;&lt;iscsi_vlan_id_b&gt;&gt;</td>
</tr>
</tbody>
</table>
3. The virtualized SAP HANA system needs one additional EPG for the vMotion network and a corresponding bridge domain:

<table>
<thead>
<tr>
<th>Application EPG</th>
<th>Bridge Domain</th>
<th>Physical Domain</th>
<th>Paths</th>
<th>Port Encap</th>
</tr>
</thead>
<tbody>
<tr>
<td>HANA-T01-vMotion</td>
<td>HANA-T01/HANA-T01-HANA</td>
<td>HANA</td>
<td>Pod-1/Node 101-102/vPC-FIA-11</td>
<td>&lt;&lt;var_vmotion_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pod-1/Node 101-102/vPC-FIB-12</td>
<td>&lt;&lt;var_vmotion_vlan_id&gt;&gt;</td>
</tr>
</tbody>
</table>

4. With respect to contracts, because vMotion communication occurs within the same EPG, no additional contract needs to be created.

Table 3 provides a map of Cisco ACI and VMware constructs.

**Table 3. Comparison of Cisco ACI and VMware constructs**

<table>
<thead>
<tr>
<th>Cisco APIC terms</th>
<th>VMware terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine controller</td>
<td>VMware vCenter (data center)</td>
</tr>
<tr>
<td>Virtual machine manager (VMM) domain</td>
<td>VMware vSphere Distributed Switch (vDS)</td>
</tr>
<tr>
<td>Endpoint group (EPG)</td>
<td>Port group</td>
</tr>
</tbody>
</table>

5. After the fabric access policies, EPGs, and bridge domains are in order, configure the vCenter domain, providing the details of the vCenter server and the login credentials for the Cisco Application Policy Infrastructure Controller (APIC) to create the virtual distributed switch through which the host networks are managed centrally.

**Cisco ACI virtual machine management (VMM)**

Cisco ACI takes a systems-based approach and provides tight integration between ACI ready physical infrastructure and VMware virtual elements. Cisco ACI integration with VMware virtual environments enables users to use a common policy based operational model across their physical and virtual environments.

6. Create a vCenter domain:
7. Add vCenter credentials and vCenter details; for vSwitch Policy, select Cisco Discovery Protocol (CDP); and for Port Channel Mode, choose MAC Pinning:

For more information
Consult the references listed here for additional information.

Certified SAP HANA Hardware Directory
Certified SAP HANA Hardware Directory: Enterprise Storage

SAP HANA TDI documentation
SAP HANA TDI: Overview
SAP HANA TDI: FAQ
SAP HANA TDI: Storage Requirements
SAP HANA TDI: Network Requirements

SAP Notes
SAP Notes Related to VMware
SAP Note 2161991: VMware vSphere configuration guidelines
SAP Note 1788665: SAP HANA Support for virtualized and partitioned (multitenant) environments
SAP Note 2393917: SAP HANA on VMware vSphere 6.5 in production
SAP Note 1943937: Hardware Configuration Check Tool—Central Note
SAP Note 2235581: SAP HANA: Supported operating systems
SAP Note 2205917 - SAP HANA DB: Recommended OS settings for SLES 12 and SLES for SAP Applications 12
SAP Note 2292690 - SAP HANA DB: Recommended OS settings for RHEL 7
Additional references

SAP Community Network: [SAP HANA TDI on Cisco UCS and VMware vSphere](#)


Cisco UCS: [Design Zone for SAP Applications](#) (technical documentation)

Cisco UCS: [Data Center Solutions for SAP](#) (customer references)


NetApp: [TR-4290 SAP HANA on NetApp FAS Systems with NFS Configuration Guide](#)

NetApp: [TR-4614 SAP HANA Backup and Recovery with SnapCenter](#)

VMware blog: [SAP on VMware updates](#)