



CYBERARK UNIVERSITY

Vault Availability
Cluster Vault

CyberArk Training

OBJECTIVES

By the end of this lesson, you will be able to:

- Describe the different solutions for Vault availability
- Describe the strengths and limitations of each model
- Deploy High Availability Cluster

VAULT AVAILABILITY OVERVIEW

VAULT AVAILABILITY SOLUTIONS

COLD

PrivateArk Replicator

- Secure replication of encrypted data to a remote Windows server for tape backup to an off-site facility

WARM

Disaster Recovery (DR)

- One way replication of vault data to a standby Vault server

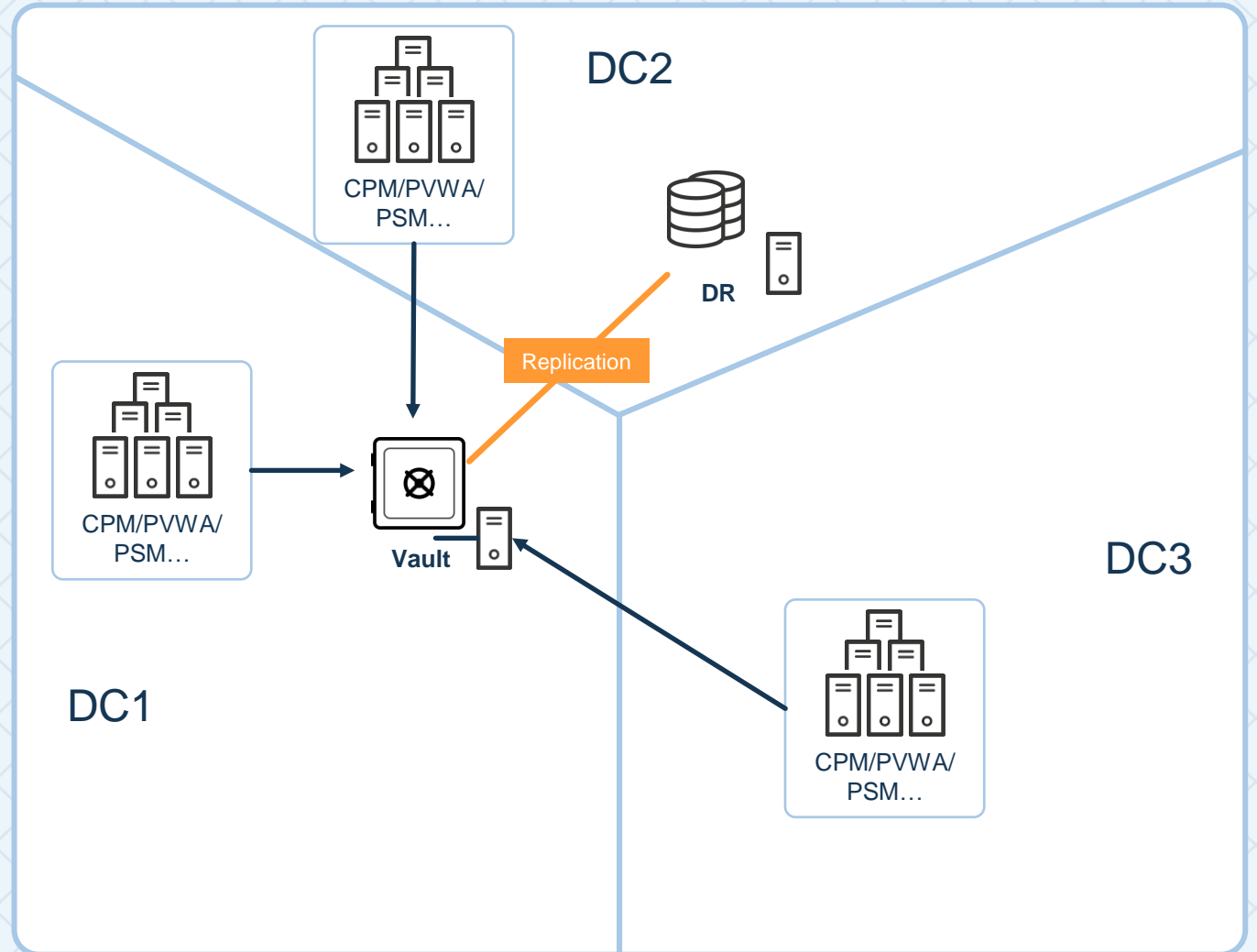
HOT

High Availability (HA)

- Cluster Vault – Two Vault servers using Clustering Services
- Distributed Vaults – Multiple Vault servers providing services at the same time

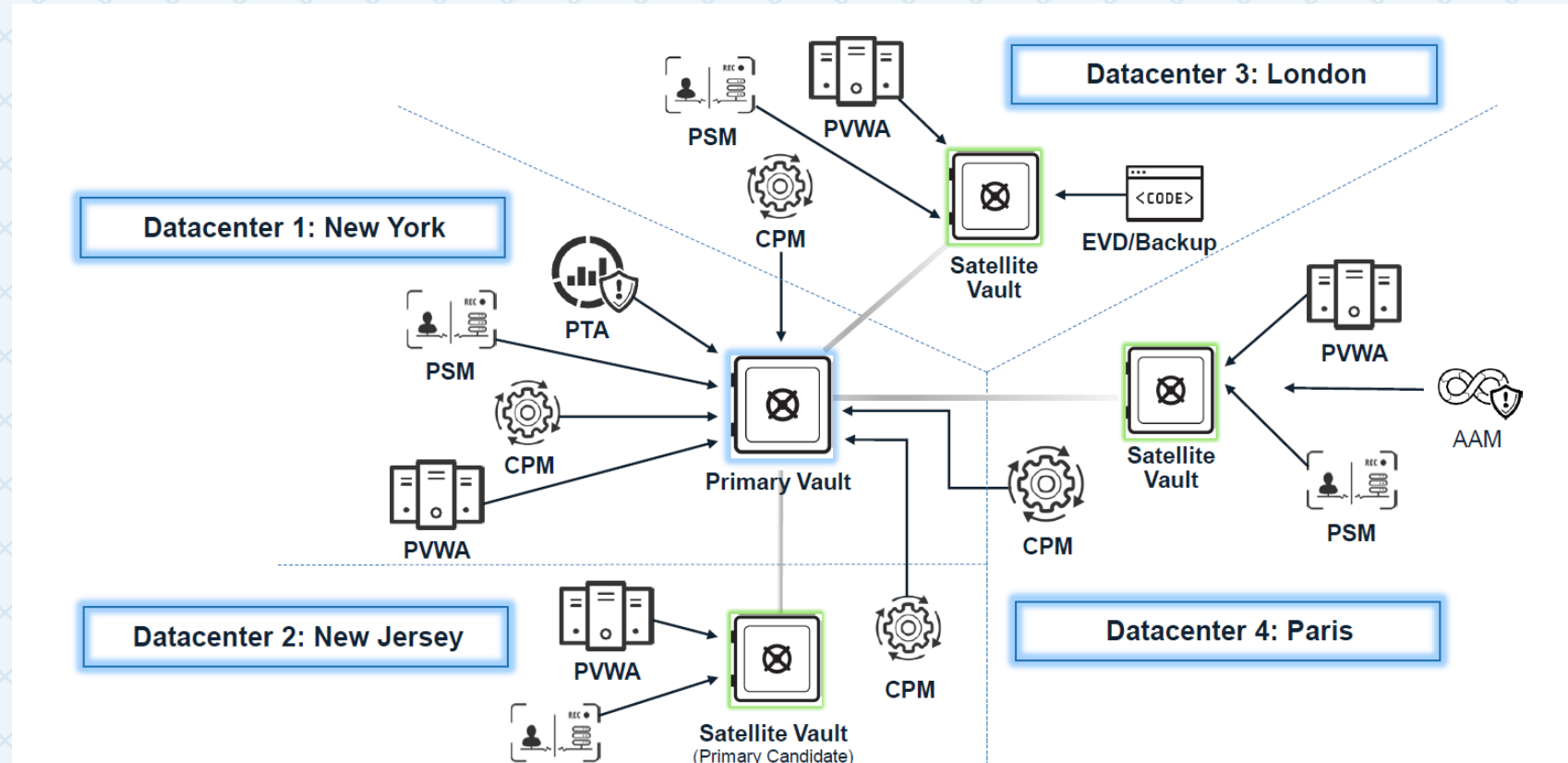
DISASTER RECOVERY

- The Disaster Recovery (DR) Vault is a replication/failover solution designed to create a stand-by copy of a Production Vault on a remote and dedicated machine
- The DR-Vault can be activated in the case of a Disaster Recovery situation either automatically **or** manually



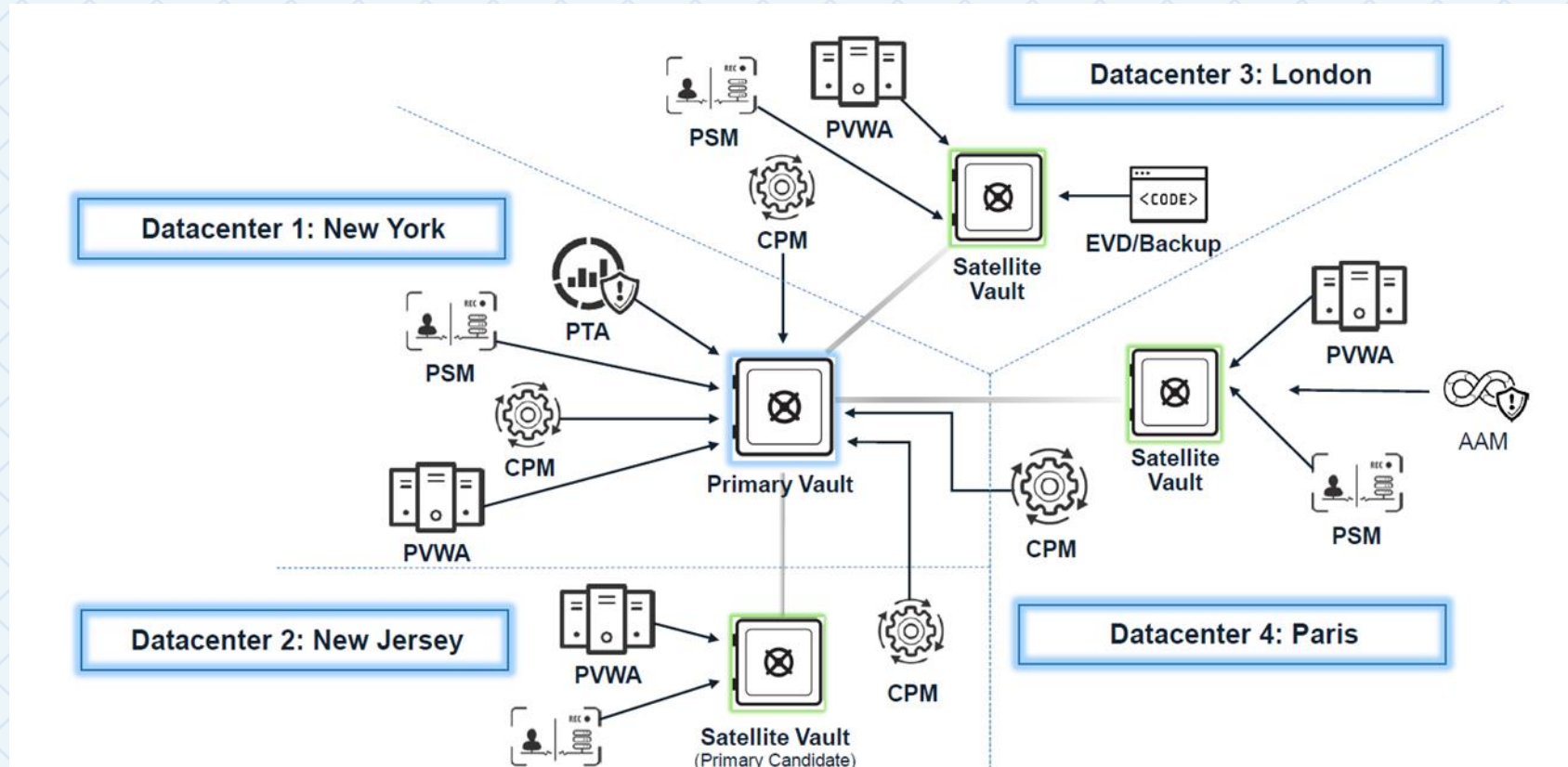
DISTRIBUTED VAULT LIMITATIONS

- You can deploy up to six Vault Servers, one Primary Vault and five Satellite Vaults
- Distributed Vaults are not supported on Cloud-based deployments
- After you migrate to Distributed Vaults architecture, you cannot migrate back to a Primary-DR architecture
- If you did not install RabbitMQ during installation or upgrade, you must upgrade to a newer version of the Vault or perform a clean installation of the Vault
- All the Vaults must be signed using the same CA Authority



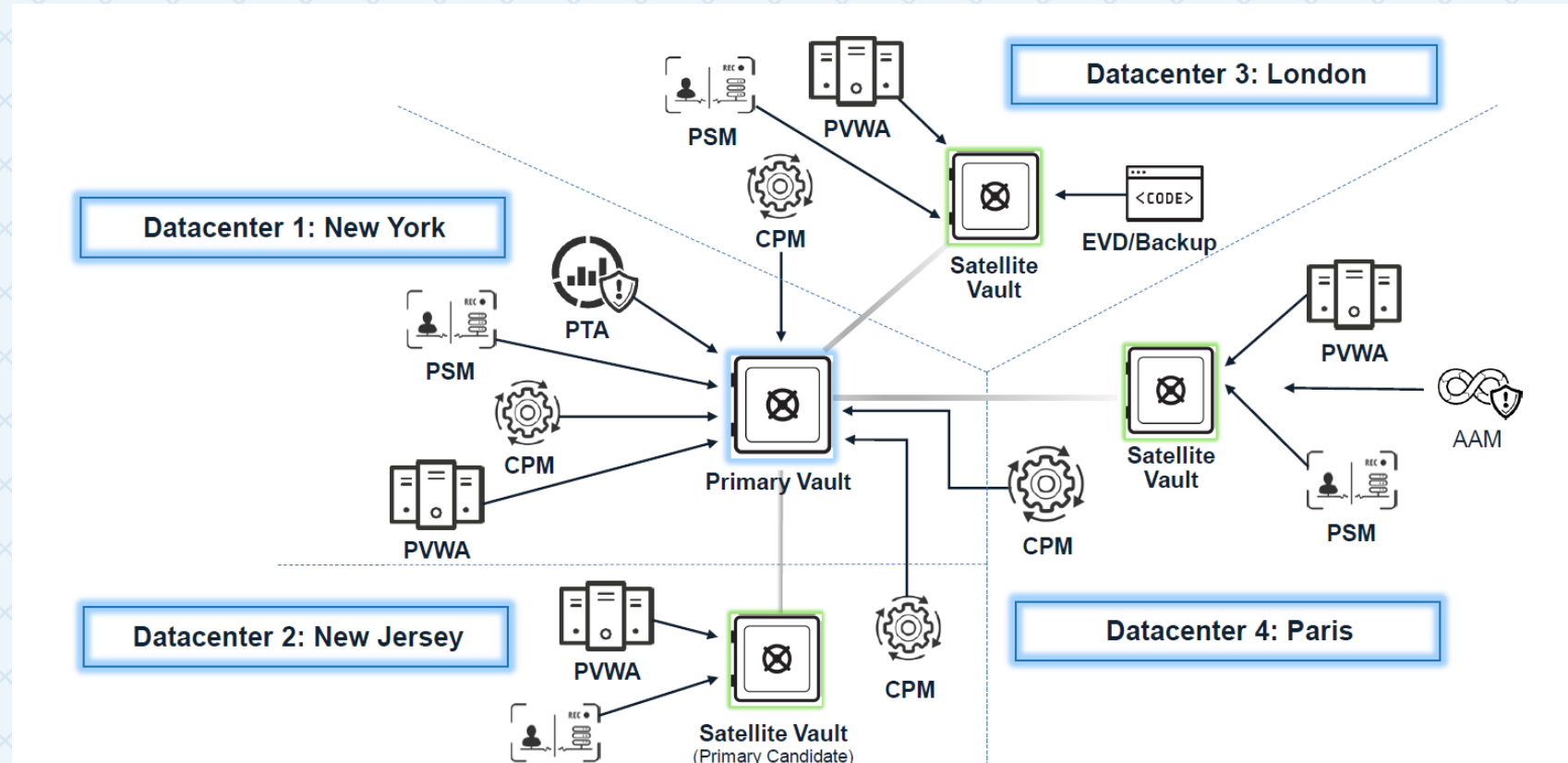
DISTRIBUTED VAULTS

- The Distributed Vaults (DV) solution spreads the load from a single primary Vault (Master) to multiple Satellite Vaults
- The Satellite Vaults are spread throughout the deployment to provide **read** requests from clients throughout the organization
- If a Satellite Vault is unavailable, clients that have been working with this Satellite Vault will reconnect to another Vault, Satellite or Master



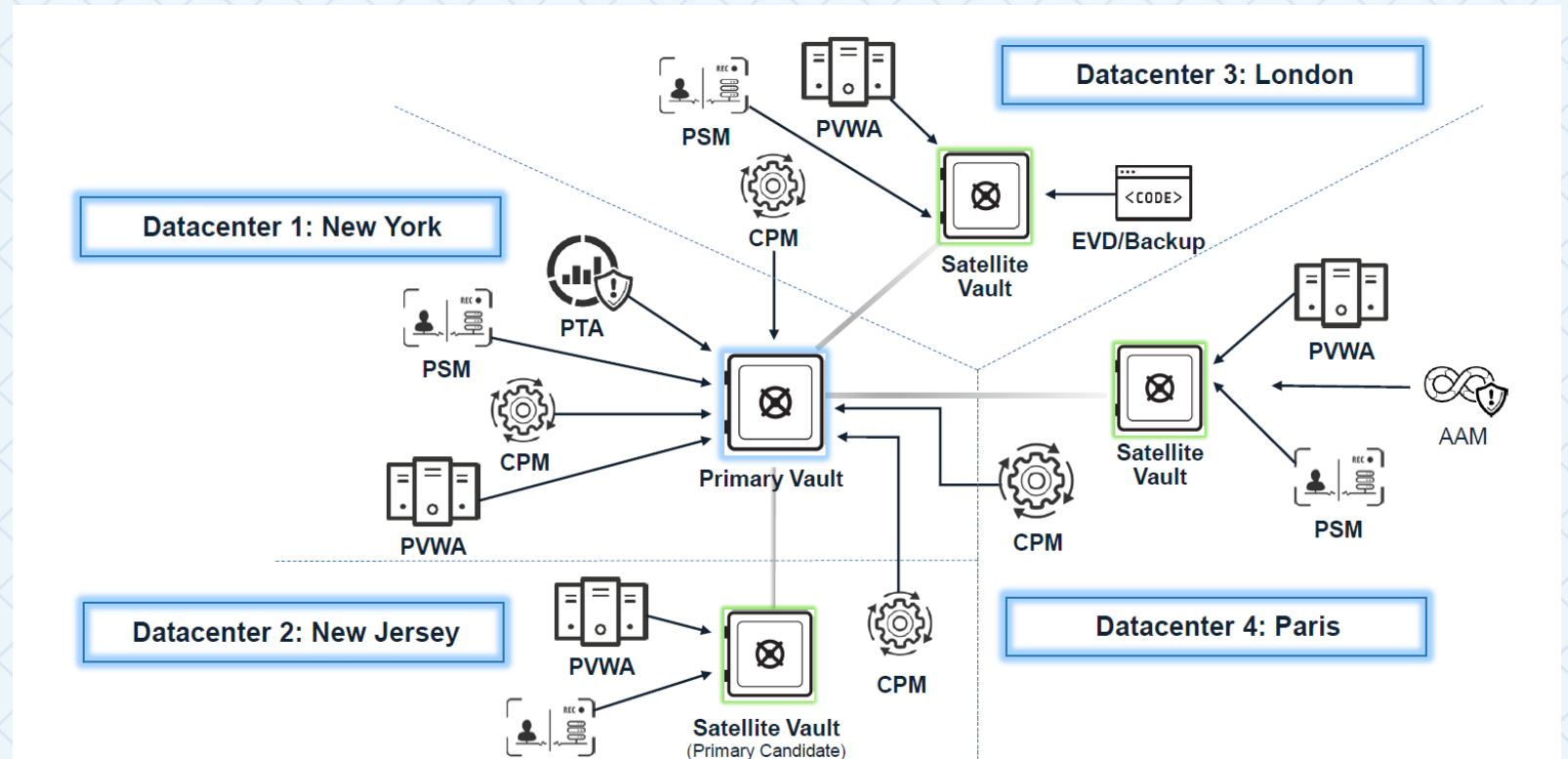
DISTRIBUTED VAULTS ACTIVE-ACTIVE SERVICES

- The PAM solution supports active/active architectures with multiple Enterprise Password Vaults
- Password retrieval and Session Management, will be available in the event of an outage, eliminating data loss



DISTRIBUTED VAULTS ACTIVE-ACTIVE SERVICES

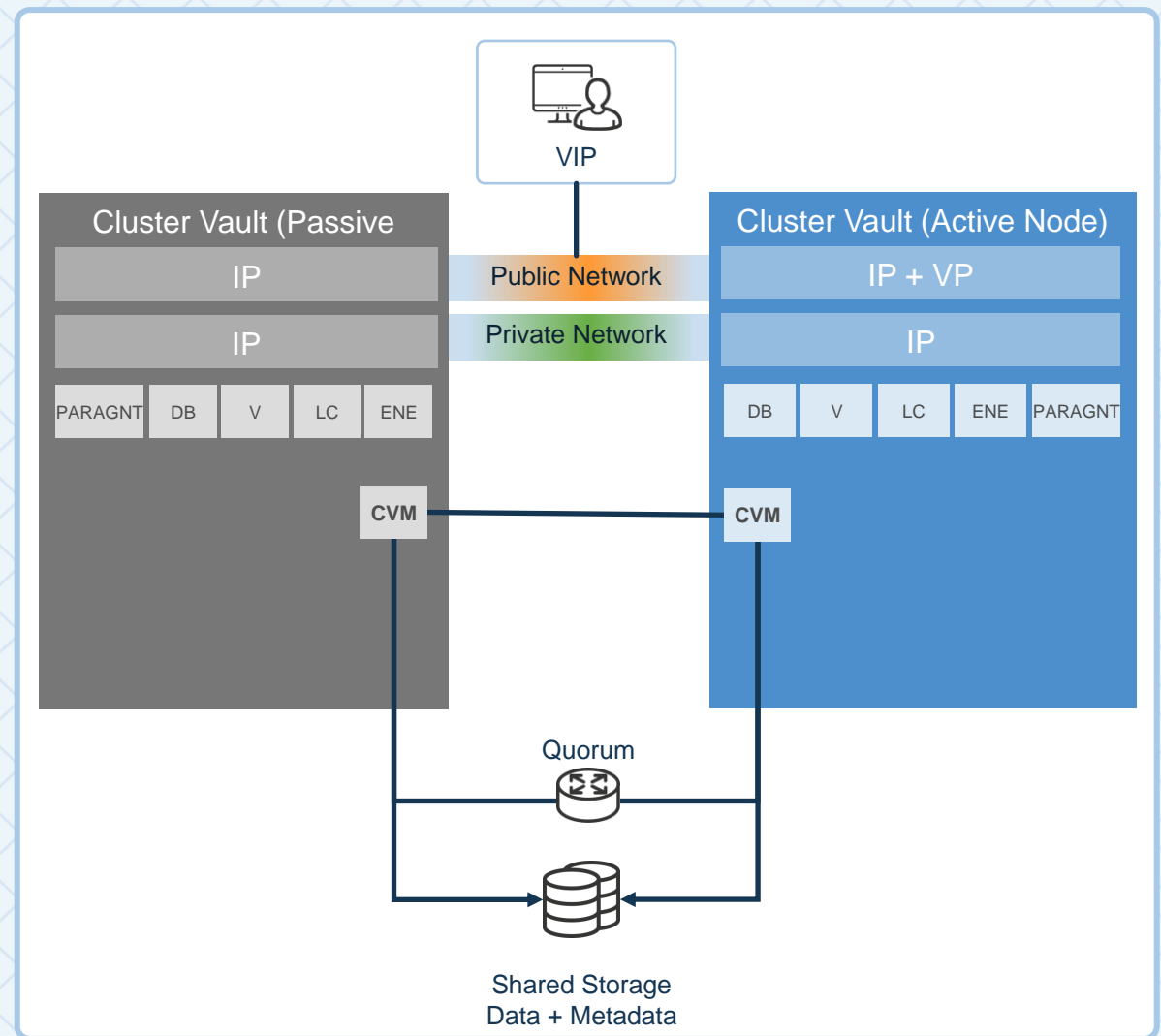
- Once connectivity is resumed, all audits and session related information will be synchronized back to the Primary Vault
- For details on implementation contact your Account Representative



CLUSTER VAULT ARCHITECTURE

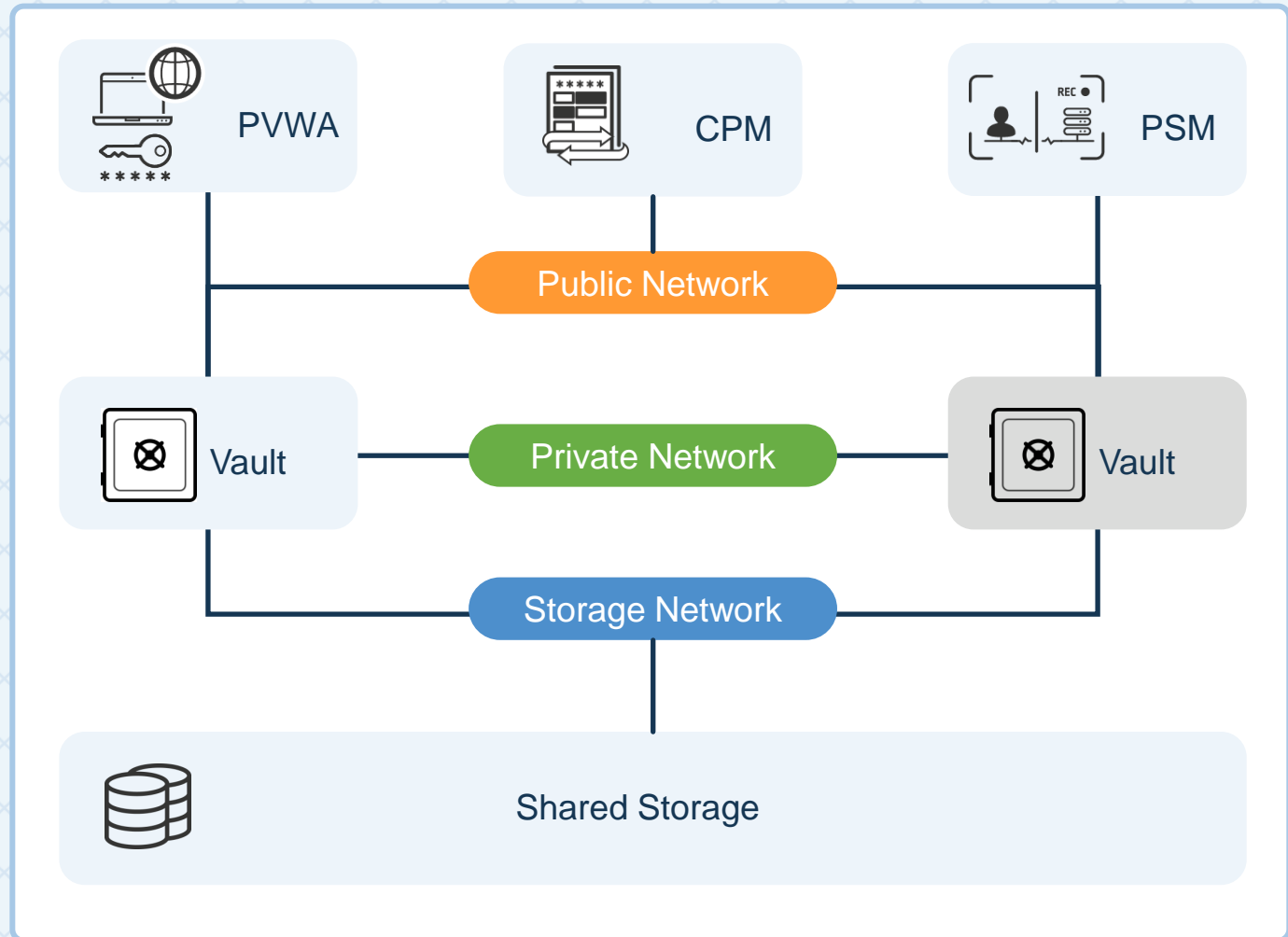
VAULT CLUSTER

- The Vault is installed as a high-availability cluster of servers which provide access to the accounts in the Vault. In this implementation, there is always one Server that is on standby in case the other Server in the cluster fails
- The component layer views the Vault Cluster as a single system allowing high availability of the Vault services without service disruption



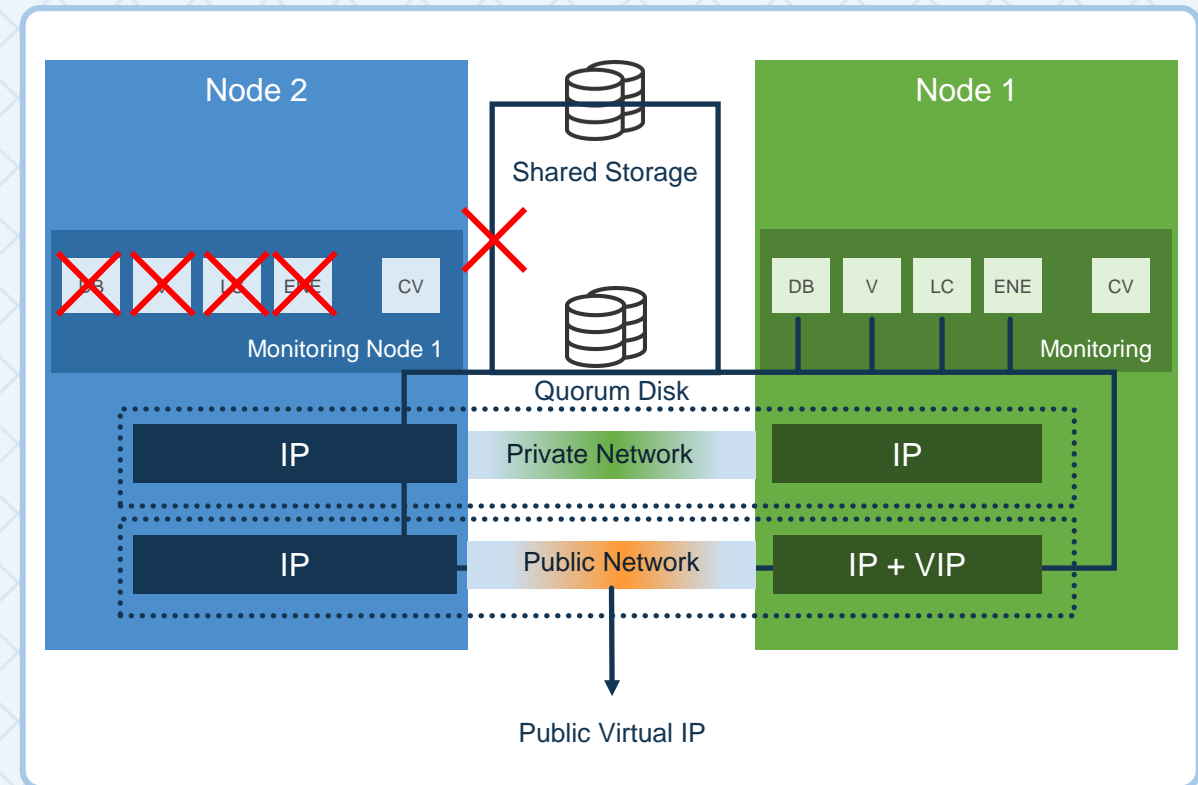
HIGH AVAILABILITY ARCHITECTURE

- Two identical vault servers
- Dedicated SAN and Cluster Shared Storage
- A single Shared Public IP address, i.e., Virtual IP
- The Cluster Vault Manager service



CYBERARK CLUSTER VAULT MANAGER (CVM)

- New service monitoring the CyberArk Digital Cluster Vault resources and connections to other CyberArk Digital Cluster Vault components
- **Active Node:** CVM will monitor the status of local resources:
 - PrivateArk Server
 - Logic Container
 - Database
 - ENE (optional)
 - PARAgent (optional)
 - The active CVM will also monitor the status of the remote passive CVM.
- **Passive Node:** CVM will monitor (via private network) the status of CVM in the active node



VIRTUAL IP

- The Cluster Vault must have only one IP exposed for clients – Virtual IP
- The Cluster Vault will allocate the VIP on the active node during start up. The CVM will monitor the VIP to ensure there are no duplicates (v9.8)
- During failover/switchover, the CVM will switch the VIP to the other node
- In order to prevent possible problems, each node should have only one single static IP.

10.10.10.10

Node A

10.10.1.1

Node B

10.10.1.2

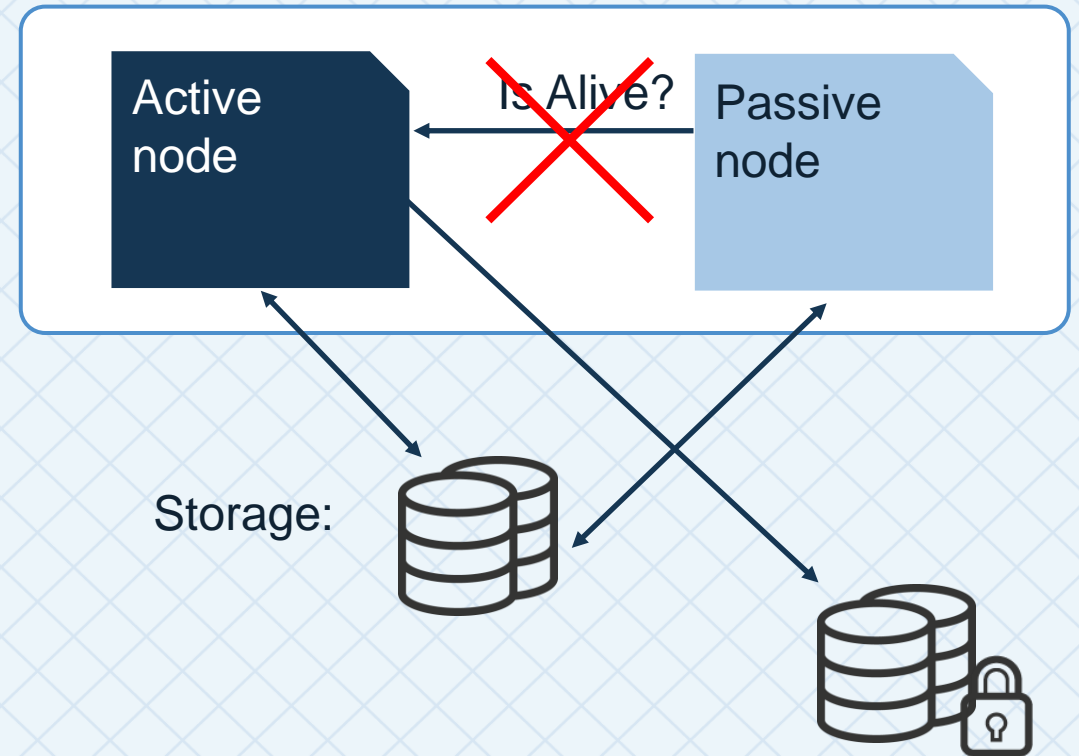
SHARED STORAGE

- The metadata (database) and data (external files) will be stored on a shared storage disk
- Both nodes are connected to the shared storage but only the active node is in “online status” and can read/write from/to the disk



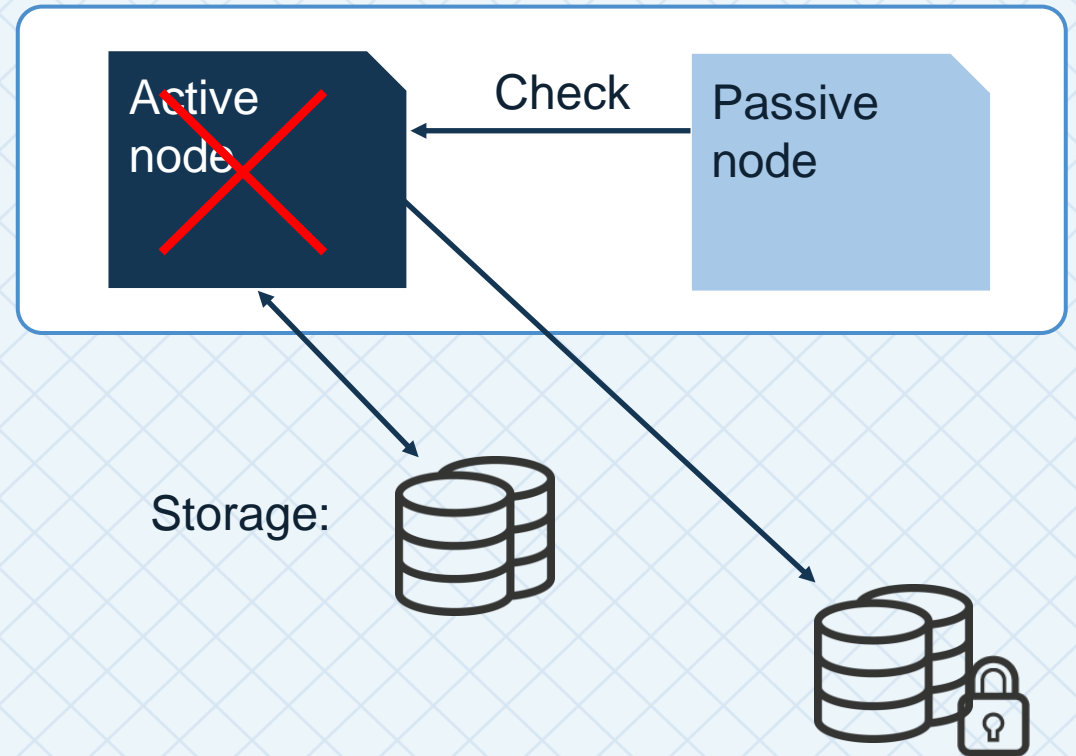
QUORUM DISK

- In order to prevent corruption and communication errors CyberArk employs the Quorum mechanism
- The Quorum uses a separate disk on the shared storage
- Quorum disk will always stay offline during normal Cluster Vault operation (except during installation) but remain **reserved** for the active node (v9.8)



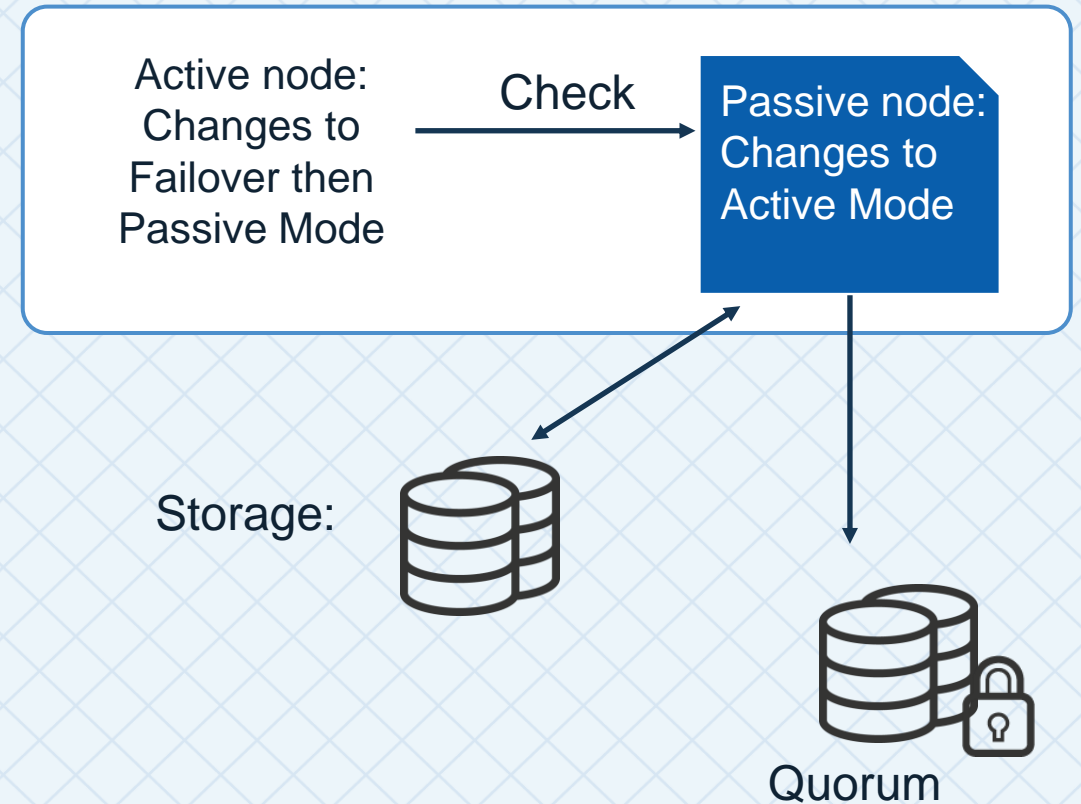
DETECTING A FAILURE

- Failover is triggered by failure of:
 - Vault services
 - Storage availability
 - Virtual IP availability
 - Loss of Quorum ownership
- The Cluster Vault service identifies a failure in one of the resources
 - The Cluster Vault service will attempt to restart a failed service once before going into failover mode



FAILOVER PROCESS

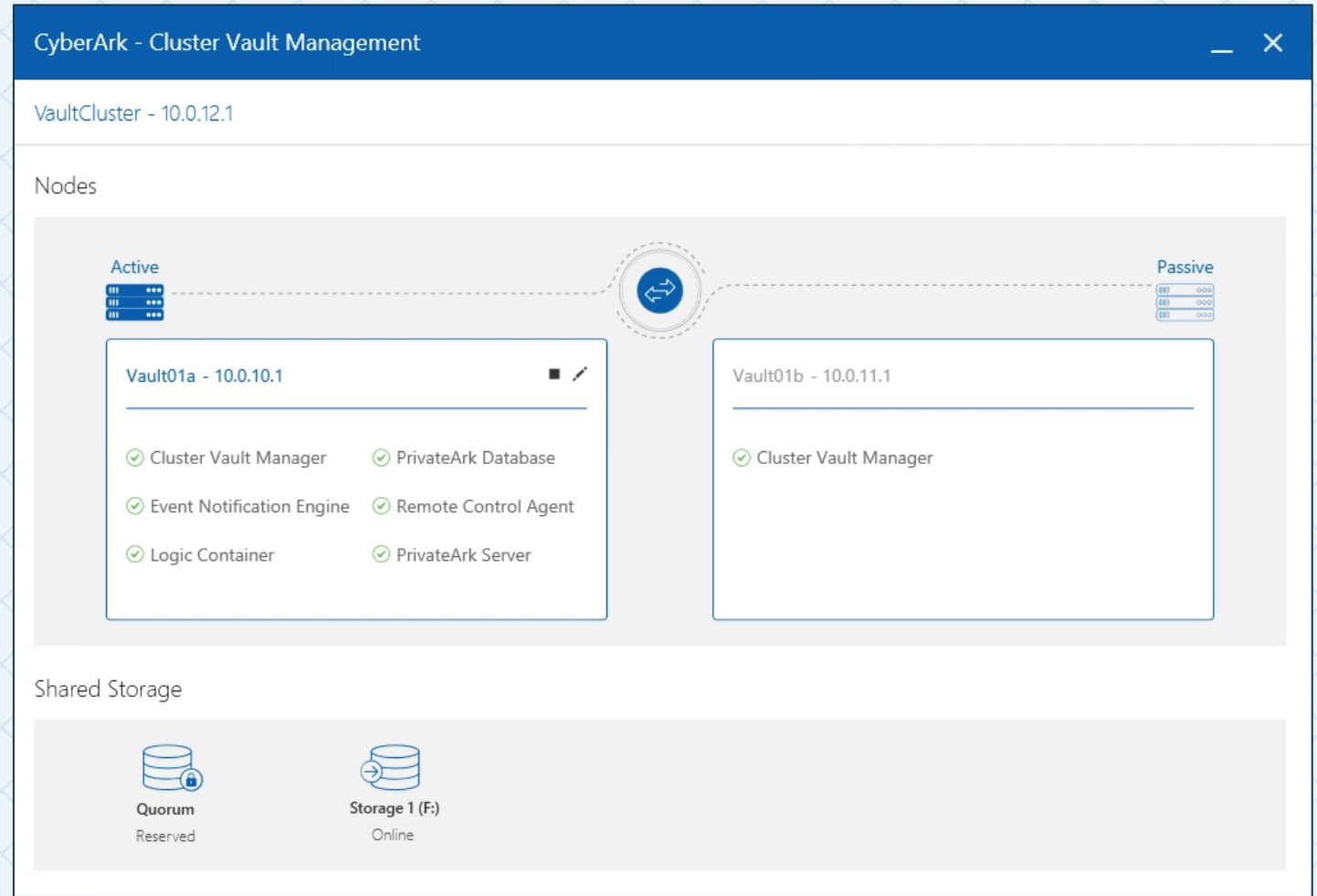
- The Cluster Vault service on the Active node changes its status to “Failover” mode and shuts down all resources
- The Cluster Vault service on the Passive node will then reserve the shared resources, such as the VIP, Shared Storage and Quorum Disk
- Once the Shared Storage is online, the Passive Node has now been promoted to the Active Node and can start the services and provide Vault services
- The Cluster Vault service on the former active node will switch its role to Passive and will start monitoring the new active node



CLUSTER VAULT MANAGEMENT

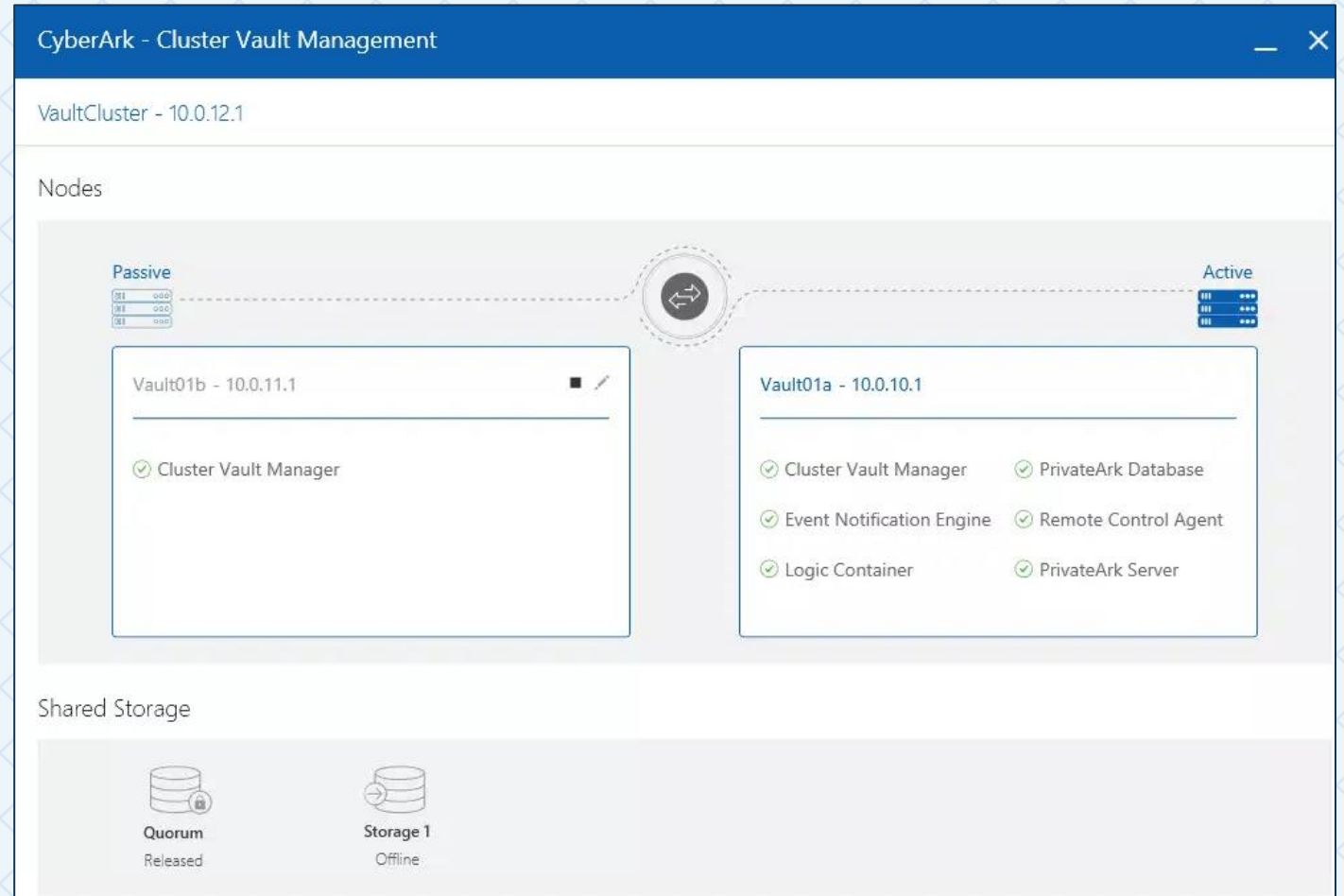
CLUSTER VAULT MANAGEMENT UTILITY – ACTIVE NODE

- The Cluster Vault is managed and controlled by the Cluster Vault Management utility
- Before restarting a Vault machine that is part of a cluster, it is highly recommended to stop the node from the Management Utility in order to make sure all resources shut down properly
- The graphic to the right illustrates how a CVM utility should look on the Active Node on the cluster



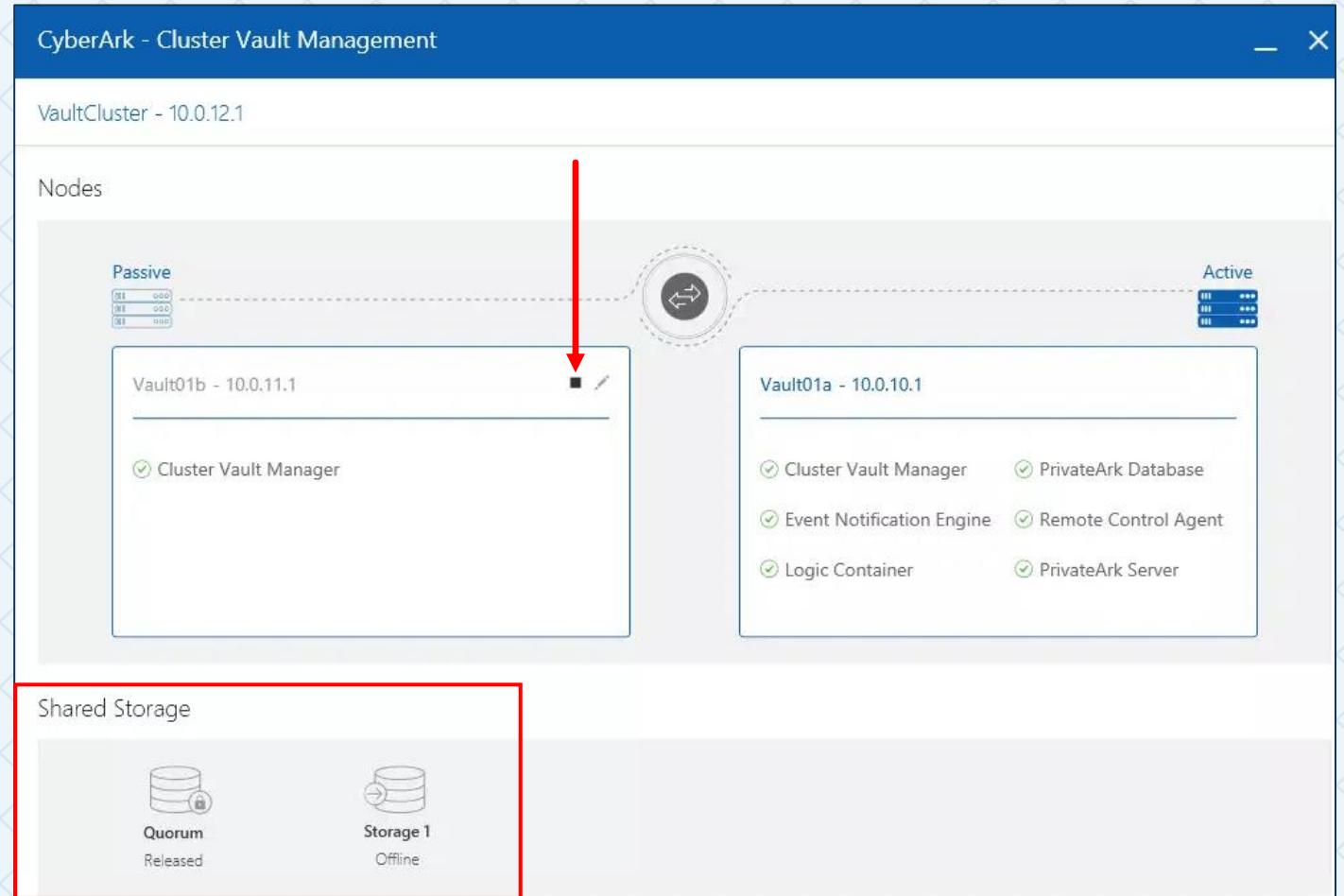
CLUSTER VAULT MANAGEMENT UTILITY – STANDBY NODE

- This is the CVM utility running on the standby node
- Note that the local node is always shown on the left, regardless of whether it is active or passive
- Shared Storage status is reported at the bottom



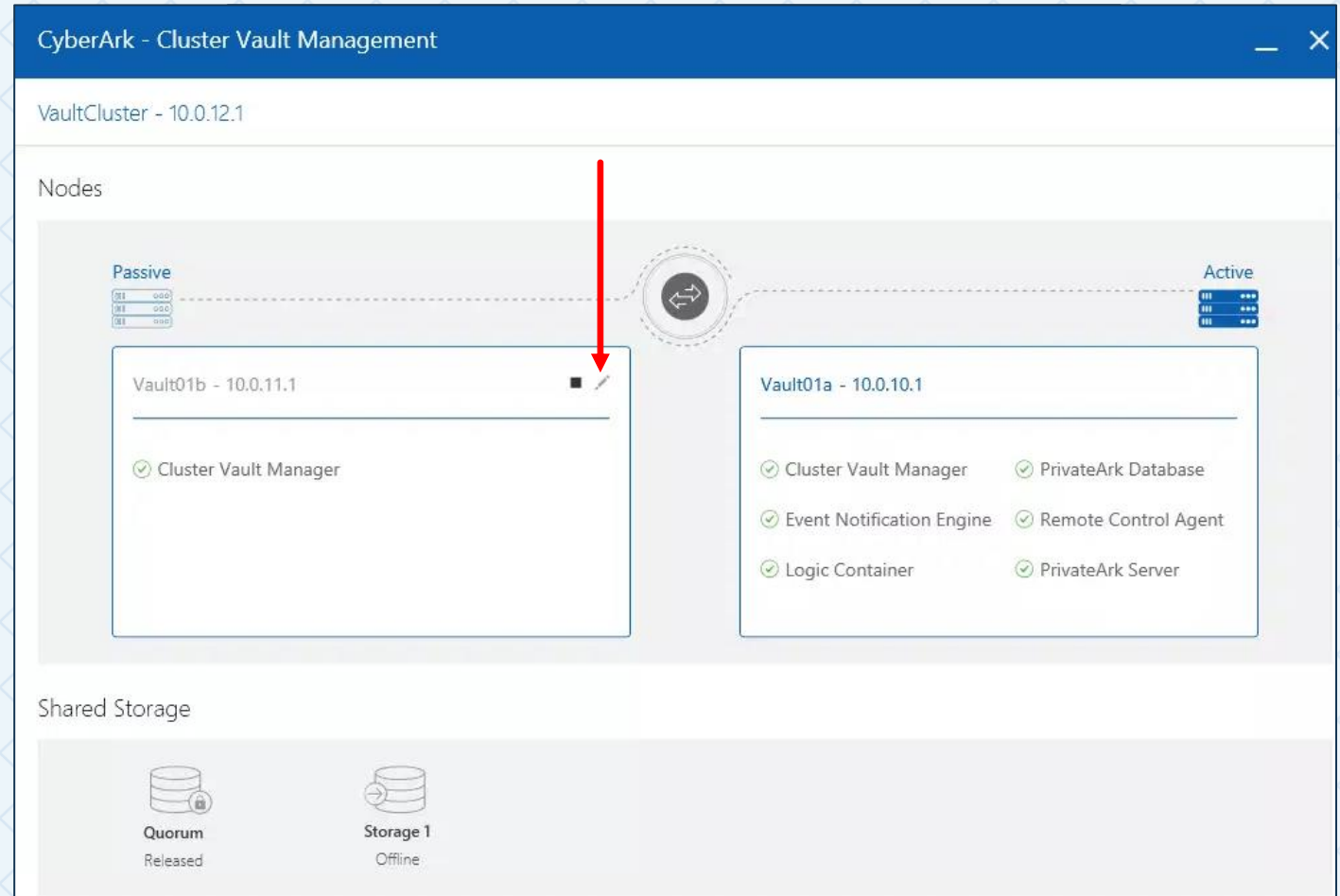
CLUSTER VAULT MANAGEMENT UTILITY – STANDBY NODE

- Selecting the black box will shut down the CVM service



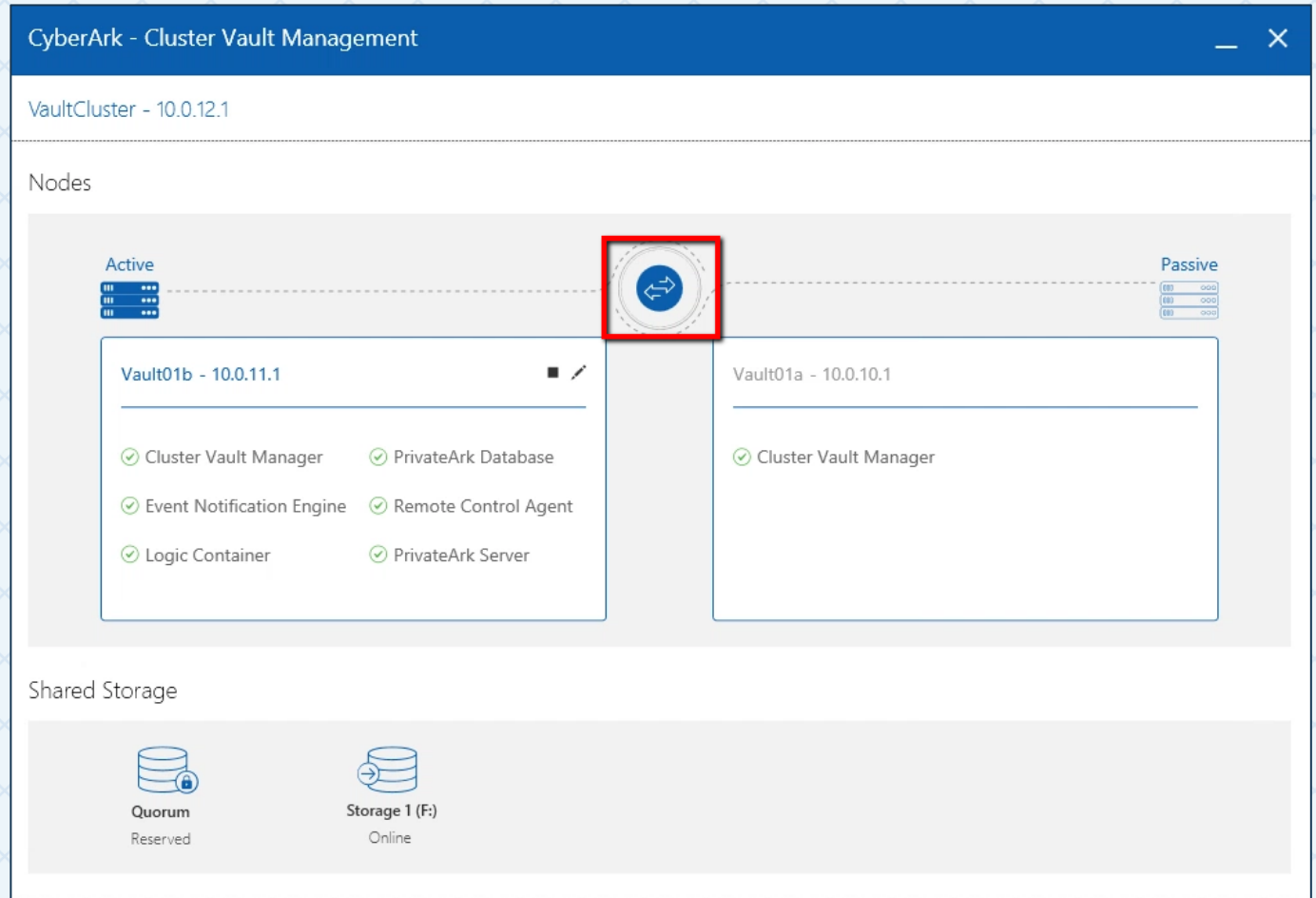
MONITORED SERVICES

- Selecting the crayon will display the Monitored Services option
- Using the CVM, the Administrator can select the services to be monitored by the Cluster Vault Manager
- Services not monitored will be ignored and will not trigger a cluster failover



SIMULATING FAILOVER

- To Perform a switchover test, open the CVM on the Active Node of the cluster
- Click the Switchover button shown highlighted
- Click Continue to confirm the message
- The operation is complete when the node status is updated.



CYBERARK DIGITAL CLUSTER VAULT SERVER INSTALLATION (PREPARATION AND REQUIREMENTS)

PREPARE THE SERVERS

- The Vault machines must meet the recommended system requirements
- Supported operating systems are Microsoft Windows Server 2012R2, Windows Server 2016 and 2019
- The two Cluster Vault Nodes must be connected directly via a private network or cross-over cable
- Both nodes should have identical specifications including memory and processor
- The clocks on both cluster nodes must be synchronized

Cluster Vault and Cluster DR Vault servers [🔗](#)

The following table lists the recommended specifications for the Cluster Vault server and the Cluster DR Vault server.

Specifications

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
<ul style="list-style-type: none">• Quad core processor (Intel compatible)• 8GB RAM• 2X 80GB SATA/SAS hot-swappable drives• RAID Controller• 2X Network adapter (1Gb)• DVD ROM• SCSI/Fibre shared disk that supports the SCSI3 protocol• Additional storage for PSM (optional) [1]	<ul style="list-style-type: none">• 2X Quad core processor (Intel compatible)• 16GB RAM• 2X 80GB SATA/SAS hot-swappable drives• RAID Controller• 2X Network adapter (1Gb)• DVD ROM• SCSI/Fibre shared disk that supports the SCSI3 protocol• Additional storage for PSM (optional) [1]	<ul style="list-style-type: none">• 2X Eight core processors (Intel compatible)• 32GB RAM• Two 250GB SAS hot-swappable drives (15K RPM)• RAID Controller• 2X Network adapter (1Gb)• DVD ROM• SCSI/Fibre shared disk that supports the SCSI3 protocol• Additional storage for PSM (optional) [1]	<ul style="list-style-type: none">• 4X Eight core processors (Intel compatible)• 64GB RAM• Two 500GB SAS hot-swappable drives (15K RPM)• RAID Controller• 2X Network adapter (1Gb)• DVD ROM• SCSI/Fibre shared disk supports the SCSI3 protocol• Additional storage for PSM (optional) [1]

Hardware and software prerequisites

For details, see [Digital Vault Server](#) and [Digital Vault Cluster \(High Availability\)](#).

STORAGE PREREQUISITES

- Shared storage must support **Persistent Reservation**
- It is recommended to use an enterprise-grade fiber-channel SAN solution
 - iSCSI network storage is not recommended for a production implementation
 - If iSCSI is used in a non-production environment, then a Windows update (KB2955164) should be installed in order to ensure database stability
 - Using iSCSI also requires a firewall rule added to dbparm.ini during installation



PREPARE THE STORAGE

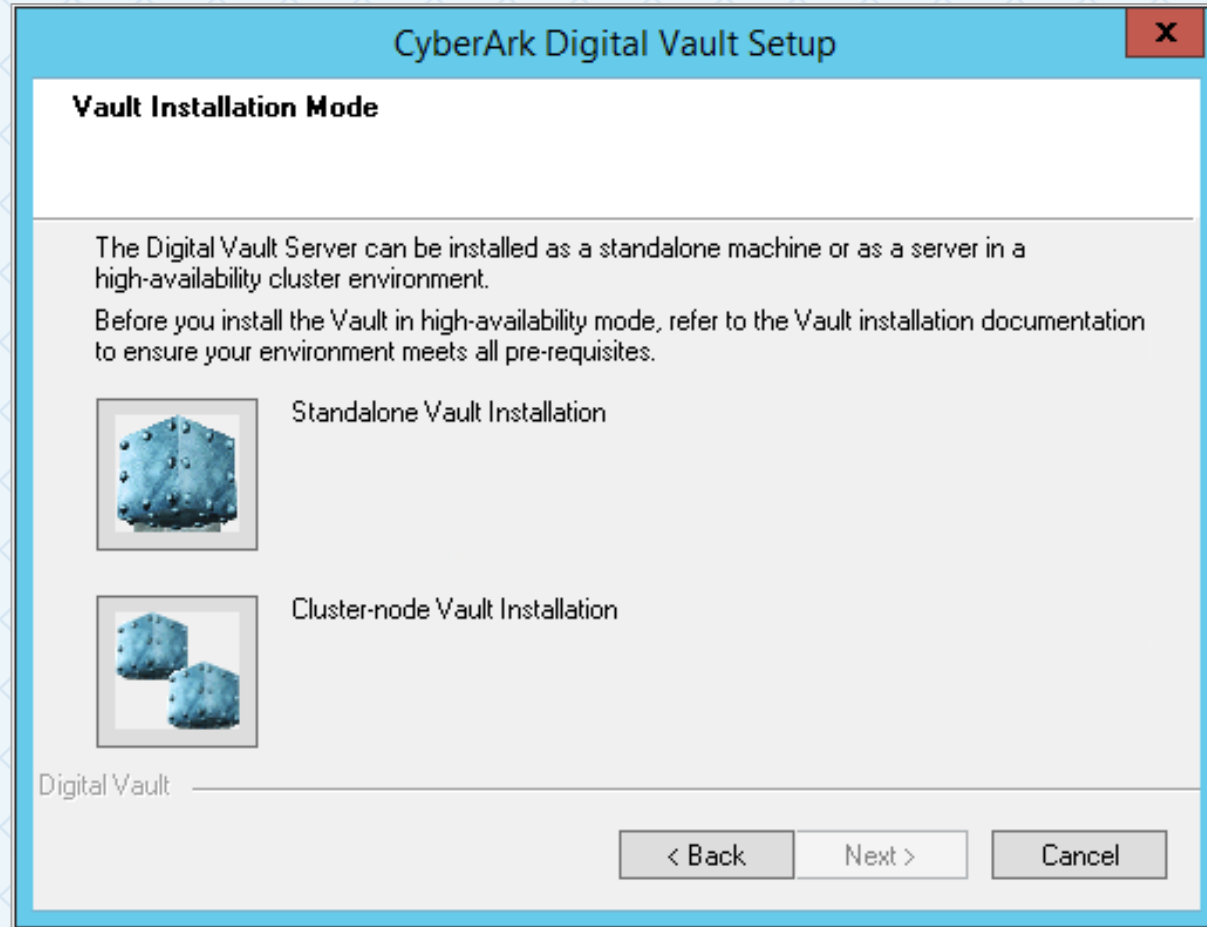
- Prepare the shared storage with two drives
 - One drive is for the Vault data, and the other drive is for the Quorum Disk
- Drive letters for the Quorum and Storage disks must be **identical** on both nodes
- During Digital Vault Cluster installation, ensure that the shared storage resources are online for ONLY the node currently being installed. After the Digital Vault Cluster is successfully installed, the CVM will manage the Shared Storage



CLUSTER INSTALLATION (INSTALL THE FIRST NODE)

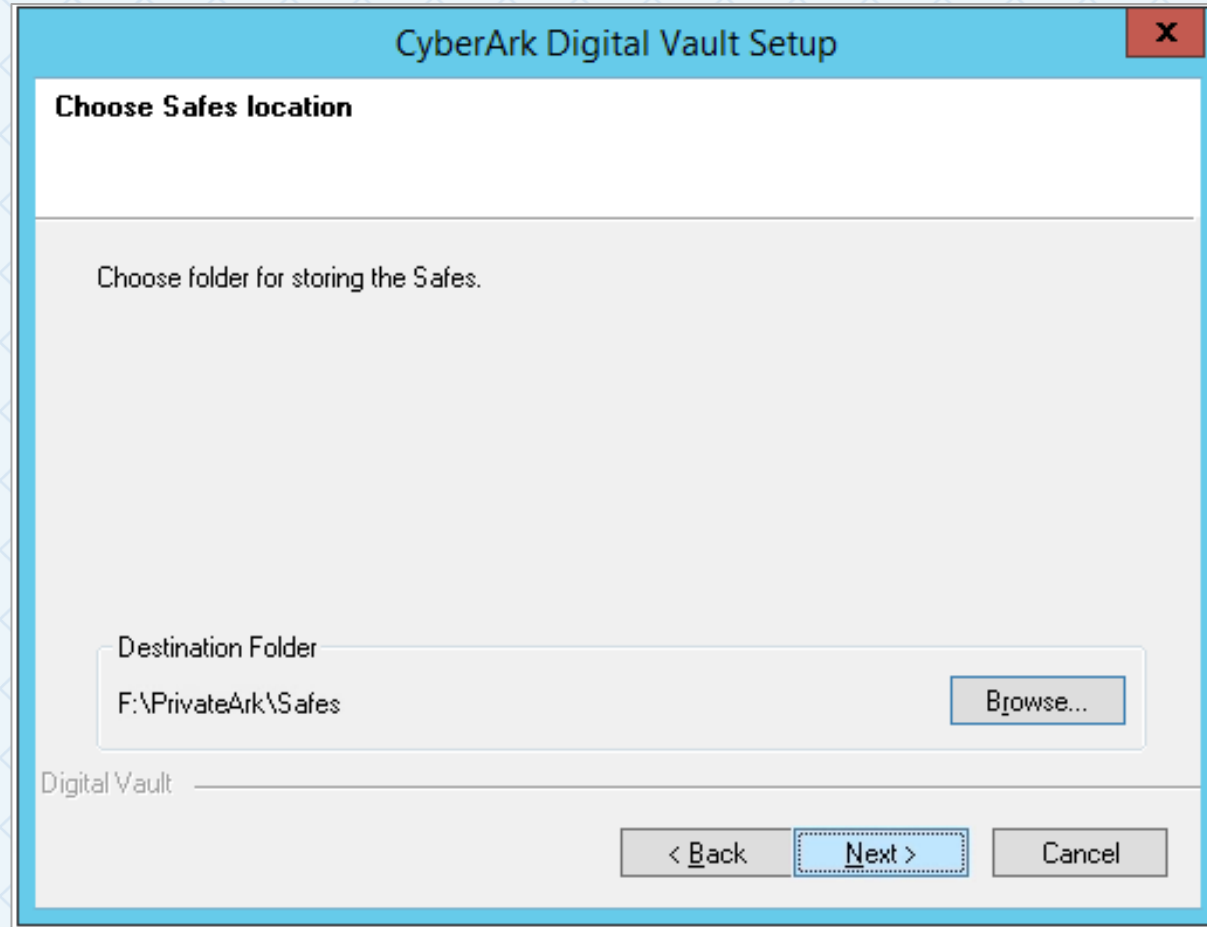
INSTALL THE FIRST NODE – VAULT INSTALLATION MODE

Launch the setup.exe and choose Cluster-Node Vault installation



INSTALL THE FIRST NODE – SAFES LOCATION

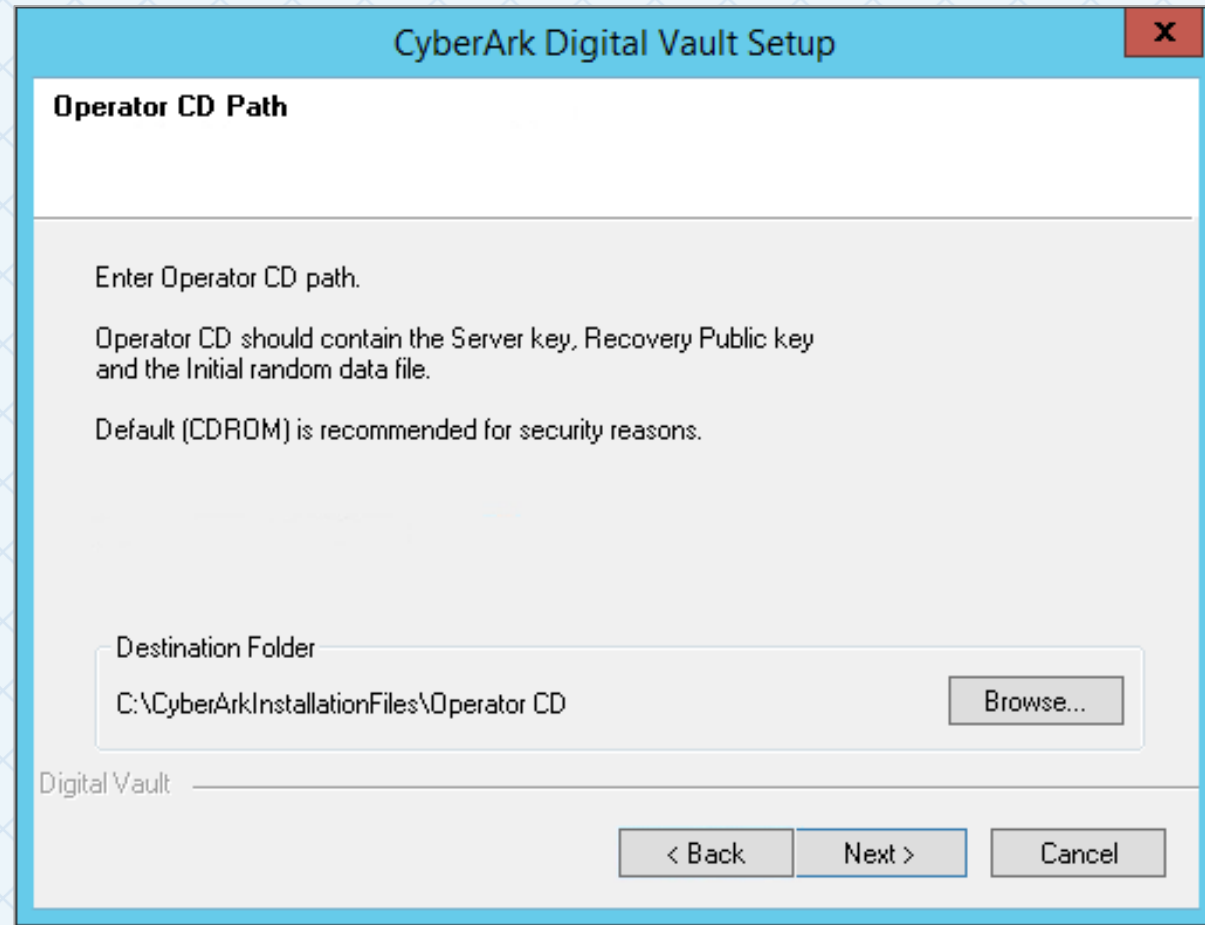
Choose the location on the **shared storage** to store the safes



The image shows a screenshot of the 'CyberArk Digital Vault Setup' window. The window has a blue title bar with the text 'CyberArk Digital Vault Setup' and a red close button with an 'x' icon. The main content area is titled 'Choose Safes location' and contains the instruction 'Choose folder for storing the Safes.' Below this, there is a text box labeled 'Destination Folder' containing the path 'F:\PrivateArk\Safes'. To the right of the text box is a 'Browse...' button. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The background of the slide features a light blue diamond pattern.

INSTALL THE FIRST NODE – OPERATOR CD PATH

- Copy the encryption keys from the operator CD to a folder on the **local drive**
- Select the folder on the local drive as the **Operator CD path**
- Complete the installation, but do not reboot immediately



The screenshot shows a window titled "CyberArk Digital Vault Setup" with a red close button in the top right corner. The window has a light blue header bar. Below the header, the title "Operator CD Path" is displayed in bold. The main area contains the following text:

Enter Operator CD path.

Operator CD should contain the Server key, Recovery Public key and the Initial random data file.

Default (CDROM) is recommended for security reasons.

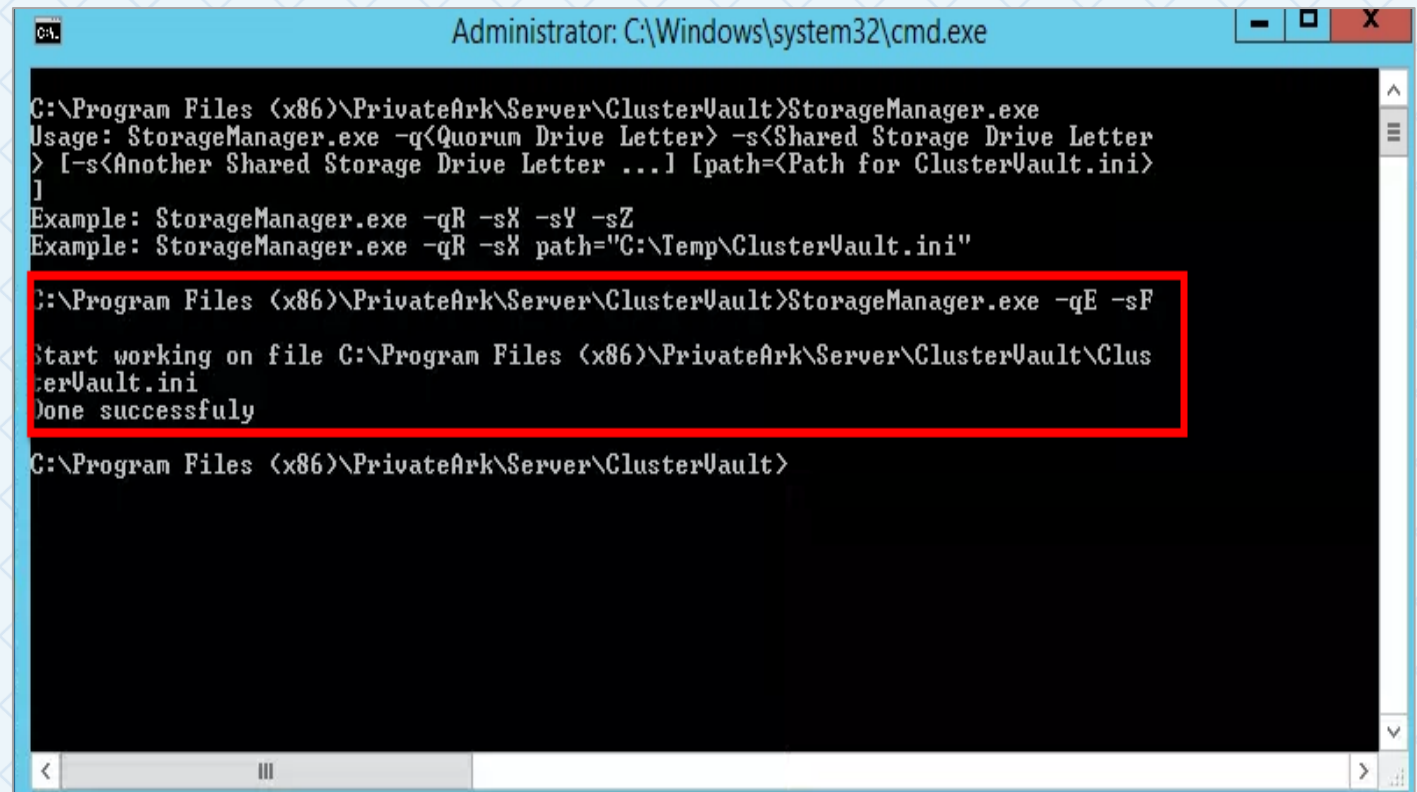
Below this text is a "Destination Folder" section with a text box containing "C:\CyberArk\InstallationFiles\Operator CD" and a "Browse..." button to its right. At the bottom of the window, there is a "Digital Vault" label followed by a horizontal line. Below this line are three buttons: "< Back", "Next >", and "Cancel".

INSTALL THE FIRST NODE – CONFIGURE STORAGE

- In an Administrators Command Window, navigate to the PrivateArk\Server\ClusterVault directory.
- Use the following command line to set the Quorum and Shared Storage drive letters

StorageManager.exe -qE -sF

- -q sets drive letter for quorum
- -s sets drive letter for shared storage



```
Administrator: C:\Windows\system32\cmd.exe

C:\Program Files (x86)\PrivateArk\Server\ClusterVault>StorageManager.exe
Usage: StorageManager.exe -q<Quorum Drive Letter> -s<Shared Storage Drive Letter>
> [-s<Another Shared Storage Drive Letter ...>] [path=<Path for ClusterVault.ini>]
]
Example: StorageManager.exe -qR -sX -sY -sZ
Example: StorageManager.exe -qR -sX path="C:\Temp\ClusterVault.ini"

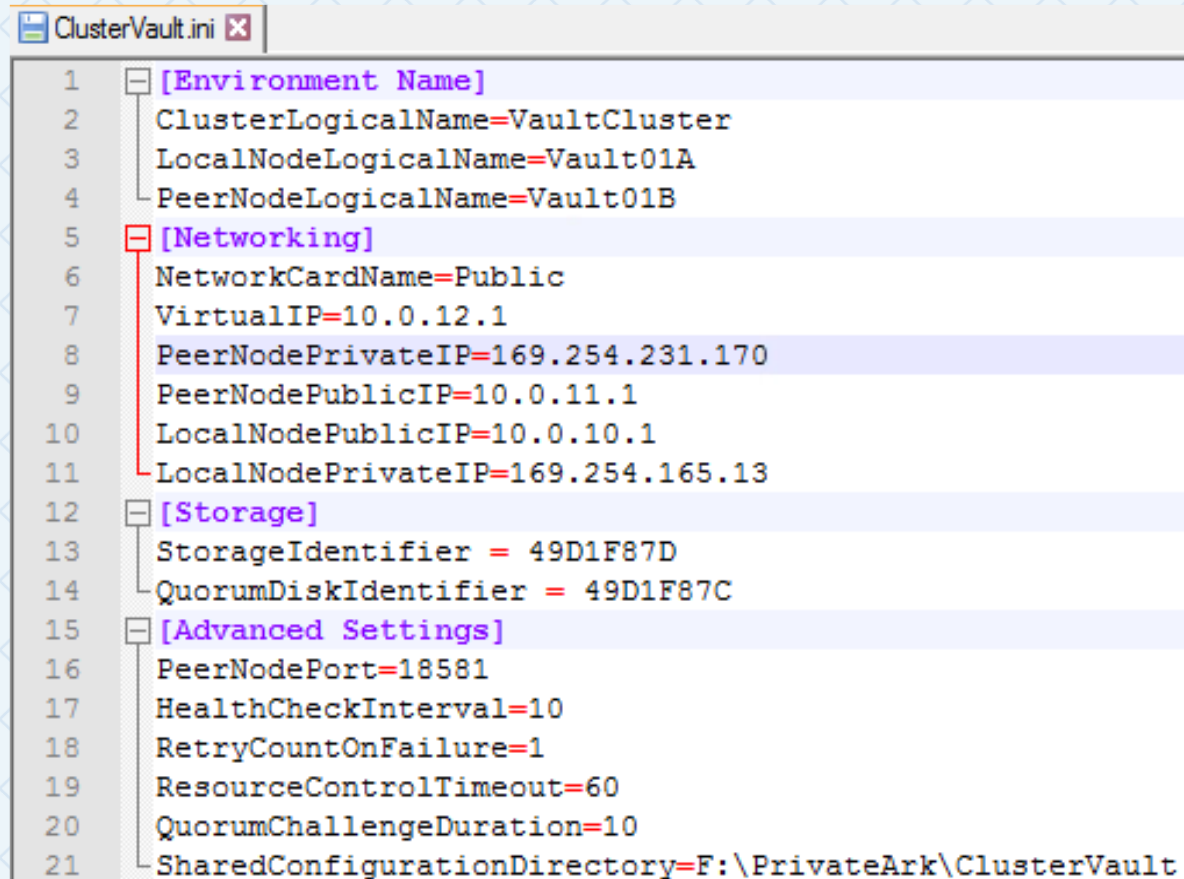
C:\Program Files (x86)\PrivateArk\Server\ClusterVault>StorageManager.exe -qE -sF
Start working on file C:\Program Files (x86)\PrivateArk\Server\ClusterVault\ClusterVault.ini
Done successfully

C:\Program Files (x86)\PrivateArk\Server\ClusterVault>
```


INSTALL THE FIRST NODE – CONFIGURE CLUSTERVAULT.INI

Set the names and IP addresses for the local and peer node in ClusterVault.ini

- Logical Names
- Virtual IP
- Peer and Local Public and Private IP addresses
- located in C:\Program Files (x86)\PrivateArk\Server\Cluster Vault\
- The information defined in the ClusterVault.ini file, is displayed by the Cluster Vault Management utility or CVM

A screenshot of a text editor window titled 'ClusterVault.ini'. The file contains configuration settings for a Cluster Vault, organized into sections: [Environment Name], [Networking], [Storage], and [Advanced Settings]. The settings include logical names, network card name, virtual IP, private and public IP addresses for both local and peer nodes, storage identifiers, and various advanced settings like port, health check interval, and retry count. The file path at the bottom is F:\PrivateArk\ClusterVault.

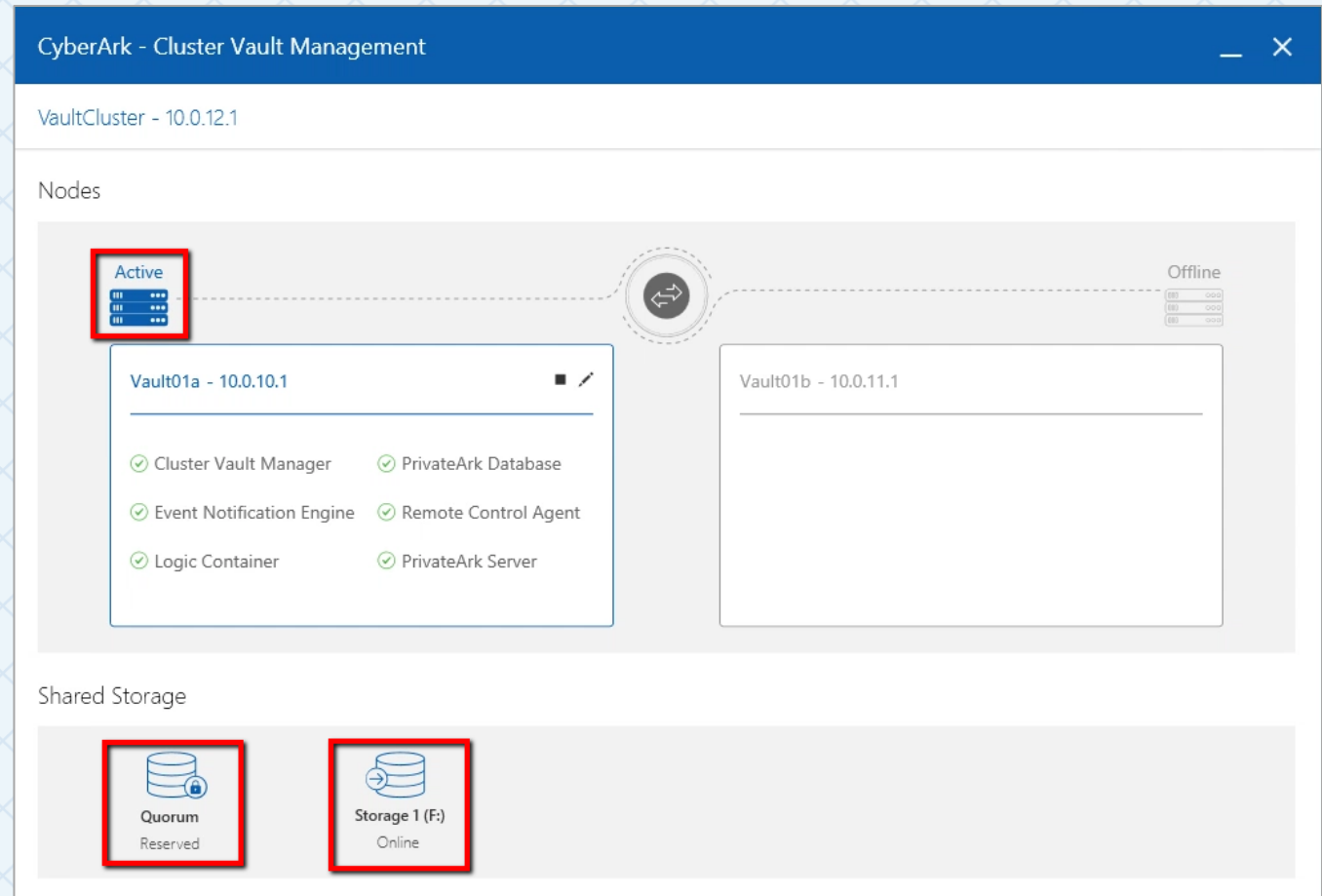
```
1 [Environment Name]
2   ClusterLogicalName=VaultCluster
3   LocalNodeLogicalName=Vault01A
4   PeerNodeLogicalName=Vault01B
5 [Networking]
6   NetworkCardName=Public
7   VirtualIP=10.0.12.1
8   PeerNodePrivateIP=169.254.231.170
9   PeerNodePublicIP=10.0.11.1
10  LocalNodePublicIP=10.0.10.1
11  LocalNodePrivateIP=169.254.165.13
12 [Storage]
13   StorageIdentifier = 49D1F87D
14   QuorumDiskIdentifier = 49D1F87C
15 [Advanced Settings]
16   PeerNodePort=18581
17   HealthCheckInterval=10
18   RetryCountOnFailure=1
19   ResourceControlTimeout=60
20   QuorumChallengeDuration=10
21   SharedConfigurationDirectory=F:\PrivateArk\ClusterVault
```

INSTALL THE FIRST NODE – REBOOT

- Restart the first node and verify that all resources have been started successfully. The following message will appear in the ClusterVaultConsole.log

CVMCS087I All the resources are running successfully

- Launch **Cluster Vault Management**, check that node is showing as “Active”, shared storage as “Online” and Quorum as “Reserved”



PREPARING FOR VAULT INSTALLATION ON SECOND NODE

COPY ENCRYPTION KEYS TO SECOND NODE

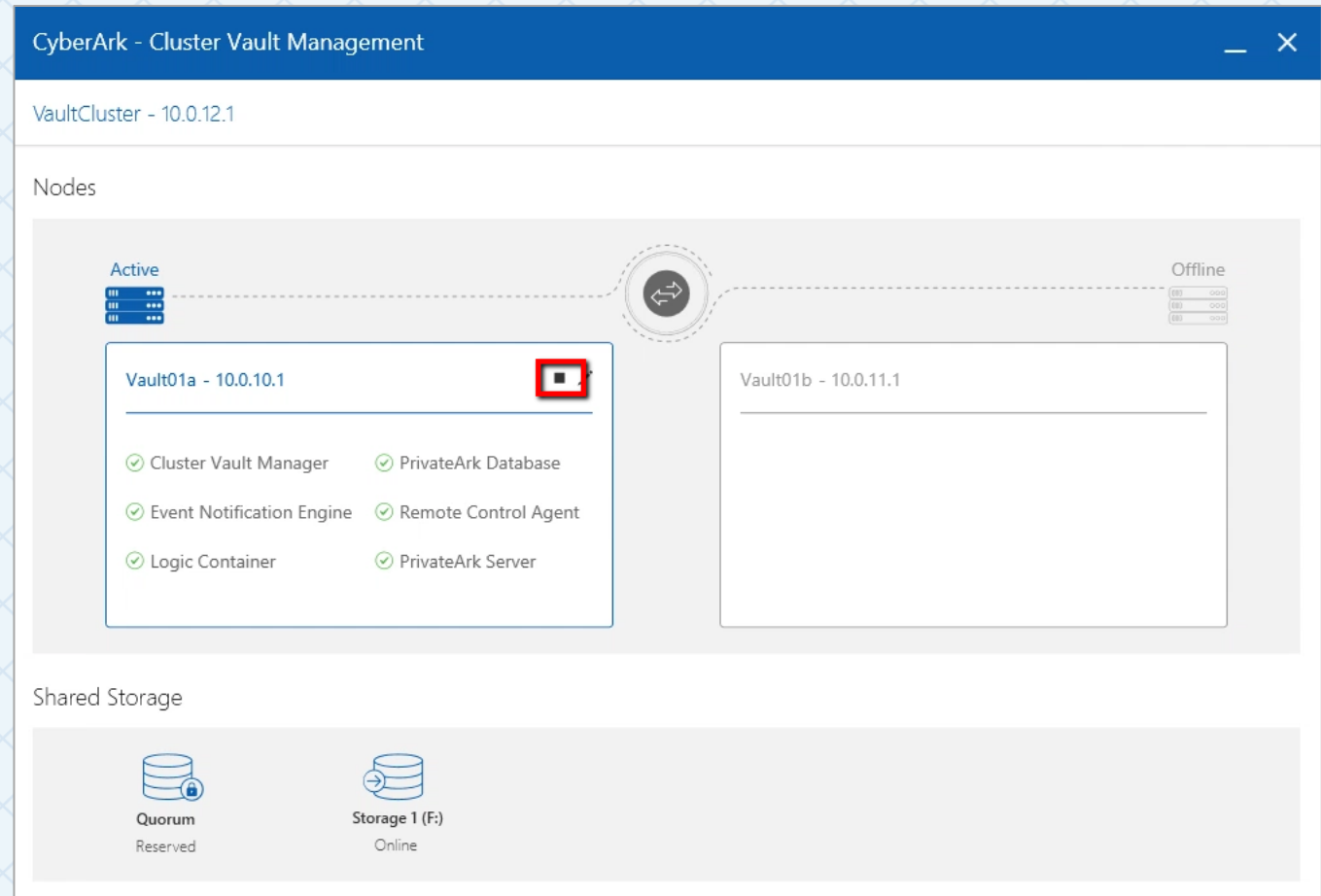
- Use the same set of Operator Keys that you used to install the first node of the Cluster Vault
- Copy the additional keys highlighted here, that were generated during the installation of the first node to the same location in the second node
- These keys will be created in the folder containing the original Operator Keys
 - Backup.key
 - VaultUser.pass
 - ReplicationUser.pass
 - VaultEmergency.pass



Demo License	10/16/2013 3:42 AM	File folder	
Backup.key	12/25/2016 9:09 AM	KEY File	1 KB
Demo.txt	3/6/2011 8:32 PM	TXT File	1 KB
DemoOperatorKeys.zip	3/6/2011 8:32 PM	Compressed (zipp...	2 KB
recpub.key	3/6/2011 8:32 PM	KEY File	1 KB
ReplicationUser.pass	12/25/2016 9:09 AM	PASS File	1 KB
rndbase.dat	3/6/2011 8:32 PM	DAT File	1 KB
server.key	3/6/2011 8:32 PM	KEY File	1 KB
Server.pem	12/25/2016 9:05 AM	PEM File	1 KB
Server.pvk	12/25/2016 9:05 AM	PVK File	2 KB
VaultEmergency.pass	12/25/2016 9:09 AM	PASS File	1 KB
VaultUser.pass	12/25/2016 9:09 AM	PASS File	1 KB

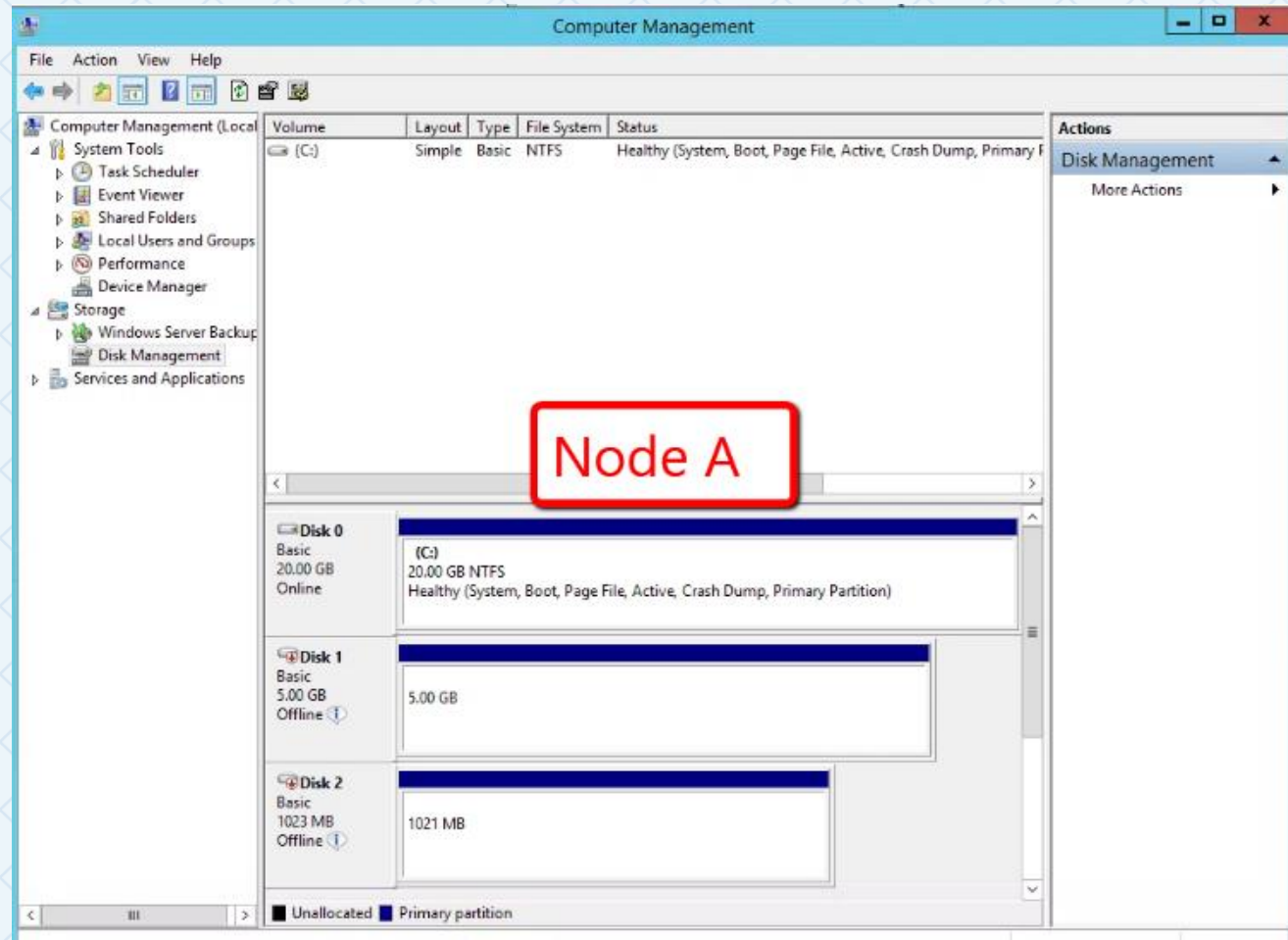
STOP SERVICES ON FIRST NODE

- Before starting the installation of the second node of the Cluster Vault, we need to stop all services on the first node
- Log on to the first node and launch Cluster Vault Management. Select the stop symbol that is highlighted in the graphic



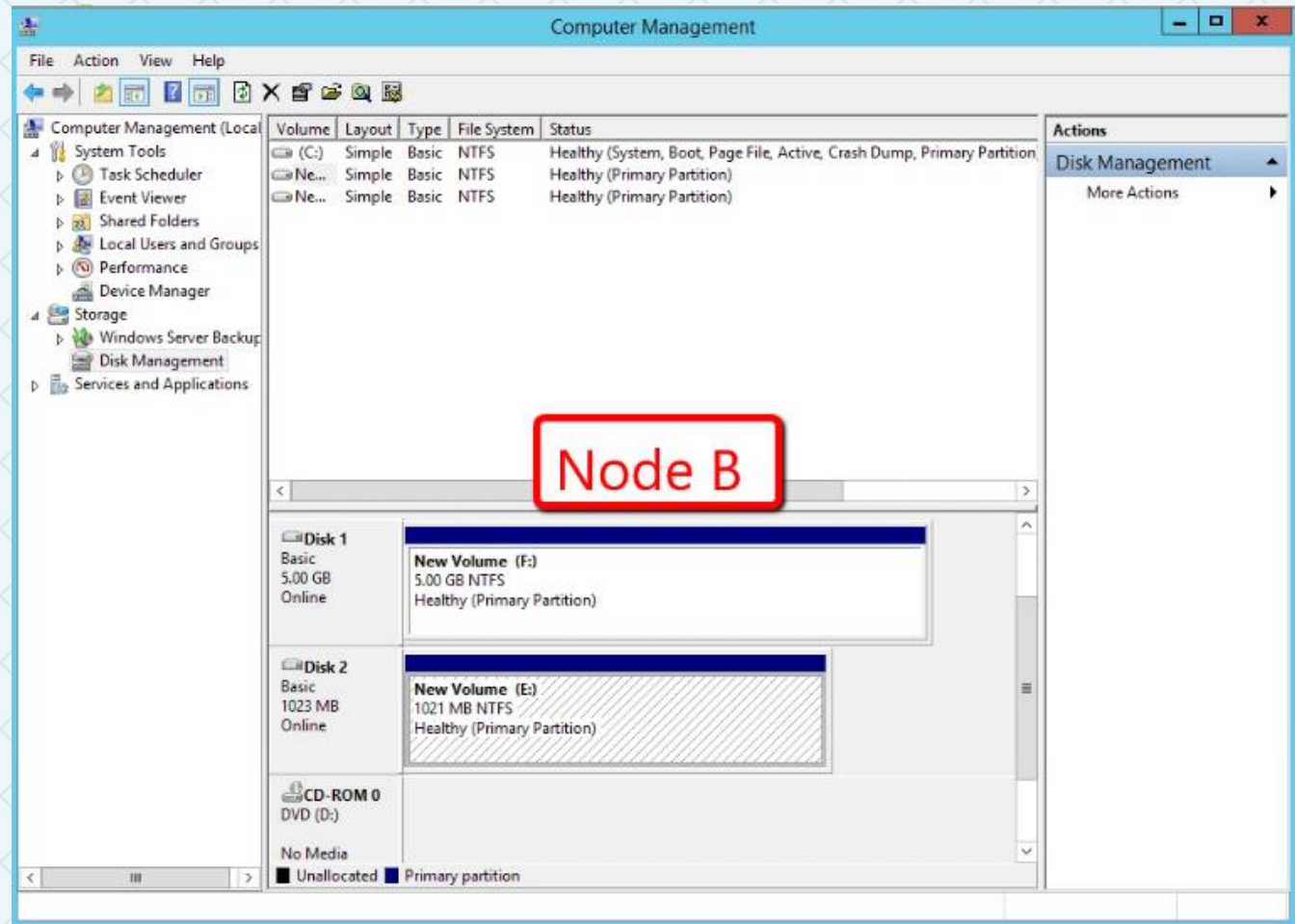
SET SHARED DISKS TO OFFLINE ON FIRST NODE

- Use the Disk Management utility to verify the shared disks are **offline** on the **first** node
- Make sure that there are no open files or folders on the shared storage
- Now it is safe to bring the disks online on the second node



BRING SHARED DISKS ONLINE ON SECOND NODE

- Use the Disk Management utility to bring the Shared Disks **online** on the **second** Node
- Ensure that the drive letters for the Quorum and Storage disks are **identical** in both nodes



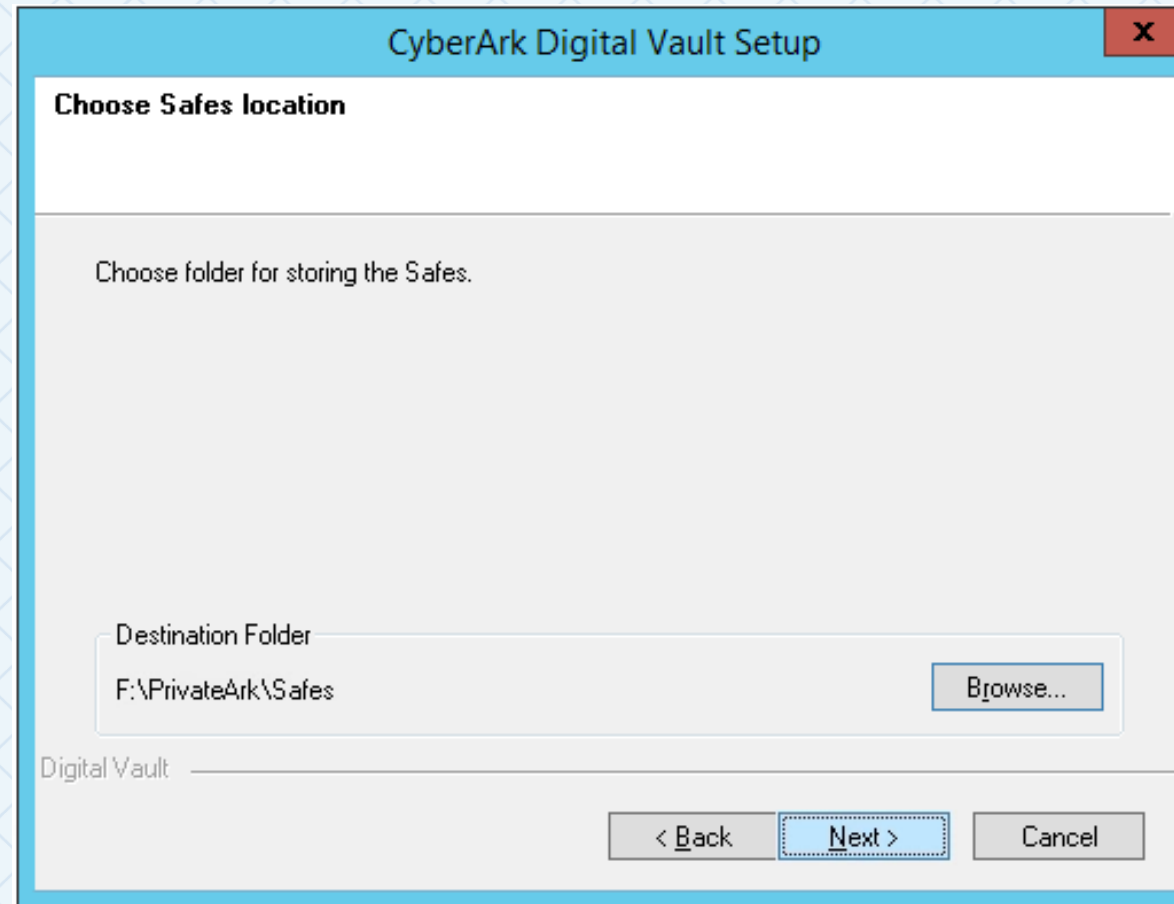
CLUSTER INSTALLATION (INSTALL THE SECOND NODE)

INSTALL THE SECOND NODE – SAFES LOCATION

Install The Vault on the Second Node

Make sure you select:

- “Cluster-Node Vault installation” as the installation mode
- the same drive letter and folder on the shared storage for the Safes location.

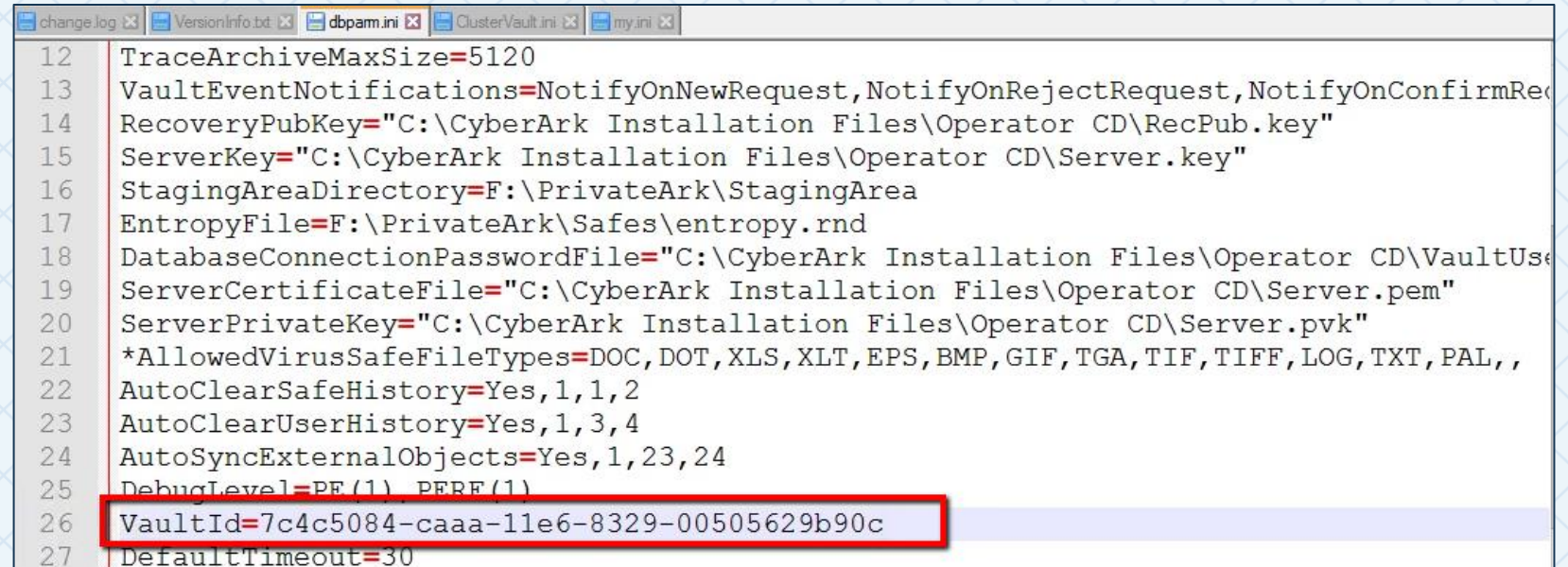


The screenshot shows a window titled "CyberArk Digital Vault Setup" with a red close button in the top right corner. The window has a light blue header bar. Below the header, the title "Choose Safes location" is displayed in bold. The main area is a light gray box with the text "Choose folder for storing the Safes." Below this, there is a text field labeled "Destination Folder" containing the path "F:\PrivateArk\Safes". To the right of the text field is a "Browse..." button. At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

INSTALL THE SECOND NODE – VAULTID

The Vault-id parameter must be consistent for both cluster nodes.

- Open **DBParm.ini** on the first node
- Copy the **Vault-id** parameter from the first node to DBParm.ini on the **second** node

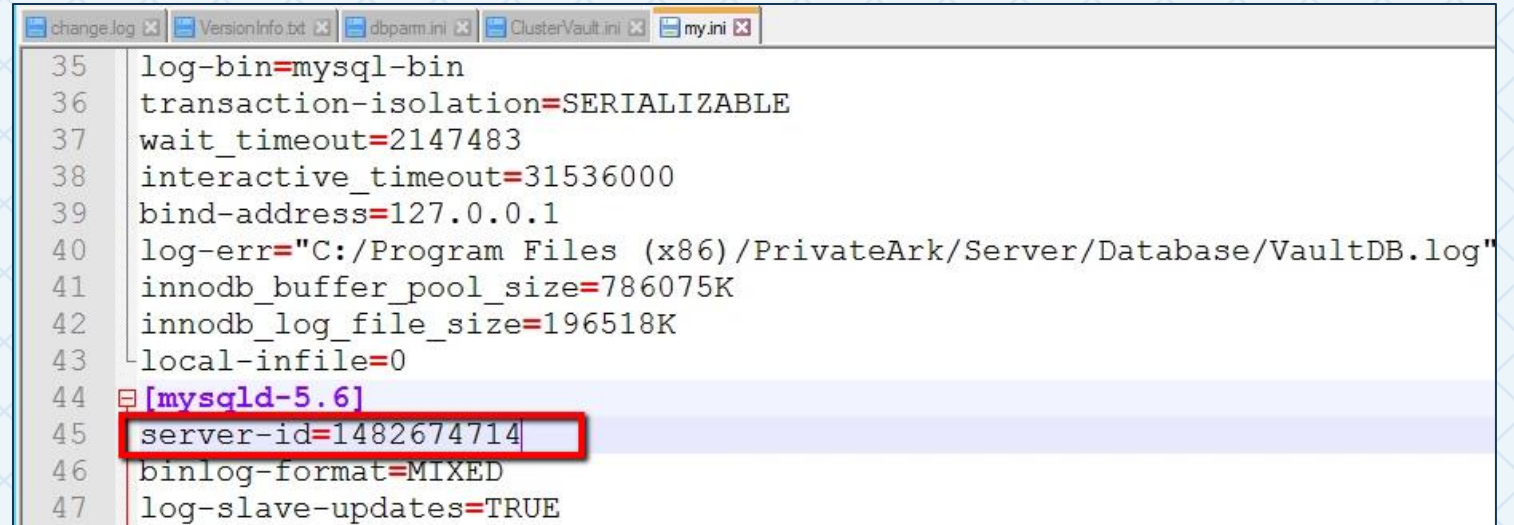


```
12 TraceArchiveMaxSize=5120
13 VaultEventNotifications=NotifyOnNewRequest,NotifyOnRejectRequest,NotifyOnConfirmRec
14 RecoveryPubKey="C:\CyberArk Installation Files\Operator CD\RecPub.key"
15 ServerKey="C:\CyberArk Installation Files\Operator CD\Server.key"
16 StagingAreaDirectory=F:\PrivateArk\StagingArea
17 EntropyFile=F:\PrivateArk\Safes\entropy.rnd
18 DatabaseConnectionPasswordFile="C:\CyberArk Installation Files\Operator CD\VaultUse
19 ServerCertificateFile="C:\CyberArk Installation Files\Operator CD\Server.pem"
20 ServerPrivateKey="C:\CyberArk Installation Files\Operator CD\Server.pvk"
21 *AllowedVirusSafeFileTypes=DOC,DOT,XLS,XLT,EPS,BMP,GIF,TGA,TIF,TIFF,LOG,TXT,PAL,,
22 AutoClearSafeHistory=Yes,1,1,2
23 AutoClearUserHistory=Yes,1,3,4
24 AutoSyncExternalObjects=Yes,1,23,24
25 DebugLevel=PE(1),PERF(1)
26 VaultId=7c4c5084-caaa-11e6-8329-00505629b90c
27 DefaultTimeout=30
```


INSTALL THE SECOND NODE – SERVER-ID

The server-id parameter must be consistent for both cluster nodes.

- Open **my.ini** on the first node in the Database subdirectory
- Copy the Server-id from the first node to the **second** node



```
35 log-bin=mysql-bin
36 transaction-isolation=SERIALIZABLE
37 wait_timeout=2147483
38 interactive_timeout=31536000
39 bind-address=127.0.0.1
40 log-err="C:/Program Files (x86)/PrivateArk/Server/Database/VaultDB.log"
41 innodb_buffer_pool_size=786075K
42 innodb_log_file_size=196518K
43 local-infile=0
44 [mysqld-5.6]
45 server-id=1482674714
46 binlog-format=MIXED
47 log-slave-updates=TRUE
```

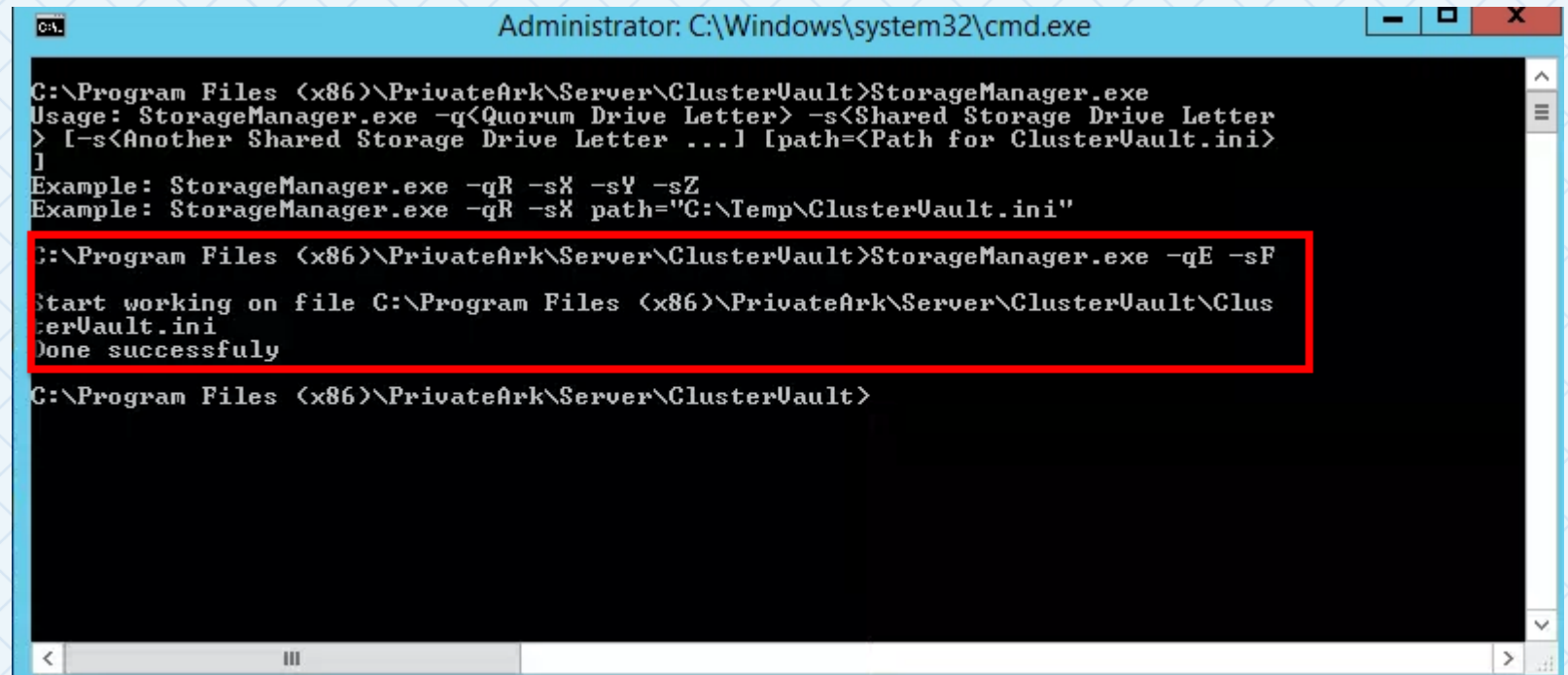
INSTALL THE SECOND NODE – CONFIGURE STORAGE

The disk identifiers must be recorded in the ClusterVault.ini file in the StorageIdentifier and QuorumDiskIdentifier parameters

- Use the following command to set the Quorum and Shared Storage drive letters:

StorageManager.exe -qE -sF

- Use the same drive letters as on the first node



```
Administrator: C:\Windows\system32\cmd.exe

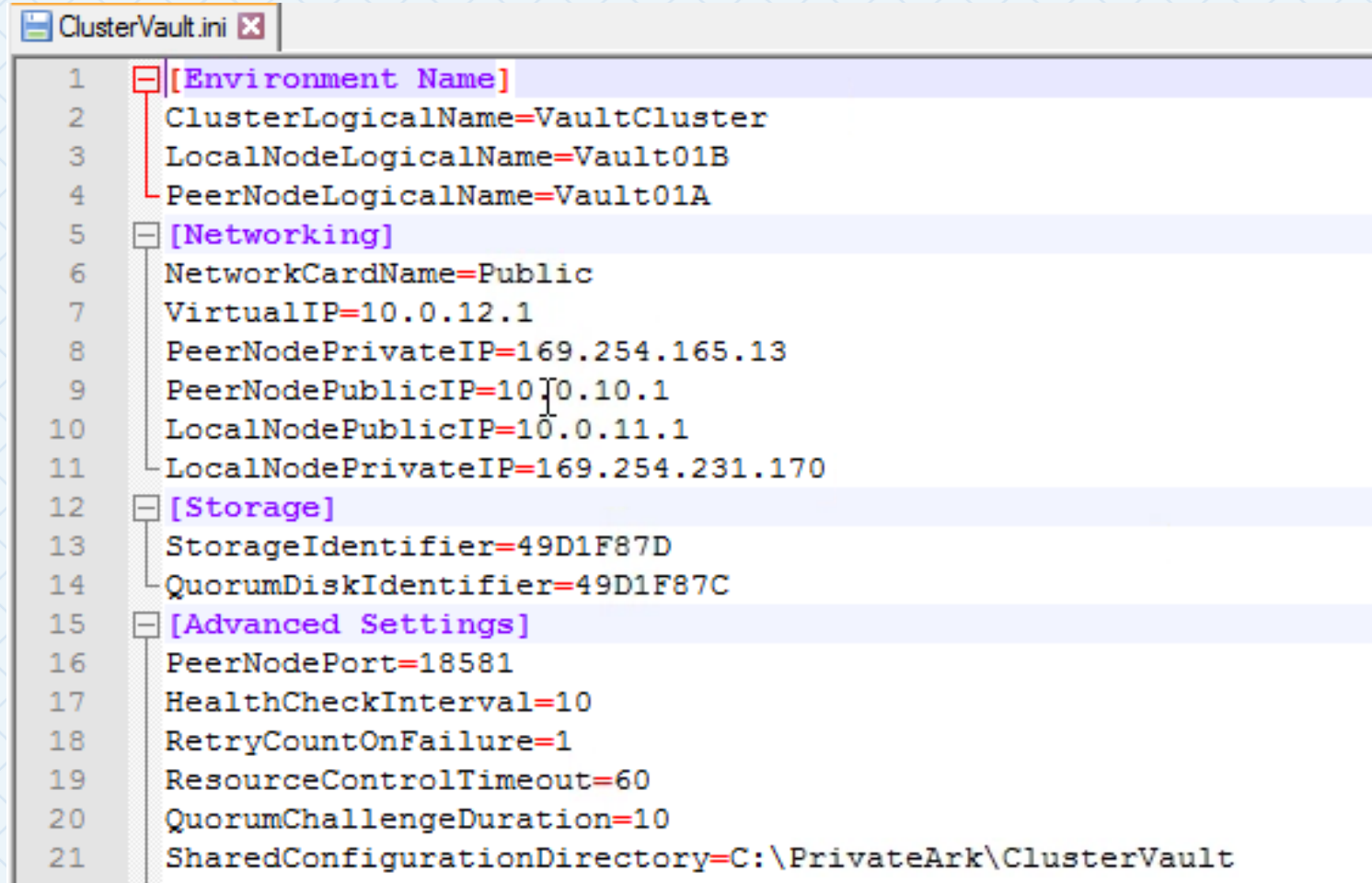
C:\Program Files (x86)\PrivateArk\Server\ClusterVault>StorageManager.exe
Usage: StorageManager.exe -q<Quorum Drive Letter> -s<Shared Storage Drive Letter>
> [-s<Another Shared Storage Drive Letter ...>] [path=<Path for ClusterVault.ini>]
Example: StorageManager.exe -qR -sX -sY -sZ
Example: StorageManager.exe -qR -sX path="C:\Temp\ClusterVault.ini"

C:\Program Files (x86)\PrivateArk\Server\ClusterVault>StorageManager.exe -qE -sF
Start working on file C:\Program Files (x86)\PrivateArk\Server\ClusterVault\Clus
terVault.ini
Done successfully

C:\Program Files (x86)\PrivateArk\Server\ClusterVault>
```

INSTALL THE SECOND NODE – CONFIGURE CLUSTERVAULT.INI

- Set the names and IP addresses for the local and peer nodes in ClusterVault.ini
 - Logical Names
 - Virtual IP
 - Peer and Local Public and Private IP addresses



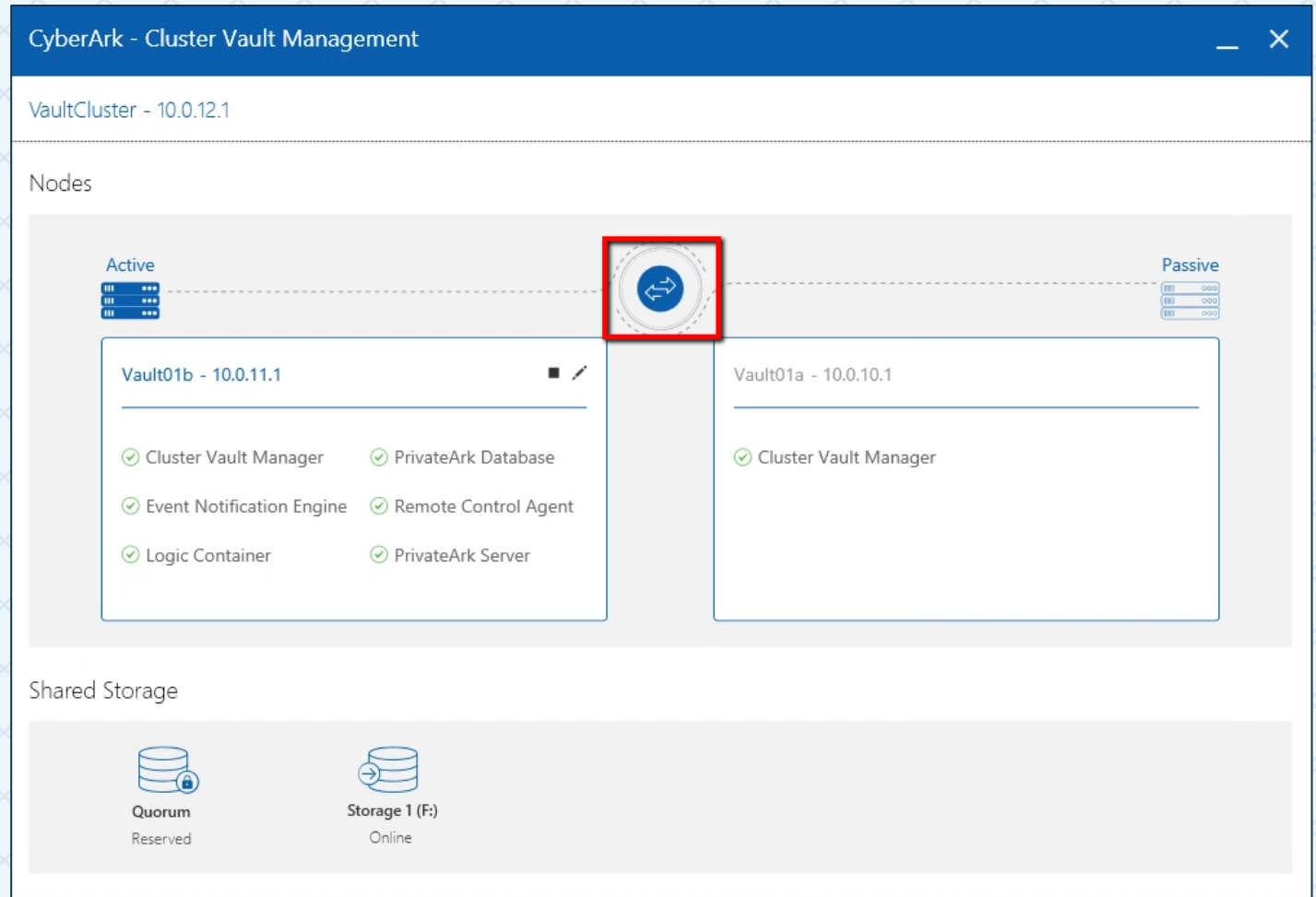
```
ClusterVault.ini
1  [Environment Name]
2  ClusterLogicalName=VaultCluster
3  LocalNodeLogicalName=Vault01B
4  PeerNodeLogicalName=Vault01A
5  [Networking]
6  NetworkCardName=Public
7  VirtualIP=10.0.12.1
8  PeerNodePrivateIP=169.254.165.13
9  PeerNodePublicIP=10.0.10.1
10 LocalNodePublicIP=10.0.11.1
11 LocalNodePrivateIP=169.254.231.170
12 [Storage]
13 StorageIdentifier=49D1F87D
14 QuorumDiskIdentifier=49D1F87C
15 [Advanced Settings]
16 PeerNodePort=18581
17 HealthCheckInterval=10
18 RetryCountOnFailure=1
19 ResourceControlTimeout=60
20 QuorumChallengeDuration=10
21 SharedConfigurationDirectory=C:\PrivateArk\ClusterVault
```

INSTALL THE SECOND NODE – REBOOT

- Restart the second node and verify that all resources have been started successfully. The following message should appear in the ClusterVaultConsole.log:

CVMCS087I All the resources are running successfully

- After the Second node has started successfully and is active, start the first node in Passive mode and then trigger a switchover to test the cluster failover process.



CLUSTER VAULT LOGS

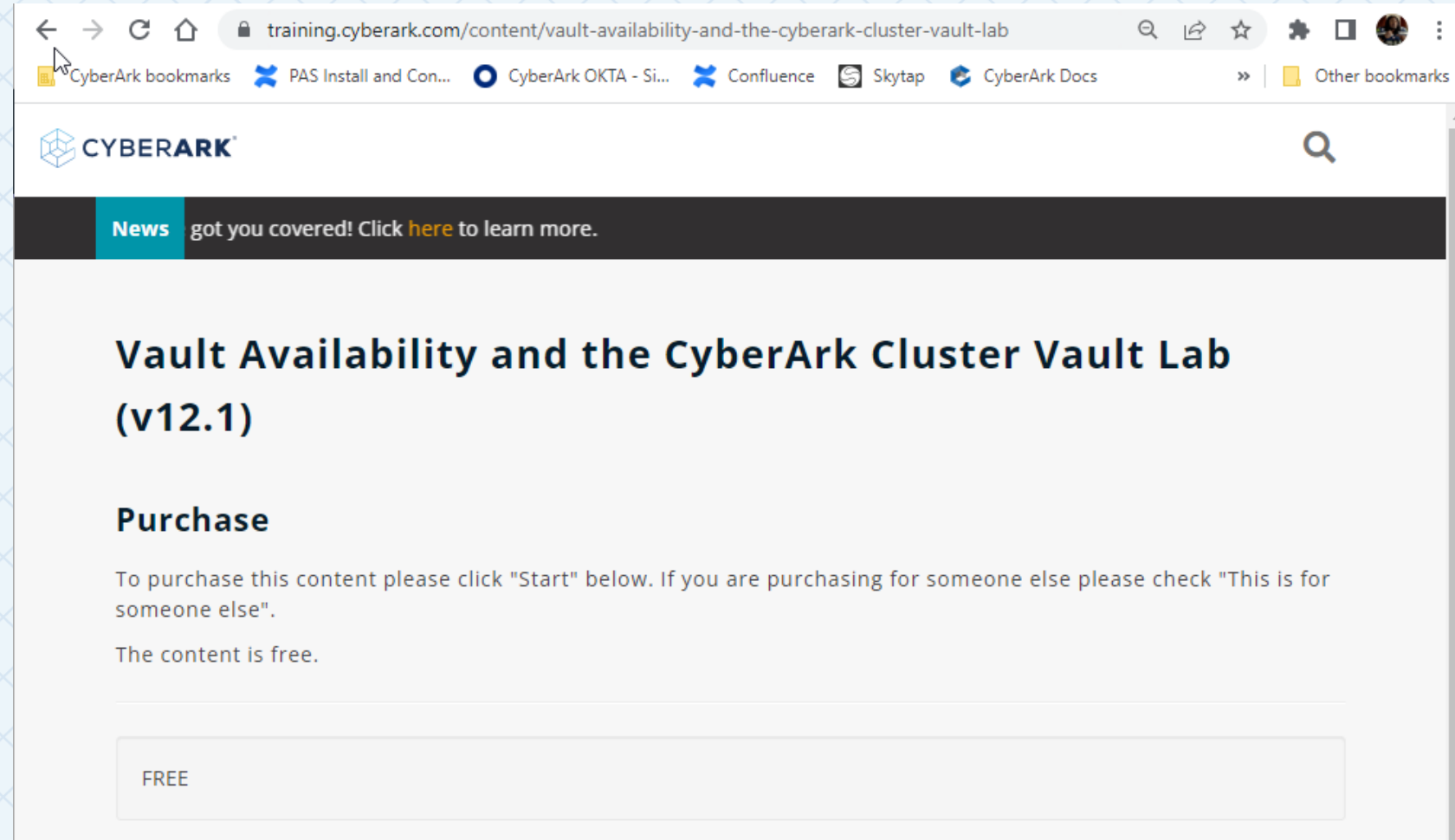
LOGS

- ClusterVaultConsole.log
 - Cluster Vault log file
- ClusterVaultTrace.log
 - Cluster Vault trace file
- Setting the debug level for the Cluster Vault can be set dynamically with no restart needed.

```
ClusterVaultTrace - Notepad
File Edit Format View Help
06/06/2016 16:47:33 3368 2204 [WARN] [Passive] CVMQU012W Quorum reservation failed with recoverable error code <6>. Operation will be retried.
06/06/2016 16:47:33 3368 2204 [INFO] [Passive] CVMCS122I Current Cluster State is: Primary Takeover State
06/06/2016 16:47:33 3368 2204 [INFO] [Passive] CVMCS139I Re-initializing services list for the CyberArk Cluster Vault Management utility.
06/06/2016 16:47:33 3368 2204 [INFO] [Passive] CVMCS163I Re-initializing the shared storage list for the CyberArk Cluster Vault Management utility.
06/06/2016 16:47:36 3368 3488 [INFO] [Takeover] CVMCM026I Peer node sent request.
06/06/2016 16:47:43 3368 2204 [INFO] [Takeover] CVMCS123I Starting up resources.
06/06/2016 16:47:43 3368 2204 [WARN] [Takeover] CVMVP046W If you configured PARAgent to send SNMP traps to a remote server, change the order of the net
06/06/2016 16:47:45 3368 2204 [INFO] [Takeover] CVMCS127I The cluster virtual IP 10.10.12.171 was acquired successfully.
06/06/2016 16:47:45 3368 2204 [INFO] [Takeover] CVMCS130I The Quorum ip is now reserved.
06/06/2016 16:47:45 3368 2204 [INFO] [Takeover] CVMCS131I Bringing online the physical drive on <\\.\PhysicalDrive2>.
06/06/2016 16:47:46 3368 2204 [INFO] [Takeover] CVMCS132I Physical drive <\\.\PhysicalDrive2> is now online
06/06/2016 16:47:46 3368 3488 [INFO] [Takeover] CVMCM026I Peer node sent request.
06/06/2016 16:47:49 3368 2204 [INFO] [Takeover] CVMCS133I The PrivateArk Database service started.
06/06/2016 16:47:51 3368 2204 [INFO] [Takeover] CVMCS133I The CyberArk Logic Container service started.
06/06/2016 16:47:56 3368 3488 [INFO] [Takeover] CVMCM026I Peer node sent request.
06/06/2016 16:47:59 3368 2204 [INFO] [Takeover] CVMCS133I The PrivateArk Server service started.
06/06/2016 16:48:06 3368 3488 [INFO] [Takeover] CVMCM026I Peer node sent request.
06/06/2016 16:48:09 3368 2204 [INFO] [Takeover] CVMCS133I The CyberArk Event Notification Engine service started.
06/06/2016 16:48:10 3368 2204 [INFO] [Takeover] CVMCS133I The PrivateArk Remote Control Agent service started.
06/06/2016 16:48:10 3368 2204 [INFO] [Takeover] CVMCS124I Resources startup completed.
06/06/2016 16:48:10 3368 2204 [INFO] [Takeover] CVMCS109I Current Cluster State is: Primary Active State
06/06/2016 16:48:10 3368 2204 [INFO] [Takeover] CVMCS139I Re-initializing services list for the CyberArk Cluster Vault Management utility.
06/06/2016 16:48:10 3368 2204 [INFO] [Takeover] CVMCS163I Re-initializing the shared storage list for the CyberArk Cluster Vault Management utility.
06/06/2016 16:48:16 3368 3488 [INFO] [Active] CVMCM026I Peer node sent request.
06/06/2016 16:48:20 3368 2204 [WARN] [Active] CVMVP046W If you configured PARAgent to send SNMP traps to a remote server, change the order of the net
06/06/2016 16:48:20 3368 2204 [INFO] [Active] CVMCS087I All the resources are running successfully.
06/06/2016 16:48:26 3368 3488 [INFO] [Active] CVMCM026I Peer node sent request.
06/06/2016 16:48:30 3368 2204 [WARN] [Active] CVMVP046W If you configured PARAgent to send SNMP traps to a remote server, change the order of the net
06/06/2016 16:48:30 3368 2204 [INFO] [Active] CVMCS087I All the resources are running successfully.
06/06/2016 16:48:36 3368 3488 [INFO] [Active] CVMCM026I Peer node sent request.
06/06/2016 16:48:40 3368 2204 [WARN] [Active] CVMVP046W If you configured PARAgent to send SNMP traps to a remote server, change the order of the net
```

LOGS

- Link to the HA Vault Cluster Lab
- <https://training.cyberark.com/content/vault-availability-and-the-cyberark-cluster-vault-lab>



THANK YOU