Using QNAP Enterprise-class ES NAS with Microsoft Windows Server and Hyper-V
Thank you for choosing QNAP products! This user manual provides detailed instructions of using the Turbo NAS (network-attached storage). Please read carefully and start to enjoy the powerful functions of the Turbo NAS!

- The Turbo NAS is hereafter referred to as the NAS.
- This manual provides the description of all the functions of the NAS. The product you purchased may not support certain functions dedicated to specific models.

Legal Notices

All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.

QNAP and the QNAP logo are trademarks of QNAP Systems, Inc. All other brands and product names referred to are trademarks of their respective holders. Further, the ® or ™ symbols are not used in the text.

Disclaimer

Information in this document is provided in connection with QNAP products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in QNAP’s terms and conditions of sale for such products, QNAP Assumes no liability whatsoever, and QNAP disclaims any express or implied warranty, relating to sale and/or use of QNAP products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

QNAP products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

In no event shall QNAP Systems, Inc. (QNAP) liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Back up the system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.

QNAP, QNAP logo, QTS, myQNAPcloud and VioStor are trademarks or registered trademarks of QNAP Systems, Inc. or its subsidiaries. Other names and brands may be claimed as the property of others.
# Table of Contents

- Designed to support critical business applications................................................................. 4
  - Preparation for installation............................................................................................................. 5
    - Install Qfinder Pro ..................................................................................................................... 5
    - Search and connect to a NAS via Qfinder Pro......................................................................... 5
  - Configure the NAS for shared storage ....................................................................................... 7
    - Disk initialization and cache acceleration.................................................................................. 7
    - Create storage pools with RAID configuration ........................................................................... 10
  - Configure Network Settings.......................................................................................................... 12
    - Create iSCSI targets and iSCSI LUNs on the ES NAS ................................................................. 13
  - Configure Windows Server for iSCSI connections .................................................................... 23
    - Enable Jumbo Frame in Windows Server ..................................................................................... 26
    - Recommended updates and hotfixes for Windows Server .......................................................... 28
  - Connect to iSCSI targets using Microsoft iSCSI initiator ............................................................ 30
  - Configure iSCSI connections with MPIO in Windows Server .................................................... 33
    - Install the MPIO Service in Windows Server .............................................................................. 34
    - Configure the MPIO Service in Windows Server ....................................................................... 38
    - Configure and start iSCSI initiator .............................................................................................. 39
  - Mount iSCSI virtual disks ............................................................................................................. 47
  - Use iSCSI disks to store Hyper-V virtual machines ..................................................................... 51
    - Install the guest operating system .............................................................................................. 57
QNAP’s Enterprise-class NAS (ES NAS) is designed from the ground up to support high-availability features with the intuitive storage management features shared throughout QNAP NAS product lines. The operating system of the ES NAS (QES) significantly improves storage management and data security, allowing ES NAS users to enjoy the benefits of easier management and reduced costs.

Improved storage management and security capabilities include:

- **Remote data synchronization**: The block-level SnapSync can provide remote backup and disaster recovery at any time, providing enterprise business consistency.
- **Higher-capacity efficiency**: Block-level deduplication and real-time data compression employed from ZFS and Thin Provisioning with Reclaim make it easy to create the most cost-effective remote virtual desktop platform and mission-critical information warehousing.
- **Well-rounded data protection and security**: Shared folder and LUN encryption protects business-sensitive data by utilizing drive-based hardware encryption in combination with a software key. In addition, WORM (Write Once Read Many) provides data tampering prevention and original content retention at a shared-folder level. LUN Encryption is available for all drive types, including flash drives (SSD).
- **High reliability, availability and serviceability**: Features dual active controllers, dual Mini-SAS channels, and redundant power supplies to support failover and to provide uninterrupted service with near-zero downtime.
- **Battery-protected write cache**: The ES NAS utilizes the advanced ZFS ZIL write caching, which is protected by a BBU (Battery Backup Unit). The battery-protected DRAM write also features cache data mirroring of both controllers to ensure a high degree of persistent and reliable integrity for cached data if a storage controller fails in a dual-controller configuration.

With so many sophisticated capabilities that are easy to deploy, the ES NAS provides a highly scalable virtualized, enterprise-class storage system to facilitate mission-critical data centers. Virtualized servers hosting multiple virtualized workloads in data centers require storage resources to meet capacity and performance requirements. In this document, we will demonstrate the use of the ES NAS with Windows Hyper-V Manager by which the storage capacity and provisioning are offloaded to the ES NAS.
Preparation for installation

Qfinder Pro is a utility that allows you to quickly search and manage your NAS on your network. Install Qfinder Pro on your Windows Server, launch it, and double-click your ES NAS to open the login page.

Install Qfinder Pro

1. Go to the QNAP website and download Qfinder Pro for your operating system:
2. Follow the instructions to install Qfinder Pro.

Search and connect to a NAS via Qfinder Pro

1. Open Qfinder Pro, then it will automatically search for QNAP NAS in the same network. Double click on your NAS in Qfinder Pro to start the Smart Installation Guide and it will guide you through the installation process to complete the firmware installation.

   ![Smart Installation Guide]

   Server not initialized yet

   'ESSEE048C' (172.17.22.7) has not been initialized yet.

   Do you want the Smart Installation Guide to guide you through the configuration process?

   ![Yes No buttons]

   Show this message next time? Always ask me

   Note: If there is no DHCP server on your network, the ES NAS will be set to its default IP address: 169.254.100.100. Enter this IP address in your browser to access your NAS and start the Smart Installation Guide to help you initialize your NAS.

   2. After setting up the ES NAS with the Smart Installation Guide, please proceed to the QES login page with your admin account and password to log in. (QES is the operating system for the ES NAS.)
Configure the NAS for shared storage

After first-time installation of the ES NAS with the Smart Installation Guide, the ES NAS is ready for use. However, additional configuration is required for the ES NAS to serve as the central storage system to manage your storage resources.

Disk initialization and cache acceleration

After you log in to the NAS, the welcome screen appears. To continue using the ES NAS, please click “Yes” to initialize the raw disks. Before you initialize drive(s), back up pre-existing data because all data on your drive(s) will be erased when they are initialized.

We recommend enabling Cache Acceleration on the ES NAS to boost access performance. Please use the following procedure to enable the Cache Acceleration feature.

1. Open Storage Manager.
2. Select “Cache Acceleration” in the left pane and click “Set SSD Drive”.

3. Select the drives for Cache Acceleration. We will enable Cache Acceleration for system drives (Drive 1~4). Click “OK” to save your changes.
4. To confirm that you want to delete data on the SSD drives, click “OK”.

5. The Cache Acceleration service should be enabled.
Create storage pools with RAID configuration

A storage pool is designed to aggregate physical hard disk drives into a large storage space and to provide enhanced RAID protection for it. Creating a storage pool is fundamental before you can allocate storage space to the servers.

Use the following procedure to create a new storage pool:

1. Go to “Storage Manager” > “Storage Pools” and click “New Storage Pool”.

2. Give a name for the storage pool, choose the controller the pool belongs to, and select the enclosure unit, hard disk drive(s), RAID type and click "Next".

3. Review the pool creation summary and click “Create”.

©2016 QNAP Systems, Inc. All Rights Reserved.
4. Please note that all data on the selected hard disk drive(s) will be erased. Click "OK" if you are certain about this.

5. A new storage pool will be created.
1. Log in to the ES NAS and go to “Control Panel” > “System Settings” > “Network”.

2. To modify a data port’s IP address, click “Edit”. Data ports are used for data services as opposed to management ports that are used for administrative purposes.

By default, iSCSI normally uses standard 1500 byte frames. You can configure the network to use other Ethernet frame sizes to adjust network performance.

High bandwidth and low latency is desirable for the iSCSI network. The ES NAS can take advantage of a maximum transmission unit (MTU) up to a 9000 byte jumbo frame if the iSCSI network supports larger MTU values.

3. A message notifies you that the associated services will be temporarily stopped. Click “OK” to continue.
4. Configure the IP address for all data ports of both storage controllers on the ES NAS.

Create iSCSI targets and iSCSI LUNs on the ES NAS

1. Log into the ES NAS as an administrator, and then go to “Storage Manager” > “iSCSI Storage”. The Quick Configuration Wizard appears.
2. Select “iSCSI Target with a mapped LUN”, and then click “Next”.  

3. Confirm that the wizard will help you create an iSCSI target with a mapped LUN. Then click “Next.”
4. Enter the target name and alias. The "Data Digest" and "Header Digest" are optional fields (under "CRC/Checksum") and are the parameters for which the iSCSI initiator is verified using cyclic redundancy check.

Header digests: Ensure the validity of the header portion of the protocol data unit (PDU). Data digests: Validate the data segment of the PDU.

Then click “Next” to continue.
5. Enter the CHAP authentication settings and click "Next". Check "Use CHAP authentication" and only the initiator will be authenticated by the iSCSI target, and users of the initiators are required to enter the username and password specified here to access the target. Check "Mutual CHAP" for two-way authentication between the iSCSI target and the initiator. The target authenticates the initiator using the first set of username and password. The initiator authenticates the target using the "Mutual CHAP" settings. Observer the following limitation on username and password:
   - Username limitation: The only valid characters are 0-9, a-z, A-Z and the maximum length is 256 characters.
   - Password limitation: The only valid characters are 0-9, a-z, A-Z and must contain 12-16 characters.

6. Select the interface the target uses for data transfer. Then click “Next”.
7. Specify the access rights for existing hosts to access the target or add a new host (more on add a new host below). Note that at least one host on the list must have the “All Access” access right (you can click the field under “Access” to edit the access right for that host). Click “Next”.

- To add a new host:
  1. Click “Create Host”.
2. Enter the host name in the Host Alias Name field. Click “+” in the “IPv4 Address/Subnet” or “IPv6 Address/Subnet” to add a new host by entering its IP address or network ID with subnet mask using CIDR notation.

3. Select the hosts’ operating system and then click “Apply”.

©2016 QNAP Systems, Inc. All Rights Reserved. 18
4. Confirm your settings and make sure that the access right is “All Access” for the added hosts. Then click “Next”.

5. Create an iSCSI LUN by completing the following:
   - Specify the name of the LUN
   - Choose the LUN allocation method
Thin Provisioning: Allocate the disk space in a flexible manner. The disk space can be allocated to the target anytime regardless of the current storage capacity available on the NAS. Over-allocation is allowed as the storage capacity of the NAS can be expanded using online RAID capacity expansion.

- Instant Allocation: Allocate the disk space to the LUN instantly. This option guarantees the disk space assigned to the LUN but may require more time to create the LUN.

- Choose the LUN location (storage pool on the NAS), the capacity, and the alert threshold.

- Choose the performance profile (generic, Hyper-V, VMware, database, or customized) from the drop-down list. Each option will set a different block size for the created LUN for optimized performance. If you are not sure about which one to choose, select “generic”.

- SSD cache: Enable SSD cache on this share folder. An SSD cache can be used to accelerate the performance of the NAS. Please note that at least one SSD needs to be installed to enable this function.

- Deduplication: ZFS deduplication is the other data reduction method available on the ES NAS. This option allows the system to reduce the amount of storage needed by eliminating duplicate copies of data. However, it must be used with caution as it can become very computationally intensive in some workloads (e.g. streaming workloads). If this option is enabled, it is recommended only to use this shared folder for workloads for which it works well and put other workloads on other shared folders that use compression instead.

- Compression: The ES NAS utilizes ZFS’s inline data reduction, offering compression and deduplication options. When this option is enabled, more CPU resources of the NAS will be used but the size of the shared folder can be reduced.

- Encryption: Enter the encryption password to encrypt the LUN. The password must be 8-16 characters long. Symbols (! @ # $ % ^ & * ( )_+ = ?) are supported. The iSCSI LUN can be encrypted using 256-bit AES encryption to provide data breach protection. Encrypted LUNs can only be mapped to an iSCSI target for normal read/write access with the authorized password. Select “Save the encryption key” for automatic unlocking and mapping the encrypted LUN when the NAS restarts.
6. Confirm the settings and click "Next".

7. Click “Finish” and the target and the mapped LUN will both show up in the list.
Configure Windows Server for iSCSI connections

Use the following procedure to configure network settings of the Windows Server. For more information on configuring TCP/IP settings, see Configure TCP/IP settings on the Microsoft TechNet website.

1. Start Network and Sharing Center by using Control Panel, from the taskbar notification area or from a command prompt.
2. Click any of the connections to configure the connection properties.
3. Click “Properties”.

![Network and Sharing Center](image)

![Ethernet 2 Status](image)

5. Do one of the following:

   - If you want IP settings to be assigned automatically by a DHCP server, VPN server, or other device that provides DHCP services that is installed on the network to which you’re connecting, click “Obtain an IP address automatically”, and then click “OK”.
   
   - If you want to specify an IPv4 address or a Domain Name Service (DNS) server address, do the following:

     Click “Use the following IP address”, and then in “IP address”, type the IP address, and an appropriate subnet mask and default gateway address.

     Click “Use the following DNS server addresses”, and then in “Preferred DNS server” and “Alternate DNS server”, type the addresses of the primary and secondary DNS servers.

   **Note:** We recommend setting a static IP network environment for controlled and more reliable connections.
6. To configure DNS, Windows Internet Name Service (WINS), and IP settings, click “Advanced”.

7. After configuring the IP settings, click “Details” to view the configured network settings.
Enable Jumbo Frame in Windows Server

1. To enable Jumbo Frame support on the Windows Server, click “Configure” in the adaptor’s Properties window.
2. Select the “Advanced” tab. Then select “Jumbo Packet” in the “property” list and choose “9014 Bytes” from the Value drop-down menu.

![Advanced tab of network adapter settings](image)

**Note:** You can use the “ping -l 9000 <NAS IP_address>” to verify whether your iSCSI network supports jumbo frames.
Recommended updates and hotfixes for Windows Server

We recommend the following hotfixes that offer reliability and performance enhancements and protect against security vulnerabilities of the Windows Server. You may choose to install these hotfixes manually or automatically. The updates and hotfixes are organized by operating system version.

Windows Server 2012 R2:


Windows Server 2012:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2796995</td>
<td>Recommended</td>
<td>Offloaded Data Transfers fail on a computer that is running Windows 8 or Windows Server 2012.</td>
</tr>
</tbody>
</table>

Windows Server 2008 R2 SP1:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2684681</td>
<td>Required</td>
<td>Iscsicpl.exe process stops responding when you try to reconnect a storage device to a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.</td>
</tr>
<tr>
<td>2754704</td>
<td>Required</td>
<td>A hotfix is available that provides a mechanism for DSM to notify MPIO that a particular path is back to online in Windows Server 2008 and Windows Server 2008 R2.</td>
</tr>
</tbody>
</table>

Windows Server 2008 R2:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>979711</td>
<td>Required</td>
<td>Stop error message on a computer that is running Windows 7 or Windows Server 2008 R2 and that has iSCSI storage: &quot;0x0000000A&quot;</td>
</tr>
<tr>
<td>2520235</td>
<td>Recommended</td>
<td>&quot;0x0000009E&quot; Stop error when you add an extra storage disk to a failover cluster in Windows Server 2008 R2</td>
</tr>
<tr>
<td>2522766</td>
<td>Required</td>
<td>The MPIO driver fails over all paths incorrectly when a transient single failure occurs in Windows Server 2008 or in Windows Server</td>
</tr>
<tr>
<td>Hotfix</td>
<td>Importance</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2528357</td>
<td>Required</td>
<td>Nonpaged pool leak when you disable and enable some storage controllers in Windows Vista, in Windows 7, in Windows 2008 or in Windows Server 2008 R2</td>
</tr>
<tr>
<td>2684681</td>
<td>Required</td>
<td>Iscsicpl.exe process stops responding when you try to reconnect a storage device to a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2</td>
</tr>
<tr>
<td>2718576</td>
<td>Required</td>
<td>MPIO disk is removed unexpectedly when a PR_IN command fails in a Windows Server 2008 R2 environment</td>
</tr>
<tr>
<td>2754704</td>
<td>Required</td>
<td>A hotfix is available that provides a mechanism for DSM to notify MPIO that a particular path is back to online in Windows Server 2008 and Windows Server 2008 R2</td>
</tr>
</tbody>
</table>

**Windows Server 2008:**

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2684681</td>
<td>Required</td>
<td>Iscsicpl.exe process stops responding when you try to reconnect a storage device to a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2</td>
</tr>
<tr>
<td>2754704</td>
<td>Required</td>
<td>A hotfix is available that provides a mechanism for DSM to notify MPIO that a particular path is back to online in Windows Server 2008 and Windows Server 2008 R2</td>
</tr>
</tbody>
</table>

**Windows Server 2003 (and Windows Server 2003 R2) SP2:**

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>945119</td>
<td>Required</td>
<td>Stop error that is related to the Storport.sys driver on a Windows Server 2003-based computer: &quot;0x000000D1 (parameter1, parameter2, parameter3, parameter4) DRIVER_IRQL_NOT_LESS_OR_EQUAL&quot;</td>
</tr>
<tr>
<td>982109</td>
<td>Required</td>
<td>Access to an MPIO-controlled storage device fails after you disconnect all data cables in Windows Server 2003.</td>
</tr>
</tbody>
</table>
Connect to iSCSI targets using Microsoft iSCSI initiator

The Microsoft iSCSI Software Initiator v2.08 is an official application for Windows hosts and enables connections from them to an external iSCSI storage array through Ethernet network adapters. If you are using Windows Server 2012, Windows Server 2008 R2, Windows 7, Windows Server 2008, and Windows Vista, the Microsoft iSCSI Software Initiator is included by default. For more information (including download links for Microsoft iSCSI Software Initiator v2.08), visit:


**Note:** To configure iSCSI targets in Windows Server with multipath support (MPIO), please refer to the “Configure iSCSI connections with MPIO in Windows Server” section.

Complete the following procedure (demonstrated using Windows Server 2012 R2) to establish a connection from the client computer that is using Microsoft iSCSI Initiator to an iSCSI target device (i.e. the ES NAS).

1. Click “Start”, type “iSCSI” in Start Search, and then under Programs, click “iSCSI Initiator”.
2. If this is the first time that you have launched Microsoft iSCSI Initiator, you receive a prompt that says the Microsoft iSCSI service is not running. You must start the service for Microsoft iSCSI Initiator to run correctly. Click “Yes” to start the service. The Microsoft iSCSI Initiator Properties dialog box opens, and the Targets tab is displayed.

```
Microsoft iSCSI

The Microsoft iSCSI service is not running. The service is required to be started for iSCSI to function correctly. To start the service now and have the service start automatically each time the computer restarts, click the Yes button.

Yes    No
```

3. Click the “Discovery” tab. To add the target portal, click “Discover Portal”, and then in the “Discover Target Portal” dialog box, type the IP address or name of the target portal to connect to. Keep the TCP port to 3260 as the default.
Note: To enter additional settings, such as the outbound IP address (when you are using multiple network adapters), and security settings (such as CHAP), click Advanced.

4. The available iSCSI targets and their status will then be shown under the "Targets" tab. Select the target you wish to connect to and click "Connect".
5. The status of the target should now display "Connected".

**Note:** For more information on Microsoft iSCSI Initiator configuration, visit [Microsoft iSCSI Initiator Step-by-Step Guide](https://technet.microsoft.com/en-us/library/ee423743.aspx) on the Microsoft TechNet website.
Configure iSCSI connections with MPIO in Windows Server

ES NAS support connections from multiple hosts with multiple-port configurations in an iSCSI storage area networking (SAN) environment and utilizes standard Ethernet infrastructure. This allows connectivity of a host computer running a Windows server-class operating system with integrated Multipath I/O (MPIO) support.

Multipath solutions employ a redundant network infrastructure to create interconnecting paths between the server, network and storage device. The alternative paths of the redundant network infrastructure allows for continued access in the event that one or more of these network devices fail.

Each Storage Controller should be connected using such redundant network infrastructure to ensure uninterrupted access to storage. The following diagram is an example of how the configuration should be implemented.

Follow these guidelines when configuring iSCSI connections:

- Do not configure any two Ethernet interfaces on the same subnet. Each Ethernet interface must be on a separate subnet.
- The QES only allows fixed IP address configuration for Ethernet ports designated for data services.
- You should always isolate iSCSI network traffic from your business network traffic by using VLANs or separate Ethernet network hardware.

The following diagram is an example of how the configuration should be implemented.
As ES NAS is a dual-controller NAS that offers failover protection, we strongly recommend using Multipath I/O (MPIO) on iSCSI connections. The following sections demonstrate how to use iSCSI Targets in Windows Server with MPIO. The demonstration uses the following configuration:

- Windows Server 2012 R2 with two 10GbE NICs:
  NIC 1 IP: 8.8.1.90
  NIC 2 IP: 8.8.2.90

- ES NAS Controller A:
  Data port 1: 8.8.1.107
  Data port 2: 8.8.2.107

- ES NAS Controller B:
  Data port 1: 8.8.1.108
  Data port 2: 8.8.2.108

Install the MPIO Service in Windows Server

To install Multipath I/O:

1. Open Server Manager.

   To open Server Manager, click “Start Menu” > “All Apps” > “Server Manager”.

2. In “Dashboard” on the left menu, click “Add roles and features” under “Configure this local server”.

3. In the “Before you begin” step, read the description, and then click “Next”.

©2016 QNAP Systems, Inc. All Rights Reserved. 34
4. In the “Select installation type” step, select “Role-based or feature-based installation”, and then click “Next”.

5. Choose “Select a server from the server pool”, select the Windows Server 2012 R2 (you can identify the server using its IP address) from Server Pool, and then click “Next”.

©2016 QNAP Systems, Inc. All Rights Reserved. 35
6. In the “Select server roles” step, click “Next”.

7. In the “Features” list, find and select “Multipath I/O”, and click “Next”.

©2016 QNAP Systems, Inc. All Rights Reserved. 36
8. On the “Confirm installation selections” window, click “Install”. Then click “Close” when it is finished.
Configure the MPIO Service in Windows Server

Use the following procedure to add MPIO support for iSCSI devices. For more information on Microsoft MPIO, see Microsoft Multipath I/O (MPIO) on the Microsoft TechNet website.

1. In “Dashboard”, click “Tools” > “MPIO” to open the “MPIO Properties” window.

2. Switch to the “Discover Multi-Paths” tab, select “Add support for iSCSI devices” to use Microsoft Multipath I/O (MPIO) with iSCSI Initiator, and then click “Add”.

©2016 QNAP Systems, Inc. All Rights Reserved.
3. Click “Yes” to reboot the server.

![Reboot Required](image)

4. After restarting the computer, log in as a domain administrator and then launch MPIO again. You should see "MSFT2005iSCSI.BusType_0x9" in the Devices list.

![MPIO Properties](image)

Configure and start iSCSI initiator

Complete the following procedure to establish a connection from the client computer that is using Microsoft iSCSI Initiator to an iSCSI target device.

1. Click “Start”, type “iSCSI” in Start Search, and then under Programs, click “iSCSI Initiator”.
2. If this is the first time that you have launched Microsoft iSCSI Initiator, you receive a prompt that says the Microsoft iSCSI service is not running. You must start the service for Microsoft iSCSI Initiator to run correctly. Click “Yes” to start the service. The Microsoft iSCSI Initiator Properties Window opens.
3. Click the “Discovery” tab. To add a target portal, click “Discover Portal”, and then in the “Discover Target Portal” dialog box, type the IP address or name of the target portal to connect to. We will add the IP addresses of the dual controller's data ports (as opposed to the administration ports) that belong to the same subnet. Keep the TCP port to 3260 as the default.
4. The available iSCSI targets and their status will then be shown under the "Targets" tab. (The two targets shown here are owned by each of the two controllers.) Select the target you wish to connect to and click "Connect".
5. Select “Enable multi-path” and click “Advanced”.

6. On the “Advanced Settings” window, select “Microsoft iSCSI Initiator” from the “Local adapter” drop-down menu. Then select an IP address from “Initiator IP” drop-down list and “Target portal IP” drop-down list respectively. Please ensure the Initiator IP and Target portal IP are in the same subnet.

7. Click “OK” to close the window.
8. It shows that one of these iSCSI targets is successfully connected. Select this target and then click “Properties”.

9. On the “Sessions” tab, select “Add session”.
10. Select “Enable multi-path”, and then click “Advanced...”.

11. Add the IP address of the other data port that belongs to a different subnet. Please ensure the Initiator IP and Target portal IP are in the same subnet. Click “OK” to close the window.

12. You should see another session was added. Click “OK” to close the window.
13. Repeat steps 3 to steps 12 to set up the other iSCSI target with MPIO.
14. After configuring both targets with MPIO, add the iSCSI volume and/or device to be persistently bound to the iSCSI service. It ensures that the iSCSI Initiator service will not complete initialization until all persistently bound volumes and devices are available to the computer. Select “Volumes and Devices” tab on the iSCSI Initiator Properties window, and then click “Auto Configure” to automatically configure all available devices. You should see a new volume named as “mpio#disk.........” in the Volume list. Click “OK” to close the window.
Mount iSCSI virtual disks

After the target has been connected, Windows will detect its presence and treat it as if a new hard disk drive has been added. The new iSCSI disk needs to be initialized and formatted before we can use it. For more information on creating and formatting partitions and volume, see Disk Management on the Microsoft TechNet website.

1. In “Dashboard” on the left menu, go to “Tools” (in the top right corner) > “Computer Management”.

2. Under the Storage folder in the left pane, select “Disk Management”. You should see a new disk appears as “Offline” in the bottom panel. Click “Offline” and select “Online” to bring this disk online.
3. The disk status becomes Not Initialized. Before you can use a disk, you must first initialize it. Click on “Not Initialized” and select “Initialize Disk” to initialize this disk.
4. The disk is now initialized. You can now create a volume on it. Click on the disk and select “New Simple Volume”.

5. Follow the on-screen instruction of the “New Simple Volume Wizard” to create a new volume and assign a drive letter to this volume. After the volume is formatted, a new drive
is attached to your PC.

6. Start Windows Explorer. Then click “This PC” and you can now use this iSCSI target as a regular disk partition.
Use iSCSI disks to store Hyper-V virtual machines

Use the following procedure to create a Hyper-V virtual machine that utilizes iSCSI storage. For more information on Hyper-V installation and other related topics, see Install Hyper-V and create a virtual machine on the Microsoft TechNet website.

1. Open Hyper-V Manager. From the navigation pane of Hyper-V Manager, select the computer running Hyper-V. Then from the Actions pane, click “New” and then click “Virtual Machine”.

2. The New Virtual Machine wizard opens. Click “Next” to create a virtual machine with a custom configuration.
3. On the “Specify Name and Location” page, type an appropriate name. Then select “Store the virtual machine in a different location” and click “Browse”.

4. Select the iSCSI drive that we have created to store the virtual machine.
5. Click “Next” to proceed.

6. Specify the generation for the virtual machine. Note that you cannot change its generation once a virtual machine has been created.
7. On the “Assign Memory” page, specify enough memory to start the guest operating system.
8. On the “Configure Networking” page, connect the virtual machine to the switch you created when you installed Hyper-V.

9. On the “Connect Virtual Hard Disk” and the following “Installation Options” pages, choose the option that is appropriate for how you plan to install the guest operating system:

If you will install the guest operating system from a DVD or an image file (an .ISO file), choose “Create a virtual hard disk”. Click “Next”, and then click the option that describes the type of media you will use. For example, to use an .iso file, click “Install an operating system from a bootable CD/DVD” and then specify the path to the .iso file.

If the guest operating system is already installed in a virtual hard disk, choose “Use an existing virtual hard disk” and click “Next”. Then, choose “Install an operating system later”.

©2016 QNAP Systems, Inc. All Rights Reserved. 55
10. On the Summary page, verify your selections and click “Finish”.
Install the guest operating system

1. From Hyper-V Manager, in the “Virtual Machines” section of the results pane, right-click the name of the virtual machine and click “Connect”.
2. The Virtual Machine Connection tool opens.
3. From the “Action” menu in the Virtual Machine Connection window, click “Start”.
4. The virtual machine starts, searches the startup devices, and loads the installation package.
5. Proceed through the installation.
6. Open the Windows Explorer and click the iSCSI drive to view all the installation files or files created on the VM.
High availability and performance optimization

Optimize MPIO policies and performance

Step 1. Open Disk Management, right-click the mounted iSCSI disk, and select Properties.
Step 2. Click on the "MPIO" tab and select the "Round Robin with Subset" in "Select the MPIO policy" field. Round Robin with Subset allows the data to be transmitted only on close to the controller path. Improve transmission efficiency. To test performance, it is recommended to select Least Queue Depth.

Step 3. Click the "Details" button to confirm that "Path Verify Enabled" is checked in DSM Details.
TIPS：MPIO Policy Description

Optimize MPIO high availability fault tolerance timer

Step 1. Press the keyboard Windows key + R button, enter regedit.

Step 2. In "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk" path, find "TimeOutValue", click the right mouse button, then press Modify.
Step 3. Click on the right Decimal option, and then enter the value on the left.

Step 4. Follow the instructions on the next page to modify the value of other registry keys.
**TIPS**: Proposed modification of the registry keys

**Registry Entries for SCSI Miniport Drivers**

Path: HKLM\SYSTEM\CurrentControlSet\Services\Disk

Value Name: TimeOutValue
Description: Timeout (seconds) after the disk is offline.
Default Value: 60
Recommended Value: 60 or adjust as necessary
Range: 1~255

**Microsoft iSCSI Initiator Driver Timers**

Path: HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318\}0001\Parameters

Value Name: DelayBetweenReconnect
Description: When the connection is interrupted, the iSCSI driver attempts to reconnect, log in. Modify this value to adjust the reconnect interval (seconds).
Default Value: 5
Recommended Value: 10

Value Name: LinkDownTime
Description: An I/O request sent, the maximum time to wait (seconds), only to determine the connection is interrupted, and then re-connected again.
Default Value: 15
Recommended Value: 300

*(Continued on next page)*
TIPS: Proposed modification of the registry keys (Continued on the previous page)

Value Name: MaxRequestHoldTime

Description: An I/O request sent out found that the target is lost, the maximum time to wait (seconds), and then reconnect.

Default Value: 60
Recommended Value: 300

Value Name: SrbTimeoutDelta

Description: The system disk driver (such as disk.sys) does not take into account the network latency when deciding on a transmission timeout. This value provides a reference time (in seconds) for network timeouts to these disk drivers.

Default Value: 15
Recommended Value: 300

Microsoft Multipath I/O (MPIO) Timers

Path: HKLM\SYSTEM\CurrentControlSet\Services\mpio\Parameters

Value Name: PathVerificationPeriod

Description: Indicate the time period (in seconds) that MPIO performs path validation.

Default Value: 30
Recommended Value: 30 or adjust as necessary

Value Name: PDORemovePeriod

Description: The amount of time (in seconds) that the MPIO LUN remains in system memory, even if all device paths fail. When this time is exceeded, the I/O operation will fail and the system will no longer attempt to recover the connection path and inform the application that I/O has failed.

Default Value: 20
Recommended Value: 600
TIPS: Proposed modification of the registry keys (Continued on the previous page)

Value Name: RetryCount

Description: The number of times that DSM (device-specific modules) must retry when it determines that an I/O request has failed.

Default Value: 3

Recommended Value: 3 or adjust as necessary

Value Name: RetryInterval

Description: Indicate the time interval (in seconds) that must be retried when DSM (device-specific modules) determines that an I/O request has failed.

Default Value: 1

Recommended Value: 1 or adjust as necessary
Optimize network performance

TIPS: Different brands, network adapter models may need different optimization, the effect may not be the same, here to Intel X540 network card as an example.

Step 1: Open Device Manager, right-click the Data-port where the card, press the "Properties".

![Device Manager screenshot](image)

- Update Driver Software...
- Disable
- Uninstall
- Scan for hardware changes
- Properties
Step 2: Click the "Advanced" page, in "Settings" to find the "Jumbo Packet" item and modify the value to 9000 or 9014 bytes.

Step 3: Click "Interrupt Moderation", and modify the value to Disabled. (This step is optional, if your card is Intel X550, it is recommended to the default value)
Step 4: Click "Performance Options", then press the "Properties" button on the right, turn off "Interrupt Moderation Rate". (This step is optional, if your card is Intel X550, it is recommended to leave the default)
Step 5. Open Windows PowerShell, enter "netsh int tcp set supplemental datacenter", until the screen shows OK.
References

Microsoft iSCSI Initiator Step-by-Step Guide. Retrieved from Microsoft TechNet

Microsoft Multipath I/O (MPIO). Retrieved from Microsoft TechNet

Install Hyper-V and create a virtual machine. Retrieved from Microsoft TechNet

Disk Management. Retrieved from Microsoft TechNet