nap

**WIP & WISP Procedures on cDOT**

**Synopsis:** To understand configuration parameters while deploying WIP/WISP in the cDOT environment

**Segment:** Unified Storage - NAS

**Authors:** Mahesha

**Contributors: Ian Daniels, Arpit Roy, Sridhar Chevendra, Unified Storage Design & Engineering**

**Document Version:** V 2.5

**Date:** 02-July-2018

Document Status: Issued

**CONFIDENTIAL INFORMATION**

This document contains information proprietary to Thomson Reuters and may not be reproduced, disclosed or used in whole or part without express permission of Thomson Reuters.

© Thomson Reuters 2017

Contents

[1 Introduction 4](#_Toc515636101)

[1.1 Management Summary 4](#_Toc515636102)

[1.2 Document Scope 4](#_Toc515636103)

[1.3 Assumptions 4](#_Toc515636104)

[1.4 References 4](#_Toc515636105)

[1.5 Change History 4](#_Toc515636106)

[1.6 Distribution List 5](#_Toc515636107)

[1.7 Glossary 5](#_Toc515636108)

[2 Understanding the components of iSCSI service 8](#_Toc515636109)

[2.1 Vserver 8](#_Toc515636110)

[2.2 LIF 8](#_Toc515636111)

[2.2.1 LIF roles 8](#_Toc515636112)

[2.2.2 Limitations 9](#_Toc515636113)

[2.3 High availability 10](#_Toc515636114)

[2.4 iGroups 11](#_Toc515636115)

[2.5 vserver naming 12](#_Toc515636116)

[2.6 Data/ISCSI LIF Naming 13](#_Toc515636117)

[2.7 Management LIF 13](#_Toc515636118)

[2.8 Portsets 13](#_Toc515636119)

[2.9 QOS 13](#_Toc515636120)

[2.10 Licenses 16](#_Toc515636121)

[2.11 Create vserver 16](#_Toc515636122)

[2.12 Enable iSCSI protocol 16](#_Toc515636123)

[2.13 Allow protocols (CIFS for FSW) 16](#_Toc515636124)

[2.14 Check the vserver status 16](#_Toc515636125)

[2.15 Create LIFs 16](#_Toc515636126)

[2.15.1 SAN Data LIF(s) 16](#_Toc515636127)

[2.15.2 CIFS Data LIF (For FSW Support) 17](#_Toc515636128)

[2.15.3 Vserver Management LIF 17](#_Toc515636129)

[2.15.4 Vserver management failover group for management 17](#_Toc515636130)

[2.16 Routing 17](#_Toc515636131)

[2.17 Create portsets 18](#_Toc515636132)

[2.18 Create CIFS Server If Using FSW 18](#_Toc515636133)

[2.19 Create data volume(s) and QoS Configuration 18](#_Toc515636134)

[2.20 Backup and snapshots 19](#_Toc515636135)

[2.21 Snapshot Autodelete Policies 19](#_Toc515636136)

[2.22 Create Qtree 19](#_Toc515636137)

[2.23 Create LUNs 19](#_Toc515636138)

[2.24 iGroups and Mapping 20](#_Toc515636139)

[2.24.1 Add the iSCSI IQNs from server(s) 20](#_Toc515636140)

[2.24.2 Binding the igroup to a portset 21](#_Toc515636141)

[2.24.3 Map Luns 21](#_Toc515636142)

[2.25 User accounts 21](#_Toc515636143)

[2.25.1 Snapdrive account on Storage 21](#_Toc515636144)

[2.25.2 Windadmin Account 22](#_Toc515636145)

[security login role create -role CIFsadmin -cmddirname version -access readonly -vserver <VSERVER> 22](#_Toc515636146)

[2.25.3 Clusterwide snapdrive role and user account 22](#_Toc515636147)

[2.25.4 SMSQL integration 22](#_Toc515636148)

[3 Snapvault Configuration 23](#_Toc515636149)

[3.1 Backup management group and Snapshot name: 23](#_Toc515636150)

[3.2 Backup storage configuration 23](#_Toc515636151)

[3.2.1 7 Days Retention (Used for above example) 25](#_Toc515636152)

[3.2.2 14 Days Retention 26](#_Toc515636153)

[3.2.3 30 Days Retention (Legacy/Exception Only) 26](#_Toc515636154)

[3.2.4 45 Days Retention 27](#_Toc515636155)

[3.3 SnapDrive configuration 28](#_Toc515636156)

[3.4 Snap info configuration 28](#_Toc515636157)

[3.5 Full backup execution 28](#_Toc515636158)

[3.6 Monitoring 29](#_Toc515636159)

[4 Host side settings 31](#_Toc515636160)

[4.1 MPIO 31](#_Toc515636161)

[4.2 ALUA 32](#_Toc515636162)

[4.3 Implementing MPIO and ALUA 33](#_Toc515636163)

[4.3.1 ALUA 33](#_Toc515636164)

[4.3.2 MPIO 33](#_Toc515636165)

[4.3.3 iSCSI initiator on the Windows server 36](#_Toc515636166)

[5 iSCSI setup and configuration 39](#_Toc515636167)

[5.1.1 Enable Microsoft iSCSI Initiator 39](#_Toc515636168)

[5.1.2 Configure iSCSI Target & Storage – POD 39](#_Toc515636169)

[5.1.3 Cluster Configuration – POD & Rack mount systems 39](#_Toc515636170)

[6 WISP requirements 40](#_Toc515636171)

[6.1.1 SQL-2016 supported platform and number of database 42](#_Toc515636172)

[6.1.2 SQL-2016 FSW Config 42](#_Toc515636173)

# Introduction

## Management Summary

This document covers iSCSI implementations on cDOT in TR environments to be used in CIS and CPS.

## Document Scope

The content in this document is intended to provide necessary steps and configuration requirements and layout of iSCSI implementations on cDOT – WIP and WISP.

Microsoft virtual guest are not currently in scope of providing iSCSI storage at this time. This might be revisited later as we expand our scope of the service.

This document also now contains the latest File Share Witness configuration which removes the need for a quorum LUN in ISCSI builds. The additional requirements for CIFS and network interfaces are all documented along with the required account for CIFS share creation.

## Assumptions

The audience is capable of understanding capacity trending and recommendations and intended to be used by Platform and Storage engineers/administrators.

## References

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Document** | **Version** | **Date** | **Author** |
| 1 | [Operational readiness Test Plan](https://theshare.thomsonreuters.com/sites/AI/storwiki/_layouts/WordViewer.aspx?id=/sites/AI/storwiki/Shared%20Documents/Projects/ClusterMode/8040%20OR%20Docs/cDOT%20Test%20Plan%20v2%206.docx&Source=https%3A%2F%2Ftheshare%2Ethomsonreuters%2Ecom%2Fsites%2FAI) | V2.5 | 5th August 2014 | Ian Daniels |
| 2 | [NetApp Solution Deployment Guidelines - cDOT replication](https://theshare.thomsonreuters.com/sites/AI/storwiki/_layouts/WordViewer.aspx?id=/sites/AI/storwiki/Shared%20Documents/Projects/ClusterMode/8040%20OR%20Docs/Thomson%20Reuters%20-%20cDOT%20Replication%20-%20Deployment%20Guidelines%20v4.docx&Source=https%3A) | V4 | May 2014 | Michael Arndt |
| 3 | [NetApp Solution Deployment Guidelines – cDOT Base Configuration](https://theshare.thomsonreuters.com/sites/AI/storwiki/_layouts/WordViewer.aspx?id=/sites/AI/storwiki/Shared%20Documents/Projects/ClusterMode/8040%20OR%20Docs/Thomson%20Reuters%20-%20cDOT%20Base%20Configuration%20-%20Deployment%20Guidelines%20v10.docx&Sourc) | V10 | August 2014 | Michael Arndt |
| 4 | [Arch Log Document](https://theshare.thomsonreuters.com/sites/dco_storage/_layouts/WordViewer.aspx?id=/sites/dco_storage/Projects%20Documents/Engineering%20Projects/INFRASTRUCTURE/TECH%20REFRESH/HDS%20Storage%20Refresh%202013/3.%20Host%20Environment%20Documents/HNAS%20Migrations/Thomson%20Reuters%20-%20Log%20Arch%20Implementation%20Document.docx&DefaultItemOpen=1) | V 1.0 | January 2014 | D&E |
| 5 | CIFS on cDOT | V 1.0 | February 2018 | Adrian Wicks |

## Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Ver** | **Date** | **Author** | **Key Changes** |
| 1.0 | 16th Sept 2014 | Dhiman Chakraborty | Initial Draft version |
| 1.1 | 24th August 2014 | Dhiman Chakraborty | Added changes to failover and high availability scenario in iSCSI for cDOT  Added naming schemes for iSCSI services  Added service accounts and ONTAP accounts requirement for Snap Manager and Snapdrive integration |
| 1.2 | 14th October 2014 | Dhiman Chakraborty | Added LIF naming schemes and other naming standards for iSCSI implementation.  Create qtree for hosting iscsi luns on top of it. |
| 1.3 | 24th October 2014 | Kevin Atkin | Replaced vsadmin account with “iscsi” and “iscsisv” account to keep same standards with 7mode. |
| 1.4 | 9th December | Dhiman Chakraborty | Replaced the vsadmin role with iscsi and iscsisv roles as appropriate. The additional commands required are also attached herewith |
| 1.5 |  | Bipul | Added the Snapvault and QOS configuration and steps |
| 1.6 |  |  | Corrected type from DP to XDP |
| 1.7 |  |  | Added application ssh to iscsi and iscsisv user |
| 1.8 |  | Bipul | Added Bkp Vserver requirement and vserver aggr-list requirement |
| 1.9 | 30-Aug-2017 | Mahesha | Added SQL-2016 supported platform and number of databases |
| 2.0 | 10-19-2017 | Mahesha | Updated the snap autodelete command. |
| 2.1 | 17-11-2017 | Ian Daniel | Updated for witness share config. Reformatted entire document. |
| 2.2 | 20-11-2017 | Ian Daniel | Updated to add reference to Arch Log Document |
| 2.3 | 19-04-2018 | Arpit Roy | Updated creation of Win Powershell user and adding members to BUILTIN\Administrators account for Ontap 8.3 and above. Added reference to CIFS on cDOT document. |
| 2.4 | 01-June\_2018 | Ian Daniel | Updated retention counts for all required retention levels |
| 2.5 | 02-July\_2018 | Ian Daniel | Updated retention counts for all required retention levels in WIP |
|  |  |  |  |

## Distribution List

|  |  |
| --- | --- |
| **Name** | **Role** |
| STO-DE-NAS-CUST | Reviewer |

## Glossary

**WIP –** Windows iSCSI Platform

**WISP –** Windows iSCSI SQL Platform

**iSCSI -** Internet Small Computer System Interface, an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval. The protocol allows clients (called initiators) to send SCSI commands (CDBs) to SCSI storage devices (targets) on remote servers. The iSCSI protocol is configured in Data ONTAP to use **TCP port number 3260**

**IQN -** Internet Qualified Name (iqn) name applies to all iSCSI HBAs and the Microsoft iSCSI Software initiator in the system. The IQN name could be considered similar to the HBA WWN numbers used to map LUNs on the SAN subsystems.

**Initiators –** Client/Server/host initiating iSCSI commands to targets/storage subsystem. TRP will focus on using Microsoft’s iSCSI software initiator rather than 3rd party iSCSI software. Microsoft iSCSI Software Initiator enables you to connect a Windows® host computer to an external iSCSI-based storage array via an Ethernet network adapter

**Target -** An iSCSI target is any device that receives iSCSI commands. The device can be an end node, such as a storage device, or it can be an intermediate device, such as a network bridge between IP and Fibre Channel devices. Each port on the storage array controller or Network Bridge is identified by one or more IP addresses. Phase one of the WISP/WIP target will be NetApp NAS storage however we will continue to evaluate best of breed storage providers to create a competitive and cost effective solutions.

**MPIO -** The Microsoft® Multipath I/O (MPIO) framework helps ensure that your data is available at all times. MPIO supports multiple data paths to storage, improves the fault tolerance of the storage connection, and in some cases, provides greater aggregate throughput by using multiple paths at the same time. This helps improve system and application performance.

**FSW** – File Share Witness – A CIFS share dedicated to a cluster and used in place of a quorum lun for Windows MS SQL Server clusters.

**Port Set –** A port set is a collection of iSCSI LIFs augmented together to serve a customer iSCSI target. Until you create a port set and bind an igroup to this port set, all initiators in the port set can access any LUN in a vserver. The port sets are used in conjunction with igroups to further limit which LIFs an initiator can use to access the designated LUNs.

For example, without a portset, initiator1 can access LUN1 over any LIF as shown below



The access can be limited by implementing port sets. Initiator1 cannot access LUN1 through LIF2 because it is not added to the portset.



**SnapDrive -**

SnapDrive software integrates with Windows Volume Manager so that storage systems can serve as virtual storage devices for application data in Windows Server 2008 and Windows Server 2012 environments. SnapDrive manages LUNs on a storage system, making these LUNs available as local disks on Windows hosts. This allows Windows hosts to interact with the LUNs just as if they belonged to a directly attached redundant array of independent disks (RAID).

SnapDrive provides the following additional features:

* It enables online storage configuration, LUN expansion, and streamlined management.
* It enables connection of up to 255 LUNs.
* It integrates Data ONTAP Snapshot technology, which creates point-in-time images of data stored on LUNs.
* It works in conjunction with SnapMirror software to facilitate disaster recovery from either asynchronously or synchronously mirrored destination volumes.
* It enables SnapVault updates of qtrees to a SnapVault destination.
* It enables management of SnapDrive on multiple hosts.
* It enables support on Microsoft cluster configurations.
* It enables iSCSI session management.

**SnapManager for SQL**

SnapManager provides rapid online backup and near-instantaneous restoration of databases by using online Snapshot technology that is part of the Data ONTAP® software. SnapManager can also leverage the SnapMirror capabilities of storage systems to provide onsite or offsite SnapManager backup set mirroring for disaster recovery.

Data management: SnapManager supports the following data management capabilities:

* Migrating databases and transaction logs to LUNs or VMDKs on storage systems
* Backing up databases and transaction logs from LUNs and VMDKs on storage systems
* Verifying the backed-up databases and transaction logs
* Managing the SnapManager backup sets
* Restoring databases and transaction logs from previously created SnapManager backup sets

You can also create and restore database from remote backups at a remote location through dataset and SnapVault integration to SnapManager.

**VSS – Microsoft Volume Shadow Copy Service –**

SnapDrive and SnapManager for SQL use VSS provider to coordinate backups. During the operation it is important to understand how the service requestor, SnapDrive and SMSQL, integrate with VSS to perform a backup of the volume. SnapDrive and SnapManager for SQL will call VSS to determine at what point in time the data at rest can be snapped. During the time the snapshot occurs there will be a pause in “write” I/O operations for up to 10 seconds however all read I/O requests will continue normal operations. If the snapshot does not occur in 10 seconds SnapDrive and SnapManager for SQL will request VSS unfreeze I/O operations to prevent any application failures or data loss from occurring. If SnapDrive and SnapManager for SQL fail to communicate with the VSS provider VSS will resume I/O after 60 seconds. Additional information can be found below.

[**http://technet.microsoft.com/en-us/library/ee923636(WS.10).aspx**](http://technet.microsoft.com/en-us/library/ee923636(WS.10).aspx)

# Understanding the components of iSCSI service

## Vserver

The Vserver provides the iSCSI target and owns the iSCSI LUN and its containing volume. The logical interfaces (LIFs) that provide paths to the LUN are owned by the vserver. A vserver can always be managed by cluster administrator.

## LIF

A LIF (logical interface) is an IP address with associated characteristics, such as a role, a home port, a home node, a routing group, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network. LIFs can be hosted on the following ports:

• Physical ports that are not part of interface groups

• Interface groups

• VLANs

• Physical ports or interface groups that host VLANs

### LIF roles

There are different roles for the LIFs. They can be categorized as:

**Node management LIF**

This provides dedicated IP address for managing a particular node; commonly use for the node’s system management.

**Cluster Management LIF**

This LIF provides a single management interface for managing the whole cluster.

**Cluster LIF**

This IP address is used for inter-cluster traffic communication.

**SAN Data LIF**

This IP address (dedicated) is associated with a vserver and is used by clients to access data from storage. This will be used by iSCSI clients to connect to the storage targets

**NAS Data LIF (Optional)**

This additional Data LIF is used by CIFS for a FSW when using clustering.

**Vserver Management LIF**

This is a mandatory LIF for iSCSI implementations using Snap managers (Snapdrive and SMSQL). The vserver management LIF allows Snap manager to communicate with other LIF to serve data when primary LIF goes inactive.

The management LIF must have the same DNS name as the SVM. Set the management LIF role to data, the protocol to none, and the firewall policy to mgmt.

**Intercluster LIF**

This is used for intercluster communication. This is out of scope for this document.

The following defines the different characteristics of the LIFs defined above.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Data LIF** | **Cluster LIF** | **Node-Management LIF** | **Cluster Management LIF** | **Intercluster LIF** |
| **Primary traffic types** | NFS server, CIFS server, NIS client, Active Directory, LDAP, WINS,  DNS client and server, iSCSI and FC server | Intracluster | SSH server, HTTPS server, NTP client, SNMP, Autosupport client, DNS client, loading code updates | SSH server, HTTPS server | Cross-cluster replication |
| **Compatible with port roles** | Data | Cluster | Node-management, data | Data | Intercluster, data |
| **Compatible with port types** | All | No interface group or VLAN | All | All | All |
| **Additional notes** | SAN LIFs do not support failover. Firewall profile for data LIFs on non-iSCSI servers will be modified to enable management over data LIF. For a FSW enabled ISCSI vserver we have to have an additional data LIF supporting CIFS. | Unauthenticated, unencrypted, essentially and internal Ethernet "bus" of the cluster. All network ports in the cluster role in a cluster. | In new node-management LIFs, the default value of the use-failover group parameter is disabled. The use-failover-group parameter can be set to either system-defined or enabled. |  | Traffic flowing over intercluster LIF is not encrypted. |

**Note**

It is recommended to have the following LIFs per ISCSI vserver:

* Two SAN Data LIFs
* One Management LIF
* One NAS Data LIF for CIFS FSW (Optional – Used for clustering)
* Intercluster LIFs (for replication)

### Limitations

iSCSI LIFs comes with certain limitations. The following limitations are only centered on iSCSI solution:

* iSCSI LIFs cannot co-exist with any other protocols
* NAS and SAN cannot co-exist on the same LIF
* The “firewall policy” option associated with a LIF is defaulted to the role of the LIF except for a vserver management LIF.
* Avoid configuring LIFs with addresses in the 192.168.1/24 and 192.168.2/24 subnets. Doing so might cause the LIFs to conflict with the private iWARP interfaces and prevent the LIFs from coming online after a node reboot or LIF migration
* An iSCSI LIF cannot be failed over! Initiators **must** use MPIO and ALUA for failover capability for Cluster-Mode in an iSCSI SAN environment.

## High availability

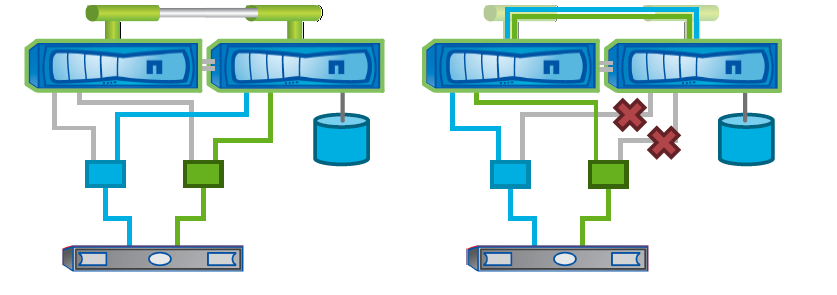
cDOT does not support failover for iSCSI LIFs. An iSCSI service is made redundant through a combination of procedures on the end host (MPIO) and storage target (ALUA and vserver management LIF).

MPIO and ALUA provide multipathing to the storage targets, and a management LIF on the vserver provides Snap Managers to communicate with other LIFs to serve data.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Data LIF** | **Cluster LIF** | **Node-Management LIF** | **Cluster Management LIF** | **Intercluster LIF** | **vserver Management LIF** |
| **Primary traffic types** | Includes all data ports on home node as well as one alternate node | Must stay on node and uses any available cluster port | Default is none, must stay on the same port on the node | Default is failover group of all data ports in the entire cluster | Must stay on node, uses any available intercluster port. | Allows snap manager(s) to communicate with other LIFs to serve data. |
| **Is Customizable** | Yes | Yes | Yes | Yes | Yes | Yes |

In cDOT, one node owns the LUN, but ports on two or more nodes may provide access (all the paths may not be optimized). Traffic for paths that are terminated at another node traverses the 10GB Ethernet interconnect network. The following illustrates direct and indirect paths in a two-node cluster; the colored lines are the paths over which data traffic flows.

1. Figure 1 Path failover cDOT



For node failover, there are different failover groups that are configured when the actual hardware installation happens and is covered in the [base configuration](#_References), the following groups are configured for different facets of failover as shown below:

🡺 Truncated o/p to only show the features (these are covered in detail in the base configuration)

eag-nasor-clus1::> failover-groups show

Failover

Group Node Port

------------------- ----------------- ----------

clusterwide

eag-nasor-clus1-8040HT-01

e0i

eag-nasor-clus1-8040HT-01

e0j

eag-nasor-clus1-8040HT-01

e0k

eag-nasor-clus1-8040HT-01

e0l

data-2001

eag-nasor-clus1-8040LT-04

a0a-2001

eag-nasor-clus1-8040LT-03

a0a-2001

eag-nasor-clus1-8040HT-02

a0a-2001

eag-nasor-clus1-8040HT-01

a0a-2001

data-2003

eag-nasor-clus1-8040LT-04

a0a-2003

eag-nasor-clus1-8040LT-03

a0a-2003

eag-nasor-clus1-8040HT-02

a0a-2003

Failover

Group Node Port

------------------- ----------------- ----------

data-2003

eag-nasor-clus1-8040HT-01

a0a-2003

mgmt

eag-nasor-clus1-8040LT-04

e0i

eag-nasor-clus1-8040LT-03

e0i

eag-nasor-clus1-8040HT-02

e0i

eag-nasor-clus1-8040HT-01

e0i

39 entries were displayed.

**Naming conventions**

## iGroups

For iSCSI iGroups the naming convention will be as follows:

**ig-<vserver\_name>-<count>**

For example, if the vserver name is iscsi-vm-01, igroup name would be as follows

**ig-iscsi-vm-01-01**

## vserver naming

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VSERVER NAME** | | | | | |
| SITE/LOCATION | CLUSTER NAME | | **VSERVER** | **TYPE** | **EXAMPLE** |
|  |  |  |
| Eagan | EG-CPS-CLSH-E01 | EG-CIS-CLSH-F01 | **EG-CPS-CLSH-E01**   **EG-CIS-CLSH-E01** | ADMIN |  |
| **EG-CIS-CLSH-E01-N01**  **EG-CPS-CLSH-E01-N02** | NODE |  |
| <GRP><TECH>-<SiteID>XXXX | DATA (Shared/Dedicated) | cpsprod-e0117  cisprod-h0049 |
| cisclnt-e0342 |
| cisded-f0197 |
| Limerick | LM-CPS-CL**AA-**M01 | LM-CIS-CL**AA-**M01 | <GRP><DataBaseType>-<SiteID>XXXX | DATA  (Archive) | cpsoracle-m0391  cismssql-m0073  cismysql-m0108 |
| DTC | DT-CPS-CL**BK-D**01 | DT-CIS-CL**BK-D**01 | <GRP>SS-CLBK-<SiteID>XX  (SS=same-site backups) | DATA  (Backup) | cps-ss-clbk-d01  cis-ss-clbk-d02 |
| <GRP>CS-CLBK-<SiteID>XX  (CS=cross-site backups) | cis-cs-clbk-d01  cps-cs-clbk-d02 |

**CPSPROD**-**F**0129 **CISCLNT**-**D**0186 **CISPROD**-**E**0129 **CPSORACLE**-**M**0004 **CISMSSQL**-**H**0084

**Site ID Site ID Site ID Site ID Site ID**

**Production**   **Client**  **Production Oracle DB MSSQL DB**

**Group**  **Group Group Group Group**

**Where,**

**CIS/CPS**  🡪 DCO group identifier

**PROD/CLNT/ORACLE/MSSQL** 🡪 Vserver Purpose/Use

**D/E/F/H/M** 🡪 Site identifier

XXXX 🡪 Vserver reserve number from Zipper

Datacenter Site Identifiers are a single alphabet character that corresponds to a physical city/datacenter. This can be found on Sharepoint for anyone unfamiliar with the SiteID relationships:

<https://theshare.thomsonreuters.com/sites/ie/storage/Lists/DC%20Addresses%20and%20Contacts/Main.aspx>

CIFS vserver names will be identical to vserver naming as all vservers that will utilize CIFS are less than 15 characters long.

## Data/ISCSI LIF Naming

Most of the times the lif names will be same as vserver name and the only addition is to add the ‘-lif-<count>’ at the end of the vserver name. This applies for all Data LIF’s,

For example,

**CISPROD**-**E**0129

Vserver name : <Group><VserverPurpose>-<SiteID>####

Then the Lif name will be like this,

<Group><VserverPurpose>-<SiteID>####-LIF-01

Example, **CISPROD**-**E**0129-LIF-01 or **CPSPROD**-**F**0276-LIF-01

## Management LIF

Please note that Snapmanagers need the same vserver name for identifying storage target from host. Henceforth, the management LIF associated to the vserver will carry the same name as that of the vserver.

For instance, in this document the vserver name is iscsi-vm-01 hence, the management LIF will also be named as **iscsi-vm-01**

## Portsets

The portsets will be named as

<vserver\_name>-port-<count>

For example, if the vserver name is iscsi-vm-01, the corresponding portset name would be:

iscsi-vm-01-port-01

For further details, please follow the C-mode\_namings\_v0.8 document.

## QOS

In the TR shared storage environment, QOS policies with specific rate limits will be configured on all volumes. One QOS policy group will be configured per Vvolume, and the policy group will be named the same as the Volume name. The QOS policy group will be applied on each Volume

For dedicated storage environments at TR, QOS policies should still be configured in the same manner as the shared environment, with the one difference being that the policy group can be set without a throughput limit. This is done in order to utilize the QOS latency statistics.ISCSI configuration and provisioning overview

When storage is made available to hosts using iSCSI, you actually provision a volume and LUN on a vserver and then connect the LUN from the host.



**Resource Information**

**The following resources are used for ISCSI testing**

|  |  |  |  |
| --- | --- | --- | --- |
| **Host Information** | | | |
| **Windows VM** | **IP address** | **Subnet** | **Network** |
| orf-iscsi-01 | 10.220.177.182 | 255.255.255.0 | 10.220.177.0 |
| orf-iscsi-02 | 10.220.177.183 | 255.255.255.0 | 10.220.177.0 |

|  |  |  |
| --- | --- | --- |
| **Storage Information** | | |
| iGroup Name | igrp\_test\_iscsi |  |
| SVM (vserver) | iscsi-vm-01 |  |
| Data LIF 1 | iscsi-vm-01-lif | 10.220.181.34/25 |
| Vserver mgmt LIF 1 | iscsi-vm-01 | 10.220.181.35/25 |
| Portset | iscsi-vm-01-port-01 |  |
| Portset members | iscsi-vm-01-lif |  |

**The following resources are used for ISCSI testing with FSW**

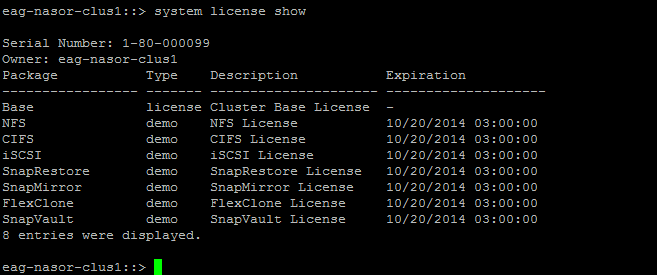
|  |  |  |
| --- | --- | --- |
| **Clustered Storage Information** | | |
| iGroup Name | ig-silab-mssql-01-01  ig-silab-mssql-01-02  ig-silab-mssql-01-03  ig-silab-mssql-01-04  ig-silab-mssql-01-05  ig-silab-mssql-01-06  ig-silab-mssql-01-07  ig-silab-mssql-01-08 |  |
| SVM (vserver) | silab-mssql-01 |  |
| Data LIF 1 | silab-mssql-01-lif01 | 10.220.181.70/25 |
| Data LIF 2 | silab-mssql-01-lif01 | 10.220.181.74/25 |
| Data LIF 3 (CIFS FSW) | silab-mssql-01-lif01 | 10.220.181.84/25 |
| Vserver mgmt LIF 1 | silab-mssql-01-mgmt-lif01 | 10.220.181.58/25 |
| Portset | silab-mssql-01-port-01 |  |
| Portset members | silab-mssql-01-lif01, silab-mssql-01-lif02 |  |

It is assumed here that aggregate for containing root volume and data volume are already in place and created as per TR standards.

## Licenses

Add iSCSI license

license add -license-code <code>



## Create vserver

vserver create -vserver iscsi-vm-01 -rootvolume iscsi-vm-01\_rootvol -aggregate aggr1\_data\_sas600\_flash\_n01 -ns-switch file -rootvolume-security-style ntfs

There will be dedicated bkp vserver for iscsi setup , It will have identical setup as primary (one mgmt lif and two data lif with iSCSI protocol only)

## Enable iSCSI protocol

eag-nasor-clus1::> vserver iscsi create -vserver iscsi-vm-01 -target-alias iscsi-vm-01 -status up

## Allow protocols (CIFS for FSW)

eag-nasor-clus1::> vserver modify -vserver iscsi-vm-01 -allowed-protocols iscsi, cifs

## Check the vserver status

eag-nasor-clus1::> vserver iscsi show

Target Target Status

Vserver Name Alias Admin

---------- -------------------------------- ---------------------------- ------

iscsi-vm-01

iqn.1992-08.com.netapp:sn.5448664a401711e4a02d123478563412:vs.16

iscsi-vm-01 up

## Create LIFs

### SAN Data LIF(s)

We are creating two SAN data LIFs here for redundancy, one LIF needs to be created on each node of a HA pair.

eag-nasor-clus1::> network interface create -vserver iscsi-vm-01 -lif iscsi-vm-01-lif01 -role data -data-protocol iscsi -home-node eag-nasor-clus1-8040LT-03 -home-port a0a-2003 -address 10.220.181.34 -netmask 255.255.255.128 -status-admin up

eag-nasor-clus1::> network interface create -vserver iscsi-vm-01 -lif iscsi-vm-01-lif02 -role data -data-protocol iscsi -home-node eag-nasor-clus1-8040LT-04 -home-port a0a-2003 -address 10.220.181.35 -netmask 255.255.255.128 -status-admin up

Enable iSCSI on the data LIF(s) using the following command:

eag-nasor-clus1::> iscsi interface enable -vserver iscsi-vm-01 -lif iscsi-vm-01-lif01

eag-nasor-clus1::> iscsi interface enable -vserver iscsi-vm-01 -lif iscsi-vm-01-lif02

### CIFS Data LIF (For FSW Support)

We create an additional CIFS capable Data LIF to enable us to support a FSW share when provisioning for a cluster.

eag-nasor-clus1::> network interface create -vserver iscsi-vm-01 -lif iscsi-vm-02-lif03 -role data -data-protocol cifs -home-node eag-nasor-clus1-8040LT-04 -home-port a0a-2003 -address 10.220.181.37 -netmask 255.255.255.128 -status-admin up

### Vserver Management LIF

Create a vserver management LIF. Please note here

1. To set the firewall policy to mgmt
2. To set the LIF data protocol set to “**none**”:
3. To ensure the management LIF is named the same as the vServer in DNS. The data management LIF resolving the vserver name is important for other tool recognition like the Snap Manager(s).
4. To ensure the vserver is properly added to either DNS or local hosts file (in all the constituents of the service, in case of a host file).

::> network interface create -vserver <vserver\_name> -lif <lif\_name> -role data -data-protocol none -home-node <node\_name> -home-port <port\_name> -address xx.xx.xx.xx -netmask xx.xx.xx.xx -status-admin up -firewall-policy mgmt -failover-group <failover-group>

**Example**

network interface create -vserver iscsi-vm-01 -lif iscsi-vm-01-mgmt-lif-01 -role data -data-protocol none -home-node eag-nasor-clus1-8040LT-04 -home-port a0a-2003 -address 10.220.181.36 -netmask 255.255.255.128 -status-admin up -firewall-policy mgmt

### Vserver management failover group for management

This is not the actual management failover group, but a group for managing iSCSI vserver. Create failover group for redundancy with the following command if it’s not already created:

eag-nasor-clus1::> failover-groups create -failover-group data-2003 -node eag-nasor-clus1-8040LT-04 -port a0a-2003

eag-nasor-clus1::> failover-groups create -failover-group data-2003 -node eag-nasor-clus1-8040LT-03 -port a0a-2003

## Routing

In case you have separate routing for iSCSI, you can use the following command to facilitate the same

network routing-groups route create -vserver <vserver\_name> -routing-group d<iscsi\_network> -destination 0.0.0.0/0 -gateway <gateway\_IP>

**Example:**

network routing-groups route create -vserver iscsi-vm-01 -routing-group d10.220.181.0/25 -destination 0.0.0.0/0 -gateway 10.220.181.126

## Create portsets

Please note that we are yet to create igroups and associate these to the igroup

eag-nasor-clus1::> lun portset create -vserver iscsi-vm-01 -portset iscsi-vm-01-port-01 -protocol iscsi -port-name iscsi-vm-01-lif

eag-nasor-clus1::> lun portset show -vserver iscsi-vm-01

Vserver Portset Protocol Port Names Igroups

--------- ------------ -------- ----------------------- ------------

iscsi-vm-01

iscsi\_vm\_01\_port

iscsi iscsi-vm-01-lif ig-iscsi-vm-01-01

Use the following command to verify the default route for each SVM (vserver)

eag-nasor-clus1::> network routing-groups route show -vserver iscsi-vm-01

Use the following command to verify LIF connectivity

eag-nasor-clus1::> network interface show -vserver iscsi-vm-01

Logical Status Network Current Current Is

Vserver Interface Admin/Oper Address/Mask Node Port Home

----------- ---------- ---------- ------------------ ------------- ------- ----

iscsi-vm-01

iscsi-vm-01-lif02

up/up 10.220.181.35/25 eag-nasor-clus1-8040LT-04

a0a-2003

true

iscsi-vm-01-lif01

up/up 10.220.181.34/25 eag-nasor-clus1-8040LT-03

a0a-2003

true

2 entries were displayed.

eag-nasor-clus1::>

## Create CIFS Server If Using FSW

You will need to setup CIFS in the relevant domain and also add permissions for the Windows team to create a share (winadmin account)

cifs server create -vserver <vsname> -cifs-server <CIFS\_Name> -domain <Domain\_Name> -ou ou=<OU\_NAME>,ou=<OU\_NAME>,ou=<OU\_NAME>

cifs server show

## Create data volume(s) and QoS Configuration

Create data volumes for service iSCSI data. Please note here to identify beforehand, the types of volumes available available, they can be thin provisioned or with a space guarantee of volume. In the example below, we have used space guarantee of “volume”

**eag-nasor-clus1::> volume create -vserver iscsi-vm-01 -volume iscsi\_vol01 -aggregate aggr1\_data\_bsas2000\_n04 -size 10GB -state online -type RW -space-guarantee** NONE

**In TR, the space guarantee will be set to “none”**

**Along with the allocated there is additional headroom required , Use below guidelines**

**0GB – 1024GB = 5GB-6GB**

**1025GB – 2048GB = 10GB**

**2049GB – 3072GB = 15GB**

**Create QoS policy group and apply it at the volume level**

**eag-nasor-clus1::> qos policy-group create -policy-group iscsi\_vol01 –vserver iscsi-vm-01 -max-throughput 6000IO**

**eag-nasor-clus1::>** volume modify **–vserver iscsi-vm-01 -volume iscsi\_vol01** -qos-policy-group **iscsi\_vol01**

## Backup and snapshots

Please use the following command to setup snapshot type. In the example below, the fractional reserve is set to none or “0”.

The snapshot reserve is set to 50 for volumes hosting iSCSI data.

eag-nasor-clus1::> volume modify -volume iscsi\_vol01 -vserver iscsi-vm-01 -percent-snapshot-space 50 -snapshot-policy none -fractional-reserve 0

## Snapshot Autodelete Policies

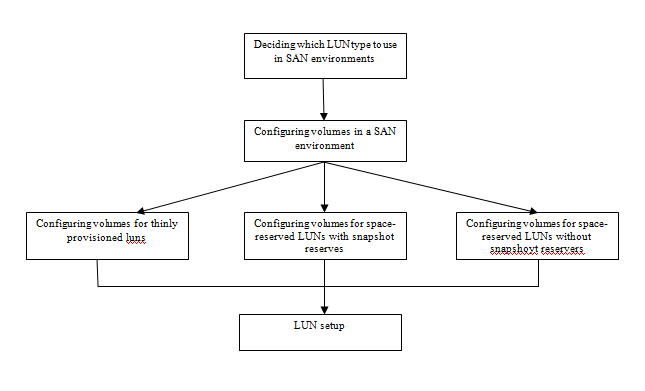
eg-si-clsn-e01::> snap autodelete modify -vserver orprod-iscsi-01 -volume cb0000\_wi\_15142\_07\_usr\_snap -enabled true -commitment try -target-free-space 20% -trigger snap\_reserve

## Create Qtree

eag-nasor-clus1::> qtree create /vol/cb0000\_wi\_15142\_07\_usr\_snap/luns -vserver orprod-iscsi-01 -security-style

## Create LUNs

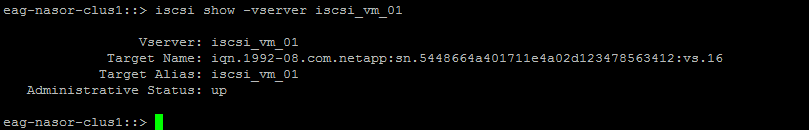
Use the following logic to select specific LUN type



Create data LUN with the following command

eag-nasor-clus1::> lun create -path /vol/iscsi\_vol01/luns/test\_lun\_01 -vserver iscsi-vm-01 -size 1024MB -ostype windows\_2008 -space-reserve enabled

Please check the iSCSI service status on the SVM (vserver) as shown below:



If the service has not started please start using the following command:

eag-nasor-clus1::> iscsi start -vserver iscsi-vm-01

## iGroups and Mapping

Create an igroup named “igrp\_test\_iscsi”

eag-nasor-clus1::> igroup create igrp\_test\_iscsi -protocol iscsi -ostype windows -vserver iscsi-vm-01

### Add the iSCSI IQNs from server(s)

Use the following command to add iSCSI hosts to the storage target igroup.

eag-nasor-clus1::> igroup add -vserver iscsi-vm-01 -igroup igrp\_test\_iscsi -initiator iqn.1991-05.com.microsoft:orf-iscsi-01.tlr.thomson.com

**Note:** ALUA is enabled by default

eag-nasor-clus1::> igroup show -v igrp\_test\_iscsi

Vserver Name: iscsi-vm-01

Igroup Name: igrp\_test\_iscsi

Protocol: iscsi

OS Type: windows

Portset Binding Igroup: -

Igroup UUID: f223769d-4256-11e4-a02d-123478563412

ALUA: true

Initiators: iqn.1991-05.com.microsoft:orf-iscsi-01.tlr.thomson.com (not logged in)

In case you need to set this up manually please use the following command:

eag-nasor-clus1::> igroup set -vserver iscsi-vm-01 -igroup igrp\_test\_iscsi alua true

### Binding the igroup to a portset

Bind the igroup to the portset created earlier

eag-nasor-clus1::> lun igroup bind -vserver iscsi-vm-01 -igroup igrp\_test\_iscsi -portset iscsi-vm-01-port-01

### Map Luns

eag-nasor-clus1::lun igroup bind -vserver iscsi-vm-01 -igroup igrp-vm6 -portset orprod-iscsi-01-port-01

eag-nasor-clus1::> lun map -vserver iscsi-vm-01 -path /vol/iscsi\_vol01/luns/test\_lun\_01 -igroup igrp\_test\_iscsi

## User accounts

Snapdrive must have a local account on the vserver to execute various Ontap API commands and to retrieve system information. Snap drive requires two accounts

* One with admin level rights to the iSCSI vserver ( default account name is vsadmin)
* One with specific permissions to the admin vserver for cluster wide operations, such as SnapMirror and licenses

Note: Please note that Ontap API user should also have SSH access via public key to vserver and mgmt LIF

### Snapdrive account on Storage

Create “iscsi” and “iscsisv” accounts for backup and snapdrive integration

**On primary vserver, create the iscsi user**

eag-nasor-clus1::> sec login create -username iscsi -application ontapi -authmethod password -role iscsi -vserver orprod-iscsi-01

security login modify -username iscsi -application ontapi -authmethod password -role vsadmin -vserver orprod-iscsi-01

eag-nasor-clus1::> sec login create -username iscsi -application ssh -authmethod password -role iscsi -vserver orprod-iscsi-01

**On backup vserver, create the iscsisv user**

eag-nasor-clus1::> sec login create -username iscsisv -application ontapi -authmethod password -role iscsisv -vserver orprod-iscsi-01

sec login modify -username iscsisv -application ontapi -authmethod password -role vsadmin -vserver orprod-iscsi-01

eag-nasor-clus1::> sec login create -username iscsisv -application ssh -authmethod password -role iscsisv -vserver orprod-iscsi-01

**Note:** While installing snapdrive, please use the IP address of the management LIF on the clients/hosts where snapdrive is being installed.

### Windadmin Account

## security login role create -role CIFsadmin -cmddirname version -access readonly -vserver <VSERVER>

security login role create -role CIFsadmin-cmddirname vserver  -access readonly -vserver <VSERVER>

security login role create -role CIFsadmin-cmddirname "vserver cifs share" -access all -vserver <VSERVER>

security login role create -role CIFsadmin-cmddirname "vserver cifs users-and-groups" -access all -vserver <VSERVER>

sec login create -username winadmin -application ontapi -authmethod password -role CIFsadmin-vserver <VSERVER>

**For OnTap 8.3 and above please add the following to the BUILTIN\ADMINISTRATORS group MGMT\m-EaganServerAdmins and TEN\m-EaganServerAdmins.**

vserver cifs users-and-groups local-group add-members -vserver <VSERVER> -group-name BUILTIN\Administrators -member-names mgmt\m-EaganServerAdmins

vserver cifs users-and-groups local-group add-members -vserver <VSERVER> -group-name BUILTIN\Administrators -member-names ten\m-EaganServerAdmins

security login create –vserver <VSERVER> -user-or-group-name mgmt\REST-SSSE-Windows-Engineering-ServerAdmins -application ontapi -authentication-method domain -role CIFsadmin

security login create –vserver <VSERVER> -user-or-group-name mgmt\m-eaganserveradmins -application ontapi -authentication-method domain -role CIFsadmin

### Clusterwide snapdrive role and user account

The admin veserver provides admin access to the cluster.

::> security login role show -vserver <admin vservername> -role <snapdrive role name>

### SMSQL integration

The SMSQL application must be assigned the admin role access to the Data ONTAP clusters at the primary and backup nodes, and the iscsi role to access the cluster vserver at the primary site for ONTAPI integration.

|  |  |  |
| --- | --- | --- |
| Credentials | vserver iscsi user password | vsm\_mt\_password |
| Customer ONTAPI (service account)user name | api\_user |
| Customer ONTAPI password (domain user) | api\_password |
| Customer ONTAPI account role | Iscsi |

Further references available [here](#_WISP_requirements)

#### Creating the user and roles and group

Create iscsi and iscsisv roles on both backup and primary nodes/vservers

**Syntax**

sec login role create –role iscsi -cmddirname <command\_directory> -access <access type> -query "" -vserver <vserver\_name>

The list of all commands that needs to be run for the role are included here



# Snapvault Configuration

We will be using SMSQL 7.1 archiving option to vault the snaps to secondary filer’s. In Cluster mode we have snapmirror type XDP to represent snapvault.

We will be backing up two Lun’s

1. UserDB and Uerlog (i.e \*\_usr\_snap)
2. Snap info (i.e \*\_ info\_snap)

There will be no storage side scheduled backup , Database will take daily hot backup with help of SMSQL via sql job

## Backup management group and Snapshot name:

The backup management group will be standard which will make the snapshot format as below

sql<snap/info>\_\_<servername>\_<time stramp>

Example :

sqlsnap\_\_orf-id346-05\_01-08-2015\_04.52.57

sqlinfo\_\_orf-id346-05\_01-08-2015\_04.52.57

## Backup storage configuration

The backup vserver will be dedicated to iSCSI. It will have one mgmt lif and at-least one iscsi (only)lif.

vserver create -vserver or-ss-clbk-e01 -rootvolume or\_ss\_clbk\_e01\_rootvol -aggregate aggr1\_data\_sas600\_flash\_n01 -ns-switch file -rootvolume-security-style ntfs

It should be peered with source vserver like standard XDP relations

The backup volume name will be as per standard and have the retention in the volume name. The following Table details retentions and ensures we retain the correct number of snapshots for each required retention level.

**WISP Retention**

|  |  |  |
| --- | --- | --- |
| Retention Specified In Volume Name | Retention Count | Retention Policy Name |
| 7 | 35 | XDP\_iscsi\_7 |
| 14 | 70 | XDP\_iscsi\_14 |
| 30 | 150 | XDP\_iscsi\_30 |
| 45 | 225 | XDP\_iscsi\_45 |

i.e : sv\_14\_or\_wi\_8040\_vm5\_info\_snap , all the volume related parameters will be same as of LION snapvault setup..

The backup vserver will have a mgmt-lif with data protocol set to none for snap drive usage.

It will also have an iSCSI LIF with data protocol assigned to iSCSI

Below is a example snapvault setup configuration for iSCSI

|  |  |
| --- | --- |
| **Source vserver** | cisprod-e0041 |
| **Source volumes** | or\_wi\_8040\_vm5\_usr\_snap, or\_wi\_8040\_vm5\_info\_snap |
| **Retention** | 7 Days |
| **Destination vserver** | or-ss-clbk-e01 |

We created or-ss-clbk-e01\_lif\_01 for vserver or-ss-clbk-e01, which will be used for iscsi (snap drive)

Create Mgmt LIF

Syntex :

network interface create -vserver <vserver\_name> -lif <lif\_name> -role data -data-protocol none -home-node <node\_name> -home-port <port\_name> -address xx.xx.xx.xx -netmask xx.xx.xx.xx -status-admin up -firewall-policy mgmt

network interface create -vserver or-ss-clbk-e01 -lif or-ss-clbk-e01-mgmt-lif -role data -data-protocol none -home-node eag-nasor-clus2-8040bkp-01 -home-port a0a-2003 -address 10.220.181.27 -netmask 255.255.255.128 -status-admin up -firewall-policy mgmt

**Create Data LIF(s)**

We will create another lif with data protocol as iscsi for the iSCSI lif

For example:

network interface create -vserver or-ss-clbk-e01 -lif or-ss-clbk-e01-lif-01 -role data -data-protocol iscsi -home-node eag-nasor-clus2-8040bkp-01 -home-port a0a-2003 -address 10.220.181.28 -netmask 255.255.255.128 -status-admin up

Portset creation is similar to primary iSCSI vserver.

1. Create volume with type DP

volume create -vserver or-ss-clbk-e01 -volume sv\_7\_or\_wi\_8040\_vm5\_usr\_snap -aggregate aggr1\_data\_msata4000\_n01 -size 160GB -state online -type DP -space-guarantee NONE

volume create -vserver or-ss-clbk-e01 -volume sv\_7\_or\_wi\_8040\_vm5\_info\_snap -aggregate aggr1\_data\_msata4000\_n01 -size 21GB -state online -type DP -space-guarantee NONE

All other parameters will be same as standard backup volume

1. Create snapmirror relation and initiate baseline

Snapmirror create -source-path cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_usr\_snap –type XDP

Snapmirror create -source-path cisprod-e0041:or\_wi\_8040\_vm5\_info\_snap -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_info\_snap –type XDP

Snasnapmirror initialize -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_info\_snap

Snasnapmirror initialize -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_usr\_snap

1. We have to create a snapmirror policy with retention and snapmirror label Daily. This snapmirror label will be used in snapmanager configuration.

### 7 Days Retention (Used for above example)

snapmirror policy create -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_7

snapmirror policy add-rule -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_7 -snapmirror-label daily -keep 35

snapmirror modify -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_usr\_snap -policy XDP\_iscsi\_7

snapmirror modify -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_info\_snap -policy XDP\_iscsi\_7

snapmirror show -destination-path or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_usr\_snap -fields policy

source-path destination-path policy

------------------------------------- -------------------------------------------- ----------

cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap or-ss-clbk-e01:sv\_7\_or\_wi\_8040\_vm5\_usr\_snap XDP\_iSCSI\_7

### 14 Days Retention

snapmirror policy create -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_14

snapmirror policy add-rule -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_14 -snapmirror-label daily -keep 70

snapmirror modify -destination-path or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_usr\_snap -policy XDP\_iscsi\_14

snapmirror modify -destination-path or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_info\_snap -policy XDP\_iscsi\_14

snapmirror show -destination-path or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_usr\_snap -fields policy

source-path destination-path policy

------------------------------------- -------------------------------------------- ----------

cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_usr\_snap XDP\_iSCSI\_14

### 30 Days Retention (Legacy/Exception Only)

snapmirror policy create -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_30

snapmirror policy add-rule -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_30 -snapmirror-label daily -keep 150

snapmirror modify -destination-path or-ss-clbk-e01:sv\_30\_or\_wi\_8040\_vm5\_usr\_snap -policy XDP\_iscsi\_30

snapmirror modify -destination-path or-ss-clbk-e01:sv\_30\_or\_wi\_8040\_vm5\_info\_snap -policy XDP\_iscsi\_30

snapmirror show -destination-path or-ss-clbk-e01:sv\_30\_or\_wi\_8040\_vm5\_usr\_snap -fields policy

source-path destination-path policy

------------------------------------- -------------------------------------------- ----------

cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap or-ss-clbk-e01:sv\_30\_or\_wi\_8040\_vm5\_usr\_snap XDP\_iSCSI\_30

### 45 Days Retention

snapmirror policy create -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_45

snapmirror policy add-rule -vserver or-ss-clbk-e01 -policy XDP\_iscsi\_45 -snapmirror-label daily -keep 225

snapmirror modify -destination-path or-ss-clbk-e01:sv\_45\_or\_wi\_8040\_vm5\_usr\_snap -policy XDP\_iscsi\_45

snapmirror modify -destination-path or-ss-clbk-e01:sv\_45\_or\_wi\_8040\_vm5\_info\_snap -policy XDP\_iscsi\_45

snapmirror show -destination-path or-ss-clbk-e01:sv\_45\_or\_wi\_8040\_vm5\_usr\_snap -fields policy

source-path destination-path policy

------------------------------------- -------------------------------------------- ----------

cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap or-ss-clbk-e01:sv\_45\_or\_wi\_8040\_vm5\_usr\_snap XDP\_iSCSI\_45

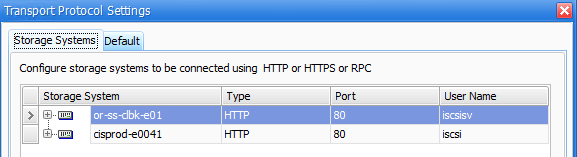
**WIP Retentions (Single SnapShot)**

|  |  |  |
| --- | --- | --- |
| Retention Specified In Volume Name | Retention Count | Retention Policy Name |
| 7 | 7 | XDP\_iscsi\_7\_1 |
| 14 | 14 | XDP\_iscsi\_14\_1 |
| 30 | 30 | XDP\_iscsi\_30\_1 |
| 45 | 45 | XDP\_iscsi\_45\_1 |

These retentions are used solely for WIP deployments .. the commands are the same but the number of snapshots is always 1. Also, for WIP, the snapmirror label is 'snapvault' as opposed to 'Daily' which is used for WISP.

## SnapDrive configuration

We have to add the backup vserver in snap drive on DB server with standard user iscsisv over http protocol



## Snap info configuration

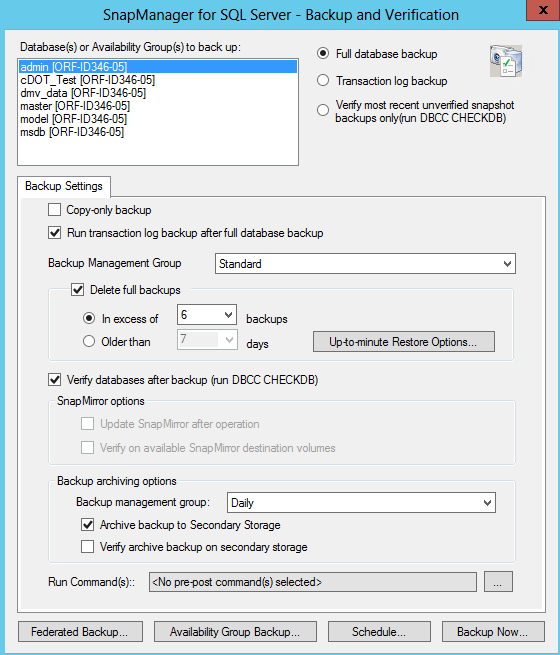
This is an important configuration on snap manager, As per standard S: should be configured as snapinfo . S: should not contain any database. This configuration normally performed by DBA’s . Backup configuration wizard on snap manager can be used for configuring this

## Full backup execution

MSSQL backup’s are scheduled as database backup jobs from Database. Below is the code DBA use to include archiving

“cd "C:\Program Files\NetApp\SnapManager for SQL Server" & SmsqlJobLauncher.exe new-backup  -svr 'ORF-ID346-05'  -d  'ORF-ID346-05', '0' -RetainBackupDays  6 -bksif -RetainSnapofSnapInfoDays 6 -mgmt standard -ArchiveBackup  -ArchivedBackupRetention Daily –Verbose “

A manual backup screen shot is below :



## Monitoring

In C-DOT snapvault updates are happening at the volume level , hence all snapshot in source volume will be copied over to destination, However any snapshot deleted over source will NOT be deleted on destination and keep for required retention.

snapmirror show -destination-path or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_usr\_snap -fields policy,state,lag-time,healthy

source-path destination-path policy state healthy lag-time

------------------------------------- -------------------------------------------- ---------- ------------ ------- --------

cisprod-e0041:or\_wi\_8040\_vm5\_usr\_snap or-ss-clbk-e01:sv\_14\_or\_wi\_8040\_vm5\_usr\_snap vault\_test Snapmirrored true 9:34:1

eag-nasor-clus2-8040bkp::>

All vserver (Primary and secondary) should have their aggr add to their aggr list. It’s needed for restore and clone.

**Example:**

::>vserver modify -vserver cisprod-e0041 -aggr-list aggr1\_data\_sas600\_flash\_n02

::> vs show -vserver cisprod-e0041

  (vserver show)

                                    Vserver: cisprod-e0041

                               Vserver Type: data

                               Vserver UUID: 905c632d-7165-11e4-abfc-123478563412

                                Root Volume: cisprod\_e0041\_rootvol

                                  Aggregate: aggr1\_data\_sas600\_flash\_n02

                        Name Service Switch: file

                        Name Mapping Switch: file

                                 NIS Domain: -

                 Root Volume Security Style: ntfs

                                LDAP Client: -

               Default Volume Language Code: C.UTF-8

                            Snapshot Policy: default

                                    Comment:

                               Quota Policy: default

                List of Aggregates Assigned: aggr1\_data\_sas600\_flash\_n02

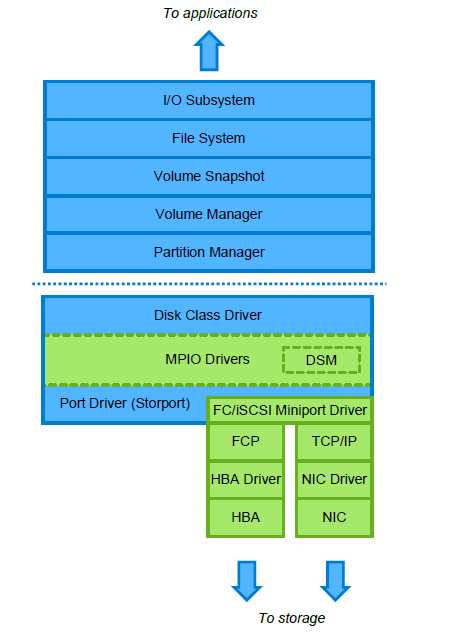
# Host side settings

## MPIO

Multipathed I/O (MPIO) is a way to multipath a LUN path from initiator to target. This way we induce a separate multipathing layer into the storage stack in a way to achieve multipath access to iSCSI targets. There are multiple implementations of multipathing mechanisms that can be implemented, here we are implementing Microsoft Native SAM (iSCSI for Windows 2003 and above).

The figure below explains how multiple paths are being used for redundancy on iSCSI targets.

1. Figure 2 MS Windows storage stack with MPIO



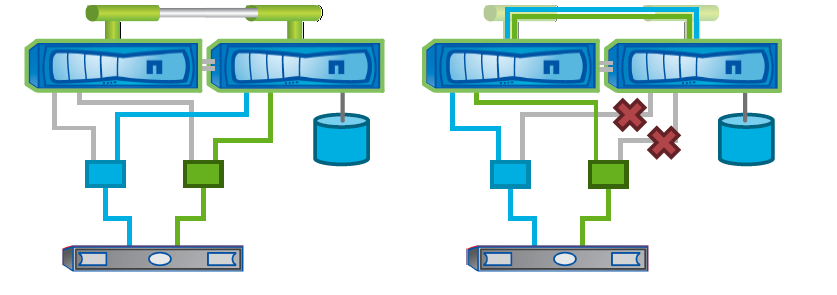
Netapp recommends utilizing failover mechanism (active-passive) over active-active configuration of MPIO.

## ALUA

In general, not all the paths have equal access to the LUN. In Clustered OnTAP, one node owns the LUN, but ports on two or more nodes may provide access, this is done by traversing the 10G cluster interconnect network.

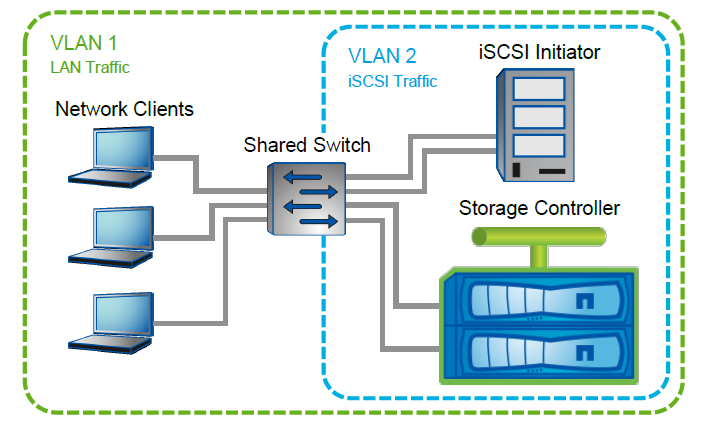
The following demonstration explains the direct and indirect paths to a LUN hosted on cDOT with a two node member. Here ALUA allows the initiator to query the target about path attributes and distinguish between primary and secondary paths. Henceforth, Microsoft native MPIO utilizes ALUA for path selection on iSCSI targets, this is generally enabled on the igroups in cDOT and is enabled by default.

1. Figure 3 Path failover mechanism in cDOT



In TR, we establish iSCSI network on the same switch servicing IP network. It is also recommended to enable jumbo frames on the physical interfaces of the NetAPP appliance, used for data ifgrps. The following describes this case.

1. Figure 4 iSCSI using a shared switch for iSCSI and IP network



## Implementing MPIO and ALUA

### ALUA

As mentioned earlier, ALUA is enabled on igroups and is enabled by default when an igroup is created. The configuration can be checked by the following feature:

eag-nasor-clus1::> igroup show -v igrp\_test\_iscsi

Vserver Name: iscsi-vm-01

Igroup Name: igrp\_test\_iscsi

Protocol: iscsi

OS Type: windows

Portset Binding Igroup: -

Igroup UUID: f223769d-4256-11e4-a02d-123478563412

ALUA: true

Initiators: iqn.1991-05.com.microsoft:orf-iscsi-01.tlr.thomson.com (not logged in)

In case you need to set this up manually please use the following command:

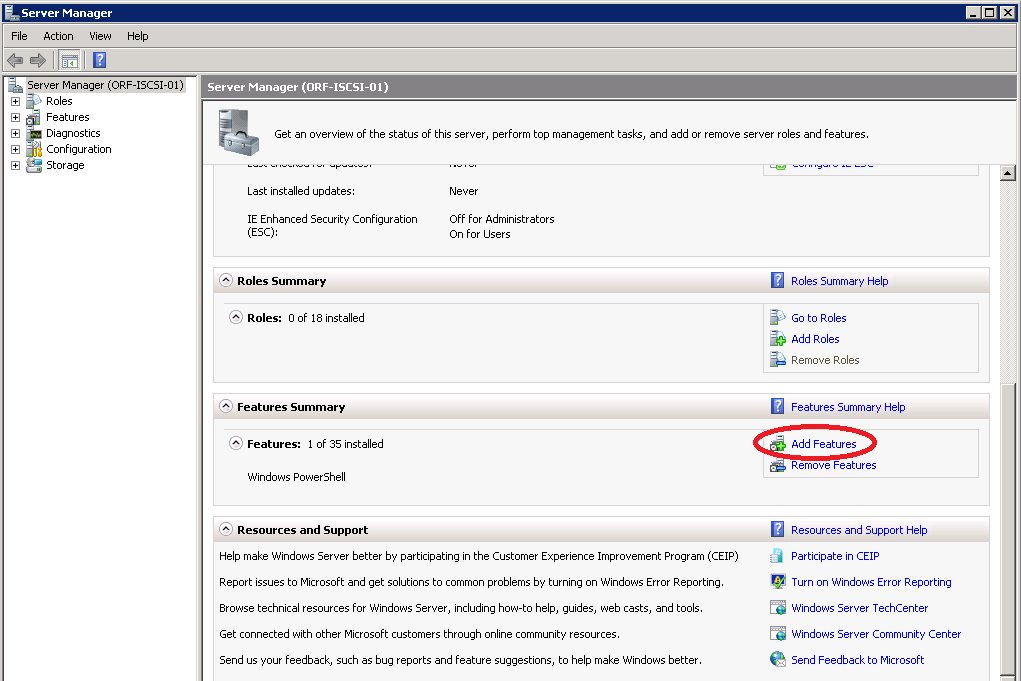
eag-nasor-clus1::> igroup set -vserver iscsi-vm-01 -igroup igrp\_test\_iscsi alua true

### MPIO

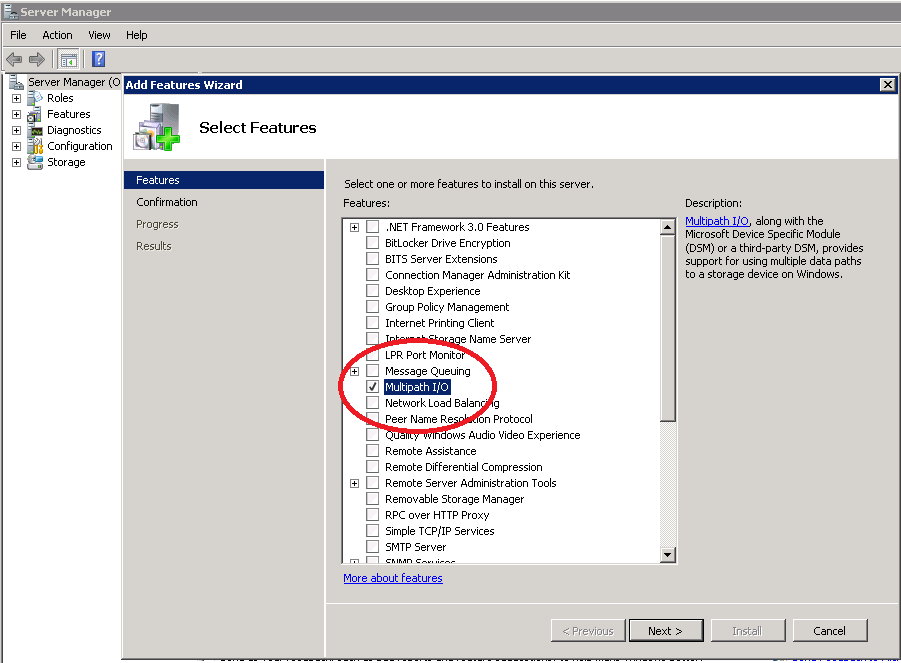
In TR, native Microsoft MPIO will be used in conjunction with ALUA on the NetAPP appliance running cDOT. MPIO is available as a feature in Windows server.The following steps explain the entire procedure.

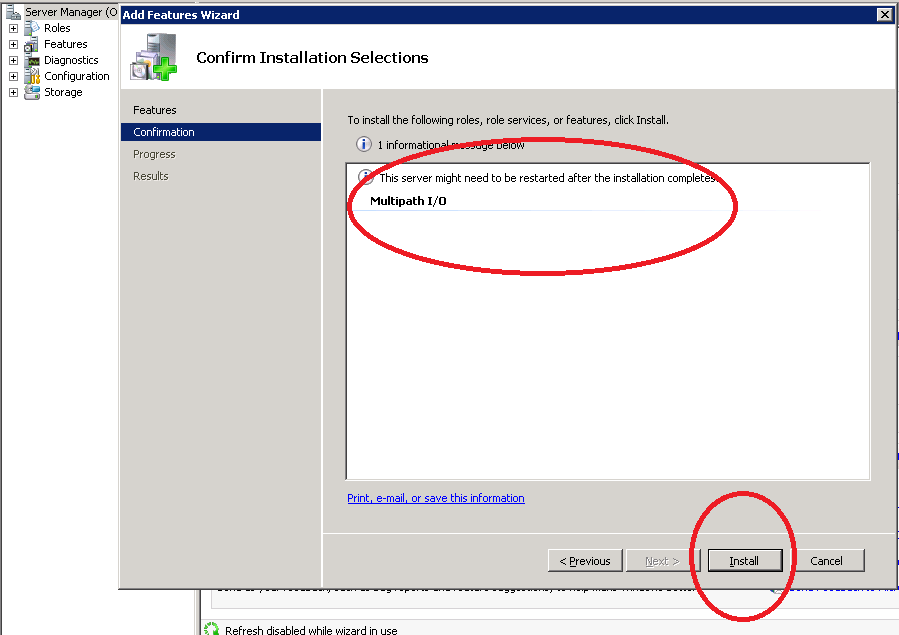
On your Windows 2008 SP2 server, go to server manager and click on add features

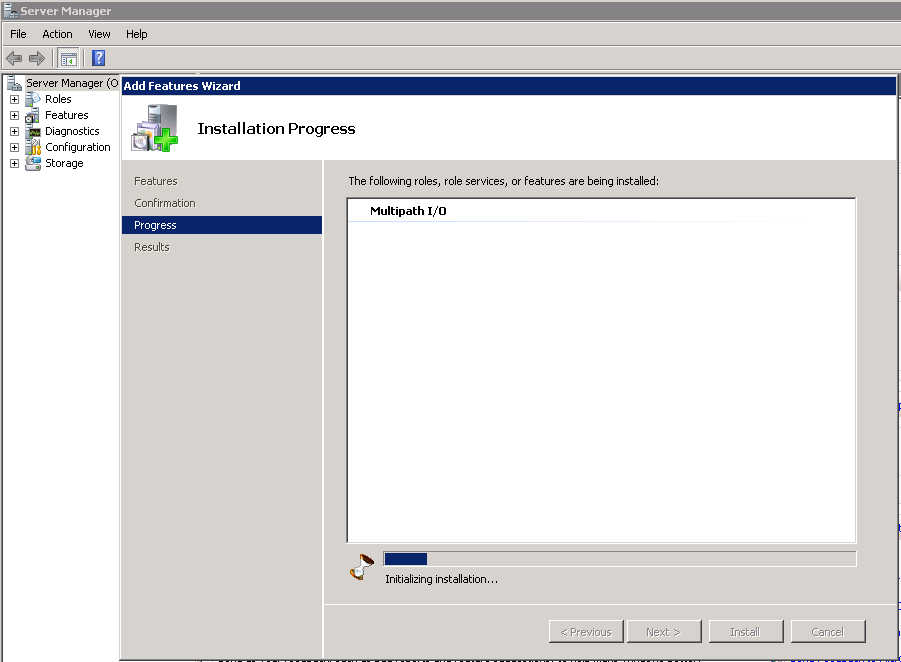
1. Figure 5 Adding addtional features from Microsoft Windows Server manager



Once you arrive on the page, click on “Multipath I/O” feature to enable the same.

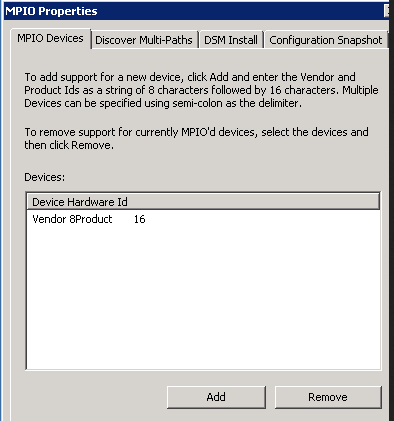




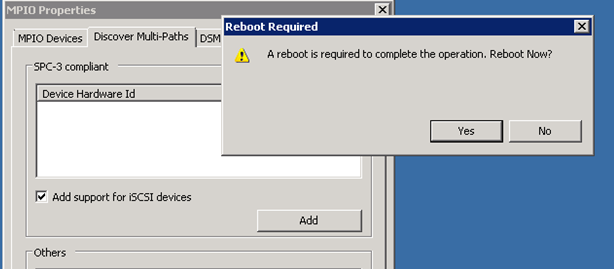


After the software is installed, it will ask for a reboot. On reboot, the installation resumes until successfully complete. Once this is complete, MPIO needs to be configured.

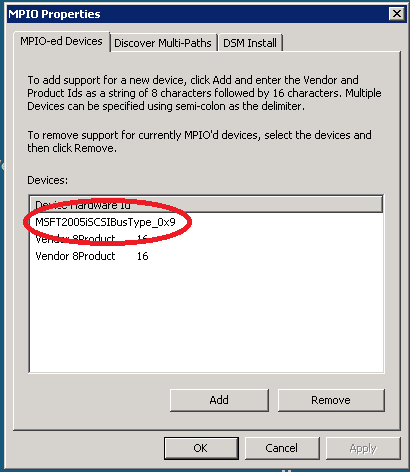
Go to Start 🡪 Administrative tools 🡪 MPIO to launch the software. You will be introduced to the following screen:



Click on “Discover Multi-Paths” and click on the checkbox “Add support for iscsi devices” as shown below (Please note: once done, this will automatically ask for a reboot)



On reboot, when you open the MPIO app again, you should be seeing iSCSI bus listed as a device:



If you notice the “Add support for iscsi devices” checkbox to be greyed out, this is actually expected and its natural.

### iSCSI initiator on the Windows server

#### Enable iSCSI initiator

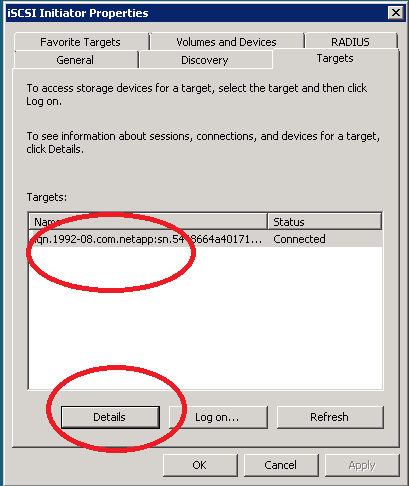
Start | Administrative Tools | iSCSI Initiator

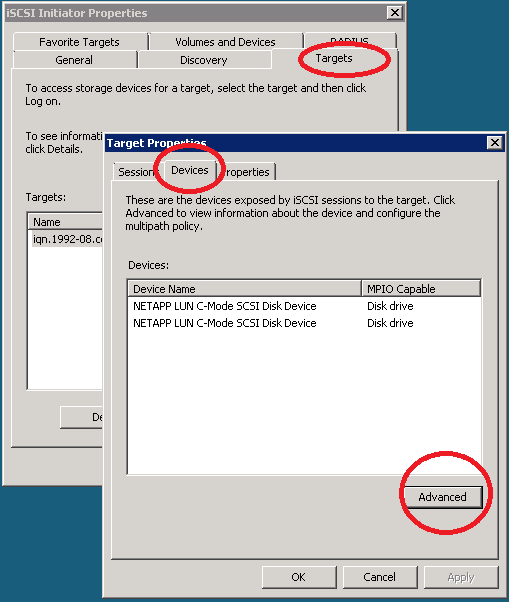
* 1. Click yes – “Popup stating iSCSI is not running, the service is required,,,,,, “ or set “Microsoft iSCSI Initiator Service” to automatic and start

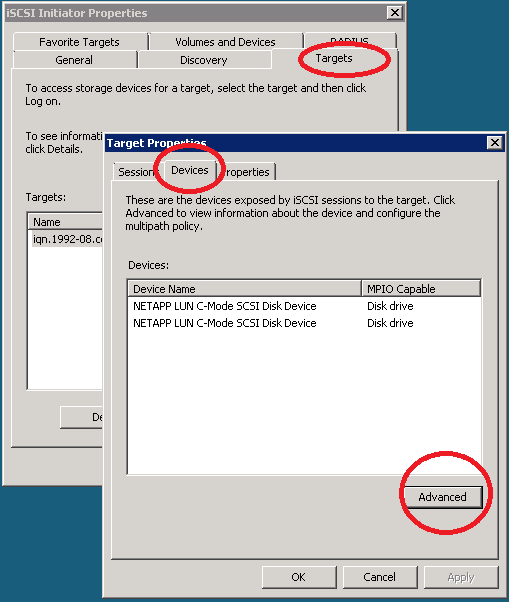
#### Configure iSCSI target & Storage

1. STOP – Storage Team will provide the engineer with the appropriate target VFiler IP address, UI & Password, proceed once received.
2. Start | Administrative Tools | iSCSI Initiator
3. Select the “Discovery” tab.
   1. “Discover Portal….”
   2. Place the IP address of the target/VFiler provided by the Storage Team.
   3. Advanced button
      1. Local Adaptor “Microsoft iSCSI Initiator”
      2. Initiator IP “Select the appropriate IP address of the host teamed NIC”
      3. Click OK | OK
4. “Targets” tab | highlight the name of the Target IQN | click “connect”
   1. Advanced | General Tab
      1. Local Adapter: “Microsoft iSCSI Initiator”
      2. Initiator IP: “NIC IP of the primary team”
      3. OK | OK
5. Clustered systems – repeat steps 1-6 under “**Configure iSCSI Target & Storage**”

**Enabling MPIO in the iSCSI application**







#### Netapp registry tuning for POD blades & Rack mounts:



# iSCSI setup and configuration

The following procedures are intended to provide manual GUI based procedures for setting up and configuring iSCSI. All steps can be automated as part of the build process.

### Enable Microsoft iSCSI Initiator

1. Start | Administrative Tools | iSCSI Initiator
   1. Click yes – “Popup stating iSCSI is not running, the service is required,,,,,, “ or set “Microsoft iSCSI Initiator Service” to automatic and start

### Configure iSCSI Target & Storage – POD

1. STOP – Storage Team will provide the engineer with the appropriate target VFiler IP address, UI & Password, proceed once received.
2. Start | Administrative Tools | iSCSI Initiator
3. Select the “Discovery” tab.
   1. “Discover Portal….”
   2. Place the IP address of the target/VFiler provided by the Storage Team.
   3. Advanced button
      1. Local Adaptor “Microsoft iSCSI Initiator”
      2. Initiator IP “Select the appropriate IP address of the host teamed NIC”
      3. Click OK | OK
4. “Targets” tab | highlight the name of the Target IQN | click “connect”
   1. Advanced | General Tab
      1. Local Adapter: “Microsoft iSCSI Initiator”
      2. Initiator IP: “NIC IP of the primary team”
      3. OK | OK
5. Clustered systems – repeat steps 1-6 under “**Configure iSCSI Target & Storage**”

### Cluster Configuration – POD & Rack mount systems

Follow PSTS clustering procedures – Documentation needs to be updated to reflect new procedures

<https://theshare.thomsonreuters.com/sites/windows/Operational%20Documents/Forms/AllItems.aspx>

# WISP requirements

**The following are “minimum” requirements that are supported as part of the WISP/ WIP project. Any down level system models, Operating Systems versions or SQL Database versions not listed at or above the below list will “NOT be supported or approved”. As new system models, Windows operating systems and SQL versions are released, Architecture along with the Data Center Platform Support/Engineering teams will evaluate, operationalize and update the WISP/WIP stacks accordingly.**

**We also need an account on vserver, a role on vserver to limit access; SSH access via public key to vserver and vserver management LIF with failover policy are required.**

**Operating System** – Windows 2008 R2 SP2

**SQL** – SQL 2008 SP2 64bit

**Network** – Nic Teaming

* + POD – 10GB Active/Passive
  + Rack mount – 2 @ 10GB Active/Active

**Hardware**

* 2 socket – POD blade
  + DL 180 or other rack mount systems are not supported
* 4 socket rack mount – x3850-x5

**Standalone & Microsoft Clustering supported**

* Each node in a cluster must be in a different chassis

**Service account --**

* **SnapDrive Service account -** 
  + Service account created in the appropriate Active Directory domain as the member server.
  + Service account must be a local admin on the machine
  + Service account should be unique to each server.
    - Account should be named as follows: svc%COMPUTERNAME%snap
  + PW should be random and only known during the build process. Should there be a need to change the password or rebuild the machine, reinstall the SnapDrive/SMSQL services, the PW should be regenerated and the server configured to use the new password. At no time should the password be stored in any documentation or repository.
* **SnapManager for SQL –** 
  + Service account – run under “local system”
  + “Local System” must be added to SQL sysadmin group

**Microsoft iSCSI initiator**

**MPIO –** out-of-scope, NIC teaming software will provide network redundancy

**Backups –** no OS level or local drive backups will be provided. All data must be placed on an iSCSI drive should data backups be required.

**Backup – NetApp provided snapshot software**

* + Volume based/File server – SnapDrive v6.4 x64 or newer
  + SQL – SnapManager for SQL v 5.2 or newer
    - SnapDrive is also a requirement for SnapManager for SQL

**Disk management –** LUN & logical drive creation created via Microsoft Disk Management

* Format NTFS, partition GPT
* Disks/LUNS should not be created, formatted or managed via SnapDrive

**Disk layout standards**

***Disk creation, deletion and administration must be completed via SnapDrive Manager or via sdcli command line interface.***

* **Volume size limit –** 6TB
* **Dynamic disk -** not supported
* **Disk cluster size –** 64K
* **SnapDrive LUN creation-** SnapDrivesupports up to 128 LUN’s
  + **Mount points -**  are supported in both standalone and clustered environments
    - MSCS – **Quorum LUN is no longer used please see FSW details.**
* **SQL –** 
  + Volume limitations & design principles -
    - Multiple databases per volume - <= 315 DB’s per server
      * 35 DB’s per volume
      * <= 200GB per database
    - Multiple databases per volume >315 DB's per server (Max DB's 1200)
      * 150 DB's per volume
        + Avg user database size <=10GB
        + Maximum user database size <=50GB

The following registry key must be set, in order to ensure that a single SMSQL snapshot is created per volume during the backup process. The SnapManager service should be restarted after setting this key: HKEY\_LOCAL\_MACHINE\SOFTWARE\NetApp\SnapManager for SQL Server\Server\MaxDbConcurrentBackup=DWORD::150

* + - Single database per volume
      * > 200GB per database
      * 6TB volume limit
* **File/other – TBD –** 
  + 6TB volume limit
* **Virtualization** – Virtual WISP/WIP (vWISP/vWIP)- 1 @ 10GbE logical NIC per logical VM guest. Network redundency provided by VM farm. MSCS is not supported.

**Issues/Patch Requirements**

[**(See appendix for more details)**](#Appendix_issues)

* **MS Patches – (**[**\\corpsoftware\nt$\Hardware\Storage\NetApp\SnapDrive\KB**](file:///\\corpsoftware\nt$\Hardware\Storage\NetApp\SnapDrive\KB)**)**
  + **KB2520235 -- <http://support.microsoft.com/kb/2520235>**
  + **KB2511500 -- <http://support.microsoft.com/kb/2511500>**
  + **KB2494016 --** [**http://support.microsoft.com/kb/2494016**](http://support.microsoft.com/kb/2494016)
  + **KB2531907 -** [**http://support.microsoft.com/kb/2531907**](http://support.microsoft.com/kb/2531907)
* **HP NIC, Teaming software & OneConnect updates**
  + [\\eg-nas-a02\nt$\Hardware\Storage\NetApp\HP\_Drivers](file:///\\eg-nas-a02\nt$\Hardware\Storage\NetApp\HP_Drivers)
    - OneConnect-Flash-2.104.281.0.iso           NIC firmware
    - cp014607.exe    NIC driver 2.104.277.1
    - cp014464.exe    NCU 10.40

### SQL-2016 supported platform and number of database

Supported platform – Windows 2016

SQL version – SQL 2016

SMSQL Version 7.2.2

Snap Drive: 7.1.4

Number of DBs supported: 1400 (Previous version SQL version was supported up to 6000)

175 DB per volume/35 DB per Snapshot

Replication (log shipping) limited to a maximum of 15 databases

### SQL-2016 FSW Config

For SQL 2016 clustering we now use a File Share Witness which requires a CIFS server and share. This is provisioned on the same ISCSI vserver containing the LUNs and is a slight risk given LUNs and share are in the same place. This risk is accepted by the MS SQL Architects.

The configuration requires an additional LIF to be provisioned on the vserver and an account that can be used by the Windows Team who then create the CIFS share. The CIFS vserver must be in a domain.

**Example configuration**

**Account and Role**

orf-lab2552::> sec login show -vserver silab-mssql-01

(security login show)

Vserver: silab-mssql-01

Authentication Acct

UserName Application Method Role Name Locked

---------------- ----------- -------------- ---------------- ------

iscsi ontapi password iscsi no

iscsi ssh password iscsi no

test ontapi password vsadmin no

vsadmin ontapi password vsadmin yes

vsadmin ssh password vsadmin yes

winadmin ontapi password CIFsadmin no

6 entries were displayed.

**Interfaces**

orf-lab2552::> net int show -vserver silab-mssql-01 -fields vserver ,data-protocol

(network interface show)

vserver lif data-protocol

-------------- -------------------- -------------

silab-mssql-01 silab-mssql-01-lif01 iscsi

silab-mssql-01 silab-mssql-01-lif02 iscsi

silab-mssql-01 silab-mssql-01-lif03 cifs

silab-mssql-01 silab-mssql-01-mgmt-lif01

none

4 entries were displayed.

**Shares**

orf-lab2552::> cifs share show -vserver silab-mssql-01 -fields vserver , share-name

vserver share-name

-------------- ----------

silab-mssql-01 admin$

silab-mssql-01 c$

silab-mssql-01 ipc$

silab-mssql-01 ORF-SQL14-03CFSW$

silab-mssql-01 ORF-SQL14-21CFSW$

silab-mssql-01 SQL16\_0102\_Witness$

silab-mssql-01 SQL16\_20\_21\_22\_Witness$

7 entries were displayed.