IBM i Support for Attaching an iSCSI VTL

Version 1.7

Background

The purpose of supporting an iSCSI virtual tape library (VTL) is to provide an offering that improves the performance of save and restore operations over Ethernet. This function is only tested and supported with a VTL from Falconstor and with a library type of Falcon on the PowerVS infrastructure.

Note: The design point for managing the system configuration uses SQL or Advanced Analysis Macros which will be covered in this document.

What's New

Version 1.7

IBM i support for secure storage of CHAP credentials in Platform KeyStore.

iSCSI Configuration SQL Services documentation moved to the IBM Documentation website.

Updated instructions for D-mode installation.

Live Partition Mobility considerations when using Platform KeyStore.

Data replication considerations when using Platform KeyStore.

Installation and Configuration

Prerequisites

IBM i version 7.2

Must have technical refresh 9 installed (MF99109).

Backup/Recovery group PTF SF99715 level 86, October 02 2024 update contains PTFS needed to run ISCSI, except the SQL and IPSec below:

MF69659
MF70034
To enable configuration using SQL, install PTF SI74769, which will require:
SI85770
SI76926
SI80334
SI79738
To enable IPsec and VPN (which requires Navigator), install PTFs:
SI73743
SI78187
SI80253
SI77743
SI76925

IBM i version 7.3

Must have technical refresh 13 installed (MF99213).

Backup/Recovery group PTF SF99724 level 70, January 2 2025 update contains PTFS needed to run iSCSI.

To enable configuration using SQL install the latest cumulative PTF package.

Also recommended:

SI79923

IBM i version 7.4

Must have technical refresh 11 installed (MF99311).

Backup/Recovery group PTF SF99664 level 45, January 2 2025 update contains PTFS needed to run iSCSI.

Also recommended:

MF69817

MJ03920

To enable IPsec and VPN (which requires Navigator) install the latest cumulative PTF package.

IBM i version 7.5

Backup/Recovery group PTF SF99954 level 15, January 2 2025 update contains PTFS needed to run iSCSI and the latest cumulative PTFs enable IPsec and VPN (which requires Navigator).

Also recommended:

MJ03921

Configuring the VTL

A Virtual Tape Library must be installed. Details are not provided by IBM for the installation process.

IBM® Navigator for i is the preferred method for configuring iSCSI targets. Refer to the following documentation for additional information.

A virtual library/drives/media must be created. Recommended type-model information is because a large portion of the compatibility testing was done with the specified type-model.

- Library: IBM only supports the Falconstor 3584. This library will be reported to the system as a 3584-403, which supports live partition mobility which is a requirement on PowerVS.
- Drives: IBM recommends IBM LTO3 or newer drives. There is a restriction that only one drive type may be in any library attached to IBM i.

- Media:

You must also create the permission information to allow the controlling system to attach to the library. (The library needs to be added to an iSCSI client definition, which defines the information required for the system to access the virtual libraries)

The IBM i design for iSCSI does not allow multiple communications connections between a given i partition and target VTL.

While the preferred method for configuring an IBM i partition is to use Navigator for i, iSCSI VTL targets may also be configured using SQL services or advanced analysis macros.

Using Platform KeyStore to Secure CHAP Credentials

As of IBM i 7.6, Challenge Handshake Authentication Protocol (CHAP) credentials for each iSCSI VTL target configuration can be stored in an encrypted non-volatile storage area on the service processor called Platform KeyStore (PKS). Refer to PowerVM introduces Platform KeyStore for more information regarding PowerVM support for PKS.

PKS must be enabled for a partition before the partition may use PKS for secure storage. For most users, a 4K allocation of PKS is of sufficient size to contain iSCSI CHAP credentials for all target configurations. However, if PKS is also used for other IBM i applications (for example, storing NVMe device locking policy information) a larger allocation of PKS may be required.

After PKS has been enabled for an IBM i 7.6 partition, all iSCSI CHAP credentials will be stored in PKS by default. This includes CHAP credentials which existed prior to installing IBM i 7.6 or enabling PKS as the system will move this data to PKS automatically. If desired, an SQL service or advanced analysis macro parameter can be used to override the default behavior and require CHAP credentials be stored in unencrypted form on disk instead of PKS. **However, since this increases the potential for exposing CHAP credentials to unauthorized individuals, a security administrator should carefully review the risks before choosing this option.**

iSCSI Configuration – SQL Services

IBM i SQL Configuration Services include procedures and views for managing iSCSI target configurations. Refer to the following Configuration Services documentation for additional information.

- ADD_ISCSI_TARGET procedure
- CHANGE_ISCSI_TARGET procedure
- REMOVE_ISCSI_TARGET procedure
- CHANGE_IOP procedure
- ISCSI_INFO view

Advanced Analysis Configuration

The Advanced Analysis macro for IBM i iSCSI configuration is ISCSISWICONFIG. To use this macro to configure iSCSI, follow these steps:

1. Access Service Tools using SST or DST. Sign in with a service tool profile that has authority to use the Display/Alter/Dump service tool.
2. Select Start a service tool.
3. Select Display/Alter/Dump.
4. Select Display/Alter storage.
5. Select Licensed Internal Code (LIC) data.
6. Select Advanced analysis. (You may have to page down to see this option)
7. On the Select Advanced Analysis Command screen, type 1 (Select) next to the top blank line under the Command column. In the blank line, type ISCSISWICONFIG and press the Enter key.
8. On the Specify Advanced Analysis Options screen, enter the desired macro options in the Options field and press the Enter key.

The available options for the ISCSISWICONFIG macro are:

-**dumpinitiators**: Dump configuration and status information for iSCSI initiators.

Before configuring any iSCSI targets, the -dumpinitiators option can be used to get the default initiator name for the IBM i partition. The system generates a default initiator name using the Universal Unique Identifier (UUID) for the partition. The UUID is available when the IBM i is running on power 8 or later hardware. If the IBM i is running on power 7 hardware or earlier, the system administrator must supply the IBM i initiator name. Note: The configuration displayed is the one currently active in the IOP. If you change the configuration it will not be displayed until the IOP is re-IPLed.

-**dumptargets**: Dump configuration and status information for all iSCSI targets. Note: The configuration displayed is the one currently active in the IOP. If you change the configuration it will not be displayed until the IOP is re-IPLed.

-**addtarget**: Configure a new target on the system using the following parameters:

-**initiatorname**: (Required) Initiator name for the local system. The user can supply an initiator name or pass the keyword *GENERATE. If *GENERATE is specified, the system will use the default initiator name. The system generates a default initiator name using the Universal Unique Identifier (UUID) for the partition. The UUID is available when the IBM i is running on power 8 or later hardware. If the IBM i is running on power 7 hardware or earlier, the system administrator must specify a unique initiator name. The -dumpinitiators option can be used before adding a target to see the system generated initiator name.

The IBM i uses the iSCSI Qualified Name (IQN) format as defined in RFC7143 for its default initiator name. An IQN type name consists of the following:

The string "iqn."   (to distinguish the name as an IQN type name)

A date code in the format yyyy-mm. From RFC7143: This date must be a date during which the naming authority owned the domain name used in this format and should be the first month in which the domain name was owned by this naming authority at 00:01 GMT of the first day of the month.

A dot (.)

The reverse domain name of the naming authority creating this iSCSI name. For example, "com.ibm".

Optional: Colon (:) followed by product and/or system specific information. The IBM i default name uses ibmi.<uuid>-i<initiator index>. The uuid is a 32-character hexadecimal identifier for the partition. The initiator index is a zero-based index. Since only one initiator is supported on IBM i, the initiator index is always '0'.

The following is an example default initiator name for IBM i:

iqn.1924-02.com.ibm:ibmi.4520920efdc3454db06b96a56d912aa5-i0

-**targethostname**: (Required) Host name or internet address of the iSCSI target system

-**targetname**: (Required) Target name: The target name is similar to the initiator name. This name is provided by the administrator of the target VTL.

-**targetport**: (Optional) Target port number, default is 3260

-**initiatorchapname**: (Optional) Initiator CHAP name. **Note:** All characters in the CHAP name are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**initiatorchapsecret** : (Optional) Initiator CHAP secret. **Note:** All characters in the CHAP secret are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**chapkeystore** : (Optional) CHAP keystore location [AVAIL | NONE | PLATFORM]. Defines the keystore area used to securely store the specified CHAP credentials.

- AVAIL will store the CHAP credentials in the encrypted keystore provided by platform hardware (PKS) if it is enabled for the partition. If PKS is not available, CHAP credentials are stored as plaintext in unencrypted storage. This is the default value.
- NONE will only store CHAP credentials as plaintext in unencrypted storage.
- PLATFORM will only store CHAP credentials in PKS. If PKS is not enabled for the partition an exception will occur.

-**reipliscsiiop:**   Re-IPL the iSCSI IOP. Ends the current connections to iSCSI targets and makes new connections based on the most recent configuration.

-**removetarget**: Remove an existing target from the system using the following parameters:

-**initiatorname**: (Required) Initiator name for local system. The user can supply an initiator name or pass the keyword *GENERATE. If *GENERATE is specified, the system will use the default initiator name.

-**targethostname**: (Required) Host name of internet address for iSCSI target system

-**targetname**: (Required) Target name

-**targetport**: (Optional) Target port number, default is 3260

-**changetarget**: Change an existing target on the system using the following parameters (note this can be used to change CHAP parameters):

-**initiatorname**: (Required) Initiator name for local system. The user can supply an initiator name or pass the keyword *GENERATE. If *GENERATE is specified, the system will use the default initiator name.

-**targethostname**: (Required) Host name of internet address for iSCSI target system

-**targetname**: (Required) Target name

-**targetport**: (Optional) Target port number, default is 3260

-**initiatorchapname**: (Optional) Initiator CHAP name. **Note:** All characters in the CHAP name are translated to upper case. Thus, the user configuration on the VTL console must also be all upper case.

-**initiatorchapsecret** : (Optional) Initiator CHAP secret. **Note:** All characters in the CHAP secret are translated to upper case. Thus, the user configuration on the VTL console must also be all upper case.

-**chapkeystore** : (Optional) CHAP keystore location [AVAIL | NONE | PLATFORM]. Defines the keystore area used to securely store the specified CHAP credentials.

- AVAIL will store the CHAP credentials in encrypted keystore provided by platform hardware (PKS) if it is enabled for the partition. If PKS is not enabled, CHAP credentials are stored as plaintext in unencrypted storage. This is the default value.

- NONE will only store CHAP credentials as plaintext in unencrypted storage.

- PLATFORM will only store CHAP credentials in PKS. If PKS is not enabled for the partition an exception will occur.

-**clearconfig**: Clear iSCSI configuration. Removes all configured iSCSI targets and takes system back to the GA state.

-**newname**: Specify one or more of the parameters needed for target configuration. Since Advanced Analysis allow a limited number of characters for parameters, the -newname and -appendname parameters allow the administrator to break the target specification into several shorter macro commands. The specify one of the names needed to configure an iSCSI target, specify -newname with -initiatorname, -targetname, -targethostname, initiatorchapname, or initiatorchapsecret and the parameter value. If there is not enough room to specify the entire name, the -appendname can be used to specify the rest of the parameter. When all necessary names are specified, the -commit option should be used to configure the target. The system stores one set of target configuration parameters, so an administrator can configure only one target at a time using this method. -newname replaces any previous target configuration parameter that may have been specified. Specify one of the following with -newname:

-**initiatorname**: (Optional) Initiator name for local system. Not needed if using the system generated initiator name. See -addtarget -initiatorname for information about initiator names.

-**targethostname**: (Optional) Host name of internet address for iSCSI target system

-**targetname**: (Optional) Target name. The target name is similar to the initiator name. This name is provided by the administrator of the target VTL.

-**initiatorchapname**: (Optional) Initiator CHAP name. **Note:** All characters in the CHAP name are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**initiatorchapsecret** : (Optional) Initiator CHAP secret. **Note:** All characters in the CHAP secret are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**appendname**: Append to name for target configuration, use one of the following:

-**initiatorname**: (Optional) Append to the initiator name for local system. Not needed if using the system generated initiator name.

-**targethostname**: (Optional) Append to the host name or internet address for iSCSI target system

-**targetname**: (Optional) Append to the target name

-**initiatorchapname**: (Optional) Initiator CHAP name. **Note:** All characters in the CHAP name are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**initiatorchapsecret** : (Optional) Initiator CHAP secret. **Note:** All characters in the CHAP secret are translated to upper case. Thus, the user configuration on the VTL console must be all upper case.

-**setport**: Specify port number for target configuration to be finalized with -commit. Not needed if the default iSCSI port is being used.

-**targetport** (Required when -setport is specified)

-**setkeystore**: (Optional) Specify the CHAP keystore location for pending commit.

-chapkeystore: (Required with -setkeystore) [AVAIL | NONE | PLATFORM]

-**commit**: Configure a target using parameters previously specified with -newname, -appendname, -setport, and -setkeystore.

To configure iSCSI on the IBM i, the administrator needs to know the following information:

- The TCP/IP host name or IP address of the VTL that is the iSCSI target.
- The iSCSI target name of the VTL. The administrator of the iSCSI target can supply this name.
- The IBM i iSCSI initiator name.
- (Optional) The iSCSI CHAP authentication credentials.

If running on power 8 or later hardware, a system generated initiator name can be generated and will have the following format:

iqn.1924-02.com.ibm:ibmi.6B9CE26E559E4763824F597B5ED7077A-i0

where 6B9CE26E559E4763824F597B5ED7077A is the UUID of the system.

The desired macro options may be too long to include within a single macro invocation in Advanced Analysis. To allow for this, each name in a target configuration specification can be configured in separate macro invocations using the -newname, -setport, and -setkeystore options of the iscsiswiconfig macro. Once all information has been specified, the configuration change is finalized using the -commit option. If a name is too long to specify in a single macro invocation, it can be split across multiple invocations using the -appendname option. Note that iscsiswiconfig -newname -initiatorname is not needed if using the system generated initiator name.

Example using the system generated initiator name and no CHAP authentication:

```
iscsiswiconfig -newname -targetname iqn.2000-03.com.xyz:vtl.vtltest.demo-39
iscsiswiconfig -newname -targethostname 10.1.1.5
iscsiswiconfig -commit
```

Example with a user supplied initiator name and no CHAP authentication:

```
iscsiswiconfig -newname -initiatorname iqn.1924-02.com.ibm:ibmi:TEST-LPID-FFFFFFFF-i0
iscsiswiconfig -newname -targetname iqn.2000-03.com.XYZ:vtl.ABC-XYB-ROCH.demo-1
iscsiswiconfig -newname -targethostname 10.1.1.5
iscsiswiconfig -commit
```

Example using the system generated initiator name with CHAP authentication:

```
iscsiswiconfig -newname -targetname iqn.2000-03.com.xyz:vtl.vtltest.chap
iscsiswiconfig -newname -targethostname 10.1.1.5
iscsiswiconfig -newname -initiatorchapname SOMECHAPNAME
iscsiswiconfig -newname -initiatorchapsecret SOMECHAPSECRET
iscsiswiconfig -commit
```

Example with a user supplied initiator name using CHAP authentication, an alternate iSCSI TCP/IP port, and a requirement to only store CHAP credentials in secure platform keystore:

```
iscsiswiconfig -newname -initiatorname iqn.1924-02.com.ibm:myinternetname.ibm.com-i0
iscsiswiconfig -newname -targetname iqn.2000-03.com.xyz:vtl.vtltest.chap
iscsiswiconfig -newname -targethostname 10.1.1.5
iscsiswiconfig -newname -initiatorchapname SOMECHAPNAME
iscsiswiconfig -newname -initiatorchapsecret SOMECHAPSECRET
iscsiswiconfig -setport -targetport 860
iscsiswiconfig -setkeystore -chapkeystore PLATFORM
iscsiswiconfig -commit
```

IPL The IOP:

After making any iSCSI configuration changes, the iSCSI controller must be IPLed for the changes to take effect. If the VTL has been power cycled the iSCSI controller also needs to be IPLed to recover the connection.

To do this use either:

- iscsiswiconfig -reipliscsiiop
- issue the STRSST command.

  select option 1 (Start a Service tool)

select option 7 (Hardware service manager)

select option 2 (Logical Hardware Resources)

select option 1 (System bus resources)

Scroll through the bus resources, look for one with a Type-Model of 298A-001, select option 6 for that resource.

Select option 4 to (IPL I/O Processor

At this point you can exit hardware service manager and SST.

If it works, there should be new tape device descriptions with names TAPMLBxx. The number of tape devices created depends on the VTL configuration.

Save/Restore and Migration

This document presumes the user is familiar with save/restore operations and mainly describes the differences when using an iSCSI VTL. For many operations, the VTL may be used exactly like a physical tape library. However, because the connection to the library is via a TCP/IP interface some combinations of IBM i and Power system levels do not support D-Mode IPL from the virtual tape library.

IBM i level	**Power system level**	**D-mode IPL supported**	**PKS supported for iSCSI CHAP**
7.5 base and earlier	Any	No	No
7.5 TR1 or later	Power10 (FW1030 or later)	Yes	No[1]
7.6	Power10 (FW1060 or later)	Yes	Yes

[1] PKS must be enabled for PowerVM to allow iSCSI D-mode IPL, but is not consumed by IBM i

When D-mode from the iSCSI VTL is not supported, the process of using a full system save to migrate a partition or recover from a disaster must follow multiple steps to use an alternate source for the D-Mode IPL while still restoring most of the saved data from the VTL.

Using an iSCSI VTL for Save/Restore while in restricted state

If the save/restore operation requires the system to be in restricted state, you will need to take the following steps to enable the iSCSI VTL to communicate over TCP/IP:

- Vary the MLB off
- ENDSBS SBS(*ALL) to get the machine in restricted state.
- When the machine is in restricted state, restart TCP with STRTCP STRSVR(*NO) STRIFC(*NO) STRPTPPRF(*NO).
- Do a NETSTAT, select Work with IPv4 or IPv6 interface status, and start the appropriate network stack(s).

- When the network interface is ACTIVE (NETSTAT Display TCP/IP stack status), vary the MLB back on.

Creating D-Mode Media/Saving the system when iSCSI D-Mode IPL is not supported

If D-Mode cannot be done from the iSCSI VTL, saving the system using the VTL must be done in two steps. Described here is a method to create a virtual optical IMGCLG and moving that to an IBM i partition capable of hosting an NFS D-mode/install of the target. Once the target is IPLed with TCPIP started, the VTL can be used to restore the bulk of the data being moved.

Full System Save:

1. Create an optical based IMGCLG on the LPAR that needs to be saved.
2. Create media large enough to contain the SAVSYS, or for multiple media, the first should be a minimum size of 4.7GB.
3. Backup the OS, BRMS (if available) and any LPPs needed to use the iSCSI VTL to the virtual optical device containing the image catalog. Suggest using:
    - GO SAVE option 22
    - SAVLIB LIB(QGPL)
    - SAVLIB LIB(QUSRSYS)
4. VFYIMGCLG is used to create the BOOTP directory required for NFS IPL. It can be done locally (and then the entire directory and file set moved to the save media), or the virtual media can be copied, and the VFYIMGCLG done as part of recovery process.

   Example:
   VFYIMGCLG IMGCLG(*image_catalog_name*) TYPE(*LIC) SORT(*YES) NFSSHR(*YES)

The virtual optical media created will be the source for D-Mode IPL.

If you are doing a disaster recovery save, the IFS files representing the optical image catalog can be archived to your iSCSI attached tape.

Backup up the rest of the user data with the iSCSI attached tape. For disaster recovery saves, you need to remember that the save (both the IMGCLG from step 4, and the rest of the data from this step) may need to be saved offsite. Suggest using:

- GO SAVE 21 or
- GO SAVE 23

(**Note:** You must specify “*NONE” for the "End TCP/IP wait time" menu option or TCPIP will be shut down, causing the iSCSI VTL to become unusable.)

(**Note**: Some of the commands issued during GO SAVE 21 and GO SAVE 23 processing do not support specifying the volume ID, so you need to set up a mounted category for the VTL or deallocate one of the drive resources from the VTL and vary it on as a stand-alone device to use for those operations.)

D-Mode IPL and System Restore when iSCSI D-Mode IPL is not supported

Provision another IBM i that will be the network install server system for the recovery. Attach your iSCSI tape and restore the image catalog.

Perform a D-Mode IPL from the network install server to restore the LIC and base OS.

Restore programs and files saved in Full System Save step 3 - "Backup the OS, BRMS (if available) and any LPPs needed to use the iSCSI VTL ..."

Example:

GO RESTORE option 22

RSTLIB LIB(QGPL)

RSTLIB LIB(QUSRSYS)

Connect the restored partition to the iSCSI tape and restore the rest of the data.

D-Mode IPL from an iSCSI VTL

If the combination of IBM i operating system level and Power system level permit a D-mode IPL from an iSCSI device, a full system save/restore using the iSCSI VTL can be performed in nearly the same manner as a physical tape library. A few differences involved when using the iSCSI VTL include extra steps to activate TCP/IP while in restricted state (as previously described) and using the HMC Network Boot wizard to initiate the D-mode IPL because configuration information must be entered before the IPL can begin.

Additionally, only a limited function TCP/IP network stack which does not contain secure connection support is available for restoring the IBM i LIC and operating system components. **Sensitive user data should not be restored until the operating system TCP/IP stack can be started and secure connections can be configured.**

Follow these steps to initiate a D-mode IPL using an iSCSI VTL:

1. Ensure that the D-mode media is mounted on one of the iSCSI VTL tape drives.
2. On the HMC, verify the partition is in the Not Activated state.
3. On the HMC, view the Partition Properties and expand Advanced Settings. Ensure Platform KeyStore Size is at least 4 KB. **Note:** this is necessary even if the IBM i partition does not support using PKS to store CHAP credentials.
4. Follow the Network Boot procedure documentation at Activating IBM i partitions to enter iSCSI Tape configuration information and start the D-mode IPL.

Live Partition Mobility Considerations

PowerVM automatically migrates Platform KeyStore to the target system during Live Partition Mobility (LPM). Therefore, an IBM i 7.6 partition with an iSCSI configuration that stores CHAP credentials in PKS can be migrated to another server without any configuration changes.

Encryption of all data during LPM was previously introduced by PowerVM on POWER9 servers, and the same encryption technique is used to securely transfer PKS from the source to the target destination.

Data Replication Considerations

Data replication creates multiple copies of the same data in different locations as a way of ensuring data availability, reliability and resilience across an organization. In the event of a hardware/system failure or other type of catastrophic event, applications can be switched over to use replica data, minimizing downtime and data loss.

Advanced data replication technologies such as Geographic Mirroring, Metro/Global Mirror, or FlashCopy can be used create and maintain consistent copies of entire storage volumes. While these are effective methods for most data replication, any *SYSBAS data which is not stored on disk will not be copied by disk replication. In particular, Platform KeyStore contents are not replicated by these techniques so CHAP credentials for iSCSI targets stored in PKS will not be copied to replica storage and may not be available if replica storage is used on a different Power server to recover from a system failure or other catastrophic event.

Several options may be used to compensate for CHAP credentials that are stored in PKS not being copied by disk replication:

- Recreate the iSCSI CHAP configuration on the target system

  Navigator, SQL services or macro interfaces can be used to restore the proper CHAP credentials on the target system once it has been started from the replicated disk images.

- Store CHAP credentials as unencrypted data on disk storage

  The CHAP keystore option can be set to *NONE using SQL services or macro interfaces to prevent CHAP credentials from being stored in PKS. Disk replication will then be able to duplicate the entire iSCSI configuration, including CHAP credentials, on the target disk volumes.

- Remove CHAP from the iSCSI configuration

  The iSCSI configuration may be modified to remove CHAP authentication from the iSCSI VTL connection protocol. The remaining iSCSI configuration data will be duplicated by disk replication and so will be available on the target system.

Note: storing CHAP credentials as unencrypted data or removing CHAP authentication from

the iSCSI protocol increases the potential for unauthorized individuals gaining access to the Virtual Tape Library. Therefore, a security administrator should carefully review the risks before using these options.