

VALIDATED REFERENCE DESIGN GUIDE

ARUBA CX NETWORKING AND NIMBLE W/SPHERE DEPLOYMENT/INTEROP GUIDE

CONTENTS

- Introduction..... 4
- Solution overview 4
 - Aruba AOS-CX Data Center Networking..... 4
 - HPE Synergy Infrastructure 5
 - HPE Nimble Storage Arrays 6
 - Nimble Considerations for iSCSI Connectivity for vSphere 7
 - vSphere Networking 7
 - Switch Connectivity..... 8
 - MTU 9
 - Flow control..... 9
 - Jumbo frame..... 9
 - VLAN 9
 - Aruba and Nimble Use Cases..... 10
- Solution Architecture - Example 11
 - Configuration Details 13
 - Configure the Network..... 13
 - Initial switch config and import into NetEdit for management 14
 - VSX configuration on Aruba CX switch A and B 15
 - Configure Interfaces (LAG, descriptions, VLANs, jumbo frames, flow control) 19
 - Configure Network Time Protocol (NTP) – Spanning Tree Protocol (STP) 22
 - Deploy the HPE Nimble Storage array 25
 - Initialize and configure the HPE Nimble Storage array 25
 - Configure the Array for data access..... 27
 - VMware Integration..... 28
 - Add HPE ProLiant servers into the HPE Nimble Storage environment 29
 - Create Virtual Volumes and apply to required hosts..... 30
 - Configure VC Modules/Server Profiles in Synergy Frame 31
 - Create an iSCSI Nimble Network..... 31
 - Configure Uplinks out of Frame (Interconnect Group) 32
 - Configure Downlinks to Server Blade (Server Profile)..... 34
 - Configure VMware and add Nimble datastore..... 36
 - vSwitch creation 36
 - VMware Storage Adapter configuration 37
 - Add new datastore 37
 - Nimble vCenter Plugin 38

© Copyright 2019 Hewlett Packard Enterprise Development LP

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

INTRODUCTION

The guide provides information on how to build a scalable network infrastructure that connects hosts to Nimble storage to address the business requirements, workloads, and applications required by our customers.

The guide describes an architecture that combines HPE Synergy 480 Gen9 Compute Modules, DL360 Gen9 Servers, HPE Nimble Storage array, and Aruba data center switches to reliably deploy and run the virtualized infrastructure.

The intended audience for this document is IT administrators and solution architects planning on deploying IP Multicast features.

SOLUTION OVERVIEW

The HPE DL/BL, Nimble Storage, and Aruba networking offers an infrastructure platform that incorporates compute, network, and storage to deliver a resilient, scalable, and flexible datacenter architecture for enterprise and cloud deployments.

Aruba AOS-CX Data Center Networking

Aruba's next-gen AOS-CX switching portfolio is purpose-built for today's digital world, satisfying the most demanding use cases from the access layer, to the core, and to the data center. Built on cloud-native principles, our portfolio gives IT the flexibility to deploy a single platform from edge access to the data center that includes intuitive management tools and distributed analytics that transform the IT network operator experience.

Built from the ground up with a combination of cutting-edge hardware and powerful AOS-CX operating system, our family of switches are designed for today's most demanding enterprise campus, branch, and data center networks.

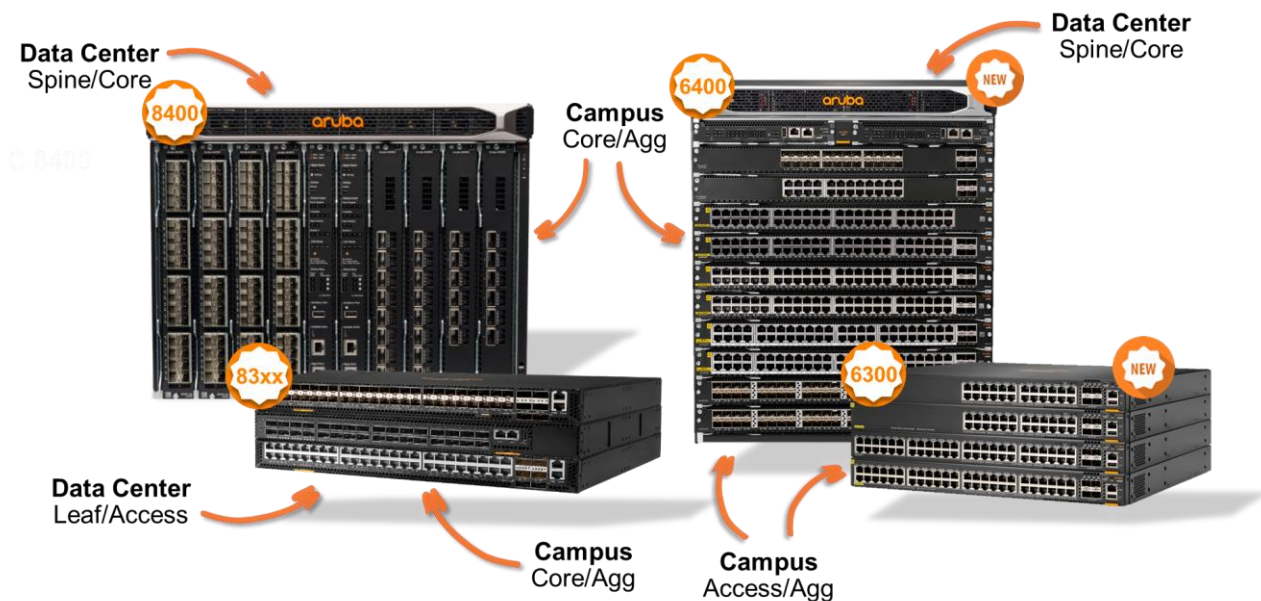
From small to large enterprise environments, Aruba's comprehensive portfolio includes solutions ideal for access, aggregation, core, and data center deployments.

The Aruba AOS-CX switches are all managed using Aruba NetEdit.

- **AOS-CX 8400 Switch Series:** Provides industry-leading line rate 10GbE/40GbE/100GbE port density in an 8-slot chassis for factor. The 8400 provides very low latency, and scalability for support of full Internet routes which allows it to fit into most enterprise core and aggregation solutions that require higher performance and higher uptime.
- **AOS-CX 832x Switch Series:** These switches serve the needs of the next generation Leaf, ToR, aggregation, and small core layers, as well as emerging data center requirements. They provide 6.4Tbps of capacity, with line-rate Gigabit Ethernet interfaces including 10Gbps, 25Gbps, 40Gbps, and 100Gbps. These switches offer a fantastic investment for customers wanting to migrate from older 1GbE/10GbE to faster 25GbE, or 10GbE/40GbE to 100GbE ports.
- **AOS-CX 6400 Switch Series:** The Aruba CX 6400 Switch Series is positioned for both Campus and data center environments. The Aruba CX 6400 are modular switches (5 slot and 10 slot) which are able to deliver the demanding access features like PoE for WiFi6, while also supporting higher speed 40/100G interfaces for more demanding environment.

- **AOS-CX 6300 Switch Series:** The Aruba CX 6300 1 RU switch is positioned for campus access layer as well as out of band deployments in data centers. The 6300 leverages access control which is smart and unified across the network with Dynamic Segmentation. The 6300 provides Power and Bandwidth for Wi-Fi 6 and Convenience through hardware flexibility.

Figure 1. Aruba CX Switch portfolio



HPE Synergy Infrastructure

HPE Synergy is an infrastructure that bridges traditional and cloud native applications through the implementation of composable infrastructure. Composable infrastructure starts with fluid resource pools. Composable pools of compute, storage, and fabric work as a single structure, ready to boot up for any workload. Such pools can also be instantly turned on and flexed to meet the needs of any business application. The fluid nature of this architecture effectively eliminates stranded resources by enabling administrators to build the environment in a way that disaggregates the underlying compute, storage, and fabric resources.

In this context, disaggregation basically means that you are able to scale each resource individually. You are not forced to add resources that are not required in order to get the resources you need.

The HPE Synergy 12000 frame is the hardware foundation for the HPE composable vision. It provides a location in which compute, storage, fabric, and management are all aggregated. The HPE Synergy 12000 frame is optimized to include all elements required to run any workload. It includes embedded management, and it is designed to support a wide range of compute modules and storage options.

For composable storage, HPE Synergy provides support for file, block, and object-based storage systems and supports a variety of both internal and external storage modules and arrays.

HPE Synergy supports both two-socket and four-socket compute modules that provide the performance, scalability, density optimization, storage simplicity, and configuration flexibility to power a variety of workloads, including business processing, IT infrastructure, web infrastructure, collaborative, and high-performance computing.

The back of the frame includes fabric interconnects, enabling flexibility with regard to storage and other interconnectivity needs. The frame is designed to be optimized for longevity. HPE has taken into consideration ongoing requirements for power, cooling, and bandwidth that might occur over the next decade.

Figure 2. HPE Synergy Frame

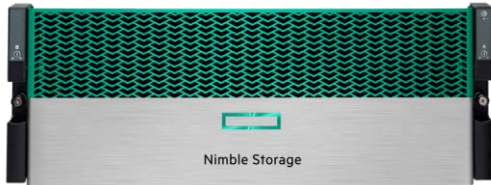


HPE Nimble Storage Arrays

The HPE Nimble Storage HF-Series array family starts at the entry level with the HF20 model and expands through the HF20H, H20C, HF40, HF40C, HF60, HF60C models up to the HF60 Scale out model at the high end. The Adaptive Flash arrays are truly adaptive. They are designed for both Primary and Secondary flash workloads. Hybrid Flash arrays are built for mixed, primary workloads, and where cost-efficient flash performance is important. It is a Secondary Flash array for backup and DR while allowing you to put your backup data to work.

The HPE Nimble Storage AF-Series array family starts at the entry level with the AF20Q model and expands through the AF20, AF40, and AF60 models up to the AF80 model at the high end. All-flash arrays can be upgraded non-disruptively from the entry level all the way up to the high-end array model. This is the next generation of the HPE Nimble Storage all-flash arrays.

Figure 3. Nimble AF20



Nimble Considerations for iSCSI Connectivity for vSphere

When deploying a Nimble solution, there are two options for base connectivity to the Nimble arrays: iSCSI or FC. This guide is solely focused on the iSCSI solution as FC deployments would require separate FC switch-based solutions.

vSphere Networking

For iSCSI connectivity between the vSphere environment and the Nimble arrays, the VMware ESXi™ host must have a minimum of two physical network interface cards (NICs). Nimble recommends to dedicate at least two physical NICs to iSCSI storage access. On the ESXi host, use the following NIC allocation model

- vmnic0 and vmnic1: For management traffic, vMotion traffic, and VM traffic
- vmnic2 and vmnic3: VMkernel ports for IP storage

The VMware software iSCSI initiator is the preferred means for connecting to Nimble storage by using the iSCSI protocol. There are two connection methods to achieve HA and load distribution:

- Method 1: One vmnic per vSwitch, and one VMkernel port per vSwitch
- Method 2: Two or more vmnics per vSwitch, and one dedicated VMkernel port per vmnic

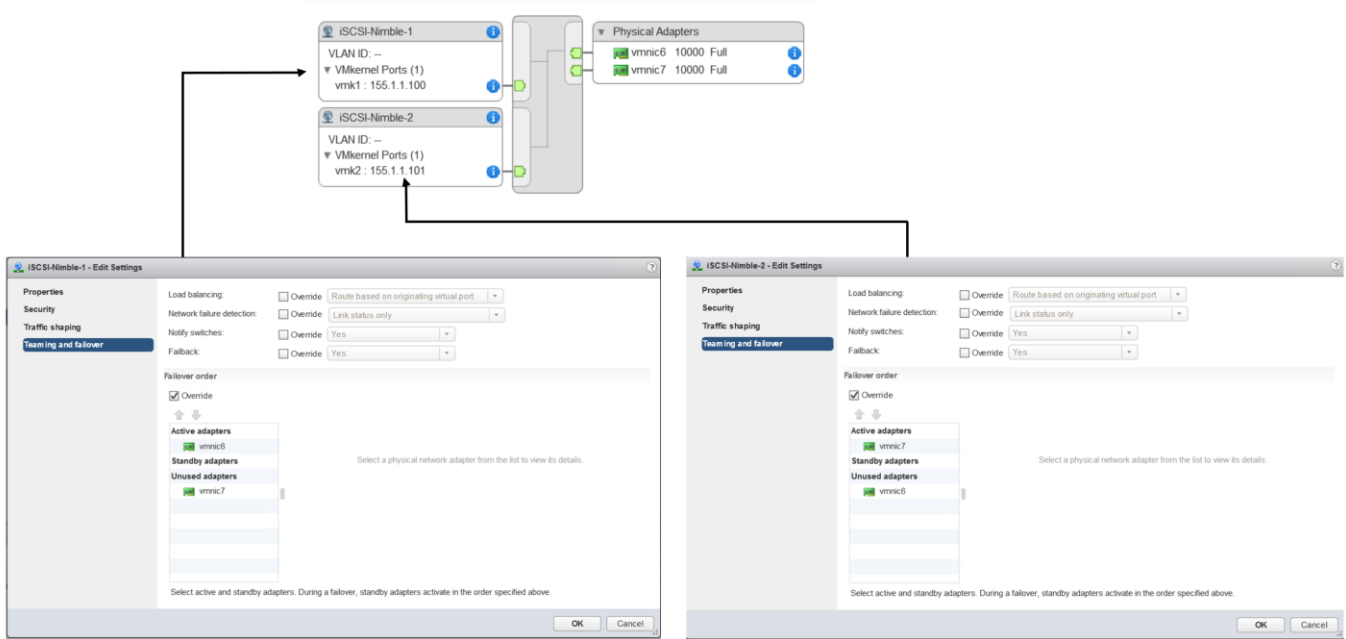
With both methods, the choice to bind VMkernel ports to the software iSCSI adapter depends on whether the ports are in the same broadcast domain and IP subnet:

- When the VMkernel ports for software iSCSI multipathing are in the same broadcast domain and IP subnet, bind the VMkernel ports to the software iSCSI adapter. Array target iSCSI ports must also reside in this broadcast domain and IP subnet.
- When the VMkernel ports for software iSCSI multipathing are in different broadcast domains and IP subnets, must not bind the VMkernel ports to the software iSCSI adapter.

For more information about whether to use iSCSI port binding, see [VMware KB 2038869](#).

Although both connection methods allow ESXi iSCSI multipathing to provide high availability and load distribution for storage access, the second method has a slight advantage. It is easier to deploy and manage because only one vSwitch is required. To use multiport NICs, ensure that iSCSI traffic spans different physical NICs instead of multiple ports on the same physical NIC. This approach prevents a single physical NIC failure from disrupting access to iSCSI storage. The following configuration illustrates this method.

Figure 4. Sample network configuration using two VMkernel ports and a single vSwitch



Switch Connectivity

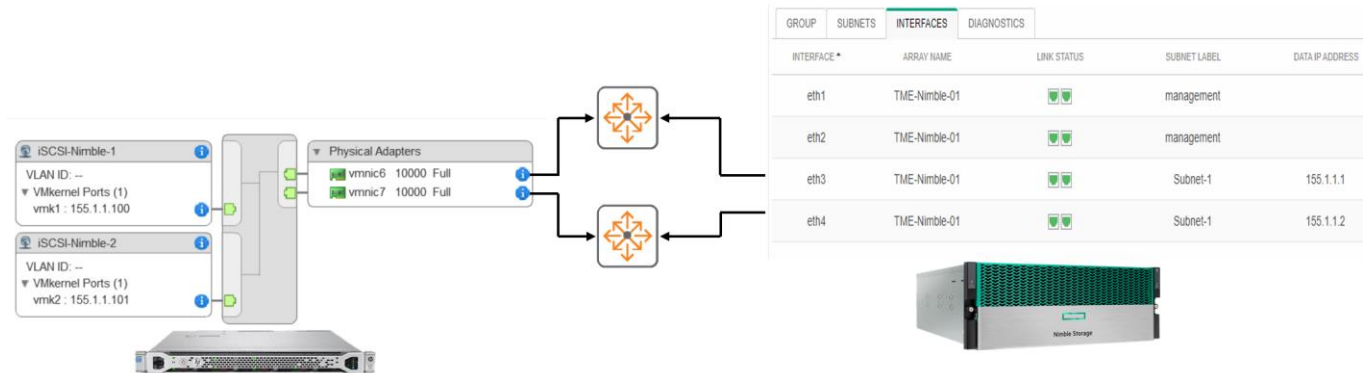
To prevent a single-switch failure that might cause a virtual infrastructure outage, Nimble recommends that use dual physical switches for the connection between the ESXi host and the Nimble array.

On a Nimble array, designate separate network interfaces for management traffic and data traffic, or share management traffic and data traffic on the same interface. Although a single interface can serve both types of traffic, Nimble recommends dedicating a pair of interfaces to management traffic and use the remaining interfaces to serve only data traffic.

Ensure that all data access interfaces are connected to the physical switch that is dedicated to storage traffic using layer 2. If the physical switch is shared with other traffic (such as management traffic, vMotion traffic, or VM networks), use a private (non-routable) address set for connectivity between the ESXi VMkernel ports and the Nimble data access interfaces.

Connect the management interface to the same network segment to which the VMware vCenter Server™ instance is connected. The Nimble Storage vCenter plugin requires network connectivity between the vCenter Server and the Nimble array management interfaces.

Figure 5. Example data path for Nimble/vSphere



MTU

Many switches define MTU differently from the initiator/target. Switches often define MTU as the frame size. End hosts almost universally define MTU as the packet size. The configured frame size on the switch might need to be larger than the packet size or the MTU value defined on the host and the array. For example, a value of 9000 on the host might require a value of 9014 or higher on the switch. This difference might vary by manufacturer.

Setting the switch MTU value to a number that is higher than the MTU value on the host or initiator does not cause problems. The switch MTU setting causes problems only when the MTU value on the intermediate device (the switch) is set to a number that is lower than the MTU value on one or both of the end devices.

Flow control

Flow control provides a mechanism for temporarily pausing the transmission of data on Ethernet networks if a sending node transmits data faster than the receiving node can accept it. Whenever possible, enable flow control on all host, switch, and array ports to ensure graceful communication between network nodes. HPE Nimble Storage array network interface cards (NICs) support flow control by default.

Jumbo frame

Ethernet frames that transport data are typically 1500 bytes in size. Anything over 1514 bytes (or 1518 with VLAN tagging) in the Ethernet frame is typically referred to as a jumbo frame. Jumbo frames are generally better suited to handle the flow of iSCSI SAN traffic. They typically consist of 9000-byte frames. Enabling jumbo frames can help to improve storage throughput and reduce latency.

VLAN

To work properly, the HPE Nimble Storage solution requires at least two VLANs. The iSCSI VLAN and the management VLAN

must be the native VLAN in the trunk port (untagged).

For more Nimble site requirements, installation instructions, and other general reference materials, see the [HPE Nimble Storage documentation page of the HPE InfoSight portal \(login required\)](#).

Aruba and Nimble Use Cases

Due to the considerations required for Nimble connectivity, the following topologies would be acceptable uses cases when working with Aruba CX networking.

Collapsed Core style networks are built using a “End-of-Row” or “Middle-of-Row” designs like the one shown below, and they are very common and simple solutions. These solutions are able to take advantage of superior MLAG style solutions like Aruba VSX, which allows for pairs of devices to appear like a single device to attached hosts and switches and enables the HA requirement so valued by customers.

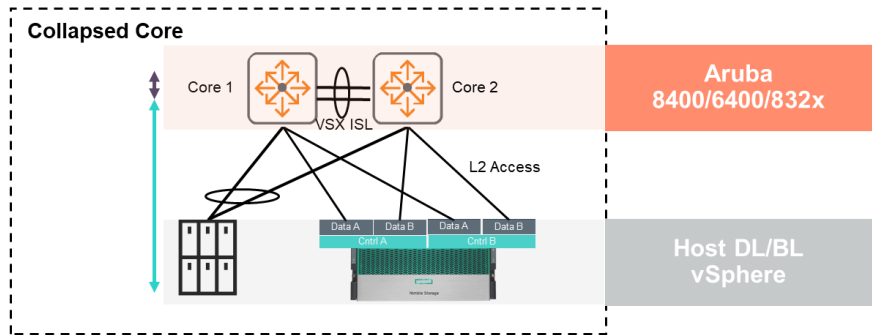
Large chassis-based switches like the Aruba 8400/6400 can be used in these solutions, but they are not mandatory. The actual switches should be based on the projected scale of the individual environment.

Since all the servers within this environment are connected directly to a HA Aruba 8325/8400/6400, they would all have access to each other for optimal east-west L2 traffic flows with no need for features such as VXLAN.

Figure 6. Collapsed Core example

Nimble solution uses:

- Jumbo Frames
- Layer 2
- Flow Control (recommended)
- Keep Mgmt and Data separate (OOB and In-Band)
- Active/Passive Controllers (IPs fail over)
- No Link Agg (LACP) support



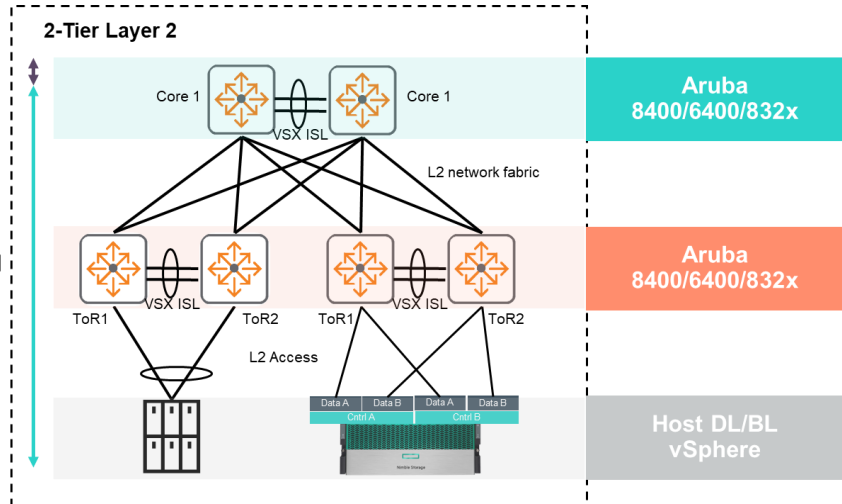
2-Tier Layer 2 solutions like the one shown below also take advantage of VSX both at the core layer and at the access layer. This provides an easy to manage HA solution which supports live upgrades on all devices, and it can scale more than the Collapse Core option.

All hosts connect to pairs of VSX switches at the Access layer to provide HA, while each of the Access Layer switches connect to each of the 2 Core Layer switches. All hosts will leverage Link Agg or LACP and the Access Layer switches will also leverage LACP to the Core Layer. This ensures that all links will be utilized as traffic flows get hashed.

Figure 7. 2-Tier Layer 2 example

Nimble solution uses:

- Jumbo Frames
- Layer 2
- Flow Control (recommended)
- Keep Mgmt and Data separate (OOB and In-Band)
- Active/Passive Controllers (IPs fail over)
- No Link Agg (LACP) support



SOLUTION ARCHITECTURE - EXAMPLE

The solution and configuration examples are based on the following topology and components:

- HPE Synergy 12000 frame
- HPE Synergy 480 Gen9 Compute Module
- HPE Virtual Connect SE 40Gb F8 Modules
- HPE Proliant DL360 Gen9 Server
- HPE Nimble Storage array CS210
- Aruba CX 8325 Data Center Switches – Data path
- Aruba CX 6300 Switch – OOB path
- VMware ESXi and vSphere 6.7 for hypervisor and management

As shown in the figure below, the solution consists of two Aruba CX 8325 Switches configured using VSX which allows them to be seen by attached devices as a single switch via MLAG. This ensures there is always a path from traffic even if a single switch fails.

The 8325s are operating as a ToR switch to provide the critical path for iSCSI traffic.

It is important to note that while the 8325 switches are configured in a VSX based MLAG solution, the Nimble array itself does not support link aggregation. The Nimble arrays operate using dual controllers in an active/standby configuration. The number and type of interfaces available will vary based on the solution, however, each interface will be assigned to a network segment.

The images below show an array that has 2 management interfaces and 2 data interfaces on each controller. All configurations to the active controller NICs will fail over to the standby controller in the event of a failover.

Figure 8. Nimble array dual controllers

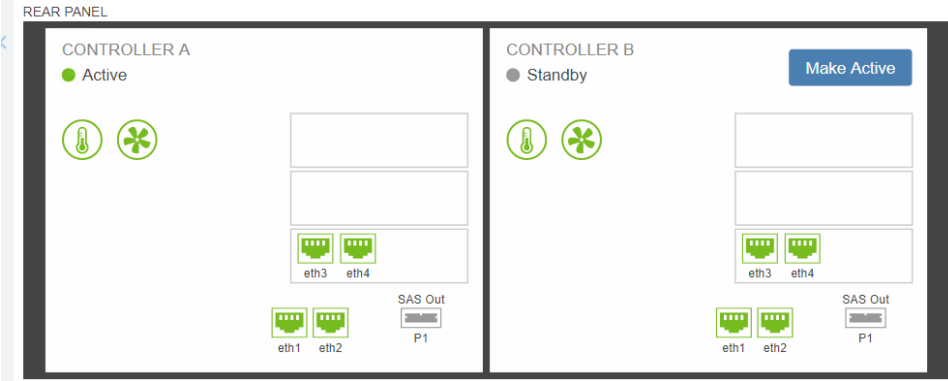


Figure 9. Nimble array NIC configuration example

GROUP	SUBNETS	INTERFACES	DIAGNOSTICS	
INTERFACE	ARRAY NAME	LINK STATUS	SUBNET LABEL	DATA IP ADDRESS
eth1	TME-Nimble-01		management	
eth2	TME-Nimble-01		management	
eth3	TME-Nimble-01		Subnet-1	155.1.1.1
eth4	TME-Nimble-01		Subnet-1	155.1.1.2

The management interfaces in this solution are connected into an Aruba CX 6300 Switch to provide the management path into the array.

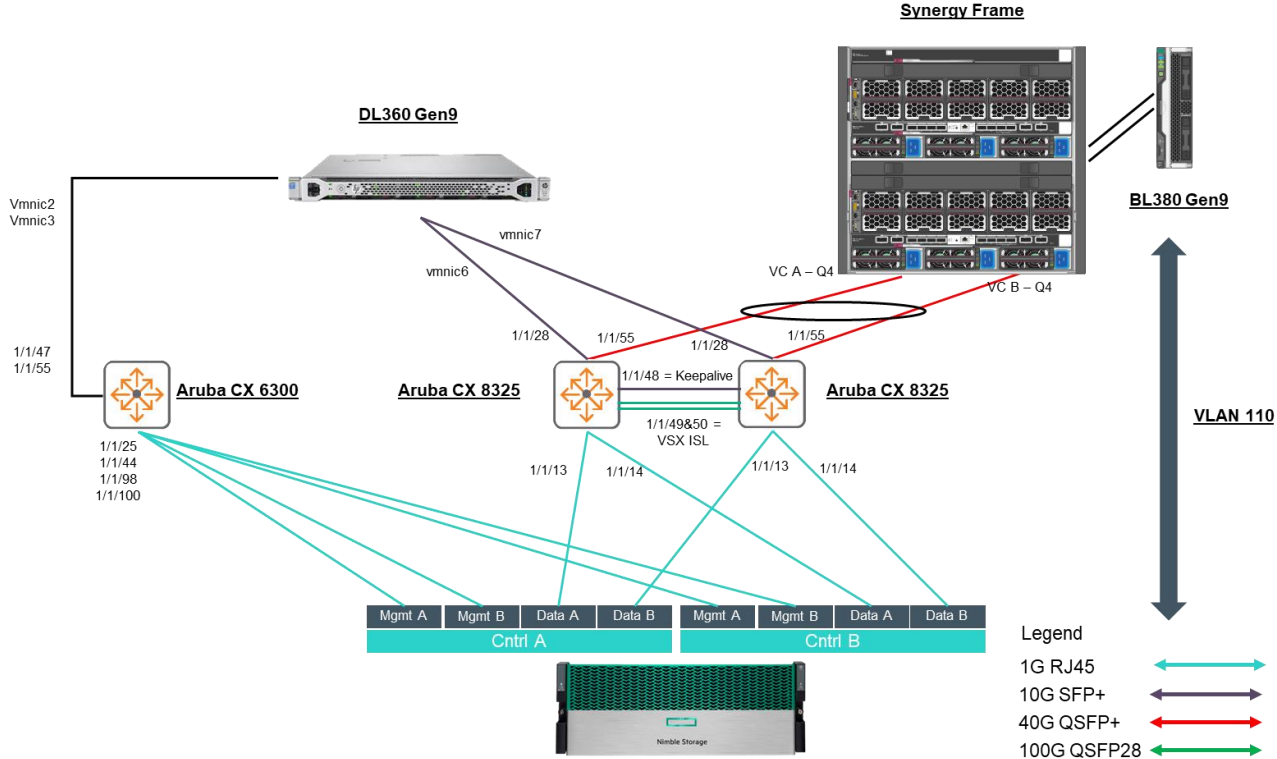
The example solution also leverages an HPE Proliant DL360 Gen9 Server as well as the Synergy Frame with a Proliant BL380 Gen9 Server. These are the hosts in a vCenter 6.7 environment that the volumes on the array are exported to and in which VMs will utilize.

The solution is leveraging 1G interfaces to connect to the Nimble array, the DL server is connected with 10GbE SFP+ interfaces, and the HPE Synergy Frame is connected using 40GbE interfaces from the HPE Virtual Connect SE 40Gb F8 modules. The solution uses one HPE Synergy 480 Gen9 Compute Module in Bay2.

This solution is leveraging an existing vCenter 6.7 environment that both hosts belong to.

Once configured properly the solution will provide for redundant storage connectivity by both server hosts with multipathing for high availability.

Figure 10. Example solution



Configuration Details

To prepare for deployment complete the following tasks:

1. Understand the physical infrastructure layout.
 - a. Collapsed Core – Used in this example
 - b. 2-Tier Layer 2
2. Configure the network.
3. Deploy the HPE Nimble Storage array
4. Configure VC Modules/Server Profiles in Synergy Frame
5. Configure VMware and add datastore

Configure the Network

The following procedures describe how to configure the Aruba CX 8325 (or 8320) switches for use in an HPE Nimble storage

environment. To configure the Aruba CX switches for HPE Nimble Storage, complete the following tasks:

1. Initial switch config and import into NetEdit for management
2. Set up the VSX configuration on Aruba CX switch A and B
3. Configure Interfaces (LAG, descriptions, VLANs, jumbo frames, flow control)
4. Add final global configs that may be needed - Network Time Protocol (NTP) – Spanning Tree Protocol (STP).

Initial switch config and import into NetEdit for management

Note that the configuration listed are for the 8325 switches used for iSCSI traffic. The mgmt ports on the server iLOs and Nimble array are all connected to a single OOB switch using a single VLAN.

For NetEdit to manage each switch, initial configs should be added via one of these options:

- Aruba CX mobile app
- Console cable
- Zero Touch Provisioning (ZTP)

Sample Initial Configuration:

```
hostname LEAF1
user admin group administrators password ciphertext AQBapUz+
ssh server vrf mgmt
interface mgmt
    no shutdown
    ip static 10.6.8.19/24
    default-gateway 10.6.8.1
! interface group 1 contains ports 1/1/1-1/1/12
system interface-group 1 speed 10g
! interface group 4 contains ports 1/1/37-1/1/48
system interface-group 4 speed 10g
https-server rest access-mode read-write
https-server vrf mgmt
```

Once the switches are configured and physically connected, ensure NetEdit has IP connectivity to switch management IPs and add all devices into NetEdit [Devices -> Action -> Add Device(s) or Add Multiple Devices].

Figure 11. Adding devices into NetEdit

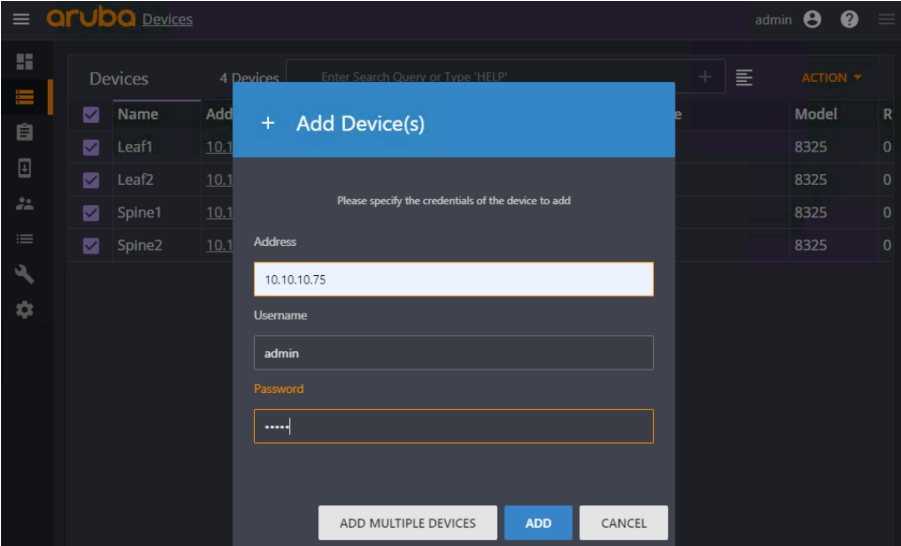


Figure 12. Devices added

Name	Address	Status	MAC	Serial	Current Firmware	Model	R
Leaf1	10.10.10.165	OK	548028-fd...	TW93KM0...	GL.10.03.0020	8325	0
Leaf2	10.10.10.163	OK	548028-fd...	TW93KM0...	GL.10.03.0020	8325	0
Leaf3	10.10.10.75	OK	548028-fd...	TW93KM0...	GL.10.03.0020	8325	0
Spine1	10.10.10.41	OK	548028-fe...	TW8BKM...	GL.10.03.0020	8325	0
Spine2	10.10.10.40	OK	548028-fe...	TW8BKM...	GL.10.03.0020	8325	0

VSX configuration on Aruba CX switch A and B

Create a VSX plan for the Aruba CX switches in NetEdit [Devices -> select switches -> Action -> Edit Running Config] and name the plan. In this setup, interface 1/1/48 is used as the keepalive, while 1/1/49 & 1/1/50 are used for the ISL link.

Figure 13. Selecting CX switches for VSX Plan

Name	Address	Status	MAC	Serial	Current Firmware	Manufacturer	Model	Running Config Modified	Cu
Zone1-Leaf2b	10.10.10.162	❌	548028-fdf400	TW93KM000K	GL.10.04.0001	Aruba	8325	12/04/19 12:01:07	52
Zone1-Leaf1a	10.10.10.165	❌	548028-fda400	TW93KM001Y	GL.10.04.0001	Aruba	8325	12/05/19 08:08:39	92
Zone1-Leaf1b	10.10.10.163	❌	548028-fd2800	TW93KM0026	GL.10.04.0001	Aruba	8325	12/05/19 08:02:41	71
Zone1-Spine2	10.10.10.40	❌	548028-fef900	TW8BKM301F	GL.10.04.0001	Aruba	8325	12/04/19 12:06:25	54
Zone1-Spine1	10.10.10.41	❌	548028-fe2900	TW8BKM3030	GL.10.04.0001	Aruba	8325	12/04/19 12:06:25	38
Zone1-Leaf2a	10.10.10.75	❌	548028-fde700	TW93KM0009	GL.10.04.0001	Aruba	8325	12/04/19 12:01:07	60
8325	10.10.10.190	✅	548028-fef900	TW8BKM304D	GL.10.03.0001AH	Aruba	8325	12/11/19 08:19:23	12
8320	10.10.10.124	✅	d06726-e2b6d2	TW87KCW01H	TL.10.04.0001	Aruba	8320	12/11/19 08:20:01	8
8325-RU33	10.10.10.153	✅	548028-fd1900	TW93KM002N	GL.10.04.0001	Aruba	8325	12/11/19 11:02:17	1
8325-RU34	10.10.10.54	✅	548028-fd5400	TW93KM0034	GL.10.04.0001	Aruba	8325	12/11/19 11:02:22	1

Figure 14. VSX Plan

+ Create Plan

Name
VSX Config Leafs

Description
Configuring VSX on all Leaf pairs

Plan Attributes

CREATE **CANCEL**

Configure VSX in both racks and right click to modify the interface IPs, keepalive settings, and roles for each device.

Note that the best practice for:

- VSX ISL physical ports is to use a LAG and select at least two ports of the same speed (2x40G or 2x50G or 2x100G).
- The Keepalive connection is to use a direct L3 circuit, which can be low speed (1G transceiver is enough, 1GBASE-T works as well) between both VSX nodes, and to use a /31 subnet as only 2 nodes will need to communicate together.
- VLAN trunking on the ISL LAG is to permit ALL VLANs, for a simpler configuration. However, specifying a restrictive

list of VLAN IDs is entirely valid if the network admin wants more control.

- LACP timers on the ISL LAG is to keep the default long timer (30s = lacp rate slow).
- ACL is to not set any access-list on the ISL LAG in order to avoid engineering complex and unnecessary ACL design. The ISL can be seen as a virtual data back-plane with security filtering being processed before or/and after crossing the ISL.
- QoS trust mode on the ISL LAG to relay on the qos trust dscp that is globally configured on the Aggregation switches. If not configured globally (which is the recommendation), qos trust dscp has to be set on the ISL LAG.
- VSX system-mac is to set the system-mac manually on the VSX primary switch. Here, we use: 02:01:00:01:00:00. The main advantage to set VSX system-mac (and not to leave it blank with default HW system-mac being used) is to be agnostic from the physical hardware MAC address. If there is a need for hardware replacement of the VSX primary, the new switch can be configured exactly with same configuration than previous unit and there will be no impact as the secondary will remain in the same cluster ID. HW replacement is hitless for the secondary.

8325 Switch A

```
interface 1/1/48
  no shutdown
  description CSX Keepalive physical link
  ip address 111.1.1.0/31
interface 1/1/49
  no shutdown
  mtu 9198
  description VSX ISL physical link
  lag 256
interface 1/1/50
  no shutdown
  mtu 9198
  description VSX ISL physical link
  lag 256
interface lag 256
  no shutdown
  description VSX ISL link
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  qos trust dscp
vsx
  system-mac 02:01:00:01:00:00
  inter-switch-link lag 256
  role Primary
```

```
vsx-sync vsx-global
keepalive peer 111.1.1.1 source 111.1.1.0

8325 Switch B
interface 1/1/48
  no shutdown
  description VSX Keepalive physical link
  ip address 111.1.1.1/31
interface 1/1/49
  no shutdown
  mtu 9198
  description VSX ISL physical link
  lag 256
interface 1/1/50
  no shutdown
  mtu 9198
  description VSX ISL physical link
  lag 256
interface lag 256
  no shutdown
  description VSX ISL link
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  qos trust dscp
vsx
  inter-switch-link lag 256
  role Secondary
  keepalive peer 111.1.1.0 source 111.1.1.1
```

Figure 15. NetEdit example config

```
25 interface lag 256
26   description VSX ISL Link
27   no shutdown
28   no routing
29   vlan trunk native 1 tag
30   vlan trunk allowed all
31   lacp mode active
32   qos trust dscp
```

Figure 16. NetEdit example config (cont)

```

54 interface 1/1/48
55     description VSX Keepalive link
56     no shutdown
57     ip address A.B.C.D/M
58 interface 1/1/49
59     description VSX ISL Physical Link
60     no shutdown
61     mtu 9198
62     lag 256
63 interface 1/1/50
64     description VSX ISL Physical Link
65     no shutdown
66     mtu 9198
67     lag 256
68 vsx
69     system-mac 02:01:00:01:00:00 (8325-RU33 (10.10.10.153))
70     inter-switch-link lag 256
71     role SEL
72     keepalive peer A.B.C.D source A.B.C.D
73     vsx-sync vsx-global (8325-RU33 (10.10.10.153))

```

Select "RETURN TO PLAN" -> "DEPLOY" -> "COMMIT" to push down and save the desired configs.

Configure Interfaces (LAG, descriptions, VLANs, jumbo frames, flow control)

Create a plan for the Aruba CX switches in NetEdit [Devices -> select switches -> Action -> Edit Running Config] and name the plan.

In this plan we will configure the interfaces and VLANs as necessary.

Note that the best practice for:

- LACP timers on the VSX LAG is to keep the default long timer (30s = lacp rate slow).
- Hashing algorithm on the VSX LAG is to keep the default I3-src-dst (alternative being I2-src-dst), and would have an effect only if at least 2 ports per VSX node are members of the same VSX LAG.

8325 Switch A and B

! Add VLANs

vlan 110

vsx-sync

description Nimble Data Segment A

- Description on 8325 Switch A

description Nimble Data Segment B

- Description on 8325 Switch B

! Configure Nimble Facing Interfaces

```
interface 1/1/13
  description Nimble Data Path A
  no shutdown
  mtu 9198
  flow-control rx
  no routing
  vlan access 110
interface 1/1/14
  description Nimble Data Path B
  no shutdown
  mtu 9198
  flow-control rx
  no routing
  vlan access 110
! Configure DL Host Facing Interfaces
interface 1/1/28
  description DL360 Gen9
  no shutdown
  mtu 9198
  flow-control rx
  no routing
  vlan access 110
! Configure BL Host Facing LAG to Synergy
interface lag 256 multi-chassis
  description Synergy Frame - Nimble Path
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed 1,110
  lacp mode active
interface 1/1/55
  description Synergy Frame - Nimble Path
  no shutdown
  mtu 9198
  flow-control rx
  lag 256
```

Figure 17. NetEdit example config

```
8 vlan 110
9     vsx-sync
10    description ROL
```

Figure 18. NetEdit example config (cont)

```
25 interface lag 256 multi-chassis
26     description VSX ISL Link
27     no shutdown
28     no routing
29     vlan trunk native 1 tag
30     vlan trunk allowed all
31     lacp mode active
32     qos trust dscp
33 interface 1/1/13
34     description Nimble Data Path A
35     no shutdown
36     mtu 9198
37     flow-control rx
38     no routing
39     vlan access 110
40 interface 1/1/14
41     description Nimble Data Path B
42     no shutdown
43     mtu 9000
44     flow-control rx
45     no routing
46     vlan access 110
47 interface 1/1/28
48     description Nimble Data Path DL360
49     no shutdown
50     mtu 9000
51     flow-control rx
52     no routing
53     vlan access 110
```

Figure 19. NetEdit example config (cont)

```

71 interface 1/1/55
72     description Synergy Frame - Nimble Path
73     no shutdown
74     mtu 9198
75     flow-control rx
76     lag 256

```

Configure Network Time Protocol (NTP) – Spanning Tree Protocol (STP)

Create an NTP/STP plan for the Aruba CX switches in NetEdit [Devices -> select switches -> Action -> Edit Running Config] and name the plan.

Note that MSTP is the recommended best practice to protect the network infrastructure against mistake or cabling errors. The configuration should be kept as simple as possible as this is a protection mechanism and not a forwarding control-plane due to VSX LAG benefits.

- Keep the default common instance 0: MST0
- Keep the default spanning-tree priority of 8.
- All endpoint access ports are admin-edge, should not receive any BPDU (BPDU guard), should not trigger Topology Change Notification.
- Let VSX secondary synchronized by vsx-sync process.
- Use loop-protection on all endpoint access ports as extra-protection mechanism (in case of MSTP BPDUs are filtered by insertion of unmanaged switches which create a loop).

Add the appropriate configurations:

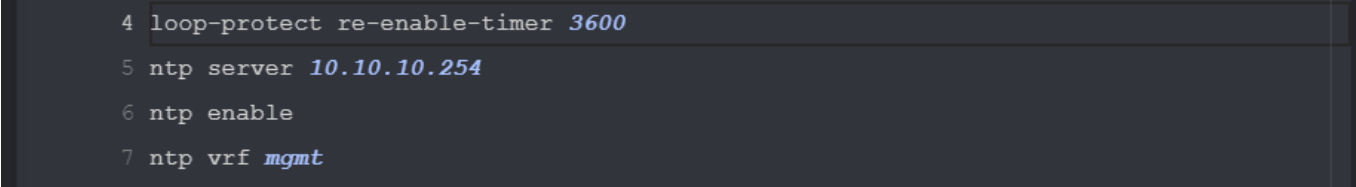
```

8325 Switch A and B
ntp server 10.10.10.254
ntp enable
ntp vrf mgmt
spanning-tree
loop-protect re-enable-timer 3600
interface 1/1/13
    spanning-tree bpdu-guard
    spanning-tree port-type admin-edge
    spanning-tree tcn-guard
    loop-protect
interface 1/1/14
    spanning-tree bpdu-guard
    spanning-tree port-type admin-edge

```

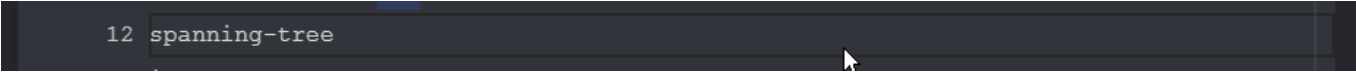
```
spanning-tree tcn-guard
loop-protect
interface 1/1/28
spanning-tree bpdu-guard
spanning-tree port-type admin-edge
spanning-tree tcn-guard
loop-protect
interface lag 256 multi-chassis
spanning-tree bpdu-guard
spanning-tree port-type admin-edge
spanning-tree tcn-guard
loop-protect
```

Figure 20. NetEdit example config

A screenshot of a NetEdit configuration window showing lines 4 through 7. The background is dark grey, and the text is light blue. A mouse cursor is visible at the end of line 7.

```
4 loop-protect re-enable-timer 3600
5 ntp server 10.10.10.254
6 ntp enable
7 ntp vrf mgmt
```

Figure 21. NetEdit example config (cont)

A screenshot of a NetEdit configuration window showing line 12. The background is dark grey, and the text is light blue. A mouse cursor is visible at the end of line 12.

```
12 spanning-tree
```

Figure 22. NetEdit example config (cont)

```
27 interface lag 256 multi-chassis
28     description VSX ISL Link
29     no shutdown
30     no routing
31     vlan trunk native 1 tag
32     vlan trunk allowed all
33     lacp mode active
34     loop-protect
35     qos trust dscp
36     spanning-tree bpdu-guard
37     spanning-tree tcn-guard
38     spanning-tree port-type admin-edge
39 interface 1/1/13
40     description Nimble Data Path A
41     no shutdown
42     mtu 9198
43     flow-control rx
44     no routing
45     vlan access 110
46     spanning-tree bpdu-guard
47     spanning-tree port-type admin-edge
48     spanning-tree tcn-guard
49     loop-protect
50 interface 1/1/14
51     description Nimble Data Path B
52     no shutdown
53     mtu 9000
54     flow-control rx
55     no routing
56     vlan access 110
57     spanning-tree bpdu-guard
58     spanning-tree port-type admin-edge
59     spanning-tree tcn-guard
60     loop-protect
```

Figure 23. NetEdit example config (cont)

```
60 interface 1/1/28
61     description Nimble Data Path DL360
62     no shutdown
63     mtu 9000
64     flow-control rx
65     no routing
66     vlan access 110
67     spanning-tree bpdu-guard
68     spanning-tree port-type admin-edge
69     spanning-tree tcn-guard
70     loop-protect
```

Deploy the HPE Nimble Storage array

The following procedures describe how to initialize and configure the Nimble array for use.

1. Initialize the HPE Nimble Storage array
2. Configure the Array for data access.
3. Deploy a new VMware vCenter® instance or use an existing one. – Using existing environment for this example
4. Add HPE ProLiant servers into the HPE Nimble Storage environment.
5. Create Virtual Volumes and apply to required hosts.

Initialize and configure the HPE Nimble Storage array

To initialize a Nimble array, connect a laptop into the provided console cable and power on the box. At the initial login prompt use admin/admin as the username/password.

Then type setup and hit enter to start the setup which will provide management access to the array. Use the parameters as needed for specific solution.

Figure 24. Nimble login and setup

```
Nimble Storage Console
searray1 login: admin
Password:
USAGE WARNING

This is a private system. This system is provided only for authorized use.
Unauthorized or improper use of this system may result in civil claims
and/or criminal charges. The array owner may monitor the system for all
lawful purposes, including but not limited to ensuring that access is
authorized and for other security reasons. Use of this system constitutes
consent to the array owner for monitoring of this system.

Administrators should ensure that this system is protected by a firewall
and implements all security procedures itemized in the Nimble Storage
documentation.
REMINDER: The Nimble Virtual Array:

1. Is for your non-production use only
2. Must not be distributed to third parties
3. Must not retain or store third party data of any kind. In the event third
   party data is placed on the Nimble Virtual Array, you are required to wipe
   such data prior to any subsequent demonstration or training.
Nimble OS $ setup
```

Figure 25. Nimble mgmt parameters

```
Terms on behalf of a company or other legal entity, you represent that you have
the authority to bind such entity to these Terms, in which case "you" shall
refer to such entity. If you do not agree to these Terms, you may not install
or use the Software.

1.      DEFINITIONS.

"Documentation" means the Software end user documentation furnished by Nimble
Storage to users.

"Software" means certain supplemental software such as applications or tools
made available to you by Nimble Storage under these Terms for use, solely at
your option. The Software is not Ancillary Software or Embedded Software as
referenced in Nimble Storage's General Terms and Conditions.
I acknowledge that I have (a) read and agree to both the terms and conditions of
sale and support and the end user license agreement with Nimble Storage, Inc. a
nd (b) received the third party software notices provided by Nimble Storage, Inc
. (yes/no/again): yes
Enter array name: hq-nimble-01
Enter group name: hq-nimblegroup-01
Enter management IP address: 10.1.1.10
Enter management netmask: 255.255.255.0
Enter default gateway IP address: 10.1.1.1
Enter domain name: nimblestorage.com
```

Configure the Array for data access

Now that the Nimble array has been initialized, log into the web GUI and complete the configuration of the Nimble Array.

Log into the array using the username/password and management IP address applied during initialization.

Once logged in click on **Administration** and then **Network**. The management IP setting should be shown on the Group tab already

Figure 26. Nimble mgmt configuration

Management IP
Used for the Web UI, CLI and replication. Resides on management subnet and floats across all "Mgmt only" and "Mgmt + Data" interfaces on that subnet.

IP ADDRESS *	NETWORK	NETMASK
10.10.10.83	10.10.10.0	255.255.255.0

iSCSI Host Connection Method

Manual ⓘ

Automatic ⓘ

Enable rebalancing ⓘ

Discovery IP Addresses

SUBNET LABEL	DISCOVERY IP	NETMASK
management		255.255.255.0
Subnet-1	155.1.1.254	255.255.0.0

Routes

DEFAULT GATEWAY *
10.10.10.254

Now proceed by adding the iSCSI data segments and configuring the data interfaces.

Select the **Subnet** tab and the **Interfaces** tab to apply the needed configurations.

In this example we are using a single segment for data traffic and we are applying IP addresses within that segment to both of the data ports available. This ensures HA and multipathing for that data traffic into the network.

Figure 27. Configured Nimble Segments and data interfaces

The screenshot shows the 'Edit' configuration page for a subnet. The 'SUBNETS' tab is active. The configuration includes:

- SUBNET LABEL: Subnet-1
- NETWORK: 155.1.0.0
- NETMASK: 255.255.0.0
- TRAFFIC ASSIGNMENT: iSCSI + Group
- DISCOVERY IP: 155.1.1.254
- TRAFFIC TYPE: Data only
- IP ADDRESS ZONE: Even / Odd
- MTU: Jumbo
- BYTES: 9000
- VLAN ID: (empty)

Below the configuration fields, there is a section for 'Assign interfaces to this subnet.' with a list of interfaces for 'TME-Nimble-01':

- eth1 (unchecked)
- eth2 (unchecked)
- eth3 (checked)
- eth4 (checked)

At the bottom, the 'Interface Assignment' table is shown:

ARRAY NAME	INTERFACE	LINK STATUS	DATA IP ADDRESS	TAGGED
TME-Nimble-01	eth3	🟢🟢	155.1.1.1	<input type="checkbox"/>
TME-Nimble-01	eth4	🟢🟢	155.1.1.2	<input type="checkbox"/>

Now proceed by adding NTP setting into Nimble by clicking on **Administration** and then **Date and Timezone**. Add the appropriate settings.

Figure 28. Nimble time configuration

The screenshot shows the 'Date / Timezone' configuration page. The 'Time' section has 'Use NTP Server' selected with a value of '10.10.10.254'. The 'Time Zone' section has 'REGION' set to 'America' and 'COUNTRY/STATE/CITY' set to 'Los_Angeles'.

VMware Integration

Now proceed by adding VMware integration settings into Nimble by clicking on **Administration** and then **VMware integration**. This will install a plug-in into vCenter allowing easy datastore/VVOL creation.

Figure 29.VMware integration

VMware Integration

Registering a vCenter will enable us to collect VMware configuration data and per-VM monitoring statistics. InfoSight provides a view of collected analytics that include performance and usage data.

Register a vCenter

VCENTER NAME *	TME-Lab
SUBNET	management
VCENTER HOST *	10.10.100.100
PORT *	443
DESCRIPTION	

CREDENTIALS

REGISTER THE FOLLOWING: (OPTIONAL)

- Web Client
- Thick Client
- VASA Provider (VVols)

UPDATE CREDENTIALS

Add HPE ProLiant servers into the HPE Nimble Storage environment

Add servers into the environment by clicking on **Manage** and then **Data Access**.

Click on the **plus** symbol to add an Initiator Group. This will be a group of hosts that will have common array access settings.

The below example shows a single host being added and being allowed to access the Subnet-1 networking segment. Note that the initiators IQN value is provided.

Figure 30. Adding hosts

EDIT INITIATOR GROUP

NAME * Host-95

SUBNETS Use selected subnets

AVAILABLE SUBNETS management

ASSOCIATED SUBNETS Subnet-1

ADD REMOVE

INITIATORS

NAME	IQN	IP ADDRESS
VMwareHost95	iqn.1998-01.com.vmware:5d6ec196-	*

ADD

SAVE CANCEL

Create Virtual Volumes and apply to required hosts

Now that hosts have been added to the Nimble array we can create storage volumes to export to the hosts.

Click on **Manage** and then **Data Storage**.

Click on the **plus** symbol to add Volume. When creating the volume, there are various options for Name, Location, Performance Policy, size, data protection levels, and which hosts can access the volume.

Figure 31. Click on Plus symbol to add volume

DATA STORAGE DATA PROTECTION DATA ACCESS PERFORMANCE POLICIES

GROUP ACTIONS

28.7 GiB of 3.9 TiB (TOTAL USED 0.7%)

2 TiB | 71.4 x SAVINGS

1 IOPS PERFORMANCE 0 MB/s

2 VOLUMES ARRAYS TME-Nimble-01

Get insights from HPE InfoSight™

VOLUMES FOLDERS

NAME *	APPLICATION	DATA	SIZE	IOPS	TOTAL MB/s	LATENCY (MS)
Nimble-1-95 default	Online Other	14.5 GiB	1 TiB	0	0 r w	0 0.5
Nimble-Blade2 default	Online Other	14.2 GiB	1 TiB	0	0 r w	0 0.6

The below screen shot shows an example configuration which leverages mostly default values.

Figure 32. Example volume creation

The screenshot shows a 'CREATE VOLUME' form with the following fields and values:

- NAME *: [Empty text input]
- LOCATION *: default [Dropdown menu]
- PERFORMANCE POLICY *: default [Dropdown menu]
- SIZE *: 50 [Text input] GIB [Dropdown menu]
- DATA PROTECTION *: Not Protected [Dropdown menu]
- ACCESS *: Select an Initiator Group [Dropdown menu]
- CHAP ACCOUNT *: Unrestricted Access, Host-95, Synergy-Blade2 [List of options]

At the bottom of the form, there is a 'More Options' link, a blue 'CREATE' button, and a 'CANCEL' button.

Configure VC Modules/Server Profiles in Synergy Frame

Before configuring VMware, the Server Profiles and HPE Virtual Connect SE 40Gb F8 Modules within the Synergy Frame still need to be created using the OneView Composer.

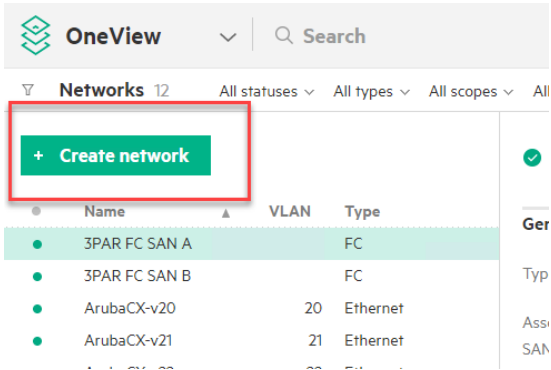
The descriptions below describe adding these connections to an already existing Synergy Frame environment. Synergy deployment and setup is beyond the scope of this document.

Create an iSCSI Nimble Network

Log into the Synergy Composer and click on **OneView** and then **Networks**.

Click on **Create network**.

Figure 33. Create network



Configure the new networks Name, Type, VLAN ID, Purpose, and preferred bandwidths.

Note: In this example we are using a single network segment, however, admins have the option to add this segment to a network set which would contain multiple segments.

Figure 34. New network configuration

The screenshot shows the 'Edit Nimble-110' configuration page. The page has a header 'Edit Nimble-110'. Below the header, there are several configuration fields:

- Name:** A text input field containing 'Nimble-110'. To its right is a tooltip that says 'A unique, descriptive name for the network'.
- Type:** A dropdown menu set to 'Ethernet'.
- VLAN:** A text input field containing '110'.
- Associate with subnet ID:** A dropdown menu set to 'none'.
- Purpose:** A dropdown menu set to 'ISCSI'.
- Preferred bandwidth:** A text input field containing '2.5' and a unit dropdown set to 'Gb/s'.
- Maximum bandwidth:** A text input field containing '20' and a unit dropdown set to 'Gb/s'.

Configure Uplinks out of Frame (Interconnect Group)

Within the Synergy Frame we now need to ensure that the Uplinks out of the frame as well as the downlinks to the server in Bay 2 are configured properly. The traffic within this segment will be tagged while passing through the Synergy frame, and therefore we used Trunk on the Aruba CX Switch configuration.

To configure the uplinks, click on **OneView** and then **Logical Interconnect Groups**.

Choose the appropriate **Logical Interconnect Group (LIG)**, click on **Actions**, and then **Edit**.

In this example we are using port Q4 from both Virtual Connect SE 40Gb F8 Modules to connect via LACP to the Aruba 8325 switches.

Click on **Add Uplink Set** to add the Q4 Uplink configuration. Add the Name, Type, LACP Timer setting and then click **Add Networks**. Choose the new Nimble segment and click **OK**.

Finish by clicking **Add Uplink Ports** and choose port Q4 with appropriate settings. Click **OK**.

The options shown in image below will configure an LACP aggregation group and it will trunk the VLAN 110 used for iSCSI.

Figure 35. LIG configuration

Edit Nimble ?

Name

Type

Connection mode

LACP timer

Networks

Name	Type	VLAN ID	Native
Nimble-110	Ethernet	110	<input type="checkbox"/> <input type="checkbox"/>

Add networks
Remove networks
Remove all

Uplink Ports

Interconnect Module	Enclosure	Bay	Port	Capability	Speed	Auto-negotiation
Virtual Connect SE 40Gb F8 Module for Synergy	1	3	Q4	Ethernet + FCoE	<input type="text" value="Auto"/>	Enabled <input type="checkbox"/>
Virtual Connect SE 40Gb F8 Module for Synergy	1	6	Q4	Ethernet + FCoE	<input type="text" value="Auto"/>	Enabled <input type="checkbox"/>

Add uplink ports
Remove uplink ports
Remove all

OK
Cancel

Now that the LIG for the Uplinks out of the chassis is created we need to push that config to the actual Interconnect modules themselves. To do that, click on **OneView** and then **Logical Interconnects**.

Because the LIG was changed, see a Yellow warning message that stats something like the following.

Figure 36. Interconnect Group inconsistency warning message

▲ The logical interconnect is inconsistent with the logical interconnect group Synergy_MLAG. Active 11/22/19 10:33:24 am

Resolution The logical interconnect can be made consistent with its logical interconnect group by updating it from group. If consistency is not desired, this alert can be cleared.

[Update from group](#)

Click on Update from group to update the Interconnect group and resolve the warning message.

Configure Downlinks to Server Blade (Server Profile)

Now that the uplinks are configured finish the Synergy configuration by adding the appropriate downlink setting which will be applied using a server profile.

Configure the server profiles by using a server profile template and applying that to a server blade, or by configuring the server profile directly.

To configure the server profile, click on **OneView** and then **Server Profiles**.

Choose the server profile for the proper server bay and click on **Actions**, and then **Edit**.





Click on **Add Connection** in the Connections section.

Note that the example configuration uses a single Mezzanine card in the Blade server. That Mezzanine card provides two 20G NICs: one of which connects to Interconnect Module A and the other connects to Interconnect Module B.

However, the Synergy configuration allows for the single NIC to be split up into separate Physical Functions as if there are up to 4 actual NICs. The example below shows Production network traffic which is already going over the virtual NIC A on both Interconnect Modules. For this configuration we will use the virtual NIC B function for this iSCSI traffic.

Figure 37. Add connection to server profile

Connections

ID	Name	Network	Port	Boot
1		Production (network set)	Mezzanine 3:2-a	managed manually  
	Type		Ethernet	
	MAC address		3A:B6:6C:C0:00:16 (v)	
	Requested virtual functions		None	
	Requested bandwidth		2.5 Gb/s	
2		Production (network set)	Mezzanine 3:1-a	managed manually  
	Type		Ethernet	
	MAC address		3A:B6:6C:C0:00:17 (v)	
	Requested virtual functions		None	
	Requested bandwidth		2.5 Gb/s	

Add connection

Create two new connections. One will be extending the iSCSI segment into Interconnect Module 1, port b (3:1-b), and the other would be for Interconnect Module 2 (3:2-b). The configuration should look like the following:

Figure 38. New iSCSI downlink connection

Edit Connection

General

Name

Function type

Network ✕ 🔍

Port ✕ 🔍

Requested bandwidth (Gb/s)

Boot

Figure 39. New completed Server Profile connections settings

Connections

ID	Name	Network	Port	Boot
1		<u>Production</u> (network set)	Mezzanine 3:2-a	managed manually 🔗 ✕
	Type	Ethernet		
	MAC address	3A:B6:6C:C0:00:14 (v)		
	Requested virtual functions	None		
	Requested bandwidth	2.5 Gb/s		
2		<u>Production</u> (network set)	Mezzanine 3:1-a	managed manually 🔗 ✕
	Type	Ethernet		
	MAC address	3A:B6:6C:C0:00:15 (v)		
	Requested virtual functions	None		
	Requested bandwidth	2.5 Gb/s		
5	Nimble-A	<u>Nimble-110</u> VLAN110	Mezzanine 3:1-b	managed manually 🔗 ✕
	Type	iSCSI		
	MAC address	3A:B6:6C:C0:00:1E (v)		
	Requested bandwidth	2.5 Gb/s		
6	Nimble-B	<u>Nimble-110</u> VLAN110	Mezzanine 3:2-b	managed manually 🔗 ✕
	Type	iSCSI		
	MAC address	3A:B6:6C:C0:00:1F (v)		
	Requested bandwidth	2.5 Gb/s		

Add connection

Configure VMware and add Nimble datastore

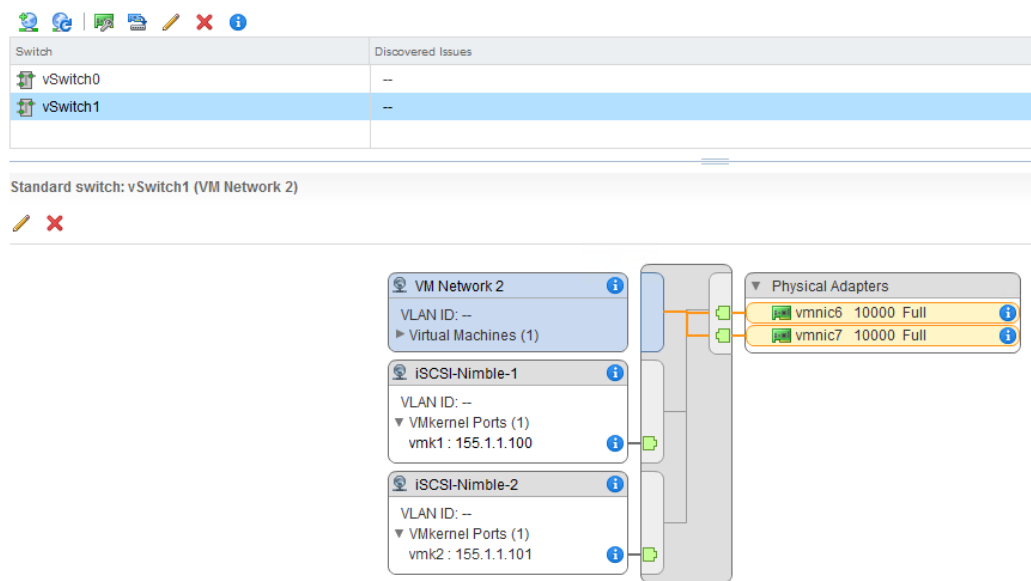
In this example we are using a vCenter 6.7 deployment that has already been deployed.

The Nimble Array has 2 hosts added as Initiators. One host is a DL360 Gen9, while the other is a BL380 Gen9 in a Synergy Frame.

The deployment shown here uses the iSCSI Software adaptor (preferred means for connecting to HPE Nimble Storage arrays). A vSwitch was created that has 2 Physical NICs and 2 VM kernel interfaces. One Kernel interface is bound to one of the NICs, while the other Kernel is bound to the other NIC.

vSwitch creation

Figure 40. VMware vSwitch creation for Nimble data



VMware Storage Adapter configuration

Figure 4.1. VMware Storage adaptors configuration

The screenshot shows the VMware Storage Adapters configuration page. It features a table of storage adapters and a detailed view of the selected iSCSI adapter.

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Smart Array P440ar						
vmhba0	SAS	Unknown	5001438034ae3790	1	2	2
iSCSI Software Adapter						
vmhba64	iSCSI	Online	iqn.1998-01.com.vmware:5d6ec196-da24-0801-8396-ecb1...	2	1	2

Port Group	VMkernel Ad...	Port Group Policy	Path Status	Physical Network Adapter
iSCSI-Nimble-1 (vS...	vmk1	Compliant	Active	vmnic6 (10 Gbit/s, Full)
iSCSI-Nimble-2 (vS...	vmk2	Compliant	Active	vmnic7 (10 Gbit/s, Full)

Add new datastore

Once the iSCSI config has been added, proceed to create a new datastore from the Nimble Volume. The image below shows a datastore that has already been added by standard vSphere methods.

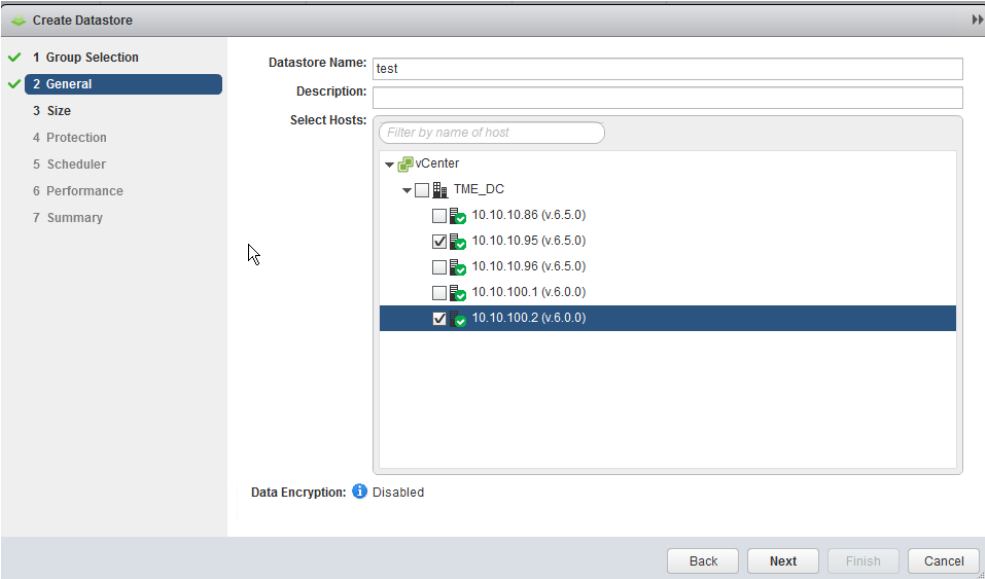
The screenshot shows the configuration page for a datastore named 'Nimble-95-a'. The left sidebar shows navigation options like Settings, General, and More. The main content area displays properties, capacity, and datastore capabilities.

Properties	
Name	Nimble-95-a
File system	
Type	VMFS 5.81
Maximum file size	62.94 TB
Maximum virtual disk size	62.00 TB
Block size	1 MB
Drive type	Flash

Capacity	
Capacity	
Total Capacity	1,023.75 GB
Provisioned Space	925.07 GB
Free Space	1,006.72 GB

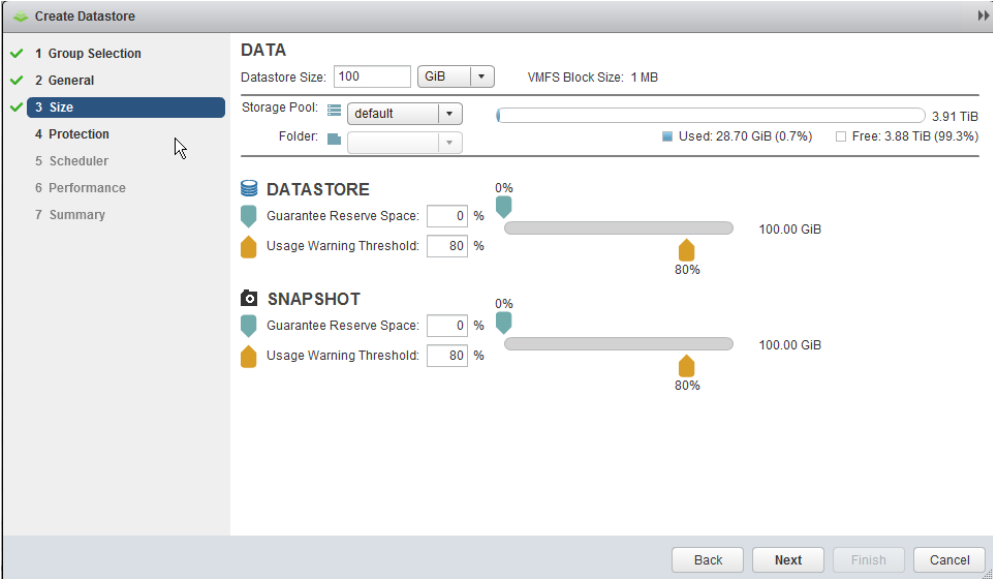
Datastore Capabilities	
Thin Provisioning	Supported
Storage I/O Control	Disabled
Hardware Acceleration	Supported on all hosts

Figure 4.3. adding servers and name to new datastore



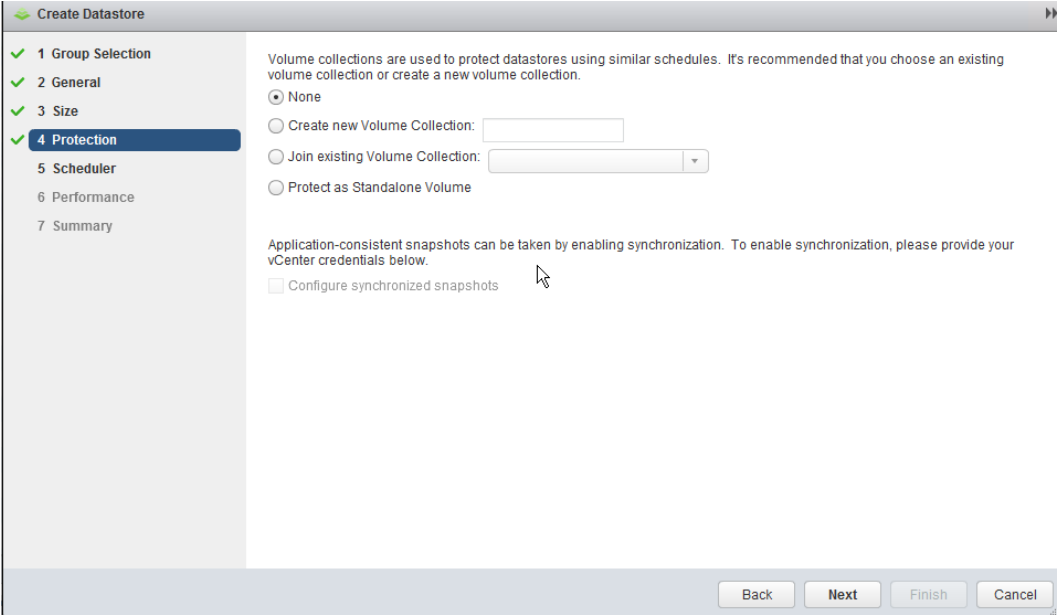
Configure size quotas with usage warning levels.

Figure 4.4. Adding quotas



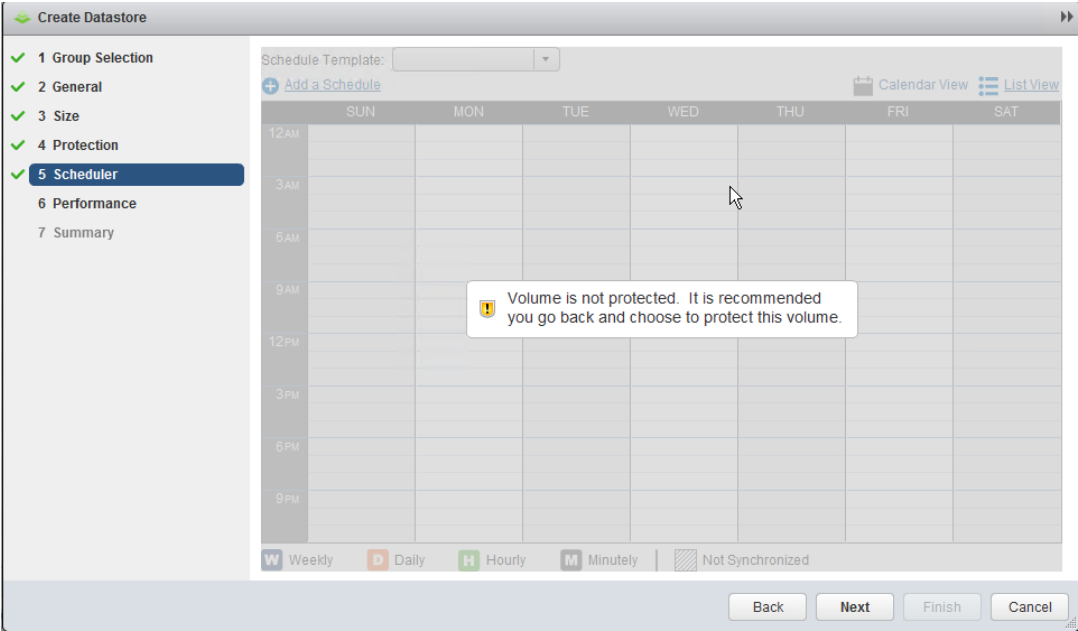
Choose Protection levels needed for volume.

Figure 45. Adding protections



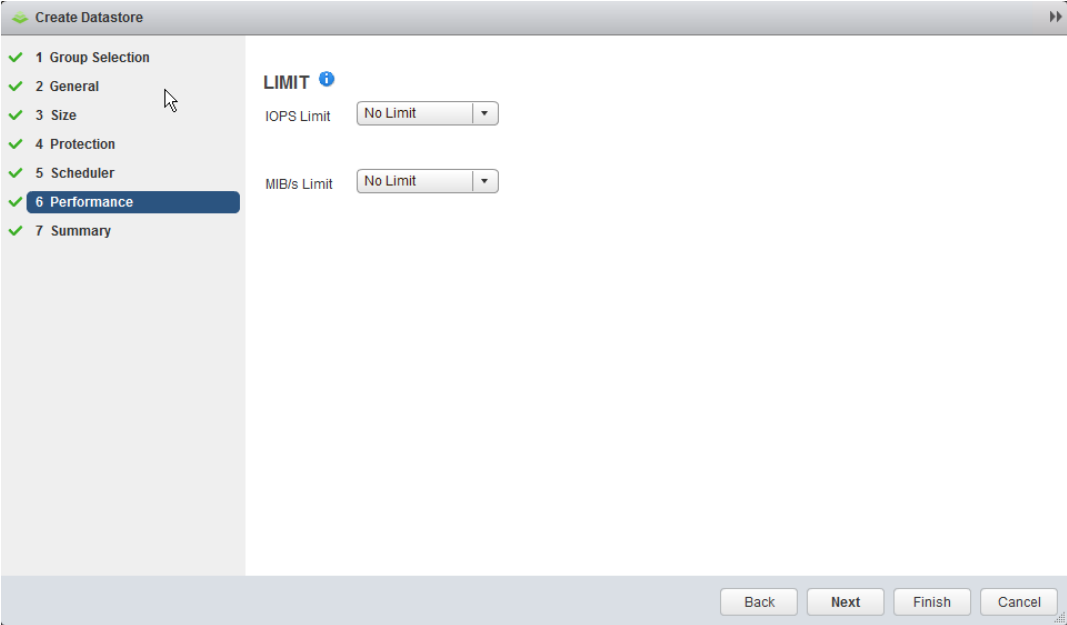
Add a schedule if necessary.

Figure 46. Adding schedule



Add performance IOPs/MBs limits, if needed.

Figure 4.7. Adding performance limits



When completed review the config and click finish.

Figure 4.8. Completed datastore

