

StorSimple documentation

Learn how to use Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

About StorSimple

OVERVIEW

[Compare StorSimple with Azure File Sync and Data Box Edge](#)

StorSimple Virtual Array

OVERVIEW

[What is StorSimple Virtual Array?](#)

GET STARTED

[Review requirements](#)

StorSimple 8000 Series

OVERVIEW

[What is StorSimple 8000 Series?](#)

GET STARTED

[Review requirements](#)

StorSimple Data Manager

OVERVIEW

[What is StorSimple Data Manager?](#)

GET STARTED

[Manage in the Azure portal](#)

StorSimple for Cloud Solutions Providers Program

OVERVIEW

[What is the StorSimple for Cloud Solutions Providers Program?](#)

GET STARTED

[Deploy](#)

Introduction to the StorSimple Virtual Array

Article • 03/22/2023 • 12 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Microsoft Azure StorSimple Virtual Array is an integrated storage solution that manages storage tasks between an on-premises virtual array running in a hypervisor and Microsoft Azure cloud storage. The virtual array is an efficient, cost-effective, and easily managed file server or iSCSI server solution that eliminates many of the issues and expenses associated with enterprise storage and data protection. The virtual array is particularly well-suited for the storage of infrequently accessed archival data.

This article provides an overview of the virtual array - here are some other resources:

- For best practices, see [StorSimple Virtual Array best practices](#).
- For an overview of the StorSimple 8000 series devices, go to [StorSimple 8000 series: a hybrid cloud solution](#).

The virtual array supports the iSCSI or Server Message Block (SMB) protocol. It runs on your existing hypervisor infrastructure and provides tiering to the cloud, cloud backup, fast restore, item-level recovery, and disaster recovery features.

The following table summarizes the important features of the StorSimple Virtual Array.

Feature	StorSimple Virtual Array
Installation requirements	Uses virtualization infrastructure (Hyper-V or VMware)
Availability	Single node

Feature	StorSimple Virtual Array
Total capacity (including cloud)	Up to 64 TB of usable capacity per virtual array
Local capacity	390 GB to 6.4 TB of usable capacity per virtual array (need to provision 500 GB to 8 TB of disk space)
Native protocols	iSCSI or SMB
Recovery time objective (RTO)	iSCSI: less than 2 minutes regardless of size
Recovery point objective (RPO)	Daily backups and on-demand backups
Storage tiering	Uses heat mapping to determine what data should be tiered in or out
Support	Virtualization infrastructure supported by the supplier
Performance	Varies depending on underlying infrastructure
Data mobility	Can restore to the same device or do item-level recovery (file server)
Storage tiers	Local hypervisor storage and cloud
Share size	Tiered: up to 20 TB; locally pinned: up to 2 TB
Volume size	Tiered: 500 GB to 5 TB; locally pinned: 50 GB to 200 GB Maximum local reservation for tiered volumes is 200 GB.
Snapshots	Crash consistent
Item-level recovery	Yes; users can restore from shares

Why use StorSimple?

StorSimple connects users and servers to Azure storage in minutes, with no application modification.

The following table describes some of the key benefits that the StorSimple Virtual Array solution provides.

Feature	Benefit
Transparent integration	The virtual array supports the iSCSI or the SMB protocol. The data movement between the local tier and the cloud tier is seamless and transparent to the user.

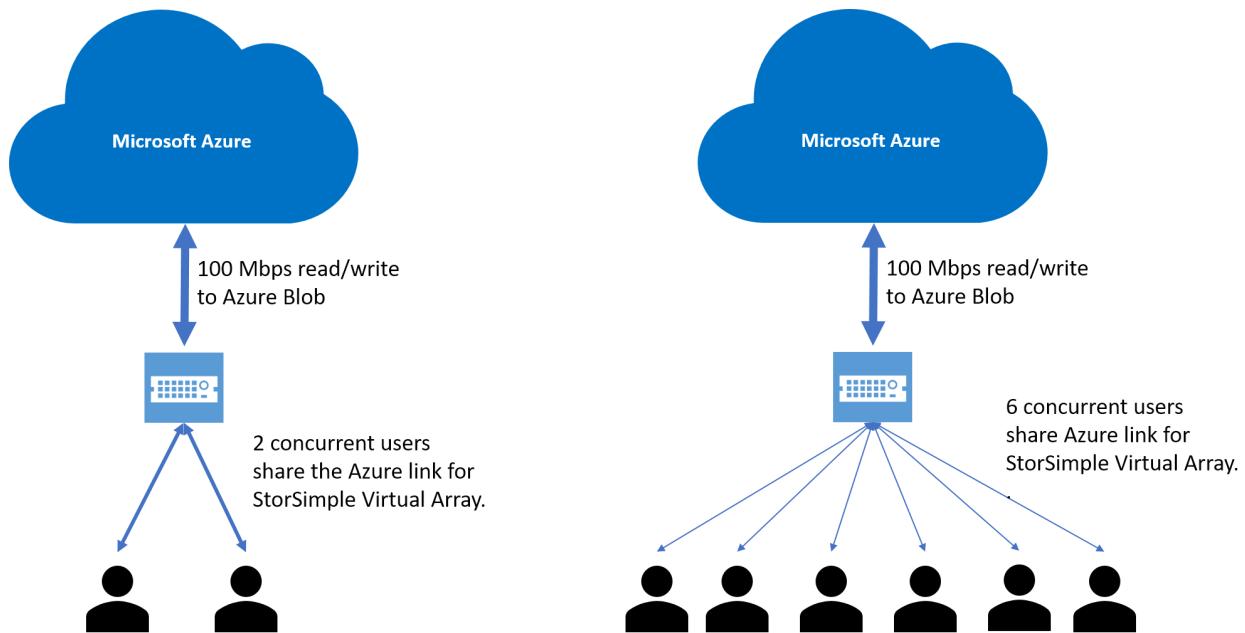
Feature	Benefit
Reduced storage costs	With StorSimple, you provision sufficient local storage to meet current demands for the most used hot data. As storage needs grow, StorSimple tiers cold data into cost-effective cloud storage. The data is deduplicated and compressed before sending to the cloud to further reduce storage requirements and expense.
Simplified storage management	StorSimple provides centralized management in the cloud using StorSimple Device Manager to manage multiple devices.
Improved disaster recovery and compliance	StorSimple facilitates faster disaster recovery by restoring the metadata immediately and restoring the data as needed. Normal operations can continue with minimal disruption.
Data mobility	Data tiered to the cloud can be accessed from other sites for recovery and migration purposes. You can restore data only to the original virtual array. However, you use disaster recovery features to restore the entire virtual array to another virtual array.

StorSimple workload summary

A summary of supported StorSimple workloads is tabulated below.

Scenario	Workload	Supported	Restrictions	Versions applicable
Remote Office/Branch Office (ROBO)	File sharing	Yes	See maximum limits for file server . See system requirements for supported SMB versions .	All versions
Cloud archiving	Archival file sharing	Yes	See maximum limits for file server . See system requirements for supported SMB versions .	All versions

The StorSimple Virtual Array is best suited for infrequently accessed data. While the virtual array has a local cache to boost performance, users should assume that the device services files at the lowest tier of storage (the cloud). Each virtual array can write and read to Azure storage at approximately 100 Mbps. That link is shared across all the requests coming into the device and can become a bottleneck as shown in the diagram below.



When multiple concurrent users access the virtual array, they all share the connection to Azure, leading to a lower performance. There is no guaranteed performance per user, and the device processes individual requests as they arrive.

StorSimple Virtual Array is not suitable for workloads that require high availability. The virtual array is a single-node device that experiences downtime when software updates are installed. Administrators should plan for a maintenance window of 30 minutes 3-4 times per year.

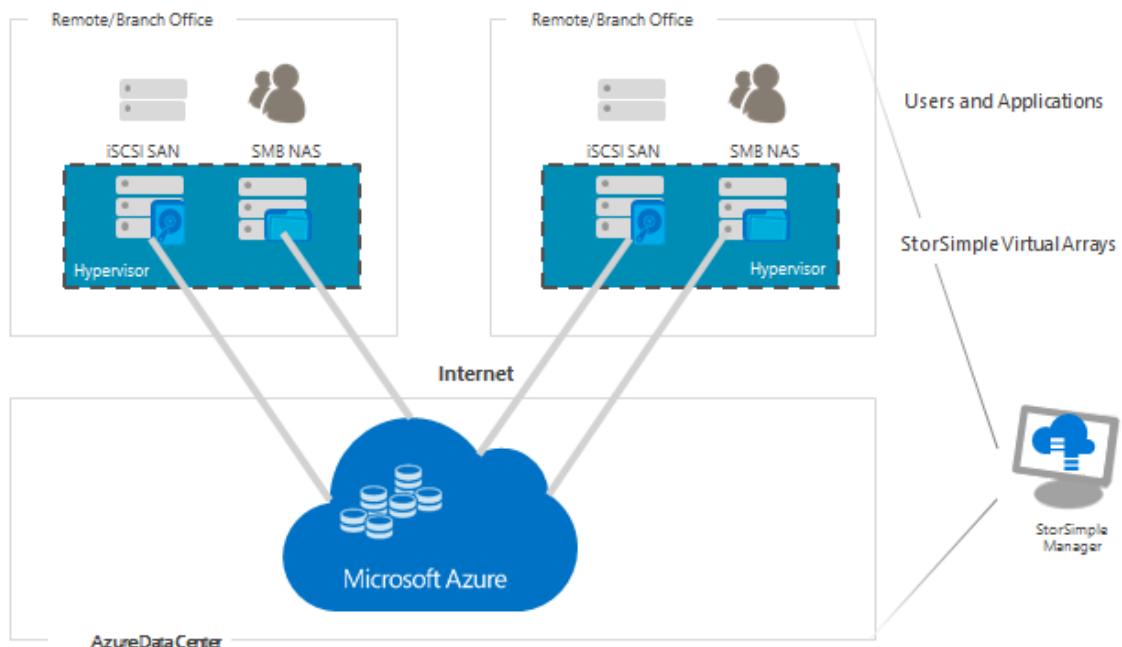
Workflows

The StorSimple Virtual Array is particularly suitable for the following workflows:

- [Cloud-based storage management](#)
- [Location-independent backup](#)
- [Data protection and disaster recovery](#)

Cloud-based storage management

You can use the StorSimple Device Manager service running in the Azure portal to manage data stored on multiple devices and in multiple locations. That is particularly useful in distributed branch scenarios. You must create separate instances of the StorSimple Device Manager service to manage virtual arrays and physical StorSimple devices. The virtual array now uses the new Azure portal instead of the Azure classic portal.



Location-independent backup

With the virtual array, cloud snapshots provide a location-independent, point-in-time copy of a volume or share. Cloud snapshots are enabled by default and cannot be disabled. All volumes and shares are backed up at the same time through a single daily backup policy, and you can take additional ad hoc backups whenever necessary.

Data protection and disaster recovery

The virtual array supports the following data protection and disaster recovery scenarios:

- **Volume or share restore** – Use the restore as new workflow to recover a volume or share. Use this approach to recover the entire volume or share.
- **Item-level recovery** – Shares allow simplified access to recent backups. You can easily recover an individual file from a special `.backup` folder available in the cloud. This restore capability is user-driven and no administrative intervention is required.
- **Disaster recovery** – Use the failover capability to recover all volumes or shares to a new virtual array. You create the new virtual array and register it with the StorSimple Device Manager service, then fail over the original virtual array. The new virtual array will then assume the provisioned resources.

StorSimple Virtual Array components

The virtual array includes the following components:

- [Virtual array](#) – A hybrid cloud storage device based on a virtual machine provisioned in your virtualized environment or hypervisor.
- [StorSimple Device Manager service](#) – An extension of the Azure portal that lets you manage one or more StorSimple devices from a single web interface that you can access from different geographical locations. You can use the StorSimple Device Manager service to create and manage services, view and manage devices and alerts, and manage volumes, shares, and existing snapshots.
- [Local web user interface](#) – A web-based UI used to configure the device so it can connect to the local network, and then register the device with the StorSimple Device Manager service.
- [Command-line interface](#) – A Windows PowerShell interface that you can use to start a support session on the virtual array. The following sections describe each component in greater detail and explains how the solution arranges data, allocates storage, and facilitates storage management and data protection.

Virtual array

The virtual array is a single-node storage solution that provides primary storage, manages communication with cloud storage, and helps to ensure the security and confidentiality of all data stored on the device.

The virtual array is available in one model that is available for download. The virtual array has a maximum capacity of 6.4 TB on the device (with an underlying storage requirement of 8 TB) and 64 TB including cloud storage.

The virtual array has the following features:

- It is cost-effective. It makes use of your existing virtualization infrastructure and can be deployed on your existing Hyper-V or VMware hypervisor.
- It resides in the datacenter and can be configured as an iSCSI server or a file server.
- It is integrated with the cloud.
- Backups are stored in the cloud, which can facilitate disaster recovery and simplify item-level recovery (ILR).
- You can apply updates to the virtual array, just as you would apply them to a physical device.

Note

A virtual array cannot be expanded. Therefore, it's important to provision adequate storage when you create the virtual array.

StorSimple Device Manager service

Microsoft Azure StorSimple provides a web-based user interface, the StorSimple Device Manager service, which enables you to centrally manage StorSimple storage. You can use the StorSimple Device Manager service to perform the following tasks:

- Manage multiple StorSimple Virtual Arrays from a single service.
- Configure and manage security settings for StorSimple Virtual Arrays. (Encryption in the cloud is dependent on Microsoft Azure APIs.)
- Configure storage account credentials and properties.
- Configure and manage volumes or shares.
- Back up and restore data on volumes or shares.
- Monitor performance.
- Review system settings and identify possible problems.

You use the StorSimple Device Manager service to do daily administration of your virtual array.

For more information, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Local web user interface

The virtual array includes a web-based UI that is used for one-time configuration and registration of the device with the StorSimple Device Manager service. You can use it to shut down and restart the virtual array, run diagnostic tests, update software, change the device administrator password, view system logs, and contact Microsoft Support to file a service request.

For information about using the web-based UI, go to [Use the web-based UI to administer your StorSimple Virtual Array](#).

Command-line interface

The included Windows PowerShell interface enables you to initiate a support session with Microsoft Support so they can help you troubleshoot and resolve issues that you might encounter on your virtual array.

Storage management technologies

In addition to the virtual array and other components, the StorSimple solution uses the following software technologies to provide quick access to important data, reduce

storage consumption, and protect data that is stored on your virtual array:

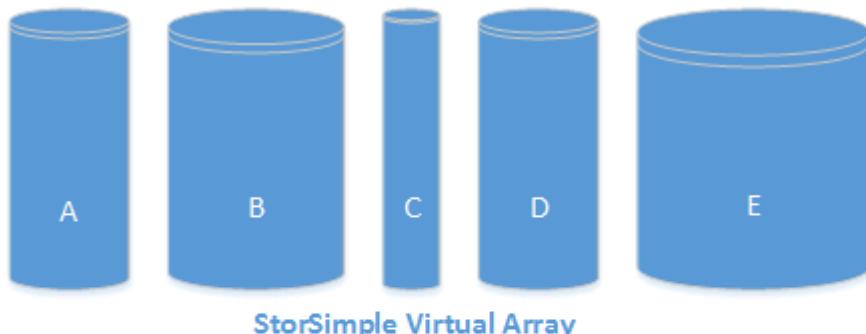
- Automatic storage tiering
- Locally pinned shares and volumes
- Deduplication and compression for data tiered or backed up to the cloud
- Scheduled and on-demand backups

Automatic storage tiering

The virtual array uses a new tiering mechanism to manage stored data across the virtual array and the cloud. There are only two tiers: the local virtual array and Azure cloud storage. The StorSimple Virtual Array automatically arranges data into the tiers based on a heat map, which tracks current usage, age, and relationships to other data. Data that is most active (hottest) is stored locally, while less active and inactive data is automatically migrated to the cloud. (All backups are stored in the cloud.) StorSimple adjusts and rearranges data and storage assignments as usage patterns change. For example, some information might become less active over time. As it becomes progressively less active, it is tiered out to the cloud. If that same data becomes active again, it is tiered in to the storage array.

Data for a particular tiered share or volume is guaranteed its own local tier space (approximately 10 percent of the total provisioned space for that share or volume). While that reduces the available storage on the virtual array for that share or volume, it ensures that tiering for one share or volume will not be affected by the tiering needs of other shares or volumes. Thus, a very busy workload on one share or volume cannot force all other workloads to the cloud.

Tiered volumes created for iSCSI have a maximum local reservation of 200 GB regardless of the size of the volume.



Each file share or volume has its own dedicated local tier space. This is fixed at 10% of the provisioned size of the share or volume, and each share or volume is guaranteed a certain amount of local space that cannot be affected by activity on the other shares or volumes.

Note

You can specify a volume as locally pinned, in which case the data remains on the virtual array and is never tiered to the cloud. For more information, go to [Locally pinned shares and volumes](#).

Important

When using StorSimple, do not convert blobs to archival, even if your device is being phased out. To retrieve data from the device, you'll need to rehydrate the blobs from archival to the hot or cool type, which results in significant costs.

Locally pinned shares and volumes

You can create appropriate shares and volumes as locally pinned. This capability ensures that data required by critical applications remains in the virtual array and is never tiered to the cloud. Locally pinned shares and volumes have the following features:

- They are not subject to cloud latencies or connectivity issues.
- They still benefit from StorSimple cloud backup and disaster recovery features.

You can restore a locally pinned share or volume as tiered or a tiered share or volume as locally pinned.

For more information about locally pinned volumes, go to [Use the StorSimple Device Manager service to manage volumes](#).

Deduplication and compression for data tiered or backed up to the cloud

StorSimple uses deduplication and data compression to further reduce storage requirements in the cloud. Deduplication reduces the overall amount of data stored by eliminating redundancy in the stored data set. As information changes, StorSimple ignores the unchanged data and captures only the changes. In addition, StorSimple reduces the amount of stored data by identifying and removing duplicate information.

Note

Data stored on the virtual array is not deduplicated or compressed. All deduplication and compression occurs just before the data is sent to the cloud.

Scheduled and on-demand backups

StorSimple data protection features enable you to create on-demand backups. Additionally, a default backup schedule ensures that data is backed up daily. Backups are taken in the form of incremental snapshots, which are stored in the cloud. Snapshots, which record only the changes since the last backup, can be created and restored quickly. These snapshots can be critically important in disaster recovery scenarios because they replace secondary storage systems (such as tape backup), and allow you to restore data to your datacenter or to alternate sites if necessary.

Managing personal information

The StorSimple Device Manager for virtual series collects personal information in two key instances:

- Alert user settings where email addresses of users are configured. This information can be cleared by the administrator.
- Users who can access the data on the shares. A list of users who can access the share data is displayed and can be exported. This list is deleted when the share is deleted.

For more information, review the [Microsoft Privacy policy at Trust Center](#).

Next steps

Learn how to [prepare the virtual array portal](#).

StorSimple Virtual Array system requirements

Article • 03/22/2023 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the important system requirements for your Microsoft Azure StorSimple Virtual Array and for the storage clients accessing the array. We recommend that you review the information carefully before you deploy your StorSimple system, and then refer back to it as necessary during deployment and subsequent operation.

The system requirements include:

- **Software requirements for storage clients** - describes the supported virtualization platforms, web browsers, iSCSI initiators, SMB clients, minimum virtual device requirements, and any additional requirements for those operating systems.
- **Networking requirements for the StorSimple device** - provides information about the ports that need to be open in your firewall to allow for iSCSI, cloud, or management traffic.

The StorSimple system requirements information published in this article applies to StorSimple Virtual Arrays only.

- For 8000 series devices, go to [System requirements for your StorSimple 8000 series device](#).

Software requirements

The software requirements include the information on the supported web browsers, SMB versions, virtualization platforms and the minimum virtual device requirements.

Supported virtualization platforms

Hypervisor	Version
Hyper-V	Windows Server 2008 R2 SP1 and later
VMware ESXi	5.0, 5.5, 6.0, and 6.5.

ⓘ Important

Do not install VMware tools on your StorSimple Virtual Array; this will result in an unsupported configuration.

Virtual device requirements

Component	Requirement
Minimum number of virtual processors (cores)	4
Memory (RAM)	8 GB For a file server, 8 GB for less than 2 million files and 16 GB for 2 - 4 million files
Disk space ¹	OS disk - 80 GB Data disk - 500 GB to 8 TB
Minimum number of network interface(s)	1
Internet bandwidth ²	Minimum bandwidth required: 5 Mbps Recommended bandwidth: 100 Mbps The speed of data transfer scales with the Internet bandwidth. For example, 100 GB of data takes 2 days to transfer at 5 Mbps which could lead to backup failures because daily backups would not complete in a day. With a bandwidth of 100 Mbps, 100 GB of data can be transferred in 2.5 hours.

¹ - Thin provisioned

² - Network requirements may vary depending on the daily data change rate. For example, if a device needs to back up 10 GB or more changes during a day, then the daily backup over a 5 Mbps connection could take up to 4.25 hours (if the data could not be compressed or deduplicated).

Supported web browsers

Component	Version	Additional requirements/notes
Microsoft Edge	Latest version	
Internet Explorer	Latest version	Tested with Internet Explorer 11
Google Chrome	Latest version	Tested with Chrome 46

Supported storage clients

The following software requirements are for the iSCSI initiators that access your StorSimple Virtual Array (configured as an iSCSI server).

Supported operating systems	Version required	Additional requirements/notes
Windows Server	2008R2 SP1, 2012, 2012R2	StorSimple can create thinly provisioned and fully provisioned volumes. It cannot create partially provisioned volumes. StorSimple iSCSI volumes are supported for only: <ul style="list-style-type: none">• Simple volumes on Windows basic disks.• Windows NTFS for formatting a volume.

The following software requirements are for the SMB clients that access your StorSimple Virtual Array (configured as a file server).

SMB Version
SMB 2.x
SMB 3.0
SMB 3.02

Important

Do not copy or store files protected by Windows Encrypting File System (EFS) to the StorSimple Virtual Array file server; this will result in an unsupported configuration.

Supported storage format

Only the Azure block blob storage is supported. Page blobs are not supported. More information [about block blobs and page blobs](#).

Networking requirements

The following table lists the ports that need to be opened in your firewall to allow for iSCSI, SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access your device. *Out* or *outbound* refers to the direction in which your StorSimple device sends data externally, beyond the deployment: for example, outbound to the Internet.

Port No. ¹	In or out	Port scope	Required	Notes
TCP 80 (HTTP)	Out	WAN	No	<p>Outbound port is used for Internet access to retrieve updates.</p> <p>The outbound web proxy is user configurable.</p>
TCP 443 (HTTPS)	Out	WAN	Yes	<p>Outbound port is used for accessing data in the cloud.</p> <p>The outbound web proxy is user configurable.</p>
UDP 53 (DNS)	Out	WAN	In some cases; see notes.	<p>This port is required only if you are using an Internet-based DNS server.</p> <p>Note that if deploying a file server, we recommend using local DNS server.</p>
UDP 123 (NTP)	Out	WAN	In some cases; see notes.	<p>This port is required only if you are using an Internet-based NTP server.</p> <p>Note that if deploying a file server, we recommend synchronizing time with your Active Directory domain controllers.</p>

Port No. ¹	In or out	Port scope	Required	Notes
TCP 80 (HTTP)	In	LAN	Yes	<p>This is the inbound port for local UI on the StorSimple device for local management.</p> <p>Note that accessing the local UI over HTTP will automatically redirect to HTTPS.</p>
TCP 443 (HTTPS)	In	LAN	Yes	This is the inbound port for local UI on the StorSimple device for local management.
TCP 3260 (iSCSI)	In	LAN	No	This port is used to access data over iSCSI.

¹ No inbound ports need to be opened on the public Internet.

ⓘ Important

Ensure that the firewall does not modify or decrypt any TLS traffic between the StorSimple device and Azure.

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your virtual array and the StorSimple Device Manager service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. This in turn will require the network administrator to monitor and update firewall rules for your StorSimple as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on StorSimple fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

ⓘ Note

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to **Azure datacenter IP ranges**.

URL pattern	Component/Functionality
<code>https://*.storsimple.windowsazure.com/*</code>	StorSimple Device Manager service
<code>https://*.accesscontrol.windows.net/*</code>	Access Control Service
<code>https://*.servicebus.windows.net/*</code>	Azure Service Bus
<code>https://login.windows.net</code>	Authentication Service
<code>http://*.backup.windowsazure.com</code>	Device registration
<code>https://crl.microsoft.com/pki/*</code>	Certificate revocation
<code>https://www.microsoft.com/pki/*</code>	
<code>https://*.core.windows.net/*</code>	Azure storage accounts and monitoring
<code>https://*.data.microsoft.com</code>	
<code>http://*.msftncsi.com</code>	
<code>https://*.windowsupdate.microsoft.com</code>	Microsoft Update servers
<code>https://*.windowsupdate.microsoft.com</code>	
<code>https://*.update.microsoft.com</code>	
<code>https://*.update.microsoft.com</code>	
<code>http://*.windowsupdate.com</code>	
<code>https://download.microsoft.com</code>	
<code>http://wustat.windows.com</code>	
<code>https://ntservicepack.microsoft.com</code>	
<code>http://*.deploy.akamaitechnologies.com</code>	Akamai CDN
<code>https://*.partners.extranet.microsoft.com/*</code>	Support package
<code>https://*.data.microsoft.com</code>	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry

Next steps

- Prepare the portal to deploy your StorSimple Virtual Array

What are StorSimple Virtual Array limits?

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Consider these limits as you plan, deploy, and operate your Microsoft Azure StorSimple Virtual Array. The following table describes these limits for the virtual device.

StorSimple Virtual Array limits

Limit identifier	Limit	Comments
Total capacity (including cloud)	Up to 64 TB per virtual device	You can fail over a full StorSimple Virtual Array to another empty array. If you try to restore to the same device, ensure that you have sufficient space on the device to complete this operation. After you have exceeded 32 TB, you cannot restore to the same device.
Maximum number of storage account credentials per device	1	
Maximum number of volumes/shares	16	
Minimum size of a tiered share	500 GB	
Minimum size of a tiered volume	500 GB	

Limit identifier	Limit	Comments
Maximum size of a tiered share	20 TB	
Maximum size of a tiered volume	5 TB	
Minimum size of a locally pinned share	50 GB	
Minimum size of a locally pinned volume	50 GB	
Maximum size of a locally pinned share	2 TB	
Maximum size of a locally pinned volume	200 GB	
Maximum number of iSCSI connections from initiators	512	
Maximum number of access control records per device	64	
Maximum number of backups retained by the virtual device in <i>.backups</i> folder for file server	5	This includes the most recent scheduled (generated by the default backup policy) and manual backups.
Maximum number of scheduled backups retained by the device	55	30 daily backups 12 monthly backups 13 yearly backups
Maximum number of manual backups retained by the device	45	
Maximum number of files per share for a file server	1 million	When performing a device restore, the restore times are proportional to number of files across all the shares on the device.

Limit identifier	Limit	Comments
Maximum number of files per volume for an iSCSI server	1 million	
Maximum number of files per virtual array	4 million	
Restore recover time	Quick restore	<p>The restore is based on the heat map and depends on the volume size.</p> <p>Backup operations can occur while a restore operation is in progress.</p>

StorSimple Virtual Array best practices

Article • 08/19/2022 • 22 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Microsoft Azure StorSimple Virtual Array is an integrated storage solution that manages storage tasks between an on-premises virtual device running in a hypervisor and Microsoft Azure cloud storage. StorSimple Virtual Array is an efficient, cost-effective alternative to the 8000 series physical array. The virtual array can run on your existing hypervisor infrastructure, supports both the iSCSI and the SMB protocols, and is well-suited for remote office/branch office scenarios. For more information on the StorSimple solutions, go to [Microsoft Azure StorSimple Overview](#).

This article covers the best practices implemented during the initial setup, deployment, and management of the StorSimple Virtual Array. These best practices provide validated guidelines for the setup and management of your virtual array. This article is targeted towards the IT administrators who deploy and manage the virtual arrays in their datacenters.

We recommend a periodic review of the best practices to help ensure your device is still in compliance when changes are made to the setup or operation flow. Should you encounter any issues while implementing these best practices on your virtual array, [contact Microsoft Support](#) for assistance.

Configuration best practices

These best practices cover the guidelines that need to be followed during the initial setup and deployment of the virtual arrays. These best practices include those related to the provisioning of the virtual machine, group policy settings, sizing, setting up the

networking, configuring storage accounts, and creating shares and volumes for the virtual array.

Provisioning

StorSimple Virtual Array is a virtual machine (VM) provisioned on the hypervisor (Hyper-V or VMware) of your host server. When provisioning the virtual machine, ensure that your host is able to dedicate sufficient resources. For more information, go to [minimum resource requirements](#) to provision an array.

Implement the following best practices when provisioning the virtual array:

	Hyper-V	VMware
Virtual machine type	Generation 2 VM for use with Windows Server 2012 or later and a .vhdx image. Generation 1 VM for use with a Windows Server 2008 or later and a .vhd image.	Use virtual machine version 8 when using .vmdk image.
Memory type	Configure as static memory . Do not use the dynamic memory option.	
Data disk type	Provision as dynamically expanding . Fixed size takes a long time. Do not use the differencing option.	Use the thin provision option.
Data disk modification	Expansion or shrinking is not allowed. An attempt to do so results in the loss of all the local data on device.	Expansion or shrinking is not allowed. An attempt to do so results in the loss of all the local data on device.

Sizing

When sizing your StorSimple Virtual Array, consider the following factors:

- Local reservation for volumes or shares. Approximately 12% of the space is reserved on the local tier for each provisioned tiered volume or share. Roughly 10% of the space is also reserved for a locally pinned volume for file system.
- Snapshot overhead. Roughly 15% space on the local tier is reserved for snapshots.

- Need for restores. If doing restore as a new operation, sizing should account for the space needed for restore. Restore is done to a share or volume of the same size.
- Some buffer should be allocated for any unexpected growth.

Based on the preceding factors, the sizing requirements can be represented by the following equation:

```
Total usable local disk size = (Total provisioned locally pinned volume/share size including space for file system) + (Max (local reservation for a volume/share) for all tiered volumes/share) + (Local reservation for all tiered volumes/shares)
```

```
Data disk size = Total usable local disk size + Snapshot overhead + buffer for unexpected growth or new share or volume
```

The following examples illustrate how you can size a virtual array based on your requirements.

Example 1:

On your virtual array, you want to be able to

- provision a 2-TB tiered volume or share.
- provision a 1-TB tiered volume or share.
- provision a 300-GB of locally pinned volume or share.

For the preceding volumes or shares, let us calculate the space requirements on the local tier.

First, for each tiered volume/share, local reservation would be equal to 12% of the volume/share size. For the locally pinned volume/share, local reservation is 10 % of the locally pinned volume/share size (in addition to the provisioned size). In this example, you need

- 240-GB local reservation (for a 2-TB tiered volume/share)
- 120-GB local reservation (for a 1-TB tiered volume/share)
- 330-GB for locally pinned volume or share (adding 10 % of local reservation to the 300 GB provisioned size)

The total space required on the local tier so far is: 240 GB + 120 GB + 330 GB = 690 GB.

Second, we need at least as much space on the local tier as the largest single reservation. This extra amount is used in case you need to restore from a cloud snapshot. In this example, the largest local reservation is 330 GB (including reservation

for file system), so you would add that to the 690 GB: $690 \text{ GB} + 330 \text{ GB} = 1020 \text{ GB}$. If we performed subsequent additional restores, we can always free up the space from the previous restore operation.

Third, we need 15 % of your total local space so far to store local snapshots, so that only 85% of it is available. In this example, that would be around $1020 \text{ GB} = 0.85 \times \text{provisioned data disk TB}$. So, the provisioned data disk would be $(1020 * (1/0.85)) = 1200 \text{ GB} = 1.20 \text{ TB} \sim 1.25 \text{ TB}$ (rounding off to nearest quartile)

Factoring in unexpected growth and new restores, you should provision a local disk of around 1.25 - 1.5 TB.

Note

We also recommend that the local disk is thinly provisioned. This recommendation is because the restore space is only needed when you want to restore data that is older than five days. Item-level recovery allows you to restore data for the last five days without requiring the extra space for restore.

Example 2:

On your virtual array, you want to be able to

- provision a 2-TB tiered volume
- provision a 300-GB locally pinned volume

Based on 12 % of local space reservation for tiered volumes/shares and 10 % for locally pinned volumes/shares, we need

- 240-GB local reservation (for 2 TB tiered volume/share)
- 330-GB for locally pinned volume or share (adding 10% of local reservation to the 300 GB provisioned space)

Total space required on the local tier is: $240 \text{ GB} + 330 \text{ GB} = 570 \text{ GB}$

The minimum local space needed for restore is 330 GB.

15 % of your total disk is used to store snapshots so that only 0.85 is available. So, the disk size is $(900 * (1/0.85)) = 1.06 \text{ TB} \sim 1.25 \text{ TB}$ (rounding off to nearest quartile)

Factoring in any unexpected growth, you can provision a 1.25 - 1.5 TB local disk.

Group policy

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory Domain Services (AD DS) containers: sites, domains, or organizational units (OUs).

If your virtual array is domain-joined, GPOs can be applied to it. These GPOs can install applications such as an antivirus software that can adversely impact the operation of the StorSimple Virtual Array.

Therefore, we recommend that you:

- Ensure that your virtual array is in its own organizational unit (OU) for Active Directory.
- Make sure that no group policy objects (GPOs) are applied to your virtual array. You can block inheritance to ensure that the virtual array (child node) does not automatically inherit any GPOs from the parent. For more information, go to [block inheritance](#).

Networking

The network configuration for your virtual array is done through the local web UI. A virtual network interface is enabled through the hypervisor in which the virtual array is provisioned. Use the [Network Settings](#) page to configure the virtual network interface IP address, subnet, and gateway. You can also configure the primary and secondary DNS server, time settings, and optional proxy settings for your device. Most of the network configuration is a one-time setup. Review the [StorSimple networking requirements](#) prior to deploying the virtual array.

When deploying your virtual array, we recommend that you follow these best practices:

- Ensure that the network in which the virtual array is deployed always has the capacity to dedicate 5-Mbps Internet bandwidth (or more).
 - Internet bandwidth need varies depending on your workload characteristics and the rate of data change.
 - The data change that can be handled is directly proportional to your Internet bandwidth. As an example when taking a backup, a 5 Mbps bandwidth can accommodate a data change of around 18 GB in 8 hours. With four times more bandwidth (20 Mbps), you can handle four times more data change (72 GB).
- Ensure connectivity to the Internet is always available. Sporadic or unreliable Internet connections to the devices may result in a loss of access to data in the cloud and could result in an unsupported configuration.

- If you plan to deploy your device as an iSCSI server:
 - We recommend that you disable the **Get IP address automatically** option (DHCP).
 - Configure static IP addresses. You must configure a primary and a secondary DNS server.
 - If defining multiple network interfaces on your virtual array, only the first network interface (by default, this interface is **Ethernet**) can reach the cloud. To control the type of traffic, you can create multiple virtual network interfaces on your virtual array (configured as an iSCSI server) and connect those interfaces to different subnets.
- To throttle the cloud bandwidth only (used by the virtual array), configure throttling on the router or the firewall. If you define throttling in your hypervisor, it will throttle all the protocols including iSCSI and SMB instead of just the cloud bandwidth.
- Ensure that time synchronization for hypervisors is enabled. If using Hyper-V, select your virtual array in the Hyper-V Manager, go to **Settings > Integration Services**, and ensure that the **Time synchronization** is checked.

Storage accounts

StorSimple Virtual Array can be associated with a single storage account. This storage account could be an automatically generated storage account, an account in the same subscription as the service, or a storage account related to another subscription. For more information, see how to [manage storage accounts for your virtual array](#).

Use the following recommendations for storage accounts associated with your virtual array.

- When linking multiple virtual arrays with a single storage account, factor in the maximum capacity (64 TB) for a virtual array and the maximum size (500 TB) for a storage account. This limits the number of full-sized virtual arrays that can be associated with that storage account to about 7.
- When creating a new storage account
 - We recommend that you create it in the region closest to the remote office/branch office where your StorSimple Virtual Array is deployed to minimize latencies.
 - Bear in mind that you cannot move a storage account across different regions. Also you cannot move a service across subscriptions.

- Use a storage account that implements redundancy between the datacenters. Geo-Redundant Storage (GRS), Zone Redundant Storage (ZRS), and Locally Redundant Storage (LRS) are all supported for use with your virtual array. For more information on the different types of storage accounts, go to [Azure storage replication](#).

Shares and volumes

For your StorSimple Virtual Array, you can provision shares when it is configured as a file server and volumes when configured as an iSCSI server. The best practices for creating shares and volumes are related to the size and the type configured.

Volume/Share size

On your virtual array, you can provision shares when it is configured as a file server and volumes when configured as an iSCSI server. The best practices for creating shares and volumes relate to the size and the type configured.

Keep in mind the following best practices when provisioning shares or volumes on your virtual device.

- The file sizes relative to the provisioned size of a tiered share can impact the tiering performance. Working with large files could result in a slow tier out. When working with large files, we recommend that the largest file is smaller than 3% of the share size.
- A maximum of 16 volumes/shares can be created on the virtual array. For the size limits of the locally pinned and tiered volumes/shares, always refer to the [StorSimple Virtual Array limits](#).
- When creating a volume, factor in the expected data consumption as well as future growth. The volume or share cannot be expanded later.
- Once the volume/share has been created, you cannot shrink the size of the volume/share on StorSimple.
- When writing to a tiered volume on StorSimple, when the volume data reaches a certain threshold (relative to the local space reserved for the volume), the IO is throttled. Continuing to write to this volume slows down the IO significantly.

Though you can write to a tiered volume beyond its provisioned capacity (we do not actively stop the user from writing beyond the provisioned capacity), you see an alert notification to the effect that you have oversubscribed. Once you see the alert, it is imperative that you take remedial measures such as delete the volume data (volume expansion is currently not supported).

- For disaster recovery use cases, as the number of allowable shares/volumes is 16 and the maximum number of shares/volumes that can be processed in parallel is also 16, the number of shares/volumes does not have a bearing on your RPO and RTOs.

Volume/Share type

StorSimple supports two volume/share types based on the usage: locally pinned and tiered. Locally pinned volumes/shares are thickly provisioned whereas the tiered volumes/shares are thinly provisioned. You cannot convert a locally pinned volume/share to tiered or *vice versa* once created.

We recommend that you implement the following best practices when configuring StorSimple volumes/shares:

- Identify the volume type based on the workloads that you intend to deploy before you create a volume. Use locally pinned volumes for workloads that require local guarantees of data (even during a cloud outage) and that require low cloud latencies. Once you create a volume on your virtual array, you cannot change the volume type from locally pinned to tiered or *vice-versa*. As an example, create locally pinned volumes when deploying SQL workloads or workloads hosting virtual machines (VMs); use tiered volumes for file share workloads.

Volume format

After you create StorSimple volumes on your iSCSI server, you need to initialize, mount, and format the volumes. This operation is performed on the host connected to your StorSimple device. Following best practices are recommended when mounting and formatting volumes on the StorSimple host.

- Perform a quick format on all StorSimple volumes.
- When formatting a StorSimple volume, use an allocation unit size (AUS) of 64 KB (default is 4 KB). The 64 KB AUS is based on testing done in-house for common StorSimple workloads and other workloads.
- When using the StorSimple Virtual Array configured as an iSCSI server, do not use spanned volumes or dynamic disks as these volumes or disks are not supported by StorSimple.

Share access

When creating shares on your virtual array file server, follow these guidelines:

- When creating a share, assign a user group as a share administrator instead of a single user.
- You can manage the NTFS permissions after the share is created by editing the shares through Windows Explorer.

Volume access

When configuring the iSCSI volumes on your StorSimple Virtual Array, it is important to control access wherever necessary. To determine which host servers can access volumes, create, and associate access control records (ACRs) with StorSimple volumes.

Use the following best practices when configuring ACRs for StorSimple volumes:

- Always associate at least one ACR with a volume.
- When assigning more than one ACR to a volume, ensure that the volume is not exposed in a way where it can be concurrently accessed by more than one non-clustered host. If you have assigned multiple ACRs to a volume, a warning message pops up for you to review your configuration.

Data security and encryption

Your StorSimple Virtual Array has data security and encryption features that ensure the confidentiality and integrity of your data. When using these features, it is recommended that you follow these best practices:

- Define a cloud storage encryption key to generate AES-256 encryption before the data is sent from your virtual array to the cloud. This key is not required if your data is encrypted to begin with. The key can be generated and kept safe using a key management system such as [Azure key vault](#).
- When configuring the storage account via the StorSimple Manager service, make sure that you enable the TLS mode to create a secure channel for network communication between your StorSimple device and the cloud.
- Regenerate the keys for your storage accounts (by accessing the Azure Storage service) periodically to account for any changes to access based on the changed list of administrators.
- Data on your virtual array is compressed and deduplicated before it is sent to Azure. We don't recommend using the Data Deduplication role service on your Windows Server host.

Operational best practices

The operational best practices are guidelines that should be followed during the day-to-day management or operation of the virtual array. These practices cover specific management tasks such as taking backups, restoring from a backup set, performing a failover, deactivating and deleting the array, monitoring system usage and health, and running virus scans on your virtual array.

Backups

The data on your virtual array is backed up to the cloud in two ways, a default automated daily backup of the entire device starting at 22:30 or via a manual on-demand backup. By default, the device automatically creates daily cloud snapshots of all the data residing on it. For more information, go to [back up your StorSimple Virtual Array](#).

The frequency and retention associated with the default backups cannot be changed but you can configure the time at which the daily backups are initiated every day. When configuring the start time for the automated backups, we recommend that:

- Schedule your backups for off-peak hours. Backup start time should not coincide with numerous host IO.
- Initiate a manual on-demand backup when planning to perform a device failover or prior to the maintenance window, to protect the data on your virtual array.

Restore

You can restore from a backup set in two ways: restore to another volume or share or perform an item-level recovery (available only on a virtual array configured as a file server). Item-level recovery allows you to do a granular recovery of files and folders from a cloud backup of all the shares on the StorSimple device. For more information, go to [restore from a backup](#).

When performing a restore, keep the following guidelines in mind:

- Your StorSimple Virtual Array does not support in-place restore. This can however be readily achieved by a two-step process: make space on the virtual array and then restore to another volume/share.
- When restoring from a local volume, keep in mind the restore will be a long running operation. Though the volume may quickly come online, the data continues to be hydrated in the background.
- The volume type remains the same during the restore process. A tiered volume is restored to another tiered volume and a locally pinned volume to another locally pinned volume.

- When trying to restore a volume or a share from a backup set, if the restore job fails, a target volume or share may still be created in the portal. It is important that you delete this unused target volume or share in the portal to minimize any future issues arising from this element.

Failover and disaster recovery

A device failover allows you to migrate your data from a *source* device in the datacenter to another *target* device located in the same or a different geographical location. The device failover is for the entire device. During failover, the cloud data for the source device changes ownership to that of the target device.

For your StorSimple Virtual Array, you can only fail over to another virtual array managed by the same StorSimple Manager service. A failover to an 8000 series device or an array managed by a different StorSimple Manager service (than the one for the source device) is not allowed. To learn more about the failover considerations, go to [prerequisites for the device failover](#).

When performing a fail over for your virtual array, keep the following in mind:

- For a planned failover, it is a recommended best practice to take all the volumes/shares offline prior to initiating the failover. Follow the operating system-specific instructions to take the volumes/shares offline on the host first and then take those offline on your virtual device.
- For a file server disaster recovery (DR), we recommend that you join the target device to the same domain as the source so that the share permissions are automatically resolved. Only the failover to a target device in the same domain is supported in this release.
- Once the DR is successfully completed, the source device is automatically deleted. Though the device is no longer available, the virtual machine that you provisioned on the host system is still consuming resources. We recommend that you delete this virtual machine from your host system to prevent any charges from accruing.
- Do note that even if the failover is unsuccessful, **the data is always safe in the cloud**. Consider the following three scenarios in which the failover did not complete successfully:
 - A failure occurred in the initial stages of the failover such as when the DR pre-checks are being performed. In this situation, your target device is still usable. You can retry the failover on the same target device.
 - A failure occurred during the actual failover process. In this case, the target device is marked unusable. You must provision and configure another target

virtual array and use that for failover.

- The failover was complete following which the source device was deleted but the target device has issues and you cannot access any data. The data is still safe in the cloud and can be easily retrieved by creating another virtual array and then using it as a target device for the DR.

Deactivate

When you deactivate a StorSimple Virtual Array, you sever the connection between the device and the corresponding StorSimple Manager service. Deactivation is a **permanent** operation and cannot be undone. A deactivated device cannot be registered with the StorSimple Manager service again. For more information, go to [deactivate and delete your StorSimple Virtual Array](#).

Keep the following best practices in mind when deactivating your virtual array:

- Take a cloud snapshot of all the data prior to deactivating a virtual device. When you deactivate a virtual array, all the local device data is lost. Taking a cloud snapshot will allow you to recover data at a later stage.
- Before you deactivate a StorSimple Virtual Array, make sure to stop or delete clients and hosts that depend on that device.
- Delete a deactivated device if you are no longer using so that it doesn't accrue charges.

Monitoring

To ensure that your StorSimple Virtual Array is in a continuous healthy state, you need to monitor the array and ensure that you receive information from the system including alerts. To monitor the overall health of the virtual array, implement the following best practices:

- Configure monitoring to track the disk usage of your virtual array data disk as well as the OS disk. If running Hyper-V, you can use a combination of System Center Virtual Machine Manager (SCVMM) and System Center Operations Manager to monitor your virtualization hosts.
- Configure email notifications on your virtual array to send alerts at certain usage levels.

Index search and virus scan applications

A StorSimple Virtual Array can automatically tier data from the local tier to the Microsoft Azure cloud. When an application such as an index search or a virus scan is used to scan the data stored on StorSimple, you need to take care that the cloud data does not get accessed and pulled back to the local tier.

We recommend that you implement the following best practices when configuring the index search or virus scan on your virtual array:

- Disable any automatically configured full scan operations.
- For tiered volumes, configure the index search or virus scan application to perform an incremental scan. This would scan only the new data likely residing on the local tier. The data that is tiered to the cloud is not accessed during an incremental operation.
- Ensure the correct search filters and settings are configured so that only the intended types of files get scanned. For example, image files (JPEG, GIF, and TIFF) and engineering drawings should not be scanned during the incremental or full index rebuild.

If using Windows indexing process, follow these guidelines:

- Do not use the Windows Indexer for tiered volumes as it recalls large amounts of data (TBs) from the cloud if the index needs to be rebuilt frequently. Rebuilding the index would retrieve all file types to index their content.
- Use the Windows indexing process for locally pinned volumes as this would only access data on the local tiers to build the index (the cloud data will not be accessed).

Byte range locking

Applications can lock a specified range of bytes within the files. If byte range locking is enabled on the applications that are writing to your StorSimple, then tiering does not work on your virtual array. For the tiering to work, all areas of the files accessed should be unlocked. Byte range locking is not supported with tiered volumes on your virtual array.

Recommended measures to alleviate byte range locking include:

- Turn off byte range locking in your application logic.
- Use locally pinned volumes (instead of tiered) for the data associated with this application. Locally pinned volumes do not tier into the cloud.
- When using locally pinned volumes with byte range locking enabled, the volume can come online before the restore is complete. In these instances, you must wait for the restore to be complete.

Multiple arrays

Multiple virtual arrays may need to be deployed to account for a growing working set of data that could spill onto the cloud thus affecting the performance of the device. In these instances, it is best to scale devices as the working set grows. This requires one or more devices to be added in the on-premises data center. When adding the devices, you could:

- Split the current set of data.
- Deploy new workloads to new device(s).
- If deploying multiple virtual arrays, we recommend that from load-balancing perspective, distribute the array across different hypervisor hosts.
- Multiple virtual arrays (when configured as a file server or an iSCSI server) can be deployed in a Distributed File System Namespace. For detailed steps, go to [Distributed File System Namespace Solution with Hybrid Cloud Storage Deployment Guide](#). Distributed File System Replication is currently not recommended for use with the virtual array.

See also

Learn how to [administer your StorSimple Virtual Array](#) via the StorSimple Manager service.

Deploy StorSimple Virtual Array - Prepare the Azure portal

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Overview

This is the first article in the series of deployment tutorials required to completely deploy your virtual array as a file server or an iSCSI server using the Resource Manager model. This article describes the preparation required to create and configure your StorSimple Device Manager service prior to provisioning a virtual array. This article also links out to a deployment configuration checklist and configuration prerequisites.

You need administrator privileges to complete the setup and configuration process. We recommend that you review the deployment configuration checklist before you begin. The portal preparation takes less than 10 minutes.

The information published in this article applies to the deployment of StorSimple Virtual Arrays in the Azure portal and Microsoft Azure Government Cloud.

Get started

The deployment workflow consists of preparing the portal, provisioning a virtual array in your virtualized environment, and completing the setup. To get started with the StorSimple Virtual Array deployment as a file server or an iSCSI server, you need to refer to the following tabulated resources.

Deployment articles

To deploy your StorSimple Virtual Array, refer to the following articles in the prescribed sequence.

#	In this step	You do this ...	And use these documents.
1.	Set up the Azure portal	Create and configure your StorSimple Device Manager service prior to provisioning a StorSimple Virtual Array.	Prepare the portal
2.	Provision the Virtual Array	For Hyper-V, provision and connect to a StorSimple Virtual Array on a host system running Hyper-V on Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.	Provision a virtual array in Hyper-V
		For VMware, provision and connect to a StorSimple Virtual Array on a host system running VMware ESXi 5.0, 5.5, 6.0 or 6.5.	Provision a virtual array in VMware
3.	Set up the Virtual Array	For your file server, perform initial setup, register your StorSimple file server, and complete the device setup. You can then provision SMB shares.	Set up virtual array as file server
		For your iSCSI server, perform initial setup, register your StorSimple iSCSI server, and complete the device setup. You can then provision iSCSI volumes.	Set up virtual array as iSCSI server

You can now begin to set up the Azure portal.

Configuration checklist

The configuration checklist describes the information that you need to collect before you configure the software on your StorSimple Virtual Array. Preparing this information ahead of time helps streamline the process of deploying the StorSimple device in your environment. Depending upon whether your StorSimple Virtual Array is deployed as a file server or an iSCSI server, you need one of the following checklists.

- Download the [StorSimple Virtual Array File Server Configuration Checklist ↗](#).

- Download the [StorSimple Virtual Array iSCSI Server Configuration Checklist](#).

Prerequisites

Here you find the configuration prerequisites for your StorSimple Device Manager service, your StorSimple Virtual Array, and the datacenter network.

For the StorSimple Device Manager service

Before you begin, make sure that:

- You have your Microsoft account with access credentials.
- You have your Microsoft Azure storage account with access credentials.
- Your Microsoft Azure subscription should be enabled for StorSimple Device Manager service.

For the StorSimple Virtual Array

Before you deploy a virtual array, make sure that:

- You have access to a host system running Hyper-V on Windows Server 2008 R2 or later or VMware (ESXi 5.0, 5.5, 6.0 or 6.5) that can be used to provision a device.
- The host system is able to dedicate the following resources to provision your virtual array:
 - A minimum of 4 cores.
 - At least 8 GB of RAM. If you plan to configure the virtual array as file server, 8 GB supports 2 million files. You need 16 GB RAM to support 2 - 4 million files.
 - One network interface.
 - A 500 GB virtual disk for system data.

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured as per the networking requirements for your StorSimple device. For more information, see the [StorSimple Virtual Array System Requirements](#).
- Your StorSimple Virtual Array has a dedicated 5 Mbps Internet bandwidth (or more) available at all times. This bandwidth should not be shared with any other applications.

Step-by-step preparation

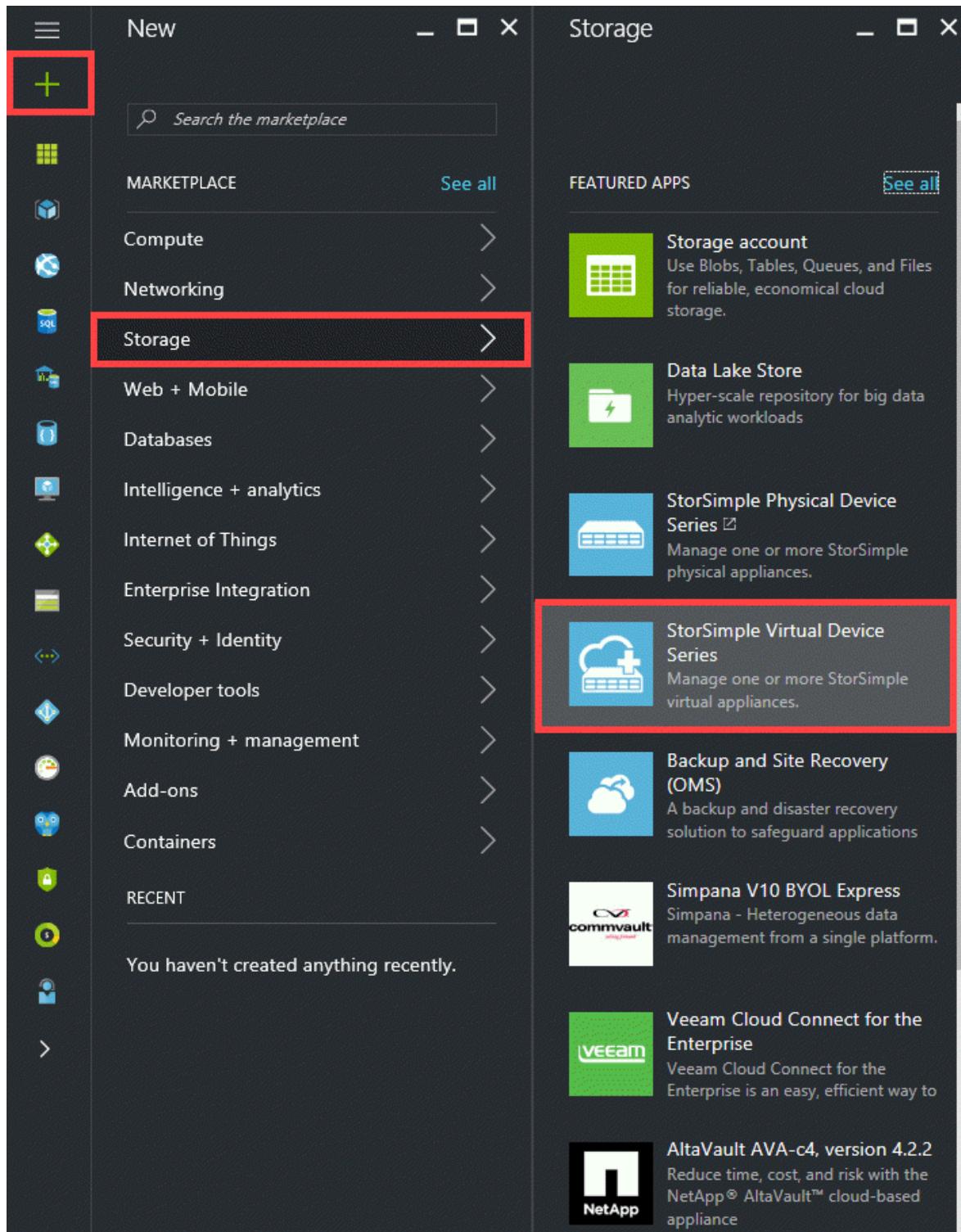
Use the following step-by-step instructions to prepare your portal for the StorSimple Device Manager service.

Step 1: Create a new service

A single instance of the StorSimple Device Manager service can manage multiple StorSimple Virtual Arrays. Perform the following steps to create an instance of the StorSimple Device Manager service. If you have an existing StorSimple Device Manager service to manage your virtual arrays, skip this step and go to [Step 2: Get the service registration key](#).

To create a new service

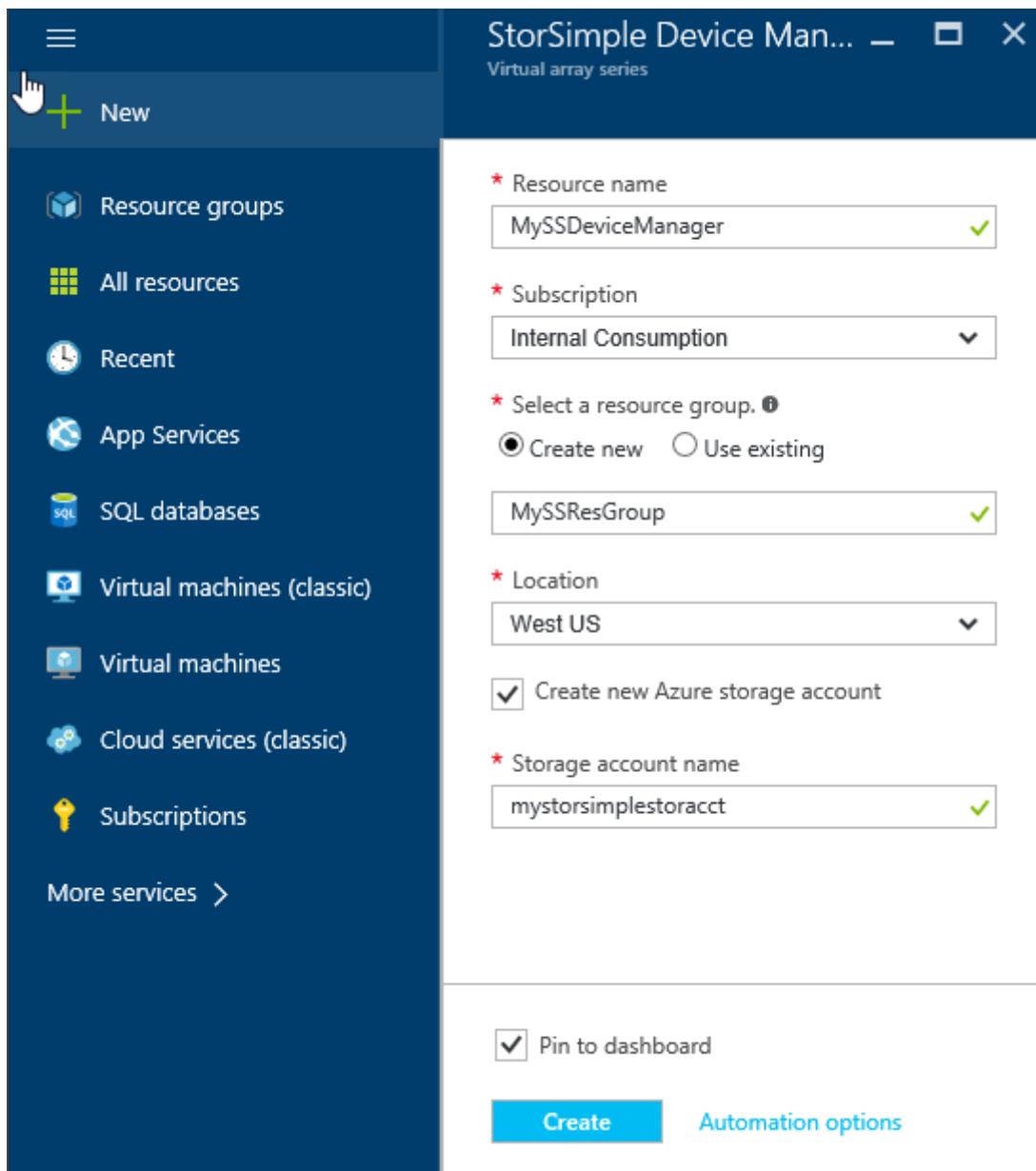
1. Sign in to the [Azure portal](#) using your Microsoft account. To deploy a device to Azure Government, sign in to the [Azure Government portal](#) instead.
2. In the Azure portal, click + **Create a resource** > **Storage** > **StorSimple Virtual Series**.



3. In the **StorSimple Device Manager** blade that opens up, do the following:

- Supply a unique **Resource name** for your service. The resource name is a friendly name that can be used to identify the service. The name can have between 2 and 50 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.
- Choose a **Subscription** from the drop-down list. The subscription is linked to your billing account. This field is not present if you have only one subscription.

- c. For **Resource group**, select an existing or create a new group. For more information, see [Azure resource groups](#).
- d. Supply a **Location** for your service. See [Azure Regions](#) for more information about which services are available in which region. In general, choose a **Location** closest to the geographical region where you want to deploy your device. You may also want to factor in the following:
 - If you have existing workloads in Azure that you also intend to deploy with your StorSimple device, we recommend that you use that datacenter.
 - Your StorSimple Device Manager and Azure storage can be in two separate locations. In such a case, you are required to create the StorSimple Device Manager and Azure storage account separately. To create an Azure storage account, navigate to Azure Storage in the Azure portal and follow the steps described in [Create a storage account](#). After you create this account, add it to the StorSimple Device Manager service by following the steps in [Configure a new storage account for the service](#).
 - If deploying the virtual device in the Government Portal, the StorSimple Device Manager service is available in US Iowa and US Virginia locations.
- e. Select **Create a new Azure storage account** to automatically create a storage account with the service. Specify a **Storage account name**. If you need your data in a different location, uncheck this box.
- f. Check **Pin to dashboard** if you want a quick link to this service on your dashboard.
- g. Click **Create** to create the StorSimple Device Manager.



You are directed to the **Service** landing page. The service creation takes a few minutes. After the service is successfully created, you will be notified appropriately and the status of the service will change to **Active**.

Important

If you did not enable the automatic creation of a storage account with your service, you will need to create at least one storage account after you have successfully created a service.

- If you did not create a storage account automatically, go to [Configure a new storage account for the service](#) for detailed instructions.
- If you enabled the automatic creation of a storage account, go to [Step 2: Get the service registration key](#).

Step 2: Get the service registration key

After the StorSimple Device Manager service is up and running, you will need to get the service registration key. This key is used to register and connect your StorSimple device with the service.

Perform the following steps in the [Azure portal](#).

To get the StorSimple service registration key

1. On the **StorSimple Device Manager** blade, click the service that you created. This opens up a new blade to the right.
2. In the blade that opens up, click **Manage > Keys**.
3. Click the copy icon to copy the service registration key and save it for later use.

Note

The service registration key is used to register all the StorSimple Device Manager devices that need to register with your StorSimple Device Manager service.

Step 3: Download the virtual array image

After you have the service registration key, you will need to download the appropriate virtual array image to provision a virtual array on your host system. The virtual array images are operating system specific and can be downloaded from the Quick Start page in the Azure portal.

Important

The software running on the StorSimple Virtual Array may only be used with the StorSimple Device Manager service.

Perform the following steps in the [Azure portal](#).

To get the virtual array image

1. Sign into the [Azure portal](#).
2. In the Azure portal, click **Browse > StorSimple Device Managers**.

3. Select an existing StorSimple Device Manager service. In the **StorSimple Device Manager** blade, click **Quick Start**.

4. Click the link corresponding to the image that you want to download from the Microsoft Download Center. The image files are approximately 4.8 GB.

- VHDX for Hyper-V on Windows Server 2012 and later
- VHD for Hyper-V on Windows Server 2008 R2 and later
- VMDK for VMWare ESXi 5.0, 5.5, 6.0 or 6.5

5. Download and unzip the file to a local drive, making a note of where the unzipped file is located.

Optional step: Configure a new storage account for the service

This step is optional and should be performed only if you did not enable the automatic creation of a storage account with your service.

If you need to create an Azure storage account in a different region, see [How to create a storage account](#) for step-by-step instructions.

Perform the following steps in the [Azure portal](#) on the StorSimple Device Manager service page to add an existing Microsoft Azure storage account.

To add a storage account credential that has the same Azure subscription as the Device Manager service

1. Navigate to your Device Manager service, select and double-click it. This opens the **Overview** blade.

2. Select **Storage account credentials** within the **Configuration** section.

3. Click **Add**.

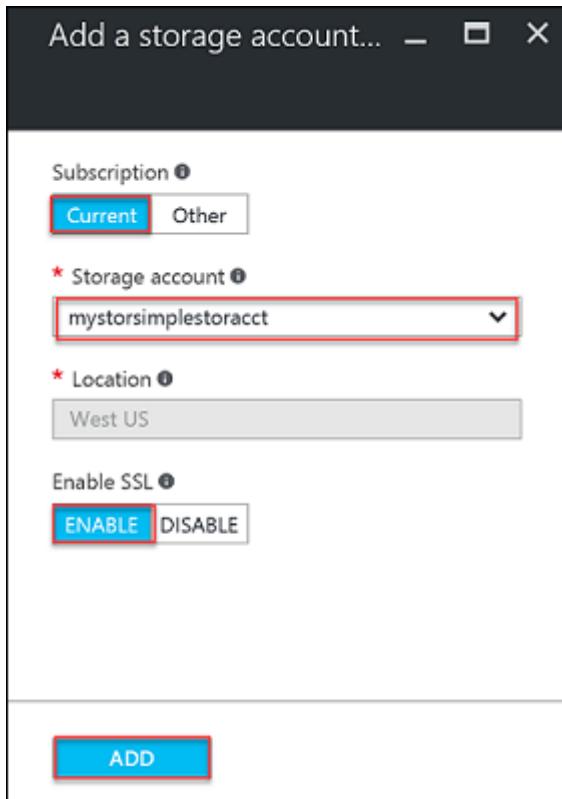
4. In the **Add a storage account** blade, do the following:

a. For **Subscription**, select **Current**.

b. Provide the name of your Azure storage account.

c. Select **Enable** to create a secure channel for network communication between your StorSimple device and the cloud. Select **Disable** only if you are operating within a private cloud.

d. Click **Add**. You are notified after the storage account is successfully created.



Next step

The next step is to provision a virtual machine for your StorSimple Virtual Array. Depending on your host operating system, see the detailed instructions in:

- [Provision a StorSimple Virtual Array in Hyper-V](#)
- [Provision a StorSimple Virtual Array in VMware](#)

Deploy the StorSimple Device Manager service for StorSimple Virtual Array

Article • 08/19/2022 • 6 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple devices. After you create the service, you can use it to manage the devices from the Microsoft Azure portal running in a browser. This allows you to monitor all the devices that are connected to the StorSimple Device Manager service from a single, central location, thereby minimizing administrative burden.

The common tasks related to a StorSimple Device Manager service are:

- Create a service
- Delete a service
- Get the service registration key
- Regenerate the service registration key

This tutorial describes how to perform each of the preceding tasks. The information contained in this article is applicable only to StorSimple Virtual Arrays. For more information on StorSimple 8000 series, go to [deploy a StorSimple Manager service](#).

Create a service

To create a service, you need to have:

- A subscription with an Enterprise Agreement
- An active Microsoft Azure storage account
- The billing information that is used for access management

You can also choose to generate a storage account when you create the service.

A single service can manage multiple devices. However, a device cannot span multiple services. A large enterprise can have multiple service instances to work with different subscriptions, organizations, or even deployment locations.

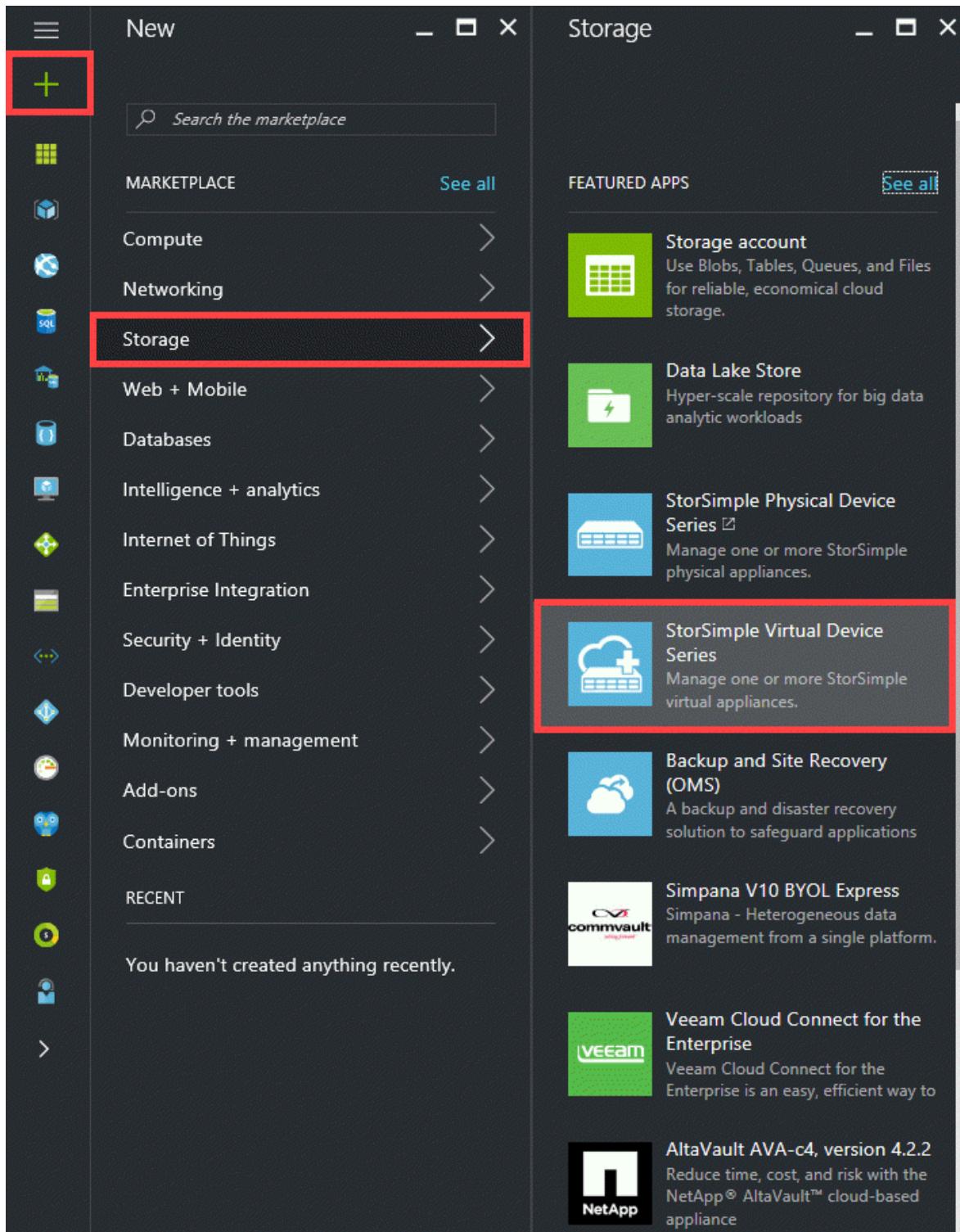
 **Note**

You need separate instances of StorSimple Device Manager service to manage StorSimple 8000 series devices and StorSimple Virtual Arrays.

Perform the following steps to create a service.

To create a new service

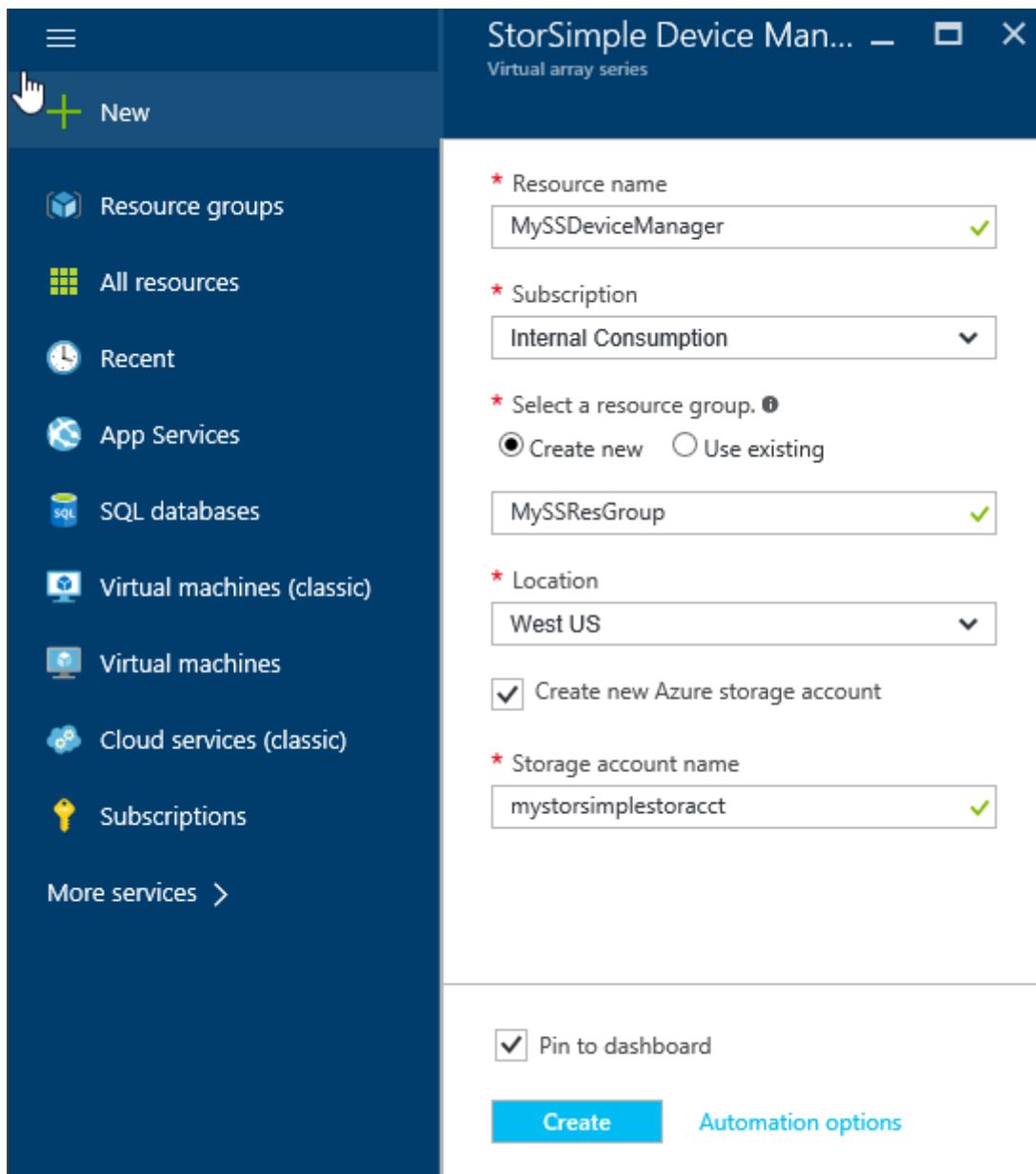
1. Sign in to the [Azure portal](#) using your Microsoft account. To deploy a device to Azure Government, sign in to the [Azure Government portal](#) instead.
2. In the Azure portal, click + **Create a resource** > **Storage** > **StorSimple Virtual Series**.



3. In the **StorSimple Device Manager** blade that opens up, do the following:

- Supply a unique **Resource name** for your service. The resource name is a friendly name that can be used to identify the service. The name can have between 2 and 50 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.
- Choose a **Subscription** from the drop-down list. The subscription is linked to your billing account. This field is not present if you have only one subscription.

- c. For **Resource group**, select an existing or create a new group. For more information, see [Azure resource groups](#).
- d. Supply a **Location** for your service. See [Azure Regions](#) for more information about which services are available in which region. In general, choose a **Location** closest to the geographical region where you want to deploy your device. You may also want to factor in the following:
 - If you have existing workloads in Azure that you also intend to deploy with your StorSimple device, we recommend that you use that datacenter.
 - Your StorSimple Device Manager and Azure storage can be in two separate locations. In such a case, you are required to create the StorSimple Device Manager and Azure storage account separately. To create an Azure storage account, navigate to Azure Storage in the Azure portal and follow the steps described in [Create a storage account](#). After you create this account, add it to the StorSimple Device Manager service by following the steps in [Configure a new storage account for the service](#).
 - If deploying the virtual device in the Government Portal, the StorSimple Device Manager service is available in US Iowa and US Virginia locations.
- e. Select **Create a new Azure storage account** to automatically create a storage account with the service. Specify a **Storage account name**. If you need your data in a different location, uncheck this box.
- f. Check **Pin to dashboard** if you want a quick link to this service on your dashboard.
- g. Click **Create** to create the StorSimple Device Manager.



You are directed to the **Service** landing page. The service creation takes a few minutes. After the service is successfully created, you will be notified appropriately and the status of the service will change to **Active**.

Delete a service

Before you delete a service, make sure that no connected devices are using it. If the service is in use, deactivate the connected devices. The deactivate operation will sever the connection between the device and the service, but preserve the device data in the cloud.

ⓘ Important

After a service is deleted, the operation cannot be reversed. Any device that was using the service will need to be factory reset before it can be used with another

service. In this scenario, the local data on the device, as well as the configuration, will be lost.

Perform the following steps to delete a service.

To delete a service

1. Go to **All resources**. Search for your StorSimple Device Manager service. Select the service that you wish to delete.

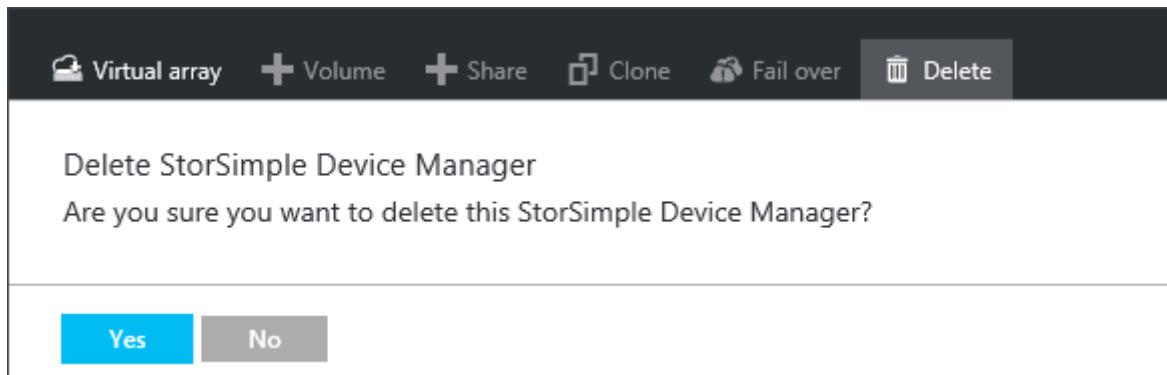
NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
MySS0715AK	StorSimple Manager...	AKSS	West US	Microsoft Azure Enterprise
MySS0810	StorSimple Manager...	MySSRG	West US	Microsoft Azure Enterprise
MySS714	StorSimple Manager...	AKSS	Southeast Asia	Microsoft Azure Enterprise
MySSAK0719	StorSimple Manager...	MySSAK	West US	Microsoft Azure Enterprise

2. Go to your service dashboard to ensure there are no devices connected to the service. If there are no devices registered with this service, you will also see a banner message to the effect. Click **Delete**.

The dashboard shows the following details:

- Essentials**: Resource group MySSRG, Location West US, Subscription name Microsoft Azure Enterprise, Subscription ID 0154f7fe-df09-4981-bf82-7ad5c1f596eb.
- Monitoring**: Alerts - Past 7 days: There are no registered devices to show alerts.
- Capacity**: PROVISIONED 0 Bytes, REMAINING 0 Bytes - Tiered. There are no registered devices to show capacity utilization.

3. When prompted for confirmation, click **Yes** in the confirmation notification.



4. It may take a few minutes for the service to be deleted. After the service is successfully deleted, you will be notified.



The list of services will be refreshed.

A screenshot of the Microsoft Azure portal. The left sidebar shows navigation options: 'New', 'Azure Portal SDK', 'Portal SDK documentation...', 'Resource groups', 'All resources', and 'SQL databases'. The main area is titled 'All resources' and shows the following details:
Subscriptions: Microsoft Azure Enterprise
MySS
NAME
MySS0715AK
MySS714
MySSAK0719

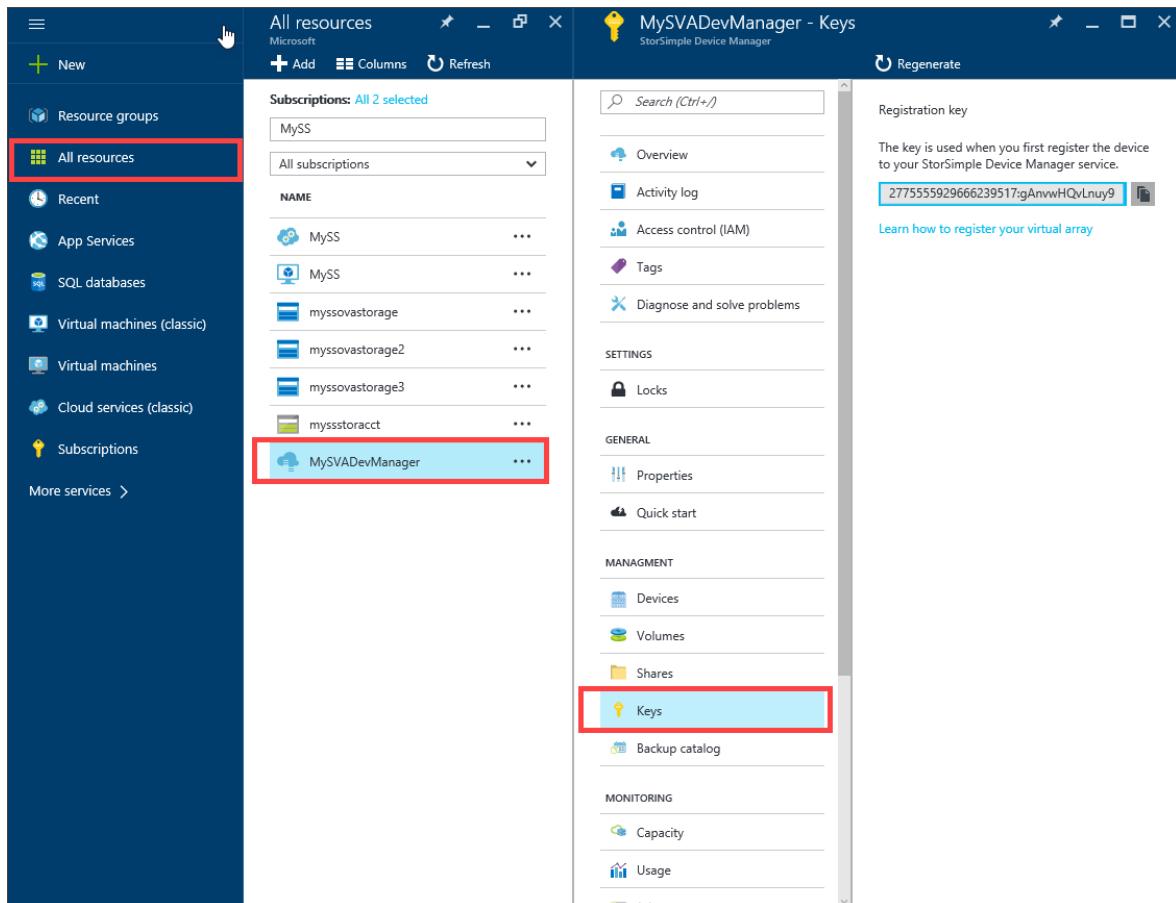
Get the service registration key

After you have successfully created a service, you will need to register your StorSimple device with the service. To register your first StorSimple device, you will need the service registration key. To register additional devices with an existing StorSimple service, you will need both the registration key and the service data encryption key (which is generated on the first device during registration). For more information about the service data encryption key, see [StorSimple security](#). You can get the registration key by accessing the **Keys** blade for your service.

Perform the following steps to get the service registration key.

To get the service registration key

1. In the StorSimple Device Manager blade, go to **Management > Keys**.



2. In the **Keys** blade, a service registration key appears. Copy the registration key using the copy icon.

Keep the service registration key in a safe location. You will need this key, as well as the service data encryption key, to register additional devices with this service. After obtaining the service registration key, you will need to configure your device through the Windows PowerShell for StorSimple interface.

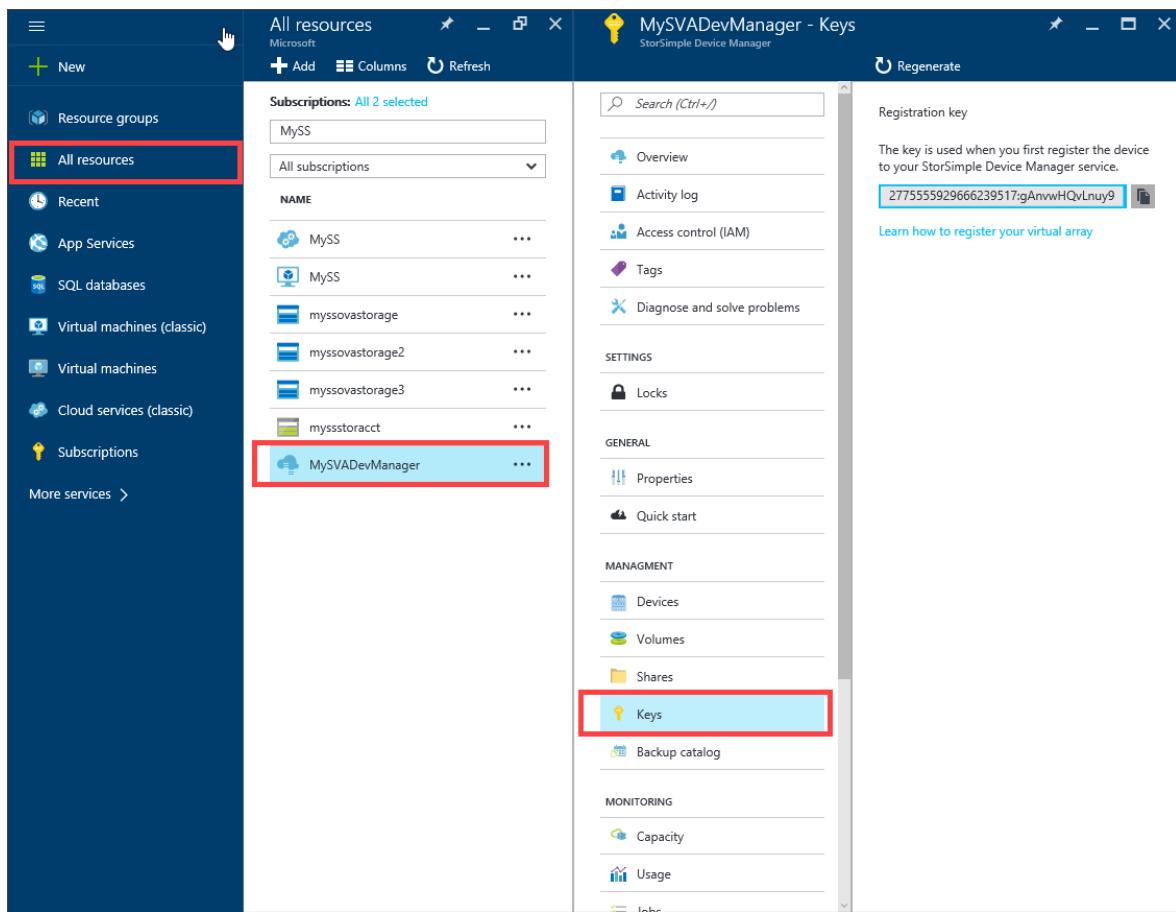
Regenerate the service registration key

You will need to regenerate a service registration key if you are required to perform key rotation or if the list of service administrators has changed. When you regenerate the key, the new key is used only for registering subsequent devices. The devices that were already registered are unaffected by this process.

Perform the following steps to regenerate a service registration key.

To regenerate the service registration key

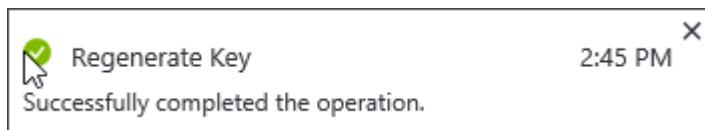
1. In the StorSimple Device Manager blade, go to Management > Keys.



2. In the Keys blade, click Regenerate.

The screenshot shows the 'MySVADevManager - Keys' blade in the StorSimple Device Manager. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick start), Management (Devices, Volumes, Shares, Keys, Backup catalog), and Monitoring (Capacity, Usage). The 'Keys' item under Management is currently selected and highlighted with a blue background. At the top right, there's a red box highlighting the 'Regenerate' button. The main content area is titled 'Registration key' and contains the text: 'The key is used when you first register the device to your StorSimple Device Manager service.' Below this is a text field containing the key value '277555929666239517:gAnvwHQvLnuy9' with a copy icon to its right. A link 'Learn how to register your virtual array' is also present. To the right of the main content, a separate window titled 'Regenerate service regi...' is shown, which contains information about regenerating the key and a 'Regenerate' button at the bottom.

3. In the **Regenerate service registration key** blade, review the action required when the keys are regenerated. All the subsequent devices that are registered with this service will use the new registration key. Click **Regenerate** to confirm. You will be notified after the registration is complete.



4. A new service registration key will appear.



Regenerate

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Locks

GENERAL

Properties

Quick start

MANAGEMENT

Devices

Volumes

Shares

Keys

Backup catalog

MONITORING

Capacity

Usage

Registration key

The key is used when you first register the device to your StorSimple Device Manager service.

2775555929666239517:9VMmEu0mt6lkH



[Learn how to register your virtual array](#)

Copy this key and save it for registering any new devices with this service.

Next steps

- Learn how to [get started](#) with a StorSimple Virtual Array.

- Learn how to [administer your StorSimple device](#).

Use the new authentication for your StorSimple

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple Virtual Arrays. To date, StorSimple Device Manager service has used an Access Control service (ACS) to authenticate the service to your StorSimple device. The ACS mechanism will be deprecated soon and replaced by an Azure Active Directory (AAD) authentication.

The information contained in this article is applicable to both StorSimple 1200 Series Virtual Arrays only. This article describes the details of the AAD authentication and the associated new service registration key and modifications to the firewall rules as applicable to the StorSimple devices.

The AAD authentication occurs in StorSimple Virtual Arrays (model 1200) running Update 1 or later.

Due to the introduction of the AAD authentication, changes occur in:

- URL patterns for firewall rules.
- Service registration key.

These changes are discussed in detail in the following sections.

URL changes for AAD authentication

To ensure that the service uses AAD-based authentication, all the users must include the new authentication URLs in their firewall rules.

If using StorSimple Virtual Array, ensure that the following URL is included in the firewall rules:

URL pattern	Cloud	Component/Functionality
<code>https://login.windows.net</code>	Azure Public	AAD authentication service
<code>https://login.microsoftonline.us</code>	US Government	AAD authentication service

For a complete list of URL patterns for StorSimple Virtual Arrays, go to [URL patterns for firewall rules](#).

If the authentication URL is not included in the firewall rules beyond the deprecation date, the users see a critical alert that their StorSimple device could not authenticate with the service. The service will not be able to communicate with the device. If the users see this alert, they need to include the new authentication URL. For more information on the alert, go to [Use alerts to monitor your StorSimple device](#).

Device version and authentication changes

If using a StorSimple Virtual Array, use the following table to determine what action you need to take based on the device software version you are running.

If your device is running	Take the following action
Update 1.0 or later and is offline. You see an alert that the URL is not allowlisted.	1. Modify the firewall rules to include the authentication URL. See authentication URLs . 2. Get the AAD registration key from the service . 3. Perform steps 1-5 to Connect to the Windows PowerShell interface of the virtual array . 4. Use <code>Invoke-HcsReRegister</code> cmdlet to register the device through the Windows PowerShell. Supply the key you got in the previous step.
Update 1.0 or later and the device is online.	No action is required.

If your device is running	Take the following action
Update 0.6 or earlier and the device is offline.	<ol style="list-style-type: none"> 1. Download Update 1.0 through catalog server. 2. Apply Update 1.0 through the local web UI. 3. Get the AAD registration key from the service. 4. Perform steps 1-5 to Connect to the Windows PowerShell interface of the virtual array. 5. Use <code>Invoke-HcsReRegister</code> cmdlet to register the device through the Windows PowerShell. Supply the key you got in the previous step.
Update 0.6 or earlier and the device is online	<p>Modify the firewall rules to include the authentication URL. Install Update 1.0 through the Azure portal.</p>

AAD-based registration keys

Beginning Update 1.0 for StorSimple Virtual Arrays, new AAD-based registration keys are used. You use the registration keys to register your StorSimple Device Manager service with the device.

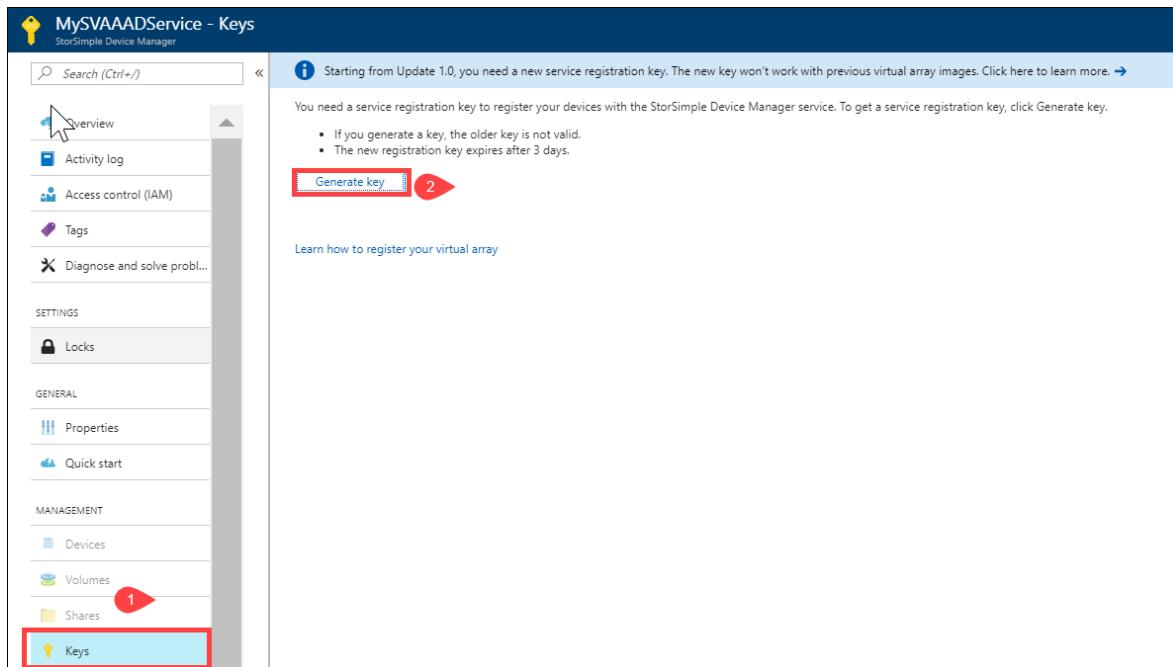
You cannot use the new AAD service registration keys if you are using a StorSimple Virtual Arrays running Update 0.6 or earlier. You need to regenerate the service registration key. Once you regenerate the key, the new key is used for registering all the subsequent devices. The old key is no longer valid.

- The new AAD registration key expires after 3 days.
- The AAD registration keys work only with StorSimple 1200 series virtual arrays running Update 1 or later. The AAD registration key from a StorSimple 8000 series device will not work.
- The AAD registration keys are longer than the corresponding ACS registration keys.

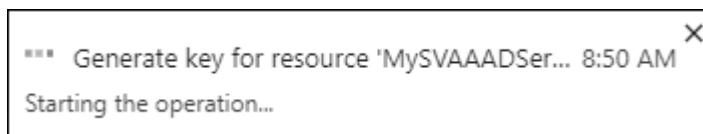
Perform the following steps to generate an AAD service registration key.

To generate the AAD service registration key

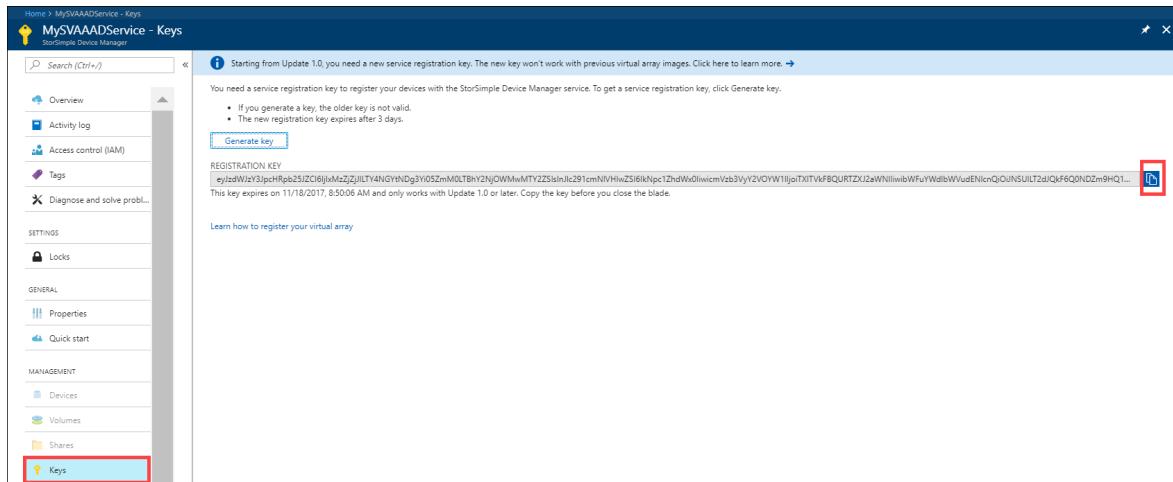
1. In **StorSimple Device Manager**, go to **Management > Keys**.



2. Click Generate key.



3. Copy the new key. The older key no longer works.



Next steps

- Learn more about how to deploy [StorSimple Virtual Array](#)

Deploy StorSimple Virtual Array - Provision in Hyper-V

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Overview

This tutorial describes how to provision a StorSimple Virtual Array on a host system running Hyper-V on Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2. This article applies to the deployment of StorSimple Virtual Arrays in Azure portal and Microsoft Azure Government Cloud.

You need administrator privileges to provision and configure a virtual array. The provisioning and initial setup can take around 10 minutes to complete.

Provisioning prerequisites

Here you will find the prerequisites to provision a virtual array on a host system running Hyper-V on Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

For the StorSimple Device Manager service

Before you begin, make sure that:

- You have completed all the steps in [Prepare the portal for StorSimple Virtual Array](#).

- You have downloaded the virtual array image for Hyper-V from the Azure portal. For more information, see [Step 3: Download the virtual array image of Prepare the portal for StorSimple Virtual Array guide](#).

 **Important**

The software running on the StorSimple Virtual Array may only be used with the StorSimple Device Manager service.

For the StorSimple Virtual Array

Before you deploy a virtual array, make sure that:

- You have access to a host system running Hyper-V on Windows Server 2008 R2 or later that can be used to provision a device.
- The host system is able to dedicate the following resources to provision your virtual array:
 - A minimum of 4 cores.
 - At least 8 GB of RAM. If you plan to configure the virtual array as file server, 8 GB supports less than 2 million files. You need 16 GB RAM to support 2 - 4 million files.
 - One network interface.
 - A 500 GB virtual disk for data.

For the network in the datacenter

Before you begin, review the networking requirements to deploy a StorSimple Virtual Array and configure the datacenter network appropriately. For more information, see [StorSimple Virtual Array networking requirements](#).

Step-by-step provisioning

To provision and connect to a virtual array, you need to perform the following steps:

1. Ensure that the host system has sufficient resources to meet the minimum virtual array requirements.
2. Provision a virtual array in your hypervisor.
3. Start the virtual array and get the IP address.

Each of these steps is explained in the following sections.

Step 1: Ensure that the host system meets minimum virtual array requirements

To create a virtual array, you need:

- The Hyper-V role installed on Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 SP1.
- Microsoft Hyper-V Manager on a Microsoft Windows client connected to the host.

Make sure that the underlying hardware (host system) on which you are creating the virtual array is able to dedicate the following resources to your virtual array:

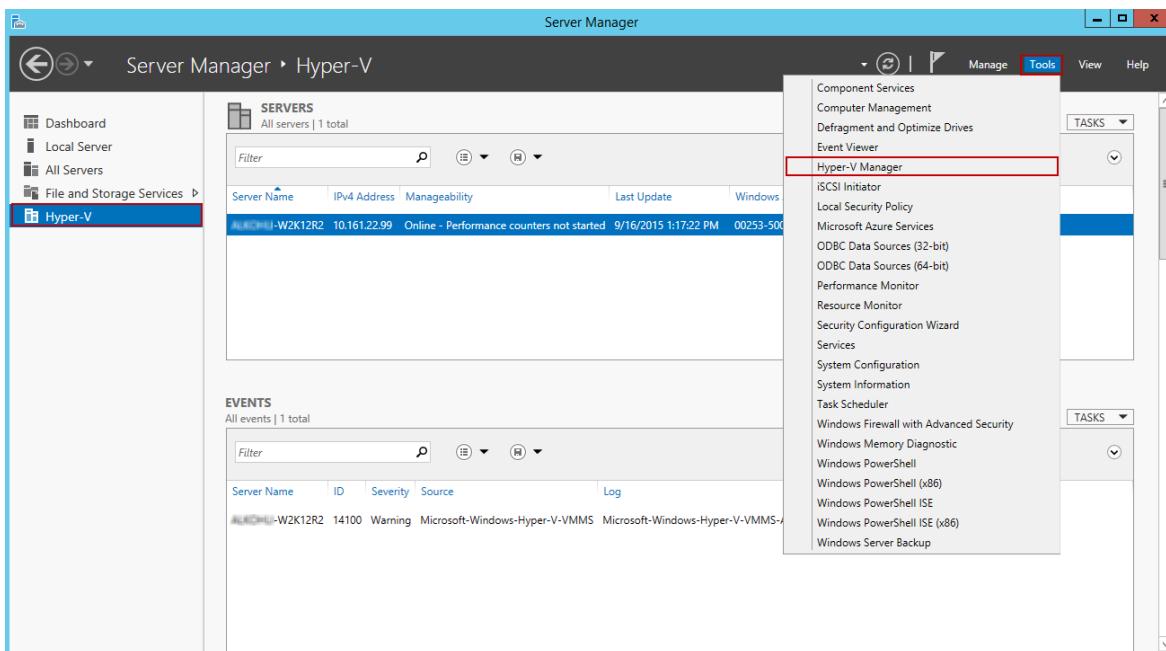
- A minimum of 4 cores.
- At least 8 GB of RAM. If you plan to configure the virtual array as file server, 8 GB supports less than 2 million files. You need 16 GB RAM to support 2 - 4 million files.
- One network interface.
- A 500 GB virtual disk for system data.

Step 2: Provision a virtual array in hypervisor

Perform the following steps to provision a device in your hypervisor.

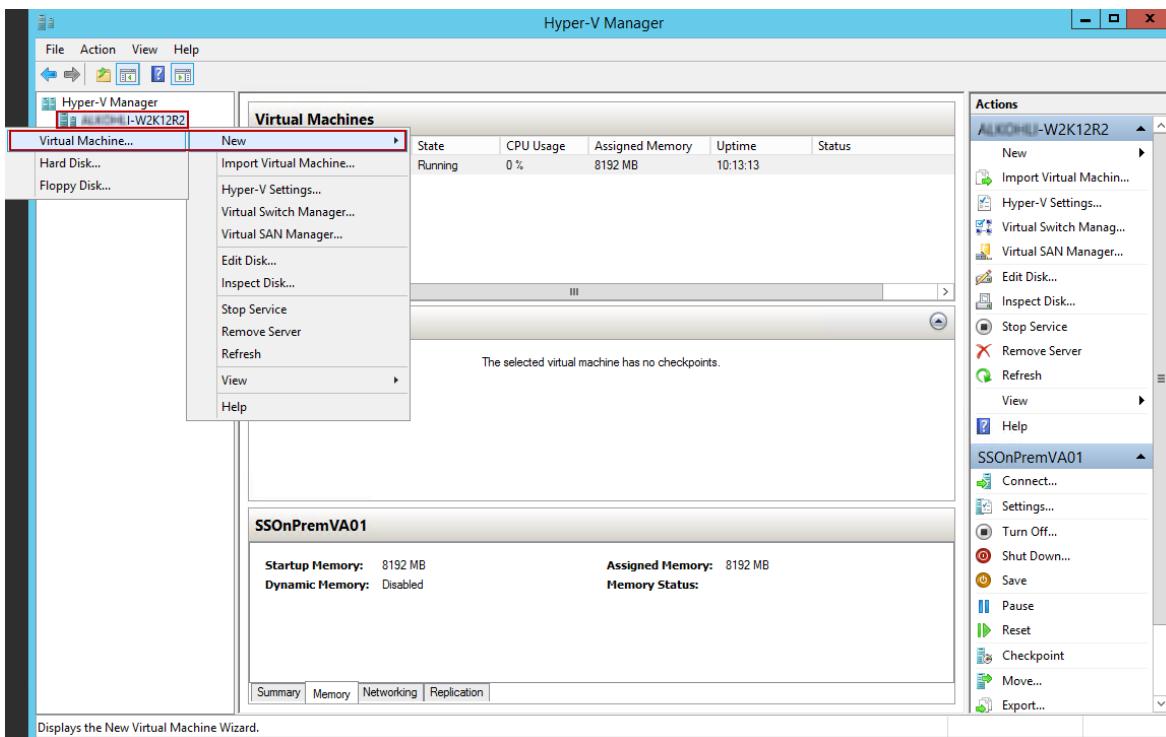
To provision a virtual array

1. On your Windows Server host, copy the virtual array image to a local drive. You downloaded this image (VHD or VHDX) through the Azure portal. Make a note of the location where you copied the image as you are using this image later in the procedure.
2. Open Server Manager. In the top right corner, click **Tools** and select **Hyper-V Manager**.

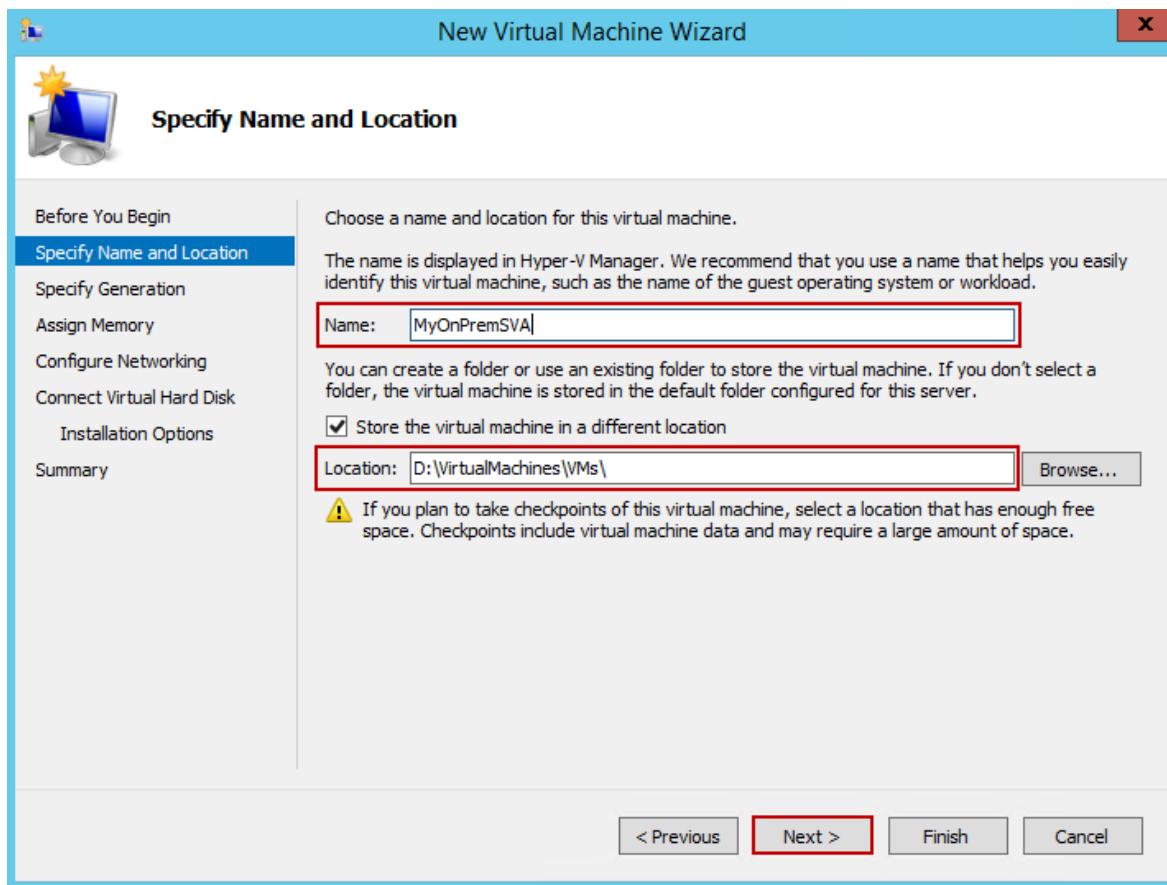


If you are running Windows Server 2008 R2, open the Hyper-V Manager. In Server Manager, click Roles > Hyper-V > Hyper-V Manager.

3. In **Hyper-V Manager**, in the scope pane, right-click your system node to open the context menu, and then click **New > Virtual Machine**.

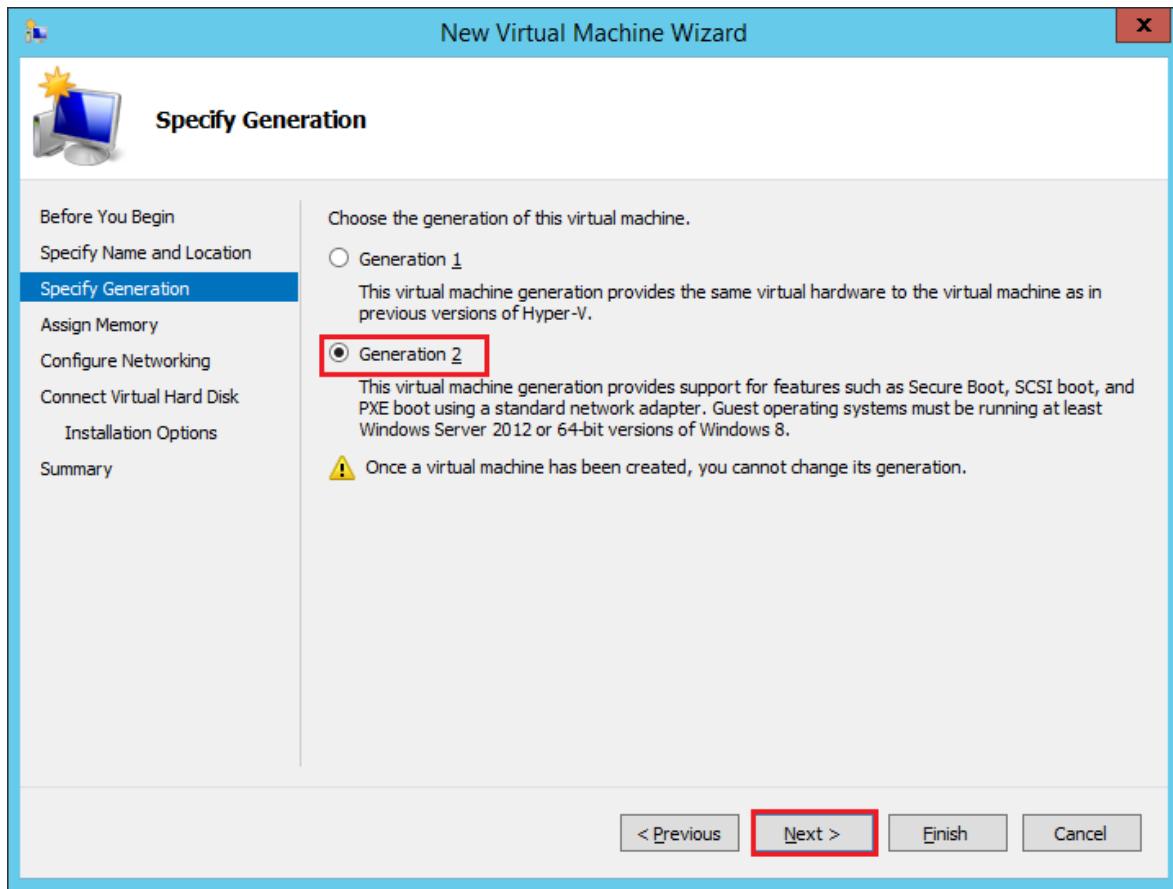


4. On the **Before you begin** page of the New Virtual Machine Wizard, click **Next**.
5. On the **Specify name and location** page, provide a **Name** for your virtual array. Click **Next**.

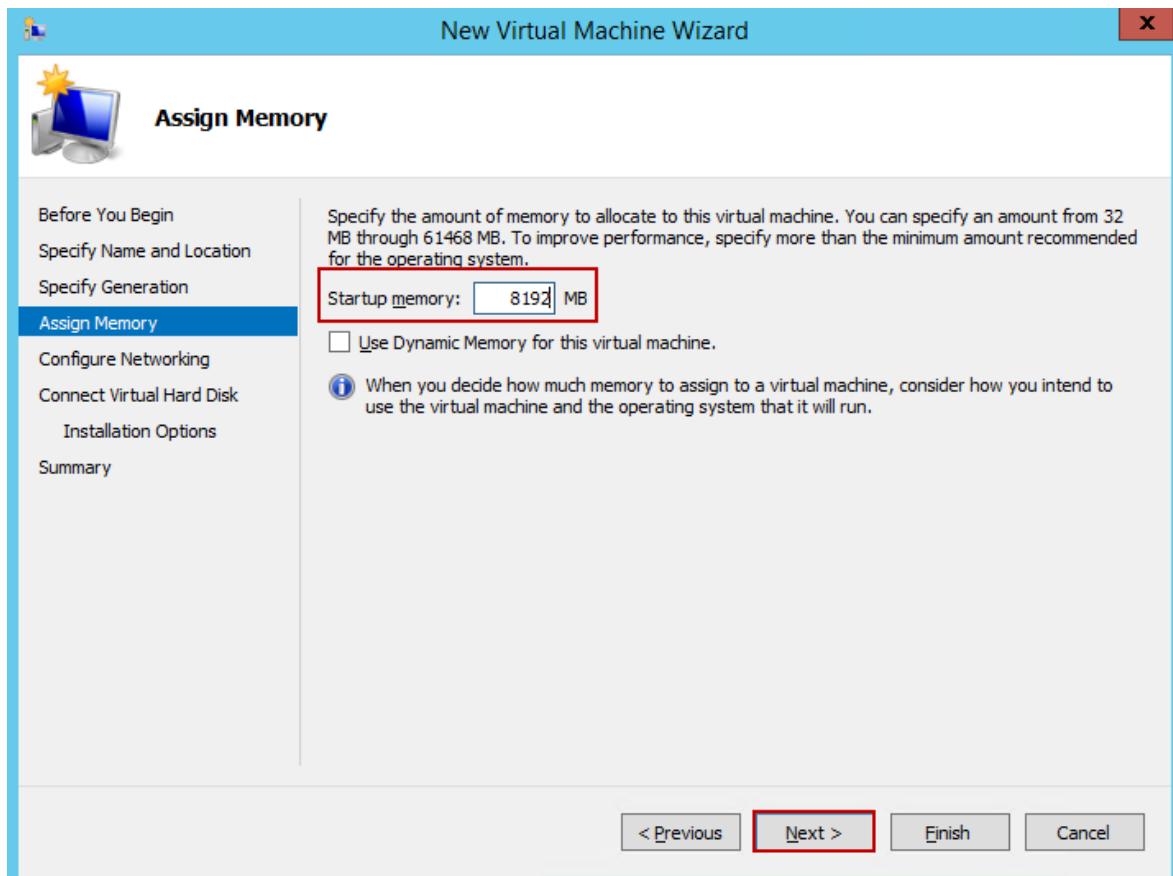


6. On the **Specify generation** page, choose the device image type, and then click **Next**. This page doesn't appear if you're using Windows Server 2008 R2.

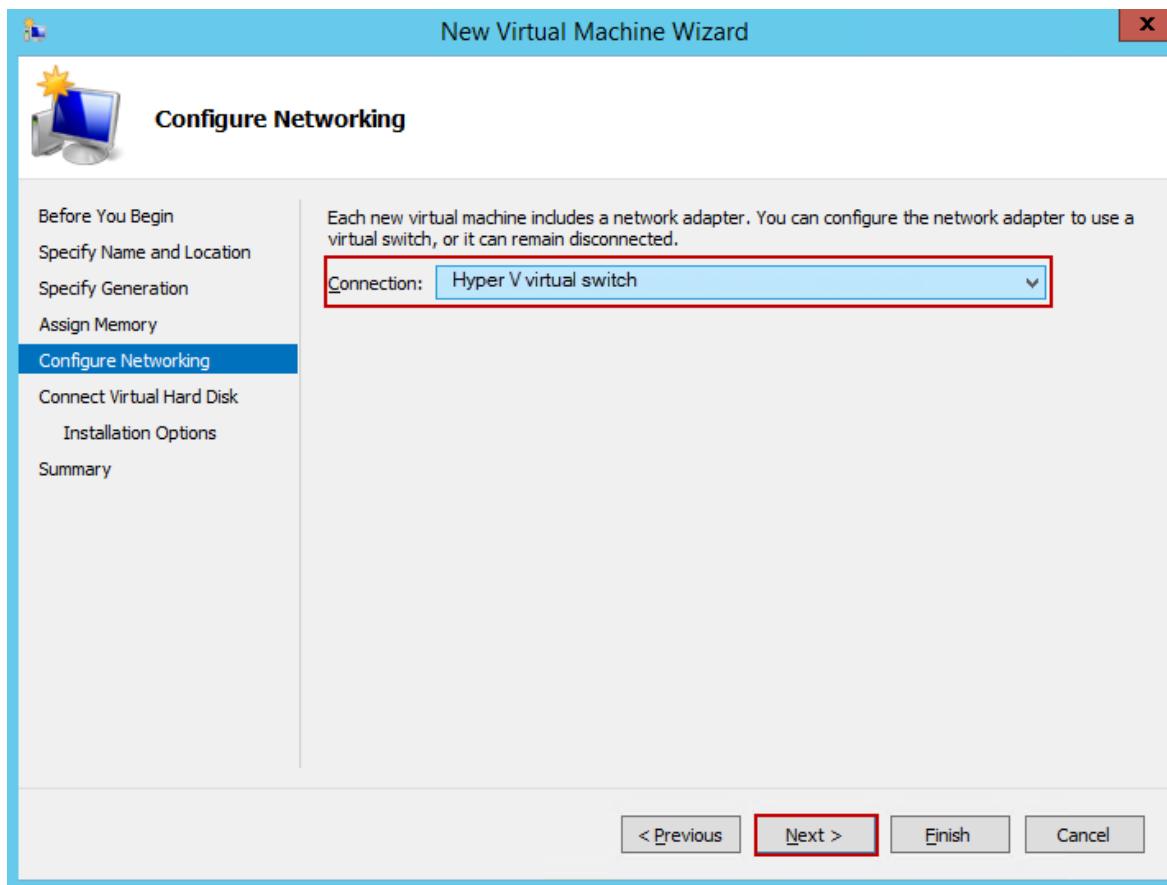
- Choose **Generation 2** if you downloaded a .vhdx image for Windows Server 2012 or later.
- Choose **Generation 1** if you downloaded a .vhd image for Windows Server 2008 R2 or later.



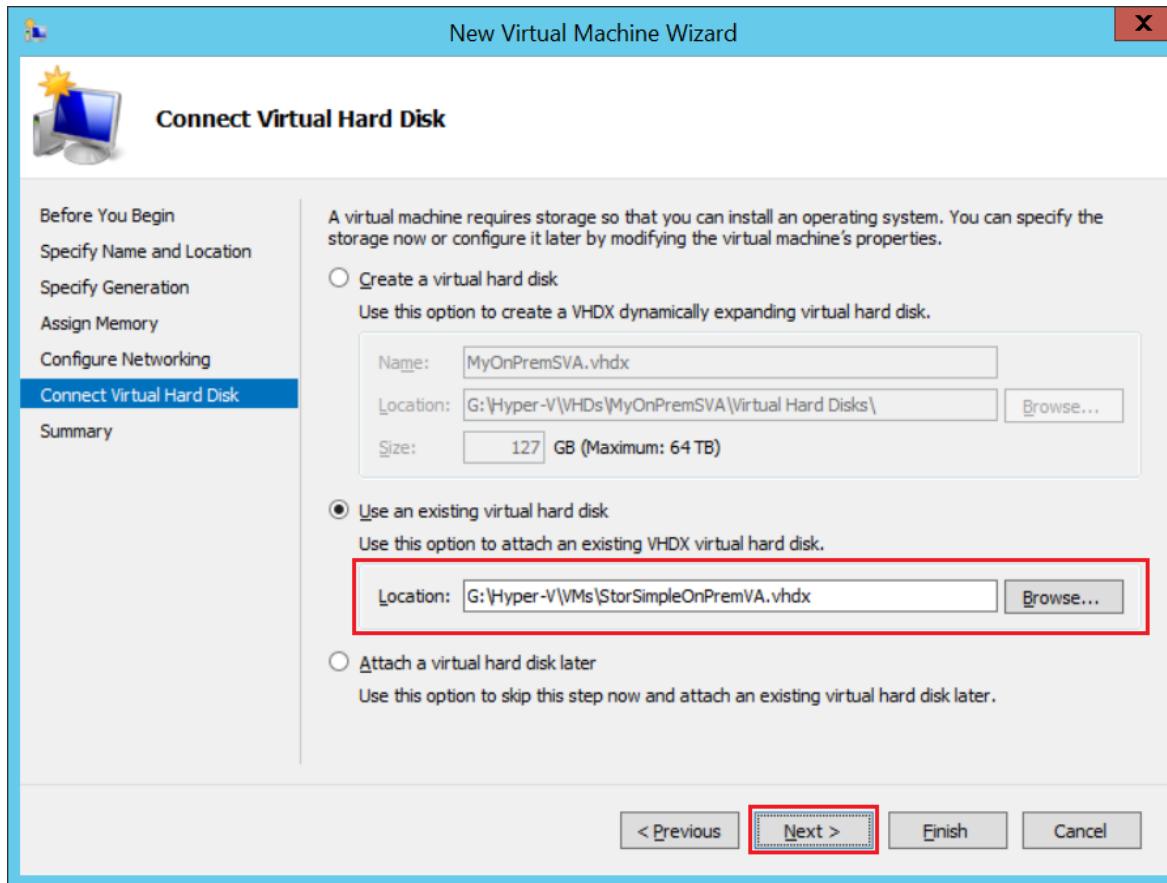
7. On the **Assign memory** page, specify a **Startup memory** of at least 8192 MB, don't enable dynamic memory, and then click **Next**.



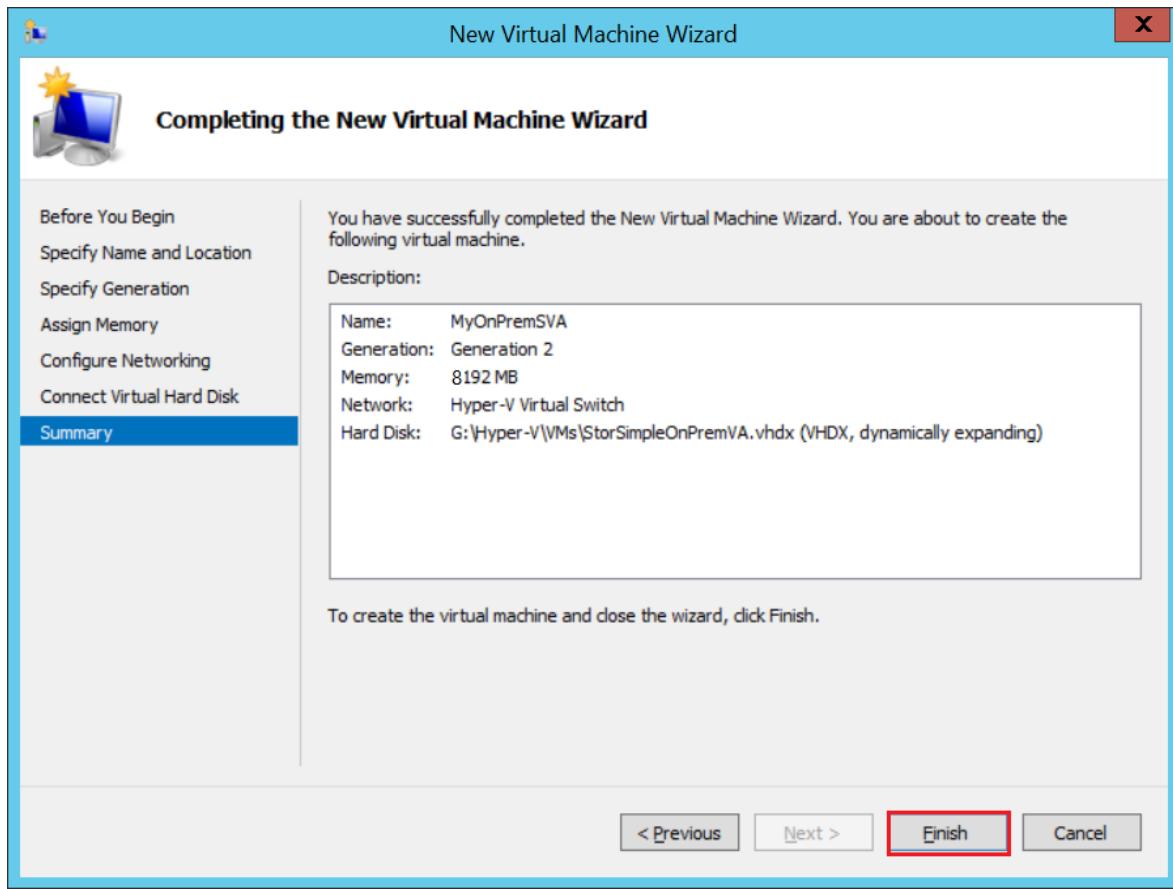
8. On the **Configure networking** page, specify the virtual switch that is connected to the Internet and then click **Next**.



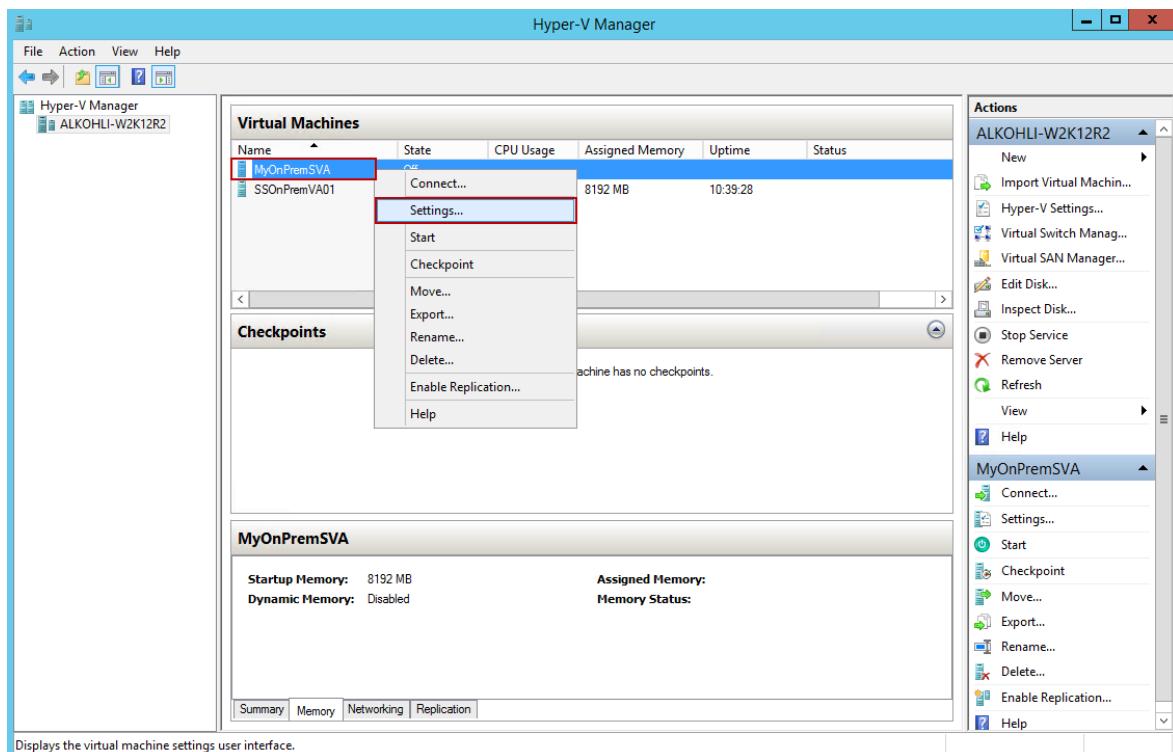
9. On the **Connect virtual hard disk** page, choose **Use an existing virtual hard disk**, specify the location of the virtual array image (.vhdx or .vhd), and then click **Next**.



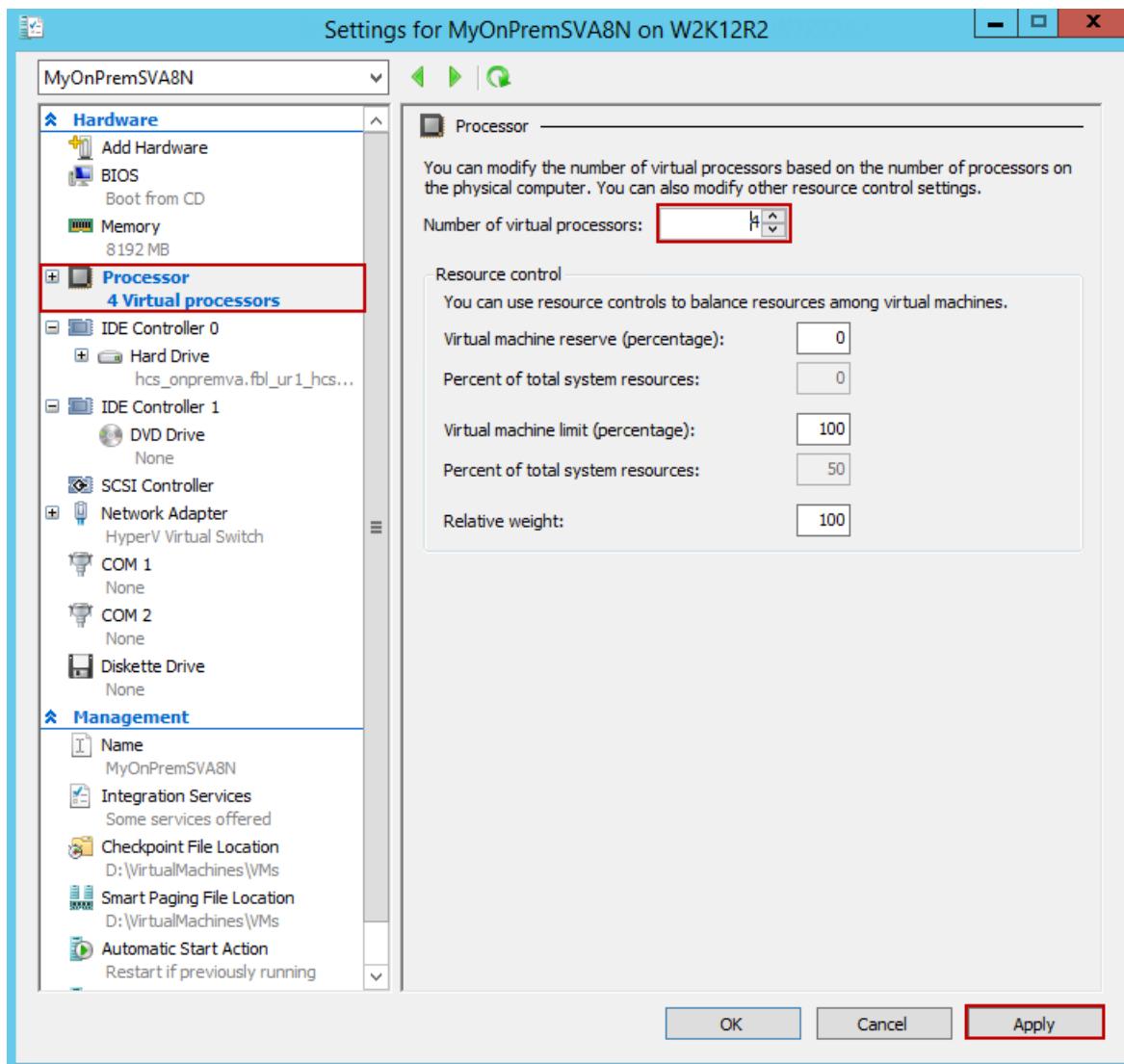
10. Review the **Summary** and then click **Finish** to create the virtual machine.



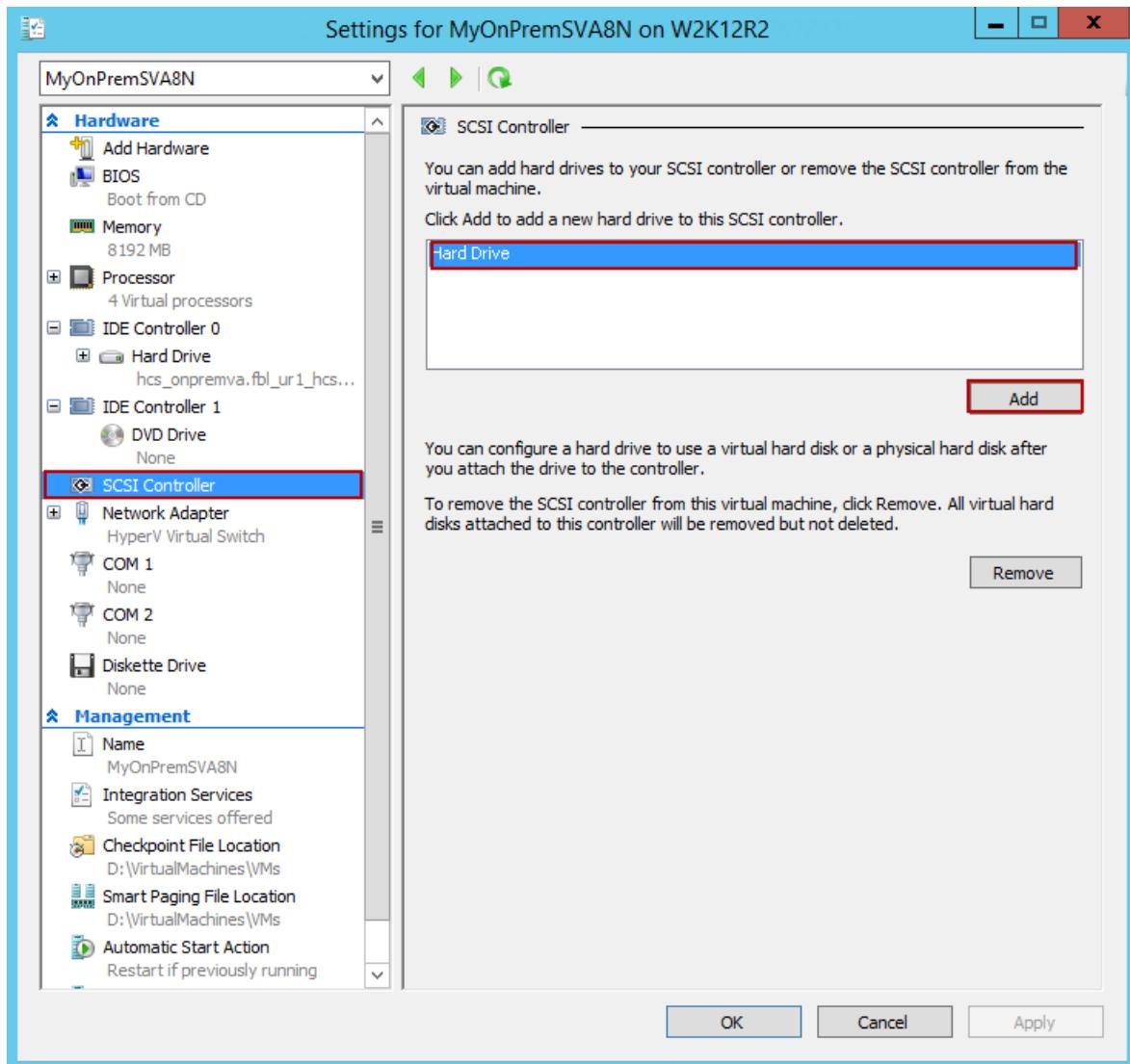
- To meet the minimum requirements, you need 4 cores. To add 4 virtual processors, select your host system in the **Hyper-V Manager** window. In the right-pane under the list of **Virtual Machines**, locate the virtual machine you just created. Select and right-click the machine name and select **Settings**.



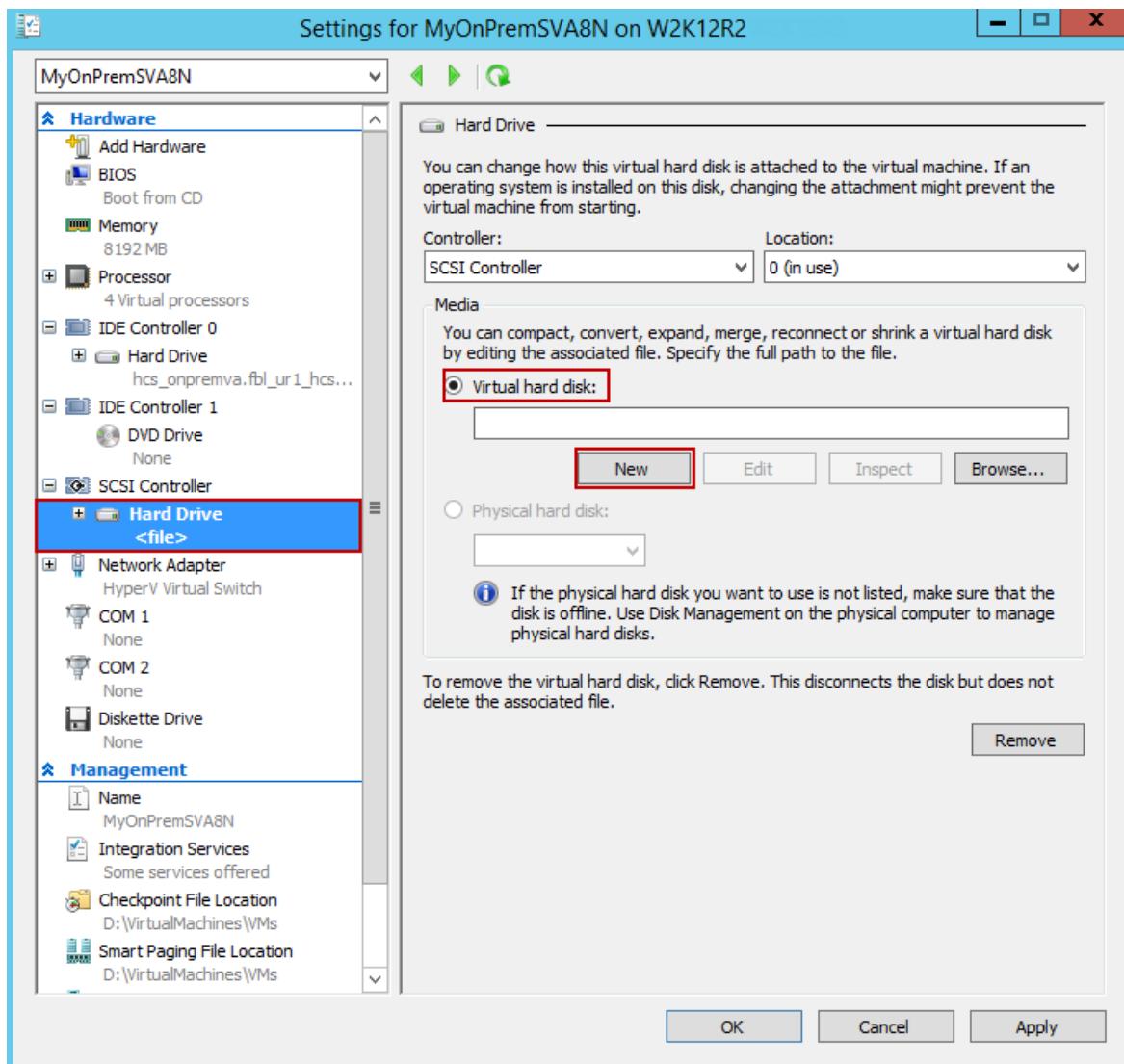
- On the **Settings** page, in the left-pane, click **Processor**. In the right-pane, set **number of virtual processors** to 4 (or more). Click **Apply**.



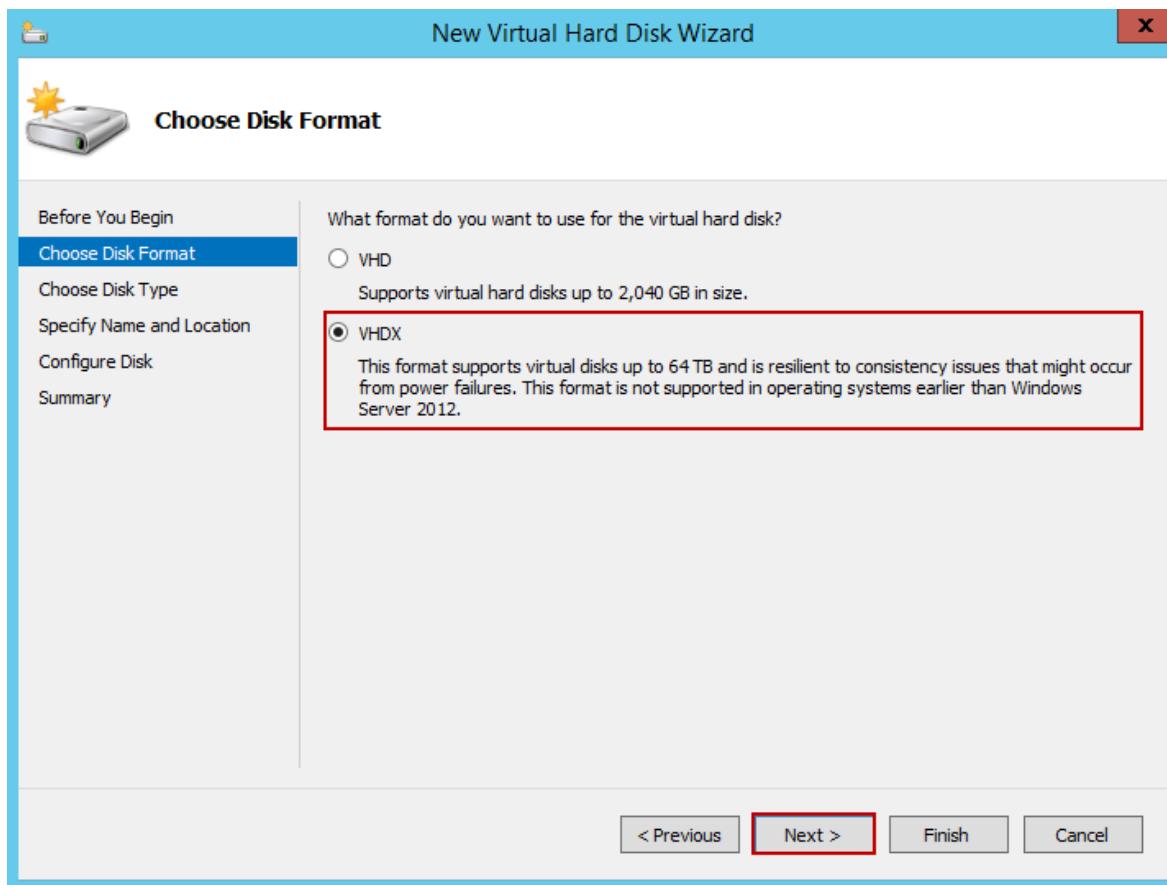
13. To meet the minimum requirements, you also need to add a 500 GB virtual data disk. In the **Settings** page:
 - a. In the left pane, select **SCSI Controller**.
 - b. In the right pane, select **Hard Drive**, and click **Add**.



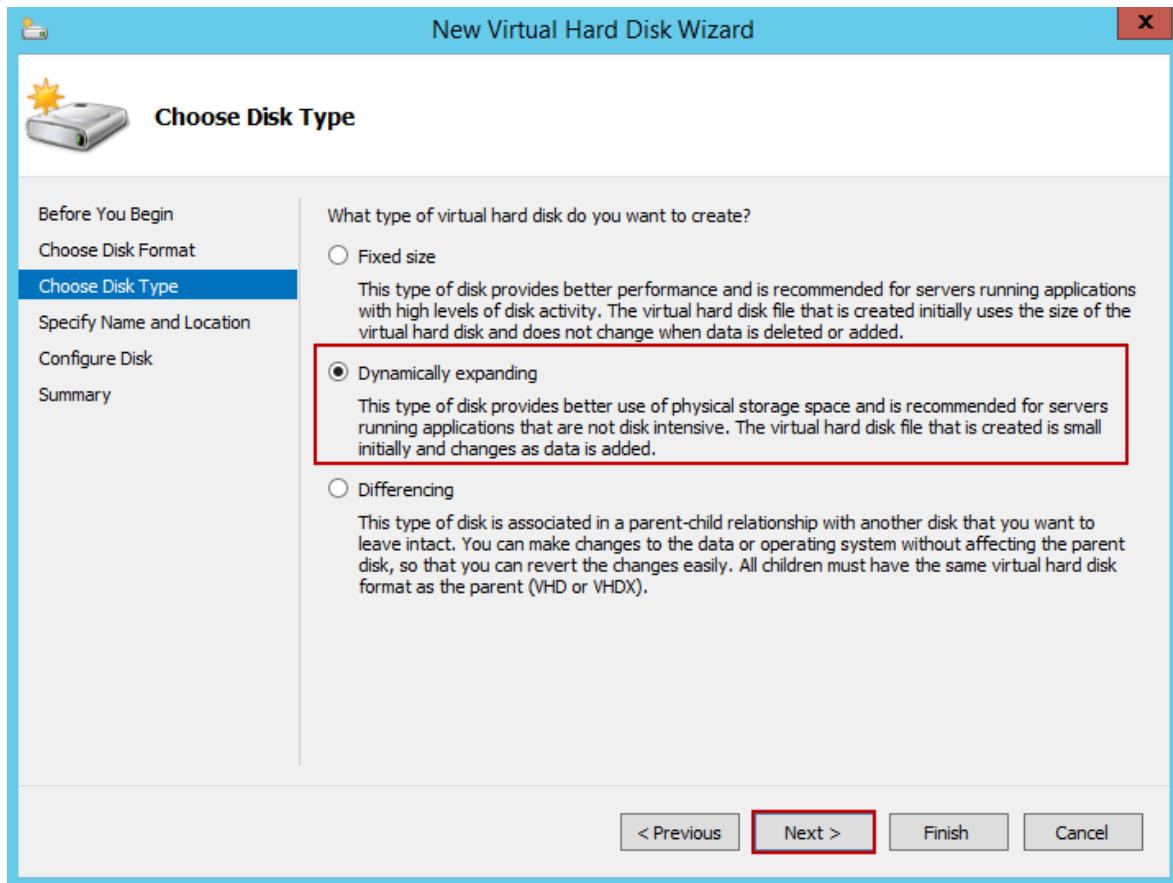
14. On the Hard drive page, select the Virtual hard disk option and click New. The New Virtual Hard Disk Wizard starts.



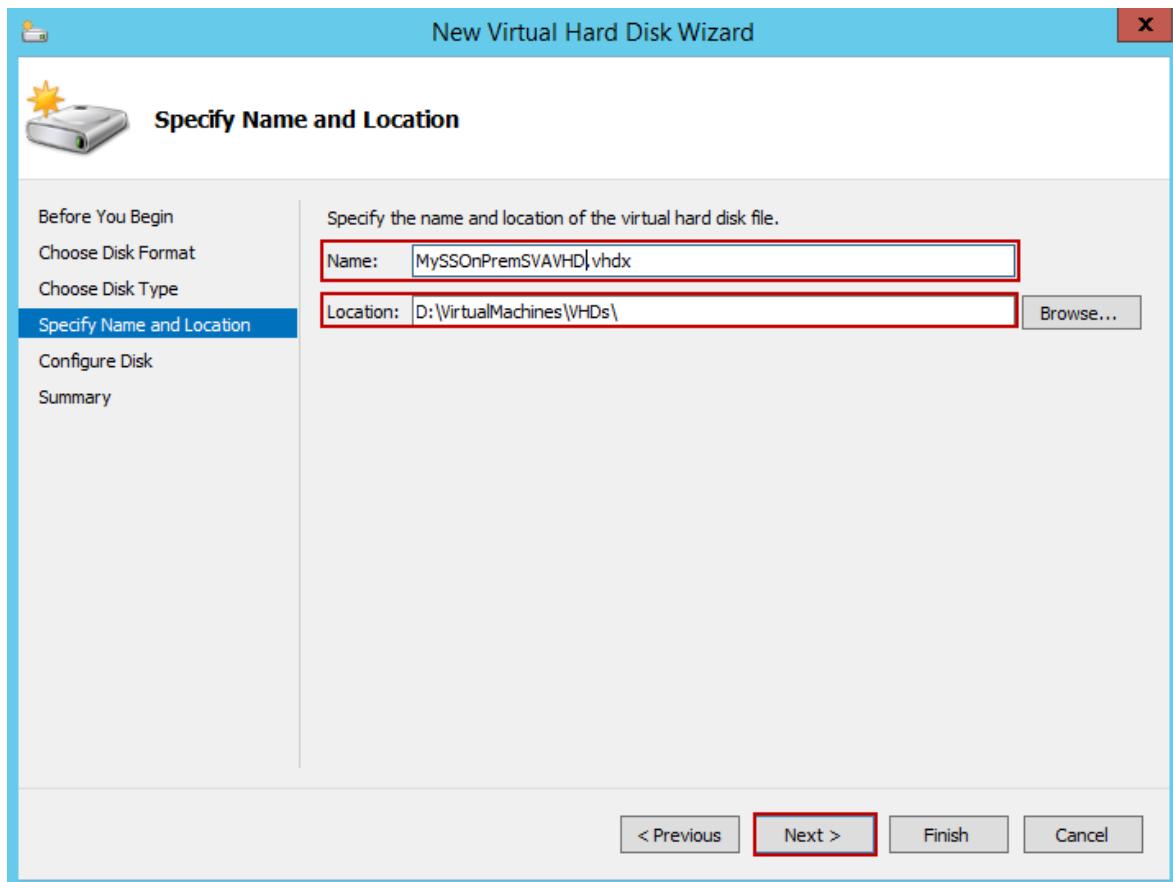
15. On the **Before you begin** page of the New Virtual Hard Disk Wizard, click **Next**.
16. On the **Choose Disk Format** page, accept the default option of **VHDX** format. Click **Next**. This screen is not presented if running Windows Server 2008 R2.



17. On the **Choose Disk Type** page, set virtual hard disk type as **Dynamically expanding** (recommended). **Fixed size** disk would work but you may need to wait a long time. We recommend that you do not use the **Differencing** option. Click **Next**. In Windows Server 2012 R2 and Windows Server 2012, **Dynamically expanding** is the default option whereas in Windows Server 2008 R2, the default is **Fixed size**.

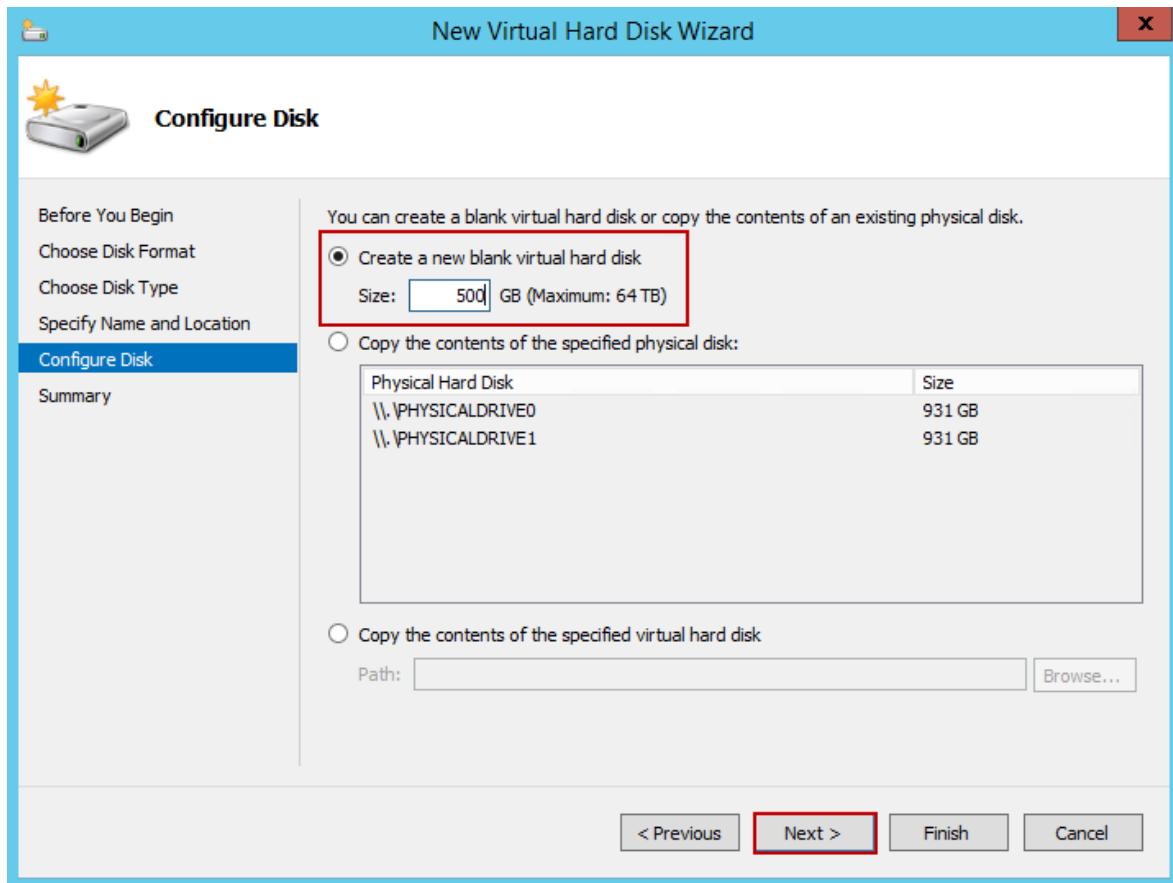


18. On the **Specify Name and Location** page, provide a **name** as well as **location** (you can browse to one) for the data disk. Click **Next**.

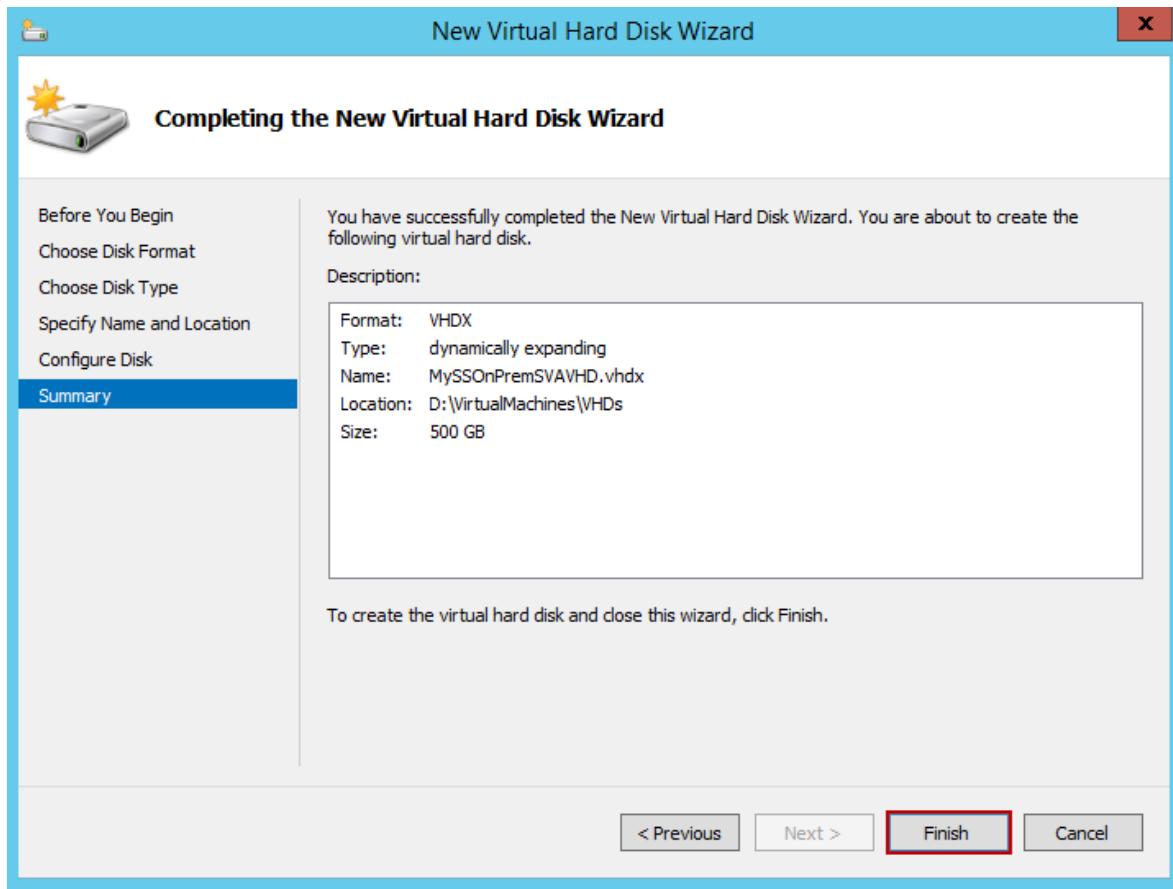


19. On the **Configure Disk** page, select the option **Create a new blank virtual hard disk** and specify the size as **500 GB** (or more). While 500 GB is the minimum

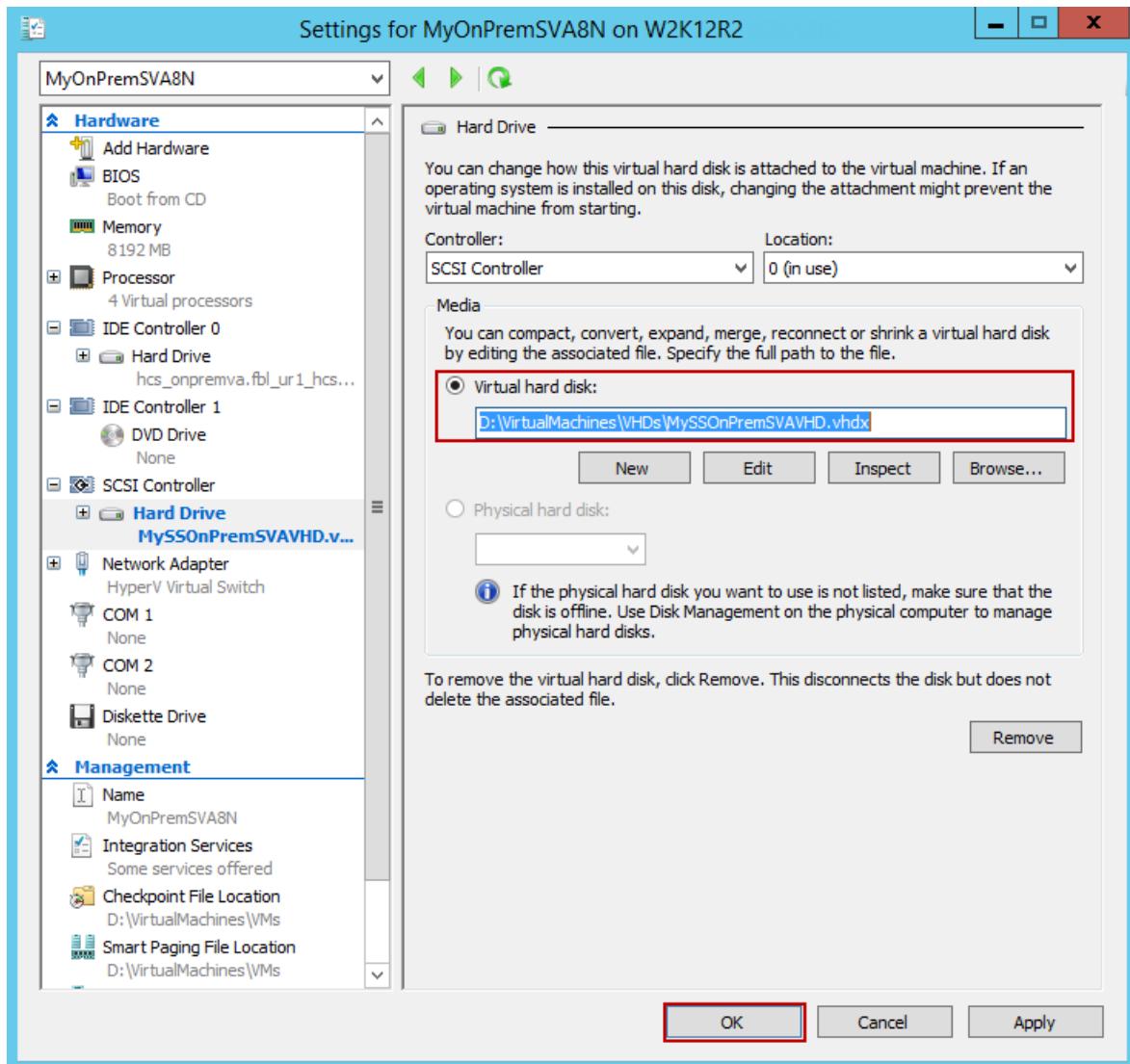
requirement, you can always provision a larger disk. Note that you cannot expand or shrink the disk once provisioned. For more information on the size of disk to provision, review the sizing section in the [best practices document](#). Click **Next**.



20. On the **Summary** page, review the details of your virtual data disk and if satisfied, click **Finish** to create the disk. The wizard closes and a virtual hard disk is added to your machine.



21. Return to the **Settings** page. Click **OK** to close the **Settings** page and return to Hyper-V Manager window.

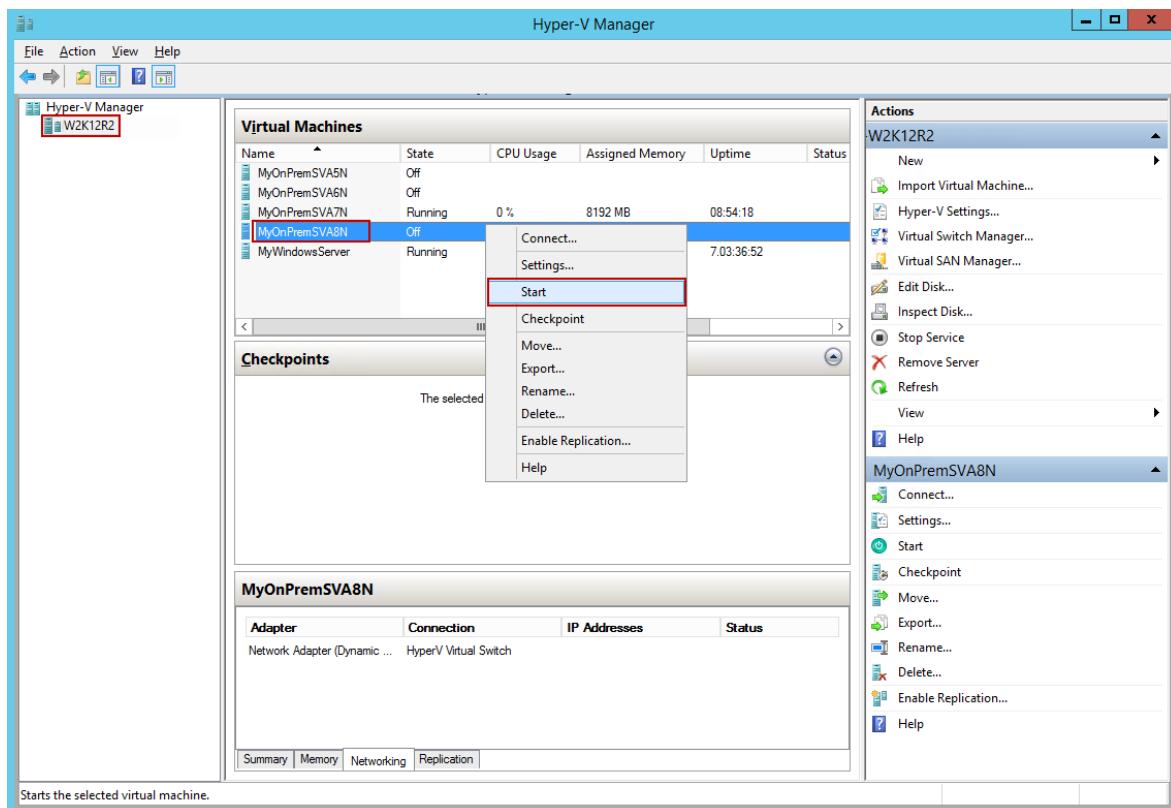


Step 3: Start the virtual array and get the IP

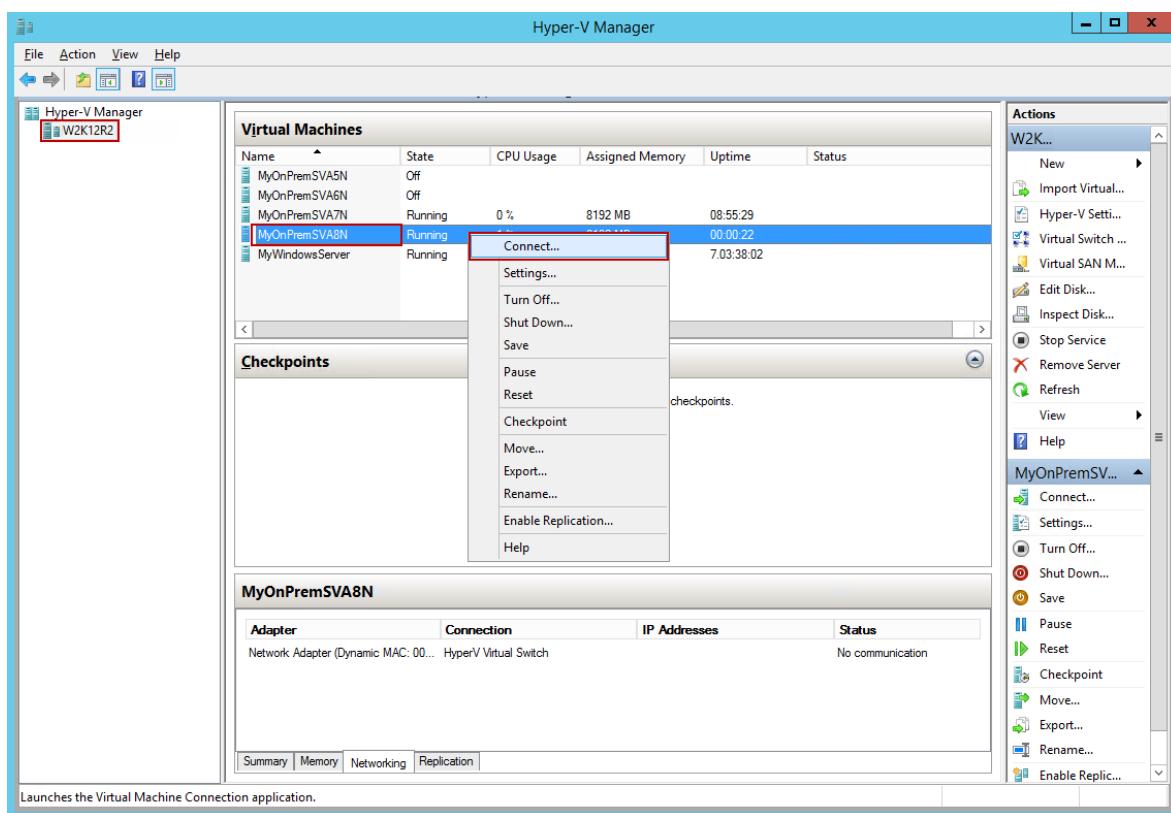
Perform the following steps to start your virtual array and connect to it.

To start the virtual array

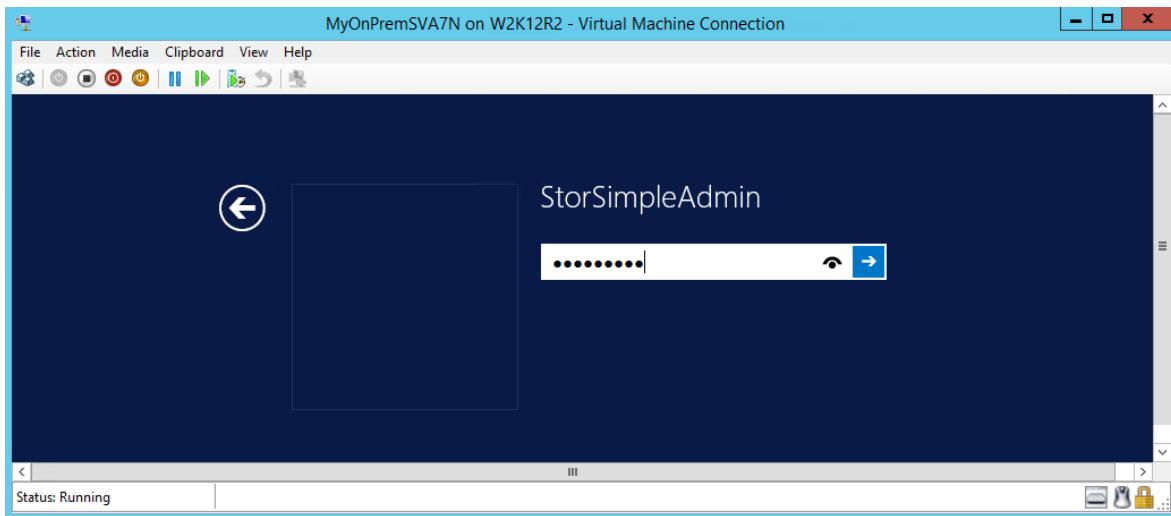
1. Start the virtual array.



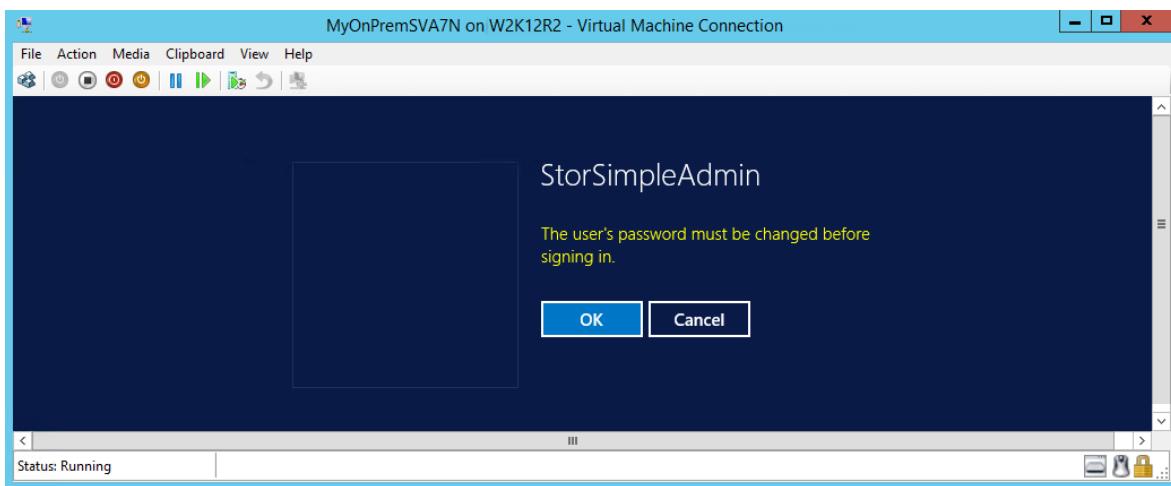
2. After the device is running, select the device, right click, and select **Connect**.



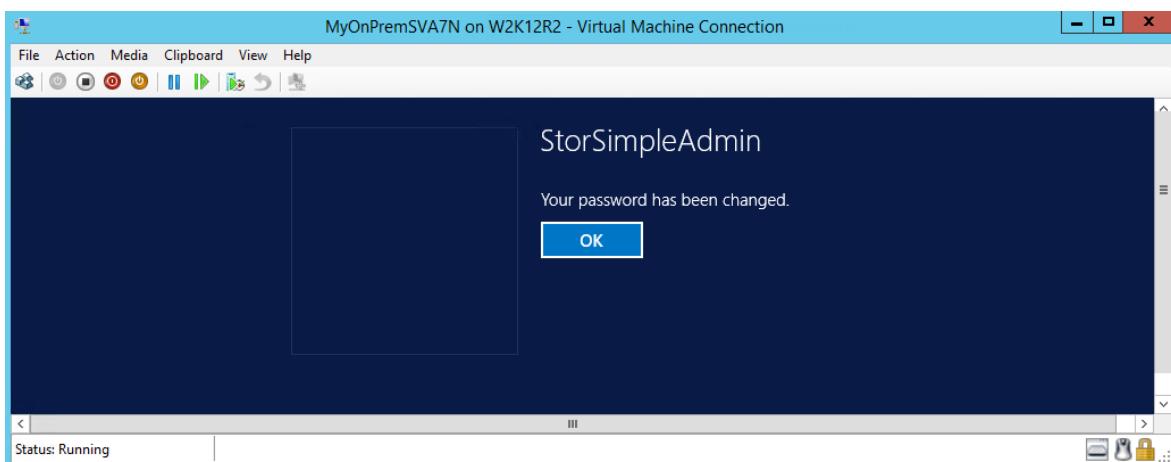
3. You may have to wait 5-10 minutes for the device to be ready. A status message is displayed on the console to indicate the progress. After the device is ready, go to **Action**. Press **Ctrl + Alt + Delete** to log in to the virtual array. The default user is *StorSimpleAdmin* and the default password is *Password1*.



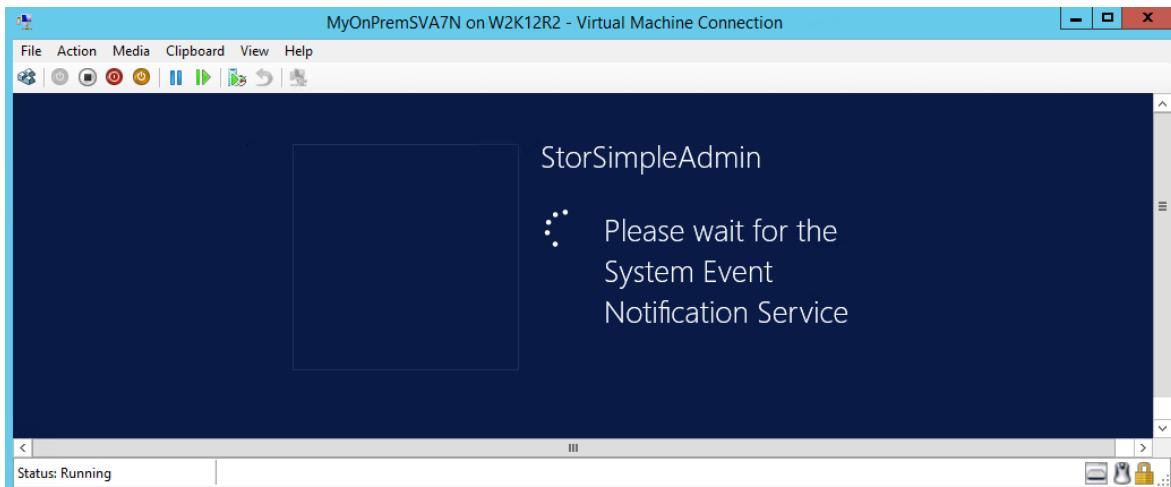
4. For security reasons, the device administrator password expires at the first logon. You are prompted to change the password.



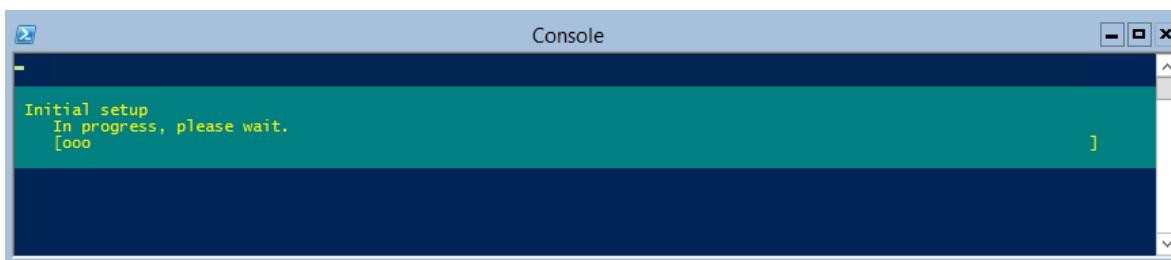
Enter a password that contains at least 8 characters. The password must satisfy at least 3 out of the following 4 requirements: uppercase, lowercase, numeric, and special characters. Reenter the password to confirm it. You are notified that the password has changed.



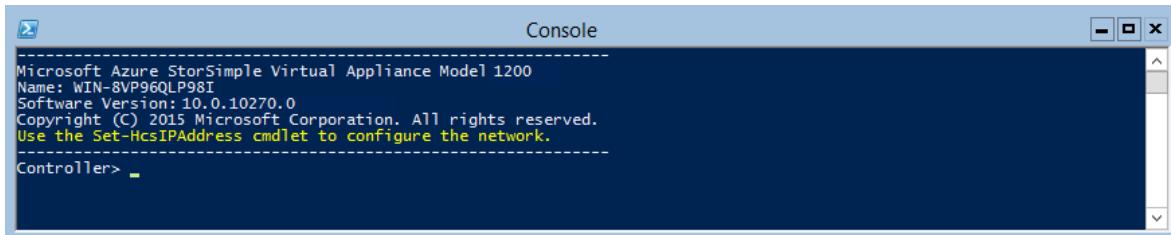
5. After the password is successfully changed, the virtual array may restart. Wait for the device to start.



The Windows PowerShell console of the device is displayed along with a progress bar.



6. Steps 6-8 only apply when booting up in a non-DHCP environment. If you are in a DHCP environment, then skip these steps and go to step 9. If you booted up your device in non-DHCP environment, you will see the following screen.



Next, configure the network.

7. Use the `Get-HcsIpAddress` command to list the network interfaces enabled on your virtual array. If your device has a single network interface enabled, the default name assigned to this interface is `Ethernet`.

```
Microsoft Azure StorSimple Virtual Appliance Model 1200
Name: WIN-KNI26M3B7NK
Software Version: 10.0.10270.0
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Use the Set-HcsIpAddress cmdlet to configure the network.

Controller> Get-HcsIpAddress

Name          : Ethernet
UseDhcp       : True
OperationalStatus : Up
IpAddress     :
Gateway      :

Controller>
```

8. Use the `Set-HcsIpAddress` cmdlet to configure the network. See the following example:

```
Set-HcsIpAddress -Name Ethernet -IpAddress 10.161.22.90 -Netmask 255.255.255.0
-Gateway 10.161.22.1
```

```
Support Console
Use the Set-HcsIpAddress cmdlet to configure the network.

Controller> Get-Help Set-HcsIpAddress

NAME
  Set-HcsIpAddress

SYNTAX
  Set-HcsIpAddress [[-Name] <string>] [[-IpAddress] <string>] [[-Netmask] <string>] [[-Gateway] <string>]
    [<CommonParameters>]

  Set-HcsIpAddress [[-UseDhcp]]  [<CommonParameters>]

ALIASES
  None

REMARKS
  None

Controller> Set-HcsIpAddress -Name Ethernet -IpAddress 10.161.22.90 -Netmask 255.255.255.0 -Gateway 10.161.22.1
```

9. After the initial setup is complete and the device has booted up, you will see the device banner text. Make a note of the IP address and the URL displayed in the banner text to manage the device. Use this IP address to connect to the web UI of your virtual array and complete the local setup and registration.

```
Microsoft Azure StorSimple Virtual Appliance Model 1200
Name: WIN-HUM9TL64KPB
Software Version: 10.0.10270.0
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Use https://10.161.22.93 to manage the appliance.

Controller>
```

10. (Optional) Perform this step only if you are deploying your device in the Government Cloud. You will now enable the United States Federal Information Processing Standard (FIPS) mode on your device. The FIPS 140 standard defines cryptographic algorithms approved for use by US Federal government computer systems for the protection of sensitive data.

- a. To enable the FIPS mode, run the following cmdlet:

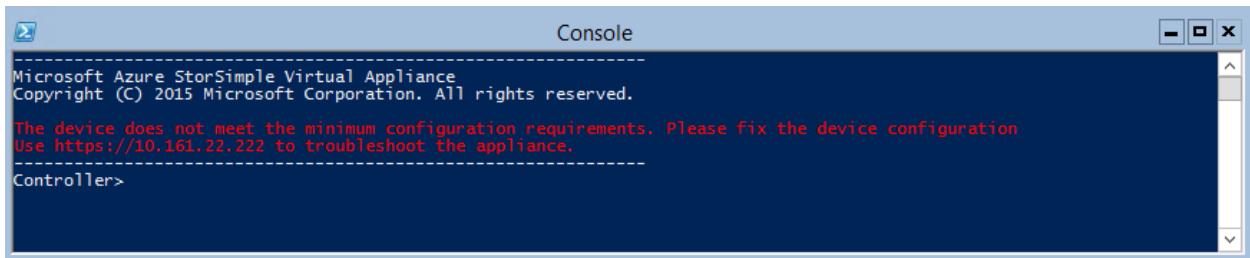
```
Enable-HcsFIPSMODE
```

- b. Reboot your device after you have enabled the FIPS mode so that the cryptographic validations take effect.

 **Note**

You can either enable or disable FIPS mode on your device. Alternating the device between FIPS and non-FIPS mode is not supported.

If your device does not meet the minimum configuration requirements, you see the following error in the banner text (shown below). Modify the device configuration so that the machine has adequate resources to meet the minimum requirements. You can then restart and connect to the device. Refer to the minimum configuration requirements in Step 1: Ensure that the host system meets minimum virtual array requirements.



If you face any other error during the initial configuration using the local web UI, refer to the following workflows:

- Run diagnostic tests to [troubleshoot web UI setup](#).
- [Generate log package and view log files](#).

Next steps

- [Set up your StorSimple Virtual Array as a file server](#)
- [Set up your StorSimple Virtual Array as an iSCSI server](#)

Deploy StorSimple Virtual Array - Provision in VMware

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Overview

This tutorial describes how to provision and connect to a StorSimple Virtual Array on a host system running VMware ESXi 5.0, 5.5, 6.0 or 6.5. This article applies to the deployment of StorSimple Virtual Arrays in Azure portal and the Microsoft Azure Government Cloud.

You need administrator privileges to provision and connect to a virtual device. The provisioning and initial setup can take around 10 minutes to complete.

Provisioning prerequisites

The prerequisites to provision a virtual device on a host system running VMware ESXi 5.0, 5.5, 6.0 or 6.5, are as follows.

For the StorSimple Device Manager service

Before you begin, make sure that:

- You have completed all the steps in [Prepare the portal for StorSimple Virtual Array](#).
- You have downloaded the virtual device image for VMware from the Azure portal.
For more information, see [Step 3: Download the virtual device image](#) of [Prepare](#)

[the portal for StorSimple Virtual Array guide.](#)

For the StorSimple virtual device

Before you deploy a virtual device, make sure that:

- You have access to a host system running Hyper-V (2008 R2 or later) that can be used to provision a device.
- The host system is able to dedicate the following resources to provision your virtual device:
 - A minimum of 4 cores.
 - At least 8 GB of RAM. If you plan to configure the virtual array as file server, 8 GB supports less than 2 million files. You need 16 GB RAM to support 2 - 4 million files.
 - One network interface.
 - A 500 GB virtual disk for system data.

For the network in datacenter

Before you begin, make sure that:

- You have reviewed the networking requirements to deploy a StorSimple virtual device and configured the datacenter network as per the requirements.

Step-by-step provisioning

To provision and connect to a virtual device, you need to perform the following steps:

1. Ensure that the host system has sufficient resources to meet the minimum virtual device requirements.
2. Provision a virtual device in your hypervisor.
3. Start the virtual device and get the IP address.

Step 1: Ensure host system meets minimum virtual device requirements

To create a virtual device, you will need:

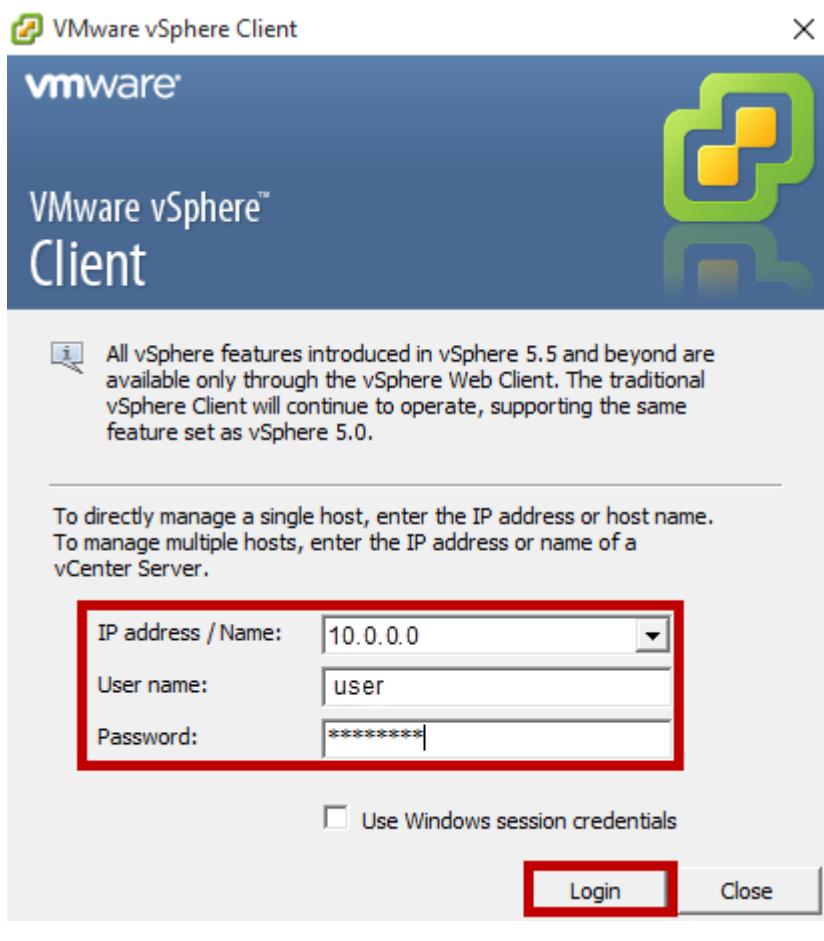
- Access to a host system running VMware ESXi Server 5.0, 5.5, 6.0 or 6.5.

- VMware vSphere client on your system to manage the ESXi host.
 - A minimum of 4 cores.
 - At least 8 GB of RAM. If you plan to configure the virtual array as file server, 8 GB supports less than 2 million files. You need 16 GB RAM to support 2 - 4 million files.
 - One network interface connected to the network capable of routing traffic to Internet. The minimum Internet bandwidth should be 5 Mbps to allow for optimal working of the device.
 - A 500 GB virtual disk for data.

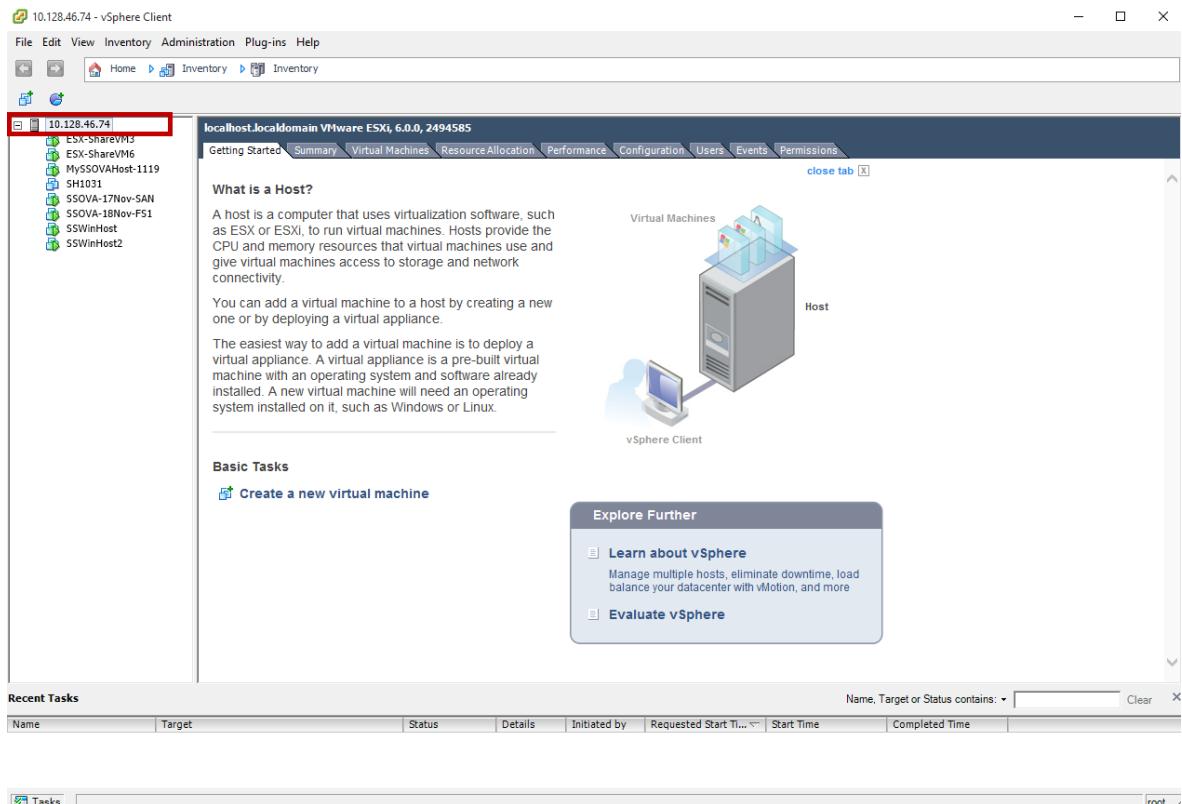
Step 2: Provision a virtual device in hypervisor

Perform the following steps to provision a virtual device in your hypervisor.

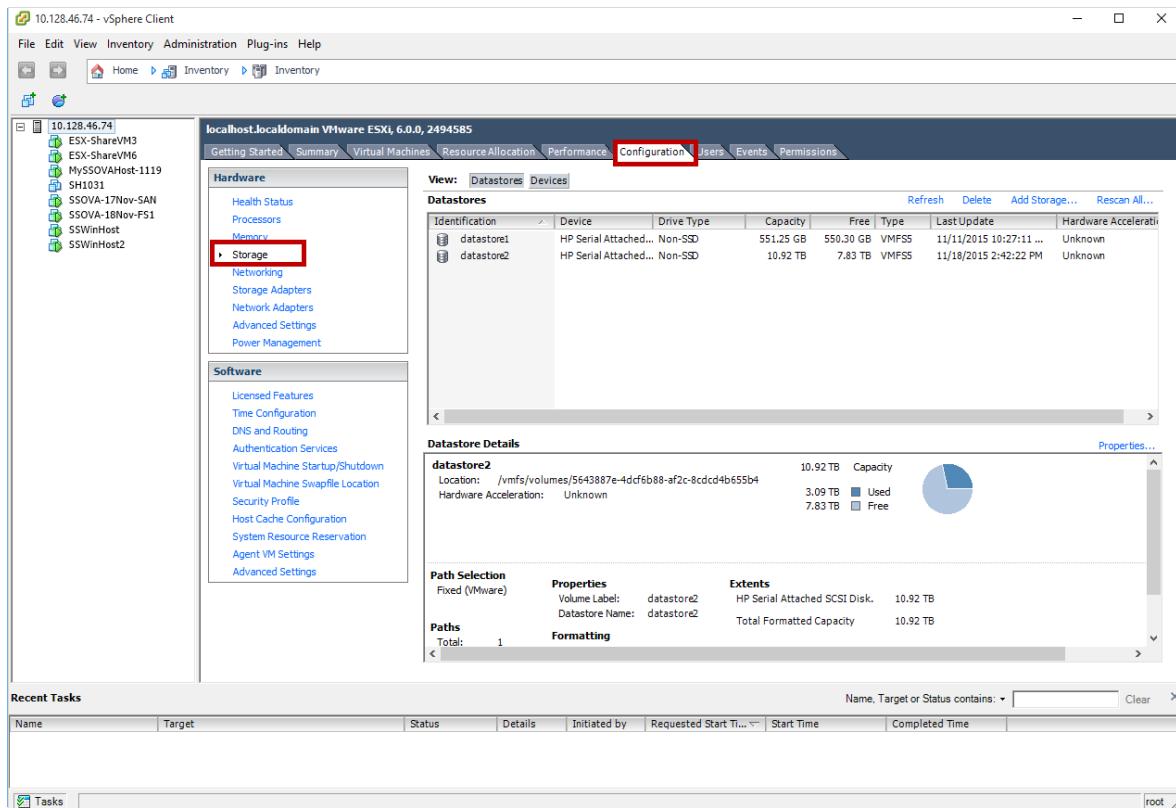
1. Copy the virtual device image on your system. You downloaded this virtual image through the Azure portal.
 - a. Ensure that you have downloaded the latest image file. If you downloaded the image earlier, download it again to ensure you have the latest image. The latest image has two files (instead of one).
 - b. Make a note of the location where you copied the image as you are using this image later in the procedure.
2. Log in to the ESXi server using the vSphere client. You need to have administrator privileges to create a virtual machine.



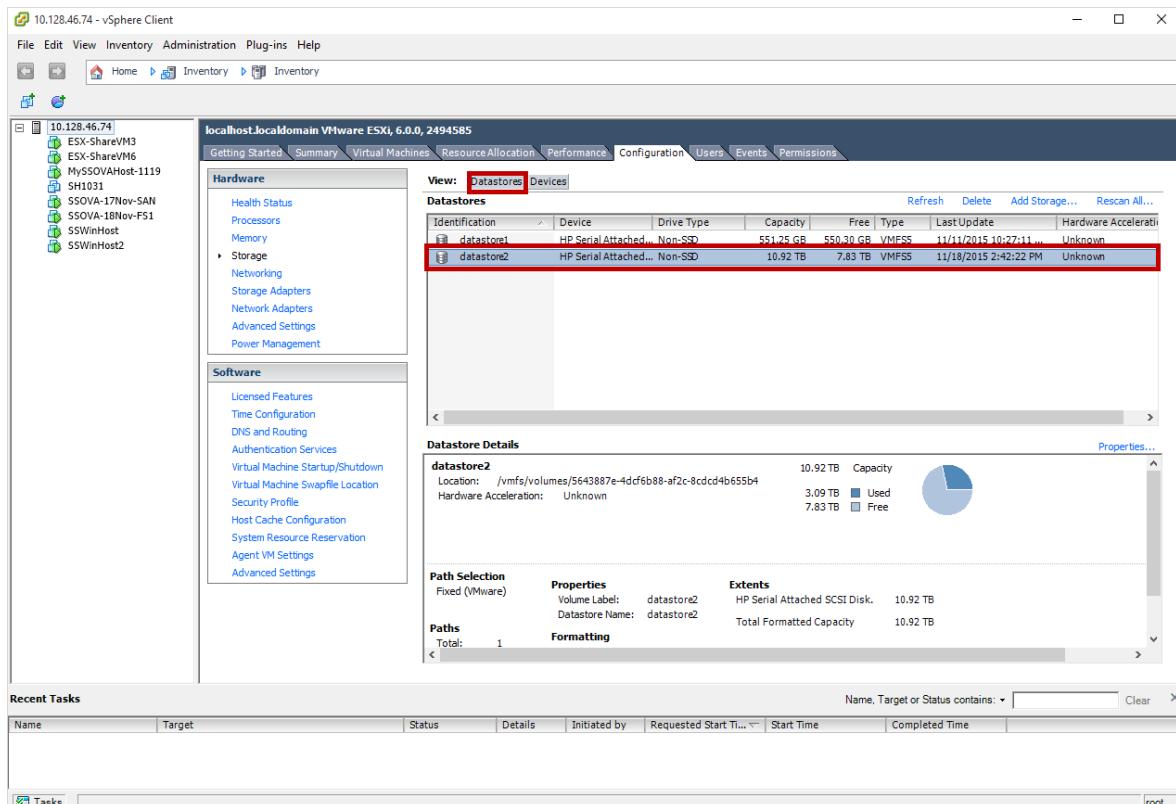
- In the vSphere client, in the inventory section in the left pane, select the ESXi Server.



- Upload the VMDK to the ESXi server. Navigate to the Configuration tab in the right pane. Under **Hardware**, select **Storage**.



5. In the right pane, under **Datastores**, select the datastore where you want to upload the VMDK. The datastore must have enough free space for the OS and data disks.

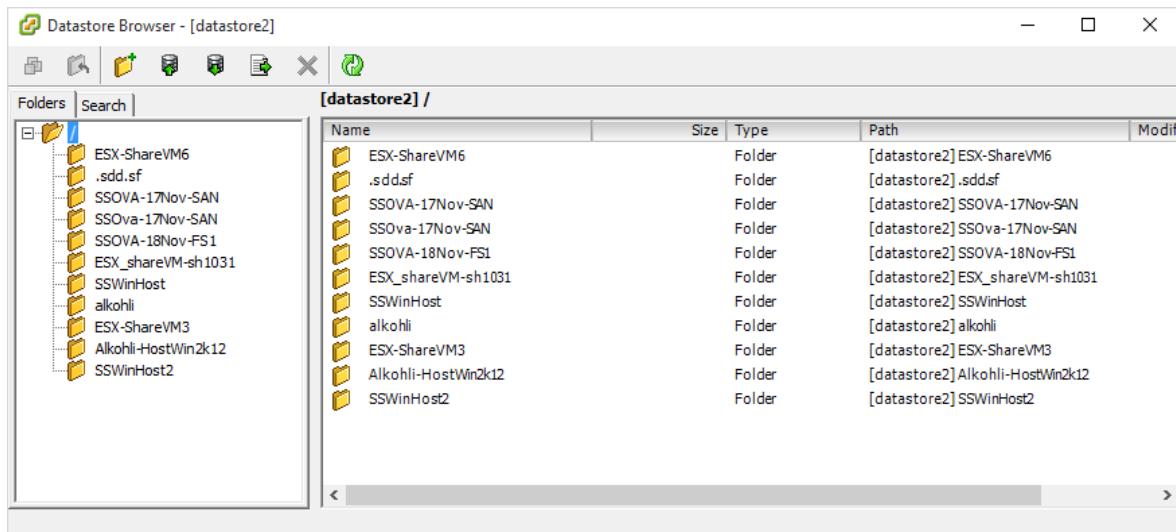


6. Right-click and select **Browse Datastore**.

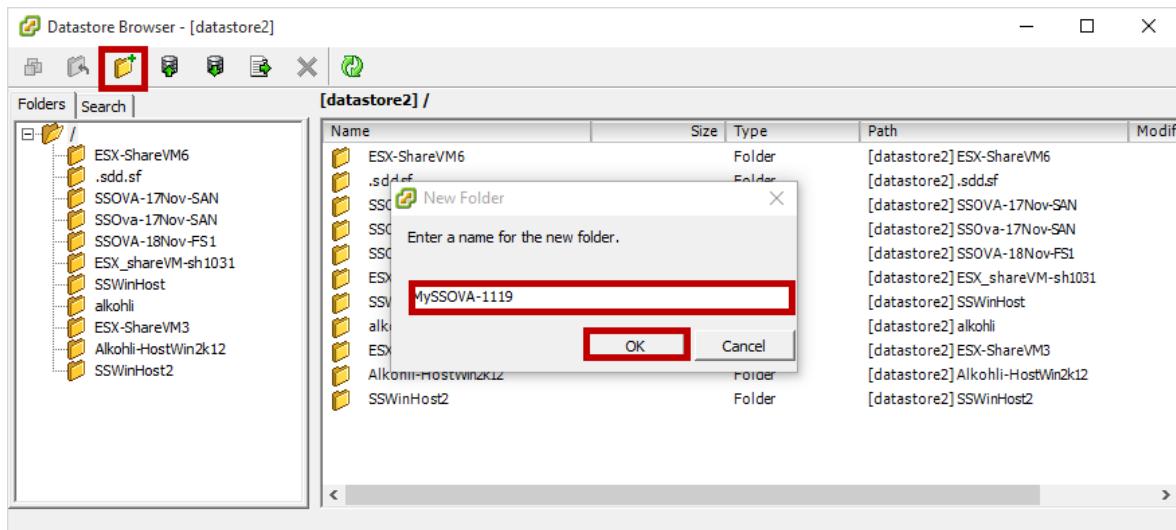
Browser Datastore...

- Rename
- Unmount
- Delete
- Refresh
- Properties...
- Copy to Clipboard Ctrl+C

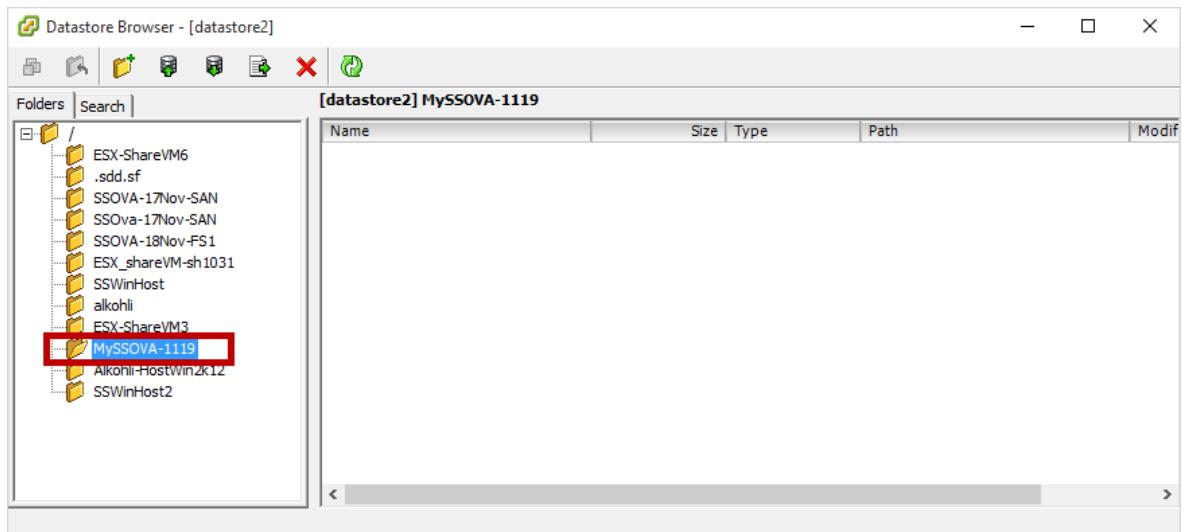
7. A Datastore Browser window appears.



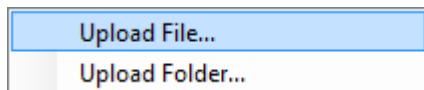
8. In the tool bar, click icon to create a new folder. Specify the folder name and make a note of it. You will use this folder name later when creating a virtual machine (recommended best practice). Click OK.



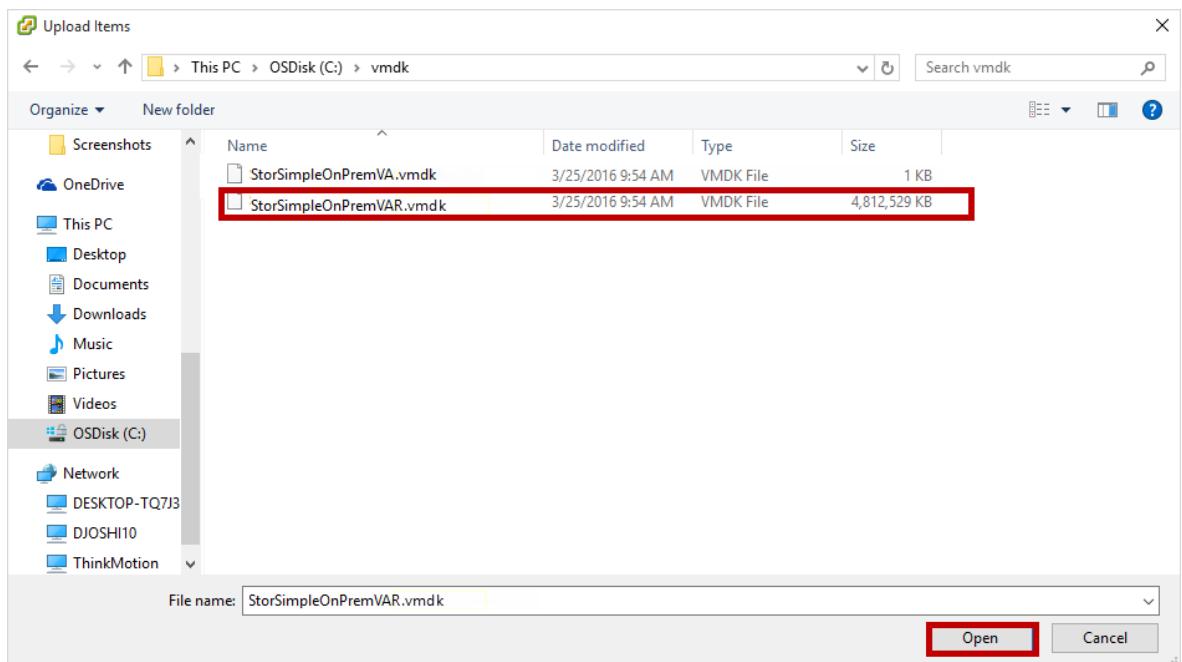
9. The new folder appears in the left pane of the Datastore Browser.



10. Click the Upload icon  and select Upload File.

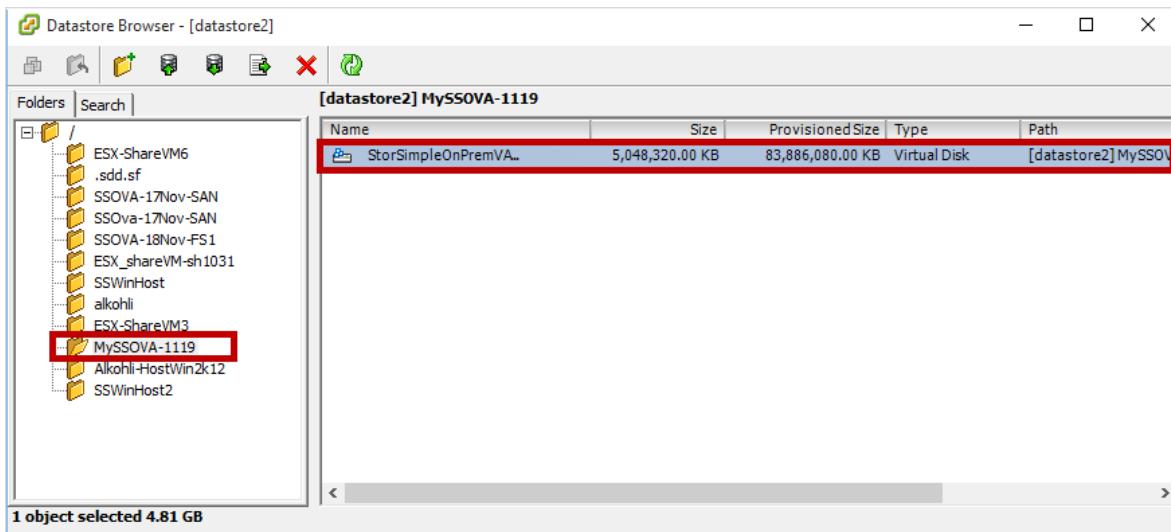


11. Browse and point to the VMDK files that you downloaded. There are two files. Select a file to upload.



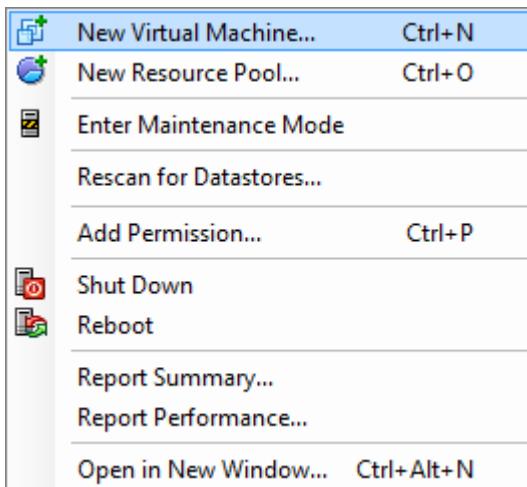
12. Click Open. The upload of the VMDK file to the specified datastore starts. It may take several minutes for the file to upload.

13. After the upload is complete, you see the file in the datastore in the folder you created.

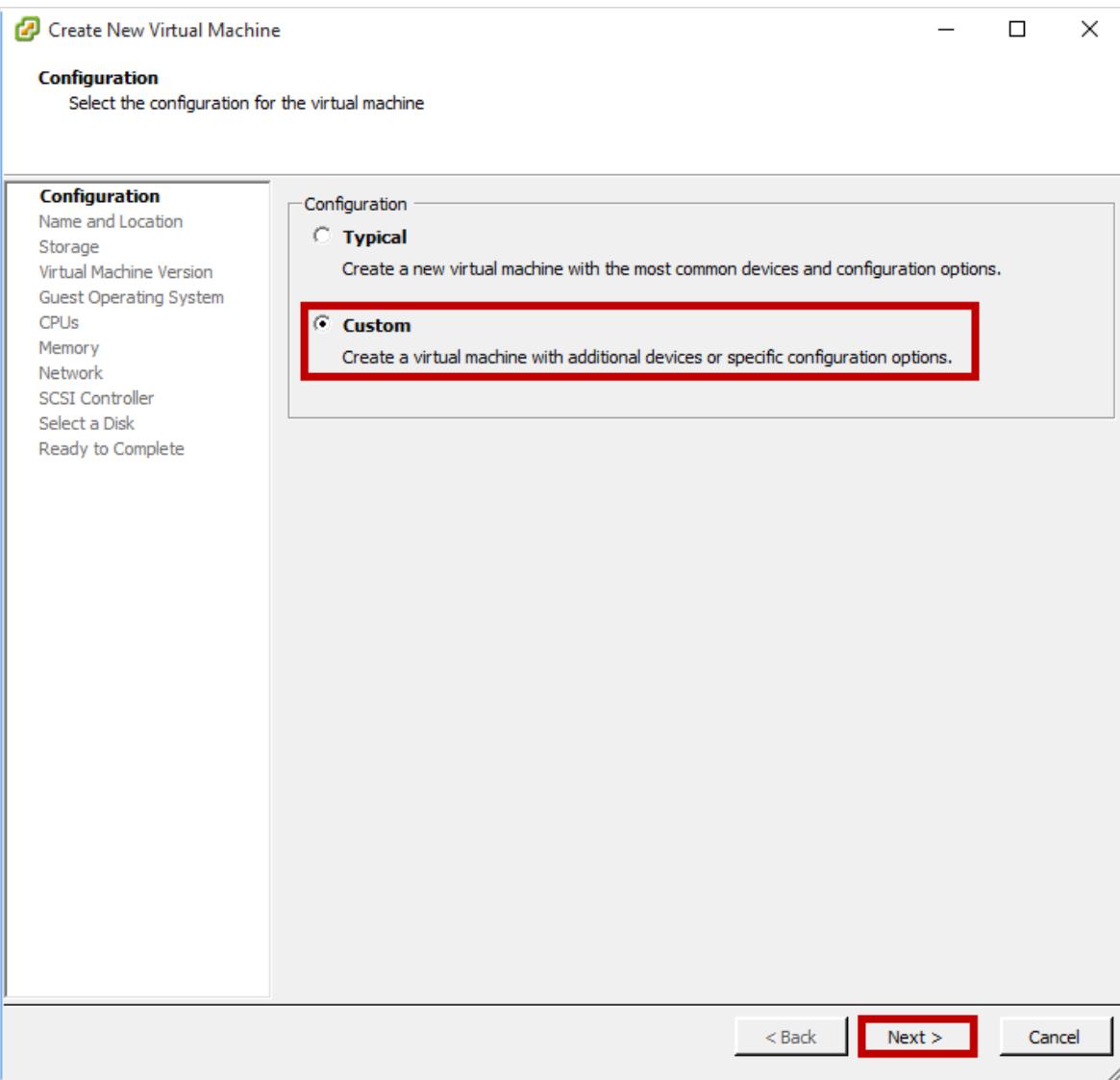


Now upload the second VMDK file to the same datastore.

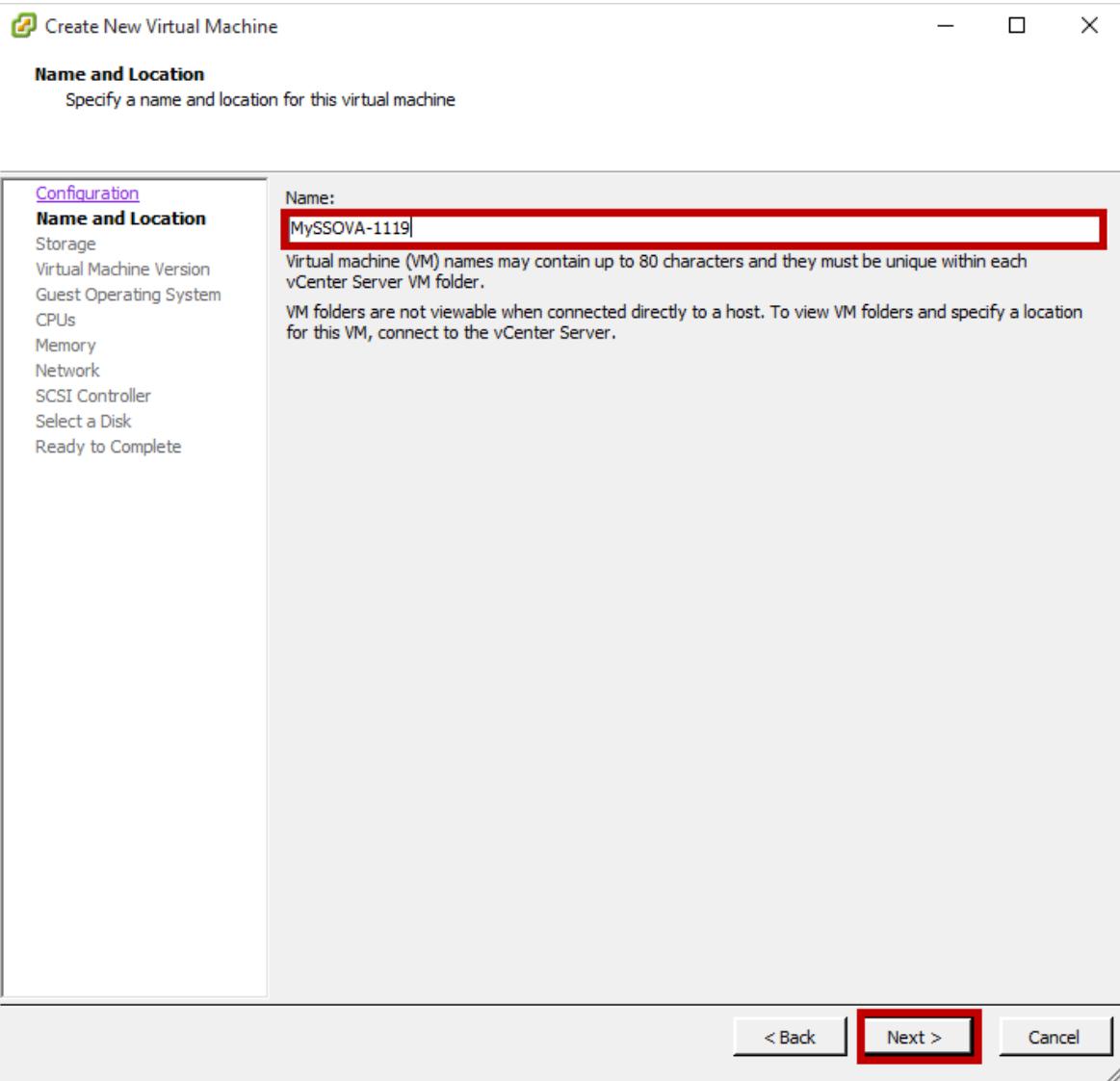
14. Return to the vSphere client window. With ESXi server selected, right-click and select New Virtual Machine.



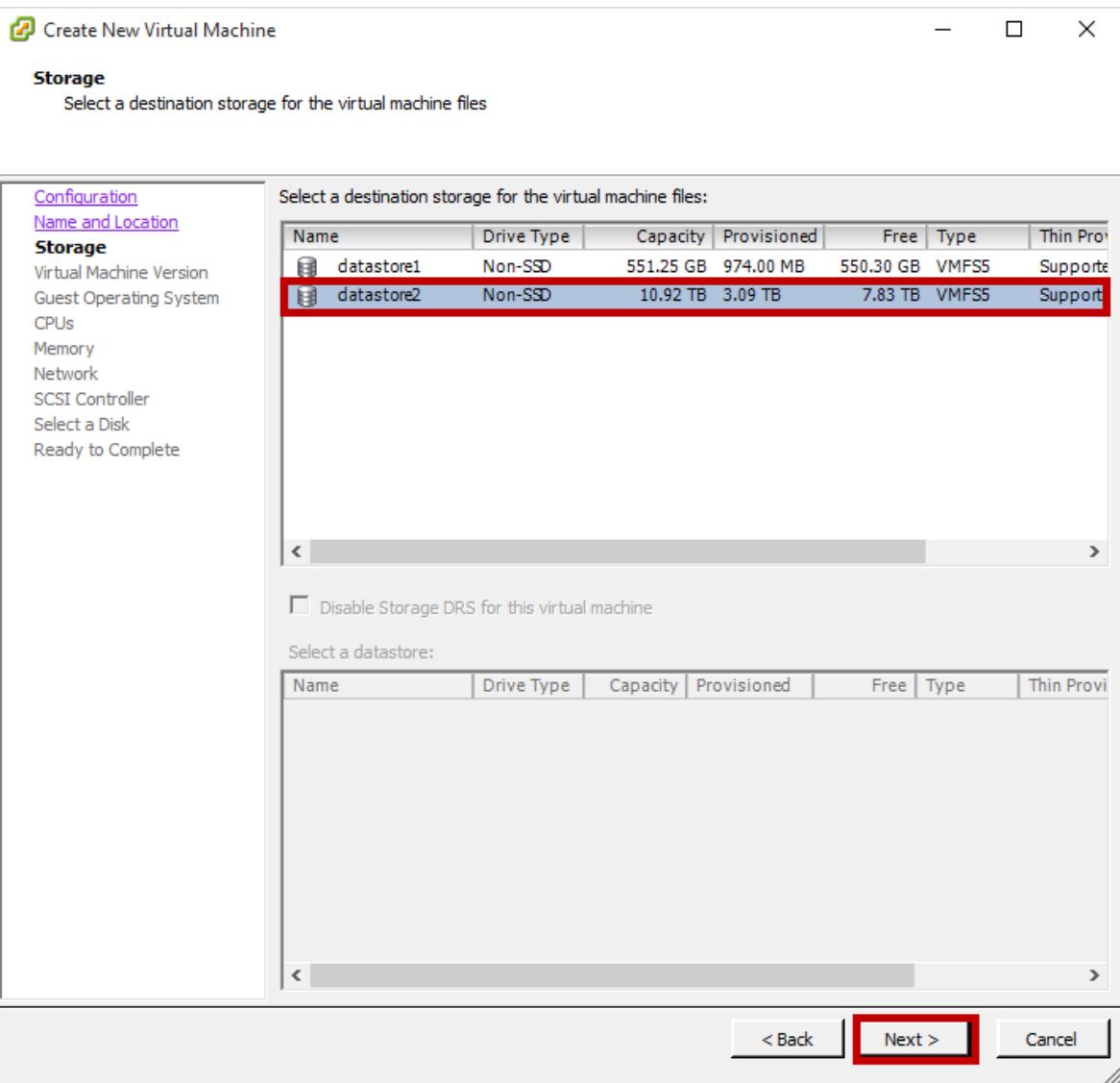
15. A Create New Virtual Machine window will appear. On the Configuration page, select the **Custom** option. Click **Next**.



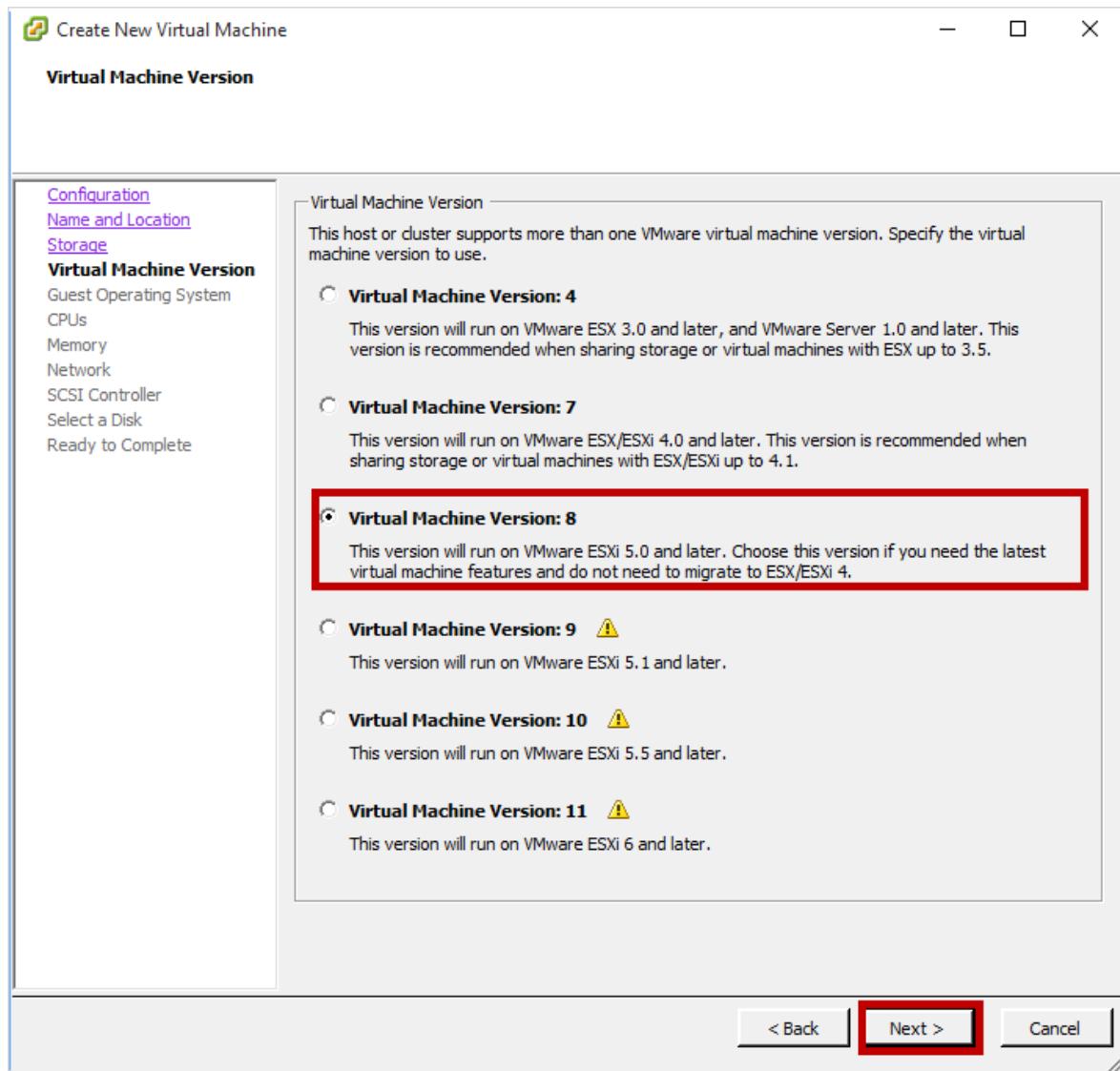
16. On the **Name and Location** page, specify the name of your virtual machine. This name should match the folder name (recommended best practice) you specified earlier in Step 8.



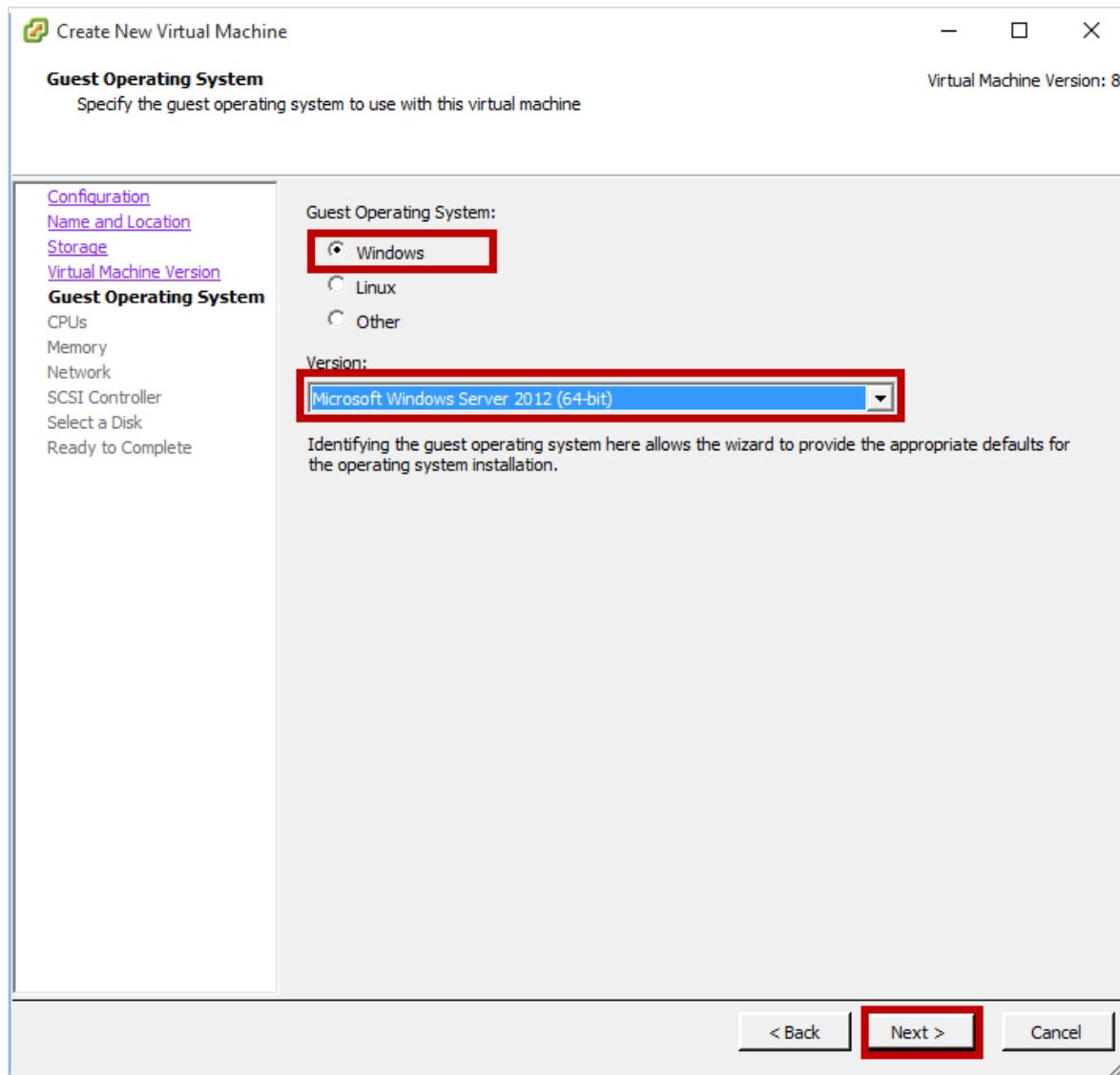
17. On the **Storage** page, select a datastore you want to use to provision your VM.



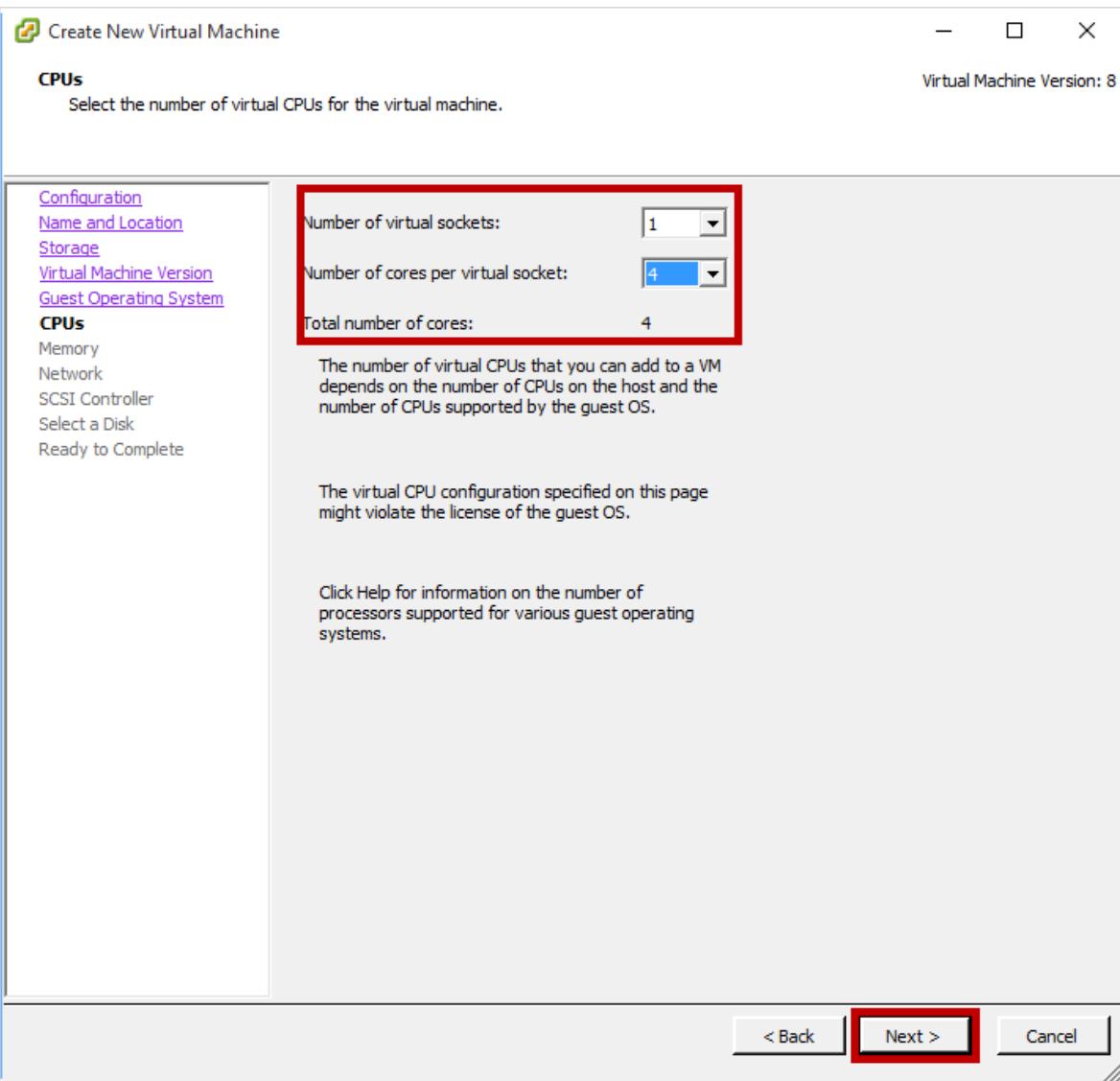
18. On the **Virtual Machine Version** page, select **Virtual Machine Version: 8**.



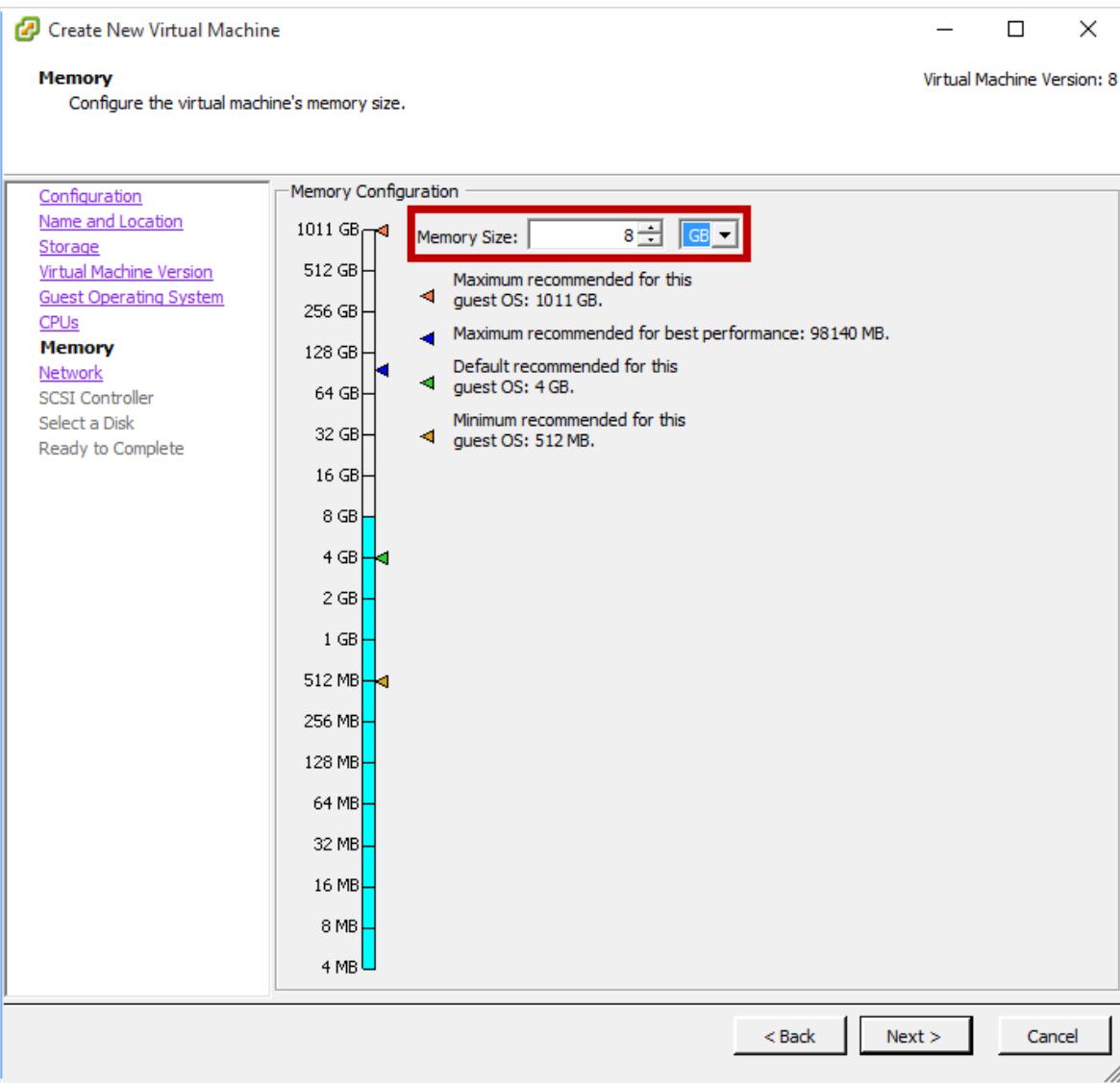
19. On the **Guest Operating System** page, select the **Guest Operating System** as **Windows**. For **Version**, from the dropdown list, select **Microsoft Windows Server 2012 (64-bit)**.



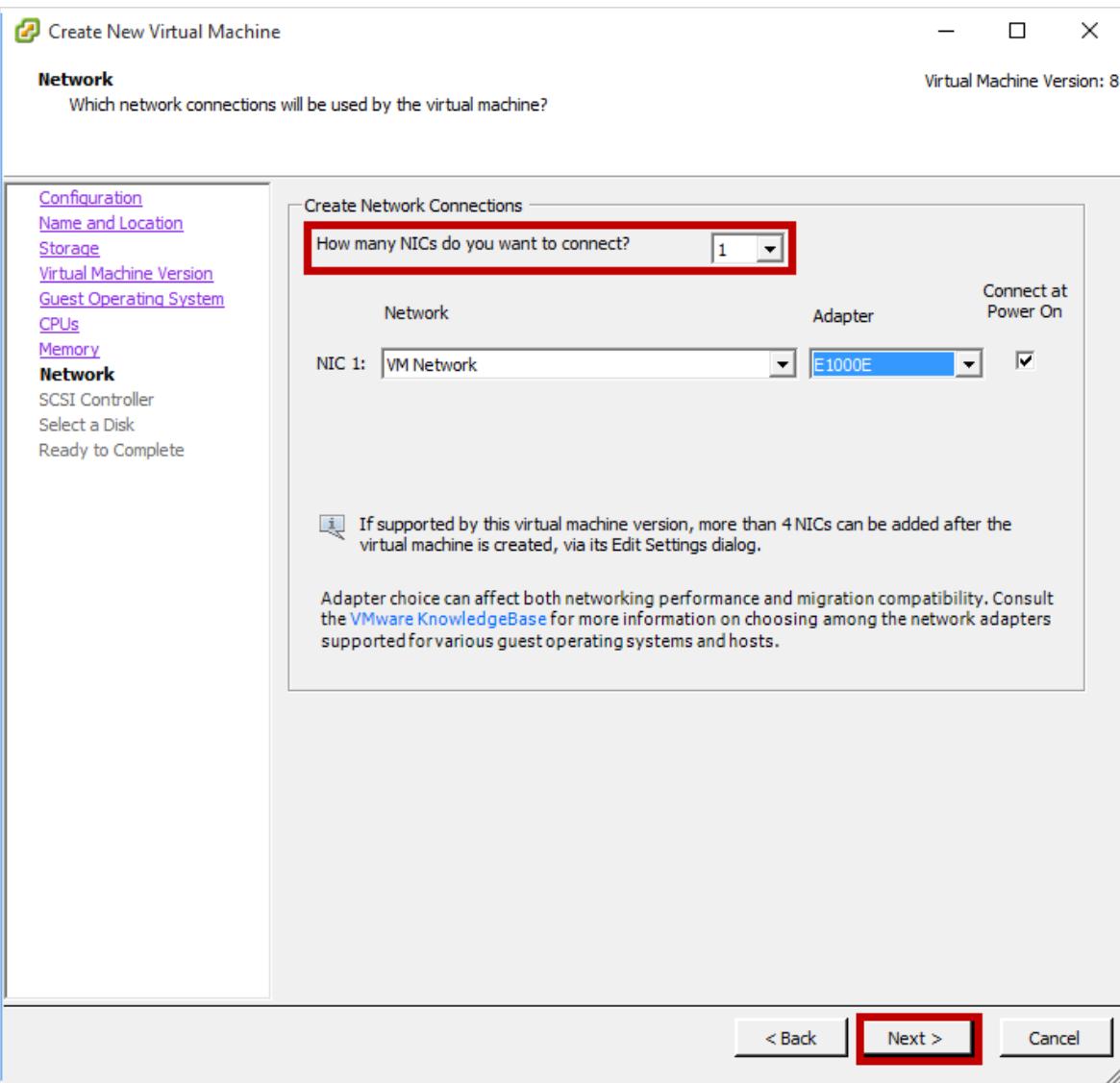
20. On the CPUs page, adjust the Number of virtual sockets and Number of cores per virtual socket so that the Total number of cores is 4 (or more). Click Next.



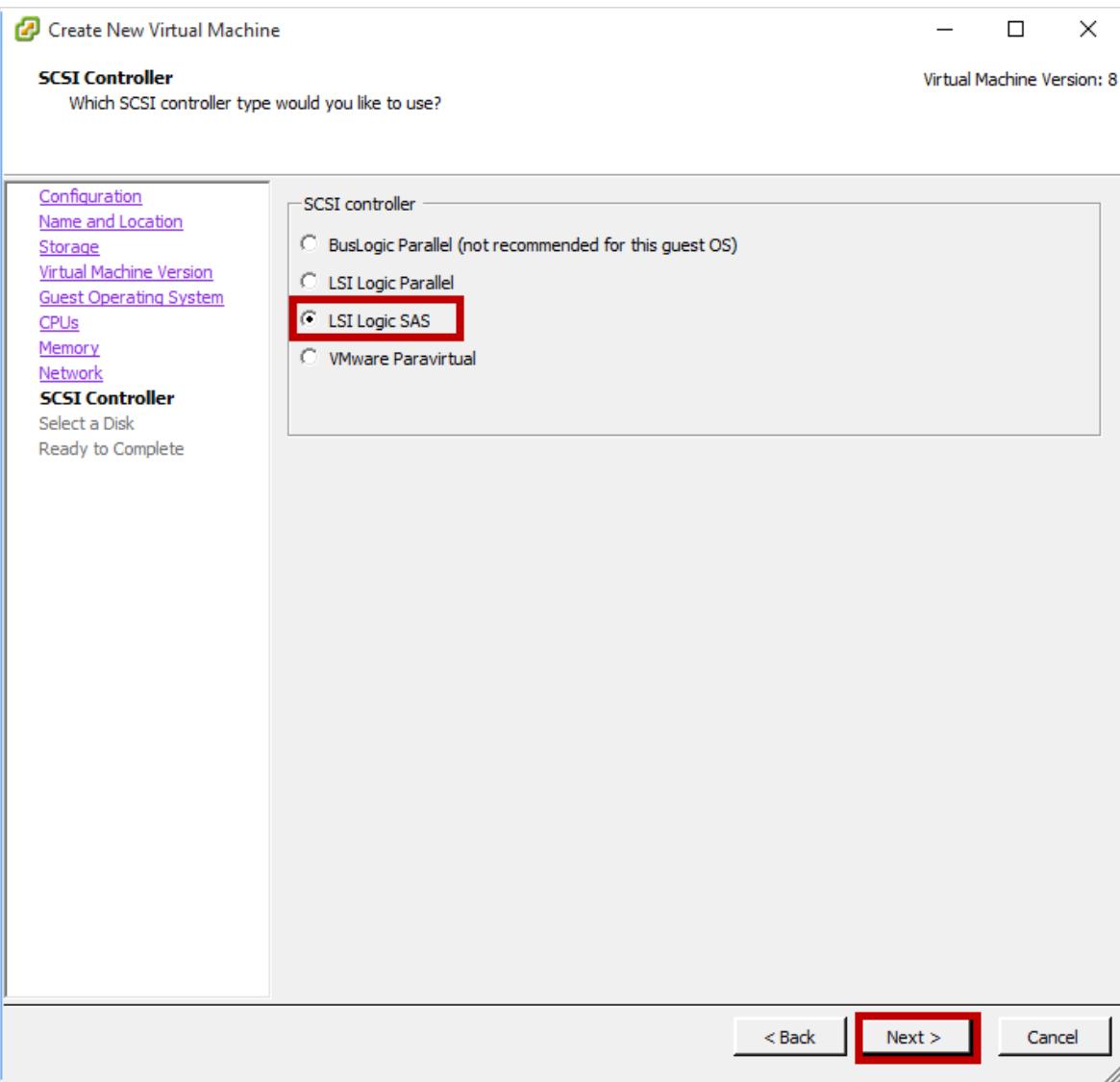
21. On the **Memory** page, specify 8 GB (or more) of RAM. Click **Next**.



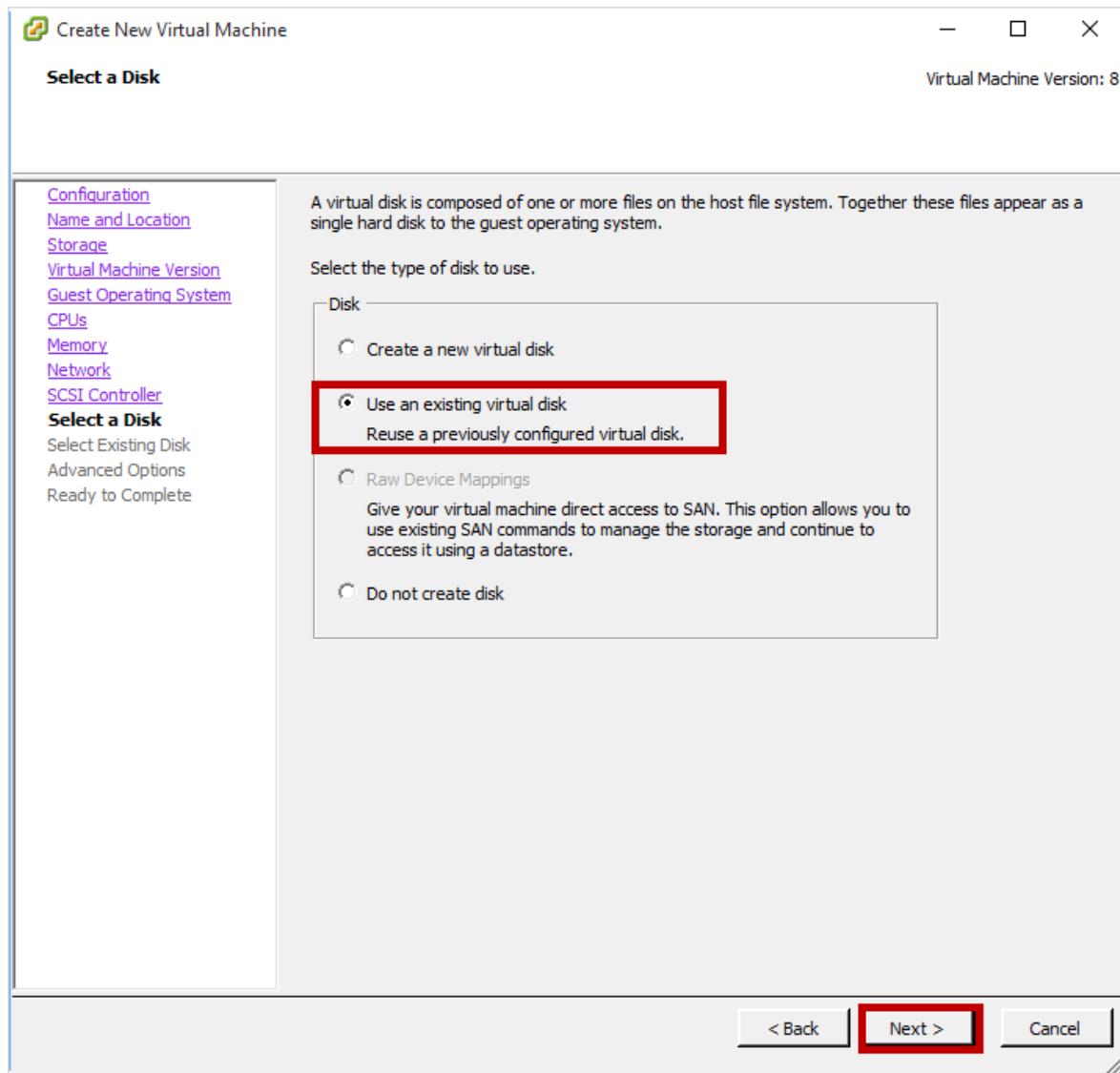
22. On the **Network** page, specify the number of the network interfaces. The minimum requirement is one network interface.



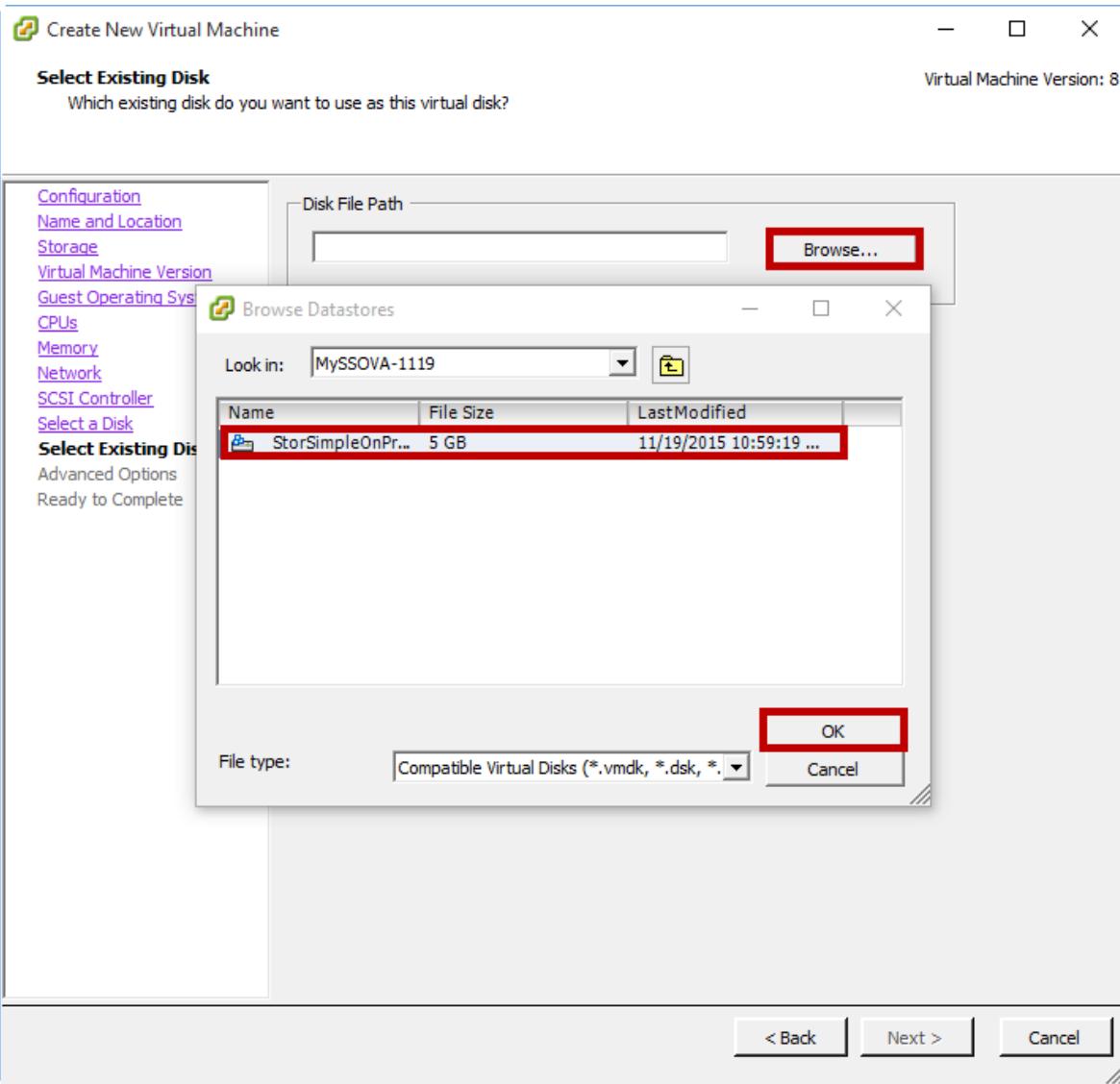
23. On the **SCSI Controller** page, accept the default LSI Logic SAS controller.



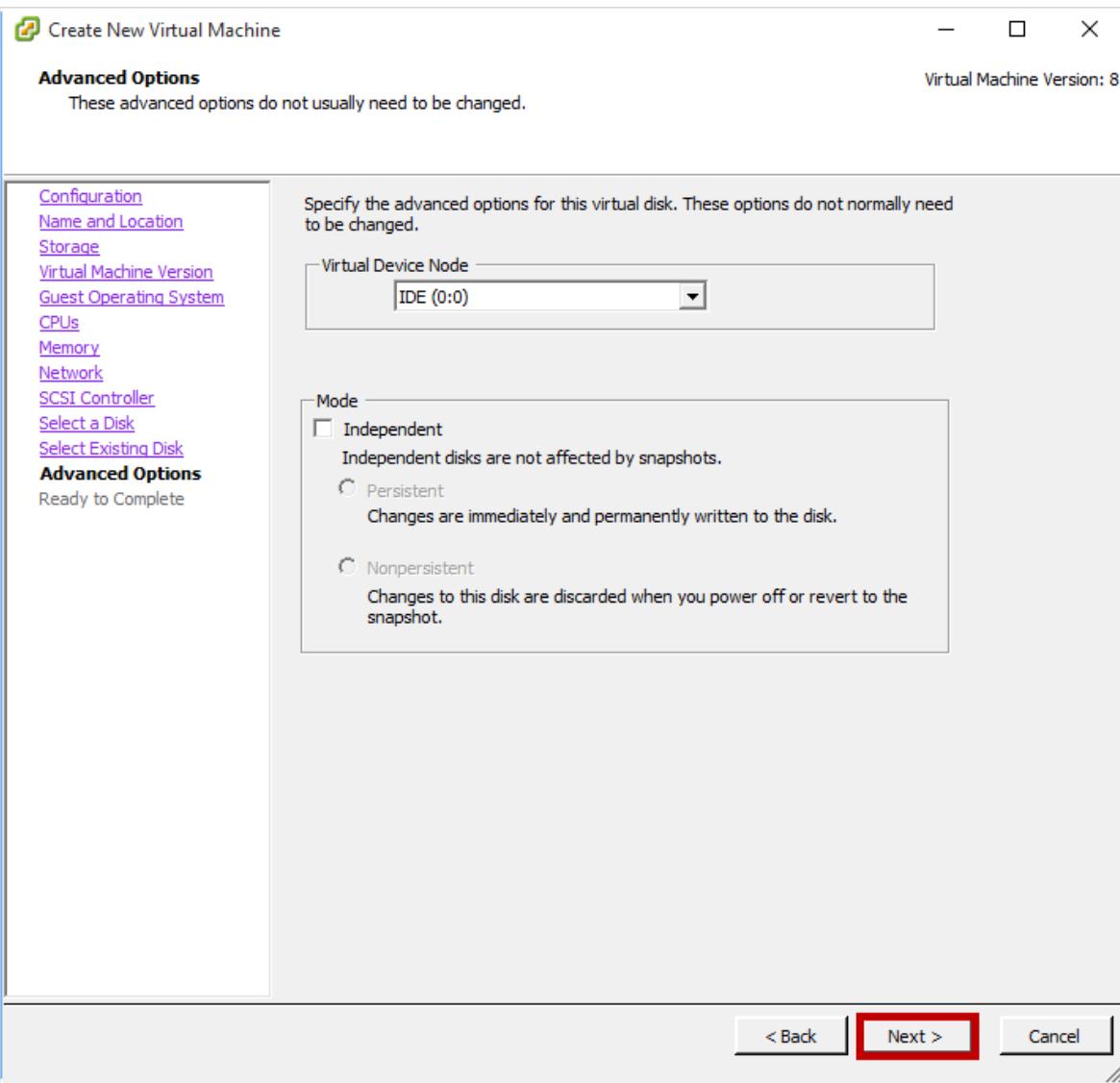
24. On the Select a Disk page, choose Use an existing virtual disk. Click Next.



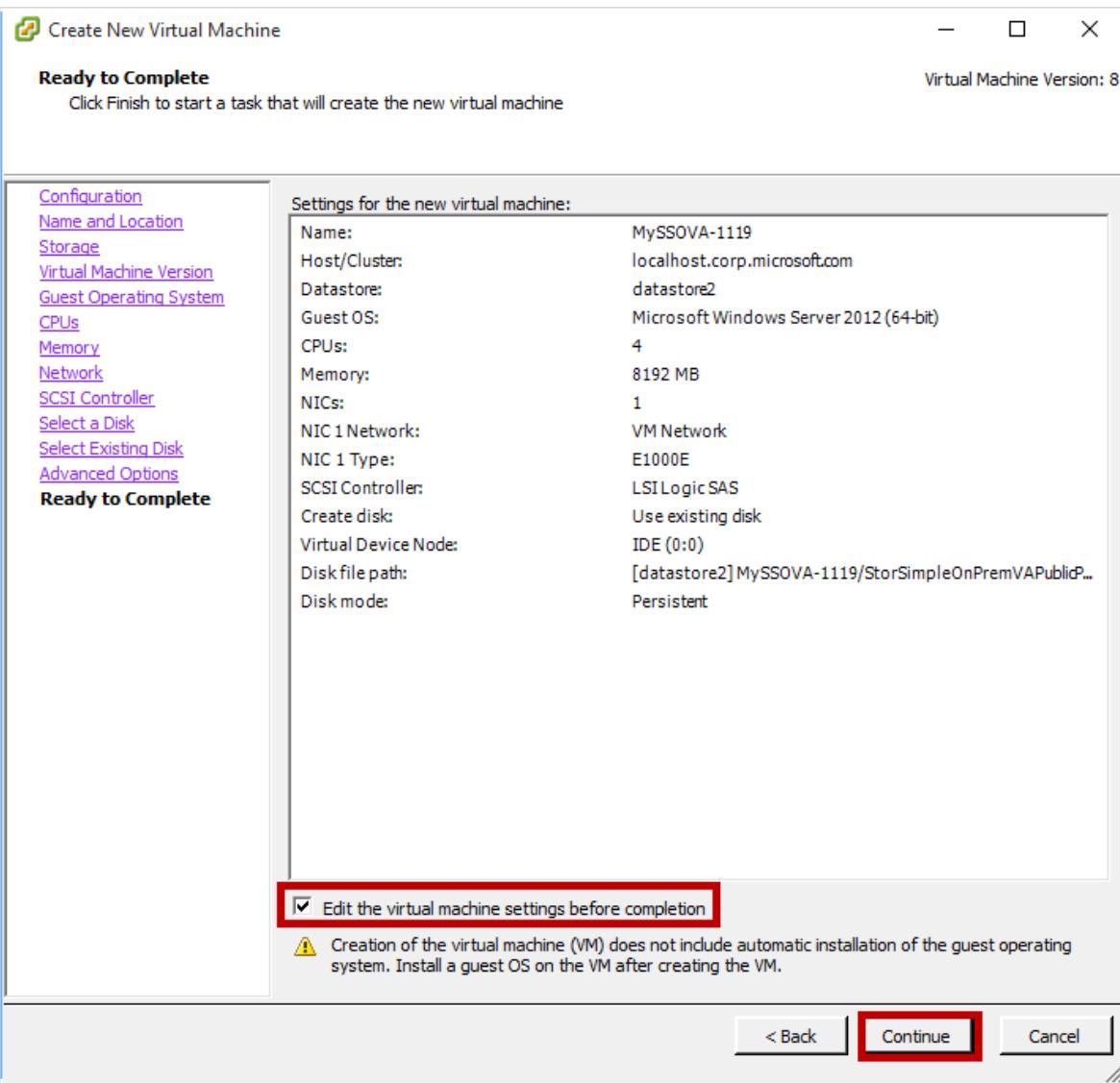
25. On the **Select Existing Disk** page, under **Disk File Path**, click **Browse**. This opens a **Browse Datastores** dialog. Navigate to the location where you uploaded the VMDK. You now see only one file in the datastore as the two files that you initially uploaded have been merged. Select the file and click **OK**. Click **Next**.



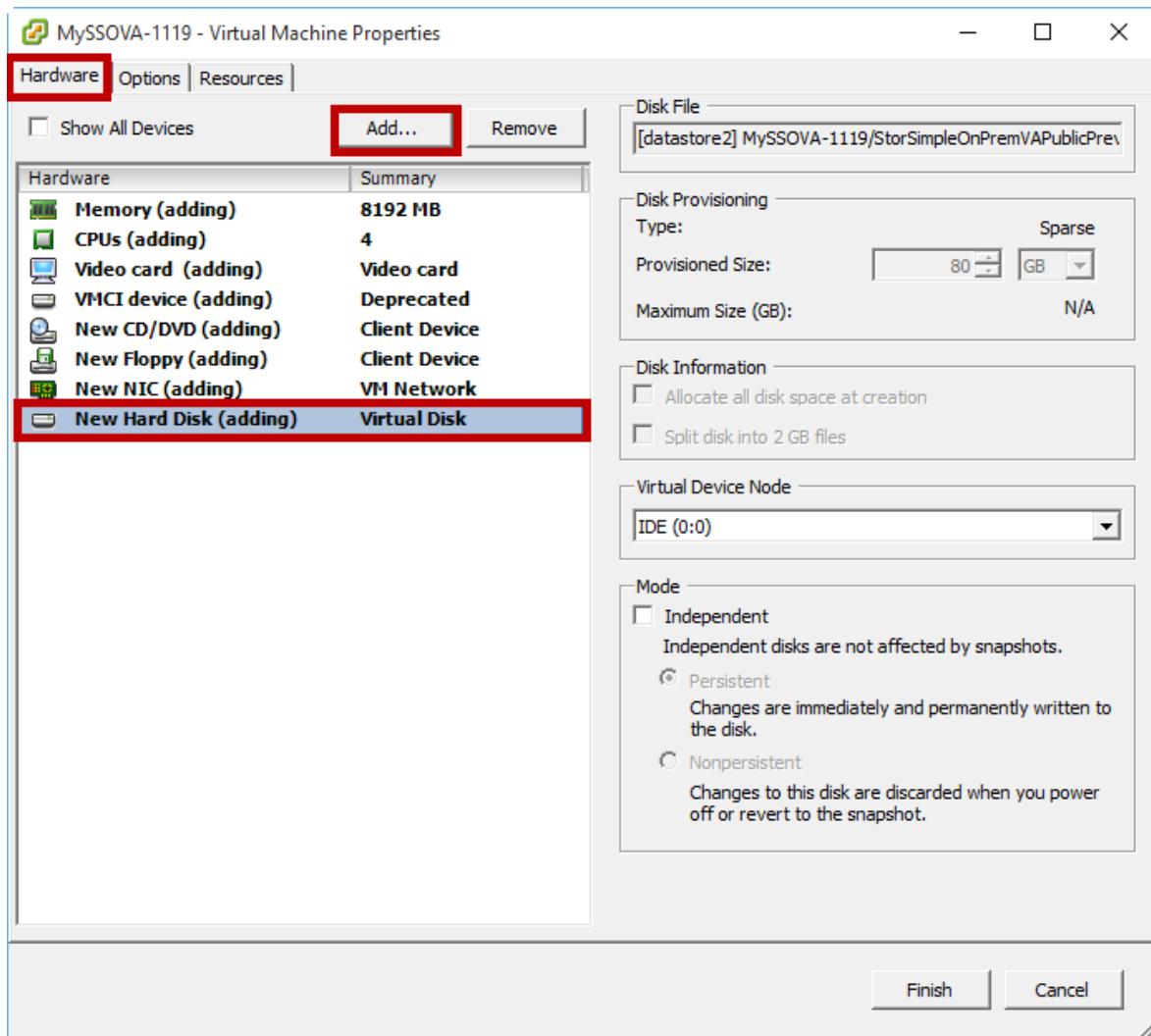
26. On the **Advanced Options** page, accept the default and click **Next**.



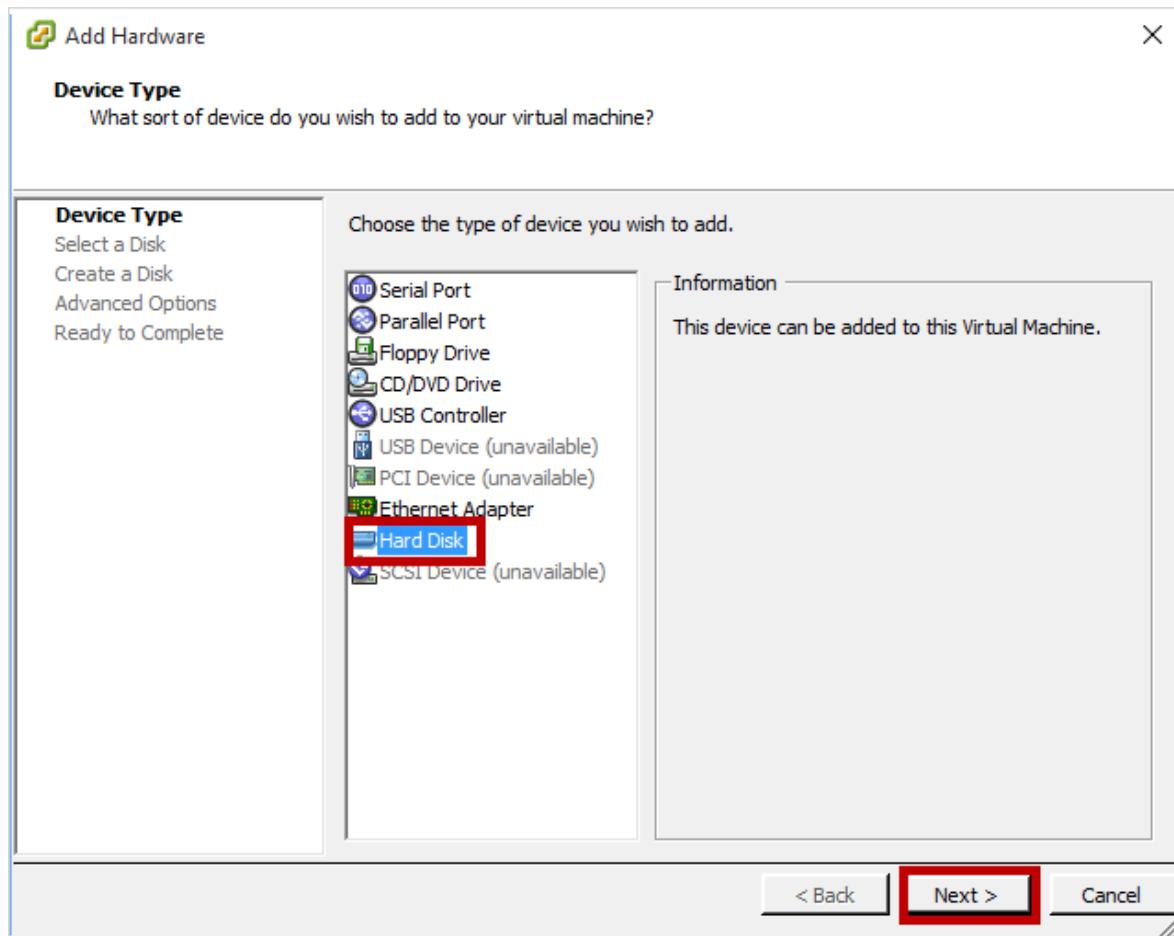
27. On the **Ready to Complete** page, review all the settings associated with the new virtual machine. Check **Edit the virtual machine settings before completion**. Click **Continue**.



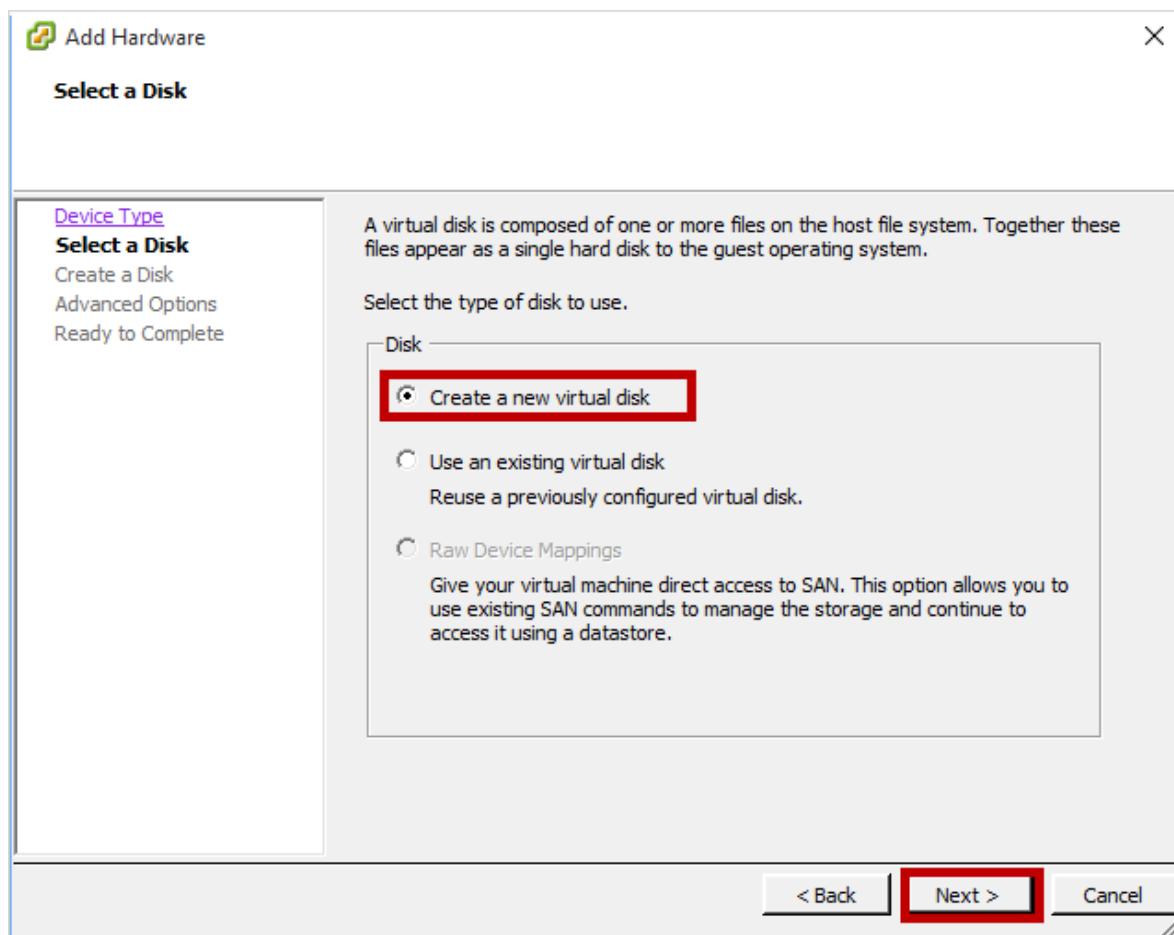
28. On the Virtual Machines Properties page, in the Hardware tab, locate the device hardware. Select New Hard Disk. Click Add.



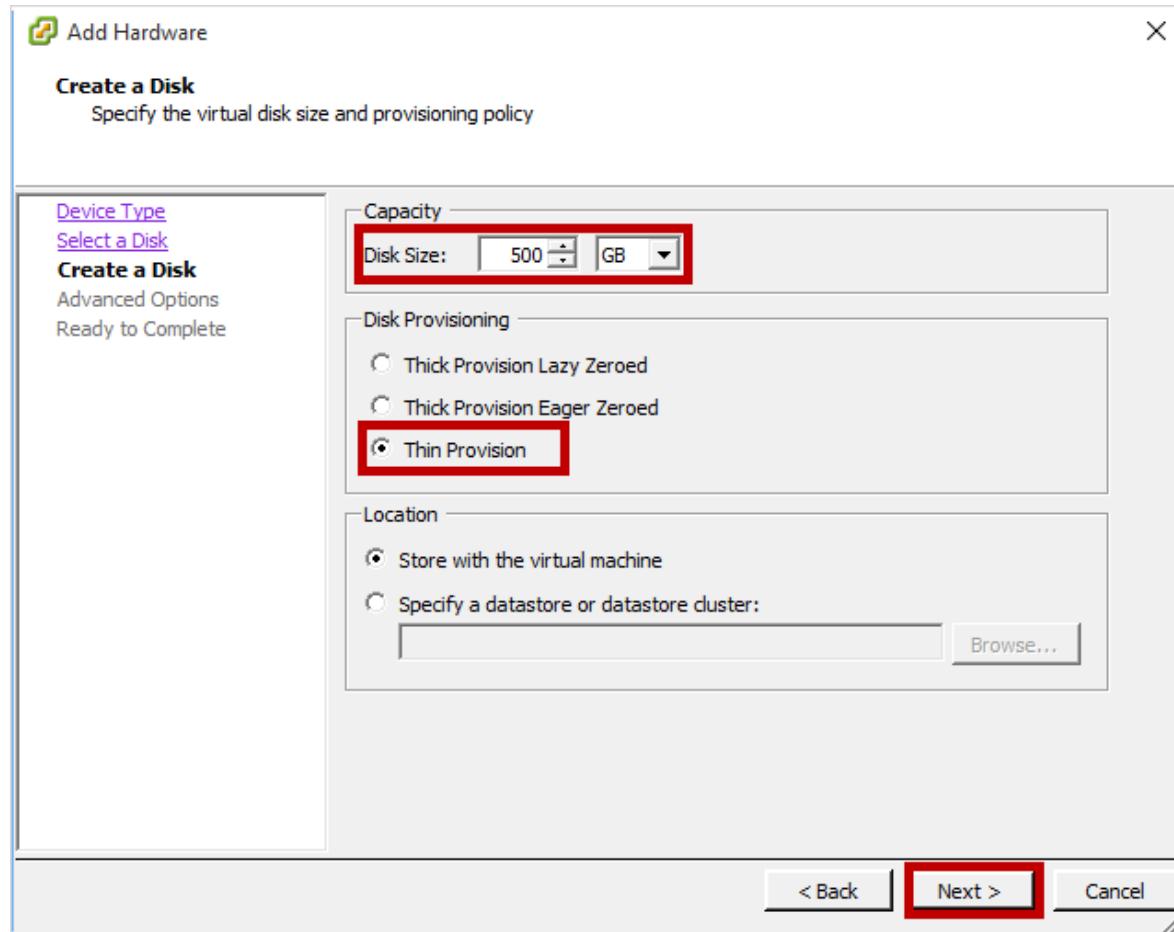
29. You see a Add Hardware window. On the Device Type page, under Choose the type of device you wish to add, select Hard Disk, and click Next.



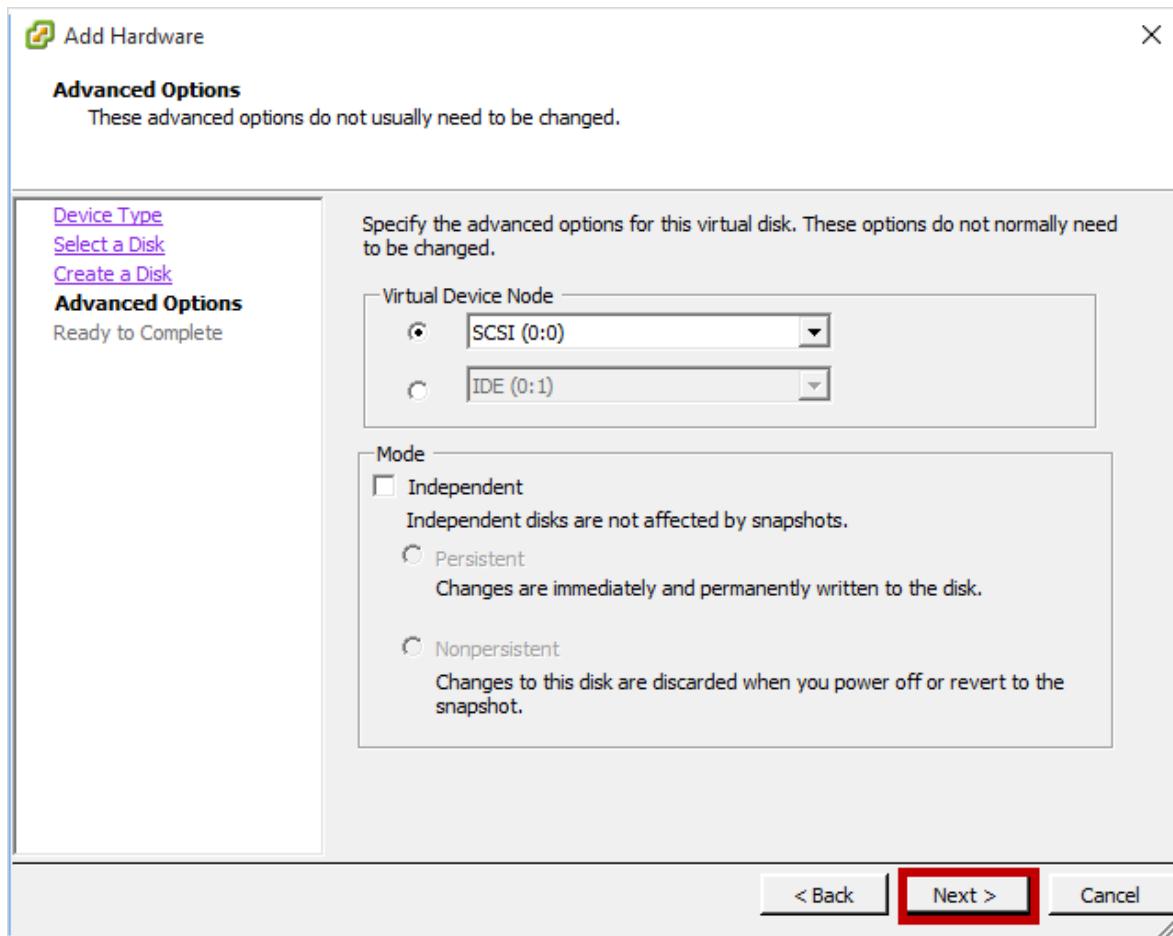
30. On the Select a Disk page, choose Create a new virtual disk. Click Next.



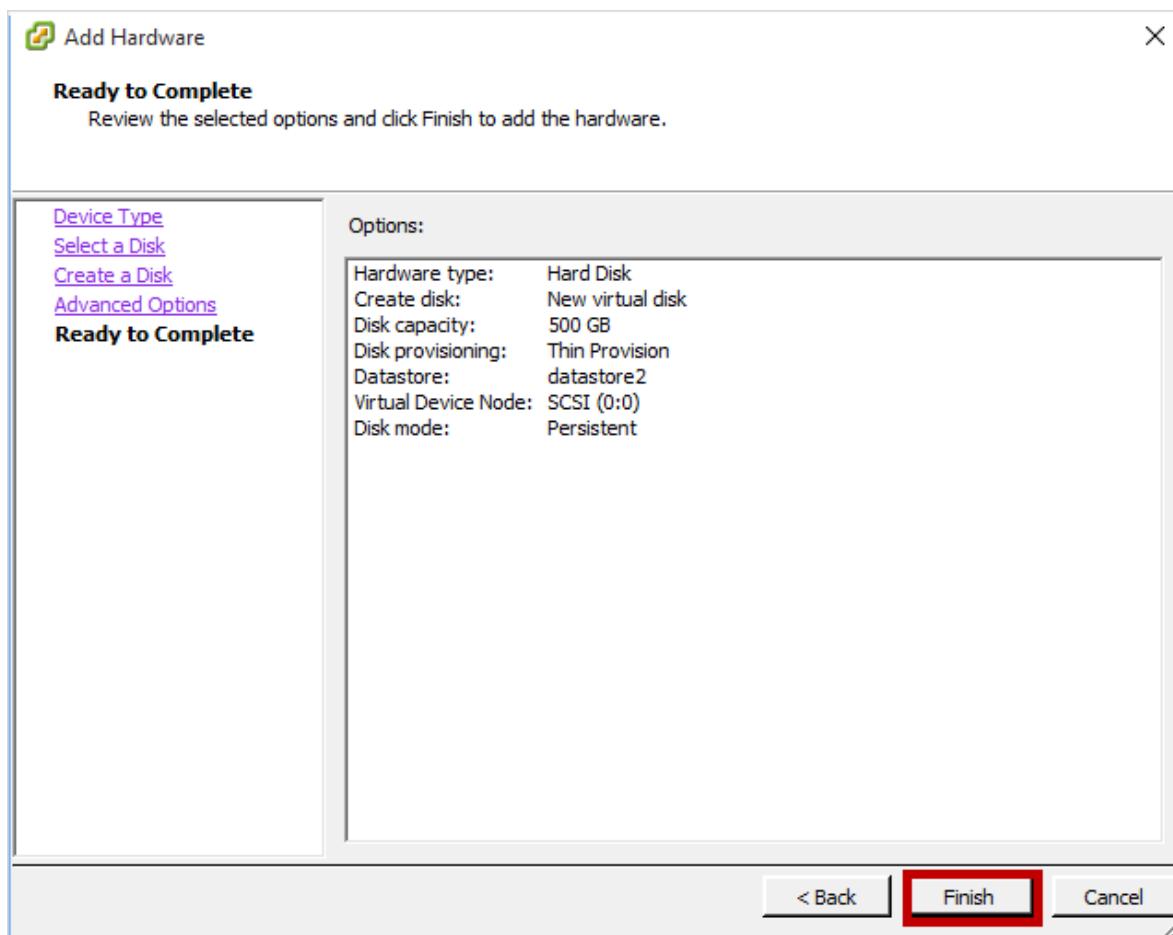
31. On the **Create a Disk** page, change the **Disk Size** to 500 GB (or more). While 500 GB is the minimum requirement, you can always provision a larger disk. Note that you cannot expand or shrink the disk once provisioned. For more information on the size of disk to provision, review the sizing section in the [best practices document](#). Under **Disk Provisioning**, select **Thin Provision**. Click **Next**.



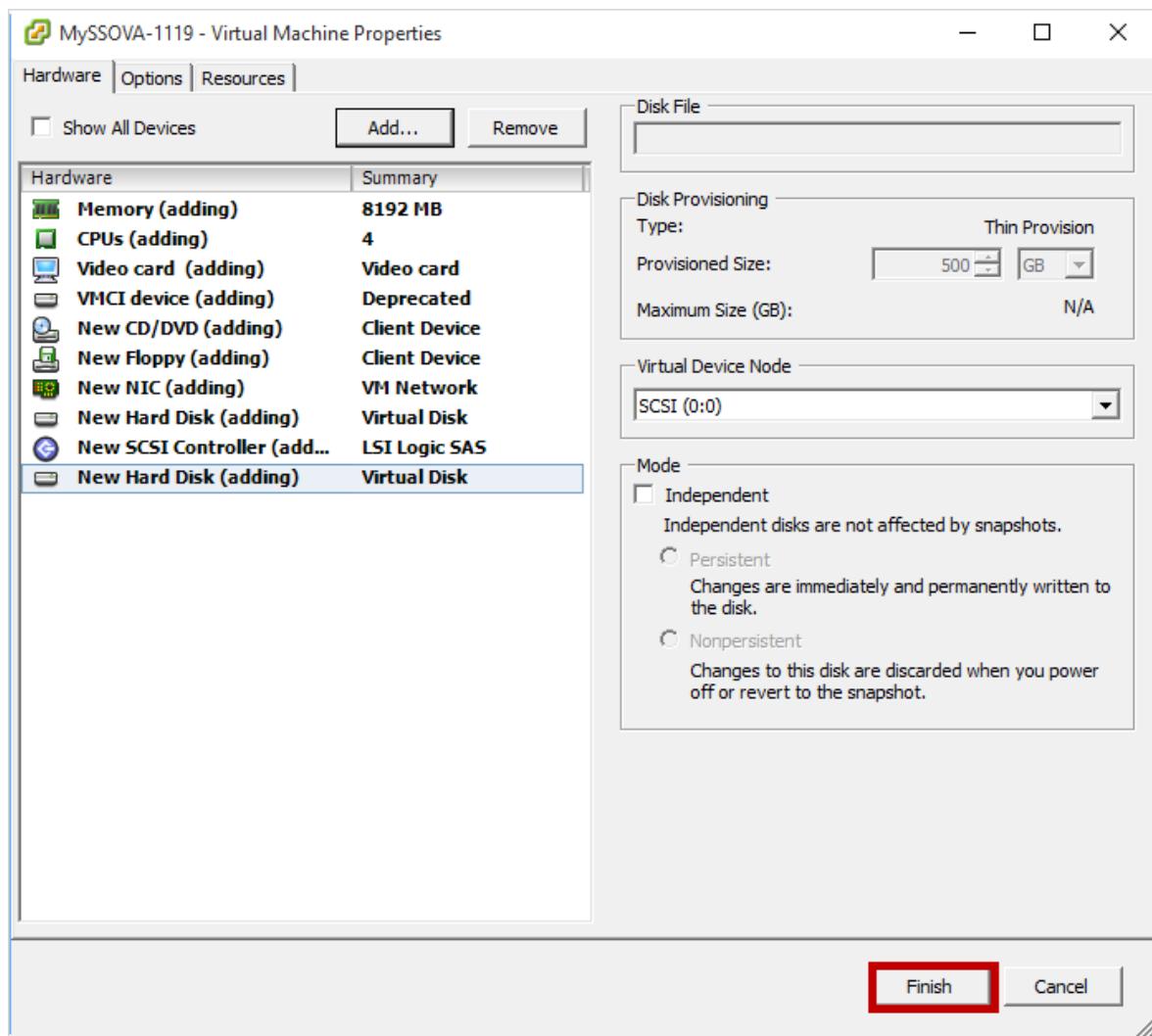
32. On the **Advanced Options** page, accept the default.



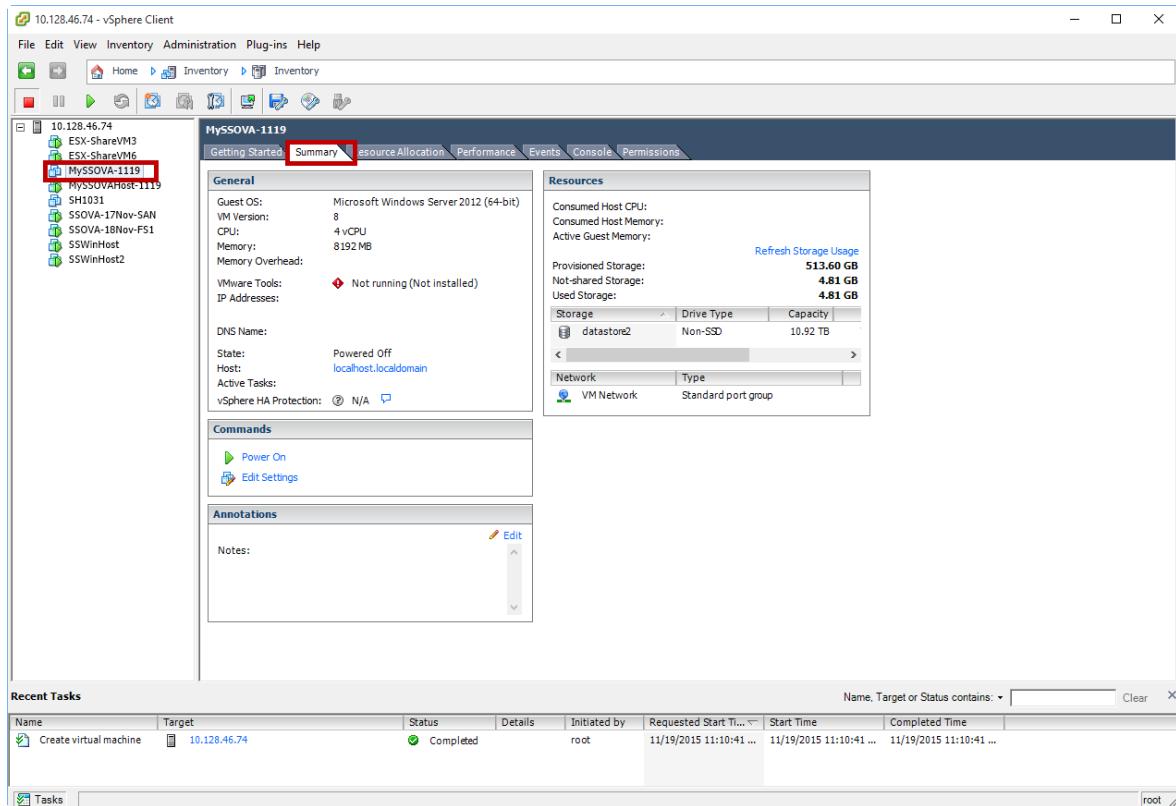
33. On the Ready to Complete page, review the disk options. Click Finish.



34. Return to the Virtual Machine Properties page. A new hard disk is added to your virtual machine. Click **Finish**.



35. With your virtual machine selected in the right pane, navigate to the **Summary** tab. Review the settings for your virtual machine.



Your virtual machine is now provisioned. The next step is to power on this machine and get the IP address.

! Note

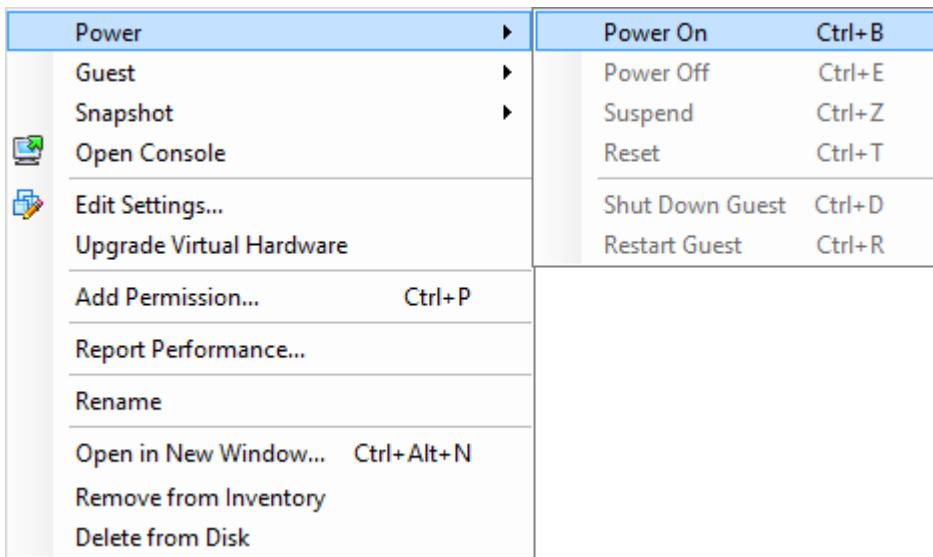
We recommend that you do not install VMware tools on your virtual array (as provisioned above). Installation of VMware tools will result in an unsupported configuration.

Step 3: Start the virtual device and get the IP

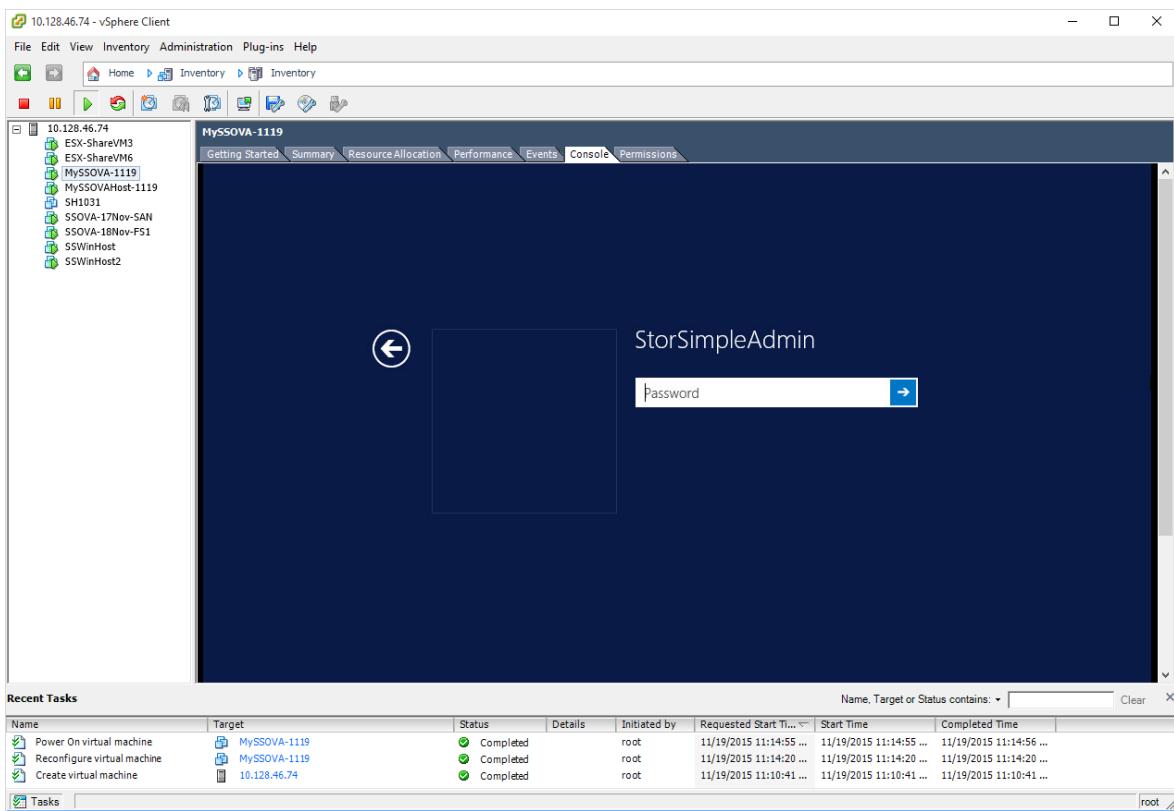
Perform the following steps to start your virtual device and connect to it.

To start the virtual device

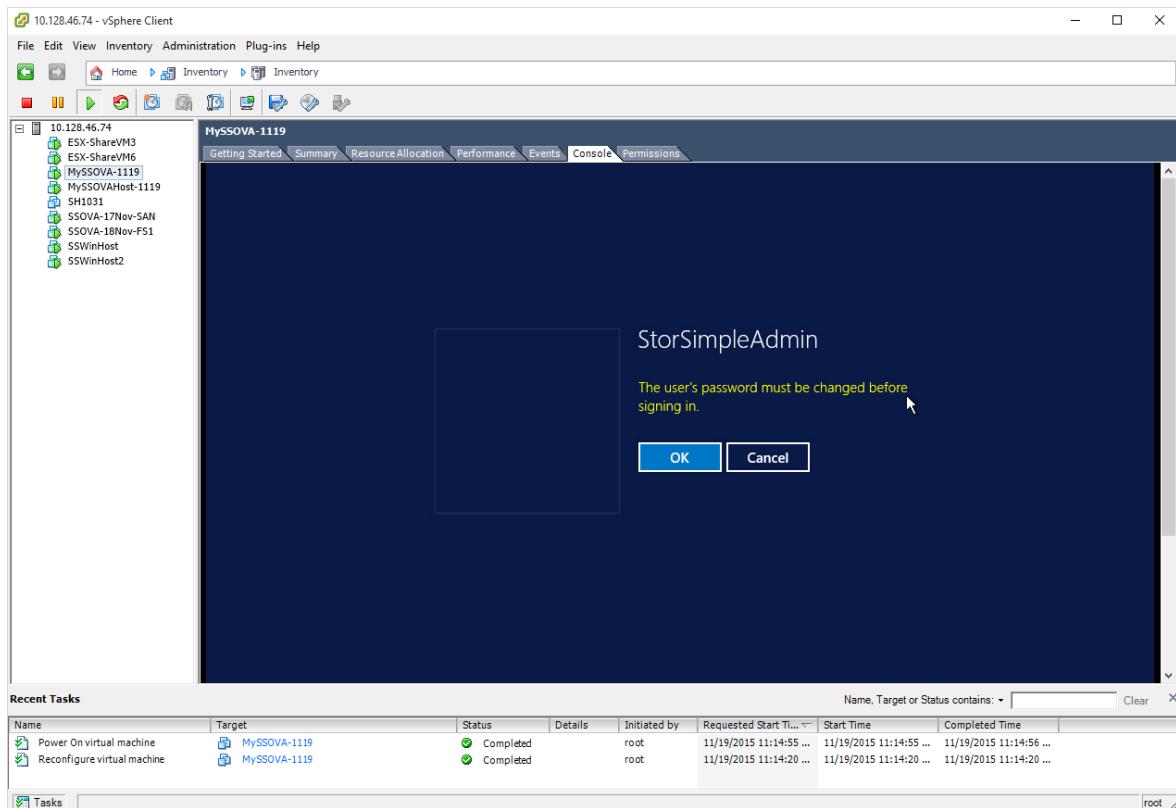
1. Start the virtual device. In the vSphere Configuration Manager, in the left pane, select your device and right-click to bring up the context menu. Select **Power** and then select **Power on**. This should power on your virtual machine. You can view the status in the bottom **Recent Tasks** pane of the vSphere client.



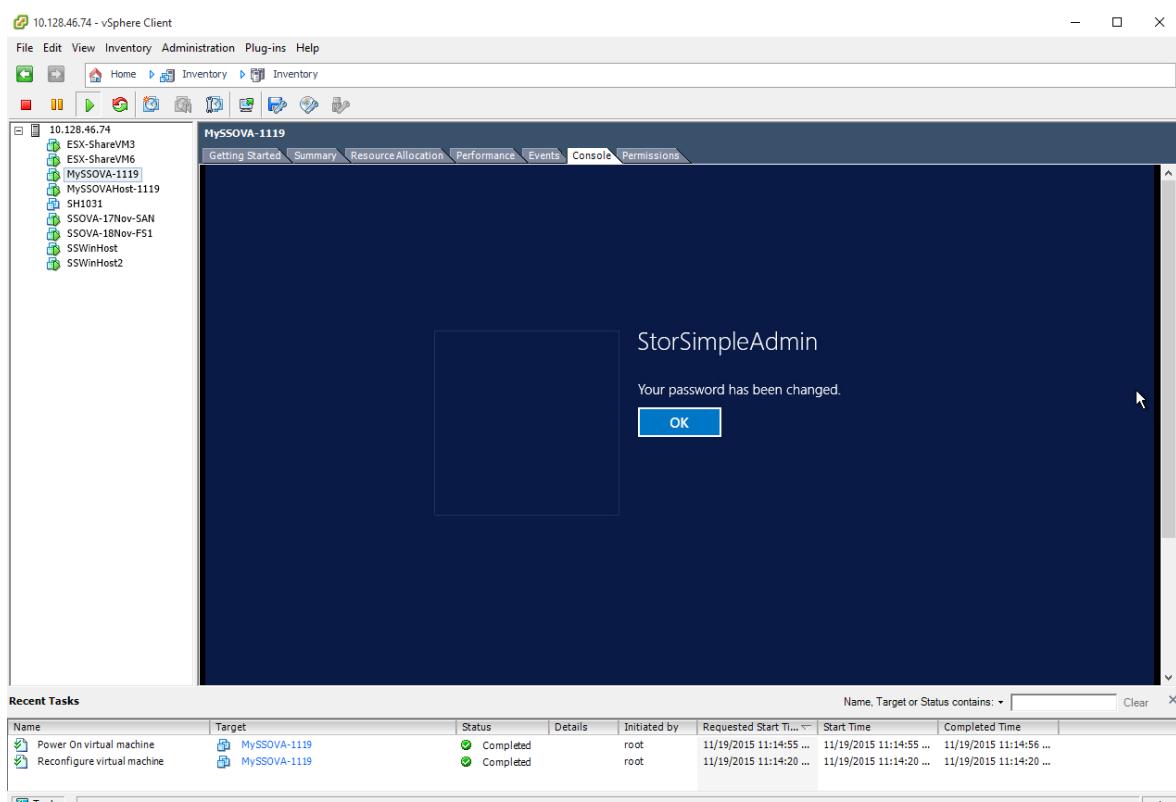
2. The setup tasks will take a few minutes to complete. Once the device is running, navigate to the **Console** tab. Send Ctrl+Alt+Delete to log in to the device. Alternatively, you can point the cursor on the console window and press Ctrl+Alt+Insert. The default user is *StorSimpleAdmin* and the default password is *Password1*.



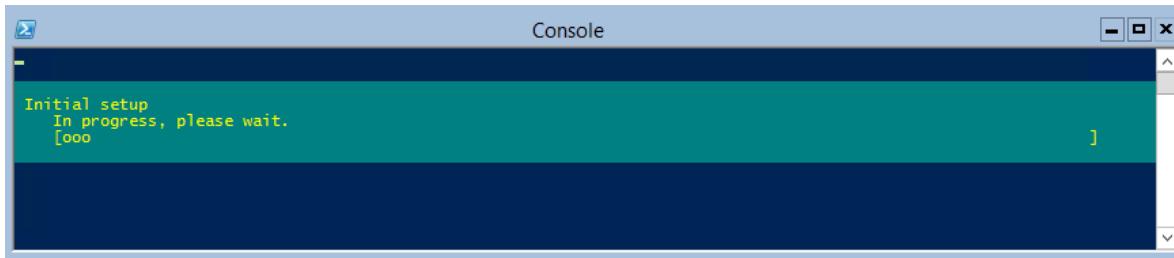
3. For security reasons, the device administrator password expires at the first logon. You are prompted to change the password.



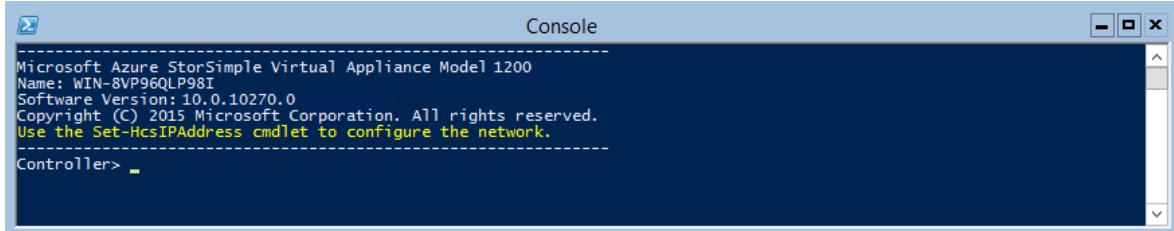
- Enter a password that contains at least 8 characters. The password must contain 3 out of 4 of these requirements: uppercase, lowercase, numeric, and special characters. Reenter the password to confirm it. You will be notified that the password has changed.



- After the password is successfully changed, the virtual device may reboot. Wait for the reboot to complete. The Windows PowerShell console of the device may be displayed along with a progress bar.

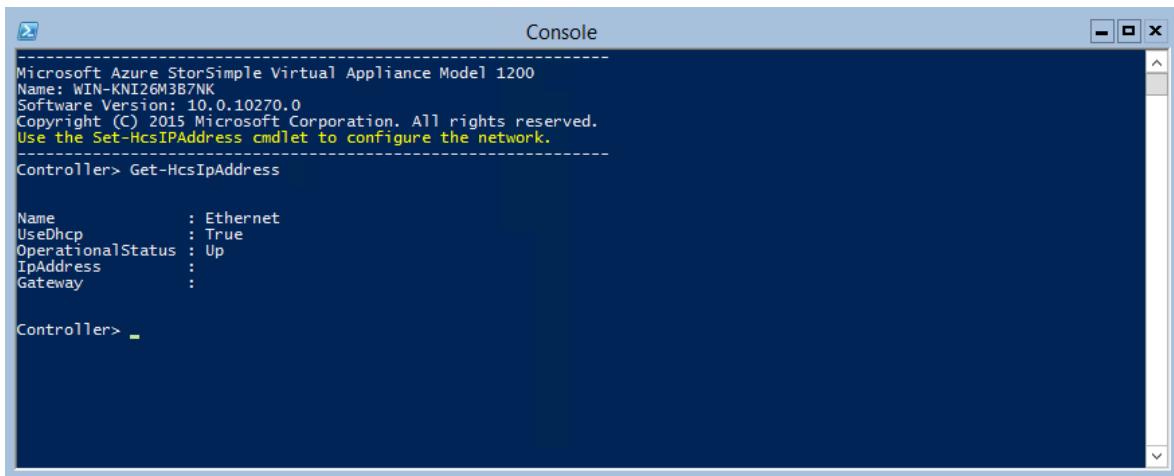


6. Steps 6-8 only apply when booting up in a non-DHCP environment. If you are in a DHCP environment, then skip these steps and go to step 9. If you booted up your device in non-DHCP environment, you will see the following screen.



Next, configure the network.

7. Use the `Get-HcsIpAddress` command to list the network interfaces enabled on your virtual device. If your device has a single network interface enabled, the default name assigned to this interface is `Ethernet`.



8. Use the `Set-HcsIpAddress` cmdlet to configure the network. An example is shown below:

```
Set-HcsIpAddress -Name Ethernet -IpAddress 10.161.22.90 -Netmask 255.255.255.0  
-Gateway 10.161.22.1
```

```
Support Console
Use the Set-HcsIpAddress cmdlet to configure the network.
Controller> Get-Help Set-HcsIpAddress
NAME
  Set-HcsIpAddress
SYNTAX
  Set-HcsIpAddress [[-Name] <string>] [[-IpAddress] <string>] [[-Netmask] <string>] [[-Gateway] <string>]
  [ <CommonParameters> ]
  Set-HcsIpAddress [[-UseDhcp]] [ <CommonParameters> ]
ALIASES
  None
REMARKS
  None

Controller> Set-HcsIpAddress -Name Ethernet -IpAddress 10.161.22.90 -Netmask 255.255.255.0 -Gateway 10.161.22.1
```

9. After the initial setup is complete and the device has booted up, you will see the device banner text. Make a note of the IP address and the URL displayed in the banner text to manage the device. You will use this IP address to connect to the web UI of your virtual device and complete the local setup and registration.

```
Console
Microsoft Azure StorSimple Virtual Appliance Model 1200
Name: WIN-HUM9TL64KPB
Software Version: 10.0.10270.0
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Use https://10.161.22.93 to manage the appliance.

Controller>
```

10. (Optional) Perform this step only if you are deploying your device in the Government Cloud. You will now enable the United States Federal Information Processing Standard (FIPS) mode on your device. The FIPS 140 standard defines cryptographic algorithms approved for use by US Federal government computer systems for the protection of sensitive data.

- a. To enable the FIPS mode, run the following cmdlet:

```
Enable-HcsFIPSMode
```

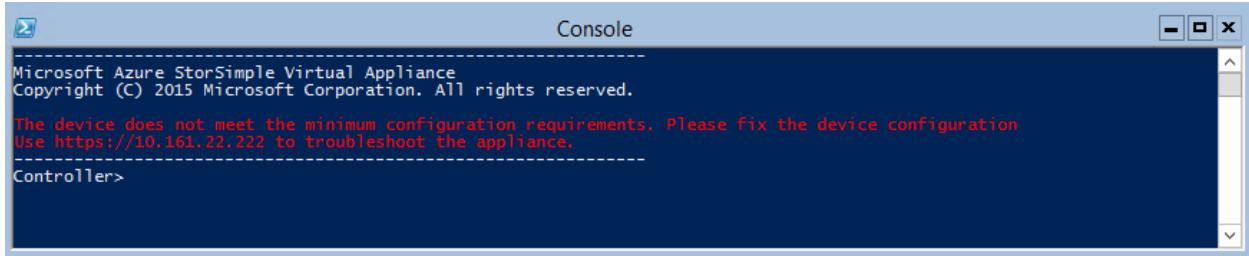
- b. Reboot your device after you have enabled the FIPS mode so that the cryptographic validations take effect.

Note

You can either enable or disable FIPS mode on your device. Alternating the device between FIPS and non-FIPS mode is not supported.

If your device does not meet the minimum configuration requirements, you will see an error in the banner text (shown below). You will need to modify the device configuration so that it has adequate resources to meet the minimum requirements. You can then

restart and connect to the device. Refer to the minimum configuration requirements in Step 1: Ensure that the host system meets minimum virtual device requirements.



The screenshot shows a Windows Command Prompt window titled "Console". The title bar also includes the text "Microsoft Azure StorSimple Virtual Appliance" and "Copyright (C) 2015 Microsoft Corporation. All rights reserved.". The main text area contains the following error message:

The device does not meet the minimum configuration requirements. Please fix the device configuration
Use <https://10.161.22.222> to troubleshoot the appliance.

Controller>

If you face any other error during the initial configuration using the local web UI, refer to the following workflows:

- Run diagnostic tests to [troubleshoot web UI setup](#).
- Generate log package and view log files.

Next steps

- Set up your StorSimple Virtual Array as a file server
- Set up your StorSimple Virtual Array as an iSCSI server

Deploy StorSimple Virtual Array - Set up as file server via Azure portal

Article • 08/19/2022 • 10 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Introduction

This article describes how to perform initial setup, register your StorSimple file server, complete the device setup, and create and connect to SMB shares. This is the last article in the series of deployment tutorials required to completely deploy your virtual array as a file server or an iSCSI server.

The setup and configuration process can take around 10 minutes to complete. The information in this article applies only to the deployment of the StorSimple Virtual Array. For the deployment of StorSimple 8000 series devices, go to: [Deploy your StorSimple 8000 series device running Update 2](#).

Setup prerequisites

Before you configure and set up your StorSimple Virtual Array, make sure that:

- You have provisioned a virtual array and connected to it as detailed in the [Provision a StorSimple Virtual Array in Hyper-V](#) or [Provision a StorSimple Virtual Array in VMware](#).
- You have the service registration key from the StorSimple Device Manager service that you created to manage StorSimple Virtual Arrays. For more information, see [Step 2: Get the service registration key for StorSimple Virtual Array](#).

- If this is the second or subsequent virtual array that you are registering with an existing StorSimple Device Manager service, you should have the service data encryption key. This key was generated when the first device was successfully registered with this service. If you have lost this key, see [Get the service data encryption key](#) for your StorSimple Virtual Array.

Step-by-step setup

Use the following step-by-step instructions to set up and configure your StorSimple Virtual Array.

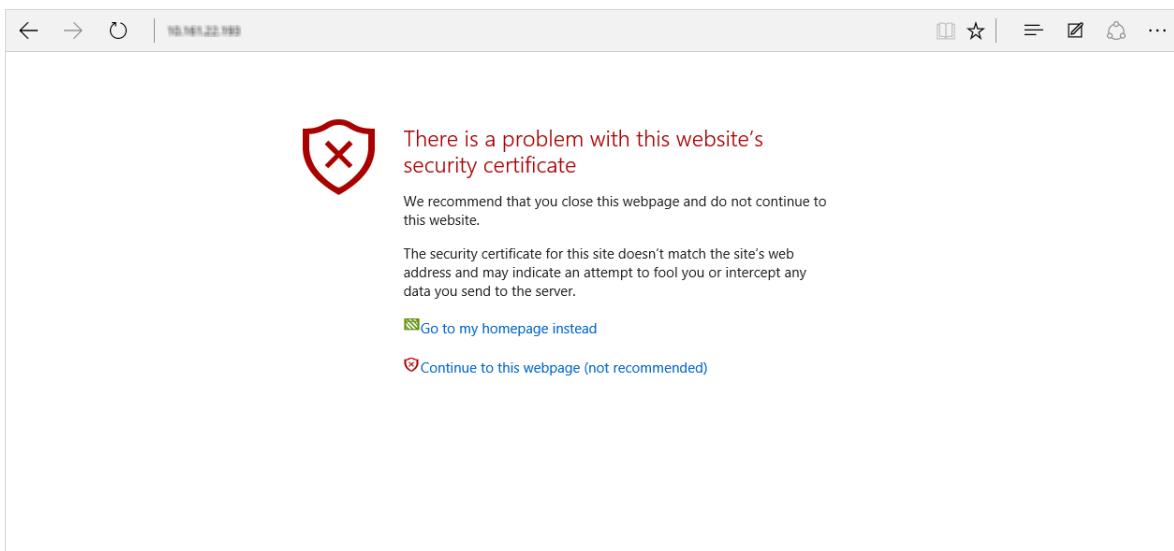
Step 1: Complete the local web UI setup and register your device

To complete the setup and register the device

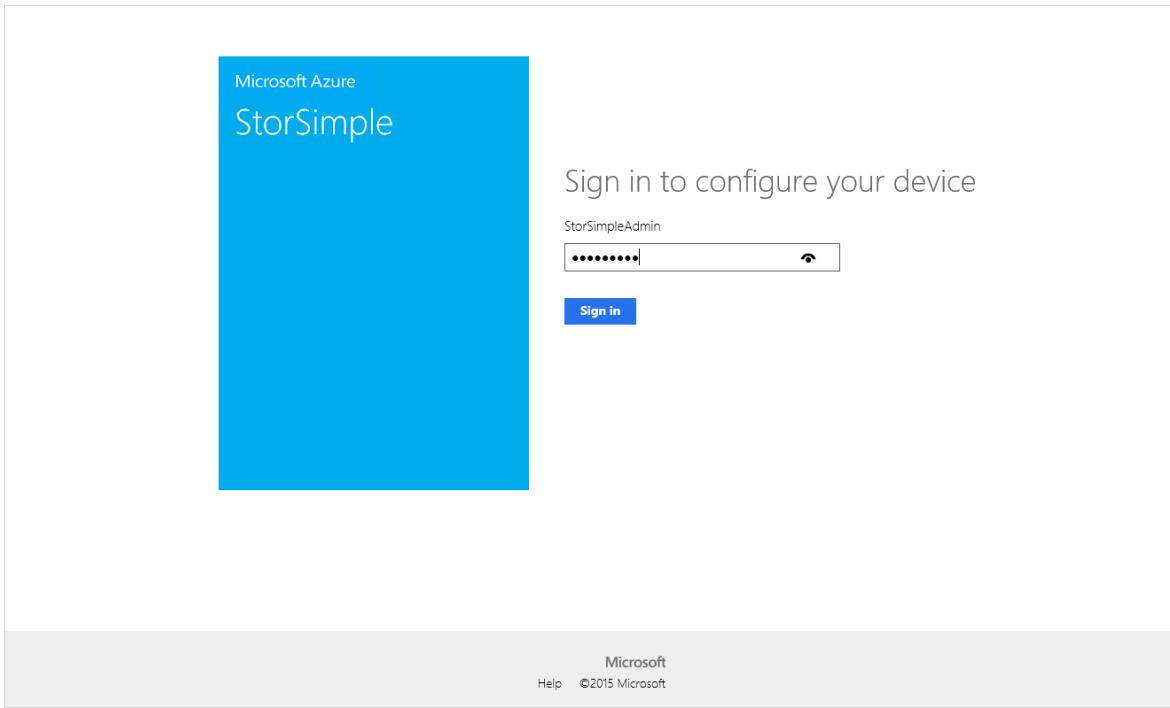
1. Open a browser window and connect to the local web UI. Type:

```
https://<ip-address of network interface>
```

Use the connection URL noted in the previous step. You see an error indicating that there is a problem with the website's security certificate. Click **Continue to this webpage**.



2. Sign in to the web UI of your virtual array as **StorSimpleAdmin**. Enter the device administrator password that you changed in Step 3: Start the virtual array in [Provision a StorSimple Virtual Array in Hyper-V](#) or in [Provision a StorSimple Virtual Array in VMware](#).



3. You are taken to the **Home** page. This page describes the various settings required to configure and register the virtual array with the StorSimple Device Manager service. The **Network settings**, **Web proxy settings**, and **Time settings** are optional. The only required settings are **Device settings** and **Cloud settings**.

4. In the **Network settings** page under **Network interfaces**, DATA 0 will be automatically configured for you. Each network interface is set by default to get IP address automatically (DHCP). Hence, an IP address, subnet, and gateway are automatically assigned (for both IPv4 and IPv6).

Configuration

[Get started](#)

Network settings

Device settings

Web proxy settings

Time settings

Cloud settings

Maintenance

Power settings

Software update

Password change

Troubleshooting

Diagnostic tests

System logs

[Contact Support](#)

Network interface: Ethernet (10 Gbps)

Get IP address automatically On Off

Name	IP address	Subnet	Gateway
IPv4	10.161.22.75	255.255.254.0	10.161.22.1
IPv6	2001:4898:4010:4012:d03c:cfc9:a68:5ace	64	

DNS servers

Name	IPv4	IPv6
Primary	10.161.48.39	
Secondary	10.161.48.40	

[Help](#) ©2015 Microsoft

If you added more than one network interface during the provisioning of the device, you can configure them here. Note you can configure your network interface as IPv4 only or as both IPv4 and IPv6. IPv6 only configurations are not supported.

5. DNS servers are required because they are used when your device attempts to communicate with your cloud storage service providers or to resolve your device by name when configured as a file server. In the **Network settings** page under the **DNS servers**:

- a. A primary and secondary DNS server are automatically configured. If you choose to configure static IP addresses, you can specify DNS servers. For high availability, we recommend that you configure a primary and a secondary DNS server.
- b. Click **Apply** to apply and validate the network settings.

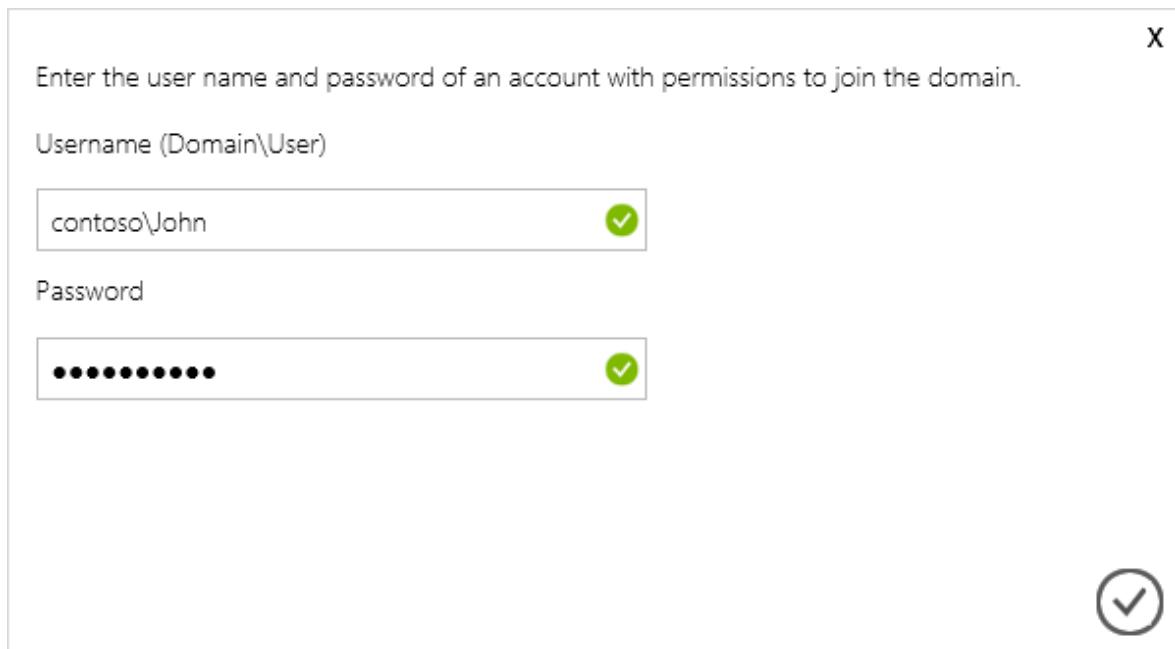
6. In the **Device settings** page:

- a. Assign a unique **Name** to your device. This name can be 1-15 characters and can contain letter, numbers and hyphens.
- b. Click the **File server** icon  for the **Type** of device that you are creating. A file server will allow you to create shared folders.
- c. As your device is a file server, you will need to join the device to a domain. Enter a **Domain name**.
- d. Click **Apply**.

7. A dialog box will appear. Enter your domain credentials in the specified format.

Click the check icon. The domain credentials are verified. You see an error message

if the credentials are incorrect.



8. Click **Apply**. This will apply and validate the device settings.

The screenshot shows the Microsoft Azure StorSimple Device configuration interface. On the left is a sidebar with navigation links: Configuration (Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Software update, Password change), and Troubleshooting (Diagnostic tests, System logs, Contact Support). The main content area is titled 'Device type' and shows two options: 'File server' (selected) and 'iSCSI server'. It includes a description for each. Below this are form fields: 'Device name' set to 'MySSOVA1121FS' with a green checkmark, 'Join domain' set to 'Yes' (selected), and 'Domain name' set to 'contoso' with a green checkmark. At the bottom of the page, a message says 'Successfully applied the settings.' and there is a large green circular 'Apply' button. The top right corner shows 'StorSimple 1200 Device' and 'Sign out'.

ⓘ Note

Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it or inherited. Group policy may install applications such as anti-virus software on the

StorSimple Virtual Array. Installing additional software is not supported and could lead to data corruption.

9. (Optionally) configure your web proxy server. Although web proxy configuration is optional, be aware that if you use a web proxy, you can only configure it here.

The screenshot shows the Microsoft Azure StorSimple 1200 Device configuration interface. The left sidebar has a blue header 'Configuration' and lists various settings like Get started, Network settings, Device settings, Web proxy settings (which is selected), Time settings, Cloud settings, Maintenance, Power settings, Software update, Password change, Troubleshooting, Diagnostic tests, System logs, and Contact Support. The main panel for 'Web proxy settings' contains fields for 'Enable web proxy' (set to 'On'), 'Web proxy URL' (empty), 'Authentication' (set to 'None'), 'Username' (empty), and 'Password' (empty). At the bottom right are 'Apply' and 'Cancel' buttons, and the footer includes 'Help', '©2015 Microsoft', and links to 'Privacy' and 'Terms of Use'.

In the **Web proxy** page:

- a. Supply the **Web proxy URL** in this format: *http://<host-IP address or FQDN>:Port number*. Note that HTTPS URLs are not supported.
- b. Specify **Authentication** as **Basic** or **None**.
- c. If using authentication, you will also need to provide a **Username** and **Password**.
- d. Click **Apply**. This will validate and apply the configured web proxy settings.

10. (Optionally) configure the time settings for your device, such as time zone and the primary and secondary NTP servers. NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

Microsoft Azure

StorSimple 1200 Device Sign out

Configuration

Get started

Network settings

Device settings

Web proxy settings

Time settings

Cloud settings

Maintenance

Power settings

Software update

Password change

Troubleshooting

Diagnostic tests

System logs

Contact Support

Time zone (UTC-08:00) Pacific Time (US & Canada)

Primary NTP server time.windows.com ✓

Secondary NTP server

Apply

Help ©2015 Microsoft

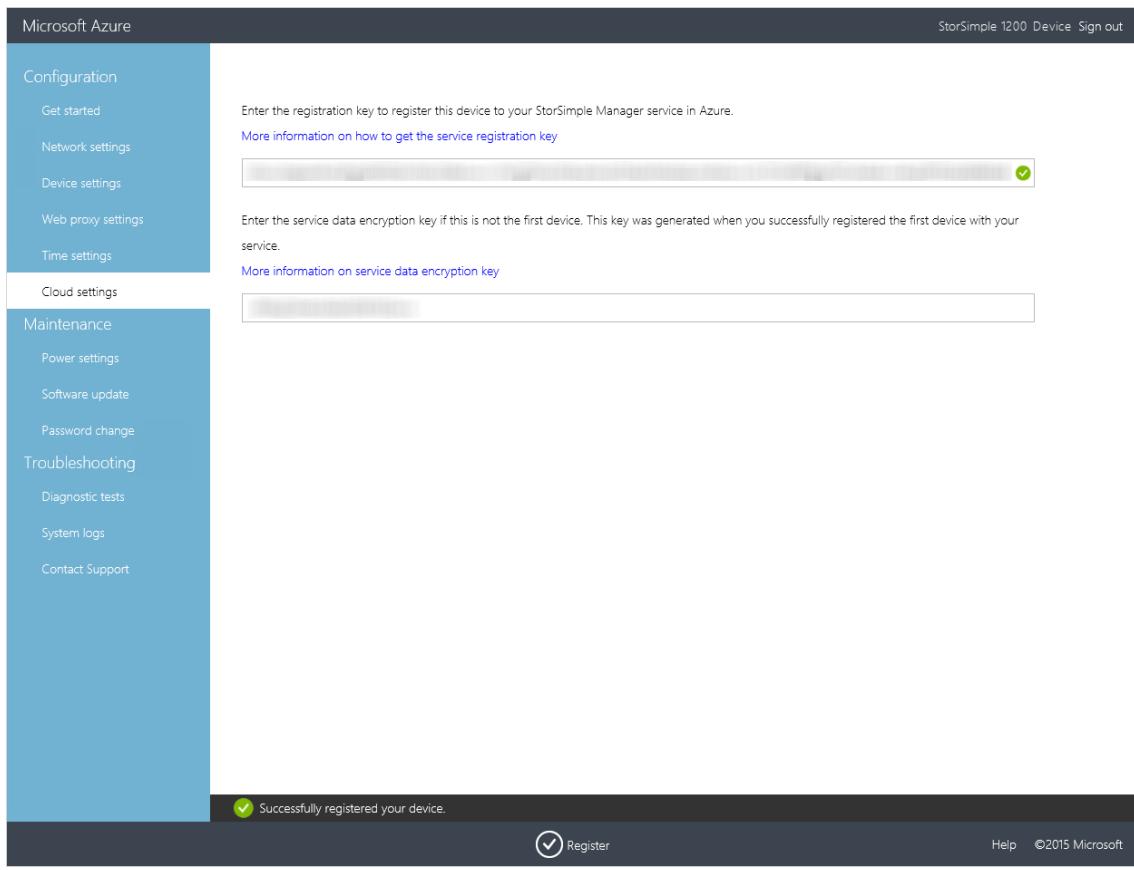
In the **Time settings** page:

- a. From the dropdown list, select the **Time zone** based on the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. Specify a **Primary NTP server** for your device or accept the default value of time.windows.com. Ensure that your network allows NTP traffic to pass from your datacenter to the Internet.
 - c. Optionally specify a **Secondary NTP server** for your device.
 - d. Click **Apply**. This will validate and apply the configured time settings.
11. Configure the cloud settings for your device. In this step, you will complete the local device configuration and then register the device with your StorSimple Device Manager service.

- a. Enter the **Service registration key** that you got in [Step 2: Get the service registration key](#) for StorSimple Virtual Array.
- b. If this is your first device registering with this service, you will be presented with the **Service data encryption key**. Copy this key and save it in a safe location. This key is required with the service registration key to register additional devices with the StorSimple Device Manager service.

If this is not the first device that you are registering with this service, you will need to provide the service data encryption key. For more information, refer to get the [service data encryption key](#) on your local web UI.

c. Click **Register**. This will restart the device. You may need to wait for 2-3 minutes before the device is successfully registered. After the device has restarted, you will be taken to the sign in page.



12. Return to the Azure portal. Go to **All resources**, search for your StorSimple Device Manager service.

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
MySS	Cloud service (classic)	MySS	Central US	MSDNonDallas
MySS	Virtual machine (classic)	MySS	Central US	MSDNonDallas
myssonestorage	Storage account (classic)	Default-Storage-NorthCentralUS	North Central US	MSDNonDallas
myssonestorage2	Storage account (classic)	Default-Storage-NorthCentralUS	North Central US	MSDNonDallas
myssonestorage3	Storage account (classic)	Default-Storage-WestUS	West US	MSDNonDallas
myssonestoreact	Storage account	MySSRG	Southeast Asia	Internal Consumption
MySVADevManager	StorSimple Device Manager	MySSRG	Southeast Asia	Internal Consumption

13. In the filtered list, select your StorSimple Device Manager service and then navigate to **Management > Devices**. In the **Devices** blade, verify that the device has successfully connected to the service and has the status **Ready to set up**.

The screenshot shows the Azure portal interface. On the left, the 'All resources' blade is open, displaying a list of subscriptions under 'MySS'. One item, 'MySSDevManager', is highlighted with a red box. In the center, the 'MySSDevManager - Devices' blade is displayed. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick-start), Management (Devices, Volumes, Shares, Keys, Backup catalog), and Monitoring (Capacity, Usage, Jobs). The main content area shows a table titled 'All statuses' with one row: 'MVSSFS1014' (Status: Ready to set up, Capacity: 385.47 GB/3.76 TB, Type: Virtual-NAS, Model: 1200). A red box highlights this row.

Step 2: Configure the device as file server

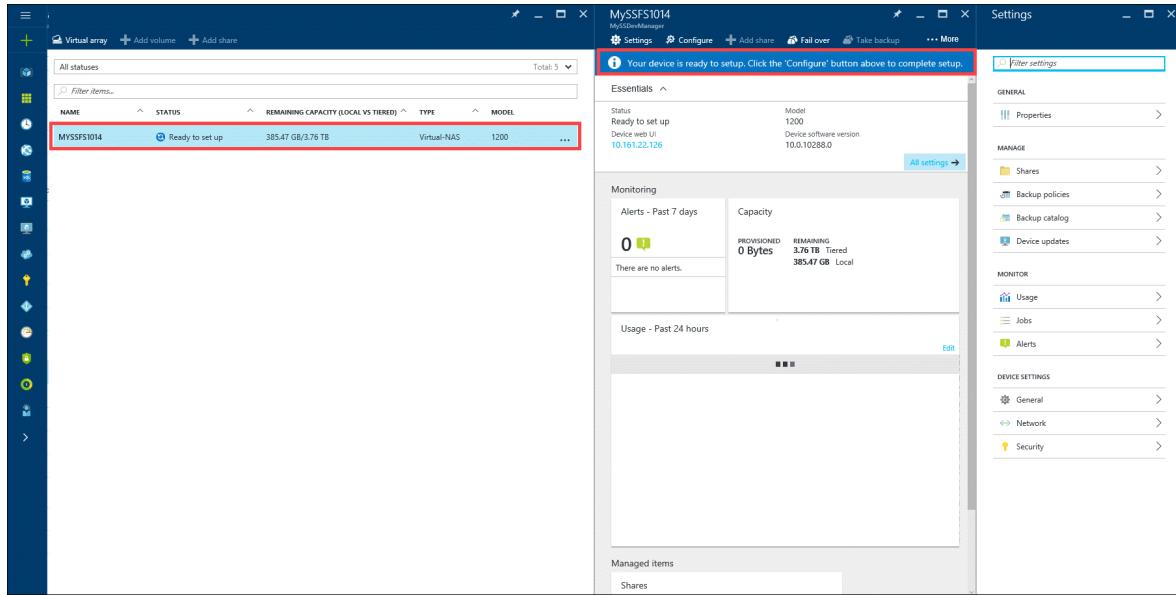
Perform the following steps in the [Azure portal](#) to complete the required device setup.

To configure the device as file server

1. Go to your StorSimple Device Manager service and then go to **Management > Devices**. In the **Devices** blade, select the device you just created. This device would show up as **Ready to set up**.

This screenshot is identical to the one above, showing the Azure portal with the 'All resources' blade open and the 'MySSDevManager - Devices' blade selected. The 'Devices' link in the left sidebar is highlighted with a red box. The main content area shows the same table with the device 'MVSSFS1014' highlighted by a red box.

2. Click the device and you will see a banner message indicating that the device is ready to setup.



3. Click **Configure** on the command bar. This opens up the **Configure** blade. In the **Configure** blade, do the following:

- The file server name is automatically populated.
- Make sure the cloud storage encryption is set to **Enabled**. This will encrypt all the data that is sent to the cloud.
- A 256-bit AES key is used with the user-defined key for encryption. Specify a 32 character key and then reenter the key to confirm it. Record the key in a key management app for future reference.
- Click **Configure required settings** to specify storage account credentials to be used with your device. Click **Add new** if there are no storage account credentials configured. Ensure that the storage account you use supports block blobs. **Page blobs are not supported.** More information about [blocks blobs and page blobs](#).

The screenshot shows two adjacent windows side-by-side.

Left Window (Configure):

- Header:** Configure - MySSFS1014
- Information Panel:** Complete the configuration of a file server on this device to create shares.
- Server Name:** MYSSFS1014
- Domain Name:** northamerica.corp.microsoft.com
- Cloud Storage Encryption:** Enabled (selected)
- Encryption Key:** A masked input field containing a long string of characters, ending with a green checkmark.
- Confirm Encryption Key:** A masked input field containing the same long string of characters, ending with a green checkmark.
- Storage Account Credential:** A blue button labeled "Configure required settings" with a right-pointing arrow.
- Bottom:** A blue "Configure" button.

Right Window (Storage account cred...):

- Information Panel:** There are no storage account credentials. Add a new storage account credential.
- Add New Button:** A blue button with a white plus sign and the text "Add new", which is highlighted with a red rectangular border.

4. In the **Add a storage account credentials** blade, do the following:

- Choose current subscription if the storage account is in the same subscription as the service. Specify other if the storage account is outside of the service subscription.
- From the dropdown list, choose an existing storage account.

- c. The location will be automatically populated based on the specified storage account.
- d. Enable TLS to ensure a secure network communication channel between the device and the cloud.
- e. Click **Add** to add this storage account credential.

The image shows three windows side-by-side:

- Configure** window (left): Shows a message to complete the configuration of a file server on the device. It includes fields for Server name (MSSFS1014), Domain name (northamerica.corp.microsoft.com), Cloud storage encryption (Enabled), and an Encryption key field. A "Storage account credential" section is highlighted in blue, containing a "Configure required settings" link.
- Storage account cred...** window (middle): Shows a message that there are no storage account credentials. It has a prominent "Add new" button.
- Add a storage account...** window (right): Shows configuration options for a new storage account. It includes a Subscription dropdown (Current selected), a Storage account dropdown (mystorsimstoragacct selected), a Location dropdown (West US selected), and an Enable SSL toggle (ENABLE selected). A red box highlights the "ADD" button at the bottom right.

- 5. Once the storage account credential is successfully created, the **Configure** blade will be updated to display the specified storage account credentials. Click **Configure**.

The screenshot shows two windows side-by-side. On the left is the main configuration page for 'MySSFS1014' with a 'Configure' button highlighted. On the right is a detailed 'Configure' dialog box for the same device.

Main Configuration Window:

- Status:** Ready to set up
- Device web UI:** 10.161.22.126
- Model:** 1200
- Device software version:** 10.0.10288.0

Monitoring:

- Alerts - Past 7 days:** 0 (No alerts)
- Capacity:** PROVISIONED 0 Bytes, REMAINING 3.76 TB Tiered, 385.47 GB Local
- Usage - Past 24 hours:** Primary Storage Used, Cloud Storage Used, Local Storage Used (all measured in Bytes).

Managed items: Shares

Configure Dialog Box:

- Server name:** MYSSFS1014
- Domain name:** northamerica.corp.microsoft.com
- Cloud storage encryption:** Enabled (radio button selected)
- Encryption key:** mystorsimstoragacct (highlighted with a red box)
- Confirm encryption key:** mystorsimstoragacct
- Storage account credential:** mystorsimstoragacct (highlighted with a red box)

Configure button (highlighted with a red box) is located at the bottom right of the dialog box.

You will see a that a file server is being created. Once the file server is successfully created, you will be notified.

✓ Configuring device 'MYSSFS1014' with t... 11:43 AM
Successfully completed the operation.

The device status will also change to **Online**.

You can proceed to add a share.

Step 3: Add a share

Perform the following steps in the [Azure portal](#) to create a share.

To create a share

1. Select the file server device you configured in the preceding step and click ... (or right-click). In the context menu, select **Add share**. Alternatively, you can click **+ Add Share** on the device command bar.

2. Specify the following share settings:

- a. A unique name for your share. The name must be a string that contains 3 to 127 characters.
- b. An optional **Description** for the share. The description will help identify the share owners.
- c. A **Type** for the share. The type can be **Tiered** or **Locally pinned**, with tiered being the default. For workloads that require local guarantees, low latencies, and higher performance, select a **Locally pinned** share. For all other data, select a **Tiered** share. A locally pinned share is thickly provisioned and ensures that the primary data on the share stays local to the device and does not spill to the cloud. A tiered share on the other hand is thinly provisioned. When you create a tiered share, 10% of the space is provisioned on the local tier and 90% of the space is provisioned in the cloud. For instance, if you provisioned a 1 TB volume, 100 GB would reside in the local space and 900 GB would be used in the cloud when the data tiers. This in turn implies that if you run out of all the local space on the device, you cannot provision a tiered share.
- d. In the **Set default full permissions to** field, assign the permissions to the user, or the group that is accessing this share. Specify the name of the user or the user group in *john@contoso.com* format. We recommend that you use a user group (instead of a single user) to allow admin privileges to access these shares. After you have assigned the permissions here, you can then use File Explorer to modify these permissions.
- e. Click **Add** to create the share.

Add share

* Share name
MySSEngg ✓

Description
For Engineering Docs ✓

* Type
Tiered

 Available total capacity : 3.76 TB.
Available local capacity : 385.47 GB.
For a tiered share, 10% of the provisioned share size is reserved locally on the device.

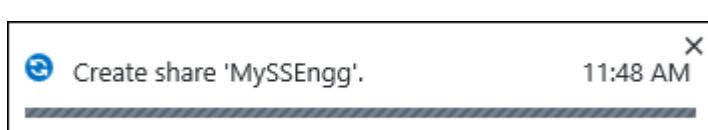
* Capacity
GB
1000 ✓

* Set default full permission to
john@contoso.com ✓

 Backup is automatically enabled on this share. You can modify the start time of the backups from the Backup policy blade under Device settings.

Create

You are notified that the share creation is in progress.



After the share is created with the specified settings, the **Shares** blade will update to reflect the new share. By default, monitoring and backup are enabled for the share.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and contains a navigation menu with sections like GENERAL, MANAGE, MONITOR, and DEVICE SETTINGS. The 'Shares' item under the MANAGE section is highlighted with a red box. The right window is titled 'Shares' and shows a list of shares for the device 'MySSFS1014 (Online)'. The table has columns for NAME, STATUS, TYPE, and CAPACITY. A single share named 'MySEnGg' is listed, with its row also highlighted by a red box. The status is 'Online', type is 'Tiered', and capacity is '0 Bytes/1000...'. There is a '...' button next to the row.

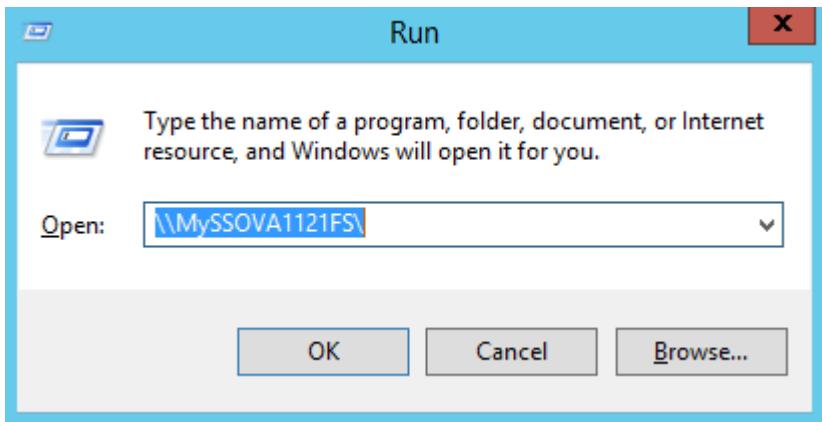
NAME	STATUS	TYPE	CAPACITY
MYSSFS1014 (1)			
MySEnGg	Online	Tiered	0 Bytes/1000...

Step 4: Connect to the share

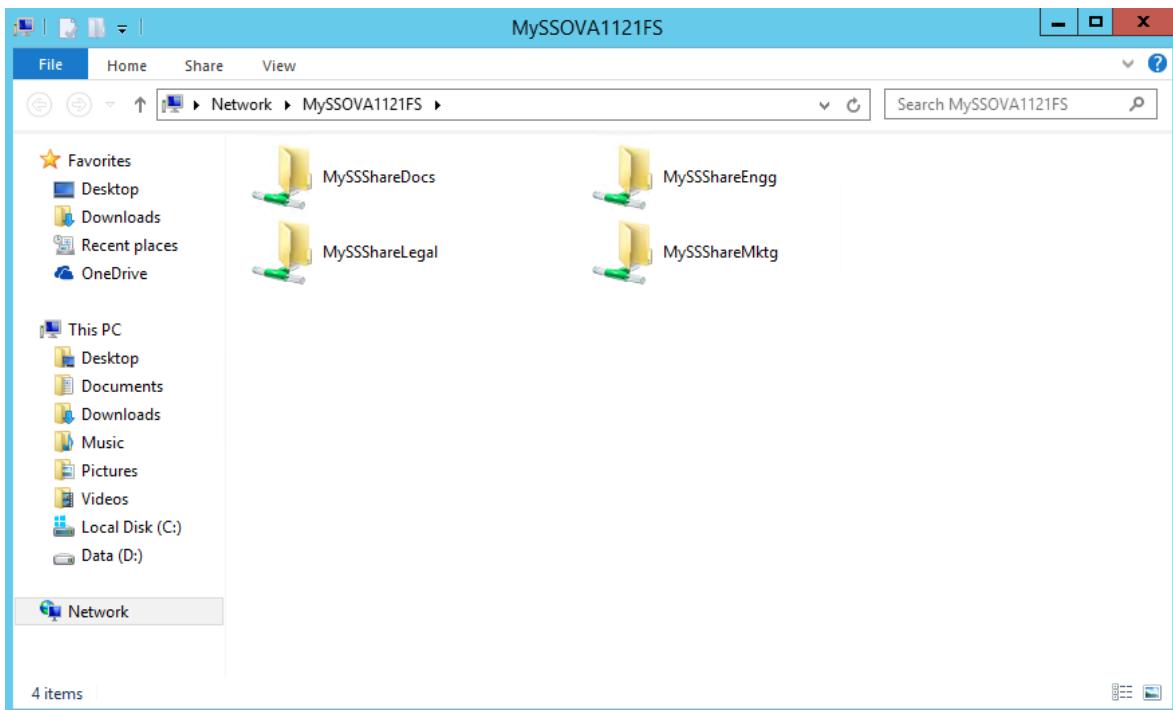
You will now need to connect to one or more shares that you created in the previous step. Perform these steps on your Windows Server host connected to your StorSimple Virtual Array.

To connect to the share

1. Press **Windows** + R. In the Run window, specify the `\|<file server name>` as the path, replacing *file server name* with the device name that you assigned to your file server. Click **OK**.



2. This opens up File Explorer. You should now be able to see the shares that you created as folders. Select and double-click a share (folder) to view the content.



3. You can now add files to these shares and take a backup.

Next steps

Learn how to use the local web UI to [administer your StorSimple Virtual Array](#).

Deploy StorSimple Virtual Array – Set up as an iSCSI server via Azure portal

Article • 08/19/2022 • 11 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Overview

This deployment tutorial applies to the Microsoft Azure StorSimple Virtual Array. This tutorial describes how to perform the initial setup, register your StorSimple iSCSI server, complete the device setup, and then create, mount, initialize, and format volumes on your StorSimple Virtual Array configured as an iSCSI server.

The procedures described here take approximately 30 minutes to 1 hour to complete. The information published in this article applies to StorSimple Virtual Arrays only.

Setup prerequisites

Before you configure and set up your StorSimple Virtual Array, make sure that:

- You have provisioned a virtual array and connected to it as described in [Deploy StorSimple Virtual Array - Provision a virtual array in Hyper-V](#) or [Deploy StorSimple Virtual Array - Provision a virtual array in VMware](#).
- You have the service registration key from the StorSimple Device Manager service that you created to manage your StorSimple Virtual Arrays. For more information, see [Step 2: Get the service registration key](#) in [Deploy StorSimple Virtual Array - Prepare the portal](#).

- If this is the second or subsequent virtual array that you are registering with an existing StorSimple Device Manager service, you should have the service data encryption key. This key was generated when the first device was successfully registered with this service. If you have lost this key, see **Get the service data encryption key** in [Use the Web UI to administer your StorSimple Virtual Array](#).

Step-by-step setup

Use the following step-by-step instructions to set up and configure your StorSimple Virtual Array:

- [Step 1: Complete the local web UI setup and register your device](#)
- Step 2: Complete the required device setup
- [Step 3: Add a volume](#)
- [Step 4: Mount, initialize, and format a volume](#)

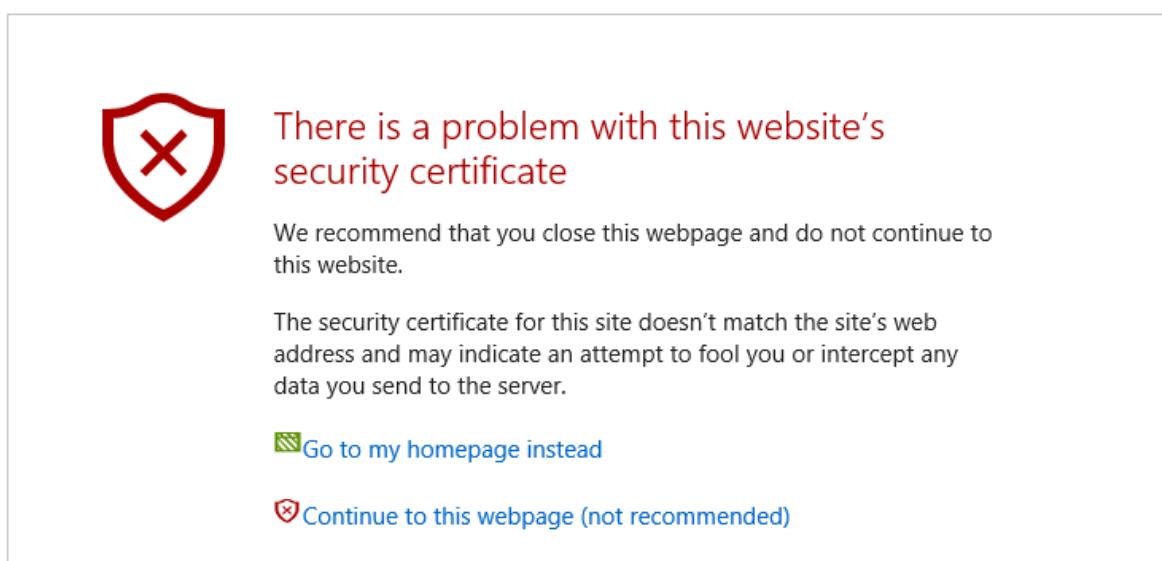
Step 1: Complete the local web UI setup and register your device

To complete the setup and register the device

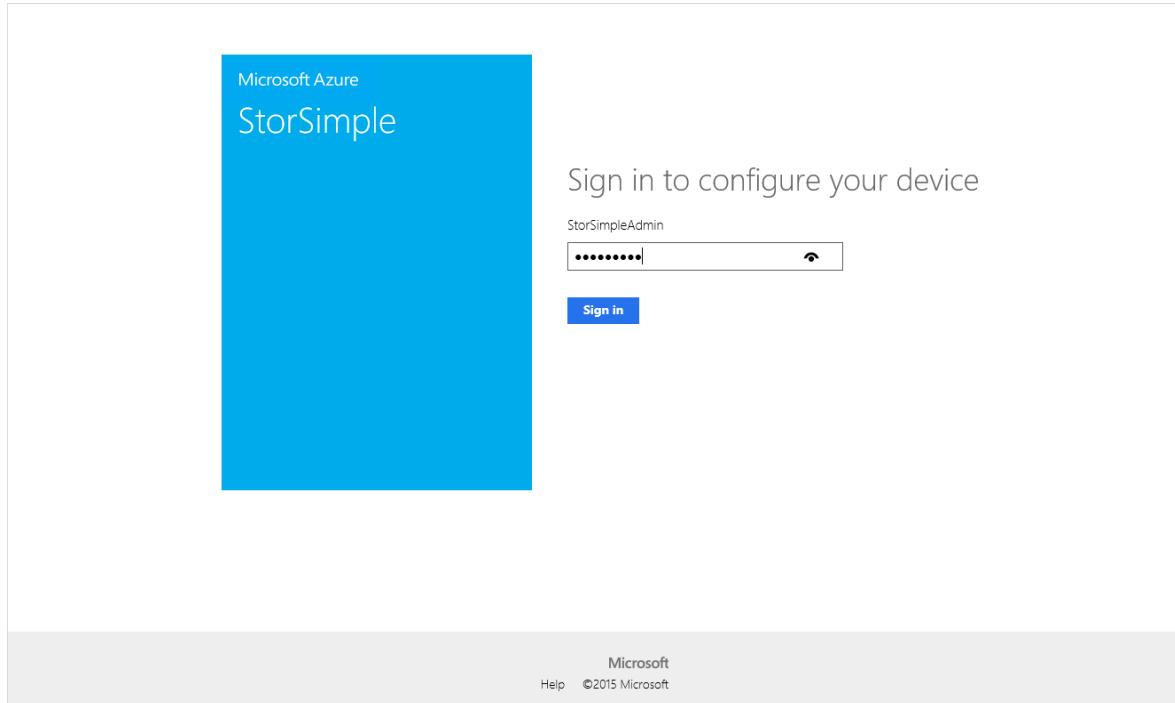
1. Open a browser window. To connect to the web UI type:

```
https://<ip-address of network interface>
```

Use the connection URL noted in the previous step. You will see an error notifying you that there is a problem with the website's security certificate. Click **Continue to this web page**.



2. Sign in to the web UI of your virtual device as **StorSimpleAdmin**. Enter the device administrator password that you changed in Step 3: Start the virtual device in [Deploy StorSimple Virtual Array - Provision a virtual device in Hyper-V](#) or [Deploy StorSimple Virtual Array - Provision a virtual device in VMware](#).



3. You will be taken to the **Home** page. This page describes the various settings required to configure and register the virtual device with the StorSimple Device Manager service. Note that the **Network settings**, **Web proxy settings**, and **Time settings** are optional. The only required settings are **Device settings** and **Cloud settings**.

A screenshot of the Microsoft Azure StorSimple Home page. The left sidebar lists navigation options: Configuration (Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Software update, Password change), Troubleshooting (Diagnostic tests, System logs, Contact Support). The main content area shows a blue icon of a server rack and the text "Your device is not configured. Here are the next steps to get you started." Below this, five numbered steps are listed: 1. Network settings (optional) - "Verify default network settings or configure static IP addresses and DNS." (links to Network settings and Learn more). 2. Device settings - "Configure the device as a file server or an iSCSI server and join a domain." (links to Device settings and Learn more). 3. Web proxy settings (optional) - "Configure these settings if you are using a web proxy server to connect to the Internet." (links to Web proxy settings and Learn more). 4. Time settings (optional) - "Configure device time zone and NTP servers." (links to Time settings and Learn more). 5. Cloud settings - "Register the device with StorSimple Manager service." (links to Cloud settings and Learn more). The bottom right corner of the page includes "Help ©2015 Microsoft".

4. On the **Network settings** page under **Network interfaces**, DATA 0 will be automatically configured for you. Each network interface is set by default to get an IP address automatically (DHCP). Therefore, an IP address, subnet, and gateway will be automatically assigned (for both IPv4 and IPv6).

As you plan to deploy your device as an iSCSI server (to provision block storage), we recommend that you disable the **Get IP address automatically** option and configure static IP addresses.

Microsoft Azure

StorSimple 1200 Device Sign out

Configuration

Get started

Network settings

Device settings

Web proxy settings

Time settings

Cloud settings

Maintenance

Power settings

Software update

Password change

Troubleshooting

Diagnostic tests

System logs

Contact Support

Network interface: Ethernet (10 Gbps)

Get IP address automatically On Off

Name	IP address	Subnet	Gateway
IPv4	10.161.22.75	255.255.254.0	10.161.22.1
IPv6	2001:4898:4010:4012:d03c:cbc9:a68:5ace	64	

DNS servers

Name	IPv4	IPv6
Primary	10.161.48.39	
Secondary	10.161.48.40	

Apply Help ©2015 Microsoft

If you added more than one network interface during the provisioning of the device, you can configure them here. Note you can configure your network interface as IPv4 only or as both IPv4 and IPv6. IPv6 only configurations are not supported.

5. DNS servers are required because they are used when your device attempts to communicate with your cloud storage service providers or to resolve your device by name if it is configured as a file server. On the **Network settings** page under the **DNS servers**:

- a. A primary and secondary DNS server will be automatically configured. If you choose to configure static IP addresses, you can specify DNS servers. For high availability, we recommend that you configure a primary and a secondary DNS server.
- b. Click **Apply**. This will apply and validate the network settings.

6. On the **Device settings** page:

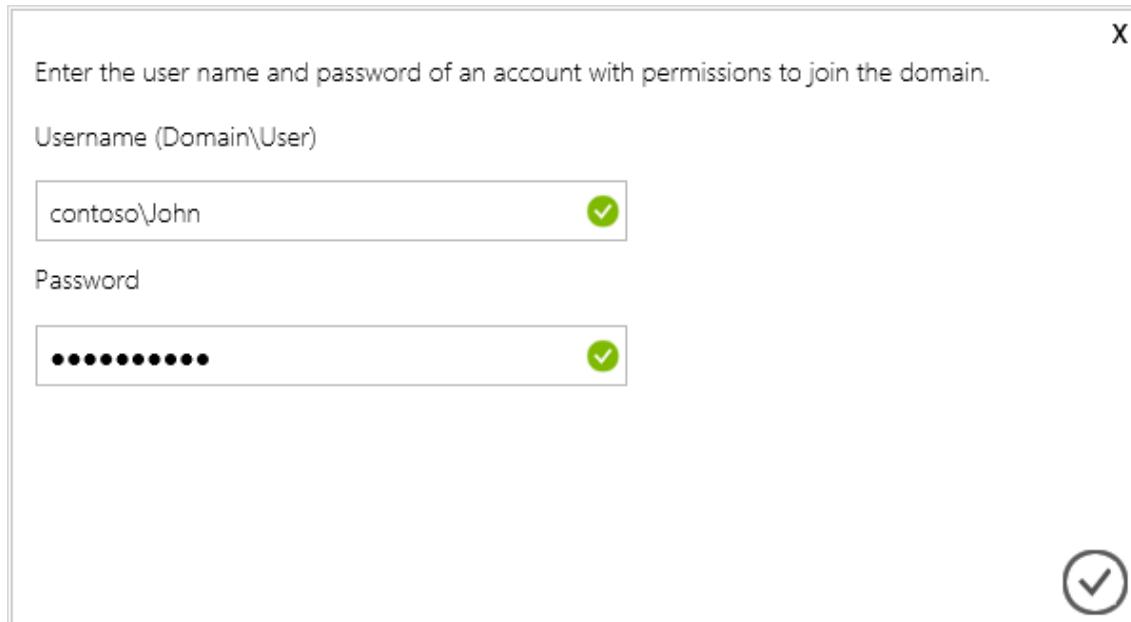
- a. Assign a unique **Name** to your device. This name can be 1-15 characters and can contain letter, numbers and hyphens.
- b. Click the **iSCSI server** icon  for the **Type** of device that you are creating. An iSCSI server will allow you to provision block storage.
- c. Specify if you want this device to be domain-joined. If your device is an iSCSI server, then joining the domain is optional. If you decide to not join your iSCSI server to a domain, click **Apply**, wait for the settings to be applied and then skip to the next step.

If you want to join the device to a domain. Enter a **Domain name**, and then click **Apply**.

 **Note**

If joining your iSCSI server to a domain, ensure that your virtual array is in its own organizational unit (OU) for Microsoft Azure Active Directory and no group policy objects (GPO) are applied to it.

- d. A dialog box will appear. Enter your domain credentials in the specified format. Click the check icon . The domain credentials will be verified. You will see an error message if the credentials are incorrect.



Enter the user name and password of an account with permissions to join the domain.

Username (Domain\User)

contoso\John 

Password

***** 



- e. Click **Apply**. This will apply and validate the device settings.
7. (Optionally) configure your web proxy server. Although web proxy configuration is optional, be aware that if you use a web proxy, you can only configure it here.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)[Software update](#)[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Enable web proxy

 On Off

Web proxy URL

Authentication

None



Username

Password

 Apply

Help ©2015 Microsoft

On the **Web proxy** page:

- a. Supply the **Web proxy URL** in this format: *http://host-IP address or FQDN:Port number*. Note that HTTPS URLs are not supported.
 - b. Specify **Authentication** as **Basic** or **None**.
 - c. If you are using authentication, you will also need to provide a **Username** and **Password**.
 - d. Click **Apply**. This will validate and apply the configured web proxy settings.
8. (Optionally) configure the time settings for your device, such as time zone and the primary and secondary NTP servers. NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

Microsoft Azure

StorSimple 1200 Device Sign out

Configuration

Get started

Network settings

Device settings

Web proxy settings

Time settings

Cloud settings

Maintenance

Power settings

Software update

Password change

Troubleshooting

Diagnostic tests

System logs

Contact Support

Time zone (UTC-08:00) Pacific Time (US & Canada)

Primary NTP server time.windows.com ✓

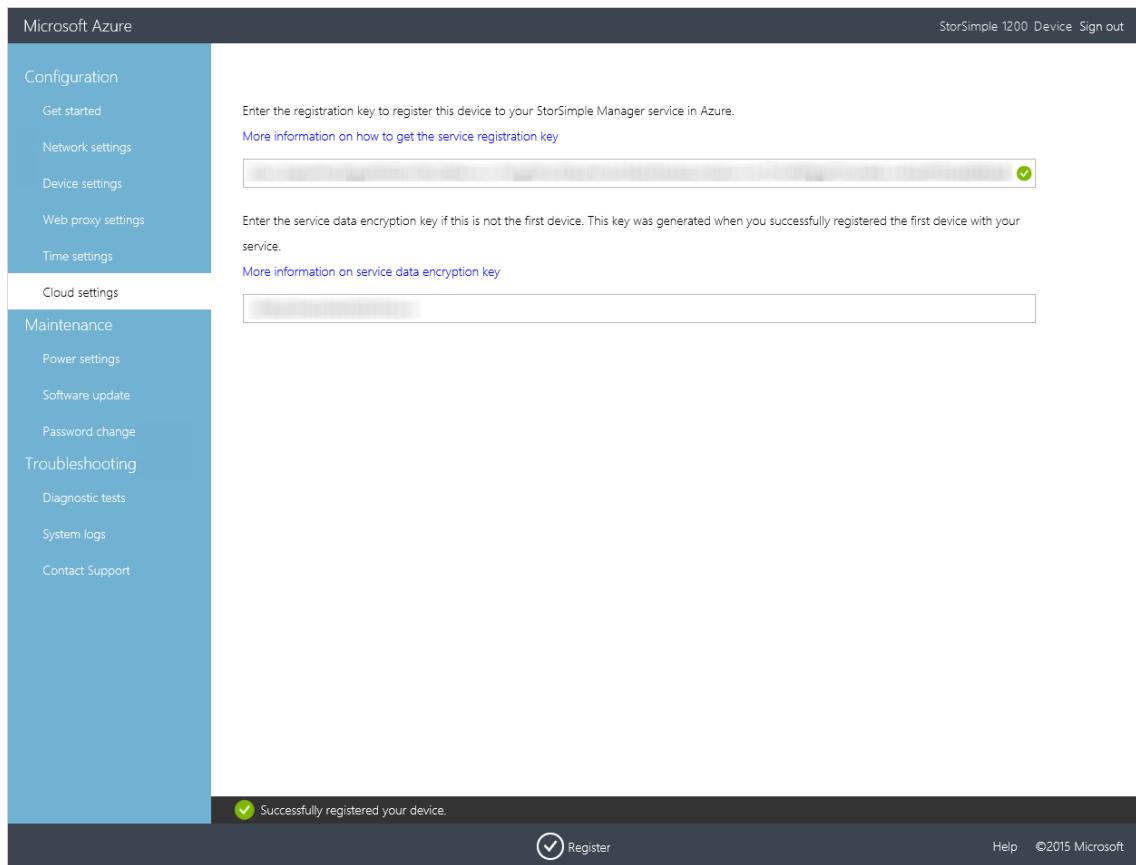
Secondary NTP server

Apply

Help ©2015 Microsoft

On the **Time settings** page:

- a. From the drop-down list, select the **Time zone** based on the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. Specify a **Primary NTP server** for your device or accept the default value of time.windows.com. Ensure that your network allows NTP traffic to pass from your datacenter to the Internet.
 - c. Optionally specify a **Secondary NTP server** for your device.
 - d. Click **Apply**. This will validate and apply the configured time settings.
9. Configure the cloud settings for your device. In this step, you will complete the local device configuration and then register the device with your StorSimple Device Manager service.
- a. Enter the **Service registration key** that you got in [Step 2: Get the service registration key in Deploy StorSimple Virtual Array - Prepare the Portal](#).
 - b. If this is not the first device that you are registering with this service, you will need to provide the **Service data encryption key**. This key is required with the service registration key to register additional devices with the StorSimple Device Manager service. For more information, refer to [Get the service data encryption key](#) on your local web UI.
 - c. Click **Register**. This will restart the device. You may need to wait for 2-3 minutes before the device is successfully registered. After the device has restarted, you will be taken to the sign in page.



10. Return to the Azure portal.

11. Navigate to the **Devices** blade of your service. If you have a lot of resources, click **All resources**, click your service name (search for it if necessary), and then click **Devices**.

12. On the **Devices** blade, verify that the device has successfully connected to the service by looking up the status. The device status should be **Ready to set up**.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
MYSSFS1014	Online	286.11 GB/279 TB	Virtual-NAS	1200
MYSSIS1014	Ready to set up	385.47 GB/3.76 TB	Virtual-iSCSI	1200

Step 2: Configure the device as iSCSI server

Perform the following steps in the Azure portal to complete the required device setup.

To configure the device as iSCSI server

1. Go to your StorSimple Device Manager service and then go to **Management > Devices**. In the **Devices** blade, select the device you just created. This device would show up as **Ready to set up**.

The screenshot shows the Microsoft Azure portal with the 'Devices' blade open for the 'MySSDevManager' service. The left sidebar shows various resources under 'Subscriptions: All 2 selected'. The main area displays a table of devices. The first device, 'MYSSFS1014', is listed as 'Online' with 286.11 GB/2.79 TB capacity. The second device, 'MYSSIS1014', is listed as 'Ready to set up' with 385.47 GB/3.76 TB capacity. Both devices are categorized as 'Virtual-NAS' and 'Virtual-iSCSI' with model 1200. A red box highlights the 'Ready to set up' status of the second device.

2. Click the device and you will see a banner message indicating that the device is ready to setup.

The screenshot shows the StorSimple Device Manager interface with the 'Devices' blade open. The left sidebar shows the 'Devices' section. The main area displays a table of devices. The second device, 'MYSSIS1014', is listed as 'Ready to set up' with 385.47 GB/3.76 TB capacity. A red box highlights the 'Ready to set up' status. On the right side, there is a 'Configure' button. Above the device table, a banner message reads: 'Your device is ready to setup. Click the 'Configure' button above to complete setup.' A red box highlights this banner message.

3. Click **Configure** on the device command bar. This opens up the **Configure** blade. In the **Configure** blade, do the following:

- The iSCSI server name is automatically populated.
- Make sure the cloud storage encryption is set to **Enabled**. This ensures that the data sent from the device to the cloud is encrypted.
- Specify a 32-character encryption key and record it in a key management app for future reference.
- Select a storage account to be used with your device. In this subscription, you can select an existing storage account, or you can click **Add** to choose an account from a different subscription.

The screenshot shows two windows side-by-side. The left window is titled 'MySSD1014' and 'MySSDManager'. It has a red box around the 'Configure' button in the top navigation bar. Below it, a message says 'Your device is ready to setup. Click the 'Configure' button above to complete setup.' The 'Essentials' section shows status: 'Ready to set up' (Device web UI: 10.161.22.165), Model: 1200, and Device software version: 10.0.10288.0. The 'Monitoring' section displays 'Alerts - Past 7 days' (0 alerts) and 'Capacity' (PROVISIONED: 0 Bytes, REMAINING: 3.76 TB Tiered, 385.47 GB Local). The 'Usage - Past 24 hours' section shows storage usage from 6 PM to 12 PM on Oct 14, categorized by Primary Storage Used, Cloud Storage Used, and Local Storage Used. The right window is titled 'Configure' and 'MySSD1014'. It has a message: 'Complete the configuration of an iSCSI server on this device to create volumes.' It asks for 'Server name' (MYSSD1014), which is 'Enabled'. It also requires an 'Encryption key' and 'Confirm encryption key', both of which are filled with a long string of asterisks and checked. A link 'Configure required settings' is shown with a right-pointing arrow. At the bottom right is a large blue 'Configure' button.

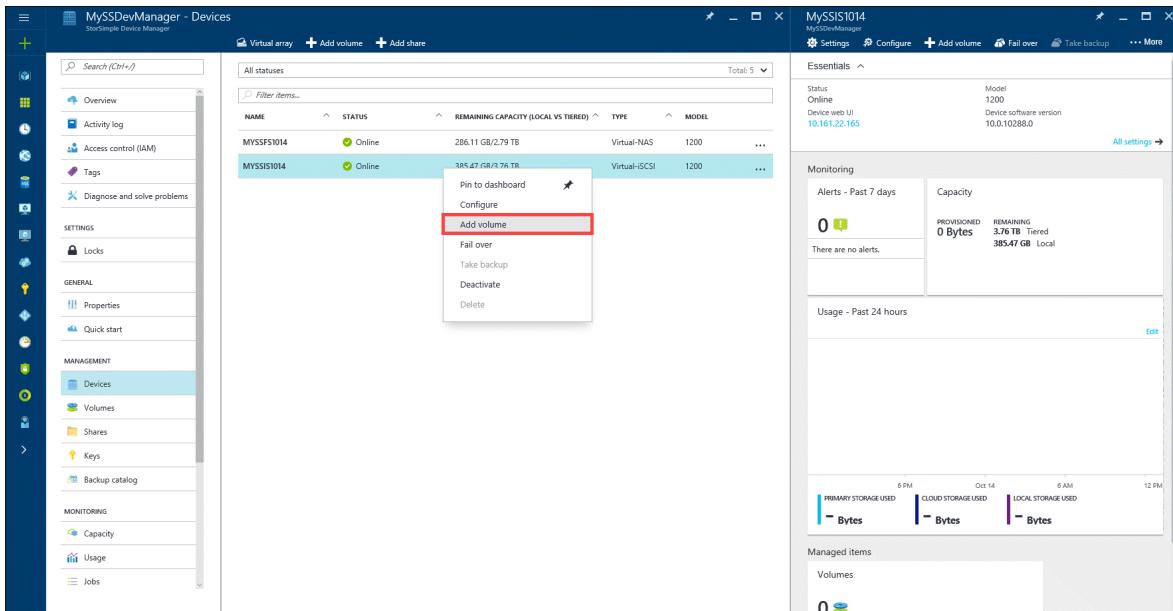
4. Click **Configure** to complete setting up the iSCSI server.

5. You will be notified that the iSCSI server creation is in progress. After the iSCSI server is successfully created, the **Devices** blade is updated and the corresponding device status is **Online**.

Step 3: Add a volume

1. In the **Devices** blade, select the device you just configured as an iSCSI server. Click ... (alternatively right-click in this row) and from the context menu, select **Add**

volume. You can also click **+ Add volume** from the command bar. This opens up the **Add volume** blade.

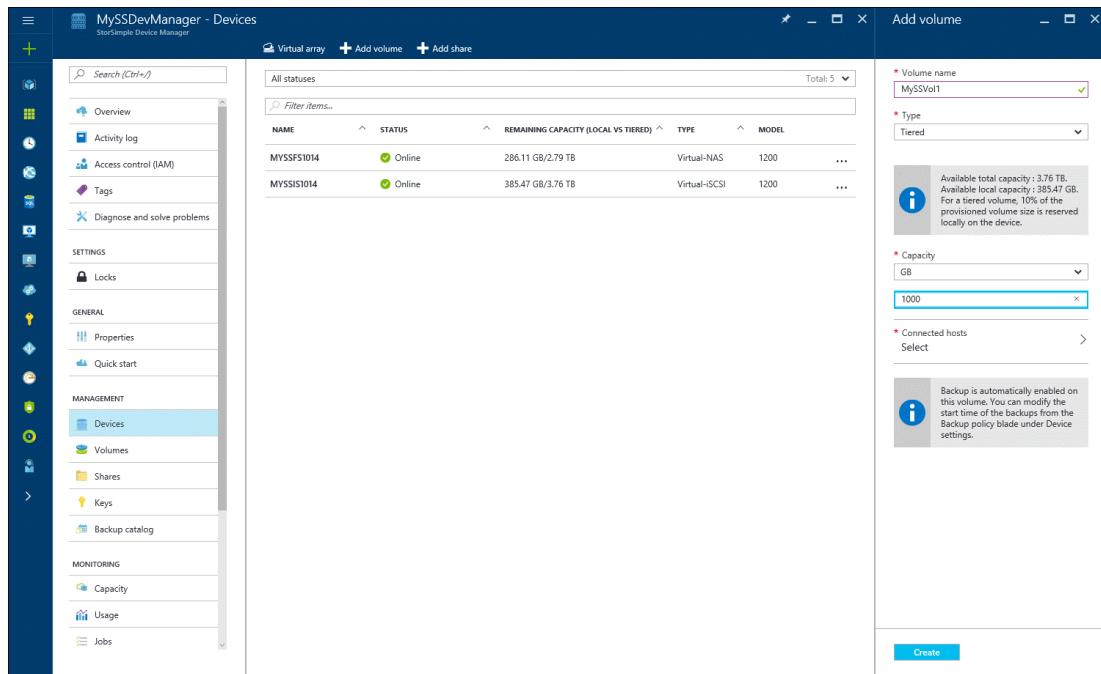


2. In the **Add volume** blade, do the following:

- In the **Volume name** field, enter a unique name for your volume. The name must be a string that contains 3 to 127 characters.
- In the **Type** dropdown list, specify whether to create a **Tiered** or **Locally pinned** volume. For workloads that require local guarantees, low latencies, and higher performance, select **Locally pinned volume**. For all other data, select **Tiered volume**.
- In the **Capacity** field, specify the size of the volume. A tiered volume must be between 500 GB and 5 TB and a locally pinned volume must be between 50 GB and 500 GB.

A locally pinned volume is thickly provisioned and ensures that the primary data in the volume stays on the device and does not spill to the cloud.

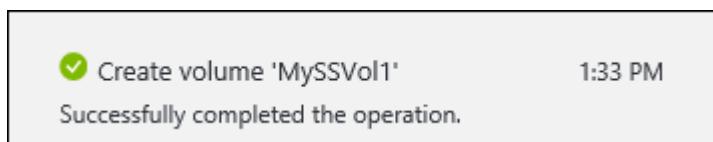
A tiered volume on the other hand is thinly provisioned. When you create a tiered volume, approximately 10% of the space is provisioned on the local tier and 90% of the space is provisioned in the cloud. For example, if you provisioned a 1 TB volume, 100 GB would reside in the local space and 900 GB would be used in the cloud when the data tiers. This in turn implies is that if you run out of all the local space on the device, you cannot provision a tiered share (because the 10% will not be available).



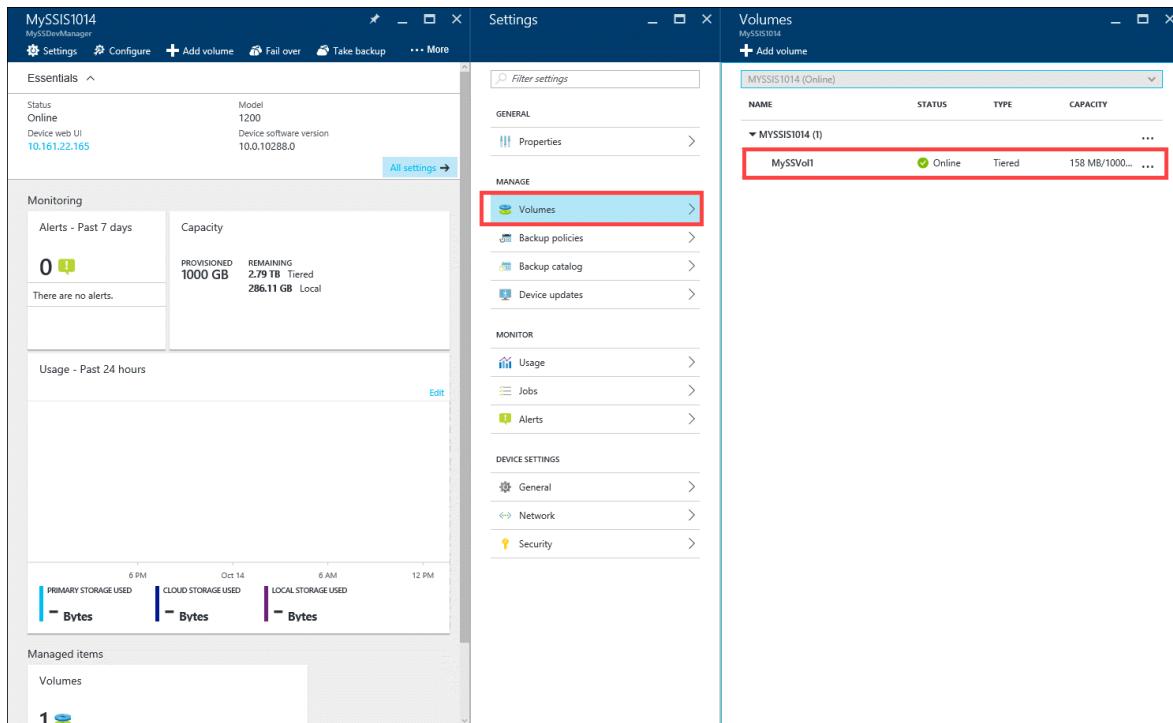
- Click **Connected hosts**, select an access control record (ACR) corresponding to the iSCSI initiator that you want to connect to this volume, and then click **Select**.
3. To add a new connected host, click **Add new**, enter a name for the host and its iSCSI Qualified Name (IQN), and then click **Add**. If you don't have the IQN, go to [Appendix A: Get the IQN of a Windows Server host](#).

The screenshot shows two windows side-by-side. The left window, titled 'Connected hosts', has a red box around its header and contains a blue button labeled 'Add new'. Below it, a message says 'No items found.' The right window, titled 'Add ACR', has a red box around its 'Name' field which contains 'MySVAhost'. Below it is an 'IQN' field containing 'iqn.1991-05.com.contoso\mysswshost.north'.

4. When you're finished configuring your volume, click **OK**. A volume will be created with the specified settings and you will see a notification. By default, monitoring and backup will be enabled for the volume.



5. To confirm that the volume was successfully created, go to the **Volumes** blade. You should see the volume listed.

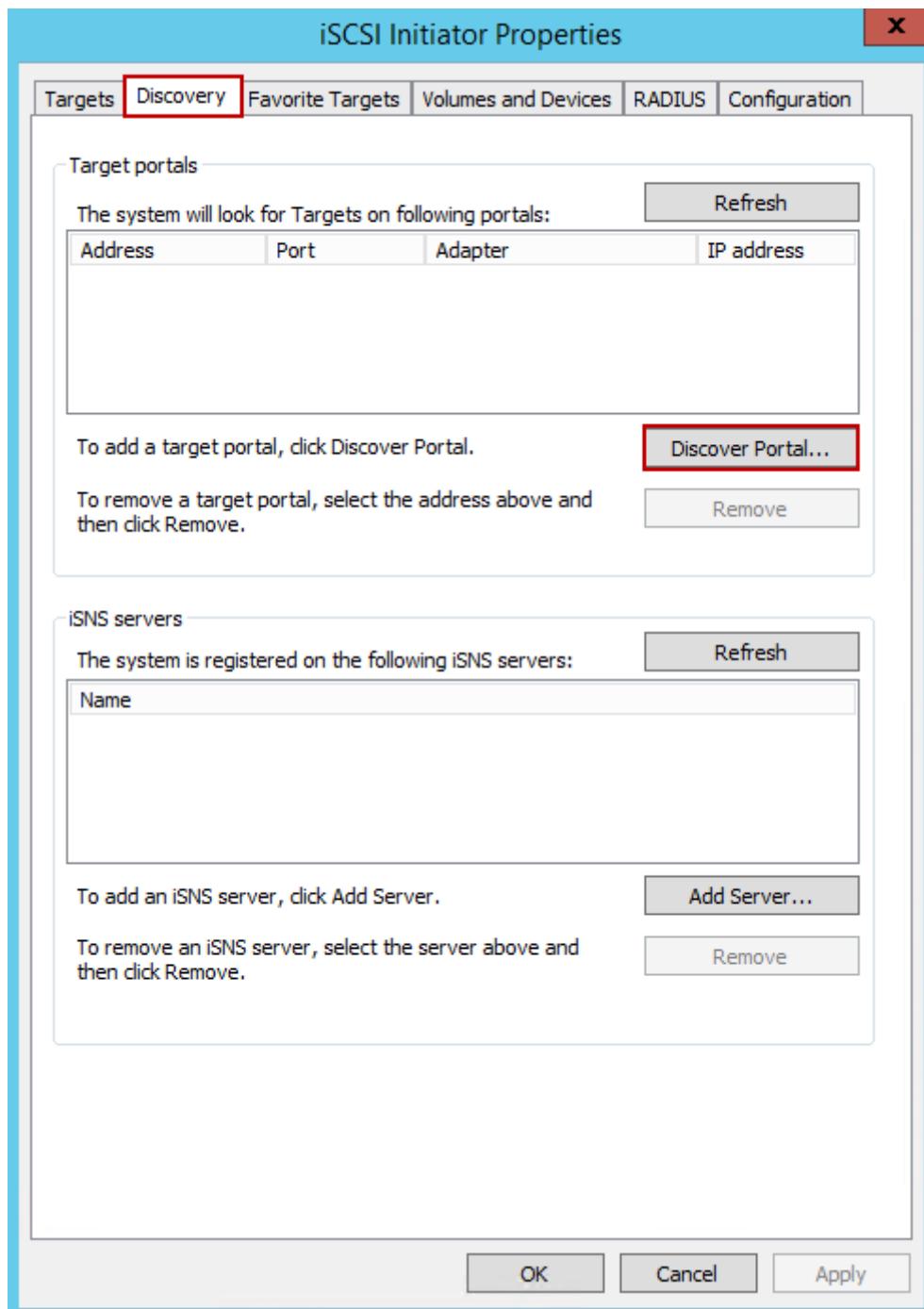


Step 4: Mount, initialize, and format a volume

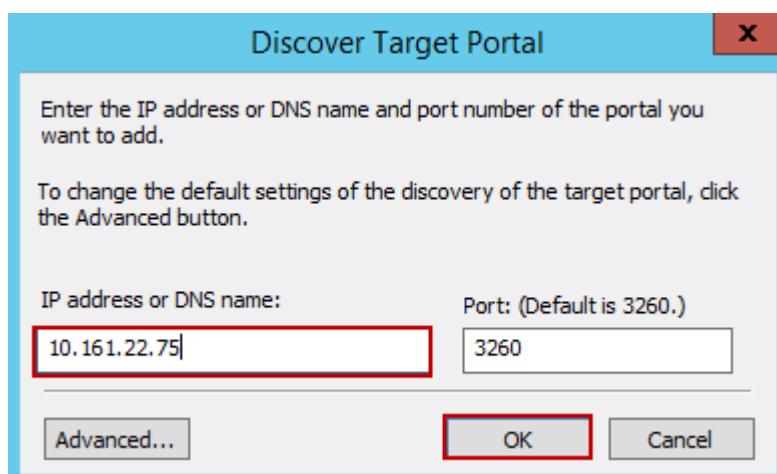
Perform the following steps to mount, initialize, and format your StorSimple volumes on a Windows Server host.

To mount, initialize, and format a volume

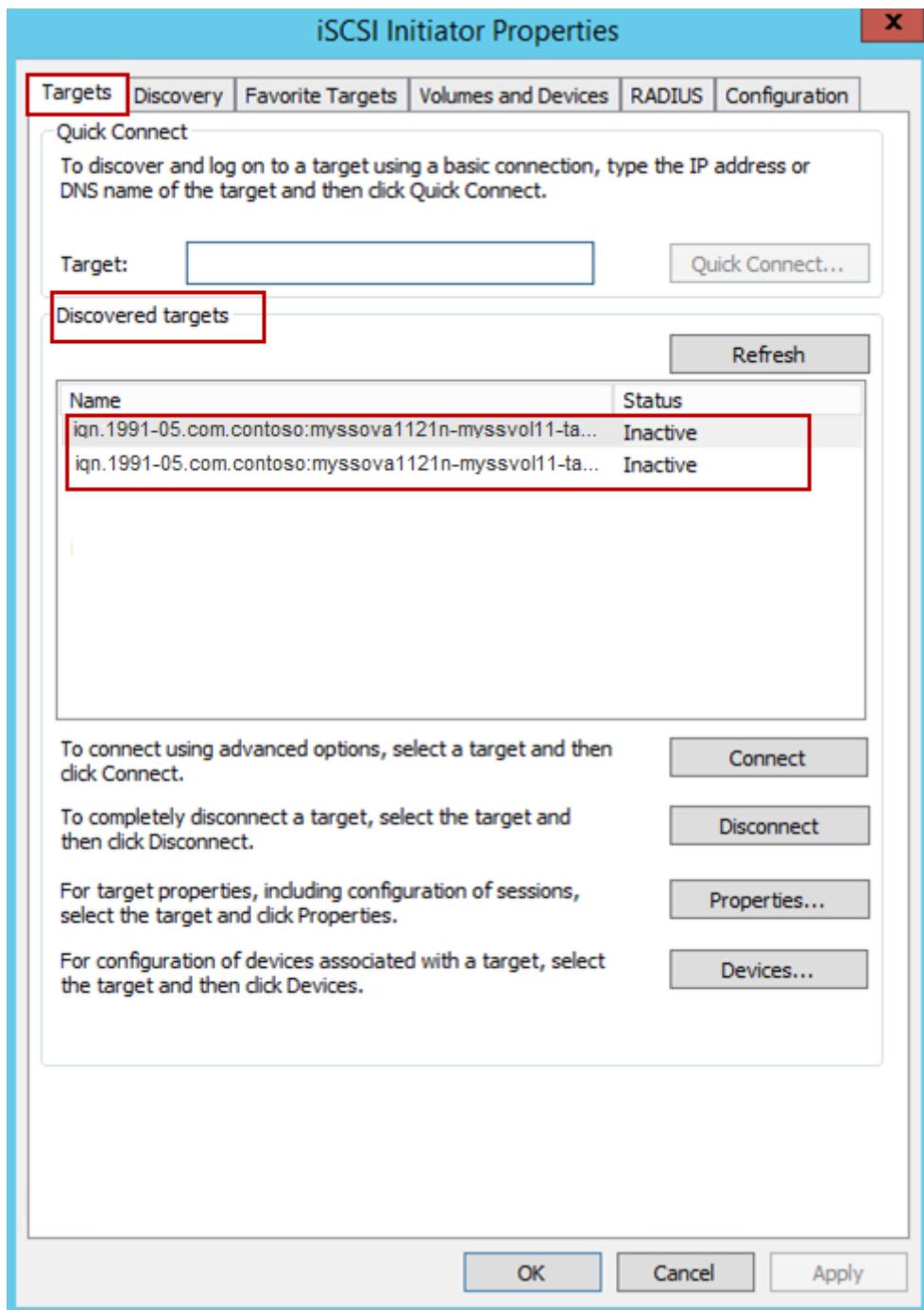
1. Open the **iSCSI initiator** app on the appropriate server.
2. In the **iSCSI Initiator Properties** window, on the **Discovery** tab, click **Discover Portal**.



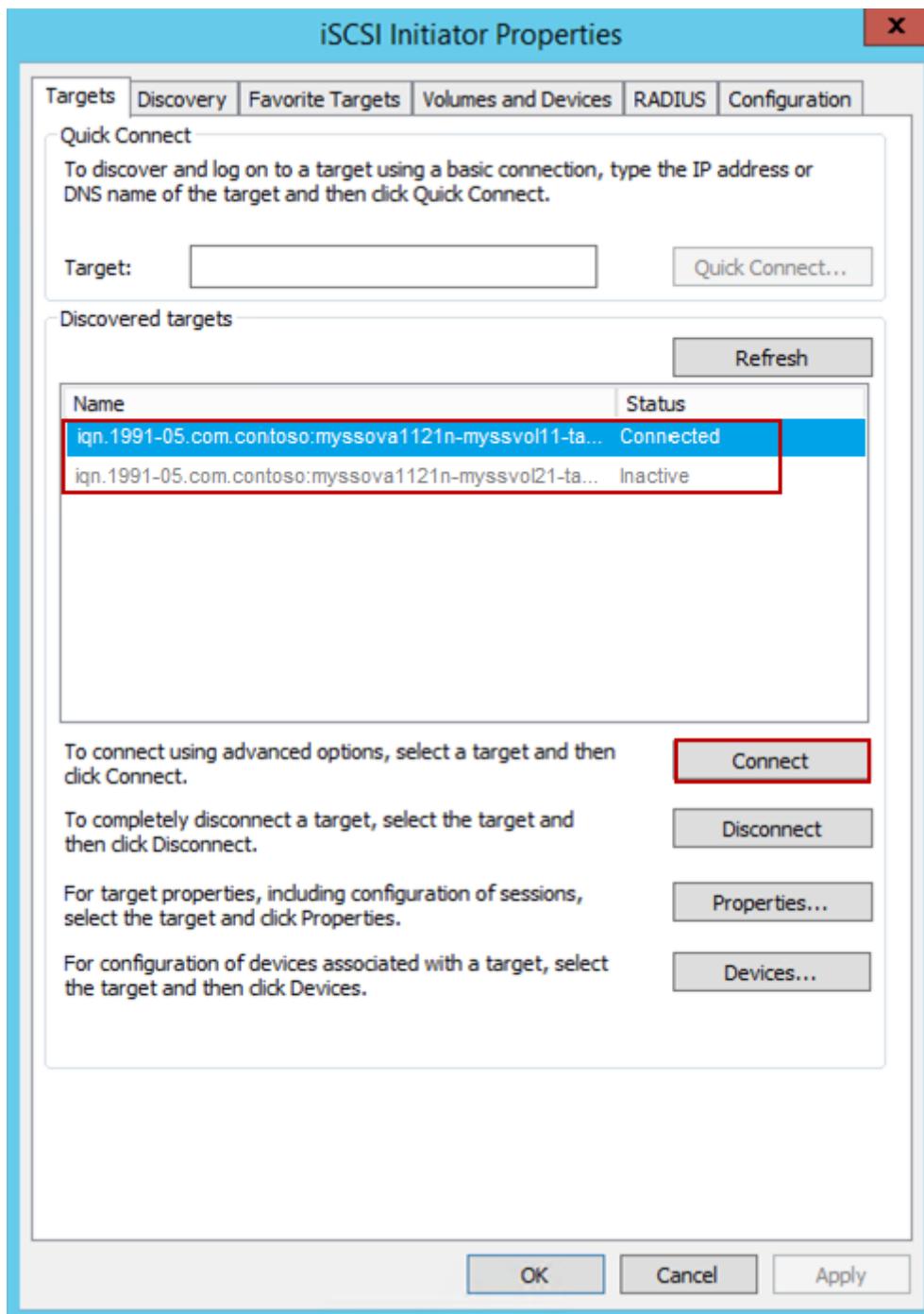
3. In the **Discover Target Portal** dialog box, supply the IP address of your iSCSI-enabled network interface, and then click **OK**.



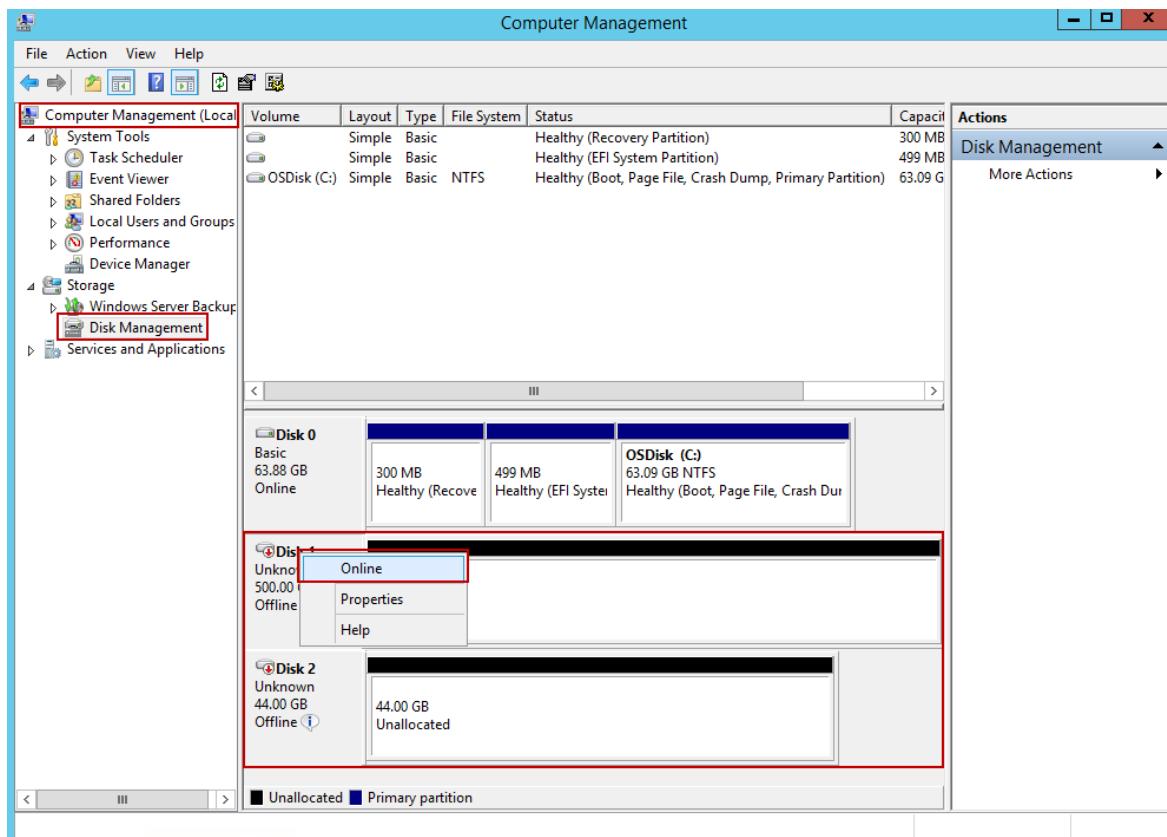
4. In the iSCSI Initiator Properties window, on the **Targets** tab, locate the **Discovered targets**. (Each volume will be a discovered target.) The device status should appear as **Inactive**.



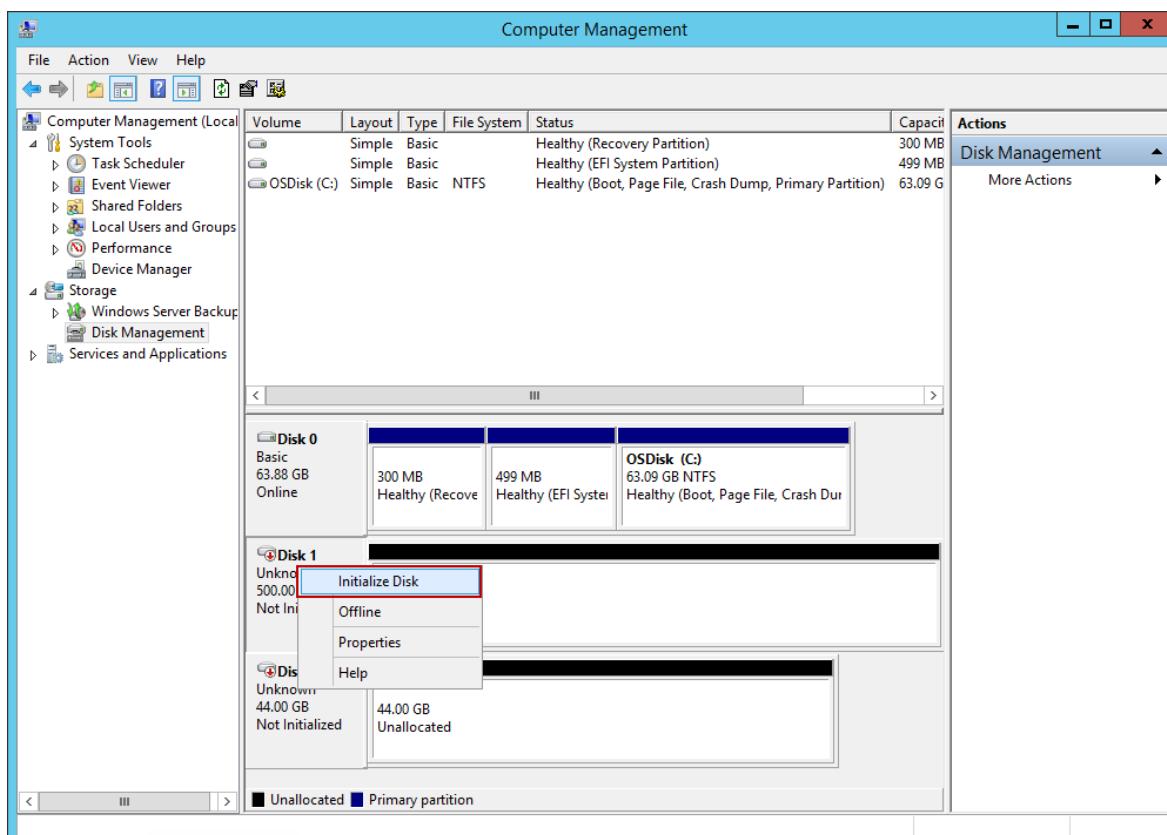
5. Select a target device and then click **Connect**. After the device is connected, the status should change to **Connected**. (For more information about using the Microsoft iSCSI initiator, see [Installing and Configuring Microsoft iSCSI Initiator](#).)



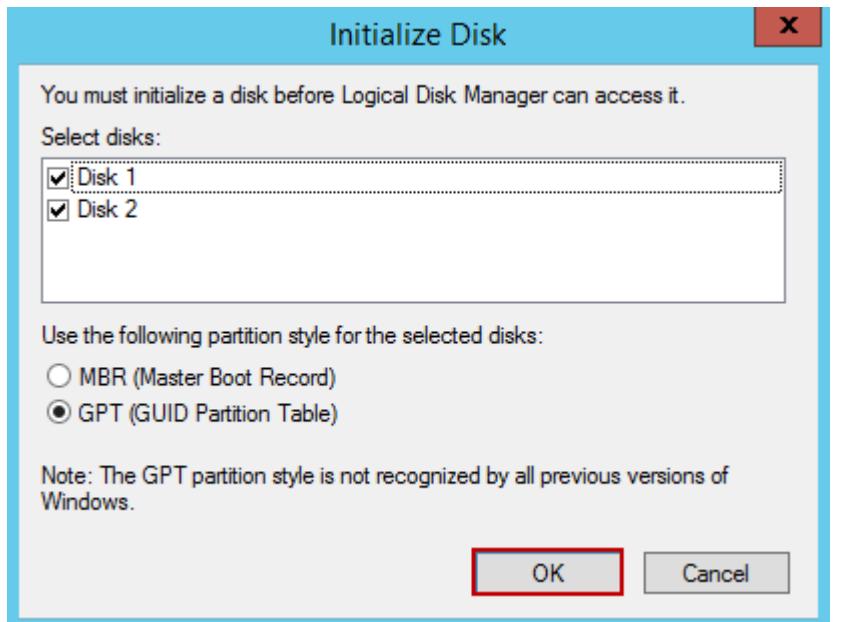
6. On your Windows host, press the Windows Logo key + X, and then click **Run**.
7. In the **Run** dialog box, type **Diskmgmt.msc**. Click **OK**, and the **Disk Management** dialog box will appear. The right pane will show the volumes on your host.
8. In the **Disk Management** window, the mounted volumes will appear as shown in the following illustration. Right-click the discovered volume (click the disk name), and then click **Online**.



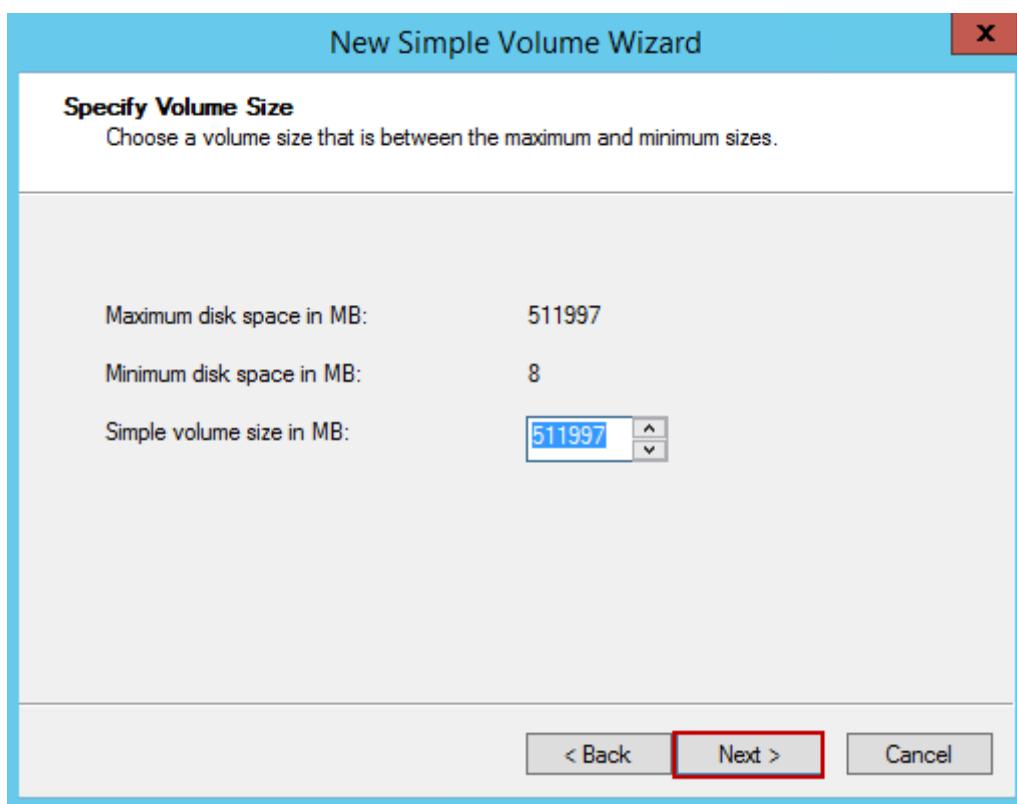
9. Right-click and select Initialize Disk.



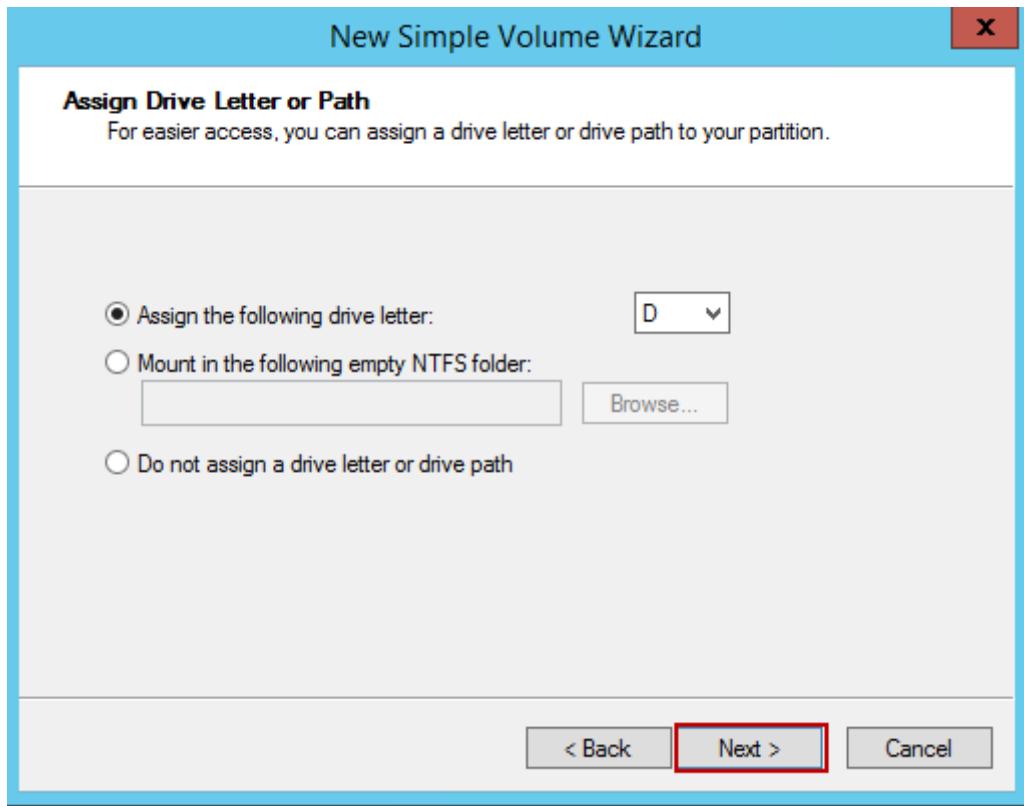
10. In the dialog box, select the disk(s) to initialize, and then click OK.



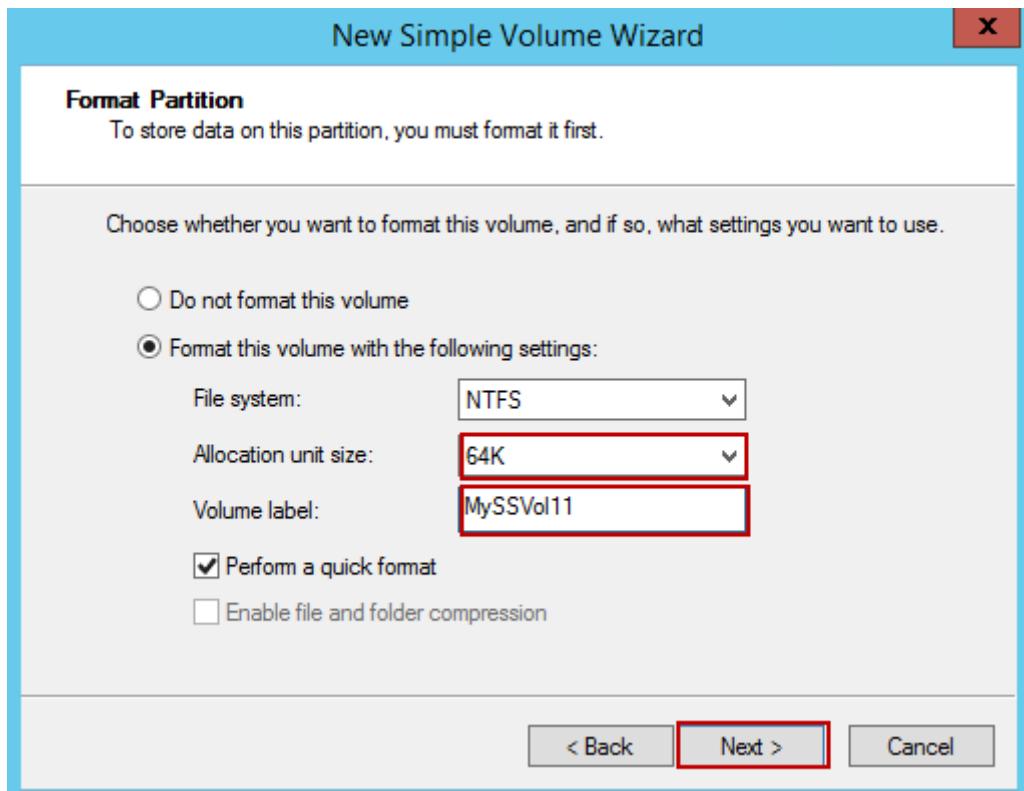
11. The New Simple Volume wizard starts. Select a disk size, and then click **Next**.



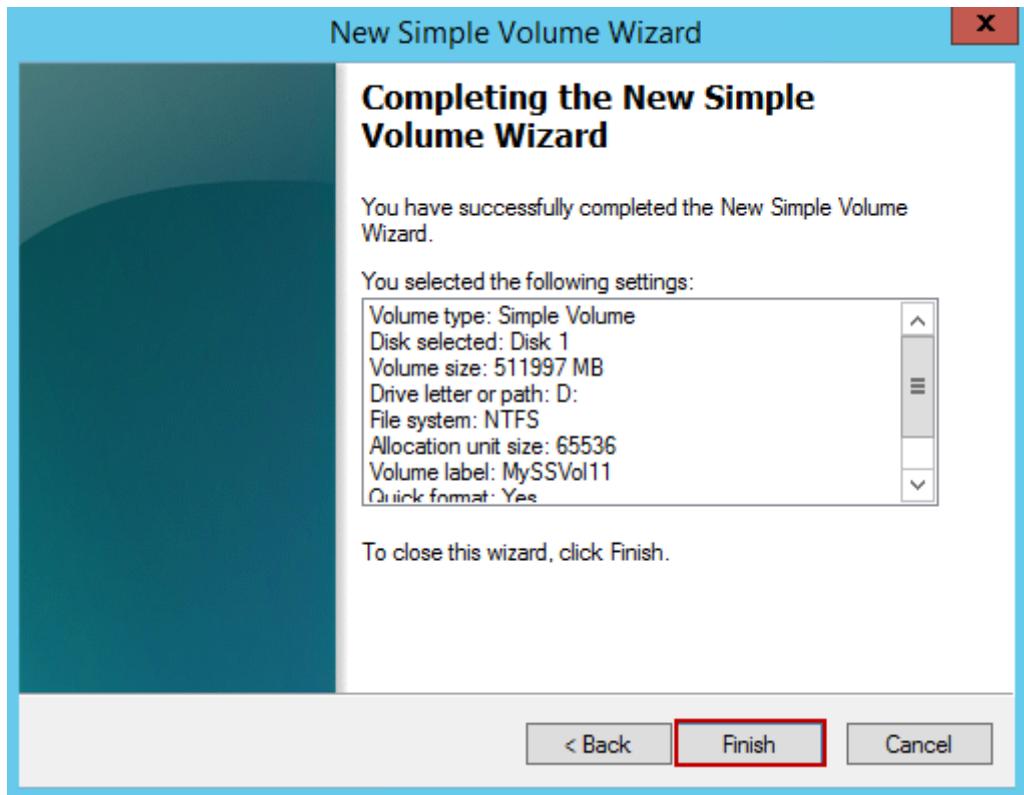
12. Assign a drive letter to the volume, and then click **Next**.



13. Enter the parameters to format the volume. **On Windows Server, only NTFS is supported.** Set the allocation unit size to 64K. Provide a label for your volume. It is a recommended best practice for this name to be identical to the volume name you provided on your StorSimple Virtual Array. Click **Next**.



14. Check the values for your volume, and then click **Finish**.



The volumes will appear as **Online** on the **Disk Management** page.

The screenshot shows the 'Computer Management' interface with the 'Disk Management' tab selected. The left navigation pane includes 'Computer Management (Local)', 'System Tools' (Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, Device Manager), 'Storage' (Windows Server Backup, Disk Management), and 'Services and Applications'. The main area displays a table of disk volumes and a detailed view of Disk 1.

Volume	Layout	Type	File System	Status	Capacity
(C:)	Simple	Basic		Healthy (Recovery Partition)	300 MB
(E:)	Simple	Basic		Healthy (EFI System Partition)	499 MB
(F:)	Simple	Basic	RAW	Formatting	44.00 G
MySSVol11...	Simple	Basic	NTFS	Healthy (Primary Partition)	500.00 G
MySSVol21...	Simple	Basic	NTFS	Healthy (Primary Partition)	44.00 G
OSDisk (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	63.09 G

Below the table, a detailed view of Disk 1 shows its partitions: 'Disk 0' (Basic, 63.88 GB, Online) with two partitions (300 MB and 499 MB); 'Disk 1' (Basic, 500.00 GB, Online) with one partition labeled 'MySSVol11 (D:)'; and 'Disk 2' (Basic, 44.00 GB, Online) with one partition labeled 'MySSVol21 (E:)'. A legend at the bottom indicates 'Unallocated' (black square) and 'Primary partition' (blue square).

Next steps

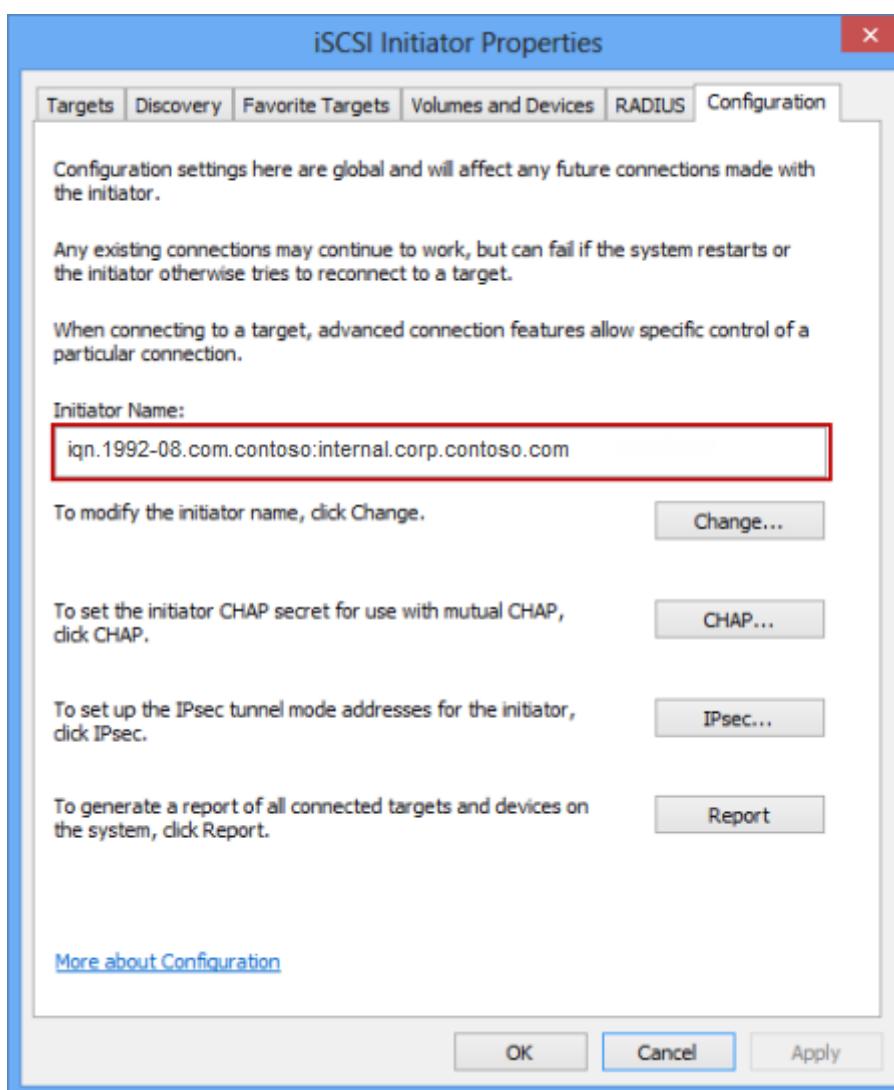
Learn how to use the local web UI to [administer your StorSimple Virtual Array](#).

Appendix A: Get the IQN of a Windows Server host

Perform the following steps to get the iSCSI Qualified Name (IQN) of a Windows host that is running Windows Server 2012.

To get the IQN of a Windows host

1. Start the Microsoft iSCSI initiator on your Windows host.
2. In the iSCSI Initiator Properties window, on the Configuration tab, select and copy the string from the Initiator Name field.



3. Save this string.

Use the StorSimple Device Manager service to administer your StorSimple Virtual Array

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Get started

Provision on Hyper-V
Provision on VMware

Set up as file server
Set up as iSCSI server

Manage

Overview

This article describes the StorSimple Device Manager service interface, including how to connect to it and the various options available, and provides links to the specific workflows that can be performed via this UI.

After reading this article, you will know how to:

- Connect to the StorSimple Device Manager service
- Navigate the StorSimple Device Manager UI
- Administer your StorSimple Virtual Array via the StorSimple Device Manager service

ⓘ Note

To view the management options available for the StorSimple 8000 series device, go to [Use the StorSimple Manager service to administer your StorSimple device](#).

Connect to the StorSimple Device Manager service

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple Virtual Arrays. You use a central Microsoft Azure portal running in a browser to manage these devices. To connect to the StorSimple Device Manager service, do the following.

To connect to the service

1. Go to <https://portal.azure.com>.
2. Using your Microsoft account credentials, log on to the Microsoft Azure portal (located at the top-right of the pane).
3. Navigate to Browse --> 'Filter' on StorSimple Device Managers to view all your device managers in a given subscription.

Use the StorSimple Device Manager service to perform management tasks

The following table shows a summary of all the common management tasks and complex workflows that can be performed within the StorSimple Device Manager service summary blade. These tasks are organized based on the blades on which they are initiated.

For more information about each workflow, click the appropriate procedure in the table.

Important

If you see the following warning, you must update the software on the devices before proceeding:

One or more StorSimple devices are running an older software version. The latest available update for TLS 1.2 is a mandatory update and should be installed immediately on these devices. TLS 1.2 is used for all Azure portal communication and without this update, the device won't be able to communicate with the StorSimple service.

StorSimple Device Manager workflows

If you want to do this ...	Use this procedure
Create a service Delete a service Get the service registration key Regenerate the service registration key	Deploy the StorSimple Device Manager service
View the activity logs	Use the StorSimple service summary
Deactivate a Virtual Array Delete a Virtual Array	Deactivate or delete a virtual array
Disaster recovery and device failover Failover prerequisites Business continuity disaster recovery (BCDR) Errors during disaster recovery	Disaster recovery and device failover for your StorSimple Virtual Array
Back up shares and volumes Take a manual backup Change the backup schedule View existing backups	Back up your StorSimple Virtual Array
Clone shares from a backup set Clone volumes from a backup set Item-level recovery (file server only)	Clone from a backup of your StorSimple Virtual Array
About storage accounts Add a storage account Edit a storage account Delete a storage account	Manage storage accounts for the StorSimple Virtual Array
About access control records Add or modify an access control record Delete an access control record	Manage access control records for the StorSimple Virtual Array
View job details	Manage StorSimple Virtual Array jobs
Configure alert settings Receive alert notifications Manage alerts Review alerts	View and manage alerts for the StorSimple Virtual Array
Modify the device administrator password	Change the StorSimple Virtual Array device administrator password
Install software updates	Update your Virtual Array

Note

You must use the local web UI for the following tasks:

- Retrieve the service data encryption key
- Create a support package
- Stop and restart a Virtual Array

Next steps

For information about the web UI and how to use it, go to [Use the StorSimple web UI to administer your StorSimple Virtual Array](#).

Install Update 1.0 on your StorSimple Virtual Array

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the steps required to install Update 1.0 on your StorSimple Virtual Array via the local web UI and via the Azure portal.

You apply the software updates or hotfixes to keep your StorSimple Virtual Array up-to-date. Before you apply an update, we recommend that you take the volumes or shares offline on the host first and then the device. This minimizes any possibility of data corruption. After the volumes or shares are offline, you should also take a manual backup of the device.

ⓘ Important

- Update 1.0 corresponds to **10.0.10296.0** software version on your device. For information on what is new in this update, go to [Release notes for Update 1.0](#).
- Keep in mind that installing an update or hotfix restarts your device. Given that the StorSimple Virtual Array is a single node device, any I/O in progress is disrupted and your device experiences downtime.
- Update 1 is available in the Azure portal only if the virtual array is running Update 0.6. For virtual arrays running pre-Update 0.6 versions, you must install Update 0.6 first and then install Update 1.

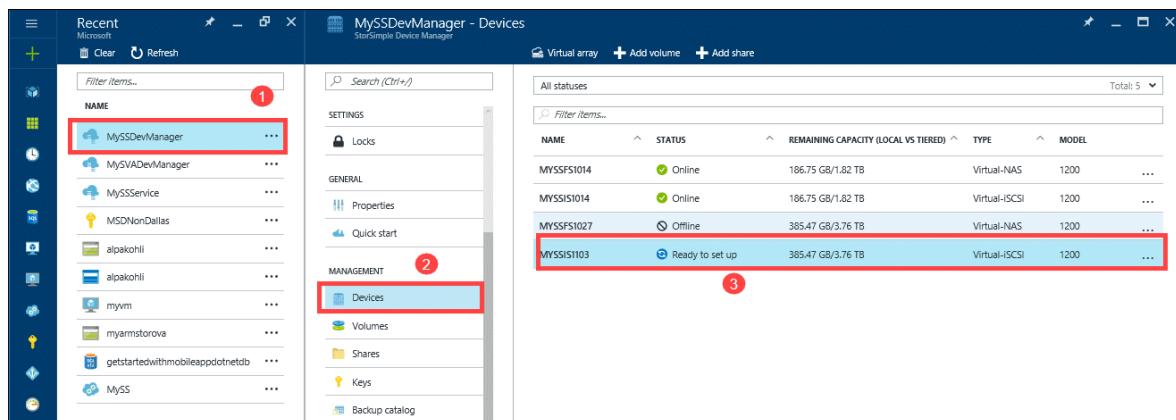
Use the Azure portal

If running Update 0.2 and later, we recommend that you install updates through the Azure portal. The portal procedure requires the user to scan, download, and then install the updates. Depending upon the software version your virtual array is running, applying update via the Azure portal is different.

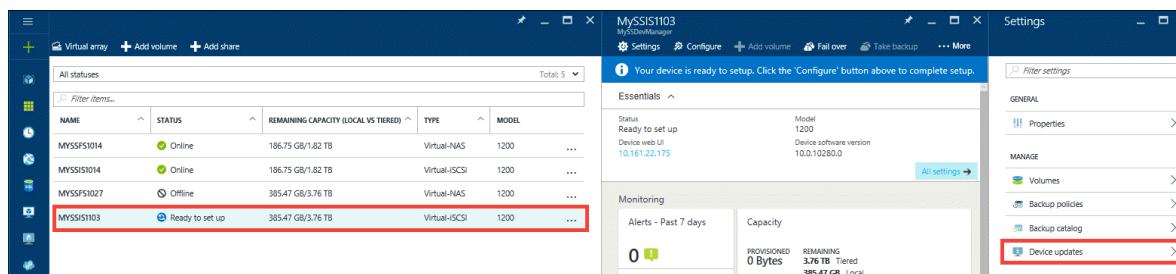
- If your virtual array is running Update 0.6, the Azure portal directly installs Update 1 (10.0.10296.0) on your device. This procedure takes around 7 minutes to complete.
- If your virtual array is running a version prior to Update 0.6, update is done in two stage. The Azure portal first installs Update 0.6 (10.0.10293.0) on your device. The virtual array reboots and the portal then installs Update 1 (10.0.10296.0) on your device. This procedure takes around 15 minutes to complete.

To install updates via the Azure portal

1. Go to your StorSimple Device Manager and select **Devices**. From the list of devices connected to your service, select and click the device you want to update.



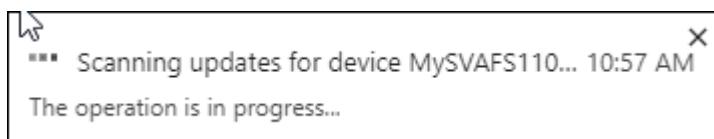
2. In the Settings blade, click **Device updates**.



3. You see a message if the software updates are available. To check for updates, you can also click **Scan**. Make a note of the software version you are running.

The screenshot shows two overlapping windows. The left window is titled 'Settings' and contains a 'Filter settings' search bar, a 'GENERAL' section with 'Properties' (highlighted with a red box), and a 'MANAGE' section with 'Shares', 'Backup policies', 'Backup catalog', and 'Device updates' (highlighted with a red box). The right window is titled 'Device updates' for device 'MySVAFS1101U04'. It has a 'Scan' button and a 'Download updates' button. A purple banner at the top says 'New updates are available.' Below it, it shows 'Last scanned' as 11/1/2017, 10:56 AM and 'Software version' as 10.0.10289.0.

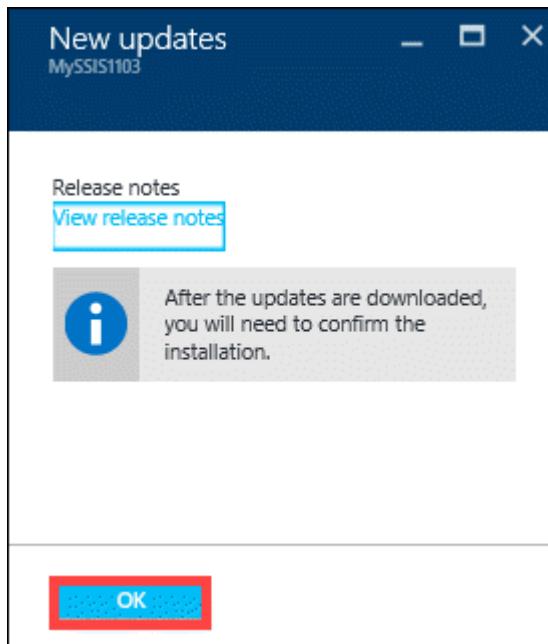
You are notified when the scan starts and completes successfully.



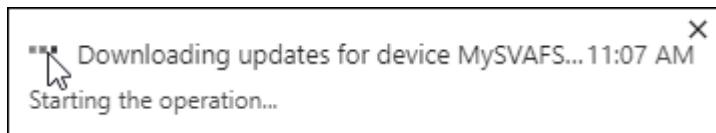
4. Once the updates are scanned, click **Download updates**.

The screenshot shows the same two windows as the previous one. The 'Device updates' blade now has a red box around the 'Download updates' button. The 'Scan' button is also highlighted with a red box.

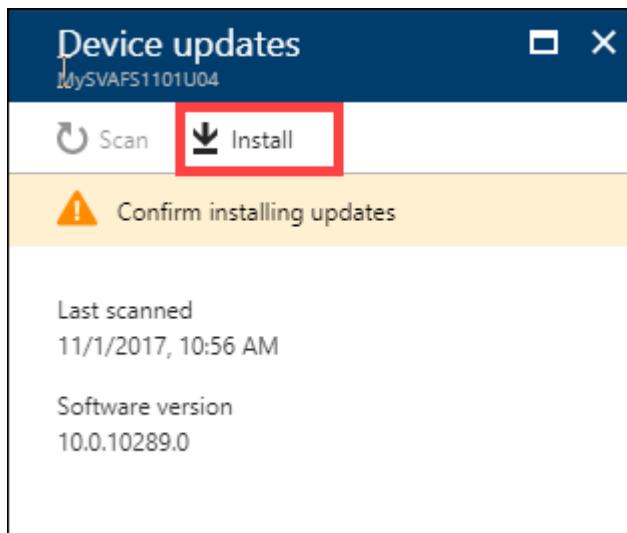
5. In the **New updates** blade, review the release notes. Also note that after the updates are downloaded, you need to confirm the installation. Click **OK**.



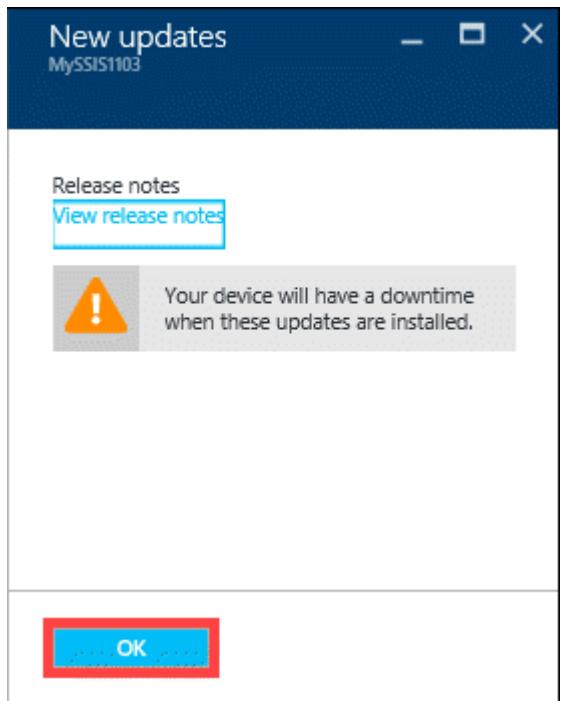
6. You are notified when the upload starts and completes successfully.



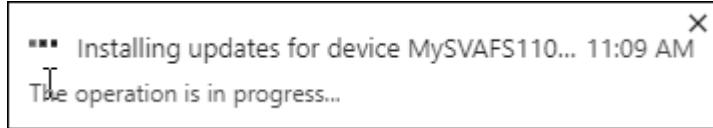
7. In the Device updates blade, click **Install**.



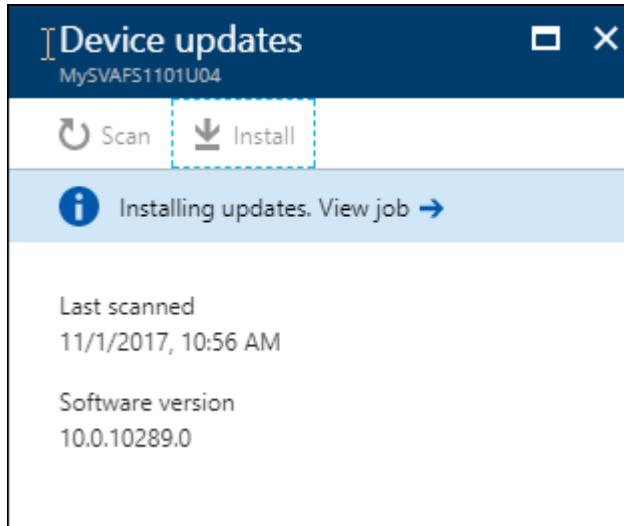
8. In the New updates blade, you are warned that the update is disruptive. As virtual array is a single node device, the device restarts after it is updated. This disrupts any IO in progress. Click **OK** to install the updates.



9. You are notified when the install job starts.



10. After the install job completes successfully, click **View Job** link in the **Device updates** blade to monitor the installation.



This action takes you to the **Install Updates** blade. You can view detailed information about the job here.

Home > AEHelsinkiTestRes - Devices > MySVAFS1101U04 > Settings > Device updates > Install updates

Install updates

Job

Refresh

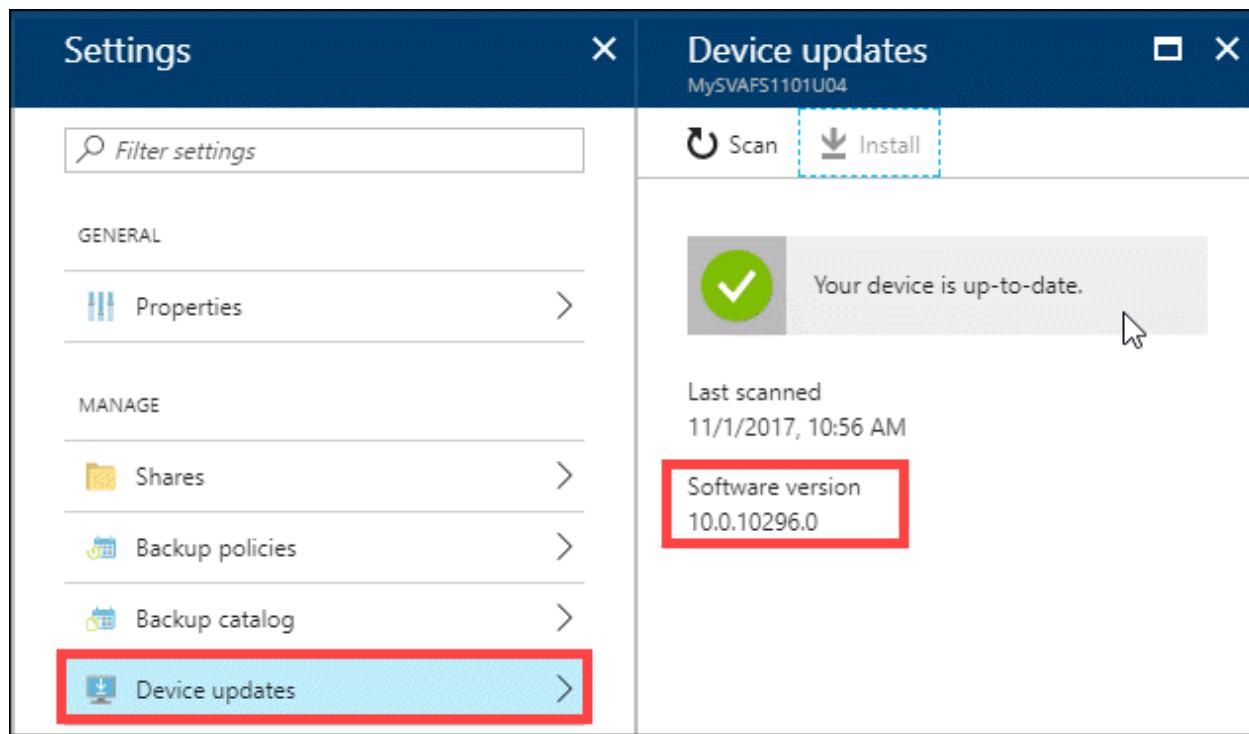
Details

Status	In progress
Entity	MySVAFS1101U04 (microsoft.storsimple/managers/devices)
Device	MY SVAFS1101U04
Started on	11/1/2017, 11:09:12
Completed on	-
Duration	1 Minute, 19 Seconds

11. If you started with a virtual array running software version Update 0.6 (10.0.10293.0), you are now running Update 1 and are done. You can skip the remaining steps. If you started with a virtual array running a software version prior to Update 0.6 (10.0.10293.0), you are now updated to Update 0.6. You see another message indicating that updates are available. Repeat steps 4-8 to install Update 1.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and contains a sidebar with 'GENERAL' and 'MANAGE' sections. Under 'GENERAL', there are links for 'Properties' and 'Device updates'. Under 'MANAGE', there are links for 'Shares', 'Backup policies', 'Backup catalog', and 'Device updates'. The 'Device updates' link in the 'MANAGE' section is highlighted with a blue selection bar. The right window is titled 'Device updates' and shows details for 'MySVAFS1101U04'. It includes a 'Scan' button, a 'Download updates' button, and a purple notification bar stating 'New updates are available.' Below the notification, it shows 'Last scanned' as '11/1/2017, 10:56 AM' and 'Software version' as '10.0.10293.0'.

After the installation is complete, go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you just updated. Go to **Settings > Manage > Device Updates**. The displayed software version should be **10.0.10296.0**.



Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

i Important

Proceed with this update only if you are running Update 0.6 (10.0.10293.0). If you are running an earlier version, [Install Update 0.6](#) on your device first and then apply Update 1.

Download the update or the hotfix

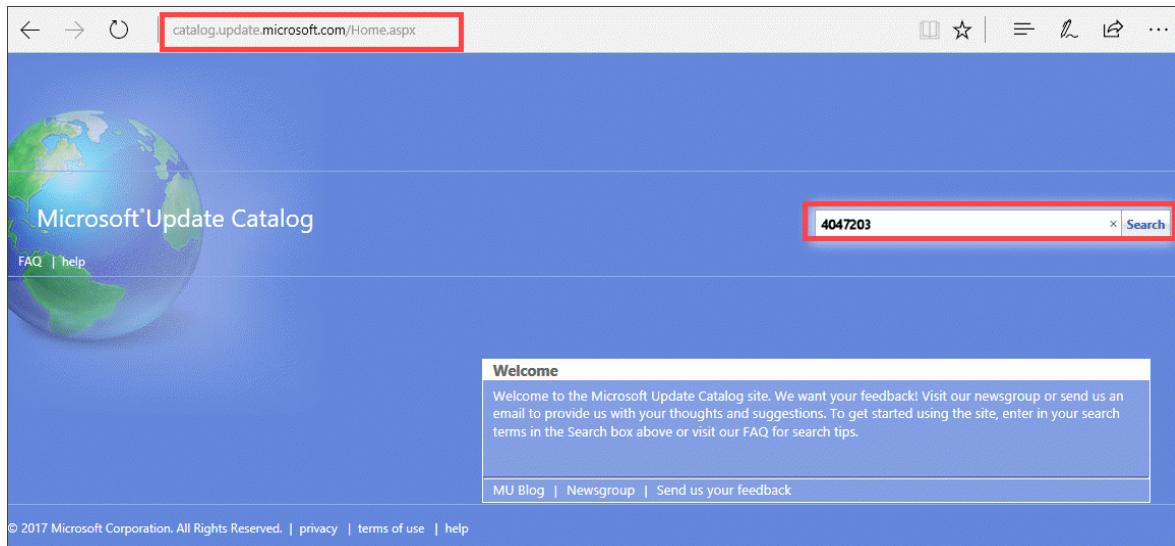
If your virtual array is running Update 0.6, perform the following steps to download Update 1 from the Microsoft Update Catalog.

To download the update or the hotfix

1. Start Internet Explorer and navigate to <https://catalog.update.microsoft.com>.
2. If you are using the Microsoft Update Catalog for the first time on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.

3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download. Enter **4047203** for Update 1.0, and then click **Search**.

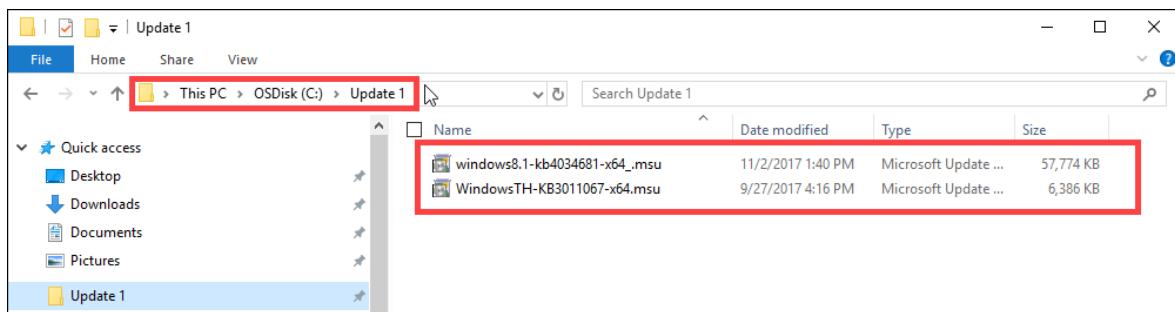
The hotfix listing appears, for example, **StorSimple Virtual Array Update 1.0**.



4. Click Download.

5. Download the two files to a folder. You can also copy the folder to a network share that is reachable from the device.

6. Open the folder where the files are located.



You see two files:

- A Microsoft Update Standalone Package file `WindowsTH-KB3011067-x64`. This file is used to update the device software.
- A file that contains cumulative updates for August `windows8.1-kb4034681-x64`. For more information on what is included in this rollup, go to [August monthly security rollup ↗](#).

Install the update or the hotfix

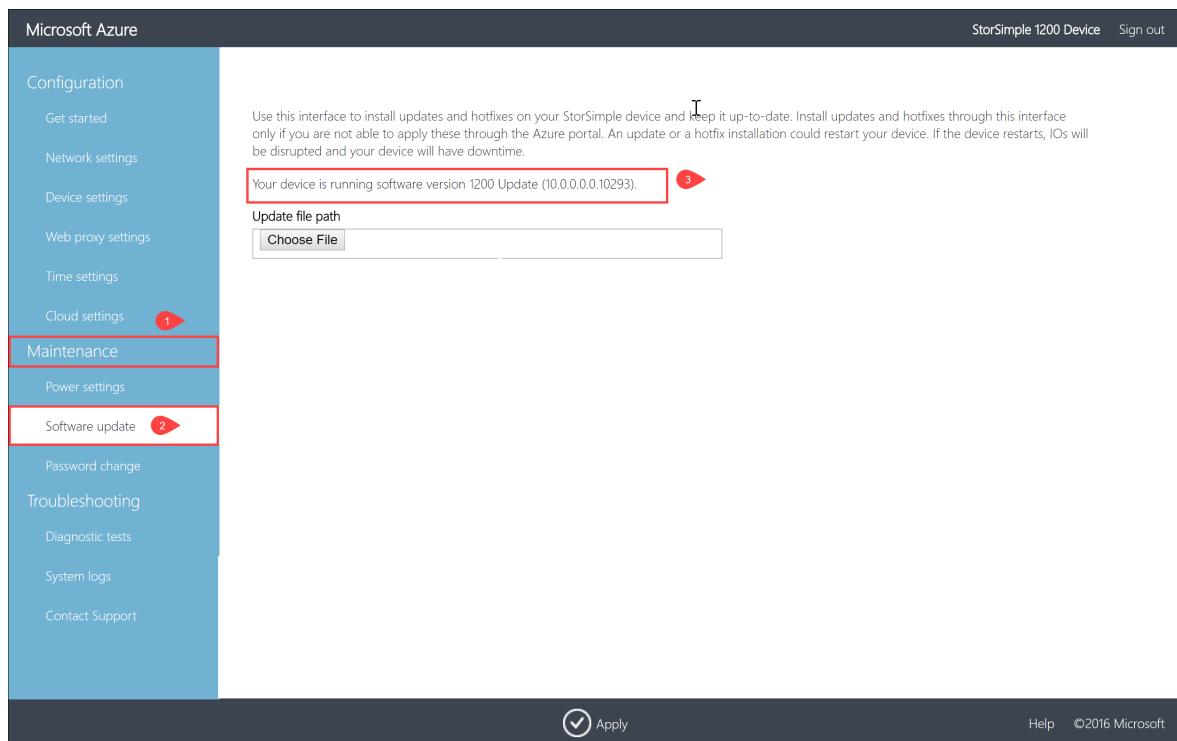
Prior to the update or hotfix installation, make sure that:

- You have the update or the hotfix downloaded either locally on your host or accessible via a network share.
- Your virtual array is running Update 0.6 (10.0.10293.0). If you are running a version prior to Update 0.6, [Install Update 0.6](#) first and then install Update 1.

This procedure takes around 4 minutes to complete. Perform the following steps to install the update or hotfix.

To install the update or the hotfix

1. In the local web UI, go to **Maintenance > Software Update**. Make a note of the software version that you are running. **Proceed with this update only if you are running Update 0.6 (10.0.10293.0). If you are running an earlier version, [Install Update 0.6](#) on your device first and then apply Update 1.**



2. In **Update file path**, enter the file name for the update or the hotfix. You can also browse to the update or hotfix installation file if placed on a network share. Click **Apply**.

Configuration

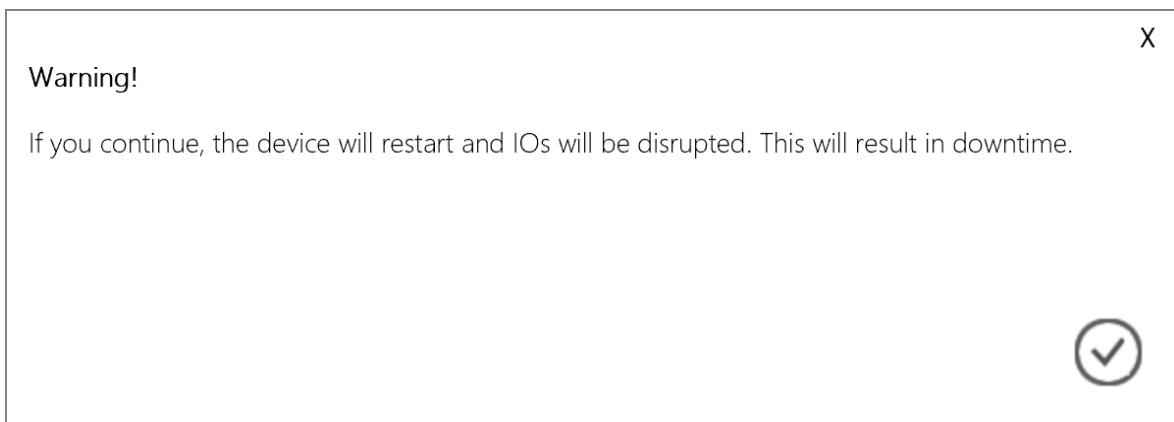
- Get started
- Network settings
- Device settings
- Web proxy settings
- Time settings
- Cloud settings 1
- Maintenance** 2
- Power settings
- Software update** 2 3
- Password change
- Troubleshooting
- Diagnostic tests
- System logs
- Contact Support

... Applying settings...

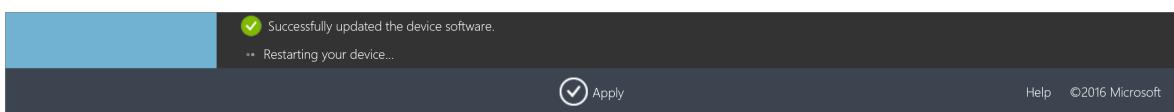
Apply 4

Help ©2016 Microsoft

3. A warning is displayed. Given the virtual array is a single node device, after the update is applied, the device restarts and there is downtime. Click the check icon.



4. The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.



5. After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has updated, in the local web UI, go to **Maintenance > Software Update**. The displayed software version should be **10.0.0.0.0.10296** for Update 1.0.

(!) Note

We report the software versions in a slightly different way in the local web UI and the Azure portal. For example, the local web UI reports **10.0.0.0.0.10296**

and the Azure portal reports 10.0.10296.0 for the same version.

The screenshot shows the Microsoft Azure StorSimple 1200 Device Configuration interface. The left sidebar has a red box around the 'Maintenance' section, which contains 'Power settings' and 'Software update'. The 'Software update' item is also highlighted with a red box. The main content area displays a message: 'Your device is running software version 1200 Update (10.0.0.0.10296)'. Below this is a 'Update file path' input field with a 'Choose File' button and the placeholder 'No file chosen'. At the bottom right of the main area are 'Apply' and 'Help' buttons, along with the copyright notice '©2016 Microsoft'.

6. Repeat steps 2-4 to install the Windows security fix using file [windows8.1-kb4012213-x64](#). The virtual array restarts after the install and you need to sign into the local web UI.

Note

If you directly applied Update 1 to a device running a version prior to Update 0.6, you are missing some updates. Please contact Microsoft Support for next steps.

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Install Update 0.6 on your StorSimple Virtual Array

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the steps required to install Update 0.6 on your StorSimple Virtual Array via the local web UI and via the Azure portal. You apply the software updates or hotfixes to keep your StorSimple Virtual Array up-to-date.

Before you apply an update, we recommend that you take the volumes or shares offline on the host first and then the device. This minimizes any possibility of data corruption. After the volumes or shares are offline, you should also take a manual backup of the device.

ⓘ Important

- Update 0.6 corresponds to 10.0.10293.0 software version on your device. For information on what is new in this update, go to [Release notes for Update 0.6](#).
- If you are running Update 0.2 or later, we recommend that you install the updates via the Azure portal. If you are running Update 0.1 or GA software versions, you must use the hotfix method via the local web UI to install Update 0.6.
- Keep in mind that installing an update or hotfix restarts your device. Given that the StorSimple Virtual Array is a single node device, any I/O in progress is

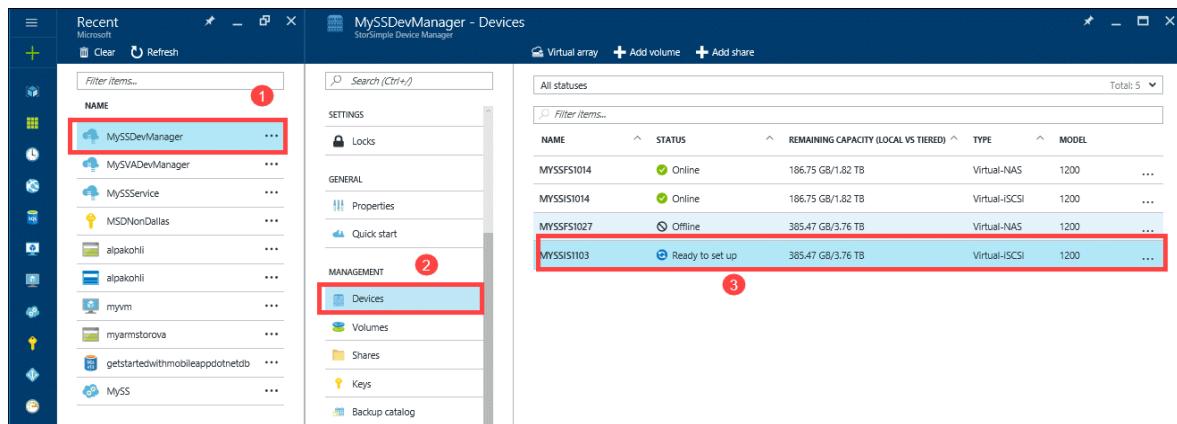
disrupted and your device experiences downtime.

Use the Azure portal

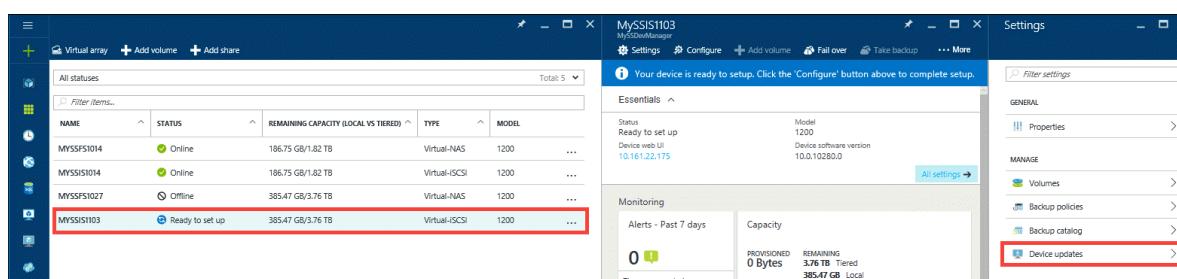
If running Update 0.2 and later, we recommend that you install updates through the Azure portal. The portal procedure requires the user to scan, download, and then install the updates. This procedure takes around 7 minutes to complete. Perform the following steps to install the update or hotfix.

To install updates via the Azure portal

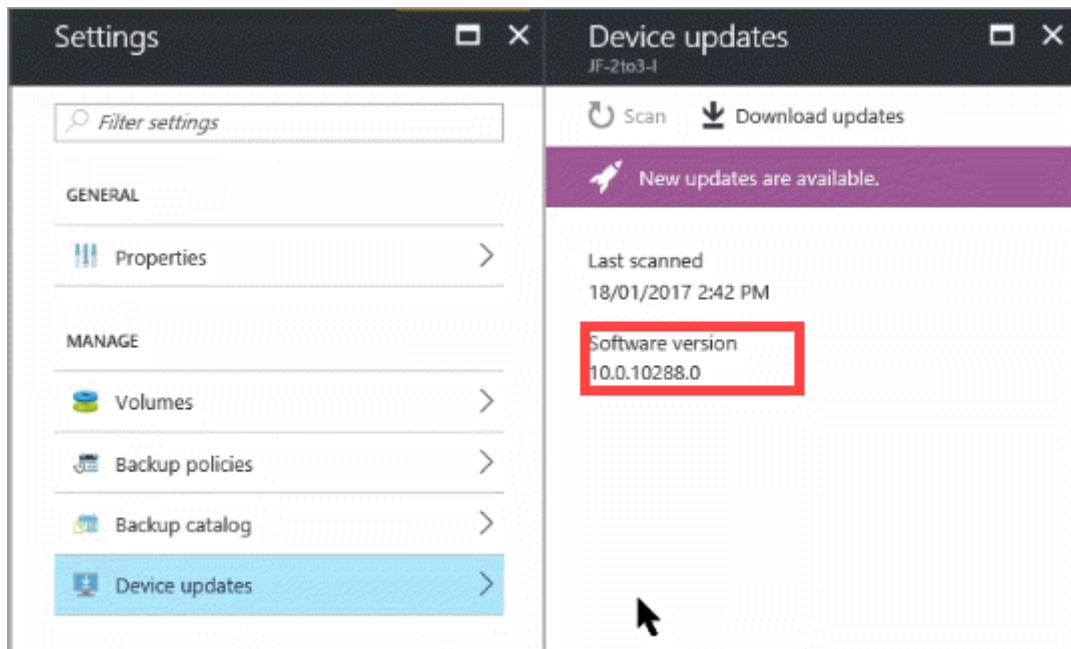
1. Go to your StorSimple Device Manager and select **Devices**. From the list of devices connected to your service, select and click the device you want to update.



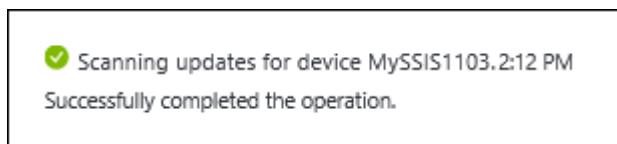
2. In the Settings blade, click **Device updates**.



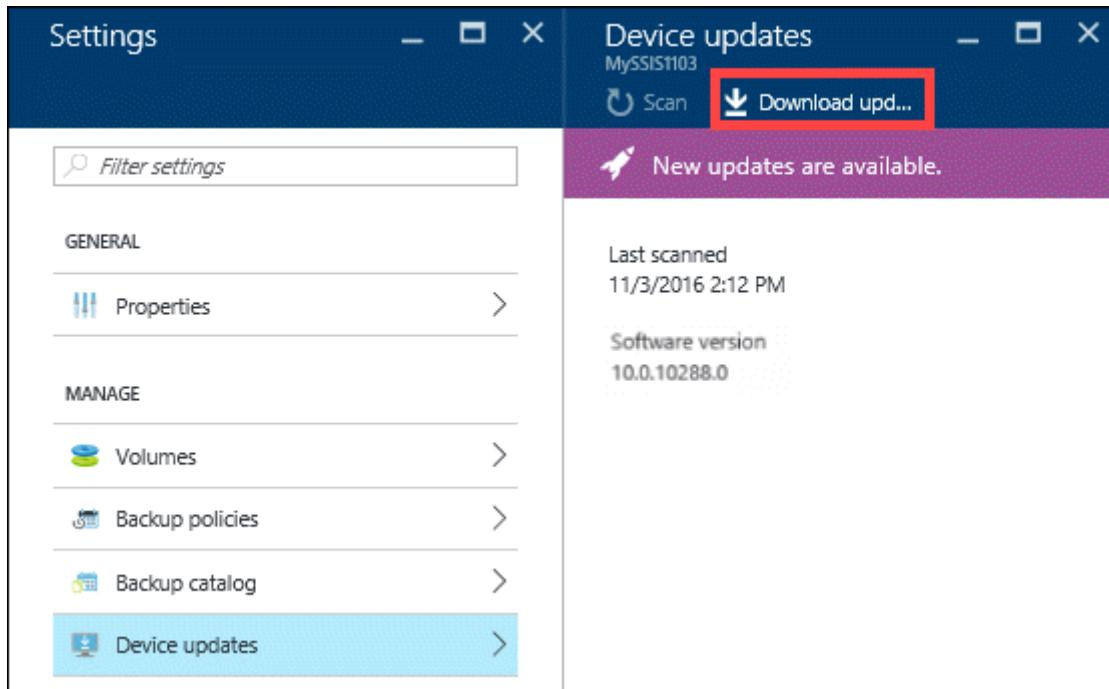
3. You see a message if the software updates are available. To check for updates, you can also click **Scan**.



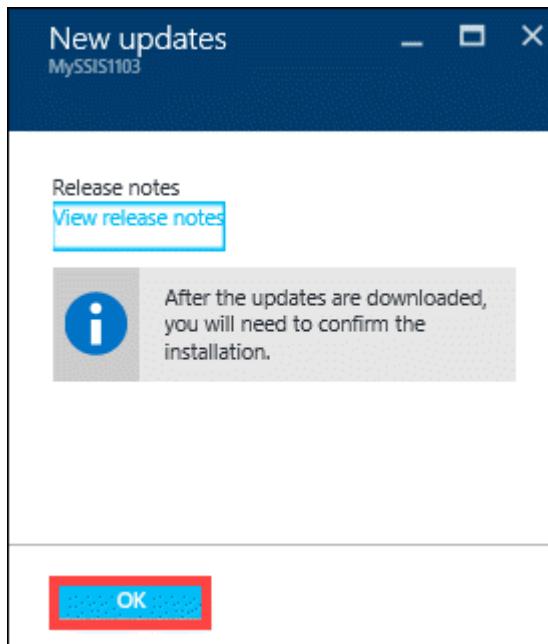
You will be notified when the scan starts and completes successfully.



4. Once the updates are scanned, click **Download updates**.



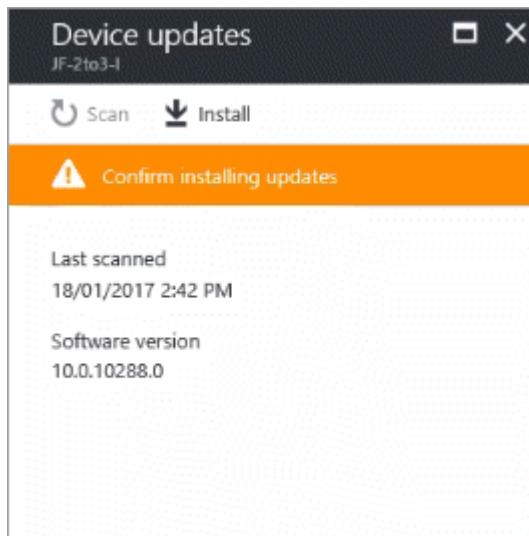
5. In the **New updates** blade, review the information that after the updates are downloaded, you need to confirm the installation. Click **OK**.



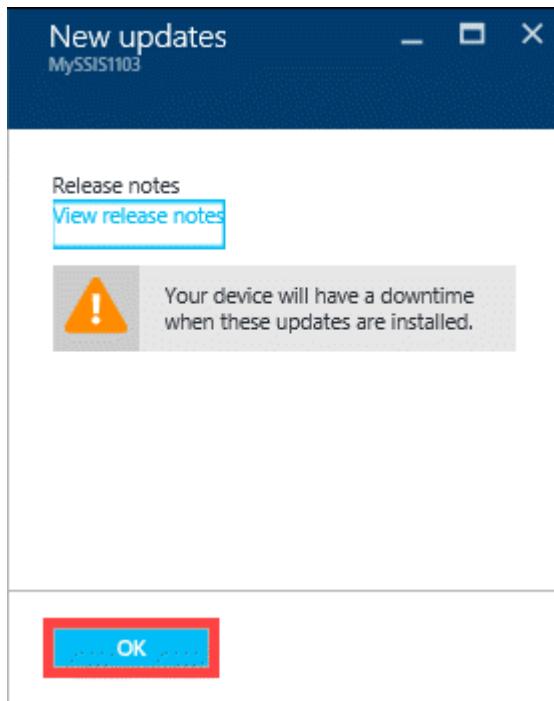
6. You are notified when the upload starts and completes successfully.



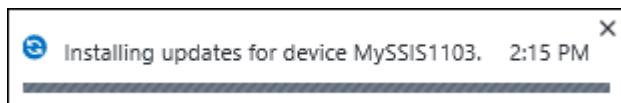
7. In the Device updates blade, click **Install**.



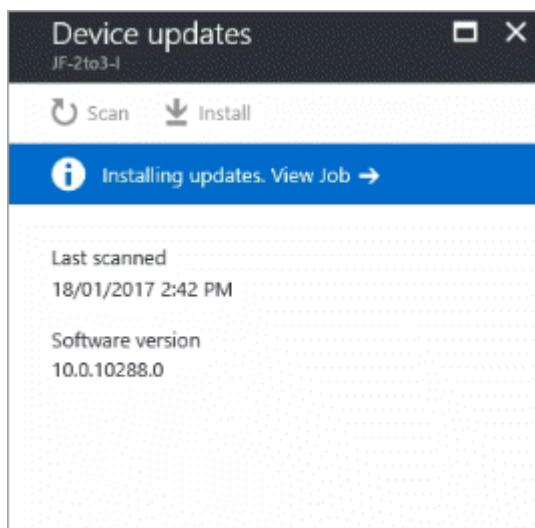
8. In the **New updates** blade, you are warned that the update is disruptive. As virtual array is a single node device, the device restarts after it is updated. This disrupts any IO in progress. Click **OK** to install the updates.



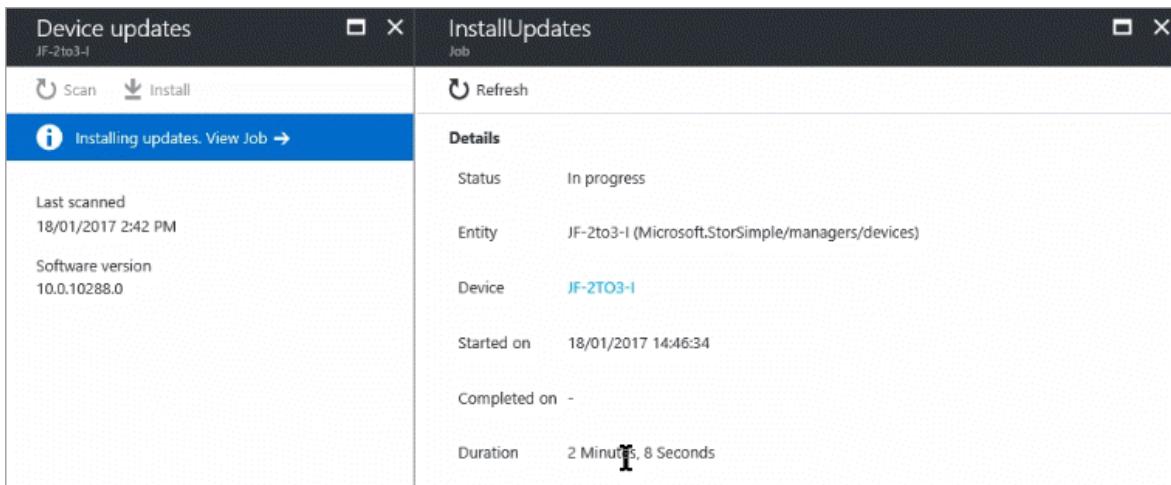
9. You are notified when the install job starts.



10. After the install job completes successfully, click **View Job** link in the **Device updates** blade to monitor the installation.



This takes you to the **Install Updates** blade. You can view detailed information about the job here.



11. After the updates are successfully installed, you see a message to this effect in the **Device updates** blade.

After the installation is complete, go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you just updated. Go to **Settings > Manage > Device Updates**. The displayed software version should be **10.0.10293.0**.

Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

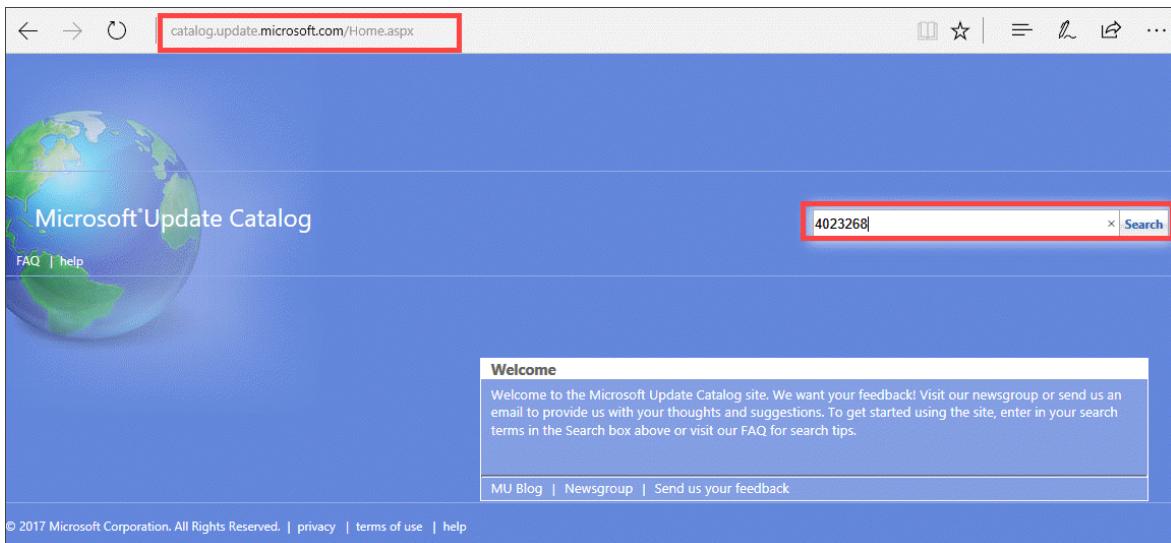
Download the update or the hotfix

Perform the following steps to download the software update from the Microsoft Update Catalog.

To download the update or the hotfix

1. Start Internet Explorer and navigate to <https://catalog.update.microsoft.com>.
2. If you are using the Microsoft Update Catalog for the first time on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.
3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download. Enter **4023268** for Update 0.6, and then click **Search**.

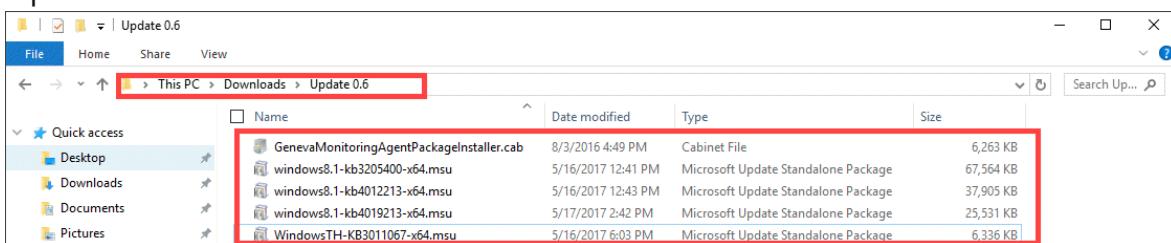
The hotfix listing appears, for example, **StorSimple Virtual Array Update 0.6**.



4. Click Download.

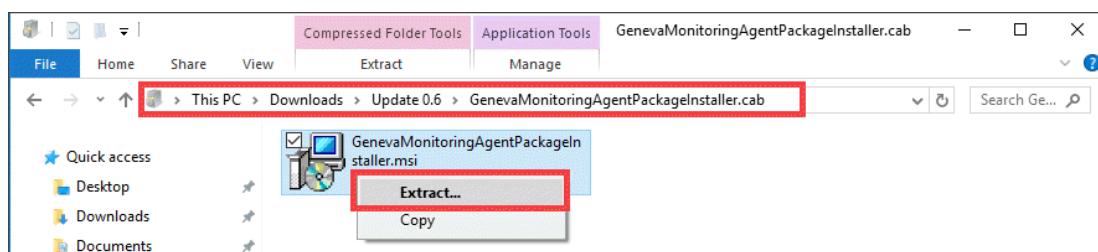
5. You should see five files to download. Download each of those files to a folder. The folder can also be copied to a network share that is reachable from the device.

6. Open the folder where the files are located.



You see:

- A Microsoft Update Standalone Package file `WindowsTH-KB3011067-x64.msu`. This file is used to update the device software.
- A Geneva Monitoring Agent Package file `GenevaMonitoringAgentPackageInstaller.cab`. This file is used to update the Monitoring and Diagnostics service (MDS) agent. Double-click the cab file. A `.msi` file is displayed. Select the file, right-click, and then **Extract** the file. You use the `.msi` file to update the agent.



Important

You do not need to update the MDS agent if you are running StorSimple Update 0.5 (0.0.10293.0).

- Three files that contain critical Windows security updates, `windows8.1-kb4012213-x64`, `windows8.1-kb3205400-x64`, and `windows8.1-kb4019213-x64`.

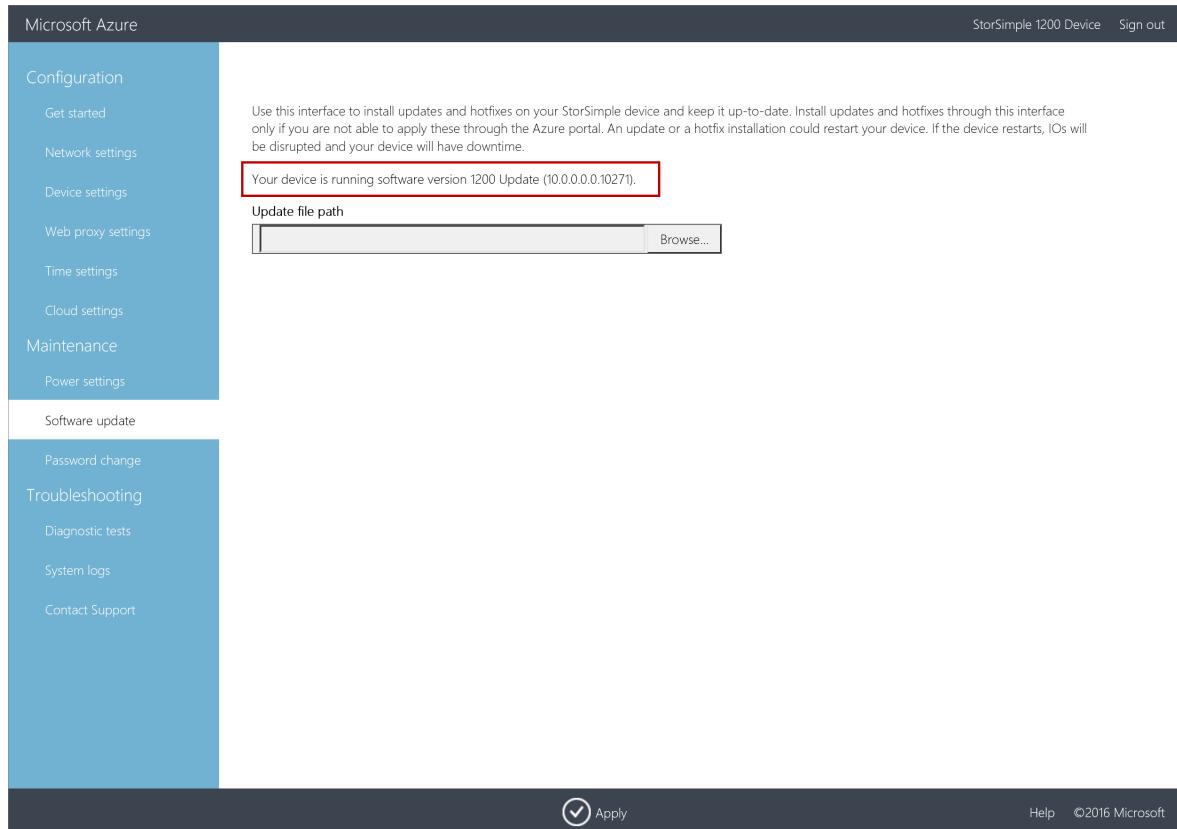
Install the update or the hotfix

Prior to the update or hotfix installation, make sure that you have the update or the hotfix downloaded either locally on your host or accessible via a network share.

Use this method to install updates on a device running GA or Update 0.1 software versions. This procedure takes approximately 12 minutes to complete. Perform the following steps to install the update or hotfix.

To install the update or the hotfix

- In the local web UI, go to **Maintenance > Software Update**. Make a note of the software version that you are running. If you are running **10.0.10290.0**, you do not need to update the MDS agent in step 6.



- In **Update file path**, enter the file name for the update or the hotfix. You can also browse to the update or hotfix installation file if placed on a network share. Click **Apply**.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)[Software update](#)[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime.

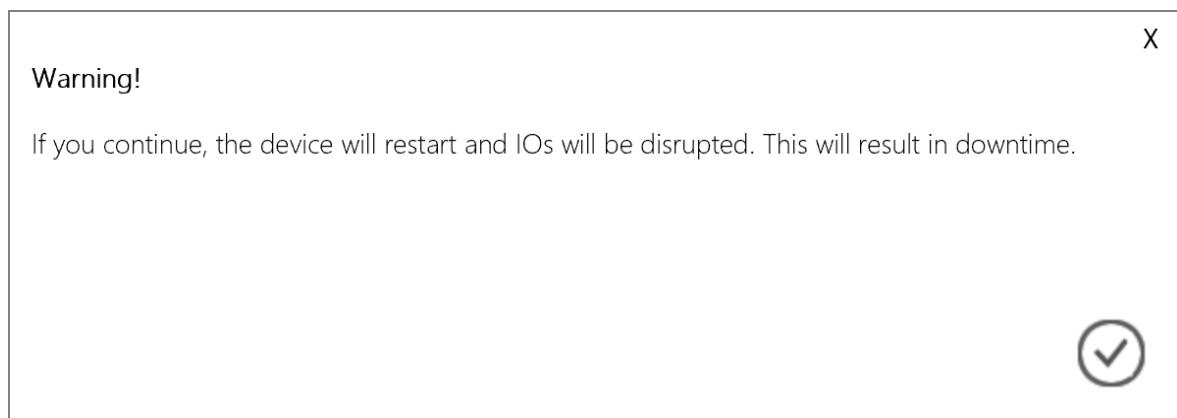
Your device is running software version 1200 Update (10.0.0.0.10271).

Update file path

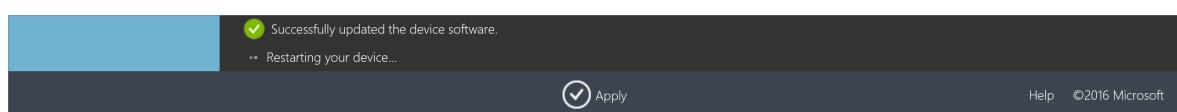
[Browse...](#) [Apply](#)

Help ©2016 Microsoft

3. A warning is displayed. Given the virtual array is a single node device, after the update is applied, the device restarts and there is downtime. Click the check icon.



4. The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.



5. After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has updated, in the local web UI, go to **Maintenance > Software Update**. The displayed software version should be **10.0.0.0.0.10293** for Update 0.6.

! Note

We report the software versions in a slightly different way in the local web UI and the Azure portal. For example, the local web UI reports **10.0.0.0.0.10293** and the Azure portal reports **10.0.10293.0** for the same version.

The screenshot shows the Microsoft Azure interface for a StorSimple 1200 Device. The left sidebar has a blue header 'Configuration' and lists several sections: Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings, Maintenance, Power settings, Software update, Password change, Troubleshooting, Diagnostic tests, System logs, and Contact Support. The 'Software update' section is currently selected. On the right, there's a message: 'Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime.' Below this is a red-bordered box containing the text 'Your device is running software version 1200 Update (10.0.0.0.293)'. There's also a 'Update file path' input field with a 'Browse...' button. At the bottom right are 'Apply' and 'Cancel' buttons, and a copyright notice: 'Help ©2016 Microsoft'.

6. Skip this step if you were running StorSimple Virtual Array Update 0.5 (**10.0.10290.0**) before you applied this update. You made a note of the software version in step 1 before you began to update. If you were running Update 0.5, your MDS agent is already up-to-date .

If you are running a software version prior to Update 0.5, the next step for you is to update the MDS agent. In the **Software Update** page, go to the **Update file path** and browse to the `GenevaMonitoringAgentPackageInstaller.msi` file. Repeat steps 2-4. After the virtual array restarts, sign into the local web UI.

7. Repeat step 2-4 to install the Windows security fixes using files `windows8.1-kb4012213-x64`, `windows8.1-kb3205400-x64`, and `windows8.1-kb4019213-x64`. The virtual array restarts after each install and you need to sign into the local web UI.

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Install Update 0.5 on your StorSimple Virtual Array

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the steps required to install Update 0.5 on your StorSimple Virtual Array via the local web UI and via the Azure portal. You need to apply software updates or hotfixes to keep your StorSimple Virtual Array up-to-date.

Before you apply an update, we recommend that you take the volumes or shares offline on the host first and then the device. This minimizes any possibility of data corruption. After the volumes or shares are offline, you should also take a manual backup of the device.

ⓘ Important

- Update 0.5 corresponds to **10.0.10290.0** software version on your device. For information on what is new in this update, go to [Release notes for Update 0.5](#).
- If you are running Update 0.2 or later, we recommend that you install the updates via the Azure portal. If you are running Update 0.1 or GA software versions, you must use the hotfix method via the local web UI to install Update 0.5.
- Keep in mind that installing an update or hotfix restarts your device. Given that the StorSimple Virtual Array is a single node device, any I/O in progress is

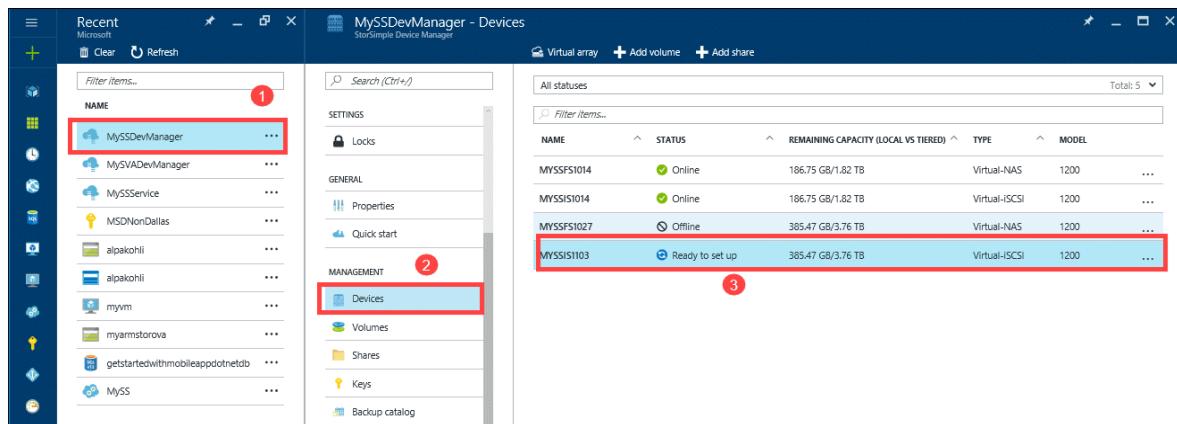
disrupted and your device experiences downtime.

Use the Azure portal

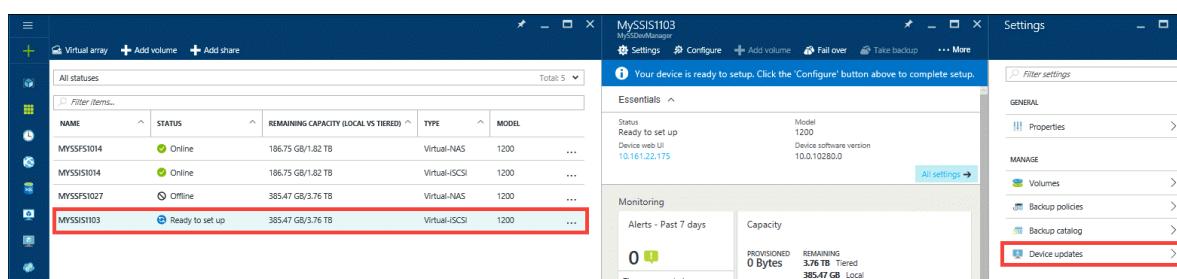
If running Update 0.2 and later, we recommend that you install updates through the Azure portal. The portal procedure requires the user to scan, download, and then install the updates. This procedure takes around 7 minutes to complete. Perform the following steps to install the update or hotfix.

To install updates via the Azure portal

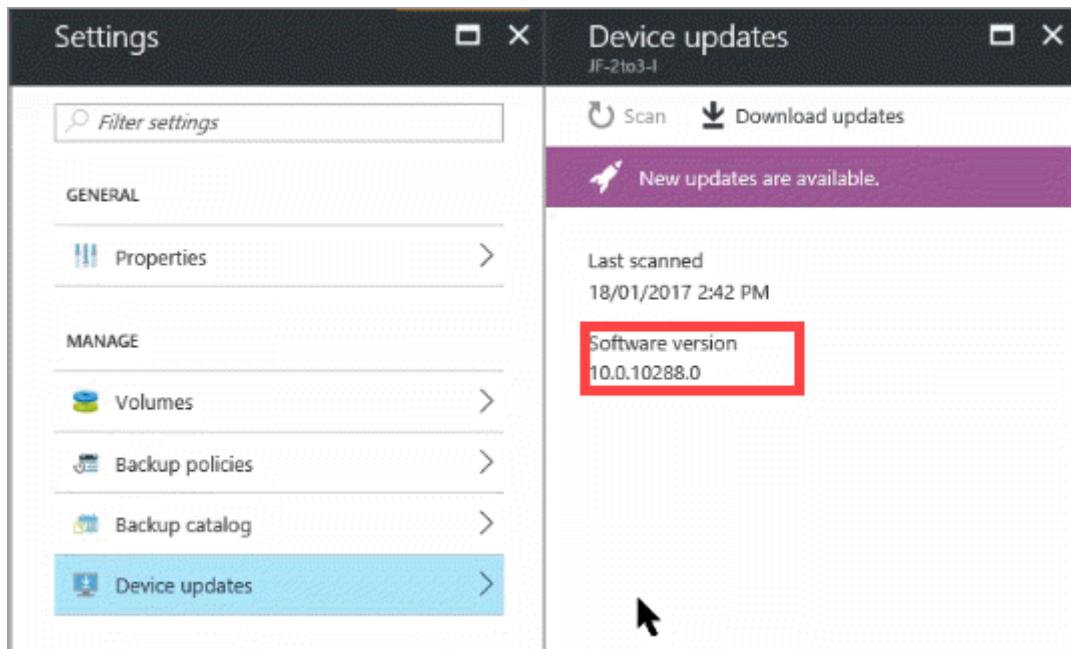
1. Go to your StorSimple Device Manager and select **Devices**. From the list of devices connected to your service, select and click the device you want to update.



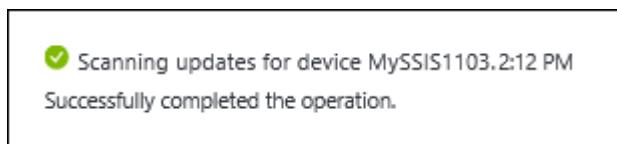
2. In the Settings blade, click **Device updates**.



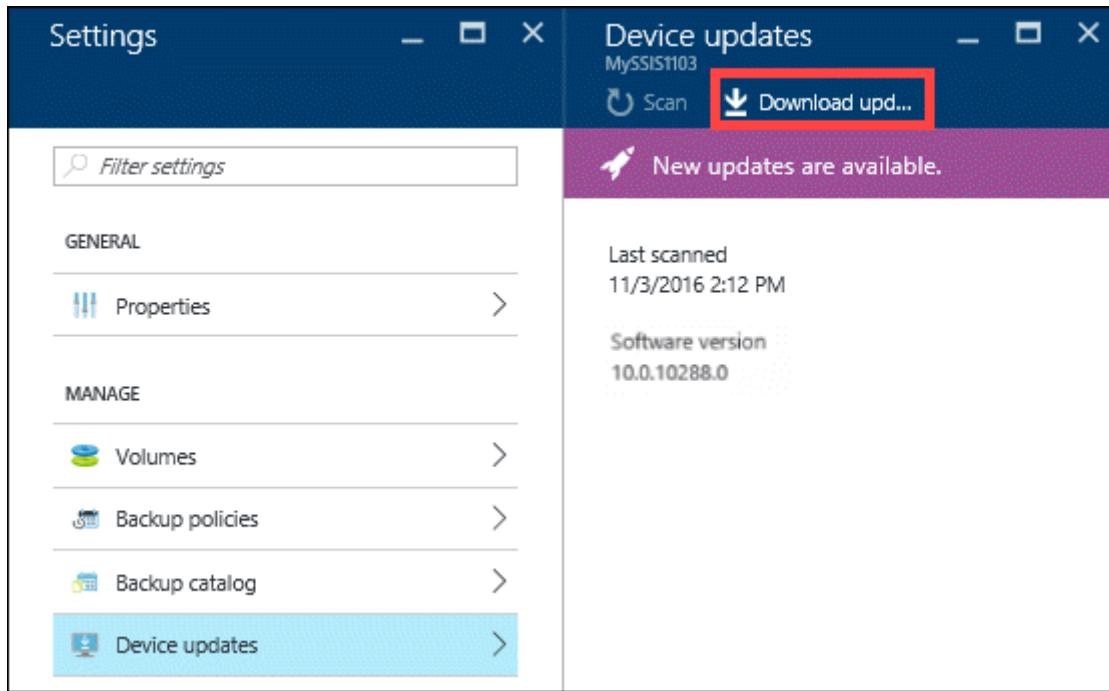
3. You see a message if the software updates are available. To check for updates, you can also click **Scan**.



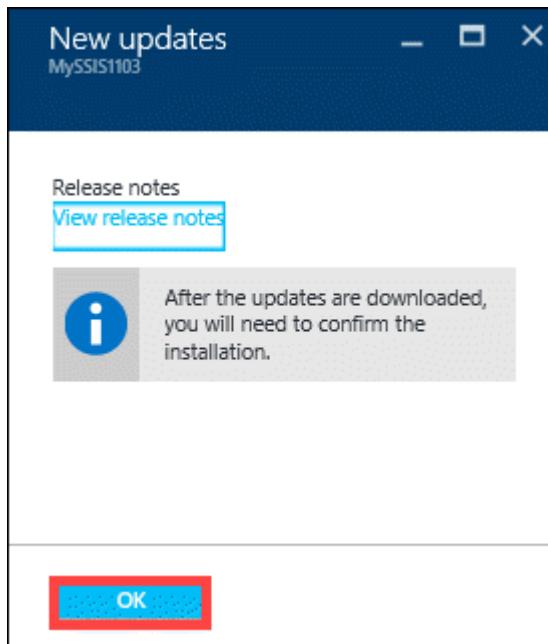
You will be notified when the scan starts and completes successfully.



4. Once the updates are scanned, click **Download updates**.



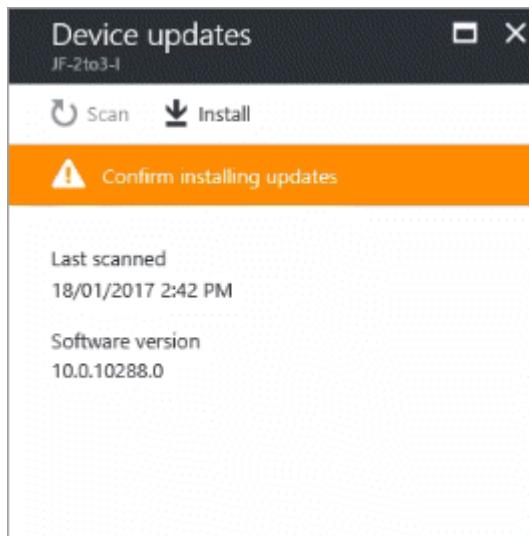
5. In the **New updates** blade, review the information that after the updates are downloaded, you need to confirm the installation. Click **OK**.



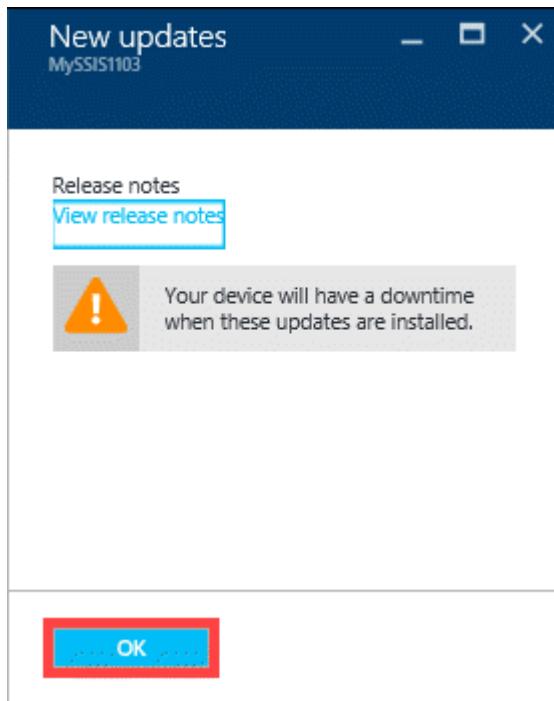
6. You are notified when the upload starts and completes successfully.



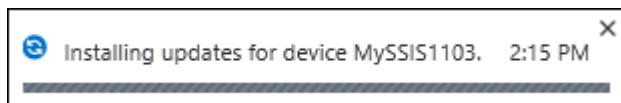
7. In the Device updates blade, click **Install**.



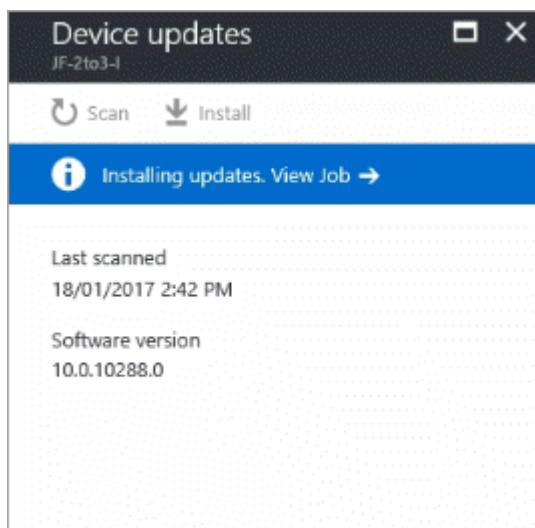
8. In the **New updates** blade, you are warned that the update is disruptive. As virtual array is a single node device, the device restarts after it is updated. This disrupts any IO in progress. Click **OK** to install the updates.



9. You are notified when the install job starts.



10. After the install job completes successfully, click **View Job** link in the **Device updates** blade to monitor the installation.



This takes you to the **Install Updates** blade. You can view detailed information about the job here.

The screenshot shows two windows side-by-side. The left window is titled 'Device updates' and has a tab bar with 'JF-2to3-I'. It contains buttons for 'Scan' and 'Install'. A blue header bar indicates 'Installing updates. View Job →'. Below this, it says 'Last scanned 18/01/2017 2:42 PM' and 'Software version 10.0.10288.0'. The right window is titled 'InstallUpdates Job' and has a 'Refresh' button. It displays 'Details' for a job: Status 'In progress', Entity 'JF-2to3-I (Microsoft.StorSimple/managers/devices)', Device 'JF-2TO3-I', Started on '18/01/2017 14:46:34', Completed on ' - ', and Duration '2 Minutes, 8 Seconds'.

11. After the updates are successfully installed, you see a message to this effect in the **Device updates** blade.

After the installation is complete, go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you just updated. Go to **Settings > Manage > Device Updates**. The displayed software version should be **10.0.10290.0**.

Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

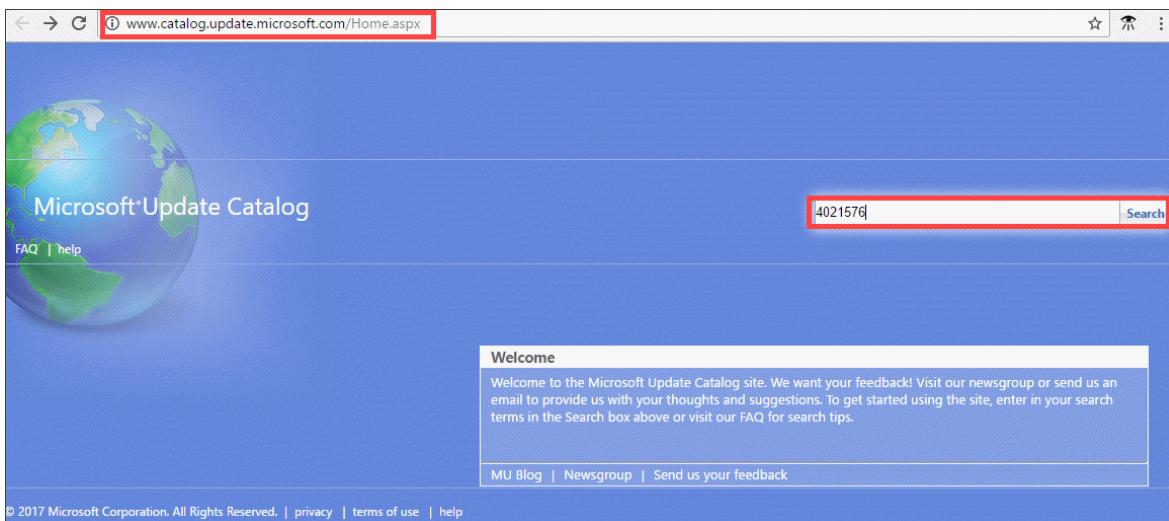
Download the update or the hotfix

Perform the following steps to download the software update from the Microsoft Update Catalog.

To download the update or the hotfix

1. Start Internet Explorer and navigate to <https://catalog.update.microsoft.com>.
2. If this is your first time using the Microsoft Update Catalog on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.
3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download. Enter **4021576** for Update 0.5, and then click **Search**.

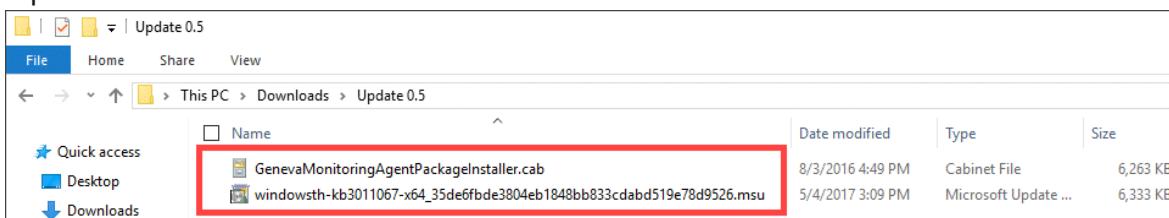
The hotfix listing appears, for example, **StorSimple Virtual Array Update 0.5**.



4. Click Download.

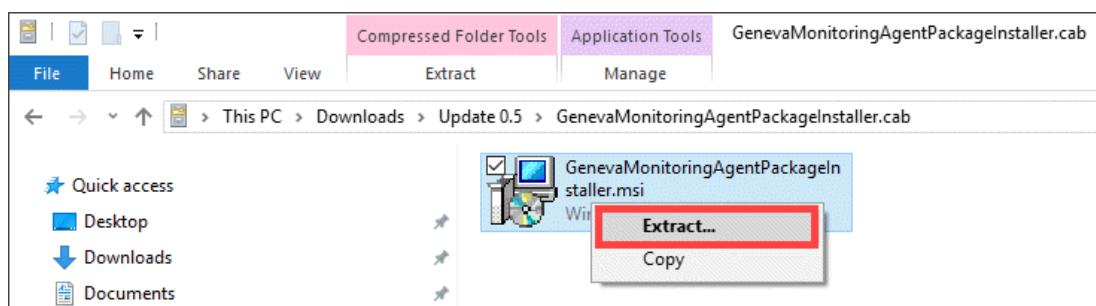
5. You should see two files to download, a *.msu* and a *.cab* file. Download each of those files to a folder. The folder can also be copied to a network share that is reachable from the device.

6. Open the folder where the files are located.



You see:

- A Microsoft Update Standalone Package file `WindowsTH-KB3011067-x64`. This file is used to update the device software.
- A Geneva Monitoring Agent Package file `GenevaMonitoringAgentPackageInstaller`. This file is used to update the Monitoring and Diagnostics service (MDS) agent. Double-click the cab file. A *.msi* is displayed. Select the file, right-click, and then **Extract** the file. You will use the *.msi* file to update the agent.



Install the update or the hotfix

Prior to the update or hotfix installation, make sure that you have the update or the hotfix downloaded either locally on your host or accessible via a network share.

Use this method to install updates on a device running GA or Update 0.1 software versions. This procedure takes less than 2 minutes to complete. Perform the following steps to install the update or hotfix.

To install the update or the hotfix

1. In the local web UI, go to **Maintenance > Software Update**.

The screenshot shows the Microsoft Azure interface for a StorSimple 1200 Device. The left sidebar has a blue background and lists various maintenance options: Configuration (Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Software update), and Troubleshooting (Password change, Diagnostic tests, System logs, Contact Support). The main content area has a white background. It displays a message: "Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime." Below this message, a red box highlights the "Update file path" input field, which contains the text "Your device is running software version 1200 Update (10.0.0.0.10271)". To the right of the input field is a "Browse..." button. At the bottom of the page, there is a dark footer bar with a "Apply" button containing a checkmark icon, and text indicating "Help ©2016 Microsoft".

2. In **Update file path**, enter the file name for the update or the hotfix. You can also browse to the update or hotfix installation file if placed on a network share. Click **Apply**.

Configuration

- Get started
 - Network settings
 - Device settings
 - Web proxy settings
 - Time settings
 - Cloud settings
- Maintenance
- Power settings
- Software update

Password change

Troubleshooting

- Diagnostic tests
 - System logs
- Contact Support

Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime.

Your device is running software version 1200 Update (10.0.0.0.10271).

Update file path

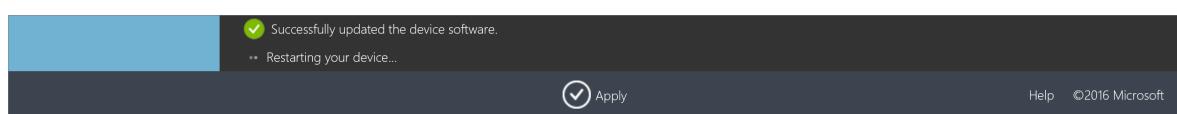
[Browse...](#) Apply

Help ©2016 Microsoft

3. A warning is displayed. Given this is a single node device, after the update is applied, the device restarts and there is downtime. Click the check icon.



4. The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.



5. After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has updated, in the local web UI, go to **Maintenance > Software Update**. The displayed software version should be **10.0.0.0.10290.0** for Update 0.5.

! Note

We report the software versions in a slightly different way in the local web UI and the Azure portal. For example, the local web UI reports **10.0.0.0.0.10290** and the Azure portal reports **10.0.10290.0** for the same version.

The screenshot shows the Microsoft Azure StorSimple 1200 Device configuration interface. The left sidebar has a blue header "Configuration" and lists several options: Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings, Maintenance, Power settings, Software update, Password change, Troubleshooting, Diagnostic tests, System logs, and Contact Support. The "Software update" section is currently selected. On the right, there is a message: "Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime." Below this, a red box highlights the message "Your device is running software version 1200 Update (10.0.0.0.0.10290)." There is also a "Update file path" input field with a "Browse..." button. At the bottom, there is an "Apply" button with a checkmark icon and a "Help" link.

6. The next step is to update the MDS agent. In the **Software Update** page, go to the **Update file path** and browse to the `GenevaMonitoringAgentPackageInstaller.msi` file. Repeat steps 2-4. After the virtual array restarts, sign into the local web UI.

The update is now complete.

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Install Update 0.4 on your StorSimple Virtual Array

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the steps required to install Update 0.4 on your StorSimple Virtual Array via the local web UI and via the Azure portal. You need to apply software updates or hotfixes to keep your StorSimple Virtual Array up-to-date.

Keep in mind that installing an update or hotfix restarts your device. Given that the StorSimple Virtual Array is a single node device, any I/O in progress is disrupted and your device experiences downtime.

Before you apply an update, we recommend that you take the volumes or shares offline on the host first and then the device. This minimizes any possibility of data corruption.

ⓘ Important

If you are running Update 0.1 or GA software versions, you must use the hotfix method via the local web UI to install update 0.3. If you are running Update 0.2 or later, we recommend that you install the updates via the Azure portal.

Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

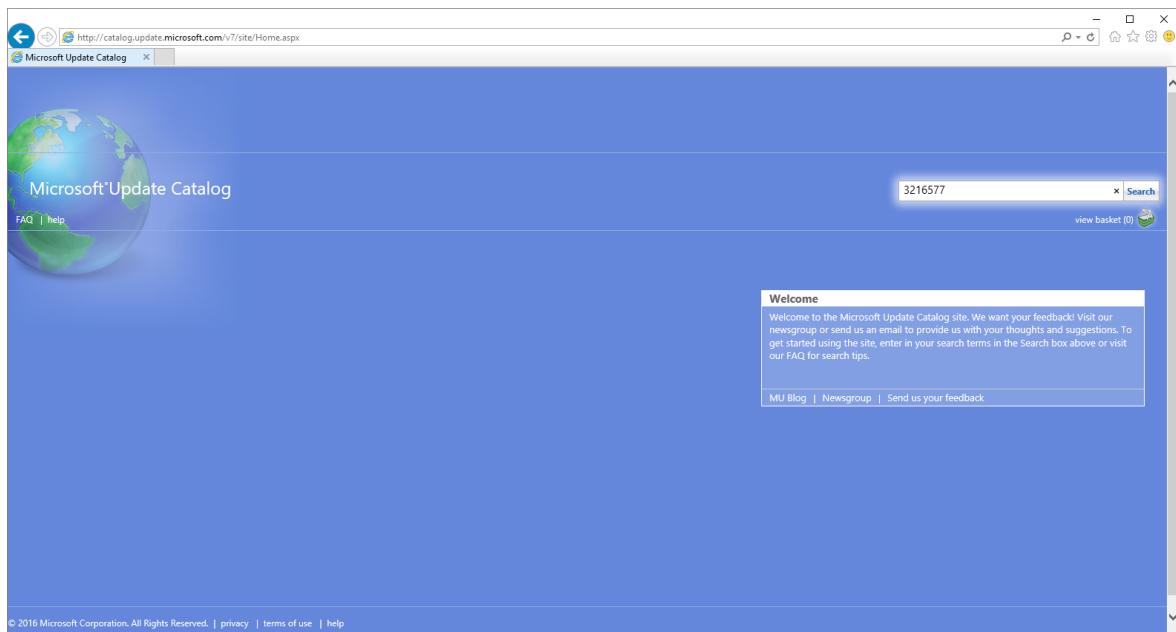
Download the update or the hotfix

Perform the following steps to download the software update from the Microsoft Update Catalog.

To download the update or the hotfix

1. Start Internet Explorer and navigate to <https://catalog.update.microsoft.com>.
2. If this is your first time using the Microsoft Update Catalog on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.
3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download. Enter **3216577** for Update 0.4, and then click **Search**.

The hotfix listing appears, for example, **StorSimple Virtual Array Update 0.4**.



4. Click **Add**. The update is added to the basket.
5. Click **View Basket**.
6. Click **Download**. Specify or **Browse** to a local location where you want the downloads to appear. The updates are downloaded to the specified location and placed in a subfolder with the same name as the update. The folder can also be copied to a network share that is reachable from the device.
7. Open the copied folder, you should see a Microsoft Update Standalone Package file WindowsTH-KB3011067-x64. This file is used to install the update or hotfix.

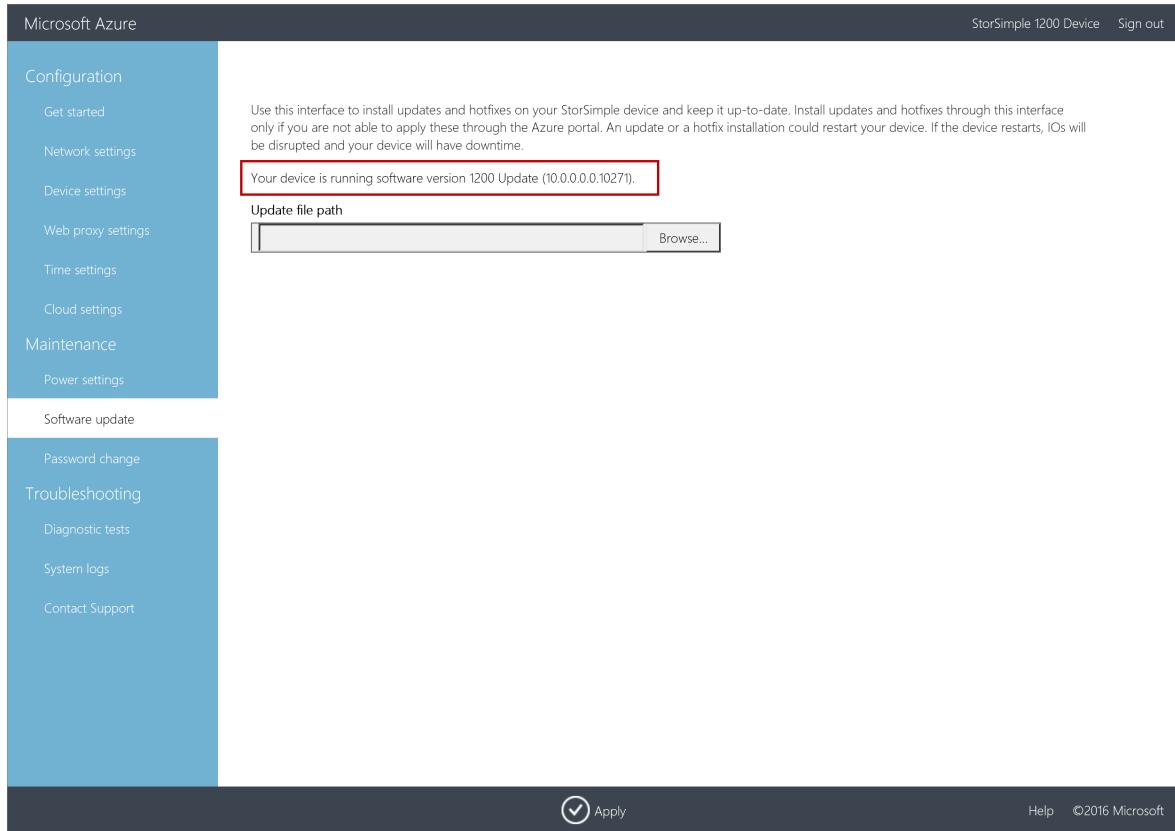
Install the update or the hotfix

Prior to the update or hotfix installation, make sure that you have the update or the hotfix downloaded either locally on your host or accessible via a network share.

Use this method to install updates on a device running GA or Update 0.1 software versions. This procedure takes less than 2 minutes to complete. Perform the following steps to install the update or hotfix.

To install the update or the hotfix

1. In the local web UI, go to **Maintenance > Software Update**.



2. In **Update file path**, enter the file name for the update or the hotfix. You can also browse to the update or hotfix installation file if placed on a network share. Click **Apply**.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)

Software update

[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime.

Your device is running software version 1200 Update (10.0.0.0.10271).

Update file path

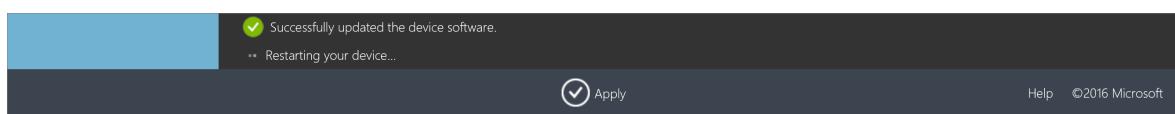
[Browse...](#) Apply

Help ©2016 Microsoft

3. A warning is displayed. Given this is a single node device, after the update is applied, the device restarts and there is downtime. Click the check icon.



4. The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.



5. After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has updated, in the local web UI, go to **Maintenance > Software Update**. The displayed software version should be **10.0.0.0.10289.0** for Update 0.4.

! Note

We report the software versions in a slightly different way in the local web UI and the Azure portal. For example, the local web UI reports **10.0.0.0.0.10289** and the Azure portal reports **10.0.10289.0** for the same version.

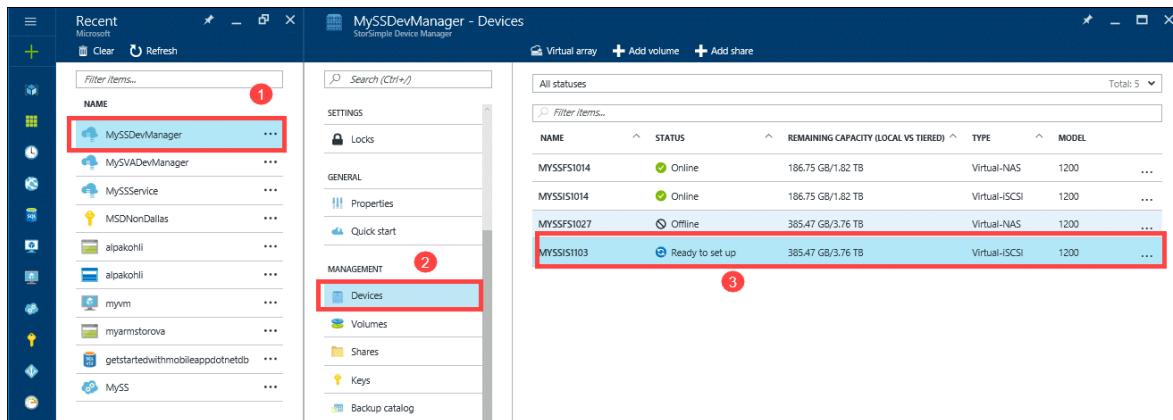
The screenshot shows the Microsoft Azure StorSimple Device Manager interface. The left sidebar has a blue header "Microsoft Azure" and a dark blue footer. The main content area has a white header "StorSimple 1200 Device" and "Sign out". The left sidebar lists several sections: Configuration (Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings), Software update (Password change, Troubleshooting (Diagnostic tests, System logs), Contact Support). The main content area has a message: "Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime." Below this is a red-bordered box containing the text "Your device is running software version 1200 Update (10.0.0.0.0.10287)". There is a "Update file path" input field with a "Browse..." button. At the bottom right are "Apply" and "Cancel" buttons, and copyright information: "Help ©2016 Microsoft".

Use the Azure portal

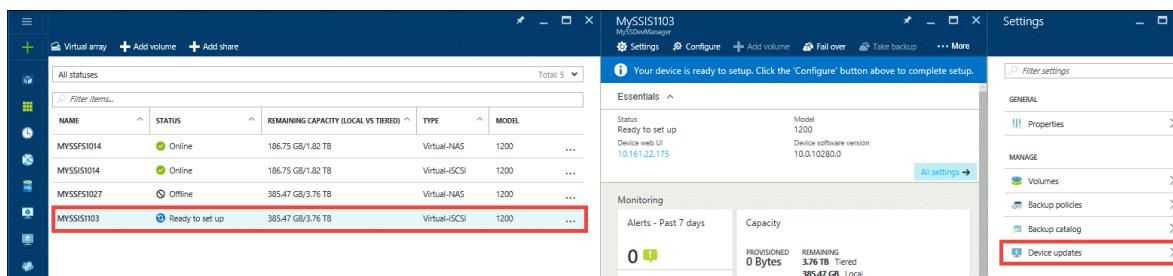
If running Update 0.2 and later, we recommend that you install updates through the Azure portal. The portal procedure requires the user to scan, download, and then install the updates. This procedure takes around 7 minutes to complete. Perform the following steps to install the update or hotfix.

To install updates via the Azure portal

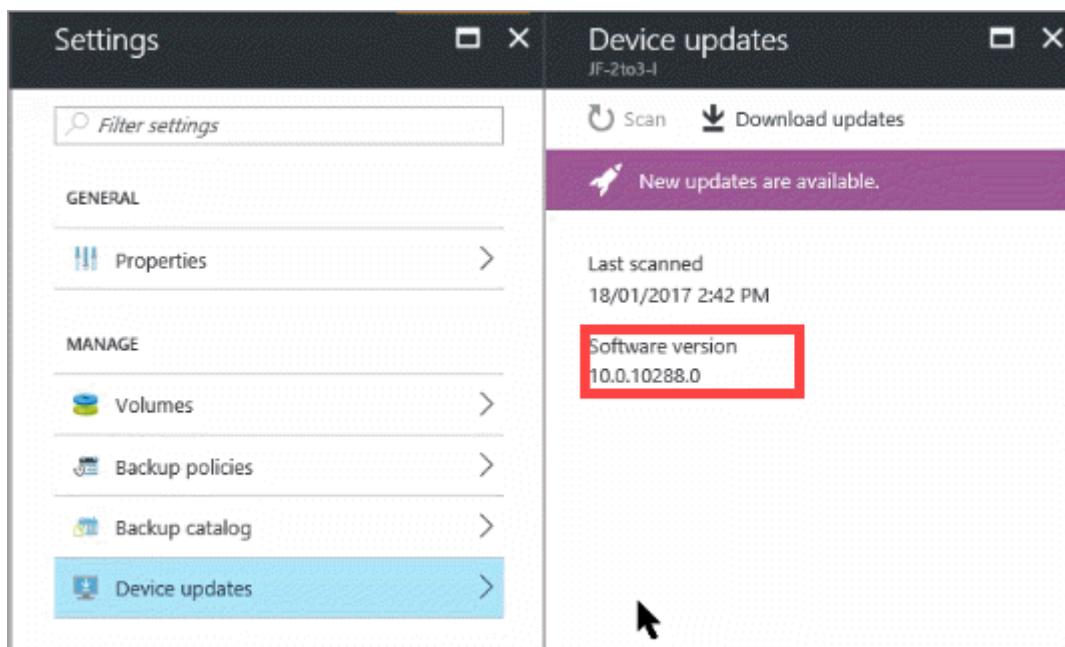
1. Go to your StorSimple Device Manager and select **Devices**. From the list of devices connected to your service, select and click the device you want to update.



2. In the Settings blade, click Device updates.



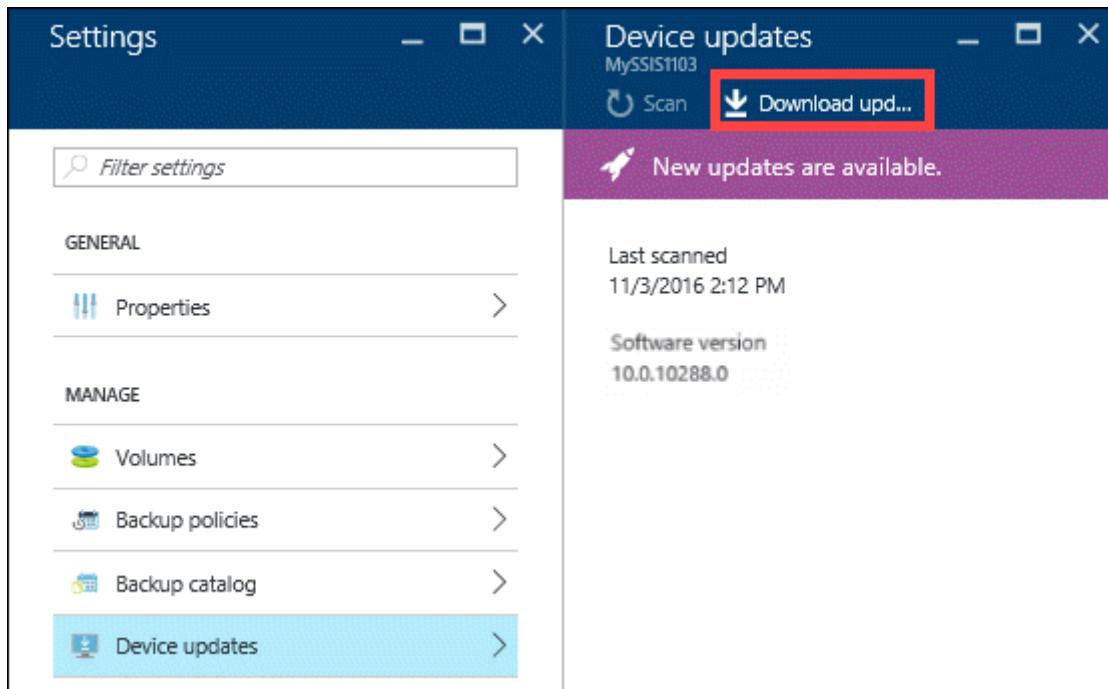
3. You see a message if the software updates are available. To check for updates, you can also click Scan.



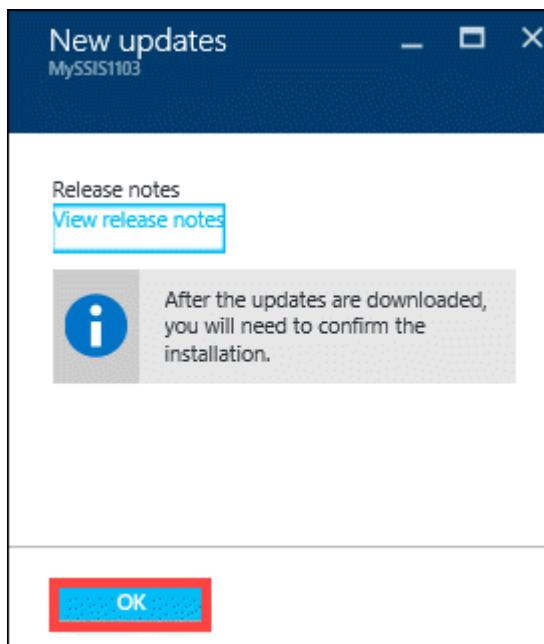
You will be notified when the scan starts and completes successfully.

Scanning updates for device MySS1103. 2:12 PM
Successfully completed the operation.

4. Once the updates are scanned, click Download updates.



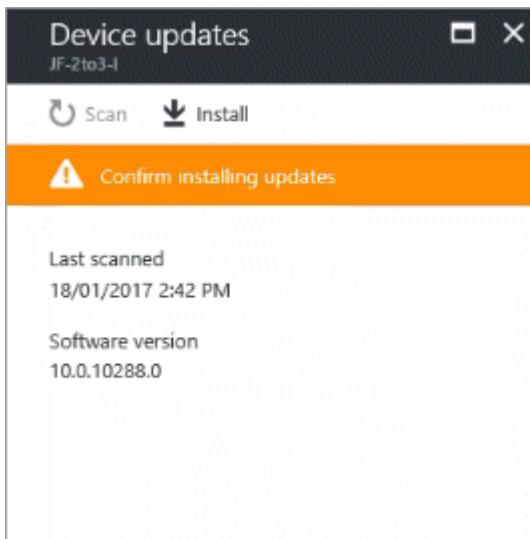
5. In the **New updates** blade, review the information that after the updates are downloaded, you need to confirm the installation. Click **OK**.



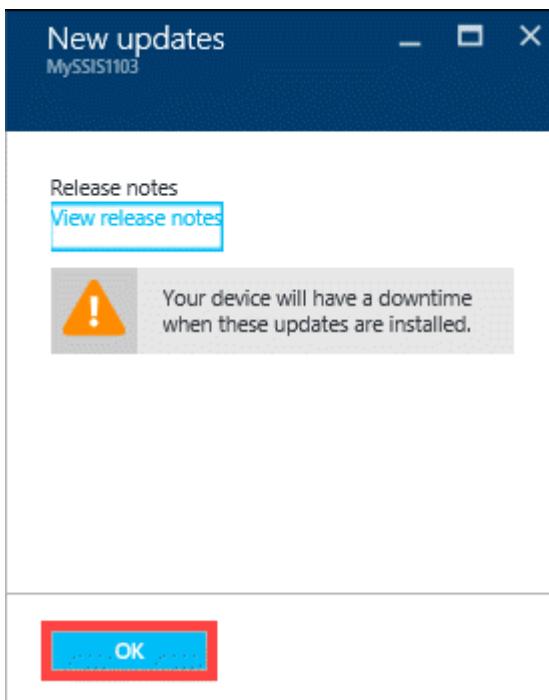
6. You are notified when the upload starts and completes successfully.



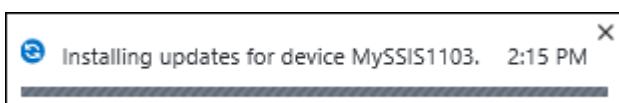
7. In the **Device updates** blade, click **Install**.



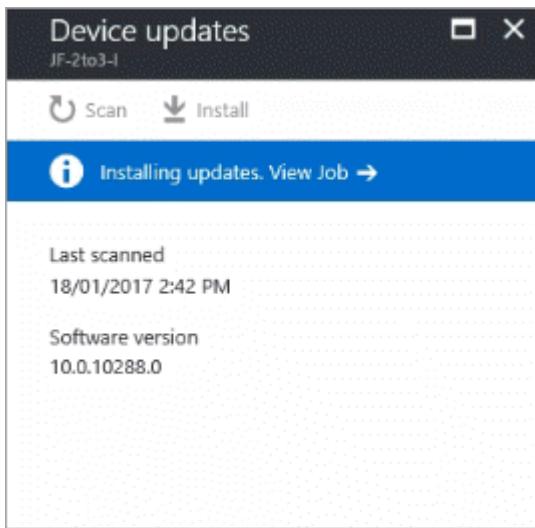
8. In the **New updates** blade, you are warned that the update is disruptive. As virtual array is a single node device, the device restarts after it is updated. This disrupts any IO in progress. Click **OK** to install the updates.



9. You are notified when the install job starts.



10. After the install job completes successfully, click **View Job** link in the **Device updates** blade to monitor the installation.



This takes you to the **Install Updates** blade. You can view detailed information about the job here.

A screenshot of a software interface titled "Device updates" (JF-2to3-I) on the left and "InstallUpdates" (Job) on the right. The left pane is identical to the previous screenshot. The right pane contains a "Details" section with the following data:

Detail	Value
Status	In progress
Entity	JF-2to3-I (Microsoft.StorSimple/managers/devices)
Device	JF-2TO3-I
Started on	18/01/2017 14:46:34
Completed on	-
Duration	2 Minutes, 8 Seconds

11. After the updates are successfully installed, you see a message to this effect in the **Device updates** blade.

After the installation is complete (as indicated by job status at 100 %), go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you want to update from the list of devices connected to this service. In the **Settings** blade, go to **Manage** section and select **Device updates**. The displayed software version should be 10.0.10289.0.

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Install Updates on your StorSimple Virtual Array - Azure portal

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the steps required to install updates on your StorSimple Virtual Array via the local web UI and via the Azure portal. You need to apply software updates or hotfixes to keep your StorSimple Virtual Array up-to-date.

Keep in mind that installing an update or hotfix restarts your device. Given that the StorSimple Virtual Array is a single node device, any I/O in progress is disrupted and your device experiences downtime.

Before you apply an update, we recommend that you take the volumes or shares offline on the host first and then the device. This minimizes any possibility of data corruption.

ⓘ Important

If you are running Update 0.1 or GA software versions, you must use the hotfix method via the local web UI to install update 0.3. If you are running Update 0.2, we recommend that you install the updates via the Azure classic portal.

Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

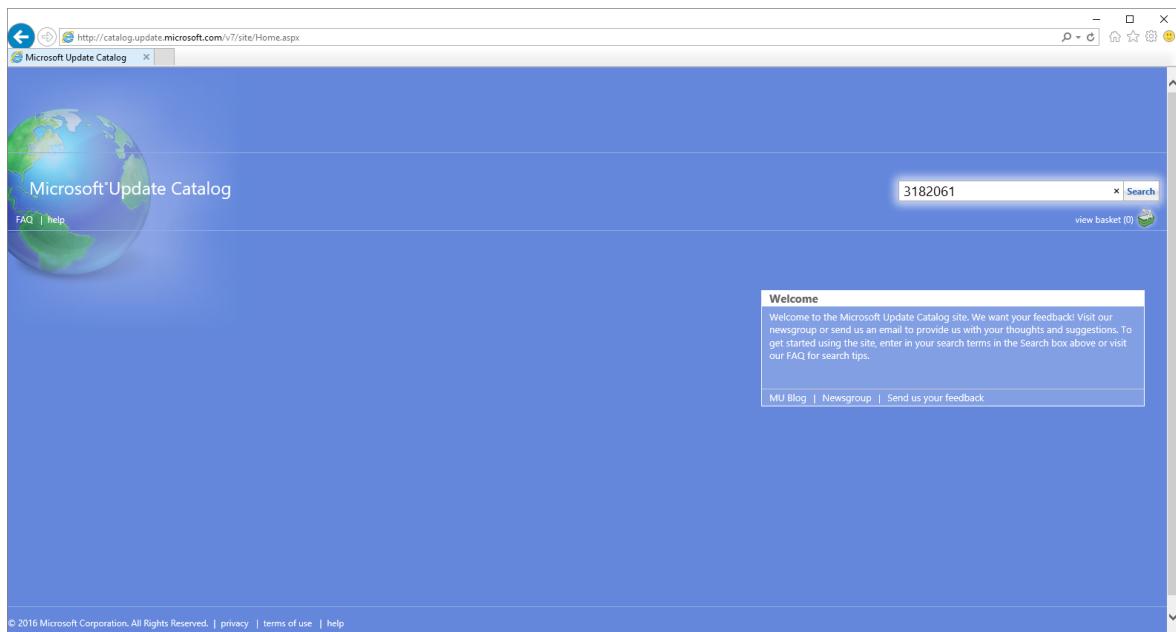
Download the update or the hotfix

Perform the following steps to download the software update from the Microsoft Update Catalog.

To download the update or the hotfix

1. Start Internet Explorer and navigate to <https://catalog.update.microsoft.com>.
2. If this is your first time using the Microsoft Update Catalog on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.
3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download. Enter **3182061** for Update 0.3, and then click **Search**.

The hotfix listing appears, for example, **StorSimple Virtual Array Update 0.3**.



4. Click **Add**. The update is added to the basket.
5. Click **View Basket**.
6. Click **Download**. Specify or **Browse** to a local location where you want the downloads to appear. The updates are downloaded to the specified location and placed in a subfolder with the same name as the update. The folder can also be copied to a network share that is reachable from the device.
7. Open the copied folder, you should see a Microsoft Update Standalone Package file WindowsTH-KB3011067-x64. This file is used to install the update or hotfix.

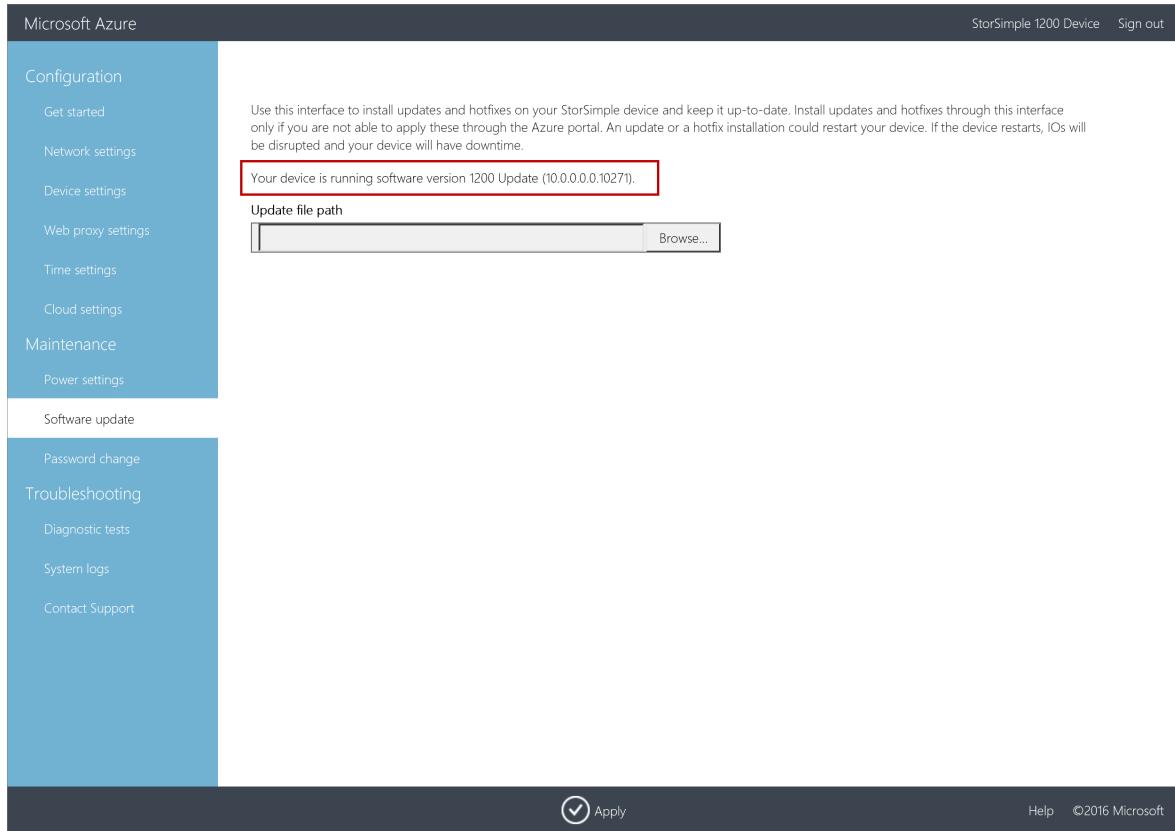
Install the update or the hotfix

Prior to the update or hotfix installation, make sure that you have the update or the hotfix downloaded either locally on your host or accessible via a network share.

Use this method to install updates on a device running GA or Update 0.1 software versions. This procedure takes less than 2 minutes to complete. Perform the following steps to install the update or hotfix.

To install the update or the hotfix

1. In the local web UI, go to **Maintenance > Software Update**.



2. In **Update file path**, enter the file name for the update or the hotfix. You can also browse to the update or hotfix installation file if placed on a network share. Click **Apply**.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)[Software update](#)[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime.

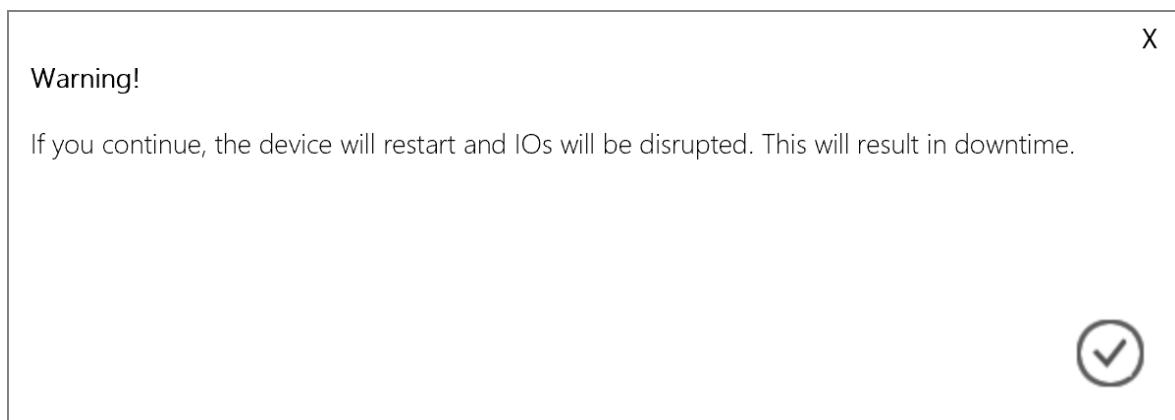
Your device is running software version 1200 Update (10.0.0.0.10271).

Update file path

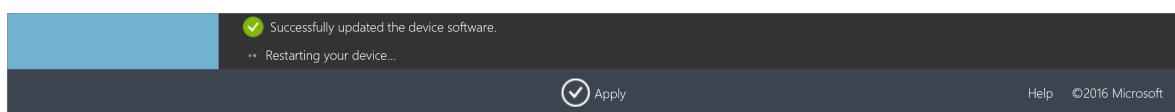
[Browse...](#) Apply

Help ©2016 Microsoft

3. A warning is displayed. Given this is a single node device, after the update is applied, the device restarts and there is downtime. Click the check icon.



4. The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.



5. After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has updated, in the local web UI, go to **Maintenance > Software Update**. The displayed software version should be **10.0.0.0.0.10288.0** for Update 0.3.

! Note

We report the software versions in a slightly different way in the local web UI and the Azure portal. For example, the local web UI reports **10.0.0.0.0.10288** and the Azure portal reports **10.0.10288.0** for the same version.

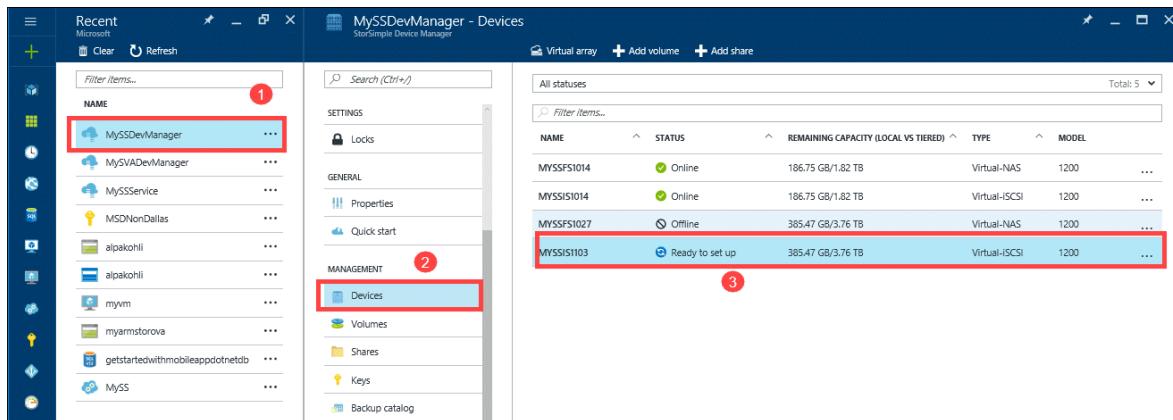
The screenshot shows the Microsoft Azure StorSimple Device Manager interface. The left sidebar has a blue header "Configuration" and a teal header "Software update". Under Configuration, it lists: Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings, Maintenance, and Power settings. Under Software update, it lists: Password change, Troubleshooting, Diagnostic tests, System logs, and Contact Support. The main content area displays a message: "Use this interface to install updates and hotfixes on your StorSimple device and keep it up-to-date. Install updates and hotfixes through this interface only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, IOs will be disrupted and your device will have downtime." Below this is a red-bordered box containing the text "Your device is running software version 1200 Update (10.0.0.0.0.10287)". There is also an "Update file path" input field with a "Browse..." button. At the bottom right are "Apply" and "Cancel" buttons, and copyright information: "Help ©2016 Microsoft".

Use the Azure portal

If running Update 0.2, we recommend that you install updates through the Azure portal. The portal procedure requires the user to scan, download, and then install the updates. This procedure takes around 7 minutes to complete. Perform the following steps to install the update or hotfix.

To install updates via the Azure portal

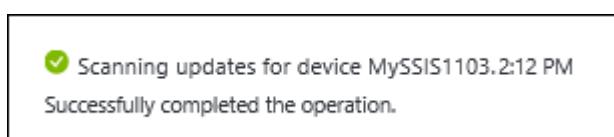
1. Go to your StorSimple Device Manager and select **Devices**. From the list of devices connected to your service, select and click the device you want to update.



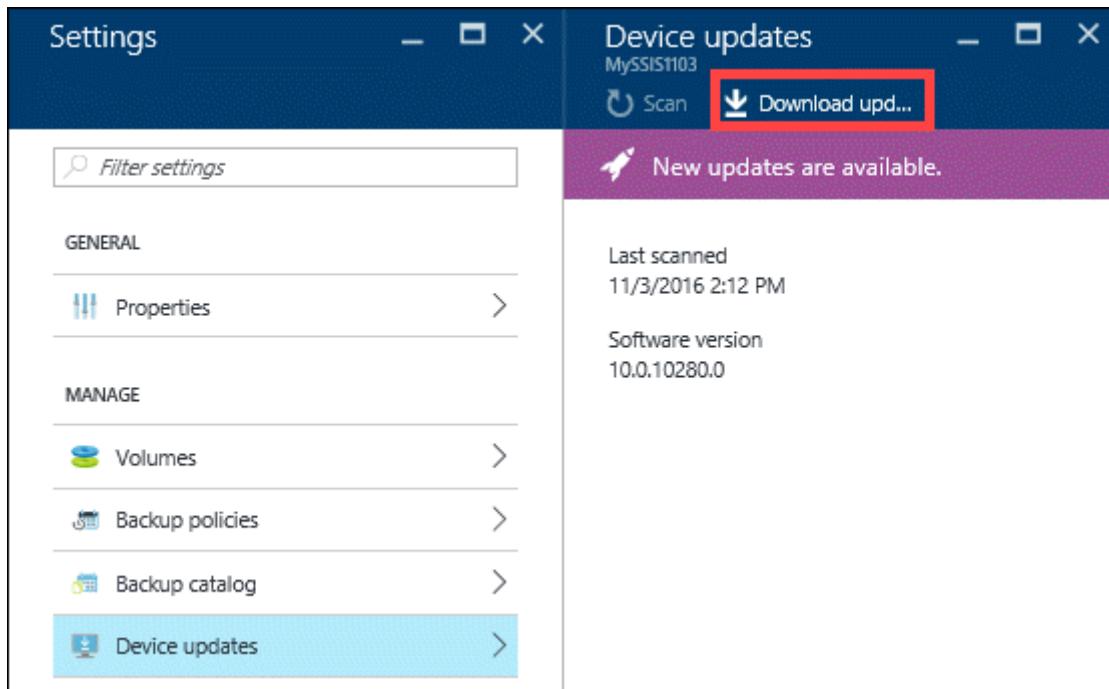
2. In the Settings blade, click Device updates.

3. You see a message if the software updates are available. To check for updates, you can also click Scan.

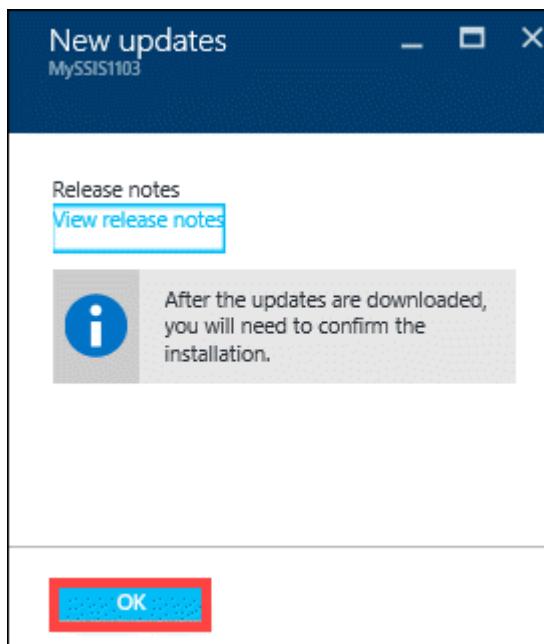
You will be notified when the scan starts and completes successfully.



4. Once the updates are scanned, click Download updates.



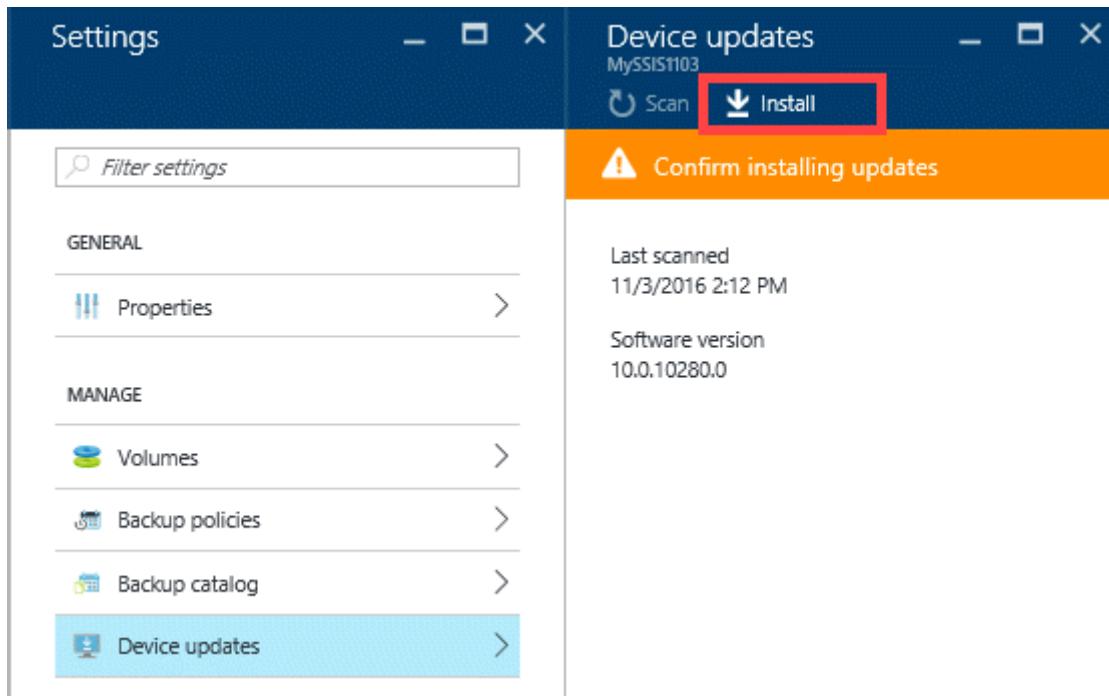
5. In the **New updates** blade, review the information that after the updates are downloaded, you need to confirm the installation. Click **OK**.



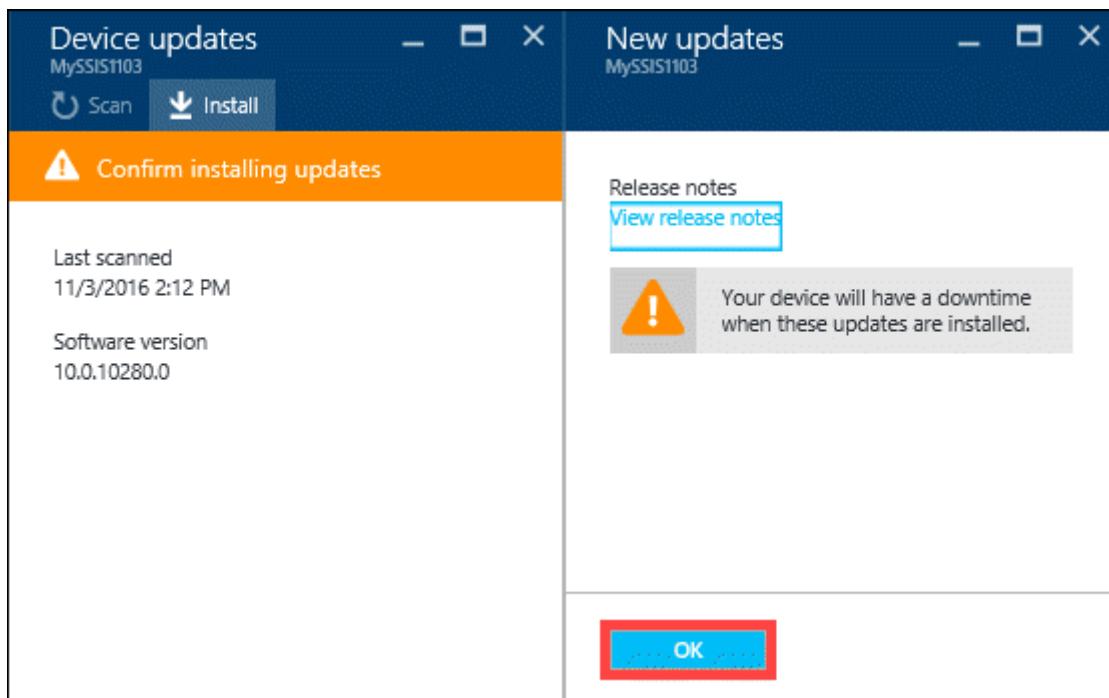
6. You are notified when the upload starts and completes successfully.



7. In the **Device updates** blade, click **Install**.



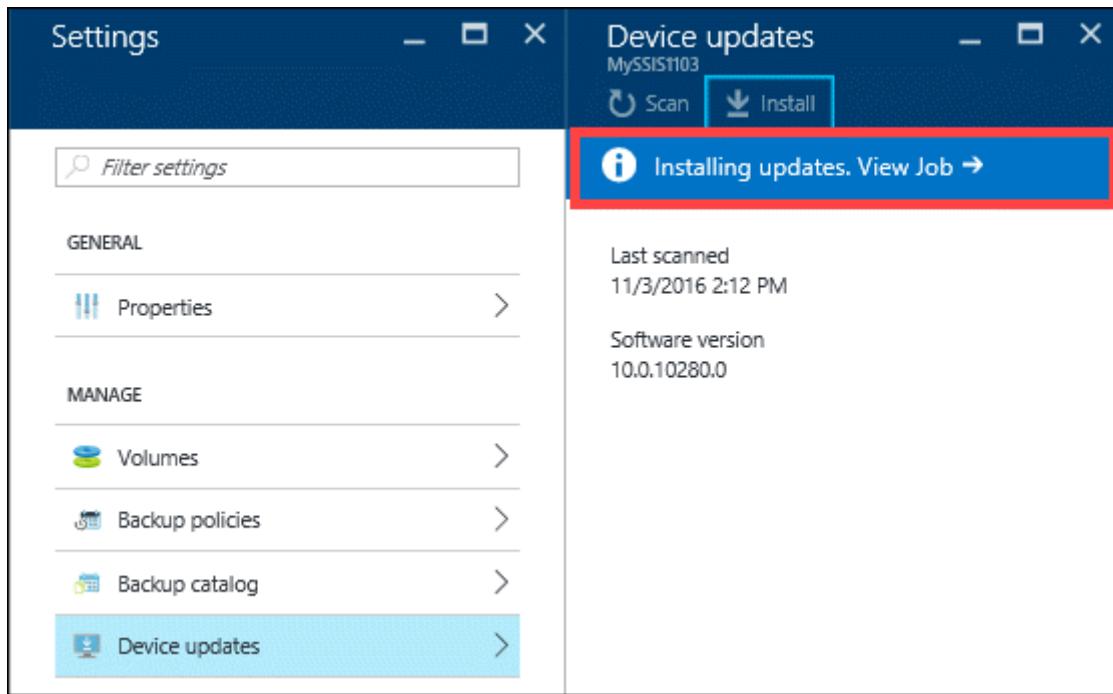
8. In the **New updates** blade, you are warned that the update is disruptive. As virtual array is a single node device, the device restarts after it is updated. This disrupts any IO in progress. Click **OK** to install the updates.



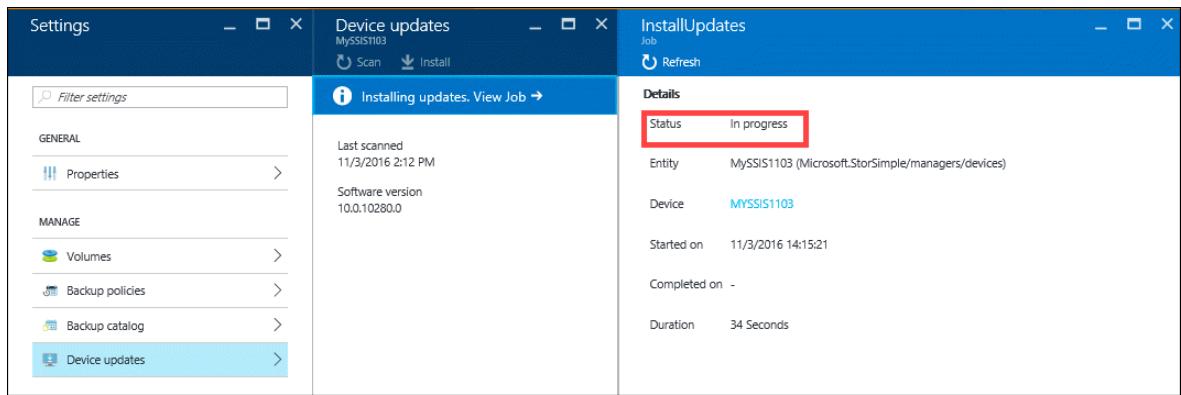
9. You are notified when the install job starts.



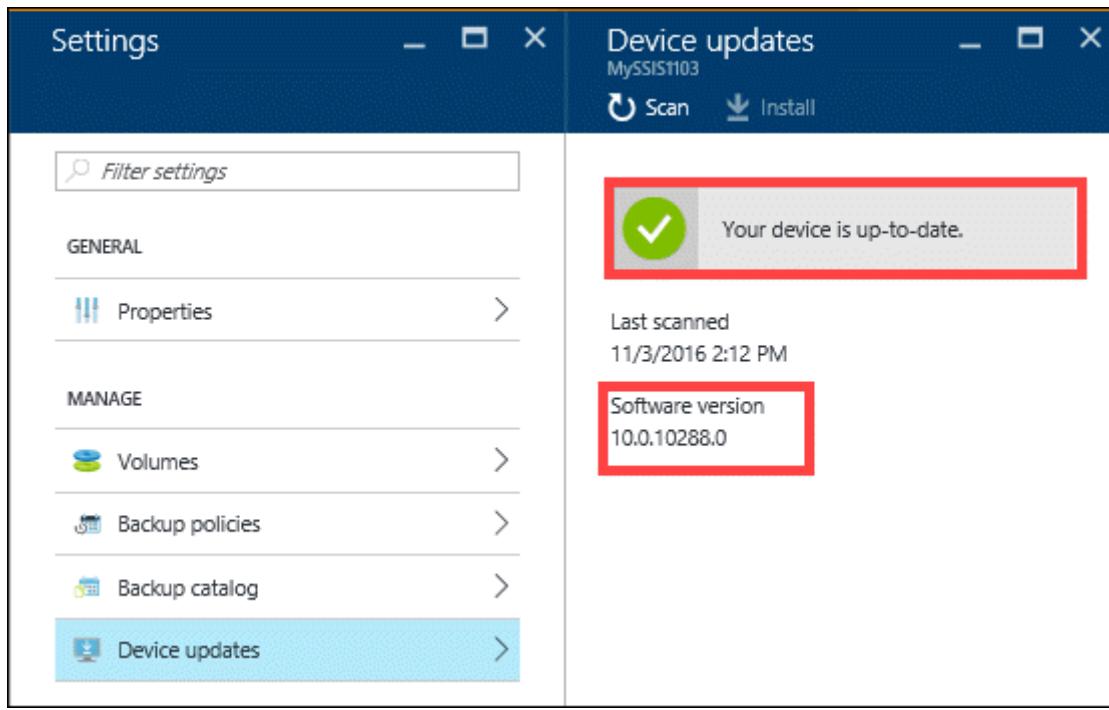
10. After the install job completes successfully, click **View Job** link in the **Device updates** blade to monitor the installation.



This takes you to the **Install Updates** blade. You can view detailed information about the job here.



11. After the updates are successfully installed, you see a message to this effect in the Device updates blade. The software version also changes to 10.0.10288.0.



After the installation is complete (as indicated by job status at 100 %), go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you want to update from the list of devices connected to this service. In the **Settings** blade, go to **Manage** section and select **Device updates**. The displayed software version should be 10.0.10288.0.

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Back up shares or volumes on your StorSimple Virtual Array

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Virtual Array is a hybrid cloud storage on-premises virtual device that can be configured as a file server or an iSCSI server. The virtual array allows the user to create scheduled and manual backups of all the shares or volumes on the device. When configured as a file server, it also allows item-level recovery. This tutorial describes how to create scheduled and manual backups and perform item-level recovery to restore a deleted file on your virtual array.

This tutorial applies to the StorSimple Virtual Arrays only. For information on 8000 series, go to [Create a backup for 8000 series device](#)

Back up shares and volumes

Backups provide point-in-time protection, improve recoverability, and minimize restore times for shares and volumes. You can back up a share or volume on your StorSimple device in two ways: **Scheduled** or **Manual**. Each of the methods is discussed in the following sections.

Change the backup start time

ⓘ Note

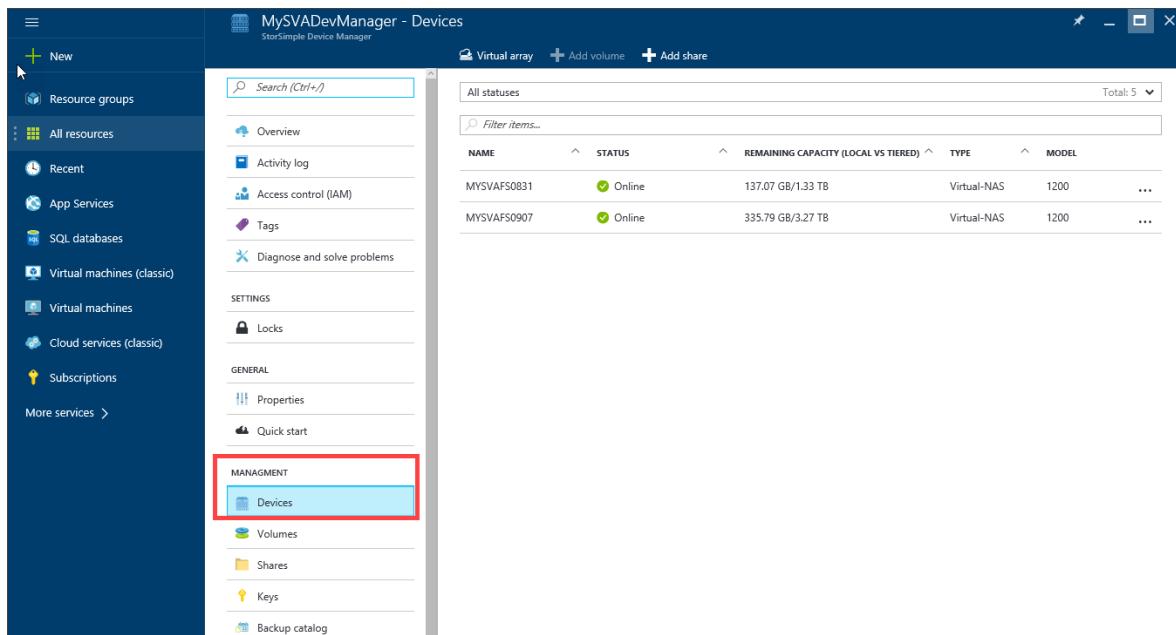
In this release, scheduled backups are created by a default policy that runs daily at a specified time and backs up all the shares or volumes on the device. It is not possible to create custom policies for scheduled backups at this time.

Your StorSimple Virtual Array has a default backup policy that starts at a specified time of day (22:30) and backs up all the shares or volumes on the device once a day. You can change the time at which the backup starts, but the frequency and the retention (which specifies the number of backups to retain) cannot be changed. During these backups, the entire virtual device is backed up. This could potentially impact the performance of the device and affect the workloads deployed on the device. Therefore, we recommend that you schedule these backups for off-peak hours.

To change the default backup start time, perform the following steps in the [Azure portal](#).

To change the start time for the default backup policy

1. Go to **Devices**. The list of devices registered with your StorSimple Device Manager service will be displayed.



2. Select and click your device. The **Settings** blade will be displayed. Go to **Manage > Backup policies**.

3. In the **Backup policies** blade, the default start time is 22:30. You can specify the new start time for the daily schedule in device time zone.

Settings

Backup policies
MYSVAFS0831

Save **Discard**

Backup is auto enabled for all shares on this device. We suggest you schedule backups during non-peak hours to optimize device performance.

Type
Cloud snapshot

* Daily schedule in device time zone ⓘ
18:00 ✓

Other schedules

Monthly	Last Friday of every month
Yearly	Last Friday of Jan every year

The schedule is configured as per the device time zone, which is:
(UTC-08:00) Pacific Time (US & Canada).

Retention

Daily backups	31 days
Monthly backups	12 months
Yearly backups	10 years

GENERAL

- Properties

MANAGE

- Shares
- Backup policies**
- Backup catalog
- Device updates

MONITOR

- Usage
- Jobs
- Alerts

DEVICE SETTINGS

- General
- Network
- Security

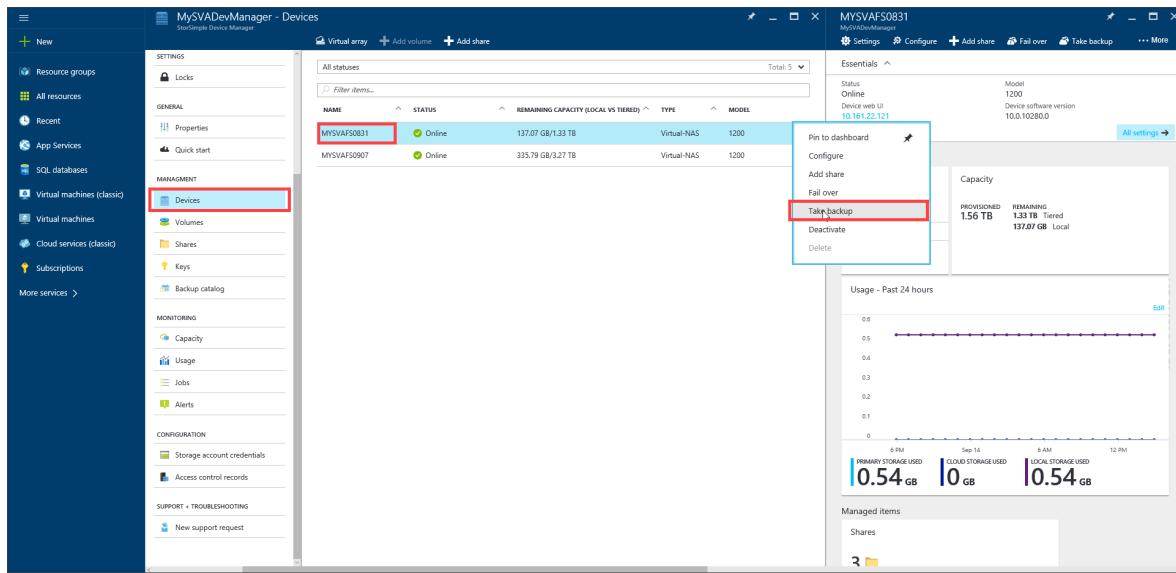
4. Click Save.

Take a manual backup

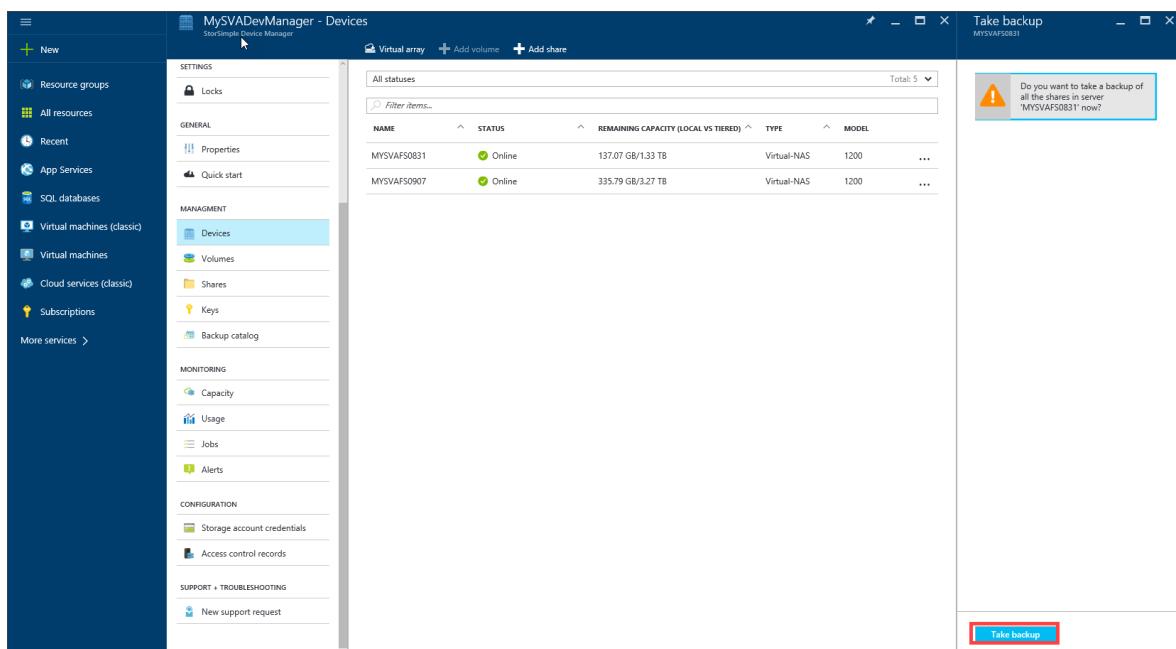
In addition to scheduled backups, you can take a manual (on-demand) backup of device data at any time.

To create a manual backup

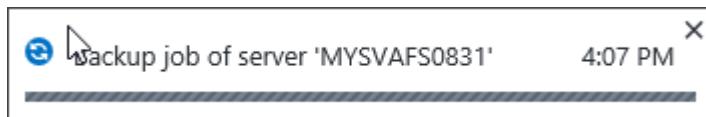
1. Go to Devices. Select your device and right-click ... at the far right in the selected row. From the context menu, select Take backup.



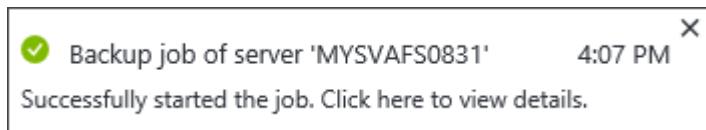
2. In the Take backup blade, click Take backup. This will backup all the shares on the file server or all the volumes on your iSCSI server.



An on-demand backup starts and you see that a backup job has started.



Once the job has successfully completed, you are notified again. The backup process then starts.



3. To track the progress of the backups and look at the job details, click the notification. This takes you to **Job details**.

Details	Value
Status	In progress
Entity	MYSVAFS0831 (Microsoft.StorSimple/managers/devices)
Device	MYSVAFS0831
Started on	9/14/2016 16:07:30
Completed on	-
Duration	27 Seconds

4. After the backup is complete, go to **Management > Backup catalog**. You will see a cloud snapshot of all the shares (or volumes) on your device.

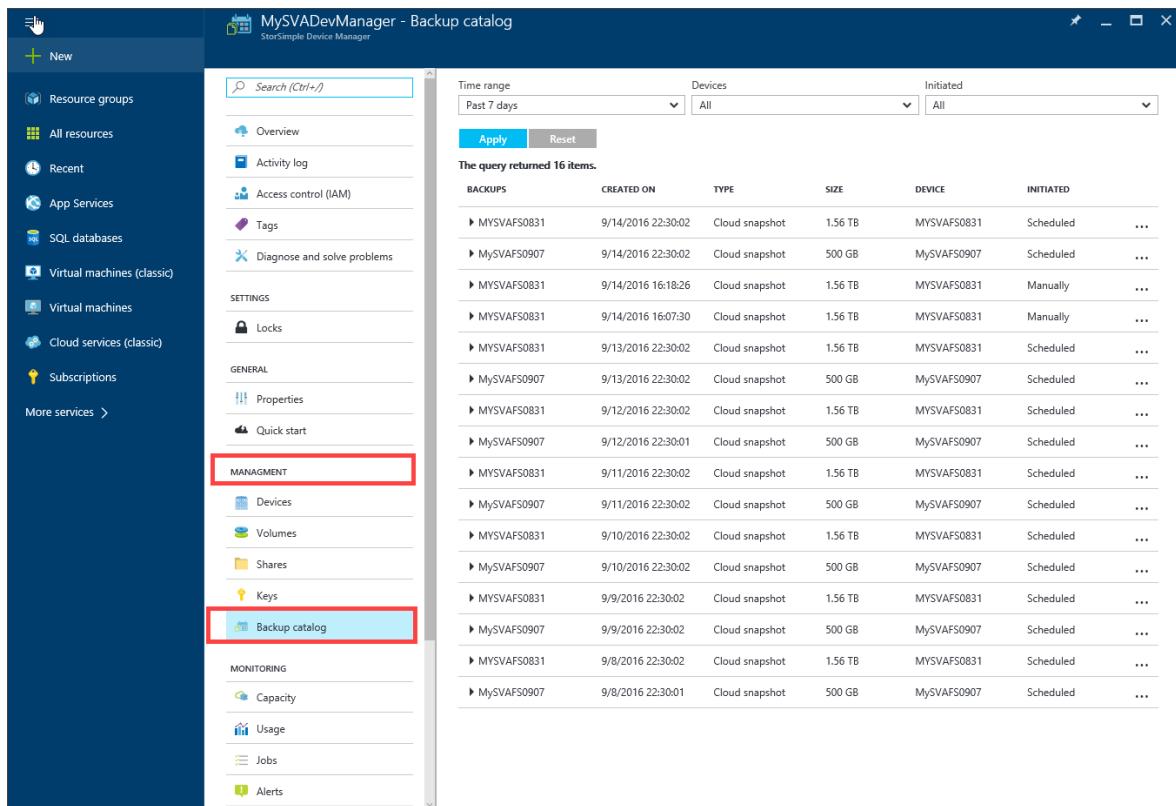
BACKUPS	CREATED ON	TYPE	SIZE	DEVICE	INITIATED
MYSVAFS0831	9/14/2016 16:18:26	Cloud snapshot	1.56 TB	MYSVAFS0831	Manually
MySSEnrgq		Locally pinned	100 GB		
MySSMltg		Tiered	500 GB		
MySSDocs		Tiered	1000 GB		
MYSVAFS0831	9/14/2016 16:07:30	Cloud snapshot	1.56 TB	MYSVAFS0831	Manually
MYSVAFS0831	9/13/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
MySVAF50907	9/13/2016 22:30:02	Cloud snapshot	500 GB	MySVAF50907	Scheduled
MYSVAFS0831	9/12/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
MYSVAFS0831	9/11/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
MYSVAFS0831	9/10/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
MySVAF50907	9/10/2016 22:30:02	Cloud snapshot	500 GB	MySVAF50907	Scheduled
MYSVAFS0831	9/9/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
MySVAF50907	9/9/2016 22:30:02	Cloud snapshot	500 GB	MySVAF50907	Scheduled
MySVAF50907	9/9/2016 22:30:02	Cloud snapshot	500 GB	MySVAF50907	Scheduled

View existing backups

To view the existing backups, perform the following steps in the Azure portal.

To view existing backups

1. Go to Devices blade. Select and click your device. In the **Settings** blade, go to Management > Backup Catalog.



The screenshot shows the Azure portal interface for 'MySVADevManager - Backup catalog'. On the left, there's a sidebar with various service links like Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, and More services. Below this is a 'MANAGEMENT' section with links for Devices, Volumes, Shares, Keys, and Backup catalog. The 'Backup catalog' link is highlighted with a blue box. The main content area shows a table of backup logs with 16 items. The columns are BACKUPS, CREATED ON, TYPE, SIZE, DEVICE, and INITIATED. The first few rows show entries like 'MySVAFS0831' created on 9/14/2016 at 22:30:02, 'MySVAFS0907' created on 9/14/2016 at 22:30:02, and so on. The 'INITIATED' column shows values like 'Scheduled' and 'Manually'.

BACKUPS	CREATED ON	TYPE	SIZE	DEVICE	INITIATED
MySVAFS0831	9/14/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/14/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/14/2016 16:18:26	Cloud snapshot	1.56 TB	MySVAFS0831	Manually
MySVAFS0831	9/14/2016 16:07:30	Cloud snapshot	1.56 TB	MySVAFS0831	Manually
MySVAFS0831	9/13/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/13/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/12/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/12/2016 22:30:01	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/11/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/11/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/10/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/10/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/9/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/9/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
MySVAFS0831	9/8/2016 22:30:02	Cloud snapshot	1.56 TB	MySVAFS0831	Scheduled
MySVAFS0907	9/8/2016 22:30:01	Cloud snapshot	500 GB	MySVAFS0907	Scheduled

2. Specify the following criteria to be used for filtering:

- **Time range** – can be **Past 1 hour**, **Past 24 hours**, **Past 7 days**, **Past 30 days**, **Past year**, and **Custom date**.
- **Devices** – select from the list of file servers or iSCSI servers registered with your StorSimple Device Manager service.
- **Initiated** – can be automatically **Scheduled** (by a backup policy) or **Manually** initiated (by you).

The screenshot shows the 'Backup catalog' blade in the StorSimple Device Manager. On the left is a navigation menu with options like 'Resource groups', 'All resources', 'Recent', etc. The 'Backup catalog' option is selected and highlighted in blue. At the top right, there are filter controls: 'Time range' set to 'Past 7 days', 'Devices' set to 'MYSVAFS0831', and 'Initiated' set to 'Manually'. A red box highlights these filter settings. Below the filters, a message says 'The query returned 16 items.' followed by a table with columns: BACKUPS, CREATED ON, TYPE, SIZE, DEVICE, and INITIATED. The table lists 16 entries, each starting with a right-pointing arrow.

BACKUPS	CREATED ON	TYPE	SIZE	DEVICE	INITIATED
▶ MYSVAFS0831	9/14/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/14/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/14/2016 16:18:26	Cloud snapshot	1.56 TB	MYSVAFS0831	Manually
▶ MYSVAFS0831	9/14/2016 16:07:30	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MYSVAFS0831	9/13/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MYSVAFS0907	9/13/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/12/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/12/2016 22:30:01	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/11/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/11/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/10/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/10/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/9/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/9/2016 22:30:02	Cloud snapshot	500 GB	MySVAFS0907	Scheduled
▶ MYSVAFS0831	9/8/2016 22:30:02	Cloud snapshot	1.56 TB	MYSVAFS0831	Scheduled
▶ MySVAFS0907	9/8/2016 22:30:01	Cloud snapshot	500 GB	MySVAFS0907	Scheduled

3. Click **Apply**. The filtered list of backups is displayed in the **Backup catalog** blade.

Note only 100 backup elements can be displayed at a given time.

This screenshot shows the same 'Backup catalog' blade after applying the filters. The red box from the previous screenshot is still highlighting the filter controls. Now, the message 'The query returned 2 items.' is displayed above a table with two rows. The table has the same columns as before: BACKUPS, CREATED ON, TYPE, SIZE, DEVICE, and INITIATED.

BACKUPS	CREATED ON	TYPE	SIZE	DEVICE	INITIATED
▶ MYSVAFS0831	9/14/2016 16:18:26	Cloud snapshot	1.56 TB	MYSVAFS0831	Manually
▶ MYSVAFS0831	9/14/2016 16:07:30	Cloud snapshot	1.56 TB	MYSVAFS0831	Manually

Next steps

Learn more about [administering your StorSimple Virtual Array](#).

Clone from a backup of your StorSimple Virtual Array

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

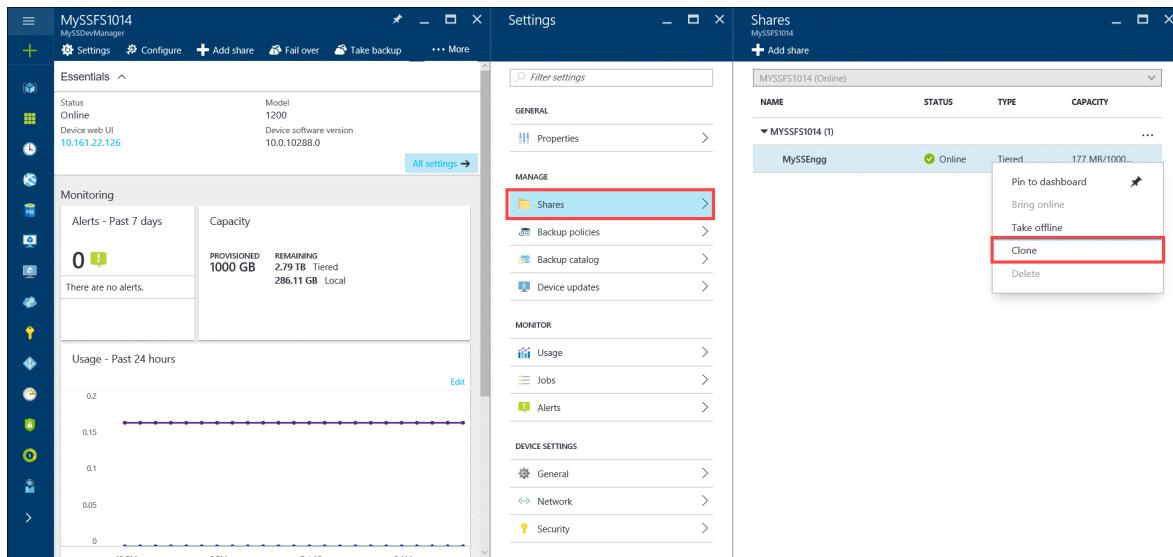
This article describes step-by-step how to clone a backup set of your shares or volumes on your Microsoft Azure StorSimple Virtual Array. The cloned backup is used to recover a deleted or lost file. The article also includes detailed steps to perform an item-level recovery on your StorSimple Virtual Array configured as a file server.

Clone shares from a backup set

Before you try to clone shares, ensure that you have sufficient space on the device to complete this operation. To clone from a backup, in the [Azure portal](#), perform the following steps.

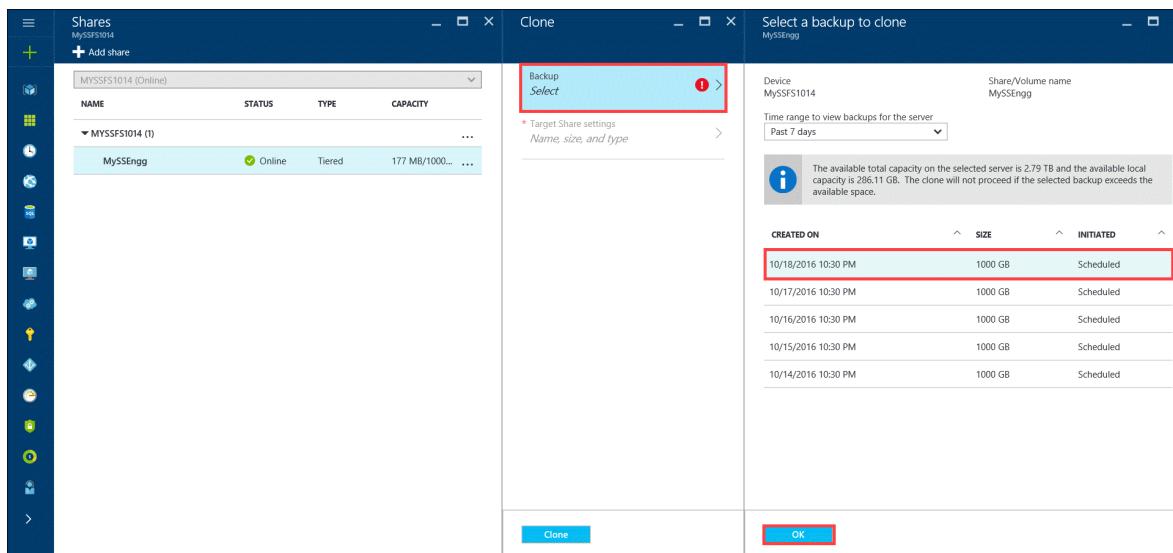
To clone a share

1. Browse to **Devices** blade. Select and click your device and then click **Shares**. Select the share that you want to clone, right-click the share to invoke the context menu. Select **Clone**.



2. In the **Clone** blade, click **Backup > Select** and then do the following:

- Filter a backup on this device based on the time range. You can choose from **Past 7 days**, **Past 30 days**, and **Past year**.
- In the list of filtered backups displayed, select a backup to clone from.
- Click **OK**.

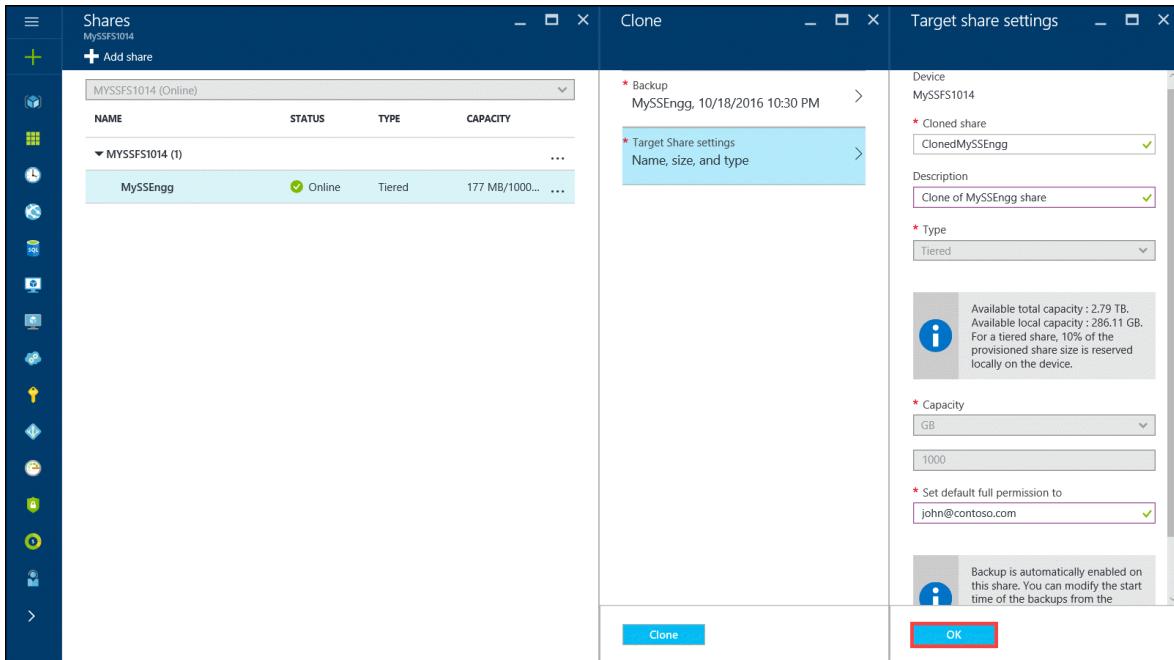


3. In the **Clone** blade, click **Target settings** and then do the following:

- Provide a share name. The share name must contain 3-127 characters.
- Optionally provide a description for the cloned share.
- You cannot change the type of the share you are restoring to. A tiered share is cloned as a tiered and a locally pinned share as locally pinned.
- The capacity is set as equal to the size of the share you are cloning from.

e. Assign the administrators for this share. You will be able to modify the share properties via File Explorer after the clone is complete.

f. Click OK.



4. Click **Clone** to start a clone job. After the job is complete, the clone operation starts and you are notified. To monitor the progress of clone, go to the **Jobs** blade and click the job to view job details.
5. After the clone is successfully created, navigate back to the **Shares** blade on your device.
6. You can now view the new cloned share in the list of shares on your device. A tiered share is cloned as tiered and a locally pinned share as a locally pinned share.

The screenshot shows the Azure portal's interface for managing storage shares. On the left, there's a vertical sidebar with various icons for different services like Storage, Compute, and Networking. The main area is titled 'Shares' and shows a single share named 'MySSFS1014'. Below the share name is a button to 'Add share'. The table lists two volumes under 'MYSSFS1014 (2)'. The first volume, 'ClonedMySSEngg', is highlighted with a red border. It has a status of 'Offline', is of type 'Tiered', and has a capacity of '0 Bytes/1000...'. The second volume, 'MySSEngg', is online, tiered, and has a capacity of '177 MB/1000...'. Both rows have a three-dot ellipsis icon at the end.

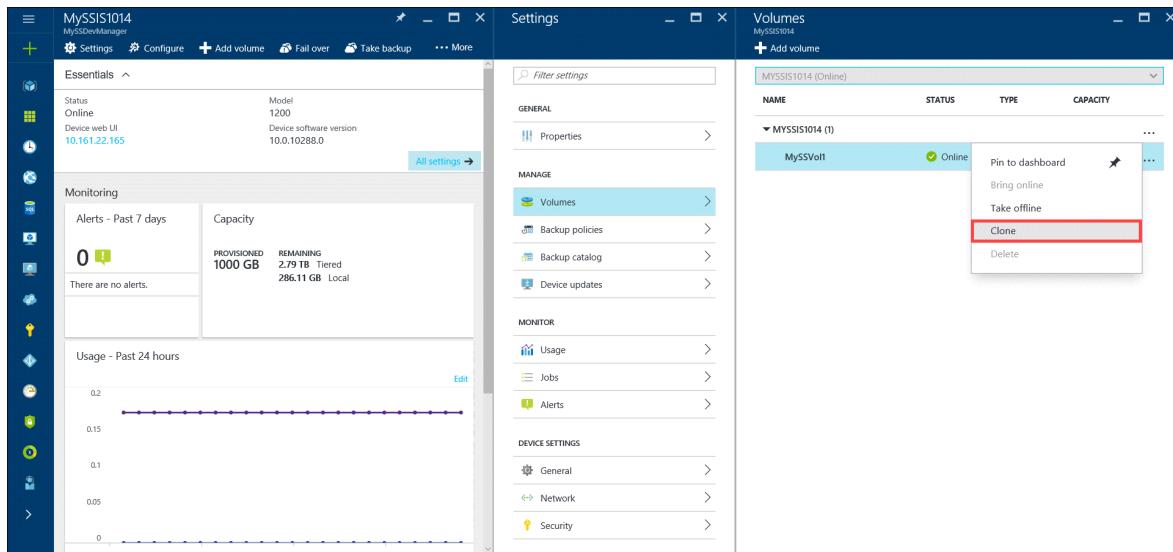
NAME	STATUS	TYPE	CAPACITY
ClonedMySSEngg	Offline	Tiered	0 Bytes/1000...
MySSEngg	Online	Tiered	177 MB/1000...

Clone volumes from a backup set

To clone from a backup, in the Azure portal, you have to perform steps similar to the ones when cloning a share. The clone operation clones the backup to a new volume on the same virtual device; you cannot clone to a different device.

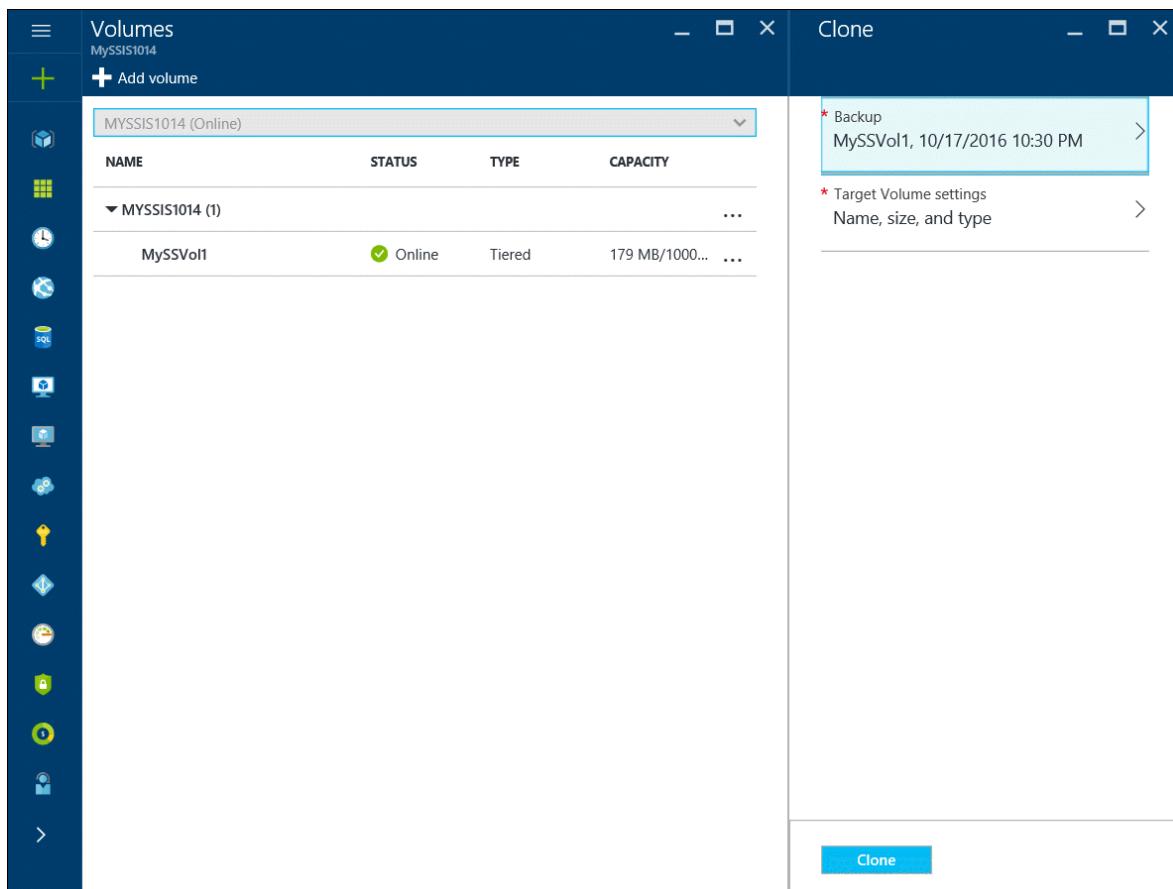
To clone a volume

1. Browse to **Devices** blade. Select and click your device and then click **Volumes**. Select the volume that you want to clone, right-click the volume to invoke the context menu. Select **Clone**.



2. In the **Clone** blade, click **Backup** and then do the following:

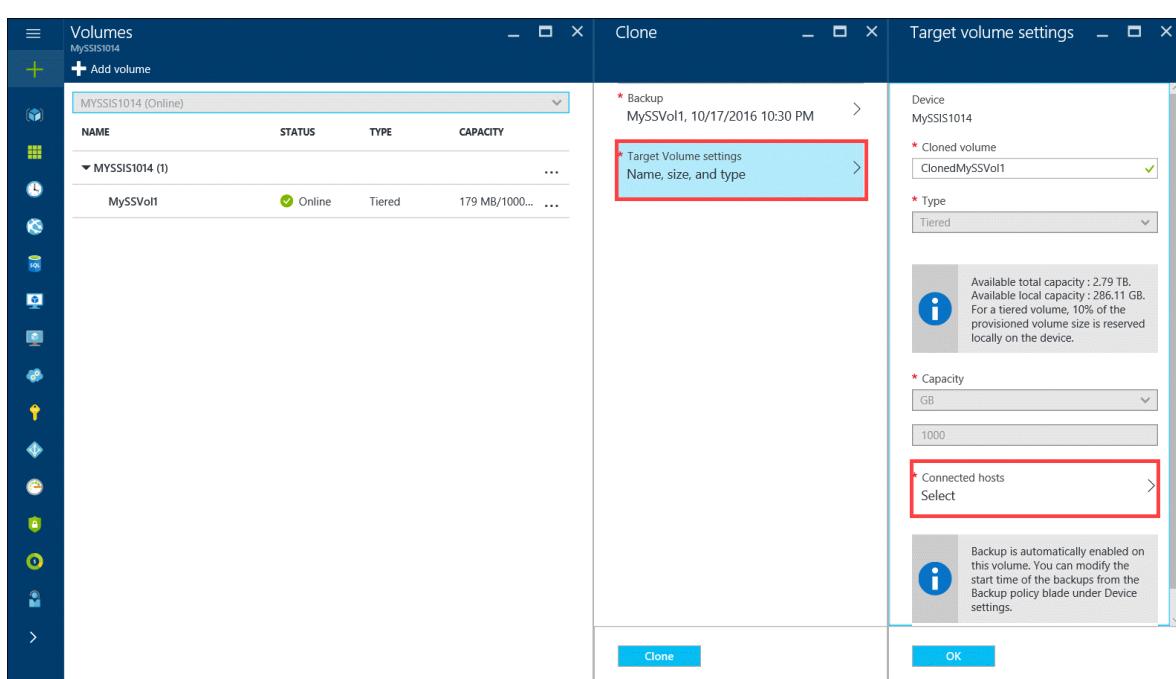
- Filter a backup on this device based on the time range. You can choose from **Past 7 days**, **Past 30 days**, and **Past year**.
- In the list of filtered backups displayed, select a backup to clone from.
- Click **OK**.



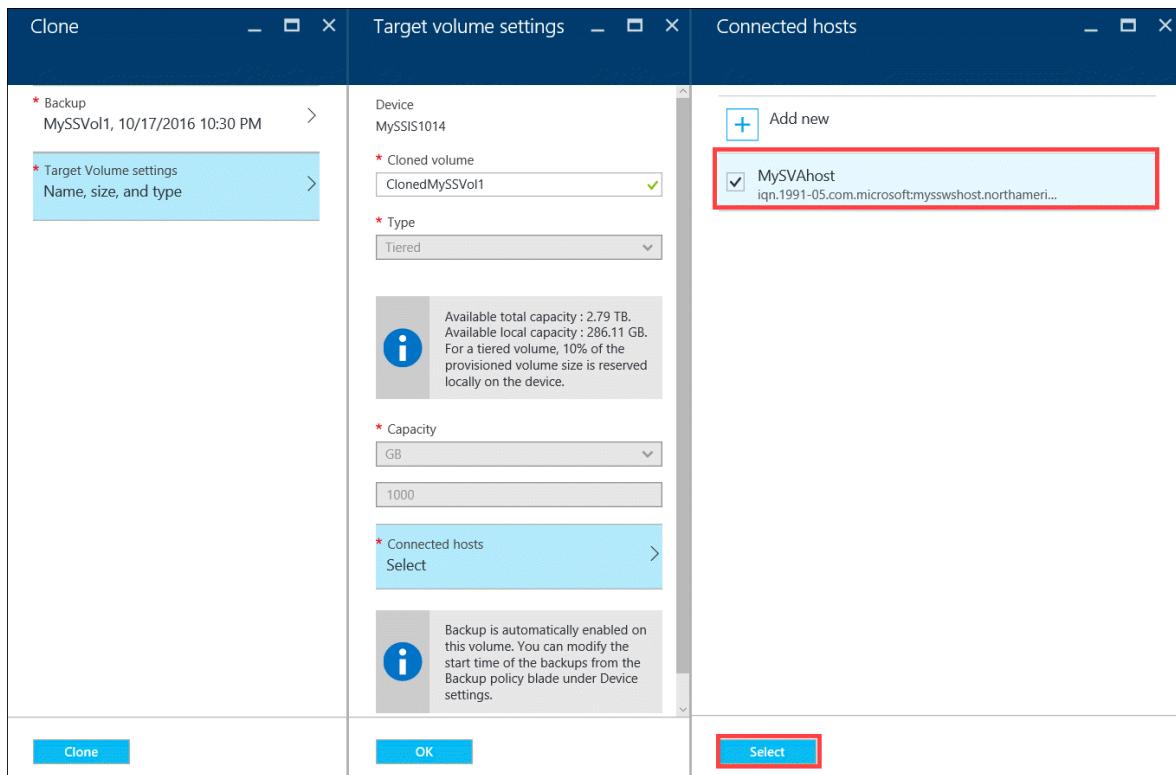
3. In the **Clone** blade, click **Target volume settings** and then do the following::

- The device name is automatically populated.

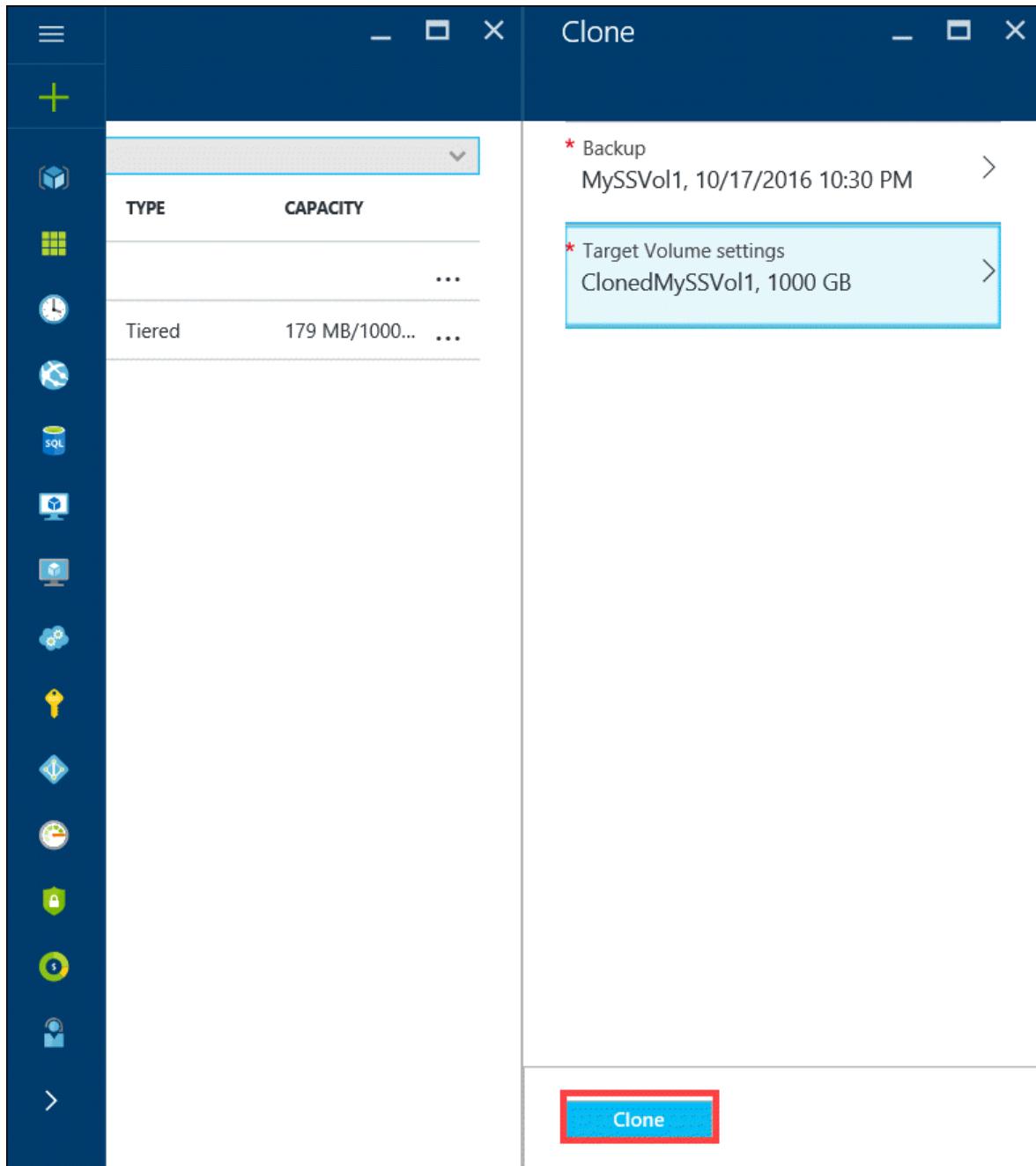
- b. Provide a volume name for the **cloned volume**. The volume name must contain 3 to 127 characters.
- c. The volume type is automatically set to the original volume. A tiered volume is cloned as tiered and a locally pinned volume as locally pinned.
- d. For the **Connected hosts**, click **Select**.



4. In the **Connected hosts** blade, select from an existing ACR or add a new ACR. To add a new ACR, you will need to provide an ACR name and the host IQN. Click **Select**.



5. Click **Clone** to launch a clone job.



6. After the clone job is created, cloning will start. Once the clone is created, it is displayed on the Volumes blade on your device. Note that a tiered volume is cloned as tiered and a locally pinned volume is cloned as a locally pinned volume.

The screenshot shows the StorSimple portal's Volumes page. On the left, there's a sidebar with icons for Home, Add volume, My shares, My devices, My reports, and Help. The main area has a title 'Volumes' and a subtitle 'MySSIS1014'. Below that is a button '+ Add volume'. The main content area shows a table with columns: NAME, STATUS, TYPE, and CAPACITY. There are two entries under 'MYSSIS1014 (2)': 'ClonedMySSVol1' (highlighted with a red box) and 'MySSVol1'. Both volumes are listed as 'Online' (indicated by a green checkmark icon), 'Tiered' (indicated by a blue icon), and have a capacity of '0 Bytes/1000...'. An ellipsis (...) icon is at the end of each row.

7. Once the volume appears online on the list of volumes, the volume is available for use. On the iSCSI initiator host, refresh the list of targets in iSCSI initiator properties window. A new target that contains the cloned volume name should appear as 'inactive' under the status column.
8. Select the target and click **Connect**. After the initiator is connected to the target, the status should change to **Connected**.
9. In the **Disk Management** window, the mounted volumes appear as shown in the following illustration. Right-click the discovered volume (click the disk name), and then click **Online**.

ⓘ Important

When trying to clone a volume or a share from a backup set, if the clone job fails, a target volume or share may still be created in the portal. It is important that you delete this target volume or share in the portal to minimize any future issues arising from this element.

Item-level recovery (ILR)

This release introduces the item-level recovery (ILR) on a StorSimple Virtual Array configured as a file server. The feature allows you to do granular recovery of files and folders from a cloud backup of all the shares on the StorSimple device. You can retrieve deleted files from recent backups using a self-service model.

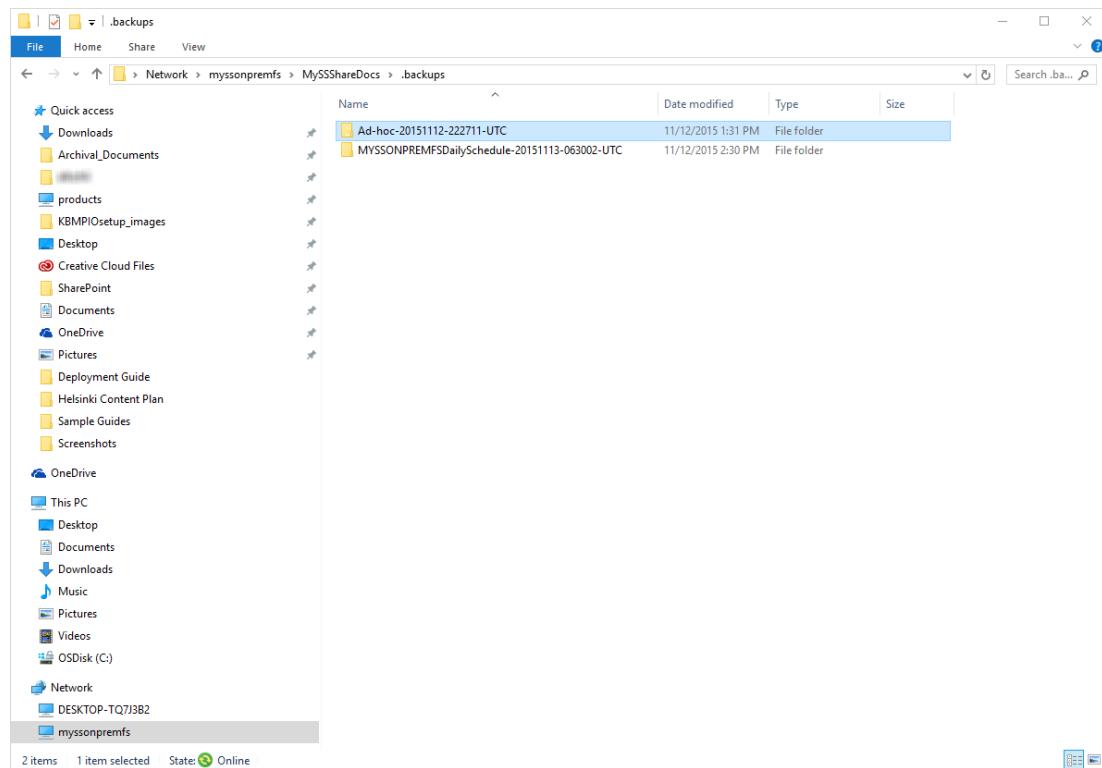
Every share has a *.backups* folder that contains the most recent backups. You can navigate to the desired backup, copy relevant files and folders from the backup and

restore them. This feature eliminates calls to administrators for restoring files from backups.

- When performing the ILR, you can view the backups through File Explorer. Click the specific share that you want to look at the backup for. You will see a *.backups* folder created under the share that stores all the backups. Expand the *.backups* folder to view the backups. The folder shows the exploded view of the entire backup hierarchy. This view is created on-demand and usually takes only a couple of seconds to create.

The last five backups are displayed in this way and can be used to perform an item-level recovery. The five recent backups include both the default scheduled and the manual backups.

- Scheduled backups** named as <Device name>DailySchedule-YYYYMMDD-HHMMSS-UTC.
- Manual backups** named as Ad-hoc-YYYYMMDD-HHMMSS-UTC.



- Identify the backup containing the most recent version of the deleted file. Though the folder name contains a UTC timestamp in each of the preceding cases, the time at which the folder was created is the actual device time when the backup started. Use the folder timestamp to locate and identify the backups.
- Locate the folder or the file that you want to restore in the backup that you identified in the previous step. Note you can only view the files or folders that you have permissions for. If you cannot access certain files or folders, contact a share

administrator. The administrator can use File Explorer to edit the share permissions and give you access to the specific file or folder. It is a recommended best practice that the share administrator is a user group instead of a single user.

4. Copy the file or the folder to the appropriate share on your StorSimple file server.

Next steps

Learn more about how to [administer your StorSimple Virtual Array using the local web UI](#).

Disaster recovery and device failover for your StorSimple Virtual Array via Azure portal

Article • 08/19/2022 • 8 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the disaster recovery for your Microsoft Azure StorSimple Virtual Array including the detailed steps to fail over to another virtual array. A failover allows you to move your data from a *source* device in the datacenter to a *target* device. The target device may be located in the same or a different geographical location. The device failover is for the entire device. During failover, the cloud data for the source device changes ownership to that of the target device.

This article is applicable to StorSimple Virtual Arrays only. To fail over an 8000 series device, go to [Device failover and disaster recovery of your StorSimple device](#).

What is disaster recovery and device failover?

In a disaster recovery (DR) scenario, the primary device stops functioning. In this scenario, you can move the cloud data associated with the failed device to another device. You can use the primary device as the *source* and specify another device as the *target*. This process is referred to as the *failover*. During failover, all the volumes or the shares from the source device change ownership and are transferred to the target device. No filtering of the data is allowed.

DR is modeled as a full device restore using the heat map-based tiering and tracking. A heat map is defined by assigning a heat value to the data based on read and write

patterns. This heat map then tiers the lowest heat data chunks to the cloud first while keeping the high heat (most used) data chunks in the local tier. During a DR, StorSimple uses the heat map to restore and rehydrate the data from the cloud. The device fetches all the volumes/shares in the last recent backup (as determined internally) and performs a restore from that backup. The virtual array orchestrates the entire DR process.

ⓘ Important

The source device is deleted at the end of device failover and hence a failback is not supported.

Disaster recovery is orchestrated through the device failover feature and is initiated from the **Devices** blade. This blade tabulates all the StorSimple devices connected to your StorSimple Device Manager service. For each device, you can see the friendly name, status, provisioned and maximum capacity, type, and model.

Prerequisites for device failover

Prerequisites

For a device failover, ensure that the following prerequisites are satisfied:

- The source device needs to be in a **Deactivated** state.
- The target device needs to show up as **Ready to set up** in the Azure portal.
Provision a target virtual array of the same or higher capacity. Use the local web UI to configure and successfully register the target virtual array.

ⓘ Important

Do not attempt to configure the registered virtual device through the service.
No device configuration should be performed through the service.

- The target device cannot have the same name as the source device.
- The source and target device have to be the same type. You can only fail over a virtual array configured as a file server to another file server. The same is true for an iSCSI server.
- For a file server DR, we recommend that you join the target device to the same domain as the source. This configuration ensures that the share permissions are

automatically resolved. Only the failover to a target device in the same domain is supported.

- The available target devices for DR are devices that have the same or larger capacity compared to the source device. The devices that are connected to your service but do not meet the criteria of sufficient space are not available as target devices.

Other considerations

- For a planned failover:
 - We recommend that you take all the volumes or shares on the source device offline.
 - We recommend that you take a backup of the device and then proceed with the failover to minimize data loss.
- For an unplanned failover, the device uses the most recent backup to restore the data.

Device failover prechecks

Before the DR begins, the device performs prechecks. These checks help ensure that no errors occur when DR commences. The prechecks include:

- Validating the storage account.
- Checking the cloud connectivity to Azure.
- Checking available space on the target device.
- Checking if an iSCSI server source device volume has
 - valid ACR names.
 - valid IQN (not exceeding 220 characters).
 - valid CHAP passwords (12-16 characters long).

If any of the preceding prechecks fail, you cannot proceed with the DR. Resolve those issues and then retry DR.

After the DR is successfully completed, the ownership of the cloud data on the source device is transferred to the target device. The source device is then no longer available in the portal. Access to all the volumes/shares on the source device is blocked and the target device becomes active.

ⓘ Important

Though the device is no longer available, the virtual machine that you provisioned on the host system is still consuming resources. Once the DR is successfully complete, you can delete this virtual machine from your host system.

Fail over to a virtual array

We recommend that you provision, configure, and register another StorSimple Virtual Array with your StorSimple Device Manager service before you run this procedure.

ⓘ Important

- You cannot fail over from a StorSimple 8000 series device to a 1200 virtual device.
- You can fail over from a Federal Information Processing Standard (FIPS) enabled virtual device to another FIPS enabled device or to a non-FIPS device deployed in the Government portal.

Perform the following steps to restore the device to a target StorSimple virtual device.

1. Provision and configure a target device that meets the [prerequisites for device failover](#). Complete the device configuration via the local web UI and register it to your StorSimple Device Manager service. If creating a file server, go to step 1 of [set up as file server](#). If creating an iSCSI server, go to step 1 of [set up as iSCSI server](#).
2. Take volumes/shares offline on the host. To take the volumes/shares offline, refer to the operating system-specific instructions for the host. If not already offline, you need to take all the volumes/shares offline on the device by doing the following.
 - a. Go to **Devices** blade and select your device.
 - b. Go to **Settings > Manage > Shares** (or **Settings > Manage > Volumes**).
 - c. Select a share/volume, right click and select **Take offline**.
 - d. When prompted for confirmation, check **I understand the impact of taking this share offline**.
 - e. Click **Take offline**.

3. In your StorSimple Device Manager service, go to **Management > Devices**. In the **Devices** blade, select and click your source device.
4. In your **Device dashboard** blade, click **Deactivate**.
5. In the **Deactivate** blade, you are prompted for confirmation. Device deactivation is a *permanent* process that cannot be undone. You are also reminded to take your shares/volumes offline on the host. Type the device name to confirm and click **Deactivate**.

Deactivate



If you continue, your device will be permanently deactivated. A deactivated device cannot be registered with the StorSimple Device Manager service again.

SUMMARY

No. of shares: 4

Total size of shares: 4.52 GB

Total size of backups: 21.79 TB

Are you sure you want to deactivate this device ?
If yes, enter the name of the device and click
Deactivate.

Type the device name

MySSVAFS0720 ✓

Deactivate

6. The deactivation starts. You will receive a notification after the deactivation is successfully completed.



7. On the Devices page, the device state will now change to **Deactivated**.

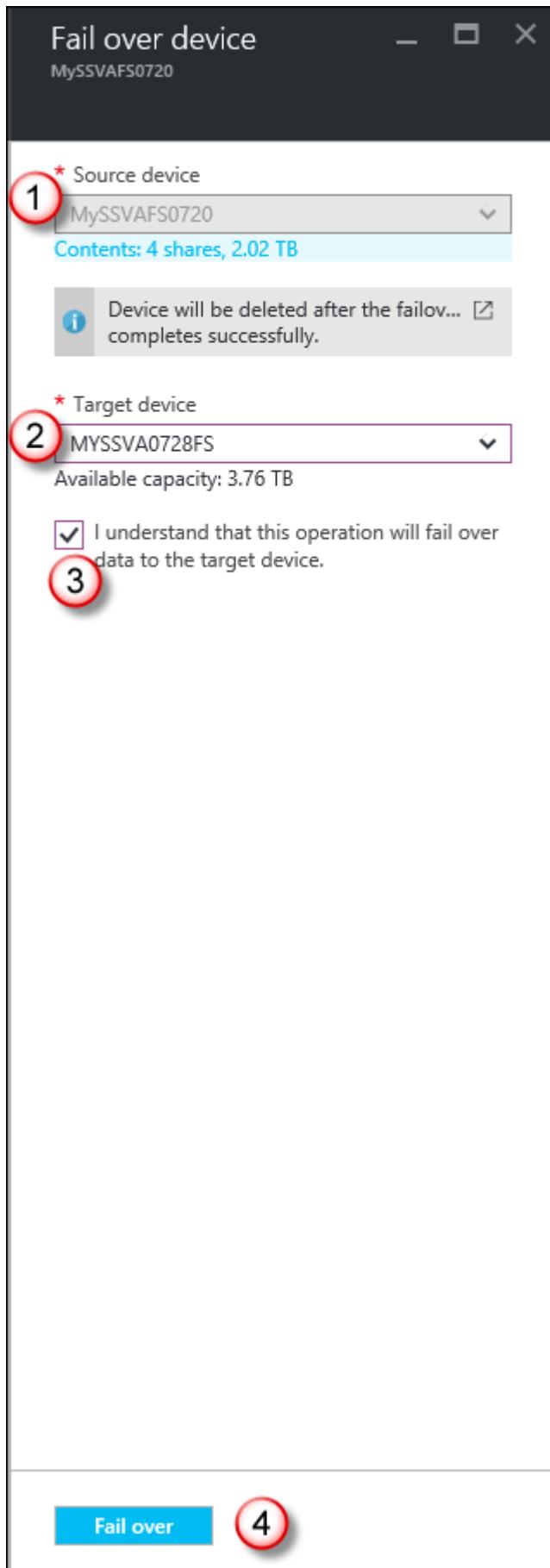
The screenshot shows the 'Devices' blade in a management interface. On the left, a table lists five devices: GYANNASDEV02 (Offline), GYANISCODEV02 (Offline), MYSSVA072BFS (Pending configuration), CSISTORMPEVA2 (Online), and MYSSVAFS0720 (Deactivated). The right side features a dashboard with sections for Monitoring (Alerts - Past Week: 0), Capacity (Provisioned: 2.02 TB, Remaining: 1.3 TB Tiered, 133.39 GB Local), Usage (Primary storage used: 4.53 GB, Cloud storage used: 2.22 GB, Local storage used: 4.53 GB), and Managed items (Shares: 4). A prominent message at the top right indicates that the device has been deactivated.

8. In the Devices blade, select and click the deactivated source device for failover.

9. In the Device dashboard blade, click **Fail over**.

10. In the Fail over device blade, do the following:

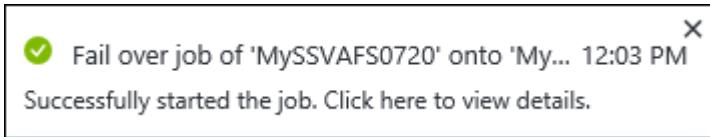
- a. The source device field is automatically populated. Note the total data size for the source device. The data size should be lesser than the available capacity on the target device. Review the details associated with the source device such as device name, total capacity, and the names of the shares that are failed over.
- b. From the dropdown list of available devices, choose a **Target device**. Only the devices that have sufficient capacity are displayed in the dropdown list.
- c. Check that **I understand that this operation will fail over data to the target device**.
- d. Click **Fail over**.



11. A failover job initiates and you receive a notification. Go to **Devices > Jobs** to monitor the failover.



12. In the **Jobs** blade, you see a failover job created for the source device. This job performs the DR prechecks.



After the DR prechecks are successful, the failover job will spawn restore jobs for each share/volume that exists on your source device.

A screenshot of the StorSimple Management UI. The left pane shows a table of jobs with columns: NAME, STATUS, ENTITY, DEVICE, STARTED ON, and DURATION. A specific row for 'Failover' is highlighted with a red box. The right pane is titled 'Failover Job' and displays detailed information about the failover process, including the status, entity, device, start time, duration, and source device. Below this, there is a 'Tasks' section showing the status of various configuration steps.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Failover	In-progress	MySSVAFS0720	MySSVAFS0728FS	7/28/2016 12:02:43	54 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/27/2016 22:30:03	1 Minute, 32 Seconds
Backup	Succeeded	CSISTORSMIPLEVA2	CSIStorSmpleVA2	7/27/2016 22:30:01	30 Seconds
Clone	Succeeded	CSISTORSMIPLEVA2	CSIStorSmpleVA2	7/27/2016 12:55:18	4 Minutes, 24 Seconds
Backup	Succeeded	CSISTORSMIPLEVA2	CSIStorSmpleVA2	7/27/2016 12:39:41	19 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/26/2016 22:30:02	1 Minute, 27 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/25/2016 22:30:02	3 Minutes, 25 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/25/2016 22:30:02	1 Minute, 49 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/24/2016 22:30:02	1 Minute, 29 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/24/2016 22:30:02	47 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/23/2016 22:30:02	1 Minute, 36 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/23/2016 22:30:01	53 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/22/2016 22:30:02	1 Minute, 19 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/22/2016 22:30:01	47 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/22/2016 4:39:05	45 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/22/2016 4:38:42	1 Minute, 16 Seconds
Backup	Succeeded	GYANNASDEV02	GyanNasDev02	7/22/2016 3:47:33	46 Seconds
Backup	Succeeded	MYSSVAFS0720	MySSVAFS0720	7/22/2016 3:42:14	1 Minute, 18 Seconds

Failover Job

Details	
Status	Running
Entity	MySSVAFS0720 (Microsoft.StorSimpleBVTD2/managers/devices)
Device	MYSSVAFS0728FS
Started on	7/28/2016 12:02:43
Completed on	-
Duration	3 Minutes, 13 Seconds
Source device	MYSSVAFS0720

Tasks

NAME	STATUS
Configure cloud credentials.	Succeeded
Configure the backup policy.	Succeeded
Configure the server.	Succeeded
Discover backups.	In-progress

13. After the failover is complete, go to the **Devices** blade.
- Select and click the StorSimple device that was used as the target device for the failover process.
 - Go to **Settings > Management > Shares** (or **Volumes** if iSCSI server). In the **Shares** blade, you can view all the shares (volumes) from the old device.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
MYSSVA0728FS	Online	133.39 GB/1.3 TB	Virtual-NAS	1200
CSISTORSMPLEVA2	Online	286.11 GB/2.79 TB	Virtual-iSCSI	1200
GYANNASDEV02	Offline	625.59 GB/6.1 TB	Virtual-NAS	1200
GYANISCIDEV02	Offline	774.63 GB/7.56 TB	Virtual-iSCSI	1200

14. You will need to [create a DNS alias](#) so that all the applications that are trying to connect can get redirected to the new device.

Errors during DR

Cloud connectivity outage during DR

If the cloud connectivity is disrupted after DR has started and before the device restore is complete, the DR will fail. You receive a failure notification. The target device for DR is marked as *unusable*. You cannot use the same target device for future DRs.

No compatible target devices

If the available target devices do not have sufficient space, you see an error to the effect that there are no compatible target devices.

Precheck failures

If one of the prechecks is not satisfied, then you see precheck failures.

Business continuity disaster recovery (BCDR)

A business continuity disaster recovery (BCDR) scenario occurs when the entire Azure datacenter stops functioning. This can affect your StorSimple Device Manager service and the associated StorSimple devices.

If there are StorSimple devices that were registered just before a disaster occurred, then these StorSimple devices may need to be deleted. After the disaster, you can recreate and configure those devices.

Next steps

Learn more about how to [administer your StorSimple Virtual Array using the local web UI](#).

Deactivate and delete a StorSimple Virtual Array

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

When you deactivate a StorSimple Virtual Array, you break the connection between the device and the corresponding StorSimple Device Manager service. This tutorial explains how to:

- Deactivate a device
- Delete a deactivated device

The information in this article applies to StorSimple Virtual Arrays only. For information on 8000 series, go to how to [deactivate or delete a device](#).

When to deactivate?

Deactivation is a PERMANENT operation and cannot be undone. You cannot register a deactivated device with the StorSimple Device Manager service again. You may need to deactivate and delete a StorSimple Virtual Array in the following scenarios:

- **Planned failover** : Your device is online and you plan to fail over your device. If you are planning to upgrade to a larger device, you may need to fail over your device. After the data ownership is transferred and the failover is complete, the source device is automatically deleted.
- **Unplanned failover** : Your device is offline and you need to fail over the device. This scenario may occur during a disaster when there is an outage in the datacenter and your primary device is down. You plan to fail over the device to a

secondary device. After the data ownership is transferred and the failover is complete, the source device is automatically deleted.

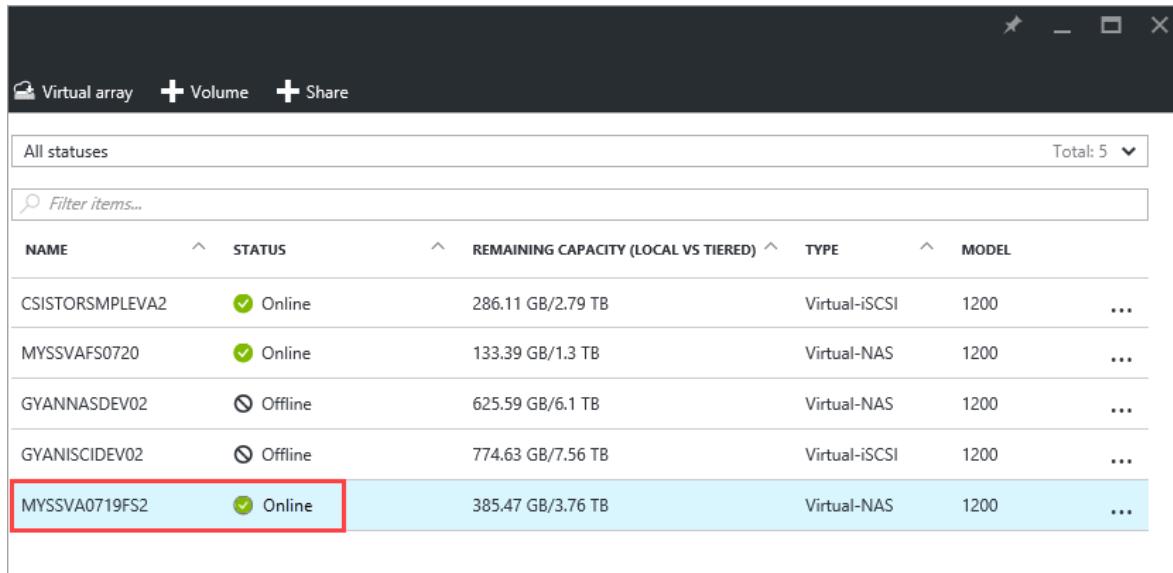
- **Decommission** : You want to decommission the device. This requires you to first deactivate the device and then delete it. When you deactivate a device, you can no longer access any data that is stored locally. You can only access and recover the data stored in the cloud. If you plan to keep the device data after deactivation, then you should take a cloud snapshot of all your data before you deactivate a device. This cloud snapshot allows you to recover all the data at a later stage.

Deactivate a device

To deactivate your device, perform the following steps. A device must be online to be deactivated.

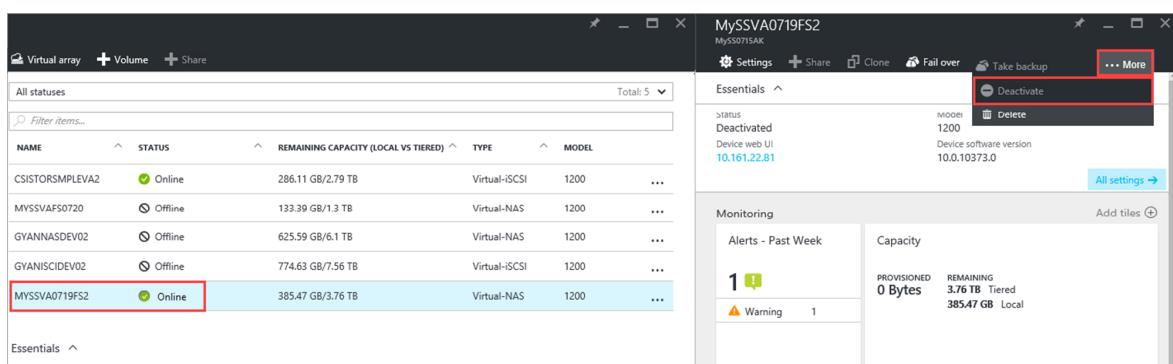
To deactivate the device

1. In your service, go to **Management > Devices**. In the **Devices** blade, click and select the device that you wish to deactivate. The device status must be **Online**.



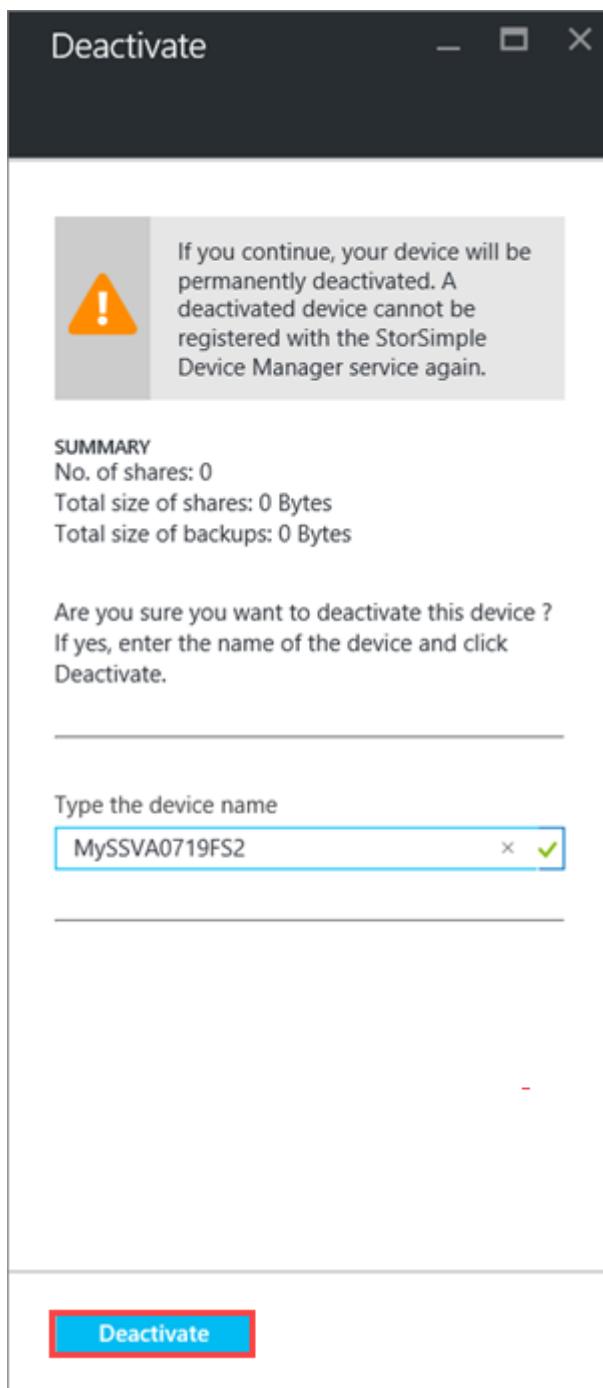
NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
CSISTORSMPEVA2	Online	286.11 GB/2.79 TB	Virtual-iSCSI	1200
MYSSVAFS0720	Online	133.39 GB/1.3 TB	Virtual-NAS	1200
GYANNASDEV02	Offline	625.59 GB/6.1 TB	Virtual-NAS	1200
GYANISCIDEV02	Offline	774.63 GB/7.56 TB	Virtual-iSCSI	1200
MYSSVA0719FS2	Online	385.47 GB/3.76 TB	Virtual-NAS	1200

2. In your **Device dashboard** blade, click **... More** and from the list, select **Deactivate**.



NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
CSISTORSMPEVA2	Online	286.11 GB/2.79 TB	Virtual-iSCSI	1200
MYSSVAFS0720	Offline	133.39 GB/1.3 TB	Virtual-NAS	1200
GYANNASDEV02	Offline	625.59 GB/6.1 TB	Virtual-NAS	1200
GYANISCIDEV02	Offline	774.63 GB/7.56 TB	Virtual-iSCSI	1200
MYSSVA0719FS2	Online	385.47 GB/3.76 TB	Virtual-NAS	1200

3. In the Deactivate blade, type the device name and then click Deactivate.



The deactivate process starts and takes a few minutes to complete.



4. After deactivation, the list of devices refreshes.

The screenshot shows the StorSimple Device Manager interface. On the left, the 'Devices' blade lists several storage arrays: CSISTORSMPEVA2 (Online), MYSSVAFS0720 (Offline), GYANNASDEV02 (Offline), GYANISCIDEV02 (Offline), and MYSSVA0719FS2 (Deactivated). The 'MYSSVA0719FS2' row is selected and highlighted with a red box. On the right, the 'Device dashboard' for 'MySSVA0719FS2' is displayed. It shows the device is 'Deactivated' with model 1200 and software version 10.161.22.81. Monitoring section shows 1 alert (yellow) and 1 warning (orange). Capacity section shows 0 bytes provisioned, 3.76 TB remaining (tiered), and 385.47 GB local.

You can now delete this device.

Delete the device

A device has to be first deactivated to delete it. Deleting a device removes it from the list of devices connected to the service. The service can then no longer manage the deleted device. The data associated with the device, however, remains in the cloud. This data then accrues charges.

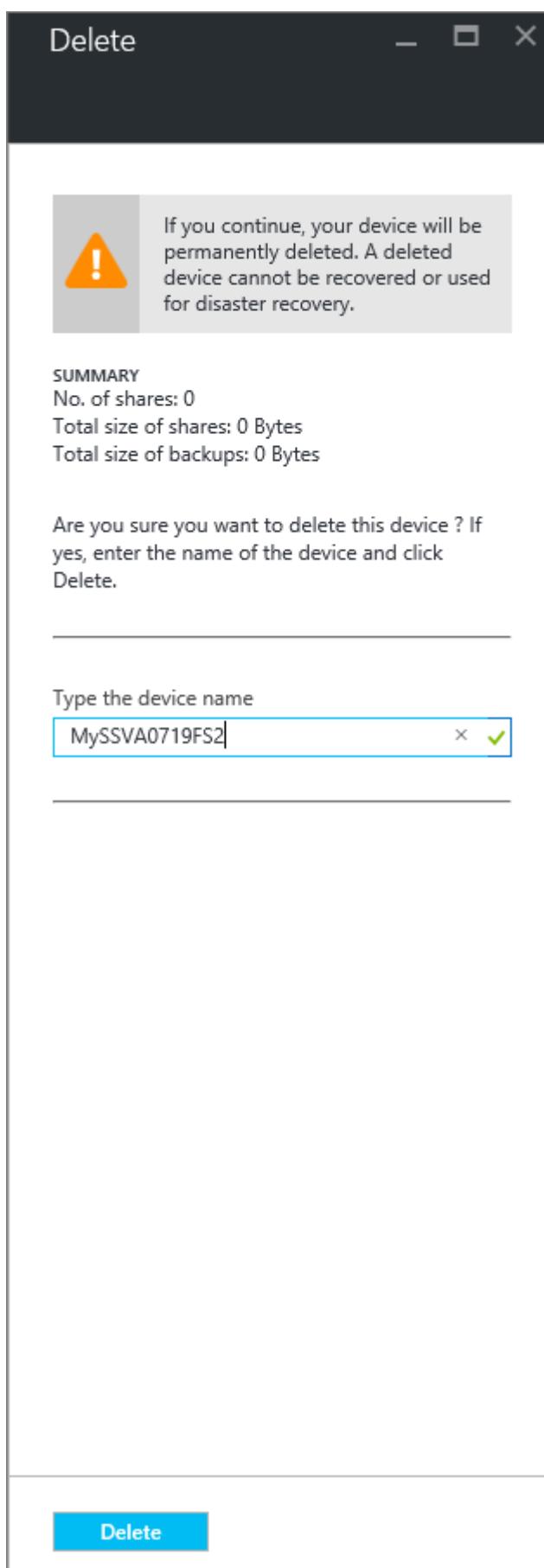
To delete the device, perform the following steps.

To delete the device

1. In your StorSimple Device Manager, go to **Management > Devices**. In the **Devices** blade, select a deactivated device that you wish to delete.
2. In the **Device dashboard** blade, click **... More** and then click **Delete**.

The screenshot shows the StorSimple Device Manager interface. On the left, the 'Devices' blade lists several storage arrays. On the right, the 'Device dashboard' for 'MySSVA0719FS2' is displayed. A message at the top states: 'This device was deactivated. You can only fail over or delete it.' The 'Delete' button is highlighted with a red box. The dashboard includes sections for 'Monitoring' (with 1 alert and 1 warning), 'Capacity' (0 bytes provisioned, 3.76 TB remaining tiered, 385.47 GB local), 'Usage - Past 24 hours' (line chart showing zero usage), and 'Managed items' (Shares section).

3. In the **Delete** blade, type the name of your device to confirm the deletion and then click **Delete**. Deleting the device does not delete the cloud data associated with the device.



4. The deletion starts and takes a few minutes to complete.



Delete 'MYSSVA0719FS2'

11:33 AM

After the device is deleted, you can view the updated list of devices.

Next steps

- For information on how to fail over, go to [Failover and disaster recovery of your StorSimple Virtual Array](#).
 - To learn more about how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple Virtual Array](#).
-

Additional resources

Documentation

[Troubleshoot issues during data copies to your Azure Data Box, Azure Data Box Heavy](#)

Describes how to troubleshoot issues when copying data to Azure Data Box and Azure Data Box Heavy devices.

[Deactivate and delete a StorSimple 8000 series device](#)

Learn how to deactivate and delete a StorSimple device that is connected to a StorSimple Device Manager service.

[Manage StorSimple 8000 series device controllers](#)

Learn how to stop, restart, shut down, or reset your StorSimple device controllers.

[StorSimple 8000 series migration to Azure File Sync](#)

Learn how to migrate a StorSimple 8100 or 8600 appliance to Azure File Sync.

[Tutorial to copy data via SMB on Azure Data Box](#)

In this tutorial, learn how to connect to and copy data from your host computer to Azure Data Box by using SMB with the local web UI.

[Tutorial to set up Azure Data Box](#)

In this tutorial, learn how to cable your Azure Data Box, connect Azure Data Box, and turn on Azure Data Box.

[Microsoft Azure Data Box Disk system requirements](#)

Learn about the software and networking requirements for your Azure Data Box Disk

[Tutorial: Use data copy service to copy to your device - Azure Data Box](#)

In this tutorial, you learn how to copy data to your Azure Data Box device via the data copy service

[Show 5 more](#)

 **Training**

Learning path

[Manage IoT devices by using IoT Hub and apps - Training](#)

Manage IoT devices by using IoT Hub and apps

Use the StorSimple Device Manager service to manage shares on the StorSimple Virtual Array

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to use the StorSimple Device Manager service to create and manage shares on your StorSimple Virtual Array.

The StorSimple Device Manager service is an extension in the Azure portal that lets you manage your StorSimple solution from a single web interface. In addition to managing shares and volumes, you can use the StorSimple Device Manager service to view and manage devices, view alerts, manage backup policies, and manage the backup catalog.

Share Types

StorSimple shares can be:

- **Locally pinned:** Data in these shares stays on the array at all times and does not spill to the cloud.
- **Tiered:** Data in these shares can spill to the cloud. When you create a tiered share, approximately 10 % of the space is provisioned on the local tier and 90 % of the space is provisioned in the cloud. For example, if you provisioned a 1 TB share, 100 GB would reside in the local space and 900 GB would be used in the cloud when the data tiers. This in turn implies that if you run out of all the local space on the device, you cannot provision a tiered share (because the 10 % required on the local tier will not be available).

Provisioned capacity

Refer to the following table for maximum provisioned capacity for each share type.

Limit identifier	Limit
Minimum size of a tiered share	500 GB
Maximum size of a tiered share	20 TB
Minimum size of a locally pinned share	50 GB
Maximum size of a locally pinned share	2 TB

The Shares blade

The **Shares** menu on your StorSimple service summary blade displays the list of storage shares on a given StorSimple array and allows you to manage them.

NAME	STATUS	TYPE	CAPACITY
Demo	Online	Tiered	237 MB/500 GB
SupportDemo	Online	Tiered	167 MB/500 GB
VendorData	Online	Tiered	237 MB/500 GB

A share consists of a series of attributes:

- **Share Name** – A descriptive name that must be unique and helps identify the share.

- **Status** – Can be online or offline. If a share is offline, users of the share will not be able to access it.
- **Type** – Indicates whether the share is **Tiered** (the default) or **Locally pinned**.
- **Capacity** – specifies the amount of data used as compared to the total amount of data that can be stored on the share.
- **Description** – An optional setting that helps describe the share.
- **Permissions** - The NTFS permissions to the share that can be managed through Windows Explorer.
- **Backup** – In case of the StorSimple Virtual Array, all shares are automatically enabled for backup.

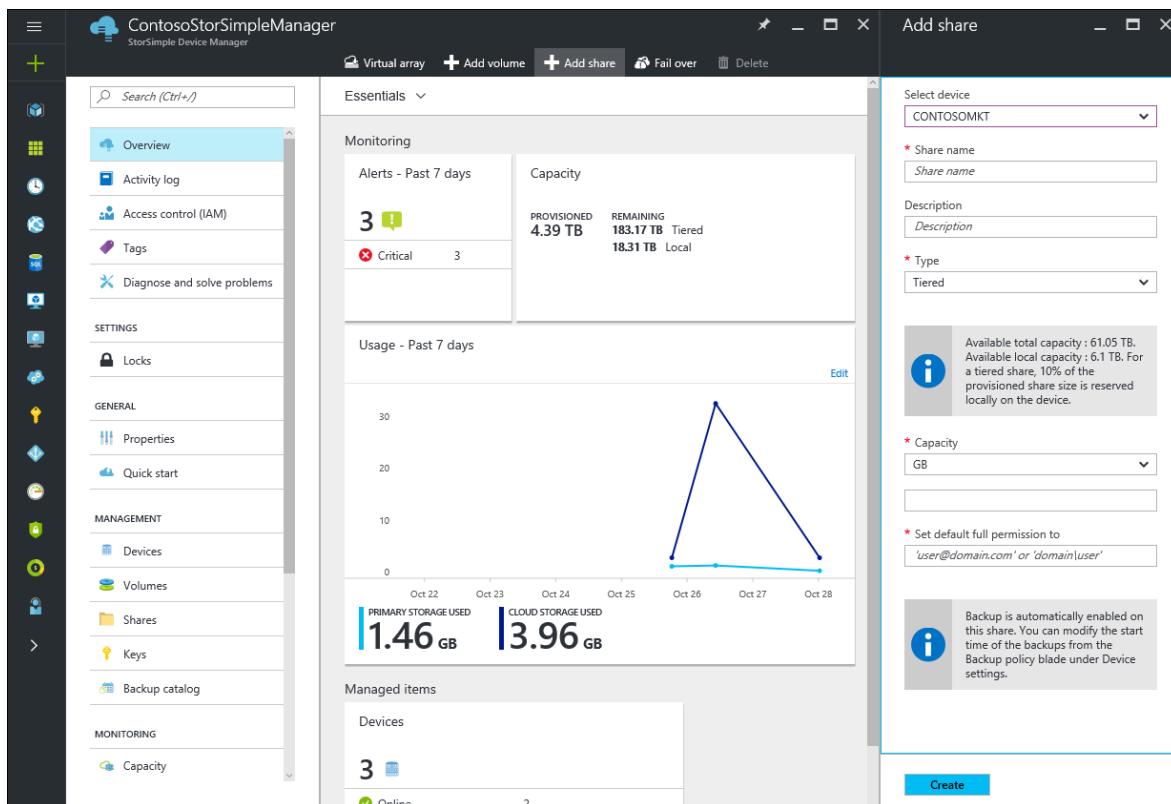
The screenshot shows the StorSimple Device Manager interface. On the left, there's a navigation sidebar with icons for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Locks, Properties, Quick start, Devices, Volumes, and Shares (which is selected). The main area displays a list of shares under 'CONTOSOMKT (Online)'. The list includes three shares: Demo, SupportDemo, and VendorData. The 'VendorData' row is currently selected. To the right of the main area, a modal dialog titled 'Update' is open for the 'VendorData' share. The dialog contains fields for Status (set to Online), Capacity (500 GB), Type (Tiered), and Description (with a placeholder 'Description'). It also lists other settings: Permission (Managed through File Explorer), Backup (Automatic), and Monitoring (Enabled). There are 'Save' and 'Discard' buttons at the bottom of the dialog.

Use the instructions in this tutorial to perform the following tasks:

- Add a share
- Modify a share
- Take a share offline
- Delete a share

Add a share

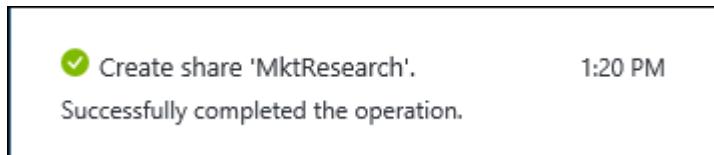
1. From the StorSimple service summary blade, click **+ Add share** from the command bar. This opens up the **Add share** blade.



2. In the **Add share** blade, do the following:

- a. In the **Share name** field, enter a unique name for your share. The name must be a string that contains 3 to 127 characters.
 - b. An optional **Description** for the share. The description will help identify the share owners.
 - c. In the **Type** dropdown list, specify whether to create a **Tiered** or **Locally pinned** share. For workloads that require local guarantees, low latencies, and higher performance, select **Locally pinned share**. For all other data, select **Tiered** share.
 - d. In the **Capacity** field, specify the size of the share. A tiered share must be between 500 GB and 20 TB and a locally pinned share must be between 50 GB and 2 TB.
 - e. In the **Set default full permissions to** field, assign the permissions to the user, or the group that is accessing this share. Specify the name of the user or the user group in *john@contoso.com* format. We recommend that you use a user group (instead of a single user) to allow admin privileges to access these shares. After you have assigned the permissions here, you can then use File Explorer to modify these permissions.
3. When you've finished configuring your share, click **Create**. A share will be created with the specified settings and you will see a notification. By default, backup will be enabled for the share.

4. To confirm that the share was successfully created, go to the **Shares** blade. You should see the share listed.

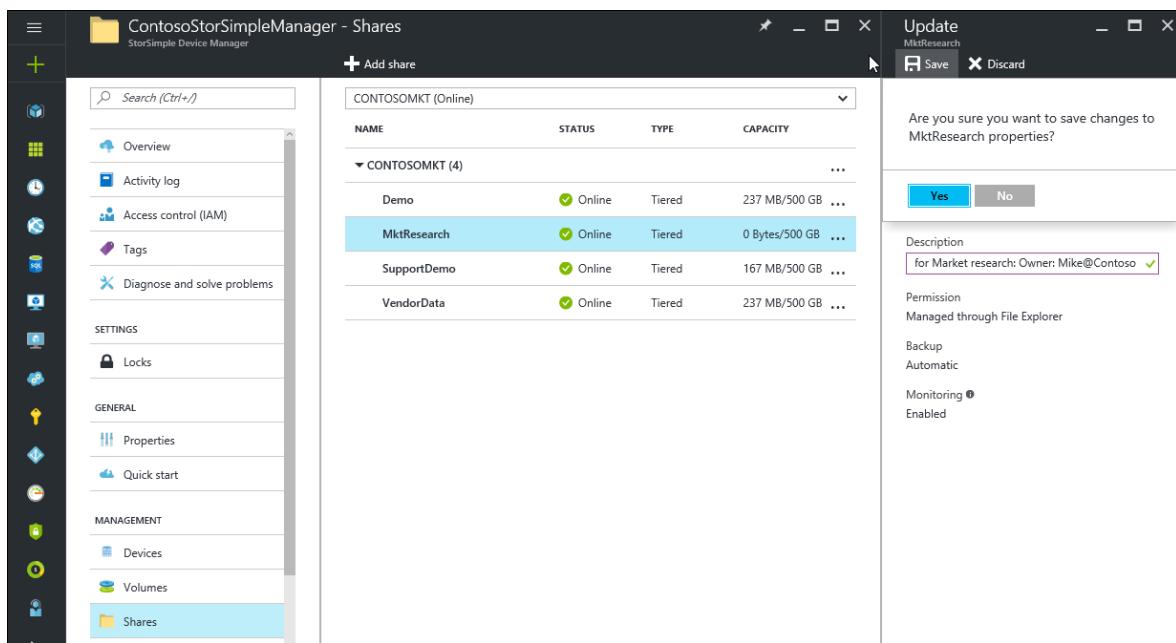


Modify a share

Modify a share when you need to change the description of the share. No other share properties can be modified once the share is created.

To modify a share

1. From the **Shares** setting on the StorSimple service summary blade, select the virtual array on which the share you wish you to modify resides.
2. Select the share to view the current description and modify it.
3. Save your changes by clicking the **Save** command bar. Your specified settings will be applied and you will see a notification.

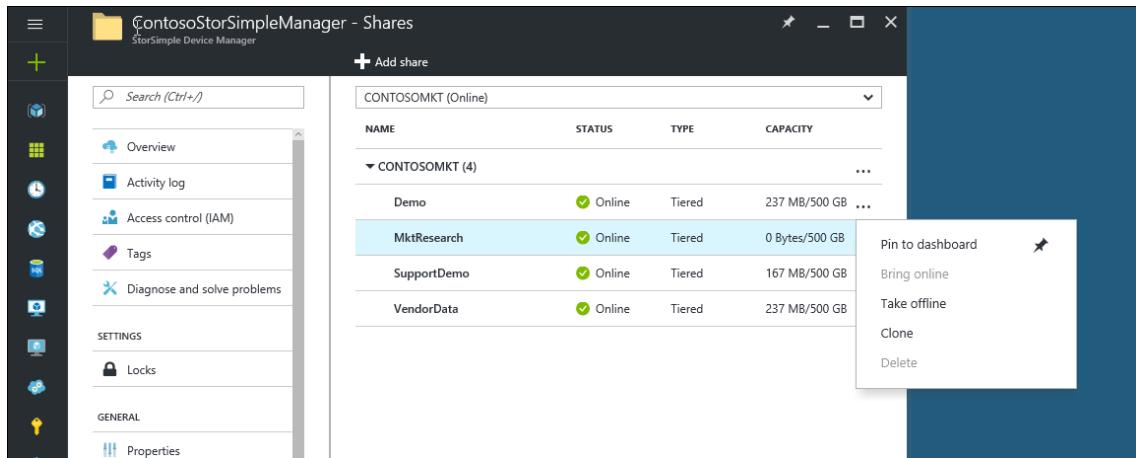


Take a share offline

You may need to take a share offline when you are planning to modify it or delete it. When a share is offline, it is not available for read-write access. You will need to take the share offline on the host as well as on the device.

To take a share offline

1. Make sure that the share in question is not in use before taking it offline.
2. Take the share on the array offline by performing the following steps:
 - a. From the **Shares** setting on the StorSimple service summary blade, select the virtual array on which the share you wish you to take offline resides.
 - b. Select the share and Click ... (alternately right-click in this row) and from the context menu, select **Take offline**.



- c. Review the information in the **Take offline** blade and confirm your acceptance of the operation. Click **Take offline** to take the share offline. You will see a notification of the operation in progress.
- d. To confirm that the share was successfully taken offline, go to the **Shares** blade. You should see the status of the share as offline.

Delete a share

ⓘ Important

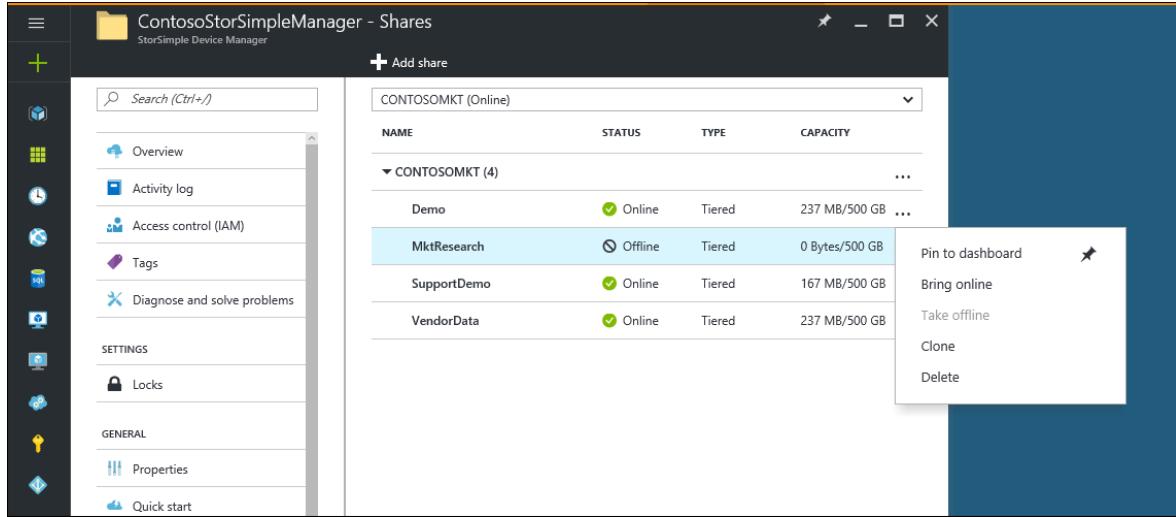
You can delete a share only if it is offline.

Complete the following steps to delete a share.

To delete a share

1. From the **Shares** setting on the StorSimple service summary blade, select the virtual array on which the share you wish to delete resides.

2. Select the share and Click ... (alternately right-click in this row) and from the context menu, select **Delete**.



3. Check the status of the share you want to delete. If the share you want to delete is not offline, take it offline first. Follow the steps in [Take a share offline](#).
4. When prompted for confirmation in the **Delete** blade, accept the confirmation and click **Delete**. The share will now be deleted and the **Shares** blade shows the updated list of shares within the virtual array.

Next steps

Learn how to [clone a StorSimple share](#).

Use StorSimple Device Manager service to manage volumes on the StorSimple Virtual Array

Article • 08/19/2022 • 5 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to use the StorSimple Device Manager service to create and manage volumes on your StorSimple Virtual Array.

The StorSimple Device Manager service is an extension in the Azure portal that lets you manage your StorSimple solution from a single web interface. In addition to managing shares and volumes, you can use the StorSimple Device Manager service to view and manage devices, view alerts, and view and manage backup policies and the backup catalog.

Volume Types

StorSimple volumes can be:

- **Locally pinned:** Data in these volumes stays on the array at all times and does not spill to the cloud.
- **Tiered:** Data in these volumes can spill to the cloud. When you create a tiered volume, approximately 10 % of the space is provisioned on the local tier and 90 % of the space is provisioned in the cloud. For example, if you provisioned a 1 TB volume, 100 GB would reside in the local space and 900 GB would be used in the cloud when the data tiers. This in turn implies that if you run out of all the local

space on the device, you cannot provision a tiered volume (because the 10 % required on the local tier will not be available).

Provisioned capacity

Refer to the following table for maximum provisioned capacity for each volume type.

Limit identifier	Limit
Minimum size of a tiered volume	500 GB
Maximum size of a tiered volume	5 TB
Minimum size of a locally pinned volume	50 GB
Maximum size of a locally pinned volume	200 GB

The Volumes blade

The **Volumes** menu on your StorSimple service summary blade displays the list of storage volumes on a given StorSimple array and allows you to manage them.

NAME	STATUS	TYPE	CAPACITY
Demo	Online	Tiered	170 MB/500 GB
Ellen-Demo	Online	Tiered	170 MB/500 GB
Specs	Online	Tiered	170 MB/500 GB
TestVolume	Offline	Tiered	170 MB/500 GB

A volume consists of a series of attributes:

- **Volume Name** – A descriptive name that must be unique and helps identify the volume.
- **Status** – Can be online or offline. If a volume is offline, it is not visible to initiators (servers) that are allowed access to use the volume.
- **Type** – Indicates whether the volume is **Tiered** (the default) or **Locally pinned**.
- **Capacity** – specifies the amount of data used as compared to the total amount of data that can be stored by the initiator (server).
- **Backup** – In case of the StorSimple Virtual Array, all volumes are automatically enabled for backup.
- **Connected hosts** – Specifies the initiators (servers) that are allowed access to this volume.

The screenshot shows the 'ContosoStorSimpleManager - Volumes' window. On the left, there's a navigation pane with icons for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Locks, Properties, Quick start, Devices, Volumes (which is selected and highlighted in blue), Shares, and Keys. The main area displays a table of volumes under 'CONTOSOENG (4)'. The table has columns for NAME, STATUS, TYPE, and CAPACITY. The 'Demo' volume is selected and highlighted in blue, with a red arrow pointing to it. Other volumes listed are 'Ellen-Demo', 'Specs', and 'TestVolume'. To the right of the table, there's a 'Update' section with fields for Demo, Save, and Discard, and a status summary for the volume.

NAME	STATUS	TYPE	CAPACITY
Demo	Online	Tiered	170 MB/500 GB
Ellen-Demo	Online	Tiered	170 MB/500 GB
Specs	Online	Tiered	170 MB/500 GB
TestVolume	Offline	Tiered	170 MB/500 GB

Update
Demo
Save Discard

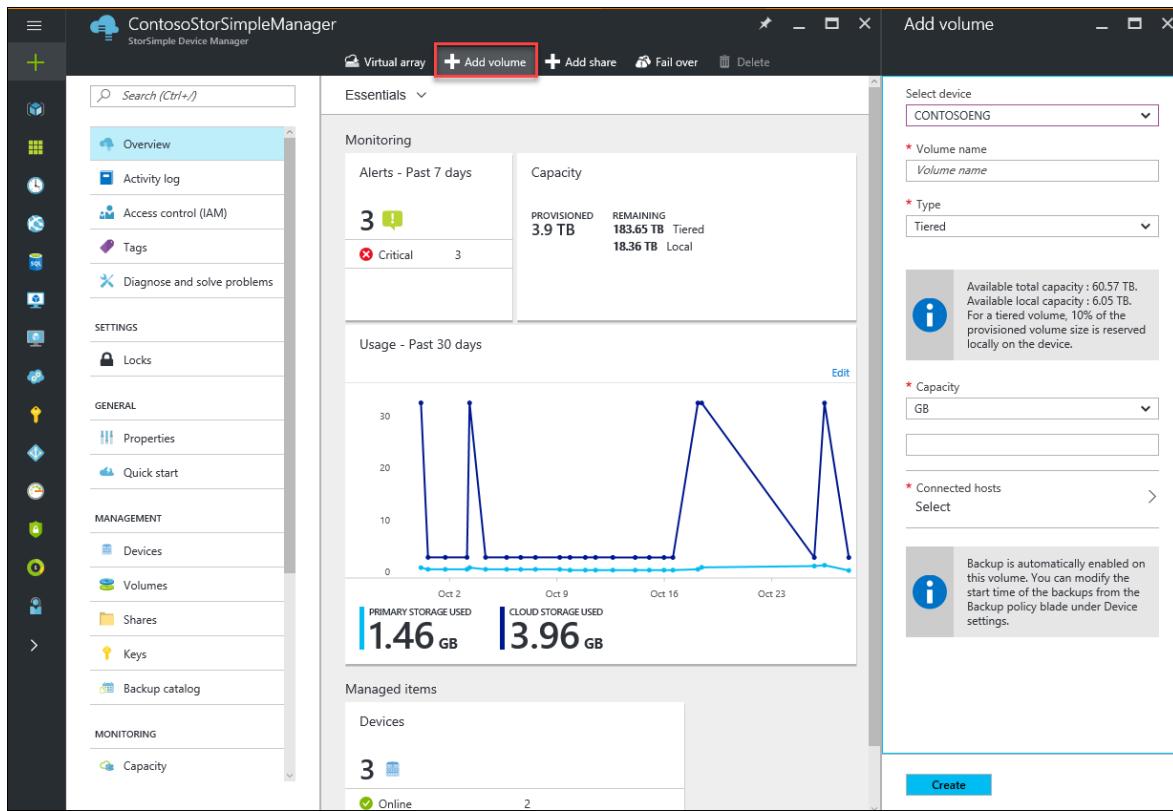
Status Online
Capacity 500 GB
Type Tiered
Backup Automatic
Monitoring Enabled
* Connected hosts EngServer >

Use the instructions in this tutorial to perform the following tasks:

- Add a volume
- Modify a volume
- Take a volume offline
- Delete a volume

Add a volume

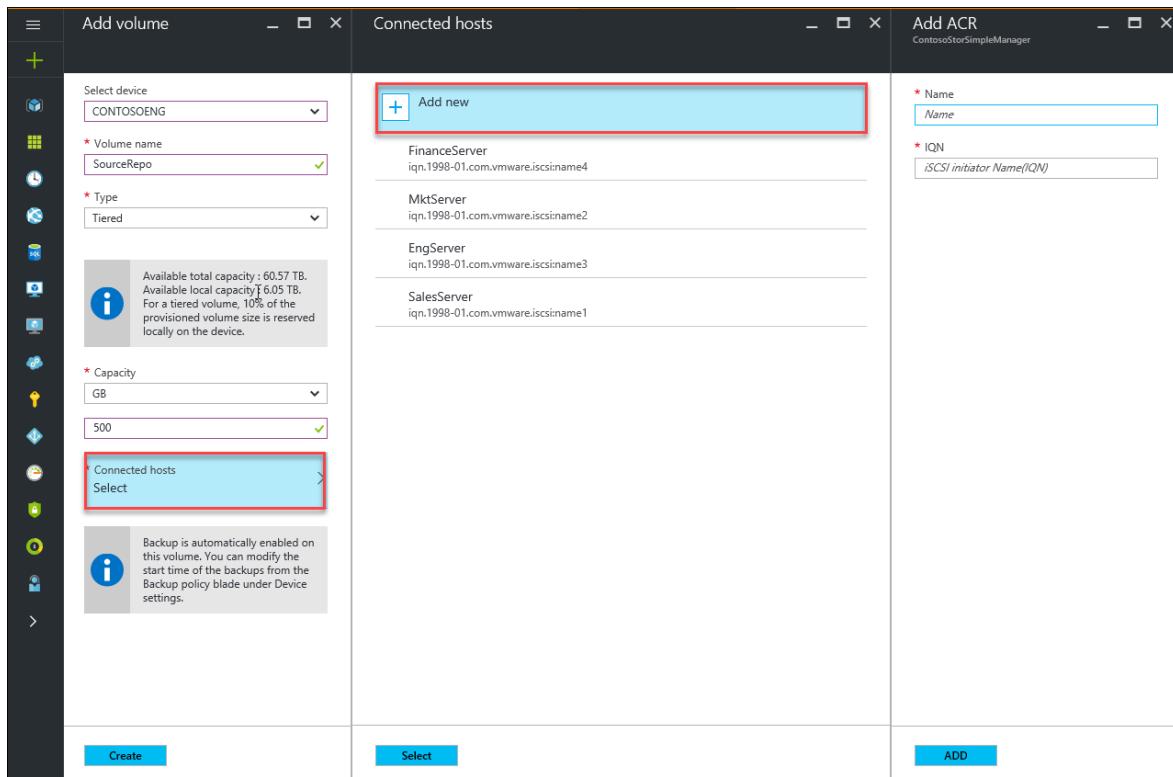
1. From the StorSimple service summary blade, click **+ Add volume** from the command bar. This opens up the **Add volume** blade.



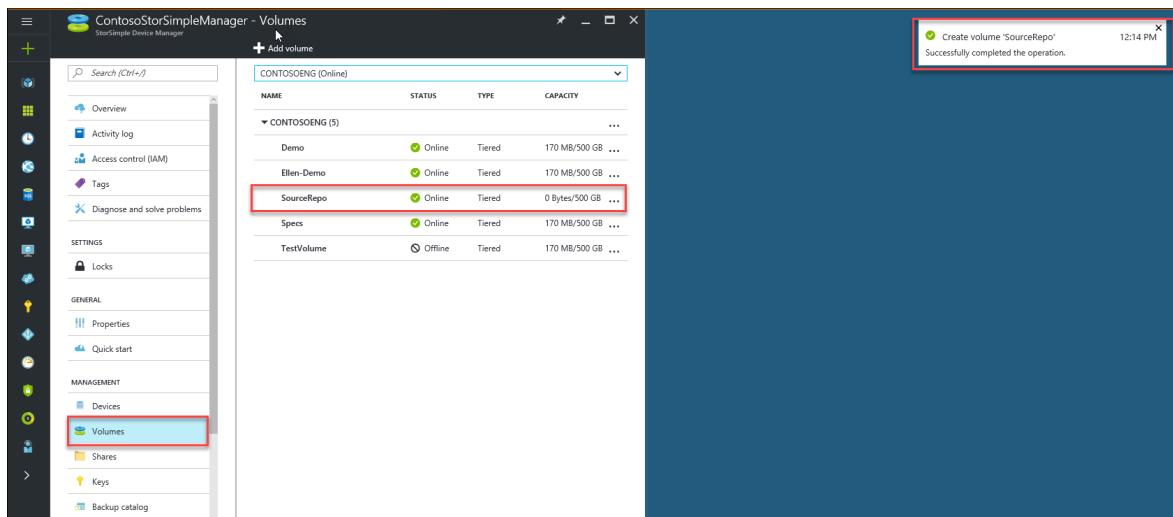
2. In the **Add volume** blade, do the following:

- In the **Volume name** field, enter a unique name for your volume. The name must be a string that contains 3 to 127 characters.
- In the **Type** dropdown list, specify whether to create a **Tiered** or **Locally pinned** volume. For workloads that require local guarantees, low latencies, and higher performance, select **Locally pinned volume**. For all other data, select **Tiered** volume.
- In the **Capacity** field, specify the size of the volume. A tiered volume must be between 500 GB and 5 TB and a locally pinned volume must be between 50 GB and 500 GB.
- Click **Connected hosts**, select an access control record (ACR) corresponding to the iSCSI initiator that you want to connect to this volume, and then click **Select**.

3. To add a new connected host, click **Add new**, enter a name for the host and its iSCSI Qualified Name (IQN), and then click **Add**.



4. When you've finished configuring your volume, click **Create**. A volume will be created with the specified settings and you will see a notification on the successful creation of the same. By default backup will be enabled for the volume.
5. To confirm that the volume was successfully created, go to the **Volumes** blade. You should see the volume listed.

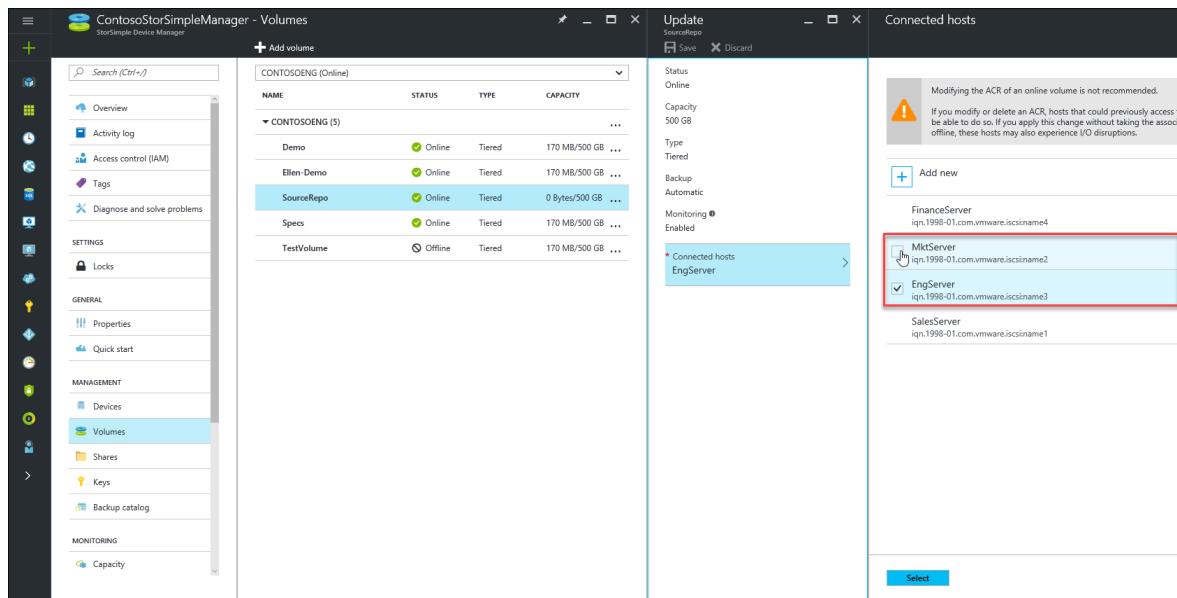


Modify a volume

Modify a volume when you need to change the hosts that access the volume. The other attributes of a volume cannot be modified once the volume has been created.

To modify a volume

- From the **Volumes** setting on the StorSimple service summary blade, select the virtual array on which the volume you wish you to modify resides.
- Select the volume and click **Connected hosts** to view the currently connected host and modify it to a different server.



- Save your changes by clicking the **Save** command bar. Your specified settings will be applied and you will see a notification.

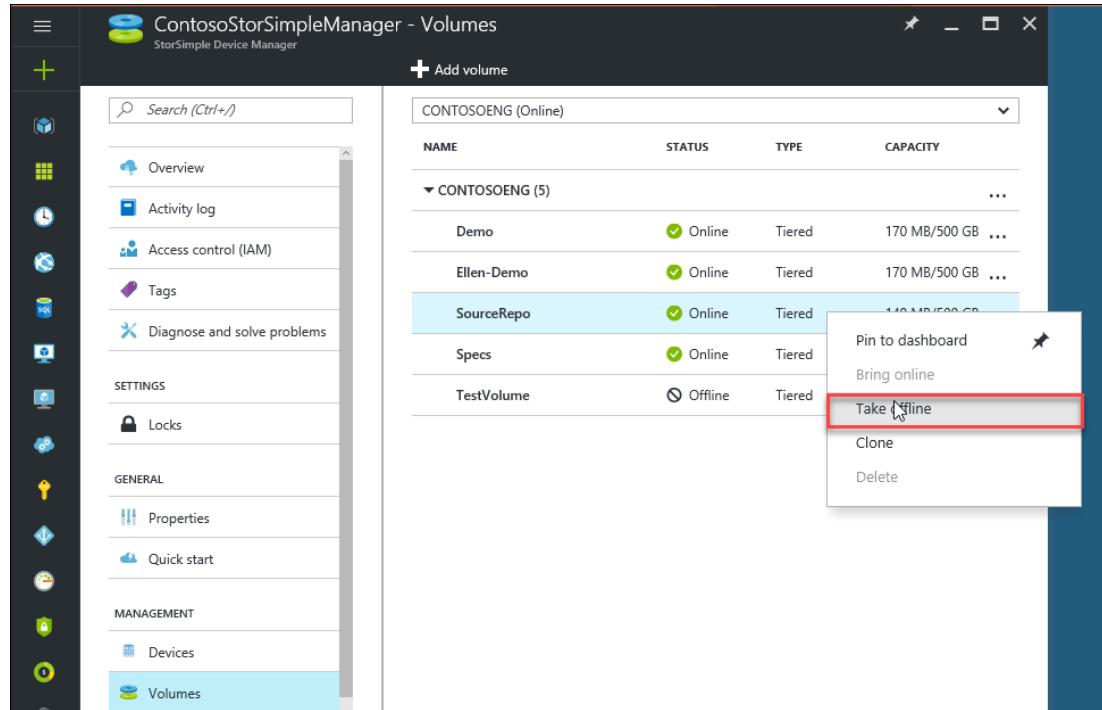
Take a volume offline

You may need to take a volume offline when you are planning to modify it or delete it. When a volume is offline, it is not available for read-write access. You will need to take the volume offline on the host as well as on the device.

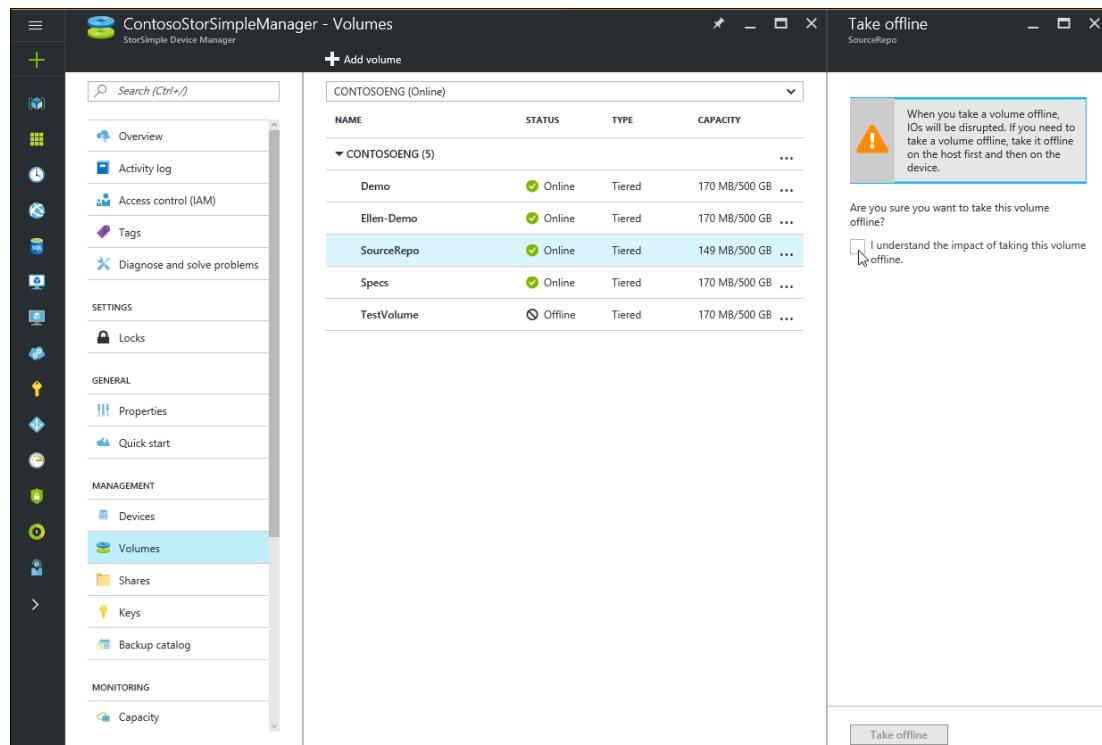
To take a volume offline

- Make sure that the volume in question is not in use before taking it offline.
- Take the volume offline on the host first. This eliminates any potential risk of data corruption on the volume. For specific steps, refer to the instructions for your host operating system.
- After the volume on the host is offline, take the volume on the array offline by performing the following steps:
 - From the **Volumes** setting on the StorSimple service summary blade, select the virtual array on which the volume you wish you to take offline resides.

- Select the volume and click ... (alternately right-click in this row) and from the context menu, select Take offline.



- Review the information in the **Take offline** blade and confirm your acceptance of the operation. Click **Take offline** to take the volume offline. You will see a notification of the operation in progress.
- To confirm that the volume was successfully taken offline, go to the **Volumes** blade. You should see the status of the volume as offline.



Delete a volume

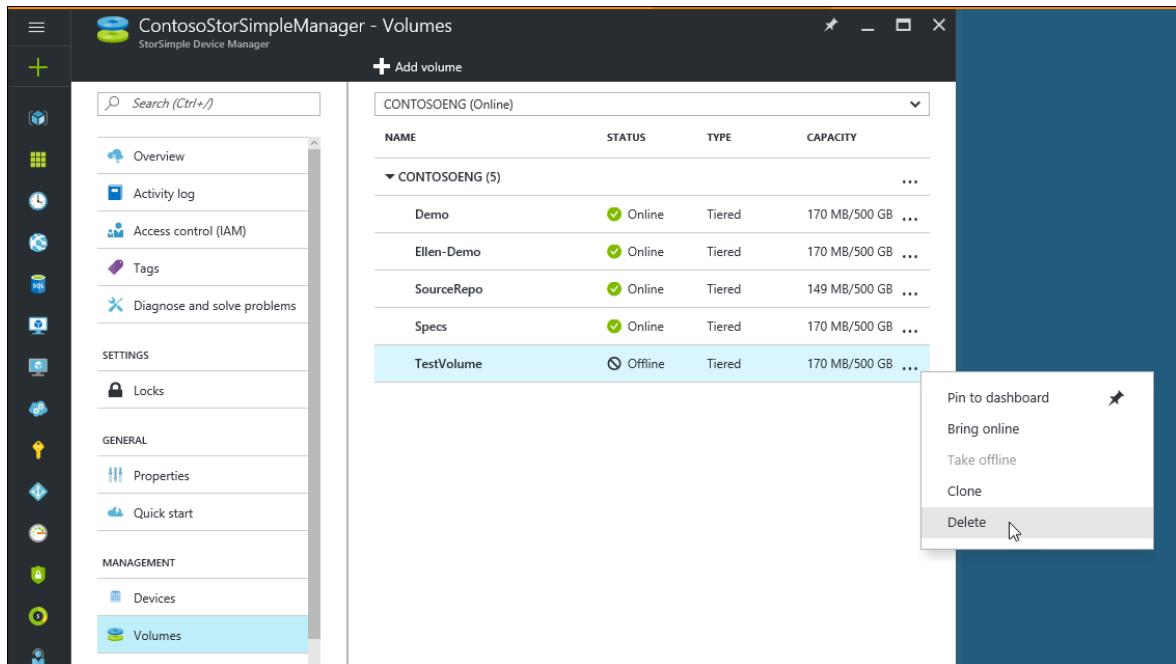
ⓘ Important

You can delete a volume only if it is offline.

Complete the following steps to delete a volume.

To delete a volume

1. From the **Volumes** setting on the StorSimple service summary blade, select the virtual array on which the volume you wish you to delete resides.
2. Select the volume and click ... (alternately right-click in this row) and from the context menu, select **Delete**.



3. Check the status of the volume you want to delete. If the volume you want to delete is not offline, take it offline first, following the steps in [Take a volume offline](#).
4. When prompted for confirmation in the **Delete** blade, accept the confirmation and click **Delete**. The volume will now be deleted and the **Volumes** blade will show the updated list of volumes within the virtual array.

Next steps

Learn how to [clone a StorSimple volume](#).

Use the service summary blade for StorSimple Device Manager connected to StorSimple Virtual Array

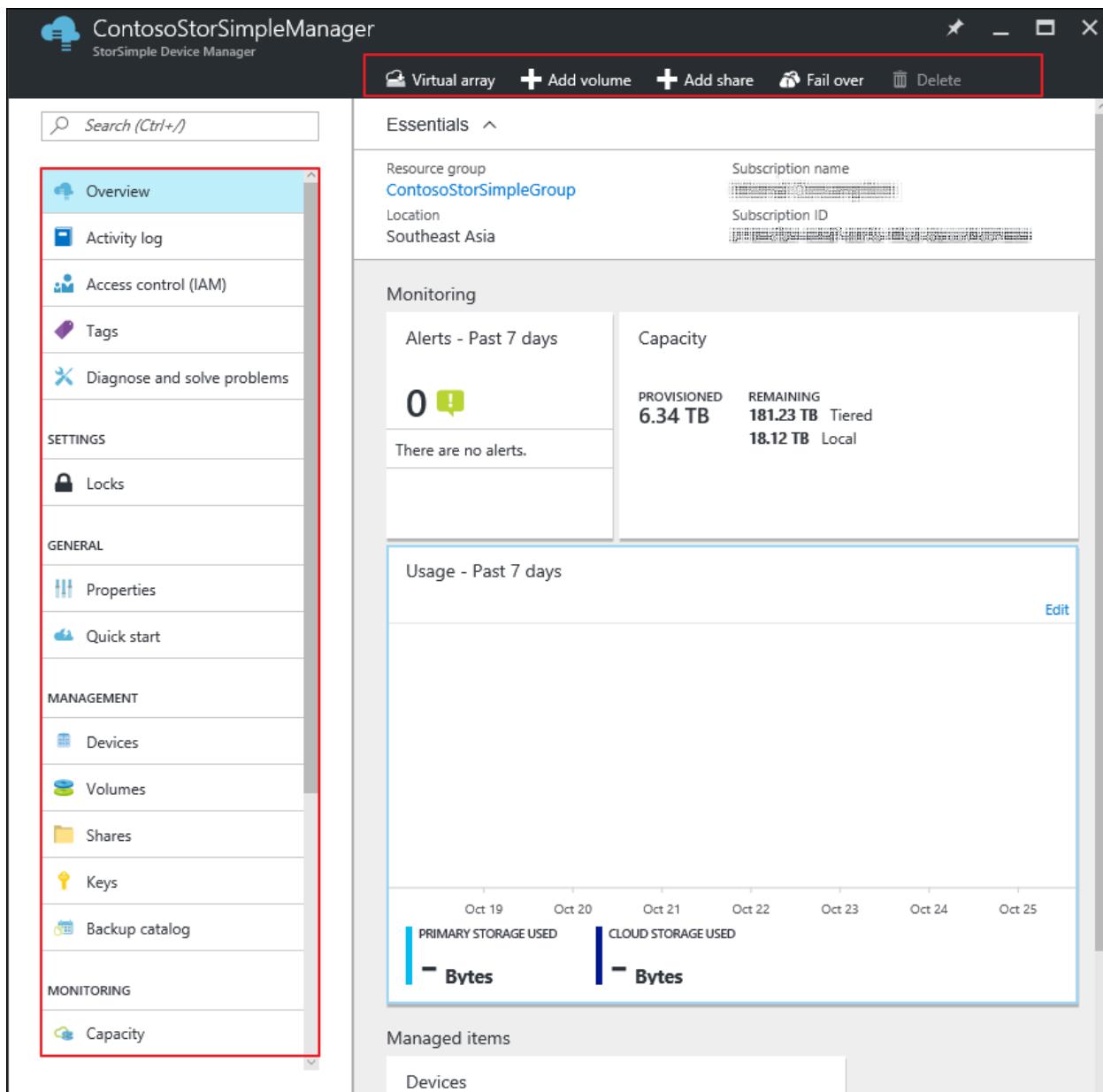
Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The service summary blade for the StorSimple Device Manager provides a summary view of the StorSimple Virtual Arrays (also known as StorSimple on-premises virtual devices or virtual devices) that are connected to your service, highlighting those that need a system administrator's attention. This tutorial introduces the service summary blade, explains the content and function, and describes the tasks that you can perform from this blade.



Management commands and essentials

In the StorSimple summary blade, you see the options for managing your StorSimple Device Manager service as well as the virtual arrays registered to this service. You see the management commands across the top of the blade and on the left side.

Use these options to perform various operations such as add shares or volumes, or monitor the various jobs running on the virtual arrays.

The essentials area captures some of the important properties such as, the resource group, location, and subscription in which your StorSimple Device Manager was created.

StorSimple Device Manager service summary

- The **Alerts** tile provides a snapshot of all the active alerts across all virtual devices, grouped by alert severity. Clicking the tile opens the **Alerts** blade, where you can click an individual alert to view additional details about that alert, including any recommended actions. You can also clear the alert if the issue has been resolved.
- The **Capacity** tile displays shows the primary storage that is provisioned and remaining across all virtual devices relative to the total storage available across all virtual devices. **Provisioned** refers to the amount of storage that is prepared and allocated for use, **Remaining** refers to the remaining capacity that can be provisioned across all virtual devices. The **Remaining Tiered** capacity is the available capacity that can be provisioned including cloud, while the **Remaining Local** is the capacity remaining on the disks attached to the virtual arrays.
- In the **Usage** chart, you can see the relevant metrics for your virtual devices. You can view the primary storage used across all virtual devices, as well as the cloud storage consumed by virtual devices over the past 7 days, the default time period. Use the **Edit** option in the top-right corner of the chart to choose a different time scale.
- The **Devices** tile provides a summary of the number of virtual arrays in your StorSimple Device Manager grouped by device status. Click this tile to open the **Devices** list blade and then click an individual device to drill into the device summary specific to the device. You can also perform device specific actions from a given device summary blade. For more information about the device summary blade, go to [Device summary blade](#).

View the activity logs

To view the various operations carried out within your StorSimple Device Manager, click the **Activity logs** link on the left side of your StorSimple service summary blade. This takes you to the **Activity logs** blade, where you can see a summary of the recent operations carried out.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Write Shares	Accepted	7 d ago	Tue Oct 18 2...	Internal Consumption	administrator@contoso.com
Clone	Accepted	7 d ago	Tue Oct 18 2...	Internal Consumption	administrator@contoso.com
GetActivationKey	Succeeded	7 d ago	Tue Oct 18 2...	Internal Consumption	administrator@contoso.com
GetActivationKey	Succeeded	7 d ago	Tue Oct 18 2...	Internal Consumption	administrator@contoso.com

Next steps

Learn how to [use the local web UI to administer your StorSimple Virtual Array](#).

Use the device summary blade for StorSimple Device Manager connected to StorSimple Virtual Array

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager device blade provides a summary view of a StorSimple Virtual Array that is registered with a given StorSimple Device Manager, highlighting those device issues that need a system administrator's attention. This tutorial introduces the device summary blade, explains the content and function, and describes the tasks that you can perform from this blade.

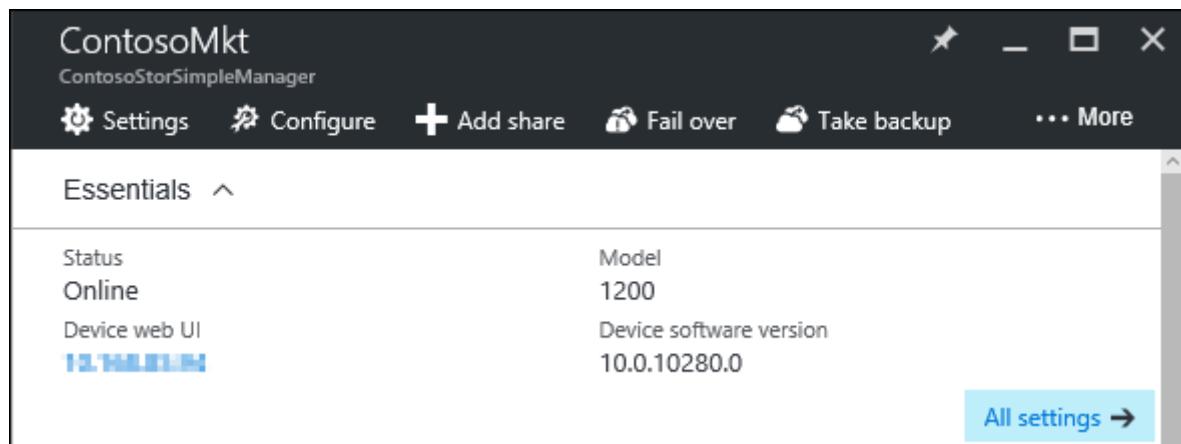
The device summary blade displays the following information:

The screenshot shows the StorSimple device blade interface. At the top, there's a navigation bar with links for Settings, Configure, Add share, Fail over, Take backup, and More. The 'More' link is highlighted with a red box. Below the navigation bar, the 'Essentials' section is open, displaying the 'Monitoring' area. It includes a summary of alerts (0), capacity (Provisioned 3.41 TB, Remaining 59.11 TB Tiered, 5.91 TB Local), and usage (Past 24 hours). A timeline chart shows storage usage from 6 PM to 12 PM on Oct 25, categorized by Primary Storage Used, Cloud Storage Used, and Local Storage Used. The 'Shares' section under Managed items shows 7 shares, all of which are online.

Management

In the StorSimple device blade, you see the options for managing your StorSimple device. You see the management commands across the top of the blade and on the left side. Use these options to add shares or volumes, or update or fail over your virtual array.

The essentials area captures some of the important properties such as, the status, model, software version as well as a link to the [Web UI](#) of the array. If you are on an internal network, you can directly launch the [local web UI](#) to administer your virtual array.



StorSimple device summary

- The **Alerts** tile provides a snapshot of all the active alerts for your virtual array, grouped by alert severity. Click the tile to open the **Alerts** blade and then click an individual alert to view additional details about that alert, including any recommended actions. You can also clear the alert if the issue has been resolved.
- The **Capacity** tile displays the primary storage that is provisioned and remaining across the virtual device relative to the total storage available for the same. **Provisioned** refers to the amount of storage that is prepared and allocated for use, **Remaining** refers to the remaining capacity that can be provisioned across this device. The **Remaining Tiered** capacity is the available capacity that can be provisioned including cloud, while the **Remaining Local** is the capacity remaining on the disks attached to this virtual array.
- In the **Usage** chart, you can view the primary storage used across your virtual array, as well as the cloud storage consumed over the past 7 days, the default time period. Use the **Edit** option in the top-right corner of the chart to choose a different time scale.
- The **Shares or Volumes** tile provides a summary of the number of shares or volumes in your device grouped by status. Click the tile to open the **Shares or Volumes** list blade, and then click on an individual share or volume to view or modify its properties. For more information, see how to [manage shares](#) or [manage volumes](#).

Next steps

Learn how to:

- [Manage shares on a StorSimple Virtual Array](#)

- Manage volumes on a StorSimple Virtual Array

Use StorSimple Device Manager to manage storage account credentials for StorSimple Virtual Array

Article • 08/19/2022 • 7 minutes to read

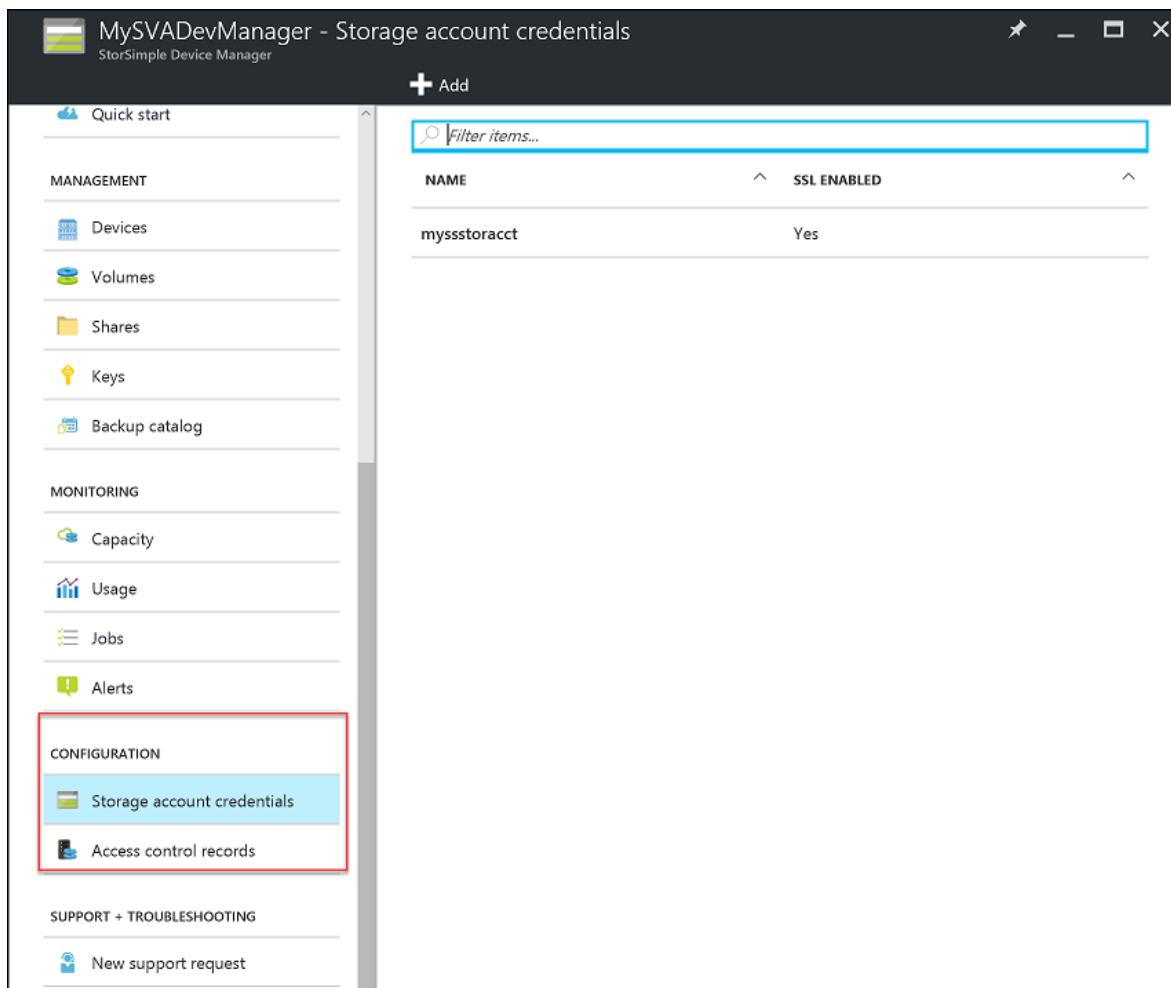
⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Configuration section of the StorSimple Device Manager service blade of your StorSimple Virtual Array presents the global service parameters that can be created in the StorSimple Manager service. These parameters can be applied to all the devices connected to the service, and include:

- Storage account credentials
- Access control records

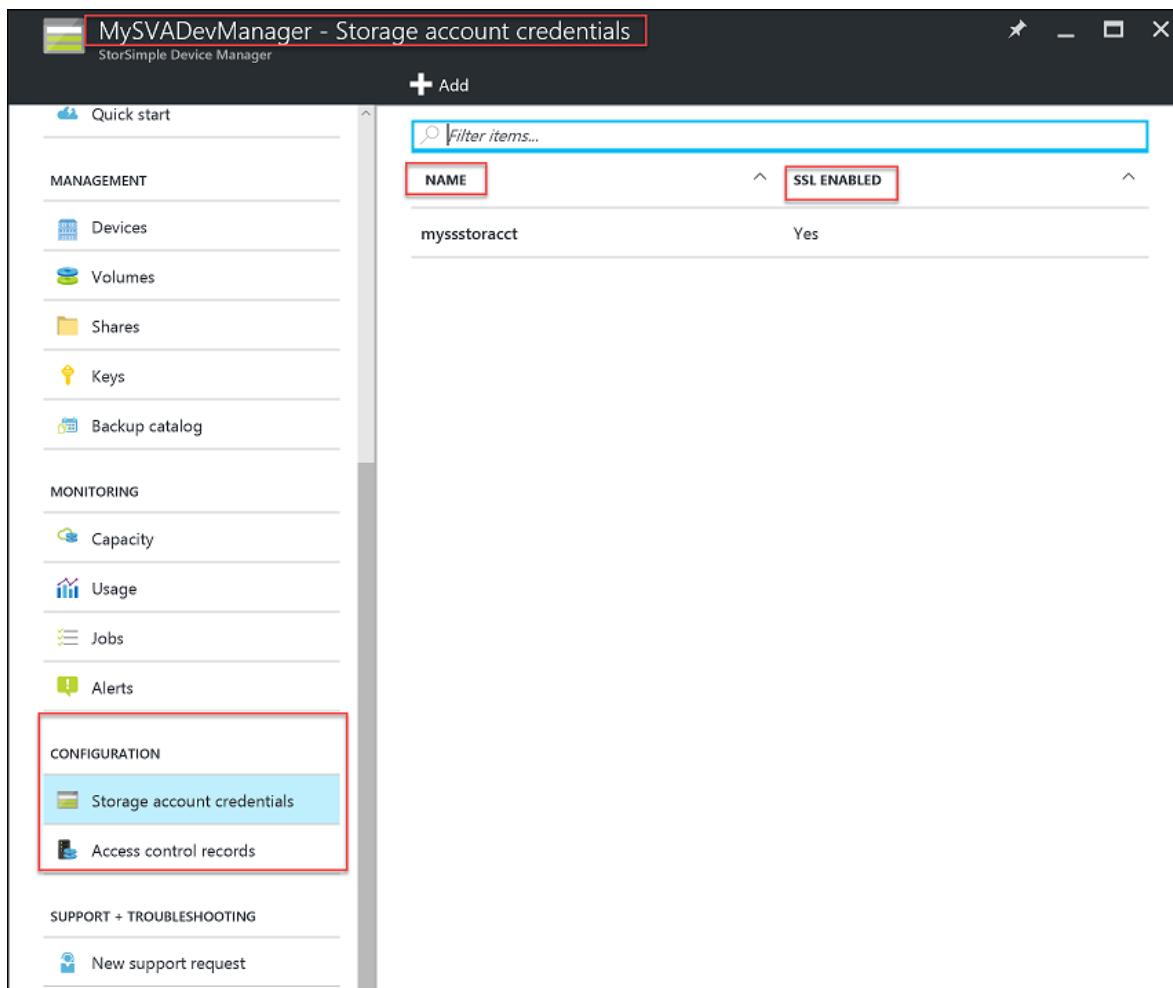


This tutorial explains how you can add, edit, or delete storage account credentials for your StorSimple Virtual Array. The information in this tutorial only applies to the StorSimple Virtual Array. For information on how to manage storage accounts in 8000 series, see [Use the StorSimple Manager service to manage your storage account](#).

Storage account credentials contain the credentials that the device uses to access your storage account with your cloud service provider. For Microsoft Azure storage accounts, these are credentials such as the account name and the primary access key.

On the **Storage account credentials** blade, all storage account credentials that are created for the billing subscription are displayed in a tabular format containing the following information:

- **Name** – The unique name assigned to the account when it was created.
- **SSL enabled** – Whether the TLS is enabled and device-to-cloud communication is over the secure channel.



The most common tasks related to storage account credentials that can be performed on the **Storage account credentials** blade are:

- Add a storage account credential
- Edit a storage account credential
- Delete a storage account credential

Types of storage account credentials

There are three types of storage account credentials that can be used with your StorSimple device.

- **Auto-generated storage account credentials** – As the name suggests, this type of storage account credential is automatically generated when the service is first created. To learn more about how this storage account credential is created, see [Create a new service](#).
- **storage account credentials in the service subscription** – These are the Azure storage account credentials that are associated with the same subscription as that of the service. To learn more about how these storage account credentials are created, see [About Azure Storage Accounts](#).

- **storage account credentials outside of the service subscription** – These are the Azure storage account credentials that are not associated with your service and likely existed before the service was created.

Add a storage account credential

You can add a storage account credential to your StorSimple Device Manager service configuration by providing a unique friendly name and access credentials that are linked to the storage account. You also have the option of enabling the Transport Layer Security (TLS) mode, previously known as Secure Sockets Layer (SSL) mode, to create a secure channel for network communication between your device and the cloud.

You can create multiple accounts for a given cloud service provider. While the storage account credential is being saved, the service attempts to communicate with your cloud service provider. The credentials and the access material that you supplied are authenticated at this time. A storage account credential is created only if the authentication succeeds. If the authentication fails, then an appropriate error message is displayed.

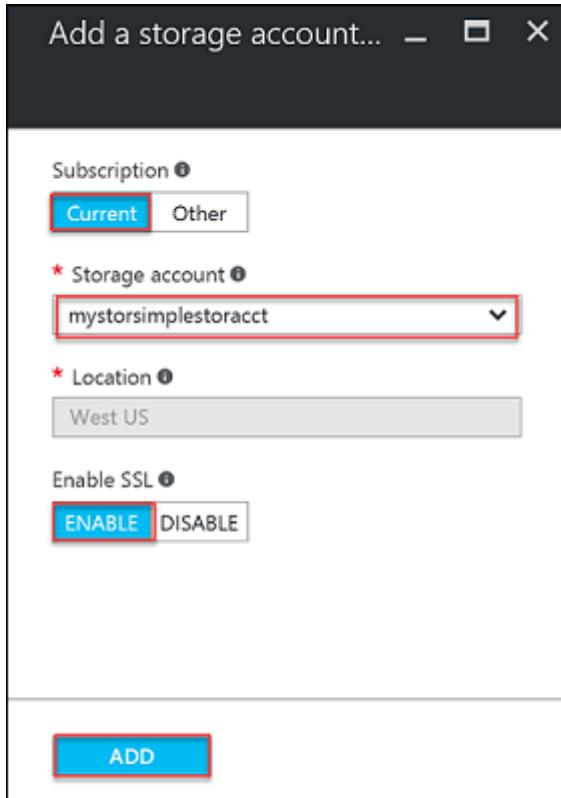
Use the following procedures to add Azure storage account credentials:

- To add a storage account credential that has the same Azure subscription as the Device Manager service
- To add an Azure storage account credential that is outside of the Device Manager service subscription

To add a storage account credential that has the same Azure subscription as the Device Manager service

1. Navigate to your Device Manager service, select and double-click it. This opens the **Overview** blade.
2. Select **Storage account credentials** within the **Configuration** section.
3. Click **Add**.
4. In the **Add a storage account** blade, do the following:
 - a. For **Subscription**, select **Current**.
 - b. Provide the name of your Azure storage account.

- c. Select **Enable** to create a secure channel for network communication between your StorSimple device and the cloud. Select **Disable** only if you are operating within a private cloud.
- d. Click **Add**. You are notified after the storage account is successfully created.

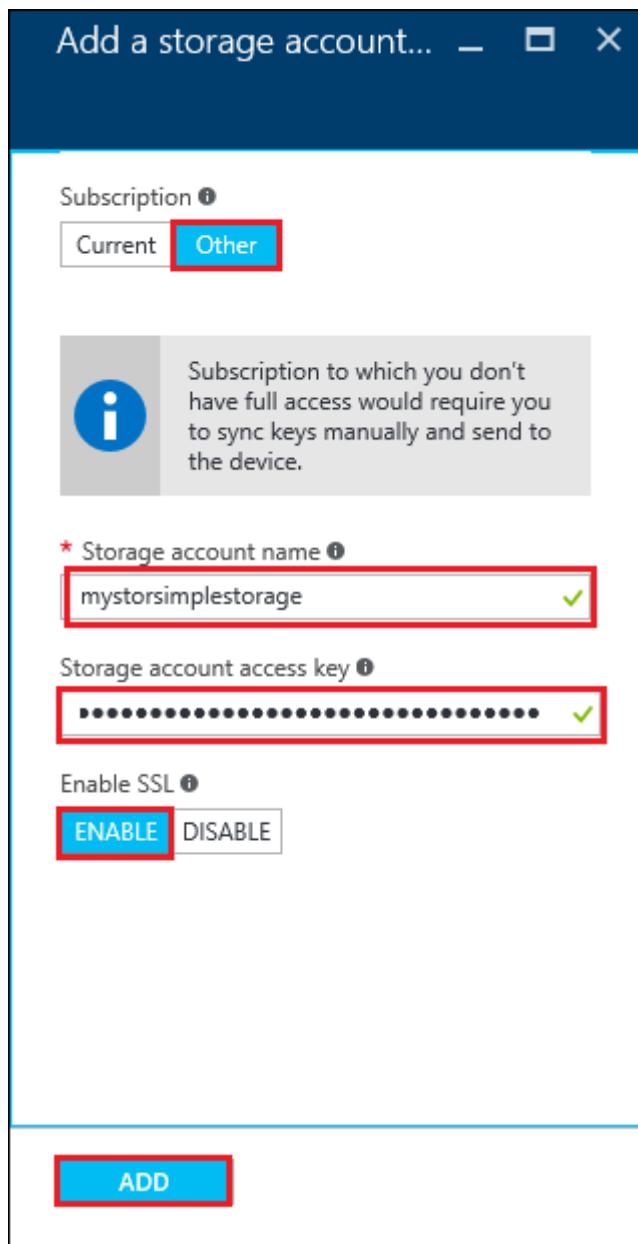


To add an Azure storage account credential that is outside of the Device Manager service subscription

1. Navigate to your Device Manager service, select and double-click it. This opens the **Overview** blade.
2. Select **Storage account credentials** within the **Configuration** section. This lists any existing storage account credentials associated with the StorSimple Device Manager service.
3. Click **Add**.
4. In the **Add a storage account** blade, do the following:
 - a. For **Subscription**, select **Other**.
 - b. Provide the name of your Azure storage account credential.
 - c. In the **Storage account access key** text box, supply the primary Access Key for your Azure storage account credential. To get this key, go to the Azure Storage

service, select your storage account credential, and click **Manage account keys**. You can now copy the primary access key.

- d. To enable TLS, click the **Enable** button to create a secure channel for network communication between your StorSimple Device Manager service and the cloud. Click the **Disable** button only if you are operating within a private cloud.
 - e. Click **Add**. You are notified after the storage account credential is successfully created.
5. The newly created storage account credential is displayed on the StorSimple Configure Device Manager service blade under **Storage account credentials**.

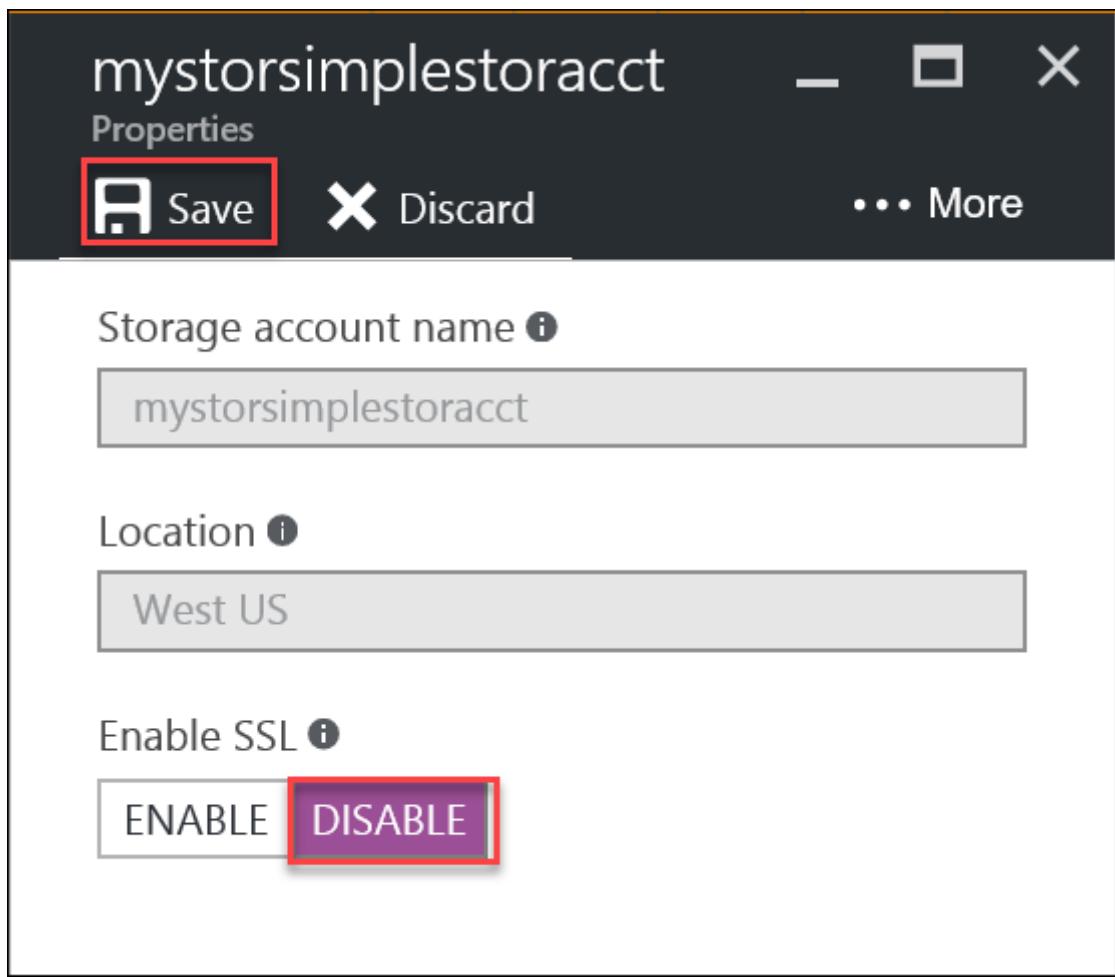


Edit a storage account credential

You can edit a storage account credential used by your device. If you edit a storage account credential that is currently in use, the fields available to modify are the access key and the TLS mode for the storage account credential. You can supply the new storage access key or modify the **Enable SSL mode** selection and save the updated settings.

To edit a storage account credential

1. Navigate to your Device Manager service, select and double-click it. This opens the **Overview** blade.
2. Select **Storage account credentials** within the **Configuration** section. This lists any existing storage account credentials associated with the StorSimple Device Manager service.
3. In the tabular list of storage account credentials, select and double-click the account that you want to modify.
4. In the storage account credential **Properties** blade, do the following:
 - a. If necessary, you can modify the **Enable SSL** mode selection.
 - b. You can choose to regenerate your storage account credential access keys. For more information, see [Manage storage account access keys](#). Supply the new storage account credential key. For an Azure storage account, this is the primary access key.
 - c. Click **Save** at the top of the **Properties** blade to save the settings. The settings are updated on the **Storage account credentials** blade.



Delete a storage account credential

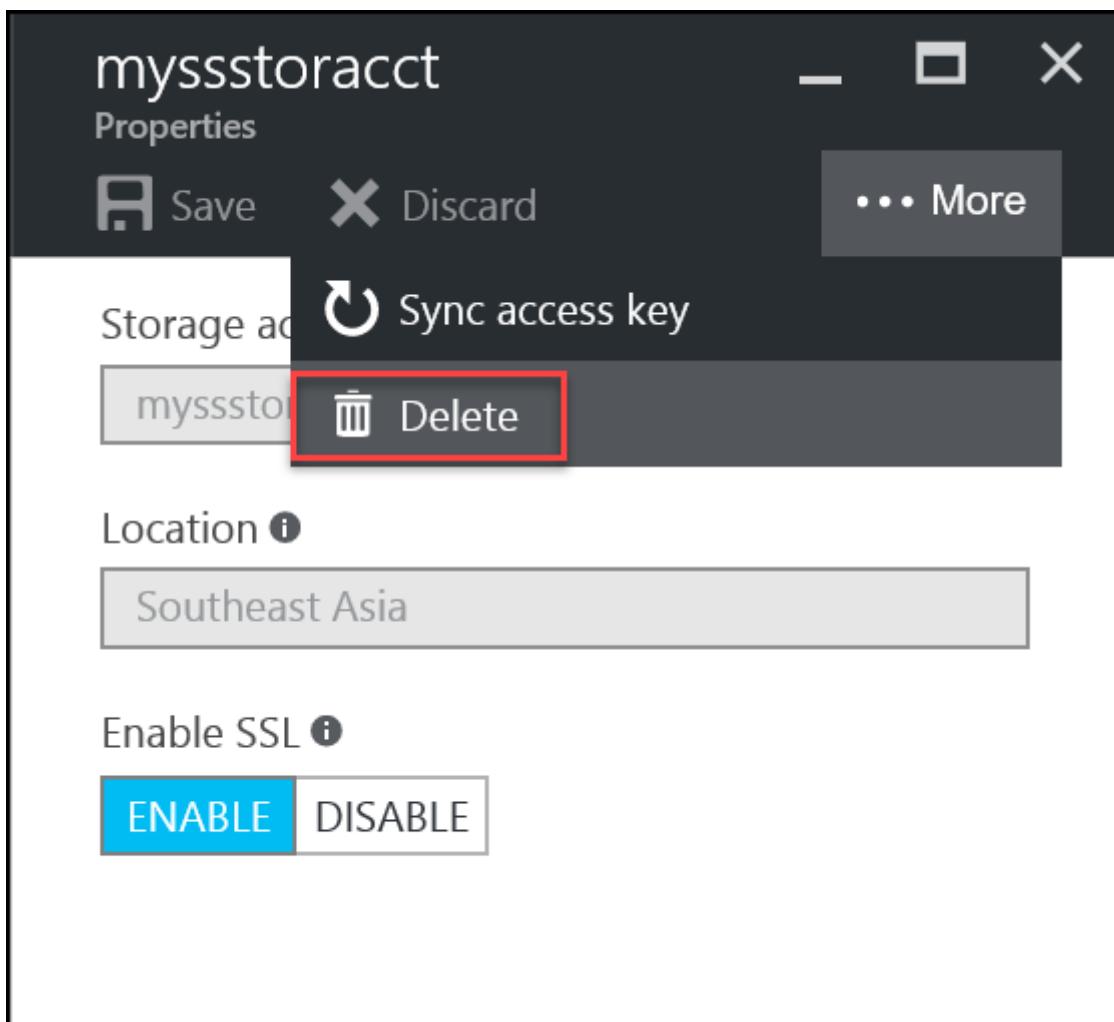
ⓘ Important

You can delete a storage account credential only if it is not in use. If a storage account credential is in use, you are notified.

To delete a storage account credential

1. Navigate to your Device Manager service, select and double-click it. This opens the **Overview** blade.
2. Select **Storage account credentials** within the **Configuration** section. This lists any existing storage account credentials associated with the StorSimple Device Manager service.
3. In the tabular list of storage account credentials, select and double-click the account that you want to delete.
4. In the storage account credential **Properties** blade, do the following:

- a. Click **Delete** to delete the credentials.
- b. When prompted for confirmation, click **Yes** to continue with the deletion. The tabular listing is updated to reflect the changes.



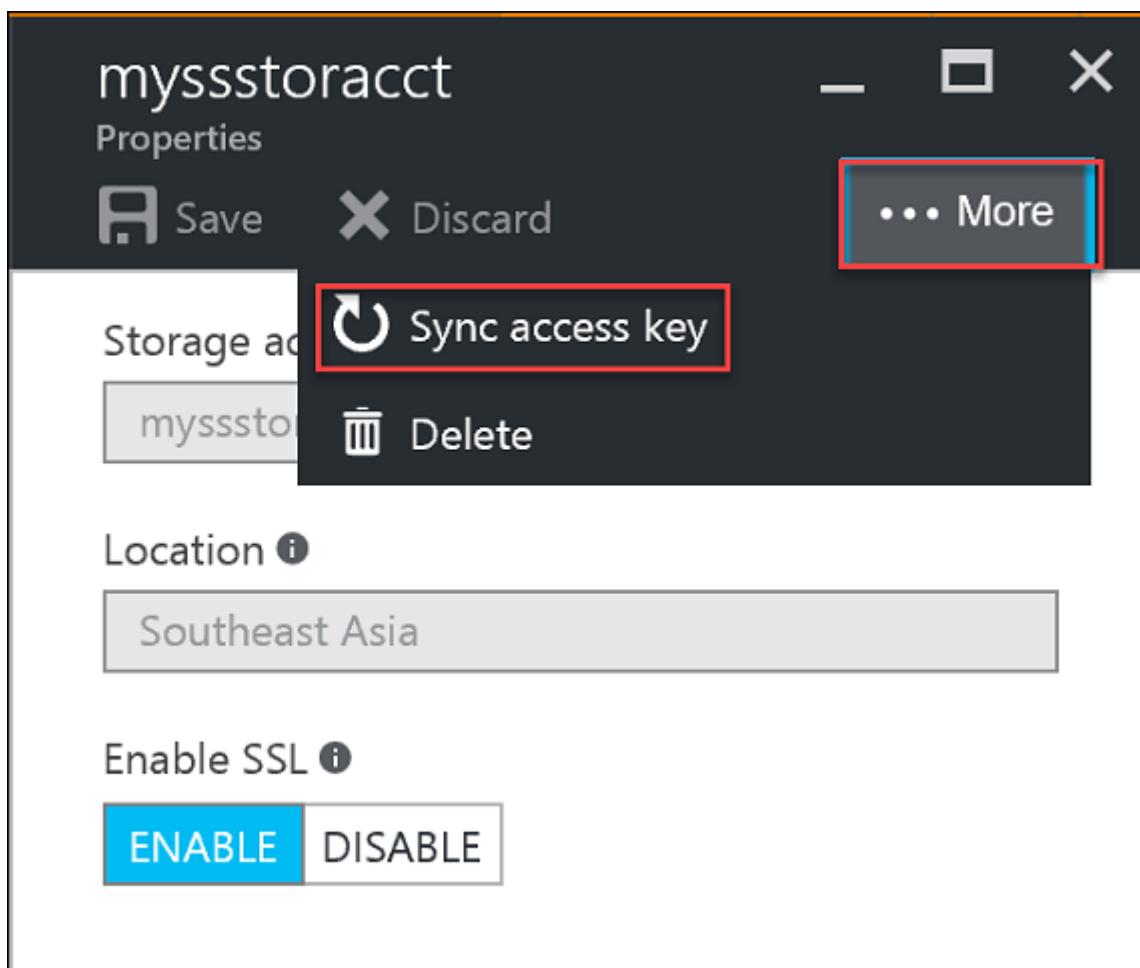
Synchronizing storage account credential keys

For security reasons, key rotation is often a requirement in data centers. A Microsoft Azure administrator can regenerate or change the primary or secondary key by directly accessing the storage account credential (via the Microsoft Azure Storage service). The StorSimple Device Manager service does not see this change automatically.

To inform the StorSimple Device Manager service of the change, you need to access the StorSimple Device Manager service, access the storage account credential, and then synchronize the primary or secondary key (depending on which one was changed). The service then gets the latest key, encrypts the keys, and sends the encrypted key to the device.

To synchronize keys for storage account credentials in the same subscription as the service (Azure only)

1. On the service landing blade, select your service, double-click the service name, and then in the **Configuration** section, click **Storage account credentials**.
2. On the **Storage account credentials** blade, in the list of Storage account credentials, select the storage account credential whose keys that you want to synchronize.
3. In the **Properties** blade for the selected storage account credential, do the following:
 - a. Click **More**, and then click **Sync access key**.
 - b. When prompted for confirmation, click **Sync key** to complete the synchronization.
4. In the StorSimple Device Manager service, you need to update the key that was previously changed in the Microsoft Azure Storage service. In the **Synchronize storage account key** blade, if the primary access key was changed (regenerated), click **Primary**, and then click **Sync Key**. If the secondary key was changed, click **Secondary**, and then click **Sync Key**.



Next steps

- Learn how to [administer your StorSimple Virtual Array](#).

Use StorSimple Device Manager to manage access control records for StorSimple Virtual Array

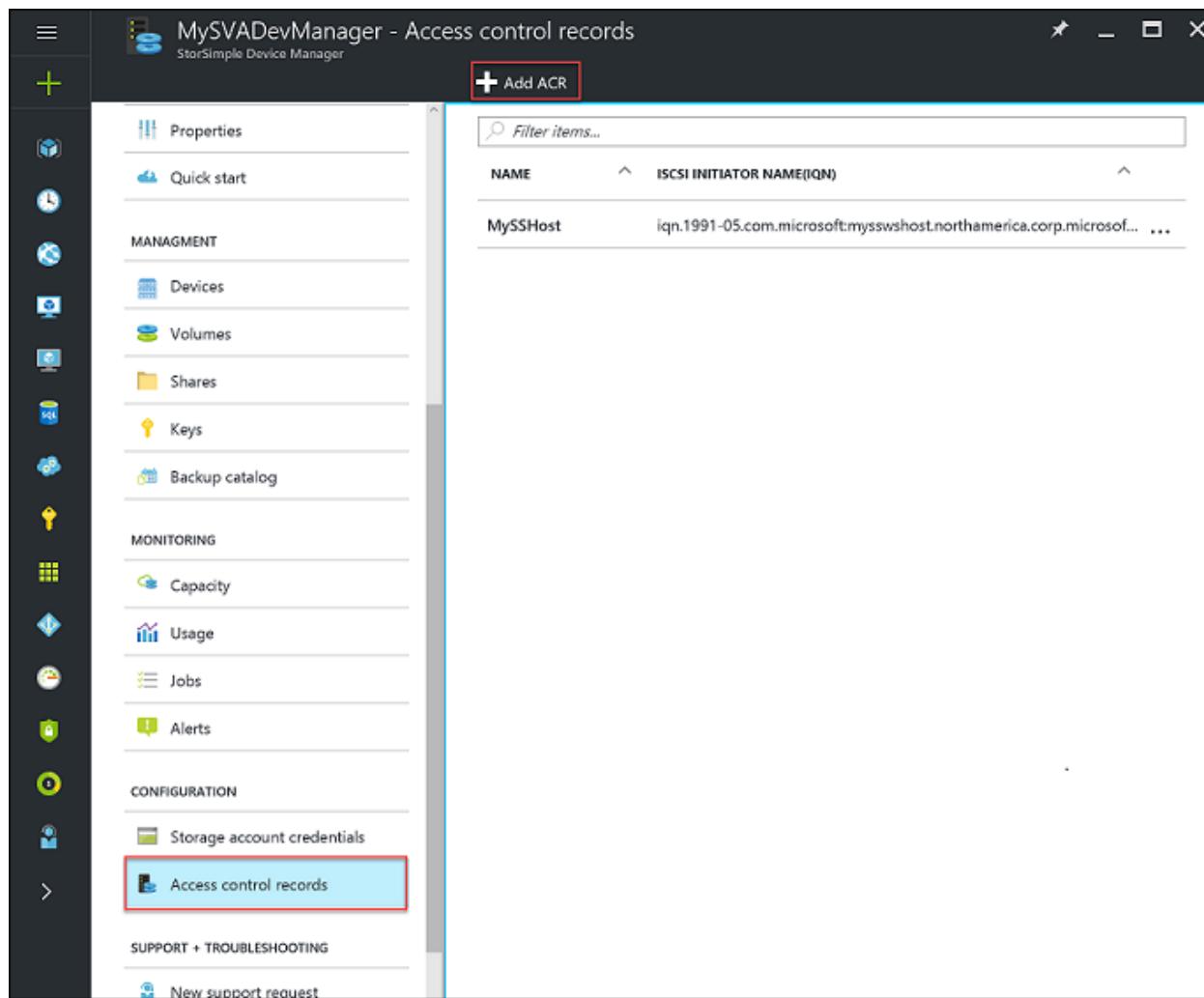
Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Access control records (ACRs) allow you to specify which hosts can connect to a volume on the StorSimple Virtual Array (also known as the StorSimple on-premises virtual device). ACRs are set to a specific volume and contain the iSCSI Qualified Names (IQNs) of the hosts. When a host tries to connect to a volume, the device checks the ACR associated with that volume for the IQN name, and if there is a match, then the connection is established. The **Access control records** blade within the **Configuration** section of your Device Manager service displays all the access control records with the corresponding IQNs of the hosts.



This tutorial explains the following common ACR-related tasks:

- Get the IQN
- Add an access control record
- Edit an access control record
- Delete an access control record

ⓘ Important

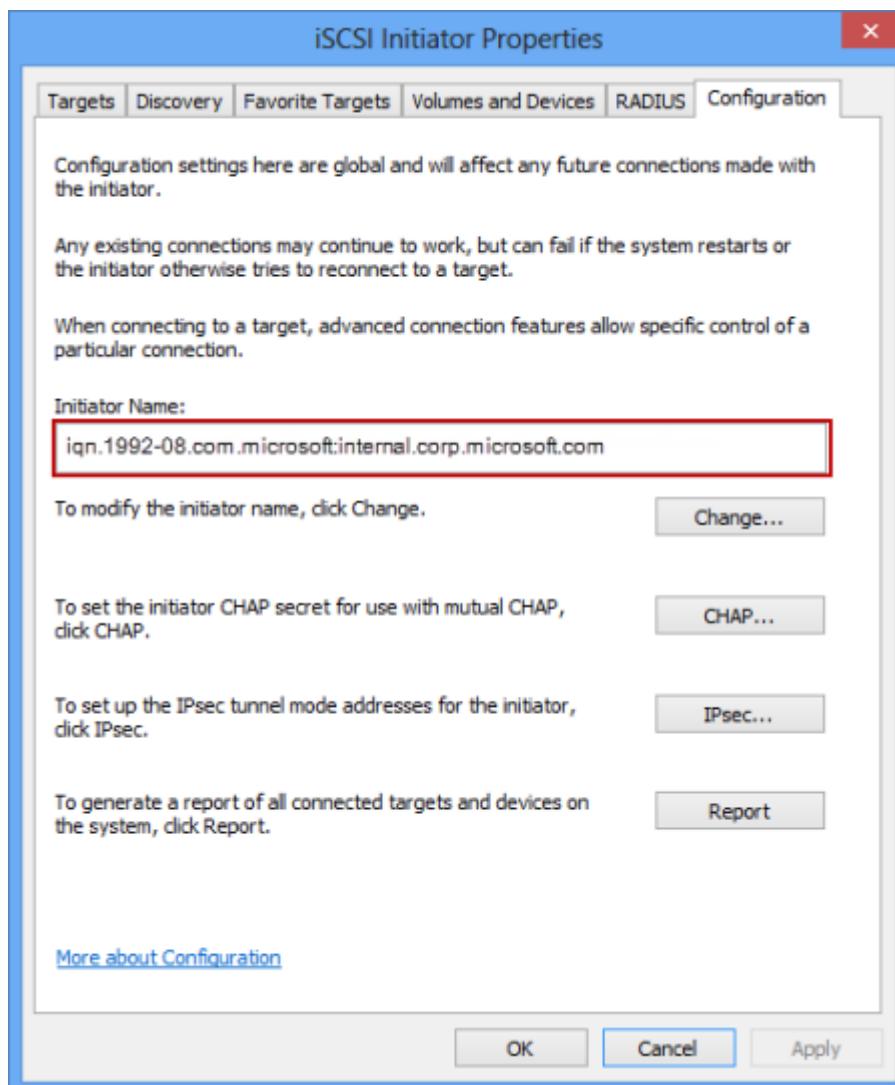
- When assigning an ACR to a volume, take care that the volume is not concurrently accessed by more than one non-clustered host because this could corrupt the volume.
- When deleting an ACR from a volume, make sure that the corresponding host is not accessing the volume because the deletion could result in a read-write disruption.

Get the IQN

Perform the following steps to get the IQN of a Windows host that is running Windows Server 2012.

To get the IQN of a Windows host

1. Start the Microsoft iSCSI initiator on your Windows host. Click **Start > Administrative Tools > iSCSI initiator**.
2. In the **iSCSI Initiator Properties** window, on the **Configuration** tab, select and copy the string from the **Initiator Name** field.



3. Save this string.

Add an ACR

You use **Access control records** blade within the **Configuration** section of your StorSimple Device Manager service to add ACRs. Typically, you associate one ACR with one volume.

For information about associating an ACR with a volume, go to [add a volume](#).

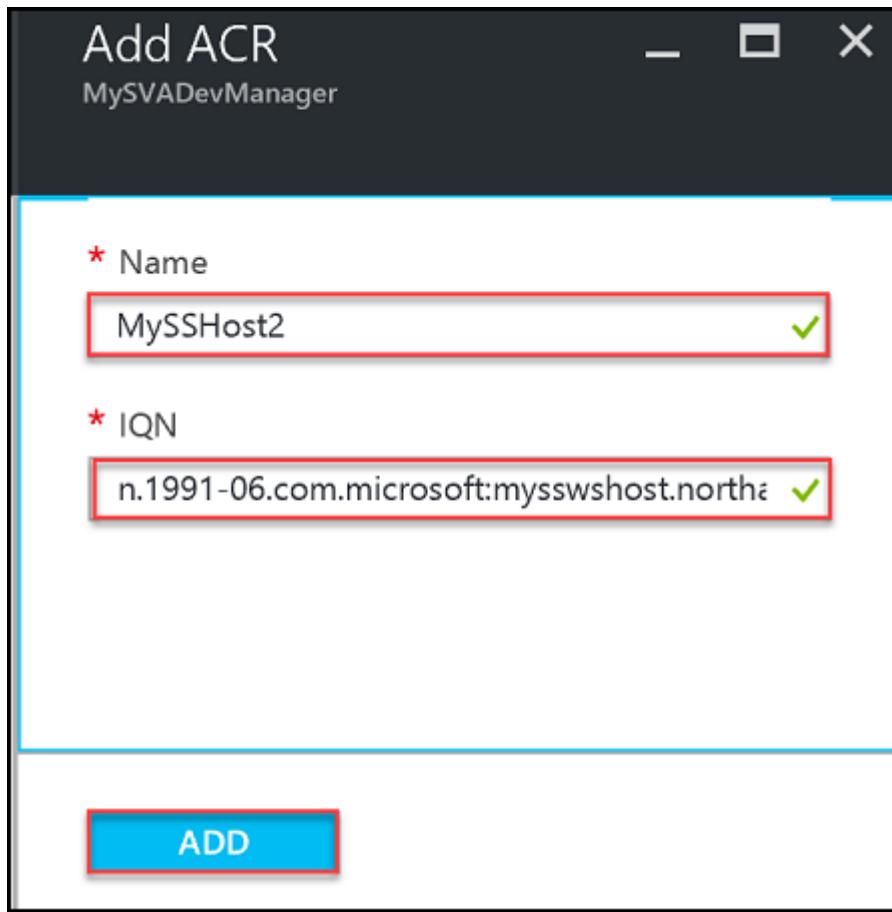
ⓘ Important

When assigning an ACR to a volume, take care that the volume is not concurrently accessed by more than one non-clustered host because this could corrupt the volume.

Perform the following steps to add an ACR.

To add an ACR

1. On the service landing page, select your service, double-click the service name, and then within the **Configuration** section, click **Access control records**.
2. In the **Access control records** blade, click **Add**.
3. In the **Add ACR** blade, do the following:
 - a. Supply a **Name** for your ACR.
 - b. Under **iSCSI Initiator Name**, provide the IQN name of your Windows host. To get the IQN of your Windows Server host, do the following:
 - c. Start the Microsoft iSCSI initiator on your Windows host. In the iSCSI Initiator Properties window, on the **Configuration** tab, select and copy the string from the **Initiator Name** field. Paste this string in the **IQN** field in the **Add ACR** blade.
 - d. Click **Add** to add the ACR.



4. The tabular listing is updated to reflect this addition.

Edit an ACR

You use the **Access control records** blade within the **Configuration** section of your Device Manager service in the Azure portal to edit ACRs.

Note

You should not modify an ACR that is currently in use. To edit an ACR associated with a volume that is currently in use, you should first take the volume offline.

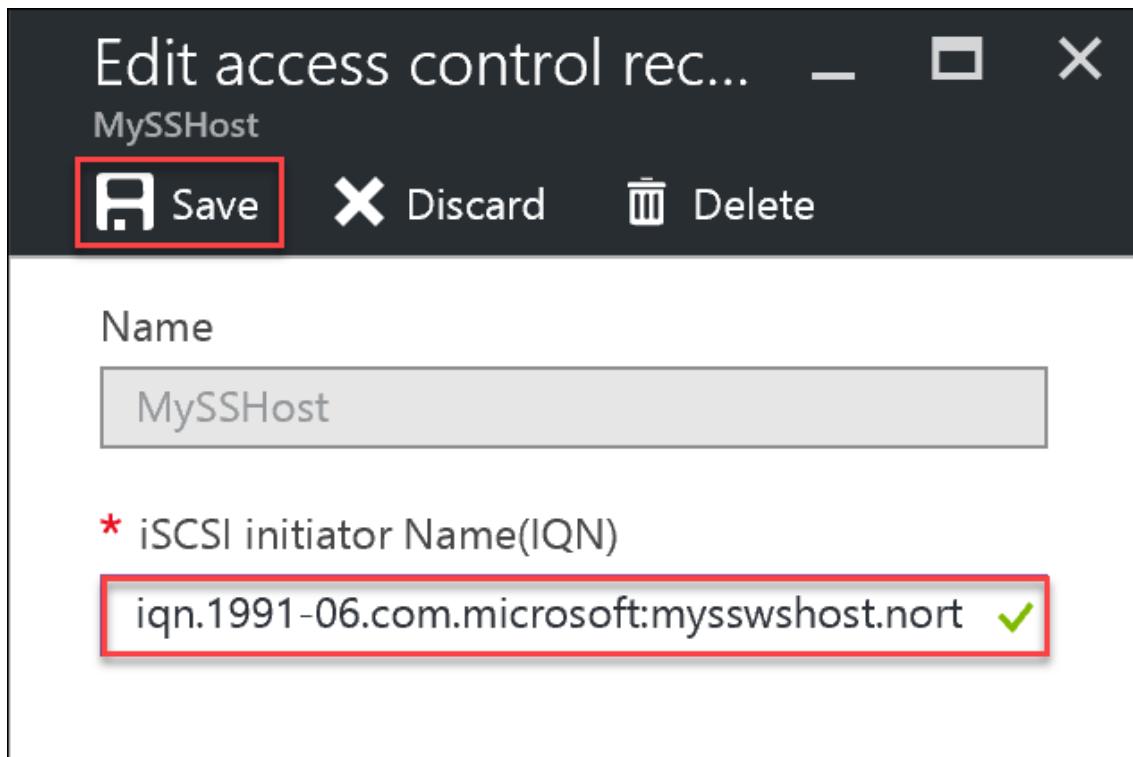
Perform the following steps to edit an ACR.

To edit an ACR

1. On the service landing page, select your service, double-click the service name, and then within the **Configuration** section, **Access control records**.
2. In the **Access control records** blade, from the tabular listing of the access control records, double-click the ACR that you wish to modify.

3. In the **Edit access control records** blade, do the following:

- a. Supply the IQN for the ACR.
- b. Click **Save** at the top of the blade to save the modified ACR. You see the following confirmation message:



Delete an access control record

You use the **Configuration** page in the Azure portal to delete ACRs.

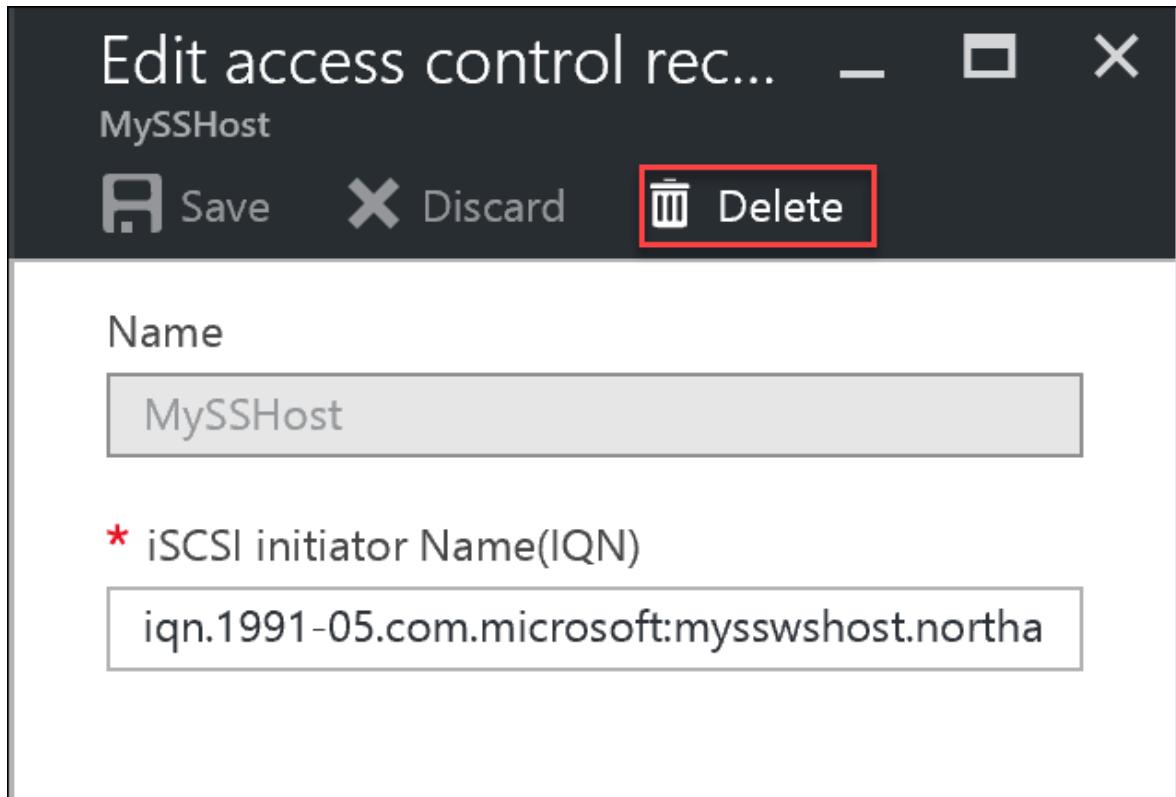
i Note

- You should not delete an ACR that is currently in use. To delete an ACR associated with a volume that is currently in use, you should first take the volume offline.
- When deleting an ACR from a volume, make sure that the corresponding host is not accessing the volume because the deletion could result in a read-write disruption.

Perform the following steps to delete an access control record.

To delete an access control record

1. On the service landing page, select your service, double-click the service name, and then within the **Configuration** section, **Access control records**.
2. In the **Access control records** blade, from the tabular listing of the access control records, double-click the ACR that you wish to delete.
3. In the Edit access control records blade, click **Delete**.



4. When prompted for confirmation, click **Delete** to continue with the deletion. The tabular listing is updated to reflect the deletion.

Delete

MySSHost



If 'MySSHost' is deleted, the corresponding host cannot access the device volumes.

Are you sure you want to continue?

Delete

Next steps

- Learn more about [adding volumes and configuring ACRs](#).

Use the StorSimple Device Manager service to view jobs for the StorSimple Virtual Array

Article • 08/19/2022 • 2 minutes to read

Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The **Jobs** blade provides a single central portal for viewing and managing jobs that are started on virtual arrays that are connected to your StorSimple Device Manager service. You can view running, completed, and failed jobs for multiple virtual devices. Results are presented in a tabular format.

The screenshot shows the 'Jobs' section of the MySVADevManager interface. On the left, a sidebar lists various management categories: GENERAL (Locks, Properties, Quick start), MANAGEMENT (Devices, Volumes, Shares, Keys, Backup catalog), MONITORING (Capacity, Usage, Jobs, Alerts), and CONFIGURATION (Storage account credentials, Access control records). The 'Jobs' item under MONITORING is highlighted with a red box. The main pane displays a table of jobs with the following data:

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Backup	Succeeded	MySSVAIS0916	MySSVAIS0916	9/20/2016 22:30:02	1 Minute, 2 Seconds
Backup	Succeeded	MySSVAIS0916	MySSVAIS0916	9/19/2016 22:30:02	54 Seconds

At the top of the main pane, there are four filter fields: Time range (Past 7 days), Devices (MYSSVAIS0916), Status (Succeeded), and Job type (All). Below the filters are 'Apply' and 'Reset' buttons. A message indicates 'The query returned 2 items.' and there is a 'Filter items...' search bar.

You can quickly find the jobs you are interested in by filtering on fields such as:

- **Time range** – Jobs can be filtered based on the date and time range.
- **Devices** – Jobs are initiated on a specific device connected to your service. The filtered jobs are then tabulated based on the following attributes:
 - **Name** – The job name can be All, Backup, Clone, Fail over, Download updates, or Install updates.
 - **Status** – Jobs can be All, In progress, Succeeded, or Failed, or Canceled.
 - **Entity** – The jobs can be associated with a volume, share, or device.
 - **Device** – The name of the device on which the job was started.
 - **Started on** – The time when the job was started.
 - **Duration** – The duration for which the job was run.
- **Status** – You can search for all, running, completed, or failed jobs.
- **Job type** – The job type can be all, backup, restore, failover, download updates, or install updates.

The list of jobs is refreshed every 30 seconds.

View job details

Perform the following steps to view the details of any job.

To view job details

1. On the **Jobs** blade, display the job(s) you are interested in by running a query with appropriate filters. You can search for completed or running jobs.
2. Select a job from the tabular list of jobs.

The screenshot shows the 'MySVAdevManager - Jobs' page in the StorSimple Device Manager. The left sidebar has a tree view with 'Jobs' selected. The main area has a 'Refresh' button and four filter dropdowns: 'Time range' (Past 7 days), 'Devices' (MYSSVAIS0916), 'Status' (Succeeded), and 'Job type' (All). Below the filters is an 'Apply' button and a 'Reset' button. A message says 'The query returned 2 items.' There is a 'Filter items...' search bar. A table lists two backup jobs:

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Backup	Succeeded	MySSVAIS0916	MySSVAIS0916	9/20/2016 22:30:02	1 Minute, 2 Seconds
Backup	Succeeded	MySSVAIS0916	MySSVAIS0916	9/19/2016 22:30:02	54 Seconds

3. At the bottom of the page, click **Details**.
4. In the **Details** dialog box, you can view status, details, and time statistics. The following illustration shows an example of the **Backup Job Details** dialog box.

The screenshot shows a window titled "Backup Job" with a "Refresh" button. The main area is titled "Details" and contains the following information:

Status	Succeeded
Entity	MySSVAIS0916 (Microsoft.StorSimple/managers/devices)
Device	MYSSVAIS0916
Started on	9/20/2016 22:30:02
Completed on	9/20/2016 22:31:04
Duration	1 Minute, 2 Seconds

Job failures when the virtual machine is paused in the hypervisor

When a job is in progress on your StorSimple Virtual Array and the device (virtual machine provisioned in hypervisor) is paused for greater than 15 minutes, the job fails. This is due to your StorSimple Virtual Array time being out of sync with the Microsoft Azure time.

You will see the following error: "Your device time is out of sync with the Microsoft Azure time by more than 15 minutes. Ensure that the hypervisor and the device times are synchronized with an NTP server. Verify that there are no connectivity issues. To troubleshoot connectivity issues, run diagnostic tests from the local web UI of your virtual device."

These failures apply to backup, restore, update, and failover jobs. If your virtual machine is provisioned in Hyper-V, the machine eventually synchronizes time with your hypervisor. Once that happens, you can restart your job.

Next steps

[Learn how to use the local web UI to administer your StorSimple Virtual Array.](#)

Change the StorSimple Virtual Array device administrator password via StorSimple Device Manager

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

When you use the Windows PowerShell interface to access the StorSimple Virtual Array, you are required to enter a device administrator password. When the StorSimple device is first provisioned and started, the default password is *Password1*. For the security of your data, the default password expires the first time that you sign in and you are required to change this password.

You can also use either the local web UI or the Azure portal to change the device administrator password at any time after the device is deployed in your production environment. Each of these procedures is described in this article.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
MYSVAFS0831	Online	137.07 GB/1.33 TB	Virtual-NAS	1200
MYSSVAIS0916	Online	87.39 GB/873.99 GB	Virtual-iSCSI	1200
MYSVAFS0907	Online	335.79 GB/3.27 TB	Virtual-NAS	1200

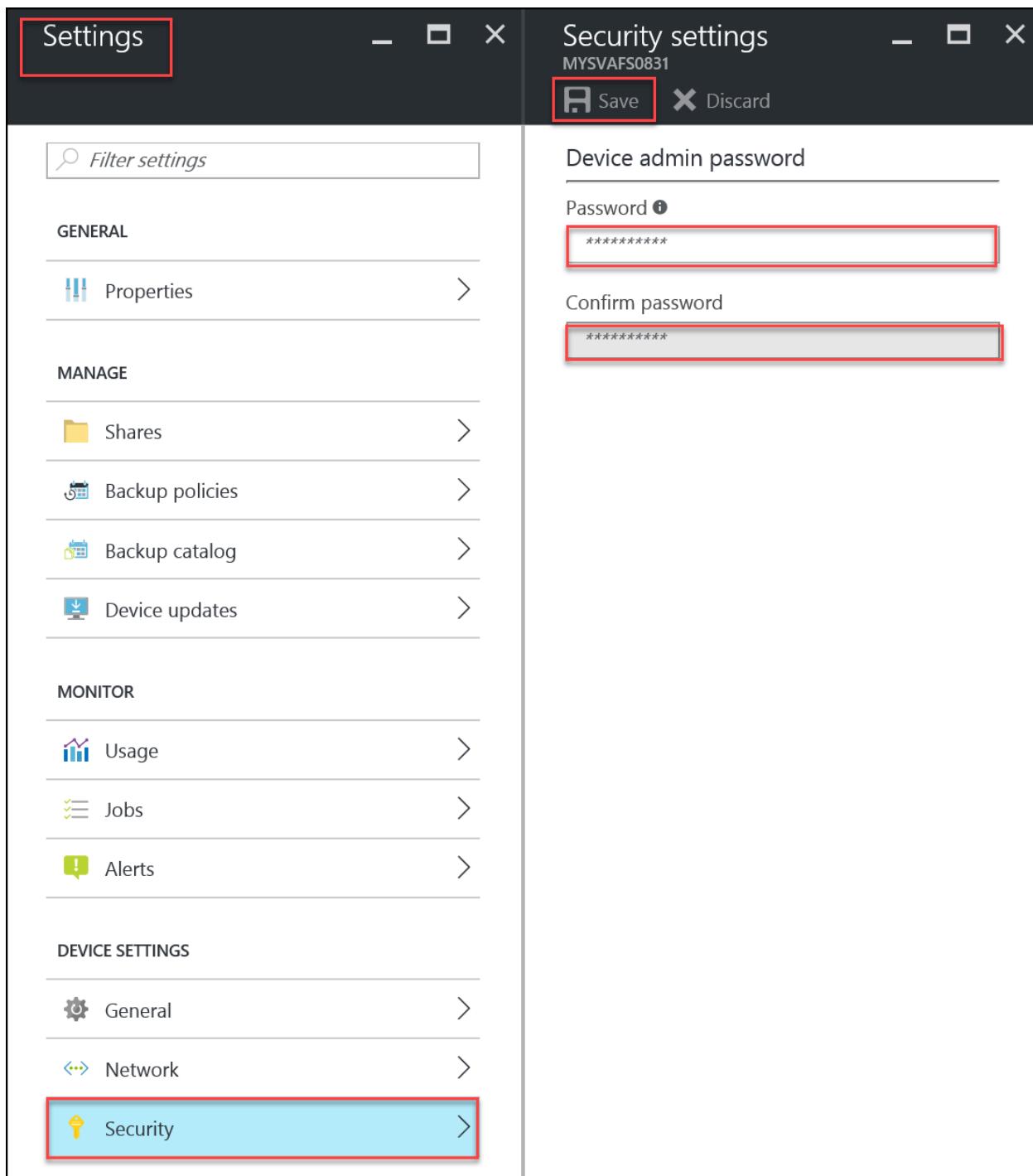
Use the Azure portal to change the password

Perform the following steps to change the device administrator password through the Azure portal.

To change the device administrator password via the Azure portal

1. On the service landing page, select your service, double-click the service name, and then within the **Management** section, click **Devices**. This opens the **Devices** blade that lists all your StorSimple Virtual Array devices.
2. In the **Devices** blade, double-click the device that requires a change of password.
3. In the **Settings** blade for your device, click **Security**.
4. In the **Security Settings** blade, do the following:
 - a. Scroll down to the **Device Administrator Password** section. Provide an administrator password that contains from 8 to 15 characters.
 - b. Confirm the password.
 - c. Click **Save** at the top of the blade.

The device administrator password is now updated. You can use this modified password to access the device locally.



Use the local web UI to change the password

Perform the following steps to change the device administrator password through the local web UI.

To change the device administrator password via the local web UI

1. In the local web UI, click Maintenance > Password change for your device.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)[Software update](#)

Password change

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Current password

New password

The password must be a string that contains at least 8 characters. The password must contain uppercase, lowercase, numeric, and special characters.

Reenter password

Apply

Help ©2015 Microsoft

2. Enter the **Current password**.

3. Provide a **New Password**. The password must be at least 8 characters long. It must contain 3 of 4 of the following: uppercase, lowercase, numeric, and special characters.

Note that your password cannot be the same as the last 24 passwords.

4. Reenter the password to confirm it.

Configuration[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)**Maintenance**[Power settings](#)[Software update](#)**Password change****Troubleshooting**[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Current password

New password



The password must be a string that contains at least 8 characters. The password must contain uppercase, lowercase, numeric, and special characters.

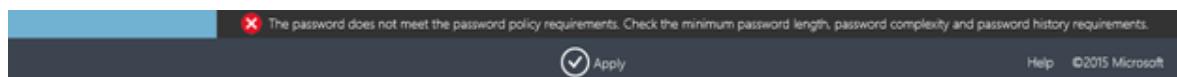
Reenter password



Apply

Help ©2015 Microsoft

5. At the bottom of the page, click **Apply**. The new password is now applied. If the password change is not successful, you see the following error:



After the password is successfully updated, you are notified. You can then use this modified password to access the device locally.

Next steps

Learn how to [administer your StorSimple Virtual Array](#).

Use StorSimple Device Manager to manage alerts for the StorSimple Virtual Array

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The alerts feature in the StorSimple Device Manager service provides a way for you to review and clear alerts related to StorSimple Virtual Arrays on a real-time basis. You can use the alerts on the **Service summary** blade to centrally monitor the health issues of your StorSimple Virtual Arrays and the overall Microsoft Azure StorSimple solution.

This tutorial describes how to configure alert notifications, common alert conditions, alert severity levels, and how to view and track alerts. Additionally, it includes alert quick reference tables, which enable you to quickly locate a specific alert and respond appropriately.

The screenshot shows the StorSimple Device Manager interface under the 'Alerts' section. The left sidebar has a tree view with 'Jobs' (marked with a red box and number 1) and 'Alerts' (marked with a red box and number 2) selected. The main pane displays a search bar and filter options: 'Time range' (Past 7 days), 'Devices' (All), 'Severity' (All), and 'Status' (Cleared). Below these are 'Apply' and 'Reset' buttons. A message states 'The query returned 2 items.' A table lists two alerts:

NAME	STATUS	SEVERITY	SOURCE	DURATION
Lost heartbeat from your device for the last 5 minutes.	Cleared	Critical	MYSSFS1014	5 Days, 19 Hours
Lost heartbeat from your device for the last 5 minutes.	Cleared	Critical	MYSSIS1014	5 Days, 19 Hours

Configure alert settings

You can choose whether you want to be notified by email of the alert conditions for each of your StorSimple Virtual Arrays. Additionally, you can identify other alert notification recipients by entering their email addresses in the **Additional email recipients** box, separated by semicolons.

! Note

You can enter a maximum of 20 email addresses per virtual array.

After you enable email notification for a virtual array, members of the notification list will receive an email message each time a critical alert occurs. The messages will be sent from *storsimple-alerts-noreply@mail.windowsazure.com* and will describe the alert condition. Recipients can click **Unsubscribe** to remove themselves from the email notification list.

To enable email notification for alerts

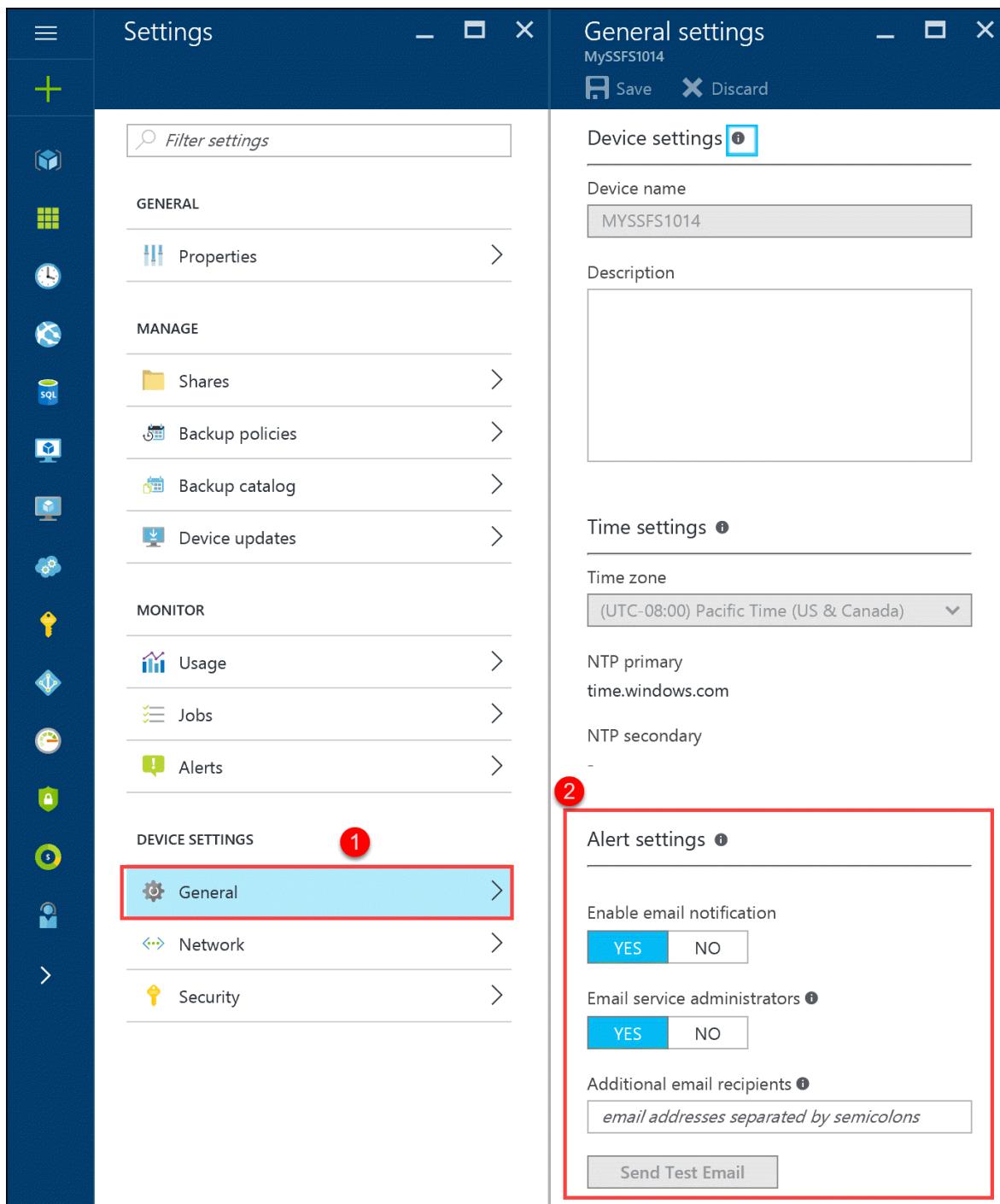
1. Go to your StorSimple Device Manager service and in the **Management** section, select and click **Devices**. From the list of devices displayed, select and click your device.

The screenshot shows the StorSimple Device Manager interface titled "MySSDevManager - Devices". On the left, there's a navigation sidebar with sections like GENERAL, MANAGEMENT (with "Devices" highlighted), MONITORING, and CONFIGURATION. The main area displays a table of devices with columns: NAME, STATUS, REMAINING CAPACITY (LOCAL VS TIERED), TYPE, and MODEL. Two devices are listed: MYSSFS1014 (Virtual-NAS) and MYSSIS1014 (Virtual-iSCSI). Both are online with 186.75 GB/1.82 TB remaining capacity. A red box highlights the first device, and a red circle with the number 2 is positioned above the STATUS column header.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
MYSSFS1014	Online	186.75 GB/1.82 TB	Virtual-NAS	1200
MYSSIS1014	Online	186.75 GB/1.82 TB	Virtual-iSCSI	1200

2. This opens up the **Settings** blade. In the **Device settings** section, select **General**.

This opens up the **General Settings** blade.



3. In the **General settings** blade, go to **Alert settings** section and set the following:
 - a. In the **Enable email notification** field, select YES.
 - b. In the **Email service administrators** field, select YES if you wish to have the service administrator and all co-administrators receive the alert notifications.
 - c. In the **Additional email recipients** field, enter the email addresses of all other recipients who should receive the alert notifications. Enter names in the format *someone@somewhere.com*. Use semicolons to separate the email addresses. You can configure a maximum of 20 email addresses per virtual device.

Alert settings i

Enable email notification

YES

NO

1

Email service administrators i

YES

NO

2

Additional email recipients i

gus.poland@contoso.com;tammy.robinson@contoso.com ✓

Send Test Email

4

- d. To send a test email notification, click **Send test email**. The StorSimple Device Manager service will display status messages as it forwards the test notification.



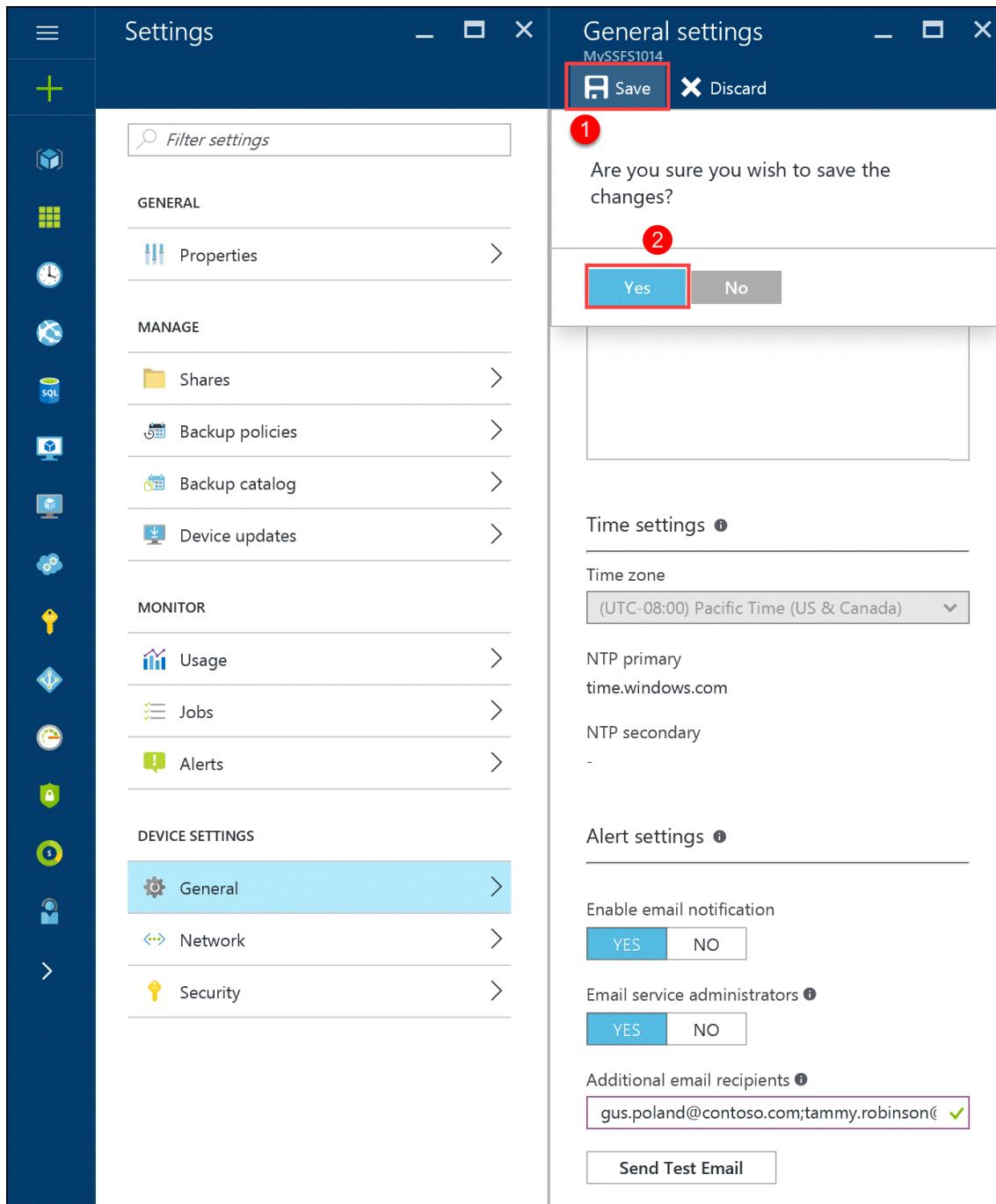
Send Test Alert Email to 'gus.poland@contoso.com' 9:00 AM



i Note

If the test notification message can't be sent, the StorSimple Device Manager service will display an appropriate message. Click **OK**, wait a few minutes, and then try to send your test notification message again.

- e. At the bottom of the page, click **Save** to save your configuration. When prompted for confirmation, click **Yes**.



Common alert conditions

Your StorSimple Virtual Array generates alerts in response to a variety of conditions. The following are the most common types of alert conditions:

- **Connectivity issues** – These alerts occur when there is difficulty in transferring data. Communication issues can occur during transfer of data to and from the Azure storage account or due to lack of connectivity between the virtual devices and the StorSimple Device Manager service. Communication issues are some of the hardest to fix because there are so many points of failure. You should always first verify that network connectivity and Internet access are available before continuing on to more advanced troubleshooting. For information about ports and

firewall settings, go to [StorSimple Virtual Array system requirements](#). For help with troubleshooting, go to [Troubleshoot with the Test-Connection cmdlet](#).

- **Performance issues** – These alerts are caused when your system isn't performing optimally, such as when it is under a heavy load.

In addition, you might see alerts related to security, updates, or job failures.

Alert severity levels

Alerts have different severity levels, depending on the impact that the alert situation will have and the need for a response to the alert. The severity levels are:

- **Critical** – This alert is in response to a condition that is affecting the successful performance of your system. Action is required to ensure that the StorSimple service is not interrupted.
- **Warning** – This condition could become critical if not resolved. You should investigate the situation and take any action required to clear the issue.
- **Information** – This alert contains information that can be useful in tracking and managing your system.

View and track alerts

The StorSimple Device Manager service summary blade provides you with a quick glance at the number of alerts on your virtual devices, arranged by severity level.

Screenshot of the MySSDevManager - StorSimple Device Manager interface.

The left sidebar contains a search bar and a list of navigation items:

- Virtual array
- Add volume
- Add share
- Fail over
- Delete

The main content area is divided into sections:

- Essentials**:
 - Resource group: MyStorSimRG
 - Location: West US
 - Subscription name: MSDNonDallas
 - Subscription ID: storssimple-abcd-1234-5678-efgh
- Monitoring**:
 - Alerts - Past 7 days**: 2 Critical alerts (highlighted with a red border).
 - Capacity**:
 - PROVISIONED: 3.9 TB
 - REMAINING: 3.64 TB Tiered, 373.51 GB Local
 - Usage - Past 7 days**: A line chart showing usage from Oct 20 to Oct 26. The Y-axis ranges from 0 to 0.8. The X-axis shows dates from Oct 20 to Oct 26. The chart shows a constant value around 0.65.
 - PRIMARY STORAGE USED**: 0.7 GB
 - CLOUD STORAGE USED**: 0 GB
- Managed items**:
 - Devices**: 2 devices
 - Offline**: 2 devices

Click the severity level to open the **Alerts** blade. The results include only the alerts that match that severity level.

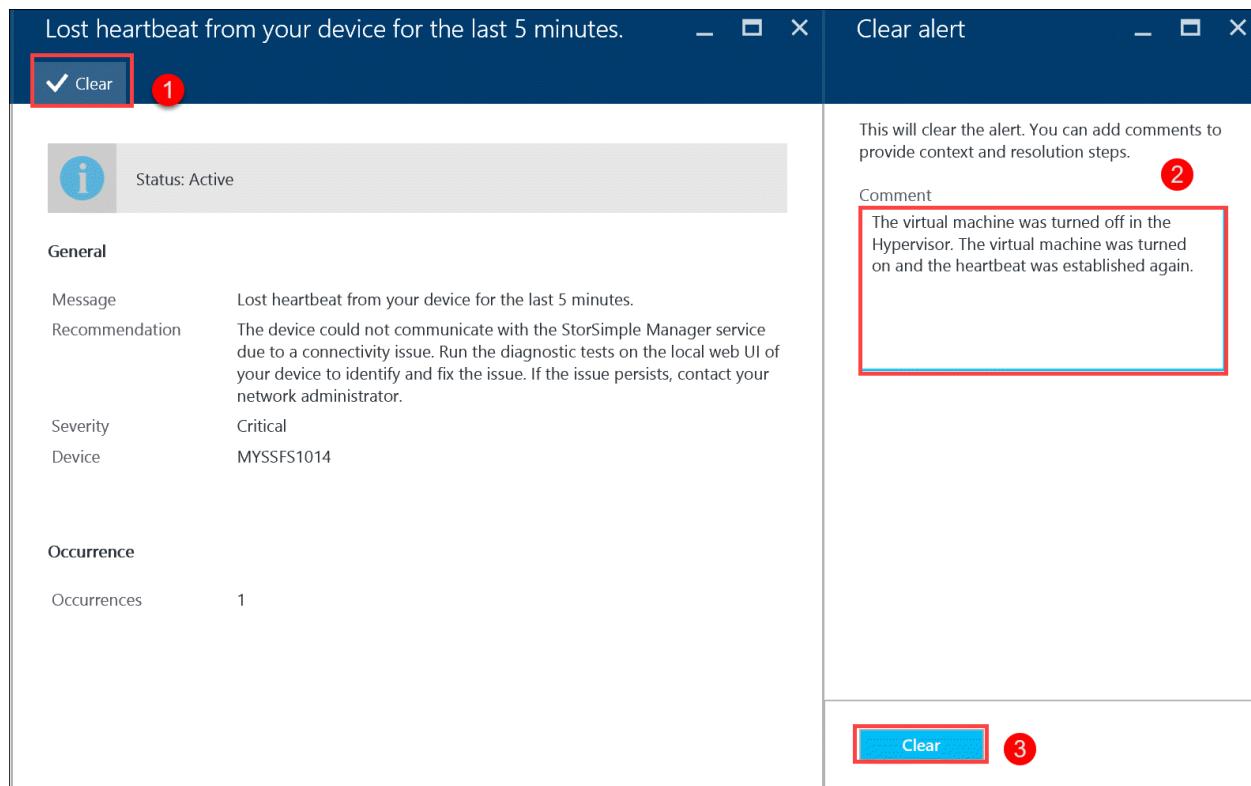
The screenshot shows the MySSDevManager StorSimple Device Manager interface. On the left, there's a navigation sidebar with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS, GENERAL, MANAGEMENT, MONITORING, and ALERTS. The ALERTS section is currently selected. In the main area, there's a 'Monitoring' section with a card for 'Alerts - Past 7 days' showing 2 critical alerts. Below it is a 'Capacity' section with a table showing provisioned (3.9 TB) and remaining (3.64 TB) storage. There's also a 'Usage - Past 7 days' chart and a 'Managed items' section showing 2 devices, one of which is listed as 'Offline'.

Click an alert in the list to get additional details for the alert, including the last time the alert was reported, the number of occurrences of the alert on the device, and the recommended action to resolve the alert.

The screenshot shows the details of a specific alert titled 'Lost heartbeat from your device for the last 5 minutes.' on the MySSDevManager interface. The left side shows the alert list with two items, both of which are highlighted with a red border. The right side provides detailed information about the alert, including its status (Active), severity (Critical), source (MYSSFS1014), and duration (16 Minutes, 56 Secs). It also includes a 'General' section with a message and recommendation, and a 'Severity' and 'Device' section.

You can copy the alert details to a text file if you need to send the information to Microsoft Support. After you have followed the recommendation and resolved the alert condition on-premises, you should clear the alert from the list. Select the alert from the list and then click **Clear**. To clear multiple alerts, select each alert, click any column except the **Alert** column, and then click **Clear** after you have selected all the alerts to be cleared.

When you click **Clear**, you will have the opportunity to provide comments about the alert and the steps that you took to resolve the issue.



Some events will be cleared by the system if another event is triggered with new information.

Sort and review alerts

The **Alerts** blade can display up to 250 alerts. If you have exceeded that number of alerts, not all alerts will be displayed in the default view. You can combine the following fields to customize which alerts are displayed:

- **Status** – You can display either **Active** or **Cleared** alerts. Active alerts are still being triggered on your system, while cleared alerts have been either manually cleared by an administrator or programmatically cleared because the system updated the alert condition with new information.
- **Severity** – You can display alerts of all severity levels (critical, warning, information), or just a certain severity, such as only critical alerts.
- **Source** – You can display alerts from all sources, or limit the alerts to those that come from either the service or one or all the virtual devices.
- **Time range** – By specifying the **From** and **To** dates and time stamps, you can look at alerts during the time period that you are interested in.

Alerts quick reference

The following tables list some of the StorSimple alerts that you might encounter, as well as additional information and recommendations where available. StorSimple Virtual

Array alerts fall into one of the following categories:

- Cloud connectivity alerts
- Configuration alerts
- Job failure alerts
- Performance alerts
- Security alerts

Cloud connectivity alerts

Alert text	Event	More information / recommended actions
Device < <i>device name</i> > is not connected to the cloud.	The named device cannot connect to the cloud.	<p>Could not connect to the cloud. This could be due to one of the following:</p> <ul style="list-style-type: none">• There may be a problem with the network settings on your device.• There may be a problem with the storage account credentials. <p>For more information on troubleshooting connectivity issues, go to the local web UI of the device.</p>

Configuration alerts

Alert text	Event	More information / recommended actions
On-premises virtual device configuration unsupported.	Slow performance.	The current configuration may result in performance degradation. Ensure that your server meets the minimum configuration requirements. For more information, go to StorSimple Virtual Array Requirements .
You are running out of provisioned disk space on < <i>device name</i> >.	Disk space warning.	You are running low on provisioned disk space. To free up space, consider moving workloads to another volume or share or deleting data.

Job failure alerts

Alert text	Event	More information / recommended actions
------------	-------	--

Alert text	Event	More information / recommended actions
Backup of <device name> couldn't be completed.	Backup job failure.	<p>Could not create a backup. Consider one of the following:</p> <ul style="list-style-type: none"> • Connectivity issues could be preventing the backup operation from successfully completing. Ensure that there are no connectivity issues. For more information on troubleshooting connectivity issues, go to the local web UI for your virtual device. • You have reached the available storage limit. To free up space, consider deleting any backups that are no longer needed. <p>Resolve the issues, clear the alert and retry the operation.</p>
Clone of <device name> couldn't be completed.	Clone job failure.	<p>Could not create a clone. Consider one of the following:</p> <ul style="list-style-type: none"> • Your backup list may not be valid. Refresh the list to verify it is still valid. • Connectivity issues could be preventing the clone operation from successfully completing. Ensure that there are no connectivity issues. • You have reached the available storage limit. To free up space, consider deleting any backups that are no longer needed. <p>Resolve the issues, clear the alert and retry the operation.</p>

Networking alerts

Alert text	Event	More information / recommended actions
Could not connect to the authentication service.	Datapath error	The URL that is used to authenticate is not reachable. Ensure that your firewall rules include the URL patterns specified for the StorSimple device. For more information on URL patterns in Azure portal, go to StorSimple Virtual Array networking requirements .

Performance alerts

Alert text	Event	More information / recommended actions
You are experiencing unexpected delays in data transfer.	Slow data transfer.	Throttling errors occur when you exceed the scalability targets of a storage service. The storage service does this to ensure that no single client or tenant can use the service at the expense of others. For more information on troubleshooting your Azure storage account, go to Monitor, diagnose, and troubleshoot Microsoft Azure Storage .

Alert text	Event	More information / recommended actions
You are running low on local reservation disk space on < <i>device name</i> >.	Slow response time.	<p>10% of the total provisioned size for <<i>device name</i>> is reserved on the local device and you are now running low on the reserved space. The workload on <<i>device name</i>> is generating a higher rate of churn or you might have recently migrated a large amount of data. This may result in reduced performance. Consider one of the following actions to resolve this:</p> <ul style="list-style-type: none"> • Increase the cloud bandwidth to this device. • Reduce or move workloads to another volume or share.

Security alerts

Alert text	Event	More information / recommended actions
Password for < <i>device name</i> > will expire in < <i>number</i> > days.	Password warning.	Your password will expire in < <i>number</i> > days. Consider changing your password. For more information, go to Change the StorSimple Virtual Array device administrator password .

Next steps

- [Learn about the StorSimple Virtual Array](#).

Use the StorSimple Device Manager service to troubleshoot the StorSimple Virtual Array

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager provides a **Diagnose and solve problems** setting within the service summary blade, which highlights some of the commonly occurring issues that can occur with your virtual array and how to solve them. This tutorial introduces the self-serve troubleshooting capability provided within the StorSimple Device Manager service.

ContosoStorSimpleManager - Diagnose and solve problems

StorSimple Device Manager

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Locks

GENERAL

Properties

Quick start

MANAGEMENT

Devices

Volumes

Shares

Keys

Backup catalog

MONITORING

Capacity

RECENT ACTIVITY

Activity for the past 24 hours

0 failed deployments | 13 role assignments | 0 errors | 0 alerts fired | See all activity

SOLUTIONS TO COMMON PROBLEMS

- > I can't create a StorSimple Device Manager.
- > My virtual array doesn't boot up.
- > I can't register my virtual array.
- > My virtual array is offline.
- > My virtual array has turned off.
- > My clone job is not completing.
- > I can't access my device in File Explorer.
- > I am not able to complete the device configuration in the Azure portal.
- > I can't open the backups in .backups folder.
- > I can't access my shares or volumes.
- > My issue is not listed

CONTACT MICROSOFT SUPPORT

If you need assistance solving your issue, please open a [support request](#).

Diagnose and solve issues

You can view some of the common problems with the StorSimple Virtual Array and review the solutions to those issues right from your StorSimple Device Manager service summary blade.

To diagnose an issue with your virtual array

1. Click **Diagnose and solve problems** setting in the left pane of your StorSimple Device Manager service summary blade to view a list of common problems.
2. **Expand** on the symptom of the issue you are encountering to review **Recommended steps** to aid you in troubleshooting the problem. If you wish, you can also review the detailed documentation links provided for further reference.

RECENT ACTIVITY
Activity for the past 24 hours
0 failed deployments | 13 role assignments | 0 errors | 0 alerts fired | See all activity

SOLUTIONS TO COMMON PROBLEMS

- > I can't create a StorSimple Device Manager.
- > My virtual array doesn't boot up.
- > I can't register my virtual array.
- > **My virtual array is offline.**

If your virtual array is offline, this could be due to one of the following reasons:

Recommended steps

1. The virtual array is not able to communicate with the StorSimple Device Manager service.
 - a. In the local web UI of the virtual array, go to **Troubleshooting > Diagnostic tests** and click **Run diagnostic tests**. Resolve the reported issues.
2. The virtual array may be turned off or paused on the hypervisor.
 - a. Your virtual array could have rebooted due to a Windows update. Wait a few minutes and try to reconnect.
 - b. In Hyper-V, your virtual array will be paused automatically when the volume that stores snapshots or virtual hard disks, runs out of available storage. The state of the virtual array is listed as *paused-critical* in Hyper-V Manager. Resolve this by creating additional space on the volume.
 - c. If you still cannot connect, check the Hyper-V host or ESX server to ensure that the VM is healthy.

Recommended documents

[Troubleshoot via the local web UI](#) ↗
[Troubleshooting Hyper-V](#) ↗

- > My virtual array has turned off.

3. If you are unable to find a reference to your issue or resolve it, reach out to Microsoft Support for further assistance.

Next steps

Learn how to [log a support ticket](#)

Use the StorSimple Device Manager service to log a Support request for the StorSimple Virtual Array

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

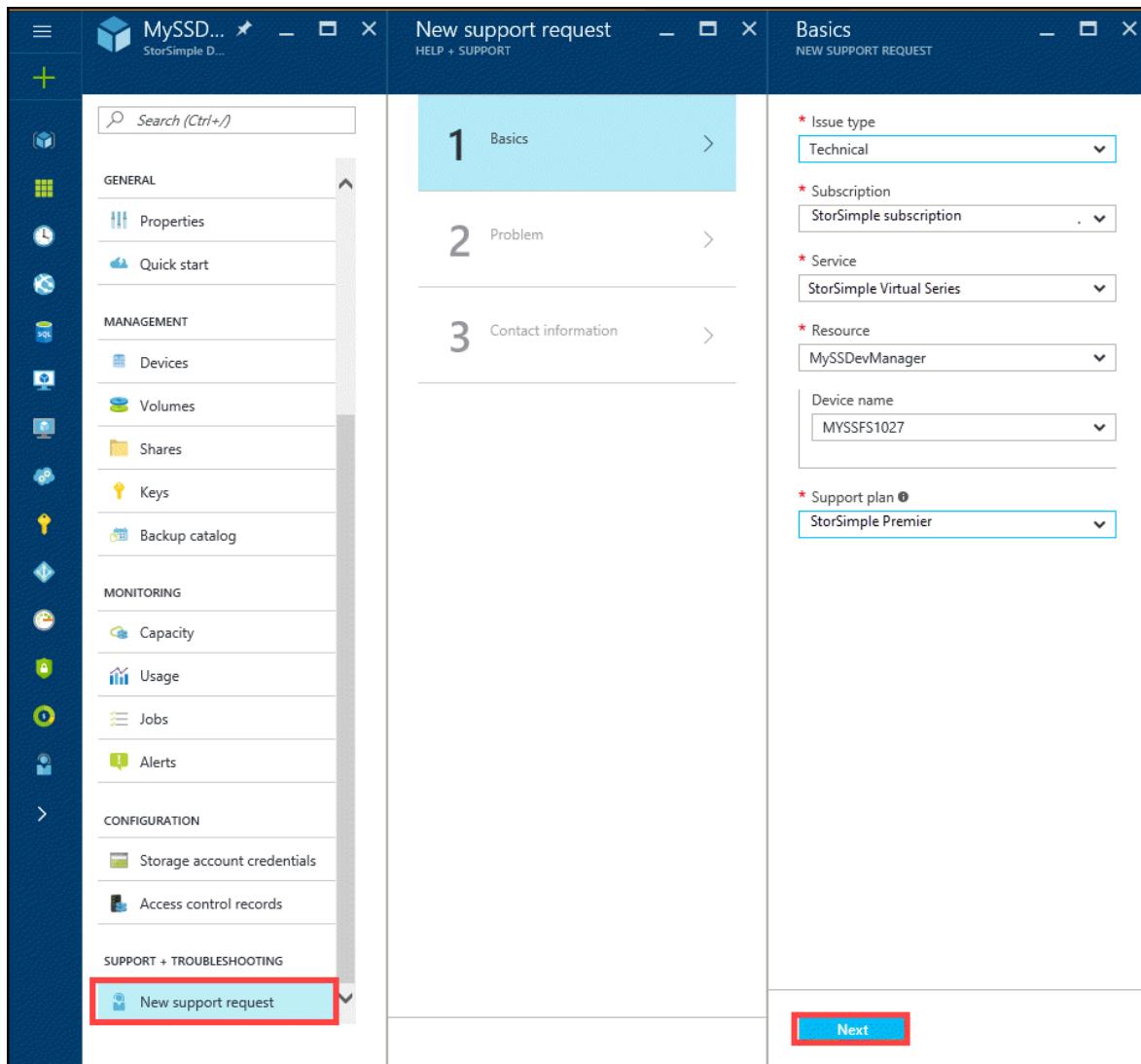
The StorSimple Device Manager provides the capability to [log a new support request](#) within the service summary blade. This article explains how you can log a new support request and manage its lifecycle from within the portal.

New support request

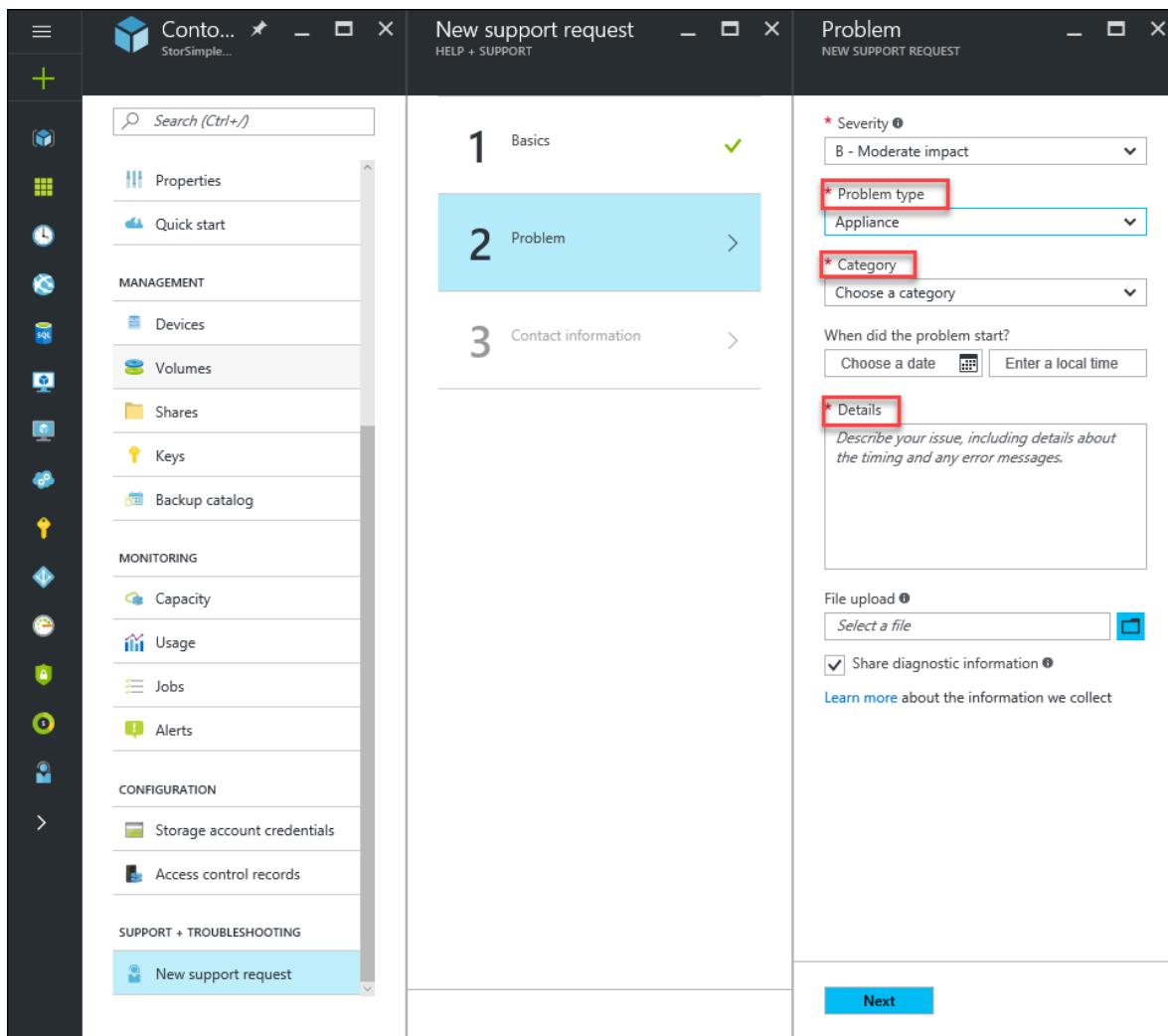
Depending upon your [support plan](#), you can create support tickets for an issue on your StorSimple Virtual array directly from the StorSimple Device Manager service summary blade.

To log a new request

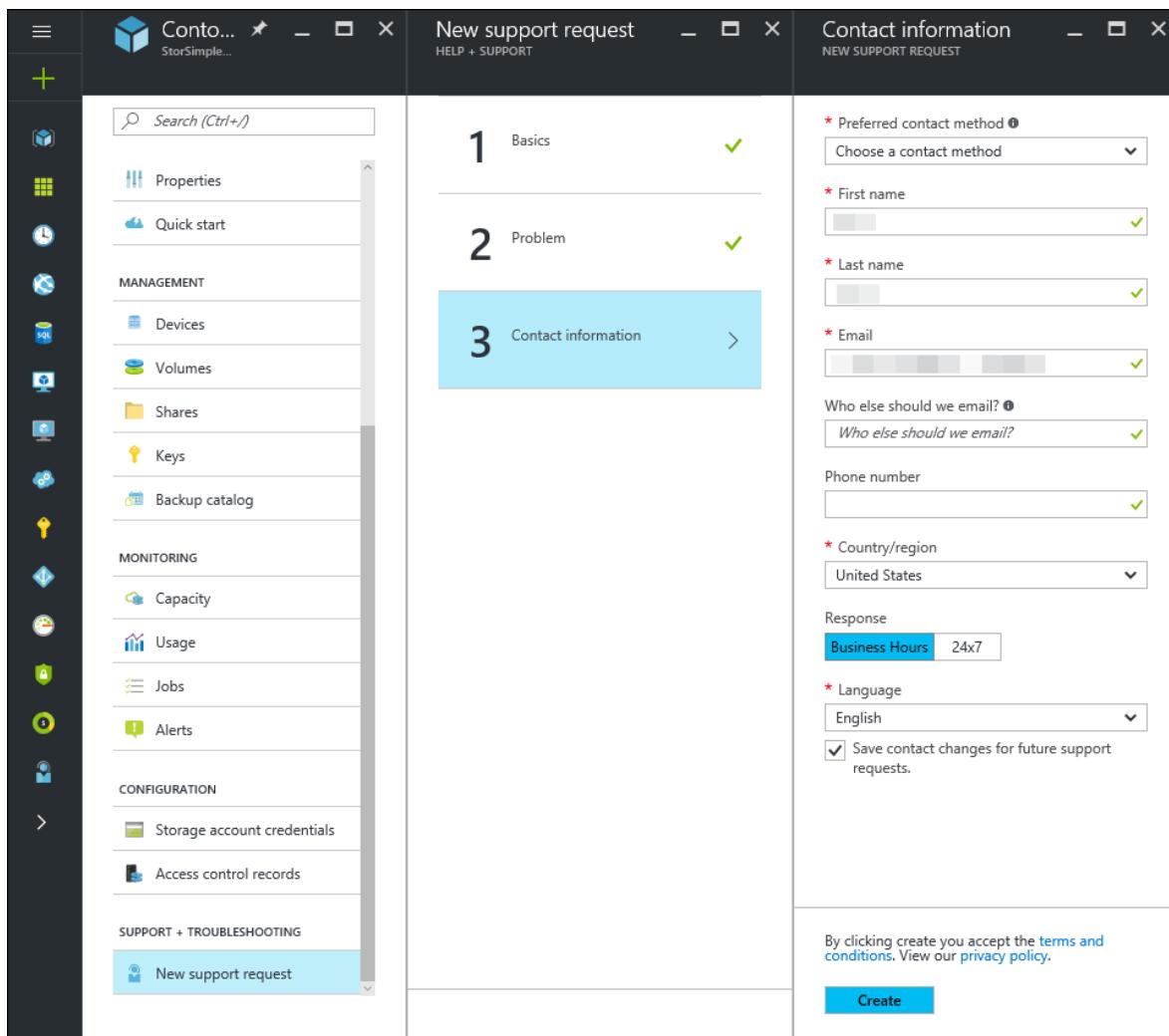
1. Go to your StorSimple Device Manager service. In the service summary blade settings, go to **SUPPORT + TROUBLESHOOTING** section and then click **New support request**.



2. In the **Basics** blade, do the following:
 - a. From the **Issue type** dropdown list, select **Technical**.
 - b. The current **Subscription**, **Service** type, and the **Resource** (StorSimple Device Manager service) are automatically chosen.
 - c. Specify one or more devices registered to your service that are experiencing issues.
 - d. Choose an appropriate **support plan** if you have multiple plans associated with your subscription. You need a paid support plan to enable Technical Support.
3. In **Step 2**, choose the **Severity** and specify if the issue is related to the array or the StorSimple Device Manager service. Also, choose a **Category** for this issue and provide more **Details** about the issue.



4. In **Step 3**, provide your contact information. Microsoft Support will use this information to reach out to you for further information, diagnosis, and resolution.



Manage a support request

After creating a support ticket, you can manage the lifecycle of the ticket from within the portal.

To manage your support requests

To get to the help and support page, navigate to **Browse > Help + support**.

≡

Help + support

+ New support r...

Help

Documentation

Azure tutorials, whitepapers, and how-to articles

Documentation center
Getting started
Blog
Training and certification
SDKs and Tools

MSDN

Information and discussion by Microsoft and the community

MSDN forums
Channel 9
API and reference catalog

Stack Overflow

Questions and answers on a wide range of Azure programming topics

Azure @ stackoverflow
azure-storage
azure-web-sites
sql-azure

Support

New support request

Manage support requests ...

Link support contract

Health

Service health

MY RESOURCES

Resource health

Next steps

Learn how to [diagnose and solve problems related to your StorSimple Virtual array](#)

Learn how to [diagnose and solve problems related to your StorSimple Virtual array](#)

Use the Web UI to administer your StorSimple Virtual Array

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



Overview

The tutorials in this article apply to the Microsoft Azure StorSimple Virtual Array (also known as the StorSimple on-premises virtual device) running March 2016 general availability (GA) release. This article describes some of the complex workflows and management tasks that can be performed on the StorSimple Virtual Array. You can manage the StorSimple Virtual Array using the StorSimple Manager service UI (referred to as the portal UI) and the local web UI for the device. This article focuses on the tasks that you can perform using the web UI.

This article includes the following tutorials:

- Get the service data encryption key
- Troubleshoot web UI setup errors
- Generate a log package
- Shut down or restart your device

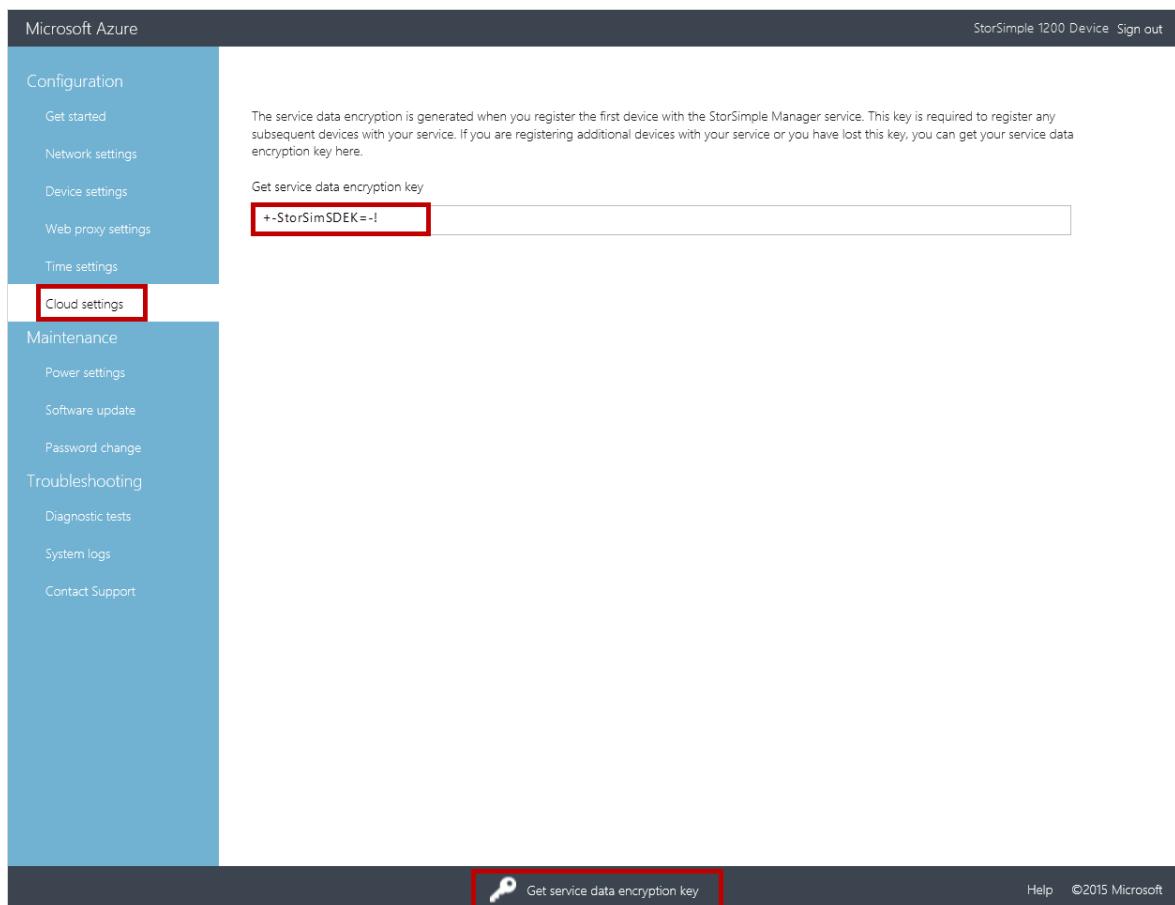
Get the service data encryption key

A service data encryption key is generated when you register your first device with the StorSimple Manager service. This key is then required with the service registration key to register additional devices with the StorSimple Manager service.

If you have misplaced your service data encryption key and need to retrieve it, perform the following steps in the local web UI of the device registered with your service.

To get the service data encryption key

1. Connect to the local web UI. Go to **Configuration > Cloud Settings**.
2. At the bottom of the page, click **Get service data encryption key**. A key will appear. Copy and save this key.



Troubleshoot web UI setup errors

In some instances when you configure the device through the local web UI, you might run into errors. To diagnose and troubleshoot such errors, you can run the diagnostics tests.

To run the diagnostic tests

1. In the local web UI, go to **Troubleshooting > Diagnostic tests**.

The screenshot shows the 'Diagnostic tests' page in the Microsoft Azure StorSimple 1200 Device interface. The left sidebar lists various configuration and troubleshooting options. The 'Diagnostic tests' link is highlighted with a red box. At the bottom of the page, there is a large 'Run Diagnostic Tests' button, also highlighted with a red box.

Run diagnostic tests to troubleshoot device issues.

Test	Status
Test network settings	Not run
Test name resolution	Not run
Test web proxy	Not run
Test time sync	Not run

Help ©2015 Microsoft

2. At the bottom of the page, click **Run Diagnostic Tests**. This will initiate tests to diagnose any possible issues with your network, device, web proxy, time, or cloud settings. You will be notified that the device is running tests.
3. After the tests have completed, the results will be displayed. The following example shows the results of diagnostic tests. Note that the web proxy settings were not configured on this device, and therefore, the web proxy test was not run. All the other tests for network settings, DNS server, and time settings were successful.

The screenshot shows the Microsoft Azure StorSimple 1200 Device local web interface. The left sidebar has a blue header 'Configuration' and a red box highlights the 'Diagnostic tests' link under the 'Troubleshooting' section. The main content area displays diagnostic test results:

Test	Status
Test network settings	✓ The network interface is configured and the gateway is reachable.
Test name resolution	✓ Name resolution is working. Successfully resolved go.microsoft.com to 2600:1406:1a:490::2c1a.
Test web proxy	🟡 Not run
Test time sync	✓ Time is synchronized with the time server. Current time on the appliance is 08:53:15

Below the table, a message says 'Successfully completed the test run.' and there is a 'Run Diagnostic Tests' button. The top right corner shows 'StorSimple 1200 Device Sign out'.

Generate a log package

A log package is comprised of all the relevant logs that can assist Microsoft Support with troubleshooting any device issues. In this release, a log package can be generated via the local web UI.

To generate the log package

1. In the local web UI, go to **Troubleshooting > System logs**.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

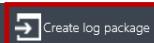
Maintenance

[Power settings](#)[Software update](#)[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Create and download a package of all the system logs if you are experiencing any issues with your device.

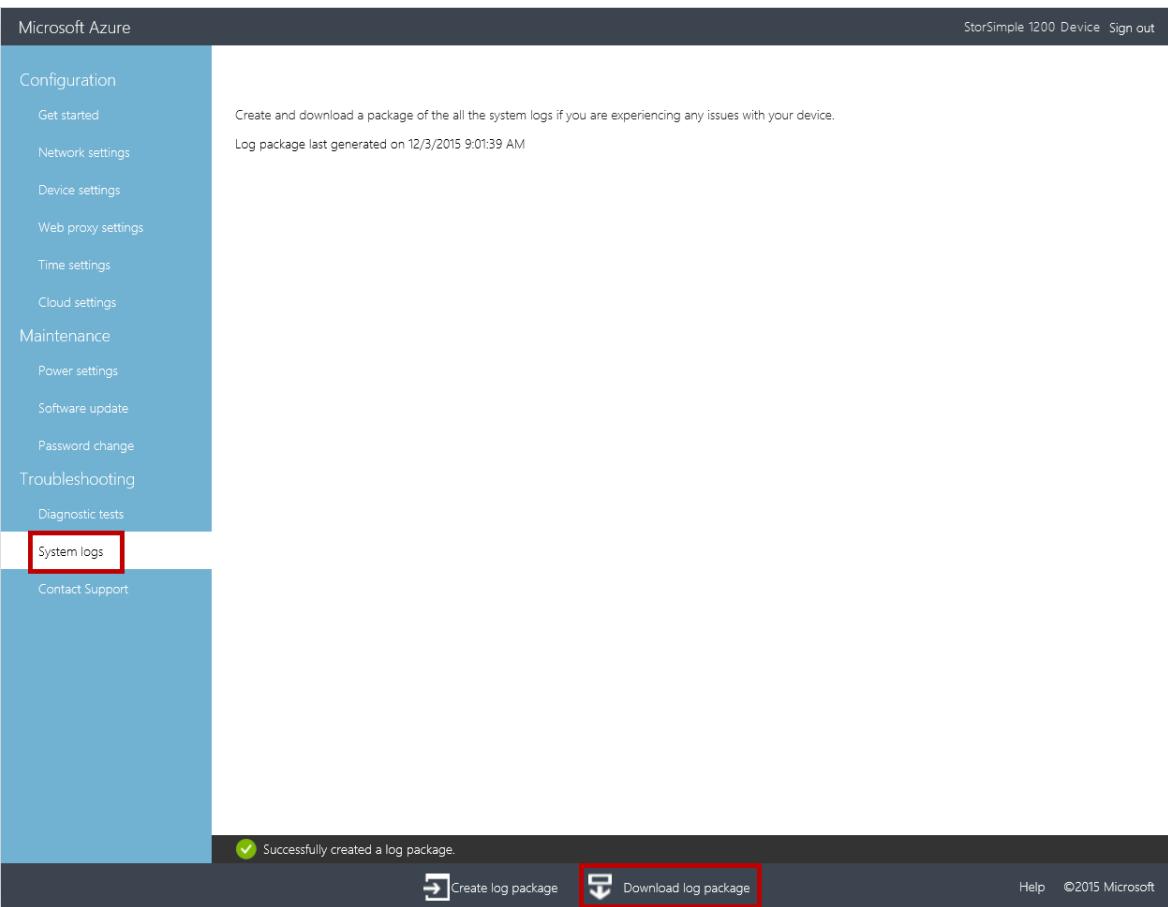


Help ©2015 Microsoft

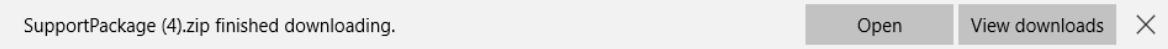
- At the bottom of the page, click **Create log package**. A package of the system logs will be created. This will take a couple of minutes.



You will be notified after the package is successfully created, and the page will be updated to indicate the time and date when the package was created.



3. Click **Download log package**. A zipped package will be downloaded on your system.



4. You can unzip the downloaded log package and view the system log files.

Shut down and restart your device

You can shut down or restart your virtual device using the local web UI. We recommend that before you restart, take the volumes or shares offline on the host and then the device. This will minimize any possibility of data corruption.

To shut down your virtual device

1. In the local web UI, go to **Maintenance > Power settings**.
2. At the bottom of the page, click **Shutdown**.

Configuration

[Get started](#)[Network settings](#)[Device settings](#)[Web proxy settings](#)[Time settings](#)[Cloud settings](#)

Maintenance

[Power settings](#)[Software update](#)[Password change](#)

Troubleshooting

[Diagnostic tests](#)[System logs](#)[Contact Support](#)

Use this interface to restart or shut down your StorSimple device. When the device restarts, IOs will be disrupted and your device will have a downtime. If you shut down the device, you will need to access the hypervisor management interface to start your device.

Restart

This will shut down and restart your device.

Shutdown

This will shut down your device.

 Restart  Shutdown

Help ©2015 Microsoft

3. A warning will appear stating that a shutdown of the device will interrupt any IO that were in progress, resulting in a downtime. Click the check icon .

Warning!

If you continue, the device will restart and IOs will be disrupted. This will result in a downtime.



You will be notified that the shutdown has been initiated.

 Successfully initiated a shutdown. Restart  Shutdown

Help ©2015 Microsoft

The device will now shut down. If you want to start your device, you will need to do that through the Hyper-V Manager.

To restart your virtual device

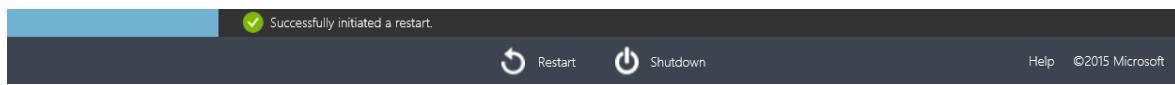
1. In the local web UI, go to **Maintenance > Power settings**.
2. At the bottom of the page, click **Restart**.

The screenshot shows the Microsoft Azure StorSimple 1200 Device maintenance interface. On the left, there's a sidebar with various settings: Configuration (Get started, Network settings, Device settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Software update, Password change), Troubleshooting (Diagnostic tests, System logs, Contact Support). The 'Power settings' link is highlighted with a red box. The main content area has a heading 'Use this interface to restart or shut down your StorSimple device. When the device restarts, IOs will be disrupted and your device will have a downtime. If you shut down the device, you will need to access the hypervisor management interface to start your device.' It contains two sections: 'Restart' (described as shutting down and restarting) and 'Shutdown' (described as shutting down). At the bottom of the main content area are 'Restart' and 'Shutdown' buttons. The footer includes 'Help' and '©2015 Microsoft'.

3. A warning will appear stating that restarting the device will interrupt any IOs that were in progress, resulting in a downtime. Click the check icon



You will be notified that the restart has been initiated.



While the restart is in progress, you will lose the connection to the UI. You can monitor the restart by refreshing the UI periodically. Alternatively, you can monitor the device restart status through the Hyper-V Manager.

Next steps

Learn how to [use the StorSimple Manager service to manage your device](#).

StorSimple Virtual Array Update 1.3 release notes

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated. As critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 1.3 corresponds to software version 10.0.10319.0.

ⓘ Important

- Update 1.3 is a critical update. We strongly recommend you install it as soon as possible.
- You can install Update 1.3 only on devices running Update 1.2.
- Updates are disruptive and restart your device. If I/O is in progress, the device incurs downtime. For detailed instructions on packages used to apply this update, go to [Download Update 1.3](#).

What's new in Update 1.3

This update contains the following improvements:

- Transport Layer Security (TLS) 1.2 is a mandatory update and must be installed. From this release onward, TLS 1.2 becomes the standard protocol for all Azure portal communication.

If you see the following warning, you must update the software on the device before proceeding:

One or more StorSimple devices are running an older software version. The latest available update for TLS 1.2 is a mandatory update and should be installed immediately on these devices. TLS 1.2 is used for all Azure portal communication and without this update, the device won't be able to communicate with the StorSimple service.

- Garbage collection bug fixes improve the performance of the garbage collection cycle when the device and storage account are in two distant regions.
- Fix for backup failures due to blob timeouts.
- Updated OS/.NET framework security patches:
 - [KB4540725](#) : March 2020 SSU (Servicing Stack Update)
 - [KB4565541](#) : July 2020 rollup
 - [KB4565622](#) : July 2020 .NET Framework update

Download Update 1.3

To download this update, go to the [Microsoft Update Catalog](#) server, and download the KB4575898 package. This package contains the following packages. Install the packages in this order:

1. **KB4540725**, which contains cumulative Windows Updates for 2012 R2 up to March 2020. For more information on what is included in this rollup, go to [March monthly security rollup](#).
2. **KB4565541**, which contains cumulative Windows Updates for 2012 R2 up to July 2020. For more information on what is included in this rollup, go to [July monthly security rollup](#).
3. **KB4565622**, which contains cumulative.NET Framework updates up to July 2020. For more information on what is included in this rollup, go to [KB4565622](#).
4. **KB3011067**, which contains device software updates.

Download KB4575898, and follow these instructions to [Apply the update via local web UI](#).

Known issues in Update 1.3

No new issues were release-noted in Update 1.3. All the release-noted issues are carried over from previous releases. To see the summary of known issues included from the

previous releases, go to [Known issues in Update 1.2](#).

Next steps

Download KB4575898 and [Apply the update via local web UI](#).

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 1.2 Release Notes](#)
- [StorSimple Virtual Array Update 1.0 Release Notes](#)
- [StorSimple Virtual Array Update 0.6 Release Notes](#)
- [StorSimple Virtual Array Update 0.5 Release Notes](#)
- [StorSimple Virtual Array Update 0.4 Release Notes](#)
- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 1.2 release notes

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated. As critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 1.2 corresponds to the software version 10.0.10311.0.

ⓘ Important

- Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime. For detailed instructions on packages used to apply this update, go to [Download Update 1.2](#).
- Update 1.2 is available to you via the Azure portal only if your device is running Update 1.0 or 1.1.

What's new in Update 1.2

This update contains the following bug fixes:

- Improved resiliency when processing deleted files.
- Improved handling exceptions in the code startup path leading to reduced failures in backups, restore, cloud-reads, and automated space reclamation.

Download Update 1.2

To download this update, go to the [Microsoft Update Catalog](#) server, and download the KB4502035 package. This package contains the following packages:

- **KB4493446** that contains cumulative Windows Updates for 2012 R2 up to April 2019. For more information on what is included in this rollup, go to [April monthly security rollup](#).
- **KB3011067** which is a Microsoft Update Standalone Package file WindowsTH-KB3011067-x64. This file is used to update the device software.

Download KB4502035 and follow these instructions to [Apply the update via local web UI](#).

Issues fixed in Update 1.2

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Deletion	In the previous versions of the software, there was an issue when the usage of the device didn't change even when files were deleted. This issue is fixed in this version. Tiering code path was made more resilient when processing deleted files.
2	Exception handling	In the previous versions of the software, there was an issue following the system reboot that could potentially lead to failures in backups, restore, reading from the cloud, and automated space reclamation. This release contains changes as to how the exceptions were handled in the startup path.

Known issues in Update 1.2

No new issues were release-noted in Update 1.2. All the release-noted issues are carried over from previous releases. To see the summary of known issues included from the previous releases, go to [Known issues in Update 1.1](#).

Next steps

Download KB4502035 and [Apply the update via local web UI](#).

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 1.1 Release Notes](#)
- [StorSimple Virtual Array Update 1.0 Release Notes](#)
- [StorSimple Virtual Array Update 0.6 Release Notes](#)
- [StorSimple Virtual Array Update 0.5 Release Notes](#)
- [StorSimple Virtual Array Update 0.4 Release Notes](#)
- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 1.0 release notes

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 1.0 corresponds to the software version 10.0.10296.0.

ⓘ Important

- Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime. For detailed instructions on how to apply the update, go to [Install Update 1.0](#).
- Update 1 is only available to you via the Azure portal if your device is running Update 0.6.

What's new in Update 1.0

Update 1.0 contains changes related to authentication of StorSimple Device Manager service and should be deployed at your earliest. This update contains the following

enhancements and bug fixes:

- **Use of Azure Active Directory (AAD) to authenticate with StorSimple Device Manager service** – From Update 1.0 onwards, Azure Active Directory is used to authenticate with the StorSimple Device Manager service. The old authentication mechanism will be deprecated by December 2017. All the users must include the new authentication URLs in their firewall rules. For more information, go to authentication URLs listed in the [Networking requirements for your StorSimple Virtual Array](#).

If the authentication URL is not included in the firewall rules, the users will see a critical alert that their StorSimple device could not authenticate with the service. If the users see this alert, they need to include the new authentication URL. For more information, go to [StorSimple networking alerts](#).

- **Performance improvement** - Several bug fixes were done to improve the speeds of cloud reads, tier-ins and tier-outs. As a result, both the backup and restore performance has improved for iSCSI and file server devices.
- **Garbage collection improvement** - This release has bug fixes that improve the performance of garbage collection cycle when the device and storage account are in two distant regions.
- **Logging improvement** - This release contains improvements to logging related to garbage collection and I/O path.

Issues fixed in Update 1.0

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	AAD-based authentication	This release contains changes that allows AAD to authenticate with the StorSimple Device Manager.
2	Garbage collection	This issue was reported at a customer site where the device and storage accounts are in different regions and the customer reported intermittent network errors thereby impacting the billing. In this release, this issue was fixed.
3	Performance	This release contains changes that result in restore/cloud reads/tier in/tier out performance improvement.
4	Update	There was an issue with update in the earlier release that resulted in backup failures at a customer site. This issue is fixed in this release.

Known issues in Update 1.0

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual arrays created in the preview release cannot be updated to a supported General Availability version.	These virtual arrays must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple Virtual Array, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.

No.	Feature	Issue	Workaround/comments
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This consumption is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release. For more information, go to Failover and disaster recovery for your StorSimple Virtual Array
10.	Azure PowerShell	The StorSimple Virtual Arrays cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-us keyboard format.	

No.	Feature	Issue	Workaround/comments
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Device Manager service and the iSCSI host.	The iSCSI host has the filesystem view. The device sees the blocks allocated when the volume was at the maximum size.
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	
15.	File server	Symbolic links are not supported.	
16.	File server	Files protected by Windows Encrypting File System (EFS) when copied over or stored on the StorSimple Virtual Array file server result in an unsupported configuration.	
17.	Updates	If you see Error code: 2359302 (hex 0x240006) when trying to install a hotfix through the local UI, then this implies that the hotfix is already installed on your device.	
18.	Updates	If you use the local web UI to install Update 1 on your virtual array, you must ensure that you are running Update 0.6. If you are running a version lower than Update 0.6, you must install Update 0.6 first and then apply Update 1. If you directly install Update 1.0 from a pre-Update 0.6 version, then you will miss some updates and the monitoring charts will not work.	

Next steps

[Install Update 1.0](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.6 Release Notes](#)
- [StorSimple Virtual Array Update 0.5 Release Notes](#)
- [StorSimple Virtual Array Update 0.4 Release Notes](#)
- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 0.6 release notes

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 0.6 corresponds to the software version 10.0.10293.0.

ⓘ Important

- Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime. For detailed instructions on how to apply the update, go to [Install Update 0.6](#).
- We strongly recommend that you install Update 0.6 immediately as it contains critical security fixes.

What's new in the Update 0.6

Update 0.6 is a critical update and should be deployed immediately. This update contains the following fixes:

- **Windows Security fixes** - This release has **Windows critical security fixes**. Review the following security updates for more information about the security issues and the associated fixes:
 - [December 2016 Security Only Quality Update for Windows 8.1 and Windows Server 2012 R2 ↗](#)
 - [March 2017 Security Only Quality Update for Windows 8.1 and Windows Server 2012 R2 ↗](#)
 - [May 9, 2017—KB4019213 \(Security-only update\) ↗](#)
- **Restore fix** - In earlier releases, there was a bug that would prevent the restore from completing. This bug has been fixed in this release.

Issues fixed in the Update 0.6

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Security	This release contains critical Windows Security updates. We suggest that you install this update immediately.
2	Restore	During a restore, there was a race condition that would prevent the restore job from completing. The bug fix addresses this race condition.

Known issues in the Update 0.6

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	

No.	Feature	Issue	Workaround/comments
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This consumption is because the used capacity for shares includes metadata.	

No.	Feature	Issue	Workaround/comments
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release. For more information, go to Failover and disaster recovery for your StorSimple Virtual Array
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-us keyboard format.	
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Device Manager service and the iSCSI host.	<p>The iSCSI host has the filesystem view.</p> <p>The device sees the blocks allocated when the volume was at the maximum size.</p>
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	
15.	File server	Symbolic links are not supported.	
16.	File server	Files protected by Windows Encrypting File System (EFS) when copied over or stored on the StorSimple Virtual Array file server result in an unsupported configuration.	

No.	Feature	Issue	Workaround/comments
17.	Updates	If you see Error code: 2359302 (hex 0x240006) when trying to install a hotfix through the local UI, then this implies that the hotfix is already installed on your device.	

Next step

[Install Update 0.6](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.5 Release Notes](#)
- [StorSimple Virtual Array Update 0.4 Release Notes](#)
- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 0.5 release notes

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 0.5 corresponds to the software version 10.0.10290.0.

ⓘ Note

Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime. For detailed instructions on how to apply the update, go to [Install Update 0.5](#).

What's new in the Update 0.5

Update 0.5 is primarily a bug-fix build. The main enhancements and bug-fixes are as follows:

- **Backup resiliency improvements** - This release has fixes that improve the backup resiliency. In the earlier releases, backups were retried only for certain exceptions.

This release retries all the backup exceptions and makes the backups more resilient.

- **Updates for storage usage monitoring** - Starting 30 June 2017, the storage usage monitoring for StorSimple Virtual Device Series will be retired. This applies to the monitoring charts on all the virtual arrays running Update 0.4 or lower. This update contains the changes required for you to continue the use of storage usage monitoring in the Azure portal. Install this critical update before June 30, 2017 to continue using the monitoring feature.

Issues fixed in the Update 0.5

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Backup resiliency	In the earlier releases, backups were retried only for certain exceptions. This release contains a fix to make backups more resilient by retrying all the backup exceptions.
2	Monitoring	The storage usage monitoring for StorSimple Virtual Device Series will be deprecated starting June 30, 2017. This action impacts the monitoring charts on the StorSimple Device Manager service running on StorSimple Virtual Arrays (1200 model). This release has updates that allow the user to continue the use of storage usage monitoring on the virtual arrays beyond June 30, 2017.
3	File server	In the earlier releases, a user could mistakenly copy encrypted files to the virtual array. This release contains a fix that would not allow copying of encrypted files to virtual array. If your device has existing encrypted files prior to the update, backups will continue to fail until all the encrypted files are deleted from the system.

Known issues in the Update 0.5

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.

No.	Feature	Issue	Workaround/comments
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.

No.	Feature	Issue	Workaround/comments
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This consumption is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release. For more information, go to Failover and disaster recovery for your StorSimple Virtual Array
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-us keyboard format.	
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Device Manager service and the iSCSI host.	The iSCSI host has the filesystem view. The device sees the blocks allocated when the volume was at the maximum size.
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	
15.	File server	Symbolic links are not supported.	

No.	Feature	Issue	Workaround/comments
16.	File server	Files protected by Windows Encrypting File System (EFS) when copied over or stored on the StorSimple Virtual Array file server result in an unsupported configuration.	

Next step

[Install Update 0.5](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.4 Release Notes](#)
- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 0.4 release notes

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 0.4 corresponds to the software version 10.0.10289.0.

ⓘ Note

Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime.

What's new in the Update 0.4

Update 0.4 is primarily a bug-fix build coupled with a few enhancements. In this version, several bugs resulting in backup failures in the previous version have been addressed. The main enhancements and bug-fixes are as follows:

- **Backup performance enhancements** - This release has made several key enhancements to improve the backup performance. As a result, the backups that

involve a large number of files see a significant reduction in the time to complete, for full and incremental backups.

- **Enhanced restore performance** - This release contains enhancements that significantly improve the restore performance when using large number of files. If using 2 - 4 million files, we recommend that you provision a virtual array with 16 GB RAM to see the improvements. When using less than 2 million files, the minimum requirement for the virtual machine continues to be 8 GB RAM.
- **Improvements to Support package** - The improvements include logging in the statistics for disk, CPU, memory, network, and cloud into the Support package thereby improving the process of diagnosing/debugging device issues.
- **Limit locally pinned iSCSI volumes to 200 GB** - For locally pinned volumes, we recommend that you limit to a 200 GB iSCSI volume on your StorSimple Virtual Array. The local reservation for tiered volumes continues to be 10 % of the provisioned volume size but is capped at 200 GB.
- **Backup-related bug fixes** - In previous versions of software, there were issues related to backups that would cause backup failures. These bugs have been addressed in this release.

Issues fixed in the Update 0.4

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Backup performance	In the earlier releases, the backups involving large number of files would take a long time to complete (in the order of days). In this release, both the full and incremental backups see a significant reduction in the time to completion.
2	Support package	Disk, CPU, memory, network, and cloud statistics are now logged in to the Support logs making the Support packages very effective in troubleshooting any device issues.
3	Backup	In earlier releases, long running backups could result in a space crunch on the device resulting in backup failures. This bug is addressed in this release by allowing no more than 5 backups to queue at one time.

No.	Feature	Issue
4	iSCSI	In earlier releases, the local reservation for tiered or locally pinned volumes was 10% of the provisioned volume size. In this release, the local reservation for all iSCSI volumes (locally pinned or tiered) is limited to 10 % with a maximum of up to 200 GB (for tiered volumes larger than 2 TB) thereby freeing up more space on the local disk. We recommend that the locally pinned volumes in this release be limited to 200 GB.

Known issues in the Update 0.4

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.

No.	Feature	Issue	Workaround/comments
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release.
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure classic portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-US keyboard format.	
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.

No.	Feature	Issue	Workaround/comments
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Manager service and the iSCSI host.	The iSCSI host has the filesystem view. The device sees the blocks allocated when the volume was at the maximum size.
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	
15.	File server	Symbolic links are not supported.	
16.	File server	Files protected by Windows Encrypting File System (EFS) when copied over or stored on the StorSimple Virtual Array file server result in an unsupported configuration.	

Next step

[Install Update 0.4](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 0.3 release notes

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 0.3 corresponds to the software version 10.0.10288.0.

ⓘ Note

Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime.

What's new in the Update 0.3

Update 0.3 is primarily a bug-fix build. In this version, several bugs resulting in backup failures in the previous version have been addressed.

Issues fixed in the Update 0.3

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Backups	<p>A problem was seen in the earlier release where the backups would fail to complete for a file share. If this issue occurred, the backup job would fail and a critical alert was raised on the StorSimple Manager service to notify the user. This issue did not affect the data on the shares or access to the data. The root cause was identified and fixed in this release.</p> <p>The fix does not apply retroactively to shares that are already seeing this issue. Customers who are seeing this issue should first apply Update 0.3, then contact Microsoft Support to perform a full system backup to fix the issue. Instead of contacting Microsoft Support, customers can also restore to a new share from a healthy backup for the affected shares.</p>
2	iSCSI	<p>An issue was seen in the earlier release where the volumes would disappear when copying data to a volume on the StorSimple Virtual Array. This issue was fixed in this release.</p> <p>The fixes take effect only on newly created volumes. The fixes do not apply retroactively to volumes that are already seeing this issue. Customers are advised to bring the affected volumes online via the Azure classic portal, perform a backup for these volumes, and then restore these volumes to new volumes.</p>

Known issues in the Update 0.3

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	

No.	Feature	Issue	Workaround/comments
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release.

No.	Feature	Issue	Workaround/comments
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure classic portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-US keyboard format.	
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Manager service and the iSCSI host. The device sees the blocks allocated when the volume was at the maximum size.	The iSCSI host has the filesystem view.
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	

Next step

[Install Update 0.3](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple Virtual Array Update 0.2 and 0.1 release notes

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates. (Microsoft Azure StorSimple Virtual Array is also known as the StorSimple on-premises virtual device or the StorSimple virtual device.)

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple virtual device, carefully review the information contained in the release notes.

Update 0.2 corresponds to the software version 10.0.10280.0; Update 0.1 is version 10.0.10279.0. The sections below list the changes for each update.

ⓘ Note

Updates are disruptive and will restart your device. If I/O are in progress, the device will incur downtime.

Issues fixed in the Update 0.2

Update 0.2 includes all changes from Update 0.1 in addition to the fix described in the following table:

Feature	Issue
Updates	In the last release, updates weren't detected automatically in the Azure classic portal, so you had to use the local Web UI to install updates. This issue is fixed in this release. After installing Update 0.2, you can install future updates using the Azure classic portal.

What's new in the Update 0.1

Update 0.1 contains the following bug fixes and improvements.

- **Improved resiliency for cloud outages:** This release has several bug fixes around disaster recovery, backup, restore, and tiering in the event of a cloud connectivity disruption.
- **Improved restore performance:** This release has bug fixes that have significantly cut down the completion time of the restore jobs.
- **Automated space reclamation optimization:** When data is deleted on thinly provisioned volumes, the unused storage blocks need to be reclaimed. This release has improved the space reclamation process from the cloud resulting in the unused space becoming available faster as compared to the previous versions.
- **New virtual disk images:** New VHD, VHDX, and VMDK are now available via the Azure classic portal. You can download these images to provision new Update 0.1 devices.
- **Improving the accuracy of jobs status in the portal:** In the earlier version of software, job status reporting in the portal was not granular. This issue is resolved in this release.
- **Domain join experience:** Bug fixes related to domain-joining and renaming of the device.

Issues fixed in the Update 0.1

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	VMDK	In some VMware versions, the OS disk was seen as sparse causing alerts and disrupting normal operations. This was fixed in this release.
2	iSCSI server	In the last release, the user was required to specify a gateway for each enabled network interface of your StorSimple virtual device. This behavior is changed in this release so that the user has to configure at least one gateway for all the enabled network interfaces.

No.	Feature	Issue
3	Support package	In the earlier version of software, Support package collection failed when the package sizes were larger than 1 GB. This issue is fixed in this release.
4	Cloud access	In the last release, if the StorSimple Virtual Array did not have network connectivity and was restarted, the local UI would have connectivity issues. This problem is fixed in this release.
5	Monitoring charts	In the previous release, following a device failover, the cloud capacity utilization charts displayed incorrect values in the Azure classic portal. This is fixed in the current release.

Known issues in the Update 0.1

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases. **The issues release noted in this release are marked with an asterisk. Almost all the issues in this list have carried over from the GA release of StorSimple Virtual Array.**

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do so will result in a loss of all the data in the local tiers of the device.	
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.

No.	Feature	Issue	Workaround/comments
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering will not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> If using locally pinned volumes and byte range locking is enabled, be aware that the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption in the absence of any data on the share. This is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This will be implemented in a later release.
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure classic portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-US keyboard format.	

No.	Feature	Issue	Workaround/comments
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you will need to take the volumes offline and then bring them online for the change to take effect.	These will be addressed in a later release.
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Manager service and the iSCSI host. The device sees the blocks allocated when the volume was at the maximum size.	The iSCSI host has the filesystem view.
14.	File server*	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	

Next step

[Install Updates](#) on your StorSimple Virtual Array.

StorSimple 8000 series: a hybrid cloud storage solution

Article • 03/22/2023 • 24 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Welcome to Microsoft Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Microsoft Azure cloud storage. StorSimple is an efficient, cost-effective, and easy to manage storage area network (SAN) solution that eliminates many of the issues and expenses that are associated with enterprise storage and data protection. It uses the proprietary StorSimple 8000 series device, integrates with cloud services, and provides a set of management tools for a seamless view of all enterprise storage, including cloud storage. The StorSimple deployment information published on the Microsoft Azure website applies to StorSimple 8000 series devices only.

StorSimple uses [storage tiering](#) to manage stored data across various storage media. The current working set is stored on-premises on solid state drives (SSDs). Data that is used less frequently is stored on hard disk drives (HDDs), and archival data is pushed to the cloud. Moreover, StorSimple uses deduplication and compression to reduce the amount of storage that the data consumes. For more information, go to [Deduplication and compression](#). For definitions of other key terms and concepts that are used in the StorSimple 8000 series documentation, go to [StorSimple terminology](#) at the end of this article.

In addition to storage management, StorSimple data protection features enable you to create on-demand and scheduled backups, and then store them locally or in the cloud. Backups are taken in the form of incremental snapshots, which means that they can be created and restored quickly. Cloud snapshots can be critically important in disaster

recovery scenarios because they replace secondary storage systems (such as tape backup), and allow you to restore data to your datacenter or to alternate sites if necessary.

Why use StorSimple?

The following table describes some of the key benefits that Microsoft Azure StorSimple provides.

Feature	Benefit
Transparent integration	Uses the iSCSI protocol to invisibly link data storage facilities. Data stored in the cloud, at the datacenter, or on remote servers appear to be stored at a single location.
Reduced storage costs	Allocates sufficient local or cloud storage to meet current demands and extends cloud storage only when necessary. It further reduces storage requirements and expense by eliminating redundant versions of the same data (deduplication) and by using compression.
Simplified storage management	Provides system administration tools to configure and manage data stored on-premises, on a remote server, and in the cloud. Additionally, you can manage backup and restore functions from a Microsoft Management Console (MMC) snap-in.
Improved disaster recovery and compliance	Doesn't require extended recovery time. Instead, it restores data as it is needed so that normal operations can continue with minimal disruption. Additionally, you can configure policies to specify backup schedules and data retention.
Data mobility	Data uploaded to Microsoft Azure cloud services can be accessed from other sites for recovery and migration purposes. Additionally, you can use StorSimple to configure StorSimple Cloud Appliances on virtual machines (VMs) running in Microsoft Azure. The VMs can then use virtual devices to access stored data for test or recovery purposes.
Business continuity	Allows StorSimple 5000-7000 series users to migrate their data to a StorSimple 8000 series device.
Availability in the Azure Government Portal	StorSimple is available in the Azure Government Portal. For more information, see Deploy your on-premises StorSimple device in the Government Portal .
Data protection and availability	The StorSimple 8000 series supports Zone Redundant Storage (ZRS), in addition to Locally Redundant Storage (LRS) and Geo-redundant storage (GRS). Refer to this article on Azure Storage redundancy options for ZRS details.

Feature	Benefit
Support for critical applications	StorSimple lets you identify appropriate volumes as locally pinned to ensure that data that is required by critical applications isn't tiered to the cloud. Locally pinned volumes aren't subject to cloud latencies or connectivity issues. For more information about locally pinned volumes, see Use the StorSimple Device Manager service to manage volumes .
Low latency and high performance	You can create cloud appliances that take advantage of the high performance, low latency features of Azure premium storage. For more information about StorSimple premium cloud appliances, see Deploy and manage a StorSimple Cloud Appliance in Azure .

StorSimple components

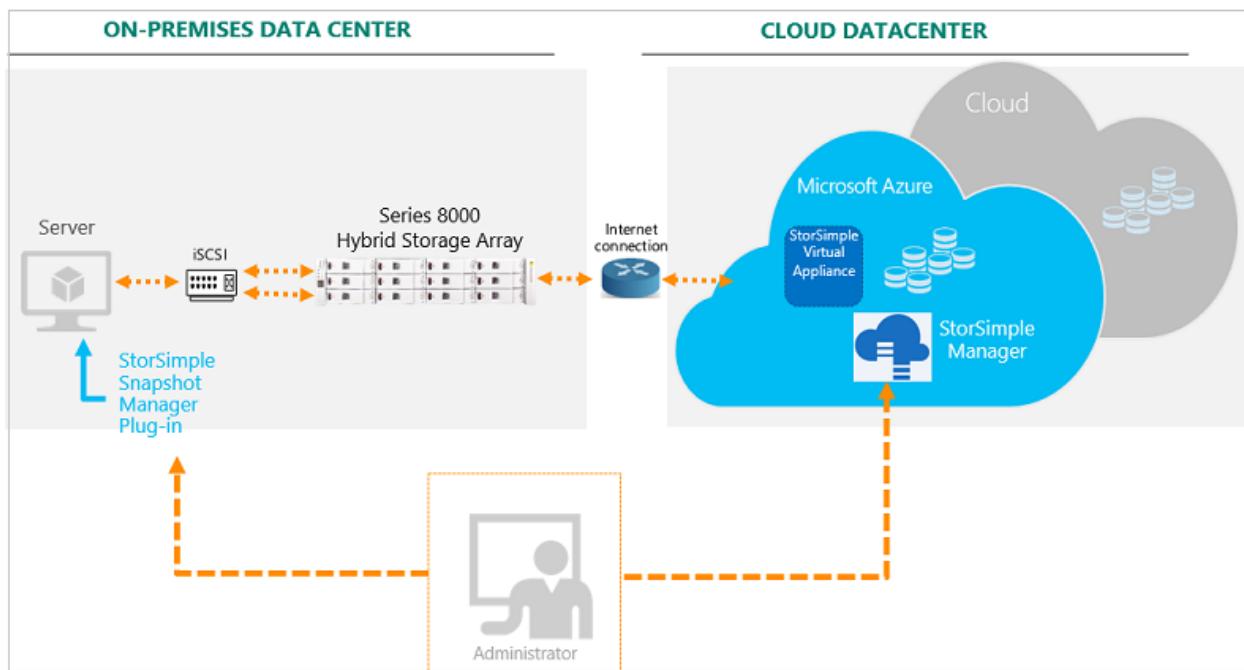
The Microsoft Azure StorSimple solution includes the following components:

- **Microsoft Azure StorSimple device** – an on-premises hybrid storage array that contains SSDs and HDDs, together with redundant controllers and automatic failover capabilities. The controllers manage storage tiering, placing currently used (or hot) data on local storage (in the device or on-premises servers), while moving less frequently used data to the cloud.
- **StorSimple Cloud Appliance** – also known as the StorSimple Virtual Appliance. A software version of the StorSimple device that replicates the architecture and most capabilities of the physical hybrid storage device. The StorSimple Cloud Appliance runs on a single node in an Azure virtual machine. Premium virtual devices, which take advantage of Azure premium storage, are available in Update 2 and later.
- **StorSimple Device Manager service** – an extension of the Azure portal that lets you manage a StorSimple device or StorSimple Cloud Appliance from a single web interface. You can use the StorSimple Device Manager service to create and manage services, view and manage devices, view alerts, manage volumes, and view and manage backup policies and the backup catalog.
- **Windows PowerShell for StorSimple** – a command-line interface that you can use to manage the StorSimple device. Windows PowerShell for StorSimple has features that allow you to register your StorSimple device, configure the network interface on your device, install certain types of updates, troubleshoot your device by accessing the support session, and change the device state. You can access Windows PowerShell for StorSimple by connecting to the serial console or using Windows PowerShell remoting.
- **Azure PowerShell StorSimple cmdlets** – a collection of Windows PowerShell cmdlets that allow you to automate service-level and migration tasks from the

command line. For more information about the Azure PowerShell cmdlets for StorSimple, go to the [cmdlet reference](#).

- **StorSimple Snapshot Manager** – an MMC snap-in that uses volume groups and the Windows Volume Shadow Copy Service to generate application-consistent backups. In addition, you can use StorSimple Snapshot Manager to create backup schedules and clone or restore volumes.
- **StorSimple Adapter for SharePoint** – a tool that transparently extends Microsoft Azure StorSimple storage and data protection to SharePoint Server farms, while making StorSimple storage viewable and manageable from the SharePoint Central Administration portal.

The diagram below provides a high-level view of the Microsoft Azure StorSimple architecture and components.



The following sections describe each of these components in greater detail and explain how the solution arranges data, allocates storage, and facilitates storage management and data protection. The last section provides definitions for some of the important terms and concepts that are related to StorSimple components and their management.

StorSimple device

The Microsoft Azure StorSimple device is an on-premises hybrid storage array that provides primary storage and iSCSI access to data stored on it. It manages communication with cloud storage, and helps to ensure the security and confidentiality of all data that is stored on the Microsoft Azure StorSimple solution.

The StorSimple device includes SSDs and hard disk drives (HDDs), as well as support for clustering and automatic failover. It contains a shared processor, shared storage, and two mirrored controllers. Each controller provides the following:

- Connection to a host computer
- Up to six network ports to connect to the local area network (LAN)
- Hardware monitoring
- Non-volatile random access memory (NVRAM), which retains information even if power is interrupted
- Cluster-aware updating to manage software updates on servers in a failover cluster so that the updates have minimal or no effect on service availability
- Cluster service, which functions like a back-end cluster, providing high availability and minimizing any adverse effects that might occur if an HDD or SSD fails or is taken offline

Only one controller is active at any point in time. If the active controller fails, the second controller becomes active automatically.

For more information, go to [StorSimple hardware components and status](#).

StorSimple Cloud Appliance

You can use StorSimple to create a cloud appliance that replicates the architecture and capabilities of the physical hybrid storage device. The StorSimple Cloud Appliance (also known as the StorSimple Virtual Appliance) runs on a single node in an Azure virtual machine. (A cloud appliance can only be created on an Azure virtual machine. You can't create one on a StorSimple device or an on-premises server.)

The cloud appliance has the following features:

- It behaves like a physical appliance and can offer an iSCSI interface to virtual machines in the cloud.
- You can create an unlimited number of cloud appliances in the cloud, and turn them on and off as necessary.
- It can help simulate on-premises environments in disaster recovery, development, and test scenarios, and can help with item-level retrieval from backups.

The StorSimple Cloud Appliance is available in two models: the 8010 device (formerly known as the 1100 model) and the 8020 device. The 8010 device has a maximum capacity of 30 TB. The 8020 device, which takes advantage of Azure premium storage, has a maximum capacity of 64 TB. (In local tiers, Azure premium storage stores data on

SSDs whereas standard storage stores data on HDDs.) You must have an Azure premium storage account to use premium storage.

For more information about the StorSimple Cloud Appliance, go to [Deploy and manage a StorSimple Cloud Appliance in Azure](#).

StorSimple Device Manager service

Microsoft Azure StorSimple provides a web-based user interface (the StorSimple Device Manager service) that enables you to centrally manage datacenter and cloud storage.

You can use the StorSimple Device Manager service to perform the following tasks:

- Configure system settings for StorSimple devices.
- Configure and manage security settings for StorSimple devices.
- Configure cloud credentials and properties.
- Configure and manage volumes on a server.
- Configure volume groups.
- Back up and restore data.
- Monitor performance.
- Review system settings and identify possible problems.

You can use the StorSimple Device Manager service to perform all administration tasks except tasks that require system down time, such as initial setup and installation of updates.

For more information, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Windows PowerShell for StorSimple

Windows PowerShell for StorSimple provides a command-line interface that you can use to create and manage the Microsoft Azure StorSimple service and set up and monitor StorSimple devices. It's a Windows PowerShell-based, command-line interface that includes dedicated cmdlets for managing your StorSimple device. Windows PowerShell for StorSimple has features that allow you to:

- Register a device.
- Configure the network interface on a device.
- Install certain types of updates.
- Troubleshoot your device by accessing the support session.
- Change the device state.

You can access Windows PowerShell for StorSimple from a serial console (on a host computer connected directly to the device) or remotely by using Windows PowerShell remoting. Some Windows PowerShell for StorSimple tasks, such as initial device registration, can only be done on the serial console.

For more information, go to [Use Windows PowerShell for StorSimple to administer your device](#).

Azure PowerShell StorSimple cmdlets

The Azure PowerShell StorSimple cmdlets are a collection of Windows PowerShell cmdlets that allow you to automate service-level and migration tasks from the command line. For more information about the Azure PowerShell cmdlets for StorSimple, go to the [cmdlet reference](#).

StorSimple Snapshot Manager

StorSimple Snapshot Manager is a Microsoft Management Console (MMC) snap-in that you can use to create consistent, point-in-time backup copies of local and cloud data. The snap-in runs on a Windows Server-based host. You can use StorSimple Snapshot Manager to:

- Configure, back up, and delete volumes.
- Configure volume groups to ensure that backed up data is application-consistent.
- Manage backup policies so that data is backed up on a predetermined schedule and stored in a designated location (locally or in the cloud).
- Restore volumes and individual files.

Backups are captured as snapshots, which record only the changes since the last snapshot was taken and require far less storage space than full backups. You can create backup schedules or take immediate backups as needed. Additionally, you can use StorSimple Snapshot Manager to establish retention policies that control how many snapshots will be saved. If you later need to restore data from a backup, StorSimple Snapshot Manager lets you select from the catalog of local or cloud snapshots.

If a disaster occurs or if you need to restore data for another reason, StorSimple Snapshot Manager restores it incrementally as it's needed. Data restoration doesn't require that you shut down the entire system while you restore a file, replace equipment, or move operations to another site.

For more information, go to [What is StorSimple Snapshot Manager?](#)

StorSimple Adapter for SharePoint

Microsoft Azure StorSimple includes the StorSimple Adapter for SharePoint, an optional component that transparently extends StorSimple storage and data protection features to SharePoint Server farms. The adapter works with a Remote Blob Storage (RBS) provider and the SQL Server RBS feature, allowing you to move BLOBs to a server backed up by the Microsoft Azure StorSimple system. Microsoft Azure StorSimple then stores the BLOB data locally or in the cloud, based on usage.

The StorSimple Adapter for SharePoint is managed from within the SharePoint Central Administration portal. So SharePoint management remains centralized, and all storage appears to be in the SharePoint farm.

For more information, go to [StorSimple Adapter for SharePoint](#).

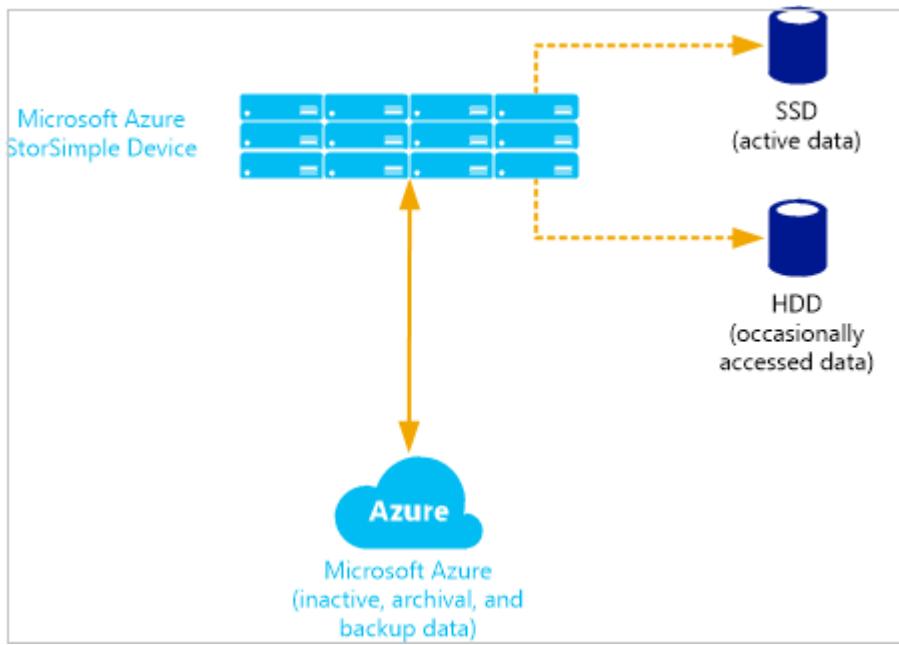
Storage management technologies

In addition to the dedicated StorSimple device, virtual device, and other components, Microsoft Azure StorSimple uses the following software technologies to provide quick access to data and to reduce storage consumption:

- [Automatic storage tiering](#)
- [Thin provisioning](#)
- [Deduplication and compression](#)

Automatic storage tiering

Microsoft Azure StorSimple automatically arranges data in logical tiers based on current usage, age, and relationship to other data. Data that is most active is stored locally, while less active and inactive data is automatically migrated to the cloud. The following diagram illustrates this storage approach.



To enable quick access, StorSimple stores very active data (hot data) on SSDs in the StorSimple device. It stores data that is used occasionally (warm data) on HDDs in the device or on servers at the datacenter. It moves inactive data, backup data, and data retained for archival or compliance purposes to the cloud.

① Note

In Update 2 or later, you can specify a volume as locally pinned, in which case the data remains on the local device and is not tiered to the cloud.

StorSimple adjusts and rearranges data and storage assignments as usage patterns change. For example, some information might become less active over time. As it becomes progressively less active, it's migrated from SSDs to HDDs and then to the cloud. If that same data becomes active again, it's migrated back to the storage device.

The storage tiering process occurs as follows:

1. A system administrator sets up a Microsoft Azure cloud storage account.
2. The administrator uses the serial console and the StorSimple Device Manager service (running in the Azure portal) to configure the device and file server, creating volumes and data protection policies. On-premises machines (such as file servers) use the Internet Small Computer System Interface (iSCSI) to access the StorSimple device.
3. Initially, StorSimple stores data on the fast SSD tier of the device.
4. As the SSD tier approaches capacity, StorSimple deduplicates and compresses the oldest data blocks, and moves them to the HDD tier.
5. As the HDD tier approaches capacity, StorSimple encrypts the oldest data blocks and sends them securely to the Microsoft Azure storage account via HTTPS.

6. Microsoft Azure creates multiple replicas of the data in its datacenter and in a remote datacenter, ensuring that the data can be recovered if a disaster occurs.
7. When the file server requests data stored in the cloud, StorSimple returns it seamlessly and stores a copy on the SSD tier of the StorSimple device.

 **Important**

When using StorSimple, do not convert blobs to archival, even if your device is being phased out. To retrieve data from the device, you'll need to rehydrate the blobs from archival to the hot or cool type, which results in significant costs.

How StorSimple manages cloud data

StorSimple deduplicates customer data across all the snapshots and the primary data (data written by hosts). While deduplication is great for storage efficiency, it makes the question of "what is in the cloud" complicated. The tiered primary data and the snapshot data overlap with each other. A single chunk of data in the cloud could be used as tiered primary data and also be referenced by several snapshots. Every cloud snapshot ensures that a copy of all the point-in-time data is locked into the cloud until that snapshot is deleted.

Data is only deleted from the cloud when there are no references to that data. For example, if we took a cloud snapshot of all the data that is in the StorSimple device and then deleted some primary data, we would see the *primary data* drop immediately. The *cloud data*, which includes the tiered data and the backups, stays the same because a snapshot is still referencing the cloud data. After the cloud snapshot is deleted (and any other snapshot that referenced the same data), cloud consumption drops. Before we remove cloud data, we check that no snapshots still reference that data. This process is called *garbage collection* and is a background service running on the device. Removal of cloud data isn't immediate as the garbage collection service checks for other references to that data before the deletion. The speed of garbage collection depends on the total number of snapshots and the total data. Typically, the cloud data is cleaned up in less than a week.

Thin provisioning

Thin provisioning is a virtualization technology in which available storage appears to exceed physical resources. Instead of reserving sufficient storage in advance, StorSimple uses thin provisioning to allocate just enough space to meet current requirements. The

elastic nature of cloud storage facilitates this approach because StorSimple can increase or decrease cloud storage to meet changing demands.

ⓘ Note

Locally pinned volumes are not thinly provisioned. Storage allocated to a local-only volume is provisioned in its entirety when the volume is created.

Deduplication and compression

Microsoft Azure StorSimple uses deduplication and data compression to further reduce storage requirements.

Deduplication reduces the overall amount of data stored by eliminating redundancy in the stored data set. As information changes, StorSimple ignores the unchanged data and captures only the changes. In addition, StorSimple reduces the amount of stored data by identifying and removing unnecessary information.

ⓘ Note

Data on locally pinned volumes is not deduplicated or compressed. However, backups of locally pinned volumes are deduplicated and compressed.

StorSimple workload summary

A summary of the supported StorSimple workloads is tabulated below.

Scenario	Workload	Supported	Restrictions	Version
Collaboration	File sharing	Yes		All versions
Collaboration	Distributed file sharing	Yes		All versions
Collaboration	SharePoint	Yes*	Supported only with locally pinned volumes	Update 2 and later
Archival	Simple file archiving	Yes		All versions
Virtualization	Virtual machines	Yes*	Supported only with locally pinned volumes	Update 2 and later

Scenario	Workload	Supported	Restrictions	Version
Database	SQL	Yes*	Supported only with locally pinned volumes	Update 2 and later
Video surveillance	Video surveillance	Yes*	Supported when StorSimple device is dedicated only to this workload	Update 2 and later
Backup	Primary target backup	Yes*	Supported when StorSimple device is dedicated only to this workload	Update 3 and later
Backup	Secondary target backup	Yes*	Supported when StorSimple device is dedicated only to this workload	Update 3 and later

Yes - Solution guidelines and restrictions should be applied.*

The following workloads aren't supported by StorSimple 8000 series devices. If deployed on StorSimple, these workloads will result in an unsupported configuration.

- Medical imaging
- Exchange
- VDI
- Oracle
- SAP
- Big data
- Content distribution
- Boot from SCSI

Following is a list of the StorSimple supported infrastructure components.

Scenario	Workload	Supported	Restrictions	Version
General	Express Route	Yes		All versions
General	DataCore FC	Yes*	Supported with DataCore SANsymphony	All versions
General	DFSR	Yes*	Supported only with locally pinned volumes	All versions
General	Indexing	Yes*	For tiered volumes, only metadata indexing is supported (no data). For locally pinned volumes, complete indexing is supported.	All versions

Scenario	Workload	Supported	Restrictions	Version
General	Anti-virus	Yes*	For tiered volumes, only scan on open and close is supported. For locally pinned volumes, full scan is supported.	All versions

Yes - Solution guidelines and restrictions should be applied.*

Following is a list of other software used with StorSimple to build solutions.

Workload type	Software used with StorSimple	Supported versions	Link to solution guide
Backup target	Veeam	Veeam v 9 and later	StorSimple as a backup target with Veeam
Backup target	Veritas Backup Exec	Backup Exec 16 and later	StorSimple as a backup target with Backup Exec
Backup target	Veritas NetBackup	NetBackup 7.7.x and later	StorSimple as a backup target with NetBackup
Global File Sharing	Talon	StorSimple with Talon	
Collaboration			

StorSimple terminology

Before deploying your Microsoft Azure StorSimple solution, we recommend that you review the following terms and definitions.

Key terms and definitions

Term (Acronym or abbreviation)	Description
access control record (ACR)	A record associated with a volume on your Microsoft Azure StorSimple device that determines which hosts can connect to it. The determination is based on the iSCSI Qualified Name (IQN) of the hosts (contained in the ACR) that are connecting to your StorSimple device.
AES-256	A 256-bit Advanced Encryption Standard (AES) algorithm for encrypting data as it moves to and from the cloud.

Term (Acronym or abbreviation)	Description
allocation unit size (AUS)	<p>The smallest amount of disk space that can be allocated to hold a file in your Windows file systems. If a file size isn't an even multiple of the cluster size, extra space must be used to hold the file (up to the next multiple of the cluster size) resulting in lost space and fragmentation of the hard disk.</p> <p>The recommended AUS for Azure StorSimple volumes is 64 KB because it works well with the deduplication algorithms.</p>
automated storage tiering	<p>Automatically moving less active data from SSDs to HDDs and then to a tier in the cloud, and then enabling management of all storage from a central user interface.</p>
backup catalog	<p>A collection of backups, usually related by the application type that was used. This collection is displayed in the Backup Catalog blade of the StorSimple Device Manager service UI.</p>
backup catalog file	<p>A file containing a list of available snapshots currently stored in the backup database of StorSimple Snapshot Manager.</p>
backup policy	<p>A selection of volumes, type of backup, and a timetable that allows you to create backups on a predefined schedule.</p>
binary large objects (BLOBs)	<p>A collection of binary data stored as a single entity in a database management system. BLOBs are typically images, audio, or other multimedia objects, although sometimes binary executable code is stored as a BLOB.</p>
Challenge Handshake Authentication Protocol (CHAP)	<p>A protocol used to authenticate the peer of a connection, based on the peer sharing a password or secret. CHAP can be one-way or mutual. With one-way CHAP, the target authenticates an initiator. Mutual CHAP requires that the target authenticate the initiator and that the initiator authenticate the target.</p>
clone	<p>A duplicate copy of a volume.</p>
Cloud as a Tier (CaaT)	<p>Cloud storage integrated as a tier within the storage architecture so that all storage appears to be part of one enterprise storage network.</p>
cloud service provider (CSP)	<p>A provider of cloud computing services.</p>
cloud snapshot	<p>A point-in-time copy of volume data that is stored in the cloud. A cloud snapshot is equivalent to a snapshot replicated on a different, off-site storage system. Cloud snapshots are particularly useful in disaster recovery scenarios.</p>
cloud storage encryption key	<p>A password or a key used by your StorSimple device to access the encrypted data sent by your device to the cloud.</p>

Term (Acronym or abbreviation)	Description
cluster-aware updating	Managing software updates on servers in a failover cluster so that the updates have minimal or no effect on service availability.
datapath	A collection of functional units that perform inter-connected data processing operations.
deactivate	A permanent action that breaks the connection between the StorSimple device and the associated cloud service. Cloud snapshots of the device remain after this process and can be cloned or used for disaster recovery.
disk mirroring	Replication of logical disk volumes on separate hard drives in real time to ensure continuous availability.
dynamic disk mirroring	Replication of logical disk volumes on dynamic disks.
dynamic disks	A disk volume format that uses the Logical Disk Manager (LDM) to store and manage data across multiple physical disks. Dynamic disks can be enlarged to provide more free space.
Extended Bunch of Disks (EBOD) enclosure	A secondary enclosure of your Microsoft Azure StorSimple device that contains extra hard drive disks for additional storage.
fat provisioning	A conventional storage provisioning in which storage space is allocated based on anticipated needs (and is usually beyond the current need). See also <i>thin provisioning</i> .
hard disk drive (HDD)	A drive that uses rotating platters to store data.
hybrid cloud storage	A storage architecture that uses local and off-site resources, including cloud storage.
Internet Small Computer System Interface (iSCSI)	An Internet Protocol (IP)-based storage networking standard for linking data storage equipment or facilities.
iSCSI initiator	A software component that enables a host computer running Windows to connect to an external iSCSI-based storage network.
iSCSI Qualified Name (IQN)	A unique name that identifies an iSCSI target or initiator.

Term (Acronym or abbreviation)	Description
iSCSI target	A software component that provides centralized iSCSI disk subsystems in storage area networks.
live archiving	A storage approach in which archival data is accessible all the time (it isn't stored off-site on tape, for example). Microsoft Azure StorSimple uses live archiving.
locally pinned volume	a volume that resides on the device and is never tiered to the cloud.
local snapshot	A point-in-time copy of volume data that is stored on the Microsoft Azure StorSimple device.
Microsoft Azure StorSimple	A powerful solution consisting of a datacenter storage appliance and software that enables IT organizations to leverage cloud storage as though it were datacenter storage. StorSimple simplifies data protection and data management while reducing costs. The solution consolidates primary storage, archive, backup, and disaster recovery (DR) through seamless integration with the cloud. By combining SAN storage and cloud data management on an enterprise-class platform, StorSimple devices enable speed, simplicity, and reliability for all storage-related needs.
Power and Cooling Module (PCM)	Hardware components of your StorSimple device consisting of the power supplies and the cooling fan; hence, the name Power and Cooling module. The primary enclosure of the device has two 764W PCMs whereas the EBOD enclosure has two 580W PCMs.
primary enclosure	Main enclosure of your StorSimple device that contains the application platform controllers.
recovery time objective (RTO)	The maximum amount of time that should be expended before a business process or system is fully restored after a disaster.
serial attached SCSI (SAS)	A type of hard disk drive (HDD).
service data encryption key	A key made available to any new StorSimple device that registers with the StorSimple Device Manager service. The configuration data transferred between the StorSimple Device Manager service and the device is encrypted using a public key and can then be decrypted only on the device using a private key. Service data encryption key allows the service to obtain this private key for decryption.
service registration key	A key that helps register the StorSimple device with the StorSimple Device Manager service so that it appears in the Azure portal for further management actions.

Term (Acronym or abbreviation)	Description
Small Computer System Interface (SCSI)	A set of standards for physically connecting computers and passing data between them.
solid state drive (SSD)	A disk that contains no moving parts; for example, a flash drive.
storage account	A set of access credentials linked to your storage account for a given cloud service provider.
StorSimple Adapter for SharePoint	A Microsoft Azure StorSimple component that transparently extends StorSimple storage and data protection to SharePoint Server farms.
StorSimple Device Manager service	An extension of the Azure portal that allows you to manage your Azure StorSimple on-premises and virtual devices.
StorSimple Snapshot Manager	A Microsoft Management Console (MMC) snap-in for managing backup and restore operations in Microsoft Azure StorSimple.
take backup	A feature that allows the user to take an interactive backup of a volume. It's an alternate way of taking a manual backup of a volume as opposed to taking an automated backup via a defined policy.
thin provisioning	A method of optimizing the efficiency with which the available storage space is used in storage systems. In thin provisioning, the storage is allocated among multiple users based on the minimum space required by each user at any given time. See also <i>fat provisioning</i> .
tiering	Arranging data in logical groupings based on current usage, age, and relationship to other data. StorSimple automatically arranges data in tiers.
volume	Logical storage areas presented in the form of drives. StorSimple volumes correspond to the volumes mounted by the host, including those volumes discovered by using iSCSI and a StorSimple device.
volume container	A grouping of volumes and the settings that apply to them. All volumes in your StorSimple device are grouped into volume containers. Volume container settings include storage accounts, encryption settings for data sent to cloud with associated encryption keys, and bandwidth consumed for operations involving the cloud.

Term (Acronym or abbreviation)	Description
volume group	In StorSimple Snapshot Manager, a volume group is a collection of volumes configured to facilitate backup processing.
Volume Shadow Copy Service (VSS)	A Windows Server operating system service that facilitates application consistency by communicating with VSS-aware applications to coordinate the creation of incremental snapshots. VSS ensures that the applications are temporarily inactive when snapshots are taken.
Windows PowerShell for StorSimple	A Windows PowerShell-based command-line interface used to operate and manage your StorSimple device. While maintaining some of the basic capabilities of Windows PowerShell, this interface has additional dedicated cmdlets that are geared towards managing a StorSimple device.

Next steps

Learn about [StorSimple security](#).

Compare StorSimple with Azure File Sync and Azure Stack Edge data transfer options

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This document provides an overview of options for on-premises data transfer to Azure, comparing: Azure Stack Edge vs. Azure File Sync vs. StorSimple 8000 series.

- [Azure Stack Edge](#) – Azure Stack Edge is an on-premises network device that moves data into and out of Azure and has AI-enabled Edge compute to pre-process data during upload. Data Box Gateway is a virtual version of the device with the same data transfer capabilities.
- [Azure File Sync](#) – Azure File Sync can be used to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. General availability of Azure File Sync was announced earlier in 2018.
- [StorSimple](#) – StorSimple is a hybrid device that helps enterprises consolidate their storage infrastructure for primary storage, data protection, archiving, and disaster recovery on a single solution by tightly integrating with Azure storage. The product lifecycle for StorSimple can be found [here](#).

Comparison summary

	StorSimple 8000	Azure File Sync	Azure Stack Edge
Overview	Tiered hybrid storage and archival	General file server storage with cloud tiering and multi-site sync.	Storage solution to pre-process data and send it over network to Azure.

	StorSimple 8000	Azure File Sync	Azure Stack Edge
Scenarios	File server, archival, backup target	File server, archival (multi-site)	Data transfer, data pre-processing including ML inferencing, IoT, archival
Edge compute	Not available	Not available	Supports running containers using Azure IoT Edge
Form factor	Physical device	Agent installed on Windows Server	Physical device
Hardware	Physical device provided from Microsoft as part of the service	Customer provided	Physical device provided from Microsoft as part of the service
Data format	Custom format	Files	Blobs or Files
Protocol support	iSCSI	SMB, NFS	SMB or NFS
Pricing	StorSimple	Azure File Sync	Data Box Edge

Next steps

- Learn about [Azure Data Box Edge](#) and [Azure Data Box Gateway](#)
- Learn about [Azure File Sync](#)

Additional resources

Documentation

[Azure data transfer options for large datasets with low or no network bandwidth](#)

Learn how to choose an Azure solution for data transfer when you have limited to no network bandwidth in your environment and you are planning to transfer large data sets.

[Storage architecture - Azure Architecture Center](#)

Get an overview of Azure Storage technologies, guidance offerings, solution ideas, and reference architectures.

[Azure Storage migration tools comparison - Unstructured data](#)

Basic functionality and comparison between tools used for migration of unstructured data

[Review your storage options - Cloud Adoption Framework](#)

Use the Cloud Adoption Framework for Azure to learn how to review your storage options for Azure workloads.

[Hybrid file share with disaster recovery for remote and local branch workers - Azure Example Scenarios](#)

Learn how to provide high-availability desktop access to file shares in an environment with many on-premises locations, and a workforce that works on-premises and remotely.

[Azure Files secured by AD DS - Azure Architecture Center](#)

Learn how to provide secure Azure Files that are secured by on-premises Windows Server Active Directory domain services (AD DS), and accessed on-premises.

[Choose an Azure solution for periodic data transfer](#)

Learn how to choose an Azure solution for data transfer when you are transferring data periodically.

[Hybrid file services - Azure Architecture Center](#)

Use Azure File Sync and Azure Files to extend file services hosting capabilities across cloud and on-premises file share resources.

[Show 5 more](#)

Training

Module

[Implement a hybrid file server infrastructure - Training](#)

Implement a hybrid file server infrastructure

Certification

[Microsoft Certified: Azure Data Fundamentals - Certifications](#)

Azure Data Fundamentals validates foundational knowledge of core data concepts and how they are implemented using Microsoft Azure data services.

StorSimple security and data protection

Article • 11/28/2022 • 19 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Security is a major concern for anyone who is adopting a new technology, especially when the technology is used with confidential or proprietary data. As you evaluate different technologies, you must consider increased risks and costs for data protection. Microsoft Azure StorSimple provides both a security and privacy solution for data protection, helping to ensure:

- **Confidentiality** – Only authorized entities can view your data.
- **Integrity** – Only authorized entities can modify or delete your data.

The Microsoft Azure StorSimple solution consists of four main components that interact with each other:

- **StorSimple Device Manager service hosted in Microsoft Azure** – The management service that you use to configure and provision the StorSimple device.
- **StorSimple device** – A physical device installed in your datacenter. All hosts and clients that generate data connect to the StorSimple device, and the device manages the data and moves it to the Azure cloud as appropriate.
- **Clients/hosts connected to the device** – The clients in your infrastructure that connect to the StorSimple device and generate data that needs to be protected.
- **Cloud storage** – The location in the Azure cloud where data is stored.

The following sections describe the StorSimple security features that help protect each of these components and the data stored on them. It also includes a list of questions that you might have about Microsoft Azure StorSimple security, and the corresponding answers.

StorSimple Device Manager service protection

The StorSimple Device Manager service is a management service hosted in Microsoft Azure and used to manage all StorSimple devices that your organization has procured. You can access the StorSimple Device Manager service by using your organizational credentials to log on to the Azure portal through a web browser.

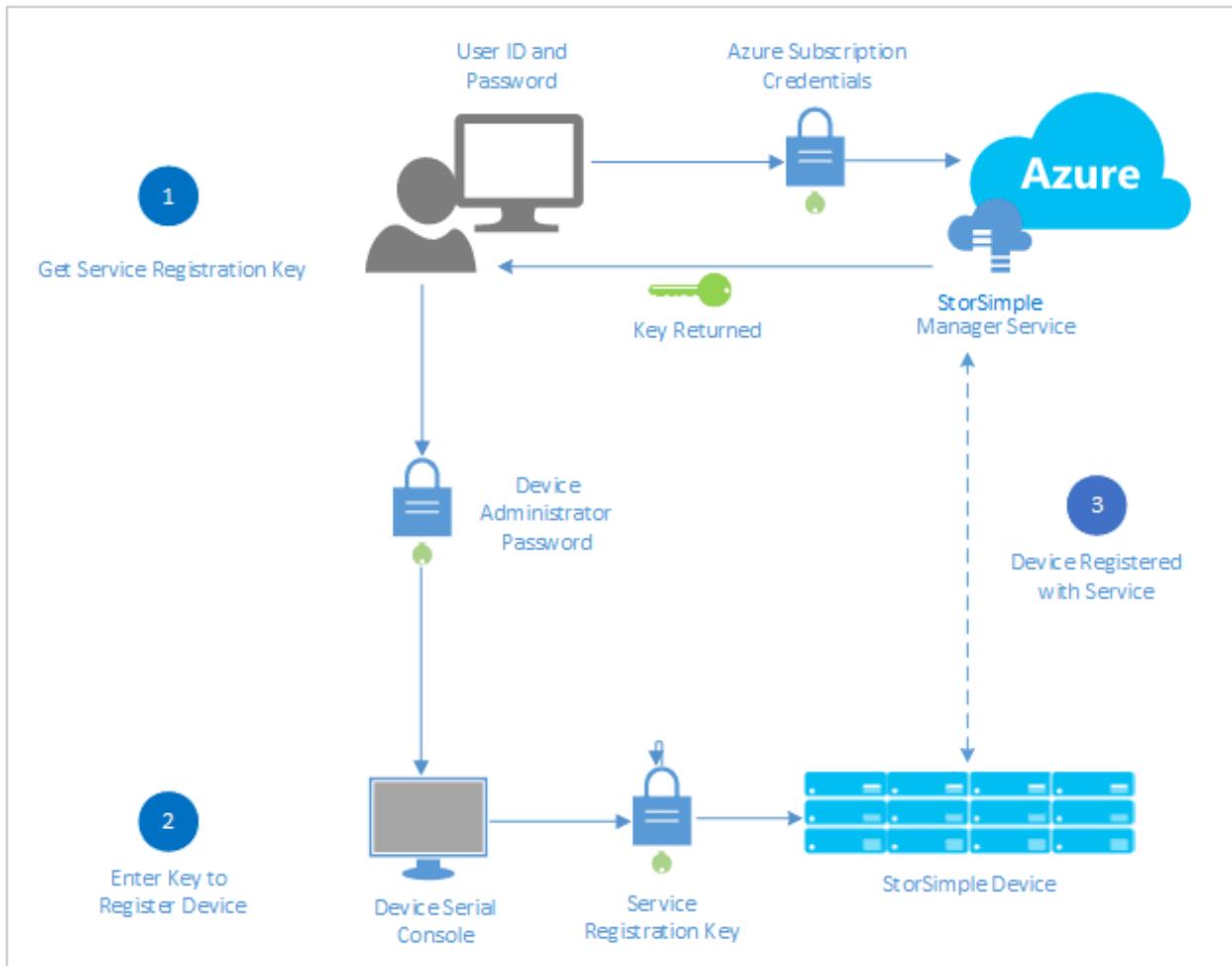
Access to the StorSimple Device Manager service requires that your organization have an Azure subscription that includes StorSimple. Your subscription governs the features that you can access in the Azure portal. If your organization does not have an Azure subscription and you want to learn more about them, see [Sign up for Azure as an organization](#).

Because the StorSimple Device Manager service is hosted in Azure, it is protected by the Azure security features. For more information about the security features provided by Microsoft Azure, go to the [Microsoft Azure Trust Center](#).

StorSimple device protection

The StorSimple device is an on-premises hybrid storage device that contains solid state drives (SSDs) and hard disk drives (HDDs), together with redundant controllers and automatic failover capabilities. The controllers manage storage tiering, placing currently used (or hot) data on local storage (in the StorSimple device or on-premises servers), while moving less frequently used data to the cloud.

Only authorized StorSimple devices are allowed to join the StorSimple Device Manager service that you created in your Azure subscription. To authorize a device, you must register it with the StorSimple Device Manager service by providing the service registration key. The service registration key is a 128-bit random key generated in the Azure portal.



To learn how get a service registration key, go to [Step 2: Get the service registration key](#).

The service registration key is a long key that contains 100+ characters. You can copy the key and save it in a text file in a secure location so that you can use it to authorize additional devices as necessary. If the service registration key is lost after you register your first device, you can generate a new key from the StorSimple Device Manager service. This will not affect the operation of existing devices.

After a device is registered, it uses tokens to communicate with Microsoft Azure. The service registration key is not used after device registration.

ⓘ Note

We recommend that you regenerate the service registration key after every use.

Protect your StorSimple solution via passwords

Passwords are an important aspect of computer security and are used extensively in the StorSimple solution to help ensure that your data is accessible to authorized users only. StorSimple allows you to configure the following passwords:

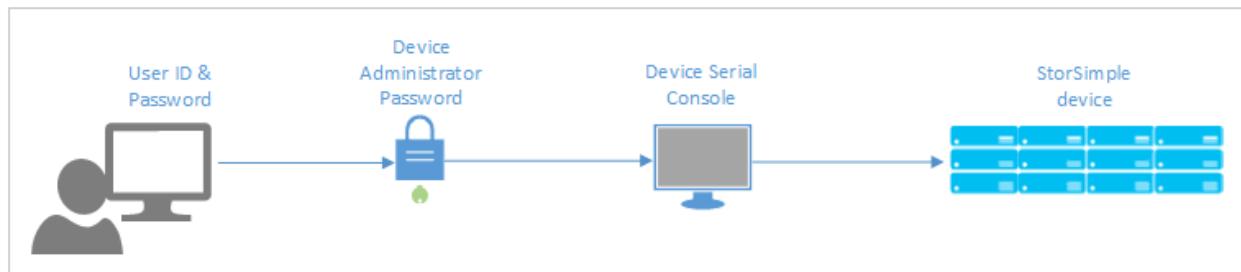
- StorSimple device administrator password
- Challenge Handshake Authentication Protocol (CHAP) initiator and target passwords
- StorSimple Snapshot Manager password

Windows PowerShell for StorSimple and the StorSimple device administrator password

Windows PowerShell for StorSimple is a command-line interface that you can use to manage the StorSimple device. Windows PowerShell for StorSimple has features that allow you to register your device, configure the network interface on your device, install certain types of updates, troubleshoot your device by accessing the support session, and change the device state. You can access Windows PowerShell for StorSimple by connecting to the serial console on the device or by using Windows PowerShell remoting.

PowerShell remoting can be done over HTTPS or HTTP. If remote management over HTTPS is enabled, you will need to download the remote management certificate from the device and install it on the remote client. For more information about PowerShell remoting, go to [Connect remotely to your StorSimple device](#).

After you use Windows PowerShell for StorSimple to connect to the device, you will need to provide the device administrator password to log on to the device.



Keep the following best practices in mind:

- Remote management is turned off by default. You can use the StorSimple Device Manager service to enable it. As a security best practice, remote access should be enabled only during the time period that it is actually needed.
- If you change the password, be sure to notify all remote access users so that they do not experience an unexpected connectivity loss.
- The StorSimple Device Manager service cannot retrieve existing passwords: it can only reset them. We recommend that you store all passwords in a secure place so that you do not have to reset a password if it is forgotten. If you do need to reset a password, be sure to notify all users before you reset it.

You can access the Windows PowerShell interface by using a serial connection to the device. You can also access it remotely by using either HTTP or HTTPS, which provide additional security. HTTPS provides a higher level of security than either a serial or HTTP connection. However, to use HTTPS, you must first install a certificate on the client computer that will access the device. You can download the remote access certificate from the device configuration page in the StorSimple Device Manager service. If the certificate for remote access is lost, you must download a new certificate and propagate it to all clients that are authorized to use remote management.

Challenge Handshake Authentication Protocol (CHAP) initiator and target passwords

CHAP is an authentication scheme used by the StorSimple device to validate the identity of remote clients. The verification is based on a shared password. CHAP can be one-way (unidirectional) or mutual (bidirectional). With one-way CHAP, the target (the StorSimple device) authenticates an initiator (host). Mutual or reverse CHAP requires that the target authenticate the initiator and then the initiator authenticate the target. Your StorSimple can be configured to use either method.

Be aware of the following when you configure CHAP:

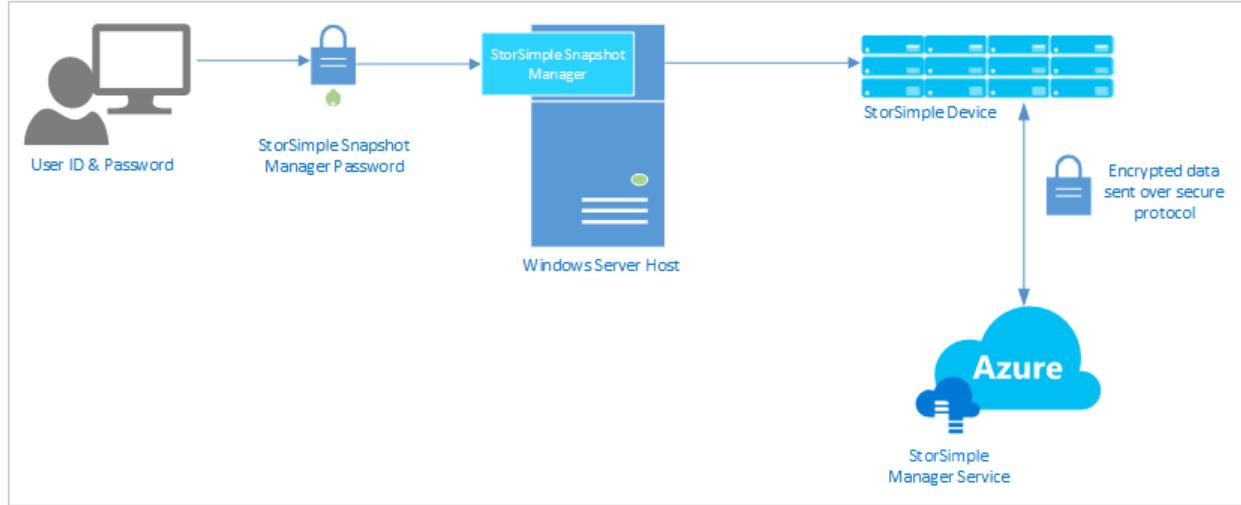
- The CHAP user name must contain fewer than 233 characters.
- The CHAP password must be between 12 and 16 characters. Attempting to use a longer user name or password will result in an authentication failure on the Windows host.
- You cannot use the same password for both the CHAP initiator and the CHAP target.
- After you set the password, it can be changed but it cannot be retrieved. If the password is changed, be sure to notify all remote access users so that they can successfully connect to the StorSimple device.

For more information about CHAP and how to configure it for your StorSimple solution, go to [Configure CHAP for your StorSimple device](#).

StorSimple Snapshot Manager password

StorSimple Snapshot Manager is a Microsoft Management Console (MMC) snap-in that uses volume groups and the Windows Volume Shadow Copy Service to generate application-consistent backups. In addition, you can use StorSimple Snapshot Manager to create backup schedules and clone or restore volumes.

When you configure a device to use StorSimple Snapshot Manager, you will be required to provide the StorSimple Snapshot Manager password. This password is first set in Windows PowerShell for StorSimple during registration. The password can also be set and changed from the StorSimple Device Manager service. This password authenticates the device with StorSimple Snapshot Manager.



The StorSimple Snapshot Manager password must be 14 to 15 characters and must contain 3 or more of a combination of uppercase, lowercase, numeric, and special characters. After you set the StorSimple Snapshot Manager password, it can be changed but it cannot be retrieved. If you change the password, be sure to notify all remote users.

For more information about StorSimple Snapshot Manager, go to [What is StorSimple Snapshot Manager?](#)

Password best practices

We recommend that you use the following guidelines to help ensure that StorSimple passwords are strong and well-protected:

- Change your passwords every three months. Changing the passwords is enforced annually.
- Use strong passwords. For more information, go to [Create stronger passwords and protect them ↗](#).
- Always use different passwords for different access mechanisms; each of the passwords you specify should be unique.
- Do not share passwords with anyone who is not authorized to access the StorSimple device.
- Do not speak about a password in front of others or hint at the format of a password.

- If you suspect that an account or password has been compromised, report the incident to your information security department.
- Treat all passwords as sensitive, confidential information.

StorSimple data protection

This section describes the StorSimple security features that protect data in transit and stored data.

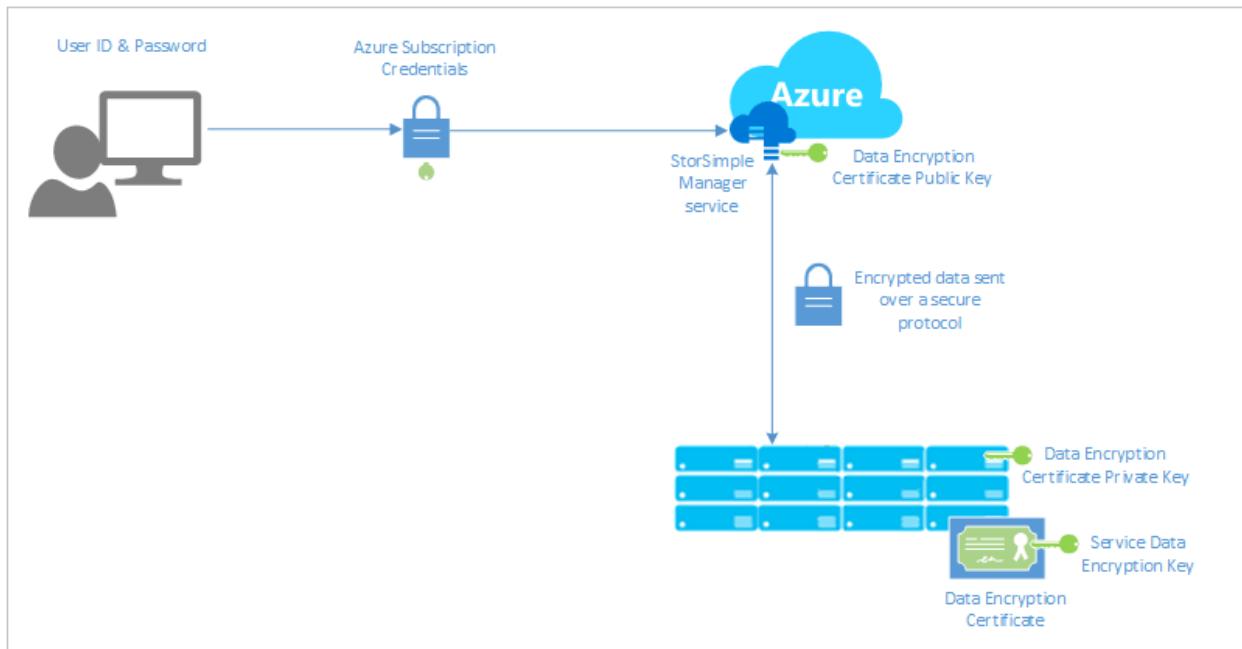
As described in other sections, passwords are used to authorize and authenticate users before they can gain access to your StorSimple solution. Another security consideration is protecting data from unauthorized users while it is being transferred between storage systems and while it is being stored. The following sections describe the data protection features provided with StorSimple.

Note

Deduplication provides additional protection for data stored on the StorSimple device and in Microsoft Azure storage. When data is deduplicated, the data objects are stored separately from the metadata used to map and access them: there is no available storage-level context to reconstruct the data based on volume structure, file system, or file name.

Protect data flowing through the service

The primary purpose of the StorSimple Device Manager service is to manage and configure the StorSimple device. The StorSimple Device Manager service runs in Microsoft Azure. You use the Azure portal to enter device configuration data, and then Microsoft Azure uses the StorSimple Device Manager service to send the data to the device. StorSimple uses a system of asymmetric key pairs to help ensure that a compromise of the Azure service will not result in a compromise of stored information.



The asymmetric key system helps protect the data that flows through the service as follows:

1. A data encryption certificate that uses an asymmetric public and private key pair is generated on the device and is used to protect the data. The keys are generated when the first device is registered.
2. The data encryption certificate keys are exported into a Personal Information Exchange (.pfx) file that is protected by the service data encryption key, which is a strong 128-bit key that is randomly generated by the first device during registration.
3. The public key of the certificate is securely made available to the StorSimple Device Manager service, and the private key remains with the device.
4. Data entering the service is encrypted using the public key and decrypted using the private key stored on the device, ensuring that the Azure service cannot decrypt the data flowing to the device.

The service data encryption key is generated on only the first device registered with the service. All subsequent devices that are registered with the service must use the same service data encryption key.

ⓘ Important

It is very important to make a copy of the service data encryption key and save it in a secure location. A copy of the service data encryption key should be stored in such a way that it can be accessed by an authorized person and can be easily communicated to the device administrator.

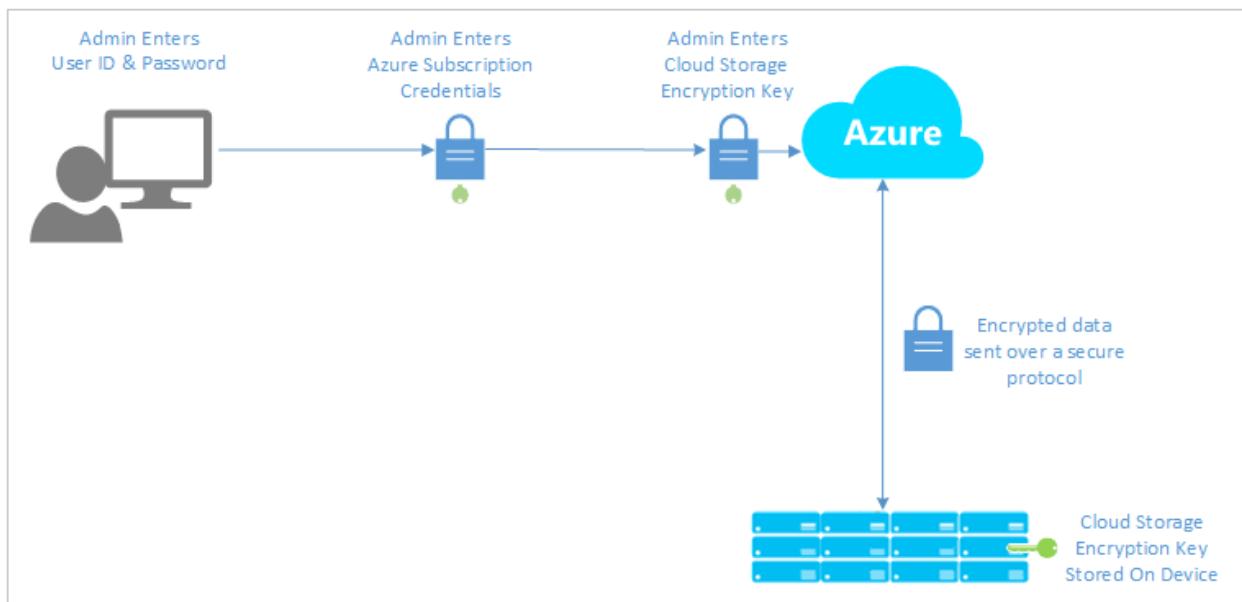
If the service data encryption key is lost, a Microsoft support person can help you to retrieve it provided that you have at least one device in an online state. We recommend that you change the service data encryption key after it is retrieved.

To change the service data encryption key and the corresponding data encryption certificate, follow the steps in [Change the service data encryption key for your StorSimple Device Manager service](#). Changing the encryption keys requires that all devices be updated with the new key. Therefore, we recommend that you change the key when all devices are online. If devices are offline, their keys can be changed at a different time. The devices with out-of-date keys will still be able to run backups, but they will not be able to restore data until the key is updated.

The service data encryption key and the data encryption certificate do not expire. However, we recommend that you change the service data encryption key annually to help prevent key compromise.

Protect data at rest

The StorSimple device manages data by storing it in tiers locally and in the cloud, depending on frequency of use. All host machines that are connected to the device send data to the device, which then moves data to the cloud, as appropriate. Data is transferred from the device to the cloud securely over the Internet. Each device has one iSCSI target that surfaces all shared volumes on that device. All data is encrypted before it is sent to cloud storage.



To help ensure the security and integrity of data moved to the cloud, StorSimple allows you to define cloud storage encryption keys as follows:

- You specify the cloud storage encryption key when you create a volume container. The key cannot be modified or added later.
- All volumes in a volume container share the same encryption key. If you want a different form of encryption for a specific volume, we recommend that you create a new volume container to host that volume.
- When you enter the cloud storage encryption key in the StorSimple Device Manager service, the key is encrypted using the public portion of the service data encryption key and then sent to the device.
- The cloud storage encryption key is not stored anywhere in the service and is known only to the device.
- Specifying a cloud storage encryption key is optional. You can send data that has been encrypted at the host to the device.

Additional security best practices

- Split traffic: isolate your iSCSI SAN from user traffic on a corporate LAN by deploying a totally separated network and using VLANs where physical isolation is not an option. A dedicated network for iSCSI storage will guarantee the safety and performance of your business-critical data. Mixing storage and user traffic over a corporate LAN is not recommended and can increase latency and cause network failures.
- For host-side network security, use network interfaces that support TCP/IP Offload Engine (TOE). TOE reduces CPU load by processing TCP on the network adapter.

Protect data via storage accounts

Each Microsoft Azure subscription can create one or more storage accounts. (A storage account provides a unique namespace for working with data stored in the Azure cloud.) Access to a storage account is controlled by the subscription and access keys associated with that storage account.

When you create a storage account, Microsoft Azure generates two 512-bit storage access keys, one of which is used for authentication when the StorSimple device accesses the storage account. Note that only one of these keys is in use. The other key is held in reserve, allowing you to rotate the keys periodically. To rotate keys, you make the secondary key active, and then delete the primary key. You can then create a new key for use during the next rotation. (For security reasons, many datacenters require key rotation.)

We recommend that you follow these best practices for key rotation:

- You should rotate storage account keys regularly to help ensure that your storage account is not accessed by unauthorized users.
- Periodically, your Azure administrator should change or regenerate the primary or secondary key by using the Storage section of the Azure portal to directly access the storage account.

Protect data via encryption

StorSimple uses the following encryption algorithms to protect data stored in or traveling between the components of your StorSimple solution.

Algorithm	Key length	Protocols/applications/comments
RSA	2048	RSA PKCS 1 v1.5 is used by the Azure portal to encrypt configuration data that is sent to the device: for example, storage account credentials, StorSimple device configuration, and cloud storage encryption keys.
AES	256	AES with CBC is used to encrypt the public portion of the service data encryption key before it is sent to the Azure portal from the StorSimple device. It is also used by the StorSimple device to encrypt data before the data is sent to the cloud storage account.

StorSimple Cloud Appliance security

Keep the following security considerations in mind when you use the StorSimple virtual device:

- The virtual device is secured through your Microsoft Azure subscription. This means that if you are using the virtual device and your Azure subscription is compromised, the data stored on your virtual device is also susceptible.
- The public key of the certificate used to encrypt data stored in Azure StorSimple is securely made available to the Azure classic portal, and the private key is retained with the StorSimple device. On the StorSimple virtual device, both the public and private keys are stored in Azure.
- The virtual device is hosted in the Microsoft Azure datacenter.

Managing personal information

The StorSimple Device Manager for both physical and virtual series collects personal information in the following key instances:

- Alert user settings where email address of users are configured. This information can be viewed and cleared by the administrator. This applies to both the StorSimple 8000 series devices and StorSimple Virtual Arrays.
 - To view and clear the settings for StorSimple 8000 series, follow the steps in [View and manage StorSimple alerts](#)
 - To view and clear the settings for StorSimple Virtual Array, follow the steps in [View and manage StorSimple alerts](#)
- Users who can access the data residing on the shares. A list of users who can access the share data is displayed and can be viewed. This list is also deleted when the shares is deleted. This applies only to StorSimple Virtual Arrays.
 - To view the list of user who can access or to delete a share, follow the steps in [Manage shares on the StorSimple Virtual Array](#)

For more information, review the Microsoft Privacy policy at [Trust Center](#).

Frequently asked questions (FAQ)

The following are some questions and answers about security and Microsoft Azure StorSimple.

Q: My service is compromised. What should be my next steps?

A: You should immediately change the service data encryption key and the storage account keys for the storage account that is being used for tiering data. For instructions, go to:

- [Change the service data encryption key](#)
- [Key rotation of storage accounts](#)

Q: I have a new StorSimple device that is asking for the service registration key. How do I retrieve it?

A: This key was created when you first created the StorSimple Device Manager service. When you use the StorSimple Device Manager service to connect to the device, you can use the service quick start page to view or regenerate the service registration key. Generating a new service registration key will not affect the existing registered devices. For instructions, go to:

- [View or regenerate the service registration key](#)

Q: I lost my service data encryption key. What do I do?

A: Contact Microsoft Support. They can log on to a support session on your device and help you retrieve the key (provided at least one device is online). Immediately after you

obtain the service data encryption key, you should change it to ensure that the new key is known only to you. For instructions, go to:

- [Change the service data encryption key](#)

Q: I authorized a device for a service data encryption key change, but did not start the key change process. What should I do?

A: If the time-out period has expired, you will need to reauthorize the device for the service data encryption key change and start the process again.

Q: I changed the service data encryption key, but I was not able to update the other devices within 4 hours. Do I have to start again?

A: The 4-hour time period is only for initiating the change. After you start the update process on the authorized StorSimple device, the authorization is valid until all devices are updated.

Q: Our StorSimple administrator has left the company. What should I do?

A: Change and reset the passwords that allow access to the StorSimple device, and change the service data encryption key to ensure that the new information is not known to unauthorized personnel. For instructions, go to:

- [Use the StorSimple Device Manager service to change your storsimple passwords](#)
- [Change the service data encryption key](#)
- [Configure CHAP for your StorSimple device](#)

Q: I want to provide the StorSimple Snapshot Manager password to a host that is connecting to the StorSimple device, but the password is not available. What can I do?

A: If you have forgotten the password, you should create a new one. Then, be sure to inform all existing users that the password has been changed and that they should update their clients to use the new password. For instructions, go to:

- [Change the StorSimple Snapshot Manager password](#)
- [Authenticate a device](#)

Q: The certificate for remote access to the Windows PowerShell for StorSimple has been changed on the device. How do I update my remote access clients?

A: You can download the new certificate from the StorSimple Device Manager service, and then provide it to be installed in the certificate store of your remote access clients. For instructions, go to:

- [Import-Certificate cmdlet](#)

Q: Is my data protected if the StorSimple Device Manager service is compromised?

A: Service configuration data is always encrypted with your public key when you view it in a web browser. Because the service doesn't have access to the private key, the service will not be able to see any data. If the StorSimple Device Manager service is compromised, there is no impact, as there are no keys stored in the StorSimple Device Manager service.

Q: If someone gains access to the data encryption certificate, will my data be compromised?

A: Microsoft Azure stores the customer's data encryption key (.pfx file) in an encrypted format. Because the .pfx file is encrypted and the StorSimple service doesn't have the service data encryption key to decrypt the .pfx file, simply getting access to the .pfx file will not expose any secrets.

Q: What happens if a governmental entity asks Microsoft for my data?

A: Because all of the data is encrypted on the service and the private key is kept with the device, the governmental entity must ask the customer for the data.

Next steps

[Deploy your StorSimple device.](#)

Available regions for your StorSimple

Article • 03/26/2023 • 5 minutes to read

⊗ Caution

StorSimple 8000 series will reach its end-of-life in December 2022. Microsoft provides a **dedicated migration service** for StorSimple 8000 series volumes and their backups. It is imperative that you stop any new StorSimple deployments and begin planning your migration now.

The StorSimple Data Manager contains a dedicated migration service for your StorSimple volumes and their backups. If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. [Review the migration guide.](#)

Overview

The Azure datacenters operate in multiple geographies around the world to meet customer's demands of performance, requirements, and preferences regarding data location. An Azure geography is a defined area of the world that contains at least one Azure Region. An Azure region is an area within a geography, containing one or more datacenters.

Choosing an Azure region is very important and the choice of region is influenced by factors such as data residency and sovereignty, service availability, performance, cost, and redundancy. For more information on how to choose a region, go to [Which Azure region is right for me?](#)

For StorSimple solution, the choice of region is specifically determined by the following factors:

- Regions where the StorSimple Device Manager service is available.
- The countries/regions where the StorSimple physical, cloud, or virtual device is available.
- The regions where the storage accounts that store StorSimple data should be located for optimum performance.

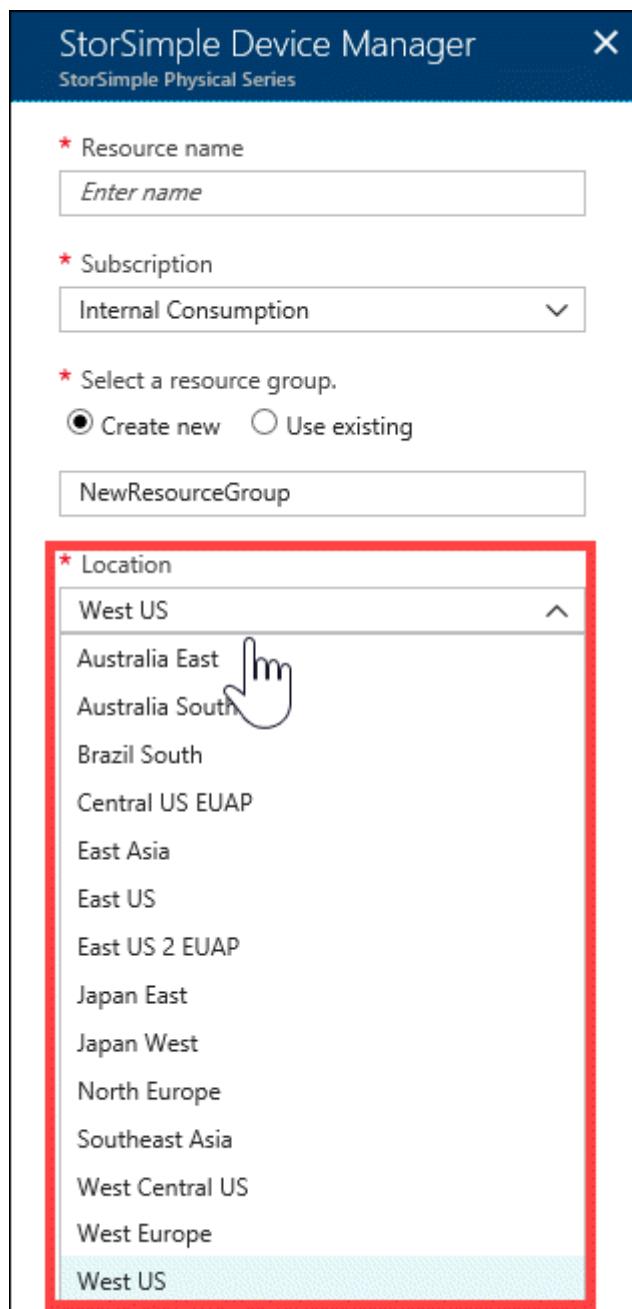
This tutorial describes the region availability for the StorSimple Device Manager service, the on-premises physical and the cloud devices. The information contained in this article is applicable to StorSimple 8000 and 1200 series devices.

Region availability for StorSimple Device Manager service

StorSimple Device Manager service is currently supported in 12 public regions and 2 Azure Government regions.

You define a region or location when you first create the StorSimple Device Manager service. In general, a location closest to the geographical region where the device is deployed is chosen. But the device and the service can also be deployed in different locations.

Here is a list of regions where StorSimple Device Manager service is available for Azure public cloud and can be deployed.



For Azure Government cloud, the StorSimple Device Manager service is available in US Gov Iowa and US Gov Virginia datacenters.

Region availability for data stored in StorSimple

StorSimple data is physically stored in Azure storage accounts and these accounts are available in all the Azure regions. When you create an Azure storage account, the primary location of the storage account is chosen and that determines the region where the data resides.

When you first create a StorSimple Device Manager service and associate a storage account with it, your StorSimple Device Manager service and Azure storage can be in two separate locations. In such a case, you are required to create the StorSimple Device Manager and Azure storage account separately.

In general, choose the nearest region to your service for your storage account. However, the nearest Microsoft Azure region might not actually be the region with the lowest latency. It is the latency that dictates network service performance and hence the performance of the solution. So if you are choosing a storage account in a different region, it is important to know what the latencies are between your service and the region associated with your storage account.

If you are using a StorSimple Cloud Appliance, then we recommend that the service and the associated storage account are in the same region. Storage accounts in a different region may result in poor performance.

Availability of StorSimple device

Depending upon the model, the StorSimple devices can be available in different geographies or countries/regions.

StorSimple physical device (Models 8100/8600)

If using a StorSimple 8100 or 8600 physical device, the device is available in the following countries/regions.

#	Country/Region	#	Country/Region	#	Country/Region	#	Country/Region
1	Australia	16	Hong Kong SAR	31	New Zealand	46	South Africa
2	Austria	17	Hungary	32	Nigeria	47	South Korea

#	Country/Region	#	Country/Region	#	Country/Region	#	Country/Region
3	Bahrain	18	Iceland	33	Norway	48	Spain
4	Belgium	19	India	34	Peru	49	Sri Lanka
5	Brazil	20	Indonesia	35	Philippines	50	Sweden
6	Canada	21	Ireland	36	Poland	51	Switzerland
7	Chile	22	Israel	37	Portugal	52	Taiwan
8	Colombia	23	Italy	38	Puerto Rico	53	Thailand
9	Czech Republic	24	Japan	39	Qatar	54	Türkiye
10	Denmark	25	Kenya	40	Romania	55	Ukraine
11	Egypt	26	Kuwait	41	Russia	56	United Arab Emirates
12	Finland	27	Macao SAR	42	Saudi Arabia	57	United Kingdom
13	France	28	Malaysia	43	Singapore	58	United States
14	Germany	29	Mexico	44	Slovakia	59	Vietnam
15	Greece	30	Netherlands	45	Slovenia	60	Croatia

This list changes as more countries/regions are added. For a most up-to-date list of the geographies, go to the Storage Array Terms Appendix in the [Product terms](#).

Microsoft can ship physical hardware and provide hardware spare parts replacement for StorSimple to the geographies in the preceding list.

Important

Do not place a StorSimple physical device in a region where StorSimple is not supported. Microsoft will not be able to ship any replacement parts to countries/regions where StorSimple is not supported.

StorSimple Cloud Appliance (Models 8010/8020)

If using a StorSimple Cloud Appliance 8010 or 8020, then the device is supported and available in all the regions where the underlying VM is supported. The 8010 uses a *Standard_A3* VM which is supported in all Azure regions.

The 8020 uses premium storage and *Standard_DS3* VM to create a cloud appliance. The 8020 is supported in Azure regions that support Premium Storage and *Standard_DS3* Azure VMs. Use [this list](#) to see if both **Virtual Machines > DS-series** and **Storage > Disk storage** are available in your region.

StorSimple Virtual Array (Model 1200)

If using a 1200 series StorSimple Virtual Array, then the virtual disk image is supported in all Azure regions.

Next steps

- Learn more about the [pricing for various StorSimple models](#).
- Learn more about [managing your StorSimple storage account](#).
- Learn more about how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

StorSimple 8000 series software, high availability, and networking requirements

Article • 08/19/2022 • 16 minutes to read

Overview

Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Welcome to Microsoft Azure StorSimple. This article describes important system requirements and best practices for your StorSimple device and for the storage clients accessing the device. We recommend that you review the information carefully before you deploy your StorSimple system, and then refer back to it as necessary during deployment and subsequent operation.

The system requirements include:

- **Software requirements for storage clients** - describes the supported operating systems and any additional requirements for those operating systems.
- **Networking requirements for the StorSimple device** - provides information about the ports that need to be open in your firewall to allow for iSCSI, cloud, or management traffic.
- **High availability requirements for StorSimple** - describes high availability requirements and best practices for your StorSimple device and host computer.

Software requirements for storage clients

The following software requirements are for the storage clients that access your StorSimple device.

Supported operating systems	Version required	Additional requirements/notes
Windows Server	2008 R2 SP1, 2012, 2012 R2, 2016	<p>StorSimple iSCSI volumes are supported for use on only the following Windows disk types:</p> <ul style="list-style-type: none"> • Simple volume on basic disk • Simple and mirrored volume on dynamic disk <p>Only the software iSCSI initiators present natively in the operating system are supported. Hardware iSCSI initiators are not supported.</p> <p>Windows Server 2012 and 2016 thin provisioning and ODX features are supported if you are using a StorSimple iSCSI volume.</p> <p>StorSimple can create thinly provisioned and fully provisioned volumes. It cannot create partially provisioned volumes.</p> <p>Reformatting a thinly provisioned volume may take a long time. We recommend deleting the volume and then creating a new one instead of reformatting. However, if you still prefer to reformat a volume:</p> <ul style="list-style-type: none"> • Run the following command before the reformat to avoid space reclamation delays: <code>fsutil behavior set disabledeletenotify 1</code> • After the formatting is complete, use the following command to re-enable space reclamation: <code>fsutil behavior set disabledeletenotify 0</code> • Apply the Windows Server 2012 hotfix as described in KB 2878635 to your Windows Server computer. <p>If you are configuring StorSimple Snapshot Manager or StorSimple Adapter for SharePoint, go to Software requirements for optional components.</p> <p>If your Windows Server client is using the SMB protocol to access the StorSimple device, go to Performance tuning for SMB file servers for guidance on increasing parallel processing.</p>
VMware ESX	5.5 and 6.0	Supported with VMware vSphere as iSCSI client. VAAI-block feature is supported with VMware vSphere on StorSimple devices.
Linux RHEL/CentOS	5, 6, and 7	Support for Linux iSCSI clients with open-iSCSI initiator versions 5, 6, and 7.
Linux	SUSE Linux 11	

 **Note**

IBM AIX is currently not supported with StorSimple.

Software requirements for optional components

The following software requirements are for the optional StorSimple components (StorSimple Snapshot Manager and StorSimple Adapter for SharePoint).

Component	Host platform	Additional requirements/notes
StorSimple Snapshot Manager	Windows Server 2008 R2 SP1, 2012, 2012 R2	<p>Use of StorSimple Snapshot Manager on Windows Server is required for backup/restore of mirrored dynamic disks and for any application-consistent backups.</p> <p>StorSimple Snapshot Manager is supported only on Windows Server 2008 R2 SP1 (64-bit), Windows Server 2012 R2, and Windows Server 2012.</p> <ul style="list-style-type: none">• If you are using Window Server 2012, you must install .NET 3.5–4.5 before you install StorSimple Snapshot Manager.• If you are using Windows Server 2008 R2 SP1, you must install Windows Management Framework 3.0 before you install StorSimple Snapshot Manager.
StorSimple Adapter for SharePoint	Windows Server 2008 R2 SP1, 2012, 2012 R2	<ul style="list-style-type: none">• StorSimple Adapter for SharePoint is only supported on SharePoint 2010 and SharePoint 2013.• RBS requires SQL Server Enterprise Edition, version 2008 R2 or 2012.

Networking requirements for your StorSimple device

Your StorSimple device is a locked-down device. However, ports need to be opened in your firewall to allow for iSCSI, cloud, and management traffic. The following table lists the ports that need to be opened in your firewall. In this table, *in* or *inbound* refers to the direction from which incoming client requests access your device. *Out* or *outbound* refers to the direction in which your StorSimple device sends data externally, beyond the deployment: for example, outbound to the Internet.

Port No.^{1,2}	In or out	Port scope	Required	Notes
TCP 80 (HTTP) ³	Out	WAN	No	<ul style="list-style-type: none"> Outbound port is used for Internet access to retrieve updates. The outbound web proxy is user configurable. To allow system updates, this port must also be open for the controller fixed IPs.
TCP 443 (HTTPS) ³	Out	WAN	Yes	<ul style="list-style-type: none"> Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable. To allow system updates, this port must also be open for the controller fixed IPs. This port is also used on both the controllers for garbage collection.
UDP 53 (DNS)	Out	WAN	In some cases; see notes.	This port is required only if you are using an Internet-based DNS server.
UDP 123 (NTP)	Out	WAN	In some cases; see notes.	This port is required only if you are using an Internet-based NTP server.
TCP 9354	Out	WAN	Yes	The outbound port is used by the StorSimple device to communicate with the StorSimple Device Manager service.
3260 (iSCSI)	In	LAN	No	This port is used to access data over iSCSI.
5985	In	LAN	No	<p>Inbound port is used by StorSimple Snapshot Manager to communicate with the StorSimple device.</p> <p>This port is also used when you remotely connect to Windows PowerShell for StorSimple over HTTP.</p>
5986	In	LAN	No	This port is used when you remotely connect to Windows PowerShell for StorSimple over HTTPS.

¹ No inbound ports need to be opened on the public Internet.

² If multiple ports carry a gateway configuration, the outbound routed traffic order will be determined based on the port routing order described in [Port routing](#), below.

³ The controller fixed IPs on your StorSimple device must be routable and able to connect to the Internet directly or via the configured web proxy. The fixed IP addresses

are used for servicing the updates to the device and for garbage collection. If the device controllers cannot connect to the Internet via the fixed IPs, you will not be able to update your StorSimple device and garbage collection will not work properly.

Important

Ensure that the firewall does not modify or decrypt any TLS traffic between the StorSimple device and Azure.

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your StorSimple device and the StorSimple Device Manager service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. This in turn will require the network administrator to monitor and update firewall rules for your StorSimple as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on StorSimple fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

Note

The device (source) IPs should always be set to all the enabled network interfaces. The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for Azure portal

URL pattern	Component/Functionality	Device IPs
<code>https://*.storsimple.windowsazure.com/*</code>	StorSimple Device	Cloud-enabled network interfaces
<code>https://*.accesscontrol.windows.net/*</code>	Manager service	
<code>https://*.servicebus.windows.net/*</code>	Access Control Service	
<code>https://login.windows.net</code>	Azure Service Bus	
	Authentication Service	

URL pattern	Component/Functionality	Device IPs
<code>https://*.backup.windowsazure.com</code>	Device registration	DATA 0 only
<code>https://crl.microsoft.com/pki/*</code> <code>https://www.microsoft.com/pki/*</code>	Certificate revocation	Cloud-enabled network interfaces
<code>https://*.core.windows.net/*</code> <code>https://*.data.microsoft.com</code> <code>http://*.msftncsi.com</code>	Azure storage accounts and monitoring	Cloud-enabled network interfaces
<code>https://*.windowsupdate.microsoft.com</code> <code>https://*.windowsupdate.microsoft.com</code> <code>https://*.update.microsoft.com</code> <code>https://*.update.microsoft.com</code> <code>http://*.windowsupdate.com</code> <code>https://download.microsoft.com</code> <code>http://wustat.windows.com</code> <code>https://ntservicepack.microsoft.com</code>	Microsoft Update servers	Controller fixed IPs only
<code>http://*.deploy.akamaitechnologies.com</code>	Akamai CDN	Controller fixed IPs only
<code>https://*.partners.extranet.microsoft.com/*</code> <code>https://dcupload.microsoft.com/</code> <code>https://*.support.microsoft.com/</code>	Support package	Cloud-enabled network interfaces

URL patterns for Azure Government portal

URL pattern	Component/Functionality	Device IPs
<code>https://*.storSimple.windowsazure.us/*</code> <code>https://*.accesscontrol.usgovcloudapi.net/*</code> <code>https://*.servicebus.usgovcloudapi.net/*</code> <code>https://login.microsoftonline.us</code>	StorSimple Device Manager service Access Control Service Azure Service Bus Authentication Service	Cloud-enabled network interfaces
<code>https://*.backup.windowsazure.us</code>	Device registration	DATA 0 only
<code>https://crl.microsoft.com/pki/*</code> <code>https://www.microsoft.com/pki/*</code>	Certificate revocation	Cloud-enabled network interfaces
<code>https://*.core.usgovcloudapi.net/*</code> <code>https://*.data.microsoft.com</code> <code>http://*.msftncsi.com</code>	Azure storage accounts and monitoring	Cloud-enabled network interfaces

URL pattern	Component/Functionality	Device IPs
<code>https://*.windowsupdate.microsoft.com</code> <code>https://*.windowsupdate.microsoft.com</code> <code>https://*.update.microsoft.com</code> <code>https://*.update.microsoft.com</code> <code>http://*.windowsupdate.com</code> <code>https://download.microsoft.com</code> <code>http://wustat.windows.com</code> <code>https://ntservicepack.microsoft.com</code>	Microsoft Update servers	Controller fixed IPs only
<code>http://*.deploy.akamaitechnologies.com</code>	Akamai CDN	Controller fixed IPs only
<code>https://*.partners.extranet.microsoft.com/*</code> <code>https://dcupload.microsoft.com/</code> <code>https://*.support.microsoft.com/</code>	Support package	Cloud-enabled network interfaces

Routing metric

A routing metric is associated with the interfaces and the gateway that route the data to the specified networks. Routing metric is used by the routing protocol to calculate the best path to a given destination, if it learns multiple paths exist to the same destination. The lower the routing metric, the higher the preference.

In the context of StorSimple, if multiple network interfaces and gateways are configured to channel traffic, the routing metrics will come into play to determine the relative order in which the interfaces will get used. The routing metrics cannot be changed by the user. You can however use the `Get-HcsRoutingTable` cmdlet to print out the routing table (and metrics) on your StorSimple device. More information on `Get-HcsRoutingTable` cmdlet in [Troubleshooting StorSimple deployment](#).

The routing metric algorithm used for Update 2 and later versions can be explained as follows.

- A set of predetermined values have been assigned to network interfaces.
- Consider an example table shown below with values assigned to the various network interfaces when they are cloud-enabled or cloud-disabled but with a configured gateway. Note the values assigned here are example values only.

Network interface	Cloud-enabled	Cloud-disabled with gateway
Data 0	1	-

Network interface	Cloud-enabled	Cloud-disabled with gateway
Data 1	2	20
Data 2	3	30
Data 3	4	40
Data 4	5	50
Data 5	6	60

- The order in which the cloud traffic will be routed through the network interfaces is:

Data 0 > Data 1 > Date 2 > Data 3 > Data 4 > Data 5

This can be explained by the following example.

Consider a StorSimple device with two cloud-enabled network interfaces, Data 0 and Data 5. Data 1 through Data 4 are cloud-disabled but have a configured gateway. The order in which traffic will be routed for this device will be:

Data 0 (1) > Data 5 (6) > Data 1 (20) > Data 2 (30) > Data 3 (40) > Data 4 (50)

The numbers in parentheses indicate the respective routing metrics.

If Data 0 fails, the cloud traffic will get routed through Data 5. Given that a gateway is configured on all other network, if both Data 0 and Data 5 were to fail, the cloud traffic will go through Data 1.

- If a cloud-enabled network interface fails, then are 3 retries with a 30 second delay to connect to the interface. If all the retries fail, the traffic is routed to the next available cloud-enabled interface as determined by the routing table. If all the cloud-enabled network interfaces fail, then the device will fail over to the other controller (no reboot in this case).
- If there is a VIP failure for an iSCSI-enabled network interface, there will be 3 retries with a 2 seconds delay. This behavior has stayed the same from the previous releases. If all the iSCSI network interfaces fail, then a controller failover will occur (accompanied by a reboot).
- An alert is also raised on your StorSimple device when there is a VIP failure. For more information, go to [alert quick reference](#).
- In terms of retries, iSCSI will take precedence over cloud.

Consider the following example: A StorSimple device has two network interfaces enabled, Data 0 and Data 1. Data 0 is cloud-enabled whereas Data 1 is both cloud and iSCSI-enabled. No other network interfaces on this device are enabled for cloud or iSCSI.

If Data 1 fails, given it is the last iSCSI network interface, this will result in a controller failover to Data 1 on the other controller.

Networking best practices

In addition to the above networking requirements, for the optimal performance of your StorSimple solution, please adhere to the following best practices:

- Ensure that your StorSimple device has a dedicated 40 Mbps bandwidth (or more) available at all times. This bandwidth should not be shared (or allocation should be guaranteed through the use of QoS policies) with any other applications.
- Ensure network connectivity to the Internet is available at all times. Sporadic or unreliable Internet connections to the devices, including no Internet connectivity whatsoever, will result in an unsupported configuration.
- Isolate the iSCSI and cloud traffic by having dedicated network interfaces on your device for iSCSI and cloud access. For more information, see how to [modify network interfaces](#) on your StorSimple device.
- Do not use a Link Aggregation Control Protocol (LACP) configuration for your network interfaces. This is an unsupported configuration.

High availability requirements for StorSimple

The hardware platform that is included with the StorSimple solution has availability and reliability features that provide a foundation for a highly available, fault-tolerant storage infrastructure in your datacenter. However, there are requirements and best practices that you should comply with to help ensure the availability of your StorSimple solution. Before you deploy StorSimple, carefully review the following requirements and best practices for the StorSimple device and connected host computers.

For more information about monitoring and maintaining the hardware components of your StorSimple device, go to [Use the StorSimple Device Manager service to monitor hardware components and status](#) and [StorSimple hardware component replacement](#).

High availability requirements and procedures for your StorSimple device

Review the following information carefully to ensure the high availability of your StorSimple device.

PCMs

StorSimple devices include redundant, hot-swappable power and cooling modules (PCMs). Each PCM has enough capacity to provide service for the entire chassis. To ensure high availability, both PCMs must be installed.

- Connect your PCMs to different power sources to provide availability if a power source fails.
- If a PCM fails, request a replacement immediately.
- Remove a failed PCM only when you have the replacement and are ready to install it.
- Do not remove both PCMs concurrently. The PCM module includes the backup battery module. Removing both of the PCMs will result in a shutdown without battery protection, and the device state will not be saved. For more information about the battery, go to [Maintain the backup battery module](#).

Controller modules

StorSimple devices include redundant, hot-swappable controller modules. The controller modules operate in an active/passive manner. At any given time, one controller module is active and is providing service, while the other controller module is passive. The passive controller module is powered on and becomes operational if the active controller module fails or is removed. Each controller module has enough capacity to provide service for the entire chassis. Both controller modules must be installed to ensure high availability.

- Make sure that both controller modules are installed at all times.
- If a controller module fails, request a replacement immediately.
- Remove a failed controller module only when you have the replacement and are ready to install it. Removing a module for extended periods will affect the airflow and hence the cooling of the system.
- Make sure that the network connections to both controller modules are identical, and the connected network interfaces have an identical network configuration.
- If a controller module fails or needs replacement, make sure that the other controller module is in an active state before replacing the failed controller module. To verify that a controller is active, go to [Identify the active controller on your device](#).

- Do not remove both controller modules at the same time. If a controller failover is in progress, do not shut down the standby controller module or remove it from the chassis.
- After a controller failover, wait at least five minutes before removing either controller module.

Network interfaces

StorSimple device controller modules each have four 1 Gigabit and two 10 Gigabit Ethernet network interfaces.

- Make sure that the network connections to both controller modules are identical, and the network interfaces that the controller module interfaces are connected to have an identical network configuration.
- When possible, deploy network connections across different switches to ensure service availability in the event of a network device failure.
- When unplugging the only or the last remaining iSCSI-enabled interface (with IPs assigned), disable the interface first and then unplug the cables. If the interface is unplugged first, then it will cause the active controller to fail over to the passive controller. If the passive controller also has its corresponding interfaces unplugged, then both the controllers will reboot multiple times before settling on one controller.
- Connect at least two DATA interfaces to the network from each controller module.
- If you have enabled the two 10 GbE interfaces, deploy those across different switches.
- When possible, use MPIO on servers to ensure that the servers can tolerate a link, network, or interface failure.

For more information about networking your device for high availability and performance, go to [Install your StorSimple 8100 device](#) or [Install your StorSimple 8600 device](#).

SSDs and HDDs

StorSimple devices include solid state disks (SSDs) and hard disk drives (HDDs) that are protected using mirrored spaces. Use of mirrored spaces ensures that the device is able to tolerate the failure of one or more SSDs or HDDs.

- Make sure that all SSD and HDD modules are installed.
- If an SSD or HDD fails, request a replacement immediately.

- If an SSD or HDD fails or requires replacement, make sure that you remove only the SSD or HDD that requires replacement.
- Do not remove more than one SSD or HDD from the system at any point in time. A failure of 2 or more disks of certain type (HDD, SSD) or consecutive failure within a short time frame may result in system malfunction and potential data loss. If this occurs, [contact Microsoft Support](#) for assistance.
- During replacement, monitor the **Shared components** in the **Hardware health** blade for the drives in the SSDs and HDDs. A green check status indicates that the disks are healthy or OK, whereas a red exclamation point indicates a failed SSD or HDD.
- We recommend that you configure cloud snapshots for all volumes that you need to protect in case of a system failure.

EBOD enclosure

StorSimple device model 8600 includes an Extended Bunch of Disks (EBOD) enclosure in addition to the primary enclosure. An EBOD contains EBOD controllers and hard disk drives (HDDs) that are protected using mirrored spaces. Use of mirrored spaces ensures that the device is able to tolerate the failure of one or more HDDs. The EBOD enclosure is connected to the primary enclosure through redundant SAS cables.

- Make sure that both EBOD enclosure controller modules, both SAS cables, and all the hard disk drives are installed at all times.
- If an EBOD enclosure controller module fails, request a replacement immediately.
- If an EBOD enclosure controller module fails, make sure that the other controller module is active before you replace the failed module. To verify that a controller is active, go to [Identify the active controller on your device](#).
- During an EBOD controller module replacement, continuously monitor the status of the component in the StorSimple Device Manager service by accessing **Monitor > Hardware health**.
- If an SAS cable fails or requires replacement (Microsoft Support should be involved to make such a determination), make sure that you remove only the SAS cable that requires replacement.
- Do not concurrently remove both SAS cables from the system at any point in time.

High availability recommendations for your host computers

Carefully review these best practices to ensure the high availability of hosts connected to your StorSimple device.

- Configure StorSimple with [two-node file server cluster configurations](#). By removing single points of failure and building in redundancy on the host side, the entire solution becomes highly available.
- Use Continuously available (CA) shares available with Windows Server 2012 (SMB 3.0) for high availability during failover of the storage controllers. For additional information for configuring file server clusters and Continuously Available shares with Windows Server 2012.

Next steps

- [Learn about StorSimple system limits](#).
- [Learn how to deploy your StorSimple solution](#).

Technical specifications and compliance for the StorSimple device

Article • 08/19/2022 • 6 minutes to read

Overview

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The hardware components of your Microsoft Azure StorSimple device adhere to the technical specifications and regulatory standards outlined in this article. The technical specifications describe the Power and Cooling Modules (PCMs), disk drives, storage capacity, and enclosures. The compliance information covers such things as international standards, safety and emissions, and cabling.

Power and Cooling Module specifications

The StorSimple device has two 100-240 V dual fan, SBB-compliant Power Cooling Modules (PCMs). This provides a redundant power configuration. If a PCM fails, the device continues to operate normally on the other PCM until the failed module is replaced.

The EBOD enclosure uses a 580 W PCM, and primary enclosure uses a 764 W PCM. The following tables list the technical specifications associated with the PCMs.

Specification	580 W PCM (EBOD)	764 W PCM (Primary)
Maximum output power	580 W	764
Frequency	50/60 Hz	50/60 Hz

Specification	580 W PCM (EBOD)	764 W PCM (Primary)
Voltage range selection	Auto ranging: 90 – 264 V AC, 47/63 Hz	Auto ranging: 90- 264 V AC, 47/63 Hz
Maximum inrush current	20 A	20 A
Power factor correction	>95% nominal input voltage	>95% nominal input voltage
Harmonics	Meets EN61000-3-2	Meets EN61000-3-2
Output	5V Standby voltage @ 2.0 A	5V Standby voltage @ 2.7 A
+5V @ 42 A	+5V @ 40 A	
+12V @ 38 A	+12V @ 38 A	
Hot pluggable	Yes	Yes
Switches and LEDs	AC ON/OFF switch and four status indicator LEDs	AC ON/OFF switch and six status indicator LEDs
Enclosure cooling	Axial cooling fans with variable fan speed control	Axial cooling fans with variable fan speed control

Power consumption statistics

The following table lists the typical power consumption data (actual values may vary from the published) for the various models of StorSimple device.

Conditions	240 V AC	240 V AC	240 V AC	110 V AC	110 V AC	110 V AC
Fans slow, drives idle	1.45 A	0.31 kW	1057.76 BTU/hr	3.19 A	0.34 kW	1160.13 BTU/hr
Fans slow, drives accessing	1.54 A	0.33 kW	1126.01 BTU/hr	3.27 A	0.36 kW	1228.37 BTU/hr
Fans fast, drives idle, two PSUs powered	2.14 A	0.49 kW	1671.95 BTU/hr	4.99 A	0.54 kW	1842.56 BTU/hr
Fans fast, drives idle, one PSU powered one idle	2.05 A	0.48 kW	1637.83 BTU/hr	4.58 A	0.50 kW	1706.07 BTU/hr
Fans fast, drives accessing, two PSUs powered	2.26 A	0.51 kW	1740.19 BTU/hr	4.95 A	0.54 kW	1842.56 BTU/hr

Conditions	240 V AC	240 V AC	240 V AC	110 V AC	110 V AC	110 V AC
Fans fast, drives accessing, one PSU powered one idle	2.14 A	0.49 kW	1671.95 BTU/hr	4.81 A	0.53 kW	1808.44 BTU/hr

Disk drive specifications

Your StorSimple device supports up to 12 3.5-inch form factor Serial Attached SCSI (SAS) disk drives. The actual drives can be a mix of solid-state drives (SSDs) or hard disk drives (HDDs), depending on the product configuration. The 12 disk drive slots are located in a 3 by 4 configuration in front of the enclosure. The EBOD enclosure allows for additional storage for another 12 disk drives. These are always HDDs.

Storage specifications

The StorSimple devices have a mix of hard disk drives and solid-state drives for both the 8100 and 8600. The total usable capacity for the 8100 and 8600 are roughly 15 TB and 38 TB respectively. The following table documents the details of SSD, HDD, and cloud capacity in the context of the StorSimple solution capacity.

Device model / Capacity	8100	8600
Number of hard disk drives (HDDs)	8	19
Number of solid-state drives (SSDs)	4	5
Single HDD capacity	4 TB	4 TB
Single SSD capacity	400 GB	800 GB
Spare capacity	4 TB	4 TB
Usable HDD capacity	14 TB	36 TB
Usable SSD capacity	800 GB	2 TB
Total usable capacity*	~ 15 TB	~ 38 TB
Maximum solution capacity (including cloud)	200 TB	500 TB

* - *The total usable capacity includes the capacity available for data, metadata, and buffers. You can provision locally pinned volumes up to 8.5 TB on the 8100 device or up to 22.5 TB on the larger 8600 device. For more information, go to [StorSimple locally pinned volumes](#).*

Enclosure dimensions and weight specifications

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The following table lists the dimensions of the enclosure in millimeters and inches.

Enclosure	Millimeters	Inches
Height	87.9	3.46
Width across mounting flange	483	19.02
Width across body of enclosure	443	17.44
Depth from front mounting flange to extremity of enclosure body	577	22.72
Depth from operations panel to furthest extremity of enclosure	630.5	24.82
Depth from mounting flange to furthest extremity of enclosure	603	23.74

Enclosure weight

Depending on the configuration, a fully loaded primary enclosure can weigh from 21 to 33 kgs and requires two persons to handle it.

Enclosure	Weight
Maximum weight (depends on the configuration)	30 kg – 33 kg
Empty (no drives fitted)	21 – 23 kg

Enclosure environment specifications

This section lists the specifications related to the enclosure environment. The temperature, humidity, altitude, shock, vibration, orientation, safety, and Electromagnetic Compatibility (EMC) are included in this category.

Temperature and humidity

Enclosure	Ambient temperature range	Ambient relative humidity	Maximum wet bulb

Enclosure	Ambient temperature range	Ambient relative humidity	Maximum wet bulb
Operational	5°C - 35°C(41°F - 95°F)	20% - 80% non-condensing-	28°C (82°F)
Non-operational	-40°C - 70°C(40°F - 158°F)	5% - 100% non-condensing	29°C (84°F)

Airflow, altitude, shock, vibration, orientation, safety, and EMC

Enclosure	Operational specifications
Airflow	System airflow is front to rear. System must be operated with a low-pressure, rear-exhaust installation. Back pressure created by rack doors and obstacles should not exceed 5 pascals (0.5 mm water gauge).
Altitude, operational	-30 meters to 3045 meters (-100 feet to 10,000 feet) with maximum operating temperature de-rated by 5°C above 7000 feet.
Altitude, non-operational	-305 meters to 12,192 meters (-1,000 feet to 40,000 feet)
Shock, operational	5g 10 ms ½ sine
Shock, non-operational	30g 10 ms ½ sine
Vibration, operational	0.21g RMS 5-500 Hz random
Vibration, non-operational	1.04g RMS 2-200 Hz random
Vibration, relocation	3g 2-200 Hz sine
Orientation and mounting	19" rack mount (2 EIA units)
Rack rails	To fit minimum 700 mm (31.50 inches) depth racks compliant with IEC 297

Enclosure	Operational specifications
Safety and approvals	CE and UL EN 61000-3, IEC 61000-3, UL 61000-3
EMC	EN55022 (CISPR - A), FCC A

International standards compliance

Your Microsoft Azure StorSimple device complies with the following international standards:

- CE - EN 60950 - 1
- CB report to IEC 60950 - 1
- UL and cUL to UL 60950 - 1

Safety compliance

Your Microsoft Azure StorSimple device meets the following safety ratings:

- System product type approval: UL, cUL, CE
- Safety compliance: UL 60950, IEC 60950, EN 60950

EMC compliance

Your Microsoft Azure StorSimple device meets the following EMC ratings.

Emissions

The device is EMC-compliant for conducted and radiated emissions levels.

- Conducted emissions limit levels: CFR 47 Part 15B Class A EN55022 Class A CISPR Class A
- Radiated emissions limit levels: CFR 47 Part 15B Class A EN55022 Class A CISPR Class A

Harmonics and flicker

The device complies with EN61000-3-2/3.

Immunity limit levels

The device complies with EN55024.

AC power cord compliance

The plug and the complete power cord assembly must meet the standards appropriate for the country/region in which the device is being used, and they must have safety approvals that are acceptable in that country/region. The following tables list standards for the USA and Europe.

AC power cords - USA (must be NRTL listed)

Component	Specification
Cord type	SV or SVT, 18 AWG minimum, 3 conductor, 2.0 meters maximum length
Plug	NEMA 5-15P grounding-type attachment plug rated 120 V, 10 A; or IEC 320 C14, 250 V, 10 A
Socket	IEC 320 C-13, 250 V, 10 A

AC power cords - Europe

Component	Specification
Cord type	Harmonized, H05-VVF-3G1.0
Socket	IEC 320 C-13, 250 V, 10 A

Supported network cables

For the 10 GbE network interfaces, DATA 2 and DATA 3, refer to the [list of supported network cables and modules](#).

Next steps

You are now ready to deploy a StorSimple device in your datacenter. For more information, see [Deploying your on-premises device](#).

What are StorSimple 8000 series system limits?

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

StorSimple provides scalable and flexible storage for your datacenter. However, there are some limits that you should keep in mind as you plan, deploy, and operate your StorSimple solution. The following table describes these limits and provides some recommendations so that you can get the most out of your StorSimple solution.

Limit identifier	Limit	Comments
Maximum number of storage account credentials	64	
Maximum number of volume containers	64	
Maximum number of volumes	255	
Maximum number of locally pinned volumes	32	

Limit identifier	Limit	Comments
Maximum number of schedules per bandwidth template	168	A schedule for every hour, every day of the week (24*7).
Maximum size of a tiered volume on physical devices	64 TB for 8100 and 8600	8100 and 8600 are physical devices.
Maximum size of a tiered volume on virtual devices in Azure	30 TB for 8010 64 TB for 8020	8010 and 8020 are virtual devices in Azure that use Standard Storage and Premium Storage respectively.
Maximum size of a locally pinned volume on physical devices	8.5 TB for 8100 22.5 TB for 8600	8100 and 8600 are physical devices.
Maximum number of iSCSI connections	512	
Maximum number of iSCSI connections from initiators	512	
Maximum number of access control records per device	64	
Maximum number of volumes per backup policy	20	
Maximum number of backups retained per schedule (in a backup policy)	64	

Limit identifier	Limit	Comments
Maximum number of schedules per backup policy	10	
Maximum number of snapshots of any type that can be retained per volume	256	This number includes local snapshots and cloud snapshots.
Maximum number of snapshots that can be present in any device	10,000	
Maximum number of volumes that can be processed in parallel for backup, restore, or clone	16	<ul style="list-style-type: none"> If there are more than 16 volumes, they are processed sequentially as processing slots become available. New backups of a cloned or a restored tiered volume cannot occur until the operation is finished. However, for a local volume, backups are allowed after the volume is online.
Restore and clone recover time for tiered volumes	< 2 minutes	<ul style="list-style-type: none"> The volume is made available within 2 minutes of restore or clone operation, regardless of the volume size. The volume performance may initially be slower than normal as most of the data and metadata still resides in the cloud. Performance may increase as data flows from the cloud to the StorSimple device. The total time to download metadata depends on the allocated volume size. Metadata is automatically brought into the device in the background at the rate of 5 minutes per TB of allocated volume data. This rate may be affected by Internet bandwidth to the cloud. The restore or clone operation is complete when all the metadata is on the device. Backup operations cannot be performed until the restore or clone operation is fully complete.

Limit identifier	Limit	Comments
Restore recover time for locally pinned volumes	< 2 minutes	<ul style="list-style-type: none"> The volume is made available within 2 minutes of the restore operation, regardless of the volume size. The volume performance may initially be slower than normal as most of the data and metadata still resides in the cloud. Performance may increase as data flows from the cloud to the StorSimple device. The total time to download metadata depends on the allocated volume size. Metadata is automatically brought into the device in the background at the rate of 5 minutes per TB of allocated volume data. This rate may be affected by Internet bandwidth to the cloud. Unlike tiered volumes, for locally pinned volumes, the volume data is also downloaded locally on the device. The restore operation is complete when all the volume data has been brought to the device. The restore operations may be long. The total time to complete the restore depends on the size of the provisioned local volume, your Internet bandwidth, and the existing data on the device. Backup operations on the locally pinned volume are allowed while the restore operation is in progress.
Processing rate for cloud snapshots	15 minutes/TB	<ul style="list-style-type: none"> Minimum time to make the cloud snapshot ready for upload, per TB of allocated volume data in backup. Total cloud snapshot time is calculated by adding this time to the snapshot upload time, which is affected by the Internet bandwidth to cloud.
Maximum client read/write throughput (when served from the SSD tier)*	920/720 MB/s with a single 10 GbE network interface	Up to 2x with MPIO and two network interfaces.
Maximum client read/write throughput (when served from the HDD tier)*	120/250 MB/s	

Limit identifier	Limit	Comments
Maximum client read/write throughput (when served from the cloud tier)* for Update 3 and later**	40/60 MB/s for tiered volumes 60/80 MB/s for tiered volumes with archival option selected during volume creation	Read throughput depends on clients generating and maintaining sufficient I/O queue depth. Speed achieved depends on the speed of the underlying storage account used.

* Maximum throughput per I/O type was measured with 100 percent read and 100 percent write scenarios. Actual throughput may be lower and depends on I/O mix and network conditions.

** Performance numbers prior to Update 3 may be lower.

Next steps

Review the [StorSimple system requirements](#).

Safely install and operate your StorSimple device

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.



READ SAFETY AND HEALTH INFORMATION

Read all the safety and health information in this article that applies to your Microsoft Azure StorSimple device. Keep all the printed guides shipped with your StorSimple device for future reference. Failure to follow instructions and properly set up, use, and care for this product can increase the risk of serious injury or death, or damage to the device or devices. A [downloadable version of this guide](#) is also available.

Safety icon conventions

Here are the icons that you will find when you review the safety precautions to be observed when setting up and running your Microsoft Azure StorSimple device.

Icon	Description
DANGER!	Indicates a hazardous situation that, if not avoided, will result in death or serious injury. This signal word is to be limited to the most extreme situations.
WARNING!	Indicates a hazardous situation that, if not avoided, could result in death or serious injury.
CAUTION!	Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.
NOTICE:	Indicates information considered important, but not hazard-related.

Icon	Description
 Electrical Shock Hazard	High voltage Shock Hazard
 Heavy Weight	
 No User Serviceable Parts	Do not access unless properly trained.
 Read All Instructions First	
 Tip Hazard	

Handling precautions



To reduce the risk of injury:

- A fully configured enclosure can weigh up to 32 kg (70 lbs); do not try to lift it by yourself.
- Before moving the enclosure, always ensure that two people are available to handle the weight. Be aware that one person attempting to lift this weight can sustain injuries.
- Do not lift the enclosure by the handles on the Power and Cooling Modules (PCMs) located at the rear of the unit. These are not designed to take the weight.

Connection precautions



To reduce the likelihood of injury, electrical shock, or death:

- When powered by multiple AC sources, disconnect all supply power for complete isolation.

- Permanently unplug the unit before you move it or if you think it has become damaged in any way.
- Provide a safe electrical earth connection to the power supply cords. Verify that the grounding of the enclosure meets the national and local requirements before applying power.
- Ensure that the power connection is always disconnected prior to the removal of a PCM from the enclosure.
- Given that the plug on the power supply cord is the main disconnect device, ensure that the socket outlets are located near the equipment and are easily accessible.



WARNING!

To reduce the likelihood of overheating or fire from the electrical connections:

- Provide a suitable power source with electrical overload protection to meet the requirements detailed in the technical specification.
- Do not use bifurcated power cords ("Y" leads).
- To comply with applicable safety, emission, and thermal requirements, no covers should be removed and all bays must be populated with plug-in modules or drive blanks.
- Ensure that the equipment is used in a manner specified by the manufacturer. If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.



NOTICE:

For the proper operation of your equipment and to prevent product damage:

- The RJ45 ports at the back of the device are for an Ethernet connection only. These must not be connected to a telecommunications network.
- Be sure to install the device in a rack that can accommodate a front-to-back cooling design.
- All plug-in modules and blank plates are part of the system enclosure. These must only be removed when a replacement can be immediately added. The system must not be run without all modules or blanks in place.

Rack system precautions

The following safety requirements must be considered when you mount the device in a rack cabinet.



WARNING!

To reduce the likelihood of injury from a tip over:

- The rack design should support the total weight of the installed enclosures and should incorporate stabilizing features suitable to prevent the rack from tipping or being pushed over during installation or normal use.
- When loading a rack, fill the rack from the bottom up and empty from the top down.
- Do not slide more than one enclosure out of the rack at a time to avoid the danger of the rack toppling over.



WARNING!

To reduce the likelihood of injury, electrical shock, or death:

- The rack should have a safe electrical distribution system. It must provide over-current protection for the enclosure and must not be overloaded by the total number of enclosures installed. The electrical power consumption rating shown on the nameplate should be observed.
- The electrical distribution system must provide a reliable ground for each enclosure in the rack.
- The design of the electrical distribution system must take into consideration the total ground leakage current from all power supplies in all enclosures. Note that each power supply in each enclosure has a ground leakage current of 1.0 mA maximum at 60 Hz, 264 volts. The rack may require labeling with "HIGH LEAKAGE CURRENT. Ground (earth) connection is essential before connecting a supply."
- The rack, when configured with the enclosures, must meet the safety requirements of UL 60950-1 and IEC 60950-1/EN 60950-1.



NOTICE:

For the proper cooling of your rack system:

- Ensure that the rack design takes into consideration the maximum enclosure operating ambient temperature of 35 degrees Celsius (95 degrees Fahrenheit). Keep the room where the rack system is cool and check that there is adequate airflow from the AC vent in the datacenter.
- The system is operated with low-pressure, rear-exhaust installation (back pressure created by rack doors and obstacles not to exceed 5 Pascal [0.5 mm water gauge]).

Power Cooling Module (PCM) precautions

The device is designed to operate with two PCMs. Each of the PCMs has a power supply and a dual-axis fan. During a critical condition, the system allows for a failure of one power supply while continuing normal operations. Two PCMs (and hence power supplies) must always be installed. A single PCM does not provide redundant power. Therefore, the failure of even one PCM can result in downtime or possible data loss.



WARNING!

To reduce the likelihood of injury, electrical shock, or death:

- Do not remove the covers from the PCM. There is a danger of electric shock inside. To return the PCM and obtain a replacement, [contact Microsoft Support](#).



NOTICE:

For the proper operation of your equipment and to prevent product damage:

- You must replace the failed PCM within 24 hours. After a PCM is removed for replacement, the replacement must be completed within 10 minutes after removal.
- Do not remove a PCM unless a replacement can be installed immediately. The enclosure must not be operated without all modules in place.

Electrostatic discharge (ESD) precautions



NOTICE:

Observe the following ESD-related precautions.

- Ensure that you have installed and checked a suitable antistatic wrist or ankle strap.
- Observe all conventional ESD precautions when handling modules and components.
- Avoid contact with backplane components and module connectors.
- ESD damage is not covered by warranty.

Battery disposal precautions

The power supply uses a special battery to protect the contents of memory during temporary, short-term power outages. The battery is seated in the PCM. Keep the following information in mind about the battery.

WARNING!

To reduce the risk of shorts, fire, explosion, injury, or death:

- Dispose of used batteries in accordance with national/regional regulations.
- Do not disassemble, crush, or heat above 60 degrees Celsius (140 degrees Fahrenheit) or incinerate. Replace the PCM battery with a supplied battery only. Use of another battery may present a risk of fire or explosion.
- Use protective end caps on the batteries if these are removed from the power supply.



NOTICE:

When shipping or otherwise transporting the batteries by air, follow the IATA Lithium Battery Guidance document available at

[https://www.iata.org/whatwedo/cargo/dgr/Pages/lithium-batteries.aspx ↗](https://www.iata.org/whatwedo/cargo/dgr/Pages/lithium-batteries.aspx)

After you have reviewed these safety notices, the next steps are to unpack, rack and cable your device.

Next steps

- For an 8100 device, go to [Install your StorSimple 8100 device](#).
- For an 8600 device, go to [Install your StorSimple 8600 device](#).

Unpack, rack-mount, and cable your StorSimple 8100 device

Article • 03/23/2020 • 10 minutes to read

⊗ Caution

StorSimple 8000 series will reach its end-of-life in December 2022. Microsoft provides a **dedicated migration service** for StorSimple 8000 series volumes and their backups. It is imperative that you stop any new StorSimple deployments and begin planning your migration now.

The StorSimple Data Manager contains a dedicated migration service for your StorSimple volumes and their backups. If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. [Review the migration guide.](#)

Overview

Your Microsoft Azure StorSimple 8100 is a single enclosure, rack-mounted device. This tutorial explains how to unpack, rack-mount, and cable the StorSimple 8100 device hardware before you configure and deploy the StorSimple device.

Unpack your StorSimple 8100 device

The following steps provide clear, detailed instructions about how to unpack your StorSimple 8100 storage device. This device is shipped in a single box.

Prepare to unpack your device

Before you unpack your device, review the following information.

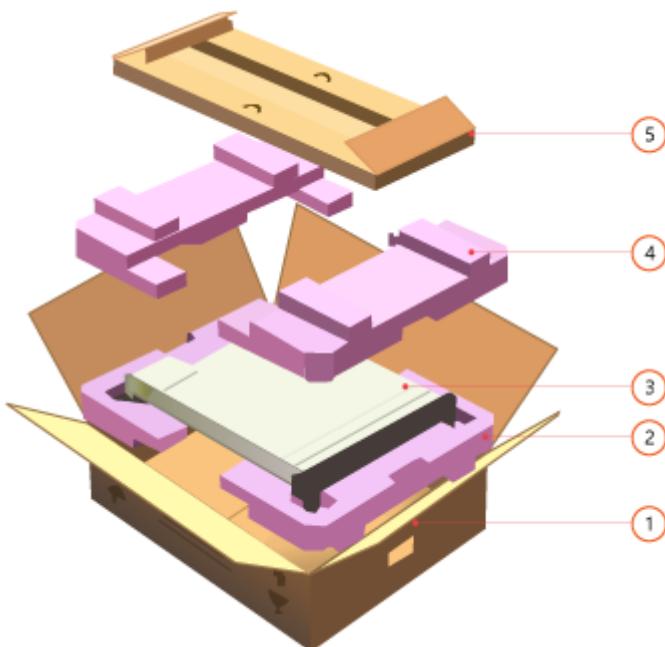


1. Make sure that you have two people available to manage the weight of the enclosure if you are handling it manually. A fully configured enclosure can weigh up to 32 kg (70 lbs.).
2. Place the box on a flat, level surface.

Next, complete the following steps to unpack your device.

To unpack your device

1. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, do not open the box. Please [contact Microsoft Support](#) to help you assess whether the device is in good working order.
2. Unpack the box. The following image shows the unpacked view of your StorSimple device.



Unpacked view of your storage device

Label	Description
1	Packing box
2	Bottom foam
3	Device
4	Top foam
5	Accessory box

3. After unpacking the box, make sure that you have:

- 1 single enclosure device
- 2 power cords

- 1 crossover Ethernet cable
- 2 serial console cables
- 1 serial-USB converter for serial access
- 1 tamper-proof T10 screwdriver
- 4 QSFP-to-SFP+ adapters for use with 10 GbE network interfaces
- 1 rack-mount kit (2 side rails with mounting hardware)
- Getting Started documentation

If you did not receive any of the items listed above, [contact Microsoft Support](#).

The next step is to rack-mount your device.

Rack-mount your StorSimple 8100 device

Follow the next steps to install your StorSimple 8100 storage device in a standard 19-inch rack with front and rear posts . The StorSimple 8100 device has a single primary enclosure.

The installation consists of multiple steps, each of which is discussed in the following procedures.

Important

StorSimple devices must be rack-mounted for proper operation.

Prepare the site

The device must be installed in a standard 19-inch rack that has both front and rear posts. Use the following procedure to prepare for rack installation.

To prepare the site for rack installation

1. Make sure that the device rests safely on a flat, stable, and level work surface (or similar).
2. Verify that the site where you intend to set up has standard AC power from an independent source or a rack power distribution unit (PDU) with an uninterruptible

power supply (UPS).

3. Make sure that one 2U slot is available on the rack in which you intend to mount the device.



Make sure that you have two people available to manage the weight if you are handling the device setup manually. A fully configured enclosure can weigh up to 32 kg (70 lbs.).

Rack prerequisites

The 8100 enclosure is designed for installation in a standard 19-inch rack cabinet with:

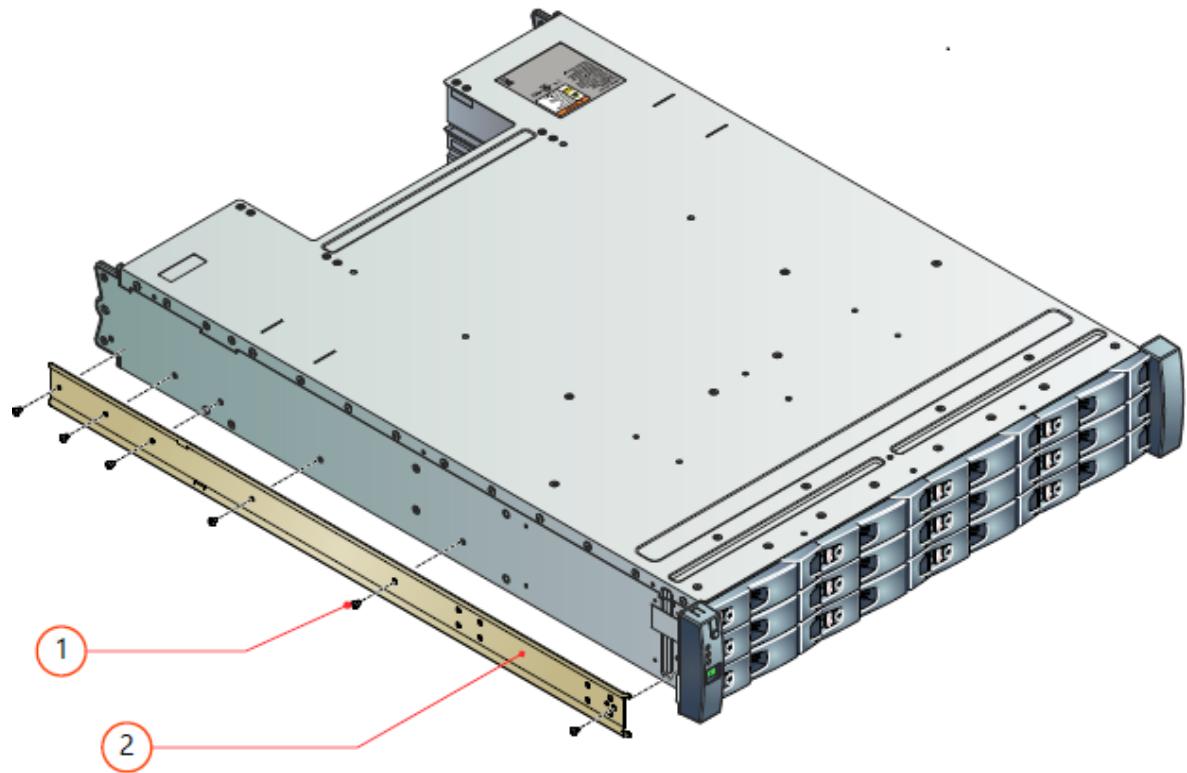
- Minimum depth of 27.84 inches from rack post to post.
- Maximum weight of 32 kg for the device
- Maximum back pressure of 5 Pascal (0.5 mm water gauge).

Rack-mounting rail kit

A set of mounting rails is provided for use with the 19-inch rack cabinet. The rails have been tested to handle the maximum enclosure weight. These rails will also allow installation of multiple enclosures without any loss of space within the rack.

To install the device on the rails

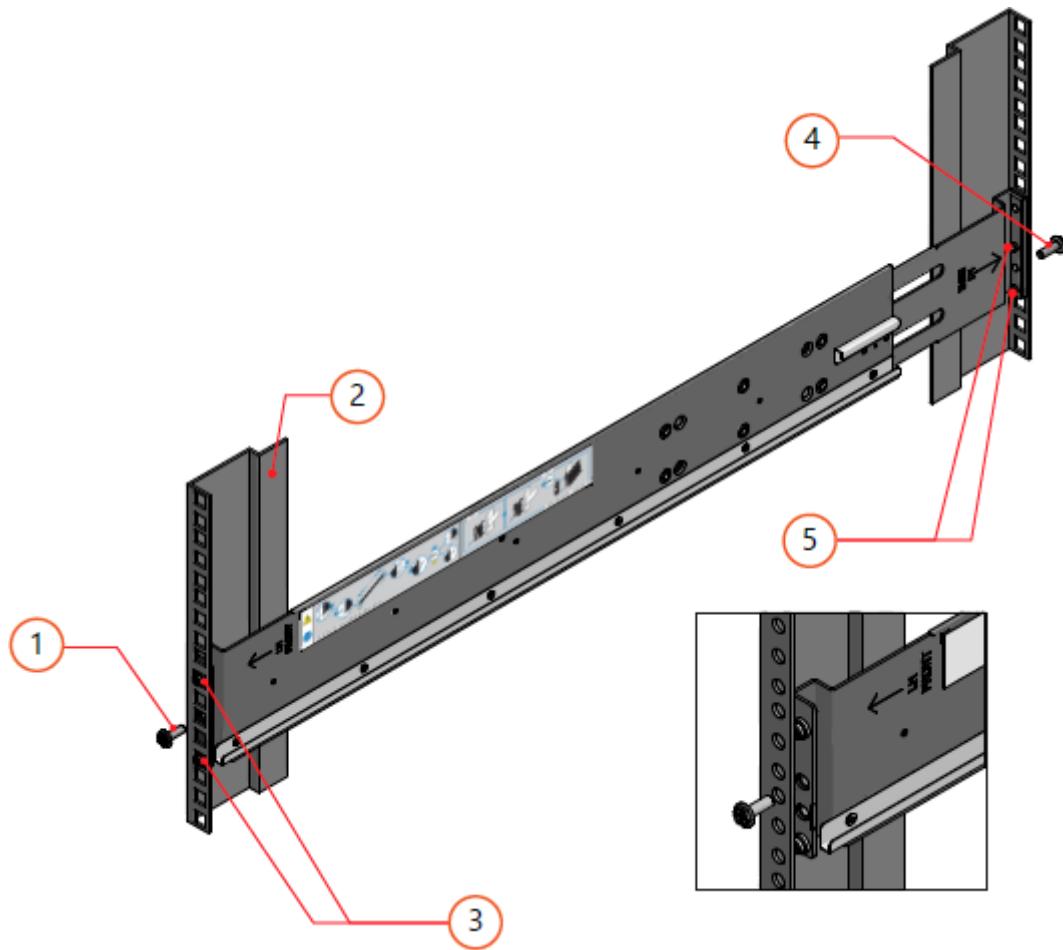
1. Perform this step only if inner rails are not installed on your device. Typically, the inner rails are installed at the factory. If rails are not installed, then install the left-rail and right-rail slides to the sides of the enclosure chassis. They attach using six metric screws on each side. To help with orientation, the rail slides are marked **LH – Front** and **RH – Front**, and the end that is affixed towards the rear of the enclosure has a tapered end.



Attaching inner rail slides to the sides of the enclosure

Label	Description
1	M 3x4 button-head screws
2	Chassis slides

2. Attach the outer left rail and outer right rail assemblies to the rack cabinet vertical members. The brackets are marked **LH**, **RH**, and **This side up** to guide you through the correct orientation.
3. Locate the rail pins at the front and rear of the rail assembly. Extend the rail to fit between the rack posts and insert the pins into the front and rear rack post vertical member holes. Be sure that the rail assembly is level.
4. Use two of the provided metric screws to secure the rail assembly to the rack vertical members. Use one screw on the front and one on the rear.
5. Repeat these steps for the other rail assembly.



Attaching outer rail assemblies to the rack

Label	Description
1	Clamping screw
2	Square-hole front rack post screw
3	Left rail front location pins
4	Clamping screw
5	Left rail rear location pins

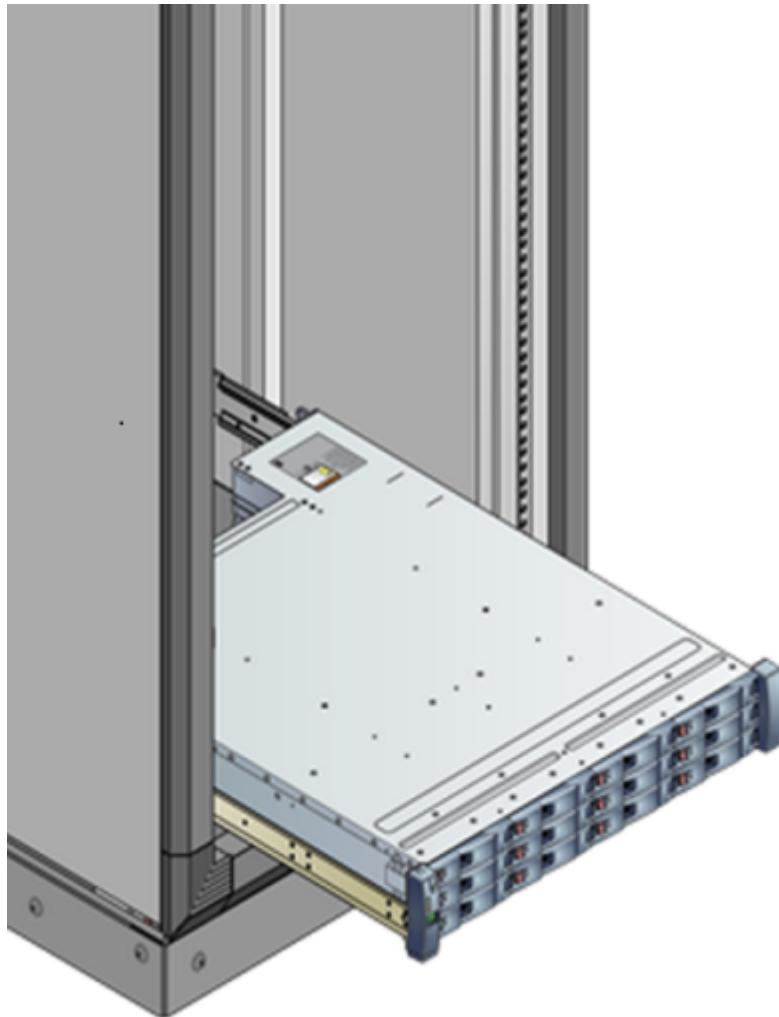
Mounting the device in the rack

Using the rack rails that were just installed, perform the following steps to mount the device in the rack.

To mount the device

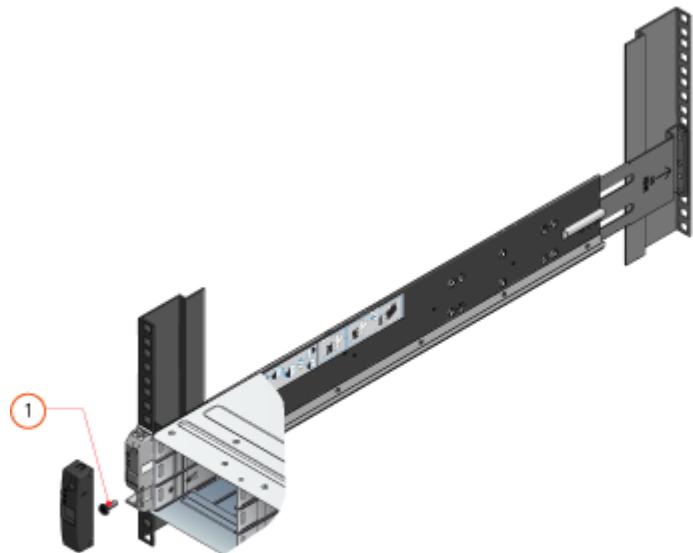
1. With an assistant, lift the enclosure and align it with the rack rails.

2. Carefully insert the device into the rails, and then push the device completely into the rack cabinet.



Mounting the device in the rack

3. Remove the left and right front flange caps by pulling the caps free. The flange caps simply snap onto the flanges.
4. Secure the enclosure in the rack by installing one provided Phillips-head screw through each flange, left and right.
5. Install the flange caps by pressing them into position and snapping them in place.



Installing the flange caps

Label	Description
1	Enclosure fastening screw

The next step is to cable your device for power, network, and serial access.

Cable your StorSimple 8100 device

The following procedures explain how to cable your StorSimple 8100 device for power, network, and serial connections.

Prerequisites

Before you begin the cabling of your device, you will need:

- Your storage device, completely unpacked and rack mounted.
- 2 power cables that came with your device
- Access to 2 Power Distribution Units (recommended).
- Network cables
- Provided serial cables
- Serial USB converter with the appropriate driver installed on your PC (if needed)
- Provided 4 QSFP-to-SFP+ adapters for use with 10 GbE network interfaces
- [Supported hardware for the 10 GbE network interfaces on your StorSimple device](#)

Power cabling

Your device includes redundant Power and Cooling Modules (PCMs). Both PCMs must be installed and connected to different power sources to ensure high availability.

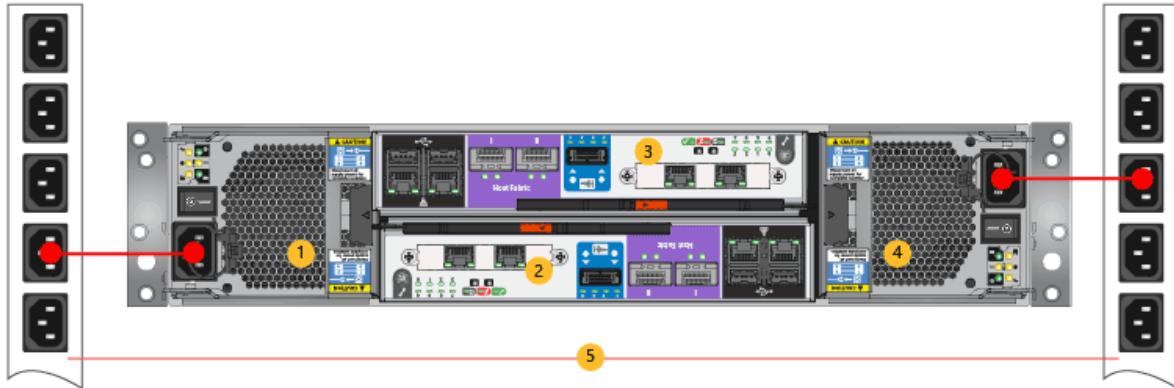
Perform the following steps to cable your device for power.

To cable for power

1. Make sure that the power switches on each of the Power and Cooling Modules (PCMs) are in the OFF position.
2. Connect the power cords to each of the PCMs in the primary enclosure.
3. Attach the power cords to the rack power distribution units (PDUs) as shown in the following image. Make sure that the two PCMs use separate power sources.

Important

To ensure high availability for your system, we recommend that you strictly adhere to the power cabling scheme shown in the following diagram.



Power cabling on an 8100 device

Label	Description
1	PCM 0
2	Controller 1
3	Controller 0
4	PCM 1
5	PDUs

4. To turn on the system, flip the power switches on both PCMs to the ON position.

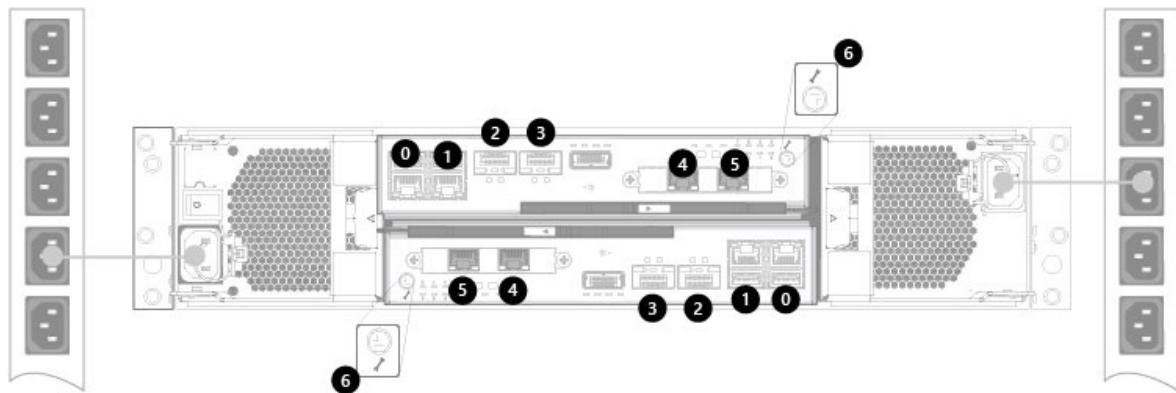
Network cabling

Your device is an active-standby configuration: at any given time, one controller module is active and processing all disk and network operations while the other controller module is on standby. If a controller fails, the standby controller is activated immediately and continues all the disk and networking operations.

To support this redundant controller failover, you need to cable your device network as described in the following steps.

To cable for network connection

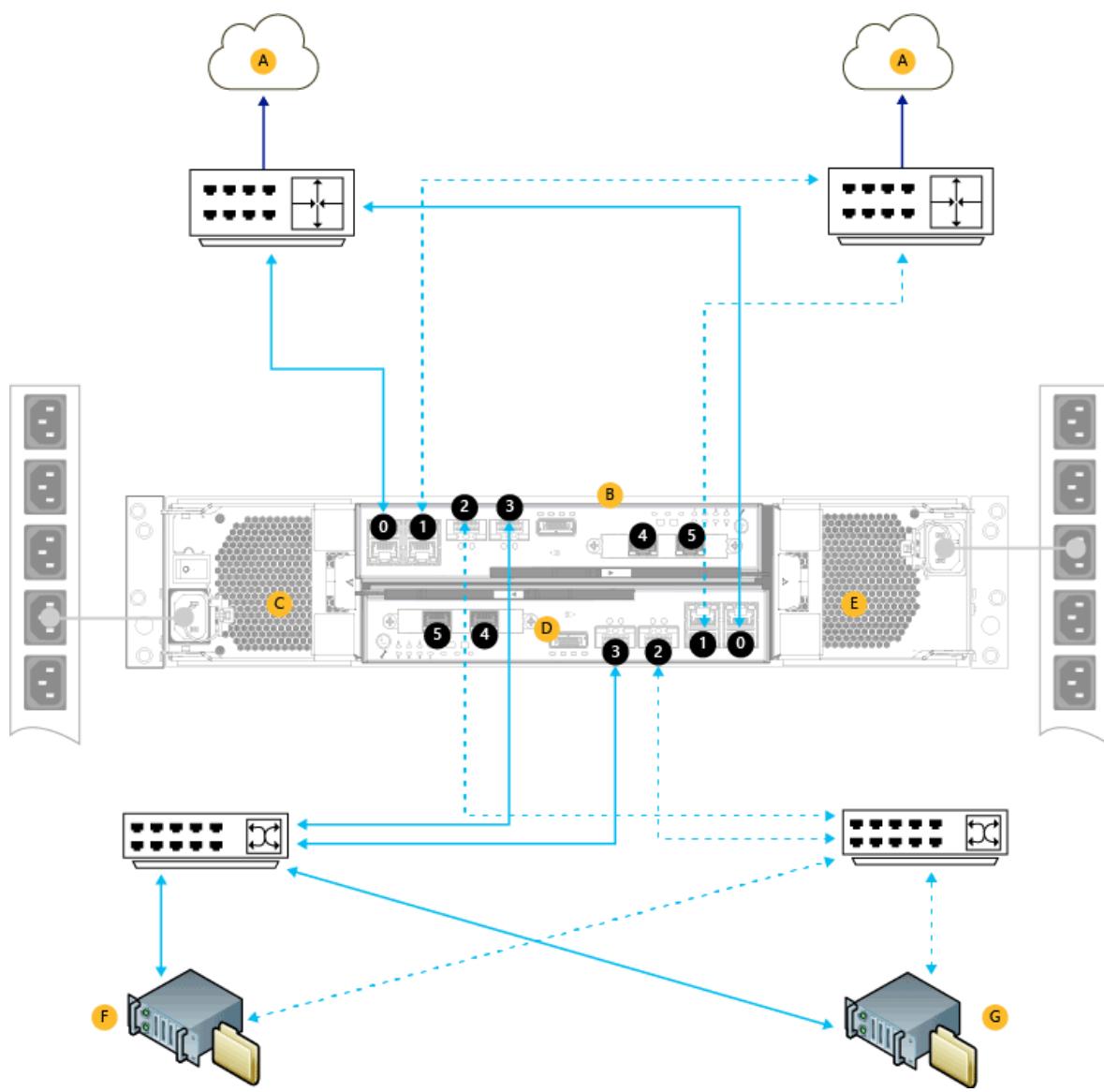
1. Your device has six network interfaces on each controller: four 1 Gbps, and two 10 Gbps Ethernet ports. Identify the various data ports on the backplane of your device.



Back of the device showing data ports

Label	Description
0,1,4,5	1 GbE network interfaces
2,3	10 GbE network interfaces
6	Serial ports

2. See the following diagram for network cabling. (The minimum network configuration is shown by solid blue lines. Additional configuration required for high availability and performance is shown by dotted lines.)



Network cabling for your device

Label	Description
A	LAN with Internet access
B	Controller 0
C	PCM 0
D	Controller 1
E	PCM 1
F, G	Hosts
0-5	Network interfaces

When cabling the device, the minimum configuration requires:

- At least two network interfaces connected on each controller with one for cloud access and one for iSCSI. The DATA 0 port is automatically enabled and configured via the serial console of the device. Apart from DATA 0, another data port also needs to be configured through the Azure classic portal. In this case, connect DATA 0 port to the primary LAN (network with Internet access). The other data ports can be connected to SAN/iSCSI LAN (VLAN) segment of the network, depending on the intended role.
- Identical interfaces on each controller connected to the same network to ensure availability if a controller failover occurs. For instance, if you choose to connect DATA 0 and DATA 3 for one of the controllers, you need to connect the corresponding DATA 0 and DATA 3 on the other controller.

Keep in mind for high availability and performance:

- When possible, configure a pair of network interface for cloud access (1 GbE) and another pair for iSCSI (10 GbE recommended) on each controller.
- When possible, connect network interfaces from each controller to two different switches to ensure availability against a switch failure. The figure illustrates the two 10 GbE network interfaces, DATA 2 and DATA 3, from each controller connected to two different switches.

For more information, refer to the **Network interfaces** under the [High availability requirements for your StorSimple device](#).

 **Note**

If you are using SFP+ transceivers with your 10 GbE network interfaces, use the provided QSFP-SFP+ adapters. For more information, go to [Supported hardware for the 10 GbE network interfaces on your StorSimple device](#).

Serial port cabling

Perform the following steps to cable your serial port.

To cable for serial connection

1. Your device has a serial port on each controller that is identified by a wrench icon. Refer to the illustration in the [Network cabling](#) section to locate the serial ports on the backplane of your device.
2. Identify the active controller on your device backplane. A blinking blue LED indicates that the controller is active.

3. Use the provided serial cables (if needed, the USB-serial converter for your laptop), and connect your console or computer (with terminal emulation to the device) to the serial port of the active controller.
4. Install the serial-USB drivers (shipped with the device) on your computer.
5. Set up the serial connection as follows: 115,200 baud, 8 data bits, 1 stop bit, no parity, and flow control set to None.
6. Verify that the connection is working by pressing Enter on the console. A serial console menu should appear.

 **Note**

Lights-Out Management: When the device is installed in a remote datacenter or in a computer room with limited access, ensure that the serial connections to both controllers are always connected to a serial console switch or similar equipment. This allows out-of-band remote control and support operations if there are network disruptions or unexpected failures.

Your device is now cabled for power, network access, and serial connectivity. The next step is to configure the software and deploy your device.

Next steps

Learn how to [deploy and configure your on-premises StorSimple device](#).

Unpack, rack-mount, and cable your StorSimple 8600 device

Article • 03/23/2020 • 13 minutes to read

⊗ Caution

StorSimple 8000 series will reach its end-of-life in December 2022. Microsoft provides a **dedicated migration service** for StorSimple 8000 series volumes and their backups. It is imperative that you stop any new StorSimple deployments and begin planning your migration now.

The StorSimple Data Manager contains a dedicated migration service for your StorSimple volumes and their backups. If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. [Review the migration guide.](#)

Overview

Your Microsoft Azure StorSimple 8600 is a dual enclosure device and consists of a primary and an EBOD enclosure. This tutorial explains how to unpack, rack-mount, and cable the StorSimple 8600 device hardware before you configure the StorSimple software.

Unpack your StorSimple 8600 device

The following steps provide clear, detailed instructions on how to unpack your StorSimple 8600 storage device. This device is shipped in two boxes, one for the primary enclosure and another for the EBOD enclosure. These two boxes are then placed in a single box.

Prepare to unpack your device

Before you unpack your device, review the following information.



1. Make sure that you have two people available to manage the weight of the device if you are handling it manually. A fully configured enclosure can weigh up to 32 kg

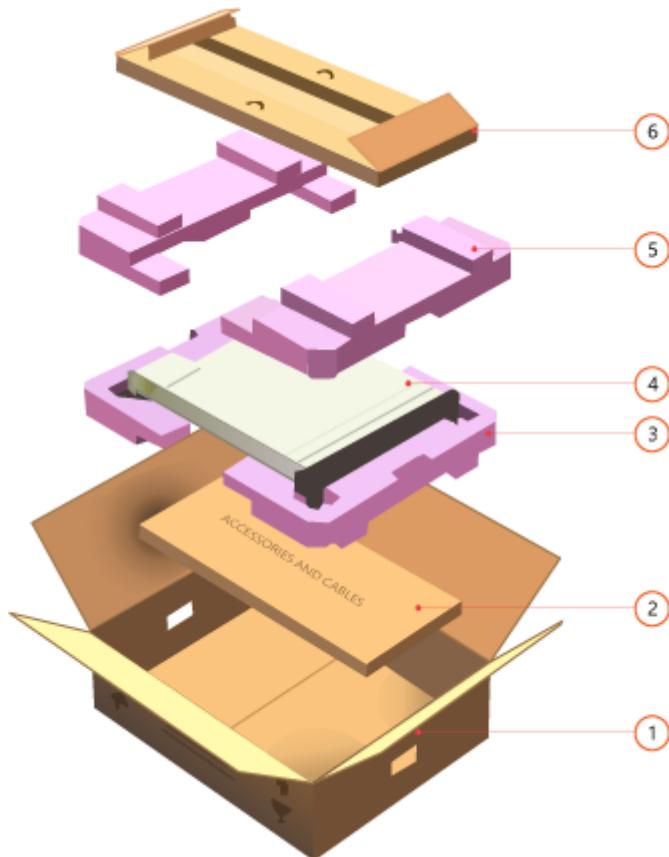
(70 lbs.).

2. Place the box on a flat, level surface.

Next, complete the following steps to unpack your device.

To unpack your device

1. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, do not open the box. Please [contact Microsoft Support](#) to help you assess whether the device is in good working order.
2. Open the outer box and then take out the two boxes corresponding to primary and EBOD enclosures. You can now unpack the primary and EBOD enclosures. The following figure shows the unpacked view of one of the enclosures.



Unpacked view of your storage device

Label	Description
1	Packing box
2	SAS cables (in accessories and cables tray)
3	Bottom foam

Label	Description
4	Device
5	Top foam
6	Accessory box

3. After unpacking the two boxes, make sure that you have:

- 1 primary enclosure (the primary enclosure and EBOD enclosure are in two separate boxes)
- 1 EBOD enclosure
- 4 power cords, 2 in each box
- 2 SAS cables (to connect the primary enclosure to EBOD enclosure)
- 1 crossover Ethernet cable
- 2 serial console cables
- 1 serial-USB converter for serial access
- 4 QSFP-to-SFP+ adapters for use with 10 GbE network interfaces
- 2 rack mount kits (4 side rails with mounting hardware, 2 each for the primary enclosure and EBOD enclosure), 1 in each box
- Getting started documentation

If you did not receive any of the items listed above, [contact Microsoft Support](#).

The next step is to rack-mount your device.

Rack-mount your StorSimple 8600 device

Follow the next steps to install your StorSimple 8600 storage device in a standard 19-inch rack with front and rear posts. This device comes with two enclosures: a primary enclosure and an EBOD enclosure. Both of these need to be rack-mounted.

The installation consists of multiple steps, each of which is discussed in the following procedures.

Important

StorSimple devices must be rack-mounted for proper operation.

Site preparation

The enclosures must be installed in a standard 19-inch rack that has both front and rear posts. Use the following procedure to prepare for rack installation.

To prepare the site for rack installation

1. Make sure that the primary and EBOD enclosures are resting safely on a flat, stable, and level work surface (or similar).
2. Verify that the site where you intend to set up has standard AC power from an independent source or a rack Power Distribution Unit (PDU) with an uninterruptible power supply (UPS).
3. Make sure that one 4U (2 X 2U) slot is available on the rack in which you intend to mount the enclosures.



Make sure that you have two people available to manage the weight if you are handling the device setup manually. A fully configured enclosure can weigh up to 32 kg (70 lbs.).

Rack prerequisites

The enclosures are designed for installation in a standard 19-inch rack cabinet with:

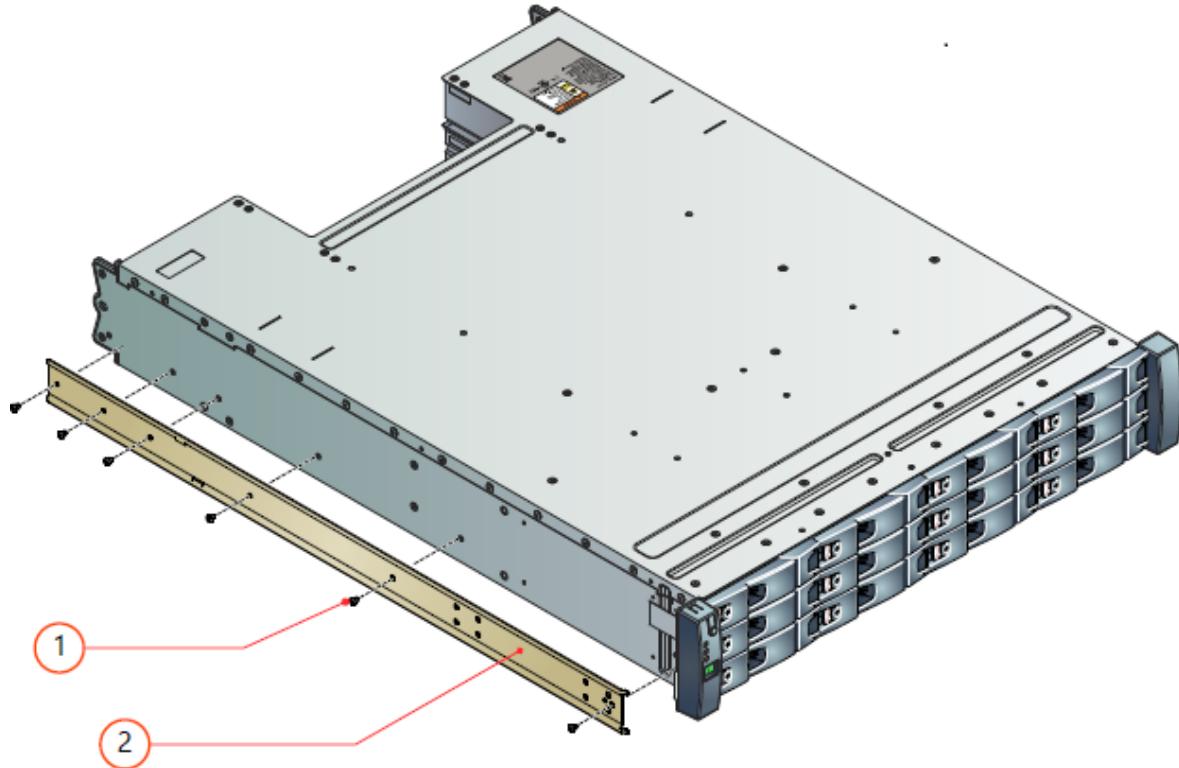
- Minimum depth of 27.84 inches from rack post to post
- Maximum weight of 32 kg for the device
- Maximum back pressure of 5 Pascal (0.5 mm water gauge)

Rack-mounting rail kit

A set of mounting rails will be provided for use with the 19-inch rack cabinet. The rails have been tested to handle the maximum enclosure weight. These rails will also allow installation of multiple enclosures without loss of space within the rack. Install the EBOD enclosure first.

To install the EBOD enclosure on the rails

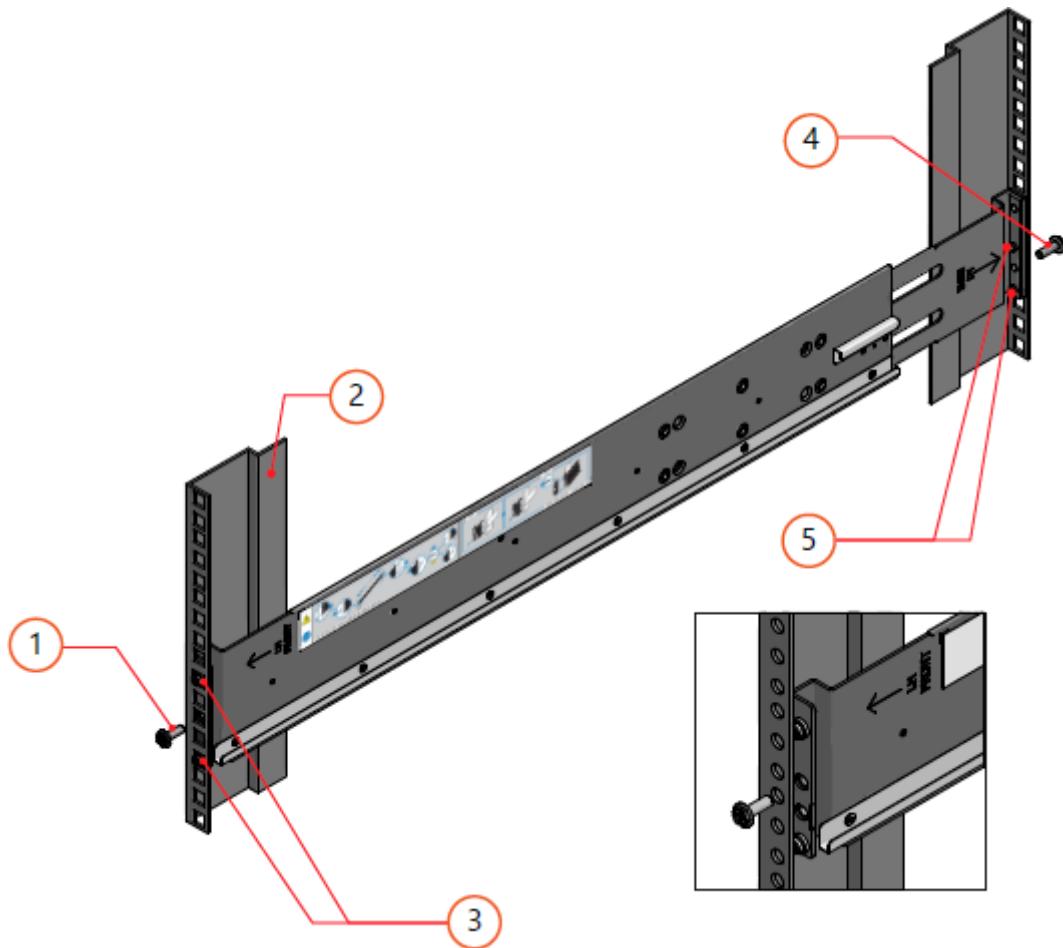
1. Perform this step only if inner rails are not installed on your device. Typically, the inner rails are installed at the factory. If rails are not installed, then install the left-rail and right-rail slides to the sides of the enclosure chassis. They attach using six metric screws on each side. To help with orientation, the rail slides are marked **LH – Front** and **RH – Front**, and the end that is affixed towards the rear of the enclosure has a tapered end.



Attaching rail slides to the sides of the enclosure

Label	Description
1	M 3x4 button-head screws
2	Chassis slides

2. Attach the left rail and right rail assemblies to the rack cabinet vertical members. The brackets are marked **LH**, **RH**, and **This side up** to guide you through correct orientation.
3. Locate the rail pins at the front and rear of the rail assembly. Extend the rail to fit between the rack posts and insert the pins into the front and rear-rack post vertical member holes. Be sure that the rail assembly is level.
4. Secure the rail assembly to the rack vertical members by using two of the metric screws provided. Use one screw on the front and one on the rear.
5. Repeat these steps for the other rail assembly.



Attaching rail assemblies to the rack

Label	Description
1	Clamping screw
2	Square-hole front rack post screw
3	Left front rail location pins
4	Clamping screw
5	Left rear rail location pins

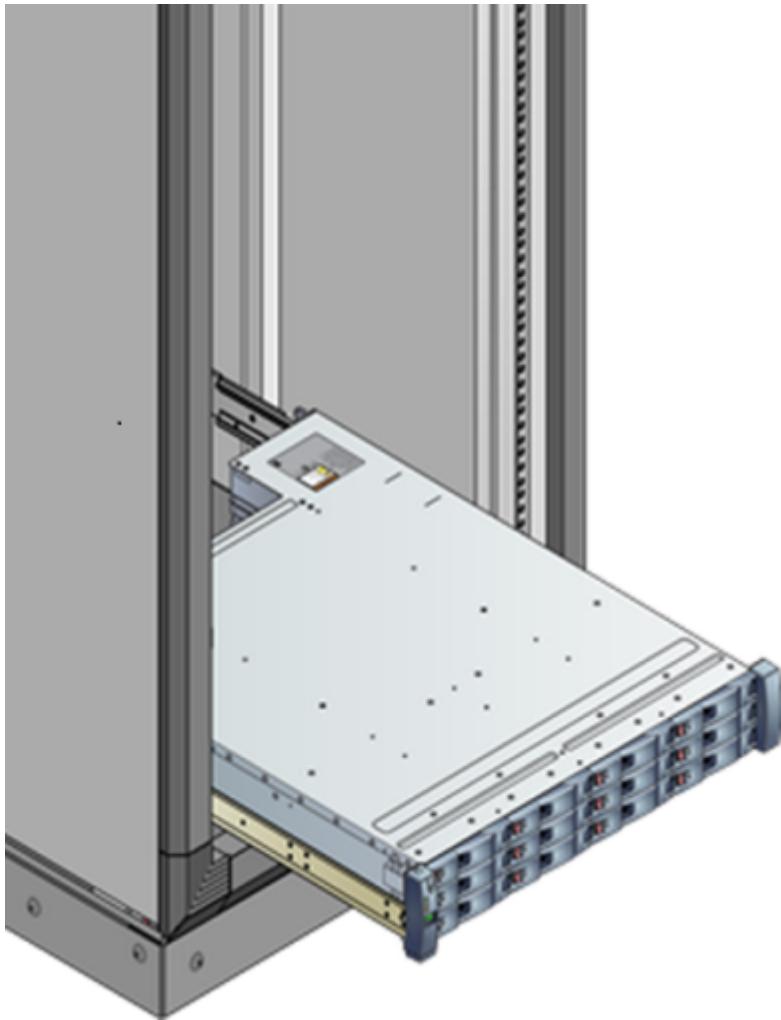
Mounting the EBOD enclosure in the rack

Using the rack rails that were just installed, perform the following steps to mount the EBOD enclosure in the rack.

To mount the EBOD enclosure

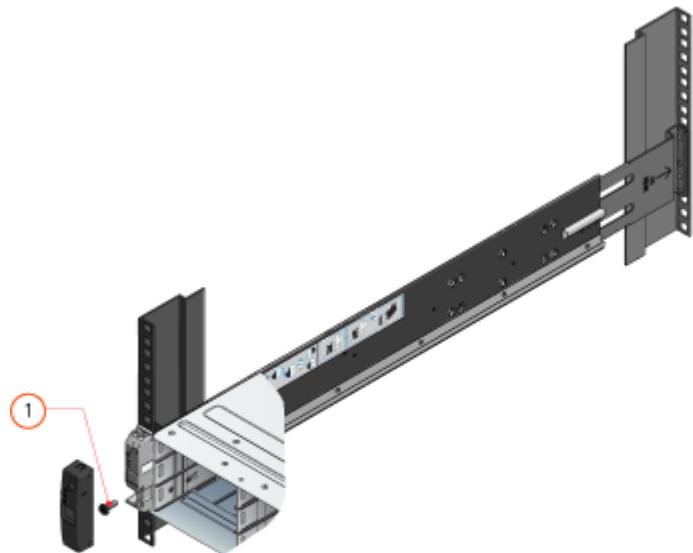
1. With an assistant, lift the enclosure and align it with the rack rails.

2. Carefully insert the enclosure into the rails, and then push it completely into the rack cabinet.



Mounting the enclosure in the rack

3. Remove the left and right front flange caps by pulling the caps free. The flange caps simply snap onto the flanges.
4. Secure the enclosure into the rack by installing one provided Phillips-head screw through each flange, left and right.
5. Install the flange caps by pressing them into position and snapping them into place.



Installing the flange caps

Label	Description
1	Enclosure fastening screw

Mounting the primary enclosure in the rack

After you have finished mounting the EBOD enclosure, you will need to mount the primary enclosure following the same steps.

ⓘ Note

- It is possible to have a few empty slots in the rack between the primary enclosure and the EBOD enclosure.
- Use the provided 2m SAS cable to connect the primary enclosure to the EBOD enclosure.
- There are no constraints on the relative placement of the head unit to the EBOD unit. Therefore, the primary enclosure can be placed in the top slot and the EBOD enclosure below — or vice versa.

The next step is to cable your device for power, network, and serial access.

Cable your StorSimple 8600 device

The following procedures explain how to cable your StorSimple 8600 device for power, network, and serial connections.

Prerequisites

Before you begin to cable your device, you will need:

- Your primary enclosure and the EBOD enclosure, completely unpacked
- 4 power cables (2 each for the primary and the EBOD enclosure) that came with your device
- 2 SAS cables supplied with the device to connect the EBOD enclosure to the primary enclosure
- Access to 2 Power Distribution Units (PDUs) (recommended)
- Network cables
- Provided serial cables
- Serial-USB converter with the appropriate driver installed on your PC (if needed)
- Provided 4 QSFP-to-SFP+ adapters for use with 10 GbE network interfaces
- [Supported hardware for the 10 GbE network interfaces on your StorSimple device](#)

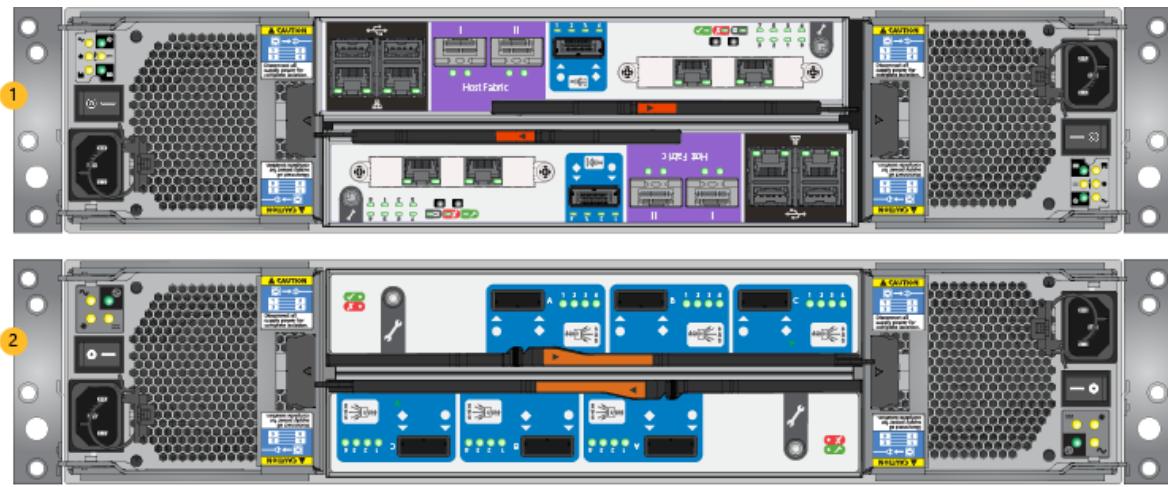
SAS and Power cabling

Your device has both a primary enclosure and an EBOD enclosure. This requires the units to be cabled together for Serial Attached SCSI (SAS) connectivity and power.

When setting up this device for the first time, perform the steps for SAS cabling first and then complete the steps for power cabling.

To attach the SAS cables

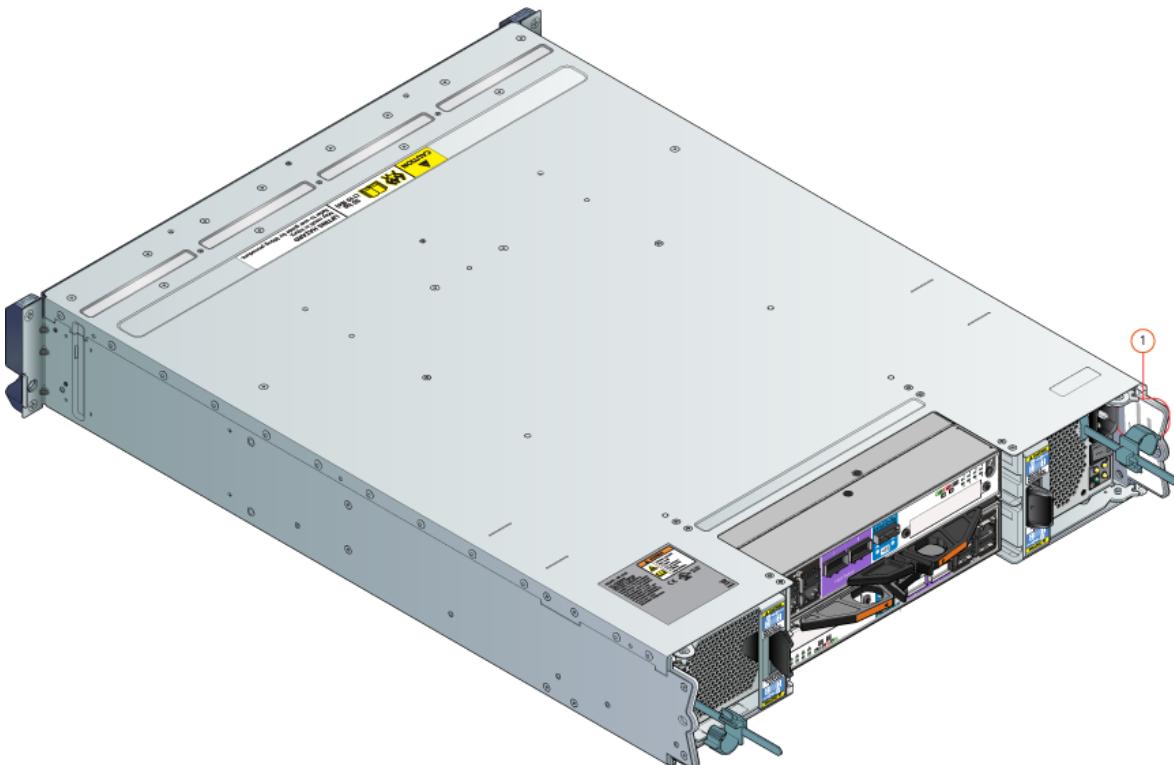
1. Identify the primary and the EBOD enclosures. The two enclosures can be identified by looking at their respective back planes. See the following image for guidance.



Back view of primary and EBOD enclosures

Label	Description
1	Primary enclosure
2	EBOD enclosure

- Locate the serial numbers on the primary and the EBOD enclosures. The serial number sticker is affixed to the back ear of each enclosure. The serial numbers must be identical on both enclosures. [Contact Microsoft Support](#) immediately if the serial numbers do not match. See the following illustration to locate the serial numbers.



Location of serial number sticker

Label	Description
1	Ear of the enclosure

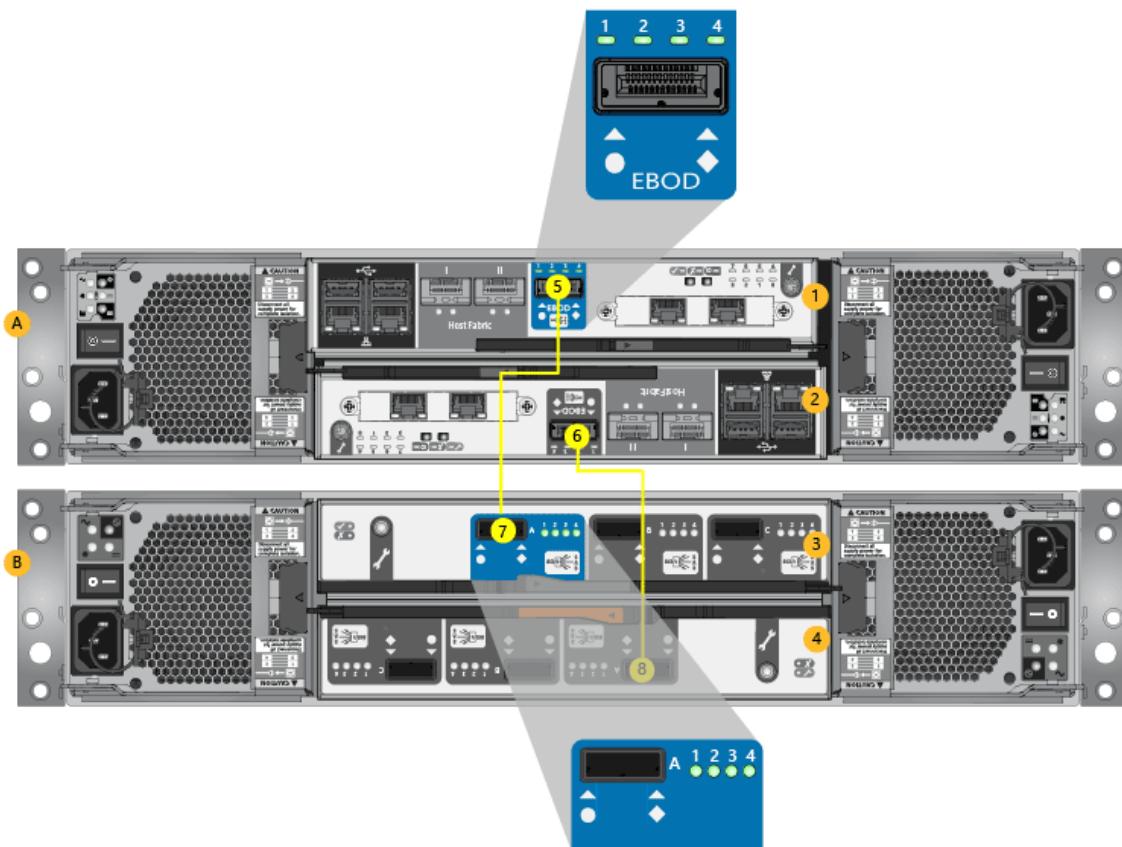
3. Use the provided SAS cables to connect the EBOD enclosure to the primary enclosure as follows:

a. Identify the four SAS ports on the primary enclosure and the EBOD enclosure.

The SAS ports are labeled as EBOD on the primary enclosure and correspond to port A on the EBOD enclosure, as shown in the SAS cabling illustration, below.

b. Use the provided SAS cables to connect the EBOD port to port A.

c. The EBOD port on controller 0 should be connected to the port A on EBOD controller 0. The EBOD port on controller 1 should be connected to the port A on EBOD controller 1. See the following illustration for guidance.



SAS cabling

Label	Description
A	Primary enclosure
B	EBOD enclosure
1	Controller 0

Label	Description
2	Controller 1
3	EBOD Controller 0
4	EBOD Controller 1
5, 6	SAS ports on primary enclosure (labeled EBOD)
7, 8	SAS ports on EBOD enclosure (Port A)

To cable your device for power

 **Note**

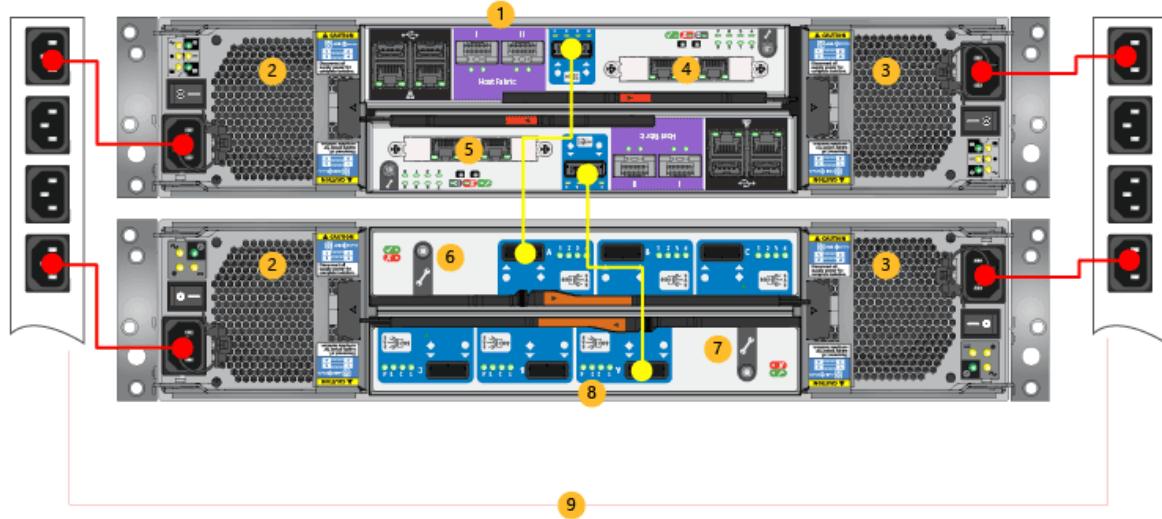
Both enclosures on your StorSimple device include redundant PCMs. For each enclosure, the PCMs must be installed and connected to different power sources to ensure high availability.

1. Make sure that the power switches on all the PCMs are in the OFF position.
2. On the primary enclosure, connect the power cords to both PCMs. The power cords are identified in red in the power cabling diagram, below.
3. Make sure that the two PCMs on the primary enclosure use separate power sources.
4. Attach the power cords to the power on the rack distribution units as shown in the power cabling diagram.
5. Repeat steps 2 through 4 for the EBOD enclosure.
6. Turn on the EBOD enclosure by flipping the power switch on each PCM to the ON position.
7. Verify that the EBOD enclosure is turned on by checking that the green LEDs on the back of the EBOD controller are turned ON.
8. Turn on the primary enclosure by flipping each PCM switch to the ON position.
9. Verify that the system is on by ensuring the device controller LEDs have turned ON.
10. Make sure that the connection between the EBOD controller and the device controller is active by verifying that the four LEDs next to the SAS port on the

EBOD controller are green.

ⓘ Important

To ensure high availability for your system, we recommend that you strictly adhere to the power cabling scheme shown in the following diagram.



Power cabling

Label	Description
1	Primary enclosure
2	PCM 0
3	PCM 1
4	Controller 0
5	Controller 1
6	EBOD controller 0
7	EBOD controller 1
8	EBOD enclosure
9	PDUs

Network cabling

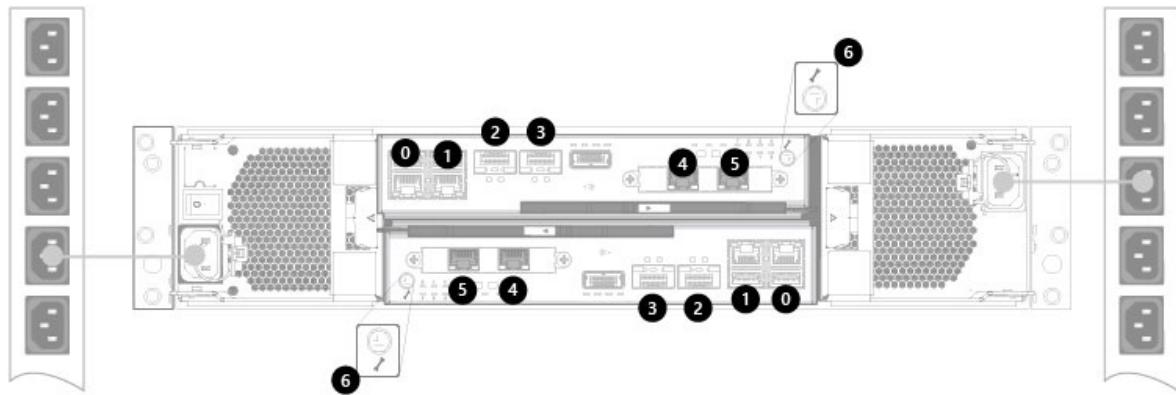
Your device is in an active-standby configuration: at any given time, one controller module is active and processing all disk and network operations while the other

controller module is on standby. If a controller failure occurs, the standby controller immediately activates and continues all the disk and networking operations.

To support this redundant controller failover, you need to cable your device network as shown in the following steps.

To cable for network connection

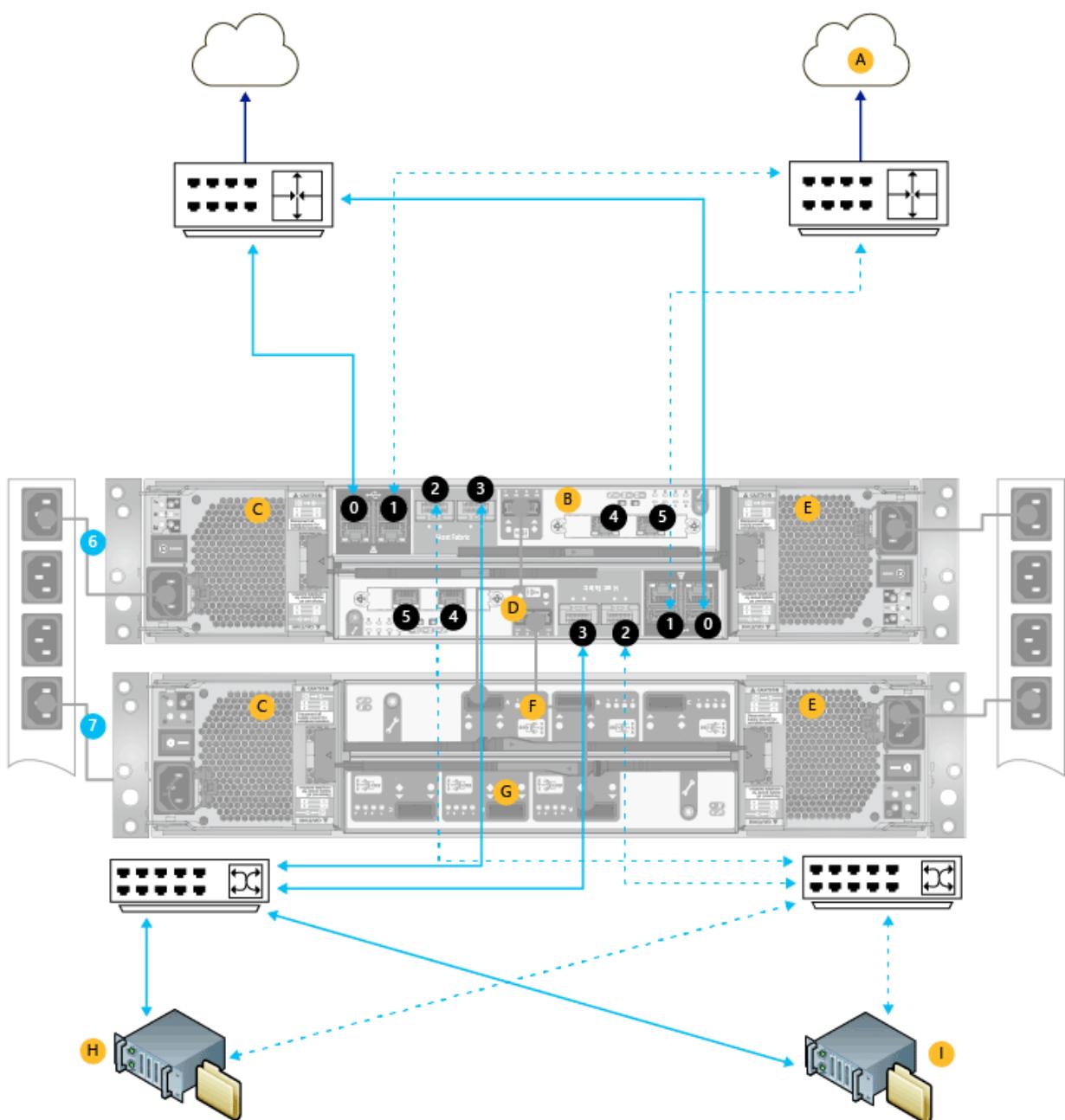
1. Your device has six network interfaces on each controller: four 1 Gbps and two 10 Gbps Ethernet ports. Refer to the following illustration to identify the data ports on the backplane of your device.



Back of your device showing the data ports

Label	Description
0,1,4,5	1 GbE network interfaces
2,3	10 GbE network interfaces
6	Serial ports

2. See the following diagram for network cabling. (The minimum network configuration is shown by solid blue lines. For high availability and performance, additional configuration required is shown by dotted lines.)



Network cabling for your device

Label	Description
A	LAN with Internet access
B	Controller 0
C	PCM 0
D	Controller 1
E	PCM 1
F	EBOD controller 0
G	EBOD controller 1
H,I	Hosts (for example, file servers)

Label	Description
0-5	Network interfaces
6	Primary enclosure
7	EBOD enclosure

When cabling the device, the minimum configuration requires:

- At least two network interfaces connected on each controller with one for cloud access and one for iSCSI. The DATA 0 port is automatically enabled and configured via the serial console of the device. Apart from DATA 0, another data port also needs to be configured through the Azure classic portal. In this case, connect DATA 0 port to the primary LAN (network with Internet access). The other data ports can be connected to SAN/iSCSI LAN (VLAN) segment of the network, depending on the intended role.
- Identical interfaces on each controller connected to the same network to ensure availability if a controller failover occurs. For instance, if you choose to connect DATA 0 and DATA 3 for one of the controllers, you need to connect the corresponding DATA 0 and DATA 3 on the other controller.

Keep in mind for high availability and performance:

- When possible, configure a pair of network interface for cloud access (1 GbE) and another pair for iSCSI (10 GbE recommended) on each controller.
- When possible, connect network interfaces from each controller to two different switches to ensure availability against a switch failure. The figure illustrates the two 10 GbE network interfaces, DATA 2 and DATA 3, from each controller connected to two different switches. For more information, refer to the **Network interfaces** under the [High availability requirements for your StorSimple device](#).

Note

If using SFP+ transceivers with your 10 GbE network interfaces, use the provided QSFP-SFP+ adapters. For more information, go to [Supported hardware for the 10 GbE network interfaces on your StorSimple device](#).

Serial port cabling

Perform the following steps to cable your serial port.

To cable for serial connection

1. Your device has a serial port on each controller that is identified by a wrench icon.
To locate the serial ports, refer to the illustration that shows the data ports on the back of your device.
2. Identify the active controller on your device backplane. A blinking blue LED indicates that the controller is active.
3. Use the provided serial cable (if needed, the USB-serial converter for your laptop), and connect your console or computer (with terminal emulation to the device) to the serial port of the active controller.
4. Install the serial-USB drivers (shipped with the device) on your computer.
5. Set up the serial connection as follows:
 - 115,200 baud
 - 8 data bits
 - 1 stop bit
 - No parity
 - Flow control set to **None**
6. Verify that the connection is working by pressing Enter on the console. A serial console menu should appear.

Note

Lights-Out Management: When the device is installed in a remote datacenter or in a computer room with limited access, ensure that the serial connections to both controllers are always connected to a serial console switch or similar equipment. This allows out-of-band remote control and support operations in case of network disruption or unexpected failures.

You have completed cabling your device for power, network access, and serial connection. The next step is to configure the software on your device.

Next steps

You are now ready to [deploy and configure your on-premises StorSimple device](#).

Supported hardware for the 10 GbE network interfaces on your StorSimple device

Article • 01/03/2022 • 4 minutes to read

⊗ Caution

StorSimple 8000 series will reach its end-of-life in December 2022. Microsoft provides a **dedicated migration service** for StorSimple 8000 series volumes and their backups. It is imperative that you stop any new StorSimple deployments and begin planning your migration now.

The StorSimple Data Manager contains a dedicated migration service for your StorSimple volumes and their backups. If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. [Review the migration guide](#).

Overview

This article provides information about supplementary hardware that works with your Microsoft Azure StorSimple device.

List of devices tested by Microsoft

Microsoft has tested the following small form-factor pluggable (SFP) transceivers, cables, and switches to ensure that they function optimally with devices. (The following tables will be updated as new hardware is tested.)

SFP+ Transceivers

Make	Model
Cisco	SFP-10G-SR

Cables

S. No.	Make	Model
1.	Cisco	SFP-H10GB-CU1M
2.	Cisco	SFP-H10GB-CU2M
3.	Cisco	SFP-H10GB-CU3M
4.	Tripp-Lite	N820-05M (OM3)

Switches

S. No.	Make	Model
1.	Cisco	N3K-C3172PQ-10GE
2.	Cisco	N3K-C3048-ZM-F
3.	Cisco	N5K-C5596UP-FA

List of devices tested in the field

This section contains the list of devices that have been successfully deployed in the field by StorSimple customers. These have not been tested by Microsoft but are likely to work with your StorSimple device.

Parameter	Value
Switch make	Juniper
Switch model	ex4550-32F
Switch operating system version	JunOS 12.3R9.4
Blade model	Ports onboard (PIC 0)
Transceiver make	Juniper
Transceiver model	Part number 740-021308 Part number 740-030658
Transceiver firmware version	Rev 01 Version 0.0 (reported)
Cable model	Duplex jumper LC/LC 50/125µ, OM3, LSZH
StorSimple model	8600

Parameter	Value
StorSimple software version	6.3.9600.17491

List of devices tested by OEM provider (Mellanox)

Mellanox has tested the following small form-factor pluggable (SFP) transceivers, cables, and switches to ensure that they function optimally with Mellanox network interfaces such as the 10 GbE network interfaces on your StorSimple device.

Cables and modules supported by Mellanox

The following table lists the cables and modules supported by Mellanox. These have not been tested by Microsoft but are likely to work with your StorSimple device.

S. No.	Speed	Model	Description	Make
1.	10 GbE	CAB-SFP-SFP-1M	passive copper cable SFP+ 10 Gb/s 1m	Arista
2.	10 GbE	CAB-SFP-SFP-2M	passive copper cable SFP+ 10 Gb/s 2m	Arista
3.	10 GbE	CAB-SFP-SFP-3M	passive copper cable SFP+ 10 Gb/s 3m	Arista
4.	10 GbE	CAB-SFP-SFP-5M	passive copper cable SFP+ 10 Gb/s 5m	Arista
5.	10 GbE	Cisco SFP-H10GBCU1M	Cisco SFP+ cable	Cisco
6.	10 GbE	Cisco SFP-H10GBCU3M	Cisco SFP+ cable	Cisco
7.	10 GbE	Cisco SFP-H10GBCU5M	Cisco SFP+ cable	Cisco
8.	10 GbE	J9281B HP X242 10G	SFP+ to SFP+ 1m Direct Attach Copper Cable	HP
9.	10 GbE	455883-B21 HP BLc	10Gb SR SFP+ Opt	HP

S. No.	Speed	Model	Description	Make
10.	10 GbE	455886-B21 HP BLc	10Gb LR SFP+ Opt	HP
11.	10 GbE	487649-B21 HP BLc	SFP+ 0.5m 10GbE Copper Cable	HP
12.	10 GbE	487652-B21 HP BLc	SFP+ 1m 10GbE Copper Cable	HP
13.	10 GbE	487655-B21 HP BLc	SFP+ 3m 10GbE Copper Cable	HP
14.	10 GbE	487658-B21 HP BLc	SFP+ 7m 10GbE Copper Cable	HP
15.	10 GbE	537963-B21 HP BLc	SFP+ 5m 10GbE Copper Cable	HP
16.	10 GbE	AP784A HP	3m C-series Passive Copper SFP+ Cable	HP
17.	10 GbE	AP785A HP	5m C-series Passive Copper SFP+ Cable	HP
18.	10 GbE	AP818A HP	1m B-series Active Copper SFP+ Cable	HP
19.	10 GbE	AP819A HP	3m B-series Active Copper SFP+ Cable	HP
20.	10 GbE	J9150A HP	X132 10G SFP+ LC SR Transceiver	HP
21.	10 GbE	J9151A HP	X132 10G SFP+ LC LR Transceiver	HP
22.	10 GbE	J9283B HP	X242 10G SFP+ SFP+ 3m DAC Cable	HP
23.	10 GbE	J9285B HP	X242 10G SFP+ SFP+ 7m DAC Cable	HP
24.	10 GbE	JD095B HP	X240 10G SFP+ SFP+ 0.65m DAC Cable	HP
25.	10 GbE	JD096B HP	X240 10G SFP+ SFP+ 1.2m DAC Cable	HP

S. No.	Speed	Model	Description	Make
26.	10 GbE	JD097B HP	X240 10G SFP+ SFP+ 3m DAD Cable	HP
27.	10 GbE	MAM1Q00A-QSA Mellanox	QSFP To SFP+ Adapter	Mellanox Technologies
28.	10 GbE	MC2309124-006 Mt	Passive Copper Cable 1x SFP+ To QSFP 10Gb/s 24awg 7m	Mellanox Technologies
29.	10 GbE	MC2309124-007 Mt	Passive Copper Cable 1x SFP+ To QSFP 10Gb/s 24awg 7m	Mellanox Technologies
30.	10 GbE	MC2309130-003 Mt	Passive Copper Cable 1x SFP+ To QSFP 10Gb/s 30awg 3m	Mellanox Technologies
31.	10 GbE	MC2309130-00A Mt	Passive Copper Cable 1x SFP+ To QSFP 10Gb/s 30awg 0.5m	Mellanox Technologies
32.	10 GbE	MC3309124-005 Mt	Passive Copper Cable 1x SFP+ 10Gb/s 24awg 5m	Mellanox Technologies
33.	10 GbE	MC3309124-007 Mt	Passive Copper Cable 1x SFP+ 10Gb/s 24awg 7m	Mellanox Technologies
34.	10 GbE	MC3309130-003 Mt	Passive Copper Cable 1x SFP+ 10Gb/s 30awg 3m	Mellanox Technologies
35.	10 GbE	MC3309130-00A Mt	Passive Copper Cable 1x SFP+ 10Gb/s 30awg 0.5m	Mellanox Technologies

Switches supported by Mellanox

The following table lists the switches supported by Mellanox. These have not been tested by Microsoft but are likely to work with your StorSimple device.

S. No.	Speed	Model	Description	Make
1.	10GbE	516733-B21	HP ProCurve 6120XG 10GbE Ethernet Blade Switch	HP
2.	10GbE	538113-B21	HP 10GbE Pass-Through Module (PTM)	HP
3.	10GbE	EN4093	IBM PureFlex System Fabric EN4093 10 Gigabit Scalable Switch Module	IBM

S. No.	Speed	Model	Description	Make
4.	1GbE	3020	Cisco Catalyst 3020 1GbE switch blade	Cisco
5.	1GbE	3020X	Cisco Catalyst 3020X 1GbE switch blade	Cisco
6.	1GbE	438030-B21	HP 1GbE switch module - GbE2c Layer 2/3 Ethernet Blade Switch	HP
7.	1GbE	6120G	HP ProCurve 6120G/XG 1GbE switch blade	HP

Next steps

[Learn more about StorSimple hardware components and status.](#)

Deploy the StorSimple Device Manager service for StorSimple 8000 series devices

Article • 08/19/2022 • 12 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple devices. After you create the service, you can use it to manage all the devices that are connected to the StorSimple Device Manager service from a single, central location, thereby minimizing administrative burden.

This tutorial describes the steps required for the creation, deletion, migration of the service and the management of the service registration key. The information contained in this article is applicable only to StorSimple 8000 series devices. For more information on StorSimple Virtual Arrays, go to [deploy a StorSimple Device Manager service for your StorSimple Virtual Array](#).

ⓘ Note

- The Azure portal supports devices running Update 5.0 or later. If your device is not up to date, install Update 5 immediately. For more information, go to [Install Update 5](#).
- If you're using a StorSimple Cloud Appliance (8010/8020), you cannot update a cloud appliance. Use the latest version of software to create a new cloud appliance with Update 5.0, and then fail over to the new cloud appliance created.

- All devices running Update 4.0 or earlier will experience reduced management functionality.

Create a service

To create a StorSimple Device Manager service, you need to have:

- A subscription with an Enterprise Agreement
- An active Microsoft Azure storage account
- The billing information that is used for access management

Only the subscriptions with an Enterprise Agreement are allowed. You can also choose to generate a default storage account when you create the service.

A single service can manage multiple devices. However, a device cannot span multiple services. A large enterprise can have multiple service instances to work with different subscriptions, organizations, or even deployment locations.

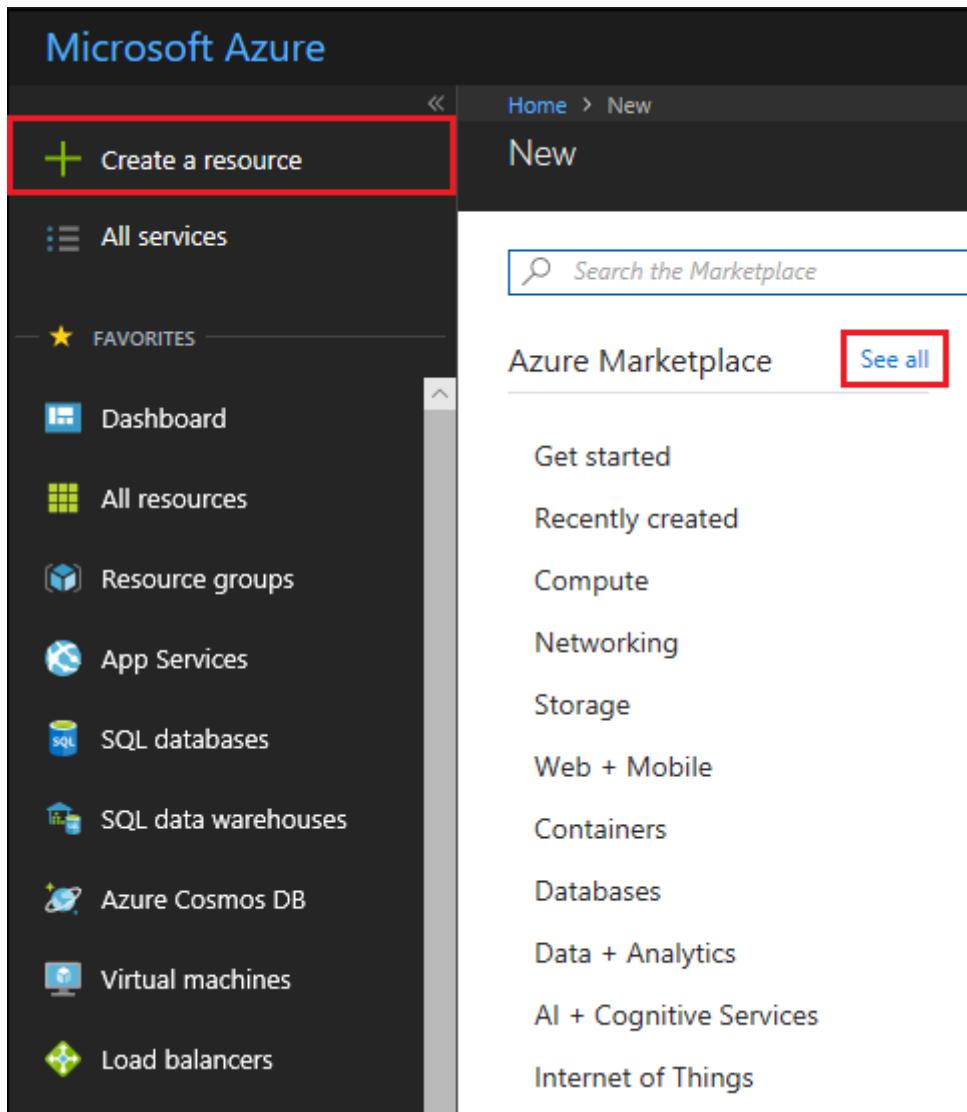
Note

You need separate instances of StorSimple Device Manager service to manage StorSimple 8000 series devices and StorSimple Virtual Arrays.

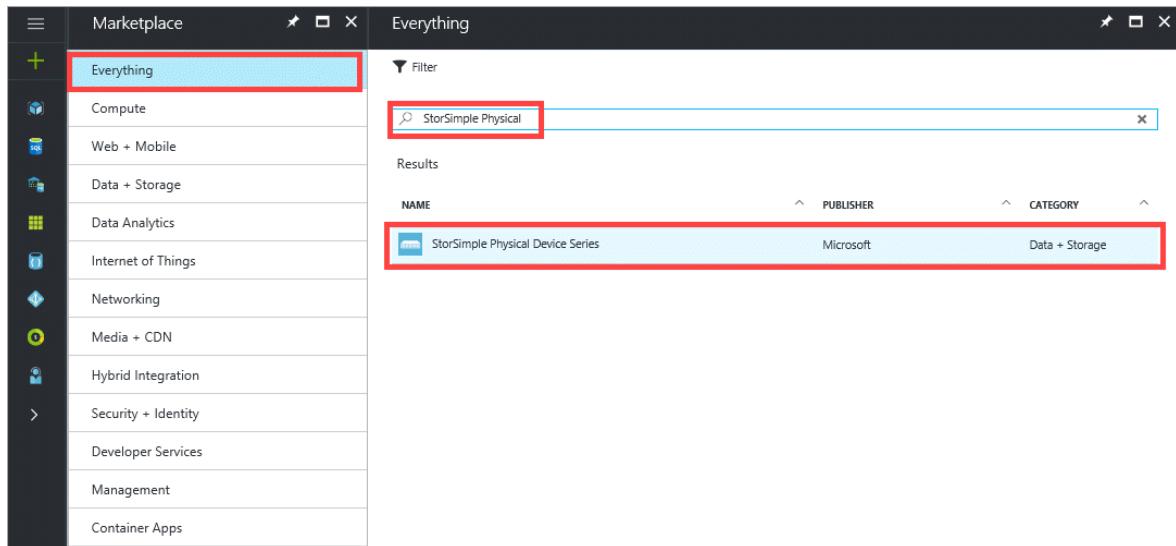
Perform the following steps to create a service.

To create a new service

1. Use your Microsoft account credentials to sign in to the [Azure portal](#).
2. In the Azure portal, click **Create a resource** and then in the marketplace, click **See all**.



Search for *StorSimple Physical*. Select and click **StorSimple Physical Device Series** and then click **Create**. Alternatively, in the Azure portal click + and then under **Storage**, click **StorSimple Physical Device Series**.



3. In the **StorSimple Device Manager** blade, do the following steps:

- a. Supply a unique **Resource name** for your service. This name is a friendly name that can be used to identify the service. The name can have between 2 and 50 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.
- b. Choose a **Subscription** from the drop-down list. The subscription is linked to your billing account. This field is not present if you have only one subscription.
- c. For **Resource group**, Use existing or Create new group. For more information, see [Azure resource groups](#).
- d. Supply a **Location** for your service. In general, choose a location closest to the geographical region where you want to deploy your device. You may also want to factor in the following considerations:
 - If you have existing workloads in Azure that you also intend to deploy with your StorSimple device, you should use that datacenter.
 - Your StorSimple Device Manager service and Azure storage can be in two separate locations. In such a case, you are required to create the StorSimple Device Manager and Azure storage account separately. To create an Azure storage account, go to the Azure Storage service in the Azure portal and follow the steps in [Create an Azure Storage account](#). After you create this account, add it to the StorSimple Device Manager service by following the steps in [Configure a new storage account for the service](#).
- e. Select **Create a new storage account** to automatically create a storage account with the service. Specify a name for this storage account. If you need your data in a different location, uncheck this box.
- f. Check **Pin to dashboard** if you want a quick link to this service on your dashboard.
- g. Click **Create** to create the StorSimple Device Manager.

StorSimple Device Manager □ X

StorSimple Physical Series

* Resource name
MySS8000DevManager1 ✓

* Subscription
Microsoft Azure Enterprise

* Select a resource group. ⓘ
 Create new Use existing
MySS8000RG1 ✓

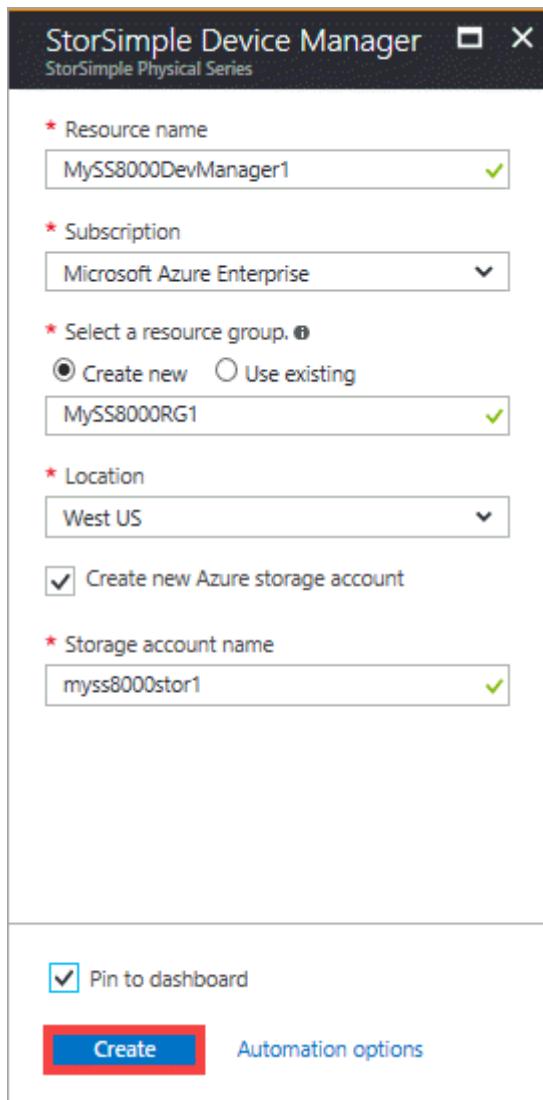
* Location
West US

Create new Azure storage account

* Storage account name
myss8000stor1 ✓

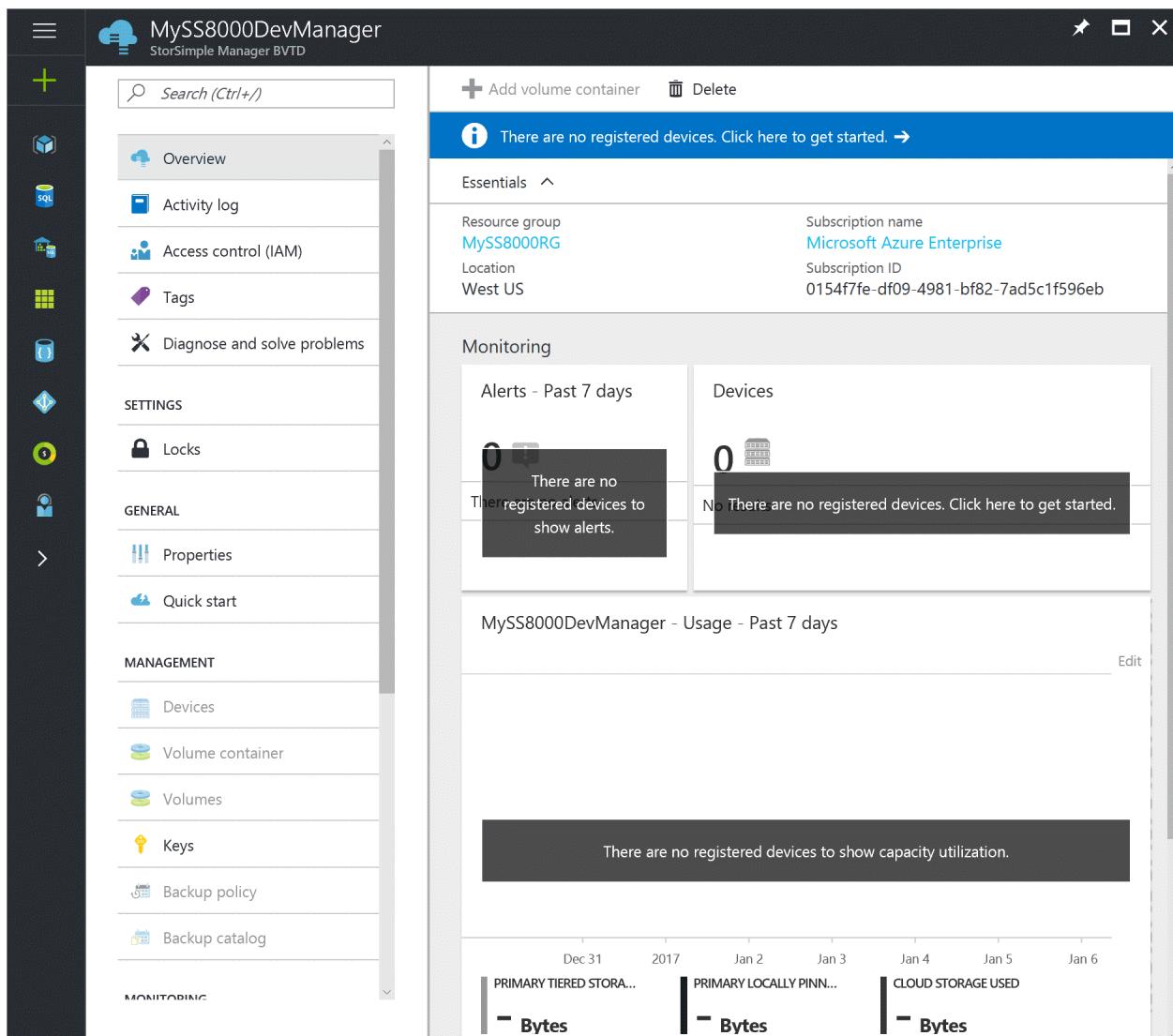
Pin to dashboard

Create Automation options



The screenshot shows the 'Create New Service' blade in the StorSimple Device Manager. It's a step-by-step wizard with several fields and options. At the top, it asks for a 'Resource name' (MySS8000DevManager1) and 'Subscription' (Microsoft Azure Enterprise). Below that, it asks to 'Select a resource group', with the 'Create new' option selected (MySS8000RG1). It also asks for a 'Location' (West US). A checkbox for 'Create new Azure storage account' is checked, and the storage account name is set to 'myss8000stor1'. At the bottom, there's a 'Pin to dashboard' checkbox (also checked) and two buttons: a large red 'Create' button and a smaller 'Automation options' link.

The service creation takes a few minutes. After the service is successfully created, you will see a notification and the new service blade opens up.



For each StorSimple Device Manager service, the following attributes exist:

- **Name** – The name that was assigned to your StorSimple Device Manager service when it was created. **The service name cannot be changed after the service is created. This is also true for other entities such as devices, volumes, volume containers, and backup policies that cannot be renamed in the Azure portal.**
- **Status** – The status of the service, which can be **Active**, **Creating**, or **Online**.
- **Location** – The geographical location in which the StorSimple device will be deployed.
- **Subscription** – The billing subscription that is associated with your service.

Delete a service

Before you delete a service, make sure that no connected devices are using it. If the service is in use, deactivate the connected devices. The deactivate operation will sever the connection between the device and the service, but preserve the device data in the cloud.

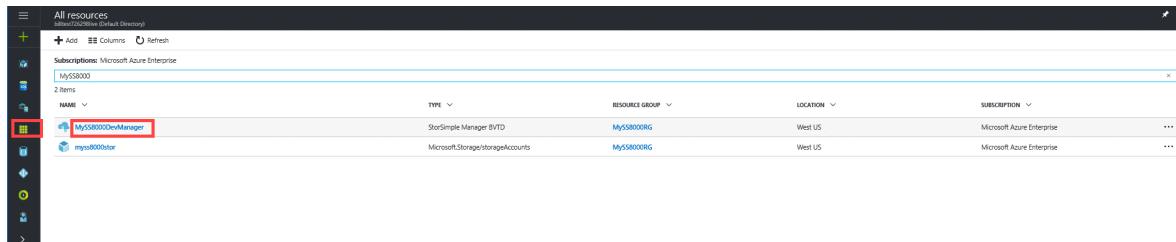
ⓘ Important

After a service is deleted, the operation cannot be reversed. Any device that was using the service needs to be reset to factory defaults before it can be used with another service. In this scenario, the local data on the device, as well as the configuration, is lost.

Perform the following steps to delete a service.

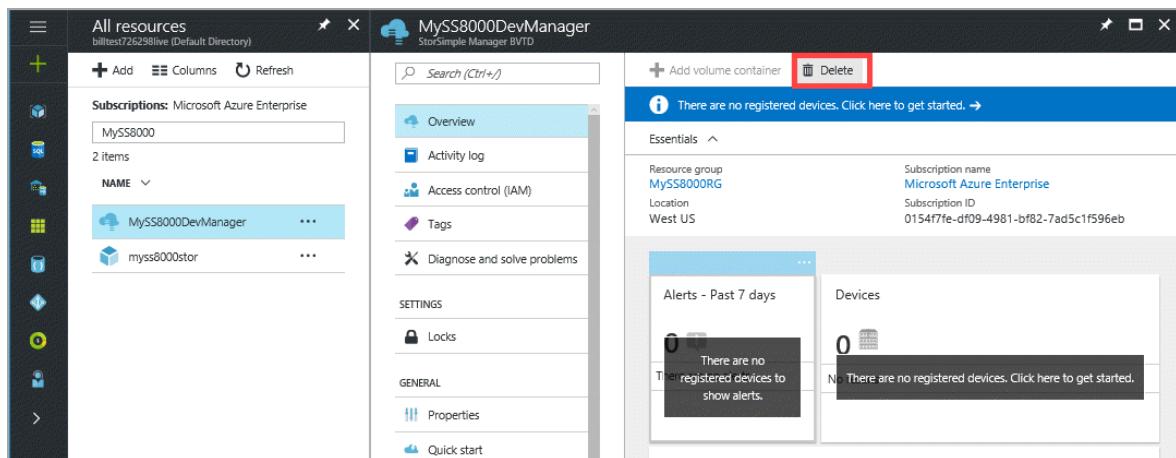
To delete a service

1. Search for the service you want to delete. Click **Resources** icon and then input the appropriate terms to search. In the search results, click the service you want to delete.



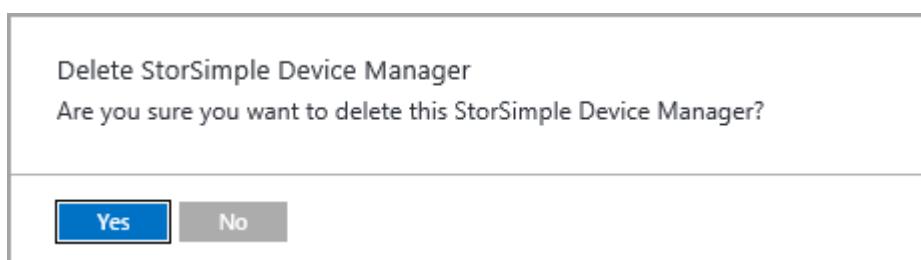
The screenshot shows the Azure portal's 'All resources' blade. A search has been performed for 'MySS8000'. The results table shows two items: 'MySS8000DevManager' (StorSimple Manager BVTD) and 'myss8000stor' (Microsoft.Storage/storageAccounts). The 'MySS8000DevManager' row is selected and highlighted with a red box.

2. This takes you to the StorSimple Device Manager service blade. Click **Delete**.



The screenshot shows the 'MySS8000DevManager' service blade. In the top right corner, there is a 'Delete' button, which is highlighted with a red box. The blade displays basic information about the resource group, location, and subscription.

3. Click **Yes** in the confirmation notification. It may take a few minutes for the service to be deleted.



The screenshot shows a confirmation dialog box. The title is 'Delete StorSimple Device Manager'. The message asks, 'Are you sure you want to delete this StorSimple Device Manager?'. At the bottom, there are two buttons: 'Yes' (highlighted with a red box) and 'No'.

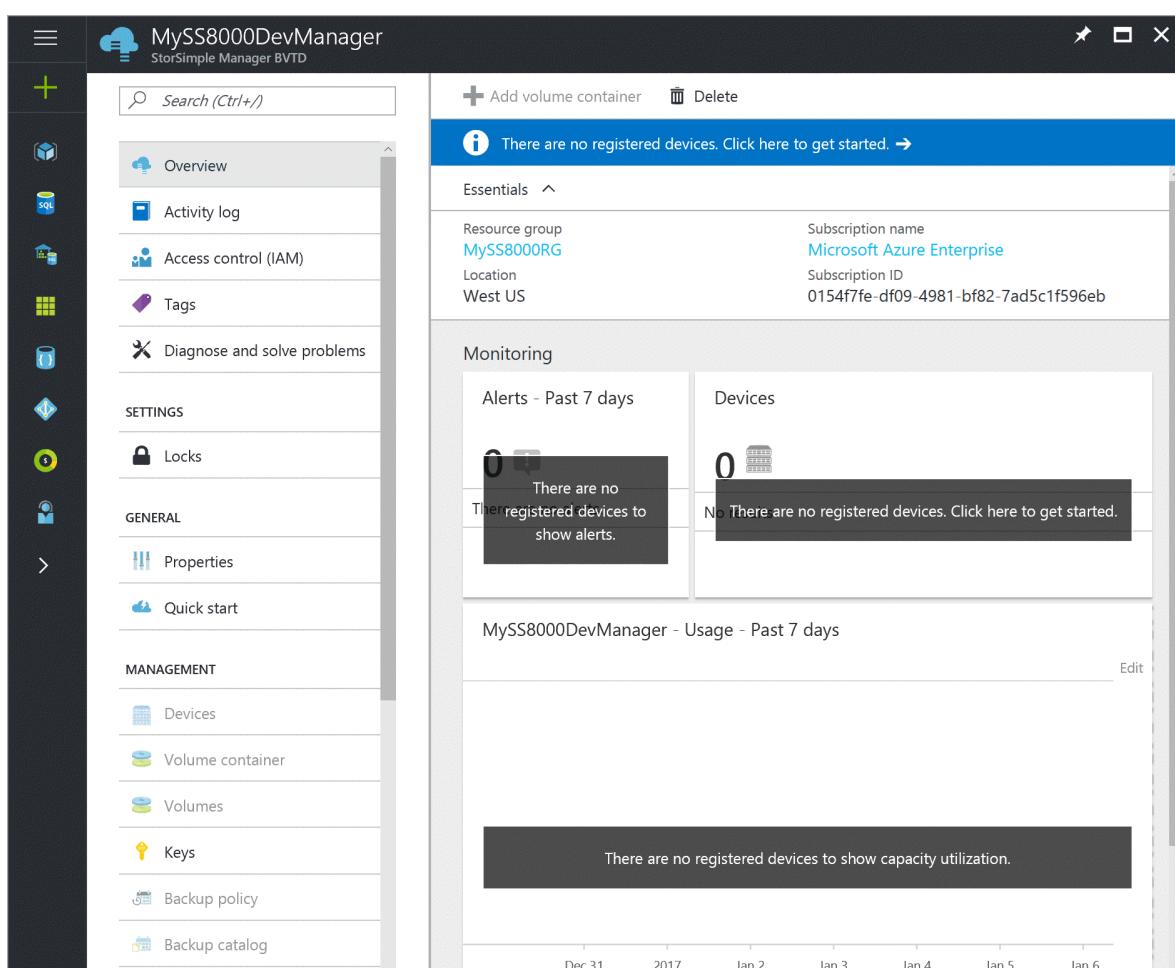
Get the service registration key

After you have successfully created a service, you will need to register your StorSimple device with the service. To register your first StorSimple device, you will need the service registration key. To register additional devices with an existing StorSimple service, you need both the registration key and the service data encryption key (which is generated on the first device during registration). For more information about the service data encryption key, see [StorSimple security](#). You can get the registration key by accessing **Keys** on your StorSimple Device Manager blade.

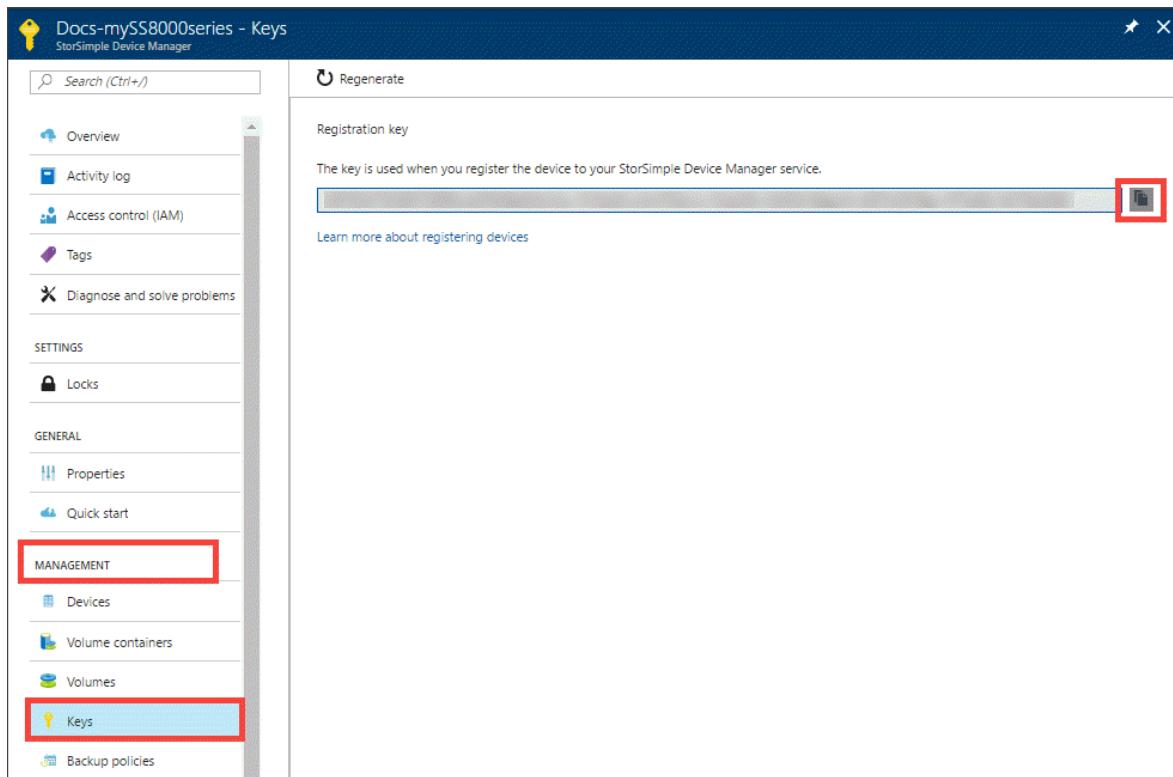
Perform the following steps to get the service registration key.

To get the StorSimple service registration key

1. On the **StorSimple Device Manager** blade, click the service that you created. This opens up a new blade to the right.



2. Go to Management > Keys.



3. In the blade that opens up, click the copy icon to copy the service registration key and save it for later use.

ⓘ Note

The service registration key is used to register all the devices that need to register with your StorSimple Device Manager service.

Keep the service registration key in a safe location. You will need this key, as well as the service data encryption key, to register additional devices with this service. After obtaining the service registration key, you must configure your device through the Windows PowerShell for StorSimple interface.

For details on how to use this registration key, see [Step 3: Configure and register the device through Windows PowerShell for StorSimple](#).

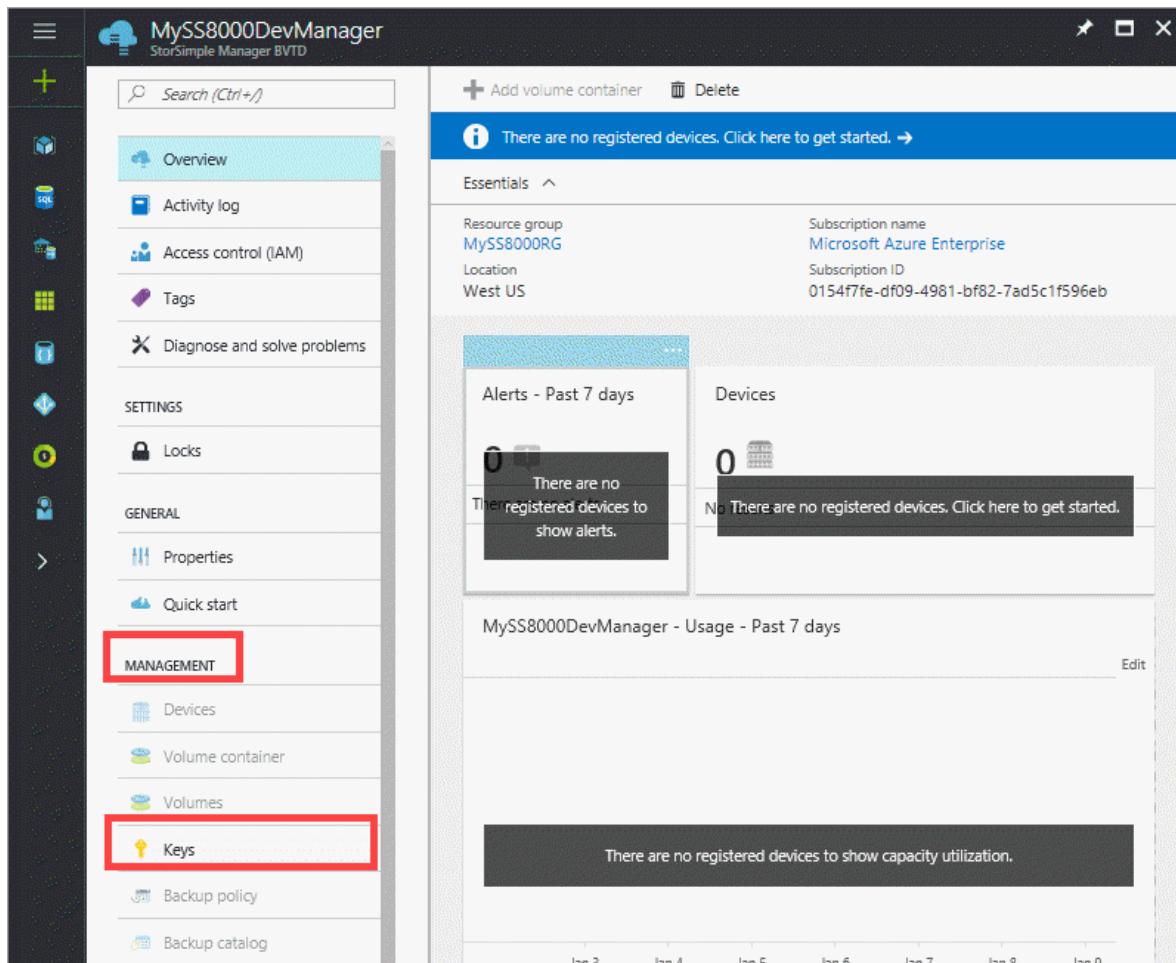
Regenerate the service registration key

You need to regenerate a service registration key if you are required to perform key rotation or if the list of service administrators has changed. When you regenerate the key, the new key is used only for registering subsequent devices. The devices that were already registered are unaffected by this process.

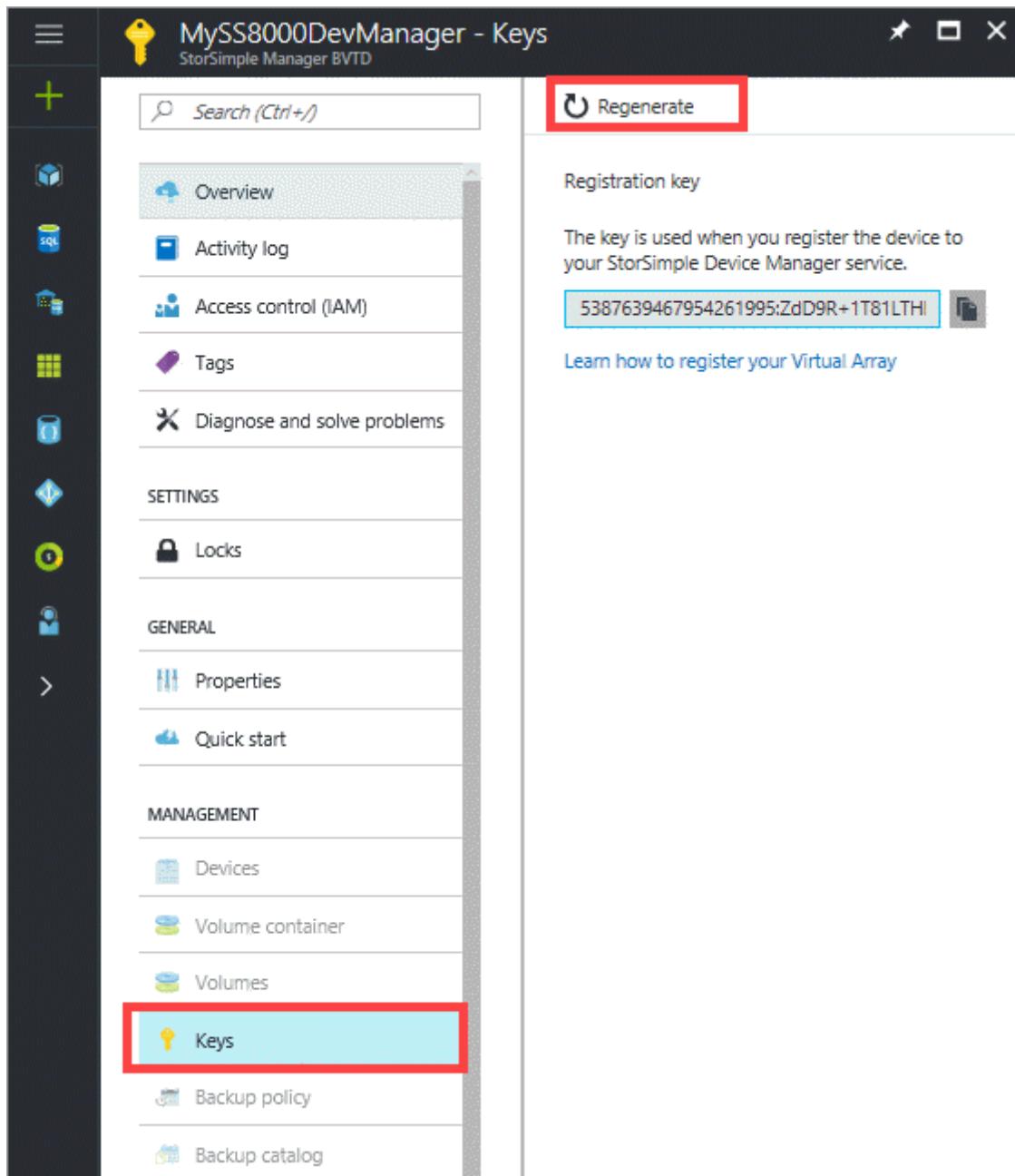
Perform the following steps to regenerate a service registration key.

To regenerate the service registration key

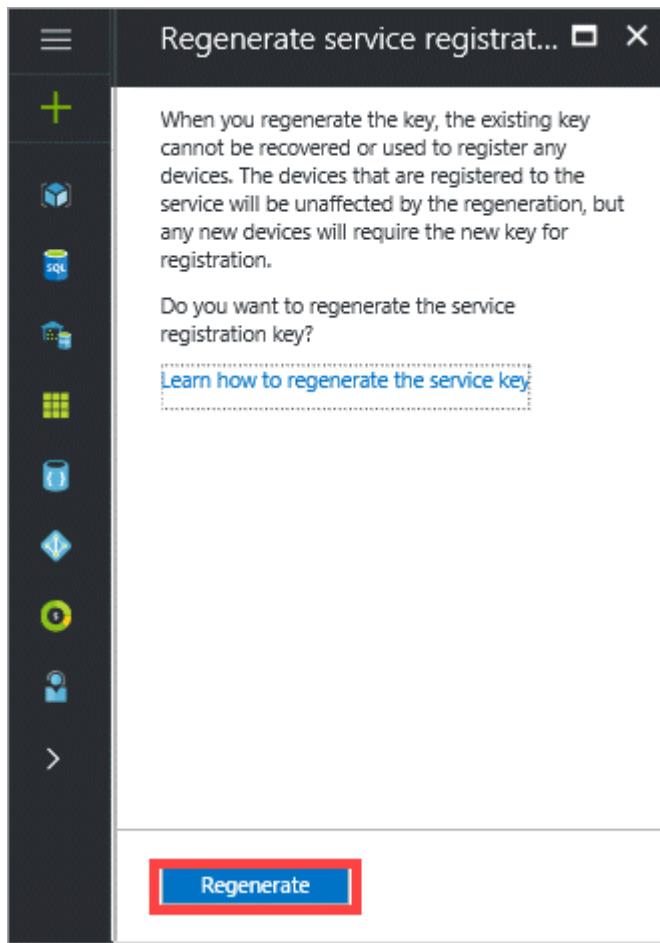
1. In the StorSimple Device Manager blade, go to Management > Keys.



2. In the Keys blade, click Regenerate.



3. In the **Regenerate service registration key** blade, review the action required when the keys are regenerated. All the subsequent devices that are registered with this service use the new registration key. Click **Regenerate** to confirm. You are notified after the regeneration is complete.



Step 1: Use Windows PowerShell script to Authorize a device to change the service data encryption key

Typically, the device administrator will request that the service administrator authorize a device to change service data encryption keys. The service administrator will then authorize the device to change the key.

This step is performed using the Azure Resource Manager based script. The service administrator can select a device that is eligible to be authorized. The device is then authorized to start the service data encryption key change process.

For more information about using the script, go to [Authorize-ServiceEncryptionRollover.ps1](#)

Which devices can be authorized to change service data encryption keys?

A device must meet the following criteria before it can be authorized to initiate service data encryption key changes:

- The device must be online to be eligible for service data encryption key change authorization.
- You can authorize the same device again after 30 minutes if the key change has not been initiated.
- You can authorize a different device, provided that the key change has not been initiated by the previously authorized device. After the new device has been authorized, the old device cannot initiate the change.
- You cannot authorize a device while the rollover of the service data encryption key is in progress.
- You can authorize a device when some of the devices registered with the service have rolled over the encryption while others have not.

Step 2: Use Windows PowerShell for StorSimple to initiate the service data encryption key change

This step is performed in the Windows PowerShell for StorSimple interface on the authorized StorSimple device.

 **Note**

No operations can be performed in the Azure portal of your StorSimple Manager service until the key rollover is completed.

If you are using the device serial console to connect to the Windows PowerShell interface, perform the following steps.

To initiate the service data encryption key change

1. Select option 1 to log on with full access.
2. At the command prompt, type:

```
Invoke-HcsmServiceDataEncryptionKeyChange
```

3. After the cmdlet has successfully completed, you will get a new service data encryption key. Copy and save this key for use in step 3 of this process. This key will be used to update all the remaining devices registered with the StorSimple Manager service.

Note

This process must be initiated within four hours of authorizing a StorSimple device.

This new key is then sent to the service to be pushed to all the devices that are registered with the service. An alert will then appear on the service dashboard. The service will disable all the operations on the registered devices, and the device administrator will then need to update the service data encryption key on the other devices. However, the I/Os (hosts sending data to the cloud) will not be disrupted.

If you have a single device registered to your service, the rollover process is now complete and you can skip the next step. If you have multiple devices registered to your service, proceed to step 3.

Step 3: Update the service data encryption key on other StorSimple devices

These steps must be performed in the Windows PowerShell interface of your StorSimple device if you have multiple devices registered to your StorSimple Manager service. The

key that you obtained in Step 2 must be used to update all the remaining StorSimple device registered with the StorSimple Manager service.

Perform the following steps to update the service data encryption on your device.

To update the service data encryption key on physical devices

1. Use Windows PowerShell for StorSimple to connect to the console. Select option 1 to log on with full access.
2. At the command prompt, type: `Invoke-HcsmServiceDataEncryptionKeyChange -ServiceDataEncryptionKey`
3. Provide the service data encryption key that you obtained in [Step 2: Use Windows PowerShell for StorSimple to initiate the service data encryption key change](#).

To update the service data encryption key on all the 8010/8020 cloud appliances

1. Download and setup [Update-CloudApplianceServiceEncryptionKey.ps1](#) PowerShell script.
2. Open PowerShell and at the command prompt, type: `Update-CloudApplianceServiceEncryptionKey.ps1 -SubscriptionId [subscription] -TenantId [tenantid] -ResourceGroupName [resource group] -ManagerName [device manager]`

This script will ensure that service data encryption key is set on all the 8010/8020 cloud appliances under the device manager.

Supported operations on devices running versions prior to Update 5.0

In the Azure portal, only the StorSimple devices running Update 5.0 and higher are supported. The devices that are running older versions have limited support. After you have migrated to the Azure portal, use the following table to understand which operations are supported on devices running versions prior to Update 5.0.

Operation	Supported
Register a device	Yes
Configure device settings such as general, network, and security	Yes

Operation	Supported
Scan, download, and install updates	Yes
Deactivate device	Yes
Delete device	Yes
Create, modify, and delete a volume container	No
Create, modify, and delete a volume	No
Create, modify, and delete a backup policy	No
Take a manual backup	No
Take a scheduled backup	Not applicable
Restore from a backupset	No
Clone to a device running Update 3.0 and later The source device is running version prior to Update 3.0.	Yes
Clone to a device running versions prior to Update 3.0	No
Failover as source device (from a device running version prior to Update 3.0 to a device running Update 3.0 and later)	Yes
Failover as target device (to a device running software version prior to Update 3.0)	No
Clear an alert	Yes
View backup policies, backup catalog, volumes, volume containers, monitoring charts, jobs, and alerts created in classic portal	Yes
Turn on and off device controllers	Yes

Next steps

- Learn more about the StorSimple deployment process.
- Learn more about [managing your StorSimple storage account](#).
- Learn more about how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Use Azure Active Directory (AD) authentication for your StorSimple

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple devices. To date, StorSimple Device Manager service has used an Access Control service (ACS) to authenticate the service to your StorSimple device. The ACS mechanism will be deprecated soon and replaced by an Azure Active Directory (Azure AD) authentication. For more information, go to the following announcements for ACS deprecation and use of Azure AD authentication.

- [The future of Azure ACS is Azure Active Directory](#)
- [Upcoming changes to the Microsoft Access Control Service](#)

This article describes the details of the Azure AD authentication and the associated new service registration key and modifications to the firewall rules as applicable to the StorSimple devices. The information contained in this article is applicable to StorSimple 8000 series devices only.

The Azure AD authentication occurs in StorSimple 8000 series device running Update 5 or later. Due to the introduction of the Azure AD authentication, changes occur in:

- URL patterns for firewall rules.
- Service registration key.

These changes are discussed in detail in the following sections.

URL changes for Azure AD authentication

To ensure that the service uses Azure AD-based authentication, all the users must include the new authentication URLs in their firewall rules.

If using StorSimple 8000 series, ensure that the following URL is included in the firewall rules:

URL pattern	Cloud	Component/Functionality
<code>https://login.windows.net</code>	Azure Public	Azure AD authentication service
<code>https://login.microsoftonline.us</code>	US Government	Azure AD authentication service

For a complete list of URL patterns for StorSimple 8000 series devices, go to [URL patterns for firewall rules](#).

If the authentication URL is not included in the firewall rules beyond the deprecation date, and the device is running Update 5, the users see a URL alert. The users need to include the new authentication URL. If the device is running a version prior to Update 5, the users see a heartbeat alert. In each case, the StorSimple device cannot authenticate with the service and the service is not able to communicate with the device.

Device version and authentication changes

If using a StorSimple 8000 series device, use the following table to determine what action you need to take based on the device software version you are running.

If your device is running	Take the following action
Update 5.0 or earlier and the device is offline.	Transport Layer Security (TLS) 1.2 is being enforced by the StorSimple Device Manager service. Install Update 5.1 (or higher): <ol style="list-style-type: none">1. Connect to Windows PowerShell on the StorSimple 8000 series device, or connect directly to the appliance via serial cable.2. Use Start-HcsUpdate to update the device. For steps, see Install regular updates via Windows PowerShell. This update is non-disruptive.3. If <code>Start-HcsUpdate</code> doesn't work because of firewall issues, install Update 5.1 (or higher) via the hotfix method.

If your device is running	Take the following action
Update 5 or later and the device is offline. You see an alert that the URL is not approved.	<ol style="list-style-type: none"> 1. Modify the firewall rules to include the authentication URL. See authentication URLs. 2. Get the Azure AD registration key from the service. 3. Connect to the Windows PowerShell interface of the StorSimple 8000 series device. 4. Use <code>Redo-DeviceRegistration</code> cmdlet to register the device through the Windows PowerShell. Supply the key you got in the previous step.
Update 4 or earlier and the device is offline.	<ol style="list-style-type: none"> 1. Modify the firewall rules to include the authentication URL. 2. Download Update 5 through catalog server. 3. Apply Update 5 through the hotfix method. 4. Get the Azure AD registration key from the service. 5. Connect to the Windows PowerShell interface of the StorSimple 8000 series device. 6. Use <code>Redo-DeviceRegistration</code> cmdlet to register the device through the Windows PowerShell. Supply the key you got in the previous step.
Update 4 or earlier and the device is online.	<p>Modify the firewall rules to include the authentication URL. Install Update 5 through the Azure portal.</p>
Factory reset to a version before Update 5.	The portal shows an Azure AD-based registration key while the device is running older software. Follow the steps in the preceding scenario for when the device is running Update 4 or earlier.

Azure AD-based registration keys

Beginning Update 5 for StorSimple 8000 series devices, new Azure AD-based registration keys are used. You use the registration keys to register your StorSimple Device Manager service with the device.

You cannot use the new Azure AD service registration keys if you are using a StorSimple 8000 series device running Update 4 or earlier (includes an older device being activated now). In this scenario, you need to regenerate the service registration key. Once you regenerate the key, the new key is used for registering all the subsequent devices. The old key is no longer valid.

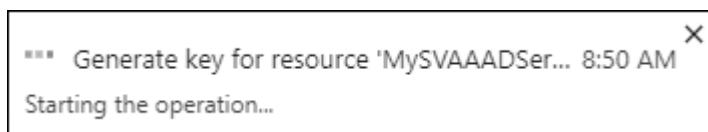
- The new Azure AD registration key expires after 3 days.
- The Azure AD registration keys work only with StorSimple 8000 series devices running Update 5 or later.

- The Azure AD registration keys are longer than the corresponding ACS registration keys.

Perform the following steps to generate an Azure AD service registration key.

To generate the Azure AD service registration key

1. In **StorSimple Device Manager**, go to **Management > Keys**. You can also use the search bar to search for **Keys**.
2. Click **Generate key**.



3. Copy the new key. The older key will no longer work.

The screenshot shows the 'ContosoDeviceMgr - Keys' page. The 'keys' link in the left sidebar is highlighted with a red box and a circled '1'. The main content area has a note about generating a key for Update 5.0. Below it, a 'Generate key' button is highlighted with a red box and a circled '2'. A large red box labeled '3' highlights the 'REGISTRATION KEY' field, which contains a long alphanumeric string: eyJzdWJzY3JpcHRpb25jZC16jlMzJzJlLT4ANGYtNDg3Yi05ZmM0LTBhY2NjOWMwMTY2ZSlnJlc291cmNVHlwZSl6lkNpc1ZhdWxOliwicmVzb3VyY2VOYW1ljoiq29udG9zb0RldmljZU1ncislm1. This key expires on 1/13/2018, 10:35:57 AM and only works with Update 5.0 or later. Copy the key before you close the blade.

ⓘ Note

If you are creating a StorSimple Cloud Appliance on the service registered to your StorSimple 8000 series device, do not generate a registration key while the creation is in progress. Wait for the creation to complete and then generate the registration key.

Next steps

- Learn more about how to deploy [StorSimple 8000 series device](#).

Deploy your on-premises StorSimple device (Update 3 and later)

Article • 03/22/2023 • 26 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Welcome to Microsoft Azure StorSimple device deployment. These deployment tutorials apply to StorSimple 8000 Series Update 3 or later. This series of tutorials includes a configuration checklist, configuration prerequisites, and detailed configuration steps for your StorSimple device.

The information in these tutorials assumes that you have reviewed the safety precautions, and unpacked, racked, and cabled your StorSimple device. If you still need to perform those tasks, start with reviewing the [safety precautions](#). Follow the device-specific instructions to unpack, rack mount, and cable your device.

- [Unpack, rack mount, and cable your 8100](#)
- [Unpack, rack mount, and cable your 8600](#)

You need administrator privileges to complete the setup and configuration process. We recommend that you review the configuration checklist before you begin. The deployment and configuration process can take some time to complete.

ⓘ Note

The StorSimple deployment information published on the Microsoft Azure website applies to StorSimple 8000 series devices only.

Deployment steps

Perform these required steps to configure your StorSimple device and connect it to your StorSimple Device Manager service. In addition to the required steps, there are optional steps and procedures you may need during the deployment. The step-by-step deployment instructions indicate when you should perform each of these optional steps.

Step	Description
PREREQUISITES	These must be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information before and during the deployment.
Deployment prerequisites	These validate the environment is ready for deployment.
STEP-BY-STEP DEPLOYMENT	These steps are required to deploy your StorSimple device in production.
Step 1: Create a new service	Set up cloud management and storage for your StorSimple device. <i>Skip this step if you have an existing service for other StorSimple devices.</i>
Step 2: Get the service registration key	Use this key to register & connect your StorSimple device with the management service.
Step 3: Configure and register the device through Windows PowerShell for StorSimple	To complete the setup using the management service, connect the device to your network and register it with Azure.
Step 4: Complete minimum device setup Best practice: Update your StorSimple device	Use the management service to complete the device setup and enable it to provide storage.
Step 5: Create a volume container	Create a container to provision volumes. A volume container has storage account, bandwidth, and encryption settings for all the volumes contained in it.
Step 6: Create a volume	Provision storage volumes on the StorSimple device for your servers.
Step 7: Mount, initialize, and format a volume Optional: Configure MPIO	Connect your servers to the iSCSI storage provided by the device. Optionally configure MPIO to ensure that your servers can tolerate link, network, and interface failure.
Step 8: Take a backup	Set up your backup policy to protect your data

Step	Description
OTHER PROCEDURES	You may need to refer to these procedures as you deploy your solution.
Configure a new storage account for the service	
Use PuTTY to connect to the device serial console	
Get the IQN of a Windows Server host	
Create a manual backup	

Deployment configuration checklist

Before you deploy your device, you need to collect information to configure the software on your StorSimple device. Preparing some of this information ahead of time helps streamline the process of deploying the StorSimple device in your environment. Download and use this checklist to note down the configuration details as you deploy your device.

- [Download StorSimple deployment configuration checklist ↗](#)

Deployment prerequisites

The following sections explain the configuration prerequisites for your StorSimple Device Manager service and your StorSimple device.

For the StorSimple Device Manager service

Before you begin, make sure that:

- You have your Microsoft account with access credentials.
- You have your Microsoft Azure storage account with access credentials.
- Your Microsoft Azure subscription is enabled for the StorSimple Device Manager service. Your subscription should be purchased through the [Enterprise Agreement ↗](#).
- You have access to terminal emulation software such as PuTTY.

For the device in the datacenter

Before configuring the device, make sure that your device is fully unpacked, mounted on a rack and fully cabled for power, network, and serial access as described in:

- Unpack, rack mount, and cable your 8100 device
- Unpack, rack mount, and cable your 8600 device

For the network in the datacenter

Before you begin, make sure that:

- The ports in your datacenter firewall are opened to allow for iSCSI and cloud traffic as described in [Networking requirements for your StorSimple device](#).

Step-by-step deployment

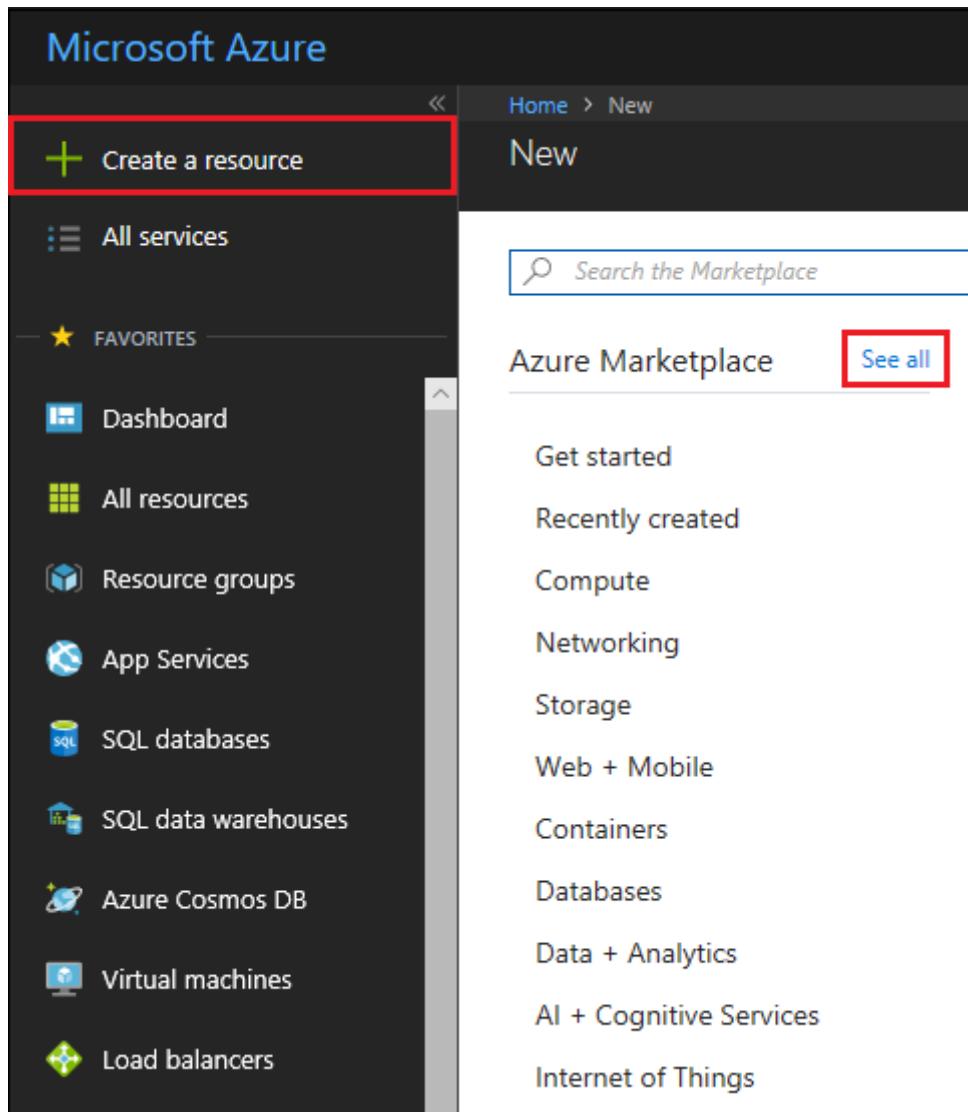
Use the following step-by-step instructions to deploy your StorSimple device in the datacenter.

Step 1: Create a new service

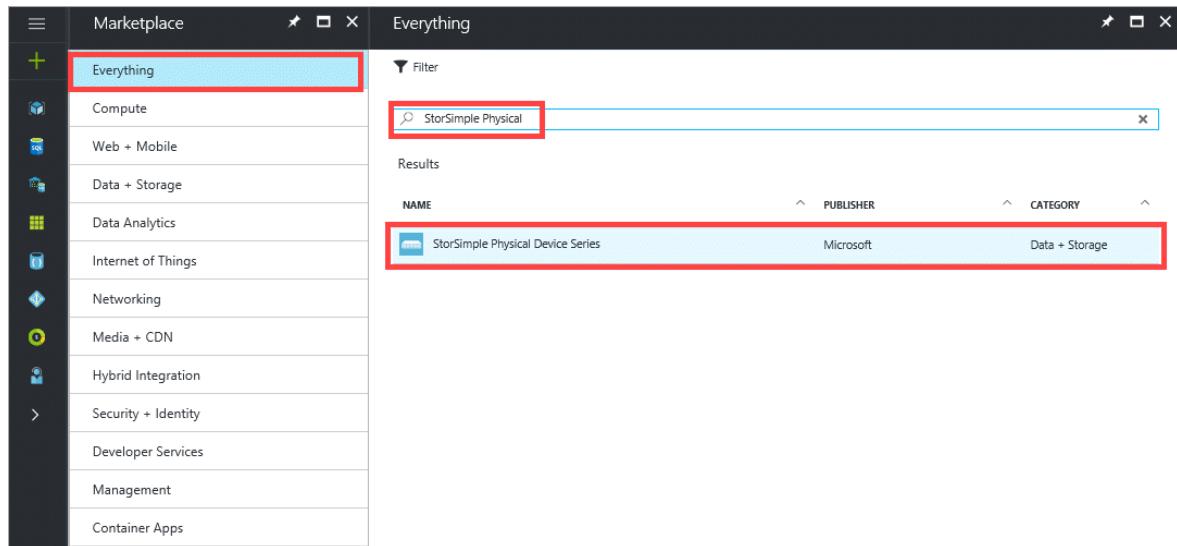
A StorSimple Device Manager service can manage multiple StorSimple devices. Perform the following steps to create an instance of the StorSimple Device Manager service.

To create a new service

1. Use your Microsoft account credentials to sign in to the [Azure portal](#).
2. In the Azure portal, click **Create a resource** and then in the marketplace, click **See all**.



Search for **StorSimple Physical**. Select and click **StorSimple Physical Device Series** and then click **Create**. Alternatively, in the Azure portal click + and then under **Storage**, click **StorSimple Physical Device Series**.



3. In the **StorSimple Device Manager** blade, do the following steps:

- a. Supply a unique **Resource name** for your service. This name is a friendly name that can be used to identify the service. The name can have between 2 and 50 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.
- b. Choose a **Subscription** from the drop-down list. The subscription is linked to your billing account. This field is not present if you have only one subscription.
- c. For **Resource group**, Use existing or Create new group. For more information, see [Azure resource groups](#).
- d. Supply a **Location** for your service. In general, choose a location closest to the geographical region where you want to deploy your device. You may also want to factor in the following considerations:
 - If you have existing workloads in Azure that you also intend to deploy with your StorSimple device, you should use that datacenter.
 - Your StorSimple Device Manager service and Azure storage can be in two separate locations. In such a case, you are required to create the StorSimple Device Manager and Azure storage account separately. To create an Azure storage account, go to the Azure Storage service in the Azure portal and follow the steps in [Create an Azure Storage account](#). After you create this account, add it to the StorSimple Device Manager service by following the steps in [Configure a new storage account for the service](#).
- e. Select **Create a new storage account** to automatically create a storage account with the service. Specify a name for this storage account. If you need your data in a different location, uncheck this box.
- f. Check **Pin to dashboard** if you want a quick link to this service on your dashboard.
- g. Click **Create** to create the StorSimple Device Manager.

StorSimple Device Manager □ X

StorSimple Physical Series

* Resource name
MySS8000DevManager1 ✓

* Subscription
Microsoft Azure Enterprise

* Select a resource group. ⓘ
 Create new Use existing
MySS8000RG1 ✓

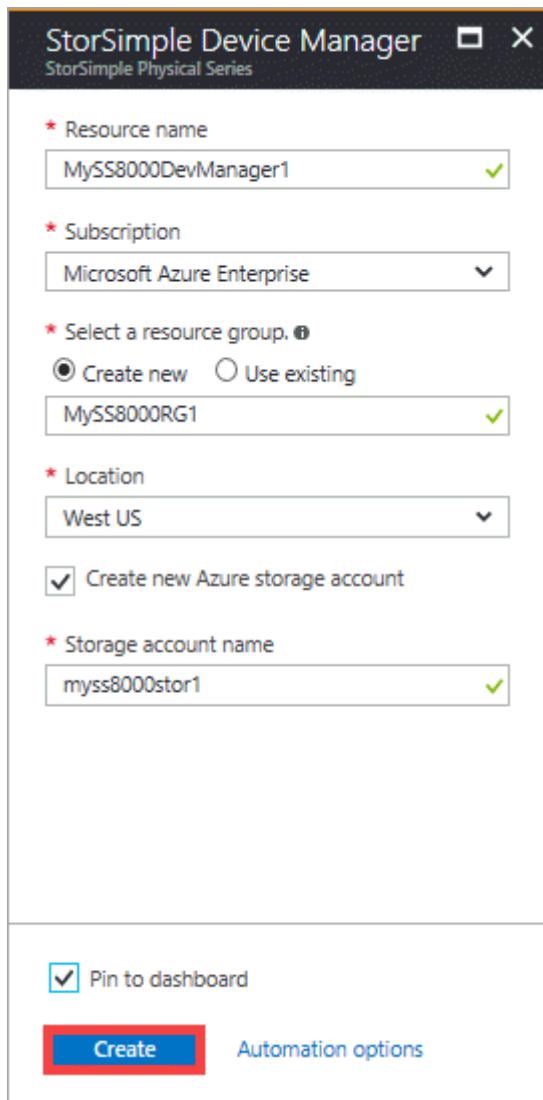
* Location
West US

Create new Azure storage account

* Storage account name
myss8000stor1 ✓

Pin to dashboard

Create Automation options



The service creation takes a few minutes. After the service is successfully created, you will see a notification and the new service blade opens up.

The screenshot shows the StorSimple Manager BVTD application window. The left sidebar contains a search bar and a list of navigation items under four main categories: SETTINGS, GENERAL, MANAGEMENT, and MONITORING. The MONITORING section is currently selected. The main content area displays the 'Essentials' and 'Monitoring' sections. In the Essentials section, it shows a resource group ('MySS8000RG'), location ('West US'), subscription name ('Microsoft Azure Enterprise'), and subscription ID ('0154f7fe-df09-4981-bf82-7ad5c1f596eb'). The Monitoring section includes 'Alerts - Past 7 days' and 'Devices' sections, both of which indicate 'There are no registered devices'. Below these, there is a chart titled 'MySS8000DevManager - Usage - Past 7 days' with three data series: 'PRIMARY TIERED STORA...', 'PRIMARY LOCALLY PINN...', and 'CLOUD STORAGE USED', all showing zero bytes used.

ⓘ Important

If you did not enable the automatic creation of a storage account with your service, you will need to create at least one storage account after you have successfully created a service. This storage account is used when you create a volume container.

- If you did not create a storage account automatically, go to [Configure a new storage account for the service](#) for detailed instructions.
- If you enabled the automatic creation of a storage account, go to [Step 2: Get the service registration key](#).

Step 2: Get the service registration key

After the StorSimple Device Manager service is up and running, you will need to get the service registration key. This key is used to register and connect your StorSimple device with the service.

Perform the following steps in the Azure portal.

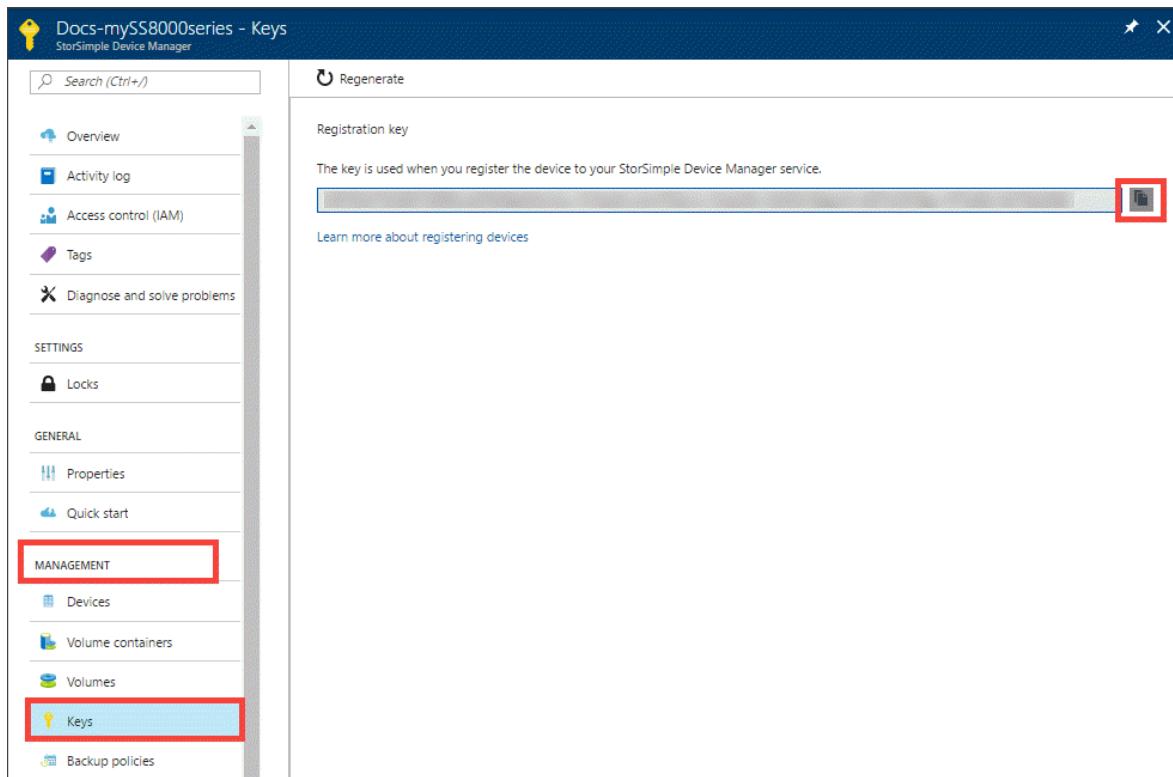
To get the StorSimple service registration key

1. On the **StorSimple Device Manager** blade, click the service that you created. This opens up a new blade to the right.

The screenshot shows the Azure portal interface with the following details:

- Left Sidebar:** Shows various service icons and a search bar labeled "Search (Ctrl+ /)".
- Top Bar:** Displays the title "MySS8000DevManager" and "StorSimple Manager BVTD".
- Overview Tab:** Selected. It contains:
 - "Add volume container" and "Delete" buttons.
 - A message: "There are no registered devices. Click here to get started." with a link icon.
 - Essentials:** Sub-sections include "Resource group MySS8000RG", "Subscription name Microsoft Azure Enterprise", "Location West US", and "Subscription ID 0154f7fe-df09-4981-bf82-7ad5c1f596eb".
 - Monitoring:** Sub-sections include "Alerts - Past 7 days" (0 alerts) and "Devices" (0 devices). Both sections have messages: "There are no registered devices to show alerts." and "No registered devices. Click here to get started." respectively.
 - Usage:** A chart titled "MySS8000DevManager - Usage - Past 7 days" with an "Edit" button. Below the chart, it says "There are no registered devices to show capacity utilization."
- Bottom:** Date range selector showing "Dec 31 2017" to "Jan 6".

2. Go to **Management > Keys**.



3. In the blade that opens up, click the copy icon to copy the service registration key and save it for later use.

① Note

The service registration key is used to register all the devices that need to register with your StorSimple Device Manager service.

Step 3: Configure and register the device through Windows PowerShell for StorSimple

Use Windows PowerShell for StorSimple to complete the initial setup of your StorSimple device as explained in the following procedure. You need to use terminal emulation software to complete this step. For more information, see [Use PuTTY to connect to the device serial console](#).

To configure and register the device

1. Access the Windows PowerShell interface on your StorSimple device serial console. See [Use PuTTY to connect to the device serial console](#) for instructions. Be sure to follow the procedure exactly or you will not be able to access the console.
2. In the session that opens up, press **Enter** one time to get a command prompt.

3. You will be prompted to choose the language that you would like to set for your device. Specify the language, and then press **Enter**.
4. In the serial console menu that is presented, choose option 1, **Log in with full access**. Complete steps 5-12 to configure the minimum required network settings for your device. **These configuration steps need to be performed on the active controller of the device**. The serial console menu indicates the controller state in the banner message. If you are not connected to the active controller, disconnect and then connect to the active controller.
5. At the command prompt, type your password. The default device password is **Password1**.
6. Type the following command: `Invoke-HcsSetupWizard`.
7. A setup wizard will appear to help you configure the network settings for the device. Supply the following information:
 - IP address for the DATA 0 network interface
 - Subnet mask
 - Gateway
 - IP address for Primary DNS server

A sample output is presented below.

```
-----  
Microsoft Azure StorSimple Appliance Model 8100  
Name: 8100-SHX0991003G44MT  
Software Version: 6.3.9600.17759  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller0 - Active  
-----  
  
Your device needs to be registered with the Microsoft Azure  
StorSimple Manager service. Please run 'Invoke-HcsSetupWizard' to set  
up your device.  
  
Controller0>Invoke-HcsSetupWizard  
  
Which IP address family would you like to configure on interface  
Data0?  
[4] IPv4 [6] IPv6 [B] Both (Default is "4"): 4  
  
Data0 IPv4 address:10.111.111.00  
Data0 IPv4 subnet: 255.255.252.0  
Data0 IPv4 gateway: 10.111.111.11
```

```
IPv4 primary DNS server [10.222.118.154]:10.222.222.111
```

In the preceding sample output, you can see that the system is validating network settings after each step in the process.

 **Note**

You may have to wait for a few minutes for the subnet mask and the DNS settings to be applied. If you get a "Check the network connectivity to Data 0" error message, check the physical network connection on the DATA 0 network interface of your active controller.

8. (Optional) configure your web proxy server. Although web proxy configuration is optional, **be aware that if you use a web proxy, you can only configure it here**. For more information, go to [Configure web proxy for your device](#).
9. Configure a Primary NTP server for your device. NTP servers are required, as your device must synchronize time so that it can authenticate with your cloud service providers. Ensure that your network allows NTP traffic to pass from your datacenter to the Internet. If this is not possible, specify an internal NTP server.

A sample output is shown below.

```
Would you like to configure a web proxy?  
[Y] Yes [N] No (Default is "N"):  
N
```

```
Primary NTP server [time.windows.com]:time.windows.com
```

10. For security reasons, the device administrator password expires after the first session, and you will need to change it now. When prompted, provide a device administrator password. A valid device administrator password must be between 8 and 15 characters. The password must contain three of the following: lowercase, uppercase, numeric, and special characters.

The device administrator password must be between 8 and 15 characters. The password must contain a combination of uppercase letters, lowercase letters, numbers and special characters.

```
Administrator Password:*****
Confirm Administrator Password:*****
```

11. The final step in the setup wizard registers your device with the StorSimple Device Manager service. For this, you will need the service registration key that you obtained in step 2. After you supply the registration key, you may need to wait for 2-3 minutes before the device is registered.

 **Note**

You can press Ctrl + C at any time to exit the setup wizard. If you have entered all the network settings (IP address for Data 0, Subnet mask, and Gateway), your entries will be retained.

A sample output is shown below.

```
The service registration key is available in the StorSimple Manager
service.
Enter service registration
key:*****
Device registration is in progress. Please wait.
```

12. After the device is registered, a Service Data Encryption key will appear. Copy this key and save it in a safe location. **This key will be required with the service registration key to register additional devices with the StorSimple Device Manager service.** Refer to [StorSimple security](#) for more information about this key.

```
10.126.82.30 - PuTTY

-----
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17759
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

-----
Your device needs to be registered with the Microsoft Azure StorSimple Manager service. Please run 'Invoke-HcsSetupWizard' to set up your device.

Controller0>Invoke-HcsSetupWizard

Which IP address family would you like to configure on interface Data0?
[4] IPv4 [6] IPv6 [B] Both (Default is "4"): 4

Data0 IPv4 address [10.126.173.90]:
Data0 IPv4 subnet [255.255.252.0]:
Data0 IPv4 gateway [10.126.172.1]:

IPv4 primary DNS server [10.222.118.154]:  
  
Would you like to configure a web proxy?
[Y] Yes [N] No (Default is "N"):  
  
Primary NTP server [time.windows.com]:  
  
The device administrator password must be between 8 and 15 characters. The password must contain a combination of uppercase letters, lowercase letters, numbers and special characters.  
Administrator Password:  
Confirm Administrator Password:  
  
The service registration key is available in the StorSimple Manager service.  
Enter service registration key:  
Device registration is in progress. Please wait.  
  
Congratulations on registering your device with Microsoft Azure StorSimple Manager service! Your service data encryption key is 9Ca5Fmar4t6hlsakGATt1Q==  
WARNING: Please save a copy of this key as it will be required for additional devices that will register with this service.

-----
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17759
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active
```

(!) Note

To copy the text from the serial console window, simply select the text. You should then be able to paste it in the clipboard or any text editor. DO NOT use Ctrl + C to copy the service data encryption key. Using Ctrl + C will cause you to exit the setup wizard. As a result, the device administrator password will not be changed and the device will revert to the default password.

13. Exit the serial console.

14. Return to the Azure portal, and complete the following steps:

- Go to your StorSimple Device Manager service.

- b. Click **Devices**.
- c. In the tabular listing of devices, verify that the device has successfully connected to the service by looking up the status. The device status should be **Ready to set up**.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Ready to set up	8.65 TB/200 TB	Physical device	8100

You may need to wait for a couple of minutes for the device status to change to **Ready to set up**.

If the device does not show up in this list, then you need to make sure that your firewall network was configured as described in [networking requirements for your StorSimple device](#). Verify that port 9354 is open for outbound communication as this is used by the service bus for StorSimple Device Manager service-to-device communication.

Step 4: Complete minimum device setup

For the minimum device configuration of your StorSimple device, you are required to:

- Provide a friendly name for your device.
- Set the device time zone.
- Assign fixed IP addresses to both the controllers.

Perform the following steps in the Azure portal to complete the minimum device setup.

To complete the minimum StorSimple device setup

Note

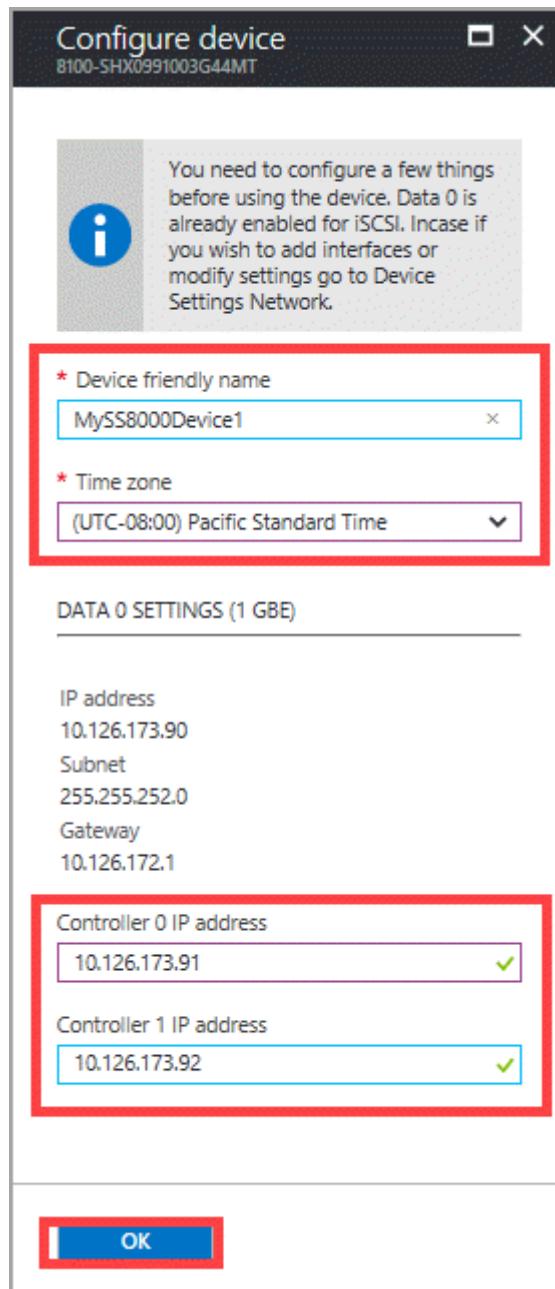
You cannot change the device name once the minimum device setup is completed.

1. From the tabular listing of devices in the **Devices** blade, select and click your device. The device is in a **Ready to set up** state. The **Configure device** blade opens up.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Ready to set up	8.65 TB/200 TB	Physical device	8100

2. In the **Configure device** blade:

- Supply a **friendly name** for your device. The default device name reflects information such as the device model and serial number. You can assign a friendly name of up to 64 characters to manage your device.
- Set the **time zone** based on the geographic location in which the device is being deployed. Your device uses this time zone for all scheduled operations.
- Under the **DATA 0 settings**:
 - Your DATA 0 network interface shows as enabled with the network settings (IP, subnet, gateway) configured via the setup wizard. DATA 0 is also automatically enabled for cloud as well as iSCSI.
 - Provide the fixed IP addresses for Controller 0 and Controller 1. **The controller fixed IP addresses need to be free IPs within the subnet accessible by the device IP address.** If the DATA 0 interface was configured for IPv4, the fixed IP addresses need to be provided in the IPv4 format. If you provided a prefix for IPv6 configuration, the fixed IP addresses are populated automatically in these fields.



The fixed IP addresses for the controller are used for servicing the updates to the device and for garbage collection. Therefore, the fixed IPs must be routable and able to connect to the Internet. You can check that your fixed controller IPs are routable by using the [Test-HcsmConnection](#) cmdlet. The following example shows fixed controller IPs are routed to the Internet and can access the Microsoft Update servers.

```

Microsoft Azure StorSimple Appliance Model 8100
Name: MySS8000Device1
Software Version: 6.3.9600.17759
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

Controller0>Test-HcsmConnection
Checking device registration state ... Success
Device registered successfully

Checking primary IPv4 DNS server [10.222.118.154] ... Success
Checking primary IPv6 DNS server ... NOT SET
Checking secondary IPv4 DNS server ... NOT SET
Checking secondary IPv6 DNS server ... NOT SET

Checking primary NTP server [time.windows.com] ... Success

Checking web proxy ... NOT SET

Checking TCP Port 80 status ... [ Ensure that TCP port 80 is open for outbound traffic on the firewall.] ... Success
Checking TCP Port 443 status ... [ Ensure that TCP port 443 is open for outbound traffic on the firewall.] ... Success
Checking TCP Port 9354 status ... [ Ensure that TCP port 9354 is open for outbound traffic on the firewall.] ... Skipped
Skipped

Checking device online ... Success

Checking device authentication ... This operation will take a few minutes.
Checking device authentication ... Success

Checking connectivity from device to service ... This operation will take a few minutes.
Checking connectivity from device to service ... Success

Checking connectivity from service to device ... Success

Controller0>Checking connectivity to Microsoft update servers ... Success
Controller0>

```

3. Click **OK**. The device configuration starts. When the device configuration is complete, you are notified. The device status changes to **Online** in the **Devices** blade.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERE...)	TYPE	MODEL
MySS8000Device1	Online	8.65 TB/200 TB	Physical device	8100

After you complete the minimum device setup, it is a best practice to [scan for and apply latest updates](#).

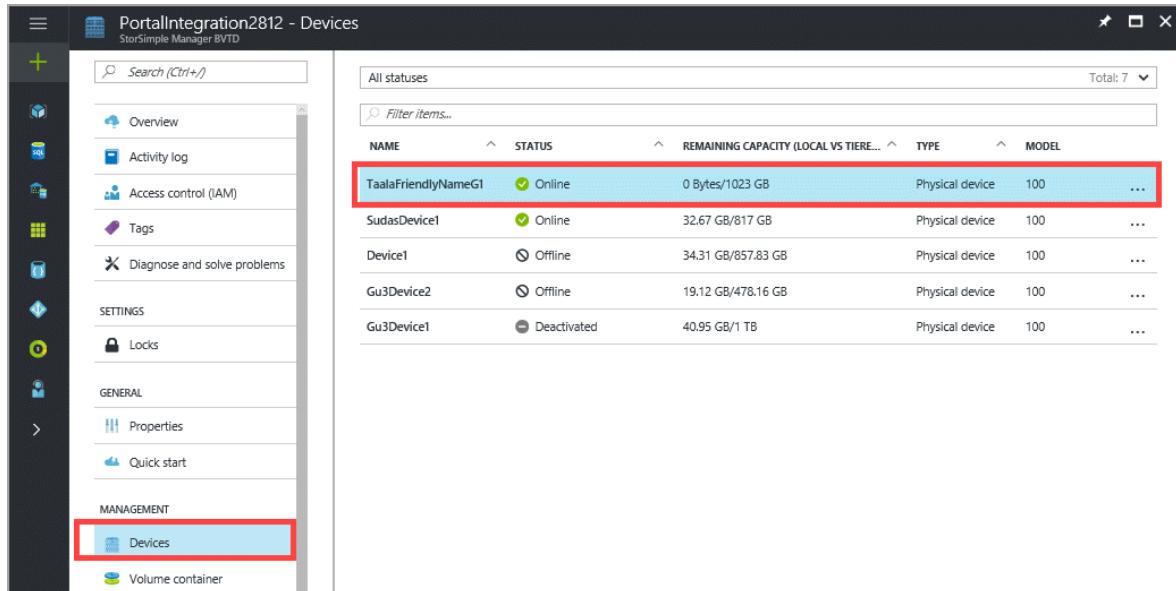
Step 5: Create a volume container

A volume container has storage account, bandwidth, and encryption settings for all the volumes contained in it. You will need to create a volume container before you can start provisioning volumes on your StorSimple device.

Perform the following steps in the Azure portal to create a volume container.

To create a volume container

1. Go to your StorSimple Device Manager service and click **Devices**. From the tabular listing of the devices, select and click a device.



NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL	...
TaalaFriendlyNameG1	Online	0 Bytes/1023 GB	Physical device	100	...
SudasDevice1	Online	32.67 GB/617 GB	Physical device	100	...
Device1	Offline	34.31 GB/857.83 GB	Physical device	100	...
Gu3Device2	Offline	19.12 GB/478.16 GB	Physical device	100	...
Gu3Device1	Deactivated	40.95 GB/1 TB	Physical device	100	...

2. In the device dashboard, click **+ Add volume container**

The screenshot shows the Dell PowerVault Management Suite interface. On the left, the 'Monitoring' section displays various metrics: 4 alerts (3 Critical, 1 Warning) and 1 volume online. Below this is a usage chart for 'TaalaFriendlyNameG1' over the past 24 hours, showing primary tiered storage, locally pinned storage, and cloud storage used. At the bottom, capacity details are shown: 1 GB provisioned, 1023 GB remaining (tiered), and 0 bytes local. On the right, the 'Settings' sidebar is open, showing sections for General, Monitor, Manage, and Device Settings. The 'Volume container' option under 'Manage' is highlighted with a red box.

3. In the **Add volume container** blade:

- The device is automatically selected.
- Supply a **Name** for your volume container. The name must be 3 to 32 characters long. You cannot rename a volume container once it is created.
- Select **Enable Cloud Storage Encryption** to enable encryption of the data sent from the device to the cloud.
- Provide and confirm a **Cloud Storage Encryption Key** that is 8 to 32 characters long. This key is used by the device to access encrypted data.
- Select a **Storage Account** to associate with this volume container. You can choose an existing storage account or the default account that is generated at

the time of service creation. You can also use the **Add new** option to specify a storage account that is not linked to this service subscription.

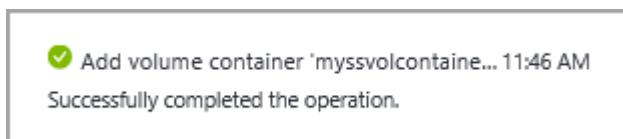
- f. Select **Unlimited** in the **Specify bandwidth** drop-down list if you wish to consume all the available bandwidth.

If you have your bandwidth usage information available, you may be able to allocate bandwidth based on a schedule by specifying **Select a bandwidth template**. For a step-by-step procedure, go to [Add a bandwidth template](#).

The screenshot shows the 'Add volume container' dialog box. It includes fields for 'Select device' (set to 'myss8000device'), 'Volume container name' (set to 'myssvolcont1'), 'Cloud storage encryption' (set to 'Enabled'), 'Encryption key' (redacted), 'Confirm encryption key' (redacted), 'Storage account credential' (set to '11d3d4e0ead6412bb0419'), and 'Bandwidth setting' (set to 'Unlimited'). The 'Create' button is at the bottom.

- g. Click **Create**.

You are notified when the volume container is successfully created.



The newly created volume container is listed in the list of volume containers for your device.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and has a sidebar with the following menu items:

- GENERAL
 - Properties
- MONITOR
 - Capacity
 - Usage
 - Performance
 - Jobs
 - Alerts
- MANAGE
 - Volumes
 - Volume container
 - Backup policy
 - Backup catalog

The 'Volume container' item is highlighted with a blue background. The right window is titled 'Volume container' and shows a table of volume containers for a device named 'SudasDevice1'. The table has columns: NAME, VOLUMES, CLOUD ST..., BANDWID..., and STORAGE... . There are three entries:

NAME	VOLUMES	CLOUD ST...	BANDWID...	STORAGE...
VC1	9	NA	0	portalintegrati... ...
myssvolcontainer1	0	NA	0	localizetest ...
vc2	2	NA	0	portalintegrati... ...

The row for 'myssvolcontainer1' is highlighted with a red box.

Step 6: Create a volume

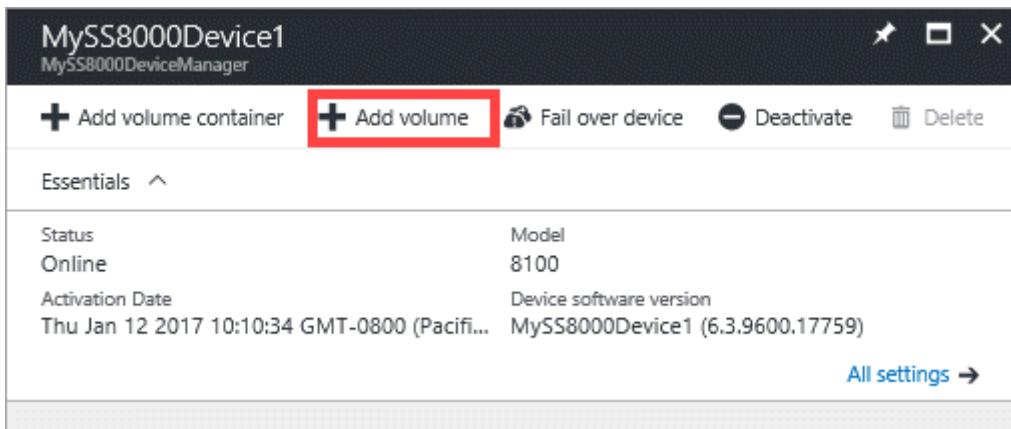
After you create a volume container, you can provision a storage volume on the StorSimple device for your servers. Perform the following steps in the Azure portal to create a volume.

ⓘ Important

StorSimple Device Manager can create both thin and fully provisioned volumes. You cannot however create partially provisioned volumes.

To create a volume

1. From the tabular listing of the devices in the **Devices** blade, select your device.
Click **+ Add volume**.



2. In the **Add a volume** blade:

- a. The **Select device** field is automatically populated with your current device.
- b. From the drop-down list, select the volume container where you need to add a volume.
- c. Type a **Name** for your volume. You cannot rename a volume once the volume is created.
- d. On the drop-down list, select the **Type** for your volume. For workloads that require local guarantees, low latencies, and higher performance, select a **Locally pinned** volume. For all other data, select a **Tiered** volume. If you are using this volume for archival data, check **Use this volume for less frequently accessed archival data**.

A tiered volume is thinly provisioned and can be created quickly. Selecting **Use this volume for less frequently accessed archival data** for tiered volume targeted for archival data changes the deduplication chunk size for your volume to 512 KB. If this field is not checked, the corresponding tiered volume uses a chunk size of 64 KB. A larger deduplication chunk size allows the device to expedite the transfer of large archival data to the cloud.

A locally pinned volume is thickly provisioned and ensures that the primary data on the volume stays local to the device and does not spill to the cloud. If you create a locally pinned volume, the device checks for available space on the local tiers to provision the volume of the requested size. The operation of creating a locally pinned volume may involve spilling existing data from the device to the cloud and the time taken to create the volume may be long. The total time depends on the size of the provisioned volume, available network bandwidth, and the data on your device.

- e. Specify the **Provisioned Capacity** for your volume. Make a note of the capacity that is available based on the volume type selected. The specified volume size

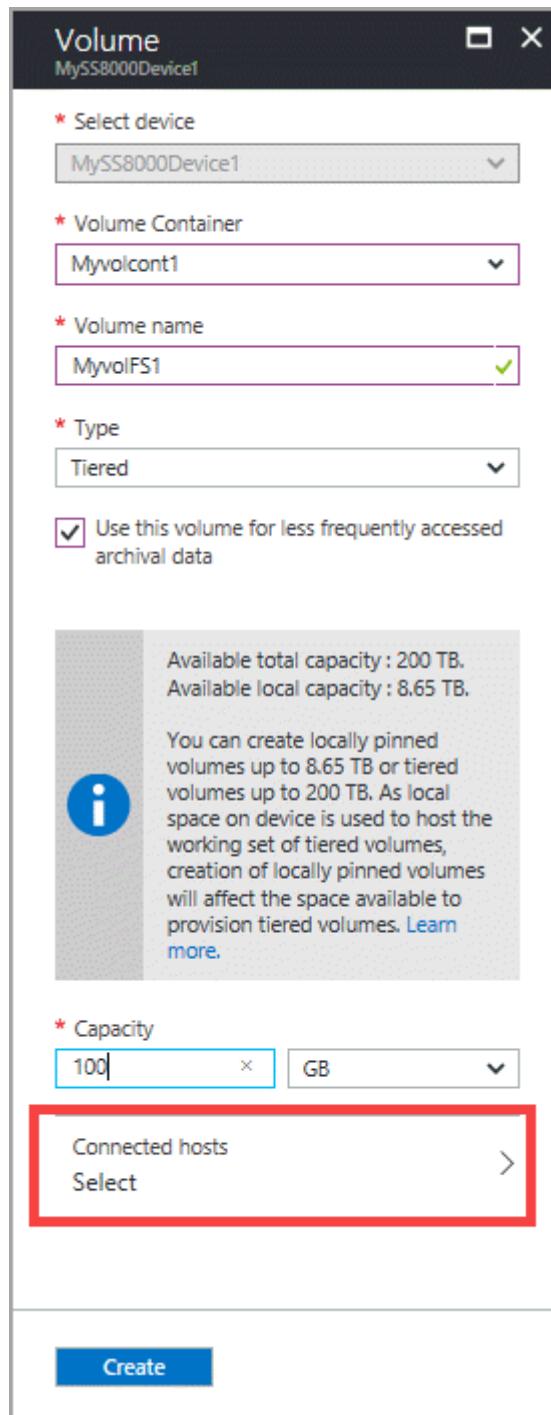
must not exceed the available space.

You can provision locally pinned volumes up to 8.5 TB or tiered volumes up to 200 TB on the 8100 device. On the larger 8600 device, you can provision locally pinned volumes up to 22.5 TB or tiered volumes up to 500 TB. As local space on the device is required to host the working set of tiered volumes, creation of locally pinned volumes impacts the space available for provisioning tiered volumes. Therefore, if you create a locally pinned volume, space available for creation of tiered volumes is reduced. Similarly, if a tiered volume is created, the available space for creation of locally pinned volumes is reduced.

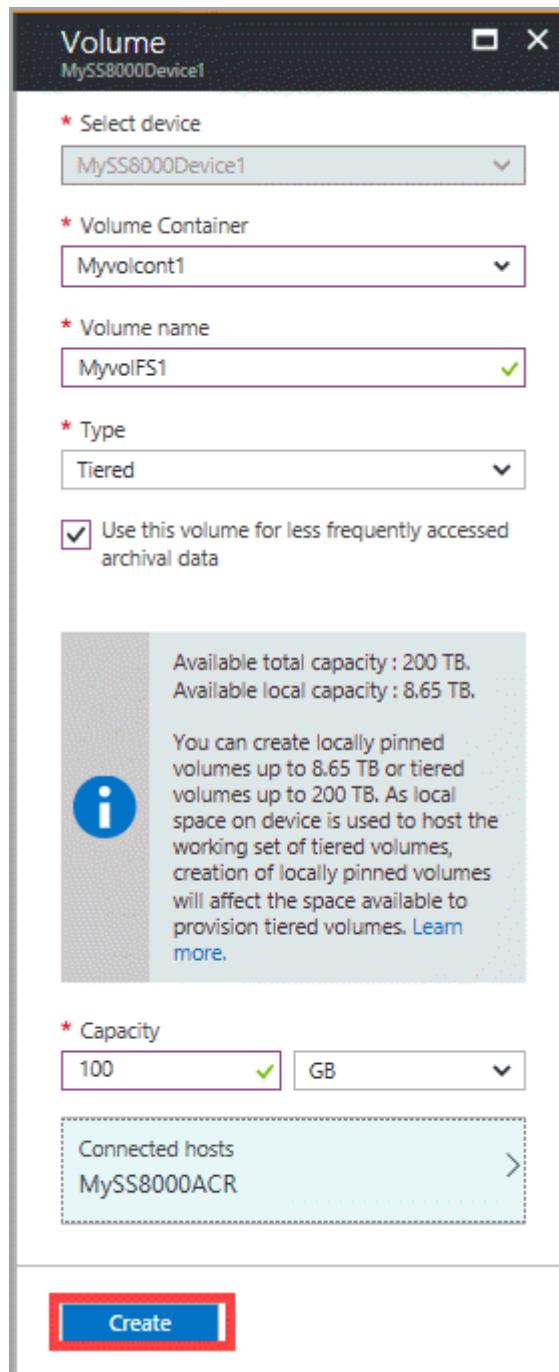
If you provision a locally pinned volume of 8.5 TB (maximum allowable size) on your 8100 device, then you have exhausted all the local space available on the device. You can't create any tiered volume from that point onwards as there is no local space on the device to host the working set of the tiered volume.

Existing tiered volumes also affect the space available. For example, if you have an 8100 device that already has tiered volumes of roughly 106 TB, only 4 TB of space is available for locally pinned volumes.

- i. In the **Connected hosts** field, click the arrow.



- ii. In the **Connected hosts** blade, choose an existing ACR or add a new ACR by performing the following steps:
 - i. Supply a **Name** for your ACR.
 - ii. Under **iSCSI Initiator Name**, provide the iSCSI Qualified Name (IQN) of your Windows host. If you don't have the IQN, go to [Get the IQN of a Windows Server host](#).
- iii. Click **Create**. A volume is created with the specified settings.



ⓘ Note

Be aware that the volume you have created here is not protected. You will need to create and associate backup policies with this volume to take scheduled backups.

Step 7: Mount, initialize, and format a volume

The following steps are performed on your Windows Server host.

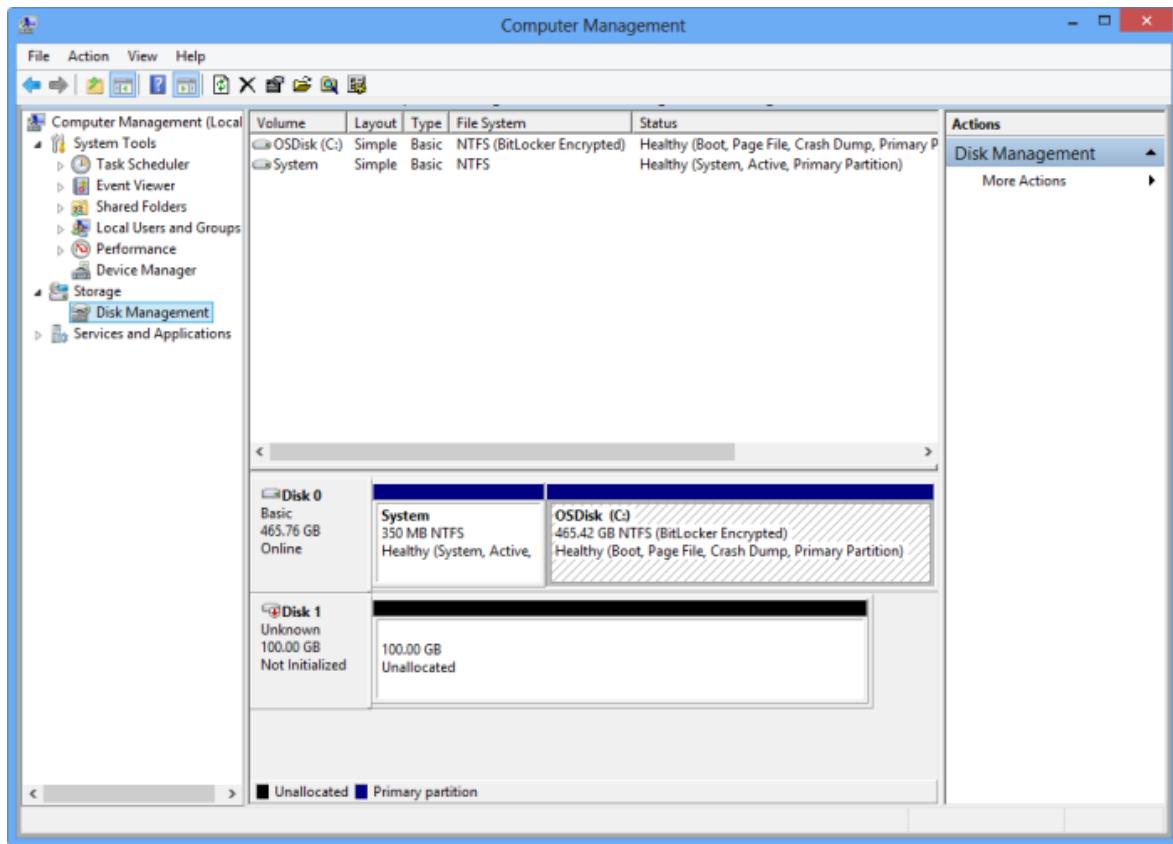
ⓘ Important

- For the high availability of your StorSimple solution, we recommend that you configure MPIO on your host servers (optional) prior to configuring iSCSI. MPIO configuration on host servers will ensure that the servers can tolerate a link, network, or interface failure.
- For MPIO and iSCSI installation and configuration instructions on Windows Server host, go to [Configure MPIO for your StorSimple device](#). These also include the steps to mount, initialize, and format StorSimple volumes.
- For MPIO and iSCSI installation and configuration instructions on a Linux host, go to [Configure MPIO for your StorSimple Linux host](#)

If you decide not to configure MPIO, perform the following steps to mount, initialize, and format your StorSimple volumes on a Windows Server host.

To mount, initialize, and format a volume

1. Start the Microsoft iSCSI initiator.
2. In the **iSCSI Initiator Properties** window, on the **Discovery** tab, click **Discover Portal**.
3. In the **Discover Target Portal** dialog box, supply the IP address of your iSCSI-enabled network interface, and then click **OK**.
4. In the **iSCSI Initiator Properties** window, on the **Targets** tab, locate the **Discovered targets**. The device status should appear as **Inactive**.
5. Select the target device and then click **Connect**. After the device is connected, the status should change to **Connected**. (For more information about using the Microsoft iSCSI initiator, see [Installing and Configuring Microsoft iSCSI Initiator](#)).
6. On your Windows host, press the Windows Logo key + X, and then click **Run**.
7. In the **Run** dialog box, type **Diskmgmt.msc**. Click **OK**, and the **Disk Management** dialog box will appear. The right pane will show the volumes on your host.
8. In the **Disk Management** window, the mounted volumes will appear as shown in the following illustration. Right-click the discovered volume (click the disk name), and then click **Online**.



9. Right-click the volume (click the disk name) again, and then click **Initialize**.
10. To format a simple volume, perform the following steps:
 - a. Select the volume, right-click it (click the right area), and click **New Simple Volume**.
 - b. In the New Simple Volume wizard, specify the volume size and drive letter and configure the volume as an NTFS file system.
 - c. Specify a 64 KB allocation unit size. This allocation unit size works well with the deduplication algorithms used in the StorSimple solution.
 - d. Perform a quick format.

Step 8: Take a backup

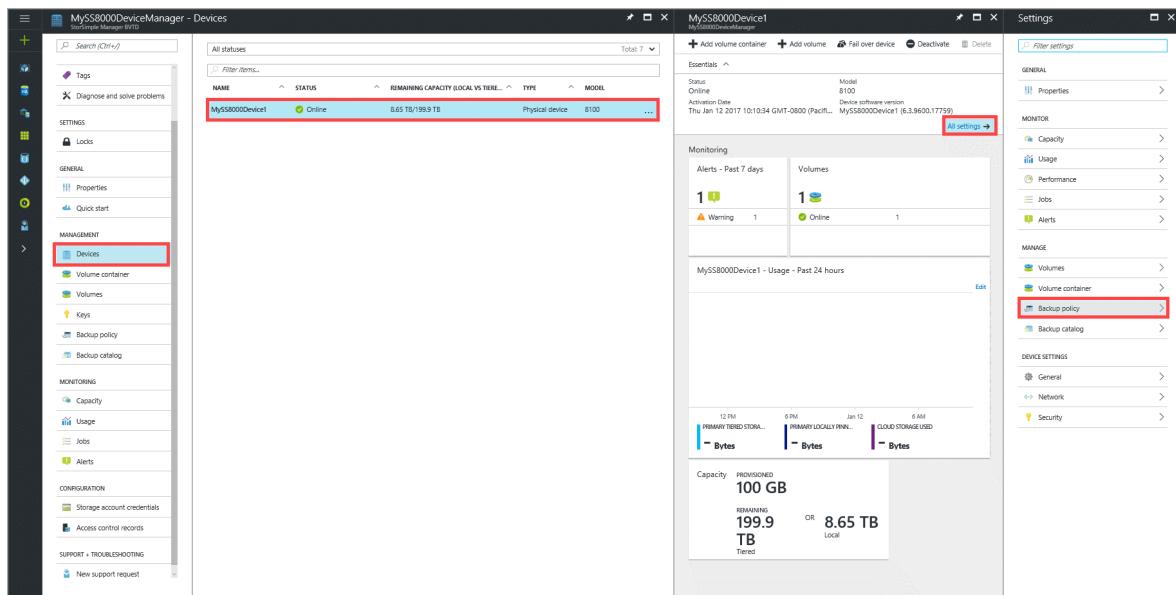
Backups provide point-in-time protection of volumes and improve recoverability while minimizing restore times. You can take two types of backup on your StorSimple device: local snapshots and cloud snapshots. Each of these backup types can be **Scheduled** or **Manual**.

Perform the following steps in the Azure portal to create a scheduled backup.

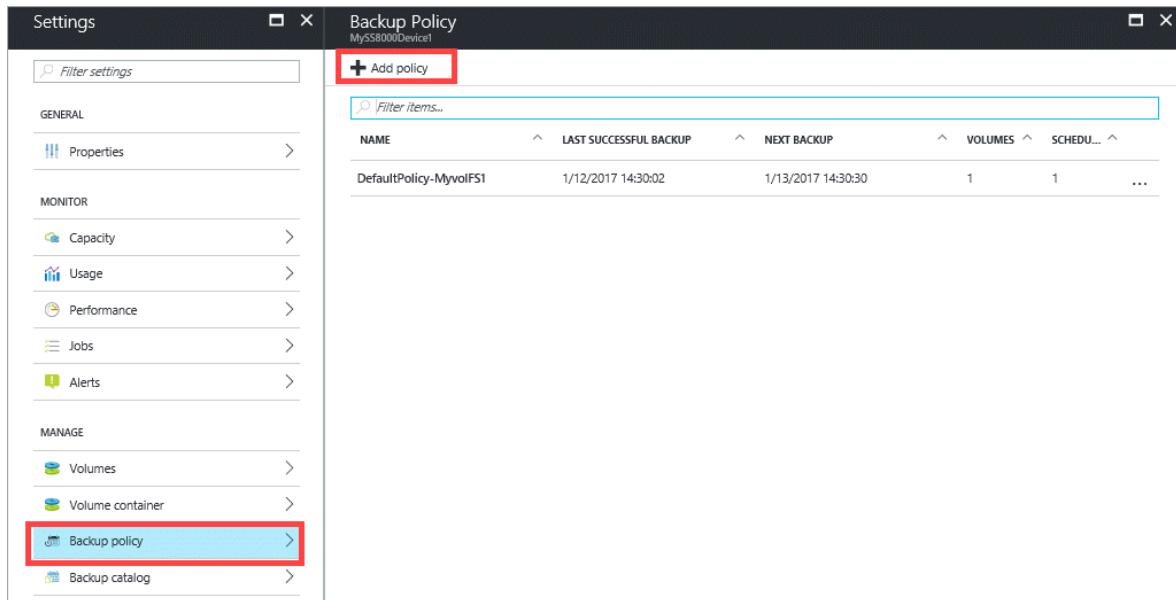
To take a backup

1. Go to your StorSimple Device Manager service. From the tabular listing of devices, select and click your device and then click **All settings**. In the **Settings** blade, go to

Settings > Manage > Backup policy.

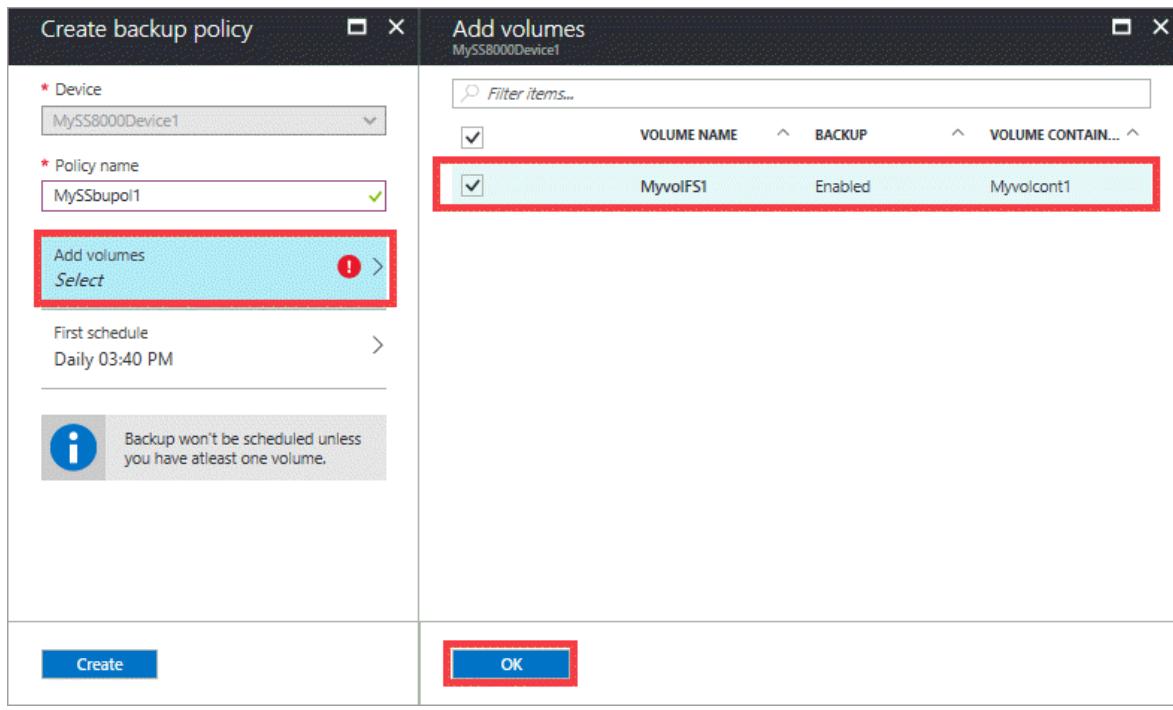


2. In the Backup policy blade, click + Add policy.



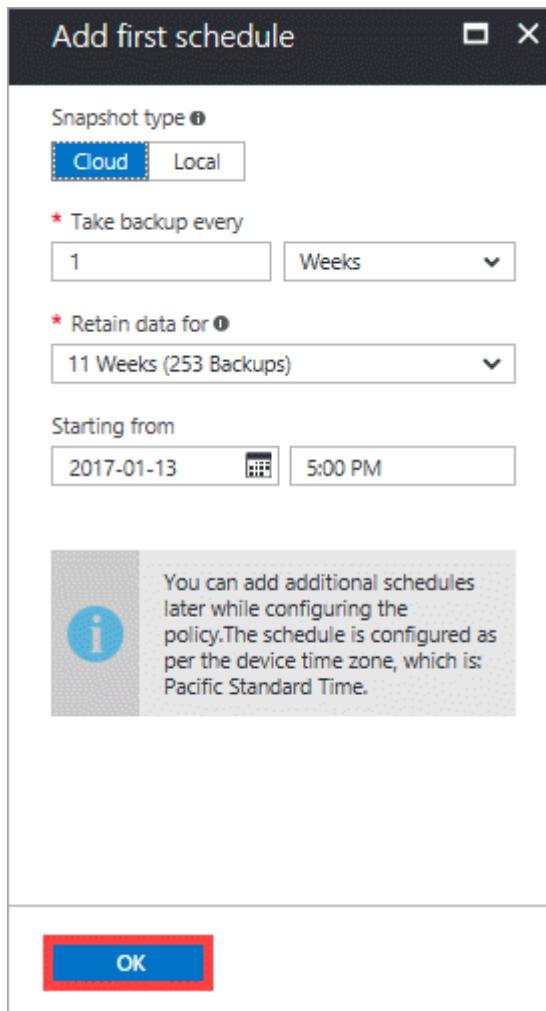
3. In the Create backup policy blade, supply a name that contains between 3 and 150 characters for your backup policy.

4. Select the volumes to be backed up. If you select more than one volume, these volumes are grouped together to create a crash-consistent backup.



5. On Add first schedule blade:

- a. Select the type of backup. For faster restores, select **Local** snapshot. For data resiliency, select **Cloud** snapshot.
- b. Specify the backup frequency in minutes, hours, days, or weeks.
- c. Select a retention time. The retention choices depend on the backup frequency. For example, for a daily policy, the retention can be specified in weeks, whereas retention for a monthly policy is in months.
- d. Select the starting time and date for the backup policy.
- e. Click **OK** to create the backup policy.



6. Click **Create** to start the backup policy creation. You are notified when the backup policy is successfully created. The list of backup policies is also updated.

NAME	LAST SUCCESSFUL BACKUP	VOLUMES	SCHEDULING
MySSbupol1	1/13/2017 17:00:00	1	1
DefaultPolicy-MyvolFS1	1/12/2017 14:30:02	1	1

You now have a backup policy that creates scheduled backups of your volume data.

You can take a manual backup at any time. For procedures, go to [Create a manual backup](#).

You have completed the device configuration.

Configure a new storage account for the service

This is an optional step that you need to perform only if you did not enable the automatic creation of a storage account with your service. A Microsoft Azure storage account is required to create a StorSimple volume container.

If you need to create an Azure storage account in a different region, see [About Azure Storage Accounts](#) for step-by-step instructions.

Perform the following steps in the Azure portal, on the **StorSimple Device Manager service** page.

To add a storage account credential in the same Azure subscription as the StorSimple Device Manager service

1. Go to your StorSimple Device Manager service. In the **Configuration** section, click **Storage account credentials**.

The screenshot shows the Azure portal interface for the resource group 'MySS8000RG'. The left sidebar contains a navigation menu with various icons and links. The 'Storage account credentials' link is highlighted with a red box.

Essentials

- Resource group: MySS8000RG
- Subscription name: Microsoft Azure Enterprise
- Location: West US
- Subscription ID: 0154f7fe-df09-4981-bf82-7ad5c1f596eb

Alerts - Past 7 days

Category	Count
Warning	1

Devices

Status	Count
Online	1

MySS8000DeviceManager - Usage - Past 7 days

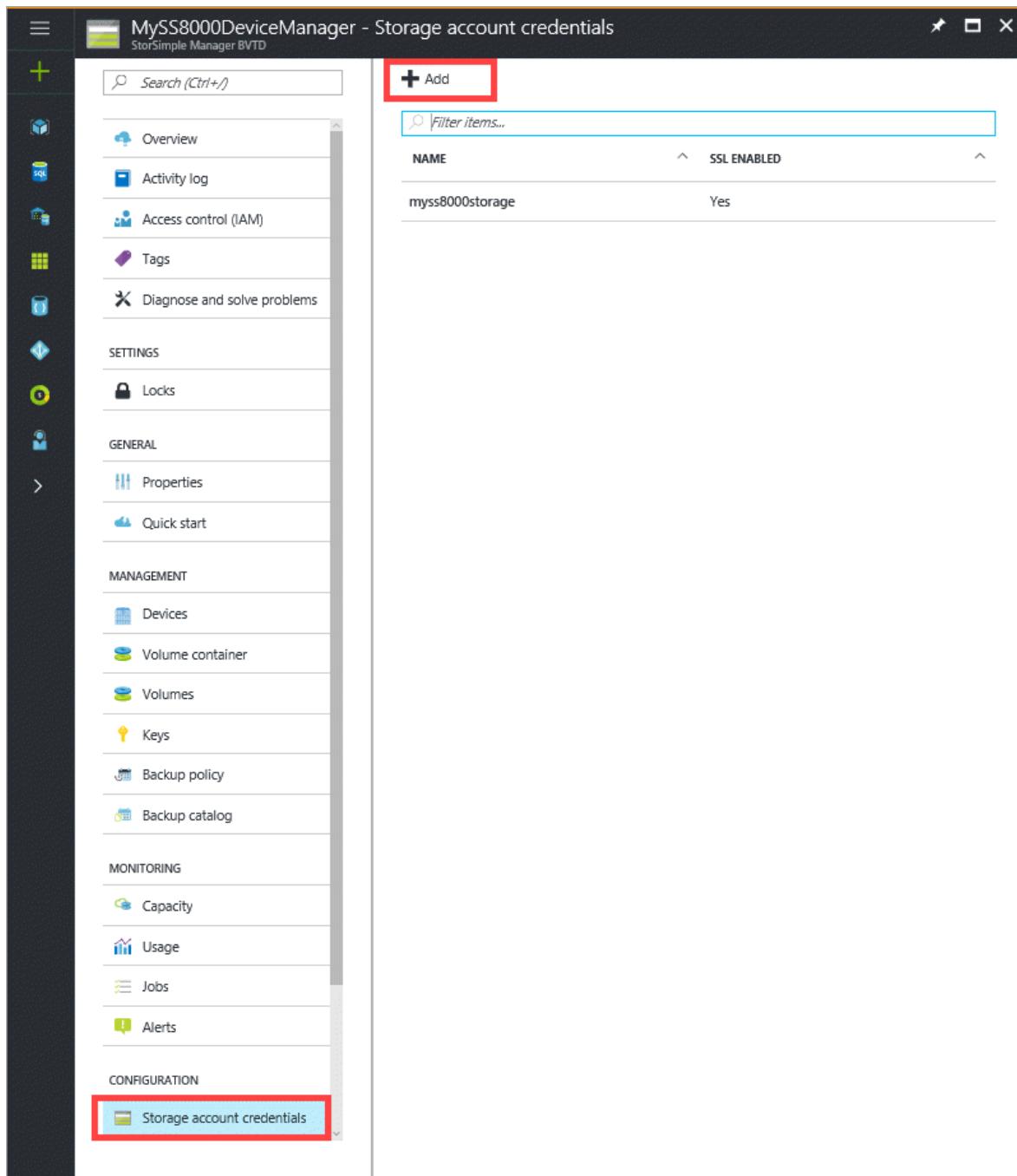
Jan 11 Jan 12 Jan 13 Jan 14 Jan 15 Jan 16 Jan 17

PRIMARY TIERED STORAGE - Bytes PRIMARY LOCALLY PINNED - Bytes CLOUD STORAGE USED - Bytes

Capacity PROVISIONED **300 GB**

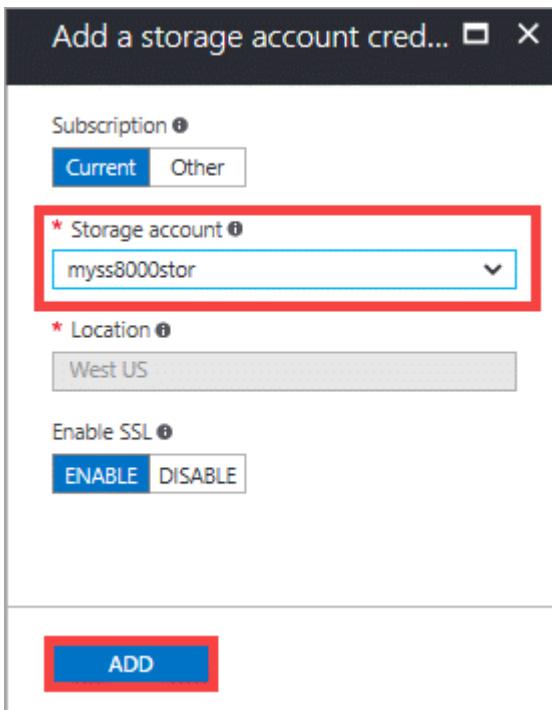
REMAINING **199.7 TB** **Tiered** OR **8.64 TB Local**

2. On the **Storage account credentials** blade, click **+ Add**.



3. In the **Add a storage account credential** blade, do the following steps:

- a. As you are adding a storage account credential in the same Azure subscription as your service, ensure that **Current** is selected.
- b. From the **storage account** dropdown list, select an existing storage account.
- c. Based on the storage account selected, the **location** will be displayed (grayed out and cannot be changed here).
- d. Select **Enable SSL Mode** to create a secure channel for network communication between your device and the cloud. Disable **Enable SSL** only if you are operating within a private cloud.



- e. Click **Add** to start the job creation for the storage account credential. You will be notified after the storage account credential is successfully created.

Add storage account credential 'myss80... 1:34 PM
Successfully completed the operation.

The newly created storage account credential will be displayed under the list of **Storage account credentials**.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	Yes

Use PuTTY to connect to the device serial console

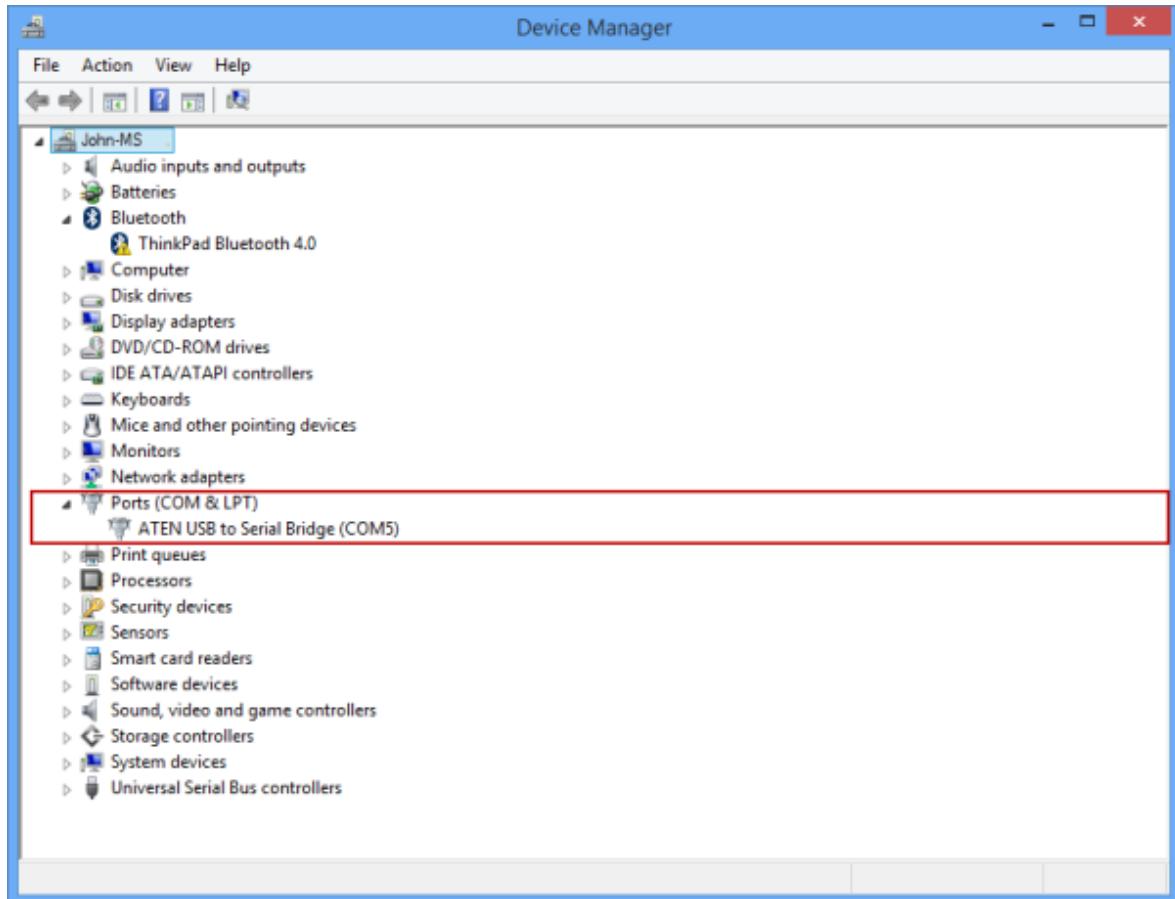
To connect to Windows PowerShell for StorSimple, you need to use terminal emulation software such as PuTTY. You can use PuTTY when you access the device directly through the serial console or by opening a telnet session from a remote computer.

To connect through the serial console

1. Connect your serial cable to the device (directly or through a USB-serial adapter).

2. Open the **Control Panel**, and then open the **Device Manager**.

3. Identify the COM port as shown in the following illustration.



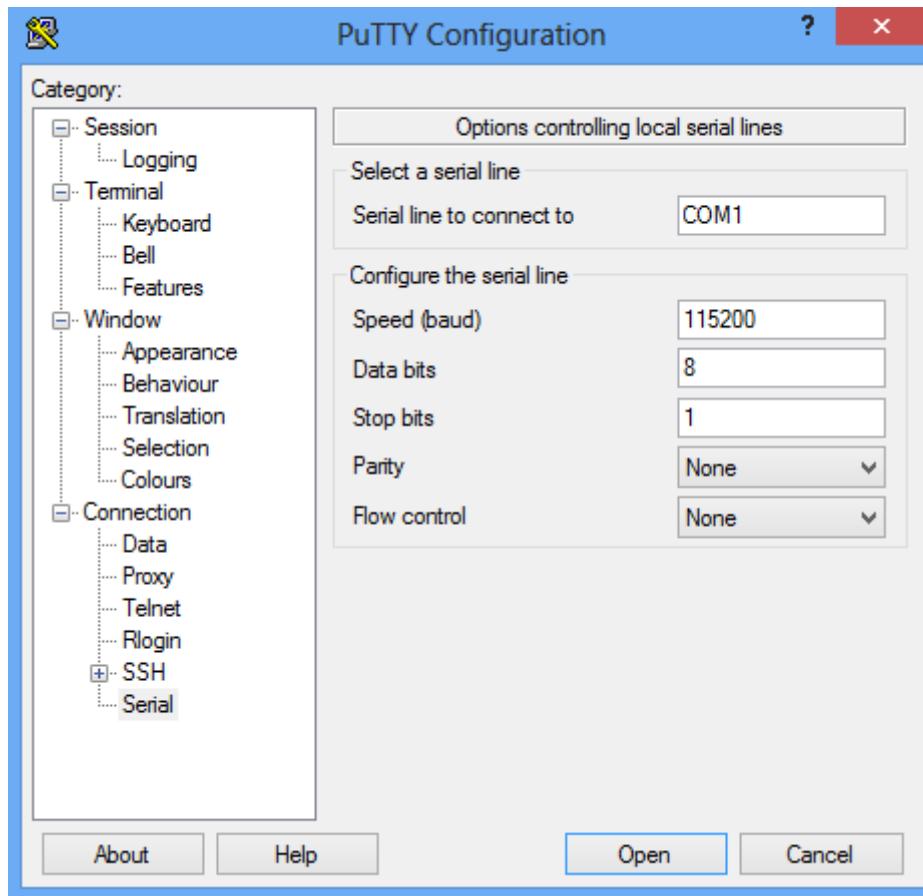
4. Start PuTTY.

5. In the right pane, change the **Connection type** to **Serial**.

6. In the right pane, type the appropriate COM port. Make sure that the serial configuration parameters are set as follows:

- Speed: 115,200
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

These settings are shown in the following illustration.



⚠ Note

If the default flow control setting does not work, try setting the flow control to XON/XOFF.

7. Click **Open** to start a serial session.

Scan for and apply updates

Updating your device can take several hours. For detailed steps on how to install the latest update, go to [Install Update 5](#).

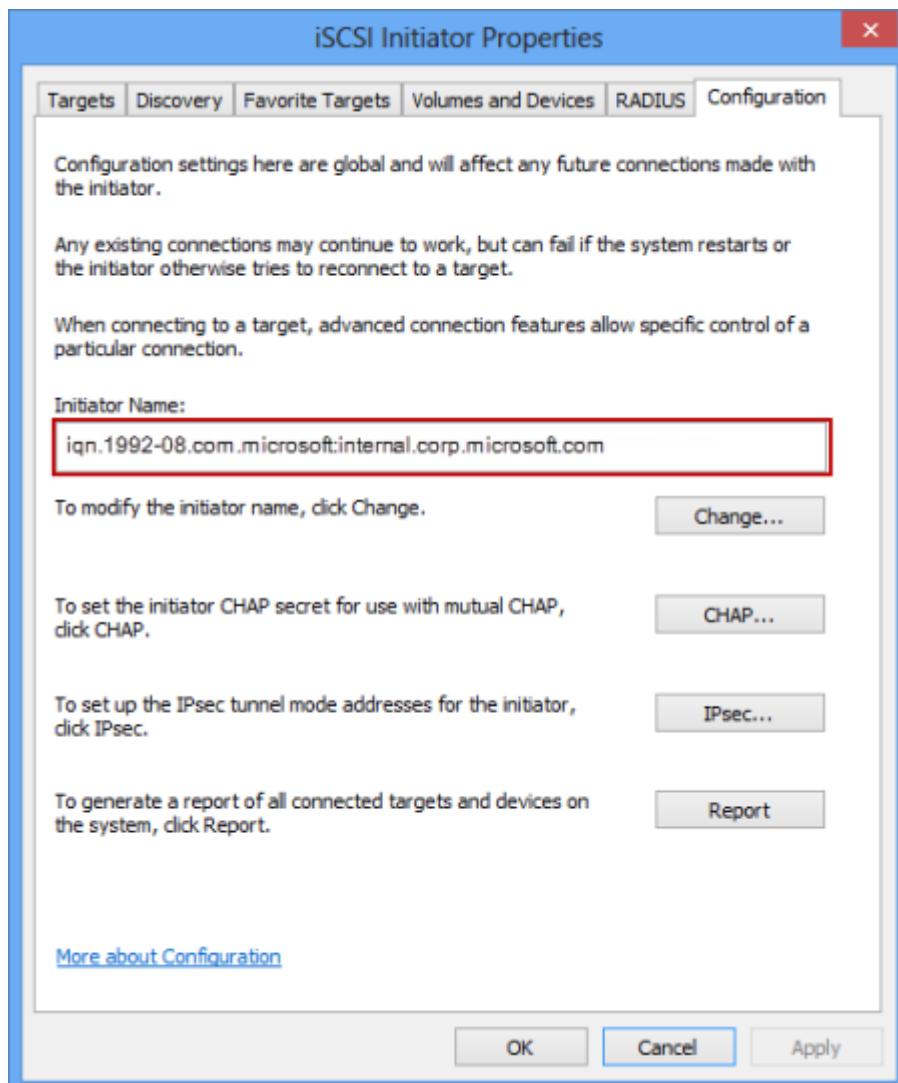
Get the IQN of a Windows Server host

Perform the following steps to get the iSCSI Qualified Name (IQN) of a Windows host that is running Windows Server® 2012.

To get the IQN of a Windows host

1. Start the Microsoft iSCSI initiator on your Windows host. Click **Start > Administrative Tools > iSCSI initiator**.

2. In the iSCSI Initiator Properties window, on the Configuration tab, select and copy the string from the Initiator Name field.



3. Save this string.

Create a manual backup

Perform the following steps in the Azure portal to create an on-demand manual backup for a single volume on your StorSimple device.

To create a manual backup

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of devices, select your device. Go to **Settings > Manage > Backup policies**.
2. The **Backup policies** blade lists all the backup policies in a tabular format, including the policy for the volume that you want to back up. Select the policy associated

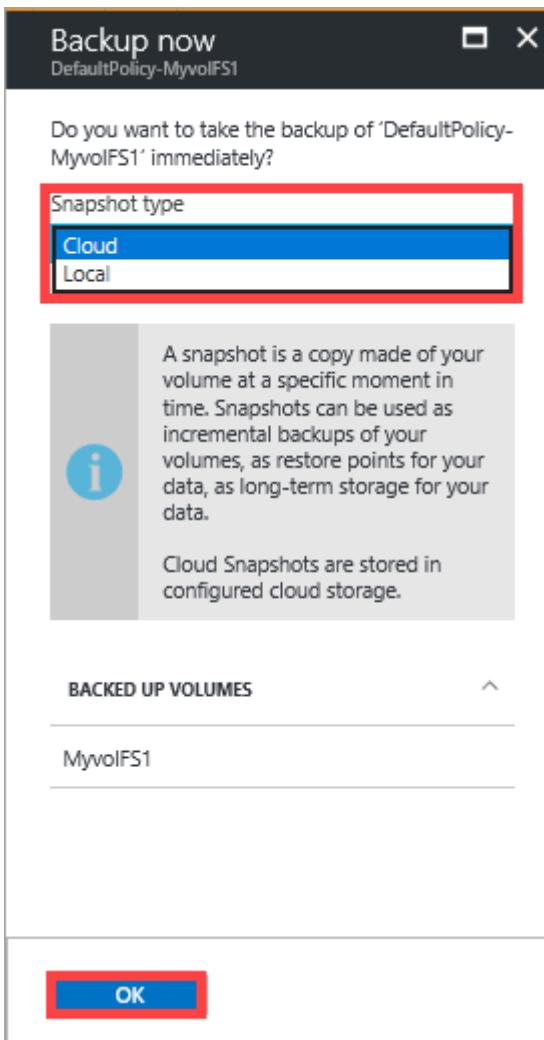
with the volume you want to back up and right-click to invoke the context menu. From the dropdown list, select **Back up now**.

The screenshot shows the 'Backup Policy' blade for a device named 'MySS8000Device1'. On the left, there's a navigation pane with sections like GENERAL, MONITOR, MANAGE, and DEVICE SETTINGS. Under MANAGE, 'Backup policy' is highlighted with a red box. The main area displays a table of backup policies. One row, 'DefaultPolicy-MyvolFS1', has a context menu open over it, also enclosed in a red box. The menu items are: Pin to dashboard, Add schedule, Add/Remove Volume, **Backup now** (which is highlighted), and Delete.

NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDULING
MySSbupol1	1/13/2017 17:00:00	1/13/2017 14:30:30	1	1
DefaultPolicy-MyvolFS1	1/12/2017 14:30:02	1/13/2017 14:30:30	1	1

3. In the **Back up now** blade, do the following steps:

- Choose the appropriate **Snapshot type** from the dropdown list: **Local** snapshot or **Cloud** snapshot. Select local snapshot for fast backups or restores, and cloud snapshot for data resiliency.



- b. Click **OK** to start a job to create a snapshot. You will see a notification at the top of the page after the job is successfully created.



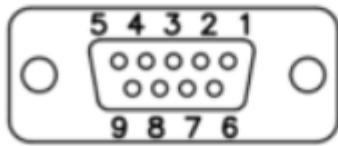
- c. To monitor the job, click the notification. This takes you to the **Jobs** blade where you can view the job progress.
4. After the backup job is finished, go to the **Backup catalog** tab.
5. Set the filter selections to the appropriate device, backup policy, and time range. The backup should appear in the list of backup sets that is displayed in the catalog.

View the pinout diagram for serial cable for StorSimple

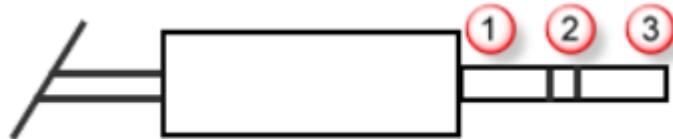
The following pinout diagram can be used for the StorSimple serial console cable.

Here the DB9 female connector is P1 and the 3.5 mm connector is P2.

P1	P2
PIN 1	NO CONNECTION
PIN 2 RX	PIN 2 TX
PIN 3 TX	PIN 3 RX
PIN 4	NO CONNECTION
PIN 5 GND	PIN 1 GND
PIN 6	NO CONNECTION
PIN 7	NO CONNECTION
PIN 8	NO CONNECTION
PIN 9	NO CONNECTION



The tip of the stereo jack is considered to be PIN 3 RX, the middle is PIN 2 TX and the base is PIN 1 GND as shown in the following diagram.



Next steps

- Configure a StorSimple Cloud Appliance.
- Use the StorSimple Device Manager service to manage your StorSimple device.

Deploy your on-premises StorSimple device in the Government portal

Article • 03/22/2023 • 25 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Welcome to Microsoft Azure StorSimple device deployment. These deployment tutorials apply to the StorSimple 8000 Series running Update 3 software or later in the Azure Government portal. This series of tutorials includes a configuration checklist, a list of configuration prerequisites, and detailed configuration steps for your StorSimple device.

The information in these tutorials assumes that you have reviewed the safety precautions, and unpacked, racked, and cabled your StorSimple device. If you still need to perform those tasks, start with reviewing the [safety precautions](#). Follow the device-specific instructions to unpack, rack mount, and cable your device.

- [Unpack, rack mount, and cable your 8100](#)
- [Unpack, rack mount, and cable your 8600](#)

You will need administrator privileges to complete the setup and configuration process. We recommend that you review the configuration checklist before you begin. The deployment and configuration process can take some time to complete.

ⓘ Note

The StorSimple deployment information published on the Microsoft Azure website applies to StorSimple 8000 series devices only.

Deployment steps

Perform these required steps to configure your StorSimple device and connect it to your StorSimple Device Manager service. In addition to the required steps, there are optional steps and procedures that you may need to complete during the deployment. The step-by-step deployment instructions indicate when you should perform each of these optional steps.

Step	Description
PREREQUISITES	These need to be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information prior to and during the deployment.
Deployment prerequisites	These validate that the environment is ready for deployment.
STEP-BY-STEP DEPLOYMENT	These steps are required to deploy your StorSimple device in production.
Step 1: Create a new service	Set up cloud management and storage for your StorSimple device. <i>Skip this step if you have an existing service for other StorSimple devices.</i>
Step 2: Get the service registration key	Use this key to register and connect your StorSimple device with the management service.
Step 3: Configure and register the device through Windows PowerShell for StorSimple	Connect the device to your network and register it with Azure to complete the setup using the management service.
Step 4: Complete the minimum device setup Optional: Update your StorSimple device.	Use the management service to complete the device setup and enable it to provide storage.
Step 5: Create a volume container	Create a container to provision volumes. A volume container has storage account, bandwidth, and encryption settings for all the volumes contained in it.
Step 6: Create a volume	Provision storage volume(s) on the StorSimple device for your servers.
Step 7: Mount, initialize, and format a volume Optional: Configure MPIO.	Connect your servers to the iSCSI storage provided by the device. Optionally, configure MPIO to ensure that your servers can tolerate link, network, and interface failure.
Step 8: Take a backup	Set up your backup policy to protect your data

Step	Description
OTHER PROCEDURES	You may need to refer to these procedures as you deploy your solution.
Configure a new storage account for the service	
Use PuTTY to connect to the device serial console	
Scan for and apply updates	
Get the IQN of a Windows Server host	
Create a manual backup	

Deployment configuration checklist

Before you deploy your StorSimple device, you will need to collect information to configure the software on your device. Preparing some of this information ahead of time will help streamline the process of deploying the StorSimple device in your environment. Download and use this checklist to note the configuration details as you deploy your device.

[Download StorSimple deployment configuration checklist](#) ↗

Deployment prerequisites

The following sections explain the configuration prerequisites for your StorSimple Device Manager service and your StorSimple device.

For the StorSimple Device Manager service

Before you begin, make sure that:

- You have your Microsoft account with access credentials.
- You have your Microsoft Azure storage account with access credentials.
- Your Microsoft Azure subscription is enabled for the StorSimple Device Manager service. Your subscription should be purchased through the [Enterprise Agreement](#) ↗.
- You have access to terminal emulation software such as PuTTY.

For the device in the datacenter

Before configuring the device, make sure that:

- Your device is fully unpacked, mounted on a rack and fully cabled for power, network, and serial access as described in:
 - [Unpack, rack mount, and cable your 8100 device](#)
 - [Unpack, rack mount, and cable your 8600 device](#)

For the network in the datacenter

Before you begin, make sure that:

- The ports in your datacenter firewall are opened to allow for iSCSI and cloud traffic as described in [Networking requirements for your StorSimple device](#).

Step-by-step deployment

Use the following step-by-step instructions to deploy your StorSimple device in the datacenter.

Step 1: Create a new service

A StorSimple Device Manager service can manage multiple StorSimple devices. Perform the following steps to create a new instance of the StorSimple Device Manager service.

To create a new service

1. Use your Microsoft account credentials to sign in to the [Microsoft Azure Government Portal](#).
2. In the Government Portal, click + and then in the marketplace, click **See all**. Search for *StorSimple Physical*. Select and click **StorSimple Physical Device Series** and then click **Create**. Alternatively, in the Government portal, click + and then under **Storage**, click **StorSimple Physical Device Series**.
3. In the **StorSimple Device Manager** blade, do the following steps:
 - a. Supply a unique **Resource name** for your service. This name is a friendly name that can be used to identify the service. The name can have between 2 and 50 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.

- b. Choose a **Subscription** from the drop-down list. The subscription is linked to your billing account. This field is not present if you have only one subscription.
- c. For **Resource group**, Use existing or Create new group. For more information, see [Azure resource groups](#).
- d. Supply a **Location** for your service. Location refers to the geographical region where you want to deploy your device. Select **USGov Iowa** or **USGov Virginia**.
- e. Select **Create a new storage account** to automatically create a storage account with the service. Specify a name for this storage account. If you need your data in a different location, uncheck this box.
- f. Check **Pin to dashboard** if you want a quick link to this service on your dashboard.
- g. Click **Create** to create the StorSimple Device Manager. The service creation takes a few minutes. After the service is successfully created, you will see a notification and the new service blade opens up.

 **Important**

If you did not enable the automatic creation of a storage account with your service, you will need to create at least one storage account after you have successfully created a service. This storage account will be used when you create a volume container.

- If you did not create a storage account automatically, go to [Configure a new storage account for the service](#) for detailed instructions.
- If you enabled the automatic creation of a storage account, go to [Step 2: Get the service registration key](#).

Step 2: Get the service registration key

After the StorSimple Device Manager service is up and running, you will need to get the service registration key. This key is used to register and connect your StorSimple device to the service.

Perform the following steps in the Government portal.

To get the StorSimple service registration key

1. On the **StorSimple Device Manager** blade, click the service that you created. This opens up a new blade to the right.

The screenshot shows the 'MySS8000DevManager StorSimple Manager BVTD' interface. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Locks, Properties, Quick start, Devices, Volume container, Volumes, Keys, Backup policy, and Backup catalog. The main area displays monitoring information: 'Essentials' (Resource group: MySS8000RG, Location: West US, Subscription name: Microsoft Azure Enterprise, Subscription ID: 0154f7fe-df09-4981-bf82-7ad5c1f596eb), 'Monitoring' (Alerts - Past 7 days: 0, Devices: 0), and 'MySS8000DevManager - Usage - Past 7 days' (Capacity utilization: 0). A search bar at the top left says 'Search (Ctrl+ /)'. A blue banner at the top right says 'There are no registered devices. Click here to get started.' with a link.

2. Go to Management > Keys.

The screenshot shows the 'Docs-mySS8000series - Keys' blade in StorSimple Device Manager. The left sidebar has a red box around the 'MANAGEMENT' section, which includes 'Devices', 'Volume containers', 'Volumes', and 'Keys'. The 'Keys' item is highlighted with a blue box. The main area shows a 'Regenerate' button and a 'Registration key' field with a copy icon (highlighted with a red box) and a 'Learn more about registering devices' link.

3. In the blade that opens up, click the copy icon to copy the service registration key and save it for later use.

Note

The service registration key is used to register all the devices that need to register with your StorSimple Device Manager service.

Step 3: Configure and register the device through Windows PowerShell for StorSimple

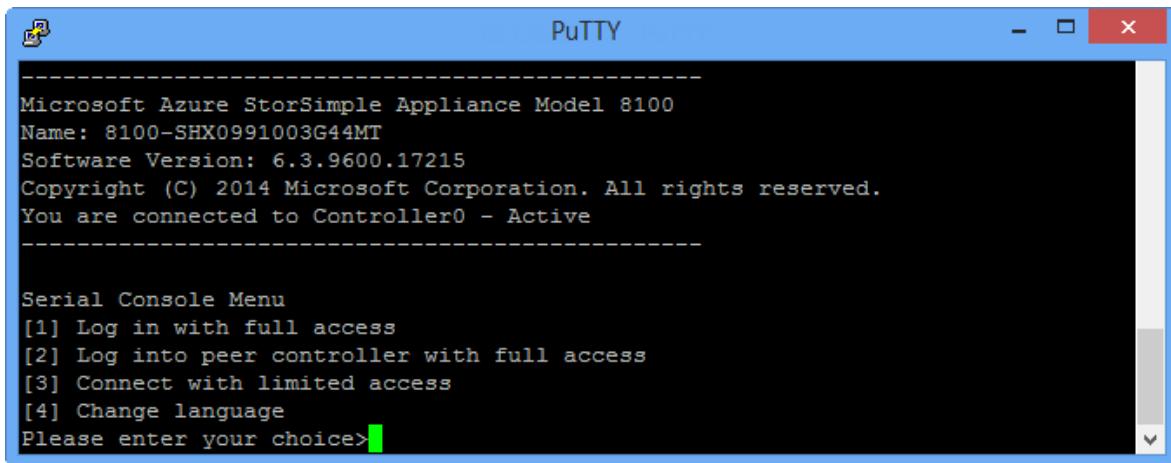
Use Windows PowerShell for StorSimple to complete the initial setup of your StorSimple device as explained in the following procedure. You will need to use terminal emulation software to complete this step. For more information, see [Use PuTTY to connect to the device serial console](#).

To configure and register the device

1. Access the Windows PowerShell interface on your StorSimple device serial console. See [Use PuTTY to connect to the device serial console](#) for instructions. Be sure to follow the procedure exactly or you will not be able to access the console.
2. In the session that opens up, press **Enter** one time to get a command prompt.
3. You will be prompted to choose the language that you would like to set for your device. Specify the language, and then press **Enter**.



4. In the serial console menu that is presented, choose option 1, **Log in with full access**.



PuTTY

```
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17215
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

-----
Serial Console Menu
[1] Log in with full access
[2] Log into peer controller with full access
[3] Connect with limited access
[4] Change language
Please enter your choice>
```

5. Perform the following steps to configure the minimum required network settings for your device.

ⓘ Important

These configuration steps need to be performed on the active controller of the device. The serial console menu indicates the controller state in the banner message. If you are not connect to the active controller, disconnect and then connect to the active controller.

- a. At the command prompt, type your password. The default device password is **Password1**.

- b. Type the following command:

```
Invoke-HcsSetupWizard
```

- c. A setup wizard will appear to help you configure the network settings for the device. Supply the following information:

- IP address for DATA 0 network interface
- Subnet mask
- Gateway
- IP address for Primary DNS server
- IP address for Primary NTP server

ⓘ Note

You may have to wait for a few minutes for the subnet mask and DNS settings to be applied.

- d. Optionally, configure your web proxy server.

Important

Although web proxy configuration is optional, be aware that if you use a web proxy, you can only configure it here. For more information, go to [Configure web proxy for your device](#).

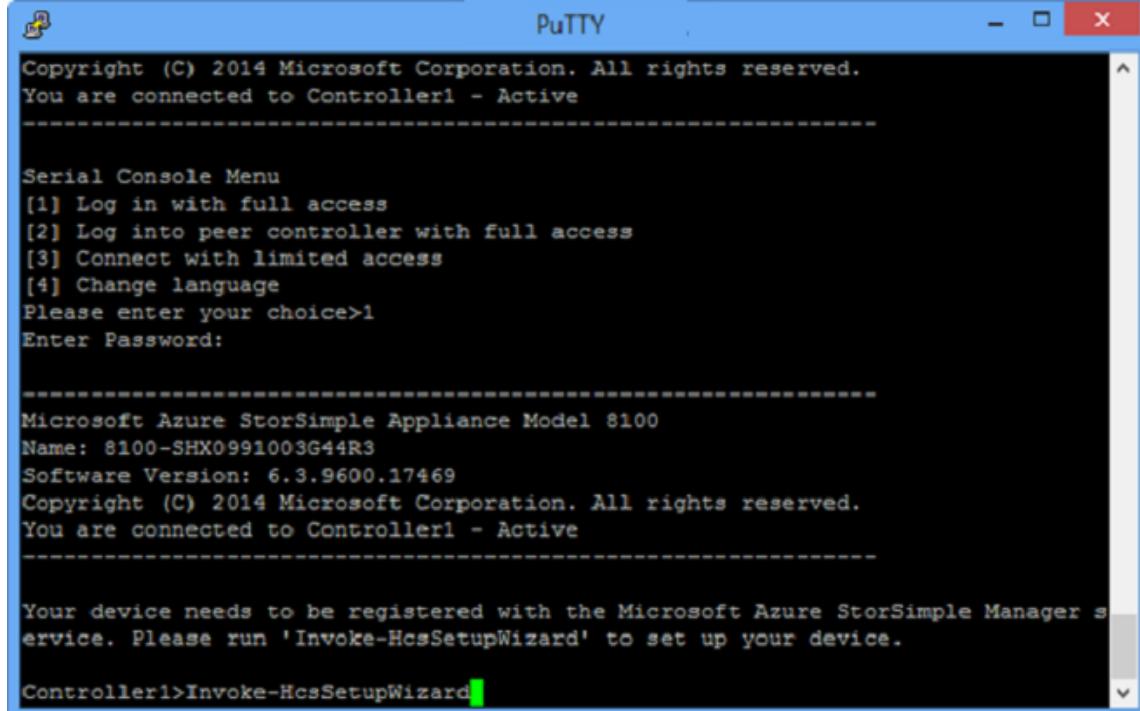
6. Press Ctrl + C to exit the setup wizard.
7. Run the following cmdlet to point the device to the Microsoft Azure Government portal (because it points to the public Azure classic portal by default). This will restart both controllers. We recommend that you use two PuTTY sessions to simultaneously connect to both controllers so that you can see when each controller is restarted.

```
Set-CloudPlatform -AzureGovt_US
```

You will see a confirmation message. Accept the default (Y).

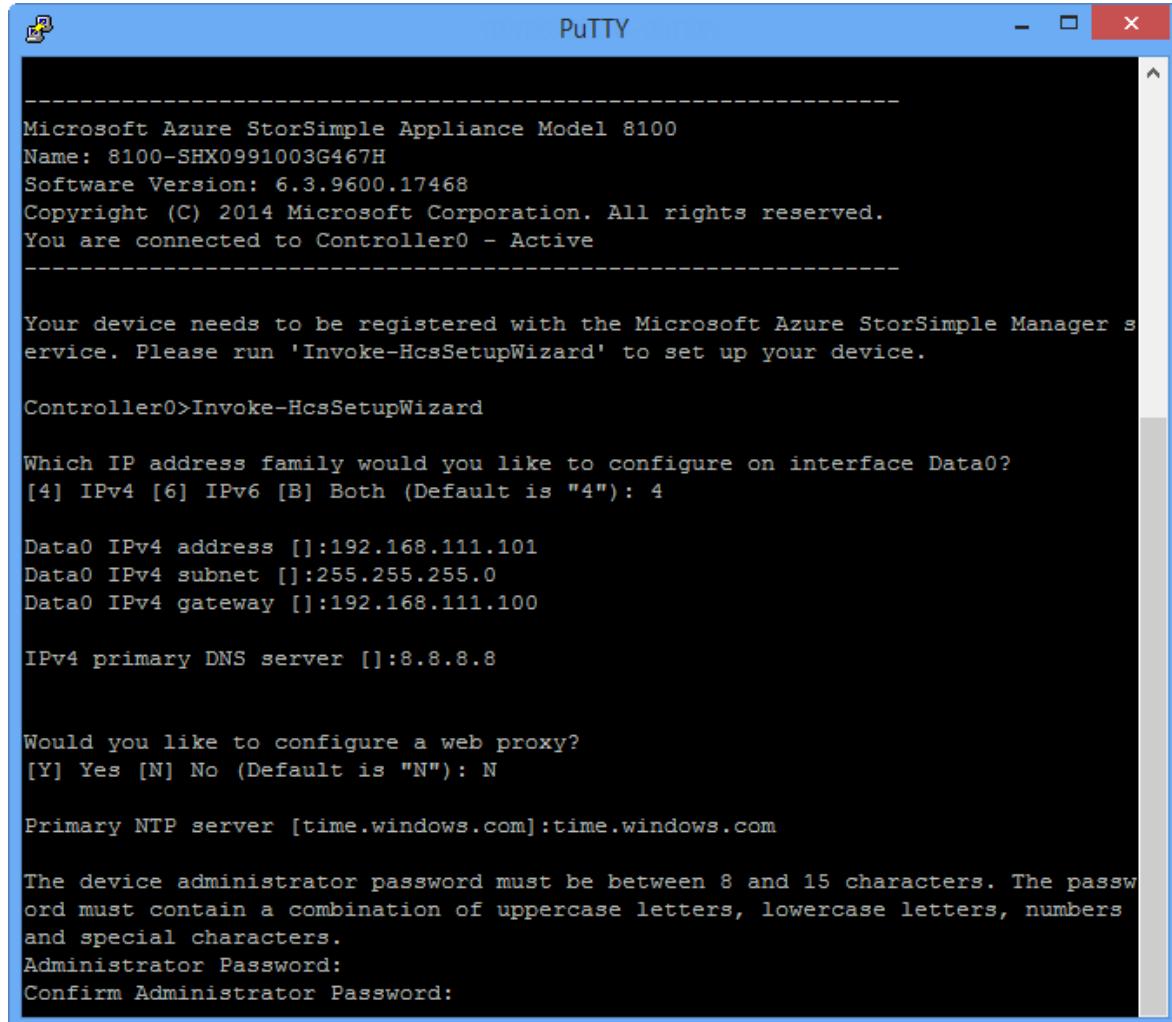
8. Run the following cmdlet to resume setup:

```
Invoke-HcsSetupWizard
```



9. Accept the network settings. You will see a validation message after you accept each setting.
10. For security reasons, the device administrator password expires after the first session, and you will need to change it now. When prompted, provide a device

administrator password. A valid device administrator password must be between 8 and 15 characters. The password must contain three of the following: lowercase, uppercase, numeric, and special characters.



The screenshot shows a PuTTY terminal window titled "PuTTY". The window displays the following text:

```
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G467H
Software Version: 6.3.9600.17468
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

-----
Your device needs to be registered with the Microsoft Azure StorSimple Manager service. Please run 'Invoke-HcsSetupWizard' to set up your device.

Controller0>Invoke-HcsSetupWizard

Which IP address family would you like to configure on interface Data0?
[4] IPv4 [6] IPv6 [B] Both (Default is "4"): 4

Data0 IPv4 address []:192.168.111.101
Data0 IPv4 subnet []:255.255.255.0
Data0 IPv4 gateway []:192.168.111.100

IPv4 primary DNS server []:8.8.8.8

Would you like to configure a web proxy?
[Y] Yes [N] No (Default is "N"): N

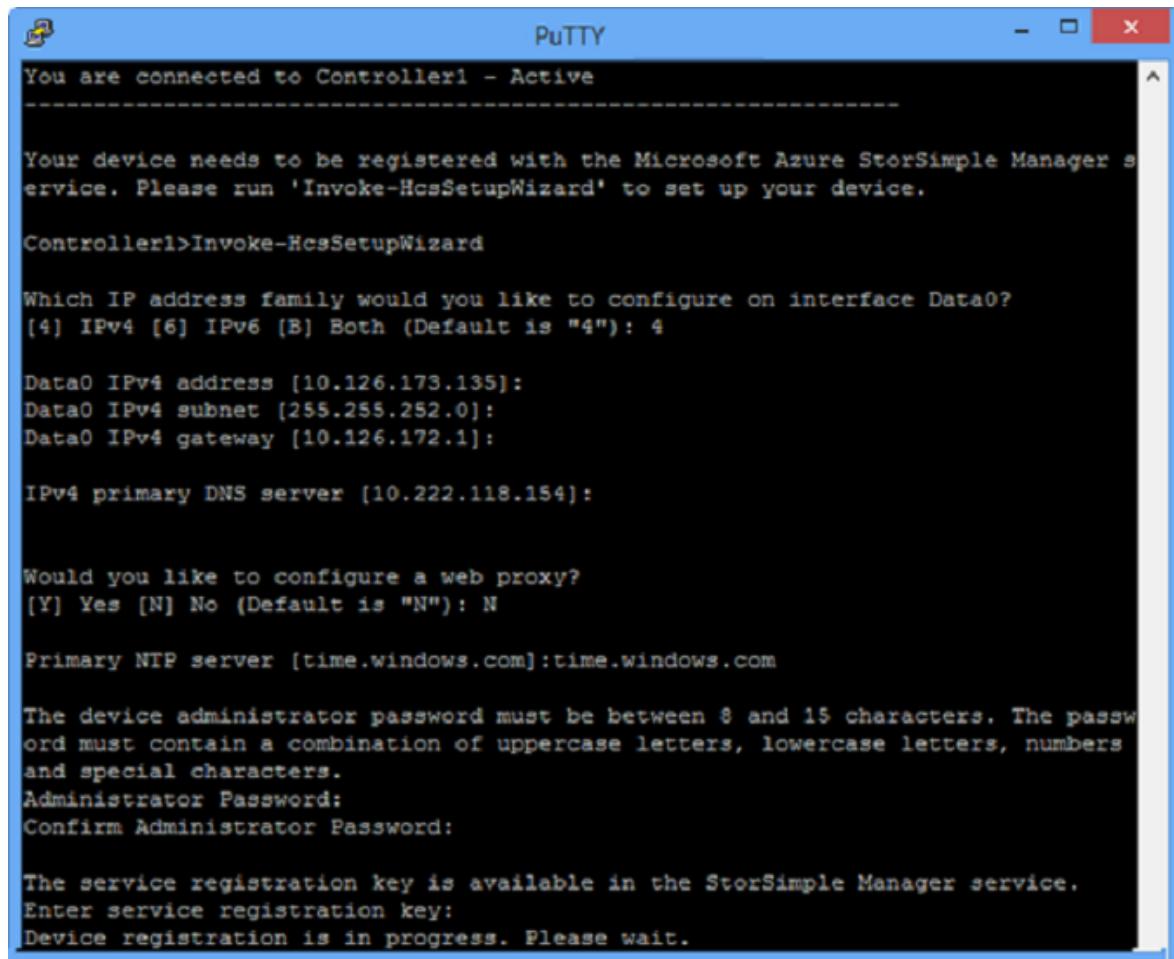
Primary NTP server [time.windows.com]:time.windows.com

The device administrator password must be between 8 and 15 characters. The password must contain a combination of uppercase letters, lowercase letters, numbers and special characters.
Administrator Password:
Confirm Administrator Password:
```

11. The final step in the setup wizard registers your device with the StorSimple Device Manager service. For this, you will need the service registration key that you obtained in [Step 2: Get the service registration key](#). After you supply the registration key, you may need to wait for 2-3 minutes before the device is registered.

 **Note**

You can press **Ctrl + C** at any time to exit the setup wizard. If you have entered all the network settings (IP address for Data 0, Subnet mask, and Gateway), your entries will be retained.



PutTY

```
You are connected to Controller1 - Active
-----
Your device needs to be registered with the Microsoft Azure StorSimple Manager service. Please run 'Invoke-HcsSetupWizard' to set up your device.

Controller1>Invoke-HcsSetupWizard

Which IP address family would you like to configure on interface Data0?
[4] IPv4 [6] IPv6 [8] Both (Default is "4") : 4

Data0 IPv4 address [10.126.173.135]: 
Data0 IPv4 subnet [255.255.252.0]: 
Data0 IPv4 gateway [10.126.172.1]: 

IPv4 primary DNS server [10.222.118.154]: 

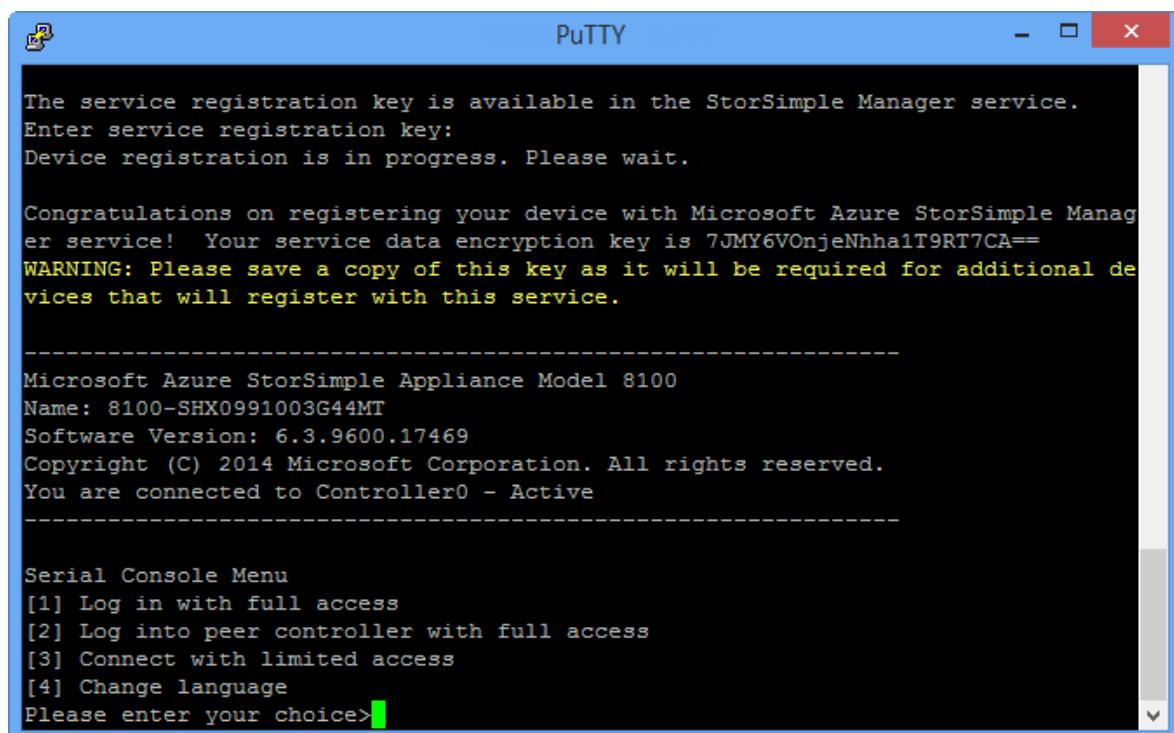
Would you like to configure a web proxy?
[Y] Yes [N] No (Default is "N") : N

Primary NTP server [time.windows.com]:time.windows.com

The device administrator password must be between 8 and 15 characters. The password must contain a combination of uppercase letters, lowercase letters, numbers and special characters.
Administrator Password:
Confirm Administrator Password:

The service registration key is available in the StorSimple Manager service.
Enter service registration key:
Device registration is in progress. Please wait.
```

12. After the device is registered, a Service Data Encryption key will appear. Copy this key and save it in a safe location. **This key is required with the service registration key to register additional devices with the StorSimple Device Manager service.** Refer to [StorSimple security](#) for more information about this key.



PutTY

```
The service registration key is available in the StorSimple Manager service.
Enter service registration key:
Device registration is in progress. Please wait.

Congratulations on registering your device with Microsoft Azure StorSimple Manager service! Your service data encryption key is 7JMY6VOnjeNhha1T9RT7CA==

WARNING: Please save a copy of this key as it will be required for additional devices that will register with this service.

-----
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17469
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active
-----

Serial Console Menu
[1] Log in with full access
[2] Log into peer controller with full access
[3] Connect with limited access
[4] Change language
Please enter your choice>
```

ⓘ Important

To copy the text from the serial console window, simply select the text. You should then be able to paste it in the clipboard or any text editor.

DO NOT use **Ctrl + C** to copy the service data encryption key. Using **Ctrl + C** will cause you to exit the setup wizard. As a result, the device administrator password will not be changed and the device will revert to the default password.

13. Exit the serial console.

14. Return to the Azure Government Portal, and complete the following steps:

- a. Go to your StorSimple Device Manager service.
- b. Click **Devices**. From the list of devices, identify the device that you are deploying. Verify that the device has successfully connected to the service by looking up the status. The device status should be **Online**.

If the device status is **Offline**, wait for a couple of minutes for the device to come online.

If the device is still offline after a few minutes, then you need to make sure that your firewall network was configured as described in [networking requirements for your StorSimple device](#).

Verify that port 9354 is open for outbound communication as this is used by the service bus for StorSimple Device Manager Service-to-device communication.

Step 4: Complete minimum device setup

For the minimum device configuration of your StorSimple device, you are required to:

- Provide a friendly name for your device.
- Set the device time zone.
- Assign fixed IP addresses to both the controllers.

Perform the following steps in the Azure Government portal to complete the minimum device setup.

To complete the minimum StorSimple device setup

① Note

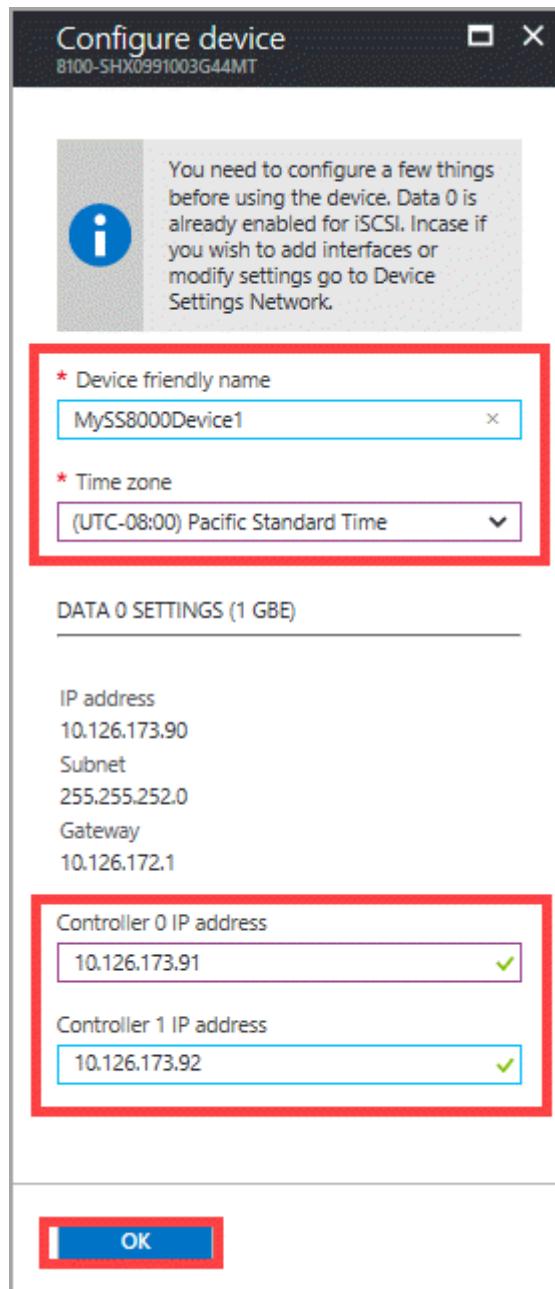
You cannot change the device name once the minimum device setup is completed.

1. From the tabular listing of devices in the **Devices** blade, select and click your device. The device is in a **Ready to set up** state. The **Configure device** blade opens up.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Ready to set up	8.65 TB/200 TB	Physical device	8100

2. In the **Configure device** blade:

- a. Supply a **friendly name** for your device. The default device name reflects information such as the device model and serial number. You can assign a friendly name of up to 64 characters to manage your device.
- b. Set the **time zone** based on the geographic location in which the device is being deployed. Your device uses this time zone for all scheduled operations.
- c. Under the **DATA 0 settings**:
 - i. Your DATA 0 network interface shows as enabled with the network settings (IP, subnet, gateway) configured via the setup wizard. DATA 0 is also automatically enabled for cloud as well as iSCSI.
 - ii. Provide the fixed IP addresses for Controller 0 and Controller 1. **The controller fixed IP addresses need to be free IPs within the subnet accessible by the device IP address.** If the DATA 0 interface was configured for IPv4, the fixed IP addresses need to be provided in the IPv4 format. If you provided a prefix for IPv6 configuration, the fixed IP addresses are populated automatically in these fields.



The fixed IP addresses for the controller are used for servicing the updates to the device and for garbage collection. Therefore, the fixed IPs must be routable and able to connect to the Internet. You can check that your fixed controller IPs are routable by using the [Test-HcsmConnection](#) cmdlet. The following example shows fixed controller IPs are routed to the Internet and can access the Microsoft Update servers.

```

Microsoft Azure StorSimple Appliance Model 8100
Name: MySS8000Device1
Software Version: 6.3.9600.17759
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

Controller0>Test-HcsmConnection
Checking device registration state ... Success
Device registered successfully

Checking primary IPv4 DNS server [10.222.118.154] ... Success
Checking primary IPv6 DNS server ... NOT SET
Checking secondary IPv4 DNS server ... NOT SET
Checking secondary IPv6 DNS server ... NOT SET

Checking primary NTP server [time.windows.com] ... Success

Checking web proxy ... NOT SET

Checking TCP Port 80 status ... [ Ensure that TCP port 80 is open for outbound traffic on the firewall.] ... Success
Checking TCP Port 443 status ... [ Ensure that TCP port 443 is open for outbound traffic on the firewall.] ... Success
Checking TCP Port 9354 status ... [ Ensure that TCP port 9354 is open for outbound traffic on the firewall.] ... Skipped
Skipped

Checking device online ... Success

Checking device authentication ... This operation will take a few minutes.
Checking device authentication ... Success

Checking connectivity from device to service ... This operation will take a few minutes.
Checking connectivity from device to service ... Success

Checking connectivity from service to device ... Success

Controller0>Checking connectivity to Microsoft update servers ... Success
Controller0>

```

3. Click **OK**. The device configuration starts. When the device configuration is complete, you are notified. The device status changes to **Online** in the **Devices** blade.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERE...)	TYPE	MODEL
MySS8000Device1	Online	8.65 TB/200 TB	Physical device	8100

Step 5: Create a volume container

A volume container has storage account, bandwidth, and encryption settings for all the volumes contained in it. You will need to create a volume container before you can start provisioning volumes on your StorSimple device.

Perform the following steps in the Government portal to create a volume container.

To create a volume container

1. Go to your StorSimple Device Manager service and click **Devices**. From the tabular listing of the devices, select and click a device.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
TaalaFriendlyNameG1	Online	0 Bytes/1023 GB	Physical device	100
SudasDevice1	Online	32.67 GB/817 GB	Physical device	100
Device1	Offline	34.31 GB/857.83 GB	Physical device	100
Gu3Device2	Offline	19.12 GB/478.16 GB	Physical device	100
Gu3Device1	Deactivated	40.95 GB/1 TB	Physical device	100

2. In the device dashboard, click **+ Add volume container**

The screenshot shows the Dell PowerVault Management Suite interface. On the left, the 'Monitoring' section displays various metrics: 4 alerts (3 Critical, 1 Warning) and 1 volume online. Below this is a usage chart for 'TaalaFriendlyNameG1' over the past 24 hours, showing primary tiered storage, locally pinned storage, and cloud storage used. At the bottom, capacity details are shown: 1 GB provisioned, 1023 GB remaining (tiered), and 0 bytes local. On the right, the 'Settings' sidebar is open, showing sections for General, Monitor, Manage, and Device Settings. The 'Volume container' option under 'Manage' is highlighted with a red box.

3. In the **Add volume container** blade:

- The device is automatically selected.
- Supply a **Name** for your volume container. The name must be 3 to 32 characters long. You cannot rename a volume container once it is created.
- Select **Enable Cloud Storage Encryption** to enable encryption of the data sent from the device to the cloud.
- Provide and confirm a **Cloud Storage Encryption Key** that is 8 to 32 characters long. This key is used by the device to access encrypted data.
- Select a **Storage Account** to associate with this volume container. You can choose an existing storage account or the default account that is generated at

the time of service creation. You can also use the **Add new** option to specify a storage account that is not linked to this service subscription.

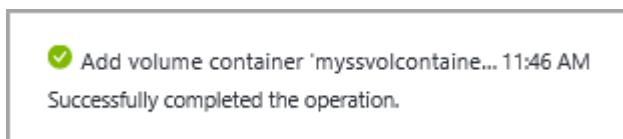
- f. Select **Unlimited** in the **Specify bandwidth** drop-down list if you wish to consume all the available bandwidth.

If you have your bandwidth usage information available, you may be able to allocate bandwidth based on a schedule by specifying **Select a bandwidth template**. For a step-by-step procedure, go to [Add a bandwidth template](#).

The screenshot shows the 'Add volume container' dialog box. It includes fields for 'Select device' (set to 'myss8000device'), 'Volume container name' (set to 'myssvolcont1'), 'Cloud storage encryption' (set to 'Enabled'), 'Encryption key' (redacted), 'Confirm encryption key' (redacted), 'Storage account credential' (set to '11d3d4e0ead6412bb0419'), and 'Bandwidth setting' (set to 'Unlimited'). The 'Create' button is at the bottom.

- g. Click **Create**.

You are notified when the volume container is successfully created.



The newly created volume container is listed in the list of volume containers for your device.

NAME	VOLUMES	CLOUD ST...	BANDWID...	STORAGE...
VC1	9	NA	0	portalintegrati... ...
myssvolcontainer1	0	NA	0	localizetest ...
vc2	2	NA	0	portalintegrati... ...

Step 6: Create a volume

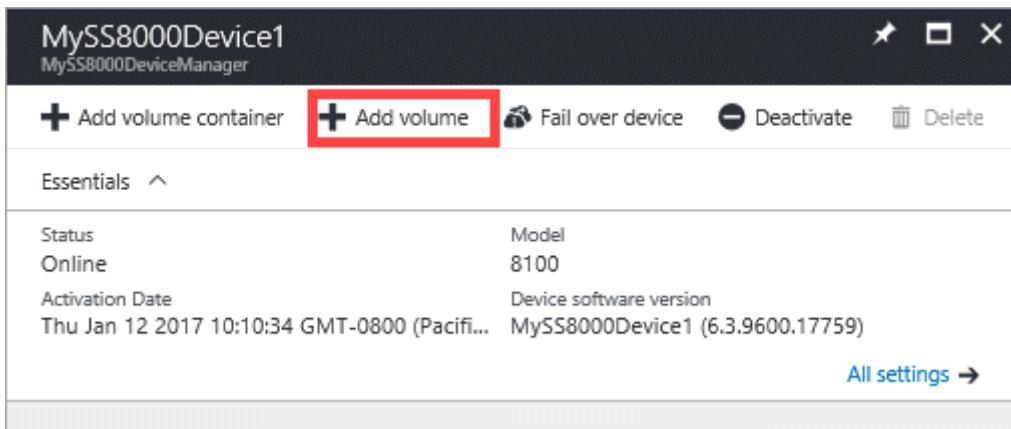
After you create a volume container, you can provision a storage volume on the StorSimple device for your servers. Perform the following steps in the Government portal to create a volume.

ⓘ Important

StorSimple Device Manager can create only thinly provisioned volumes. You cannot however create partially provisioned volumes.

To create a volume

1. From the tabular listing of the devices in the **Devices** blade, select your device.
Click **+ Add volume**.



2. In the **Add a volume** blade:

- a. The **Select device** field is automatically populated with your current device.
- b. From the drop-down list, select the volume container where you need to add a volume.
- c. Type a **Name** for your volume. You cannot rename a volume once the volume is created.
- d. On the drop-down list, select the **Type** for your volume. For workloads that require local guarantees, low latencies, and higher performance, select a **Locally pinned** volume. For all other data, select a **Tiered** volume. If you are using this volume for archival data, check **Use this volume for less frequently accessed archival data**.

A tiered volume is thinly provisioned and can be created quickly. Selecting **Use this volume for less frequently accessed archival data** for tiered volume targeted for archival data changes the deduplication chunk size for your volume to 512 KB. If this field is not checked, the corresponding tiered volume uses a chunk size of 64 KB. A larger deduplication chunk size allows the device to expedite the transfer of large archival data to the cloud.

A locally pinned volume is thickly provisioned and ensures that the primary data on the volume stays local to the device and does not spill to the cloud. If you create a locally pinned volume, the device checks for available space on the local tiers to provision the volume of the requested size. The operation of creating a locally pinned volume may involve spilling existing data from the device to the cloud and the time taken to create the volume may be long. The total time depends on the size of the provisioned volume, available network bandwidth, and the data on your device.

- e. Specify the **Provisioned Capacity** for your volume. Make a note of the capacity that is available based on the volume type selected. The specified volume size

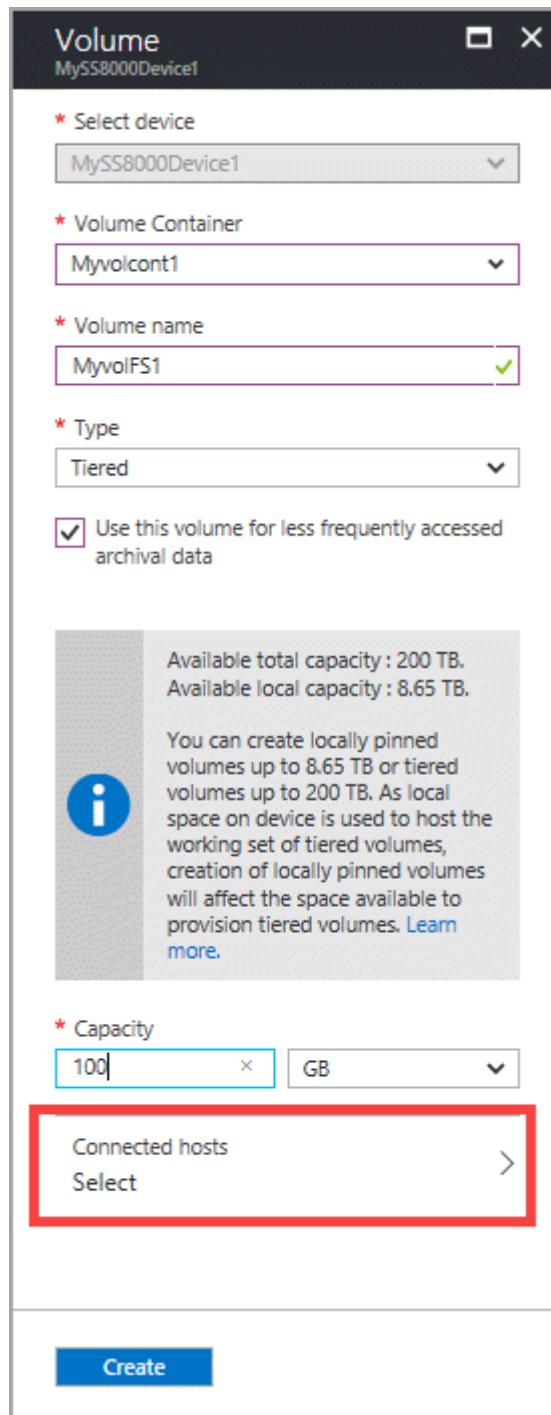
must not exceed the available space.

You can provision locally pinned volumes up to 8.5 TB or tiered volumes up to 200 TB on the 8100 device. On the larger 8600 device, you can provision locally pinned volumes up to 22.5 TB or tiered volumes up to 500 TB. As local space on the device is required to host the working set of tiered volumes, creation of locally pinned volumes impacts the space available for provisioning tiered volumes. Therefore, if you create a locally pinned volume, space available for creation of tiered volumes is reduced. Similarly, if a tiered volume is created, the available space for creation of locally pinned volumes is reduced.

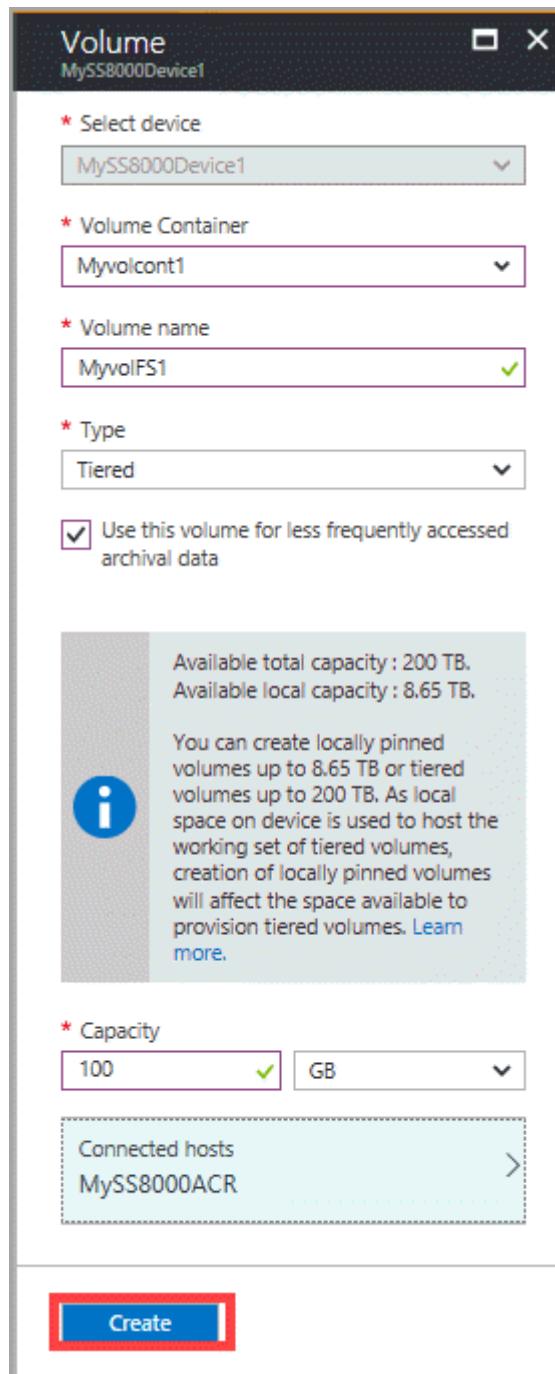
If you provision a locally pinned volume of 8.5 TB (maximum allowable size) on your 8100 device, then you have exhausted all the local space available on the device. You can't create any tiered volume from that point onwards as there is no local space on the device to host the working set of the tiered volume.

Existing tiered volumes also affect the space available. For example, if you have an 8100 device that already has tiered volumes of roughly 106 TB, only 4 TB of space is available for locally pinned volumes.

- i. In the **Connected hosts** field, click the arrow.



- ii. In the **Connected hosts** blade, choose an existing ACR or add a new ACR by performing the following steps:
 - i. Supply a **Name** for your ACR.
 - ii. Under **iSCSI Initiator Name**, provide the iSCSI Qualified Name (IQN) of your Windows host. If you don't have the IQN, go to [Get the IQN of a Windows Server host](#).
- iii. Click **Create**. A volume is created with the specified settings.



ⓘ Note

Be aware that the volume you have created here is not protected. You will need to create and associate backup policies with this volume to take scheduled backups.

Step 7: Mount, initialize, and format a volume

Perform these steps on your Windows Server host.

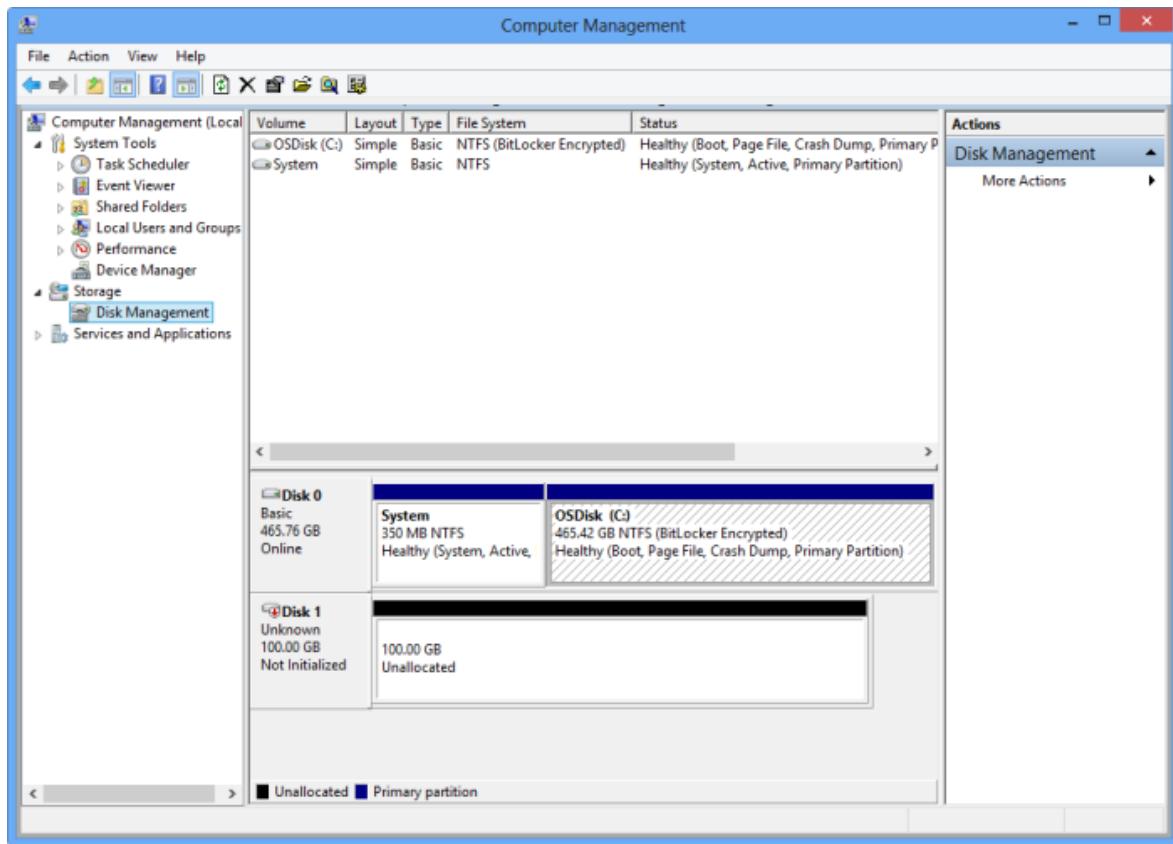
ⓘ Important

- For the high availability of your StorSimple solution, we recommend that you configure MPIO on your host servers (optional) prior to configuring iSCSI. MPIO configuration on host servers will ensure that the servers can tolerate a link, network, or interface failure.
- For MPIO and iSCSI installation and configuration instructions on Windows Server host, go to [Configure MPIO for your StorSimple device](#). These will also include the steps to mount, initialize and format StorSimple volumes.
- For MPIO and iSCSI installation and configuration instructions on a Linux host, go to [Configure MPIO for your StorSimple Linux host](#)

If you decide not to configure MPIO, perform the following steps to mount, initialize, and format your StorSimple volumes on a Windows Server host.

To mount, initialize, and format a volume

1. Start the Microsoft iSCSI initiator.
2. In the **iSCSI Initiator Properties** window, on the **Discovery** tab, click **Discover Portal**.
3. In the **Discover Target Portal** dialog box, supply the IP address of your iSCSI-enabled network interface, and then click **OK**.
4. In the **iSCSI Initiator Properties** window, on the **Targets** tab, locate the **Discovered targets**. The device status should appear as **Inactive**.
5. Select the target device and then click **Connect**. After the device is connected, the status should change to **Connected**. (For more information about using the Microsoft iSCSI initiator, see [Installing and Configuring Microsoft iSCSI Initiator](#)).
6. On your Windows host, press the Windows Logo key + X, and then click **Run**.
7. In the **Run** dialog box, type **Diskmgmt.msc**. Click **OK**, and the **Disk Management** dialog box will appear. The right pane will show the volumes on your host.
8. In the **Disk Management** window, the mounted volumes will appear as shown in the following illustration. Right-click the discovered volume (click the disk name), and then click **Online**.



9. Right-click the volume (click the disk name) again, and then click **Initialize**.

10. To format a simple volume, perform the following steps:

- a. Select the volume, right-click it (click the right area), and click **New Simple Volume**.
- b. In the New Simple Volume wizard, specify the volume size and drive letter and configure the volume as an NTFS file system.
- c. Specify a 64 KB allocation unit size. This allocation unit size works well with the deduplication algorithms used in the StorSimple solution.
- d. Perform a quick format.



Video available

To watch a video that demonstrates how to mount, initialize, and format a StorSimple volume, click [here ↗](#).

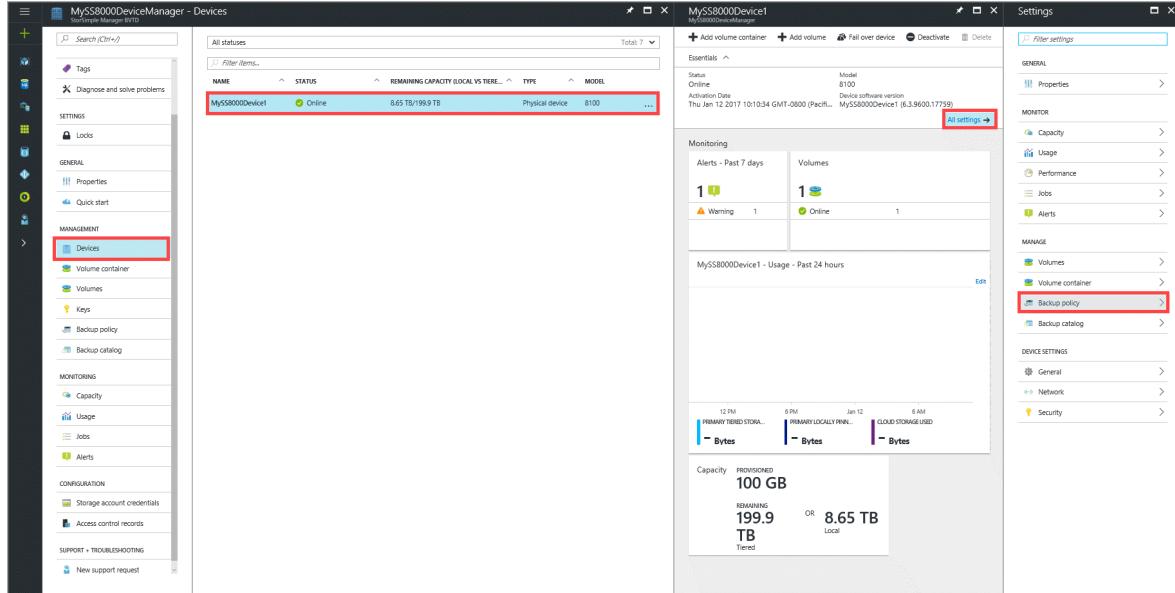
Step 8: Take a backup

Backups provide point-in-time protection of volumes and improve recoverability while minimizing restore times. You can take two types of backup on your StorSimple device: local snapshots and cloud snapshots. Each of these backup types can be **Scheduled** or **Manual**.

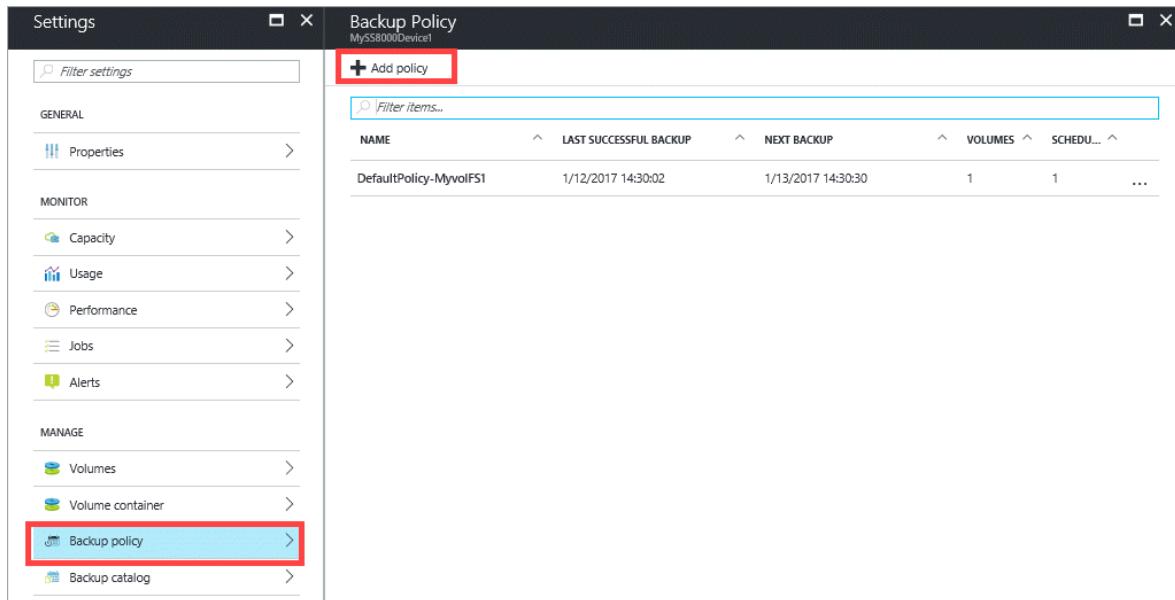
Perform the following steps in the Government portal to create a scheduled backup.

To take a backup

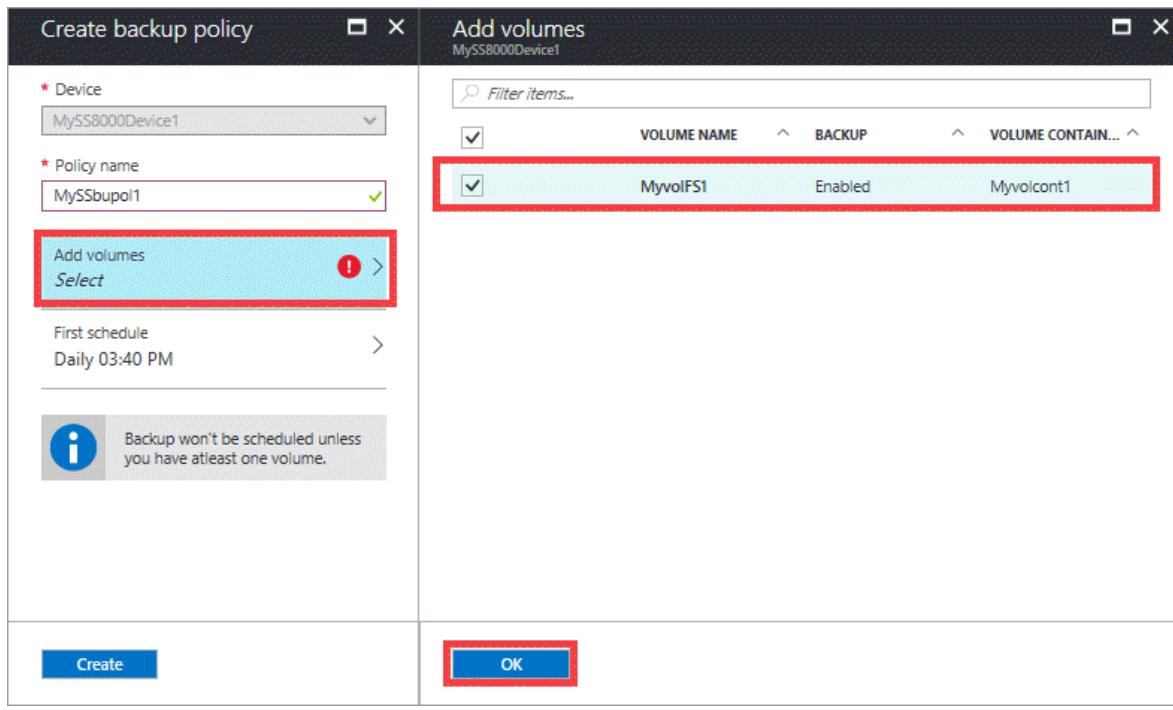
1. Go to your StorSimple Device Manager service. From the tabular listing of devices, select and click your device and then click **All settings**. In the **Settings** blade, go to **Settings > Manage > Backup policy**.



2. In the **Backup policy** blade, click **+ Add policy**.

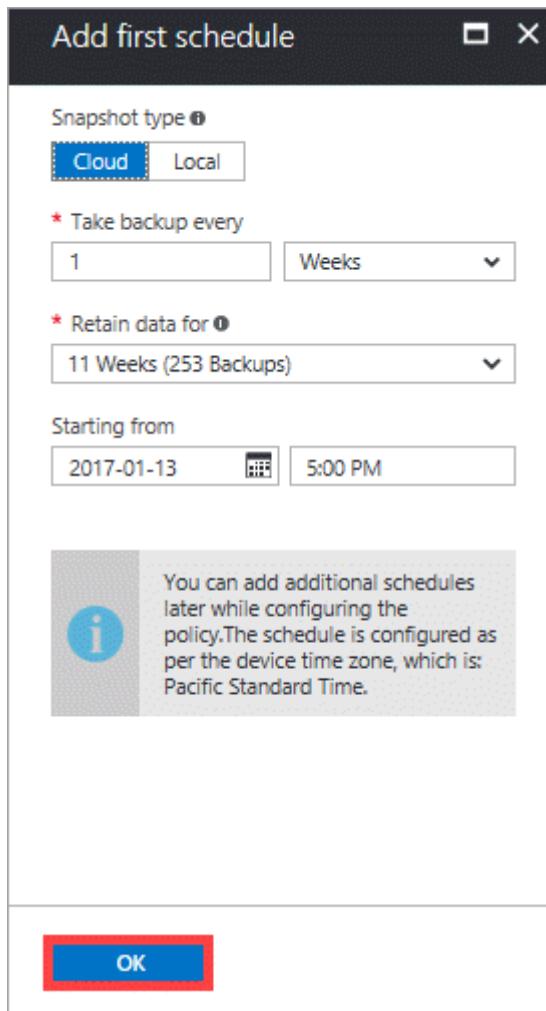


3. In the **Create backup policy** blade, supply a name that contains between 3 and 150 characters for your backup policy.
4. Select the volumes to be backed up. If you select more than one volume, these volumes are grouped together to create a crash-consistent backup.



5. On Add first schedule blade:

- a. Select the type of backup. For faster restores, select **Local** snapshot. For data resiliency, select **Cloud** snapshot.
- b. Specify the backup frequency in minutes, hours, days, or weeks.
- c. Select a retention time. The retention choices depend on the backup frequency. For example, for a daily policy, the retention can be specified in weeks, whereas retention for a monthly policy is in months.
- d. Select the starting time and date for the backup policy.
- e. Click **OK** to create the backup policy.



6. Click **Create** to start the backup policy creation. You are notified when the backup policy is successfully created. The list of backup policies is also updated.

NAME	LAST SUCCESSFUL BACKUP	VOLUMES	SCHEDULING
MySSbupol1	1/13/2017 17:00:00	1	1
DefaultPolicy-MyvolFS1	1/12/2017 14:30:02	1	1

You now have a backup policy that creates scheduled backups of your volume data.

You can take a manual backup at any time. For procedures, go to [Create a manual backup](#).

Configure a new storage account for the service

This is an optional step that you need to perform only if you did not enable the automatic creation of a storage account with your service. A Microsoft Azure storage account is required to create a StorSimple volume container.

If you need to create an Azure storage account in a different region, see [About Azure Storage Accounts](#) for step-by-step instructions.

Perform the following steps in the Government portal, on the **StorSimple Device Manager service** page.

To add a storage account credential in the same Azure subscription as the StorSimple Device Manager service

1. Go to your StorSimple Device Manager service. In the Configuration section, click **Storage account credentials**.

The screenshot shows the Azure portal interface for the resource group 'MySS8000RG'. The left sidebar contains a navigation menu with various icons and links. The 'Storage account credentials' link is highlighted with a red box.

Essentials

- Resource group: MySS8000RG
- Subscription name: Microsoft Azure Enterprise
- Location: West US
- Subscription ID: 0154f7fe-df09-4981-bf82-7ad5c1f596eb

Alerts - Past 7 days

Category	Count
Warning	1

Devices

Status	Count
Online	1

MySS8000DeviceManager - Usage - Past 7 days

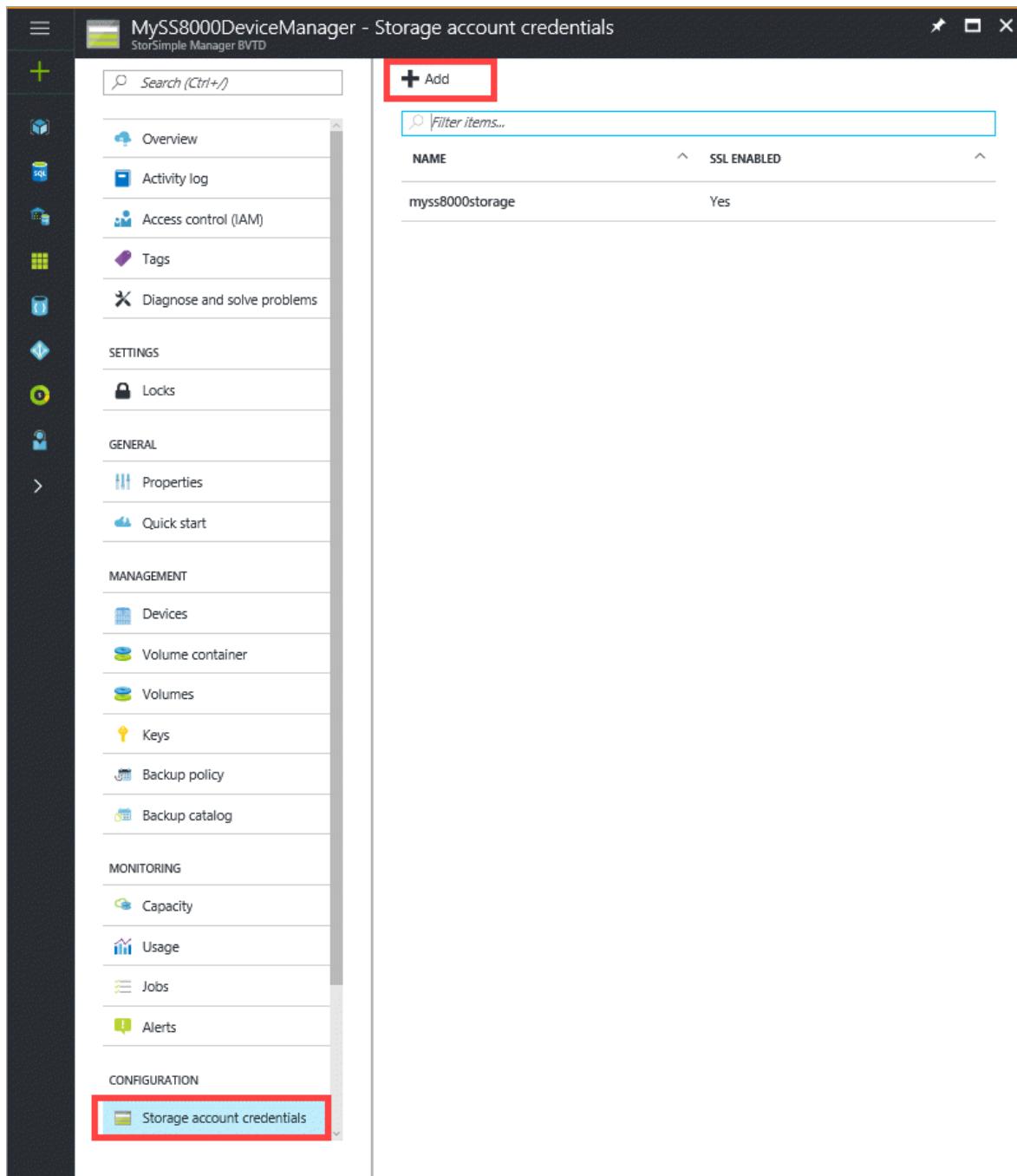
Jan 11 Jan 12 Jan 13 Jan 14 Jan 15 Jan 16 Jan 17

PRIMARY TIERED STORAGE - Bytes PRIMARY LOCALLY PINNED - Bytes CLOUD STORAGE USED - Bytes

Capacity PROVISIONED **300 GB**

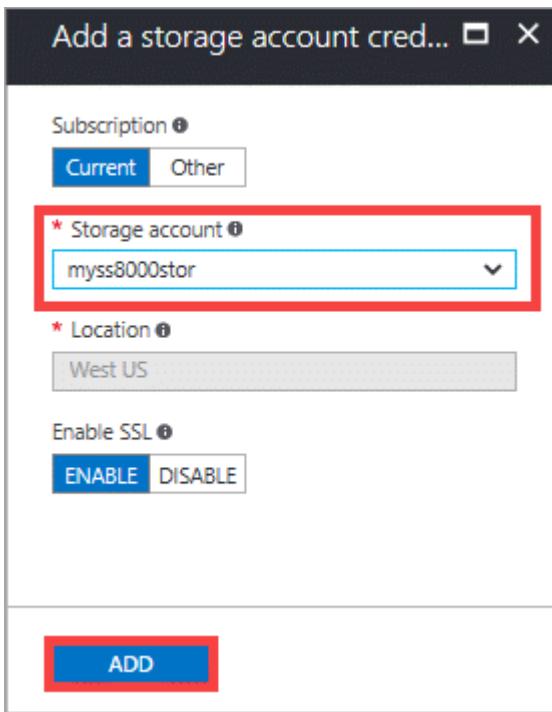
REMAINING **199.7 TB** **Tiered** OR **8.64 TB Local**

2. On the **Storage account credentials** blade, click **+ Add**.



3. In the **Add a storage account credential** blade, do the following steps:

- a. As you are adding a storage account credential in the same Azure subscription as your service, ensure that **Current** is selected.
- b. From the **storage account** dropdown list, select an existing storage account.
- c. Based on the storage account selected, the **location** will be displayed (grayed out and cannot be changed here).
- d. Select **Enable SSL Mode** to create a secure channel for network communication between your device and the cloud. Disable **Enable SSL** only if you are operating within a private cloud.



- e. Click **Add** to start the job creation for the storage account credential. You will be notified after the storage account credential is successfully created.

Add storage account credential 'myss80... 1:34 PM
Successfully completed the operation.

The newly created storage account credential will be displayed under the list of **Storage account credentials**.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	Yes

Use PuTTY to connect to the device serial console

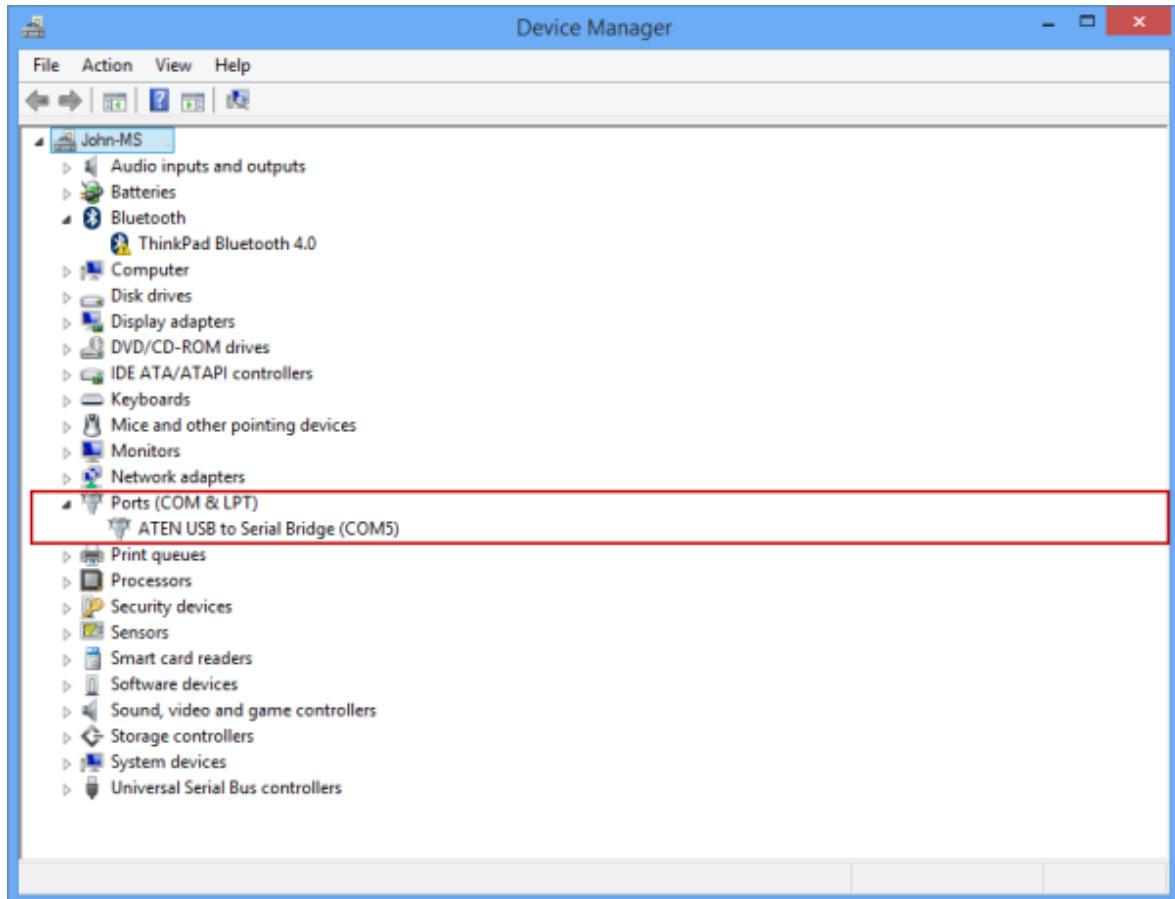
To connect to Windows PowerShell for StorSimple, you need to use terminal emulation software such as PuTTY. You can use PuTTY when you access the device directly through the serial console or by opening a telnet session from a remote computer.

To connect through the serial console

1. Connect your serial cable to the device (directly or through a USB-serial adapter).

2. Open the **Control Panel**, and then open the **Device Manager**.

3. Identify the COM port as shown in the following illustration.



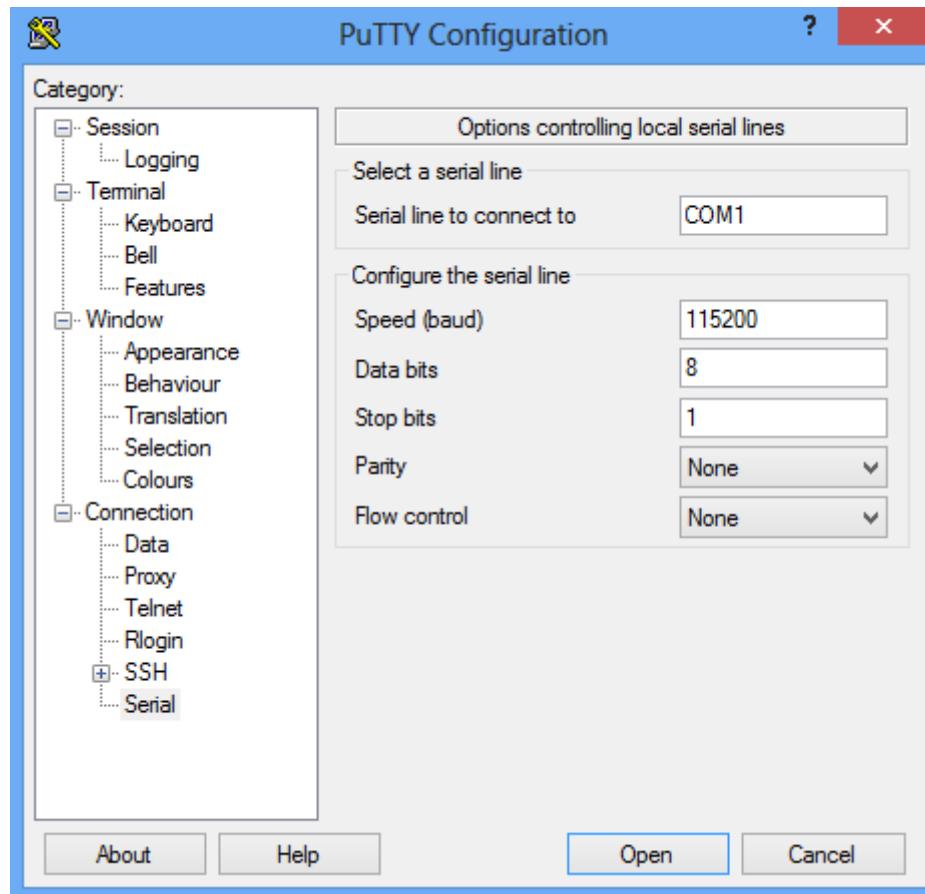
4. Start PuTTY.

5. In the right pane, change the **Connection type** to **Serial**.

6. In the right pane, type the appropriate COM port. Make sure that the serial configuration parameters are set as follows:

- Speed: 115,200
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

These settings are shown in the following illustration.



⚠ Note

If the default flow control setting does not work, try setting the flow control to XON/XOFF.

7. Click **Open** to start a serial session.

Scan for and apply updates

Updating your device can take several hours. For detailed steps on how to install the latest update, go to [Install Update 4](#).

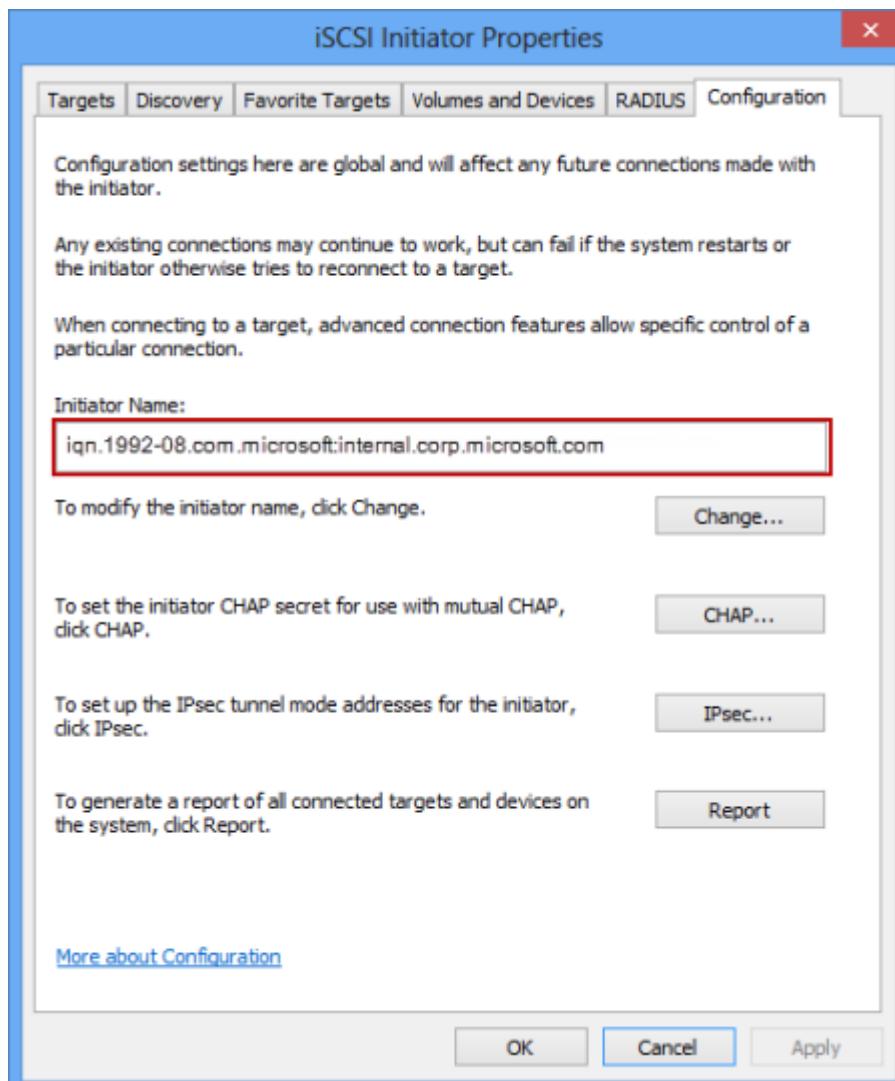
Get the IQN of a Windows Server host

Perform the following steps to get the iSCSI Qualified Name (IQN) of a Windows host that is running Windows Server® 2012.

To get the IQN of a Windows host

1. Start the Microsoft iSCSI initiator on your Windows host. Click **Start > Administrative Tools > iSCSI initiator**.

2. In the iSCSI Initiator Properties window, on the Configuration tab, select and copy the string from the Initiator Name field.



3. Save this string.

Create a manual backup

Perform the following steps in the Government portal to create an on-demand manual backup for a single volume on your StorSimple device.

To create a manual backup

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of devices, select your device. Go to **Settings > Manage > Backup policies**.
2. The **Backup policies** blade lists all the backup policies in a tabular format, including the policy for the volume that you want to back up. Select the policy associated

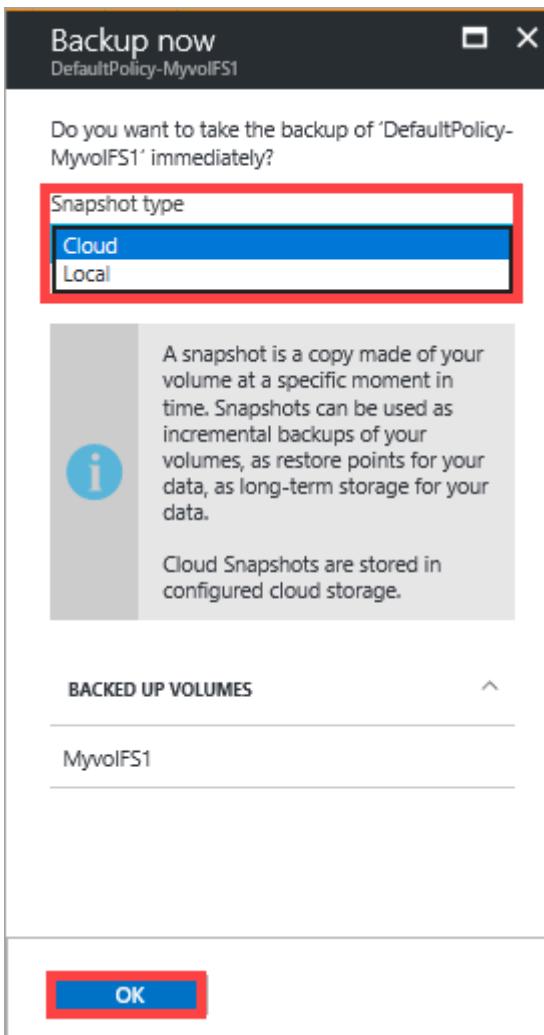
with the volume you want to back up and right-click to invoke the context menu. From the dropdown list, select **Back up now**.

The screenshot shows the 'Backup Policy' blade for a device named 'MySS8000Device1'. On the left, there's a navigation pane with sections like GENERAL, MONITOR, MANAGE, and DEVICE SETTINGS. Under MANAGE, 'Backup policy' is highlighted with a red box. The main area displays a table of backup policies. One row, 'DefaultPolicy-MyvolFS1', has a context menu open over it, also enclosed in a red box. The menu items are: Pin to dashboard, Add schedule, Add/Remove Volume, **Backup now** (which is highlighted in grey), and Delete.

NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDULING
MySSbupol1	1/13/2017 17:00:00	1/13/2017 14:30:30	1	1
DefaultPolicy-MyvolFS1	1/12/2017 14:30:02	1/13/2017 14:30:30	1	1

3. In the **Back up now** blade, do the following steps:

- Choose the appropriate **Snapshot type** from the dropdown list: **Local** snapshot or **Cloud** snapshot. Select local snapshot for fast backups or restores, and cloud snapshot for data resiliency.



- b. Click **OK** to start a job to create a snapshot. You will see a notification at the top of the page after the job is successfully created.



- c. To monitor the job, click the notification. This takes you to the **Jobs** blade where you can view the job progress.
4. After the backup job is finished, go to the **Backup catalog** tab.
5. Set the filter selections to the appropriate device, backup policy, and time range. The backup should appear in the list of backup sets that is displayed in the catalog.

Next steps

- Configure a [virtual device](#).
- Use the [StorSimple Device Manager service](#) to manage your StorSimple device.

Deploy and manage a StorSimple Cloud Appliance in Azure (Update 3 and later)

Article • 08/19/2022 • 21 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple 8000 Series Cloud Appliance is an additional capability that comes with your Microsoft Azure StorSimple solution. The StorSimple Cloud Appliance runs on a virtual machine in a Microsoft Azure virtual network, and you can use it to back up and clone data from your hosts.

This article describes the step-by-step process to deploy and manage a StorSimple Cloud Appliance in Azure. After reading this article, you will:

- Understand how the cloud appliance differs from the physical device.
- Be able to create and configure the cloud appliance.
- Connect to the cloud appliance.
- Learn how to work with the cloud appliance.

This tutorial applies to all the StorSimple Cloud Appliances running Update 3 and later.

Cloud appliance model comparison

The StorSimple Cloud Appliance is available in two models, a standard 8010 (formerly known as the 1100) and a premium 8020 (introduced in Update 2). The following table presents a comparison of the two models.

Device model	8010 ¹	8020
--------------	-------------------	------

Device model	8010 ¹	8020
Maximum capacity	30 TB	64 TB
Azure VM	Standard_A3 (4 cores, 7 GB memory)	Standard_DS3 (4 cores, 14 GB memory)
Region availability	All Azure regions	Azure regions that support Premium Storage and DS3 Azure VMs Use this list to see if both Virtual Machines > DS-series and Storage > Disk storage are available in your region.
Storage type	Uses Azure Standard Storage for local disks Learn how to create a Standard Storage account	Uses Azure Premium Storage for local disks ²
Workload guidance	Item level retrieval of files from backups	Cloud dev and test scenarios Low latency and higher performance workloads Secondary device for disaster recovery

¹ Formerly known as the 1100.

² Both the 8010 and 8020 use Azure Standard Storage for the cloud tier. The difference only exists in the local tier within the device.

How the cloud appliance differs from the physical device

The StorSimple Cloud Appliance is a software-only version of StorSimple that runs on a single node in a Microsoft Azure Virtual Machine. The cloud appliance supports disaster recovery scenarios in which your physical device is not available. The cloud appliance is appropriate for use in item-level retrieval from backups, on-premises disaster recovery, and cloud dev and test scenarios.

Differences from the physical device

The following table shows some key differences between the StorSimple Cloud Appliance and the StorSimple physical device.

	Physical device	Cloud appliance
Location	Resides in the datacenter.	Runs in Azure.
Network interfaces	Has six network interfaces: DATA 0 through DATA 5.	Has only one network interface: DATA 0.
Registration	Registered during the initial configuration step.	Registration is a separate task.
Service data encryption key	Regenerate on the physical device and then update the cloud appliance with the new key.	Cannot regenerate from the cloud appliance.
Supported volume types	Supports both locally pinned and tiered volumes.	Supports only tiered volumes.

Prerequisites for the cloud appliance

The following sections explain the configuration prerequisites for your StorSimple Cloud Appliance. Before you deploy a cloud appliance, review the security considerations for using a cloud appliance.

Keep the following security considerations in mind when you use the StorSimple Cloud Appliance:

- The cloud appliance is secured through your Microsoft Azure subscription. This means that if you are using the cloud appliance and your Azure subscription is compromised, the data stored on your cloud appliance is also susceptible.
- The public key of the certificate used to encrypt data stored in StorSimple is securely made available to the Azure portal, and the private key is retained with the StorSimple Cloud Appliance. On the StorSimple Cloud Appliance, both the public and private keys are stored in Azure.
- The cloud appliance is hosted in the Microsoft Azure datacenter.

Azure requirements

Before you provision the cloud appliance, you need to make the following preparations in your Azure environment:

- Ensure that you have a StorSimple 8000 series physical device (model 8100 or 8600) deployed and running in your datacenter. Register this device with the same

StorSimple Device Manager service that you intend to create a StorSimple Cloud Appliance for.

- For the cloud appliance, [configure a virtual network on Azure](#). If using Premium Storage, you must create a virtual network in an Azure region that supports Premium Storage. The Premium Storage regions are regions that correspond to the row for Disk storage in the [list of Azure Services by Region](#).
- We recommend that you use the default DNS server provided by Azure instead of specifying your own DNS server name. If your DNS server name is not valid or if the DNS server is not able to resolve IP addresses correctly, the creation of the cloud appliance fails.
- Point-to-site and site-to-site are optional, but not required. If you wish, you can configure these options for more advanced scenarios.
- You can create [Azure Virtual Machines](#) (host servers) in the virtual network that can use the volumes exposed by the cloud appliance. These servers must meet the following requirements:
 - Be Windows or Linux VMs with iSCSI Initiator software installed.
 - Be running in the same virtual network as the cloud appliance.
 - Be able to connect to the iSCSI target of the cloud appliance through the internal IP address of the cloud appliance.
 - Make sure you have configured support for iSCSI and cloud traffic on the same virtual network.

StorSimple requirements

Make the following updates to your StorSimple Device Manager service before you create a cloud appliance:

- Add [access control records](#) for the VMs that are going to be the host servers for your cloud appliance.
- Use a [storage account](#) in the same region as the cloud appliance. Storage accounts in different regions may result in poor performance. You can use a Standard or Premium Storage account with the cloud appliance. More information on how to create a [Standard Storage account](#).
- Use a different storage account for cloud appliance creation from the one used for your data. Using the same storage account may result in poor performance.

Make sure that you have the following information before you begin:

- Your Azure portal account with access credentials.

- A copy of the service data encryption key from your physical device registered to the StorSimple Device Manager service.

Create and configure the cloud appliance

Before performing these procedures, make sure that you have met the [Prerequisites for the cloud appliance](#).

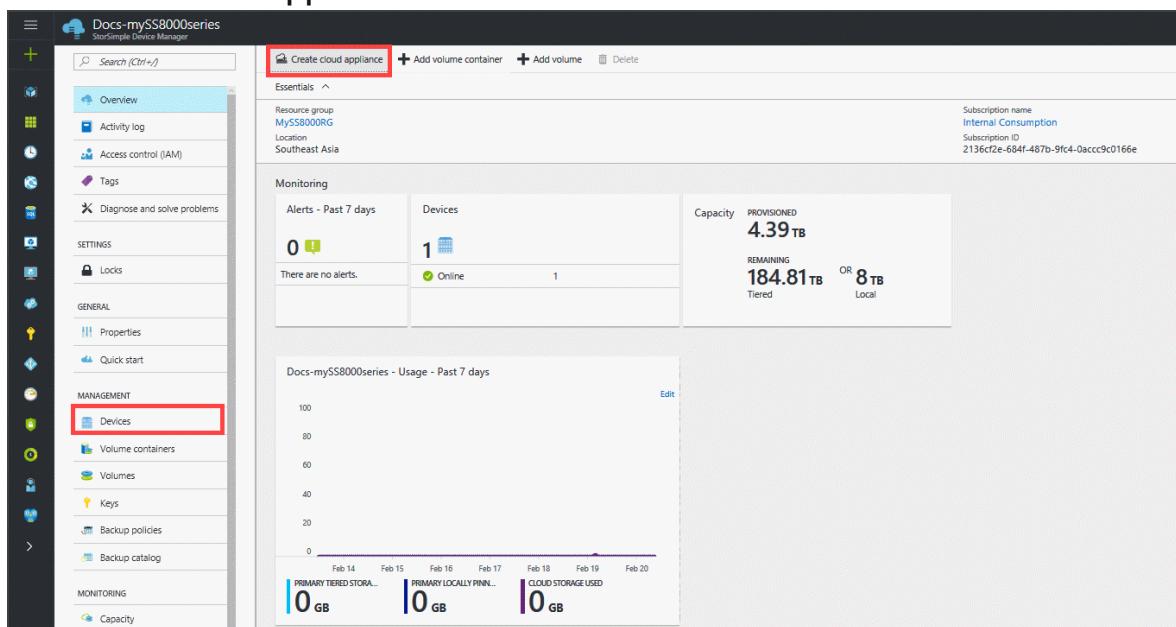
Perform the following steps to create a StorSimple Cloud Appliance.

Step 1: Create a cloud appliance

Perform the following steps to create the StorSimple Cloud Appliance.

To create a cloud appliance

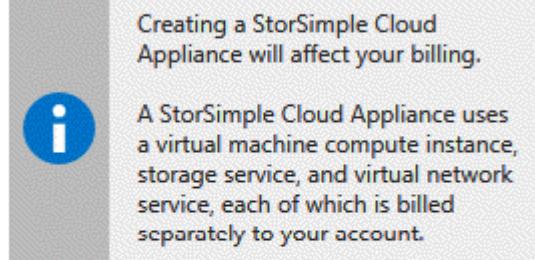
1. In the Azure portal, go to the **StorSimple Device Manager** service.
2. Go to the **Devices** blade. From the command bar in the service summary blade, click **Create cloud appliance**.



3. In the **Create cloud appliance** blade, specify the following details.

Create cloud appliance

Docs-mySS8000series



* Cloud appliance name

MySCA1

* Device model

8010

* Device software version

StorSimple 8000 Series Update 4

* Virtual network

MySCAvnet

* Subnet

default

* Storage account

myssstoracct

I understand that this cloud appliance will be hosted in the Microsoft datacenter. [Learn more.](#)

Create

- a. **Name** – A unique name for your cloud appliance.
- b. **Model** - Choose the model of the cloud appliance. An 8010 device offers 30 TB of Standard Storage whereas 8020 has 64 TB of Premium Storage. Specify 8010 to deploy item level retrieval scenarios from backups. Select 8020 to deploy high performance, low latency workloads, or use as a secondary device for disaster recovery.
- c. **Version** - Choose the version of the cloud appliance. The version corresponds to the version of the virtual disk image that is used to create the cloud appliance. Given the version of the cloud appliance determines which physical device you

fail over or clone from, it is important that you create an appropriate version of the cloud appliance.

- d. **Virtual network** – Specify a virtual network that you want to use with this cloud appliance. If using Premium Storage, you must select a virtual network that is supported with the Premium Storage account. The unsupported virtual networks are grayed out in the dropdown list. You are warned if you select an unsupported virtual network.
- e. **Subnet** - Based on the virtual network selected, the dropdown list displays the associated subnets. Assign a subnet to your cloud appliance.
- f. **Storage account** – Select a storage account to hold the image of the cloud appliance during provisioning. This storage account should be in the same region as the cloud appliance and virtual network. It should not be used for data storage by either the physical or the cloud appliance. By default, a new storage account is created for this purpose. However, if you know that you already have a storage account that is suitable for this use, you can select it from the list. If creating a premium cloud appliance, the dropdown list only displays Premium Storage accounts.

 **Note**

The cloud appliance can only work with the Azure storage accounts.

- g. Select the checkbox to indicate that you understand that the data stored on the cloud appliance is hosted in a Microsoft datacenter.
 - When you use only a physical device, your encryption key is kept with your device; therefore, Microsoft cannot decrypt it.
 - When you use a cloud appliance, both the encryption key and the decryption key are stored in Microsoft Azure. For more information, see [security considerations for using a cloud appliance](#).
- h. Click **Create** to provision the cloud appliance. The device may take around 30 minutes to be provisioned. You are notified when the cloud appliance is successfully created. Go to Devices blade, and the list of devices refreshes to display the cloud appliance. The status of the appliance is **Ready to set up**.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX099103G44MT	Online	8 TB/184.81 TB	Physical device	8100
myscal	Ready to set up	0 Bytes/30 TB	Cloud appliance	1100

If the creation of the cloud appliance fails in this step, you may not have connectivity to the Internet. For more information, go to [troubleshoot Internet connectivity failures when creating a cloud appliance](#).

Step 2: Configure and register the cloud appliance

Before you start this procedure, make sure that you have a copy of the service data encryption key. The service data encryption key is created when you registered your first StorSimple physical device with the StorSimple Device Manager service. You were instructed to save it in a secure location. If you do not have a copy of the service data encryption key, you must contact Microsoft Support for assistance.

Perform the following steps to configure and register your StorSimple Cloud Appliance.

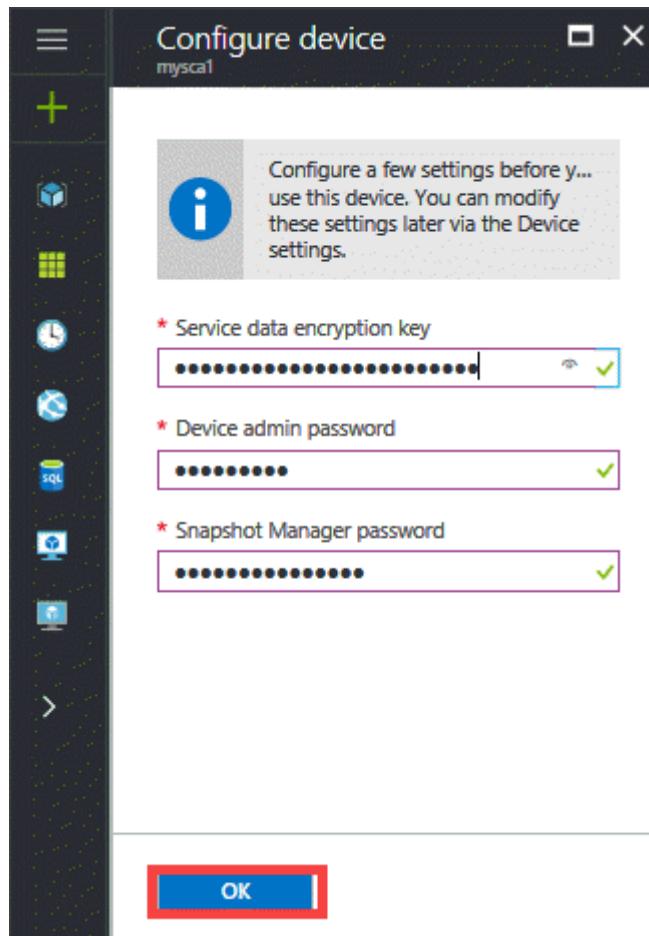
To configure and register the cloud appliance

1. Select and click the StorSimple Cloud Appliance you created in the **Devices** blade.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX099103G44MT	Online	8 TB/184.81 TB	Physical device	8100
myscal	Ready to set up	0 Bytes/30 TB	Cloud appliance	1100

2. In the **Configure device** blade, do the following steps:

- a. Enter the **Service Data Encryption Key** in the space provided. This key is generated when you registered the first physical device with your StorSimple Device Manager service.
- b. Enter the **Device admin password** and **Snapshot Manager password** of the specified length and settings.
- c. Click **OK** to finish the initial configuration and registration of the cloud appliance.



After the configuration and registration is complete, the device will come online. (It may take several minutes for the device to come online.)

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SH00991003G44MT	Online	8 TB/164.81 TB	Physical device	8100
myscal	Online	0 Bytes/50 TB	Cloud appliance	1100

Step 3: (Optional) Modify the device configuration settings

The following section describes the device configuration settings needed for the StorSimple Cloud Appliance if you want to use CHAP, StorSimple Snapshot Manager or change the device administrator password.

Configure the CHAP initiator

This parameter contains the credentials that your cloud appliance (target) expects from the initiators (servers) that are attempting to access the volumes. The initiators provide a CHAP user name and a CHAP password to identify themselves to your device during this authentication. For detailed steps, go to [Configure CHAP for your device](#).

Configure the CHAP target

This parameter contains the credentials that your cloud appliance uses when a CHAP-enabled initiator requests mutual or bi-directional authentication. Your cloud appliance uses a Reverse CHAP user name and Reverse CHAP password to identify itself to the initiator during this authentication process.

 **Note**

CHAP target settings are global settings. When these settings are applied, all the volumes connected to the cloud appliance use CHAP authentication.

For detailed steps, go to [Configure CHAP for your device](#).

Configure the StorSimple Snapshot Manager password

StorSimple Snapshot Manager software resides on your Windows host and allows administrators to manage backups of your StorSimple device in the form of local and cloud snapshots.

 **Note**

For the cloud appliance, your Windows host is an Azure virtual machine.

When configuring a device in the StorSimple Snapshot Manager, you are prompted to provide the StorSimple device IP address and password to authenticate your storage

device. For detailed steps, go to [Configure StorSimple Snapshot Manager password](#).

Change the device administrator password

When you use the Windows PowerShell interface to access the cloud appliance, you are required to enter a device administrator password. For the security of your data, you must change this password before the cloud appliance can be used. For detailed steps, go to [Configure device administrator password](#).

Connect remotely to the cloud appliance

Remote access to your cloud appliance via the Windows PowerShell interface is not enabled by default. You must enable remote management on the cloud appliance first, and then on the client used to access the cloud appliance.

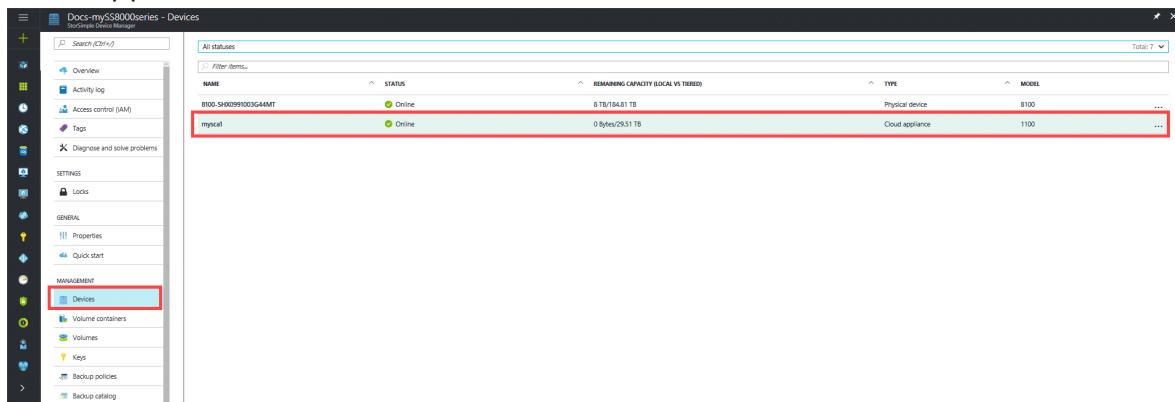
The following two-step procedure describes how to connect remotely to your cloud appliance.

Step 1: Configure remote management

Perform the following steps to configure remote management for your StorSimple Cloud Appliance.

To configure remote management on cloud appliance

1. In your StorSimple Device Manager service, click **Devices**. Select and click your cloud appliance from the list of devices connected to the service.



2. Go to **Settings > Security** to open the **Security settings** blade.

Settings

□ X

 Filter settings

GENERAL

 Properties >

MANAGE

 Volumes >

 Volume containers >

 Backup policies >

 Backup catalog >

MONITOR

 Capacity >

 Usage >

 Performance >

 Hardware health >

 Jobs >

 Alerts >

DEVICE SETTINGS

 General >

 Security >

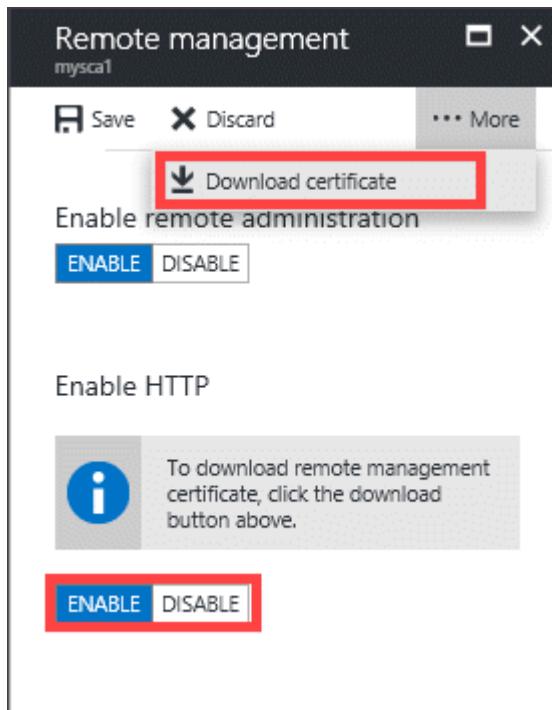
 Device updates >

3. Go to the **Remote Management** section. Click **Remote management** box.

The screenshot shows two adjacent blades. The left blade is titled "Security settings" and "mysca1". It contains sections for "Password" (with a "PASSWORD" field and a message "Password was set"), "CHAP" (with options "CHAP" and "No CHAP"), and "Remote management" (with a "REMOTE MANAGEMENT" field containing "Enabled"). A red box highlights the "REMOTE MANAGEMENT" field. The right blade is titled "Remote management" and "mysca1". It has a "Save" and "Discard" button at the top, along with a "... More" button. It features an "Enable remote administration" section with an "ENABLE" button (which is blue) and a "DISABLE" button. Below this is an "Enable HTTP" section with an "ENABLE" button (blue) and a "DISABLE" button. A note says "To download remote management certificate, click the download button above." with an information icon.

4. In the **Remote management** blade:

- a. Ensure **Enable remote administration** is enabled.
- b. The default is to connect over HTTPS. You can choose to connect using HTTP. Connecting over HTTP is acceptable only on trusted networks. Ensure that HTTP is enabled.
- c. From the command bar at the top of blade, click ... **More** and then click **Download certificate** to download a remote management certificate. You can specify a location in which to save this file. This certificate should be installed on the client or host machine that you use to connect to the cloud appliance.



5. Click **Save** and when prompted, confirm the changes.

Step 2: Remotely access the cloud appliance

After you enable remote management on the cloud appliance, use Windows PowerShell remoting to connect to the appliance from another virtual machine inside the same virtual network. For example, you can connect from the host VM that you configured and used to connect iSCSI. In most deployments, you will open a public endpoint to access your host VM that you can use for accessing the cloud appliance.

⚠ Warning

For enhanced security, we strongly recommend that you use HTTPS when connecting to the endpoints and then delete the endpoints after you have completed your PowerShell remote session.

You must follow the procedures in [Connecting remotely to your StorSimple device](#) to set up remoting for your cloud appliance.

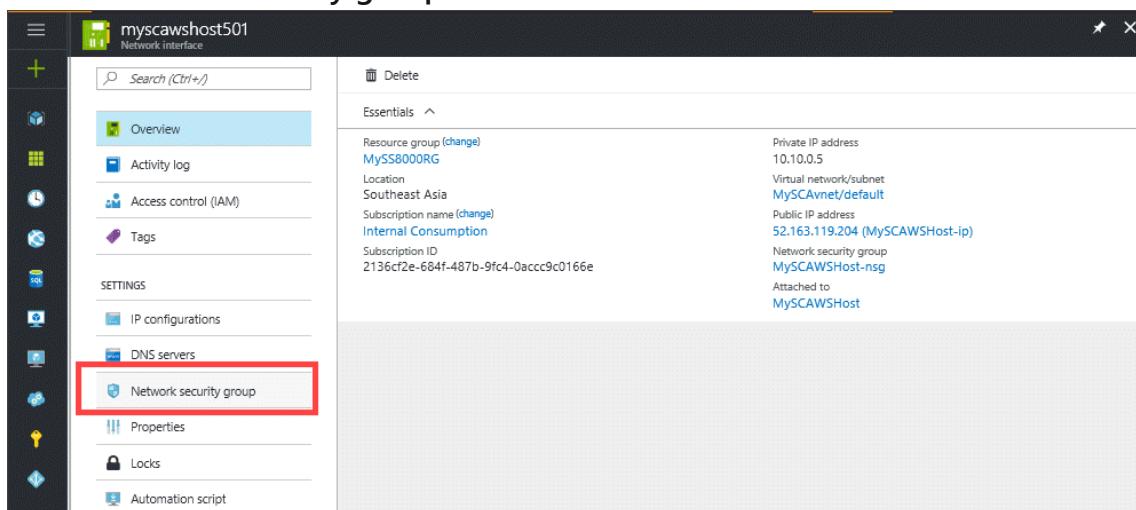
Connect directly to the cloud appliance

You can also connect directly to the cloud appliance. To connect directly to the cloud appliance from another computer outside the virtual network or outside the Microsoft Azure environment, you must create additional endpoints.

Perform the following steps to create a public endpoint on the cloud appliance.

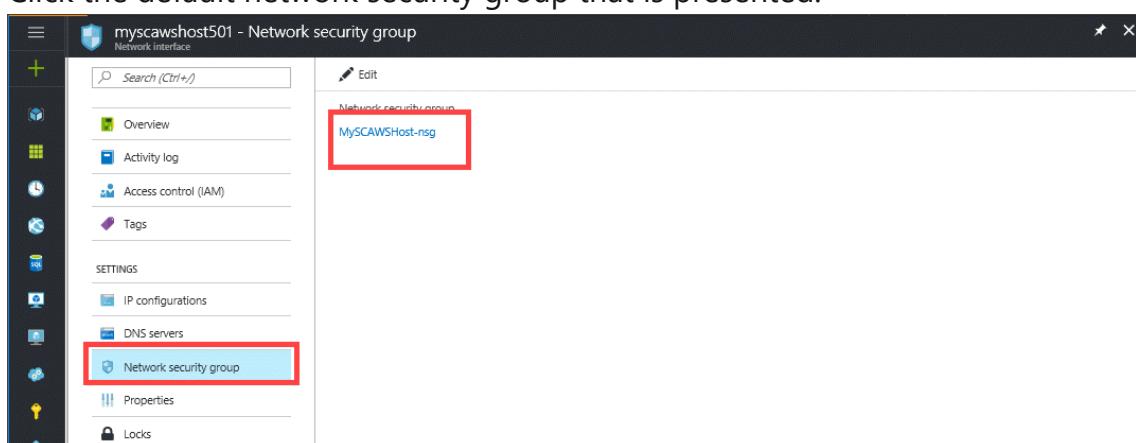
To create public endpoints on the cloud appliance

1. Sign in to the Azure portal.
2. Go to **Virtual Machines**, and then select and click the virtual machine that is being used as your cloud appliance.
3. You need to create a network security group (NSG) rule to control the flow of traffic in and out of your virtual machine. Perform the following steps to create an NSG rule.
 - a. Select **Network security group**.



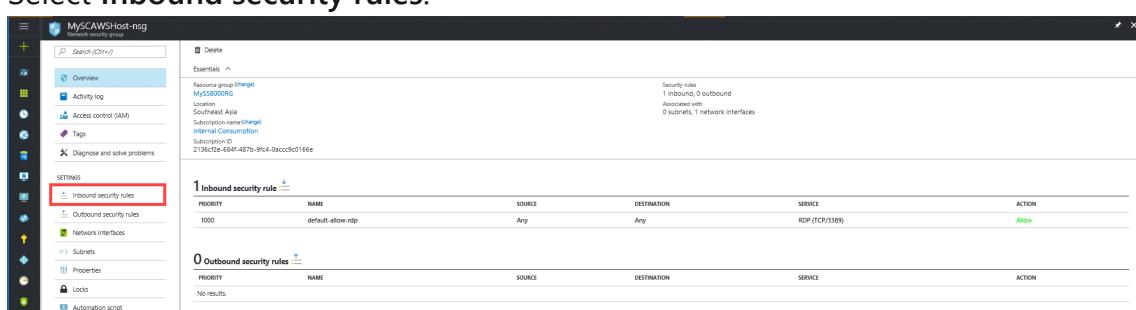
The screenshot shows the Azure portal interface for a network interface named 'myscawhost501'. The left sidebar has a 'Network security group' option highlighted with a red box. The main pane displays the 'Essentials' section with details about the resource group, location, subscription, and attached network security group 'MySCAWSHost-nsg'.

- b. Click the default network security group that is presented.



The screenshot shows the 'Network security group' settings for 'myscawhost501'. The 'Network security group' option is highlighted with a red box. The main pane displays the 'Network security group' section with the name 'MySCAWSHost-nsg'.

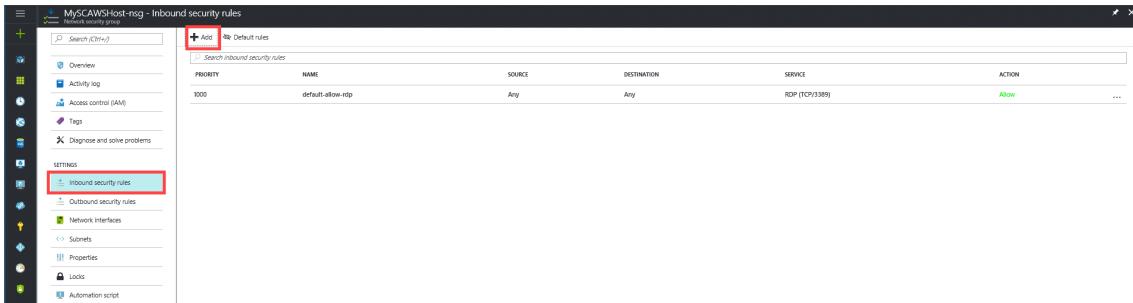
- c. Select **Inbound security rules**.



The screenshot shows the 'Inbound security rules' section for 'MySCAWSHost-nsg'. It lists one rule: 'default-allow-rdp' with priority 1000, source Any, destination Any, service RDP (TCP/3389), and action Allow.

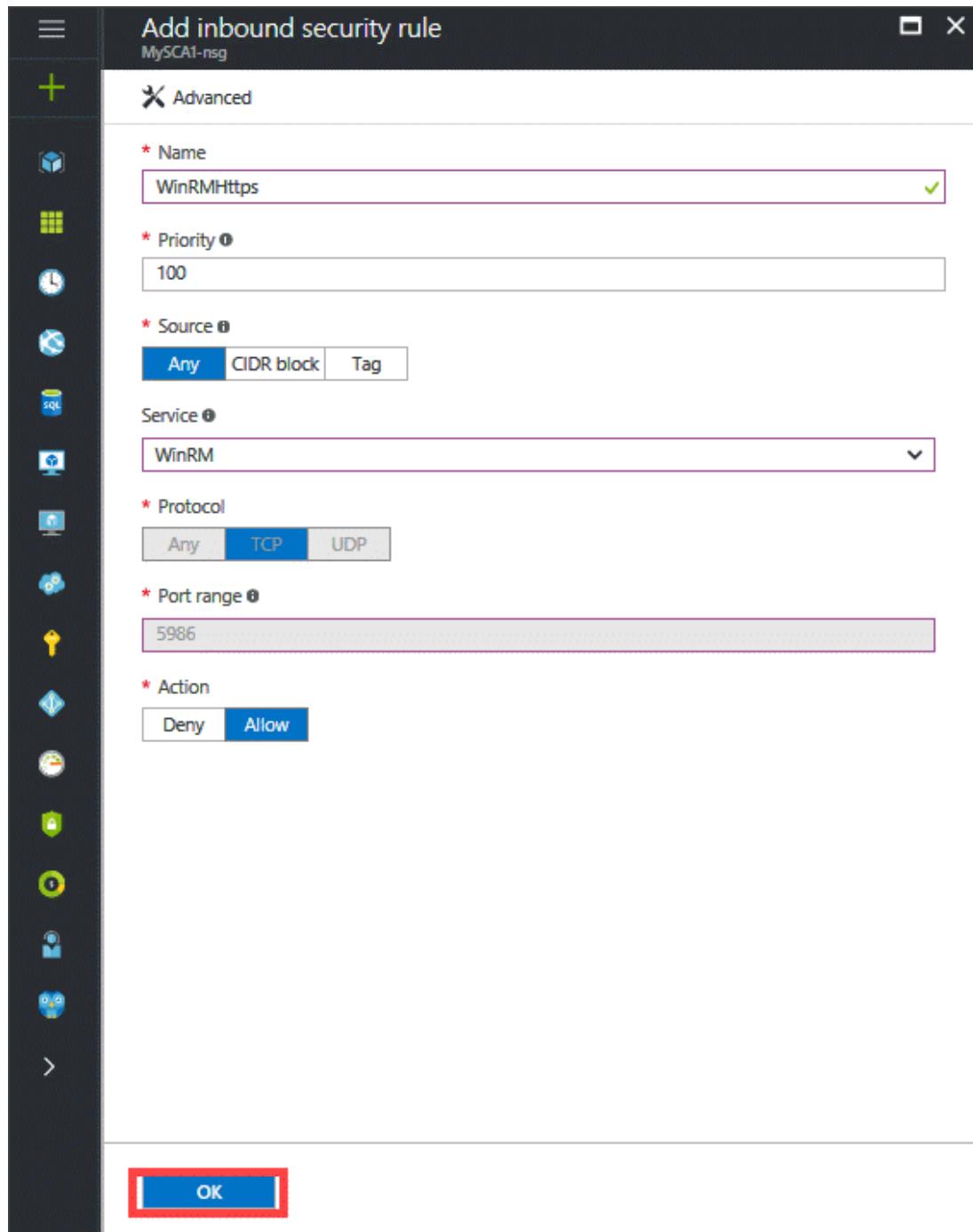
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1000	default-allow-rdp	Any	Any	RDP (TCP/3389)	Allow

d. Click **+ Add** to create an inbound security rule.



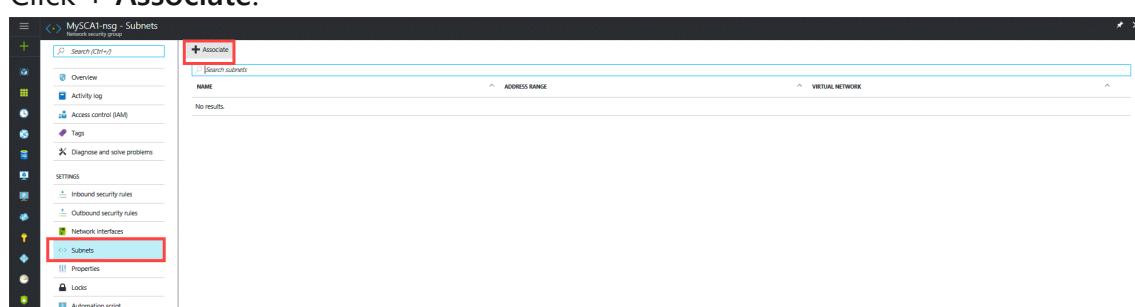
In the Add inbound security rule blade:

- i. For the **Name**, type the following name for the endpoint: WinRMHttps.
- ii. For the **Priority**, select a number lesser than 1000 (which is the priority for the default rule). Higher the value, lower the priority.
- iii. Set the **Source** to **Any**.
- iv. For the **Service**, select **WinRM**. The **Protocol** is automatically set to **TCP** and the **Port range** is set to **5986**.
- v. Click **OK** to create the rule.



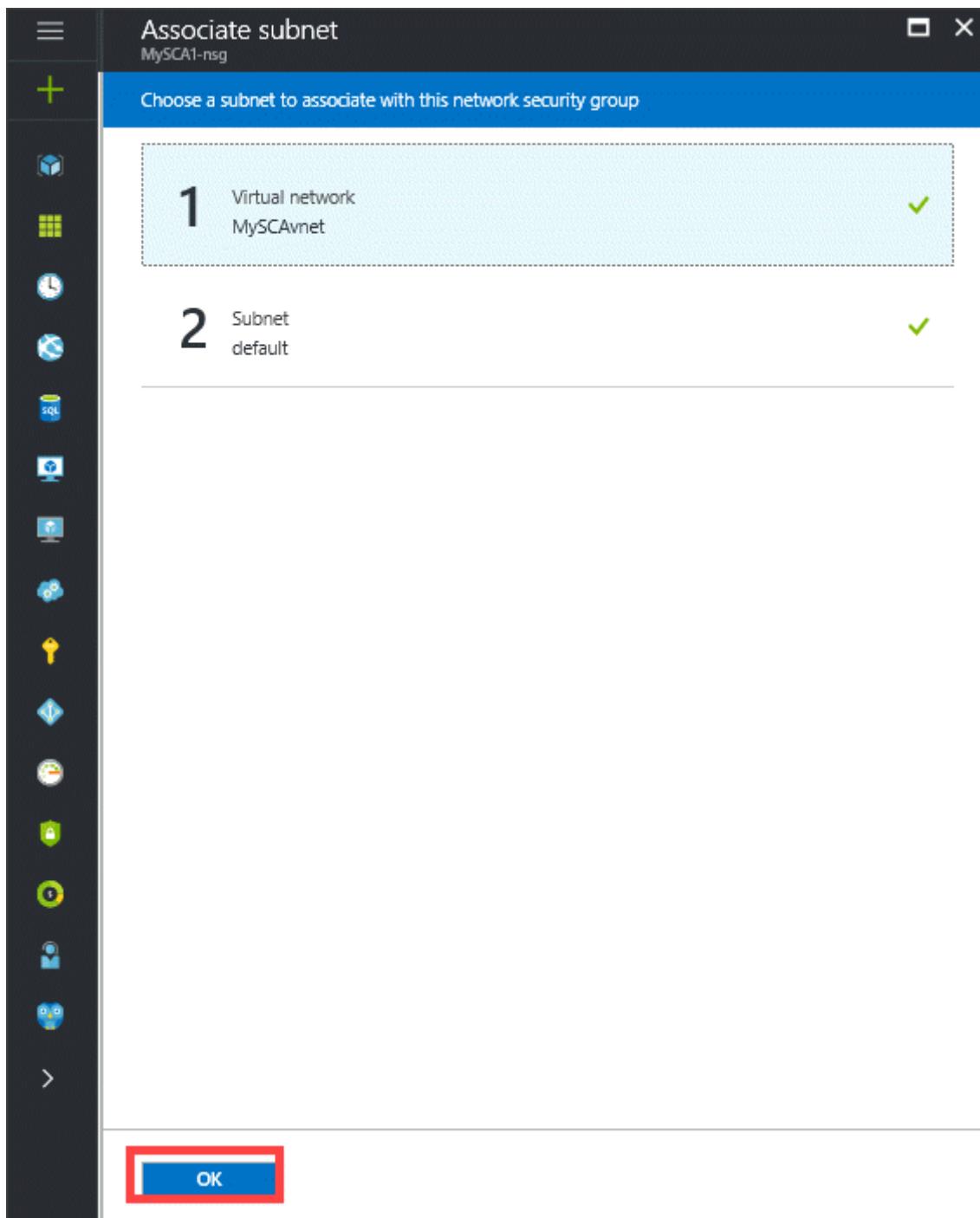
4. Your final step is to associate your network security group with a subnet or a specific network interface. Perform the following steps to associate your network security group with a subnet.

- Go to Subnets.
- Click + Associate.



c. Select your virtual network, and then select the appropriate subnet.

d. Click **OK** to create the rule.



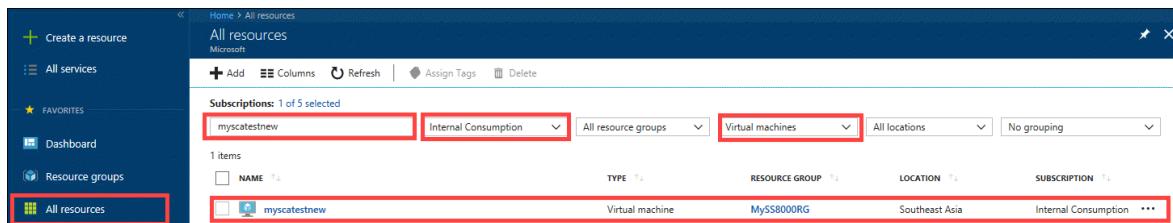
After the rule is created, you can view its details to determine the Public Virtual IP (VIP) address. Record this address.

We recommend that you connect from another virtual machine inside the same virtual network because this practice minimizes the number of public endpoints on your virtual network. In this case, connect to the virtual machine through a Remote Desktop session and then configure that virtual machine for use as you would any other Windows client on a local network. You do not need to append the public port number because the port is already known.

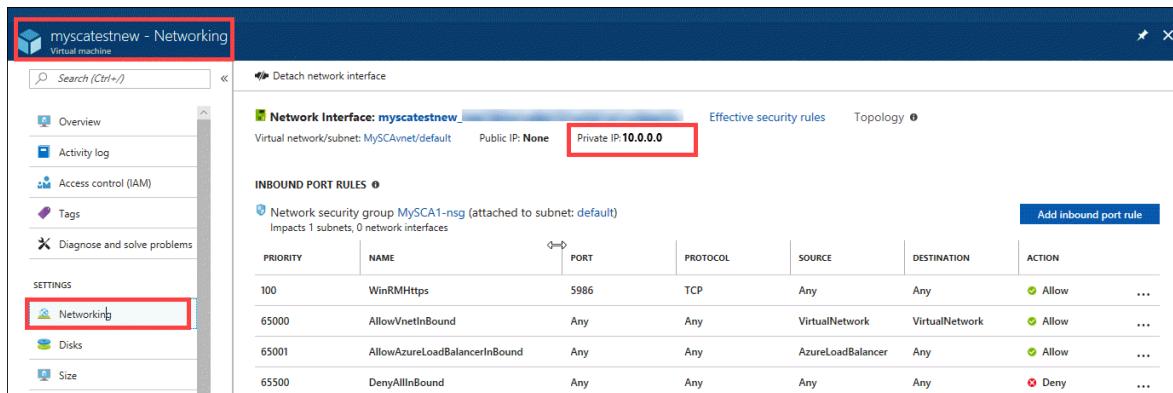
Get private IP for the cloud appliance

For the cloud appliance to connect to the host server in the same virtual network, you need the internal or the private IP address of the cloud appliance. Perform the following steps to get the private IP address of the cloud appliance

1. Go to the underlying virtual machine for your cloud appliance. The virtual machine has the same name as your cloud appliance. Go to **All resources**, provide the name of cloud appliance and subscription, and select type as virtual machines. In the list of virtual machines presented, select and click the virtual machine corresponding to the cloud appliance.



2. Go to **Settings > Networking**. In the right pane, you see the private IP address of the cloud appliance. Make a note of it.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	WinRMHttps	5986	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Work with the StorSimple Cloud Appliance

Now that you have created and configured the StorSimple Cloud Appliance, you are ready to start working with it. You can work with volume containers, volumes, and backup policies on a cloud appliance just as you would on a physical StorSimple device. The only difference is that you need to make sure that you select the cloud appliance from your device list. Refer to [use the StorSimple Device Manager service to manage a cloud appliance](#) for step-by-step procedures of the various management tasks for the cloud appliance.

The following sections discuss some of the differences you encounter when working with the cloud appliance.

Maintain a StorSimple Cloud Appliance

Because it is a software-only device, maintenance for the cloud appliance is minimal when compared to maintenance for the physical device.

You cannot update a cloud appliance. Use the latest version of software to create a new cloud appliance.

Storage accounts for a cloud appliance

Storage accounts are created for use by the StorSimple Device Manager service, by the cloud appliance, and by the physical device. When you create your storage accounts, we recommend that you use a region identifier in the friendly name. This helps ensure that the region is consistent throughout all of the system components. For a cloud appliance, it is important that all the components are in the same region to prevent performance issues.

For a step-by-step procedure, go to [add a storage account](#).

Deactivate a StorSimple Cloud Appliance

When you deactivate a cloud appliance, the action deletes the VM and the resources created when it was provisioned. After the cloud appliance is deactivated, it cannot be restored to its previous state. Before you deactivate the cloud appliance, make sure to stop or delete clients and hosts that depend on it.

Deactivating a cloud appliance results in the following actions:

- The cloud appliance is removed.
- The OS disk and data disks created for the cloud appliance are removed.
- The hosted service and virtual network created during provisioning are retained. If you are not using them, you should delete them manually.
- Cloud snapshots created for the cloud appliance are retained.

For a step-by-step procedure, go to [Deactivate and delete your StorSimple device](#).

As soon as the cloud appliance is shown as deactivated on the StorSimple Device Manager service blade, you can delete the cloud appliance from device list on the **Devices** blade.

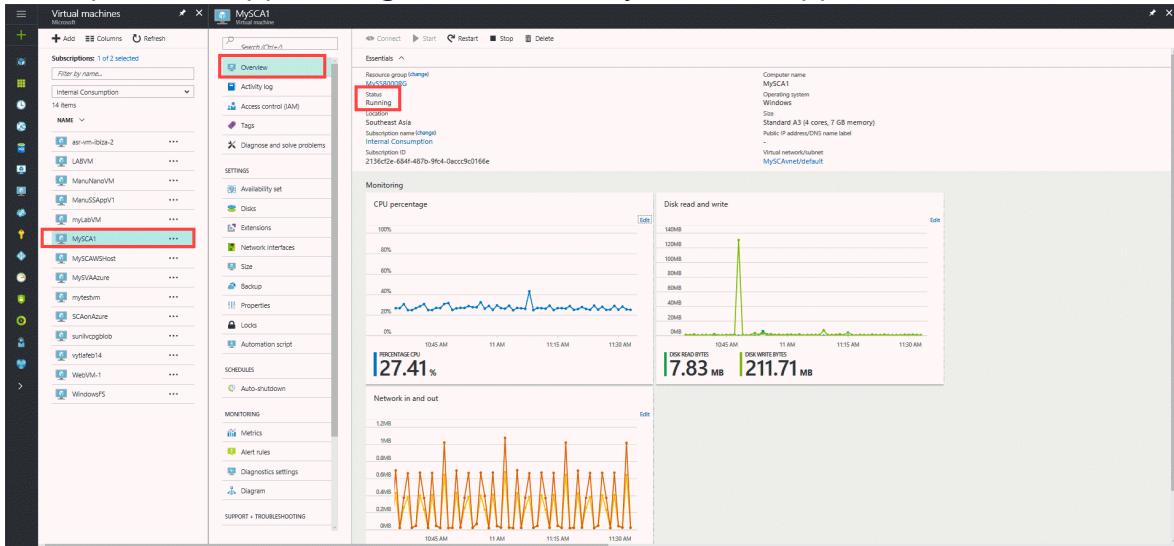
Start, stop, and restart a cloud appliance

Unlike the StorSimple physical device, there is no power on or power off button to push on a StorSimple Cloud Appliance. However, there may be occasions where you need to stop and restart the cloud appliance.

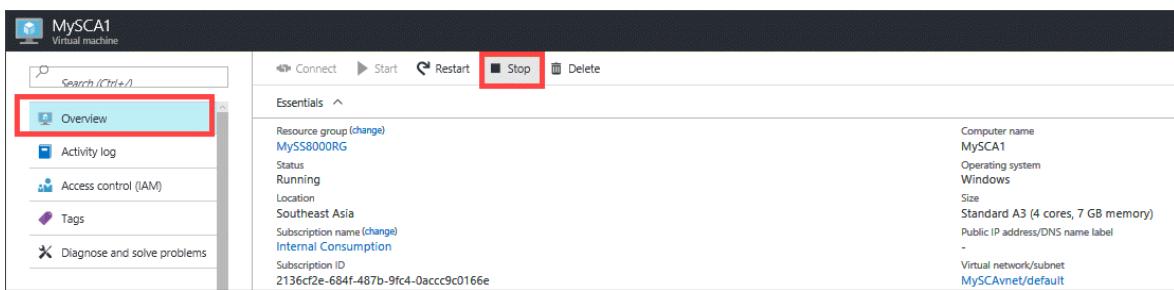
The easiest way for you to start, stop, and restart a cloud appliance is via the Virtual Machines service blade. Go the Virtual machine service. From the list of VMs, identify the VM corresponding to your cloud appliance (same name), and click the VM name. When you look at your virtual machine blade, the cloud appliance status is **Running** because it is started by default after it is created. You can start, stop, and restart a virtual machine at any time.

To stop and start a cloud appliance

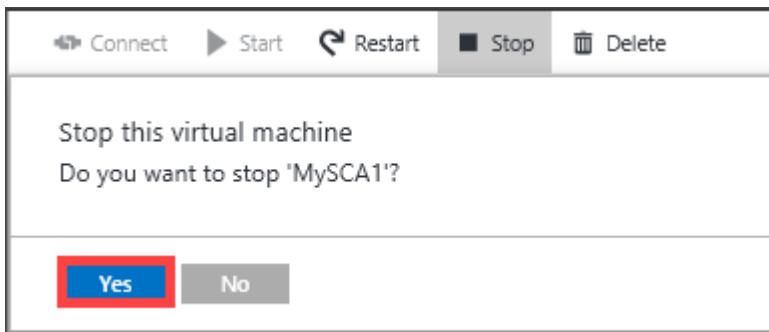
1. To stop a cloud appliance, go to the VM for your cloud appliance.



2. From the command bar, click Stop.



3. When prompted for confirmation, click Yes.



4. When you stop a VM, it gets deallocated. While the cloud appliance is stopping, its status is **Deallocating**. After the cloud appliance is stopped, its status is **Stopped (deallocated)**.

Setting	Value
Computer name	MySCA1
Operating system	Windows
Size	Standard A3 (4 cores, 7 GB memory)
Public IP address/DNS name label	-
Virtual network/subnet	MySCAvnet/default

5. Once a VM is stopped, click **Start** (button becomes available) to start the VM. After the cloud appliance has started up, its status is **Started**.

Setting	Value
Computer name	MySCA1
Operating system	Windows
Size	Standard A3 (4 cores, 7 GB memory)
Public IP address/DNS name label	-
Virtual network/subnet	MySCAvnet/default

Use the following cmdlets to stop and start a cloud appliance.

```
Stop-AzureVM -ServiceName "MyStorSimpleService1" -Name "MyStorSimpleDevice"
```

```
Start-AzureVM -ServiceName "MyStorSimpleService1" -Name "MyStorSimpleDevice"
```

To restart a cloud appliance

To restart a cloud appliance, go to the VM for your cloud appliance. From the command bar, click **Restart**. When prompted, confirm the restart. When the cloud appliance is ready for you to use, its status is **Running**.

Connect	Start	Restart	Stop	Delete
Essentials ^				
Resource group (change)				Computer name
MySS8000RG				MySCA1
Status	Running			Operating system
Location	Southeast Asia			Windows
Subscription name (change)	Internal Consumption			Size
Subscription ID	2136cf2e-684f-487b-9fc4-0accc9c0166e			Standard A3 (4 cores, 7 GB memory)
				Public IP address/DNS name label
				-
				Virtual network/subnet
				MySCAvnet/default

Use the following cmdlet to restart a cloud appliance.

```
Restart-AzureVM -ServiceName "MyStorSimpleService1" -Name "MyStorSimpleDevice"
```

Reset to factory defaults

If you decide that you want to start over with your cloud appliance, deactivate and delete it and then create a new one.

Fail over to the cloud appliance

Disaster recovery (DR) is one of the key scenarios that the StorSimple Cloud Appliance was designed for. In this scenario, the physical StorSimple device or entire datacenter may not be available. Fortunately, you can use a cloud appliance to restore operations in an alternate location. During DR, the volume containers from the source device change ownership and are transferred to the cloud appliance.

The prerequisites for DR are:

- The cloud appliance is created and configured.
- All the volumes within the volume container are offline.
- The volume container that you fail over, has an associated cloud snapshot.

ⓘ Note

- When using a cloud appliance as the secondary device for DR, keep in mind that the 8010 has 30 TB of Standard Storage and 8020 has 64 TB of Premium Storage. The higher capacity 8020 cloud appliance may be more suited for a DR scenario.

For a step-by-step procedure, go to [fail over to a cloud appliance](#).

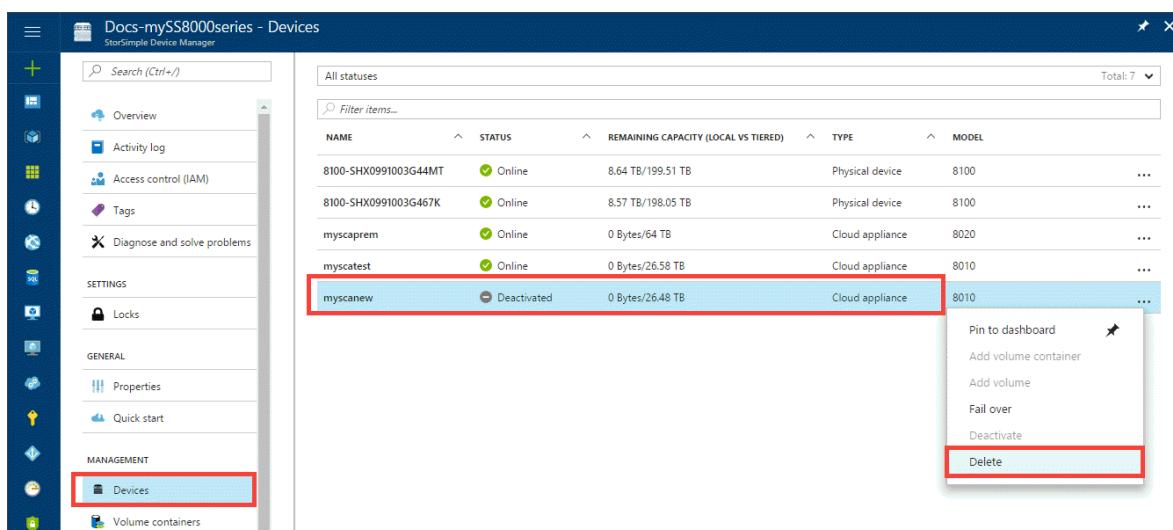
Delete the cloud appliance

If you previously configured and used a StorSimple Cloud Appliance but now want to stop accruing compute charges for its use, you must stop the cloud appliance. Stopping the cloud appliance deallocates the VM. This action will stop from charges accruing on your subscription. The storage charges for the OS and data disks will however continue.

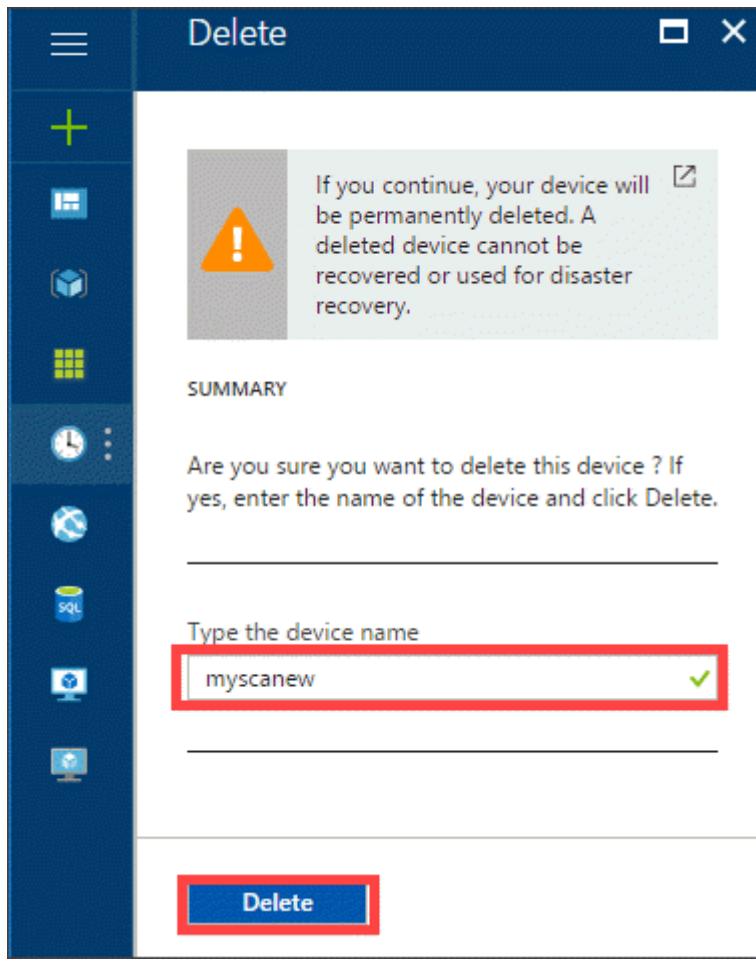
To stop all the charges, you must delete the cloud appliance. To delete the backups created by the cloud appliance, you can deactivate or delete the device. For more information, see [Deactivate and delete a StorSimple device](#).

To delete a cloud appliance

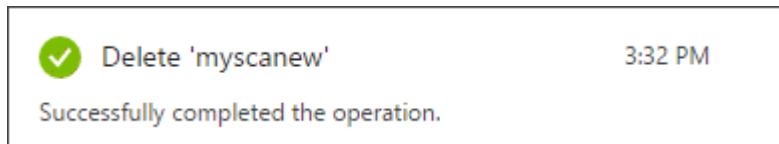
1. Sign in to the Azure portal.
2. You can only delete a deactivated device that does not contain data. Delete the data on the device first or you can [fail over the data](#) in volume containers to another device. Once the data is deleted, you are ready to deactivate the device.
3. In your StorSimple Device Manager service page, click **Devices** and then select the device. Right-click and select **Deactivate**.
4. Once the device is deactivated, right-click the device and select **Delete**.



5. Type the device name to confirm the deletion. After the device is deleted, the device list updates.



6. You are notified after the device is deleted.



7. The list of devices updates to indicate the deleted device.

The screenshot shows the 'Devices' list in the StarSimple Device Manager. The left sidebar has sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS (Locks), GENERAL (Properties, Quick start), and MANAGEMENT (Devices). The 'Devices' item is highlighted with a red box. The main pane displays a table of devices with columns: NAME, STATUS, REMAINING CAPACITY (LOCAL VS TIERED), TYPE, and MODEL. The table shows four entries: 8100-SHX0991003G44MT, 8100-SHX0991003G467K, myscaprem, and myscatest. The 'myscaprem' row is highlighted with a light blue background.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.64 TB/199.51 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100
myscaprem	Online	0 Bytes/64 TB	Cloud appliance	8020
mysctest	Online	0 Bytes/26.58 TB	Cloud appliance	8010

Troubleshoot Internet connectivity errors

During the creation of a cloud appliance, if there is no connectivity to the Internet, the creation step fails. To troubleshoot Internet connectivity failures, perform the following steps in the Azure portal:

1. [Create a Windows virtual machine in the Azure portal](#). This virtual machine should use the same storage account, VNet, and subnet as used by your cloud appliance. If there is an existing Windows Server host in Azure using the same storage account, VNet, and subnet, you can also use it to troubleshoot the Internet connectivity.
2. Remote log into the virtual machine created in the preceding step.
3. Open a command window inside the virtual machine (Win + R and then type `cmd`).
4. Run the following cmd at the prompt.

```
nslookup windows.net
```

5. If `nslookup` fails, then Internet connectivity failure is preventing the cloud appliance from registering to the StorSimple Device Manager service.
6. Make the required changes to your virtual network to ensure that the cloud appliance is able to access Azure sites such as *windows.net*.

Next steps

- Learn how to [use the StorSimple Device Manager service to manage a cloud appliance](#).
- Understand how to [restore a StorSimple volume from a backup set](#).

Deploy the StorSimple Snapshot Manager MMC snap-in

Article • 08/22/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Snapshot Manager is a Microsoft Management Console (MMC) snap-in that simplifies data protection and backup management in a Microsoft Azure StorSimple environment. With StorSimple Snapshot Manager, you can manage Microsoft Azure StorSimple on-premises and cloud storage as if it were a fully integrated storage system, thus simplifying backup and restore processes and reducing costs.

This tutorial describes configuration requirements, as well as procedures for installing, removing, and upgrading StorSimple Snapshot Manager.

(!) Note

- You cannot use StorSimple Snapshot Manager to manage Microsoft Azure StorSimple Virtual Arrays (also known as StorSimple on-premises virtual devices).
- If you plan to install StorSimple Update 2 on your StorSimple device, be sure to download the latest version of StorSimple Snapshot Manager and install it **before you install StorSimple Update 2**. The latest version of StorSimple Snapshot Manager is backward compatible and works with all released versions of Microsoft Azure StorSimple. If you are using the previous version of StorSimple Snapshot Manager, you will need to update it (you do not need to uninstall the previous version before you install the new version).

StorSimple Snapshot Manager installation

StorSimple Snapshot Manager can be installed on computers that are running the Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 R2 operating system. On servers running Windows 2008 R2, you must also install Windows Server 2008 SP1 and Windows Management Framework 3.0.

Before you install or upgrade the StorSimple Snapshot Manager snap-in for the Microsoft Management Console (MMC), make sure that the Microsoft Azure StorSimple device and host server are configured correctly.

Configure prerequisites

The following steps provide a high-level overview of configuration tasks that you must complete before you install the StorSimple Snapshot Manager. For complete Microsoft Azure StorSimple configuration and setup information, including system requirements and step-by-step instructions, see [Deploy your on-premises StorSimple device](#).

 **Important**

Before you begin, review the [Deployment configuration checklist](#) and [Deployment prerequisites](#) in [Deploy your on-premises StorSimple device](#).

Before you install StorSimple Snapshot Manager

1. Unpack, mount, and connect the Microsoft Azure StorSimple device as described in [Install your StorSimple 8100 device](#) or [Install your StorSimple 8600 device](#).
 2. Make sure that your host computer is running one of the following operating systems:
 - Windows Server 2008 R2 (on servers running Windows 2008 R2, you must also install Windows Server 2008 SP1 and Windows Management Framework 3.0)
 - Windows Server 2012
 - Windows Server 2012 R2
- For a StorSimple virtual device, the host must be a Microsoft Azure Virtual Machine.

3. Make sure that you meet all the Microsoft Azure StorSimple configuration requirements. For details, go to [Deployment prerequisites](#).
4. Connect the device to the host and perform the initial configuration. For details, go to [Deployment steps](#).
5. Create volumes on the device, assign them to the host, and verify that the host can mount and use them. StorSimple Snapshot Manager supports the following types of volumes:
 - Basic volumes
 - Simple volumes
 - Dynamic volumes
 - Mirrored dynamic volumes (RAID 1)
 - Cluster-shared volumes

For information about creating volumes on the StorSimple device or StorSimple virtual device, go to [Step 6: Create a volume](#), in [Deploy your on-premises StorSimple device](#).

Install a new StorSimple Snapshot Manager

Before installing StorSimple Snapshot Manager, make sure that the volumes you created on the StorSimple device or StorSimple virtual device are mounted, initialized, and formatted as described in [Configure prerequisites](#).

Important

- For a StorSimple virtual device, the host must be a Microsoft Azure Virtual Machine.
- The host must be running Windows 2008 R2, Windows Server 2012, or Windows Server 2012 R2. If your server is running Windows Server 2008 R2, you must also install Windows Server 2008 SP1 and Windows Management Framework 3.0.
- You must configure an iSCSI connection from the host to the StorSimple device before you can connect the device to StorSimple Snapshot Manager.

Follow these steps to complete a fresh installation of StorSimple Snapshot Manager. If you are installing an upgrade, go to [Upgrade or reinstall StorSimple Snapshot Manager](#).

- Step 1: Install StorSimple Snapshot Manager
- Step 2: Connect StorSimple Snapshot Manager to a device
- Step 3: Verify the connection to the device

Step 1: Install StorSimple Snapshot Manager

Use the following steps to install StorSimple Snapshot Manager.

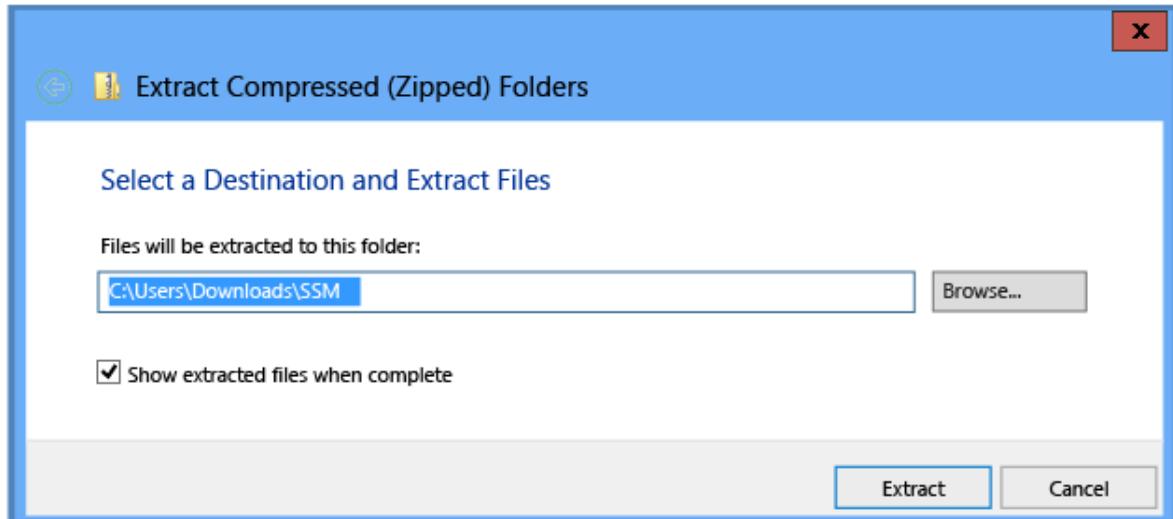
To install StorSimple Snapshot Manager

1. Download the StorSimple Snapshot Manager software (go to [StorSimple Snapshot Manager](#) in the Microsoft Download Center) and save it locally on the host.
2. In File Explorer, right-click the compressed folder, and then click **Extract all**.
3. In the **Extract Compressed (Zipped) Folders** window, in the **Select a destination and extract files** box, type or browse to the path where you would like to file to be extracted.

ⓘ Important

You must install StorSimple Snapshot Manager on the C: drive.

4. Select the **Show extracted files when complete** check box, and then click **Extract**.



5. When the extraction is finished, the destination folder opens. Double-click the application setup icon that appears in the destination folder.

6. When the **Setup Successful** message appears, click **Close**. You should see the StorSimple Snapshot Manager icon on your desktop.

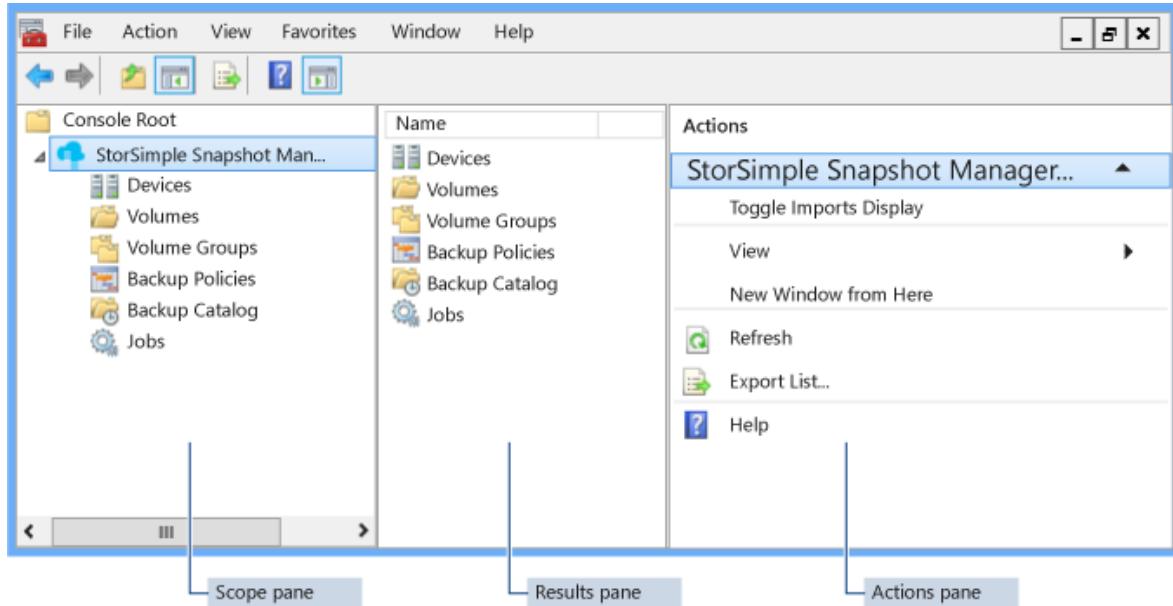


Step 2: Connect StorSimple Snapshot Manager to a device

Use the following steps to connect StorSimple Snapshot Manager to a StorSimple device.

To connect StorSimple Snapshot Manager to a device

1. Click the StorSimple Snapshot Manager icon on your desktop. The StorSimple Snapshot Manager window appears. The window contains a **Scope** pane, a **Results** pane, and an **Actions** pane.



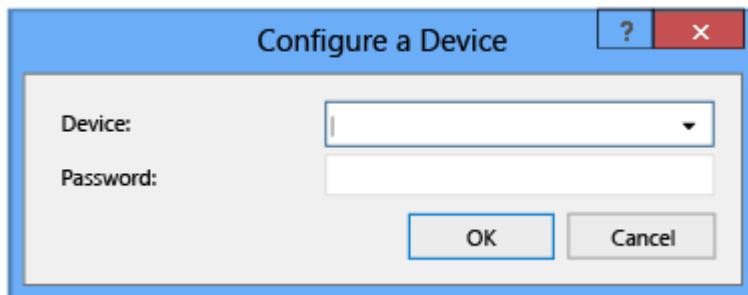
- The **Scope** pane (the left pane) contains a list of nodes organized in a tree structure. You can expand some nodes to select a view or specific data related to that node. Click the arrow icon to expand or collapse a node. Right-click an item in the **Scope** pane to see a list of available actions for that item.
- The **Results** pane (the center pane) contains detailed status information about the node, view, or data that you selected in the **Scope** pane.

- The **Actions** pane lists the operations that you can perform on the node, view, or data that you selected in the **Scope** pane.

For a complete description of the StorSimple Snapshot Manager user interface, see [StorSimple Snapshot Manager user interface](#).

2. In the Scope pane, right-click the **Devices** node, and then click **Configure a device**.

The **Configure a Device** dialog box appears.



3. In the **Device** list box, select the IP address of the Microsoft Azure StorSimple device or virtual device. In the **Password** text box, type the StorSimple Snapshot Manager password that you created for the device in the Azure portal. Click **OK**.

4. StorSimple Snapshot Manager searches for the device that you identified. If the device is available, StorSimple Snapshot Manager adds a connection. You can [verify the connection to the device](#) to confirm that the connection was added successfully.

If the device is unavailable for any reason, StorSimple Snapshot Manager returns an error message. Click **OK** to close the error message, and then click **Cancel** to close the **Configure a Device** dialog box.

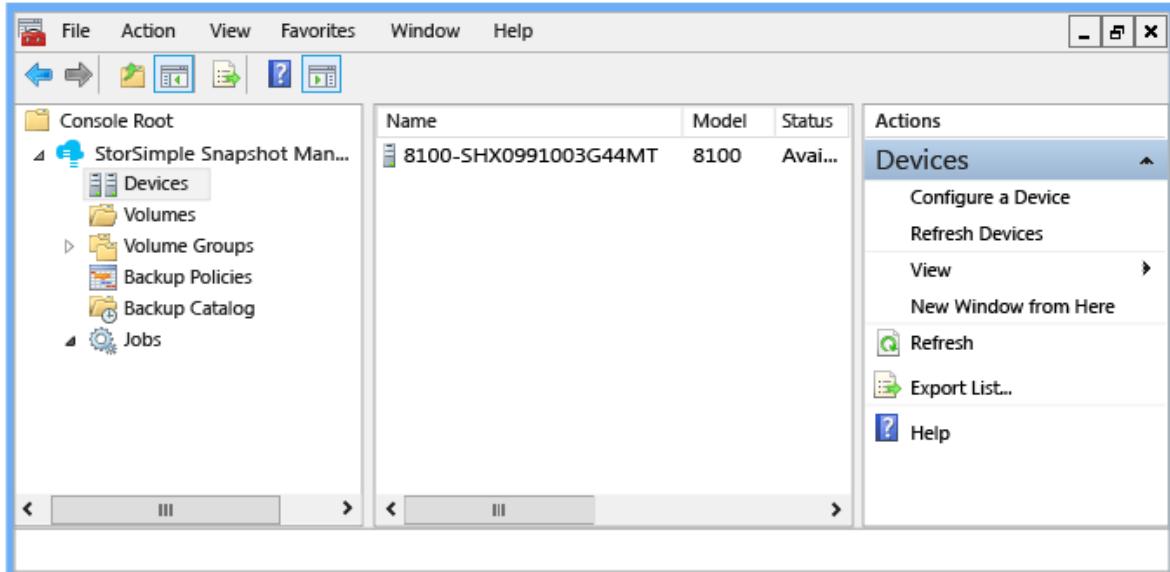
5. When it connects to a device, StorSimple Snapshot Manager imports each volume group configured for that device, provided that the volume group has associated backups. Volume groups that do not have associated backups are not imported. Additionally, backup policies that were created for a volume group are not imported. To see the imported groups, right-click the top-most **Volume Groups** node in the **Scope** pane, and click **Toggle imported groups**.

Step 3: Verify the connection to the device

Use the following steps to verify that StorSimple Snapshot Manager is connected to the StorSimple device.

To verify the connection

1. In the Scope pane, click the Devices node.



2. Check the **Results** pane:

- If a green indicator appears on the device icon and **Available** appears in the **Status** column, then the device is connected.
- If a red indicator appears on the device icon and **Unavailable** appears in the **Status** column, then the device is not connected.
- If **Refreshing** appears in the **Status** column, then StorSimple Snapshot Manager is retrieving volume groups and associated backups for a connected device.

Upgrade or reinstall StorSimple Snapshot Manager

You should uninstall StorSimple Snapshot Manager completely before you upgrade or reinstall the software.

Before reinstalling StorSimple Snapshot Manager, back up the existing StorSimple Snapshot Manager database on the host computer. This saves the backup policies and configuration information so that you can easily restore this data from backup.

Follow these steps if you are upgrading or reinstalling StorSimple Snapshot Manager:

- Step 1: Uninstall StorSimple Snapshot Manager
- Step 2: Back up the StorSimple Snapshot Manager database
- Step 3: Reinstall StorSimple Snapshot Manager and restore the database

Step 1: Uninstall StorSimple Snapshot Manager

Use the following steps to uninstall StorSimple Snapshot Manager.

To uninstall StorSimple Snapshot Manager

1. On the host computer, open the **Control Panel**, click **Programs**, and then click **Programs and Features**.
2. In the left pane, click **Uninstall or change a program**.
3. Right-click **StorSimple Snapshot Manager**, and then click **Uninstall**.
4. This starts the StorSimple Snapshot Manager Setup program. Click **Modify Setup**, and then click **Uninstall**.

Note

If there are any MMC processes running in the background, such as StorSimple Snapshot Manager or Disk Management, the uninstall will fail and you will receive a message to close all instances of MMC before you attempt to uninstall the program. Select **Automatically close applications and attempt to restart them after setup is complete**, and then click **OK**.

5. When the uninstall process is finished, a **Setup Successful** message appears. Click **Close**.

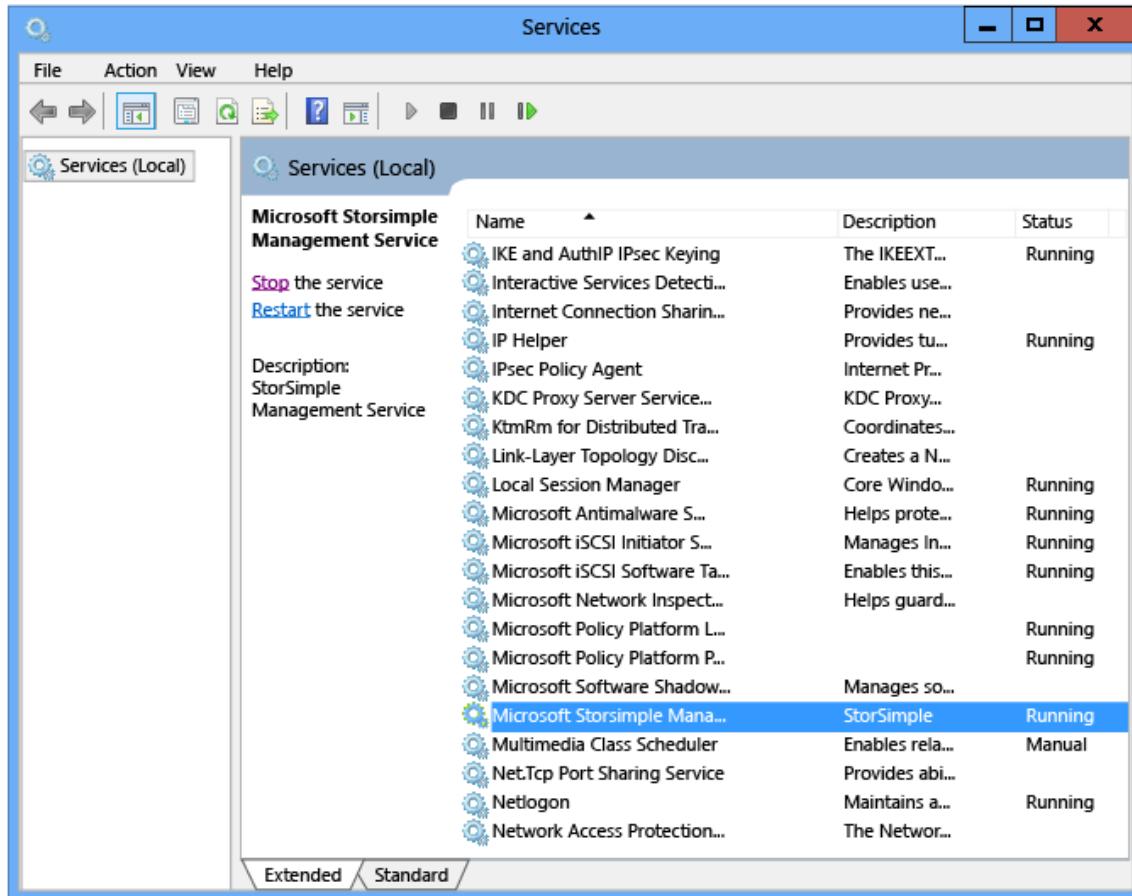
Step 2: Back up the StorSimple Snapshot Manager database

Use the following steps to create and save a copy of the StorSimple Snapshot Manager database.

To back up the database

1. Stop the Microsoft StorSimple Management Service:
 - a. Start Server Manager.
 - b. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - c. On the **Services** page, select **Microsoft StorSimple Management Service**.

- d. In the right pane, under Microsoft StorSimple Management Service, click Stop the service.



2. Browse to C:\ProgramData\Microsoft\StorSimple\BACatalog.

! Note

ProgramData is a hidden folder.

3. Find the catalog XML file, copy the file, and store the copy in a safe location or in the cloud.

Name	Date modified	Type	Size
BACatalog	3/4/2014 10:34 AM	File folder	
BACatalog.bak	2/12/2014 12:31 PM	File folder	
ManagementService_2014-02-13_...	2/19/2014 5:42 AM	Text Doc...	1,025 KB
ManagementService_2014-02-13_...	2/19/2014 10:27 AM	Text Doc...	1,025 KB
ManagementService_2014-02-13_...	2/19/2014 5:27 PM	Text Doc...	1,025 KB
ManagementService_2014-02-13_...	2/20/2014 11:27 AM	Text Doc...	1,025 KB
ManagementService_2014-02-13_...	2/20/2014 2:07 PM	Text Doc...	164 KB
ManagementService_2014-02-20_...	2/21/2014 7:08 AM	Text Doc...	1,025 KB
ManagementService_2014-02-20_...	2/22/2014 1:23 AM	Text Doc...	1,025 KB
ManagementService_2014-02-20_...	2/22/2014 7:53 PM	Text Doc...	1,025 KB
ManagementService_2014-02-20_...	2/23/2014 2:08 PM	Text Doc...	1,025 KB
ManagementService_2014-02-20_...	2/24/2014 8:23 AM	Text Doc...	1,025 KB
ManagementService_2014-02-20_...	2/25/2014 2:38 AM	Text Doc...	1,025 KB
Management Service_2014-02-20_...	2/25/2014 9:08 PM	Text Doc...	1,025 KB

4. Restart the Microsoft StorSimple Management Service:
 - a. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - b. On the **Services** page, select the **Microsoft StorSimple Management Service**.
 - c. In the right pane, under **Microsoft StorSimple Management Service**, click **Restart the service**.

Step 3: Reinstall StorSimple Snapshot Manager and restore the database

To reinstall StorSimple Snapshot Manager, follow the steps in [Install a new StorSimple Snapshot Manager](#). Then, use the following procedure to restore the StorSimple Snapshot Manager database.

To restore the database

1. Stop the Microsoft StorSimple Management Service:
 - a. Start Server Manager.
 - b. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - c. On the **Services** page, select **Microsoft StorSimple Management Service**.
 - d. In the right pane, under **Microsoft StorSimple Management Service**, click **Stop the service**.
2. Browse to C:\ProgramData\Microsoft\StorSimple\BACatalog.

Note

ProgramData is a hidden folder.

3. Delete the catalog XML file, and replace it with the version that you saved earlier.
4. Restart the Microsoft StorSimple Management Service:
 - a. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - b. On the **Services** page, select **Microsoft StorSimple Management Service**.
 - c. In the right pane, under **Microsoft StorSimple Management Service**, click **Restart the service**.

Next steps

- To learn more about StorSimple Snapshot Manager, go to [What is StorSimple Snapshot Manager?](#).
- To learn more about the StorSimple Snapshot Manager user interface, go to [StorSimple Snapshot Manager user interface](#).
- To learn more about using StorSimple Snapshot Manager, go to [Use StorSimple Snapshot Manager to administer your StorSimple solution](#).

Install and configure the StorSimple Adapter for SharePoint

Article • 08/22/2022 • 22 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Adapter for SharePoint is a component that lets you provide Microsoft Azure StorSimple flexible storage and data protection to SharePoint Server farms. You can use the adapter to move Binary Large Object (BLOB) content from the SQL Server content databases to the Microsoft Azure StorSimple hybrid cloud storage device.

The StorSimple Adapter for SharePoint functions as a Remote BLOB Storage (RBS) provider and uses the SQL Server Remote BLOB Storage feature to store unstructured SharePoint content (in the form of BLOBs) on a file server that is backed by a StorSimple device.

ⓘ Note

The StorSimple Adapter for SharePoint supports SharePoint Server 2010 Remote BLOB Storage (RBS). It does not support SharePoint Server 2010 External BLOB Storage (EBS).

- To download the StorSimple Adapter for SharePoint, go to [StorSimple Adapter for SharePoint](#) in the Microsoft Download Center.
- For information about planning for RBS and RBS limitations, go to [Deciding to use RBS in SharePoint 2013](#) or [Plan for RBS \(SharePoint Server 2010\)](#).

The rest of this overview briefly describes the role of the StorSimple Adapter for SharePoint and the SharePoint capacity and performance limits that you should be

aware of before you install and configure the adapter. After you review this information, go to [StorSimple Adapter for SharePoint installation](#) to begin setting up the adapter.

StorSimple Adapter for SharePoint benefits

In a SharePoint site, content is stored as unstructured BLOB data in one or more content databases. By default, these databases are hosted on computers that are running SQL Server and are located in the SharePoint Server farm. BLOBS can rapidly increase in size, consuming large amounts of on-premises storage. For this reason, you might want to find another, less-expensive storage solution. SQL Server provides a technology called Remote Blob Storage (RBS) that lets you store BLOB content in the file system, outside the SQL Server database. With RBS, BLOBS can reside in the file system on the computer that is running SQL Server, or they can be stored in the file system on another server computer.

RBS requires that you use an RBS provider, such as the StorSimple Adapter for SharePoint, to enable RBS in SharePoint. The StorSimple Adapter for SharePoint works with RBS, letting you move BLOBS to a server backed up by the Microsoft Azure StorSimple system. Microsoft Azure StorSimple then stores the BLOB data locally or in the cloud, based on usage. BLOBS that are very active (typically referred to as Tier 1 or hot data) reside locally. Less active data and archival data reside in the cloud. After you enable RBS on a content database, any new BLOB content created in SharePoint is stored on the StorSimple device and not in the content database.

The Microsoft Azure StorSimple implementation of RBS provides the following benefits:

- By moving BLOB content to a separate server, you can reduce the query load on SQL Server, which can improve SQL Server responsiveness.
- Azure StorSimple uses deduplication and compression to reduce data size.
- Azure StorSimple provides data protection in the form of local and cloud snapshots. Also, if you place the database itself on the StorSimple device, you can back up the content database and BLOBS together in a crash consistent way. (Moving the content database to the device is only supported for the StorSimple 8000 series device. This feature is not supported for the 5000 or 7000 series.)
- Azure StorSimple includes disaster recovery features including failover, file and volume recovery (including test recovery), and rapid restoration of data.
- You can use data recovery software, such as Kroll Ontrack PowerControls, with StorSimple snapshots of BLOB data to perform item-level recovery of SharePoint content. (This data recovery software is a separate purchase.)
- The StorSimple Adapter for SharePoint plugs into the SharePoint Central Administration portal, allowing you to manage your entire SharePoint solution from a central location.

Moving BLOB content to the file system can provide other cost savings and benefits. For example, using RBS can reduce the need for expensive Tier 1 storage and, because it shrinks the content database, RBS can reduce the number of databases required in the SharePoint Server farm. However, other factors, such as database size limits and the amount of non-RBS content, can also affect storage requirements. For more information about the costs and benefits of using RBS, see [Plan for RBS \(SharePoint Foundation 2010\)](#) and [Deciding to use RBS in SharePoint 2013](#).

Capacity and performance limits

Before you consider using RBS in your SharePoint solution, you should be aware of the tested performance and capacity limits of SharePoint Server 2010 and SharePoint Server 2013, and how these limits relate to acceptable performance. For more information, see [Software Boundaries and Limits for SharePoint 2013](#).

Review the following before you configure RBS:

- Make sure that the total size of the content (the size of a content database plus the size of any associated externalized BLOBs) does not exceed the RBS size limit supported by SharePoint. This limit is 200 GB.

To measure content database and BLOB size

1. Run this query on the Central Administration WFE. Start the SharePoint Management Shell, and then enter the following Windows PowerShell command to get the size of the content databases:

```
Get-SPContentDatabase | Select-Object -ExpandProperty DiskSizeRequired
```

This step gets the size of the content database on the disk.

2. Run one of the following SQL queries in SQL Management Studio on the SQL server box on each content database, and add the result to the number obtained in step 1.

On SharePoint 2013 content databases, enter:

```
SELECT SUM([Size]) FROM [ContentDatabaseName].[dbo].[DocStreams] WHERE  
[Content] IS NULL
```

On SharePoint 2010 content databases, enter:

```
SELECT SUM([Size]) FROM [ContentDatabaseName].[dbo].[AllDocs] WHERE  
[Content] IS NULL
```

This step gets the size of the BLOBS that have been externalized.

- We recommend that you store all BLOB and database content locally on the StorSimple device. The StorSimple device is a two-node cluster for high availability. Placing the content databases and BLOBS on the StorSimple device provides high availability.

Use traditional SQL Server migration best practices to move the content database to the StorSimple device. Move the database only after all BLOB content from the database has been moved to the file share via RBS. If you choose to move the content database to the StorSimple device, we recommend that you configure the content database storage on the device as a primary volume.

- In Microsoft Azure StorSimple, if using tiered volumes, there is no way to guarantee that content stored locally on the StorSimple device will not be tiered to Microsoft Azure cloud storage. Hence, we recommend using StorSimple locally pinned volumes in conjunction with SharePoint RBS. This will ensure that all BLOB content remains locally on the StorSimple device, and is not moved to Microsoft Azure.
- If you do not store the content databases on the StorSimple device, use traditional SQL Server high availability best practices that support RBS. SQL Server clustering supports RBS, while SQL Server mirroring does not.

 **Warning**

If you have not enabled RBS, we do not recommend moving the content database to the StorSimple device. This is an untested configuration.

StorSimple Adapter for SharePoint installation

Before you can install the StorSimple Adapter for SharePoint, you must configure the StorSimple device and make sure that the SharePoint Server farm and SQL Server instantiation meet all prerequisites. This tutorial describes configuration requirements, as well as procedures for installing and upgrading the StorSimple Adapter for SharePoint.

Configure prerequisites

Before you can install the StorSimple Adapter for SharePoint, make sure that the StorSimple device, SharePoint Server farm, and SQL Server instantiation meet the

following prerequisites.

System requirements

The StorSimple Adapter for SharePoint works with the following hardware and software:

- Supported operating system – Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 R2
- Supported SharePoint versions – SharePoint Server 2010 or SharePoint Server 2013
- Supported SQL Server versions – SQL Server 2008 Enterprise Edition, SQL Server 2008 R2 Enterprise Edition, or SQL Server 2012 Enterprise Edition
- Supported StorSimple devices – StorSimple 8000 series, StorSimple 7000 series, or StorSimple 5000 series.

StorSimple device configuration prerequisites

The StorSimple device is a block device and as such requires a file server on which the data can be hosted. We recommend that you use a separate server rather than an existing server from the SharePoint farm. This file server must be on the same local area network (LAN) as the SQL Server computer that hosts the content databases.

Tip

- If you configure your SharePoint farm for high availability, you should deploy the file server for high availability also.
- If you do not store the content database on the StorSimple device, use traditional high availability best practices that support RBS. SQL Server clustering supports RBS, while SQL Server mirroring does not.

Make sure that your StorSimple device is configured correctly, and that appropriate volumes to support your SharePoint deployment are configured and accessible from your SQL Server computer. Go to [Deploy your on-premises StorSimple device](#) if you have not yet deployed and configured your StorSimple device. Note the IP address of the StorSimple device; you will need it during StorSimple Adapter for SharePoint installation.

In addition, make sure that the volume to be used for BLOB externalization meets the following requirements:

- The volume must be formatted with a 64 KB allocation unit size.

- Your web front end (WFE) and application servers must be able to access the volume via a Universal Naming Convention (UNC) path.
- The SharePoint Server farm must be configured to write to the volume.

Note

After you install and configure the adapter, all BLOB externalization must go through the StorSimple device (the device will present the volumes to SQL Server and manage the storage tiers). You cannot use any other targets for BLOB externalization.

If you plan to use StorSimple Snapshot Manager to take snapshots of the BLOB and database data, be sure to install StorSimple Snapshot Manager on the database server so that it can use the SQL Writer Service to implement the Windows Volume Shadow Copy Service (VSS).

Important

StorSimple Snapshot Manager does not support the SharePoint VSS Writer and cannot take application-consistent snapshots of SharePoint data. In a SharePoint scenario, StorSimple Snapshot Manager provides only crash-consistent backups.

SharePoint farm configuration prerequisites

Make sure that your SharePoint Server farm is correctly configured, as follows:

- Verify that your SharePoint Server farm is in a healthy state, and check the following:
 - All SharePoint WFE and application servers registered in the farm are running and can be pinged from the server on which you will be installing the StorSimple Adapter for SharePoint.
 - The SharePoint Timer service (SPTimerV3 or SPTimerV4) is running on each WFE server and application server.
 - Both the SharePoint Timer service and the IIS application pool under which the SharePoint Central Administration site is running have administrative privileges.
 - Make sure that Internet Explorer Enhanced Security Context (IE ESC) is disabled. Follow these steps to disable IE ESC:

1. Close all instances of Internet Explorer.
2. Start the Server Manager.
3. In the left pane, click **Local Server**.
4. On the right pane, next to **IE Enhanced Security Configuration**, click **On**.
5. Under **Administrators**, click **Off**.
6. Click **OK**.

Remote BLOB Storage (RBS) prerequisites

Make sure that you are using a supported version of SQL Server. Only the following versions are supported and able to use RBS:

- SQL Server 2008 Enterprise Edition
- SQL Server 2008 R2 Enterprise Edition
- SQL Server 2012 Enterprise Edition

BLOBS can be externalized on only those volumes that the StorSimple device presents to SQL Server. No other targets for BLOB externalization are supported.

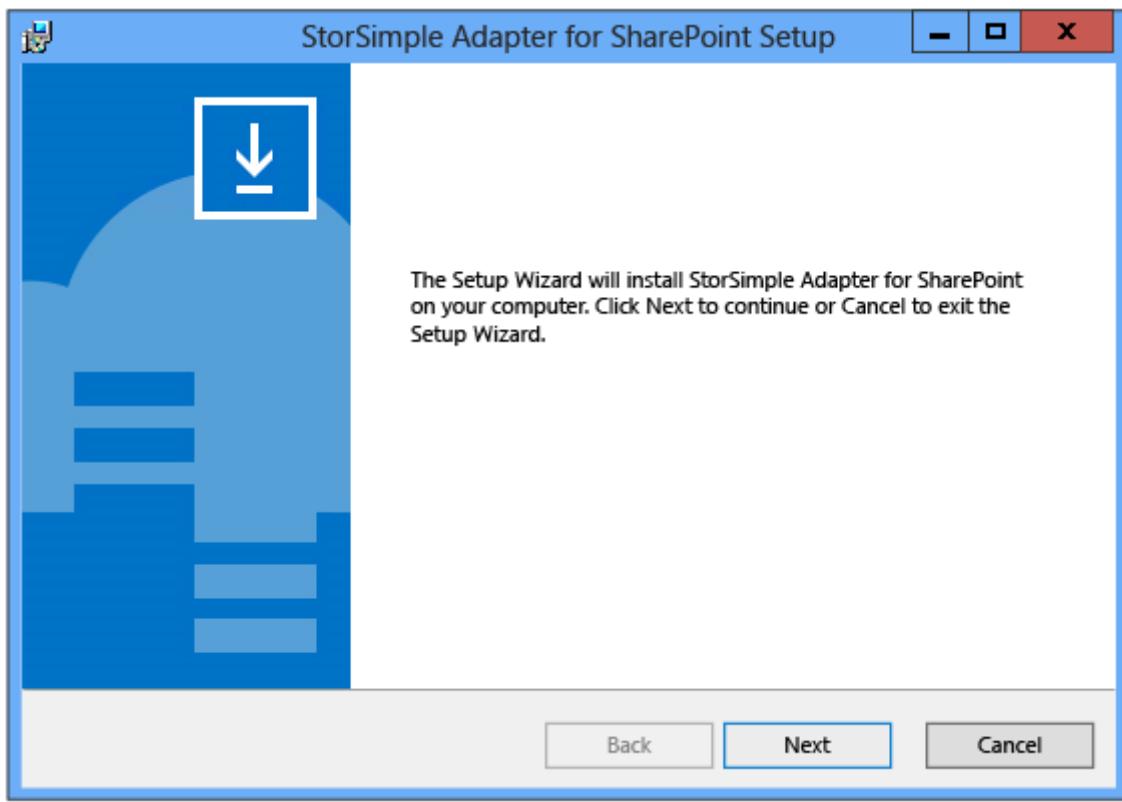
When you have completed all prerequisite configuration steps, go to [Install the StorSimple Adapter for SharePoint](#).

Install the StorSimple Adapter for SharePoint

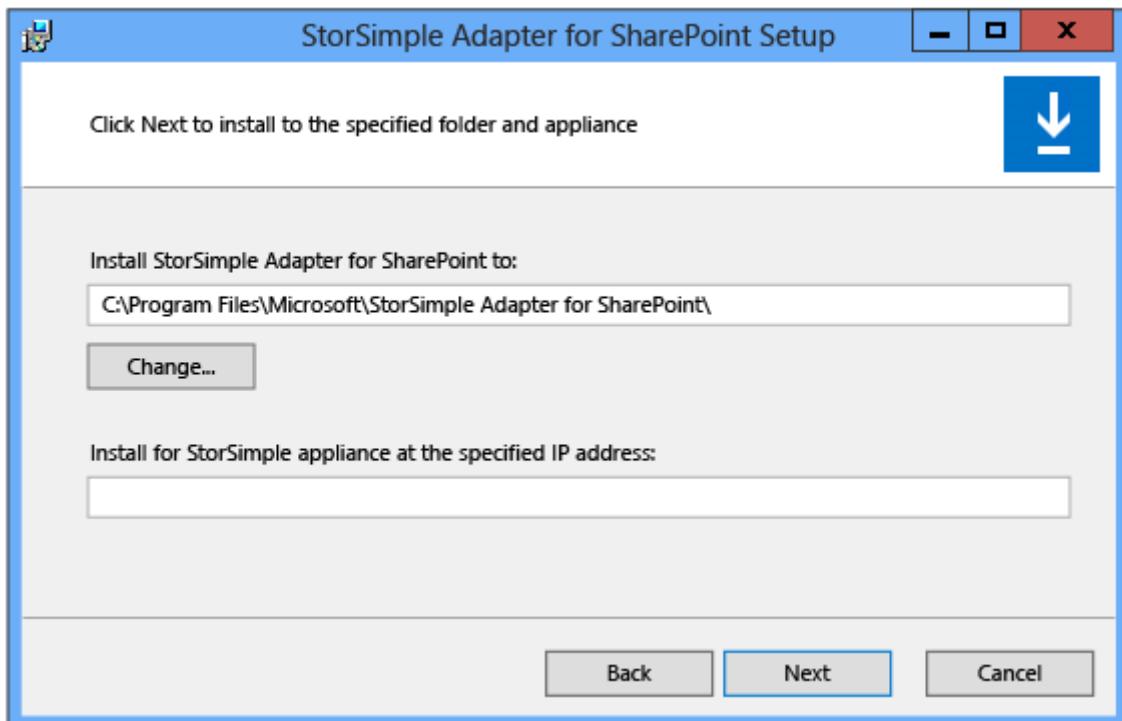
Use the following steps to install the StorSimple Adapter for SharePoint. If you are reinstalling the software, see [Upgrade or reinstall the StorSimple Adapter for SharePoint](#). The time required for the installation depends on the total number of SharePoint databases in your SharePoint Server farm.

To install the StorSimple Adapter for SharePoint

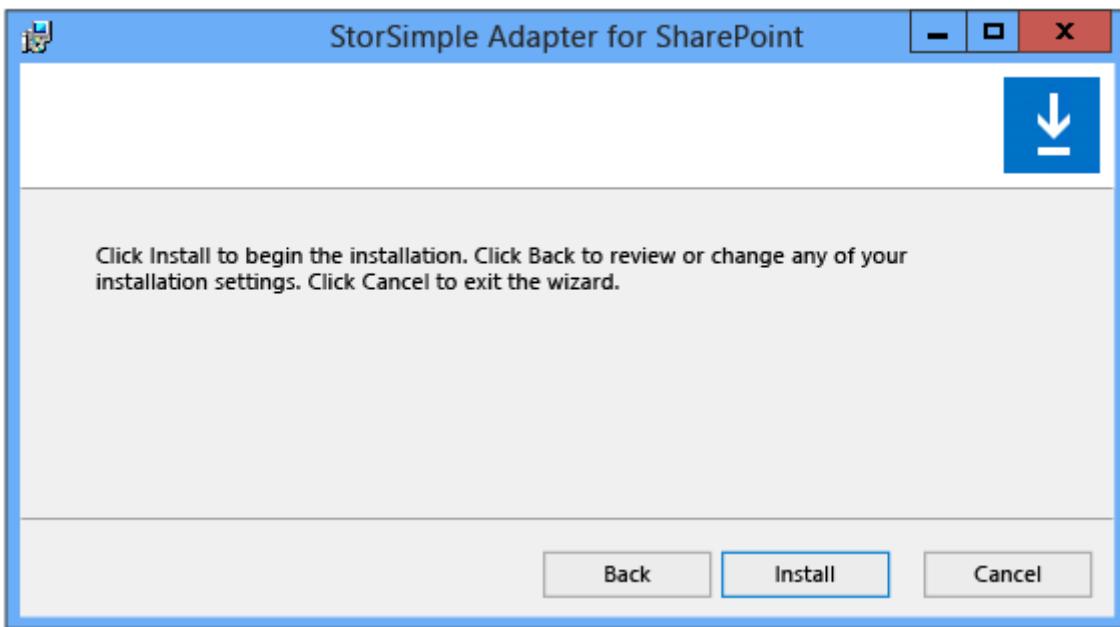
1. Copy the installer to the web front end (WFE) server that is also configured to run the SharePoint Central Administration web application.
2. Use an account with administrator privileges to sign in to the WFE server.
3. Double-click the installer. The StorSimple Adapter for SharePoint Setup Wizard starts. Click **Next** to begin the installation.



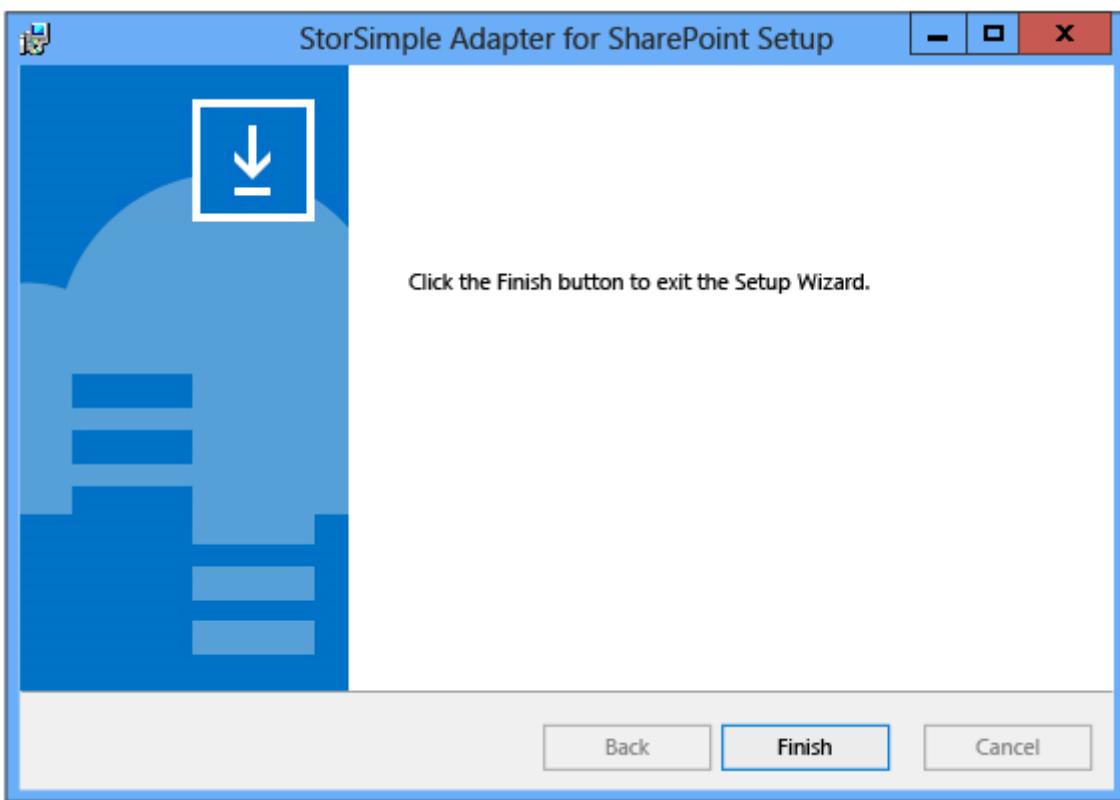
4. In the StorSimple Adapter for SharePoint setup configuration page, select an installation location, type the IP address for the DATA 0 network interface on your StorSimple device, and then click **Next**.



5. In the setup confirmation page, click **Install**.



6. Click Finish to close the Setup Wizard.



7. Open the SharePoint Central Administration page. You should see a StorSimple Configuration group that contains the StorSimple Adapter for SharePoint links.

8. Go to the next step: [Configure RBS](#).

Configure RBS

After you install the StorSimple Adapter for SharePoint, configure RBS as described in the following procedure.

💡 Tip

The StorSimple Adapter for SharePoint plugs into the SharePoint Central Administration page, allowing RBS to be enabled or disabled on each content database in the SharePoint farm. However, enabling or disabling RBS on the content database causes an IIS reset, which, depending on your farm configuration, can momentarily disrupt the availability of the SharePoint web front end (WFE). (Factors such as the use of a front-end load balancer, the current server workload, and so on, can limit or eliminate this disruption.) To protect users from a disruption, we recommend that you enable or disable RBS only during a planned maintenance window.

ⓘ Note

When making changes to the StorSimple Adapter for SharePoint RBS configuration, you must be logged on with a user account that belongs to the Domain Admins group. Additionally, you must access the configuration page from a browser running on the same host as Central Administration.

To configure RBS

1. Open the SharePoint Central Administration page, and browse to **System Settings**.
2. In the **Azure StorSimple** section, click **Configure StorSimple Adapter**.



System Settings

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Configuration Wizards



Servers

[Manage servers in this farm](#) | [Manage services on server](#)



E-mail and Text Messages (SMS)

[Configure outgoing e-mail settings](#) |

[Configure incoming e-mail settings](#) |

[Configure mobile account](#)



Farm Management

[Configure alternate access mappings](#) |

[Manage farm features](#) | [Manage farm solutions](#)

[Manage user solutions](#) | [Configure privacy options](#)

[Configure cross-firewall access zone](#)



Azure StorSimple

[Configure StorSimple Adapter](#)

3. On the **Configure StorSimple Adapter** page:

- a. Make sure that the **Enable editing path** check box is selected.
- b. In the text box, type the Universal Naming Convention (UNC) path of the BLOB store.

① Note

The BLOB store volume must be hosted on an iSCSI volume configured on the StorSimple device.

- c. Click the **Enable** button below each of the content databases that you want to configure for remote storage.

① Note

The BLOB store must be shared and reachable by all web front-end (WFE) servers, and the user account that is configured for the SharePoint Server farm must have access to the share.



Configure StorSimple Adapter

Central Administration	Version	6.3.9600.17116
Application Management	Current version of the StorSimple Adapter for SharePoint.	
System Settings	BLOB Store Path	
Monitoring	Specify the UNC path of the Blob store. Typically, this is the path to a share configured on the StorSimple appliance volume.	<input checked="" type="checkbox"/> Enable editing the path \\127.0.0.1\blobs Example: \\ServerName\Share.Name
Backup and Restore		
Security		
Upgrade and Migration	Remote BLOB Storage (RBS) Configuration	
General Application Settings	Enable or disable RBS database.	WSS_Content (RBS is currently enabled) <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Configuration Wizards		

When you enable or disable RBS, you will also see the following message.

Configure StorSimple Adapter ⓘ

Changed BLOB storage path to: \\shrpt13-fs12\blobs.
Completed updating databases, please log back in to Central Administration web site after a few minutes to continue...

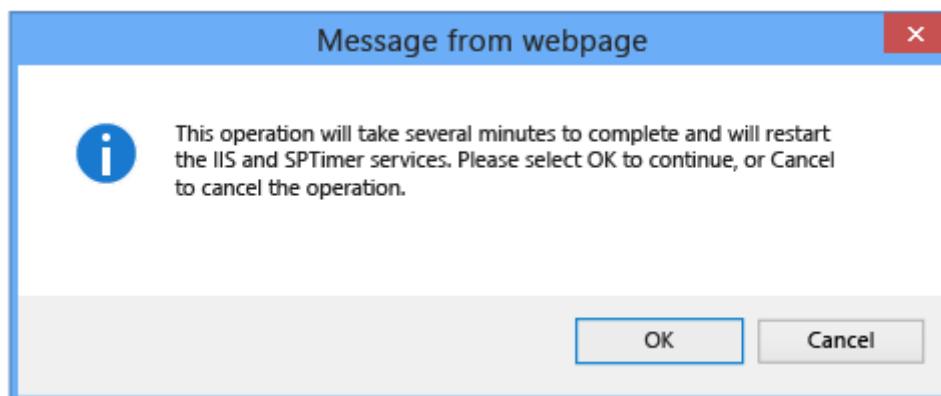
Version

Current version of the StorSimple Adapter for SharePoint.

BLOB Store Path

Specify the UNC path of the BLOB store. Typically, this is the path to a share configured on a StorSimple appliance volume.

- d. Click the **Update** button to apply the configuration. When you click the **Update** button, the RBS configuration status will be updated on all WFE servers, and the entire farm will be RBS-enabled. The following message appears.



ⓘ Note

If you are configuring RBS for a SharePoint farm with a very large number of databases (greater than 200), the SharePoint Central Administration web page might time out. If that occurs, refresh the page. This does not affect the configuration process.

4. Verify the configuration:

- a. Sign in to the SharePoint Central Administration website, and browse to the **Configure StorSimple Adapter** page.
- b. Check the configuration details to make sure that they match the settings that you entered.

5. Verify that RBS works correctly:

- a. Upload a document to SharePoint.
- b. Browse to the UNC path that you configured. Make sure that the RBS directory structure was created and that it contains the uploaded object.

6. (Optional) You can use the Microsoft RBS `Migrate()` PowerShell cmdlet included with SharePoint to migrate existing BLOB content to the StorSimple device. For more information, see [Migrate content into or out of RBS in SharePoint 2013](#) or [Migrate content into or out of RBS \(SharePoint Foundation 2010\)](#).

7. (Optional) On test installations, you can verify that the BLOBS were moved out of the content database as follows:

- a. Start SQL Management Studio.
- b. Run the `ListBlobsInDB_2010.sql` or `ListBlobsInDB_2013.sql` query, as follows.

```
**ListBlobsInDB_2013.sql**

USE WSS_Content
GO

SELECT DocStreams.DocId,
       LeafName AS Name,
       Content,
       AllDocs.Size AS OrigSizeOfContent,
       LEN(CAST(Content AS VARBINARY(MAX))) AS SizeOfContentInDB,
       DocStreams.RbsId,
       TimeLastModified
FROM DocStreams
     INNER JOIN AllDocs ON DocStreams.DocId = AllDocs.Id
```

```

        ORDER BY TimeLastModified DESC
        GO

**ListBlobsInDB_2010.sql**

USE WSS_Content
GO

SELECT AllDocStreams.Id,
       LeafName AS Name,
       Content,
       AllDocs.Size AS OrigSizeOfContent,
       LEN(CAST(Content AS VARBINARY(MAX))) AS SizeOfContentInDB,
       RbsId,
       TimeLastModified
  FROM AllDocStreams
       INNER JOIN AllDocs ON AllDocStreams.Id = AllDocs.Id
  ORDER BY TimeLastModified DESC
  GO

```

If RBS was configured correctly, a NULL value should appear in the SizeOfContentInDB column for any object that was uploaded and successfully externalized with RBS.

8. (Optional) After you configure RBS and move all BLOB content to the StorSimple device, you can move the content database to the device. If you choose to move the content database, we recommend that you configure the content database storage on the device as a primary volume. Then, use established SQL Server best practices to migrate the content database to the StorSimple device.

 **Note**

Moving the content database to the device is only supported for the StorSimple 8000 series (it is not supported for the 5000 or 7000 series).

If you store BLOBs and the content database in separate volumes on the StorSimple device, we recommend that you configure them in the same volume container. This ensures that they will be backed up together.

 **Warning**

If you have not enabled RBS, we do not recommend moving the content database to the StorSimple device. This is an untested configuration.

9. Go to the next step: [Configure garbage collection](#).

Configure garbage collection

When objects are deleted from a SharePoint site, they are not automatically deleted from the RBS store volume. Instead, an asynchronous, background maintenance program deletes orphaned BLOBs from the file store. System administrators can schedule this process to run periodically or they can start it whenever necessary.

This maintenance program (Microsoft.Data.SqlRemoteBlobs.Maintainer.exe) is automatically installed on all SharePoint WFE servers and application servers when you enable RBS. The program is installed in the following location: *boot drive:\Program Files\Microsoft SQL Remote Blob Storage 10.50\Maintainer*

For information about configuring and using the maintenance program, see [Maintain RBS in SharePoint Server 2013](#).

Important

The RBS maintainer program is resource intensive. You should schedule it to run only during periods of light activity on the SharePoint farm.

Delete orphaned BLOBs immediately

If you need to delete orphaned BLOBs immediately, you can use the following instructions. Note that these instructions are an example of how this can be done in a SharePoint 2013 environment with the following components:

- The content database name is WSS_Content.
- The SQL Server name is SHRPT13-SQL12\SHRPT13.
- The web application name is SharePoint – 80.

In this procedure, you will:

1. [Prepare to run the Maintainer executable](#) .
2. [Prepare the content database and Recycle Bin for immediate deletion of orphaned BLOBs](#).
3. [Run Maintainer.exe](#).
4. [Revert the content database and Recycle Bin settings](#).

To prepare to run the Maintainer

1. On the Web front-end server, open the SharePoint 2013 Management Shell as an administrator.
2. Navigate to the folder `boot drive:\Program Files\Microsoft SQL Remote Blob Storage 10.50\Maintainer`.
3. Rename `Microsoft.Data.SqlRemoteBlobs.Maintainer.exe.config` to `web.config`.
4. Use `aspnet_regiis -pdf connectionStrings` to decrypt the `web.config` file.
5. In the decrypted `web.config` file, under the `connectionStrings` node, add the connection string for your SQL server instance and the content database name. See the following example.

```
<add name="RBSMaintainerConnectionWSSContent" connectionString="Data
Source=SHRPT13-SQL12\SHRPT13;Initial Catalog=WSS_Content;Integrated
Security=True;Application Name="Remote Blob Storage Maintainer for
WSS_Content"" providerName="System.Data.SqlClient" />
```

6. Use `aspnet_regiis -pef connectionStrings` to re-encrypt the `web.config` file.
7. Rename `web.config` to `Microsoft.Data.SqlRemoteBlobs.Maintainer.exe.config`.

To prepare the content database and Recycle Bin to immediately delete orphaned BLOBs

1. On the SQL Server, in SQL Management Studio, run the following update queries for the target content database:

```
use WSS_Content

exec mssqlrbs.rbs_sp_set_config_value 'garbage_collection_time_window' , 'time
00:00:00'

exec mssqlrbs.rbs_sp_set_config_value 'delete_scan_period' , 'time 00:00:00'
```

2. On the web front-end server, under **Central Administration**, edit the **Web Application General Settings** for the desired content database to temporarily disable the Recycle Bin. This action will also empty the Recycle Bin for any related site collections. To do this, click **Central Administration -> Application Management -> Web Applications (Manage web applications) -> SharePoint -> General Application Settings**. Set the **Recycle Bin Status** to **OFF**.

Web Application General Settings

If this setting is on, most of the pages in the _Layouts folder will reference the site masterpage and show the customizations that have been made to that master page. When the master page is broken or unavailable, some vital _Layouts pages, such as Settings.aspx, will reference the default SharePoint look and feel.

Recycle Bin

Specify whether the Recycle Bins of all of the sites in this web application are turned on. Turning off the Recycle Bins will empty all the Recycle Bins in the web application.

The second stage Recycle Bin stores items that end users have deleted from their Recycle Bin for easier restore if needed. [Learn about configuring the Recycle Bin](#).

Maximum Upload Size

Specify the maximum size to allow for a single upload to any site. No single file, group of files, or content, can be uploaded if the combined size is greater than this setting.

Customer Experience Improvement Program
Collect web site analytics about web pages on this web application. Please read the Administration guide before turning this on for web applications available over the public

Recycle Bin Status:

On Off

Delete items in the Recycle Bin:

After days
 Never

Second stage Recycle Bin:

Add percent of live site quota for second stage deleted items.
 Off

Maximum upload size:

MB

Enable Customer Experience Improvement Program

Yes
 No

Warning: In order for Customer Experience Improvement Program (CEIP) to collect data, both CEIP and browser CEIP, at the farm level, should be enabled.

To run the Maintainer

- On the web front-end server, in the SharePoint 2013 Management Shell, run the Maintainer as follows:

```
Microsoft.Data.SqlRemoteBlobs.Maintainer.exe -ConnectionStringName RBSMaintainerConnectionWSSContent -Operation GarbageCollection - GarbageCollectionPhases rdo
```

① Note

Only the `GarbageCollection` operation is supported for StorSimple at this time. Also note that the parameters issued for `Microsoft.Data.SqlRemoteBlobs.Maintainer.exe` are case sensitive.

To revert the content database and Recycle Bin settings

1. On the SQL Server, in SQL Management Studio, run the following update queries for the target content database:

```
use WSS_Content

exec mssqlrbs.rbs_sp_set_config_value 'garbage_collection_time_window' , 'days
30'

exec mssqlrbs.rbs_sp_set_config_value 'delete_scan_period' , 'days 30'

exec mssqlrbs.rbs_sp_set_config_value 'orphan_scan_period' , 'days 30'
```

2. On the web front-end server, in **Central Administration**, edit the **Web Application General Settings** for the desired content database to re-enable the Recycle Bin. To do this, click **Central Administration -> Application Management -> Web Applications (Manage web applications)** -> **SharePoint - 80 -> General Application Settings**. Set the Recycle Bin Status to **ON**.

Upgrade or reinstall the StorSimple Adapter for SharePoint

Use the following procedure to upgrade SharePoint Server and then reinstall StorSimple Adapter for SharePoint or to simply upgrade or reinstall the adapter in an existing SharePoint Server farm.

Important

Review the following information before you attempt to upgrade your SharePoint software and/or upgrade or reinstall the StorSimple Adapter for SharePoint:

- Any files that were previously moved to external storage via RBS will not be available until the reinstallation is finished and the RBS feature is enabled again. To limit user impact, perform any upgrade or reinstallation during a planned maintenance window.

- The time required for the upgrade/reinstallation can vary, depending on the total number of SharePoint databases in the SharePoint Server farm.
- After the upgrade/reinstallation is complete, you need to enable RBS for the content databases. See [Configure RBS](#) for more information.
- If you are configuring RBS for a SharePoint farm that has a very large number of databases (greater than 200), the **SharePoint Central Administration** page might time out. If that occurs, refresh the page. This does not affect the configuration process.

Upgrade SharePoint 2010 to SharePoint 2013 and then install the StorSimple Adapter for SharePoint

Important

Any files that were previously moved to external storage via RBS will not be available until the upgrade is finished and the RBS feature is enabled again. To limit user impact, perform any upgrade or reinstallation during a planned maintenance window.

To upgrade SharePoint 2010 to SharePoint 2013 and then install the adapter

1. In the SharePoint 2010 farm, note the BLOB store path for the externalized BLOBs and the content databases for which RBS is enabled.
2. Install and configure the new SharePoint 2013 farm.
3. Move databases, applications, and site collections from the SharePoint 2010 farm to the new SharePoint 2013 farm. For instructions, go to [Overview of the upgrade process to SharePoint 2013](#).
4. Install the StorSimple Adapter for SharePoint on the new farm. Go to [Install the StorSimple Adapter for SharePoint](#) for procedures.
5. Using the information that you noted in step 1, enable RBS for the same set of content databases and provide the same BLOB store path that was used in the SharePoint 2010 installation. Go to [Configure RBS](#) for procedures. After you complete this step, previously externalized files should be accessible from the new farm.

Upgrade the StorSimple Adapter for SharePoint

Important

You should schedule this upgrade to occur during a planned maintenance window for the following reasons:

- Previously externalized content will not be available until the adapter is reinstalled.
- Any content uploaded to the site after you uninstall the previous version of the StorSimple Adapter for SharePoint, but before you install the new version, will be stored in the content database. You will need to move that content to the StorSimple device after you install the new adapter. You can use the Microsoft `RBS Migrate()` PowerShell cmdlet included with SharePoint to migrate the content. For more information, see [Migrate content into or out of RBS](#).

To upgrade the StorSimple Adapter for SharePoint

1. Uninstall the previous version of StorSimple Adapter for SharePoint.

Note

This will automatically disable RBS on the content databases. However, existing BLOBs will remain on the StorSimple device. Because RBS is disabled and the BLOBs have not been migrated back to the content databases, any requests for those BLOBs will fail.

2. Install the new StorSimple Adapter for SharePoint. The new adapter will automatically recognize the content databases that were previously enabled or disabled for RBS and will use the previous settings.

StorSimple Adapter for SharePoint removal

The following procedures describe how to move the BLOBs back to the SQL Server content databases and then uninstall the StorSimple Adapter for SharePoint.

Important

You have to move the BLOBS back to the content databases before you uninstall the adapter software.

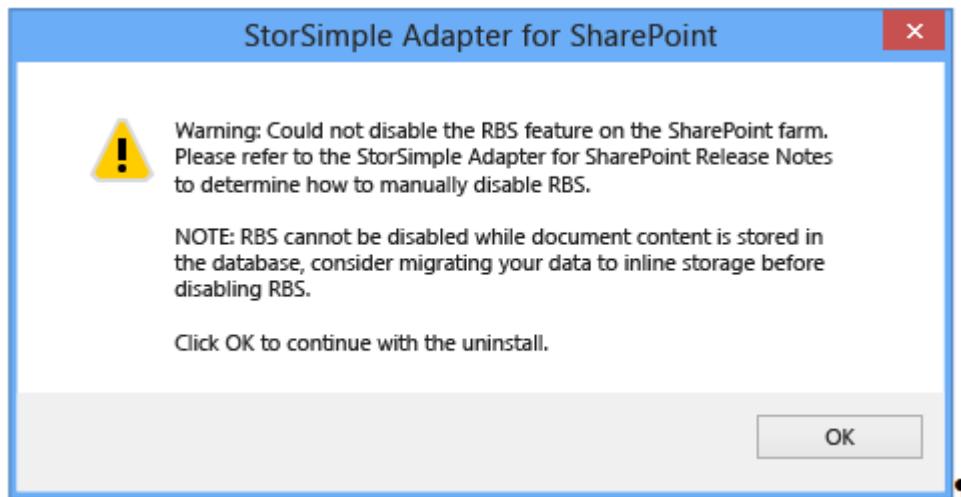
Before you begin

Collect the following information before you move the data back to the SQL Server content databases and begin the adapter removal process:

- The names of all the databases for which RBS is enabled
- The UNC path of the configured BLOB store

Move the BLOBs back to the content databases

Before you uninstall the StorSimple Adapter for SharePoint software, you must migrate all of the BLOBs that were externalized back to the SQL Server content databases. If you attempt to uninstall the StorSimple Adapter for SharePoint before you move all the BLOBs back to the content databases, you will see the following warning message.



To move the BLOBs back to the content databases

1. Download each of the externalized objects.
2. Open the **SharePoint Central Administration** page, and browse to **System Settings**.
3. Under **Azure StorSimple**, click **Configure StorSimple Adapter**.
4. On the **Configure StorSimple Adapter** page, click the **Disable** button below each of the content databases that you want to remove from external BLOB storage.
5. Delete the objects from SharePoint, and then upload them again.

Alternatively, you can use the Microsoft `RBS Migrate()` PowerShell cmdlet included with SharePoint. For more information, see [Migrate content into or out of RBS](#).

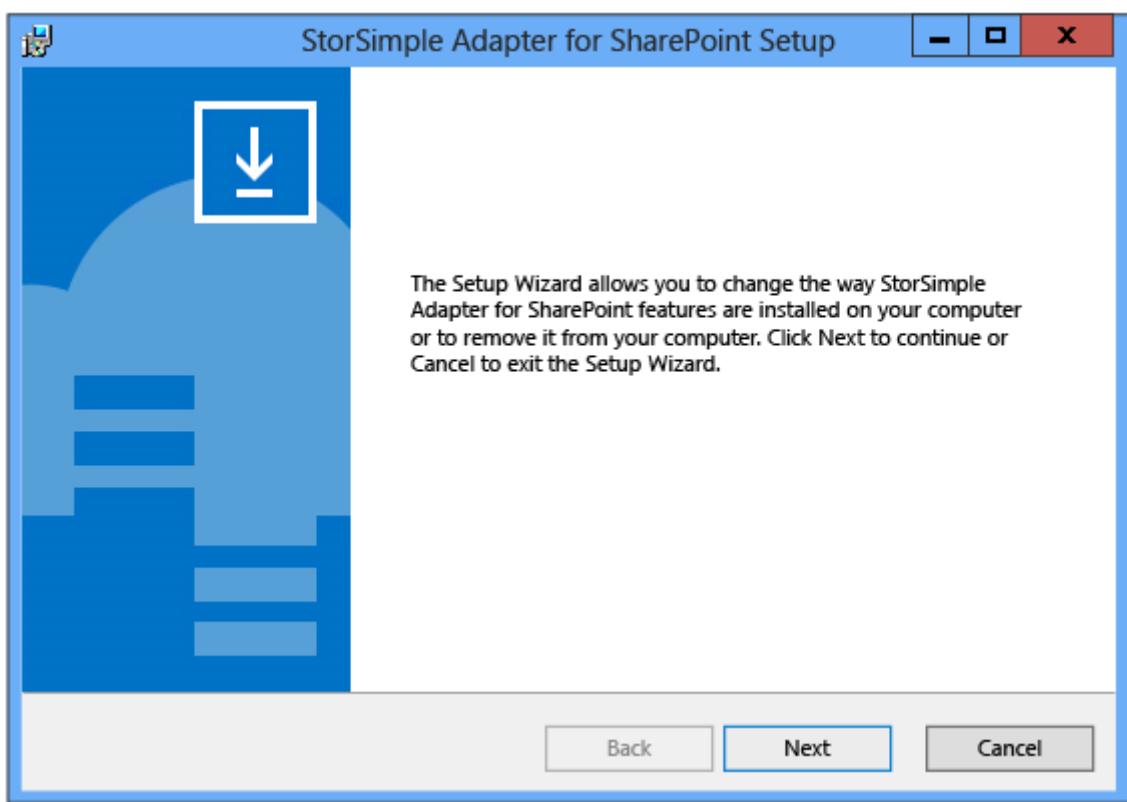
After you move the BLOBs back to the content database, go to the next step: [Uninstall the adapter](#).

Uninstall the adapter

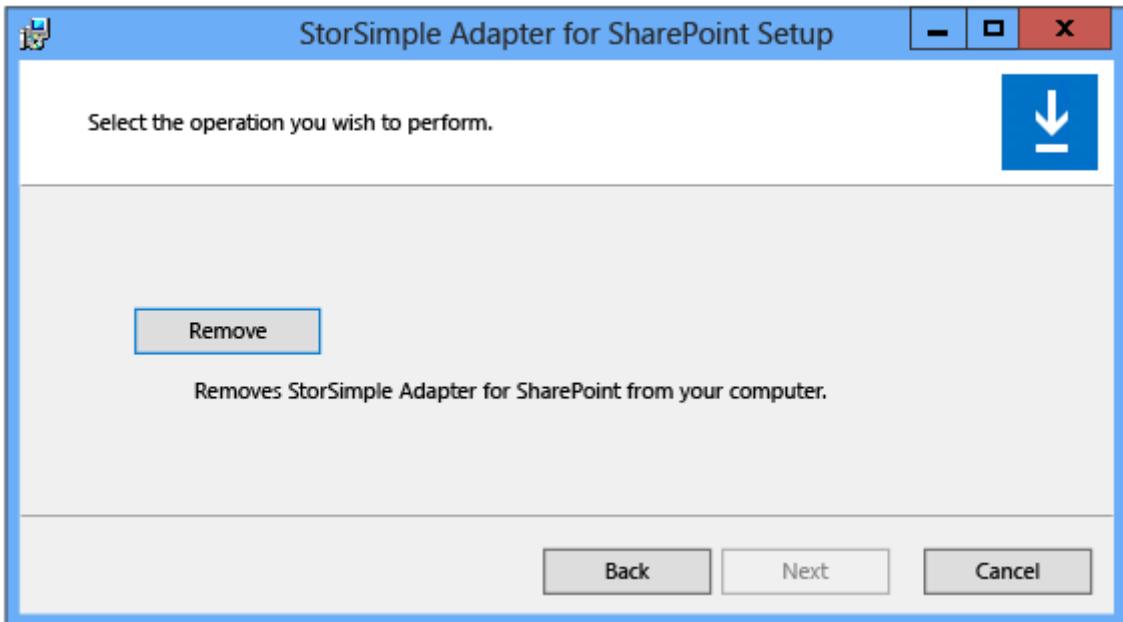
After you move the BLOBs back to the SQL Server content databases, use one of the following options to uninstall the StorSimple Adapter for SharePoint.

To use the installation program to uninstall the adapter

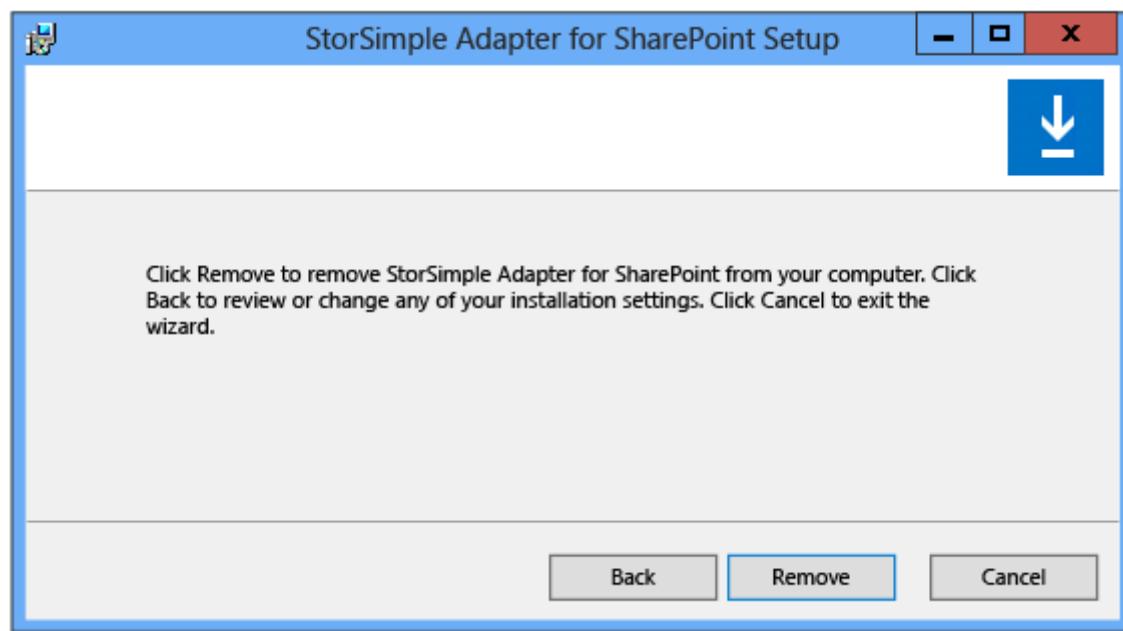
1. Use an account with administrator privileges to log on to the web front-end (WFE) server.
2. Double-click the StorSimple Adapter for SharePoint installer. The Setup Wizard starts.



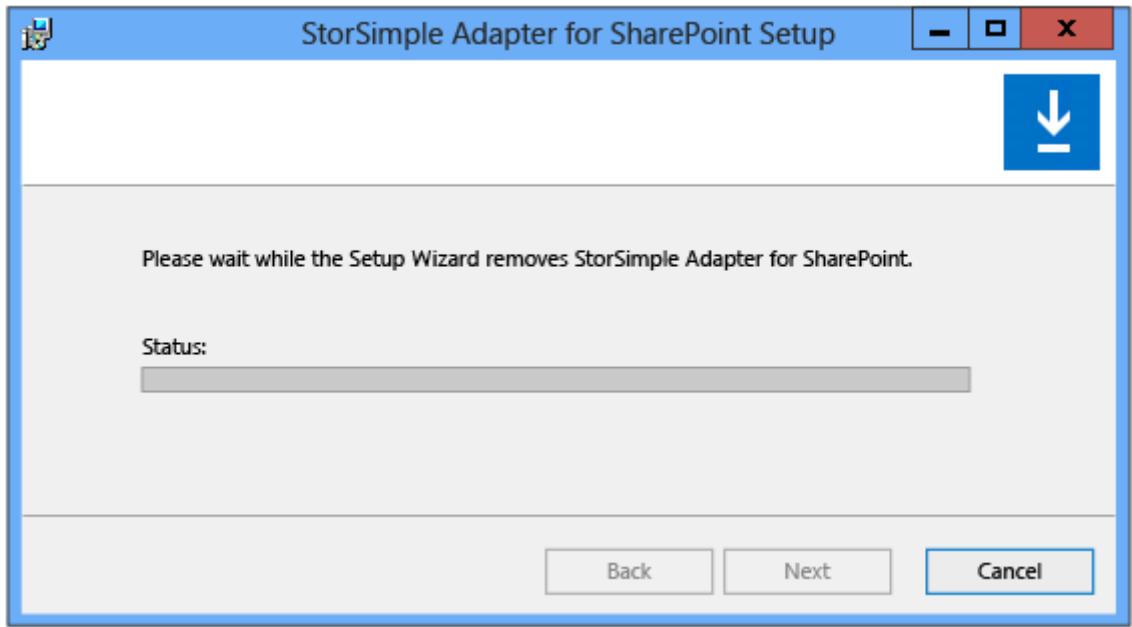
3. Click **Next**. The following page appears.



4. Click **Remove** to select the removal process. The following page appears.



5. Click **Remove** to confirm the removal. The following progress page appears.



6. When the removal is complete, the finish page appears. Click **Finish** to close the Setup Wizard.

To use the Control Panel to uninstall the adapter

1. Open the Control Panel, and then click **Programs and Features**.
2. Select **StorSimple Adapter for SharePoint**, and then click **Uninstall**.

Next steps

[Learn more about StorSimple.](#)

Use the StorSimple Device Manager service to administer your StorSimple device

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the StorSimple Device Manager service interface, including how to connect to it, the various options available, and links out to the specific workflows that can be performed via this UI. This guidance is applicable to both; the StorSimple physical device and the cloud appliance.

After reading this article, you will learn to:

- Connect to StorSimple Device Manager service
- Administer your StorSimple device via the StorSimple Device Manager service

Connect to StorSimple Device Manager service

The StorSimple Device Manager service runs in Microsoft Azure and connects to multiple StorSimple devices. You use a central Microsoft Azure portal running in a browser to manage these devices. To connect to the StorSimple Device Manager service, do the following.

To connect to the service

1. Navigate to <https://portal.azure.com/>.

2. Using your Microsoft account credentials, log on to the Microsoft Azure portal (located at the top-right of the pane).
3. Scroll down the left navigation pane to access the StorSimple Device Manager service.

Administer StorSimple device using StorSimple Device Manager service

The following table shows a summary of all the common management tasks and complex workflows that can be performed within the StorSimple Device Manager service UI. These tasks are organized based on the UI blades on which they are initiated.

For more information about each workflow, click the appropriate procedure in the table.

ⓘ Important

If you see the following warning, you must update the software on the devices before proceeding:

One or more StorSimple devices are running an older software version. The latest available update for TLS 1.2 is a mandatory update and should be installed immediately on these devices. TLS 1.2 is used for all Azure portal communication and without this update, the device won't be able to communicate with the StorSimple service.

StorSimple Device Manager workflows

If you want to do this ...	Use this procedure.
Create a service Delete a service Get service registration key Regenerate service registration key	Deploy a StorSimple Device Manager service
View the activity logs	Use the StorSimple Device Manager service summary
Change the service data encryption key View the operation logs	Use the StorSimple Device Manager service dashboard
Deactivate a device Delete a device	Deactivate or delete a device

If you want to do this ...	Use this procedure.
Learn about disaster recovery and device failover Failover to a physical device Failover to a virtual device Business continuity disaster recovery (BCDR)	Failover and disaster recovery for your StorSimple device
List backups for a volume Select a backup set Delete a backup set	Manage backups
Clone a volume	Clone a volume
Restore a backup set	Restore a backup set
About storage accounts Add a storage account Edit a storage account Delete a storage account Key rotation of storage accounts	Manage storage accounts
About bandwidth templates Add a bandwidth template Edit a bandwidth template Delete a bandwidth template Use a default bandwidth template Create an all-day bandwidth template that starts at a specified time	Manage bandwidth templates
About access control records Create an access control record Edit an access control record Delete an access control record	Manage access control records
View job details Cancel a job	Manage jobs
Receive alert notifications Manage alerts Review alerts	View and manage StorSimple alerts
Create monitoring charts	Monitor your StorSimple device
Add a volume container Modify a volume container Delete a volume container	Manage volume containers

If you want to do this ...	Use this procedure.
Add a volume Modify a volume Take a volume offline Delete a volume Monitor a volume	Manage volumes
Modify device settings Modify time settings Modify DNS.md settings Configure network interfaces	Modify device configuration for your StorSimple device
View web proxy settings	Configure web proxy for your device
Modify device administrator password Modify StorSimple Snapshot Manager password	Change StorSimple passwords
Configure remote management	Connect remotely to your StorSimple device
Configure alert settings	View and manage StorSimple alerts
Configure CHAP for your StorSimple device	Configure CHAP for your StorSimple device
Add a backup policy Add or modify a schedule Delete a backup policy Take a manual backup Create a custom backup policy with multiple volumes and schedules	Manage backup policies
Stop device controllers Restart device controllers Shut down device controllers Reset your device to factory defaults (Above are for on-premises device only)	Manage StorSimple device controller
Learn about StorSimple hardware components Monitor hardware status (Above are for on-premises device only)	Monitor hardware components
Create a support package	Create and manage a Support package
Install software updates	Update your device

Next steps

If you experience any issues with the day-to-day operation of your StorSimple device or with any of its hardware components, refer to:

- [Troubleshoot using the Diagnostics tool](#)
- [Use StorSimple monitoring indicator LEDs](#)

If you cannot resolve the issues and you need to create a service request, refer to [Contact Microsoft Support](#).

Restore a StorSimple volume from a backup set

Article • 08/19/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes the restore operation performed on a StorSimple 8000 series device using an existing backup set. Use the **Backup catalog** blade to restore a volume from a local or cloud backup. The **Backup catalog** blade displays all the backup sets that are created when manual or automated backups are taken. The restore operation from a backup set brings the volume online immediately while data is downloaded in the background.

Before you restore

Before you start a restore, review the following caveats:

- **You must take the volume offline** – Take the volume offline on both the host and the device before you initiate the restore operation. Although the restore operation automatically brings the volume online on the device, you must manually bring the device online on the host. You can bring the volume online on the host as soon as the volume is online on the device. (You do not need to wait until the restore operation is finished.) For procedures, go to [Take a volume offline](#).
- **Volume type after restore** – Deleted volumes are restored based on the type in the snapshot; that is, volumes that were locally pinned are restored as locally pinned volumes and volumes that were tiered are restored as tiered volumes.

For existing volumes, the current usage type of the volume overrides the type that is stored in the snapshot. For example, if you restore a volume from a snapshot that was taken when the volume type was tiered and that volume type is now locally pinned (due to a conversion operation that was performed), then the volume will be restored as a locally pinned volume. Similarly, if an existing locally pinned volume was expanded and subsequently restored from an older snapshot taken when the volume was smaller, the restored volume will retain the current expanded size.

You cannot convert a volume from a tiered volume to a locally pinned volume or from a locally pinned volume to a tiered volume while the volume is being restored. Wait until the restore operation is finished, and then you can convert the volume to another type. For information about converting a volume, go to [Change the volume type](#).

- **The volume size is reflected in the restored volume** – This is an important consideration if you are restoring a locally pinned volume that has been deleted (because locally pinned volumes are fully provisioned). Make sure that you have sufficient space before you attempt to restore a locally pinned volume that was previously deleted.
- **You cannot expand a volume while it is being restored** – Wait until the restore operation is finished before you attempt to expand the volume. For information about expanding a volume, go to [Modify a volume](#).
- **You can perform a backup while you restore a local volume** – For procedures go to [Use the StorSimple Device Manager service to manage backup policies](#).
- **You can cancel a restore operation** – If you cancel the restore job, then the volume will be rolled back to the state that it was in before you initiated the restore operation. For procedures, go to [Cancel a job](#).

How does restore work

For devices running Update 4 or later, a heatmap-based restore is implemented. As the host requests to access data reach the device, these requests are tracked and a heatmap is created. High request rate results in data chunks with higher heat whereas lower request rate translates to chunks with lower heat. You must access the data at least twice to be marked as *hot*. A file that is modified is also marked as *hot*. Once you initiate the restore, then proactive hydration of data occurs based on the heatmap. For versions earlier than Update 4, the data is downloaded during restore based on access only.

The following caveats apply to heatmap-based restores:

- Heatmap tracking is enabled only for tiered volumes and locally pinned volumes are not supported.
- Heatmap-based restore is not supported when cloning a volume to another device.
- If there is an in-place restore and a local snapshot for the volume to be restored exists on the device, then we do not rehydrate (as data is already available locally).
- By default, when you restore, the rehydration jobs are initiated that proactively rehydrate data based on the heatmap.

In Update 4, Windows PowerShell cmdlets can be used to query running rehydration jobs, cancel a rehydration job, and get the status of the rehydration job.

- `Get-HcsRehydrationJob` - This cmdlet gets the status of the rehydration job. A single rehydration job is triggered for one volume.
- `Set-HcsRehydrationJob` - This cmdlet allows you to pause, stop, resume the rehydration job, when the rehydration is in progress.

For more information on rehydration cmdlets, go to [Windows PowerShell cmdlet reference for StorSimple](#).

With automatic rehydration, typically higher transient read performance is expected. The actual magnitude of improvements depends on various factors such as access pattern, data churn, and data type.

To cancel a rehydration job, you can use the PowerShell cmdlet. If you wish to permanently disable rehydration jobs for all the future restores, [contact Microsoft Support](#).

How to use the backup catalog

The **Backup Catalog** blade provides a query that helps you to narrow your backup set selection. You can filter the backup sets that are retrieved based on the following parameters:

- **Time range** – The date and time range when the backup set was created.
- **Device** – The device on which the backup set was created.
- **Backup policy or Volume** – The backup policy or volume associated with this backup set.

The filtered backup sets are then tabulated based on the following attributes:

- **Name** – The name of the backup policy or volume associated with the backup set.
- **Type** – Backup sets can be local snapshots or cloud snapshots. A local snapshot is a backup of all your volume data stored locally on the device, whereas a cloud snapshot refers to the backup of volume data residing in the cloud. Local snapshots provide faster access, whereas cloud snapshots are chosen for data resiliency.
- **Size** – The actual size of the backup set.
- **Created on** – The date and time when the backups were created.
- **Volumes** - The number of volumes associated with the backup set.
- **Initiated** – The backups can be initiated automatically according to a schedule or manually by a user. (You can use a backup policy to schedule backups. Alternatively, you can use the **Take backup** option to take an interactive or on-demand backup.)

How to restore your StorSimple volume from a backup

You can use the **Backup Catalog** blade to restore your StorSimple volume from a specific backup. Keep in mind, however, that restoring a volume will revert the volume to the state it was in when the backup was taken. Any data that was added after the backup operation will be lost.

Warning

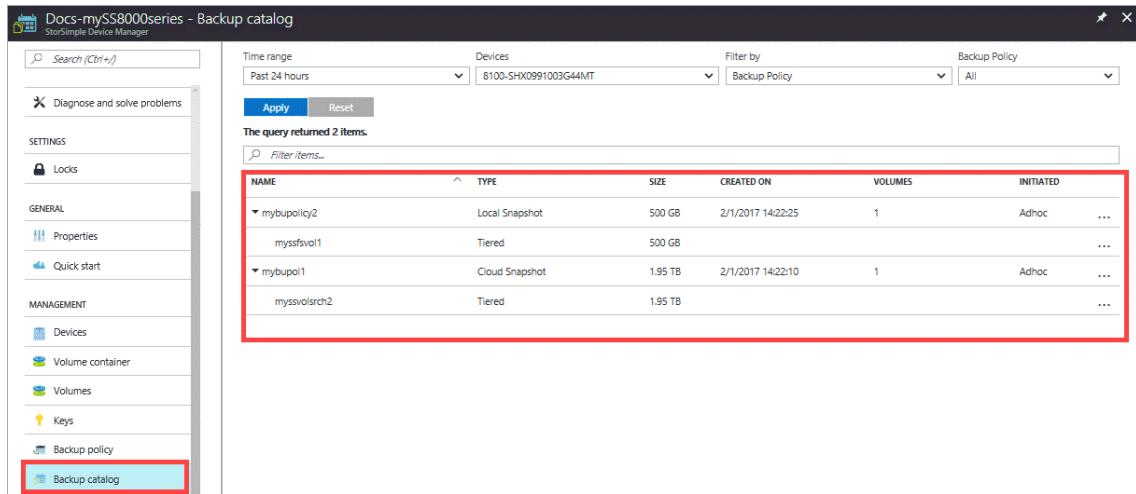
Restoring from a backup will replace the existing volumes from the backup. This may cause the loss of any data that was written after the backup was taken.

To restore your volume

1. Go to your StorSimple Device Manager service and then click **Backup catalog**.
2. Select a backup set as follows:
 - a. Specify the time range.
 - b. Select the appropriate device.
 - c. In the drop-down list, choose the volume or backup policy for the backup that you wish to select.

d. Click **Apply** to execute this query.

The backups associated with the selected volume or backup policy should appear in the list of backup sets.



The screenshot shows the 'Backup catalog' tab in the StorSimple Device Manager. The left sidebar has a 'Backup catalog' item highlighted with a red box. The main area displays a table of backup sets with the following data:

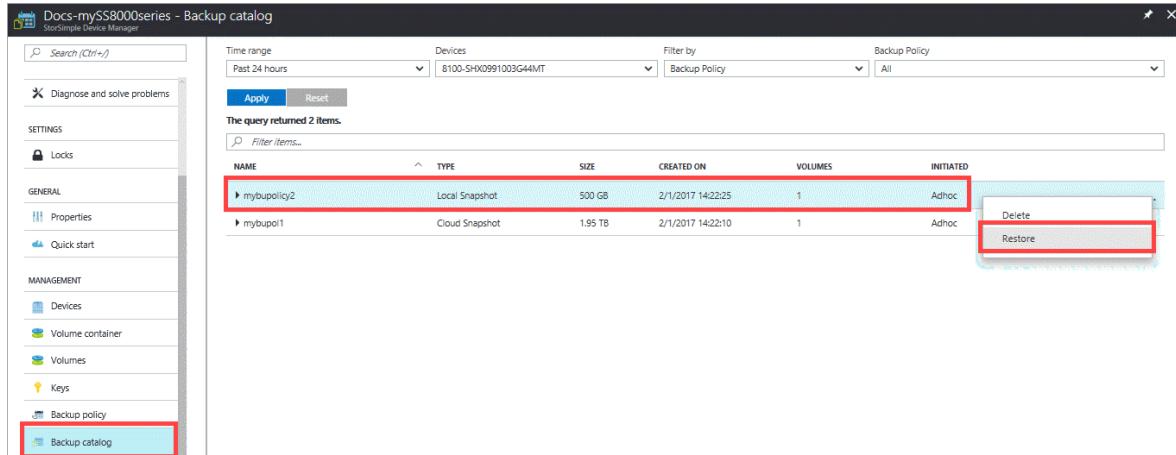
NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupolicy2	Local Snapshot	500 GB	2/1/2017 14:22:25	1	Adhoc
myssfsvol1	Tiered	500 GB			...
mybupol1	Cloud Snapshot	1.95 TB	2/1/2017 14:22:10	1	Adhoc
myssvolsrch2	Tiered	1.95 TB			...

3. Expand the backup set to view the associated volumes. These volumes must be taken offline on the host and device before you can restore them. Access the volumes on the **Volumes** blade of your device, and then follow the steps in [Take a volume offline](#) to take them offline.

Important

Make sure that you have taken the volumes offline on the host first, before you take the volumes offline on the device. If you do not take the volumes offline on the host, it could potentially lead to data corruption.

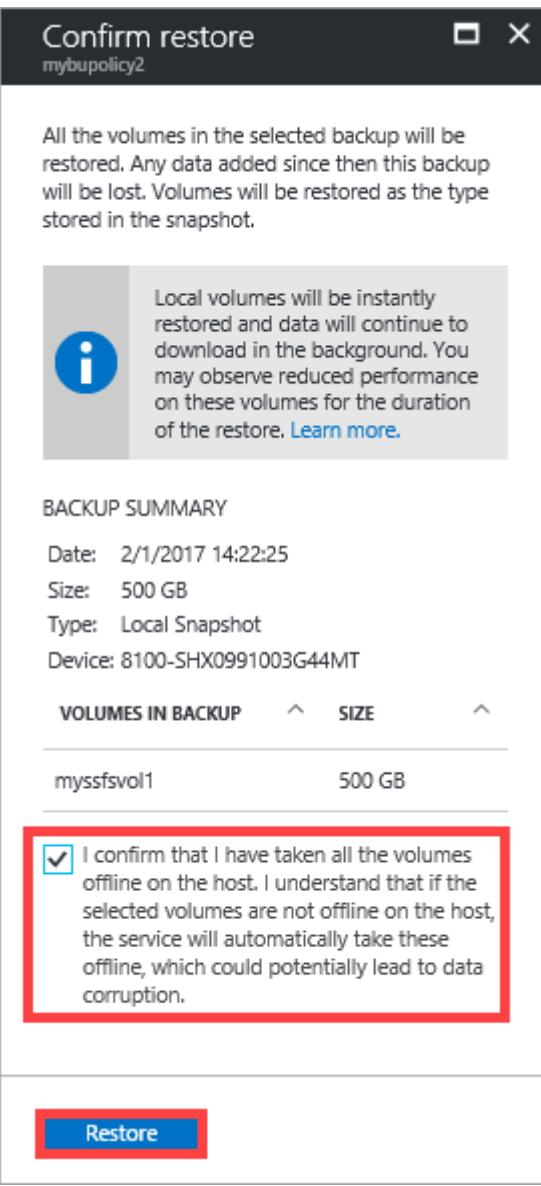
4. Navigate back to the **Backup Catalog** tab and select a backup set. Right-click and then from the context menu, select **Restore**.



The screenshot shows the 'Backup catalog' tab in the StorSimple Device Manager. The left sidebar has a 'Backup catalog' item highlighted with a red box. The main area displays a table of backup sets with the following data. The 'mybupol1' row is selected and highlighted with a red box. A context menu is open over this row, with the 'Restore' option highlighted with a red box.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupol1	Cloud Snapshot	1.95 TB	2/1/2017 14:22:10	1	Adhoc

5. You will be prompted for confirmation. Review the restore information, and then select the confirmation check box.



6. Click **Restore**. This initiates a restore job that you can view by accessing the **Jobs** page.

The screenshot shows the 'Jobs' page with the following details:

- Time range:** Past 24 hours
- Devices:** All
- Status:** All
- Job type:** All

The table displays the following jobs:

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Restore backup	Succeeded	mybupolicy2	8100-SHX0991003G44MT	2/1/2017 14:55:34	20 Seconds
Manual backup	Succeeded	mybupo1	8100-SHX0991003G44MT	2/1/2017 14:22:10	1 Minute, 48 Seconds
Manual backup	Succeeded	mybupol1	8100-SHX0991003G44MT	2/1/2017 14:22:25	4 Seconds
Manual backup	Succeeded	mybupo1	8100-SHX0991003G44MT	2/1/2017 13:30:00	1 Minute, 48 Seconds

7. After the restore is complete, verify that the contents of your volumes are replaced by volumes from the backup.

If the restore fails

You will receive an alert if the restore operation fails for any reason. If this occurs, refresh the backup list to verify that the backup is still valid. If the backup is valid and you are restoring from the cloud, then connectivity issues might be causing the problem.

To complete the restore operation, take the volume offline on the host and retry the restore operation. Note that any modifications to the volume data that were performed during the restore process will be lost.

Next steps

- Learn how to [Manage StorSimple volumes](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service in Azure portal to clone a volume

Article • 08/19/2022 • 5 minutes to read

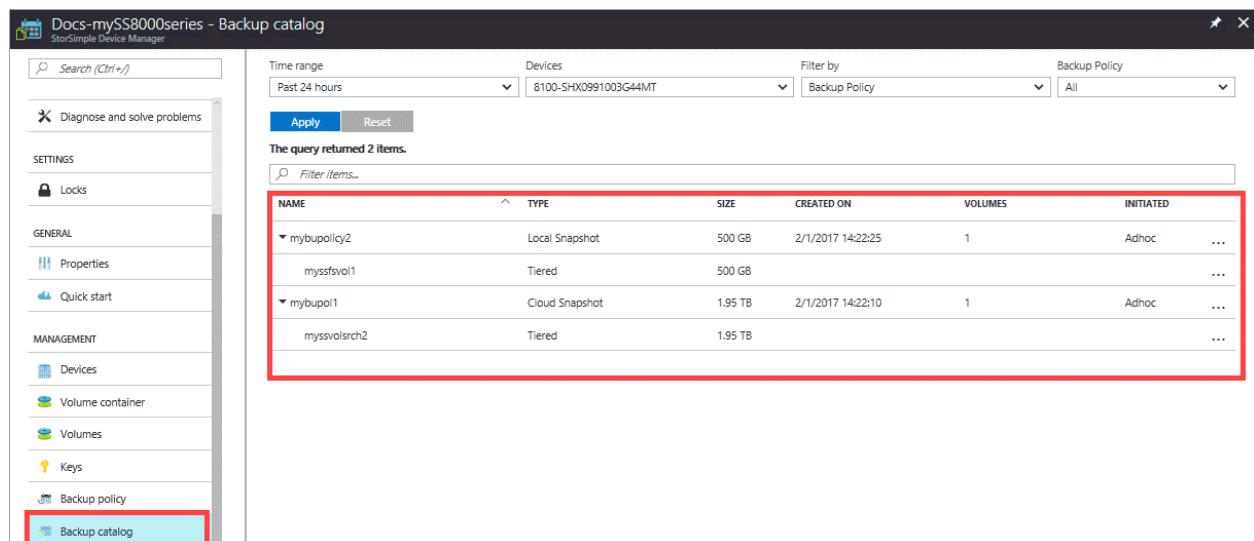
⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes how you can use a backup set to clone an individual volume via the **Backup catalog** blade. It also explains the difference between *transient* and *permanent* clones. The guidance in this tutorial applies to all the StorSimple 8000 series device running Update 3 or later.

The StorSimple Device Manager service **Backup catalog** blade displays all the backup sets that are created when manual or automated backups are taken. You can then select a volume in a backup set to clone.



The screenshot shows the 'Backup catalog' blade in the StorSimple Device Manager service. The left sidebar has a red box around the 'Backup catalog' item. The main area shows a table of backup sets with the following data:

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED	...
mybupolicy2	Local Snapshot	500 GB	2/1/2017 14:22:25	1	Adhoc	...
myssfsvol1	Tiered	500 GB				...
mybupol1	Cloud Snapshot	1.95 TB	2/1/2017 14:22:10	1	Adhoc	...
myssvolsrch2	Tiered	1.95 TB				...

Considerations for cloning a volume

Consider the following information when cloning a volume.

- A clone behaves in the same way as a regular volume. Any operation that is possible on a volume is available for the clone.
- Monitoring and default backup are automatically disabled on a cloned volume. You would need to configure a cloned volume for any backups.
- A locally pinned volume is cloned as a tiered volume. If you need the cloned volume to be locally pinned, you can convert the clone to a locally pinned volume after the clone operation is successfully completed. For information about converting a tiered volume to a locally pinned volume, go to [Change the volume type](#).
- If you try to convert a cloned volume from tiered to locally pinned immediately after cloning (when it is still a transient clone), the conversion fails with the following error message:

```
Unable to modify the usage type for volume {0}. This can happen if the volume  
being modified is a transient clone and hasn't been made permanent. Take a  
cloud snapshot of this volume and then retry the modify operation.
```

This error is received only if you are cloning on to a different device. You can successfully convert the volume to locally pinned if you first convert the transient clone to a permanent clone. Take a cloud snapshot of the transient clone to convert it to a permanent clone.

Create a clone of a volume

You can create a clone on the same device, another device, or even a cloud appliance by using a local or cloud snapshot.

The procedure below describes how to create a clone from the backup catalog.

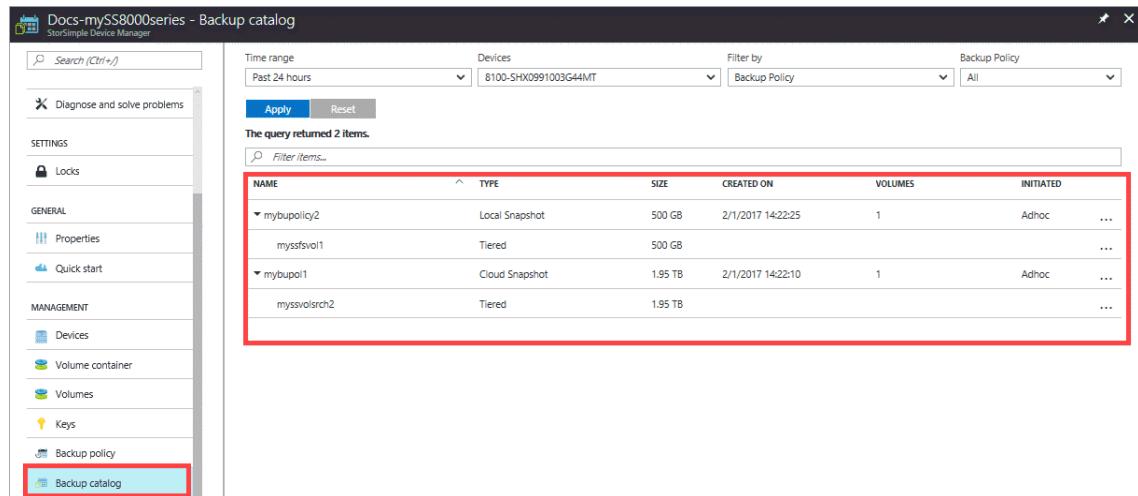
Perform the following steps to create a clone of your volume from the backup catalog.

To clone a volume

1. Go to your StorSimple Device Manager service and then click **Backup catalog**.
2. Select a backup set as follows:

- a. Select the appropriate device.
- b. In the drop-down list, choose the volume or backup policy for the backup that you wish to select.
- c. Specify the time range.
- d. Click **Apply** to execute this query.

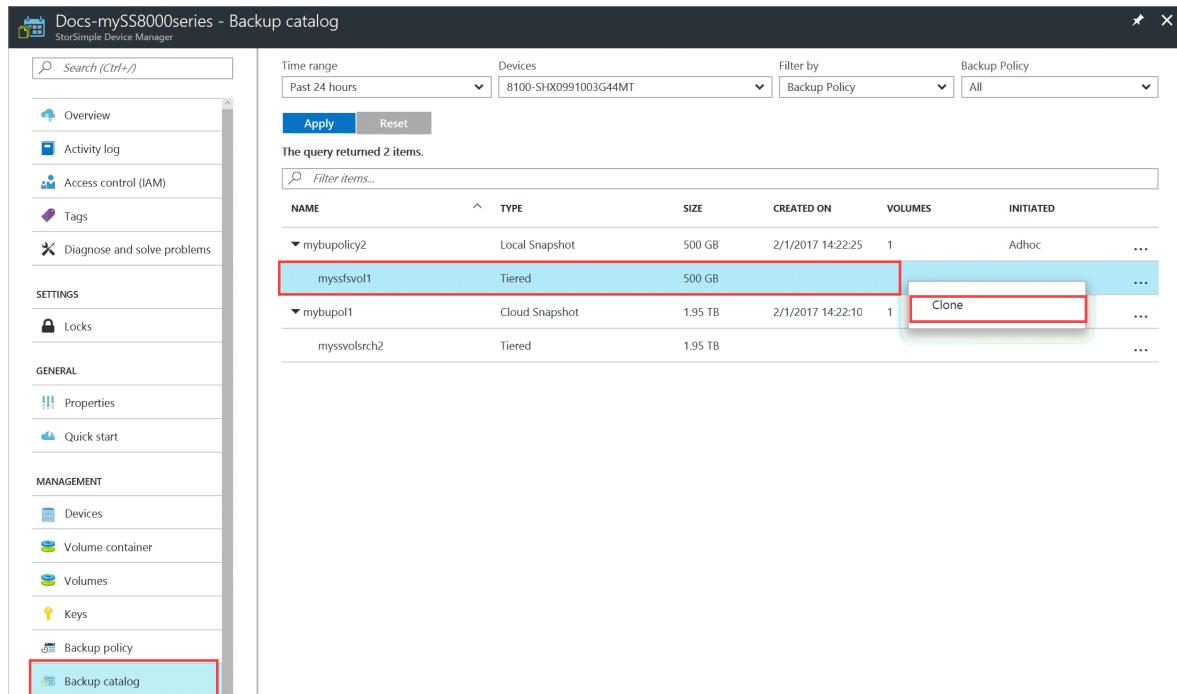
The backups associated with the selected volume or backup policy should appear in the list of backup sets.



The screenshot shows the 'Backup catalog' page of the StorSimple Device Manager. The left sidebar includes options like 'Locks', 'Properties', 'Quick start', 'Devices', 'Volume container', 'Volumes', 'Keys', 'Backup policy', and 'Backup catalog'. The 'Backup catalog' option is highlighted with a red box. The main area displays a table of backup sets with columns: NAME, TYPE, SIZE, CREATED ON, VOLUMES, and INITIATED. The table shows four items: 'mybupolicy2' (Local Snapshot, 500 GB, 2/1/2017 14:22:25, 1, Adhoc), 'myssfsvol1' (Tiered, 500 GB, ...), 'mybupo1' (Cloud Snapshot, 1.95 TB, 2/1/2017 14:22:10, 1, Adhoc), and 'myssvolsrch2' (Tiered, 1.95 TB, ...). A red box highlights the entire table area.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupolicy2	Local Snapshot	500 GB	2/1/2017 14:22:25	1	Adhoc
myssfsvol1	Tiered	500 GB			...
mybupo1	Cloud Snapshot	1.95 TB	2/1/2017 14:22:10	1	Adhoc
myssvolsrch2	Tiered	1.95 TB			...

3. Expand the backup set to view the associated volume and select a volume in a backup set. Right-click and then from the context menu, select **Clone**.



This screenshot is similar to the previous one but focuses on a specific backup set. The 'myssfsvol1' row in the table is highlighted with a blue selection bar. A context menu is open over this row, with the 'Clone' option highlighted with a red box. The rest of the interface is identical to the first screenshot, including the sidebar and the overall layout of the backup catalog page.

4. In the **Clone** blade, do the following steps:

- a. Identify a target device. This is the location where the clone will be created. You can choose the same device or specify another device.

 **Note**

Make sure that the capacity required for the clone is lower than the capacity available on the target device.

- b. Specify a unique volume name for your clone. The name must contain between 3 and 127 characters.

 **Note**

The **Clone Volume As** field will be **Tiered** even if you are cloning a locally pinned volume. You cannot change this setting; however, if you need the cloned volume to be locally pinned as well, you can convert the clone to a locally pinned volume after you successfully create the clone. For information about converting a tiered volume to a locally pinned volume, go to [Change the volume type](#).

- c. Under **Connected hosts**, specify an access control record (ACR) for the clone. You can add a new ACR or choose from the existing list. The ACR will determine which hosts can access this clone.

Clone

myssfsvol1



Device

8100-SHX0991003G44MT



Required capacity : 500 GB.
Available capacity : 8.5 TB.
Clone as: Tiered volume.

* Volume name

Clonedmyssfsvol1

Connected hosts

myssacr1



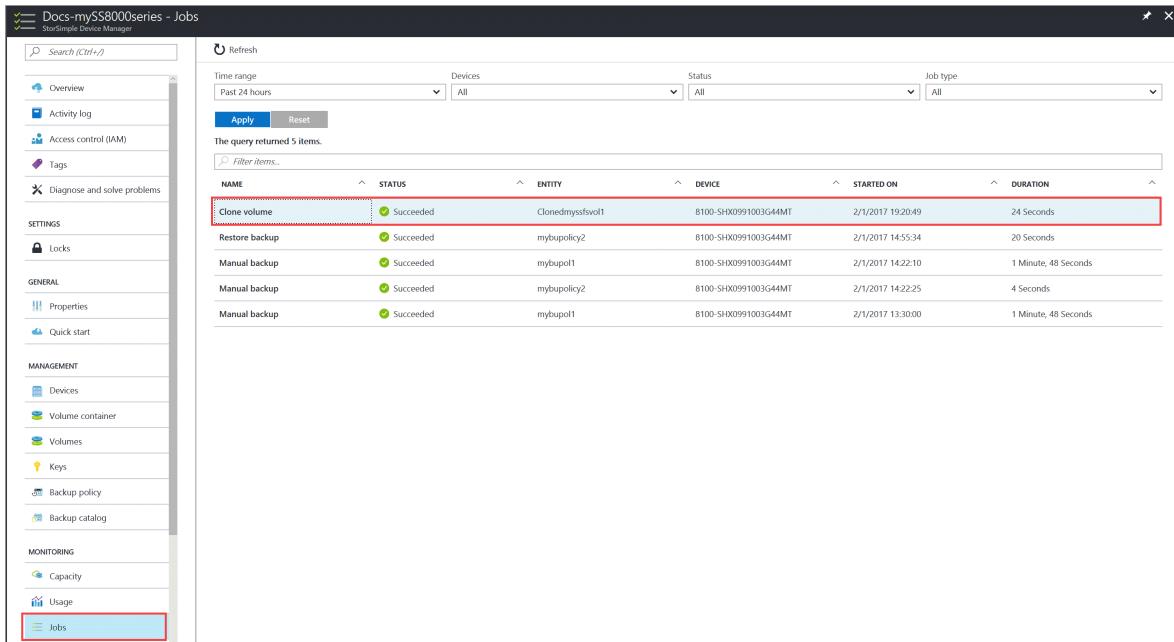
Backup

Not enabled

Clone

d. Click **Clone** to complete the operation.

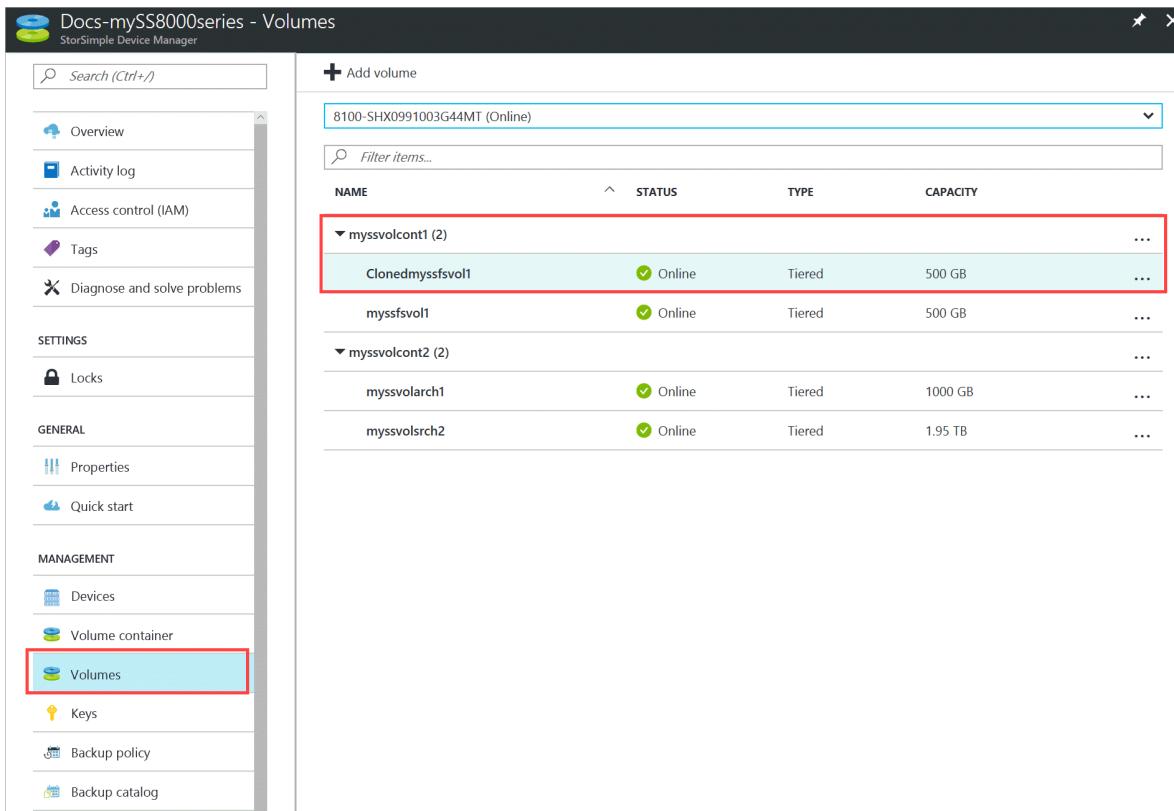
5. A clone job is initiated and you are notified when the clone is successfully created. Click the job notification or go to **Jobs** blade to monitor the clone job.



The screenshot shows the 'Jobs' blade in the StorSimple Device Manager. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick start), Management (Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog), Monitoring (Capacity, Usage), and Jobs. The 'Jobs' section is highlighted with a red box. The main area displays a table of jobs with columns: NAME, STATUS, ENTITY, DEVICE, STARTED ON, and DURATION. One job, 'Clone volume', is highlighted with a red box and has a status of 'Succeeded'. Other listed jobs include 'Restore backup', 'Manual backup', and two more 'Manual backup' entries.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Clone volume	Succeeded	Clonedmyssfsvol1	8100-SH00991003G44MT	2/1/2017 19:20:49	24 Seconds
Restore backup	Succeeded	mybupolicy2	8100-SH00991003G44MT	2/1/2017 14:55:34	20 Seconds
Manual backup	Succeeded	mybupol1	8100-SH00991003G44MT	2/1/2017 14:22:10	1 Minute, 48 Seconds
Manual backup	Succeeded	mybupolicy2	8100-SH00991003G44MT	2/1/2017 14:22:25	4 Seconds
Manual backup	Succeeded	mybupol1	8100-SH00991003G44MT	2/1/2017 13:30:00	1 Minute, 48 Seconds

6. After the clone job is complete, go to your device and then click **Volumes**. In the list of volumes, you should see the clone that was just created in the same volume container that has the source volume.



The screenshot shows the 'Volumes' blade in the StorSimple Device Manager. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick start), Management (Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog), and Volumes. The 'Volumes' section is highlighted with a red box. The main area displays a table of volumes with columns: NAME, STATUS, TYPE, and CAPACITY. A new volume, 'Clonedmyssfsvol1', is listed under a volume container named 'myssvolcont1 (2)'. This volume is online, tiered, and has a capacity of 500 GB. Other volumes listed include 'myssfsvol1' and 'myssvolcont2 (2)' with its sub-volumes 'myssvolarch1' and 'myssvolsrch2'.

NAME	STATUS	TYPE	CAPACITY
Clonedmyssfsvol1	Online	Tiered	500 GB
myssfsvol1	Online	Tiered	500 GB
myssvolcont2 (2)			
myssvolarch1	Online	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB

A clone that is created this way is a transient clone. For more information about clone types, see [Transient vs. permanent clones](#).

Transient vs. permanent clones

Transient clones are created only when you clone to another device. You can clone a specific volume from a backup set to a different device managed by the StorSimple Device Manager. The transient clone has references to the data in the original volume and uses that data to read and write locally on the target device.

After you take a cloud snapshot of a transient clone, the resulting clone is a *permanent* clone. During this process, a copy of the data is created on the cloud and the time to copy this data is determined by the size of the data and the Azure latencies (this is an Azure-to-Azure copy). This process can take days to weeks. The transient clone becomes a permanent clone and doesn't have any references to the original volume data that it was cloned from.

Scenarios for transient and permanent clones

The following sections describe example situations in which transient and permanent clones can be used.

Item-level recovery with a transient clone

You need to recover a one-year-old Microsoft PowerPoint presentation file. Your IT administrator identifies the specific backup from that time, and then filters the volume. The administrator then clones the volume, locates the file that you are looking for, and provides it to you. In this scenario, a transient clone is used.

Testing in the production environment with a permanent clone

You need to verify a testing bug in the production environment. You create a clone of the volume in the production environment and then take a cloud snapshot of this clone to create an independent cloned volume. In this scenario, a permanent clone is used.

Next steps

- Learn how to [restore a StorSimple volume from a backup set](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Connect remotely to your StorSimple 8000 series device

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

You can remotely connect to your device via Windows PowerShell. When you connect this way, you do not see a menu. (You see a menu only if you use the serial console on the device to connect.) With Windows PowerShell remoting, you connect to a specific runspace. You can also specify the display language.

For more information about using Windows PowerShell remoting to manage your device, go to [Use Windows PowerShell for StorSimple to administer your StorSimple device](#).

This tutorial explains how to configure your device for remote management and then how to connect to Windows PowerShell for StorSimple. You can use HTTP or HTTPS to remotely connect via Windows PowerShell. However, when you are deciding how to connect to Windows PowerShell for StorSimple, consider the following information:

- Connecting directly to the device serial console is secure, but connecting to the serial console over network switches is not. Be cautious of the security risk when connecting to the device serial console over network switches.
- Connecting through an HTTP session might offer more security than connecting through the serial console over the network. Although this is not the most secure method, it is acceptable on trusted networks.
- Connecting through an HTTPS session with a self-signed certificate is the most secure and the recommended option.

You can connect remotely to the Windows PowerShell interface. However, remote access to your StorSimple device via the Windows PowerShell interface is not enabled by default. You must enable remote management on the device first, and then on the client that is used to access your device.

The steps described in this article were performed on a host system running Windows Server 2012 R2.

Connect through HTTP

Connecting to Windows PowerShell for StorSimple through an HTTP session offers more security than connecting through the serial console of your StorSimple device. Although this is not the most secure method, it is acceptable on trusted networks.

You can use either the Azure portal or the serial console to configure remote management. Select from the following procedures:

- Use the Azure portal to enable remote management over HTTP
- [Use the serial console to enable remote management over HTTP](#)

After you enable remote management, use the following procedure to prepare the client for a remote connection.

- [Prepare the client for remote connection](#)

Use the Azure portal to enable remote management over HTTP

Perform the following steps in the Azure portal to enable remote management over HTTP.

To enable remote management through the Azure portal

1. Go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you want to configure for remote management. Go to **Device settings > Security**.
2. In the **Security settings** blade, click **Remote Management**.
3. In the **Remote management** blade, set **Enable Remote Management** to **Yes**.
4. You can now choose to connect using HTTP. (The default is to connect over HTTPS.) Make sure that HTTP is selected.

 **Note**

Connecting over HTTP is acceptable only on trusted networks.

5. Click **Save** and when prompted for confirmation, select **Yes**.

Use the serial console to enable remote management over HTTP

Perform the following steps on the device serial console to enable remote management.

To enable remote management through the device serial console

1. On the serial console menu, select option 1. For more information about using the serial console on the device, go to [Connect to Windows PowerShell for StorSimple via device serial console](#).
2. At the prompt, type: `Enable-HcsRemoteManagement -AllowHttp`
3. You are notified about the security vulnerabilities of using HTTP to connect to the device. When prompted, confirm by typing **Y**.
4. Verify that HTTP is enabled by typing: `Get-HcsSystem`
5. Verify that the **RemoteManagementMode** field shows **HttpsAndHttpEnabled**.The following illustration shows these settings in PuTTY.

```
Controller0>Enable-HcsRemoteManagement -AllowHttp  
This will allow remote PowerShell users to connect to this device over HTTP. This is known to have security vulnerabilities and should only be done on trusted networks. HTTPS is recommended. Are you sure you want to enable HTTP?  
[Y] Yes [N] No (Default is "Y"): Y  
Controller0>Get-HcsSystem  
  
InstanceId : 53f93409-bb74-4005-a2f7-f3745fab4a4b  
Name : 8100 -SHX0991003G44MT  
Model : 8100  
SerialNumber : SHX0991003G44MT  
TimeZone : (UTC-08:00) Pacific Time (US & Canada)  
CurrentController : Controller0  
ActiveController : Controller0  
Controller0Status : Normal  
Controller1Status : Normal  
SystemMode : Normal  
HcsSoftwareVersion : 6.3.9600.17022  
ApiVersion : 9.0.0.0  
VhdVersion : 6.3.9600.17022  
OSVersion : 6.3.9600.0  
Capacity : 329853488332800  
RemoteManagementMode : HttpsAndHttpEnabled  
  
Controller0>
```

Prepare the client for remote connection

Perform the following steps on the client to enable remote management.

To prepare the client for remote connection

1. Start a Windows PowerShell session as an administrator. If using a Windows 10 client, by default, the Windows Remote Management service is set to manual. You may need to start the service by typing:

```
Start-Service WinRM
```

2. Type the following command to add the IP address of the StorSimple device to the client's trusted hosts list:

```
Set-Item wsman:\localhost\Client\TrustedHosts <device_ip> -Concatenate -Force
```

Replace *<device_ip>* with the IP address of your device; for example:

```
Set-Item wsman:\localhost\Client\TrustedHosts 10.126.173.90 -Concatenate -  
Force
```

3. Type the following command to save the device credentials in a variable:

```
$cred = Get-Credential
```

4. In the dialog box that appears:

- Type the user name in this format: *device_ip\SSAdmin*.
- Type the device administrator password that was set when the device was configured with the setup wizard. The default password is *Password1*.

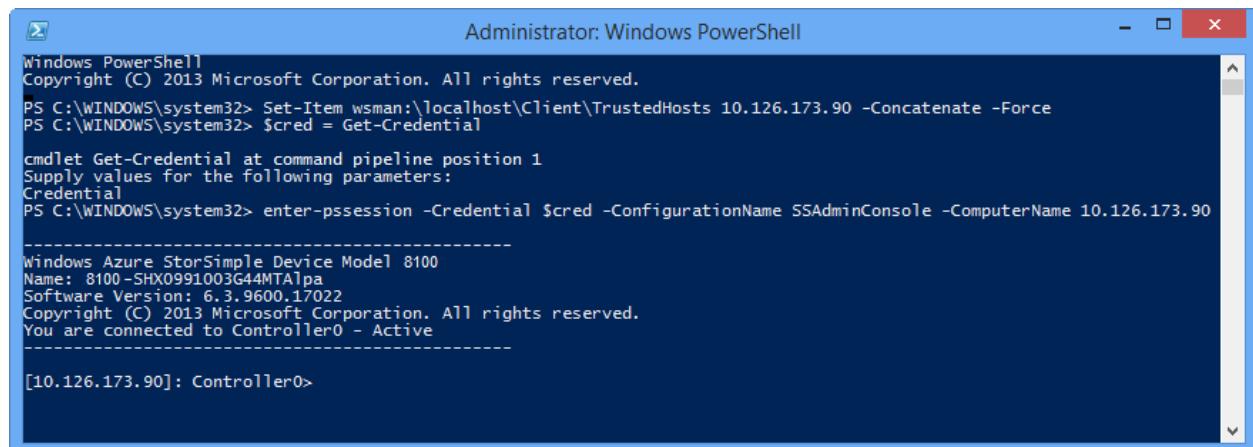
5. Start a Windows PowerShell session on the device by typing this command:

```
Enter-PSSession -Credential $cred -ConfigurationName SSAdminConsole -  
ComputerName <device_ip>
```

 **Note**

To create a Windows PowerShell session for use with the StorSimple virtual device, append the **-Port** parameter and specify the public port that you configured in Remoting for StorSimple Virtual Appliance.

At this point, you should have an active remote Windows PowerShell session to the device.



The screenshot shows an Administrator Windows PowerShell window. The title bar reads "Administrator: Windows PowerShell". The command history shows:

```
Windows PowerShell  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.  
PS C:\WINDOWS\system32> Set-Item wsman:\localhost\Client\TrustedHosts 10.126.173.90 -Concatenate -Force  
PS C:\WINDOWS\system32> $cred = Get-Credential  
cmdlet Get-Credential at command pipeline position 1  
Supply values for the following parameters:  
Credential  
PS C:\WINDOWS\system32> enter-pssession -Credential $cred -ConfigurationName SSAdminConsole -ComputerName 10.126.173.90  
  
-----  
Windows Azure StorSimple Device Model 8100  
Name: 8100-SHX0991003G44MTA1pa  
Software Version: 6.3.9600.17022  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.  
You are connected to Controller0 - Active  
  
[10.126.173.90]: Controller0>
```

Connect through HTTPS

Connecting to Windows PowerShell for StorSimple through an HTTPS session is the most secure and recommended method of remotely connecting to your Microsoft Azure StorSimple device. The following procedures explain how to set up the serial console and client computers so that you can use HTTPS to connect to Windows PowerShell for StorSimple.

You can use either the Azure portal or the serial console to configure remote management. Select from the following procedures:

- Use the Azure portal to enable remote management over HTTPS
- [Use the serial console to enable remote management over HTTPS](#)

After you enable remote management, use the following procedures to prepare the host for a remote management and connect to the device from the remote host.

- [Prepare the host for remote management](#)
- [Connect to the device from the remote host](#)

Use the Azure portal to enable remote management over HTTPS

Perform the following steps in the Azure portal to enable remote management over HTTPS.

To enable remote management over HTTPS from the Azure portal

1. Go to your StorSimple Device Manager service. Select **Devices** and then select and click the device you want to configure for remote management. Go to **Device settings > Security**.
2. In the **Security settings** blade, click **Remote Management**.
3. Set **Enable Remote Management** to **Yes**.
4. You can now choose to connect using HTTPS. (The default is to connect over HTTPS.) Make sure that **HTTPS** is selected.
5. Click ... and then click **Download Remote Management Certificate**. Specify a location to save this file. You need to install this certificate on the client or host computer that you will use to connect to the device.
6. Click **Save** and then click **Yes** when prompted for confirmation.

Use the serial console to enable remote management over HTTPS

Perform the following steps on the device serial console to enable remote management.

To enable remote management through the device serial console

1. On the serial console menu, select option 1. For more information about using the serial console on the device, go to [Connect to Windows PowerShell for StorSimple](#)

via device serial console.

2. At the prompt, type:

```
Enable-HcsRemoteManagement
```

This should enable HTTPS on your device.

3. Verify that HTTPS has been enabled by typing:

```
Get-HcsSystem
```

Make sure that the **RemoteManagementMode** field shows **HttpsEnabled**. The following illustration shows these settings in PuTTY.

```
Controller1>Enable-HcsRemoteManagement
Controller1>Get-HcsSystem

InstanceId          : 53f93409-bb74-4005-a2f7-f3745fab4a4b
Name               : 8100-SHX0991003G44MT
Model              : 8100
SerialNumber       : SHX0991003G44MT
TimeZone           : (UTC-08:00) Pacific Time (US & Canada)
CurrentController  : Controller1
ActiveController   : Controller1
Controller0Status  : Normal
Controller1Status  : Normal
SystemMode         : Normal
HcsSoftwareVersion: 6.3.9600.17022
ApiVersion         : 9.0.0.0
VhdVersion         : 6.3.9600.17022
OSVersion          : 6.3.9600.0
Capacity           : 329853488332800
RemoteManagementMode: HttpsEnabled

Controller1>
```

4. From the output of `Get-HcsSystem`, copy the serial number of the device and save it for later use.

 **Note**

The serial number maps to the CN name in the certificate.

5. Obtain a remote management certificate by typing:

```
Get-HcsRemoteManagementCert
```

A certificate similar to the following will appear.

```
Controller1>Get-HcsRemoteManagementCert
-----BEGIN CERTIFICATE-----
MIIEIDCCAwgIBAgIQVHdbUmUoG7VNTqwWc1DcsTANBgkqhkiG9w0BAQUFADCBpjEgMB4GA1UE
CwwXSGNzUmVtb3R1TWFuYWd1bWVudEN1cnQxHjAcBgNVBAoMFU1pY3Jvc29mdCBDb3Jwb3JhdGlv
bjEjMCEGA1UEAwwaU0hYMDk5MTAwM0c0NE1UQ29udHJvbGxlcjExIzAhBgNVBAMMG1NIWDA5OTEw
MDNHNDRNVENvbnRyb2xsZXIwMRgwFgYDVQQDDA9TSFgwOTkxMDAzRzQ0TVQwIBcNMTQwMjEyMDkw
MjQxWhgPMjExMzAyMTIwOTAyNDFaMIGMSAwHgYDVQQLDBdIY3NS2W1vdGVNYW5hZ2VtZW50Q2Vy
dDEeMBwGA1UECgwVTWljqcm9zb2Z0IENvcnBvcml0aW9uMSMwIQYDVQQDBpTSFgwOTkxMDAzRzQ0
TVRDb250cm9sbGVyMTEjMCEGA1UEAwwaU0hYMDk5MTAwM0c0NE1UQ29udHJvbGxlcjAxGDAWBgNV
BAMMD1NIWDA5OTEwMDNHNDRNVDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOFRG28z
x/NWgMJobDdF4NeV0MLLiump1U4nRwkYX/Tszbu7smbvWhbvvhvrU41GIst3Nv5cR9odVbeaP9f8
emIFZ9dKh3U5svoXoyJo0w/PI8fuRgw1vEAXxfuwjO5o1RUPrED+wQwEZERrcCe9uHr1gS2vg9mT
uvOCd+iX7Y2uA6q5zxhVb9X2oWoE8wRHv666FlzjE8PBdMV0mZCxxuqmqAGL8YLx5WXWhV6xJvFT
9fnzjQsvcRYZudCnByp136pKESVtz25XJmzwIGGBaJkX4bdsdD1ZfsaDu4OmW9mceKNaH3NnPuWn
3A9418t9b52dCjsAJUdZYANqUb8R5McCAwEAAaNGMEQwEwYDVR01BAwwCgYIKwYBBQUH AwEwHQYD
VR0OBByEFI8KJUylQPBQt7Yh75oLiOfE0NF4MA4GA1UdDwEB/wQEawIFIDANBgkqhkiG9w0BAQUF
AAOCAQEA1qIr6FwkYLRyrBQsK2wrnwIZvQaETxwVJy/E5AaZLuEWL2d8ktxvX8hefdy2TDn73K3B
b+3n8a+Z23okkMw1rIw2mbM0ILwLY/WCuNWlcthxQtemlhKVUqtY6zmuu/d1V5er6cKRHQNeaxJE
Cd9QvU4V9Et/Kq3rqSilzR1+xmlln7ok6qafeSy90EHS5JkQzoBjbuNkgjV71s8OnaBqB6Iue15kY
b0v3avWIzRxtajmdlWaNUoa/58NRbjkL98Gls4p53plZun3ldU/CBjLGGe8O3yjwk6X01ufV3is0
YuVwi3cQ1qtiiuDMNow99Cu8vhIqcUaiTuTKY00mD/mL0g==
-----END CERTIFICATE-----
Controller1>
```

6. Copy the information in the certificate from **-----BEGIN CERTIFICATE-----** to **-----END CERTIFICATE-----** into a text editor such as Notepad, and save it as a .cer file. (You will copy this file to your remote host when you prepare the host.)

① Note

To generate a new certificate, use the `Set-HcsRemoteManagementCert` cmdlet.

Prepare the host for remote management

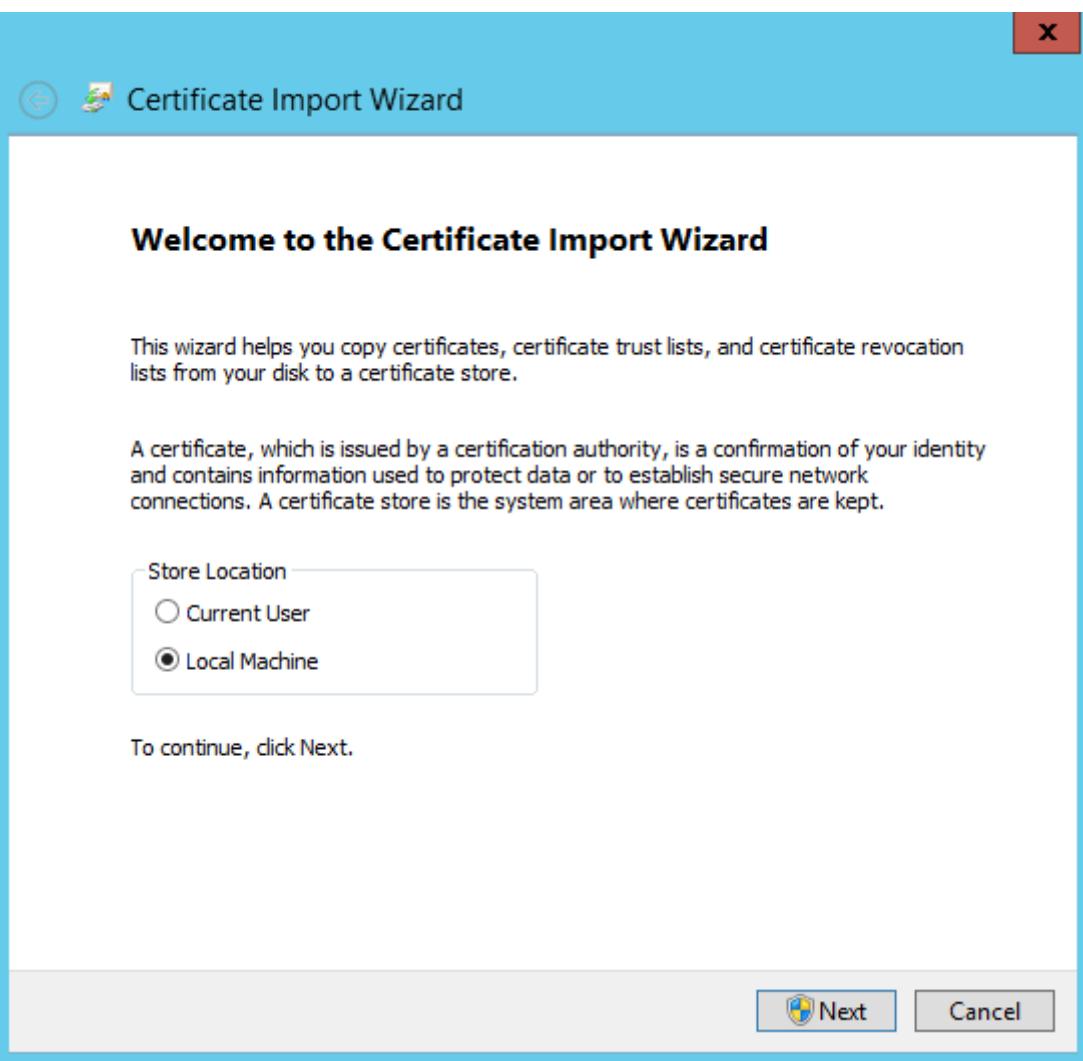
To prepare the host computer for a remote connection that uses an HTTPS session, perform the following procedures:

- Import the .cer file into the root store of the client or remote host.
- Add the device serial numbers to the hosts file on your remote host.

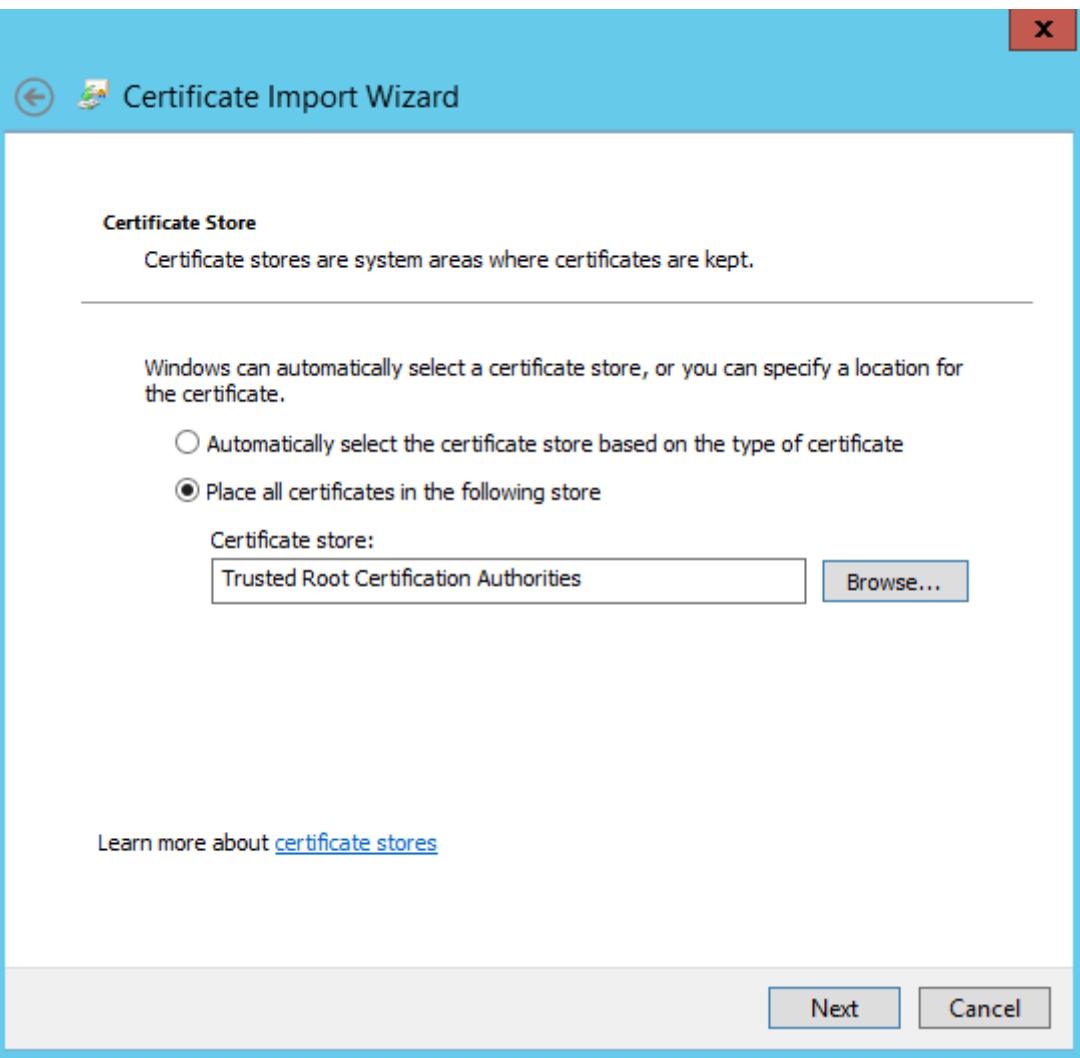
Each of the preceding procedures, is described below.

To import the certificate on the remote host

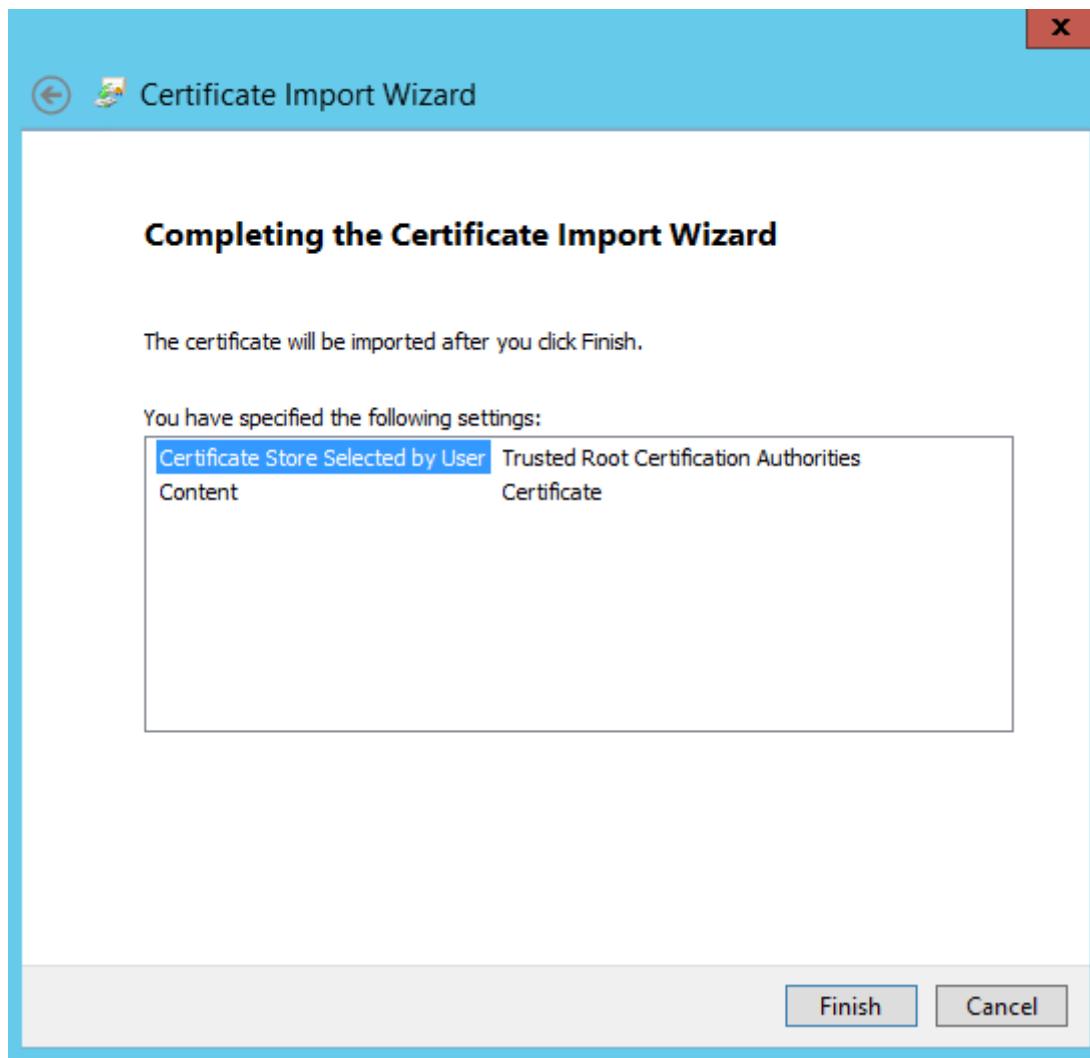
1. Right-click the .cer file and select **Install certificate**. This starts the Certificate Import Wizard.



2. For **Store location**, select **Local Machine**, and then click **Next**.
3. Select **Place all certificates in the following store**, and then click **Browse**. Navigate to the root store of your remote host, and then click **Next**.

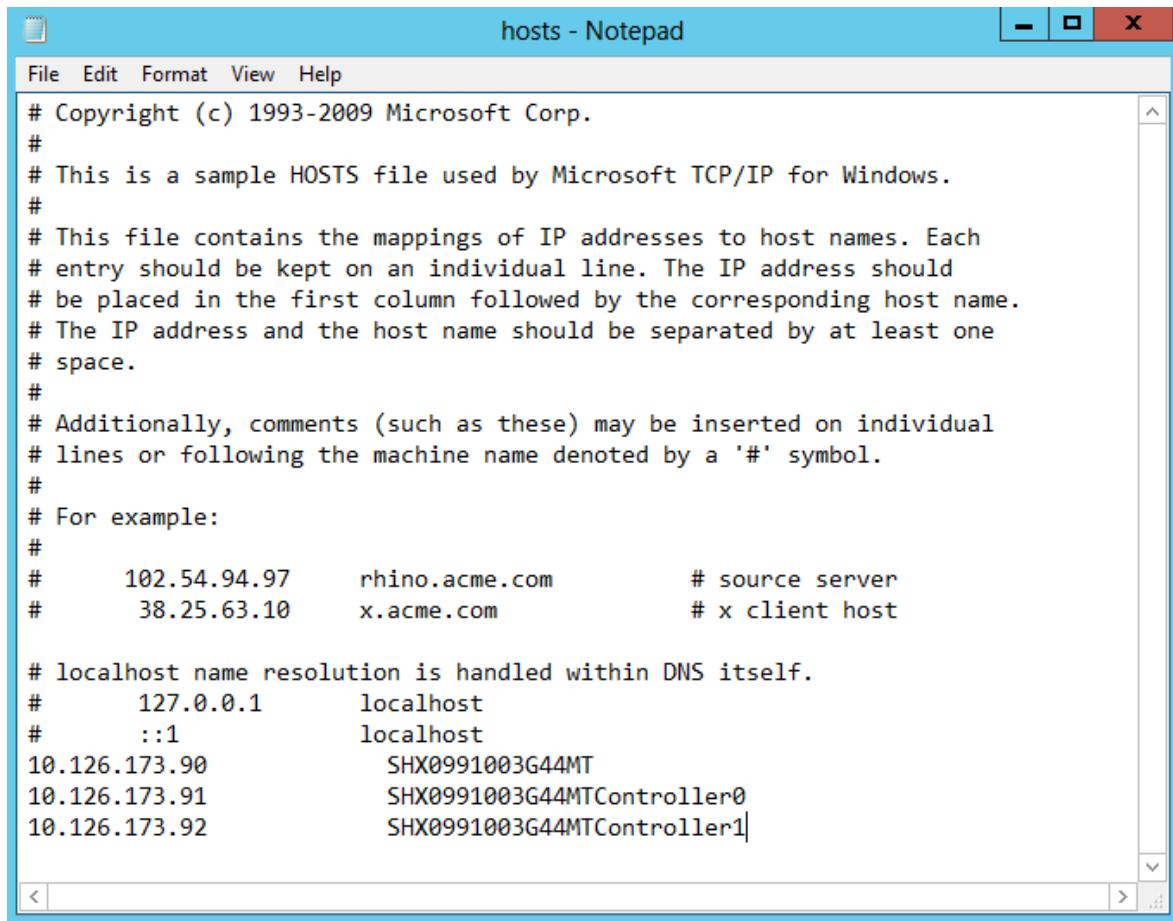


4. Click **Finish**. A message that tells you that the import was successful appears.



To add device serial numbers to the remote host

1. Start Notepad as an administrator, and then open the hosts file located at \\Windows\System32\Drivers\etc.
2. Add the following three entries to your hosts file: **DATA 0 IP address, Controller 0 Fixed IP address, and Controller 1 Fixed IP address.**
3. Enter the device serial number that you saved earlier. Map this to the IP address as shown in the following image. For Controller 0 and Controller 1, append **Controller0** and **Controller1** at the end of the serial number (CN name).



The screenshot shows a Windows Notepad window titled "hosts - Notepad". The window contains the standard sample HOSTS file text, which includes comments about the file's purpose, examples of IP-to-hostname mappings, and localhost entries. The file ends with three IP addresses (10.126.173.90, 10.126.173.91, 10.126.173.92) followed by their corresponding host names (SHX0991003G44MT, SHX0991003G44MTController0, and SHX0991003G44MTController1).

```
# Copyright (c) 1993-2009 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97    rhino.acme.com        # source server  
#      38.25.63.10    x.acme.com            # x client host  
  
# localhost name resolution is handled within DNS itself.  
#      127.0.0.1        localhost  
#      ::1              localhost  
10.126.173.90          SHX0991003G44MT  
10.126.173.91          SHX0991003G44MTController0  
10.126.173.92          SHX0991003G44MTController1
```

4. Save the hosts file.

Connect to the device from the remote host

Use Windows PowerShell and TLS to enter an SSAdmin session on your device from a remote host or client. The SSAdmin session maps to option 1 in the [serial console](#) menu of your device.

Perform the following procedure on the computer from which you want to make the remote Windows PowerShell connection.

To enter an SSAdmin session on the device by using Windows PowerShell and TLS

1. Start a Windows PowerShell session as an administrator. If using a Windows 10 client, by default, the Windows Remote Management service is set to manual. You may need to start the service by typing:

```
Start-Service WinRM
```

2. Add the device IP address to the client's trusted hosts by typing:

```
Set-Item wsman:\localhost\Client\TrustedHosts <device_ip> -Concatenate -Force
```

Where <device_ip> is the IP address of your device; for example:

```
Set-Item wsman:\localhost\Client\TrustedHosts 10.126.173.90 -Concatenate -  
Force
```

3. To create a new credential, type:

```
$cred = New-Object pscredential @("<IP of target device>\SSAdmin", (ConvertTo-SecureString -Force -AsPlainText "<Device Administrator Password>"))
```

Where <IP of target device> is the IP address of DATA 0 for your device; for example, **10.126.173.90** as shown in the preceding image of the hosts file. Also, supply the administrator password for your device.

4. Create a session by typing:

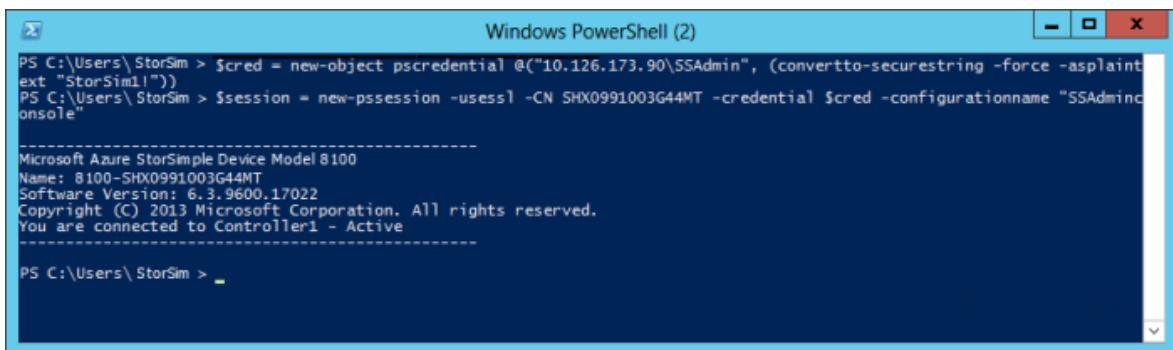
```
$session = New-PSSession -UseSSL -ComputerName <Serial number of target  
device> -Credential $cred -ConfigurationName "SSAdminConsole"
```

For the -ComputerName parameter in the cmdlet, provide the <serial number of target device>. This serial number was mapped to the IP address of DATA 0 in the hosts file on your remote host; for example, **SHX0991003G44MT** as shown in the following image.

5. Type:

```
Enter-PSSession $session
```

6. You will need to wait a few minutes, and then you will be connected to your device via HTTPS over TLS. You see a message that indicates you are connected to your device.



The screenshot shows a Windows PowerShell window titled "Windows PowerShell (2)". The command entered is:

```
PS C:\Users\StorSim > $cred = new-object pscredential @("10.126.173.90\SSAdmin", (convertto-securestring -force -asplaintext "StorSim1!"))  
PS C:\Users\StorSim > $session = new-pssession -usessl -CN SHX0991003G44MT -credential $cred -configurationname "SSAdminConsole"  
  
-----  
Microsoft Azure StorSimple Device Model 8100  
Name: 8100-SHX0991003G44MT  
Software Version: 6.3.9600.17022  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.  
You are connected to Controller1 - Active  
-----  
PS C:\Users\StorSim > _
```

The output shows the device details and a connection message indicating it is connected to Controller1 - Active.

Next steps

- Learn more about [using Windows PowerShell to administer your StorSimple device](#).

- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).
-

Additional resources

Documentation

[Manage StorSimple 8000 series device controllers](#)

Learn how to stop, restart, shut down, or reset your StorSimple device controllers.

[PowerShell for StorSimple device management](#)

Learn how to use Windows PowerShell for StorSimple to manage your StorSimple device.

[Deactivate and delete a StorSimple 8000 series device](#)

Learn how to deactivate and delete a StorSimple device that is connected to a StorSimple Device Manager service.

[Troubleshoot issues during data copies to your Azure Data Box, Azure Data Box Heavy](#)

Describes how to troubleshoot issues when copying data to Azure Data Box and Azure Data Box Heavy devices.

[Administer Azure Data Box/Azure Data Box Heavy using local web UI](#)

Describes how to use the local web UI to administer your Data Box and Data Box Heavy devices

[Tutorial to copy data to Azure Data Box Disk](#)

In this tutorial, learn how to copy data from your host computer to Azure Data Box Disk and then generate checksums to verify data integrity.

[Troubleshoot share connection failure during data copy to Azure Data Box](#)

Describes how to identify network issues preventing SMB share connections during data copy to an Azure Data Box.

[Use logs to troubleshoot upload issues in Azure Data Box Disk - Azure Data Box Disk](#)

Describes how to use copy/error logs to troubleshoot issues seen when uploading data to Azure Data Box Disk.

[Show 5 more](#)

Training

Module

[Manage single and multiple computers by using Windows PowerShell remoting - Training](#)

This module explains how to use remoting to perform administration on remote computers.

Deactivate and delete a StorSimple device

Article • 08/22/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes how to deactivate and delete a StorSimple device that is connected to a StorSimple Device Manager service. The guidance in this article applies only to StorSimple 8000 series devices including the StorSimple Cloud Appliances. If you are using a StorSimple Virtual Array, then go to [Deactivate and delete a StorSimple Virtual Array](#).

Deactivation severs the connection between the device and the corresponding StorSimple Device Manager service. You may wish to take a StorSimple device out of service (for example, if you are replacing or upgrading your device or if you are no longer using StorSimple). If so, you need to deactivate the device before you can delete it.

When you deactivate a device, any data that was stored locally on the device is no longer accessible. Only the data associated with the device that was stored in the cloud can be recovered. When you deactivate a device, any data that was stored locally on the device is no longer accessible. Only the data associated with the device that was stored in the cloud can be recovered. After you have deactivated the device, if you would like to keep it, go to [Keep my StorSimple 8000 series appliance](#).

⚠ Warning

Deactivation is a PERMANENT operation and cannot be undone. A deactivated device cannot be registered with the StorSimple Device Manager service unless it is

reset to factory defaults.

The factory reset process deletes all the data that was stored locally on your device. Therefore, you must take a cloud snapshot of all your data before you deactivate a device. This cloud snapshot allows you to recover all the data at a later stage.

Note

- Before you deactivate a StorSimple physical device or cloud appliance, ensure that the data from the deleted volume container is actually deleted from the device. You can monitor the cloud consumption charts and when you see the cloud usage drop because of the backups you have deleted, then you can proceed to deactivate the device. If you deactivate the device before this drop occurs, the data is stranded in the storage account and accrues charges.
- Before you deactivate a StorSimple physical device or cloud appliance, stop or delete clients and hosts that depend on that device.
- If the storage account(s) or the containers in the storage account associated with the volume containers are already deleted before deleting the data from the device, you will receive an error and may not be able to delete the data. We recommend that you delete the data on the device before you delete the Storage Account or containers therein. However, in this situation, you will have to proceed with device deactivation and deletion assuming that the data is already removed from the storage account.

After reading this tutorial, you will be able to:

- Deactivate a device and delete the data.
- Deactivate a device and retain the data.

Deactivate and delete data

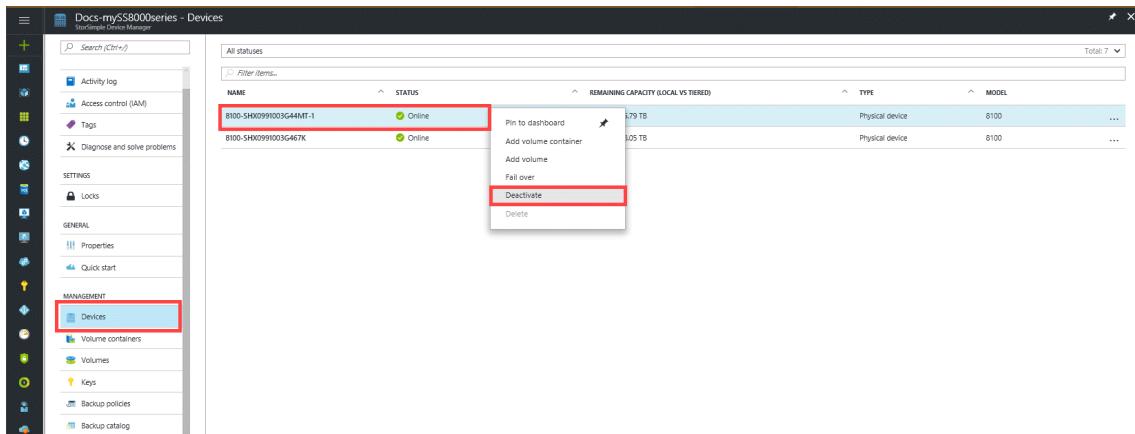
If you are interested in deleting the device completely and do not want to retain the data on the device, then complete the following steps.

To deactivate the device and delete the data

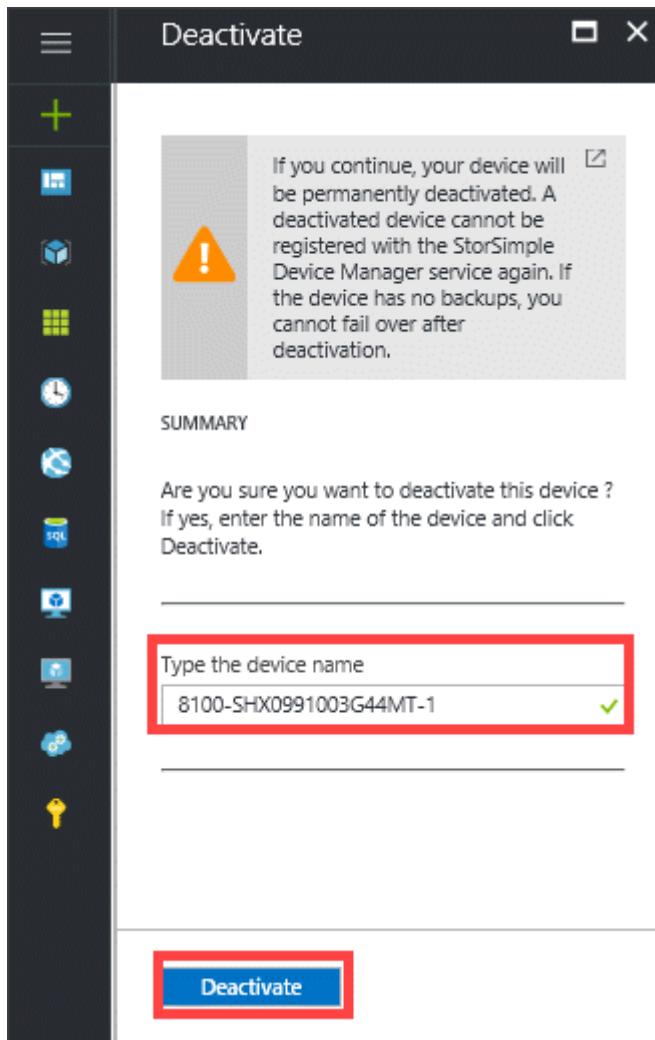
1. Before you deactivate a device, you must delete all the volume containers (and the volumes) associated with the device. You can delete volume containers only after you have deleted the associated backups. Refer to the note in the above overview before you deactivate a StorSimple physical device or cloud appliance.

2. Deactivate the device as follows:

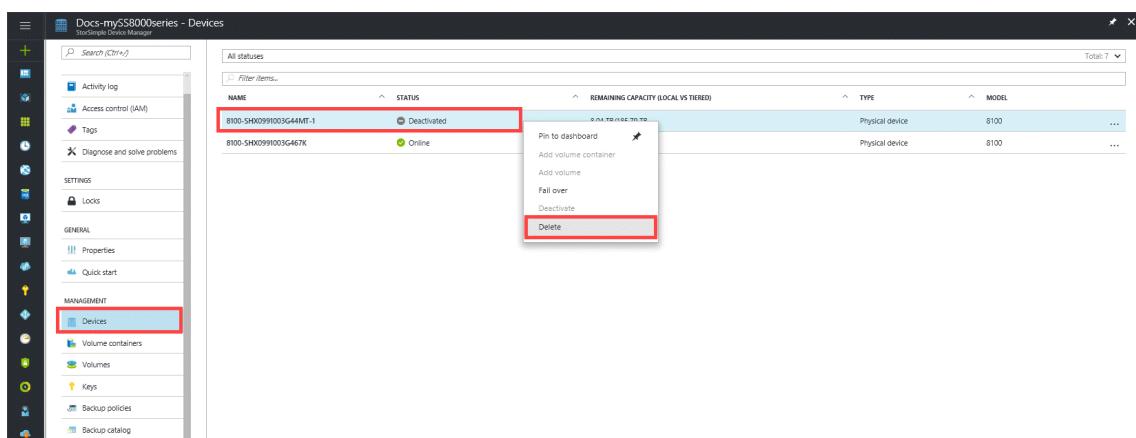
- Go to your StorSimple Device Manager service and click **Devices**. In the **Devices** blade, select the device that you wish to deactivate, right-click, and then click **Deactivate**.



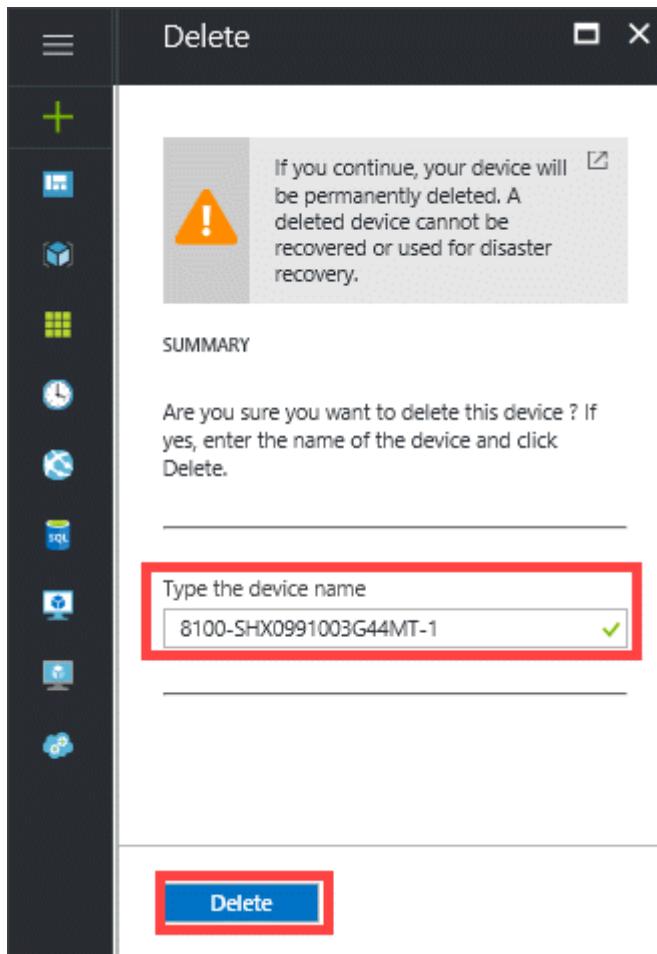
- In the **Deactivate** blade, type the device name to confirm and then click **Deactivate**. The deactivate process starts and takes a few minutes to complete.



3. After deactivation, you can delete the device completely. Deleting a device removes it from the list of devices connected to the service. The service can then no longer manage the deleted device. Use the following steps to delete the device:
- Go to your StorSimple Device Manager service and click **Devices**. In the **Devices** blade, select the deactivated device that you wish to delete, right-click, and then click **Delete**.



- In the **Delete** blade, type the device name to confirm and then click **Delete**. The deletion takes a few minutes to complete.



- c. After the deletion is successfully complete, you are notified. The device list also updates to reflect the deletion.

Deactivate and retain data

If you are interested in deleting the device but want to retain the data, then complete the following steps:

To deactivate a device and retain the data

1. Deactivate the device. All the volume containers and the snapshots of the device remain.
 - a. Go to your StorSimple Device Manager service and click **Devices**. In the **Devices** blade, select the device that you wish to deactivate, right-click, and then click **Deactivate**.

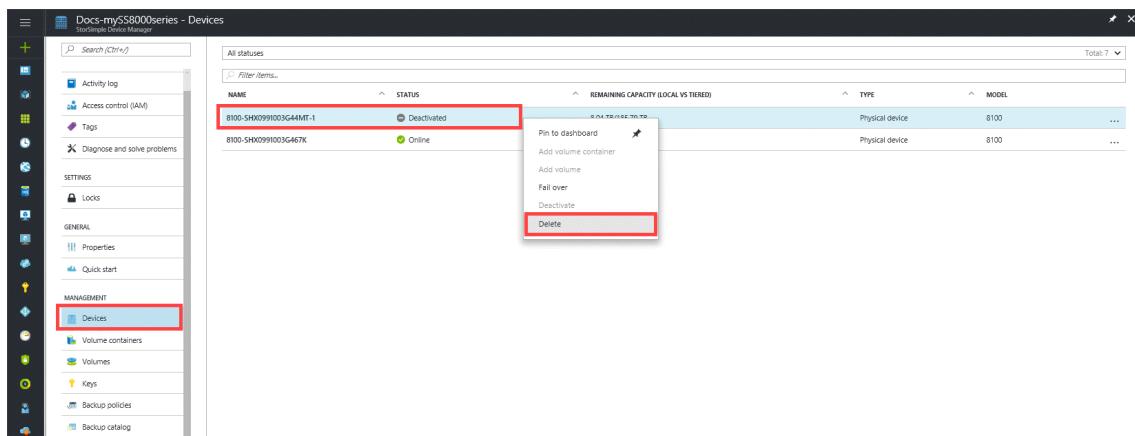
The screenshot shows the 'Devices' section of the StorSimple Device Manager. On the left, there's a sidebar with icons for Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick start), and Management (Devices, Volume containers, Volumes, Keys, Backup policies, Backup catalog). The 'Devices' icon is highlighted with a red box. The main area lists devices with columns for Name, Status, Remaining Capacity (Local vs Tiered), Type, and Model. Two devices are listed: '8100-SHX0991003G44MT-1' (Online, 1.79 TB, Physical device, 8100) and '8100-SHX0991003G467K' (Online, 1.05 TB, Physical device, 8100). A context menu is open over the first device, with 'Deactivate' highlighted by a red box.

- b. In the **Deactivate** blade, type the device name to confirm and then click **Deactivate**. The deactivate process starts and takes a few minutes to complete.

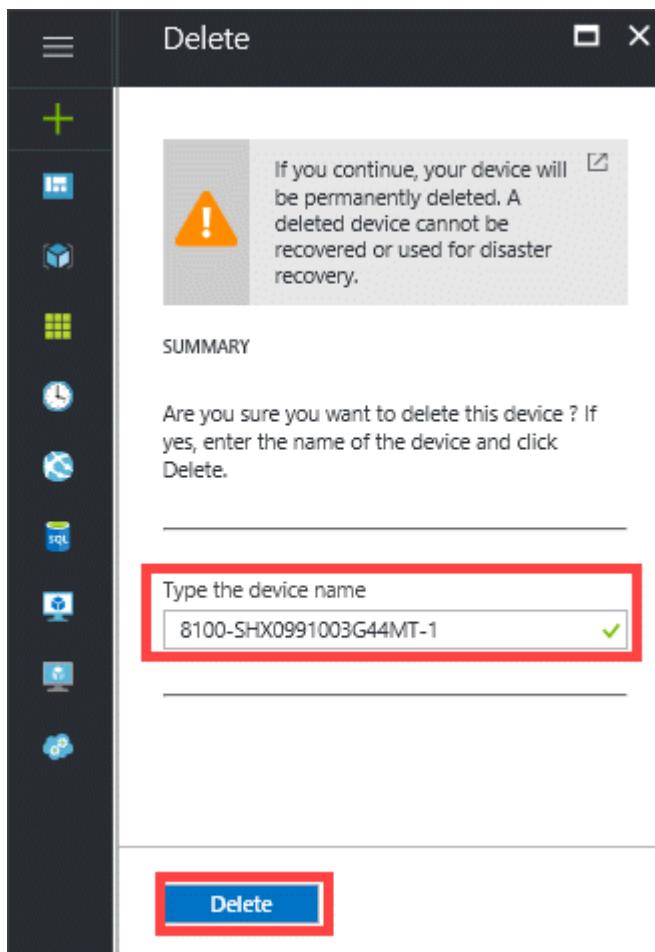
The screenshot shows the 'Deactivate' blade. On the left is a vertical toolbar with icons for Add (+), Home, Devices, Volume containers, Volumes, Keys, SRL, Failover, and Help. The main area has a title bar 'Deactivate' with close and minimize buttons. A warning message box contains text: 'If you continue, your device will be permanently deactivated. A deactivated device cannot be registered with the StorSimple Device Manager service again. If the device has no backups, you cannot fail over after deactivation.' Below it is a 'SUMMARY' section with the question 'Are you sure you want to deactivate this device ?' and instructions to enter the device name and click 'Deactivate'. A text input field contains the device name '8100-SHX0991003G44MT-1', which is highlighted with a red box. At the bottom is a large blue 'Deactivate' button, also highlighted with a red box.

2. You can now fail over the volume containers and the associated snapshots. For procedures, go to [Failover and disaster recovery for your StorSimple device](#).
3. After deactivation and failover, you can delete the device completely. Deleting a device removes it from the list of devices connected to the service. The service can then no longer manage the deleted device. To delete the device, complete the following steps:

- a. Go to your StorSimple Device Manager service and click **Devices**. In the **Devices** blade, select the deactivated device that you wish to delete, right-click, and then click **Delete**.



- b. In the **Delete** blade, type the device name to confirm and then click **Delete**. The deletion takes a few minutes to complete.



- c. After the deletion is successfully complete, you are notified. The device list also updates to reflect the deletion.

Deactivate and delete a cloud appliance

For a StorSimple Cloud Appliance, deactivation from the portal deallocates and deletes the virtual machine, and the resources created when it was provisioned. After the cloud appliance is deactivated, it cannot be restored to its previous state.

The screenshot shows the 'Devices' page in the StorSimple Device Manager. On the left, there's a navigation sidebar with 'Devices' selected. The main area displays a table of devices with columns: NAME, STATUS, REMAINING CAPACITY (LOCAL VS TIERED), TYPE, and MODEL. A context menu is open over the 'myscanew' row, which is highlighted with a red box. The menu options are: Pin to dashboard, Add volume container, Add volume, Fail over, Deactivate (which is highlighted with a red box), and Delete.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.66 TB/200 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100
myscanew	Online	0.0 TB/0.00 TB	Cloud appliance	8010
myscaprem	Online		Cloud appliance	8020

Deactivation results in the following actions:

- The StorSimple Cloud Appliance is removed from the service.
- The virtual machine for the StorSimple Cloud Appliance is deleted.
- The OS disk and data disks created for the StorSimple Cloud Appliance are retained. If you are not using these entities, you should delete them manually.
- The hosted service and Virtual Network that were created during provisioning are retained. If you are not using these entities, you should delete them manually.
- Cloud snapshots created by the StorSimple Cloud Appliance are retained.

After the cloud appliance is deactivated, you can delete it from the list of devices. Select the deactivated device, right-click, and then click **Delete**. StorSimple notifies you once the device is deleted and the list of devices updates.

Next steps

- To restore the deactivated device to factory defaults, go to [Reset the device to factory default settings](#).
- For technical assistance, [contact Microsoft Support](#).
- To learn more about how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).
- After you have deactivated the device, if you would like to keep it, go to [Keep my StorSimple 8000 series appliance](#).

Failover and disaster recovery for your StorSimple 8000 series device

Article • 08/19/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the device failover feature for the StorSimple 8000 series devices and how this feature can be used to recover StorSimple devices if a disaster occurs. StorSimple uses device failover to migrate the data from a source device in the datacenter to another target device. The guidance in this article applies to StorSimple 8000 series physical devices and cloud appliances running software versions Update 3 and later.

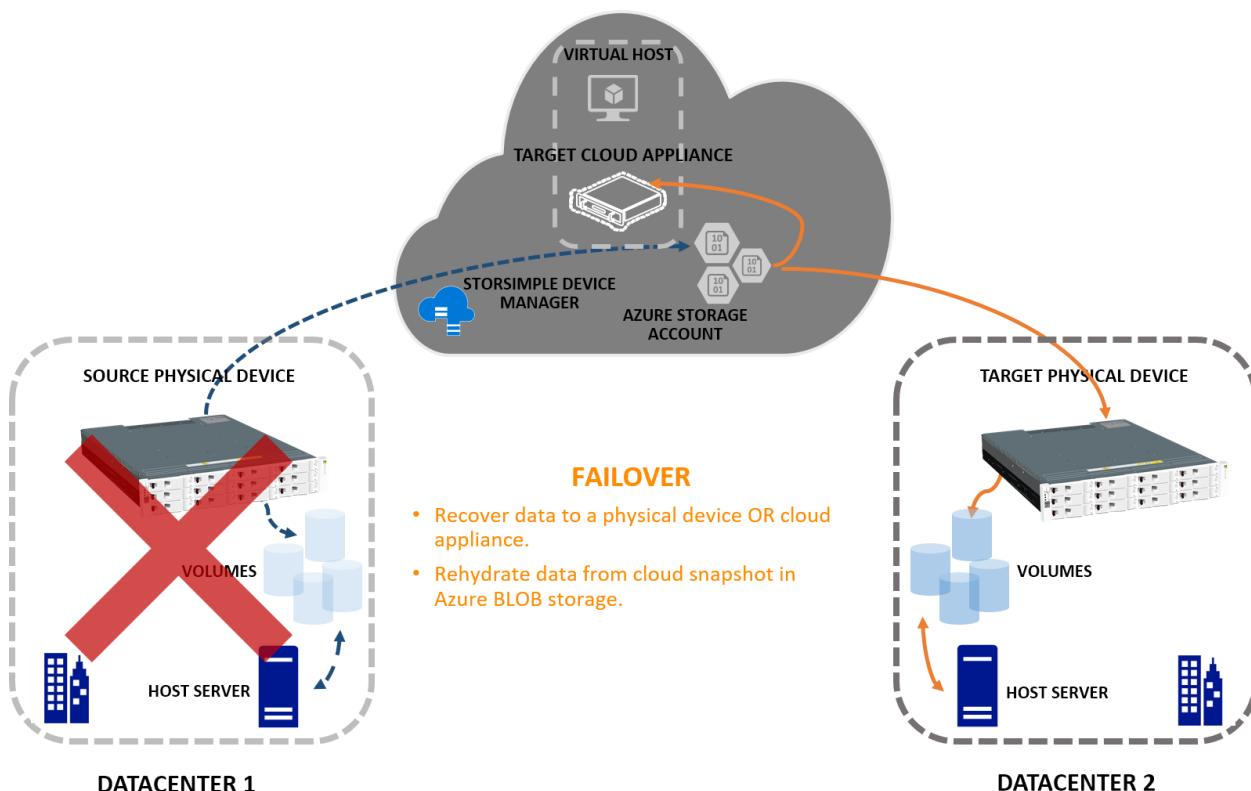
StorSimple uses the **Devices** blade to start the device failover feature in the event of a disaster. This blade lists all the StorSimple devices connected to your StorSimple Device Manager service.

The screenshot shows the StorSimple Device Manager interface. On the left, there's a navigation sidebar with various icons and sections like 'General' and 'Management'. The 'Devices' section is highlighted with a red box. The main pane displays a table of devices with columns for Name, Status, Remaining Capacity (Local vs Tiered), Type, and Model. Two devices are listed: '8100-SHX0991003G44MT' and '8100-SHX0991003G467K', both marked as 'Online'.

Name	Status	Remaining Capacity (Local vs Tiered)	Type	Model
8100-SHX0991003G44MT	Online	8 TB/184.81 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.59 TB/198.54 TB	Physical device	8100

Disaster recovery (DR) and device failover

In a disaster recovery (DR) scenario, the primary device stops functioning. StorSimple uses the primary device as *source* and moves the associated cloud data to another *target* device. This process is referred to as the *failover*. The following graphic illustrates the process of failover.



The target device for a failover could be a physical device or even a cloud appliance. The target device may be located in the same or a different geographical location than the source device.

source device.

During the failover, you can select volume containers for migration. StorSimple then changes the ownership of these volume containers from the source device to the target device. Once the volume containers change ownership, StorSimple deletes these containers from the source device. After the deletion is complete, you can fail back the target device. *Fallback* transfers the ownership back to the original source device.

Cloud snapshot used during device failover

Following a DR, the most recent cloud backup is used to restore the data to the target device. For more information on cloud snapshots, see [Use the StorSimple Device Manager service to take a manual backup](#).

On a StorSimple 8000 series, backup policies are associated with backups. If there are multiple backup policies for the same volume, then StorSimple selects the backup policy with the largest number of volumes. StorSimple then uses the most recent backup from the selected backup policy to restore the data on the target device.

Suppose there are two backup policies, *defaultPol* and *customPol*:

- *defaultPol*: One volume, *vol1*, runs daily starting at 10:30 PM.
- *customPol*: Four volumes, *vol1*, *vol2*, *vol3*, *vol4*, runs daily starting at 10:00 PM.

In this case, StorSimple prioritizes for crash-consistency and uses *customPol* as it has more volumes. The most recent backup from this policy is used to restore data. For more information on how to create and manage backup policies, go to [Use the StorSimple Device Manager service to manage backup policies](#).

Common considerations for device failover

Before you fail over a device, review the following information:

- Before a device failover starts, all the volumes within the volume containers must be offline. In an unplanned failover, StotSimple volumes will automatically go offline. But if you are performing a planned failover (to test DR), you must take all the volumes offline.
- Only the volume containers that have an associated cloud snapshot are listed for DR. There must be at least one volume container with an associated cloud snapshot to recover data.
- If there are cloud snapshots that span across multiple volume containers, StorSimple fails over these volume containers as a set. In a rare instance, if there

are local snapshots that span across multiple volume containers but associated cloud snapshots do not, StorSimple does fail over the local snapshots and the local data is lost after DR.

- The available target devices for DR are devices that have sufficient space to accommodate the selected volume containers. Any devices that do not have sufficient space, are not listed as target devices.
- After a DR (for a limited duration), the data access performance can be affected significantly, as the device needs to access the data from the cloud and store it locally.

Device failover across software versions

A StorSimple Device Manager service in a deployment may have multiple devices, both physical and cloud, all running different software versions.

Use the following table to determine if you can fail over or fail back to another device running a different software version and how the volume types behave during DR.

Failover and fallback across software versions

Fail over/ Fail back from	Physical device	Cloud appliance
Update 3 to Update 4	Tiered volumes fail over as tiered. Locally pinned volumes fail over as locally pinned.	Locally pinned volumes fail over as tiered.
	Following a failover when you take a snapshot on the Update 4 device, heatmap-based tracking kicks in.	
Update 4 to Update 3	Tiered volumes fail over as tiered. Locally pinned volumes fail over as locally pinned.	Locally pinned volumes fail over as tiered.
	Backups used to restore retain heatmap metadata. Heatmap-based tracking is not available in Update 3 following a fallback.	

Device failover scenarios

If there is a disaster, you may choose to fail over your StorSimple device:

- To a physical device.
- To itself.
- To a cloud appliance.

The preceding articles provide detailed steps for each of the above failover cases.

Failback

For Update 3 and later versions, StorSimple also supports failback. Failback is just the reverse of failover, the target becomes the source and the original source device during the failover now becomes the target device.

During failback, StorSimple re-synchronizes the data back to the primary location, halts the I/O and application activity, and transitions back to the original location.

After a failover is complete, StorSimple performs the following actions:

- StorSimple cleans the volume containers that are failed over from the source device.
- StorSimple initiates a background job per volume container (failed over) on the source device. If you attempt to fail back while the job is in progress, you receive a notification to that effect. Wait until the job is complete to start the failback.
- The time taken to complete the deletion of volume containers depends on various factors such as amount of data, age of the data, number of backups, and the network bandwidth available for the operation.

If you are planning test failovers or test failbacks, we recommend that you test volume containers with less data (Gbs). Usually, you can start the failback 24 hours after the failover is complete.

Frequently asked questions

Q. What happens if the DR fails or has partial success?

A. If the DR fails, we recommend that you try again. The second device failover job is aware of the progress of the first job and starts from that point onwards.

Q. Can I delete a device while the device failover is in progress?

A. You cannot delete a device while a DR is in progress. You can only delete your device after the DR is complete. You can monitor the device failover job progress in the **Jobs** blade.

Q. When does the garbage collection start on the source device so that the local data on source device is deleted?

A. Garbage collection is enabled on the source device only after the device is completely cleaned. The cleanup includes cleaning up objects that have failed over from the source device such as volumes, backup objects (not data), volume containers, and policies.

Q. What happens if the delete job associated with the volume containers in the source device fails?

A. If the delete job fails, then you can manually delete the volume containers. In the **Devices** blade, select your source device and click **Volume containers**. Select the volume containers that you failed over and in the bottom of the blade, click **Delete**. After you have deleted all the failed over volume containers on the source device, you can start the failback. For more information, go to [Delete a volume container](#).

Business continuity disaster recovery (BCDR)

A business continuity disaster recovery (BCDR) scenario occurs when the entire Azure datacenter stops functioning. This scenario can affect your StorSimple Device Manager service and the associated StorSimple devices.

If a StorSimple device was registered just before a disaster occurred, then this device may need to undergo a factory reset. After the disaster, the StorSimple device shows up in the Azure portal as offline. This device must be deleted from the portal. Reset the device to factory defaults and register it again with the service.

Next steps

If you are ready to perform a device failover, choose one of the following scenarios for detailed instructions:

- [Fail over to another physical device](#)
- [Fail over to the same device](#)
- [Fail over to StorSimple Cloud Appliance](#)

If you have failed over your device, choose from one of the following options:

- [Deactivate or delete your StorSimple device.](#)
- [Use the StorSimple Device Manager service to administer your StorSimple device.](#)

Fail over to a StorSimple 8000 series physical device

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes the steps required to fail over a StorSimple 8000 series physical device to another StorSimple physical device if there is a disaster. StorSimple uses the device failover feature to migrate data from a source physical device in the datacenter to another physical device. The guidance in this tutorial applies to StorSimple 8000 series physical devices running software versions Update 3 and later.

To learn more about device failover and how it is used to recover from a disaster, go to [Failover and disaster recovery for StorSimple 8000 series devices](#).

To fail over a StorSimple physical device to a StorSimple Cloud Appliance, go to [Fail over to a StorSimple Cloud Appliance](#). To fail over a physical device to itself, go to [Fail over to the same StorSimple physical device](#).

Prerequisites

- Ensure that you have reviewed the considerations for device failover. For more information, go to [Common considerations for device failover](#).
- You must have a StorSimple 8000 series physical device deployed in the datacenter. The device must run Update 3 or later software version. For more information, go to [Deploy your on-premises StorSimple device](#).

Steps to fail over to a physical device

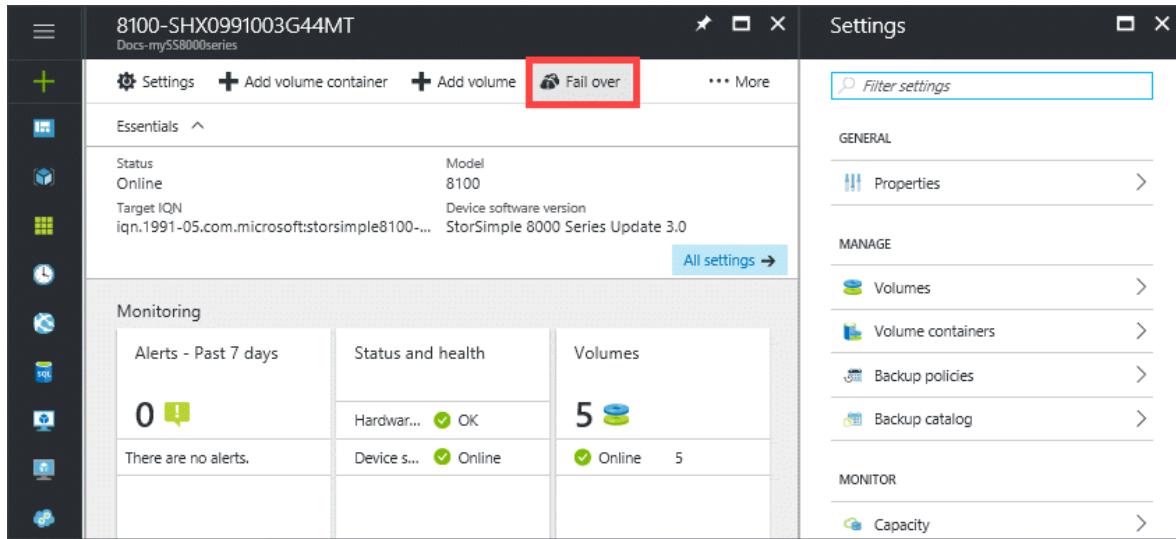
Perform the following steps to restore your device to a target physical device.

1. Verify that the volume container you want to fail over has associated cloud snapshots. For more information, go to [Use StorSimple Device Manager service to create backups](#).
2. Go to your StorSimple Device Manager and then click **Devices**. In the Devices blade, go to the list of devices connected with your service.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8 TB/184.81 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.59 TB/198.54 TB	Physical device	8100

3. Select and click your source device. The source device has the volume containers that you want to fail over. Go to **Settings > Volume Containers**.
4. Select a volume container that you would like to fail over to another device. Click the volume container to display the list of volumes within this container. Select a volume, right-click, and click **Take Offline** to take the volume offline. Repeat this process for all the volumes in the volume container.
5. Repeat the previous step for all the volume containers you would like to fail over to another device.

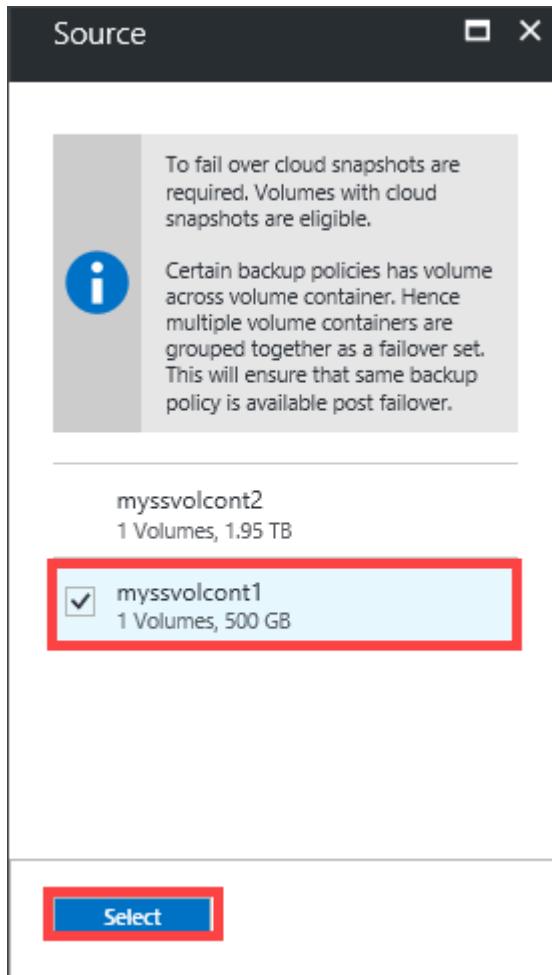
6. Go back to the Devices blade. From the command bar, click Fail over.



The screenshot shows the 'Devices' blade for a device named '8100-SHX0991003G44MT'. The top navigation bar includes 'Settings', 'Add volume container', 'Add volume', 'Fail over' (which is highlighted with a red box), and 'More'. Below the navigation bar, there's an 'Essentials' section showing the device status as 'Online', model '8100', and target IQN 'iqn.1991-05.com.microsoft:storsimple8100~...'. It also displays 'Device software version' as 'StorSimple 8000 Series Update 3.0'. A 'Monitoring' section shows 'Alerts - Past 7 days' (0 alerts), 'Status and health' (Hardware OK), and 'Volumes' (5 volumes, all online). On the right side, there's a 'Settings' pane with sections for 'GENERAL' (Properties), 'MANAGE' (Volumes, Volume containers, Backup policies, Backup catalog), and 'MONITOR' (Capacity).

7. In the Fail over blade, perform the following steps:

- Click **Source**. The volume containers with volumes associated with cloud snapshots are displayed. Only the containers displayed are eligible for failover. In the list of volume containers, select the volume containers you would like to fail over. **Only the volume containers with associated cloud snapshots and offline volumes are displayed.**

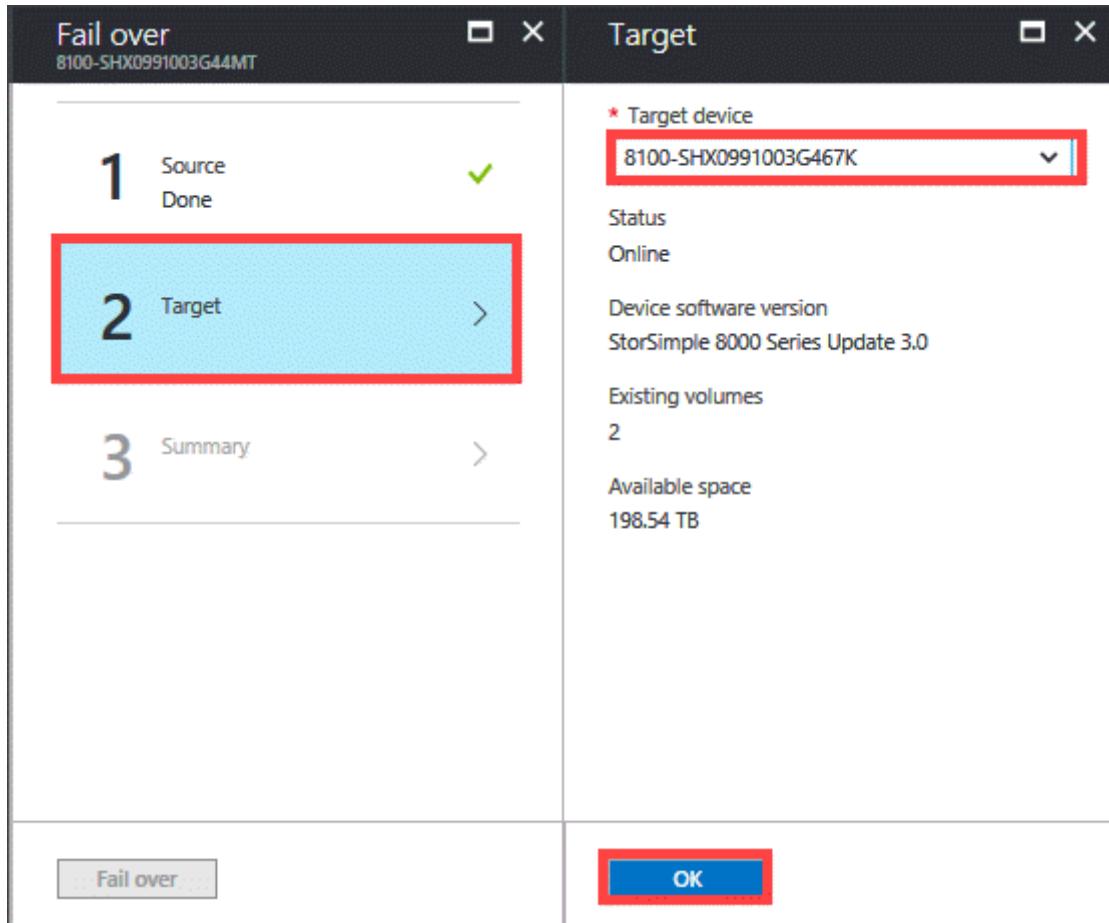


The screenshot shows the 'Source' blade. It contains a message box with information about failover requirements: 'To fail over cloud snapshots are required. Volumes with cloud snapshots are eligible.' and 'Certain backup policies has volume across volume container. Hence multiple volume containers are grouped together as a failover set. This will ensure that same backup policy is available post failover.' Below this, there's a list of volume containers:

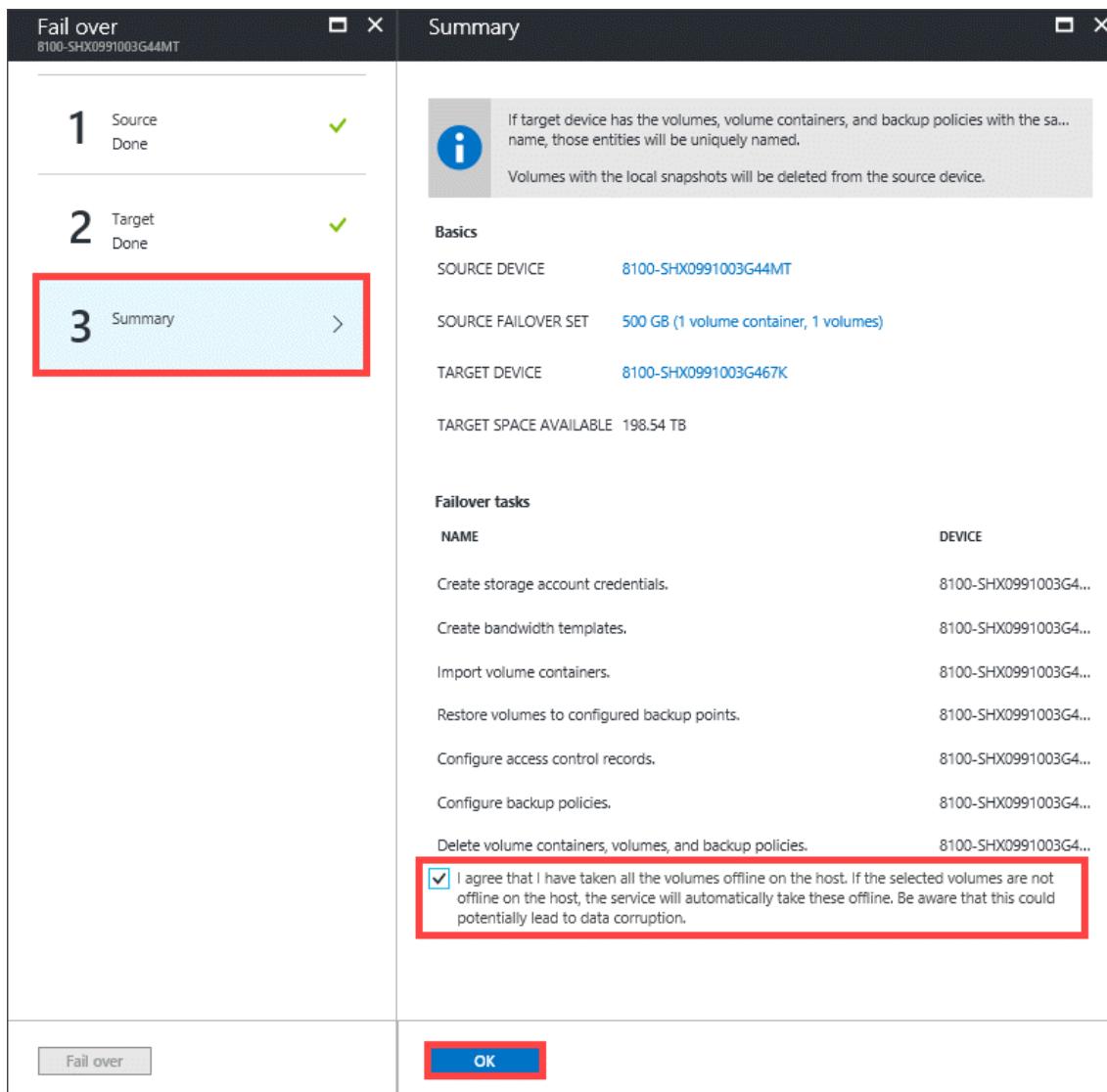
- myssvolcont2
1 Volumes, 1.95 TB
- myssvolcont1
1 Volumes, 500 GB

A large red box highlights the 'myssvolcont1' entry. At the bottom of the blade is a blue 'Select' button, which is also highlighted with a red box.

- b. Click **Target**. For the volume containers selected in the previous step, select a target device from the drop-down list of available devices. Only the devices that have sufficient capacity to accommodate source volume containers are displayed in the list.



- c. Finally, review all the failover settings under **Summary**. After you have reviewed the settings, select the checkbox indicating that the volumes in selected volume containers are offline. Click **OK**.



8. StorSimple creates a failover job. Click the job notification to monitor the failover job via the **Jobs** blade.

If the volume container that you failed over has local volumes, then you see individual restore jobs for each local volume (not for tiered volumes) in the container. These restore jobs may take quite some time to complete. It is likely that the failover job may complete earlier. These volumes will have local guarantees only after the restore jobs are complete.

Fail over volume containers

Job

Refresh Cancel

Details

Status	Succeeded
Entity	8100-SHX0991003G44MT (Microsoft.StorSimple/managers/devices)
Device	8100-SHX0991003G467K
Started on	3/3/2017 10:28:27
Completed on	3/3/2017 10:31:33
Duration	3 Minutes, 6 Seconds
Processed data	500 GB out of 500 GB

Tasks

NAME	STATUS
Creation of storage account credentials	Succeeded
Transfer of volume containers and backups	Succeeded
Restoration of volumes	Succeeded
Creation of ACRs	Succeeded
Creation of backup schedules	Succeeded

9. After the failover is completed, go to the **Devices** blade.

a. Select the device that was used as the target device for the failover process.

All statuses				
<input type="text"/> Filter items...				
NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.04 TB/185.79 TB	Physical device	8100 ...
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100 ...

b. Go to the **Volume Containers** blade. All the volume containers, along with the volumes from the old device, should be listed.

The screenshot displays two windows from the StorSimple Device Manager. The left window, titled 'Volume container', lists volume containers with columns for NAME, VOLUMES, CLOUD STORAGE, BANDWIDTH SETTING, and STORAGE ACCOUNT. It shows two entries: 'myssvc1' with 2 volumes and 'myssvolcont1' with 1 volume. The 'myssvolcont1' row is highlighted with a red box. The right window, titled 'myssvolcont1', provides detailed information about the volume container, including its storage account ('myss8000storageacct'), bandwidth setting ('Unlimited'), encryption status ('Enabled'), and volume count ('1'). A sub-panel titled 'Volumes' shows one volume listed as 'Online' with a value of '1', also highlighted with a red box.

Next steps

- After you have performed a failover, you may need to [deactivate or delete your StorSimple device](#).
- For information about how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Fail over to your StorSimple Cloud Appliance

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes the steps required to fail over a StorSimple 8000 series physical device to a StorSimple Cloud Appliance if there is a disaster. StorSimple uses the device failover feature to migrate data from a source physical device in the datacenter to a cloud appliance running in Azure. The guidance in this tutorial applies to StorSimple 8000 series physical devices and cloud appliances running software versions Update 3 and later.

To learn more about device failover and how it is used to recover from a disaster, go to [Failover and disaster recovery for StorSimple 8000 series devices](#).

To fail over a StorSimple physical device to another physical device, go to [Fail over to a StorSimple physical device](#). To fail over a device to itself, go to [Fail over to the same StorSimple physical device](#).

Prerequisites

- Ensure that you have reviewed the considerations for device failover. For more information, go to [Common considerations for device failover](#).
- You must have a StorSimple Cloud Appliance created and configured before running this procedure. If running Update 3 software version or later, consider using an 8020 cloud appliance for the DR. The 8020 model has 64 TB and uses

Premium Storage. For more information, go to [Deploy and manage a StorSimple Cloud Appliance](#).

Steps to fail over to a cloud appliance

Perform the following steps to restore the device to a target StorSimple Cloud Appliance.

1. Verify that the volume container you want to fail over has associated cloud snapshots. For more information, go to [Use StorSimple Device Manager service to create backups](#).
2. Go to your StorSimple Device Manager service and click **Devices**. In the **Devices** blade, go to the list of devices connected with your service.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.04 TB/185.79 TB	Physical device	8100 ...
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100 ...
myscanew	Online	0 Bytes/29.9 TB	Cloud appliance	8010 ...
myscaprem	Online	0 Bytes/64 TB	Cloud appliance	8020 ...

3. Select and click your source device. The source device has the volume containers that you want to fail over. Go to **Settings > Volume Containers**.

NAME	VOLUMES	CLOUD STORAGE	BANDWIDTH SETTING	STORAGE ACCOUNT
myssvolcont2	2	915.6 KB	Unlimited	myss8000storageacct ...
myvolcont3	1	134.54 KB	MyBWTemplate	myss8000storageacct ...

4. Select a volume container that you would like to fail over to another device. Click the volume container to display the list of volumes within this container. Select a volume, right-click, and click **Take Offline** to take the volume offline.

The screenshot shows the 'Volumes' blade for a volume container named 'myssvolcont2'. It lists two volumes: 'myssvolarch1' and 'myssvolsrch2'. The 'myssvolarch1' row is selected and highlighted with a red box. A context menu is open over this row, listing options: 'Pin to dashboard', 'Modify', 'Restore', 'Clone', 'Take offline' (which is also highlighted with a red box), 'Bring online', and 'Delete'. The 'myssvolsrch2' row is also visible below it.

5. Repeat this process for all the volumes in the volume container.

The screenshot shows the 'Volumes' blade for the same volume container 'myssvolcont2'. The two volumes, 'myssvolarch1' and 'myssvolsrch2', are now both listed as 'Offline' (indicated by a red circle icon). The 'myssvolarch1' row is selected and highlighted with a red box. The context menu from the previous step is no longer visible.

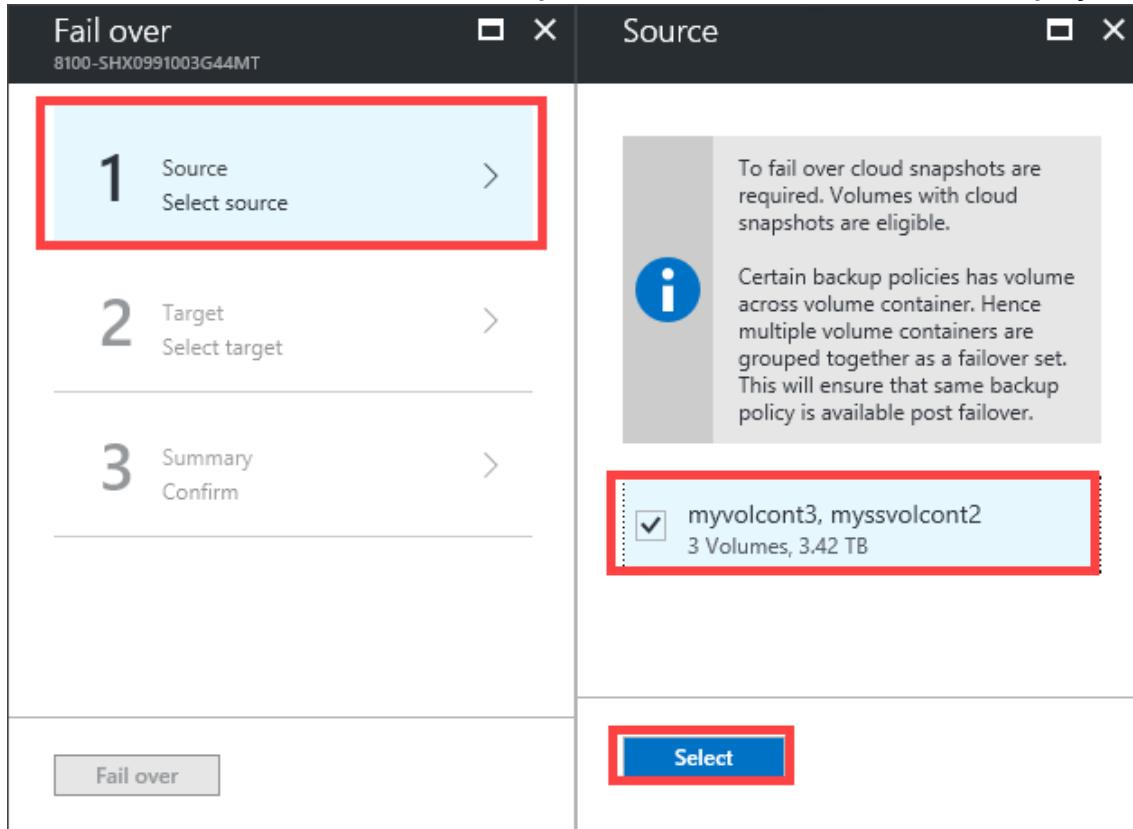
6. Repeat the previous step for all the volume containers you would like to fail over to another device.

7. Go back to the **Devices** blade. From the command bar, click **Fail over**.

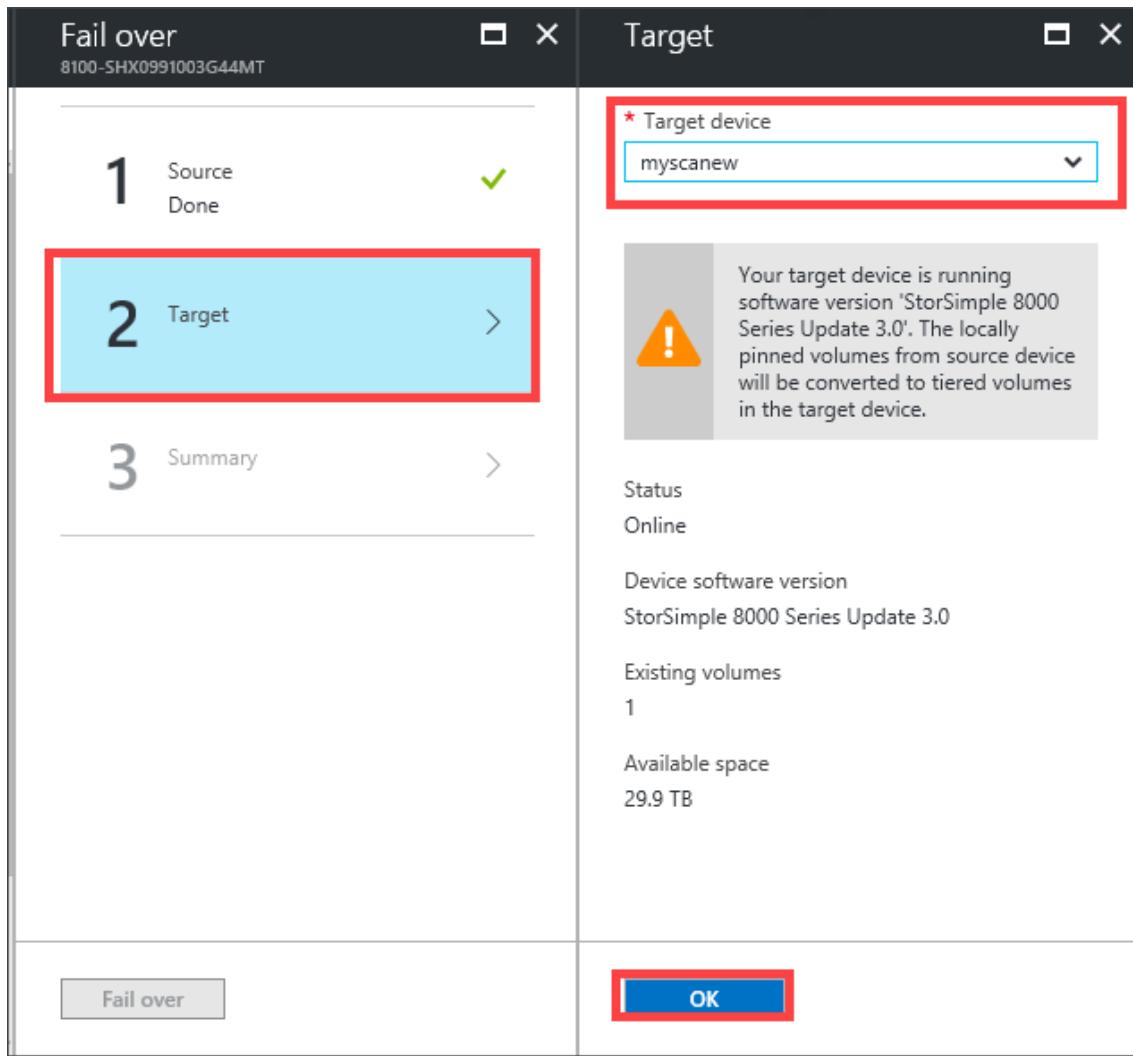
The screenshot shows the 'Devices' blade for a device with the serial number '8100-SHX0991003G44MT' and model 'Docs-mySS8000series'. The command bar at the top includes 'Settings', '+ Add volume container', '+ Add volume', a red-highlighted 'Fail over' button, and 'More'. Below the command bar, there's an 'Essentials' section with status information: 'Status: Online', 'Model: 8100', 'Target IQN: iqn.1991-05.com.microsoft:storsimple8100...', and 'Device software version: StorSimple 8000 Series Update 4.0'. At the bottom right of the blade, there's a link 'All settings →'.

8. In the **Fail over** blade, perform the following steps:

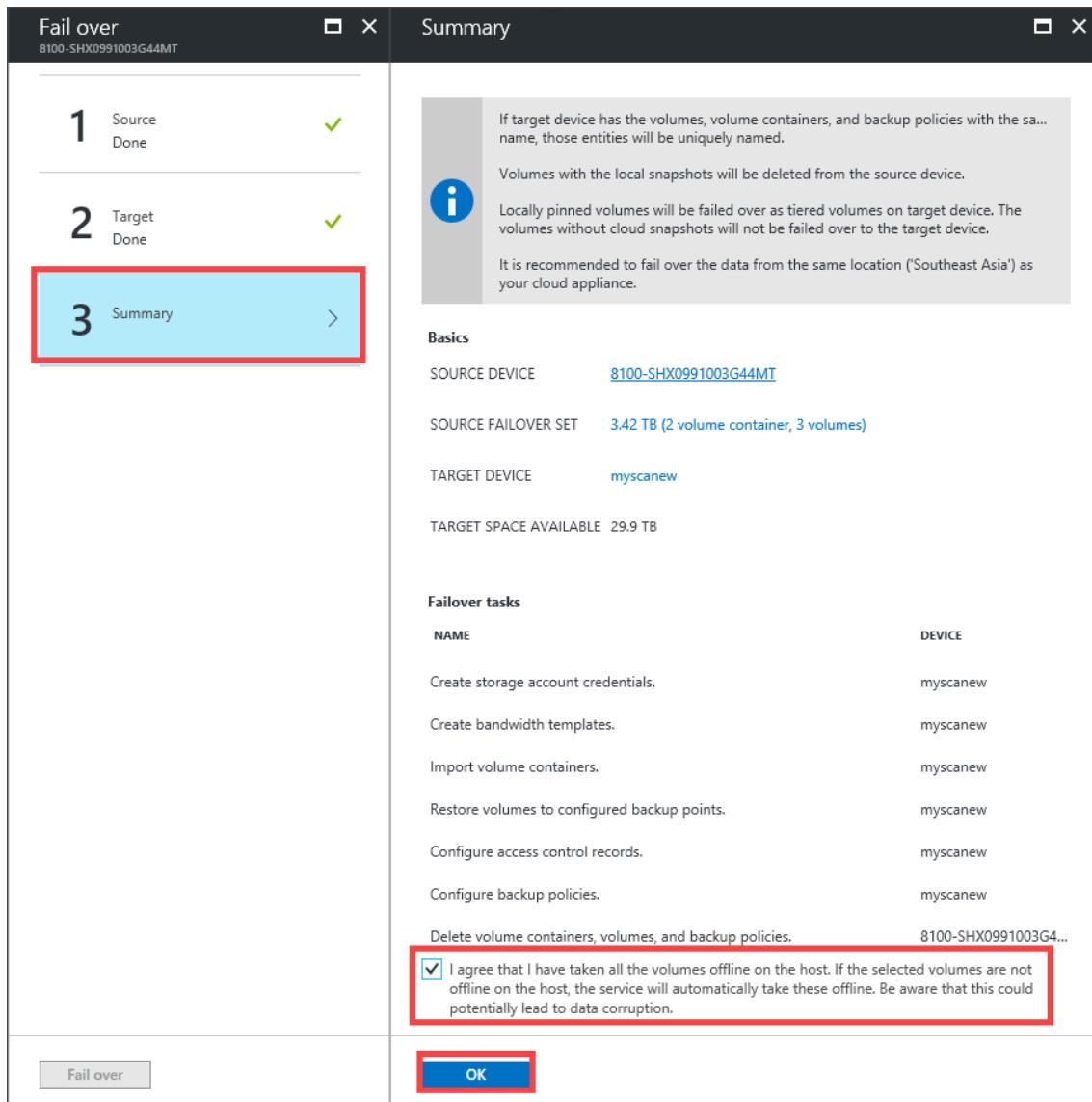
- a. Click **Source**. Select the volume containers to fail over. **Only the volume containers with associated cloud snapshots and offline volumes are displayed.**



- b. Click **Target**. Select a target cloud appliance from the dropdown list of available devices. **Only the devices that have sufficient capacity to accommodate source volume containers are displayed in the list.**



- c. Review the failover settings under **Summary** and select the checkbox indicating that the volumes in selected volume containers are offline.



9. A failover job is created. To monitor the failover job, click the job notification.

Fail over volume containers

Job

Refresh Cancel

Details

Status	Succeeded
Entity	8100-SHX0991003G44MT (Microsoft.StorSimple/managers/devices)
Device	8100-SHX0991003G467K
Started on	3/3/2017 10:28:27
Completed on	3/3/2017 10:31:33
Duration	3 Minutes, 6 Seconds
Processed data	500 GB out of 500 GB

Tasks

NAME	STATUS
Creation of storage account credentials	✓ Succeeded
Transfer of volume containers and backups	✓ Succeeded
Restoration of volumes	✓ Succeeded
Creation of ACRs	✓ Succeeded
Creation of backup schedules	✓ Succeeded

10. After the failover is completed, go back to the **Devices** blade.

a. Select the device that was used as the target for the failover.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	✓ Online	8.04 TB/185.79 TB	Physical device	8100 ...
8100-SHX0991003G467K	✓ Online	8.57 TB/198.05 TB	Physical device	8100 ...

b. Click **Volume Containers**. All the volume containers, along with the volumes from the old device, should be listed.

If the volume container that you failed over has locally pinned volumes, those volumes are failed over as tiered volumes. Locally pinned volumes are not supported on a StorSimple Cloud Appliance.

NAME	STATUS	TYPE	CAPACITY	BACKUP	CONNECTED...	MONITORING
myssfsvol1_1	Online	Tiered (Archived)	500 GB	Enabled	myssacr1	Disabled

Next steps

- After you have performed a failover, you may need to deactivate or delete your [StorSimple device](#).
- For information about how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Fail over your StorSimple physical device to same device

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes the steps required to fail over a StorSimple 8000 series physical device to itself if there is a disaster. StorSimple uses the device failover feature to migrate data from a source physical device in the datacenter to another physical device. The guidance in this tutorial applies to StorSimple 8000 series physical devices running software versions Update 3 and later.

To learn more about device failover and how it is used to recover from a disaster, go to [Failover and disaster recovery for StorSimple 8000 series devices](#).

To fail over a physical device to another physical device, go to [Fail over to the same StorSimple physical device](#). To fail over a StorSimple physical device to a StorSimple Cloud Appliance, go to [Fail over to a StorSimple Cloud Appliance](#).

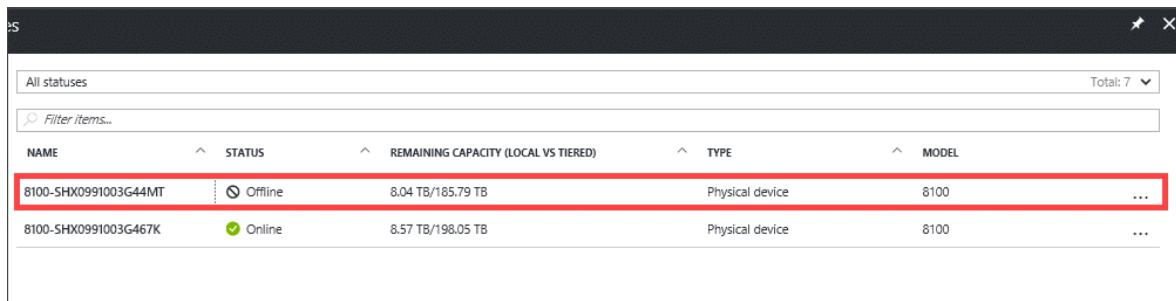
Prerequisites

- Ensure that you have reviewed the considerations for device failover. For more information, go to [Common considerations for device failover](#).

Steps to fail over to the same device

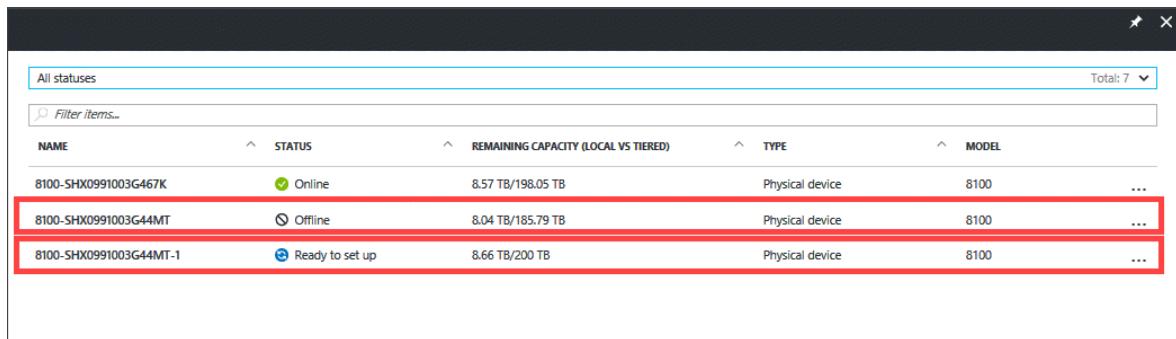
Perform the following steps if you need to fail over to the same device.

1. Take cloud snapshots of all the volumes in your device. For more information, go to [Use StorSimple Device Manager service to create backups](#).
2. Reset your device to factory defaults. Follow the detailed instructions in [how to reset a StorSimple device to factory default settings](#).
3. Go to the StorSimple Device Manager service and then select **Devices**. In the **Devices** blade, the old device should show as **Offline**.



NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Offline	8.04 TB/185.79 TB	Physical device	8100 ...
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100 ...

4. Configure your device and register it again with your StorSimple Device Manager service. The newly registered device should show as **Ready to set up**. The device name for the new device is the same as the old device but appended with a numeral to indicate that the device was reset to factory default and registered again.



NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100 ...
8100-SHX0991003G44MT	Offline	8.04 TB/185.79 TB	Physical device	8100 ...
8100-SHX0991003G44MT-1	Ready to set up	8.66 TB/200 TB	Physical device	8100 ...

5. For the new device, complete the device setup. For more information, go to [Step 4: Complete minimum device setup](#). On the **Devices** blade, the status of the device changes to **Online**.

Important

Complete the minimum configuration first, or your DR may fail.

All statuses							Total: 7
NAME		STATUS	REMAINING CAPACITY (LOCAL VS TIERED)		TYPE	MODEL	
8100-SHX0991003G467K		Online	8.57 TB/198.05 TB		Physical device	8100	...
8100-SHX0991003G44MT		Offline	8.04 TB/185.79 TB		Physical device	8100	...
8100-SHX0991003G44MT-1		Online	8.66 TB/200 TB		Physical device	8100	...

6. Select the old device (status offline) and from the command bar, click **Fail over**. In the **Fail over** blade, select old device as the source and specify the target device as the newly registered device.

Fail over
8100-SHX0991003G44MT

Summary

1 Source Done ✓

2 Target Done ✓

3 Summary >

Basics

SOURCE DEVICE 8100-SHX0991003G44MT

SOURCE FAILOVER SET 3.42 TB (2 volume container, 3 volumes)

TARGET DEVICE 8100-SHX0991003G44MT-1

TARGET SPACE AVAILABLE 200 TB

Failover tasks

NAME	DEVICE
Create storage account credentials.	8100-SHX0991003G4...
Create bandwidth templates.	8100-SHX0991003G4...
Import volume containers.	8100-SHX0991003G4...
Restore volumes to configured backup points.	8100-SHX0991003G4...
Configure access control records.	8100-SHX0991003G4...
Configure backup policies.	8100-SHX0991003G4...
Delete volume containers, volumes, and backup policies.	8100-SHX0991003G4...

I agree that I have taken all the volumes offline on the host. If the selected volumes are not offline on the host, the service will automatically take these offline. Be aware that this could potentially lead to data corruption.

Fail over **OK**

For detailed instructions, refer to Fail over to another physical device.

7. A device restore job is created that you can monitor from the **Jobs** blade.
8. After the job has successfully completed, access the new device and navigate to the **Volume containers** blade. Verify that all the volume containers from the old

device have migrated to the new device.

The screenshot shows the 'Volume container' section of the StorSimple Device Manager. On the left, under 'MANAGE', the 'Volume containers' link is highlighted with a red box. The main area displays two volume containers: 'myssvolcont2' and 'myvolcont3'. Both containers have a value of 2 under 'VOLUMES' and 0 Bytes under 'CLOUD STORAGE'. Under 'BANDWIDTH SETTING', 'myssvolcont2' is set to 'Unlimited' and 'myvolcont3' is set to 'MyBWTemplate'. Under 'STORAGE ACCOUNT', both are associated with 'myss8000storageacct'. A red box highlights the entire list of volume containers.

9. After the failover is complete, you can deactivate and delete the old device from the portal. Select the old device (offline), right-click, and then select **Deactivate**. After the device is deactivated, the status of the device is updated.

The screenshot shows the 'Devices' section of the StorSimple Device Manager. It lists three devices: '8100-SHX0991003G44MT-1' (Online), '8100-SHX0991003G467K' (Online), and '8100-SHX0991003G44MT' (Offline). The third device is highlighted with a red box. A context menu is open on the right, with the 'Delete' option highlighted with a red box.

10. Select the deactivated device, right-click, and then select **Delete**. This deletes the device from the list of devices.

The screenshot shows the 'Devices' section again. The third device, '8100-SHX0991003G44MT', is now listed as 'Deactivated'. A context menu is open on the right, with the 'Delete' option highlighted with a red box.

Next steps

- After you have performed a failover, you may need to [deactivate or delete your StorSimple device](#).
- For information about how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Additional resources

Training

Learning path

[Manage IoT devices by using IoT Hub and apps - Training](#)

Manage IoT devices by using IoT Hub and apps

Use the StorSimple Device Manager service to manage your backup catalog

Article • 08/19/2022 • 4 minutes to read

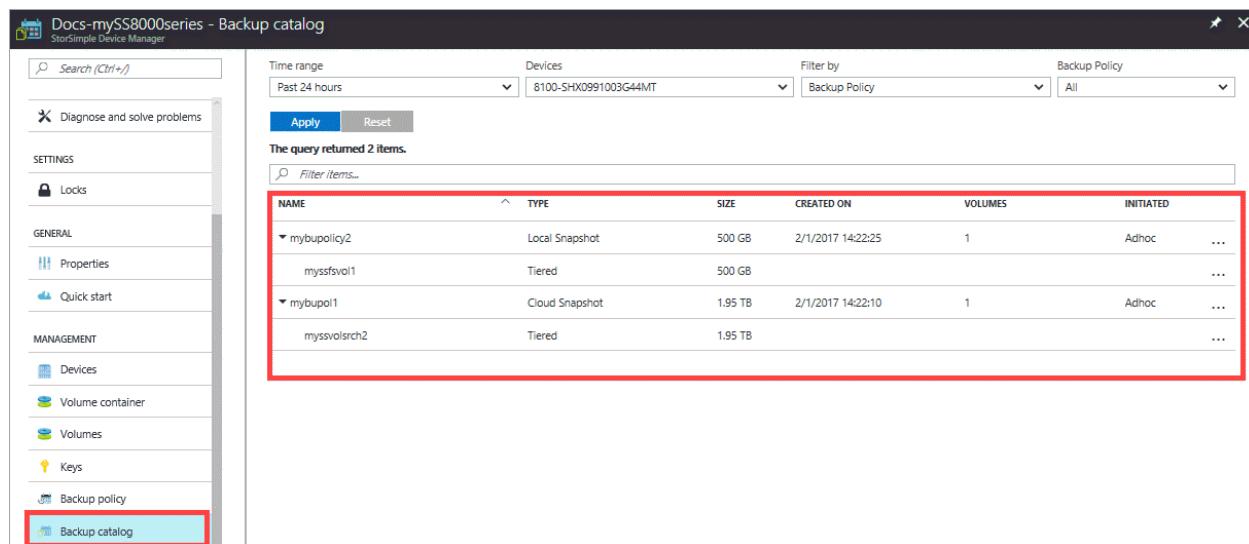
⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service **Backup Catalog** blade displays all the backup sets that are created when manual or scheduled backups are taken. You can use this page to list all the backups for a backup policy or a volume, select or delete backups, or use a backup to restore or clone a volume.

This tutorial explains how to list, select, and delete a backup set. To learn how to restore your device from backup, go to [Restore your device from a backup set](#). To learn how to clone a volume, go to [Clone a StorSimple volume](#).



The screenshot shows the 'Backup catalog' blade in the StorSimple Device Manager interface. The left sidebar has a red box around the 'Backup catalog' link. The main area shows a table with two rows of backup sets. A red box highlights the second row, which contains 'mybupol1'. The table columns are NAME, TYPE, SIZE, CREATED ON, VOLUMES, and INITIATED.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupolc2	Local Snapshot	500 GB	2/1/2017 14:22:25	1	Adhoc
myssfsvol1	Tiered	500 GB			...
mybupol1	Cloud Snapshot	1.95 TB	2/1/2017 14:22:10	1	Adhoc
myssvolsrch2	Tiered	1.95 TB			...

The **Backup Catalog** blade provides a query to narrow your backup set selection. You can filter the backup sets that are retrieved, based on the following parameters:

- **Device** – The device on which the backup set was created.
- **Backup policy or Volume** – The backup policy or volume associated with this backup set.
- **From and To** – The date and time range when the backup set was created.

The filtered backup sets are then tabulated based on the following attributes:

- **Name** – The name of the backup policy or volume associated with the backup set.
- **Size** – The actual size of the backup set.
- **Created On** – The date and time when the backups were created.
- **Type** – Backup sets can be local snapshots or cloud snapshots. A local snapshot is a backup of all your volume data stored locally on the device, whereas a cloud snapshot refers to the backup of volume data residing in the cloud. Local snapshots provide faster access, whereas cloud snapshots are chosen for data resiliency.
- **Initiated By** – The backups can be initiated automatically by a schedule or manually by a user. You can use a backup policy to schedule backups. Alternatively, you can use the **Take backup** option to take a manual backup.

List backup sets for a backup policy

Complete the following steps to list all the backups for a backup policy.

To list backup sets

1. Go to your StorSimple Device Manager service and click **Backup catalog**.
2. Filter the selections as follows:
 - a. Specify the time range.
 - b. Select the appropriate device.
 - c. Filter by **Backup policy** to view the corresponding the backups.
 - d. From the backup policy dropdown list, choose **All** to view all the backups on the selected device.
 - e. Click **Apply** to execute this query.

The backups associated with the selected backup policy should appear in the list of backup sets.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupo1	Cloud Snapshot	1.95 TB	2/1/2017 13:30:00	1	Adhoc

Select a backup set

Complete the following steps to select a backup set for a volume or backup policy.

To select a backup set

1. Go to your StorSimple Device Manager service and click **Backup catalog**.
2. Filter the selections as follows:
 - a. Specify the time range.
 - b. Select the appropriate device.
 - c. Filter by volume or backup policy for the backup that you wish to select.
 - d. Click **Apply** to execute this query.

The backups associated with the selected volume or backup policy should appear in the list of backup sets.

The screenshot shows the 'Backup catalog' page of the StorSimple Device Manager. On the left is a navigation sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS (Locks), GENERAL (Properties, Quick start), MANAGEMENT (Devices, Volume container, Volumes, Keys), Backup policy, and Backup catalog. The 'Backup catalog' option is highlighted with a red box. The main pane displays a table with one item: mybupo1. The table has columns: NAME, TYPE, SIZE, CREATED ON, VOLUMES, and INITIATED. The row for mybupo1 is also highlighted with a red box.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupo1	Cloud Snapshot	1.95 TB	2/1/2017 13:30:00	1	Adhoc

3. Select and expand a backup set. You can now see the backup sets broken down by the volumes that it contains. The **Restore** and **Delete** options are available via the context menu (right-click) for the backup set. You can perform either of these actions on the backup set that you selected.

This screenshot shows the 'Backup catalog' page after filtering by the volume 'myssfsvo1'. The table now lists two items: mybupo1 and myssfsvo1. The row for mybupo1 is expanded, revealing its contents. The expanded view shows mybupo1 with a volume 'myssfsvo1'. The table columns are: NAME, TYPE, SIZE, CREATED ON, VOLUMES, and INITIATED. The rows for mybupo1 and myssfsvo1 are highlighted with a red box.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybupo1	Cloud Snapshot	1.95 TB	2/1/2017 13:30:00	1	Adhoc
myssfsvo1	Tiered	1.95 TB			

Delete a backup set

Delete a backup when you no longer wish to retain the data associated with it. Perform the following steps to delete a backup set.

To delete a backup set

Go to your StorSimple Device Manager service and click **Backup catalog**.

1. Filter the selections as follows:

- Specify the time range.
- Select the appropriate device.
- Filter by volume or backup policy for the backup that you wish to select.
- Click **Apply** to execute this query.

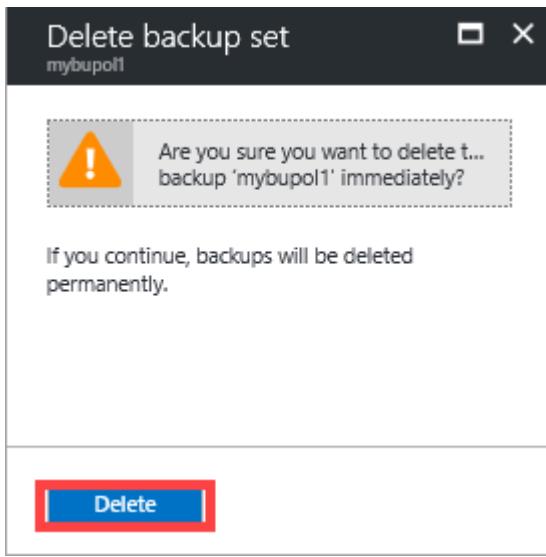
The backups associated with the selected volume or backup policy should appear in the list of backup sets.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybups1	Cloud Snapshot	1.95 TB	2/1/2017 13:30:00	1	Adhoc

2. Select and expand a backup set. You can now see the backup sets broken down by the volumes that it contains. The **Restore** and **Delete** options are available via the context menu (right-click) for the backup set. Right-click the selected backup set and from the context menu, select **Delete**.

NAME	TYPE	SIZE	CREATED ON	VOLUMES	INITIATED
mybups1	Cloud Snapshot	1.95 TB	2/1/2017 13:30:00		Adhoc
mysvolsrch2	Tiered	1.95 TB			

3. When prompted for confirmation, review the displayed information and click **Delete**. The selected backup is deleted permanently.



4. You will be notified when the deletion is in progress and when it has successfully finished. After the deletion is done, refresh the query on this page. The deleted backup set will no longer appear in the list of backup sets.

Next steps

- Learn how to [use the backup catalog to restore your device from a backup set](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service in Azure portal to manage backup policies

Article • 08/19/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to use the StorSimple Device Manager service [Backup policy](#) blade to control backup processes and backup retention for your StorSimple volumes. It also describes how to complete a manual backup.

When you back up a volume, you can choose to create a local snapshot or a cloud snapshot. If you are backing up a locally pinned volume, we recommend that you specify a cloud snapshot. Taking a large number of local snapshots of a locally pinned volume coupled with a data set that has a lot of churn will result in a situation in which you could rapidly run out of local space. If you choose to take local snapshots, we recommend that you take fewer daily snapshots to back up the most recent state, retain them for a day, and then delete them.

When you take a cloud snapshot of a locally pinned volume, you copy only the changed data to the cloud, where it is deduplicated and compressed.

The Backup policy blade

The [Backup policy](#) blade for your StorSimple device allows you to manage backup policies and schedule local and cloud snapshots. Backup policies are used to configure backup schedules and backup retention for a collection of volumes. Backup policies

enable you to take a snapshot of multiple volumes simultaneously. This means that the backups created by a backup policy will be crash-consistent copies.

The backup policies tabular listing also allows you to filter the existing backup policies by one or more of the following fields:

- **Policy name** – The name associated with the policy. The different types of policies include:
 - Scheduled policies, which are explicitly created by the user.
 - Imported policies, which were originally created in the StorSimple Snapshot Manager. These have a tag that describes the StorSimple Snapshot Manager host that the policies were imported from.

 **Note**

Automatic or default backup policies are no longer enabled at the time of volume creation.

- **Last successful backup** – The date and time of the last successful backup that was taken with this policy.
- **Next backup** – The date and time of the next scheduled backup that will be initiated by this policy.
- **Volumes** – The volumes associated with the policy. All the volumes associated with a backup policy are grouped together when backups are created.
- **Schedules** – The number of schedules associated with the backup policy.

The frequently used operations that you can perform for backup policies are:

- Add a backup policy
- Add or modify a schedule
- Add or remove a volume
- Delete a backup policy
- Take a manual backup

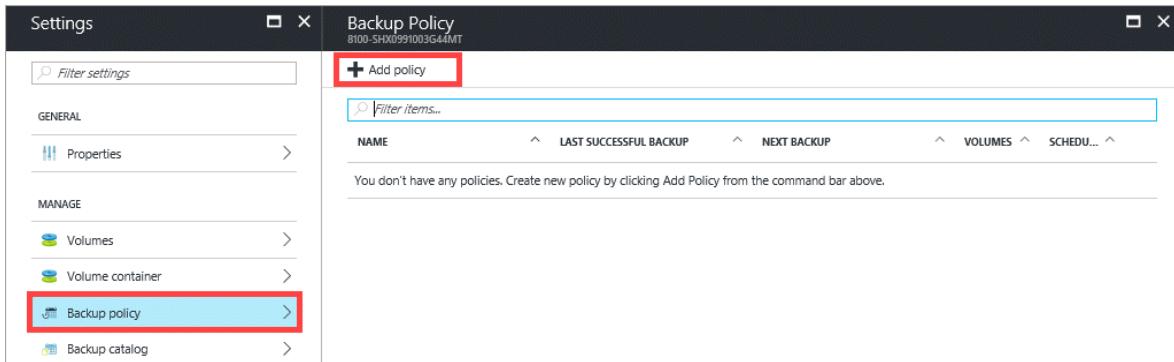
Add a backup policy

Add a backup policy to automatically schedule your backups. When you first create a volume, there is no default backup policy associated with your volume. You need to add and assign a backup policy to protect volume data.

Perform the following steps in the Azure portal to add a backup policy for your StorSimple device. After you add the policy, you can define a schedule (see [Add or modify a schedule](#)).

To add a StorSimple backup policy

1. Go to your StorSimple device and click **Backup policy**.
2. In the **Backup policy** blade, click **+ Add policy** from the command bar.



3. In the **Create backup policy** blade, do the following steps:
 - a. **Select device** is automatically populated based on the device you selected.
 - b. Specify a backup **Policy name** that has from 3 to 150 characters. Once the policy is created, you cannot rename the policy.
 - c. To assign volumes to this backup policy, select **Add volumes** and then from the tabular listing of volumes, click the check box(es) to assign one or more volumes to this backup policy.

The screenshot shows the 'Create backup policy' blade. The 'Select device' dropdown is set to 'myss8000device'. The 'Policy name' field contains 'mybppol1'. The 'Add volumes' section is highlighted with a red box. It shows a dropdown menu with '0 selected' and a list of volumes: 'myssvol1' and 'FIRST SCNEAUE'. Below the volume list is a 'Daily 07:00 PM' schedule entry. At the bottom is a 'Create' button.

- d. To define a schedule for this backup policy, click **First schedule** and then modify the following parameters:

The screenshot shows the 'Create backup policy' dialog box. At the top, it says 'Select device' with 'myss8000device' selected. Below that is 'Policy name *' with 'mybppol1' entered. Under 'Add volumes *' is a dropdown with 'myssvol1'. The 'First schedule' section is highlighted with a red box; it contains a dropdown with 'Daily 07:00 PM'. At the bottom is a blue 'Create' button.

- i. For **Snapshot type**, select **Cloud or Local**.
- ii. Indicate the frequency of backups (specify a number and then choose **Days** or **Weeks** from the drop-down list).
- iii. Enter a retention schedule.
- iv. Enter a time and date for the backup policy to begin.
- v. Click **OK** to define the schedule.

ⓘ Note

When you reach 64 backups for a schedule and want to retain those backups, you can **disable the schedule** and then add a new schedule with a maximum retention of 64 backups. This workaround will work until you reach the limit of 256 backups per volume. At that point, you'll need to delete older backups before you can take new backups.

- e. Click **Create** to create a backup policy.
- f. You are notified when the backup policy is created. The newly added policy is displayed in the tabular view on the **Backup Policy** blade.

NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDULED
mybupol1	2/1/2017 22:30:30	2/1/2017 22:30:30	2	1

Add or modify a schedule

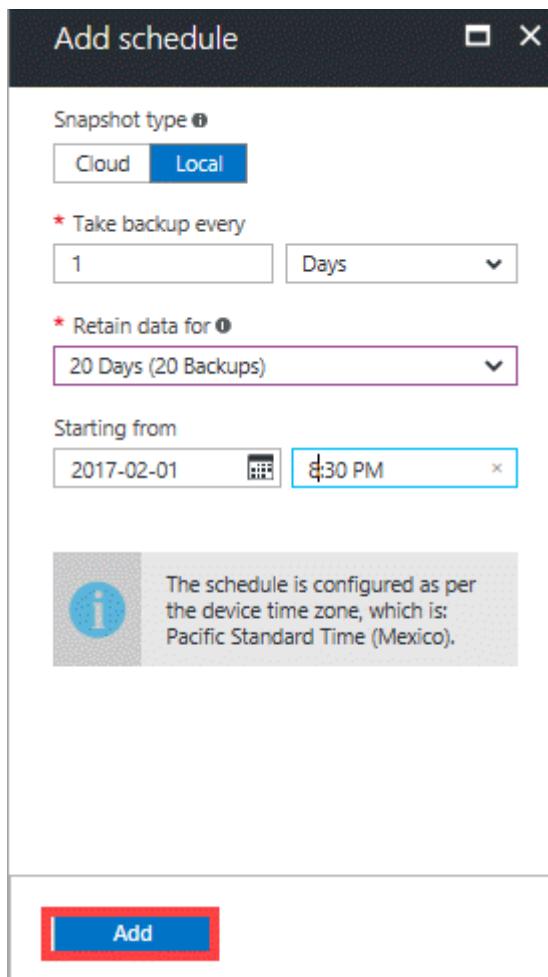
You can add or modify a schedule that is attached to an existing backup policy on your StorSimple device. Perform the following steps in the Azure portal to add or modify a schedule.

To add or modify a StorSimple backup schedule

1. Go to your StorSimple device and click **Backup policy**.
2. In the tabular listing of the policies, select and click the policy that you want to modify. Right-click to invoke the context menu and then select **Add schedule**.

NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDULED
mybupol1	2/1/2017 22:30:30	2/1/2017 22:30:30	2	1

3. In the **Add schedule** blade, modify the snapshot type, backup frequency, retention, and start date and time. Click **Add**.



4. You are notified when the backup policy creation is complete. The backup policy list is also updated.

NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDULED
mybupol1	2/1/2017 20:30:30		2	2

Disable a schedule

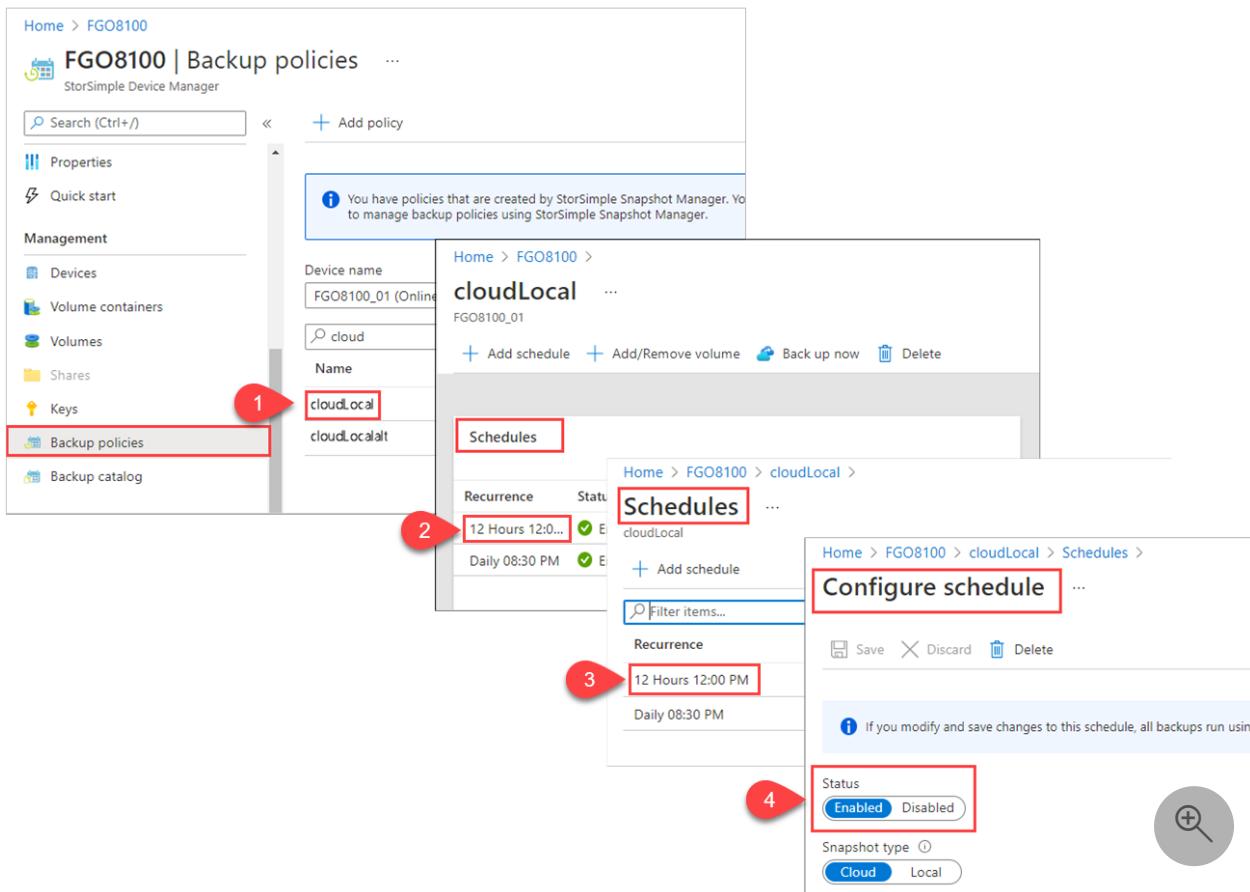
Use the following procedure if you need to disable a back policy. For example, you may want to disable a schedule that's reached the maximum 64 backups and then add a new schedule to take more backups.

To disable a backup policy, do these steps:

1. Go to your StorSimple device and click **Backup policies**.

2. Drill down from the backup policy to the schedule that you want to disable:

- a. Click the backup policy to open **Schedules** for the policy.
- b. Click the policy again to open the **Schedules** dialog box.
- c. Click the schedule you want to disable to open **Configure schedule**. In the **Status** field, select **Disabled**.

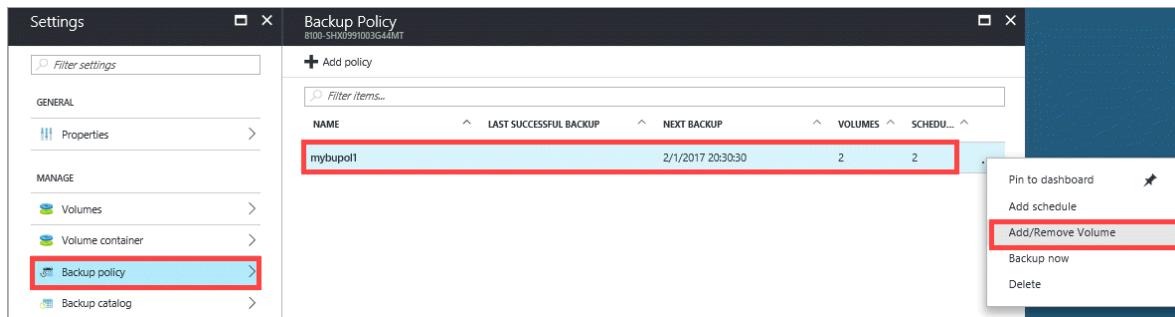


Add or remove a volume

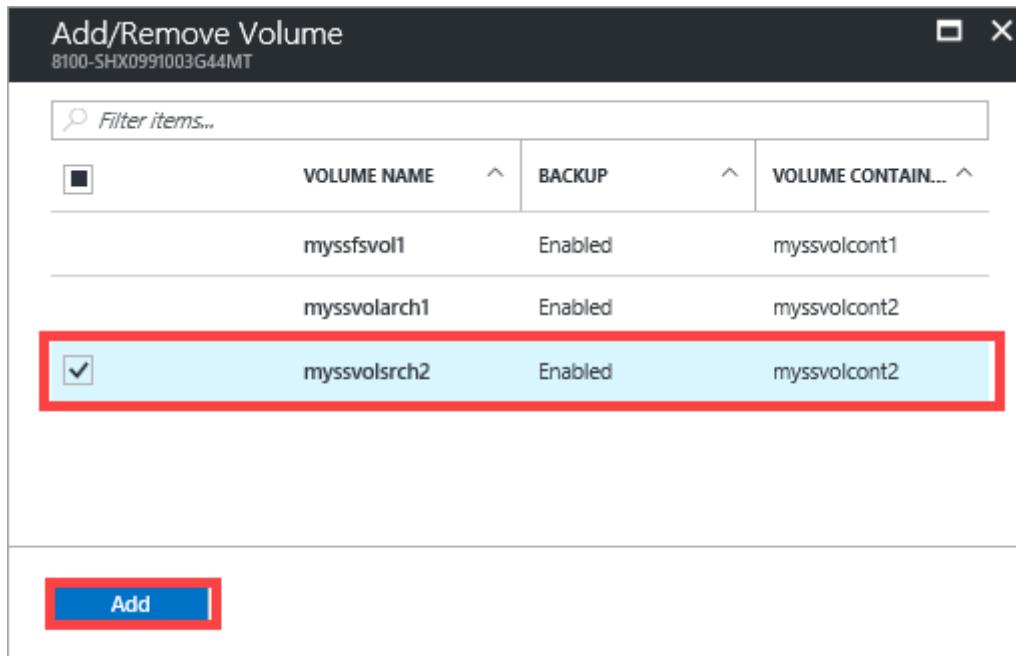
You can add or remove a volume assigned to a backup policy on your StorSimple device. Perform the following steps in the Azure portal to add or remove a volume.

To add or remove a volume

1. Go to your StorSimple device and click **Backup policy**.
2. In the tabular listing of the policies, select and click the policy that you want to modify. Right-click to invoke the context menu and then select **Add/remove volume**.



3. In the **Add/remove volume** blade, select or clear the check box(es) to add or remove the volume. Multiple volumes are selected/cleared by checking or clearing the corresponding checkboxes.



If you assign volumes from different volume containers to a backup policy, then you will need to remember to fail over those volume containers together. You will see a warning to that effect.

The screenshot shows the 'Add/Remove Volume' interface. At the top, there is a warning message: 'You selected volumes which are part of different volume containers. This will impact your failover unit. During failover all the volume containers of selected volumes needs to be failed over together.' Below this is a table with columns: VOLUME NAME, BACKUP, and VOLUME CONTAIN... The rows for 'myssfsvol1', 'myssvolarch1', and 'myssvolsrch2' are selected and highlighted with a red box. Each row contains a checked checkbox in the first column, the volume name, its backup status (Enabled), and its volume container name.

	VOLUME NAME	BACKUP	VOLUME CONTAIN...
<input checked="" type="checkbox"/>	myssfsvol1	Enabled	myssvolcont1
<input checked="" type="checkbox"/>	myssvolarch1	Enabled	myssvolcont2
<input checked="" type="checkbox"/>	myssvolsrch2	Enabled	myssvolcont2

Add

4. You are notified when the backup policy is modified. The backup policy list is also updated.

The screenshot shows the 'Backup Policy' interface. On the left, there is a navigation menu with options: Properties, Volumes, Volume container, Backup policy (which is selected and highlighted with a red box), and Backup catalog. The main area displays a table of backup policies. The columns are: NAME, LAST SUCCESSFUL BACKUP, NEXT BACKUP, VOLUMES, and SCHEDUL... The row for 'mybupol1' is selected and highlighted with a red box. The 'VOLUMES' column shows the number 1.

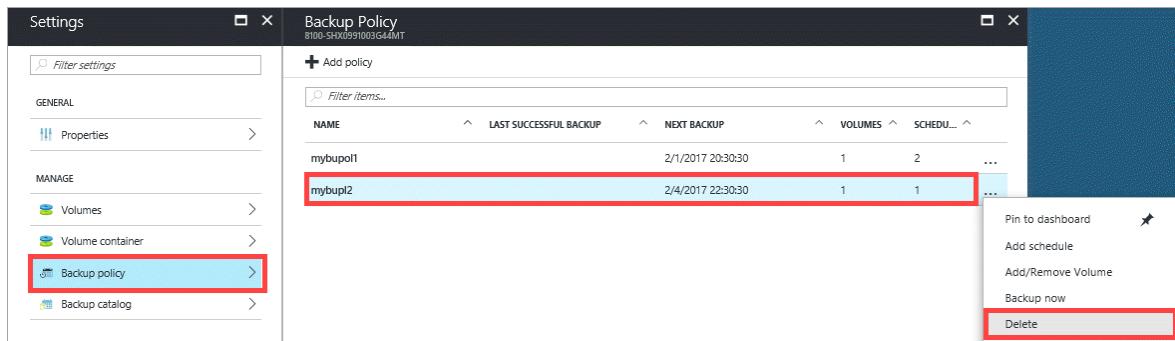
NAME	LAST SUCCESSFUL BACKUP	NEXT BACKUP	VOLUMES	SCHEDUL...
mybupol1	2/1/2017 20:30:30		1	2 ...

Delete a backup policy

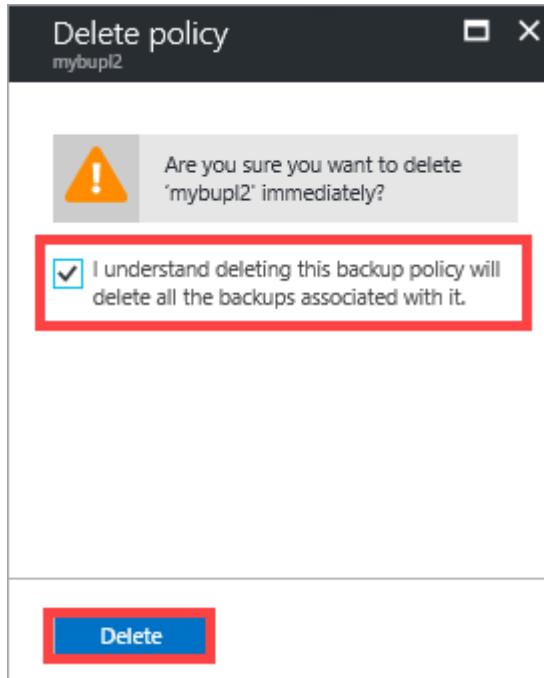
Perform the following steps in the Azure portal to delete a backup policy on your StorSimple device.

To delete a StorSimple backup policy

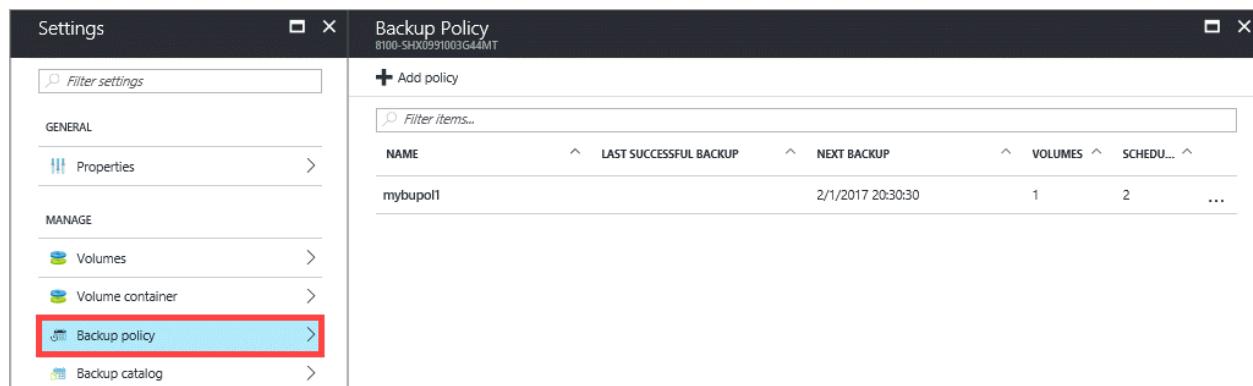
1. Go to your StorSimple device and click **Backup policy**.
2. In the tabular listing of backup policies, select the policy you want to delete. Right-click and from the context menu, select **Delete**.



3. You will be prompted for confirmation. Keep in mind that deleting a backup policy will delete all the associated backups. Click **Yes** to delete.



The backup policies list will be updated to display the new list of policies.

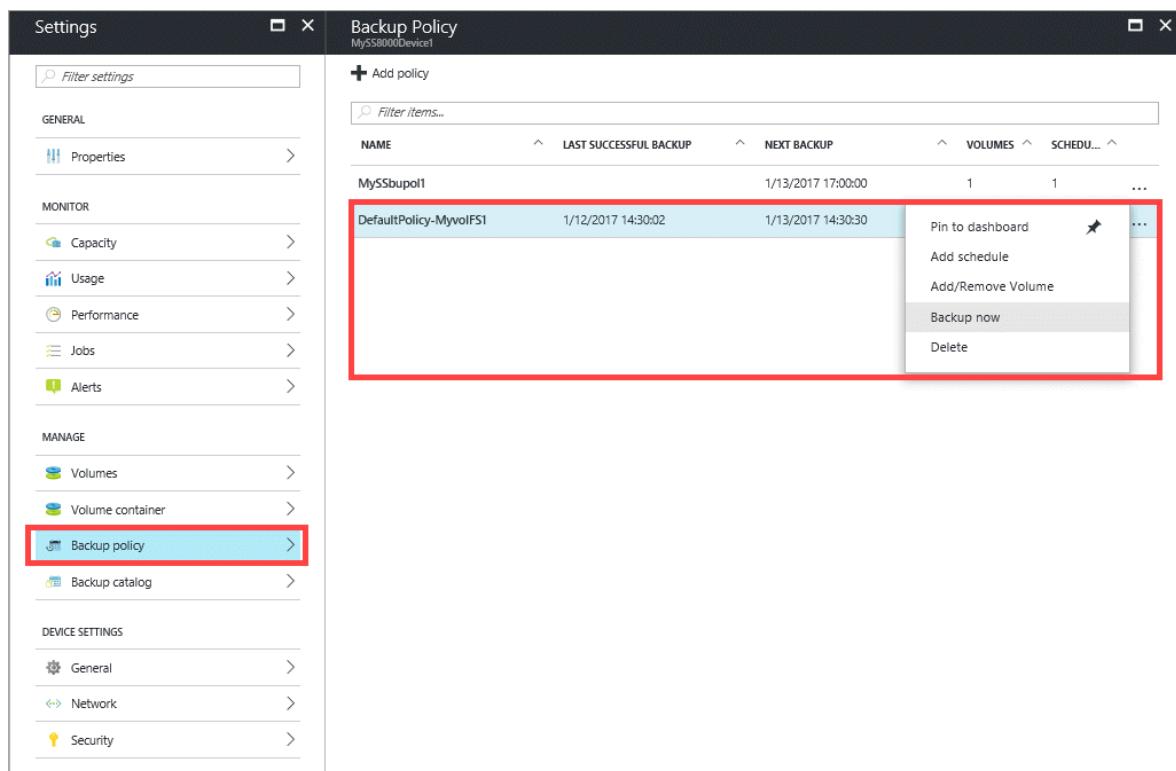


Take a manual backup

Perform the following steps in the Azure portal to create an on-demand (manual) backup for a single volume.

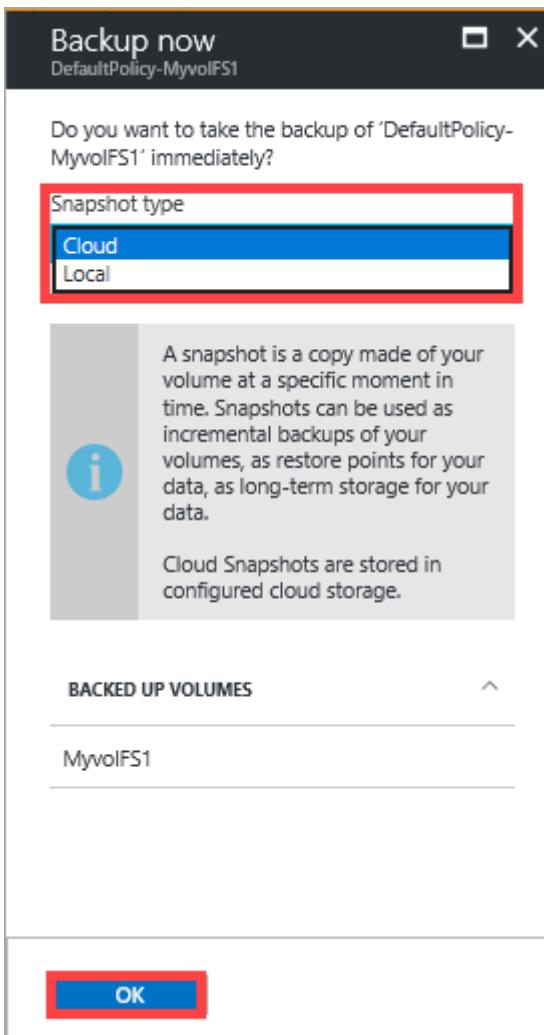
To create a manual backup

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of devices, select your device. Go to **Settings > Manage > Backup policies**.
2. The **Backup policies** blade lists all the backup policies in a tabular format, including the policy for the volume that you want to back up. Select the policy associated with the volume you want to back up and right-click to invoke the context menu. From the dropdown list, select **Back up now**.



3. In the **Back up now** blade, do the following steps:

- a. Choose the appropriate **Snapshot type** from the dropdown list: **Local** snapshot or **Cloud** snapshot. Select local snapshot for fast backups or restores, and cloud snapshot for data resiliency.



- b. Click **OK** to start a job to create a snapshot. You will see a notification at the top of the page after the job is successfully created.



- c. To monitor the job, click the notification. This takes you to the **Jobs** blade where you can view the job progress.
4. After the backup job is finished, go to the **Backup catalog** tab.
5. Set the filter selections to the appropriate device, backup policy, and time range. The backup should appear in the list of backup sets that is displayed in the catalog.

Next steps

Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to manage your storage account credentials

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Configuration section in the StorSimple Device Manager service blade presents all the global service parameters that can be created in the StorSimple Device Manager service. These parameters can be applied to all the devices connected to the service, and include:

- Storage account credentials
- Bandwidth templates
- Access control records

This tutorial explains how to add, edit, or delete storage account credentials, or rotate the security keys for a storage account.

The screenshot shows the 'MySS8000DeviceManager - Storage account credentials' window. On the left, a navigation pane lists various management categories: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS (Locks), GENERAL (Properties, Quick start), MANAGEMENT (Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog), MONITORING (Capacity, Usage, Jobs, Alerts), and CONFIGURATION (Storage account credentials). The 'Storage account credentials' item is currently selected and highlighted with a blue bar. The main right pane displays a table titled 'Add' with two rows of storage account credentials. The columns are 'NAME' and 'SSL ENABLED'. The first row has 'myss8000stor' in the NAME column and 'Yes' in the SSL ENABLED column. The second row has 'myss8000storage' in the NAME column and 'Yes' in the SSL ENABLED column. A red box highlights the first row.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	Yes

Storage accounts contain the credentials that the StorSimple device uses to access your storage account with your cloud service provider. For Microsoft Azure storage accounts, these are credentials such as the account name and the primary access key.

On the **Storage account credentials** blade, all storage accounts that are created for the billing subscription are displayed in a tabular format containing the following information:

- **Name** – The unique name assigned to the account when it was created.
- **SSL enabled** – Whether the TLS is enabled and device-to-cloud communication is over the secure channel.
- **Used by** – The number of volumes using the storage account.

The most common tasks related to storage accounts that can be performed are:

- Add a storage account
- Edit a storage account
- Delete a storage account
- Key rotation of storage accounts

Types of storage accounts

There are three types of storage accounts that can be used with your StorSimple device.

- **Auto-generated storage accounts** – As the name suggests, this type of storage account is automatically generated when the service is first created. To learn more about how this storage account is created, see [Step 1: Create a new service](#) in [Deploy your on-premises StorSimple device](#).
- **Storage accounts in the service subscription** – These are the Azure storage accounts that are associated with the same subscription as that of the service. To learn more about how these storage accounts are created, see [About Azure Storage Accounts](#).
- **Storage accounts outside of the service subscription** – These are the Azure storage accounts that are not associated with your service and likely existed before the service was created.

Add a storage account

You can add a storage account by providing a unique friendly name and access credentials that are linked to the storage account (with the specified cloud service provider). You also have the option of enabling the Transport Layer Security (TLS) mode, previously known as Secure Sockets Layer (SSL) mode, to create a secure channel for network communication between your device and the cloud.

You can create multiple accounts for a given cloud service provider. Be aware, however, that after a storage account is created, you cannot change the cloud service provider.

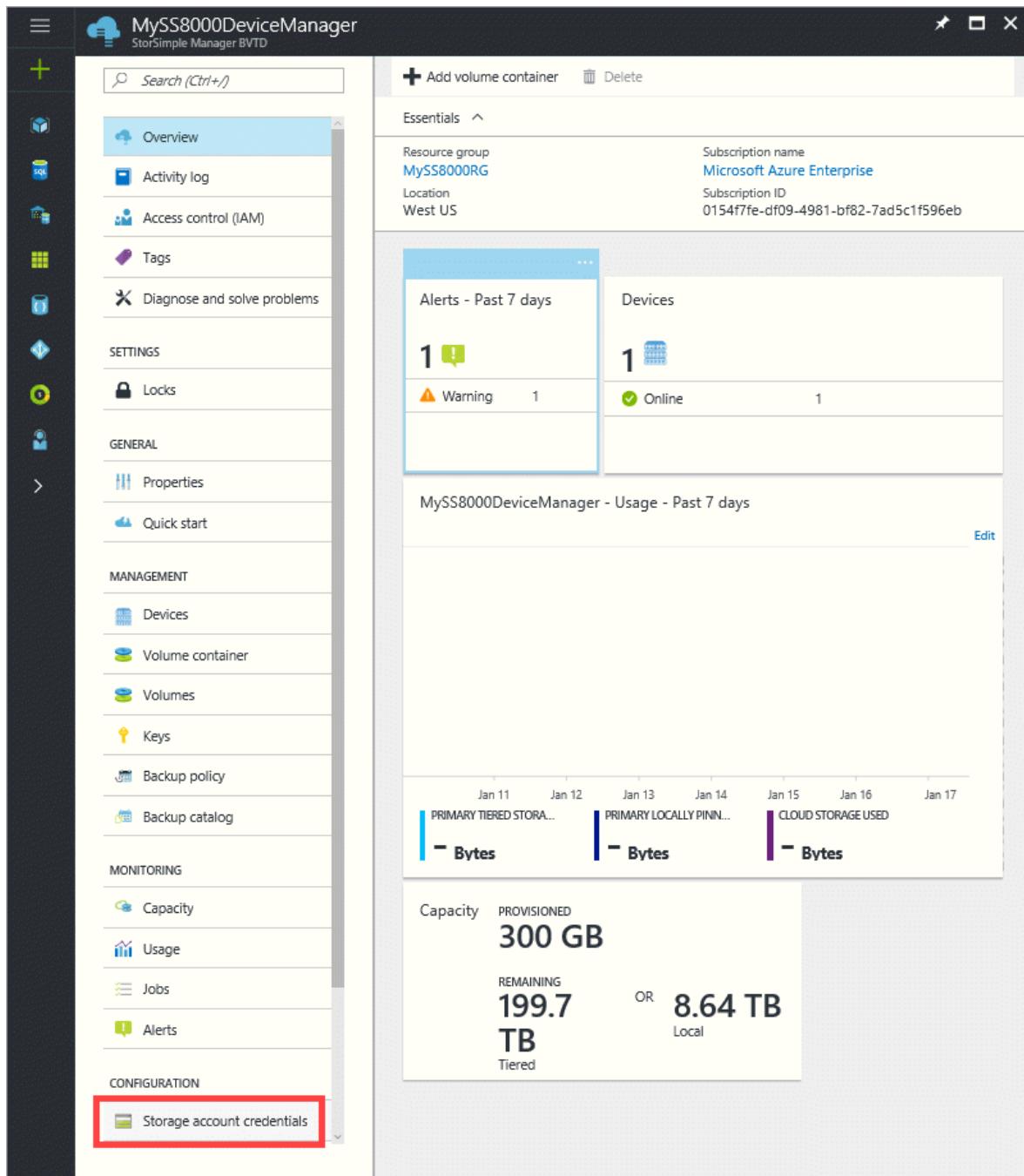
While the storage account is being saved, the service attempts to communicate with your cloud service provider. The credentials and the access material that you supplied will be authenticated at this time. A storage account is created only if the authentication succeeds. If the authentication fails, then an appropriate error message will be displayed.

Use the following procedures to add Azure storage account credentials:

- To add a storage account credential that has the same Azure subscription as the Device Manager service
- To add an Azure storage account credential that is outside of the Device Manager service subscription

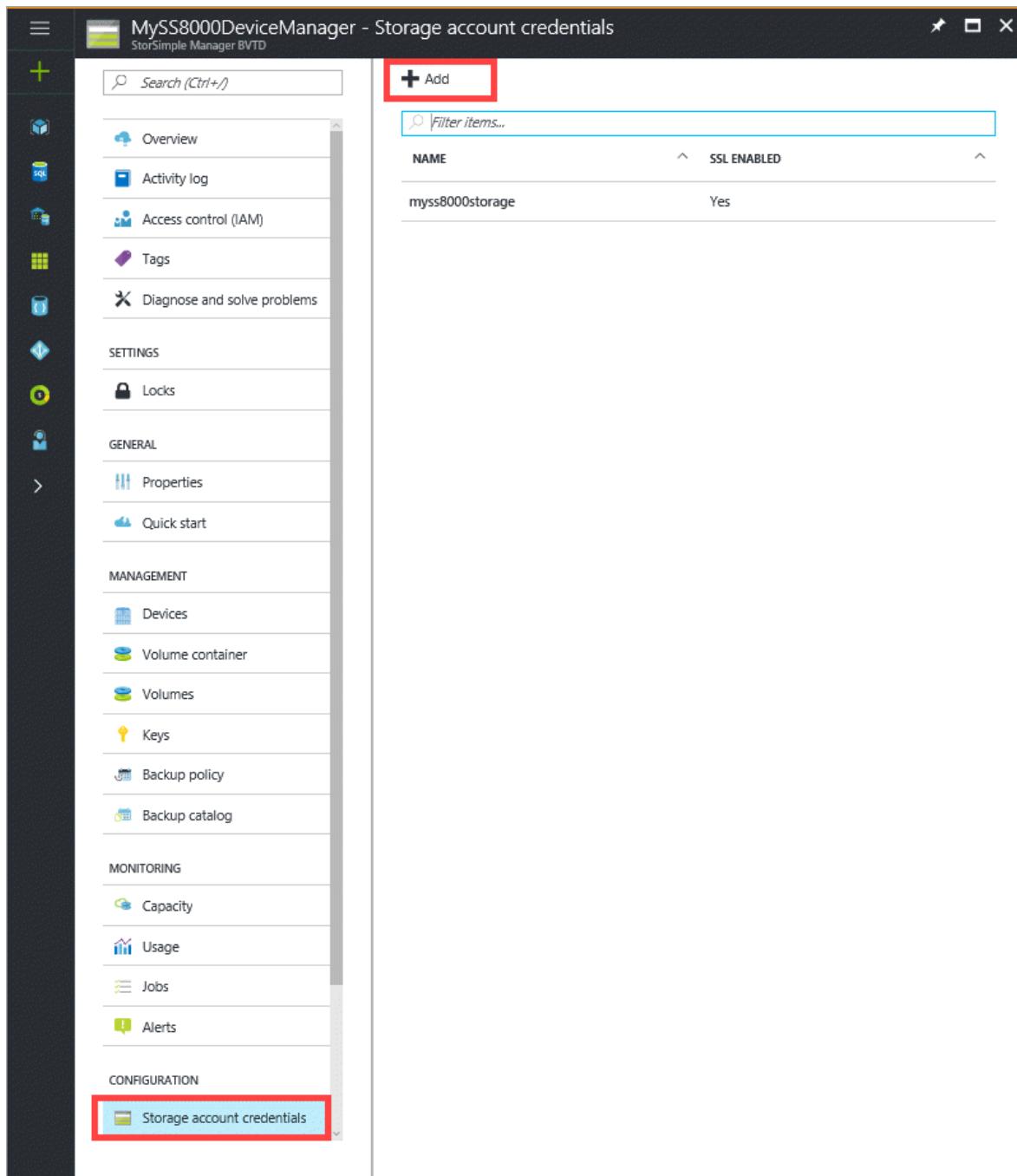
To add a storage account credential in the same Azure subscription as the StorSimple Device Manager service

1. Go to your StorSimple Device Manager service. In the Configuration section, click Storage account credentials.



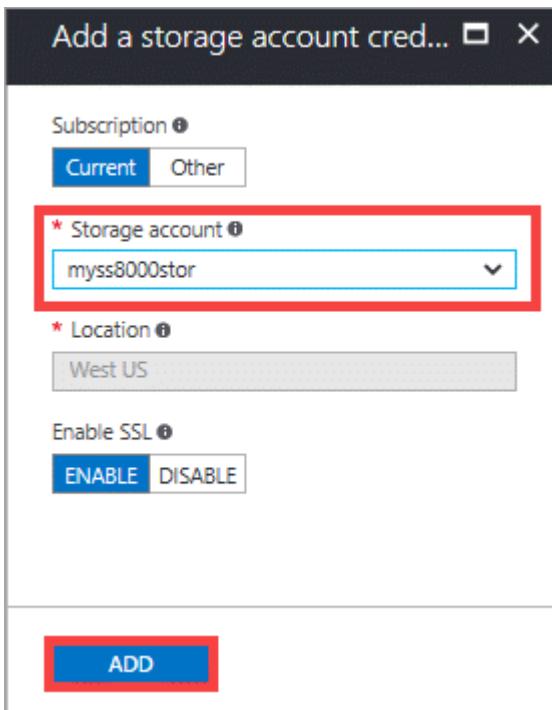
The screenshot shows the Microsoft Azure portal interface for the 'MySS8000DeviceManager' resource group. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Quick start, Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog, Capacity, Usage, Jobs, and Alerts. The 'Storage account credentials' option is located under the 'CONFIGURATION' section at the bottom of the list, and it is highlighted with a red box. The main content area displays an 'Essentials' blade with information about the resource group, including its name ('MySS8000ORG'), location ('West US'), and subscription details ('Microsoft Azure Enterprise' with ID '0154f7fe-df09-4981-bf82-7ad5c1f596eb'). Below this is a summary card for 'Alerts - Past 7 days' showing 1 warning, and another card for 'Devices' showing 1 online device. At the bottom, there's a chart titled 'MySS8000DeviceManager - Usage - Past 7 days' showing storage usage over time, with capacity and provisioned values of 300 GB and remaining storage of 199.7 TB Tiered.

2. On the Storage account credentials blade, click + Add.



3. In the **Add a storage account credential** blade, do the following steps:

- a. As you are adding a storage account credential in the same Azure subscription as your service, ensure that **Current** is selected.
- b. From the **storage account** dropdown list, select an existing storage account.
- c. Based on the storage account selected, the **location** will be displayed (grayed out and cannot be changed here).
- d. Select **Enable SSL Mode** to create a secure channel for network communication between your device and the cloud. Disable **Enable SSL** only if you are operating within a private cloud.



- e. Click **Add** to start the job creation for the storage account credential. You will be notified after the storage account credential is successfully created.

Add storage account credential 'myss80... 1:34 PM
Successfully completed the operation.

The newly created storage account credential will be displayed under the list of **Storage account credentials**.

The screenshot shows the 'MySS8000DeviceManager - Storage account credentials' blade in the StorSimple Manager BVTD. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), General (Properties, Quick start), Management (Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog), Monitoring (Capacity, Usage, Jobs, Alerts), and Configuration (Storage account credentials). The 'Storage account credentials' link is highlighted with a blue selection bar. The main pane displays a table titled 'Add' with a single row. The row contains two columns: 'NAME' and 'SSL ENABLED'. The 'NAME' column has the value 'myss8000stor' and the 'SSL ENABLED' column has the value 'Yes'. The entire row is highlighted with a red border.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	Yes

To add an Azure storage account credential outside of the StorSimple Device Manager service subscription

1. Navigate to your StorSimple Device Manager service, select and double-click it. This opens the **Overview** blade.
2. Select **Storage account credentials** within the **Configuration** section. This lists any existing storage account credentials associated with the StorSimple Device Manager service.
3. Click **Add**.

4. In the **Add a storage account credential** blade, do the following:
 - a. For **Subscription**, select **Other**.
 - b. Provide the name of your Azure storage account credential.
 - c. In the **Storage account access key** text box, supply the primary Access Key for your Azure storage account credential. To get this key, go to the Azure Storage service, select your storage account credential, and click **Manage account keys**. You can now copy the primary access key.
 - d. To enable TLS, click the **Enable** button to create a secure channel for network communication between your StorSimple Device Manager service and the cloud. Click the **Disable** button only if you are operating within a private cloud.
 - e. Click **Add**. You are notified after the storage account credential is successfully created.
5. The newly created storage account credential is displayed on the StorSimple Configure Device Manager service blade under **Storage account credentials**.

Edit a storage account

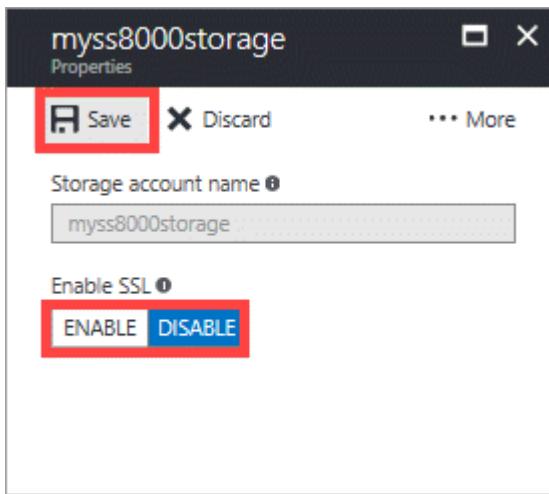
You can edit a storage account that is used by a volume container. If you edit a storage account that is currently in use, the only field available to modify is the access key for the storage account. You can supply the new storage access key and save the updated settings.

To edit a storage account

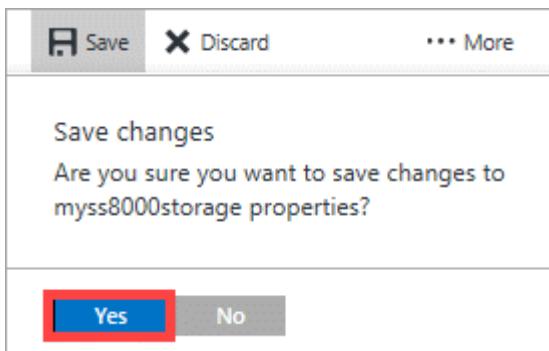
1. Go to your StorSimple Device Manager service. In the **Configuration** section, click **Storage account credentials**.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	Yes

2. In the **Storage account credentials** blade, from the list of storage account credentials, select and click the one you wish to edit.
3. You can modify the **Enable SSL** selection. You can also click **More...** and then select **Sync access key to rotate** your storage account access keys. Go to [Key rotation of storage accounts](#) for more information on how to perform key rotation. After you have modified the settings, click **Save**.



4. When prompted for confirmation, click **Yes**.



The settings will be updated and saved for your storage account.

Delete a storage account

i Important

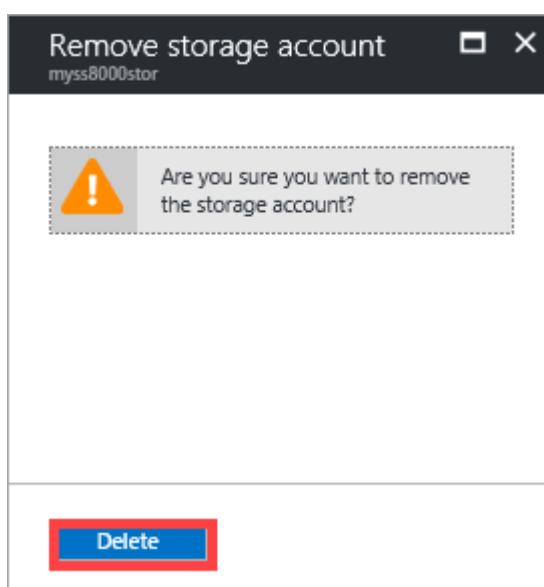
You can delete a storage account only if it is not used by a volume container. If a storage account is being used by a volume container, first delete the volume container and then delete the associated storage account.

To delete a storage account

1. Go to your StorSimple Device Manager service. In the **Configuration** section, click **Storage account credentials**.
2. In the tabular list of storage accounts, hover over the account that you wish to delete. Right-click to invoke the context menu and click **Delete**.

The screenshot shows the StorSimple Manager interface for managing storage account credentials. The left sidebar lists various management categories. Under the 'CONFIGURATION' section, 'Storage account credentials' is selected and highlighted with a red box. In the main pane, a table lists storage accounts. The row for 'myss8000stor' is selected and highlighted with a red box. A context menu is open over this row, with the 'Delete' option highlighted with a red box.

3. When prompted for confirmation, click Yes to continue with the deletion. The tabular listing will be updated to reflect the changes.



Key rotation of storage accounts

For security reasons, key rotation is often a requirement in data centers. Each Microsoft Azure subscription can have one or more associated storage accounts. The access to these accounts is controlled by the subscription and access keys for each storage account.

When you create a storage account, Microsoft Azure generates two 512-bit storage access keys that are used for authentication when the storage account is accessed. Having two storage access keys allows you to regenerate the keys with no interruption to your storage service or access to that service. The key that is currently in use is the *primary* key and the backup key is referred to as the *secondary* key. One of these two keys must be supplied when your Microsoft Azure StorSimple device accesses your cloud storage service provider.

What is key rotation?

Typically, applications use only one of the keys to access your data. After a certain period of time, you can have your applications switch over to using the second key. After you have switched your applications to the secondary key, you can retire the first key and then generate a new key. Using the two keys this way allows your applications access to the data without incurring any downtime.

The storage account keys are always stored in the service in an encrypted form. However, these can be reset via the StorSimple Device Manager service. The service can get the primary key and secondary key for all the storage accounts in the same subscription, including accounts created in the Storage service as well as the default storage accounts generated when the StorSimple Device Manager service was first created. The StorSimple Device Manager service will always get these keys from the Azure classic portal and then store them in an encrypted manner.

Rotation workflow

A Microsoft Azure administrator can regenerate or change the primary or secondary key by directly accessing the storage account (via the Microsoft Azure Storage service). The StorSimple Device Manager service does not see this change automatically.

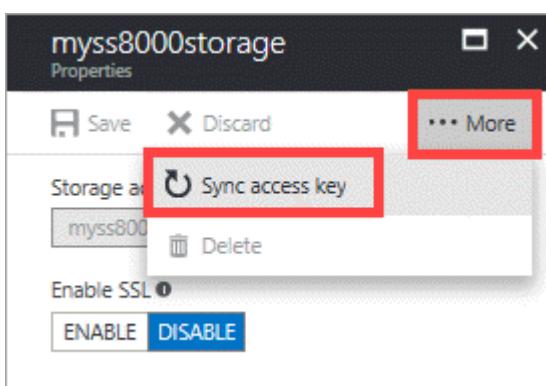
To inform the StorSimple Device Manager service of the change, you will need to access the StorSimple Device Manager service, access the storage account, and then synchronize the primary or secondary key (depending on which one was changed). The service then gets the latest key, encrypts the keys, and sends the encrypted key to the device.

To synchronize keys for storage accounts in the same subscription as the service

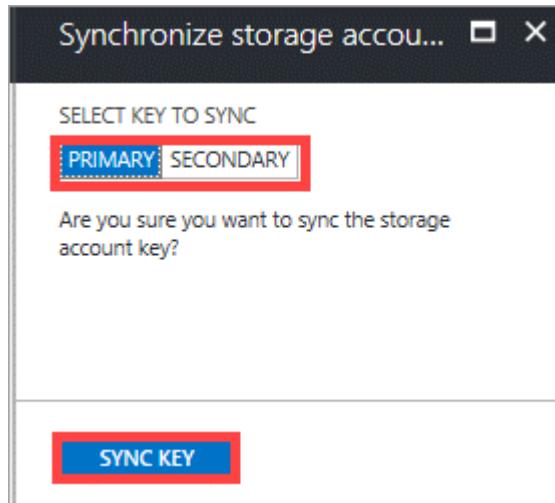
1. Go to your StorSimple Device Manager service. In the Configuration section, click **Storage account credentials**.
2. From the tabular listing of storage accounts, click the one that you want to modify.

NAME	SSL ENABLED
myss8000stor	Yes
myss8000storage	No

3. Click ...More and then select Sync access key to rotate.



4. In the StorSimple Device Manager service, you need to update the key that was previously changed in the Microsoft Azure Storage service. If the primary access key was changed (regenerated), select **primary** key. If the secondary key was changed, select **secondary** key. Click **Sync key**.



You will be notified after the key is successfully synchronized.

To synchronize keys for storage accounts outside of the service subscription

1. On the Services page, click the **Configure** tab.
2. Click **Add/Edit Storage Accounts**.
3. In the dialog box, do the following:
 - a. Select the storage account with the access key that you want to update.
 - b. You will need to update the storage access key in the StorSimple Device Manager service. In this case, you can see the storage access key. Enter the new key in the **Storage Account Access Key** box.
 - c. Save your changes. Your storage account access key should now be updated.

Next steps

- Learn more about [StorSimple security](#).
- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to manage StorSimple volume containers

Article • 08/19/2022 • 5 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to use the StorSimple Device Manager service to create and manage StorSimple volume containers.

A volume container in a Microsoft Azure StorSimple device contains one or more volumes that share storage account, encryption, and bandwidth consumption settings. A device can have multiple volume containers for all its volumes.

A volume container has the following attributes:

- **Volumes** – The tiered or locally pinned StorSimple volumes that are contained within the volume container.
- **Encryption** – An encryption key that can be defined for each volume container. This key is used for encrypting the data that is sent from your StorSimple device to the cloud. A military-grade AES-256 bit key is used with the user-entered key. To secure your data, we recommend that you always enable cloud storage encryption.
- **Storage account** – The Azure storage account that is used to store the data. All the volumes residing in a volume container share this storage account. You can choose a storage account from an existing list, or create a new account when you create the volume container and then specify the access credentials for that account.
- **Cloud bandwidth** – The bandwidth consumed by the device when the data from the device is being sent to the cloud. If you want the device to consume all

available bandwidth, set this field to **Unlimited**. You can also create and apply a bandwidth template to allocate bandwidth based on a schedule.

The following procedures explain how to use the StorSimple **Volume containers** blade to complete the following common operations:

- Add a volume container
- Modify a volume container
- Delete a volume container

Add a volume container

Perform the following steps to add a volume container.

To create a volume container

1. Go to your StorSimple Device Manager service and click **Devices**. From the tabular listing of the devices, select and click a device.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERE...)	TYPE	MODEL
TaalaFriendlyNameG1	Online	0 Bytes/1023 GB	Physical device	100
SudasDevice1	Online	32.67 GB/817 GB	Physical device	100
Device1	Offline	34.31 GB/857.83 GB	Physical device	100
Gu3Device2	Offline	19.12 GB/478.16 GB	Physical device	100
Gu3Device1	Deactivated	40.95 GB/1 TB	Physical device	100

2. In the device dashboard, click **+ Add volume container**

The screenshot shows the Dell EMC PowerVault Device Manager interface. On the left, the 'Monitoring' section displays alert counts (4 Critical, 1 Warning) and volume status (1 Online). Below it is the 'TaalaFriendlyNameG1 - Usage - Past 24 hours' section, which includes a timeline from 12 PM to 6 AM showing storage usage across Primary Tiered Storage, Primary Locally Pinned Storage, and Cloud Storage Used. Capacity details show 1 GB provisioned and 1023 GB remaining. On the right, the 'Settings' pane is open, showing a list of management options: General, Monitor, Manage, and Device Settings. Under 'Manage', the 'Volume container' option is highlighted with a red box.

3. In the **Add volume container** blade:

- The device is automatically selected.
- Supply a **Name** for your volume container. The name must be 3 to 32 characters long. You cannot rename a volume container once it is created.
- Select **Enable Cloud Storage Encryption** to enable encryption of the data sent from the device to the cloud.
- Provide and confirm a **Cloud Storage Encryption Key** that is 8 to 32 characters long. This key is used by the device to access encrypted data.
- Select a **Storage Account** to associate with this volume container. You can choose an existing storage account or the default account that is generated at

the time of service creation. You can also use the **Add new** option to specify a storage account that is not linked to this service subscription.

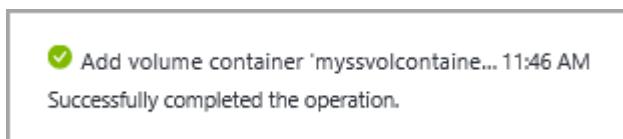
- f. Select **Unlimited** in the **Specify bandwidth** drop-down list if you wish to consume all the available bandwidth.

If you have your bandwidth usage information available, you may be able to allocate bandwidth based on a schedule by specifying **Select a bandwidth template**. For a step-by-step procedure, go to [Add a bandwidth template](#).

The screenshot shows the 'Add volume container' configuration page. It includes fields for selecting a device, naming the container, enabling encryption, setting an encryption key, confirming the key, choosing a storage account credential, and specifying a bandwidth setting. The 'Bandwidth setting' dropdown is highlighted with a red border, indicating it's the current focus or step in the process.

- g. Click **Create**.

You are notified when the volume container is successfully created.



The newly created volume container is listed in the list of volume containers for your device.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and contains a navigation menu with sections like GENERAL, MONITOR, and MANAGE. The 'Volume container' option under MANAGE is highlighted with a blue selection bar. The right window is titled 'Volume container SudasDevice1' and displays a table of volume containers. The table has columns: NAME, VOLUMES, CLOUD ST..., BANDWID..., and STORAGE... . There are three rows: 'VC1' with 9 volumes, 'myssvolcontainer1' with 0 volumes (which is highlighted with a red box), and 'vc2' with 2 volumes. The 'NAME' column is sorted in descending order.

NAME	VOLUMES	CLOUD ST...	BANDWID...	STORAGE...
VC1	9	NA	0	portalintegrati... ...
myssvolcontainer1	0	NA	0	localizetest ...
vc2	2	NA	0	portalintegrati... ...

Modify a volume container

Perform the following steps to modify a volume container.

Note

You cannot modify the encryption settings and the storage account credentials associated with a volume container after it is created.

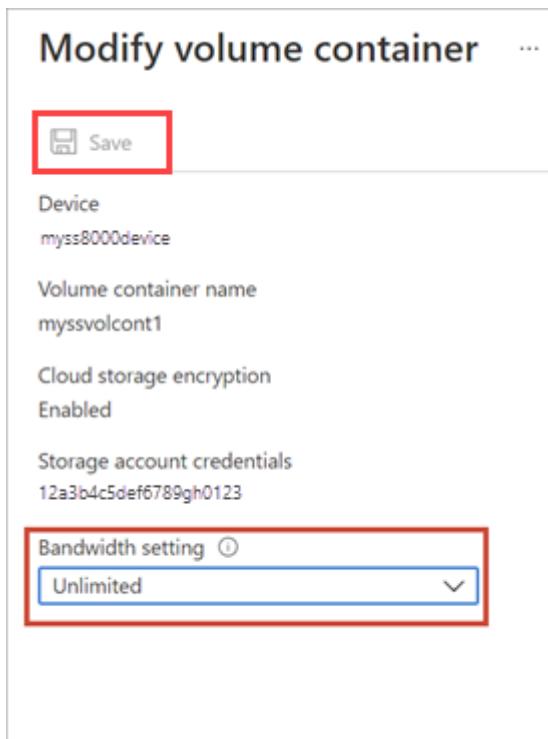
To modify a volume container

1. Go to your StorSimple Device Manager service, and then navigate to **Management** > **Volume containers**.
2. From the tabular list of volume containers, select the volume container you want to modify. On the **Devices** page, select the device, double-click it, and then click the **Volume containers** tab.
3. In the tabular listing of the volume containers, select the volume container that you want to modify. In the blade that opens up, click **Modify** from the command bar.

The screenshot shows two side-by-side blades. The left blade is titled 'Volume container' and lists three volume containers: 'myssvc1', 'myssvolcont2', and 'myvolcont3'. The right blade is titled 'myssvc1' and shows its details: Storage account 'myss8000storageacct', Bandwidth setting 'Unlimited', and Encryption 'Enabled'. A red box highlights the 'Modify' button in the top right corner of the right blade.

4. In the **Modify volume container** blade, do the following steps:

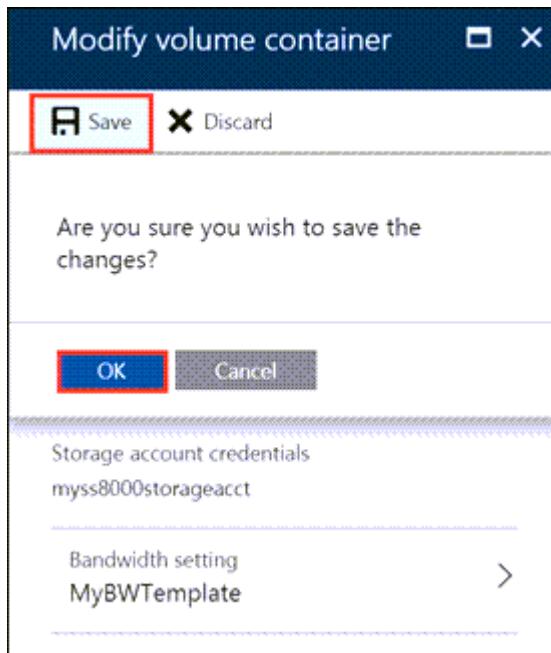
- The name, encryption key, and storage account associated with the volume container cannot be changed after they are specified. Change the associated bandwidth setting.



- Click **OK**.

5. In the next page of the **Modify Volume Container** dialog box:

- From the drop-down list, choose an existing bandwidth template.
- Review the schedule settings for the specified bandwidth template.
- Click **Save** and confirm the changes.



The **Volume containers** blade is updated to reflect the changes.

Delete a volume container

A volume container has volumes within it. It can be deleted only if all the volumes contained in it are first deleted. Perform the following steps to delete a volume container.

To delete a volume container, you must

- delete volumes in the volume container. If the volume container has associated volumes, take those volumes offline first. Follow the steps in [Take a volume offline](#). After the volumes are offline, you can delete them.
- delete associated backup policies and cloud snapshots. Check if the volume container has associated backup policies and cloud snapshots. If so, then [delete the backup policies](#). This will also delete the cloud snapshots.

When the volume container has no associated volumes, backup policies, and cloud snapshots, you can delete it. Perform the following procedure to delete a volume container.

To delete a volume container

1. Go to your StorSimple Device Manager service and click **Devices**. Select and click the device and then go to **Settings > Manage > Volume containers**.

The screenshot shows two windows side-by-side. The left window is titled 'TaalaFriendlyNameG1' and displays monitoring information. It includes a summary of alerts (4 total, 3 Critical, 1 Warning), a list of volumes (1 Online), and a usage chart for the past 24 hours. The right window is titled 'Settings' and lists various management options. The 'Volume container' option is highlighted with a red box.

TaalaFriendlyNameG1

PortalIntegration2812

+ Add volume container + Add volume Fail over device Deactivate Delete

Essentials ^

Status Online Model 100
Activation Date Device software version
Thu Jan 05 2017 00:52:29 GMT-0600 (Pacific) TaalaFriendlyNameG1 (6.3.9600.17566)

All settings →

Monitoring

Alerts - Past 7 days Volumes

4 ! 1

Critical 3 Online 1

Warning 1

TaalaFriendlyNameG1 - Usage - Past 24 hours Edit

12 PM 6 PM Jan 11 6 AM

PRIMARY TIERED STOR... PRIMARY LOCALLY PINN... CLOUD STORAGE USED

- Bytes - Bytes - Bytes

Capacity PROVISIONED 1 GB
REMAINING 1023 GB Tiered OR 0 Bytes Local

Settings

Filter settings

GENERAL Properties

MONITOR Capacity Usage Performance Jobs Alerts

MANAGE Volumes Volume container > Backup policy Backup catalog

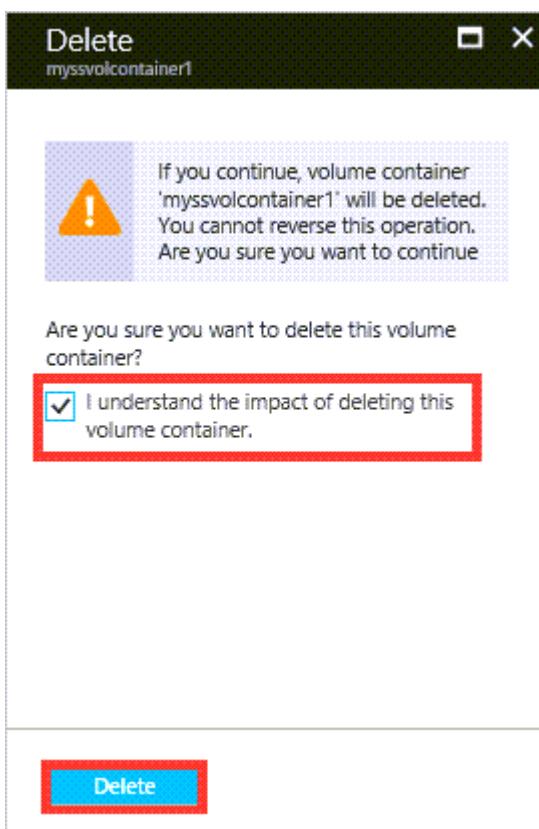
DEVICE SETTINGS General Network Security

- From the tabular list of volume containers, select the volume container you want to delete, right click ... and then select **Delete**.

The screenshot shows the 'Volume container' list screen. On the left, there's a navigation sidebar with sections like GENERAL, MONITOR, and MANAGE. Under MANAGE, 'Volume container' is selected and highlighted in blue. The main area displays a table of volume containers. The first row, 'myssvolcontainer1', is also highlighted in blue. To the right of the table, there are buttons for 'Pin to dashboard' and 'Delete'. A red box highlights the 'Delete' button.

NAME	VOLUMES	CLOUD ST...	BANDWID...	STORAGE...
VC1	9	NA	0	portalintegrati...
myssvolcontainer1	0	NA	0	localizedtest
vc2	2	NA	0	portalintegrati...

3. If a volume container has no associated volumes, backup policies, and cloud snapshots, then it can be deleted. When prompted for confirmation, review and select the checkbox stating the impact of deleting the volume container. Click **Delete** to then delete the volume container.



The list of volume containers is updated to reflect the deleted volume container.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and contains a navigation menu with sections for GENERAL, MONITOR, and MANAGE. Under MANAGE, 'Volume container' is selected and highlighted with a blue background. The right window is titled 'Volume container SudasDevice1' and displays a table of volume containers. The table has columns for NAME, VOLUMES, CLOUD ST..., BANDWID..., and STORAGE... . There are two entries: 'VC1' with 9 volumes and 'vc2' with 2 volumes. Both entries have 'NA' in the CLOUD ST... column and '0' in the BANDWID... and STORAGE... columns. A 'portalintegrati...' string is visible at the end of the first row.

NAME	VOLUMES	CLOUD ST...	BANDWID...	STORAGE...
VC1	9	NA	0	portalintegrati... ...
vc2	2	NA	0	portalintegrati... ...

Next steps

- Learn more about [managing StorSimple volumes](#).
- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to manage volumes (Update 3 or later)

Article • 08/19/2022 • 16 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to use the StorSimple Device Manager service to create and manage volumes on the StorSimple 8000 series devices running Update 3 and later.

The StorSimple Device Manager service is an extension in the Azure portal that lets you manage your StorSimple solution from a single web interface. Use the Azure portal to manage volumes on all your devices. You can also create and manage StorSimple services, manage devices, backup policies, and backup catalog, and view alerts.

Volume types

StorSimple volumes can be:

- **Locally pinned volumes:** Data in these volumes remains on the local StorSimple device at all times.
- **Tiered volumes:** Data in these volumes can spill to the cloud.

An archival volume is a type of tiered volume. The larger deduplication chunk size used for archival volumes allows the device to transfer larger segments of data to the cloud.

If necessary, you can change the volume type from local to tiered or from tiered to local. For more information, go to [Change the volume type](#).

Locally pinned volumes

Locally pinned volumes are fully provisioned volumes that do not tier data to the cloud, thereby ensuring local guarantees for primary data, independent of cloud connectivity. Data on locally pinned volumes is not deduplicated and compressed; however, snapshots of locally pinned volumes are deduplicated.

Locally pinned volumes are fully provisioned; therefore, you must have sufficient space on your device when you create them. You can provision locally pinned volumes up to a maximum size of 8 TB on the StorSimple 8100 device and 20 TB on the 8600 device. StorSimple reserves the remaining local space on the device for snapshots, metadata, and data processing. You can increase the size of a locally pinned volume to the maximum space available, but you cannot decrease the size of a volume once created.

When you create a locally pinned volume, the available space for creation of tiered volumes is reduced. The reverse is also true: if you have existing tiered volumes, the space available for creating locally pinned volumes will be lower than the maximum limits stated above. For more information on local volumes, refer to the [frequently asked questions on locally pinned volumes](#).

Tiered volumes

Tiered volumes are thinly provisioned volumes in which the frequently accessed data stays local on the device and less frequently used data is automatically tiered to the cloud. Thin provisioning is a virtualization technology in which available storage appears to exceed physical resources. Instead of reserving sufficient storage in advance, StorSimple uses thin provisioning to allocate just enough space to meet current requirements. The elastic nature of cloud storage facilitates this approach because StorSimple can increase or decrease cloud storage to meet changing demands.

If you are using the tiered volume for archival data, select the **Use this volume for less frequently accessed archival data** check box to change the deduplication chunk size for your volume to 512 KB. If you do not select this option, the corresponding tiered volume will use a chunk size of 64 KB. A larger deduplication chunk size allows the device to expedite the transfer of large archival data to the cloud.

Provisioned capacity

Refer to the following table for maximum provisioned capacity for each device and volume type. (Note that locally pinned volumes are not available on a virtual device.)

Type	Maximum tiered volume size	Maximum locally pinned volume size
Physical devices		
8100	64 TB	8 TB
8600	64 TB	20 TB
Virtual devices		
8010	30 TB	N/A
8020	64 TB	N/A

The volumes blade

The **Volumes** blade allows you to manage the storage volumes that are provisioned on the Microsoft Azure StorSimple device for your initiators (servers). It displays the list of volumes on the StorSimple devices connected to your service.

NAME	STATUS	TYPE	CAPACITY
myssvolcont1 (2)			
Clonedmyssfsvol1	Online	Tiered	500 GB
myssfsvol1	Online	Tiered	500 GB
myssvolcont2 (2)			
myssvolarch1	Online	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB

A volume consists of a series of attributes:

- **Volume Name** – A descriptive name that must be unique and helps identify the volume. This name is also used in monitoring reports when you filter on a specific volume. Once the volume is created, it cannot be renamed.
- **Status** – Can be online or offline. If a volume is offline, it is not visible to initiators (servers) that are allowed access to use the volume.
- **Capacity** – specifies the total amount of data that can be stored by the initiator (server). Locally-pinned volumes are fully provisioned and reside on the StorSimple device. Tiered volumes are thinly provisioned and the data is deduplicated. With

thinly provisioned volumes, your device doesn't pre-allocate physical storage capacity internally or on the cloud according to configured volume capacity. The volume capacity is allocated and consumed on demand.

- **Type** – Indicates whether the volume is **Tiered** (the default) or **Locally pinned**.

Use the instructions in this tutorial to perform the following tasks:

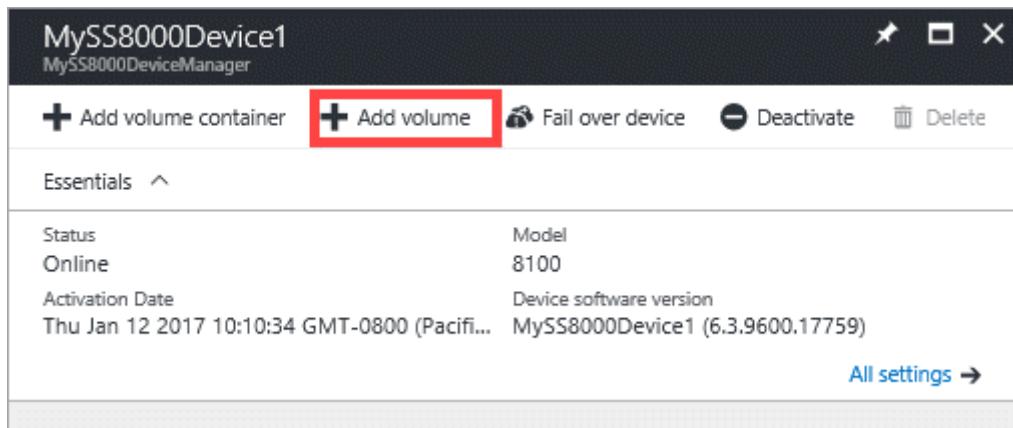
- Add a volume
- Modify a volume
- Change the volume type
- Delete a volume
- Take a volume offline
- Monitor a volume

Add a volume

You [created a volume](#) during deployment of your StorSimple 8000 series device. Adding a volume is a similar procedure.

To add a volume

1. From the tabular listing of the devices in the **Devices** blade, select your device. Click **+ Add volume**.



2. In the **Add a volume** blade:
 - a. The **Select device** field is automatically populated with your current device.
 - b. From the drop-down list, select the volume container where you need to add a volume.
 - c. Type a **Name** for your volume. Once the volume is created, you cannot rename the volume.

d. On the drop-down list, select the **Type** for your volume. For workloads that require local guarantees, low latencies, and higher performance, select a **Locally pinned** volume. For all other data, select a **Tiered** volume. If you are using this volume for archival data, check **Use this volume for less frequently accessed archival data**.

A tiered volume is thinly provisioned and can be created quickly. Selecting **Use this volume for less frequently accessed archival data** for tiered volume targeted for archival data changes the deduplication chunk size for your volume to 512 KB. If this field is not checked, the corresponding tiered volume uses a chunk size of 64 KB. A larger deduplication chunk size allows the device to expedite the transfer of large archival data to the cloud.

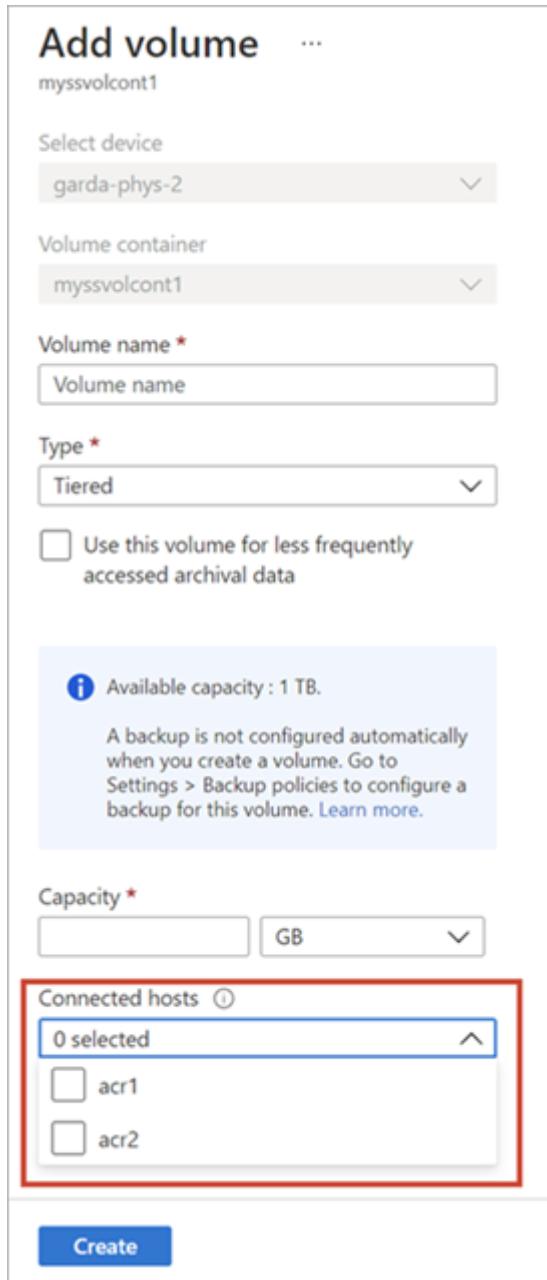
A locally pinned volume is thickly provisioned and ensures that the primary data on the volume stays local to the device and does not spill to the cloud. If you create a locally pinned volume, the device checks for available space on the local tiers to provision the volume of the requested size. The operation of creating a locally pinned volume may involve spilling existing data from the device to the cloud and the time taken to create the volume may be long. The total time depends on the size of the provisioned volume, available network bandwidth, and the data on your device.

e. Specify the **Provisioned Capacity** for your volume. Make a note of the capacity that is available based on the volume type selected. The specified volume size must not exceed the available space.

You can provision locally pinned volumes up to 8.5 TB or tiered volumes up to 200 TB on the 8100 device. On the larger 8600 device, you can provision locally pinned volumes up to 22.5 TB or tiered volumes up to 500 TB. As local space on the device is required to host the working set of tiered volumes, creation of locally pinned volumes impacts the space available for provisioning tiered volumes. Therefore, if you create a locally pinned volume, space available for creation of tiered volumes is reduced. Similarly, if a tiered volume is created, the available space for creation of locally pinned volumes is reduced.

If you provision a locally pinned volume of 8.5 TB (maximum allowable size) on your 8100 device, then you have exhausted all the local space available on the device. You can't create any tiered volume from that point onwards as there is no local space on the device to host the working set of the tiered volume. Existing tiered volumes also affect the space available. For example, if you have an 8100 device that already has tiered volumes of roughly 106 TB, only 4 TB of space is available for locally pinned volumes.

f. In the **Connected hosts** field, click the arrow, and then select each ACR you want to connect. In the **Connected hosts** blade, choose an existing ACR or add a new ACR. If you choose a new ACR, then supply a **Name** for your ACR, provide the **iSCSI Qualified Name (IQN)** of your Windows host. If you don't have the IQN, go to Get the IQN of a Windows Server host.



g. When you finish your settings, click **Create**.

A volume is created with the specified settings. Your new volume is ready to use.

① Note

If you create a locally pinned volume and then create another locally pinned volume immediately afterwards, the volume creation jobs run sequentially. The first volume creation job must finish before the next volume creation job can begin.

Modify a volume

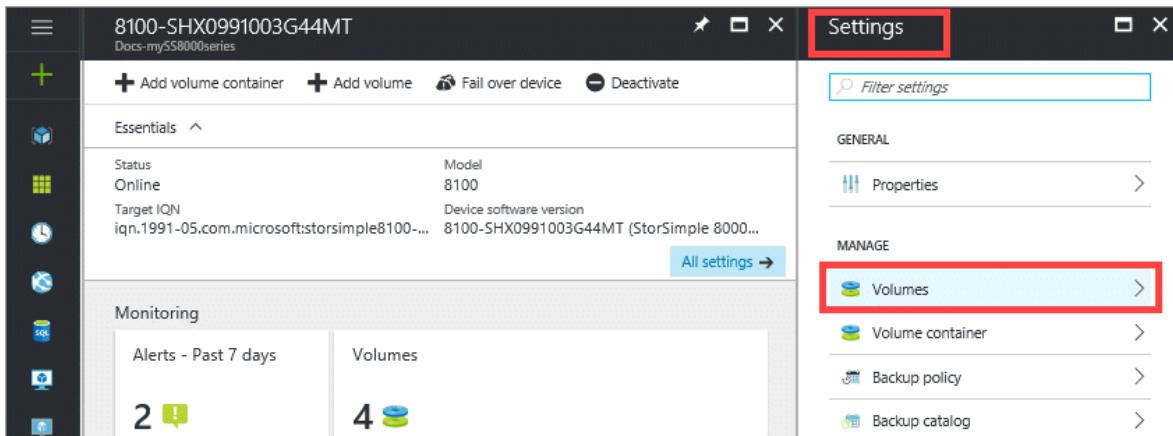
Modify a volume when you need to expand it or change the hosts that access the volume.

ⓘ Important

- If you modify the volume size on the device, the volume size needs to be changed on the host as well.
- The host-side steps described here are for Windows Server 2012 (2012R2). Procedures for Linux or other host operating systems will be different. Refer to your host operating system instructions when modifying the volume on a host running another operating system.

To modify a volume

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of the devices, select the device that has the volume that you intend to modify. Click **Settings > Volumes**.



2. From the tabular listing of volumes, select the volume and right-click to invoke the context menu. Select **Take offline** to take the volume you will modify offline.

The screenshot shows the StorSimple Volumes interface. A context menu is open over a volume named "myssvolarch1". The menu options are: Pin to dashboard, Modify, Take offline (which is highlighted with a red box), Bring online, and Delete.

NAME	STATUS	TYPE	CAPACITY
myssfsvol1	Online	Tiered	500 GB
myssvolts2	Online	Locally pinned	200 GB
myssvolcont1 (2)			
myssvolarch1	Online	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB
myssvolcont2 (2)			

3. In the **Take offline** blade, review the impact of taking the volume offline and select the corresponding checkbox. Ensure that the corresponding volume on the host is offline first. For information on how to take a volume offline on your host server connected to StorSimple, refer to operating system specific instructions. Click **Take offline**.

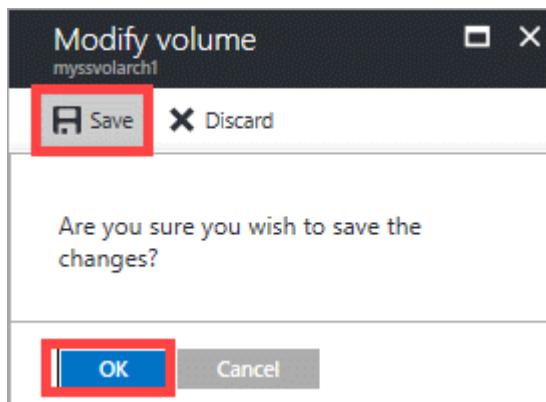


4. After the volume is offline (as shown by the volume status), select the volume and right-click to invoke the context menu. Select **Modify volume**.

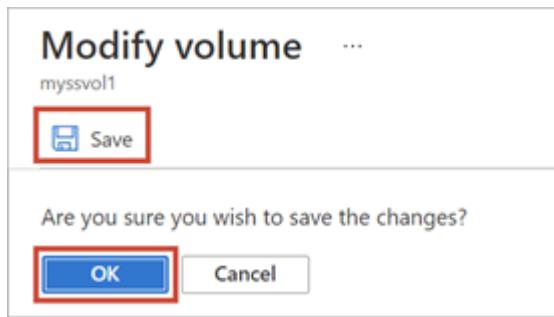
NAME	STATUS	TYPE	CAPACITY
myssfsvol1	Online	Tiered	500 GB
myssvols2	Online	Locally pinned	200 GB
myssvolarch1	Offline	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB

5. In the **Modify volume** blade, you can make the following changes:

- The volume **Name** cannot be edited.
- Convert the **Type** from locally pinned to tiered or from tiered to locally pinned (see [Change the volume type](#) for more information).
- Increase the **Provisioned Capacity**. The **Provisioned Capacity** can only be increased. You cannot shrink a volume after it is created.
- Under **Connected hosts**, you can modify the ACR. To modify an ACR, the volume must be offline.



6. Click **Save** to save your changes. When prompted for confirmation, click **Yes**. The Azure portal will display an updating volume message. It will display a success message when the volume has been successfully updated.



7. If you are expanding a volume, complete the following steps on your Windows host computer:
 - a. Go to **Computer Management** ->**Disk Management**.
 - b. Right-click **Disk Management** and select **Rescan Disks**.
 - c. In the list of disks, select the volume that you updated, right-click, and then select **Extend Volume**. The Extend Volume wizard starts. Click **Next**.
 - d. Complete the wizard, accepting the default values. After the wizard is finished, the volume should show the increased size.

① Note

- Expansion of a volume typically takes about 30 minutes.
- If you expand a locally pinned volume and then expand another locally pinned volume immediately afterwards, the volume expansion jobs run sequentially. The first volume expansion job must finish before the next volume expansion job can begin.

Change the volume type

You can change the volume type from tiered to locally pinned or from locally pinned to tiered. However, this conversion should not be a frequent occurrence.

Tiered to local volume conversion considerations

Some reasons for converting a volume from tiered to locally pinned are:

- Local guarantees regarding data availability and performance
- Elimination of cloud latencies and cloud connectivity issues.

Typically, these are small existing volumes that you want to access frequently. A locally pinned volume is fully provisioned when it is created.

If you are converting a tiered volume to a locally pinned volume, StorSimple verifies that you have sufficient space on your device before it starts the conversion. If you have insufficient space, you will receive an error and the operation will be canceled.

Note

Before you begin a conversion from tiered to locally pinned, make sure that you consider the space requirements of your other workloads.

Conversion from a tiered to a locally pinned volume can adversely affect device performance. Additionally, the following factors might increase the time it takes to complete the conversion:

- There is insufficient bandwidth.
- There is no current backup.

To minimize the effects that these factors may have:

- Review your bandwidth throttling policies and make sure that a dedicated 40 Mbps bandwidth is available.
- Schedule the conversion for off-peak hours.
- Take a cloud snapshot before you start the conversion.

If you are converting multiple volumes (supporting different workloads), then you should prioritize the volume conversion so that higher priority volumes are converted first. For example, you should convert volumes that host virtual machines (VMs) or volumes with SQL workloads before you convert volumes with file share workloads.

Local to tiered volume conversion considerations

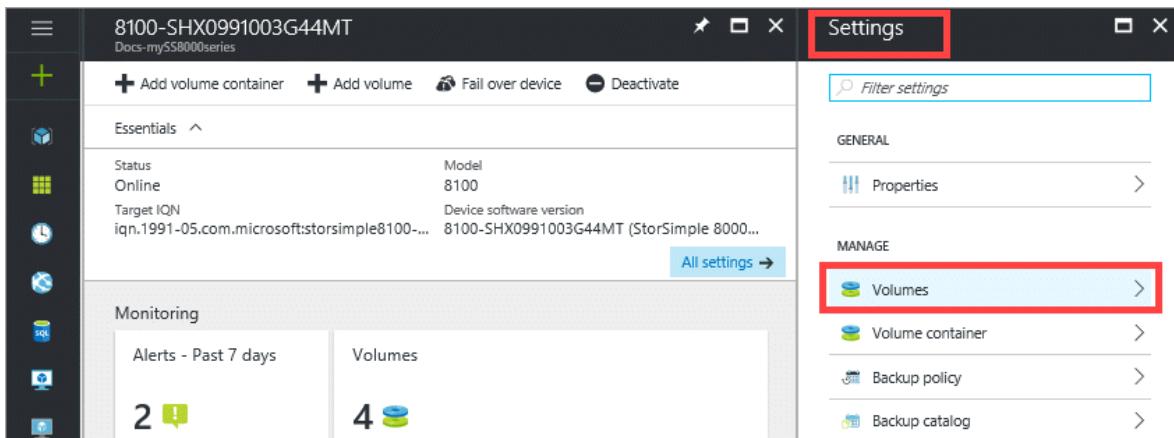
You may want to change a locally pinned volume to a tiered volume if you need additional space to provision other volumes. When you convert the locally pinned volume to tiered, the available capacity on the device increases by the size of the released capacity. If connectivity issues prevent the conversion of a volume from the local type to the tiered type, the local volume will exhibit properties of a tiered volume until the conversion is complete. This is because some data might have spilled to the cloud. This spilled data continues to occupy local space on the device that cannot be freed until the operation is restarted and completed.

Note

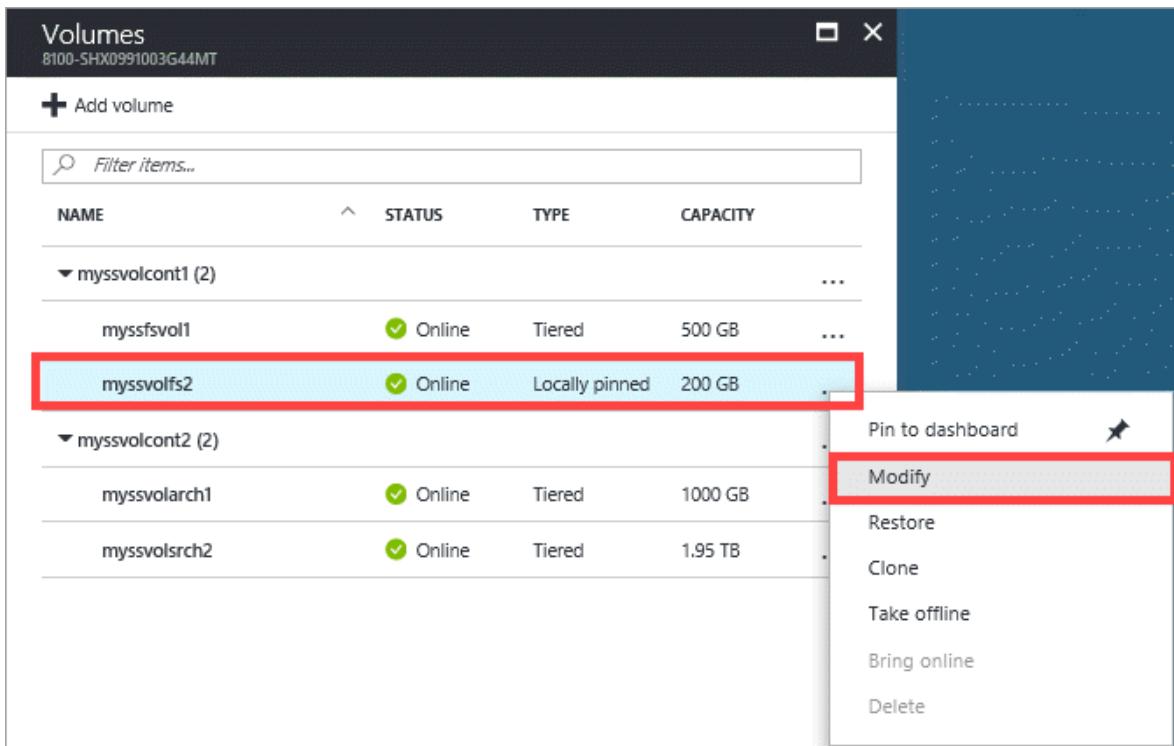
Converting a volume can take some time and you cannot cancel a conversion after it starts. The volume remains online during the conversion, and you can take backups, but you cannot expand or restore the volume while the conversion is taking place.

To change the volume type

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of the devices, select the device that has the volume that you intend to modify. Click **Settings > Volumes**.

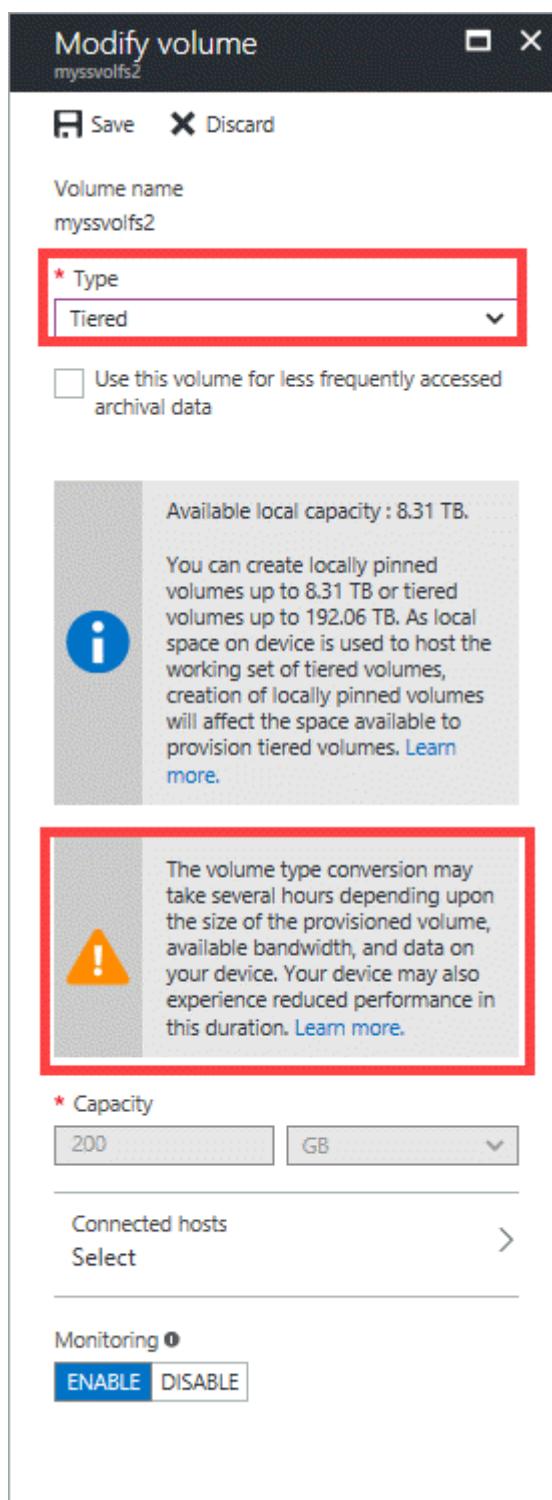


2. From the tabular listing of volumes, select the volume and right-click to invoke the context menu. Select **Modify**.

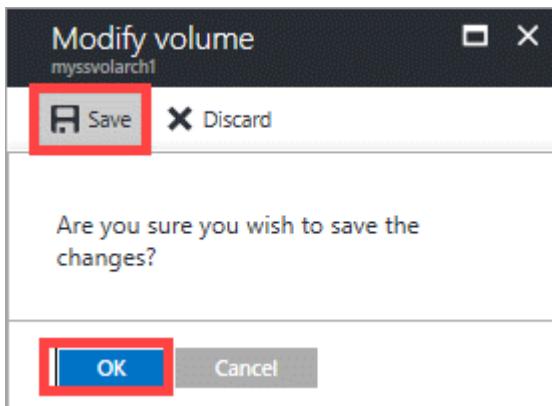


3. On the **Modify volume** blade, change the volume type by selecting the new type from the Type drop-down list.

- If you are changing the type to **Locally pinned**, StorSimple will check to see if there is sufficient capacity.
- If you are changing the type to **Tiered** and this volume will be used for archival data, select the **Use this volume for less frequently accessed archival data** check box.
- If you are configuring a locally pinned volume as tiered or *vice-versa*, the following message appears.



4. Click **Save** to save the changes. When prompted for confirmation, click **Yes** to start the conversion process.



5. The Azure portal displays a notification for the job creation that would update the volume. Click on the notification to monitor the status of the volume conversion job.

The screenshot shows a 'Modify volume' dialog box with the title 'Job'. It contains the following information:

Details	
Status	In progress (5%)
Entity	myssvols2 (Microsoft.StorSimple/managers/devices/volumeContainers/volumes)
Device	8100-SHX0991003G44MT
Started on	1/31/2017 11:10:47
Completed on	-
Duration	57 Seconds

Tasks

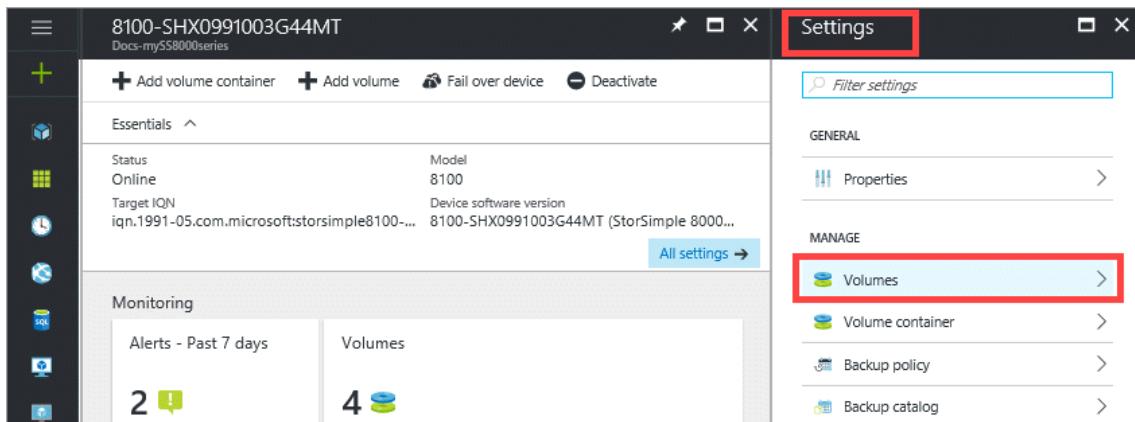
NAME	STATUS
Preparation to modify volume completed	✓ Succeeded
ACR creation not required	✓ Succeeded

Take a volume offline

You may need to take a volume offline when you are planning to modify or delete the volume. When a volume is offline, it is not available for read-write access. You must take the volume offline on the host and the device.

To take a volume offline

1. Make sure that the volume in question is not in use before taking it offline.
2. Take the volume offline on the host first. This eliminates any potential risk of data corruption on the volume. For specific steps, refer to the instructions for your host operating system.
3. After the host is offline, take the volume on the device offline by performing the following steps:
 - a. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of the devices, select the device that has the volume that you intend to modify. Click **Settings > Volumes**.

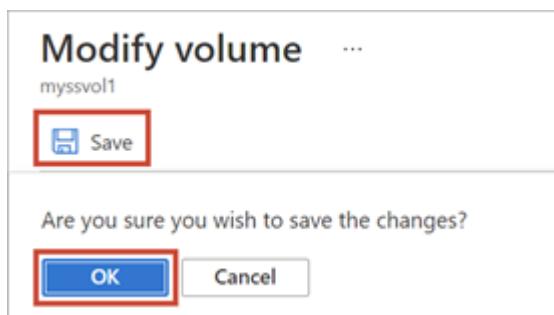


- b. From the tabular listing of volumes, select the volume and right-click to invoke the context menu. Select **Take offline** to take the volume you will modify offline.

The screenshot shows the Volumes interface with two volume groups: myssvolcont1 and myssvolcont2. In myssvolcont2, the volume myssvolarch1 is selected and highlighted with a red box. A context menu is open over this volume, listing options: Pin to dashboard, Modify, Take offline (which is also highlighted with a red box), Bring online, and Delete.

NAME	STATUS	TYPE	CAPACITY
myssfsvol1	Online	Tiered	500 GB
myssvolfs2	Online	Locally pinned	200 GB
myssvolarch1	Online	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB

4. In the **Take offline** blade, review the impact of taking the volume offline and select the corresponding checkbox. Click **Take offline**.



You are notified when the volume is offline. The volume status also updates to Offline.

5. After a volume is offline, if you select the volume and right-click, **Bring Online** option becomes available in the context menu.

① Note

The **Take Offline** command sends a request to the device to take the volume offline. If hosts are still using the volume, this results in broken connections, but taking the volume offline will not fail.

Delete a volume

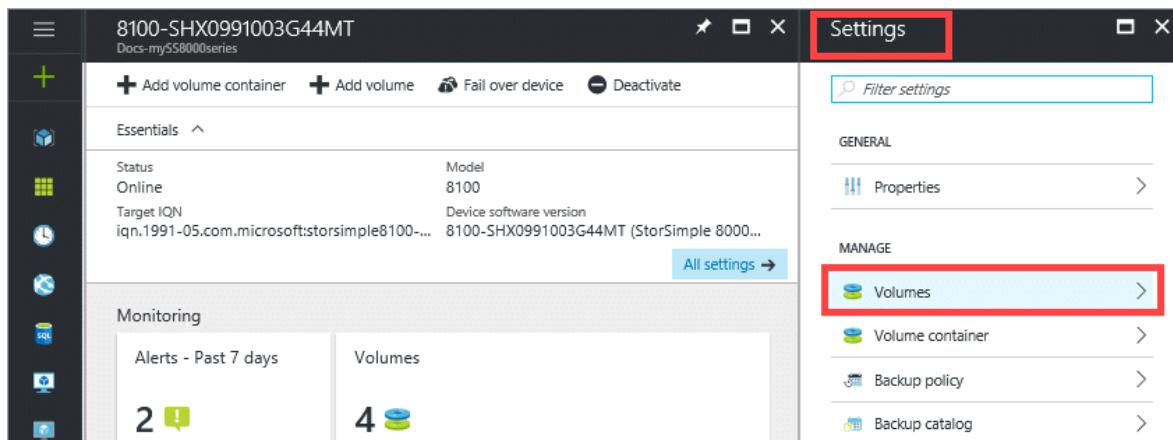
ⓘ Important

You can delete a volume only if it is offline.

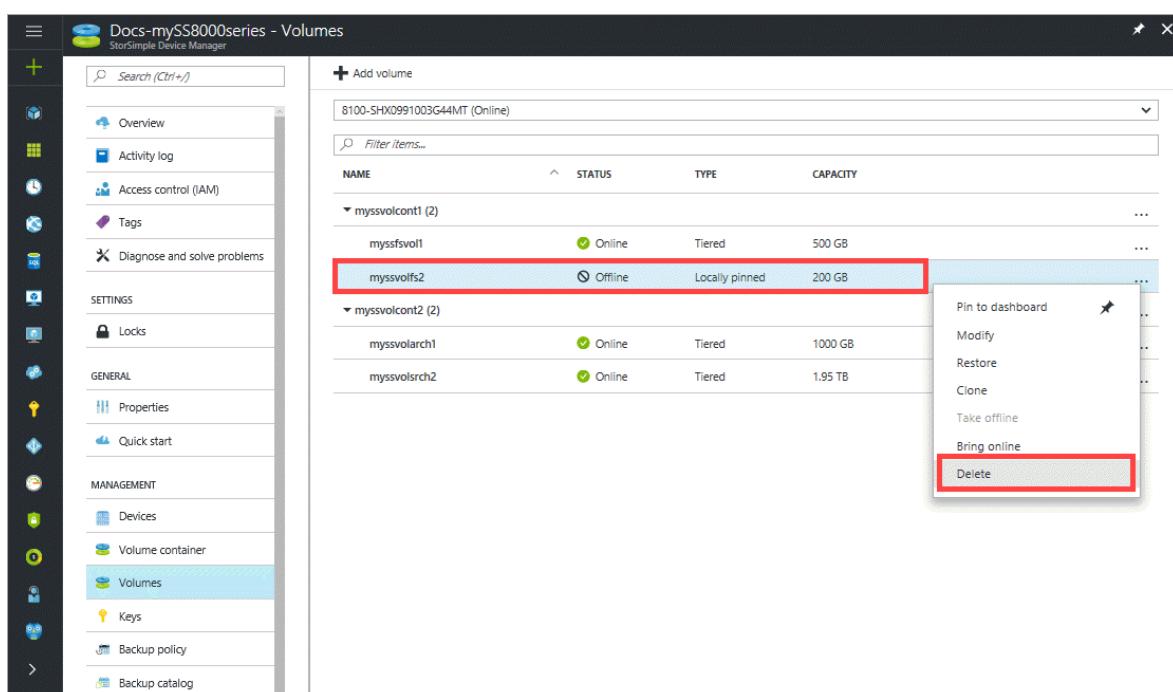
Complete the following steps to delete a volume.

To delete a volume

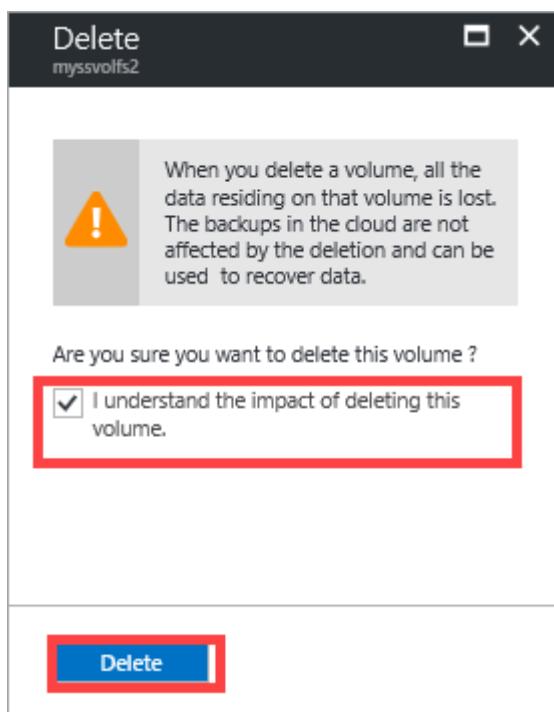
1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of the devices, select the device that has the volume that you intend to modify. Click **Settings > Volumes**.



2. Check the status of the volume you want to delete. If the volume you want to delete is not offline, take it offline first. Follow the steps in [Take a volume offline](#).
3. After the volume is offline, select the volume, right-click to invoke the context menu and then select **Delete**.



4. In the **Delete** blade, review and select the checkbox against the impact of deleting a volume. When you delete a volume, all the data that resides on the volume is lost.



5. After the volume is deleted, the tabular list of volumes updates to indicate the deletion.

The screenshot shows the 'Docs-mySS8000series - Volumes' page in the StorSimple Device Manager. The left sidebar has a 'VOLUMES' section with a red box around it. The main area displays a table of volumes:

NAME	STATUS	TYPE	CAPACITY
mysssvol1	Online	Tiered	500 GB
myssvolcont1 (1)			
myssvolcont2 (2)			
myssvolarch1	Online	Tiered	1000 GB
myssvolsrch2	Online	Tiered	1.95 TB

⚠ Note

If you delete a locally pinned volume, the space available for new volumes may not be updated immediately. The StorSimple Device Manager Service

updates the local space available periodically. We suggest you wait for a few minutes before you try to create the new volume.

Additionally, if you delete a locally pinned volume and then delete another locally pinned volume immediately afterwards, the volume deletion jobs run sequentially. The first volume deletion job must finish before the next volume deletion job can begin.

Monitor a volume

Volume monitoring allows you to collect I/O-related statistics for a volume. Monitoring is enabled by default for the first 32 volumes that you create. Monitoring of additional volumes is disabled by default.

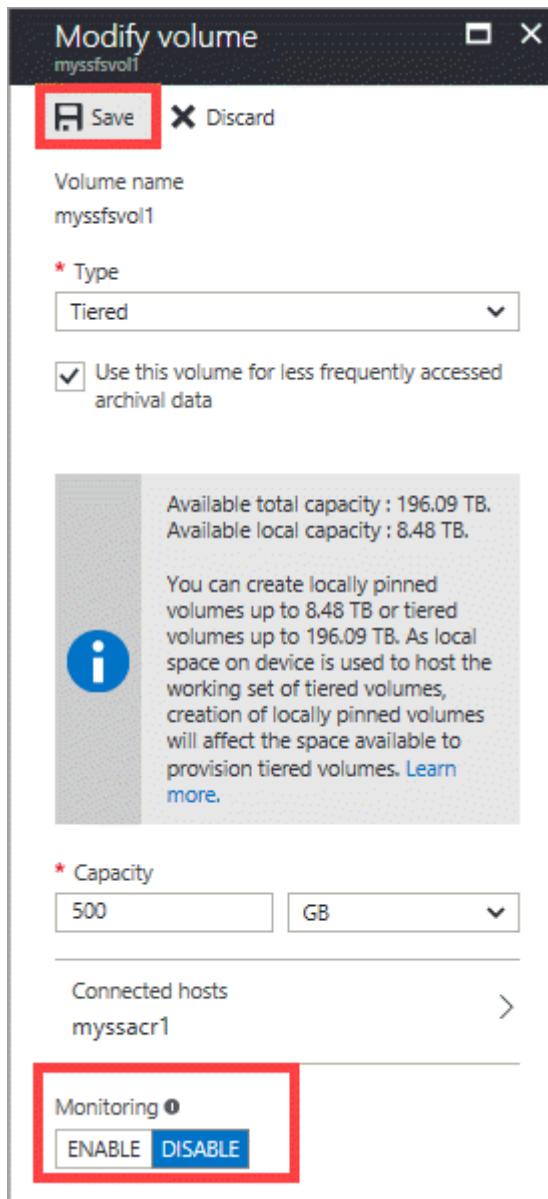
 **Note**

Monitoring of cloned volumes is disabled by default.

Perform the following steps to enable or disable monitoring for a volume.

To enable or disable volume monitoring

1. Go to your StorSimple Device Manager service and then click **Devices**. From the tabular listing of the devices, select the device that has the volume that you intend to modify. Click **Settings > Volumes**.
2. From the tabular listing of volumes, select the volume and right-click to invoke the context menu. Select **Modify**.
3. In the **Modify volume** blade, for **Monitoring** select **Enable** or **Disable** to enable or disable monitoring.



4. Click **Save** and when prompted for confirmation, click **Yes**. The Azure portal displays a notification for updating the volume and then a success message, after the volume is successfully updated.

Next steps

- Learn how to [clone a StorSimple volume](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

StorSimple locally pinned volumes: frequently asked questions (FAQ)

FAQ

Overview

Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The following are questions and answers that you might have when you create a StorSimple locally pinned volume, convert a tiered volume to a locally pinned volume (and vice versa), or back up and restore a locally pinned volume.

Questions and answers are arranged into the following categories

- Creating a locally pinned volume
- Backing up a locally pinned
- Converting a tiered volume to a locally pinned volume
- Restoring a locally pinned volume
- Failing over a locally pinned volume

Questions about creating a locally pinned volume

What is the maximum size of a locally pinned volume that I can create on the 8000 series devices?

On devices running StorSimple 8000 Series Update 3.0, you can provision locally pinned volumes up to 8.5 TB or tiered volumes up to 200 TB on the 8100 device. On the larger 8600 device, you can provision locally pinned volumes up to 22.5 TB or tiered volumes up to 500 TB.

I recently upgraded my 8100 device to Update 3.0 and when I try to create a locally pinned volume, the maximum available size is only 6 TB and not 8.5 TB. Why can't I create an 8.5 TB volume?

If your device is running update 3.0, you can provision locally pinned volumes up to 8.5 TB OR tiered volumes up to 200 TB on the 8100 device. If your device already has tiered volumes, then the space available for creating a locally pinned volume will be proportionally lower than this maximum limit. For example, if approximately 106 TB of tiered volumes have already been provisioned on your 8100 device (which is half of the tiered capacity), then the maximum size of a local volume that you can create on the 8100 device will be correspondingly reduced to 4 TB (roughly half of the maximum locally pinned volume capacity).

Because some local space on the device is used to host the working set of tiered volumes, the available space for creating a locally pinned volume is reduced if the device has tiered volumes. Conversely, creating a locally pinned volume proportionally reduces the available space for tiered volumes. The following tables summarizes the available tiered capacity on the 8100 and 8600 devices when locally pinned volumes are created.

Update 3.0

Locally pinned volumes provisioned capacity	Available capacity to be provisioned for tiered volumes - 8100	Available capacity to be provisioned for tiered volumes - 8600
0	200 TB	500 TB
1 TB	176.5 TB	477.8 TB

Locally pinned volumes provisioned capacity	Available capacity to be provisioned for tiered volumes - 8100	Available capacity to be provisioned for tiered volumes - 8600
4 TB	105.9 TB	411.1 TB
8.5 TB	0 TB	311.1 TB
10 TB	NA	277.8 TB
15 TB	NA	166.7 TB
22.5 TB	NA	0 TB

Why is locally pinned volume creation a long running operation?

Locally pinned volumes are thickly provisioned. To create space on the local tiers of the device, some data from existing tiered volumes might be pushed to the cloud during the provisioning process. And since this depends upon the size of the volume being provisioned, the existing data on your device and the available bandwidth to the cloud, the time taken to create a local volume may be several hours.

How long does it take to create a locally pinned volume?

Because locally pinned volumes are thickly provisioned, some existing data from tiered volumes might be pushed to the cloud during the provisioning process. Therefore, the time taken to create a locally pinned volume depends upon multiple factors, including the size of the volume, the data on your device and the available bandwidth. On a freshly installed device that has no volumes, the time to create a locally pinned volume is about 10 minutes per terabyte of data. However, creation of local volumes may take several hours based on the factors explained above on a device that is in use.

I want to create a locally pinned volume. Are there any best practices I need to be aware of?

Locally pinned volumes are suitable for workloads that require local guarantees of data at all times and are sensitive to cloud latencies. While considering usage of local volumes for any of your workloads, please be aware of the following:

- Locally pinned volumes are thickly provisioned, and creating local volumes impacts the available space for tiered volumes. Therefore, we suggest you start with smaller-sized volumes and scale up as your storage requirement increases.
- Provisioning of local volumes is a long running operation that might involve pushing existing data from tiered volumes to the cloud. As a result, you may experience reduced performance on these volumes.
- Provisioning of local volumes is a time consuming operation. The actual time involved depends on multiple factors: the size of the volume being provisioned, data on your device, and available bandwidth. If you have not backed up your existing volumes to the cloud, then volume creation is slower. We suggest you take cloud snapshots of your existing volumes before you provision a local volume.
- You can convert existing tiered volumes to locally pinned volumes, and this conversion involves provisioning of space on the device for the resulting locally pinned volume (in addition to bringing down tiered data, if any, from the cloud). Again, this is a long running operation that depends on factors we've discussed above. We suggest that you back up your existing volumes prior to conversion as the process will be even slower if existing volumes are not backed up. Your device might also experience reduced performance during this process.

More information on how to [create a locally pinned volume](#)

Can I create multiple locally pinned volumes at the same time?

Yes, but any locally pinned volume creation and expansion jobs are processed sequentially.

Locally pinned volumes are thickly provisioned and this requires creation of local space on the device (which might result in existing data from tiered volumes to be pushed to the cloud during the provisioning process). Therefore, if a provisioning job is in progress, other local volume creation jobs will be queued until that job is finished.

Similarly, if an existing local volume is being expanded or a tiered volume is being converted to a locally pinned volume, then the creation of a new locally pinned volume is queued until the previous job is completed. Expanding the size of a locally pinned volume involves the expansion of the existing local space for that volume. Conversion from a tiered to locally pinned volume also involves the creation of local space for the

resulting locally pinned volume. In both of these operations, creation or expansion of local space is a long running job.

You can view these jobs in the **Jobs** blade of the StorSimple Device Manager service. The job that is actively being processed is continually updated to reflect the progress of space provisioning. The remaining locally pinned volume jobs are marked as running, but their progress is stalled and they are picked in the order they were queued.

I deleted a locally pinned volume. Why don't I see the reclaimed space reflected in the available space when I try to create a new volume?

If you delete a locally pinned volume, the space available for new volumes may not be updated immediately. The StorSimple Device Manager Service updates the local space available approximately every hour. We suggest you wait for an hour before you try to create the new volume.

Are locally pinned volumes supported on the cloud appliance?

Locally pinned volumes are not supported on the cloud appliance (8010 and 8020 devices formerly referred to as the StorSimple virtual device).

Can I use the Azure PowerShell cmdlets to create and manage locally pinned volumes?

No, you cannot create locally pinned volumes via Azure PowerShell cmdlets (any volume you create via Azure PowerShell is tiered). We also suggest that you do not use the Azure PowerShell cmdlets to modify any properties of a locally pinned volume, as it will have the undesired effect of modifying the volume type to tiered.

Questions about backing up a locally pinned volume

Are local snapshots of locally pinned volumes supported?

Yes, you can take local snapshots of your locally pinned volumes. However, we strongly suggest that you regularly back up your locally pinned volumes with cloud snapshots to ensure that your data is protected in the eventuality of a disaster.

Do note that local snapshots of locally pinned volumes can also tier out to the cloud and are not guaranteed to stay in the local tier of the device.

Are there any guidelines for managing local snapshots for locally pinned volumes?

Frequent local snapshots alongside a high rate of data churn in the locally pinned volume might cause local space on the device to be consumed quickly and result in data from tiered volumes being pushed to the cloud. We therefore suggest you minimize the number of local snapshots.

I received an alert stating that my local snapshots of locally pinned volumes might be invalidated. When can this happen?

Frequent local snapshots alongside a high rate of data churn in the locally pinned volume might cause local space on the device to be consumed quickly. If the local tiers of the device are heavily used, an extended cloud outage might result in the device becoming full, and incoming writes to the volume might result in invalidation of the snapshots (as no space exists to update the snapshots to refer to the older blocks of data that have been overwritten). In such a situation the writes to the volume will continue to be served, but the local snapshots might be invalid. There is no impact to your existing cloud snapshots.

The alert warning is to notify you that such a situation can arise and ensure you address the same in a timely manner by either reviewing your local snapshots schedules to take less frequent local snapshots or deleting older local snapshots that are no longer required.

If the local snapshots are invalidated, you will receive an information alert notifying you that the local snapshots for the specific backup policy have been invalidated alongside the list of timestamps of the local snapshots that were invalidated. These snapshots will be auto-deleted and you will no longer be able to view them in the **Backup Catalogs** blade in the Azure portal.

Questions about converting a tiered volume to a locally pinned volume

I'm observing some slowness on the device while converting a tiered volume to a locally pinned volume. Why is this happening?

The conversion process involves two steps:

1. Provisioning of space on the device for the soon-to-be-converted locally pinned volume.
2. Downloading any tiered data from the cloud to ensure local guarantees.

Both of these steps are long running operations that are dependent on the size of the volume being converted, data on the device, and available bandwidth. As some data from existing tiered volumes might spill to the cloud as part of the provisioning process, your device might experience reduced performance during this time. In addition, the conversion process can be slower if:

- Existing volumes have not been backed up to the cloud; so we suggest you backup your volumes prior to initiating a conversion.
- Bandwidth throttling policies have been applied, which might constrain the available bandwidth to the cloud; we therefore recommend you have a dedicated 40 Mbps or more connection to the cloud.
- The conversion process can take several hours due to the multiple factors explained above; therefore, we suggest that you perform this operation during non-peaks times or on a weekend to avoid the impact on end consumers.

More information on how to [convert a tiered volume to a locally pinned volume](#)

Can I cancel the volume conversion operation?

No, you cannot cancel the conversion operation once initiated. As discussed in the previous question, please be aware of the potential performance issues that you might encounter during the process, and follow the best practices listed above when you plan your conversion.

What happens to my volume if the conversion operation fails?

Volume conversion can fail due to cloud connectivity issues. The device may eventually stop the conversion process after a series of unsuccessful attempts to bring down tiered data from the cloud. In such a scenario, the volume type will continue to be the source volume type prior to conversion, and:

- A critical alert will be raised to notify you of the volume conversion failure. More information on [alerts related to locally pinned volumes](#)
- If you are converting a tiered to a locally pinned volume, the volume will continue to exhibit properties of a tiered volume as data might still reside on the cloud. We suggest that you resolve the connectivity issues and then retry the conversion operation.
- Similarly, when conversion from a locally pinned to a tiered volume fails, although the volume will be marked as a locally pinned volume, it will function as a tiered volume (because data could have spilled to the cloud). However, it will continue to occupy space on the local tiers of the device. This space will not be available for other locally pinned volumes. We suggest that you retry this operation to ensure that the volume conversion is complete and the local space on the device can be reclaimed.

Questions about restoring a locally pinned volume

Are locally pinned volumes restored instantly?

Yes, locally pinned volumes are restored instantly. As soon as the metadata information for the volume is pulled from the cloud as part of the restore operation, the volume is brought online and can be accessed by the host. However, local guarantees for the volume data will not be present until all the data has been downloaded from the cloud, and you may experience reduced performance on these volumes for the duration of the restore.

How long does it take to restore a locally pinned volume?

Locally pinned volumes are restored instantly and brought online as soon as the volume metadata information is retrieved from the cloud, while the volume data continues to be downloaded in the background. This latter part of the restore operation--getting back the local guarantees for the volume data--is a long running operation and might take several hours for all the data to be made local again. The time taken to complete the

same depends on multiple factors, such as the size of the volume being restored and the available bandwidth. If the original volume that is being restored has been deleted, additional time will be taken to create the local space on the device as part of the restore operation.

I need to restore my existing locally pinned volume to an older snapshot (taken when the volume was tiered). Will the volume be restored as tiered in this case?

No, the volume will be restored as a locally pinned volume. Although the snapshot dates to the time when the volume was tiered, while restoring existing volumes, StorSimple always uses the type of volume on the disk as it exists currently.

I extended my locally pinned volume recently, but I now need to restore the data to a time when the volume was smaller in size. Will restore resize the current volume and will I need to extend the size of the volume once the restore is completed?

Yes, the restore will resize the volume, and you will need to extend the size of the volume after the restore is completed.

Can I change the type of a volume during restore?

No, you cannot change the volume type during restore.

- Volumes that have been deleted are restored as the type stored in the snapshot.
- Existing volumes are restored based on their current type, irrespective of the type stored in the snapshot (refer to the previous two questions).

I need to restore my locally pinned volume, but I picked an incorrect point in time snapshot. Can I cancel the current restore operation?

Yes, you can cancel an on-going restore operation. The state of the volume will be rolled back to the state at the start of the restore. However, any writes that were made to the volume while the restore was in progress will be lost.

I started a restore operation on one of my locally pinned volumes, and now I see a snapshot in my backlog catalog that I don't recollect creating. What is this used for?

This is the temporary snapshot that is created prior to the restore operation and is used for rollback in case the restore is canceled or fails. Do not delete this snapshot; it will be automatically deleted when the restore is complete. This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur.

Can I clone a locally pinned volume?

Yes, you can. However, the locally pinned volume will be cloned as a tiered volume by default. More information on how to [clone a locally pinned volume](#)

Questions about failing over a locally pinned volume

I need to fail over my device to another physical device. Will my locally pinned volumes be failed over as locally pinned or tiered?

The locally pinned volumes are failed over as Locally pinned if the target device is running StorSimple 8000 series update 3 or higher.

More information on [failover and DR of locally pinned volumes across versions](#)

Are locally pinned volumes instantly restored during disaster recovery (DR)?

Yes, locally pinned volumes are restored instantly during failover. As soon as the metadata information for the volume is pulled from the cloud as part of the failover operation, the volume is brought online on the target device and can be accessed by the host. Meanwhile, the volume data will continue to download in the background, and you may experience reduced performance on these volumes for the duration of the failover.

I see the failover job completed, how can I track the progress of locally pinned volume that is being restored on the target device?

During a failover operation, the failover job is marked as complete once all the volumes in the failover set have been instantly restored and brought online on the target device. This includes any locally pinned volumes that might have been failed over; however, local guarantees of the data will only be available when all the data for the volume has been downloaded. You can track this progress for each locally pinned volume that was failed over by monitoring the corresponding restore jobs that are created as part of the failover. These individual restore jobs will only be created for locally pinned volumes.

Can I change the type of a volume during failover?

No, you cannot change the volume type during a failover. If you are failing over to another physical device that is running StorSimple 8000 series update 3, the volumes are failed over based on the volume type stored in the snapshot.

Can I fail over a volume container with locally pinned volumes to the cloud appliance?

Yes, you can. The locally pinned volumes will be failed over as tiered volumes. More information on [failover and DR of locally pinned volumes across versions](#)

Azure role-based access control for StorSimple

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article provides a brief description of how Azure role-based access control (Azure RBAC) can be used for your StorSimple device. Azure RBAC offers fine-grained access management for Azure. Use Azure RBAC to grant just the right amount of access to the StorSimple users to do their jobs instead of giving everyone unrestricted access. For more information on the basics of access management in Azure, see [What is Azure role-based access control \(Azure RBAC\)](#).

This article applies to StorSimple 8000 series devices running Update 3.0 or later in the Azure portal.

ⓘ Note

We recommend that you use the Azure Az PowerShell module to interact with Azure. See [Install Azure PowerShell](#) to get started. To learn how to migrate to the Az PowerShell module, see [Migrate Azure PowerShell from AzureRM to Az](#).

Azure roles for StorSimple

Azure RBAC can be assigned based on the roles. The roles ensure certain permission levels based on the available resources in the environment. There are two types of roles that StorSimple users can choose from: built-in or custom.

- **Built-in roles** - The built-in roles can be owner, contributor, reader, or user access administrator. For more information, see [Built-in roles for Azure Role-based Access Control](#).

- **Custom roles** - If the built-in roles do not suit your needs, you can create Azure custom roles for StorSimple. To create a Azure custom role, start with a built-in role, edit it, and then import it back in the environment. The download and upload of the role are managed using either Azure PowerShell or the Azure CLI. For more information, see [Create custom roles for Role-based Access Control](#).

To view the different roles available for a StorSimple device user in the Azure portal, go to your StorSimple Device Manager service and then go to **Access control (IAM) > Roles**.

Create a custom role for StorSimple Infrastructure Administrator

In the following example, we start with the built-in role **Reader** that allows users to view all the resource scopes but not to edit them or create new ones. We then extend this role to create a new custom role StorSimple Infrastructure admin. This role is assigned to users who can manage the infrastructure for the StorSimple devices.

1. Run Windows PowerShell as an administrator.

2. Log in to Azure.

```
Connect-AzAccount
```

3. Export the Reader role as a JSON template on your computer.

PowerShell

```
Get-AzRoleDefinition -Name "Reader"  
Get-AzRoleDefinition -Name "Reader" | ConvertTo-Json | Out-File  
C:\ssrbaccustom.json
```

4. Open the JSON file in Visual Studio. You see that a typical Azure role consists of three main sections, **Actions**, **NotActions**, and **AssignableScopes**.

In the **Action** section, all the permitted operations for this role are listed. Each action is assigned from a resource provider. For a StorSimple infrastructure admin, use the `Microsoft.StorSimple` resource provider.

Use PowerShell to see all the resource providers available and registered in your subscription.

```
Get-AzResourceProvider
```

You can also check for all the available PowerShell cmdlets to manage the resource providers.

In the **NotActions** sections, all the restricted actions for a particular Azure role are listed. In this example, no actions are restricted.

Under the **AssignableScopes**, the subscription IDs are listed. Ensure that the Azure role contains the explicit subscription ID where it is used. If the correct subscription ID is not specified, you are not allowed to import the role in your subscription.

Edit the file keeping in mind the preceding considerations.

JSON

```
{  
    "Name": "StorSimple Infrastructure Admin",  
    "Id": "<guid>",  
    "IsCustom": true,  
    "Description": "Lets you view everything, but not make any changes  
except for Clear alerts, Clear settings, install, download etc.",  
    "Actions": [  
        "Microsoft.StorSimple/managers/alerts/read",  
  
        "Microsoft.StorSimple/managers/devices/volumeContainers/read",  
        "Microsoft.StorSimple/managers/devices/jobs/read",  
  
        "Microsoft.StorSimple/managers/devices/alertSettings/read",  
  
        "Microsoft.StorSimple/managers/devices/alertSettings/write",  
        "Microsoft.StorSimple/managers/clearAlerts/action",  
  
        "Microsoft.StorSimple/managers/devices/networkSettings/read",  
  
        "Microsoft.StorSimple/managers/devices/publishSupportPackage/action",  
  
        "Microsoft.StorSimple/managers/devices/scanForUpdates/action",  
  
        "Microsoft.StorSimple/managers/devices/metrics/read"  
  
    ],  
    "NotActions": [  
    ],  
    "AssignableScopes": [  
        "/subscriptions/<subscription_ID>/"  
    ]  
}
```

5. Import the Azure custom role back into the environment.

```
New-AzRoleDefinition -InputFile "C:\ssrbaccustom.json"
```

This role should now appear in the list of roles in the Access control blade.

NAME	Custom	Built-in	USERS	GROUPS
Owner			5	1
Contributor			23	0
Reader			0	0
StorSimple Infrastructure Admin			1	0
User Access Administrator			1	0
Azure Service Deploy Release Management Contributor			0	0

For more information, go to [Custom roles](#).

Sample output for custom role creation via the PowerShell

PowerShell

```
Connect-AzAccount
```

Output

```
Environment      : AzureCloud
Account         : john.doe@contoso.com
TenantId        : <tenant_ID>
SubscriptionId  : <subscription_ID>
SubscriptionName : Internal Consumption
CurrentStorageAccount :
```

PowerShell

```
Get-AzRoleDefinition -Name "Reader"
```

Output

```
Name      : Reader
Id       : <guid>
IsCustom : False
Description : Lets you view everything, but not make any changes.
```

```
Actions      : {*/read}
NotActions   : {}
AssignableScopes : {/}
```

PowerShell

```
Get-AzRoleDefinition -Name "Reader" | ConvertTo-Json | Out-File C:\ssrbaccustom.json
New-AzRoleDefinition -InputFile "C:\ssrbaccustom.json"
```

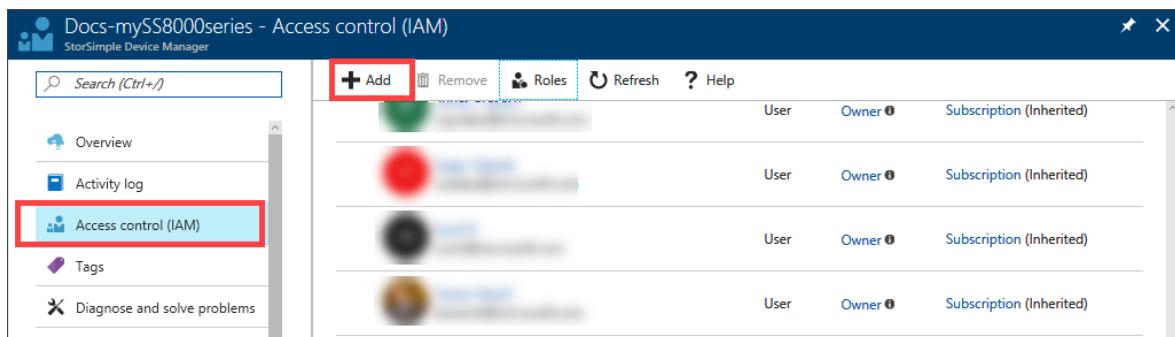
Output

```
Name      : StorSimple Infrastructure Admin
Id        : <tenant_ID>
IsCustom  : True
Description : Lets you view everything, but not make any changes except for Clear alerts, Clear settings, install, download etc.
Actions    : {Microsoft.StorSimple/managers/alerts/read,
              Microsoft.StorSimple/managers/devices/volumeContainers/read,
              Microsoft.StorSimple/managers/devices/jobs/read,
              Microsoft.StorSimple/managers/devices/alertSettings/read...}
NotActions : {}
AssignableScopes : {/subscriptions/<subscription_ID>/}
```

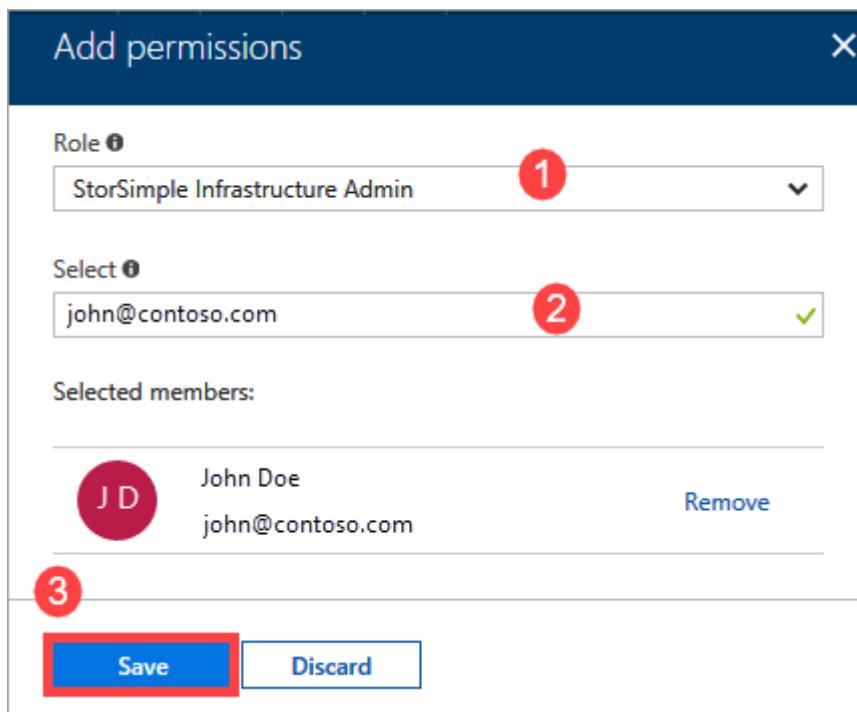
Add users to the custom role

You grant access from within the resource, resource group, or subscription that is the scope of the role assignment. When providing access, bear in mind that the access granted at the parent node is inherited by the child. For more information, go to [Azure role-based access control \(Azure RBAC\)](#).

1. Go to **Access control (IAM)**. Click **+ Add** on the Access control blade.



2. Select the role that you wish to assign, in this case it is the **StorSimple Infrastructure Admin**.
3. Select the user, group, or application in your directory that you wish to grant access to. You can search the directory with display names, email addresses, and object identifiers.
4. Select **Save** to create the assignment.



An **Adding user** notification tracks the progress. After the user is successfully added, the list of users in Access control is updated.

View permissions for the custom role

Once this role is created, you can view the permissions associated with this role in the Azure portal.

1. To view the permissions associated with this role, go to **Access control (IAM)** > **Roles** > **StorSimple Infrastructure Admin**. The list of users in this role is displayed.
2. Select a StorSimple Infrastructure Admin user and click **Permissions**.

3. The permissions associated with this role are displayed.

RESOURCE PROVIDER	PERMISSIONS
Microsoft Authorization	Partial
Microsoft Monitoring Insights	Partial
Microsoft Resources	Partial
Microsoft StorSimple Device Manager	Partial

RESOURCE TYPE	READ
Microsoft Authorization	
Classic subscription administrator	✓
Management lock	✓
Permission	✓
Policy assignment	✓
Policy definition	✓
Policy set definition	✓
Provider operations	✓
Role assignment	✓
Role definition	✓

Next steps

Learn how to [Assign custom roles for internal and external users](#).

Use the StorSimple Manager service to manage access control records

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Access control records (ACRs) allow you to specify which hosts can connect to a volume on the StorSimple device. ACRs are set to a specific volume and contain the iSCSI Qualified Names (IQNs) of the hosts. When a host tries to connect to a volume, the device checks the ACR associated with that volume for the IQN name and if there is a match, then the connection is established. The access control records in the **Configuration** section of your StorSimple Device Manager service blade display all the access control records with the corresponding IQNs of the hosts.

This tutorial explains the following common ACR-related tasks:

- Add an access control record
- Edit an access control record
- Delete an access control record

ⓘ Important

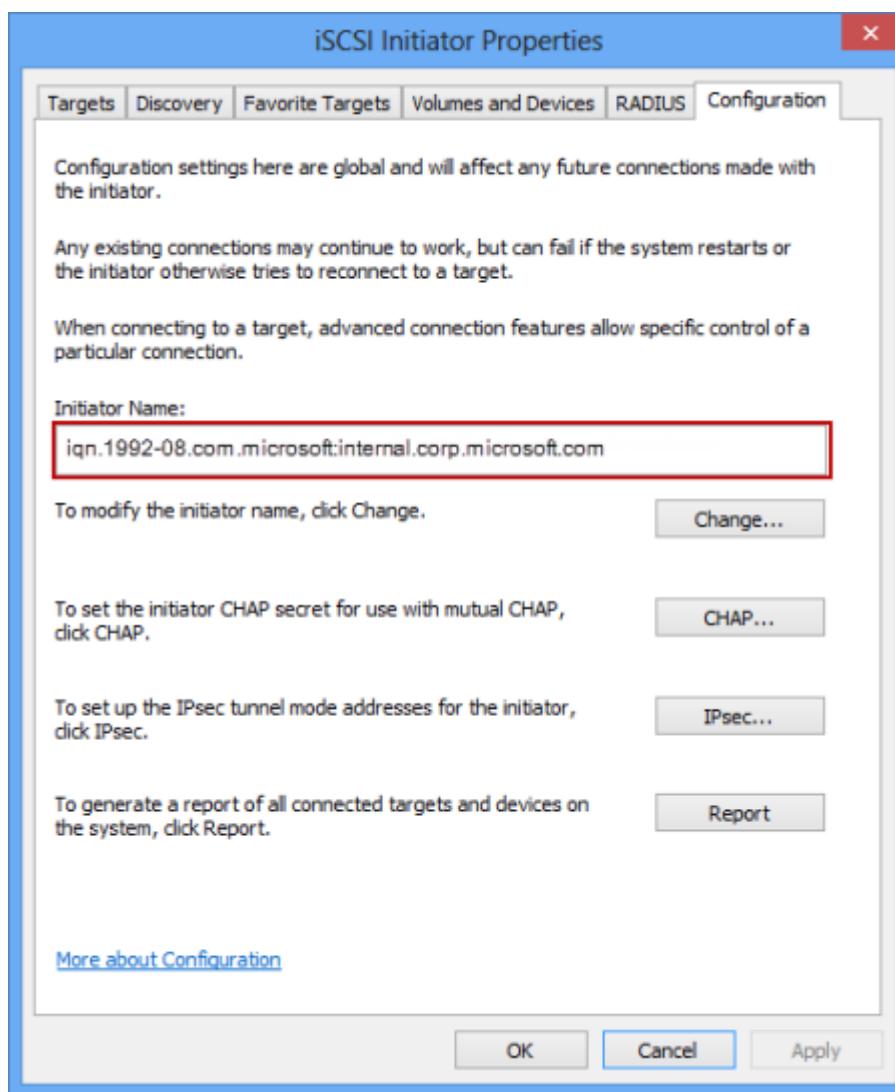
- When assigning an ACR to a volume, take care that the volume is not concurrently accessed by more than one non-clustered host because this could corrupt the volume.
- When deleting an ACR from a volume, make sure that the corresponding host is not accessing the volume because the deletion could result in a read-write disruption.

Get the IQN

Perform the following steps to get the IQN of a Windows host that is running Windows Server 2012.

To get the IQN of a Windows host

1. Start the Microsoft iSCSI initiator on your Windows host. Click **Start > Administrative Tools > iSCSI initiator**.
2. In the **iSCSI Initiator Properties** window, on the **Configuration** tab, select and copy the string from the **Initiator Name** field.



3. Save this string.

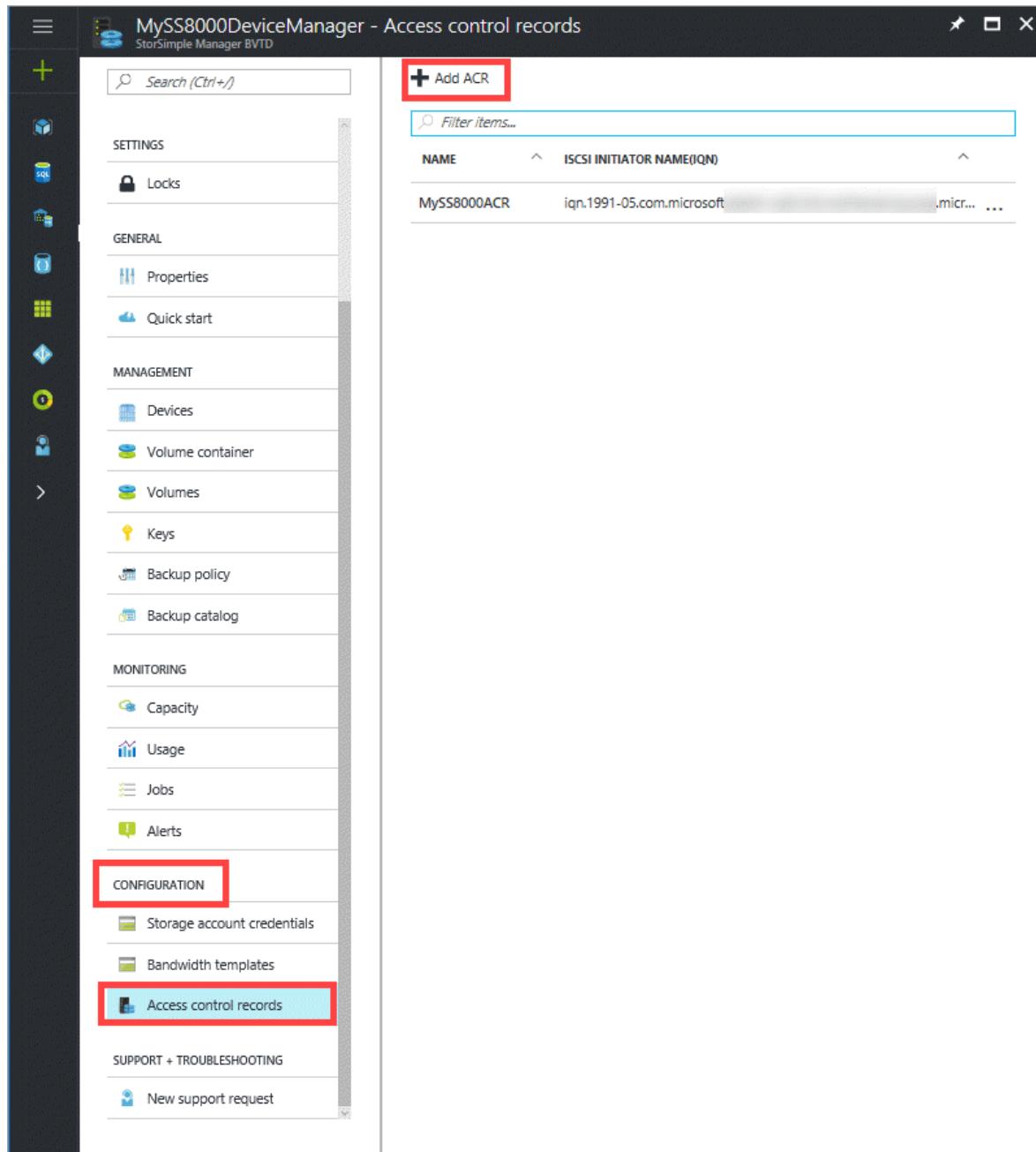
Add an access control record

You use the **Configuration** section in the StorSimple Device Manager service blade to add ACRs. Typically, you will associate one ACR with one volume.

Perform the following steps to add an ACR.

To add an ACR

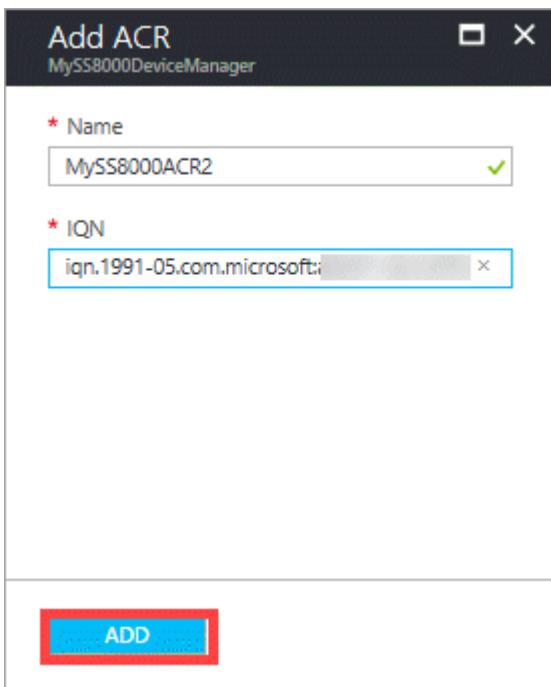
1. Go to your StorSimple Device Manager service, double-click the service name, and then within the Configuration section, click Access control records.
2. In the Access control records blade, click + Add ACR.



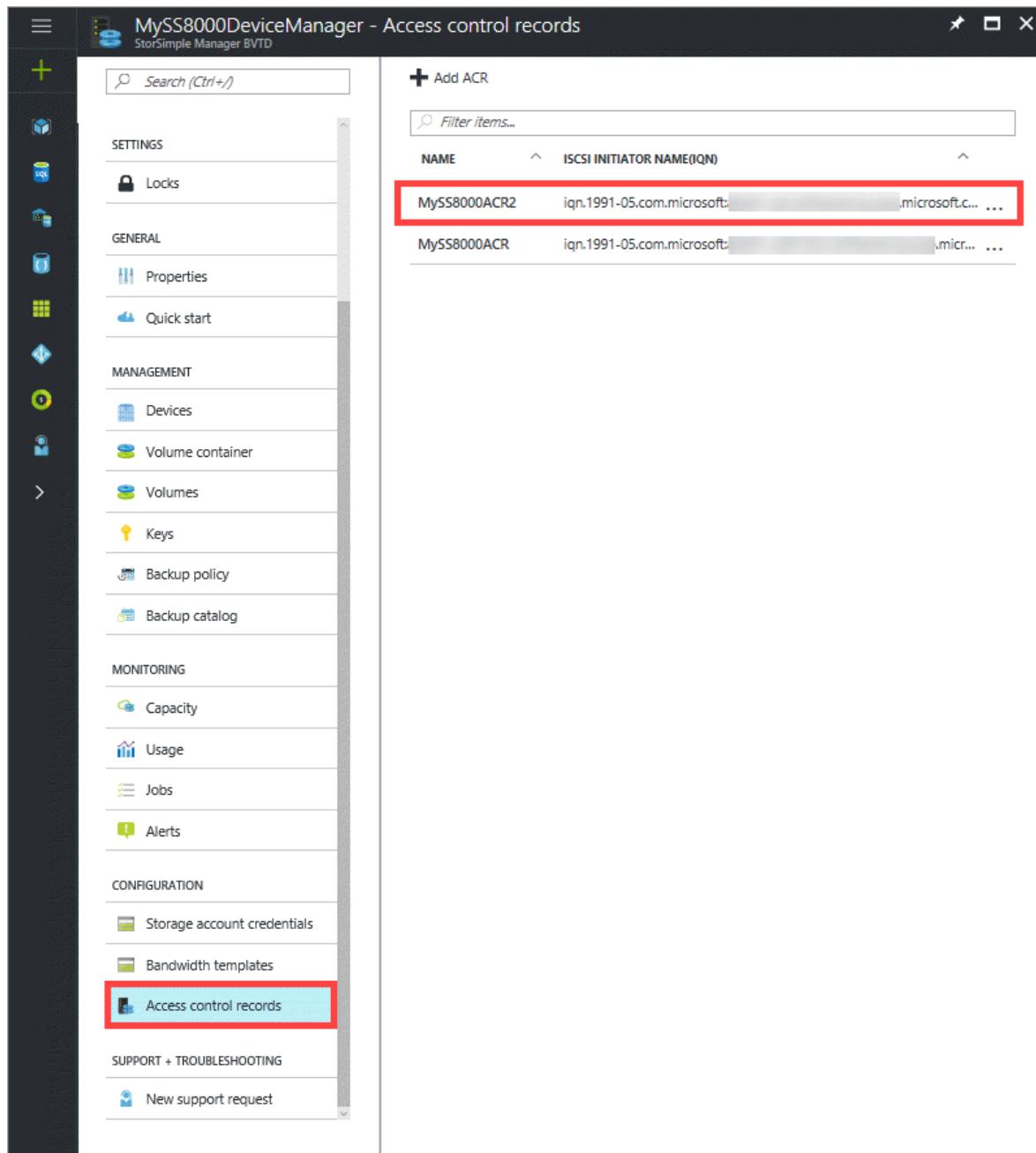
3. In the Add ACR blade, do the following steps:

- a. Supply a name for your ACR.
- b. Provide the IQN name of your Windows Server host under iSCSI Initiator Name (IQN).

c. Click Add to create the ACR.



4. The newly added ACR will display in the tabular listing of ACRs.



Edit an access control record

You use the **Configuration** section in the StorSimple Device Manager service blade to edit ACRs.

! Note

It is recommended that you modify only those ACRs that are currently not in use. To edit an ACR associated with a volume that is currently in use, you must first take the volume offline.

Perform the following steps to edit an ACR.

To edit an access control record

1. Go to your StorSimple Device Manager service, double-click the service name, and then within the Configuration section, click Access control records.

NAME	ISCSI INITIATOR NAME(IQN)
MySS8000ACR	iqn.1991-05.com.microsoft

2. In the tabular listing of the access control records, click and select the ACR that you wish to modify.

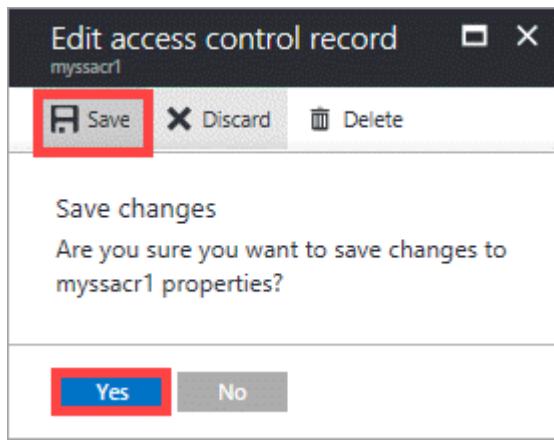
The screenshot shows the 'Access control records' blade in the StorSimple Device Manager. On the left, a navigation pane lists various management categories like Settings, General, Management, Monitoring, and Configuration. Under Configuration, 'Access control records' is highlighted with a red box. The main pane displays a table titled 'Add ACR' with two entries:

NAME	ISCSI INITIATOR NAME(IQN)	
myssacr2	iqn.1991-05.com.microsoft:....microsoft.com	...
myssacr1	iqn.1991-05.com.microsoft:....microsoft.com	...

3. In the **Edit access control record** blade, provide a different IQN corresponding to another host.

The screenshot shows the 'Edit access control record' blade for 'myssacr1'. At the top, there are 'Save', 'Discard', and 'Delete' buttons. Below them is a 'Name' field containing 'myssacr1'. Underneath is an 'iSCSI initiator Name(IQN)' field containing 'microsoft:svc-m3cu8ta.northamerica.corp.m' with a green checkmark. This entire input field is also outlined with a red box.

4. Click **Save**. When prompted for confirmation, click **Yes**.



5. You are notified when the ACR is updated. The tabular listing also updates to reflect the change.

Delete an access control record

You use the **Configuration** section in the StorSimple Device Manager service blade to delete ACRs.

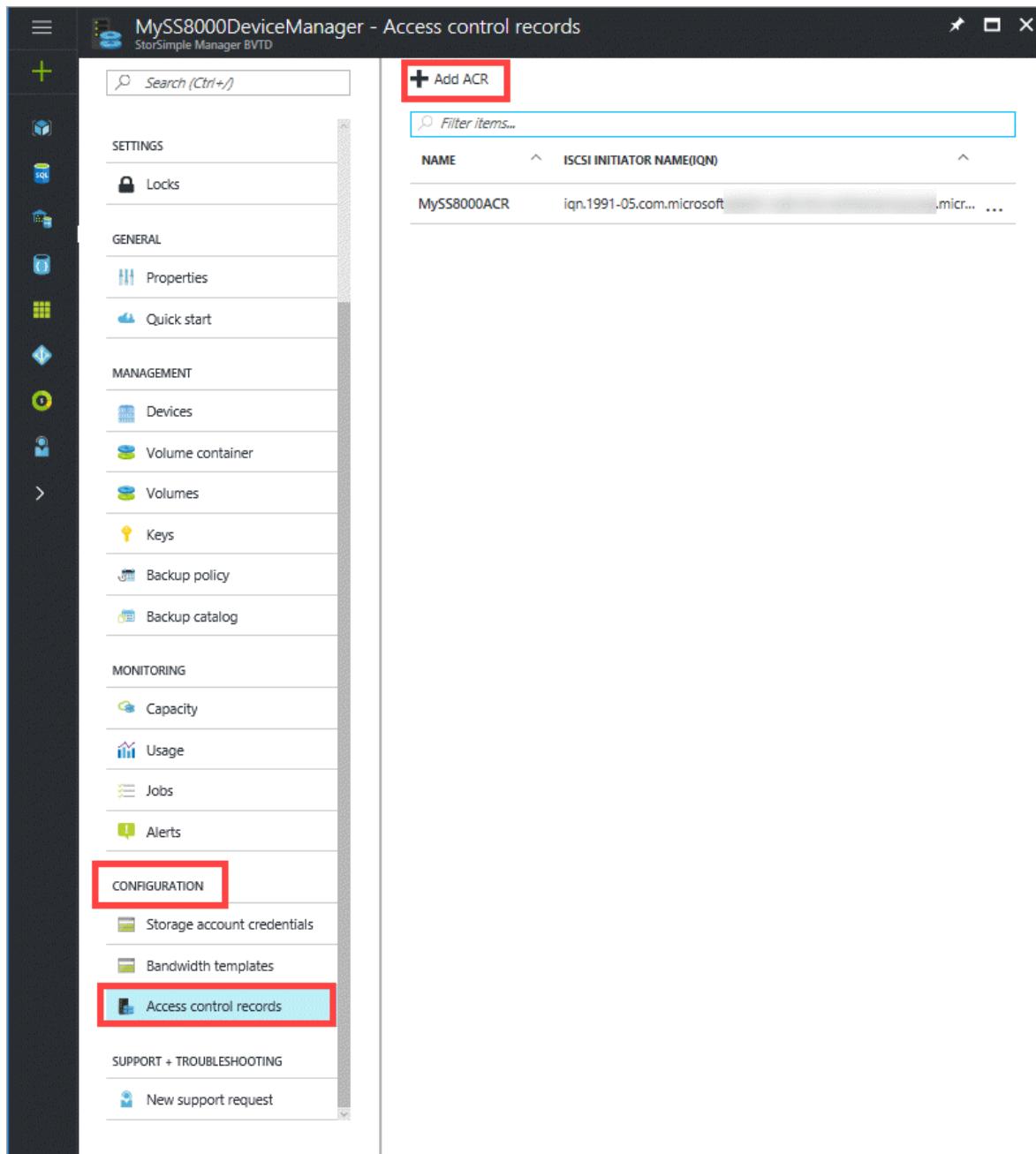
Note

You can delete only those ACRs that are currently not in use. To delete an ACR associated with a volume that is currently in use, you must first take the volume offline.

Perform the following steps to delete an access control record.

To delete an access control record

1. Go to your StorSimple Device Manager service, double-click the service name, and then within the **Configuration** section, click **Access control records**.



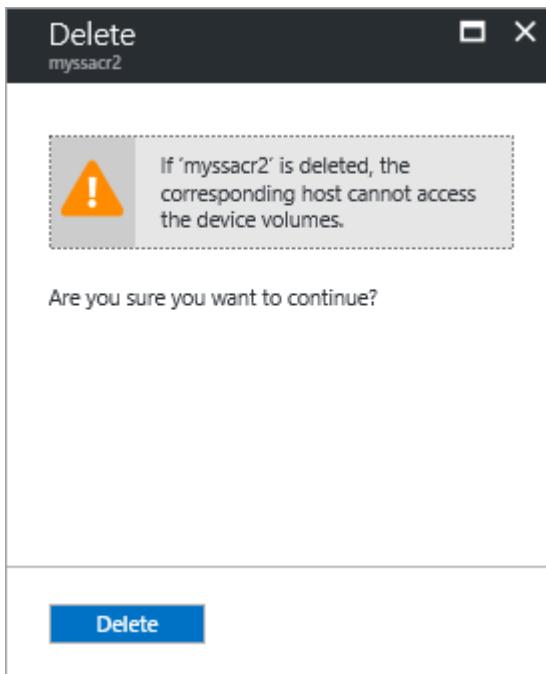
2. In the tabular listing of the access control records, click and select the ACR that you wish to delete.

The screenshot shows the 'Access control records' page in the StorSimple Device Manager. On the left, a navigation pane lists various management categories: SETTINGS (Locks), GENERAL (Properties, Quick start), MANAGEMENT (Devices, Volume container, Volumes, Keys, Backup policy, Backup catalog), MONITORING (Capacity, Usage, Jobs, Alerts), CONFIGURATION (Storage account credentials, Bandwidth templates, **Access control records**), and SUPPORT + TROUBLESHOOTING (New support request). The 'Access control records' item is highlighted with a red box. The main content area displays a table titled 'Add ACR' with columns 'NAME' and 'ISCSI INITIATOR NAME(IQN)'. Two entries are listed: 'myssacr1' with IQN 'iqn.1991-05.com.microsoft:microsoft.com' and 'myssacr2' with IQN 'iqn.1991-05.com.microsoft:microsoft.com'. Both rows have a red box around them. A search bar at the top is labeled 'Search (Ctrl+Shift+F)'.

3. Right-click to invoke the context menu and select **Delete**.

This screenshot shows the same 'Access control records' page after a right-click on the row for 'myssacr2'. A context menu is open, with the 'Delete' option highlighted. The menu also includes 'Pin to dashboard' and other options. The row for 'myssacr2' is highlighted with a red box, and the entire context menu area is also enclosed in a red box.

4. When prompted for confirmation, review the information and then click **Delete**.



5. You are notified when the deletion completes. The tabular listing is updated to reflect the deletion.

A screenshot of the StorSimple Device Manager interface. The left sidebar shows navigation categories like SETTINGS, GENERAL, MANAGEMENT, MONITORING, and CONFIGURATION. Under CONFIGURATION, the "Access control records" item is highlighted with a red box. The main pane displays a table titled "Access control records" with one row selected, also highlighted with a red box. The table columns are NAME, ISCSI INITIATOR NAME(IQN), and ... (ellipsis). The selected row contains "myssacr1", "iqn.1991-05.com.microsoft", and "...".

Next steps

- Learn more about [managing StorSimple volumes](#).
- Learn more about [using the StorSimple Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to manage StorSimple bandwidth templates

Article • 08/19/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Bandwidth templates allow you to configure network bandwidth usage across multiple time-of-day schedules to tier the data from the StorSimple device to the cloud.

With bandwidth throttling schedules you can:

- Specify customized bandwidth schedules depending on the workload network usages.
- Centralize management and reuse the schedules across multiple devices in an easy and seamless manner.

ⓘ Note

This feature is available only for StorSimple physical devices (models 8100 and 8600) and not for StorSimple Cloud Appliances (models 8010 and 8020).

The Bandwidth templates blade

The **Bandwidth templates** blade has all the bandwidth templates for your service in a tabular format, and contains the following information:

- **Name** – A unique name assigned to the bandwidth template when it was created.

- **Schedule** – The number of schedules contained in a given bandwidth template.
- **Used by** – The number of volumes using the bandwidth templates.

You can also find additional information to help configure bandwidth templates in:

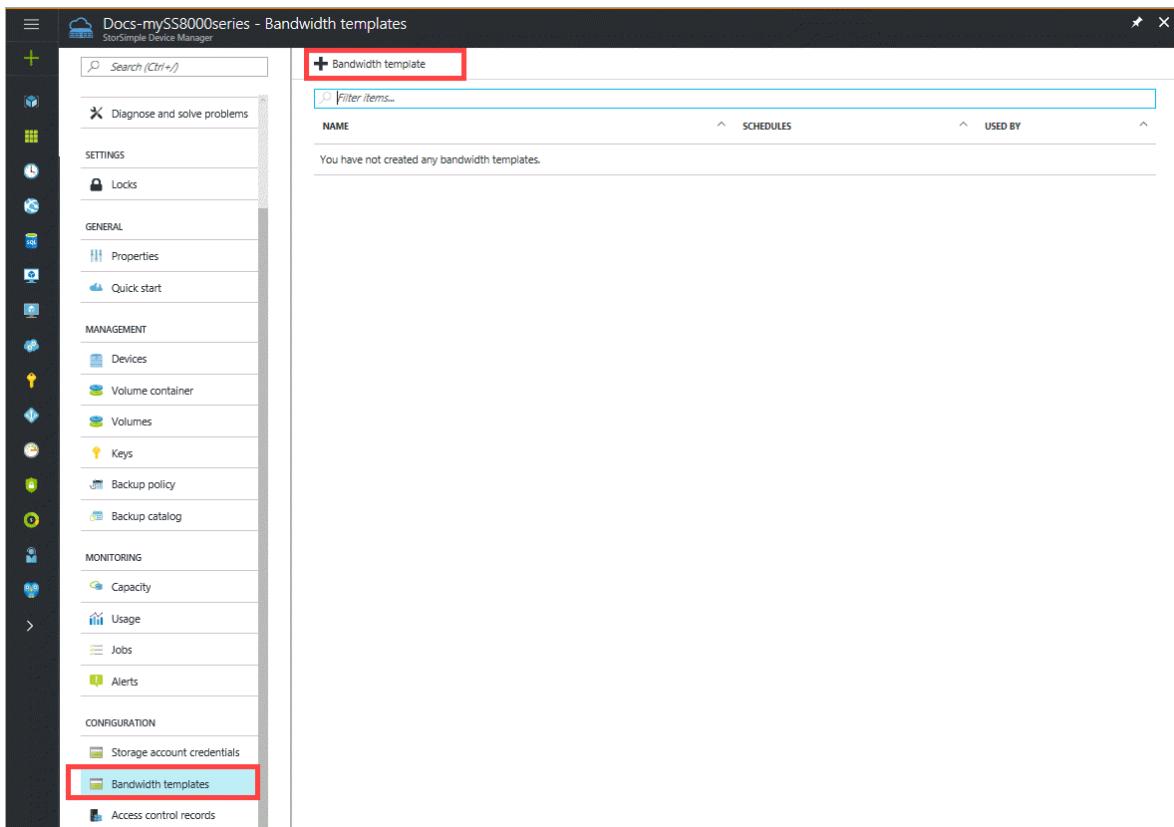
- [Questions and answers about bandwidth templates](#)
- [Best practices for bandwidth templates](#)

Add a bandwidth template

Perform the following steps to create a new bandwidth template.

To add a bandwidth template

1. Go to your StorSimple Device Manager service, click **Bandwidth templates** and then click **+ Add Bandwidth template**.



2. In the **Add bandwidth template** blade, do the following steps:

- a. Specify a unique name for your bandwidth template.
- b. Define a bandwidth schedule. To create a schedule:
 - i. From the drop-down list, choose the **Days** of the week the schedule is configured for. You can select multiple days.

ii. Enter a **Start Time** in *hh:mm* format. This is when the schedule will begin.

iii. Enter an **End Time** in *hh:mm* format. This is when the schedule will stop.

Note

Overlapping schedules are not allowed. If the start and end times will result in an overlapping schedule, you will see an error message to that effect.

iv. Specify the **Bandwidth Rate**. This is the bandwidth in Megabits per second (Mbps) used by your StorSimple device in operations involving the cloud (both uploads and downloads). Supply a number between 1 and 1,000 for this field.

Days	Start Time	End Time	Bandwidth Rate
0 selected	Enter time in 'hh:mm' format.	Enter time in 'hh:mm' format.	Enter rate in Mbps
Monday,Saturday,Sunday	00:00	23:59	1
Tuesday,Wednesday,Thursday,Fri...	08:00	17:00	100

Repeat the above steps to define multiple schedules for your template until you are done.

v. Click **Add** to start creating a bandwidth template. The created template is added to the list of bandwidth templates.

Edit a bandwidth template

Perform the following steps to edit a bandwidth template.

To edit a bandwidth template

1. Go to your StorSimple Device Manager service and click **Bandwidth templates**.
2. In the list of bandwidth templates, select the template you wish to delete. Right-click and from the context menu, select **Delete**.
3. When prompted for confirmation, click **OK**. This should delete the bandwidth template.
4. The list of bandwidth templates updates to reflect the deletion.

Note

You cannot save your changes if the edited schedule overlaps with an existing schedule in the bandwidth template that you are modifying.

Delete a bandwidth template

Perform the following steps to delete a bandwidth template.

To delete a bandwidth template

1. Go to your StorSimple Device Manager service and click **Bandwidth templates**.
2. In the list of bandwidth templates, select the template you wish to delete. Right-click and from the context menu, select **Delete**.
3. When prompted for confirmation, click **OK**. This should delete the bandwidth template.
4. The list of bandwidth templates updates to reflect the deletion.

If the template is in use by any volume(s), you will not be allowed to delete it. You will see an error message indicating that the template is in use. An error message dialog box will appear advising you that all the references to the template should be removed.

You can delete all the references to the template by accessing the **Volume Containers** page and modifying the volume containers that use this template so that they use another template or use a custom or unlimited bandwidth setting. When all the references have been removed, you can delete the template.

Use a default bandwidth template

A default bandwidth template is provided and is used by volume containers by default to enforce bandwidth controls when accessing the cloud. The default template also

serves as a ready reference for users who create their own templates. The details of this default template are:

- **Name** – Unlimited nights and weekends
- **Schedule** – A single schedule from Monday to Friday that applies a bandwidth rate of 1 Mbps between 8 AM and 5 PM device time. The bandwidth is set to Unlimited for the remainder of the week.

The default template can be edited. The usage of this template (including edited versions) is tracked.

Create an all-day bandwidth template that starts at a specified time

Follow this procedure to create a schedule that starts at a specified time and runs all day. In the example, the schedule starts at 9 AM in the morning and runs until 9 AM the next morning. It's important to note that the start and end times for a given schedule must both be contained on the same 24 hour schedule and cannot span multiple days. If you need to set up bandwidth templates that span multiple days, you will need to use multiple schedules (as shown in the example).

To create an all-day bandwidth template

1. Create a schedule that starts at 9 AM in the morning and runs until midnight.
2. Add another schedule. Configure the second schedule to run from midnight until 9 AM in the morning.
3. Save the bandwidth template.

The composite schedule will then start at a time of your choosing and run all-day.

Questions and answers about bandwidth templates

Q. What happens to bandwidth controls when you are in between the schedules? (A schedule has ended and another one has not started yet.)

A. In such cases, no bandwidth controls will be employed. This means that the device can use unlimited bandwidth when tiering data to the cloud.

Q. Can you modify bandwidth templates on an offline device?

A. You will not be able to modify bandwidth templates on volumes containers if the corresponding device is offline.

Q. Can you edit a bandwidth template associated with a volume container when the associated volumes are offline?

A. You can modify a bandwidth template associated with a volume container whose volumes are offline. Note that when volumes are offline, no data will be tiered from the device to the cloud.

Q. Can you delete a default template?

A. Although you can delete a default template, it is not a good idea to do so. The usage of a default template, including edited versions, is tracked. The tracking data is analyzed and over the course of time, is used to improve the default template.

Q. How do you determine that your bandwidth templates need to be modified?

A. One of the signs that you need to modify the bandwidth templates is when you start seeing the network slow down or choke multiple times in a day. If this happens, monitor the storage and usage network by looking at the I/O Performance and Network Throughput charts.

From the network throughput data, identify the time of day and the volume containers in which the network bottleneck occurs. If this happens when data is being tiered to the cloud (get this information from I/O performance for all volume containers for device to cloud), then you will need to modify the bandwidth templates associated with your volume containers.

After the modified templates are in use, you will need to monitor the network again for significant latencies. If these still exist, then you will need to revisit your bandwidth templates.

Q. What happens if multiple volume containers on my device have schedules that overlap but different limits apply to each?

A. Let's assume that you have a device with 3 volume containers. The schedules associated with these containers completely overlap. For each of these containers, the bandwidth limits used are 5, 10, and 15 Mbps respectively. When I/O are occurring on all of these containers at the same time, the minimum of the 3 bandwidth limits may be applied: in this case, 5 Mbps as these outgoing I/O requests share the same queue.

Best practices for bandwidth templates

Follow these best practices for your StorSimple device:

- Configure bandwidth templates on your device to enable variable throttling of the network throughput by the device at different times of the day. These bandwidth templates when used with backup schedules can effectively leverage additional network bandwidth for cloud operations during off-peak hours.
- Calculate the actual bandwidth required for a particular deployment based on the size of the deployment and the required recovery time objective (RTO).

Next steps

Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to view and manage jobs (Update 3 and later)

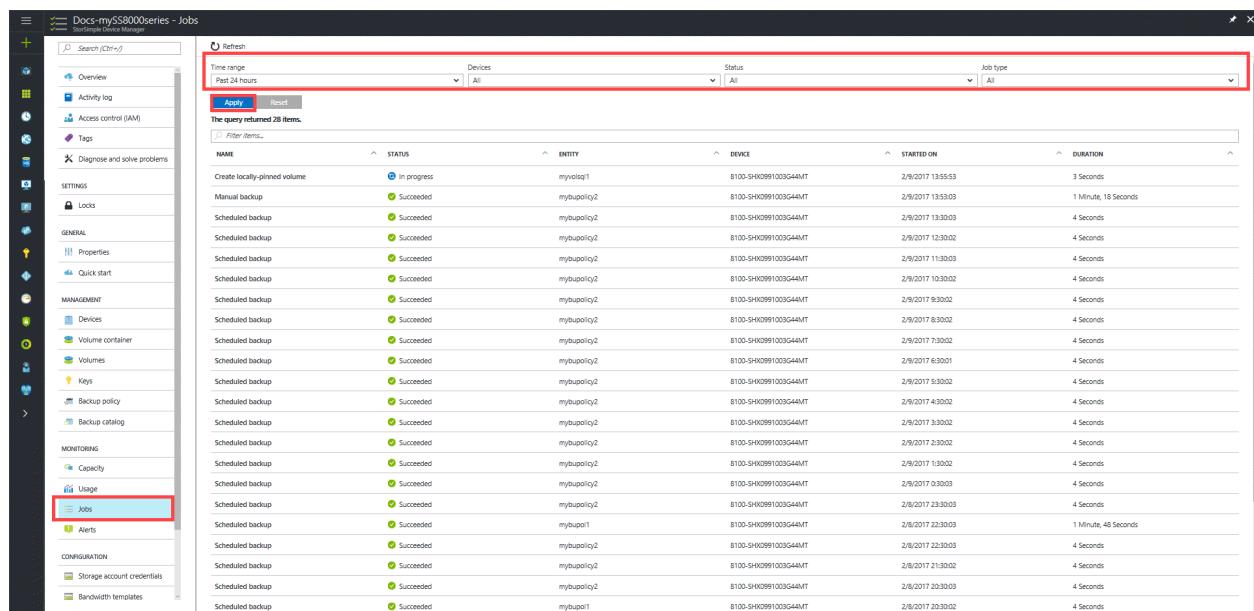
Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The **Jobs** blade provides a single central portal for viewing and managing jobs that were started on devices connected to your StorSimple Device Manager service. You can view scheduled, running, completed, canceled, and failed jobs for multiple devices. Results are presented in a tabular format.



The screenshot shows the 'Jobs' blade in the StorSimple Device Manager interface. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, and Jobs (which is highlighted with a red box). The main area has a search bar and filtering options for Time range (Past 24 hours), Devices (All), Status (All), and Job type (All). A table lists 28 items, each with a status icon (green for succeeded, blue for in progress), name, entity, device, start time, and duration. Most entries show a duration of '4 Seconds'.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Create locally-pinned volume	In progress	mybup01	8100-SH02991003G44MT	2/9/2017 13:55:53	3 Seconds
Manual backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 13:53:03	1 Minute, 18 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 13:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 12:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 11:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 10:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 9:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 8:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 7:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 6:30:01	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 5:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 4:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 3:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 2:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 1:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/9/2017 0:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 23:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 22:30:03	1 Minute, 48 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 22:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 21:30:02	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 20:30:03	4 Seconds
Scheduled backup	Succeeded	mybup01	8100-SH02991003G44MT	2/8/2017 20:30:02	4 Seconds

You can quickly find the jobs you are interested in by filtering on fields such as:

- **Status** – Jobs can be in progress, succeeded, canceled, failed, canceling, or succeeded with errors.

- **Time range** – Jobs can be filtered based on the date and time range. The ranges are past 1 hour, past 24 hours, past 7 days, past 30 days, past year, or custom date.
- **Type** – The job type can be scheduled backup, manual backup, restore backup, clone volume, fail over volume containers, create locally-pinned volume, modify volume, install updates, collect support logs and create cloud appliance.
- **Devices** – Jobs are initiated on a certain device connected to your service.

The filtered jobs are then tabulated on the basis of the following attributes:

- **Name** – scheduled backup, manual backup, restore backup, clone volume, fail over volume containers, create locally pinned volume, modify volume, install updates, collect support logs, or create cloud appliance.
- **Status** – running, completed, canceled, failed, canceling, or completed with errors.
- **Entity** – The jobs can be associated with a volume, a backup policy, or a device. For example, a clone job is associated with a volume, whereas a scheduled backup job is associated with a backup policy. A device job is created as a result of a disaster recovery (DR) or a restore operation.
- **Device** – The name of the device on which the job was started.
- **Started on** – The time when the job was started.
- **Duration** – The time required to complete the job.

The list of jobs is refreshed every 30 seconds.

You can perform the following job-related actions on this page:

- View job details
- Cancel a job

View job details

Perform the following steps to view the details of any job.

To view job details

1. Go to your StorSimple Device Manager service and then click **Jobs**.
2. In the **Jobs** blade, display the job(s) you are interested in by running a query with appropriate filters. You can search for completed, running, or canceled jobs.

The screenshot shows the 'Jobs' section of the Microsoft Docs - mySS8000series - Jobs page in the Azure portal. The 'Jobs' section is highlighted with a red box. The table lists 29 items, mostly scheduled backups, with columns for Name, Status, Entity, Device, Started On, Duration, and Job type.

Name	Status	Entity	Device	Started On	Duration	Job type
Create locally-pinned volume	In progress	myvsql01	8100-SH00991035G44UT	2/9/2017 13:55:53	3 Seconds	
Manual backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 13:53:03	1 Minute, 18 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 13:08:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 12:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 11:30:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 12:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 9:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 8:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 7:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 6:30:01	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 3:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 4:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 3:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 2:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 1:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/9/2017 0:30:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/8/2017 23:30:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq1	8100-SH00991035G44UT	2/8/2017 22:30:03	1 Minute, 48 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/8/2017 22:30:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/8/2017 21:30:02	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq2	8100-SH00991035G44UT	2/8/2017 20:30:03	4 Seconds	
Scheduled backup	Succeeded	mybuqlsq1	8100-SH00991035G44UT	2/8/2017 20:30:02	4 Seconds	

3. Select and click a job.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Create locally-pinned volume	Succeeded	myvdp01	8100-5H0K0991003G44MT	2/9/2017 13:55:53	3 Seconds
Manual backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 13:53:03	1 Minute, 18 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 13:30:23	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 12:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 11:30:03	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 10:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 9:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 8:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 7:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 6:30:01	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 5:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 4:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 3:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 2:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 1:30:02	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/9/2017 0:30:03	4 Seconds
Scheduled backup	Succeeded	mybuop1q2	8100-5H0K0991003G44MT	2/8/2017 23:30:03	4 Seconds
Scheduled backup	Succeeded	myvdp01	8100-5H0K0991003G44MT	2/8/2017 22:30:03	1 Minute, 48 Seconds

4. In the job details blade, you can view the status, details, time statistics, and data statistics.

The screenshot shows the 'Manual backup' job details page. On the left is a vertical toolbar with icons for Refresh, Cancel, and various management functions. The main area displays the following job details:

Details	
Status	Succeeded
Entity	mybupolicy2 (Microsoft.StorSimple/managers/devices/backupPolicies)
Device	8100-SHX0991003G44MT
Started on	2/9/2017 13:53:03
Completed on	2/9/2017 13:54:22
Duration	1 Minute, 19 Seconds
Processed data	500 GB out of 500 GB
Backup type	CloudSnapshot

Cancel a job

Perform the following steps to cancel a running job.

ⓘ Note

Some jobs, such as modifying a volume to change the volume type or expanding a volume, cannot be canceled.

To cancel a job

1. On the **Jobs** page, display the running job(s) that you want to cancel by running a query with appropriate filters. Select the job.
2. Right-click on the selected job to invoke the context menu and click **Cancel**.

The screenshot shows the 'Jobs' page with a list of running and completed jobs. A red box highlights the 'Create locally-pinned volume' job, which is currently 'In progress'. Another red box highlights the 'Cancel' option in the context menu for this job. The table columns are: NAME, STATUS, ENTITY, DEVICE, STARTED ON, and DURATION.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Create locally-pinned volume	In progress	myvolq1	8100-SHX0991003G44MT	2/9/2017 13:55:53	3 Seconds
Manual backup	Succeeded	mybupolicy2	8100-SHX0991003G44MT	2/9/2017 13:53:03	1 Minute, 18 S
Scheduled backup	Succeeded	mybupolicy2	8100-SHX0991003G44MT	2/9/2017 13:30:03	4 Seconds

3. When prompted for confirmation, click **Yes**. This job is now canceled.

Next steps

- Learn how to [manage your StorSimple backup policies](#).
 - Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).
-

Additional resources

Training

Learning path

[Create jobs in Microsoft Dynamics 365 Business Central - Training](#)

Are you going to use jobs to track project costs with Business Central? This learning path discusses creating new jobs, using job planning lines, and job task lines.

Change the device mode on your StorSimple device

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article provides a brief description of the various modes in which your StorSimple device can operate. Your StorSimple device can function in three modes: normal, maintenance, and recovery.

After reading this article, you will know:

- What the StorSimple device modes are
- How to figure out which mode the StorSimple device is in
- How to change from normal to maintenance mode and *vice versa*

The above management tasks can only be performed via the Windows PowerShell interface of your StorSimple device.

About StorSimple device modes

Your StorSimple device can operate in normal, maintenance, or recovery mode. Each of these modes is briefly described below.

Normal mode

This is defined as the normal operational mode for a fully configured StorSimple device. By default, your device should be in normal mode.

Maintenance mode

Sometimes the StorSimple device may need to be placed into maintenance mode. This mode allows you to perform maintenance on the device and install disruptive updates, such as those related to disk firmware.

You can put the system into maintenance mode only via the Windows PowerShell for StorSimple. All I/O requests are paused in this mode. Services such as non-volatile random access memory (NVRAM) or the clustering service are also stopped. Both the controllers are restarted when you enter or exit this mode. When you exit the maintenance mode, all the services will resume and should be healthy. This may take a few minutes.

 **Note**

Maintenance mode is only supported on a properly functioning device. It is not supported on a device in which one or both of the controllers are not functioning.

Recovery mode

Recovery mode can be described as "Windows Safe Mode with network support". Recovery mode engages the Microsoft Support team and allows them to perform diagnostics on the system. The primary goal of recovery mode is to retrieve the system logs.

If your system goes into recovery mode, you should contact Microsoft Support for next steps. For more information, go to [Contact Microsoft Support](#).

 **Note**

You cannot place the device in recovery mode. If the device is in a bad state, recovery mode tries to get the device into a state in which Microsoft Support personnel can examine it.

Determine StorSimple device mode

To determine the current device mode

1. Log on to the device serial console by following the steps in [Use PuTTY to connect to the device serial console](#).

2. Look at the banner message in the serial console menu of the device. This message explicitly indicates whether the device is in maintenance or recovery mode. If the message does not contain any specific information pertaining to the system mode, the device is in normal mode.

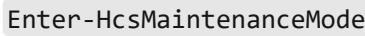
Change the StorSimple device mode

You can place the StorSimple device into maintenance mode (from normal mode) to perform maintenance or install maintenance mode updates. Perform the following procedures to enter or exit maintenance mode.

Important

Before entering maintenance mode, verify that both device controllers are healthy by accessing the **Device settings > Hardware health** for your device in the Azure portal. If one or both the controllers are not healthy, contact Microsoft Support for the next steps. For more information, go to [Contact Microsoft Support](#).

To enter maintenance mode

1. Log on to the device serial console by following the steps in [Use PuTTY to connect to the device serial console](#).
2. In the serial console menu, choose option 1, **Log in with full access**. When prompted, provide the **device administrator password**. The default password is: **Password1**.
3. At the command prompt, type

Enter-HcsMaintenanceMode
4. You will see a warning message telling you that maintenance mode will disrupt all I/O requests and sever the connection to the Azure portal, and you will be prompted for confirmation. Type **Y** to enter maintenance mode.
5. Both controllers will restart. When the restart is complete, the serial console banner will indicate that the device is in maintenance mode. A sample output is shown below.

```
-----  
Microsoft Azure StorSimple Appliance Model 8100  
Name: 8100-SHX0991003G44MT  
Software Version: 6.3.9600.17820  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller0 - Passive  
-----
```

```
Controller0>Enter-HcsMaintenanceMode  
Checking device state...
```

In maintenance mode, your device will not service IOs and will be disconnected from the Microsoft Azure StorSimple Manager service. Entering maintenance mode will end the current session and reboot both controllers, which takes a few minutes to complete. Are you sure you want to enter maintenance mode?

```
[Y] Yes [N] No (Default is "Y"): Y
```

```
<BOTH CONTROLLERS RESTART>
```

```
-----MAINTENANCE MODE-----  
Microsoft Azure StorSimple Appliance Model 8100  
Name: 8100-SHX0991003G44MT  
Software Version: 6.3.9600.17820  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller0 - Passive  
-----
```

```
Serial Console Menu  
[1] Log in with full access  
[2] Log into peer controller with full access  
[3] Connect with limited access  
[4] Change language  
Please enter your choice>
```

To exit maintenance mode

1. Log on to the device serial console. Verify from the banner message that your device is in maintenance mode.
2. At the command prompt, type:

```
Exit-HcsMaintenanceMode
```

3. A warning message and a confirmation message will appear. Type **Y** to exit maintenance mode.

4. Both controllers will restart. When the restart is complete, the serial console banner indicates that the device is in normal mode. A sample output is shown below.

```
-----MAINTENANCE MODE-----
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17820
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0
```

```
-----  
Controller0>Exit-HcsMaintenanceMode  
Checking device state...
```

Before exiting maintenance mode, ensure that any updates that are required on both controllers have been applied. Failure to install on each controller could result in data corruption. Exiting maintenance mode will end the current session and reboot both controllers, which takes a few minutes to complete. Are you sure you want to exit maintenance mode?

```
[Y] Yes [N] No (Default is "Y"): Y
```

```
<BOTH CONTROLLERS RESTART>
```

```
-----  
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17820
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active
```

```
-----  
Serial Console Menu
[1] Log in with full access
[2] Log into peer controller with full access
[3] Connect with limited access
[4] Change language
Please enter your choice>
```

Next steps

Learn how to [apply normal and maintenance mode updates](#) on your StorSimple device.

Use the StorSimple Device Manager service to change your StorSimple passwords

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Azure portal **Device settings** option contains all the device parameters that you can reconfigure on a StorSimple device that is managed by a StorSimple Device Manager service. This tutorial explains how you can use the **Security** option under **Device settings** to change your device administrator or StorSimple Snapshot Manager password.

Change the device administrator password

When you use Windows PowerShell interface to access the StorSimple device, you are required to enter a device administrator password. When the first StorSimple device is registered with a service, the default password for this interface is *Password1*. For the security of your data, you are required to change this password at the end of the registration process. You cannot exit from the registration process without changing this password. For more information, see [Step 3: Configure and register the device through Windows PowerShell for StorSimple](#).

The password that was first set through the Windows PowerShell interface during registration can be changed later via the Azure portal. Perform the following steps to change the device administrator password.

To change the device administrator password

1. Go to your StorSimple Device Manager service and click **Devices**.
2. From the tabular listing of devices, select and click the device whose password you intend to change.

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
MySS8000Device1	Online	8.64 TB/199.7 TB	Physical device	8100

3. In the **Settings** blade, go to **Device settings > Security**.

MySS8000Device1

Monitoring

Alerts - Past 7 days	Volumes
0 !	2
There are no alerts.	Online 2

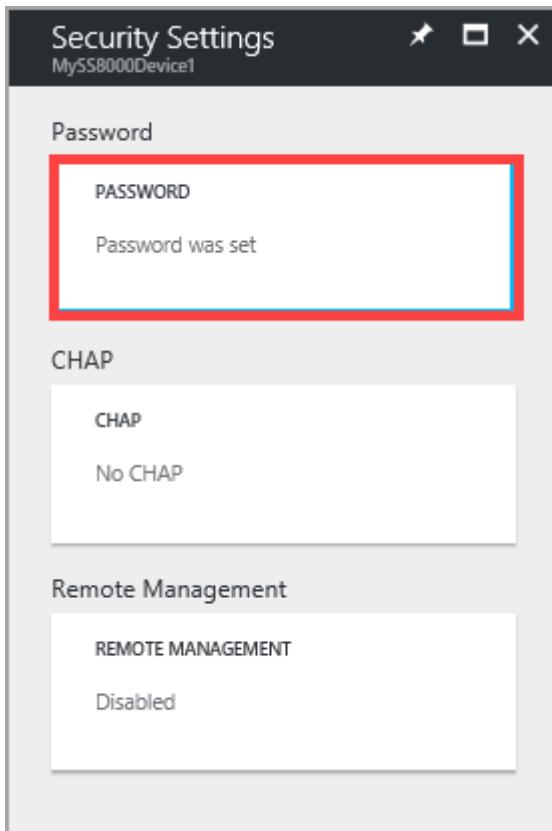
MySS8000Device1 - Usage - Past 24 hours

6 PM	Jan 19	6 AM	12 PM
PRIMARY TIERED STOR...	PRIMARY LOCALLY PINN...	CLOUD STORAGE USED	

Settings

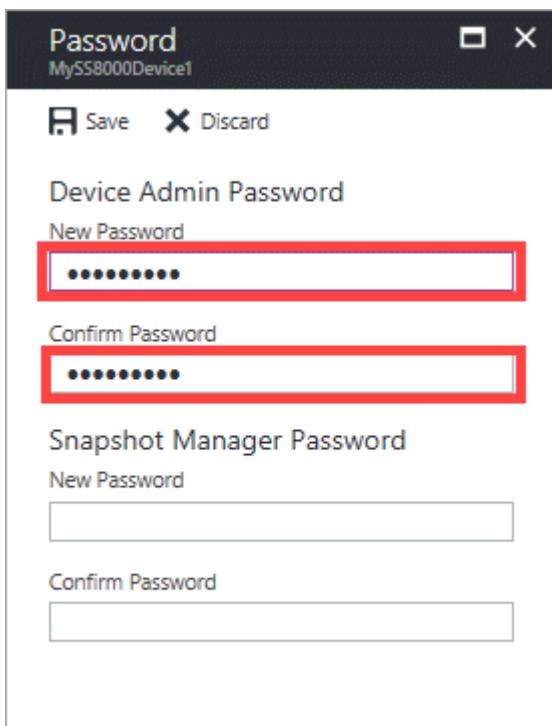
- GENERAL
- MONITOR
- Usage
- Jobs
- DEVICE SETTINGS
- Network
- Security

4. In the **Security settings** blade, click **Password** to change the device administrator password.

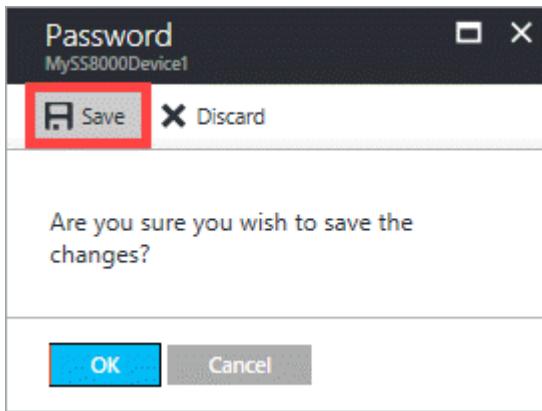


5. In the **Password** blade, provide an administrator password that contains from 8 to 15 characters. The password must be a combination of 3 or more of uppercase, lowercase, numeric, and special characters.

6. Confirm the password.



7. Click **Save** and when prompted for confirmation, click **Yes**.



The device administrator password should now be updated. You can use this modified password to access the Windows PowerShell interface.

Set the StorSimple Snapshot Manager password

StorSimple Snapshot Manager software resides on your Windows host and allows administrators to manage backups of your StorSimple device in the form of local and cloud snapshots.

When configuring a device in StorSimple Snapshot Manager, you will be prompted to provide the device IP address and password to authenticate your storage device.

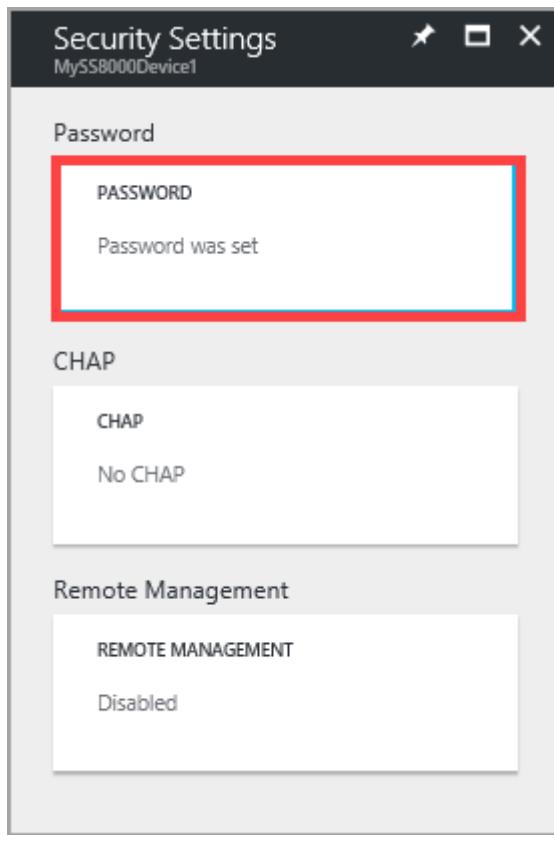
You can set or change the password for StorSimple Snapshot Manager via the Azure portal. Perform the following steps to set or change the StorSimple Snapshot Manager password.

To set the StorSimple Snapshot Manager password

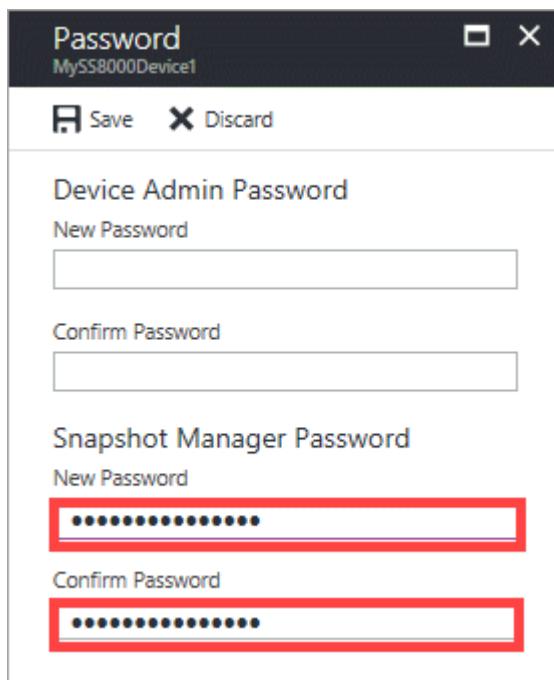
1. Go to your StorSimple Device Manager service and click **Devices**.
2. From the tabular listing of devices, select and click the device whose StorSimple Snapshot Manager password you intend to set or change.

3. In the Settings blade, go to Device settings > Security.

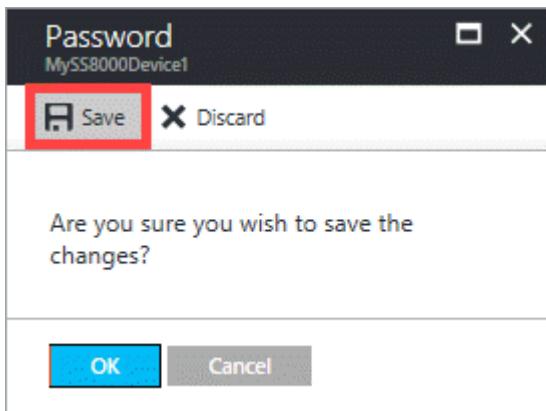
4. In the Security settings blade, click Password to set or change the StorSimple Snapshot Manager password.



5. In the **Password** blade, enter a password that is 14 or 15 characters. Make sure that the password contains a combination of 3 or more of uppercase, lowercase, numeric, and special characters.
6. Confirm the password.



7. Click **Save** and when prompted for confirmation, click **Yes**.



The StorSimple Snapshot Manager password should now be updated.

Next steps

- Learn more about [StorSimple security](#).
- Learn more about [modifying your device configuration](#).
- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to modify your StorSimple device configuration

Article • 08/19/2022 • 8 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Azure portal **Device settings** section in the **Settings** blade contains all the device parameters that you can reconfigure on a StorSimple device that is managed by a StorSimple Device Manager service. This tutorial explains how you can use the **Settings** blade to perform the following device-level tasks:

- Modify device friendly name
- Modify device time settings
- Assign a secondary DNS
- Modify network interfaces
- Swap or reassign IPs

Modify device friendly name

You can use the Azure portal to change the device name and assign it a unique friendly name of your choice. Use the **General settings** blade on your device to modify the device friendly name. The friendly name can contain any characters and can be a maximum of 64 characters long.

ⓘ Note

You can only modify the device name in the Azure portal before the device setup is complete. Once the minimum device setup is complete, you cannot change the device name.

The screenshot shows three windows side-by-side. The left window is the main device monitoring interface for '8100-SHX0991003G44MT'. It displays status information like 'Status: Online', 'Model: 8100', and 'Device software version: StorSimple 8000 Series Update 4.0'. The middle window is the 'Settings' blade, and the right window is the 'General settings' blade for the same device. Both the 'Device name' field (containing '8100-SHX0991003G44MT') and the 'General' item under 'DEVICE SETTINGS' are highlighted with red boxes.

A StorSimple device that is connected to the StorSimple Device Manager service is assigned a default name. The default name typically reflects the serial number of the device. For example, a default device name that is 15 characters long, such as 8600-SHX0991003G44HT, indicates the following:

- **8600** – Indicates the device model.
- **SHX** – Indicates the manufacturing site.
- **0991003** - Indicates a specific product.
- **G44HT**- The last 5 digits are incremented to create unique serial numbers. This might not be a sequential set.

Modify device description

Use the **General settings** blade on your device to modify the device description.

The screenshot shows two windows side-by-side. On the left is the 'Monitoring' blade for a device named '8100-SHX0991003G44MT'. It displays a timeline from 12 PM to 6 AM, showing usage for Primary Tiered Storage (0 GB), Primary Locally Pinned Storage (0 GB), and Cloud Storage Used (0.001 GB). The 'General' section shows the device is online and healthy. On the right is the 'General settings' blade, which includes sections for Device settings (Device name: 8100-SHX0991003G44MT), Time settings (Time zone: UTC-08:00 Pacific Standard Time), Alert settings, and Device settings. A red box highlights the 'Description' field in the Device settings section, and another red box highlights the 'General' link under Device settings.

A device description usually helps identify the owner and the physical location of the device. The description field must contain fewer than 256 characters.

Modify time settings

Your device must synchronize time in order to authenticate with your cloud storage service provider. Use the **General settings** blade on your device to modify the device time settings.

Select your time zone from the drop-down list. You can specify up to two Network Time Protocol (NTP) servers:

- **Primary NTP server** - The configuration is required and is specified when you use Windows PowerShell for StorSimple to configure your device. You can specify the default Windows Server `time.windows.com` as your NTP server. You can view the primary NTP server configuration through the Azure portal, but you must use the Windows PowerShell interface to change it. Use the `Set-HcsNTPClientServerAddress` cmdlet to modify the Primary NTP server of your device. For more information, go to [syntax for Set-HcsNTPClientServerAddress cmdlet](#).
- **Secondary NTP server** - The configuration is optional. You can use the portal to configure a secondary NTP server.

When configuring the NTP server, ensure that your network allows the NTP traffic to pass from your datacenter to the Internet. When specifying a public NTP server, you must make sure that your network firewalls and other security devices are configured to allow NTP traffic to travel to and from the outside network. If bidirectional NTP traffic is not permitted, you must use an internal NTP server (a Windows domain controller provides this function). If your device cannot synchronize time, it may not be able to communicate with your cloud storage provider.

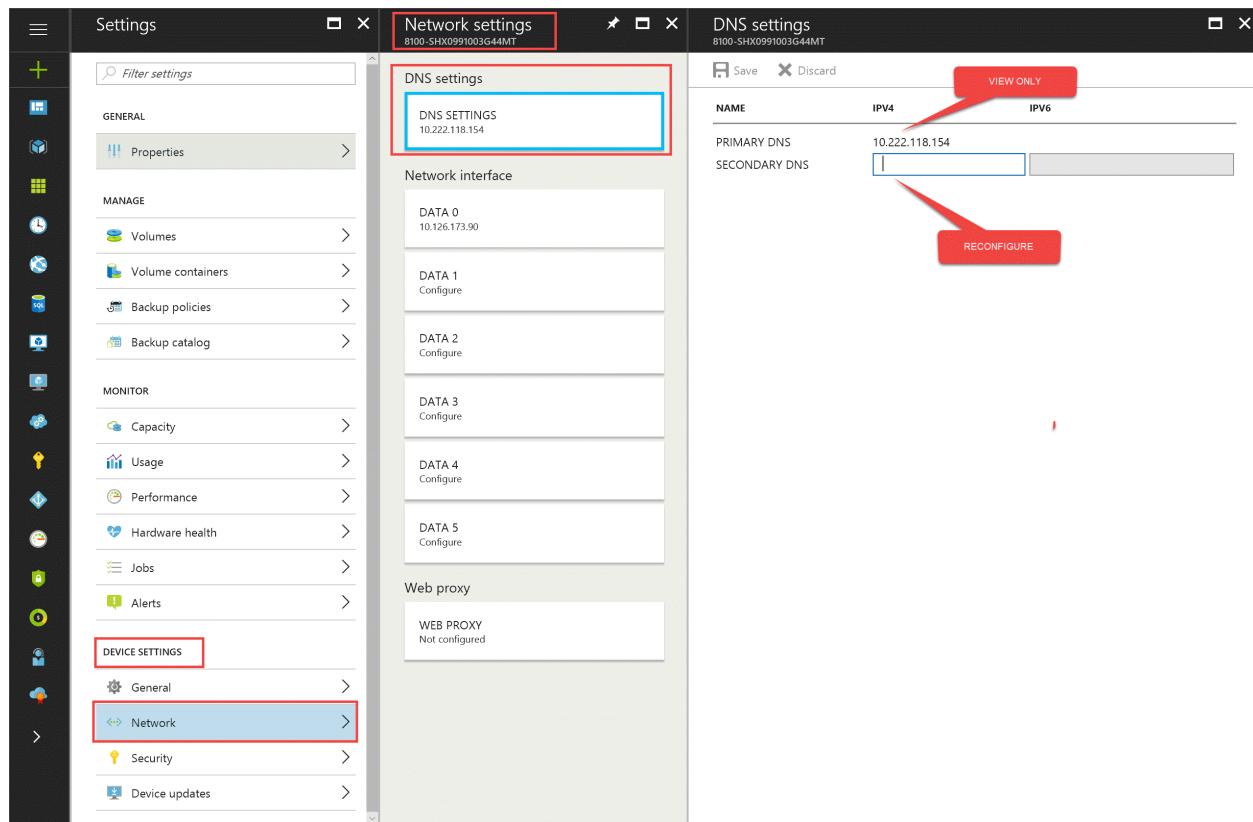
To see a list of public NTP servers, go to the [NTP Servers Web](#).

What happens if the device is deployed in a different time zone?

If the device is deployed in a different time zone, the device time zone will change. Given that all the backup policies use the device time zone, the backup policies will automatically adjust in accordance with the new time zone. No user intervention is required.

Modify DNS settings

A DNS server is used when your device attempts to communicate with your cloud storage service provider. Use the **Network settings** blade on your device to view and modify the configured DNS settings.



For high availability, you are required to configure both the primary and the secondary DNS servers during the initial device deployment.

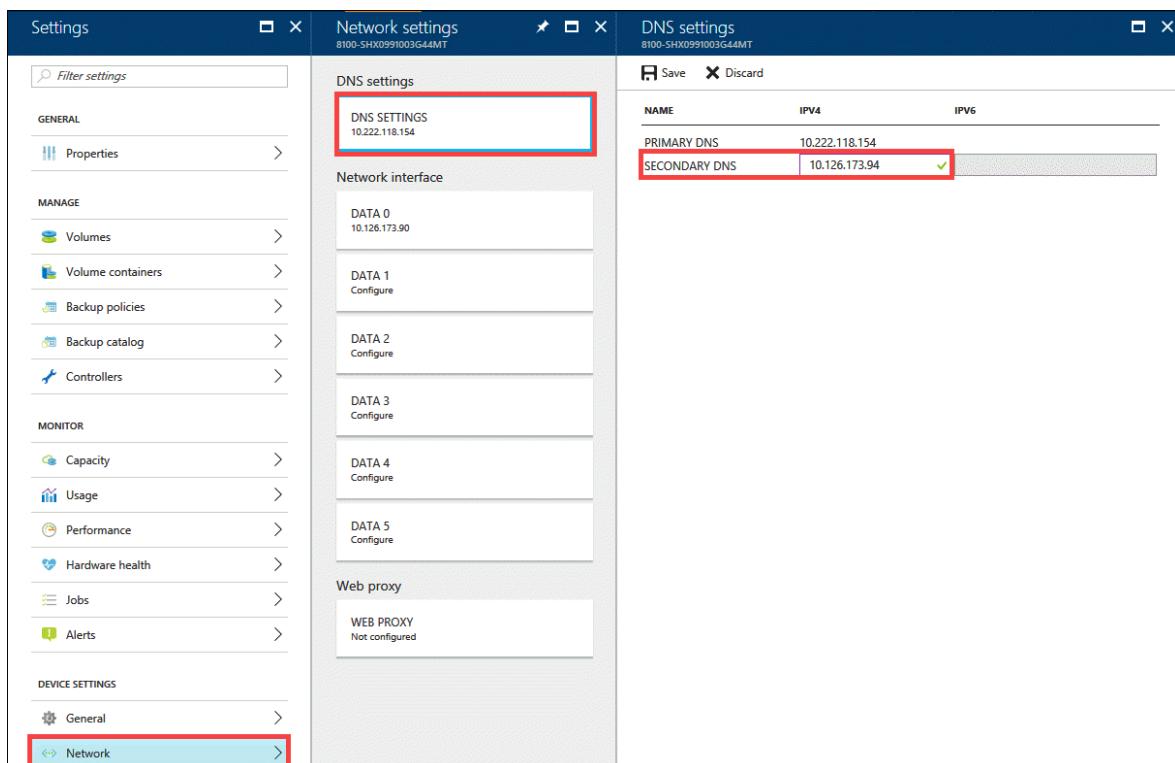
Primary DNS server - You use the Windows PowerShell for StorSimple to first specify the Primary DNS server during the initial setup. You can reconfigure the primary DNS server only via the Windows PowerShell interface. Use the `Set-`

`HcsDNSClientServerAddress` cmdlet to modify the primary DNS server of your device. For more information, go to syntax for `Set-HcsDNSClientServerAddress` cmdlet.

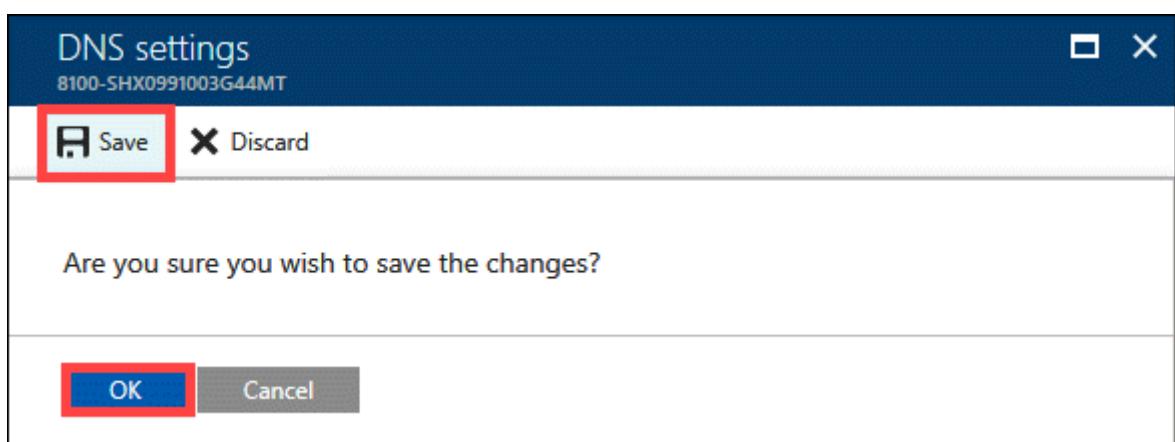
Secondary DNS server - To modify the secondary DNS server, use the `Set-HcsDNSClientServerAddress` cmdlet in the Windows PowerShell interface of the device or **Network settings** blade of your StorSimple device in the Azure portal.

To modify the secondary DNS server in Azure portal, perform the following steps.

1. Go to your StorSimple Device Manager service. From the list of devices, select and click your device.
2. In the **Settings** blade, go to **Device settings > Network**. This opens up the **Network settings** blade. Click **DNS settings** tile. Modify the secondary DNS server IP address.



3. From the command bar, click **Save** and when prompted for confirmation, click **OK**.



Modify network interfaces

Your device has six device network interfaces, four of which are 1 GbE and two of which are 10 GbE. These interfaces are labeled as DATA 0 – DATA 5. DATA 0, DATA 1, DATA 4, and DATA 5 are 1 GbE, whereas DATA 2 and DATA 3 are 10 GbE network interfaces.

Use the **Network settings** blade to configure each of the interfaces to be used.

The screenshot shows the 'Settings' interface on the left and the 'Network settings' blade on the right. The 'Network settings' blade displays DNS settings and a list of network interfaces (DATA 0 to DATA 5). The 'Network' option in the 'Device settings' menu is highlighted with a red box. The 'Network interface' section is also highlighted with a red box.

Settings

- GENERAL
 - Properties
- MANAGE
 - Volumes
 - Volume containers
 - Backup policies
 - Backup catalog
- MONITOR
 - Capacity
 - Usage
 - Performance
 - Hardware health
 - Jobs
 - Alerts
- DEVICE SETTINGS**
 - General
 - Network**
 - Security
 - Device updates

Network settings

DNS settings

DNS SETTINGS
10.222.118.154

Network interface

- DATA 0
10.126.173.90
- DATA 1
Configure
- DATA 2
Configure
- DATA 3
Configure
- DATA 4
Configure
- DATA 5
Configure

Web proxy

WEB PROXY
Not configured

To ensure high availability, we recommend that you have at least two iSCSI interfaces and two cloud-enabled interfaces on your device. We recommend but do not require that unused interfaces be disabled.

For each network interface, the following parameters are displayed:

- **Speed** – Not a user-configurable parameter. DATA 0, DATA 1, DATA 4, and DATA 5 are always 1 GbE, whereas DATA 2 and DATA 3 are 10 GbE interfaces.

 **Note**

Speed and duplex are always auto-negotiated. Jumbo frames are not supported.

- **Interface state** – An interface can be enabled or disabled. If enabled, the device will attempt to use the interface. We recommend that only those interfaces that are connected to the network and used be enabled. Disable any interfaces that you are not using.
- **Interface type** – This parameter allows you to isolate iSCSI traffic from cloud storage traffic. This parameter can be one of the following:
 - **Cloud enabled** – when enabled, the device will use this interface to communicate with the cloud.
 - **iSCSI enabled** – when enabled, the device will use this interface to communicate with the iSCSI host.

We recommend that you isolate iSCSI traffic from cloud storage traffic. Also note if your host is within the same subnet as your device, you do not need to assign a gateway; however, if your host is in a different subnet than your device, you will need to assign a gateway.

- **IP address** – When you configure any of the network interfaces, you must configure a virtual IP (VIP). This can be IPv4 or IPv6 or both. Both the IPv4 and IPv6 address families are supported for the device network interfaces. When using IPv4, specify a 32-bit IP address (xxx.xxx.xxx.xxx) in dot-decimal notation. When using IPv6, simply supply a 4-digit prefix, and a 128-bit address will be generated automatically for your device network interface based on that prefix.
- **Subnet** – This refers to the subnet mask and is configured via the Windows PowerShell interface.
- **Gateway** – This is the default gateway that should be used by this interface when it attempts to communicate with nodes that are not within the same IP address space (subnet). The default gateway must be in the same address space (subnet) as the interface IP address, as determined by the subnet mask.

- **Fixed IP address** – This field is available only while you configure the DATA 0 interface. For operations such as updates or troubleshooting the device, you may need to connect directly to the device controller. The fixed IP address can be used to access both the active and the passive controller on your device.

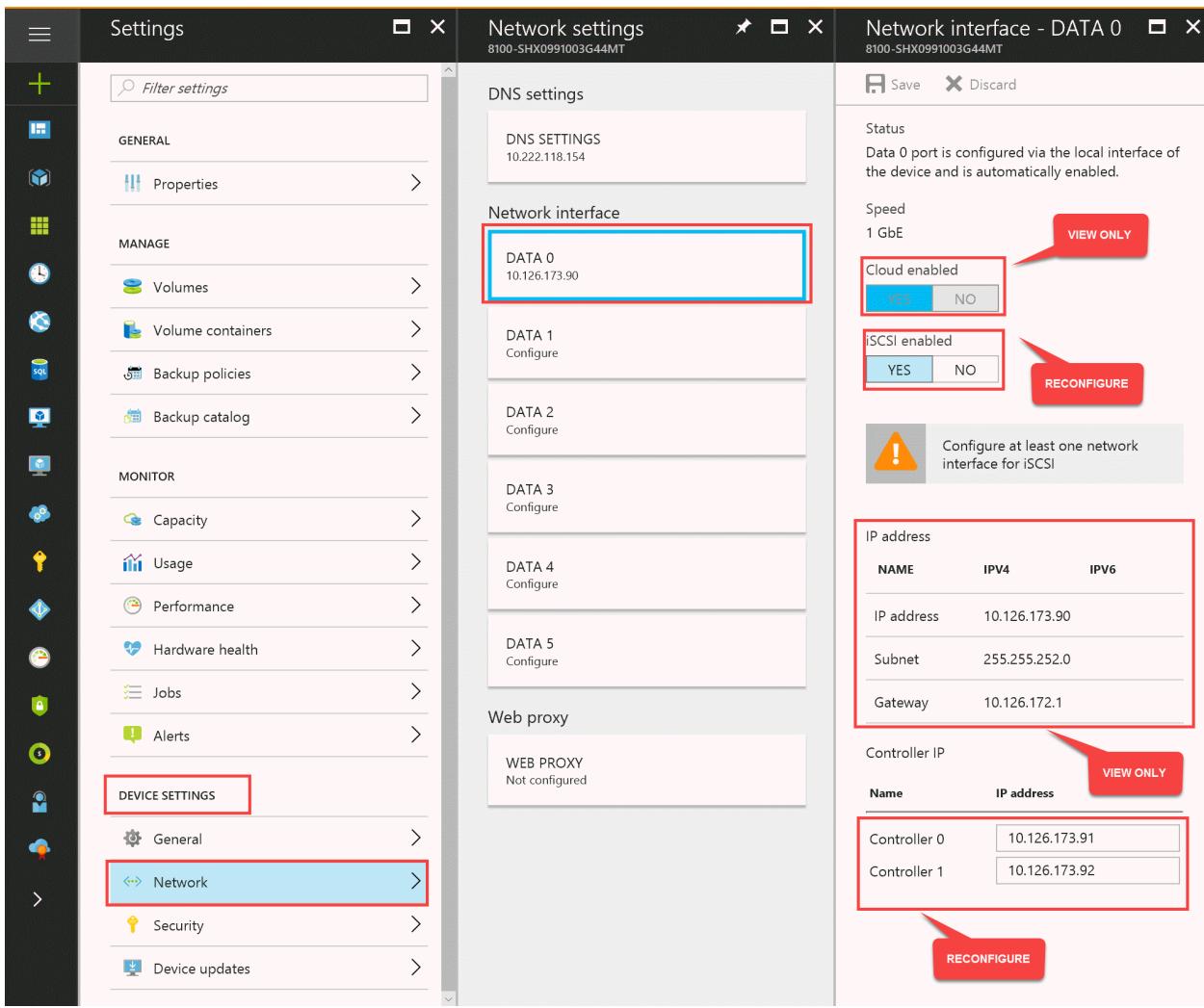
 **Note**

- To ensure proper operation, verify the interface speed and duplex on the switch that each device interface is connected to. Switch interfaces should either negotiate with or be configured for Gigabit Ethernet (1000 Mbps) and be full-duplex. Interfaces operating at slower speeds or in half-duplex will result in performance issues.
- To minimize disruptions and downtime, we recommend that you enable portfast on each of the switch ports that the iSCSI network interface of your device will be connecting to. This will ensure that network connectivity can be established quickly in the event of a failover.

Configure DATA 0

DATA 0 is cloud-enabled by default. When configuring DATA 0, you are also required to configure two fixed IP addresses, one for each controller. These fixed IP addresses can be used to access the device controllers directly and are useful when you install updates on the device, for garbage collection to work properly or when you access the controllers for the purpose of troubleshooting.

You can reconfigure the fixed IP controllers via the DATA 0 settings blade.

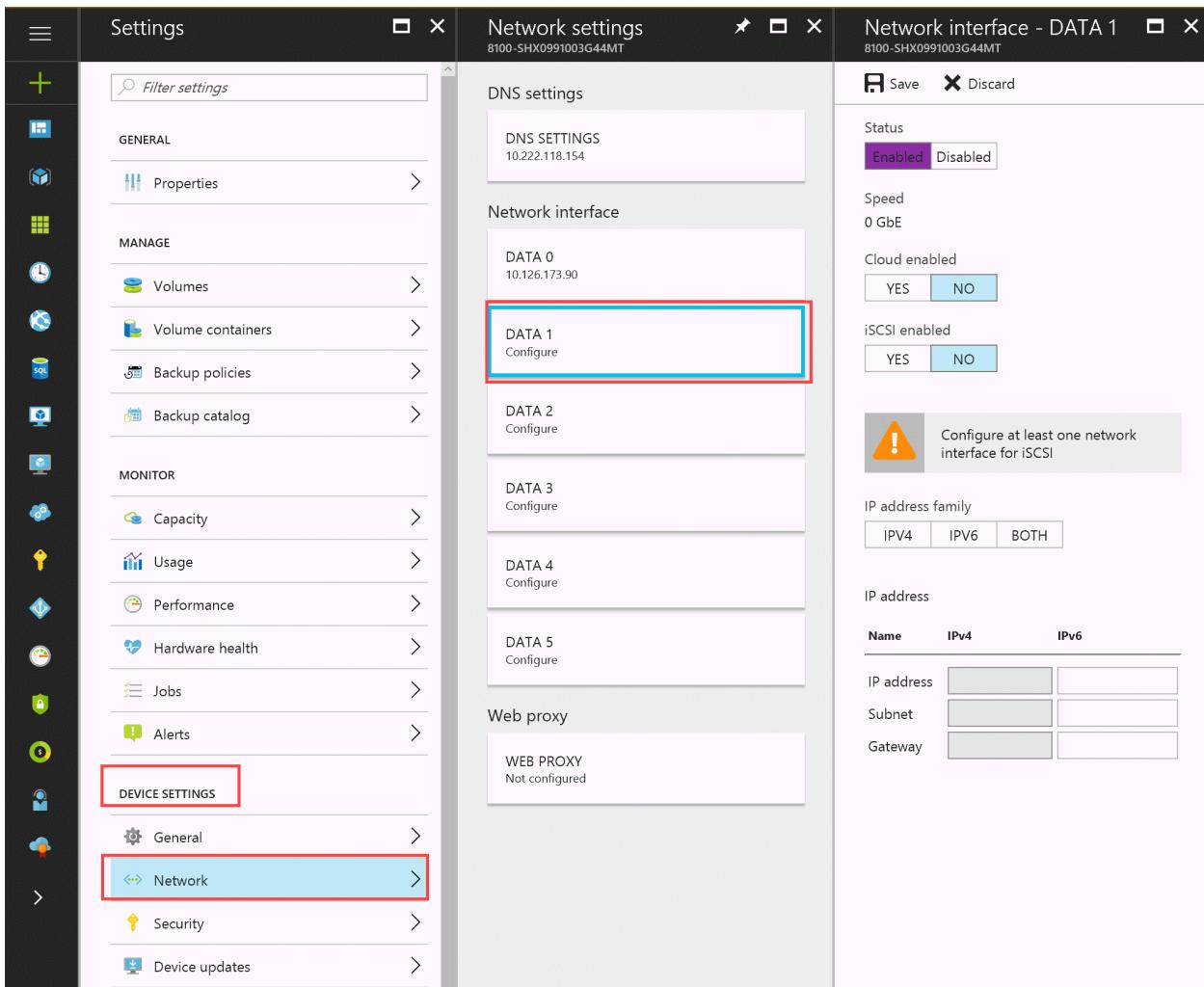


ⓘ Note

The fixed IP addresses for the controller are used for servicing the updates to the device and for space reclamation algorithms (garbage collection) to work properly. Therefore, the fixed IPs must be routable and able to connect to the Internet.

Configure DATA 1 - DATA 5

For DATA 1 - DATA 5 network interfaces, you can configure all the network settings as shown in the following screenshot:



Swap or reassign IPs

Currently, if any network interface on the controller is assigned a VIP that is in use (by the same device or another device in the network), then the controller will fail over. If you swap or reassign VIPs for a device network interface, you must follow a proper procedure as you could create a duplicate IP situation.

Perform the following steps to swap or reassign the VIPs for any of the network interfaces:

To reassign IPs

1. Clear the IP address for both interfaces.
2. After the IP addresses are cleared, assign the new IP addresses to the respective interfaces.

Next steps

- Learn how to [configure MPIO](#) for your StorSimple device.

- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Turn on or turn off your StorSimple 8000 series device

Article • 08/22/2022 • 12 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Shutting down a Microsoft Azure StorSimple device is not required as a part of normal system operation. However, you may need to turn on a new device or a device that had to be shut down. Generally, a shutdown is required in cases in which you must replace failed hardware, physically move a unit, or take a device out of service. This tutorial describes the required procedure for turning on and shutting down your StorSimple device in different scenarios.

Turn on a new device

The steps for turning on a StorSimple device for the first time differ depending on whether the device is an 8100 or an 8600 model. The 8100 has a single primary enclosure, whereas the 8600 is a dual-enclosure device with a primary enclosure and an EBOD enclosure. The detailed steps for both models are covered in the following sections.

- [New device with primary enclosure only](#)
- [New device with EBOD enclosure](#)

New device with primary enclosure only

The StorSimple 8100 model is a single enclosure device. Your device includes redundant Power and Cooling Modules (PCMs). Both PCMs must be installed and connected to

different power sources to ensure high availability.

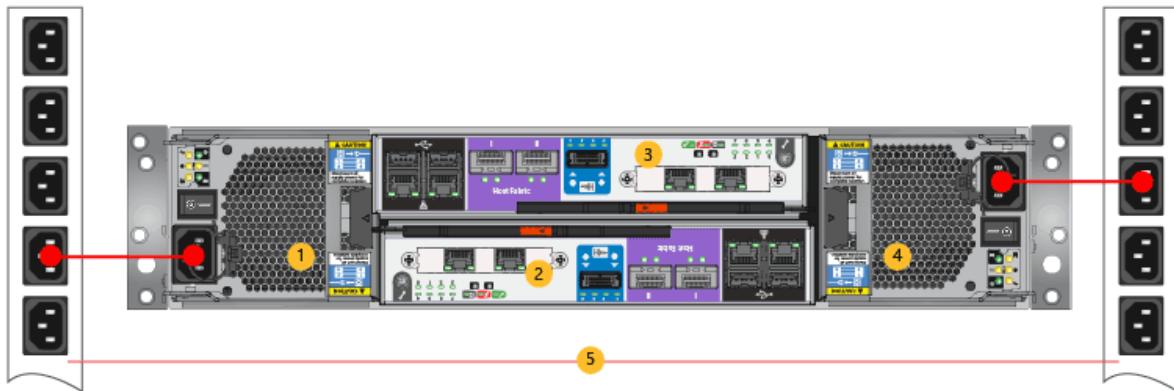
Perform the following steps to cable your device for power.

To cable for power

1. Make sure that the power switches on each of the Power and Cooling Modules (PCMs) are in the OFF position.
2. Connect the power cords to each of the PCMs in the primary enclosure.
3. Attach the power cords to the rack power distribution units (PDUs) as shown in the following image. Make sure that the two PCMs use separate power sources.

Important

To ensure high availability for your system, we recommend that you strictly adhere to the power cabling scheme shown in the following diagram.



Power cabling on an 8100 device

Label	Description
1	PCM 0
2	Controller 1
3	Controller 0
4	PCM 1
5	PDUs

4. To turn on the system, flip the power switches on both PCMs to the ON position.

Note

For complete device setup and cabling instructions, go to [Install your StorSimple 8100 device](#). Make sure that you follow the instructions exactly.

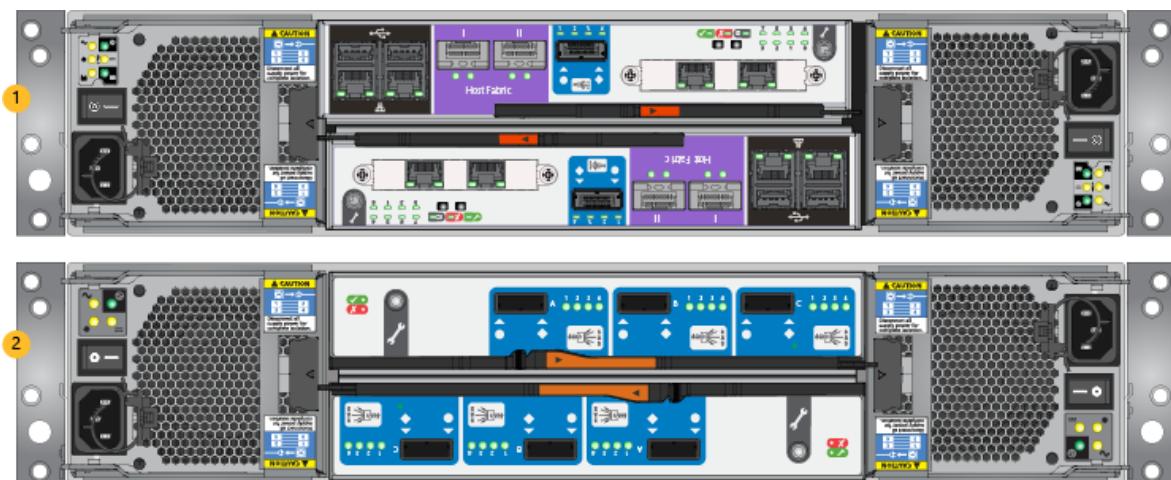
New device with EBOD enclosure

The StorSimple 8600 model has both a primary enclosure and an EBOD enclosure. This requires the units to be cabled together for Serial Attached SCSI (SAS) connectivity and power.

When setting up this device for the first time, perform the steps for SAS cabling first and then complete the steps for power cabling.

To attach the SAS cables

1. Identify the primary and the EBOD enclosures. The two enclosures can be identified by looking at their respective back planes. See the following image for guidance.

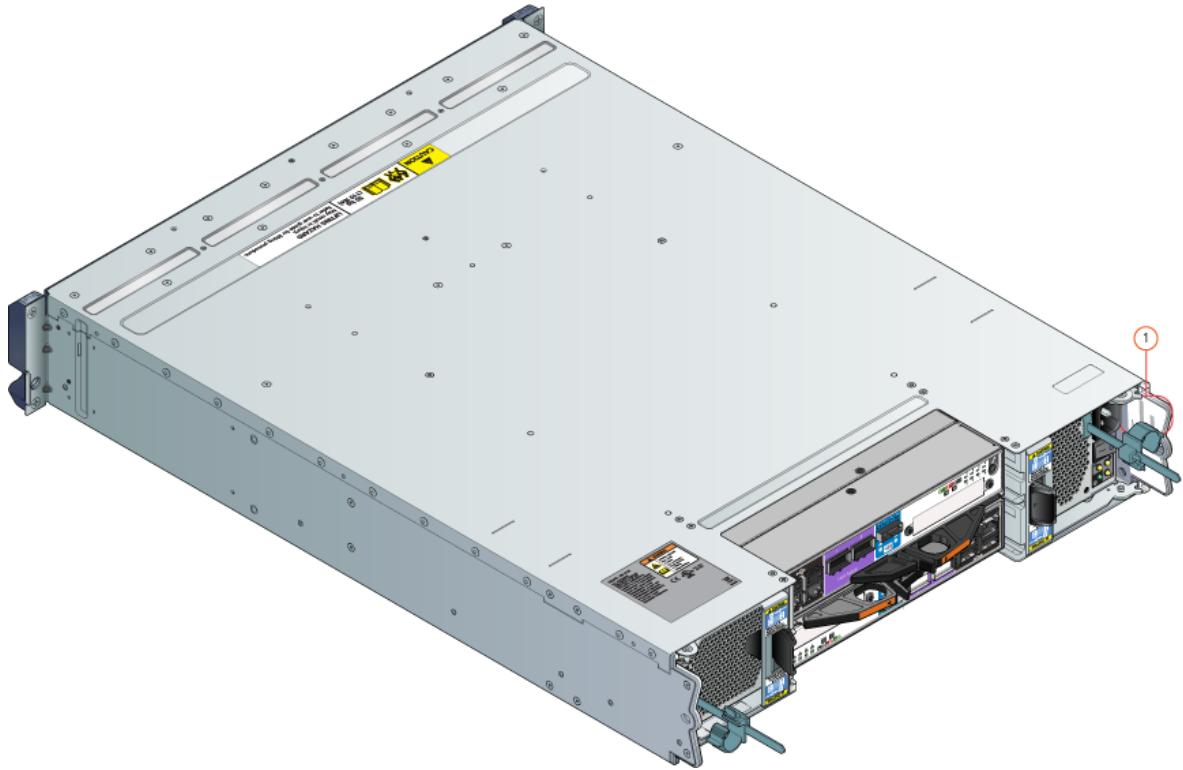


Back view of primary and EBOD enclosures

Label	Description
1	Primary enclosure
2	EBOD enclosure

2. Locate the serial numbers on the primary and the EBOD enclosures. The serial number sticker is affixed to the back ear of each enclosure. The serial numbers must be identical on both enclosures. [Contact Microsoft Support](#) immediately if

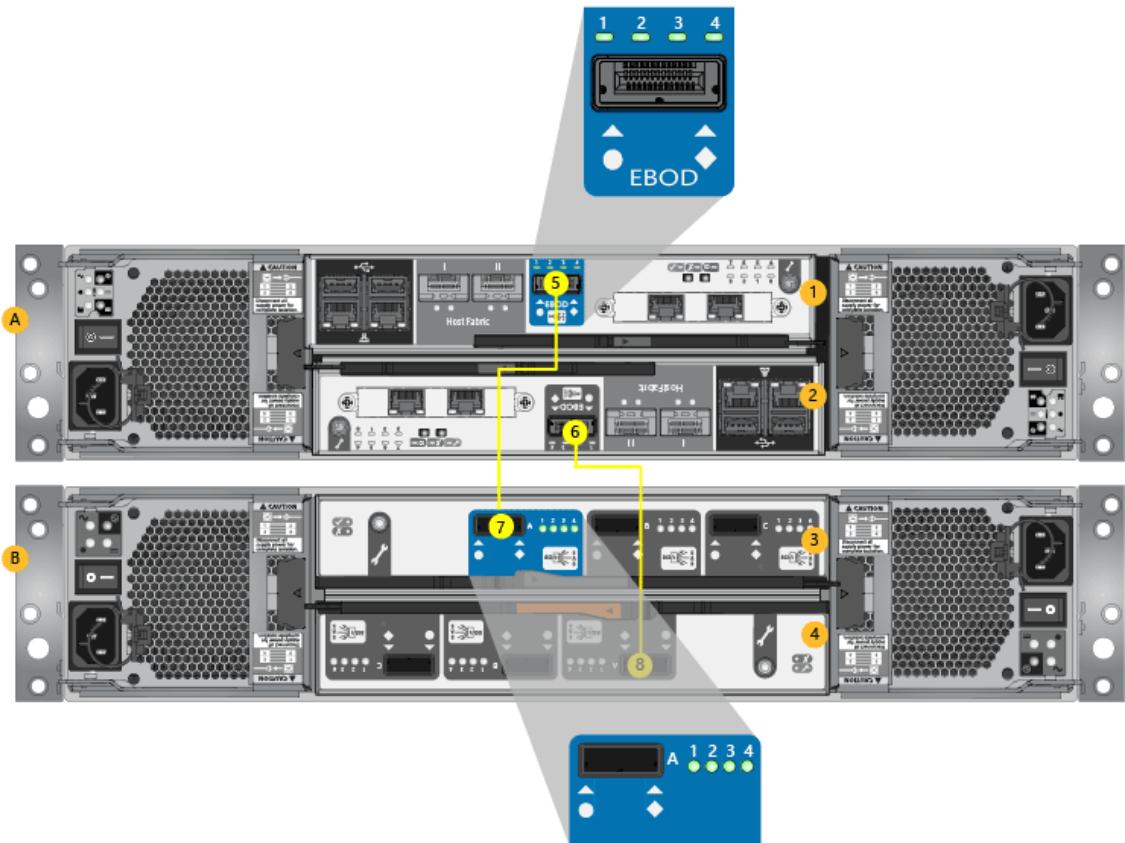
the serial numbers do not match. See the following illustration to locate the serial numbers.



Location of serial number sticker

Label	Description
1	Ear of the enclosure

3. Use the provided SAS cables to connect the EBOD enclosure to the primary enclosure as follows:
 - a. Identify the four SAS ports on the primary enclosure and the EBOD enclosure. The SAS ports are labeled as EBOD on the primary enclosure and correspond to port A on the EBOD enclosure, as shown in the SAS cabling illustration, below.
 - b. Use the provided SAS cables to connect the EBOD port to port A.
 - c. The EBOD port on controller 0 should be connected to the port A on EBOD controller 0. The EBOD port on controller 1 should be connected to the port A on EBOD controller 1. See the following illustration for guidance.



SAS cabling

Label	Description
A	Primary enclosure
B	EBOD enclosure
1	Controller 0
2	Controller 1
3	EBOD Controller 0
4	EBOD Controller 1
5, 6	SAS ports on primary enclosure (labeled EBOD)
7, 8	SAS ports on EBOD enclosure (Port A)

To cable your device for power

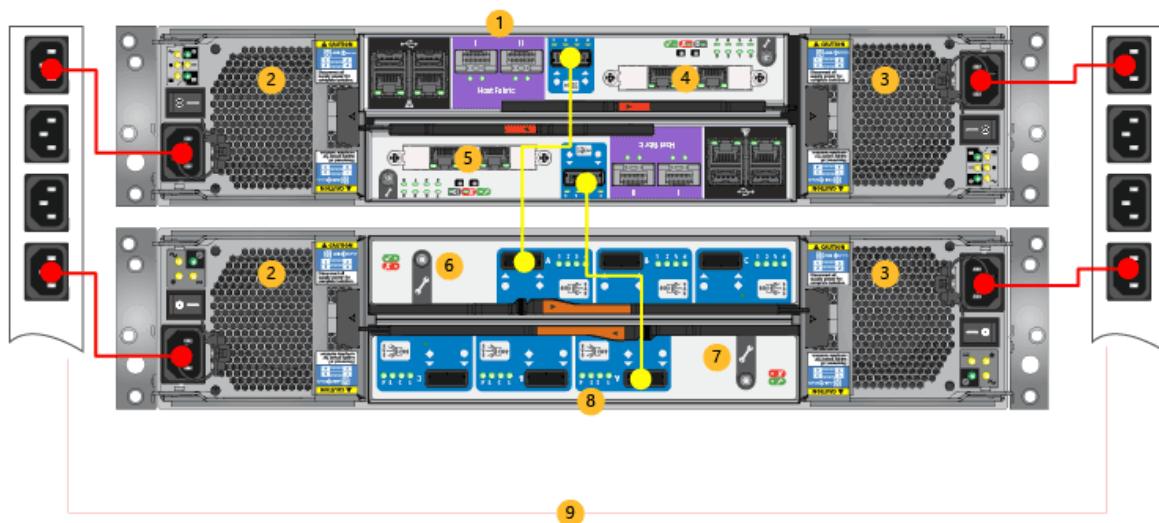
Note

Both enclosures on your StorSimple device include redundant PCMs. For each enclosure, the PCMs must be installed and connected to different power sources to ensure high availability.

1. Make sure that the power switches on all the PCMs are in the OFF position.
2. On the primary enclosure, connect the power cords to both PCMs. The power cords are identified in red in the power cabling diagram, below.
3. Make sure that the two PCMs on the primary enclosure use separate power sources.
4. Attach the power cords to the power on the rack distribution units as shown in the power cabling diagram.
5. Repeat steps 2 through 4 for the EBOD enclosure.
6. Turn on the EBOD enclosure by flipping the power switch on each PCM to the ON position.
7. Verify that the EBOD enclosure is turned on by checking that the green LEDs on the back of the EBOD controller are turned ON.
8. Turn on the primary enclosure by flipping each PCM switch to the ON position.
9. Verify that the system is on by ensuring the device controller LEDs have turned ON.
10. Make sure that the connection between the EBOD controller and the device controller is active by verifying that the four LEDs next to the SAS port on the EBOD controller are green.

ⓘ Important

To ensure high availability for your system, we recommend that you strictly adhere to the power cabling scheme shown in the following diagram.



Power cabling

Label	Description
1	Primary enclosure
2	PCM 0
3	PCM 1
4	Controller 0
5	Controller 1
6	EBOD controller 0
7	EBOD controller 1
8	EBOD enclosure
9	PDUs

 **Note**

For complete device setup and cabling instructions, go to [Install your StorSimple 8600 device](#). Make sure that you follow the instructions exactly.

Turn on a device after shutdown

The steps for turning on a StorSimple device after it has been shut down are different depending on whether the device is an 8100 or an 8600 model. The 8100 has a single primary enclosure, whereas the 8600 is a dual-enclosure device with a primary enclosure and an EBOD enclosure.

- Device with primary enclosure only
- Device with EBOD enclosure

Device with primary enclosure only

After a shutdown, use the following procedure to turn on a StorSimple device with a primary enclosure and no EBOD enclosure.

To turn on a device with a primary enclosure only

1. Make sure that the power switches on both Power and Cooling Modules (PCMs) are in the OFF position. If the switches are not in the OFF position, then flip them to the OFF position and wait for the lights to go off.
2. Turn on the device by flipping the power switches on both PCMs to the ON position. The device should turn on.
3. Check the following to verify that the device is fully on:
 - a. The OK LEDs on both PCM modules are green.
 - b. The status LEDs on both controllers are solid green.
 - c. The blue LED on one of the controllers is blinking, which indicates that the controller is active.

If any of these conditions are not met, then your device is not healthy. Please [contact Microsoft Support](#).

Device with EBOD enclosure

After a shutdown, use the following procedure to turn on a StorSimple device with a primary enclosure and an EBOD enclosure. Perform each step in sequence exactly as described. Failure to do so could result in data loss.

To turn on a device with a primary and an EBOD enclosure

1. Make sure that the EBOD enclosure is connected to the primary enclosure. For more information, see [Install your StorSimple 8600 device](#).
2. Make sure that the Power and Cooling Modules (PCMs) on both the EBOD and primary enclosures are in the OFF position. If the switches are not in the OFF position, then flip them to the OFF position and wait for the lights to go off.
3. Turn on the EBOD enclosure first by flipping the power switches on both PCMs to the ON position. The PCM LEDs should be green. A green EBOD controller LED on this unit indicates that the EBOD enclosure is on.
4. Turn on the primary enclosure by flipping the power switches on both PCMs to the ON position. The entire system should now be on.
5. Verify that the SAS LEDs are green, which ensures that the connection between the EBOD enclosure and the primary enclosure is good.

Turn on a device after a power loss

A power outage or interruption can shut down a StorSimple device. The power outage can happen on one of the power supplies or both power supplies. The recovery steps are different depending on whether the device is an 8100 or an 8600 model. The 8100 has a single primary enclosure, whereas the 8600 is a dual-enclosure device with a primary enclosure and an EBOD enclosure. This section describes the recovery procedure for each scenario.

- [Device with primary enclosure only](#)
- [Device with EBOD enclosure](#)

Device with primary enclosure only

The system can continue its normal operation if there is power loss to one of its power supplies. However, to ensure high availability of the device, restore power to the power supply as soon as possible.

If there is a power outage or power interruption on both power supplies, the system will shut down in an orderly and controlled manner. When the power is restored, the system will automatically turn on.

Device with EBOD enclosure

Power loss on one power supply

The system can continue its normal operation if there is power loss to one of its power supplies on the primary enclosure or the EBOD enclosure. However, to ensure high availability of the device, please restore power to the power supply as soon as possible.

Power loss on both power supplies on primary and EBOD enclosures

If there is a power outage or power interruption on both power supplies, the EBOD enclosure will shut down immediately and the primary enclosure will shut down in an orderly and controlled manner. When power is restored, the appliance will start automatically.

If the power is switched off manually, then take the following steps to restore power to the system.

1. Turn on the EBOD enclosure.
2. After the EBOD enclosure is on, turn on the primary enclosure.

Power loss on both power supplies on EBOD enclosure

When you set up your cables, you must ensure that the EBOD is never connected alone to a separate PDU. If the EBOD and primary enclosure fail at the same time, the system will recover.

If only the EBOD enclosure fails on both power supplies, the system will not automatically recover. Take the following steps to turn on the system and restore it to a healthy state:

1. If the primary enclosure is turned on, switch off both Power and Cooling Modules (PCMs).
2. Wait for a few minutes for the system to shut down.
3. Turn on the EBOD enclosure.
4. After the EBOD enclosure is on, turn on the primary enclosure.

Turn on a device after the primary and EBOD enclosure connection is lost

If the connection is lost between the standby controller and the corresponding EBOD controller, the device continues to work. If the connection between the system active controller and the corresponding EBOD controller is lost, failover should occur and the device should continue to work as normal.

When both Serial Attached SCSI (SAS) cables are removed or the connection between the EBOD enclosure and the primary enclosure is severed, the device will stop working. At this point, perform the following steps.

To turn on the device after connection is lost

1. Access the back of the device.
2. If the SAS cable connection between the EBOD enclosure and the primary enclosure is broken, all SAS lane LEDs on the EBOD enclosure will be off.
3. Shut down both Power and Cooling Modules (PCMs) on the EBOD enclosure and the primary enclosure.
4. Wait until all the lights on the back of both the enclosures turn off.
5. Reinsert the SAS cables, and ensure that there is a good connection between the EBOD enclosure and the primary enclosure.
6. Turn on the EBOD enclosure first by flipping both PCM switches to the ON position.
7. Ensure that the EBOD enclosure is on by checking that the green LED is ON.

8. Turn on the primary enclosure.
9. Ensure that the primary enclosure is on by checking that the controller green LED is ON.
10. Verify that the EBOD enclosure connection with the primary enclosure is good by checking that the SAS lane LEDs (four per EBOD controller) are all ON.

 **Important**

If the SAS cables are defective or the connection between the EBOD enclosure and the primary enclosure is not good, when you turn on the system, it will go into recovery mode. Please [contact Microsoft Support](#) if this happens.

Turn off a running device

A running StorSimple device may need to be shut down if it is being moved, taken out of service, or has a malfunctioning component that needs to be replaced. The steps are different depending on whether the StorSimple device is an 8100 or an 8600 model. The 8100 has a single primary enclosure, whereas the 8600 is a dual-enclosure device with a primary enclosure and an EBOD enclosure. This section details the steps to shut down a running device.

- [Device with primary enclosure](#)
- [Device with EBOD enclosure](#)

Device with primary enclosure

To shut down the device in an orderly and controlled manner, you can do it through the Azure portal or via the Windows PowerShell for StorSimple.

 **Important**

Do not shut down a running device by using the power button on the back of the device.

Before shutting down the device, make sure that all the device components are healthy. In the Azure portal, navigate to **Devices > Monitor > Hardware health**, and verify that status of all the components is green. This is true only for a healthy system. If the system is being shut down to replace a malfunctioning component, you will see a failed (red) or degraded (yellow) status for the respective component in the **Hardware Status**.

After you access the Windows PowerShell for StorSimple or the Azure portal, follow the steps in [shut down a StorSimple device](#).

Device with EBOD enclosure

Important

Before shutting down the primary enclosure and the EBOD enclosure, ensure that all the device components are healthy. In the Azure portal, navigate to **Devices > Monitor > Hardware health**, and verify that all the components are healthy.

To shut down a running device with EBOD enclosure

1. Follow all the steps listed in [shut down a StorSimple device](#) for the primary enclosure.
2. After the primary enclosure is shut down, shut down the EBOD by flipping off both Power and Cooling Module (PCM) switches.
3. To verify that the EBOD has shut down, check that all lights on the back of the EBOD enclosure are off.

Note

The SAS cables that are used to connect the EBOD enclosure to the primary enclosure should not be removed until after the system is shut down.

Next steps

[Contact Microsoft Support](#) if you encounter problems when turning on or shutting down a StorSimple device.

Configure Multipath I/O for your StorSimple device

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This tutorial describes the steps you should follow to install and use the Multipath I/O (MPIO) feature on a host running Windows Server 2012 R2 and connected to a StorSimple physical device. The guidance in this article applies to StorSimple 8000 series physical devices only. MPIO is currently not supported on a StorSimple Cloud Appliance.

Microsoft built support for the Multipath I/O (MPIO) feature in Windows Server to help build highly available, fault-tolerant iSCSI network configurations. MPIO uses redundant physical path components — adapters, cables, and switches — to create logical paths between the server and the storage device. If there is a component failure, causing a logical path to fail, multipathing logic uses an alternate path for I/O so that applications can still access their data. Additionally depending on your configuration, MPIO can also improve performance by rebalancing the load across all these paths. For more information, see [MPIO overview](#).

For the high-availability of your StorSimple solution, MPIO should be configured on your StorSimple device. When MPIO is installed on your host servers running Windows Server 2012 R2, the servers can then tolerate a link, network, or interface failure.

MPIO configuration summary

MPIO is an optional feature on Windows Server and is not installed by default. It should be installed as a feature through Server Manager.

Follow these steps to configure MPIO on your StorSimple device:

- Step 1: Install MPIO on the Windows Server host

- Step 2: Configure MPIO for StorSimple volumes
- Step 3: Mount StorSimple volumes on the host
- Step 4: Configure MPIO for high availability and load balancing

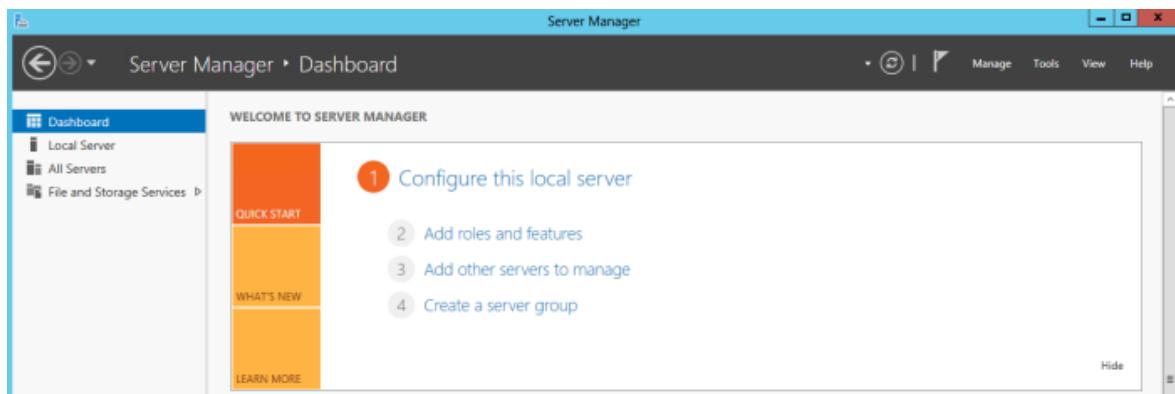
Each of the preceding steps is discussed in the following sections.

Step 1: Install MPIO on the Windows Server host

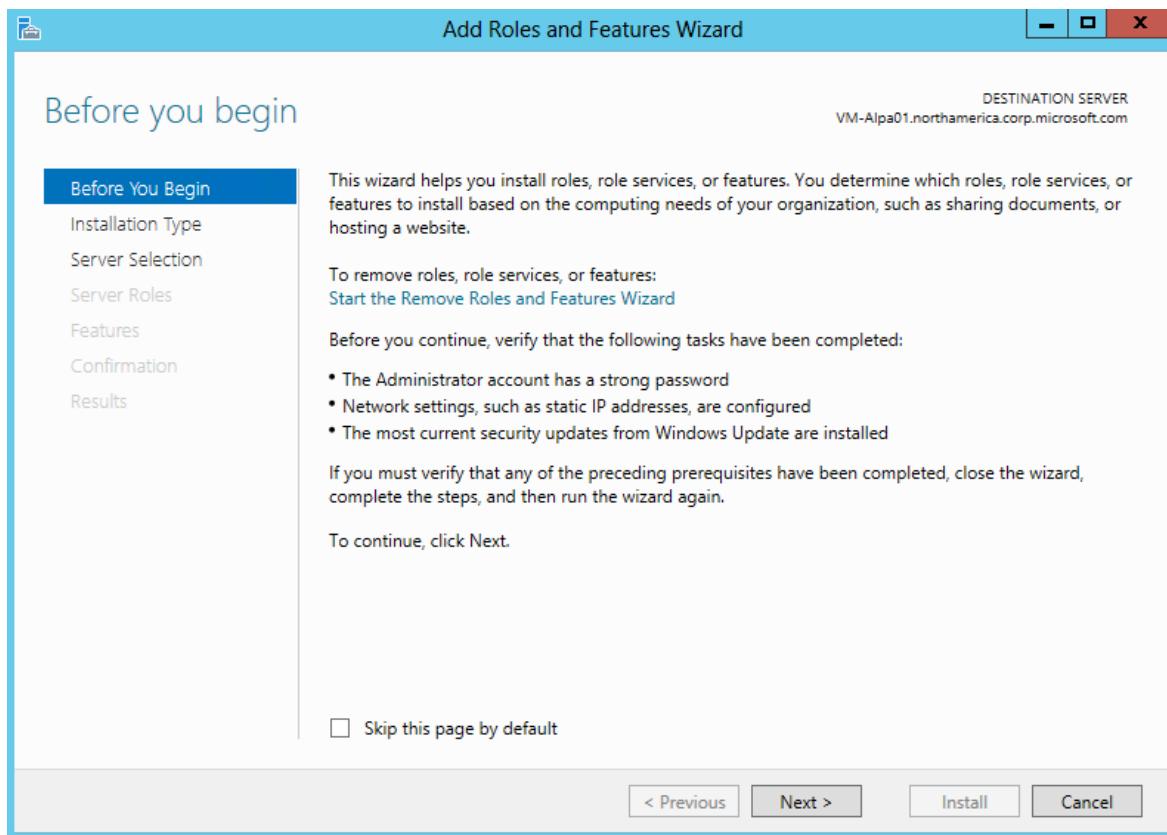
To install this feature on your Windows Server host, complete the following procedure.

To install MPIO on the host

1. Open Server Manager on your Windows Server host. By default, Server Manager starts when a member of the Administrators group logs on to a computer that is running Windows Server 2012 R2 or Windows Server 2012. If the Server Manager is not already open, click **Start > Server Manager**.

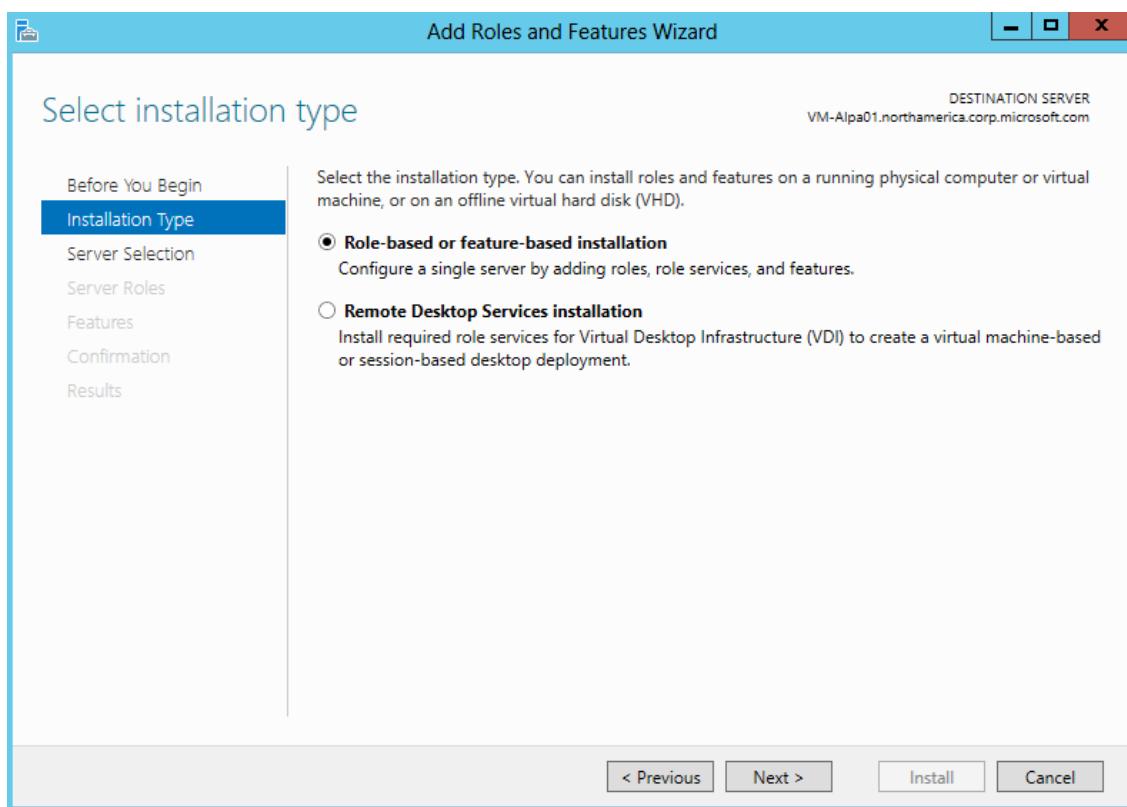


2. Click **Server Manager > Dashboard > Add roles and features**. This starts the **Add Roles and Features** wizard.

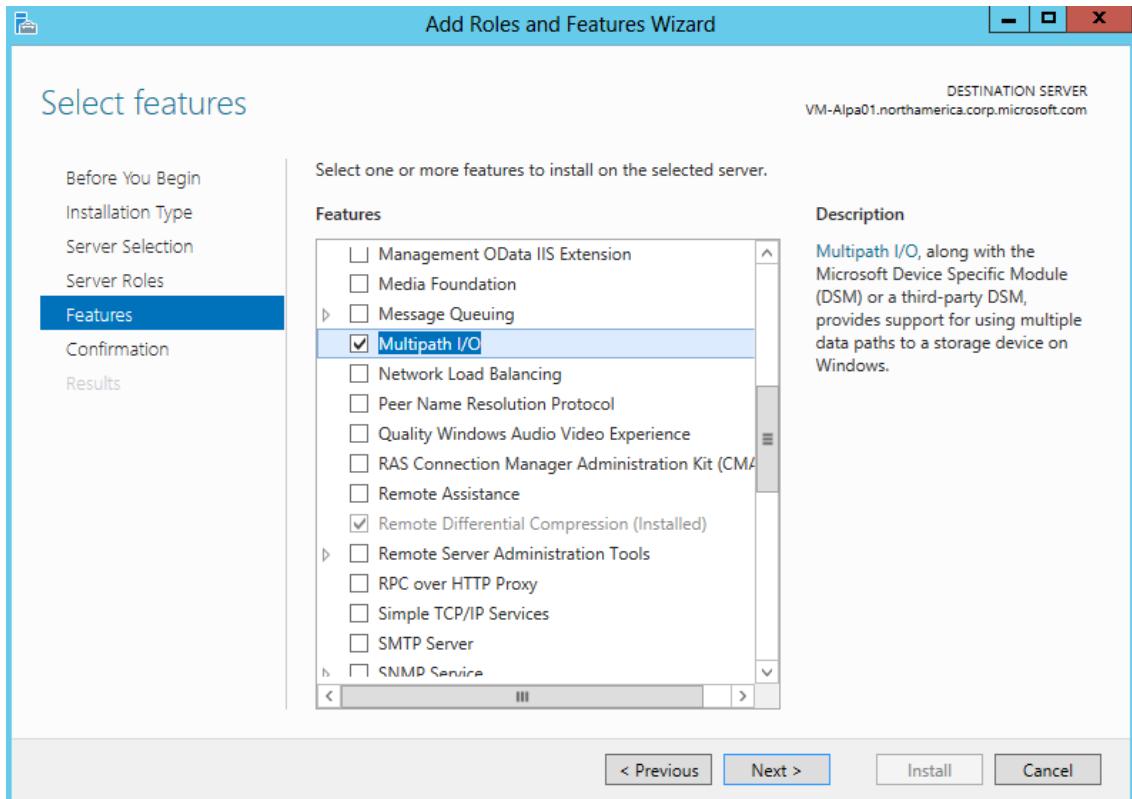


3. In the Add Roles and Features wizard, perform the following steps:

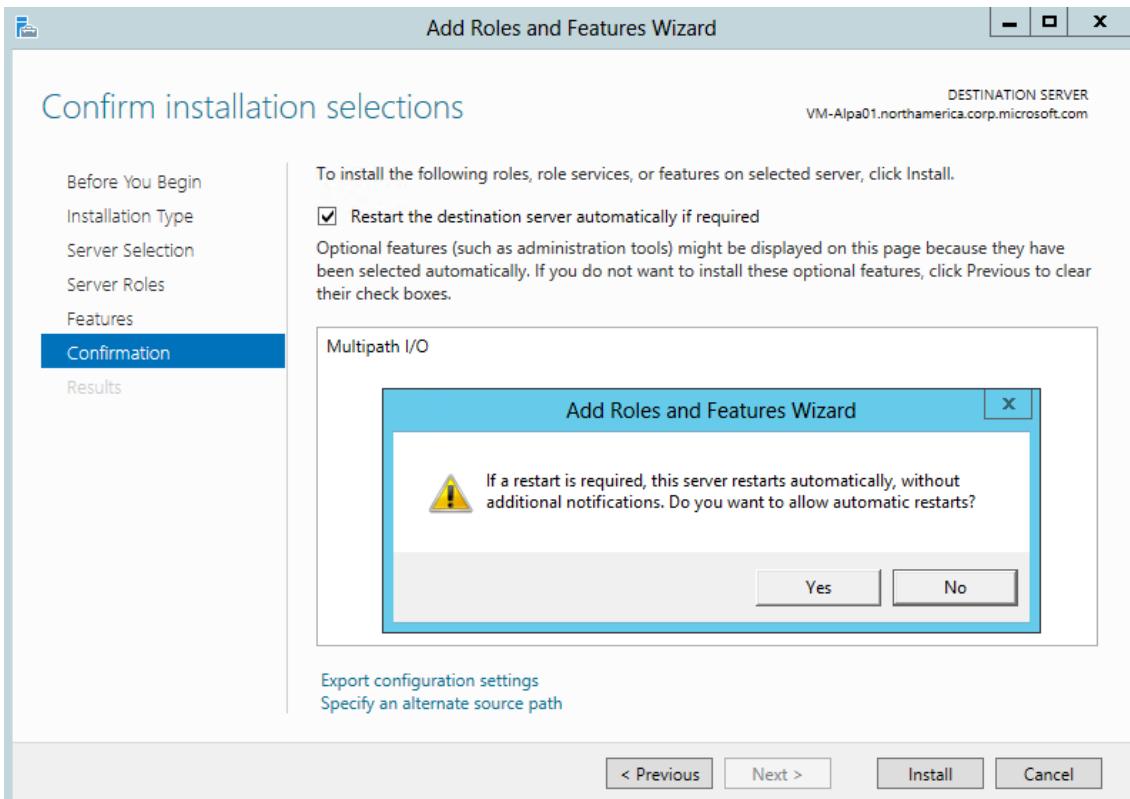
- On the **Before you begin** page, click **Next**.
- On the **Select installation type** page, accept the default setting of **Role-based or feature-based installation**. Click **Next**.



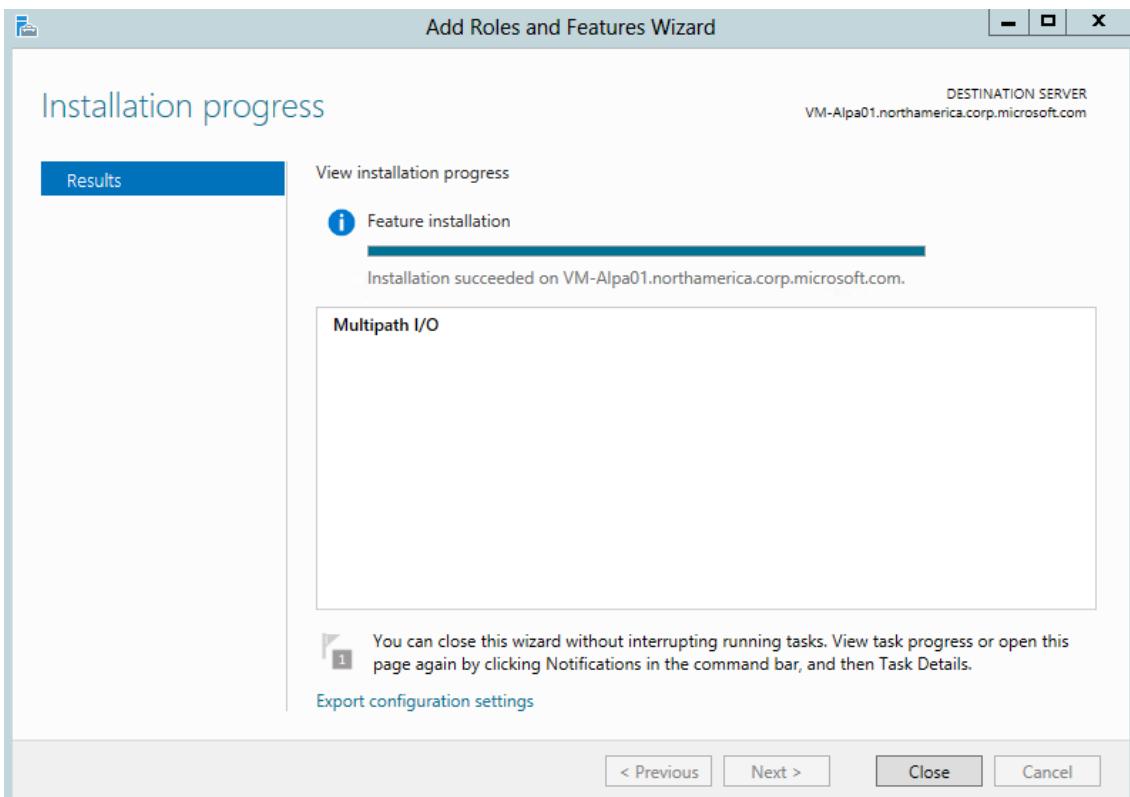
- c. On the **Select destination server** page, choose **Select a server from the server pool**. Your host server should be discovered automatically. Click **Next**.
- d. On the **Select server roles** page, click **Next**.
- e. On the **Select features** page, select **Multipath I/O**, and click **Next**.



- f. On the **Confirm installation selections** page, confirm the selection, and then select **Restart the destination server automatically if required**, as shown below. Click **Install**.



- g. You are notified when the installation is complete. Click **Close** to close the wizard.

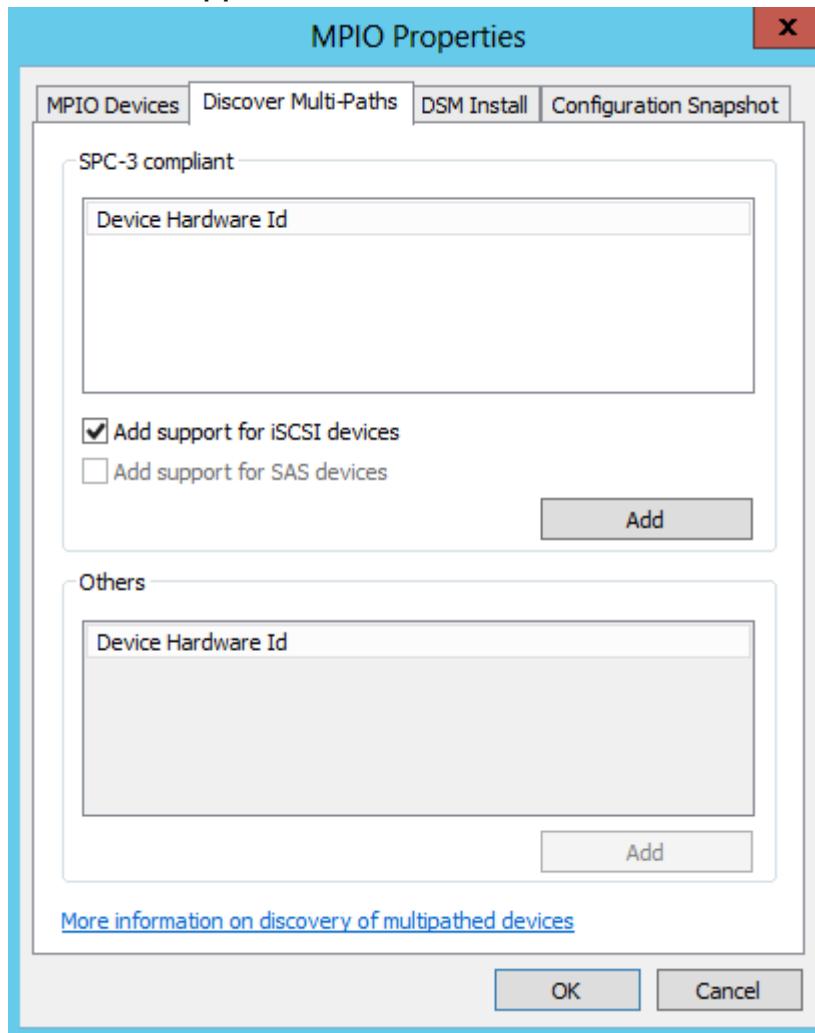


Step 2: Configure MPIO for StorSimple volumes

MPIO must be configured to identify StorSimple volumes. To configure MPIO to recognize StorSimple volumes, perform the following steps.

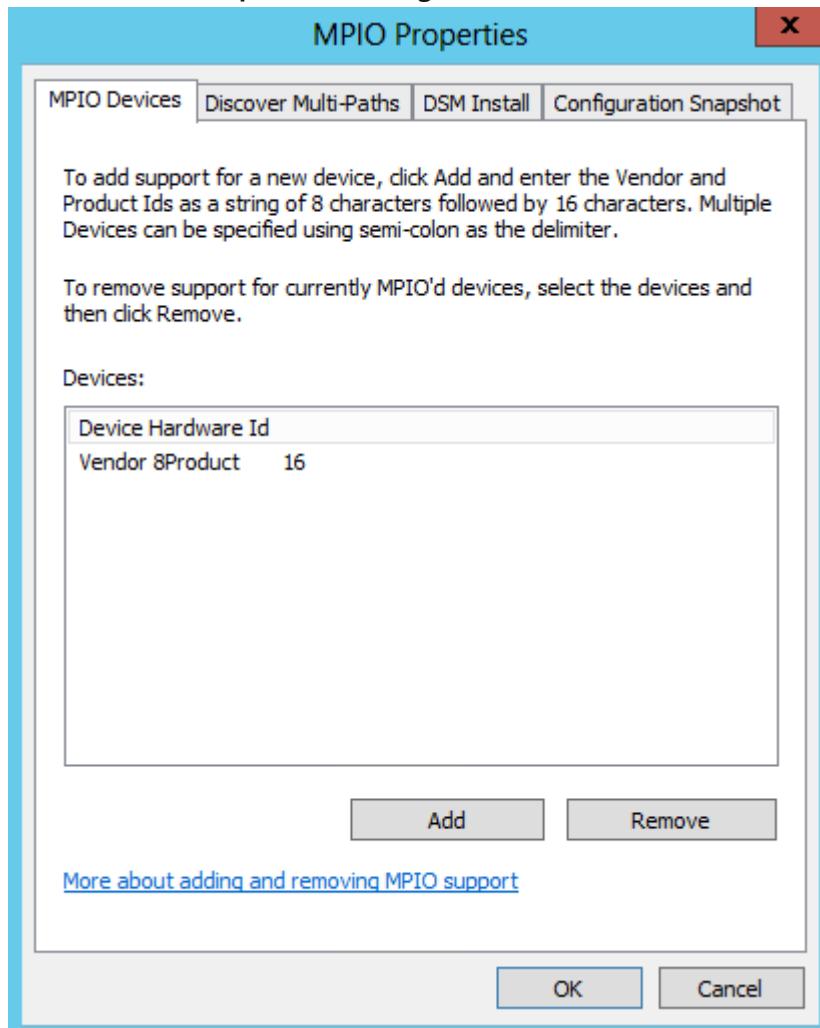
To configure MPIO for StorSimple volumes

1. Open the MPIO configuration. Click Server Manager > Dashboard > Tools > MPIO.
2. In the MPIO Properties dialog box, select the Discover Multi-Paths tab.
3. Select Add support for iSCSI devices, and then click Add.

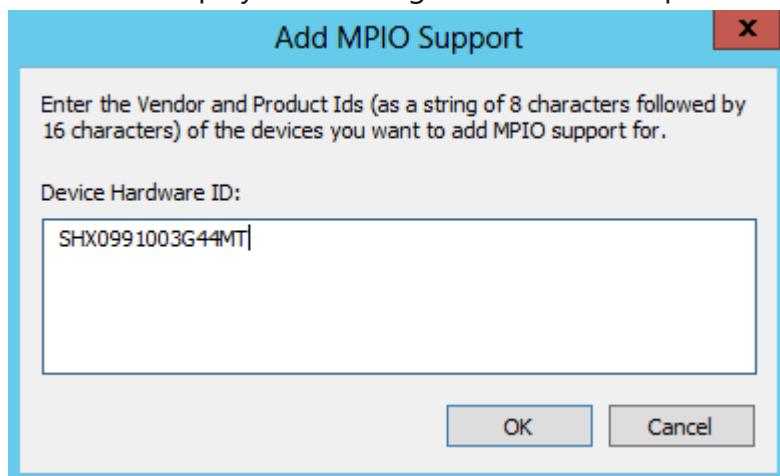


4. Reboot the server when prompted.

5. In the MPIO Properties dialog box, click the MPIO Devices tab. Click Add.



6. In the Add MPIO Support dialog box, under Device Hardware ID, enter your device serial number. To get the device serial number, access your StorSimple Device Manager service. Navigate to **Devices > Dashboard**. The device serial number is displayed in the right **Quick Glance** pane of the device dashboard.



7. Reboot the server when prompted.

Step 3: Mount StorSimple volumes on the host

After MPIO is configured on Windows Server, volume(s) created on the StorSimple device can be mounted and can then take advantage of MPIO for redundancy. To mount a volume, perform the following steps.

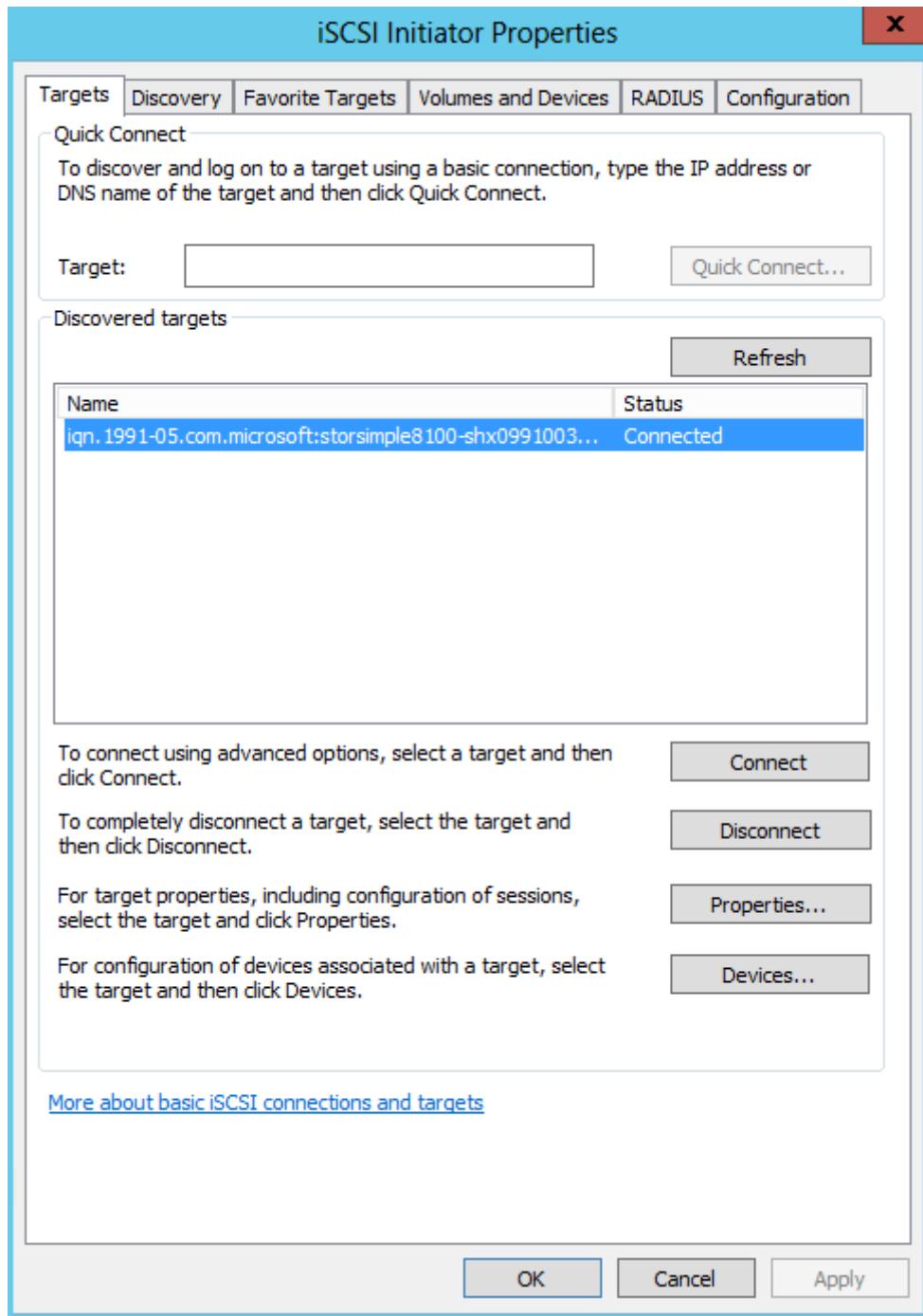
To mount volumes on the host

1. Open the **iSCSI Initiator Properties** window on the Windows Server host. Click **Server Manager > Dashboard > Tools > iSCSI Initiator**.
2. In the **iSCSI Initiator Properties** dialog box, click the **Discovery** tab, and then click **Discover Target Portal**.
3. In the **Discover Target Portal** dialog box, perform the following steps:
 - a. Enter the IP address of the DATA port of your StorSimple device (for example, enter DATA 0).
 - b. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.

 **Important**

If you are using a private network for iSCSI connections, enter the IP address of the DATA port that is connected to the private network.

4. Repeat steps 2-3 for a second network interface (for example, DATA 1) on your device. Keep in mind that these interfaces should be enabled for iSCSI. For more information, see [Modify network interfaces](#).
5. Select the **Targets** tab in the **iSCSI Initiator Properties** dialog box. You should see the StorSimple device target IQN under **Discovered Targets**.



6. Click **Connect** to establish an iSCSI session with your StorSimple device. A **Connect to Target** dialog box appears.
7. In the **Connect to Target** dialog box, select the **Enable multi-path** check box. Click **Advanced**.
8. In the **Advanced Settings** dialog box, perform the following steps:
 - a. On the **Local Adapter** drop-down list, select **Microsoft iSCSI Initiator**.
 - b. On the **Initiator IP** drop-down list, select the IP address of the host.
 - c. On the **Target Portal IP** drop-down list, select the IP of device interface.
 - d. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.
9. Click **Properties**. In the **Properties** dialog box, click **Add Session**.

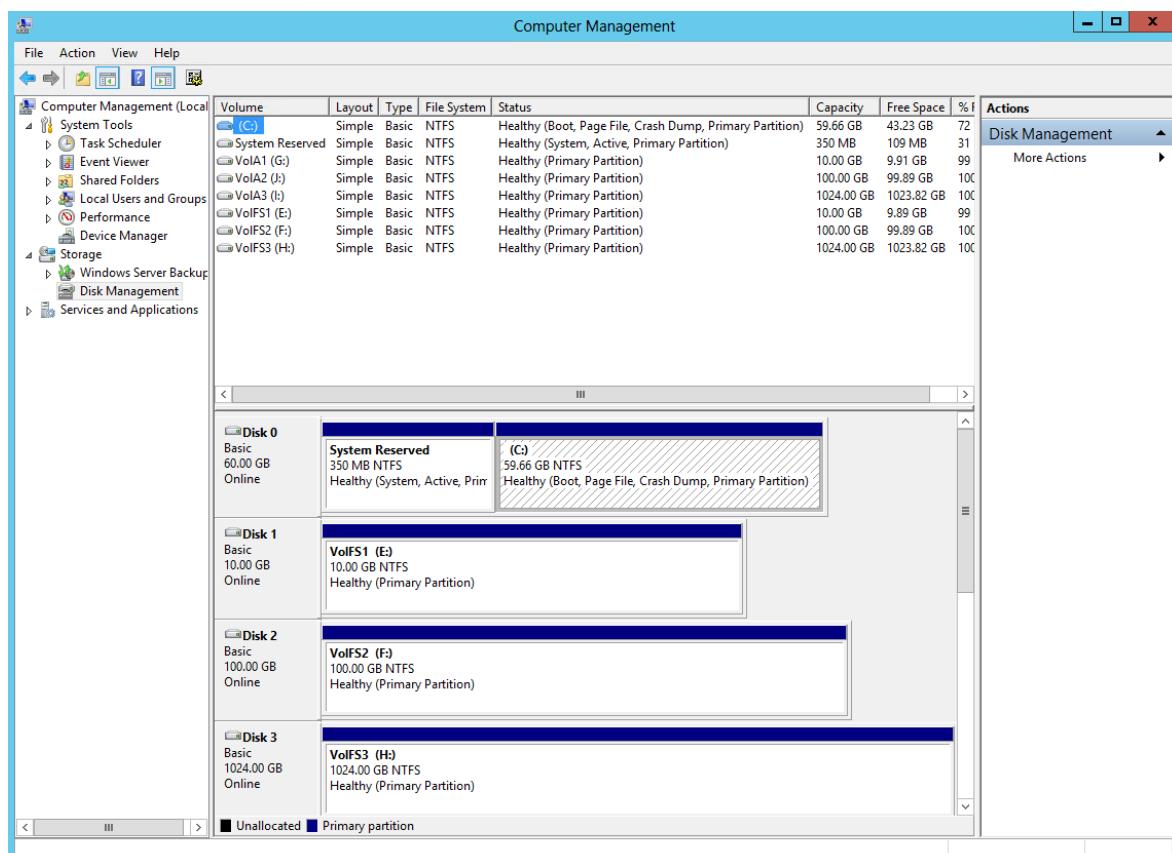
10. In the **Connect to Target** dialog box, select the **Enable multi-path** check box. Click **Advanced**.

11. In the **Advanced Settings** dialog box:

- On the **Local adapter** drop-down list, select Microsoft iSCSI Initiator.
- On the **Initiator IP** drop-down list, select the IP address corresponding to the host. In this case, you are connecting two network interfaces on the device to a single network interface on the host. Therefore, this interface is the same as that provided for the first session.
- On the **Target Portal IP** drop-down list, select the IP address for the second data interface enabled on the device.
- Click **OK** to return to the iSCSI Initiator Properties dialog box. You have added a second session to the target.

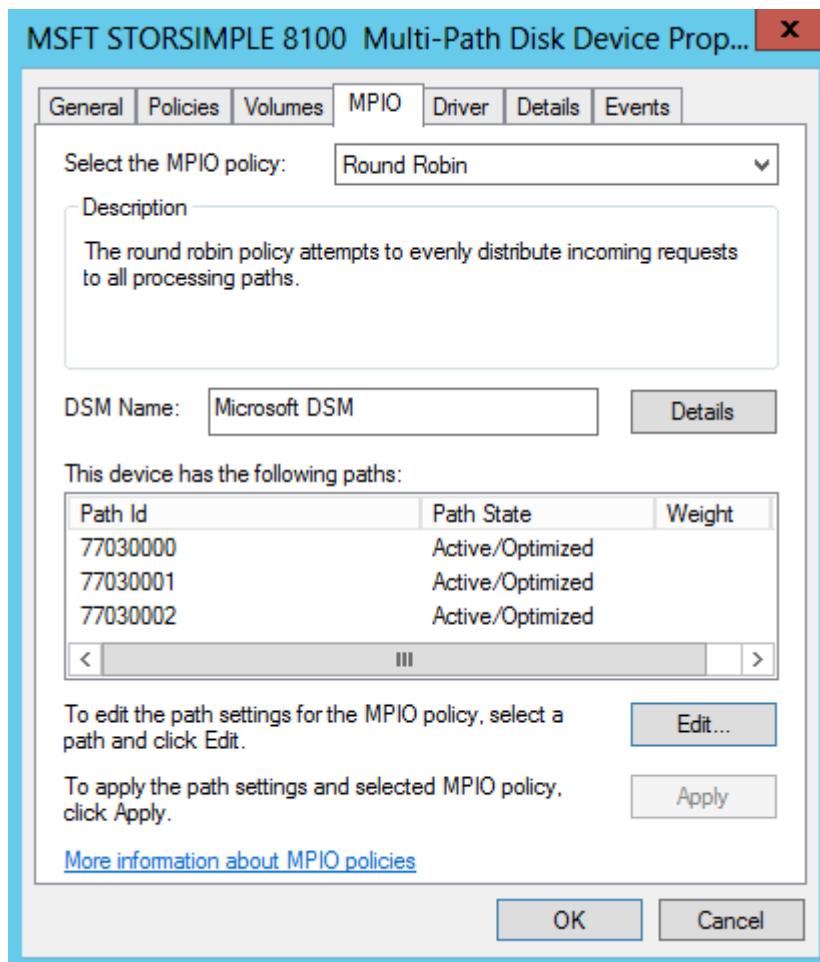
12. Open **Computer Management** by navigating to **Server Manager > Dashboard > Computer Management**. In the left pane, click **Storage > Disk Management**. The volume created on the StorSimple device that are visible to this host appears under **Disk Management** as new disk(s).

13. Initialize the disk and create a new volume. During the format process, select a block size of 64 KB.



14. Under **Disk Management**, right-click the **Disk** and select **Properties**.

15. In the StorSimple Model ##### Multi-Path Disk Device Properties dialog box, click the MPIO tab.



16. In the **DSM Name** section, click **Details** and verify that the parameters are set to the default parameters. The default parameters are:

- Path Verify Period = 30
- Retry Count = 3
- PDO Remove Period = 20
- Retry Interval = 1
- Path Verify Enabled = Unchecked.

Note

Do not modify the default parameters.

Step 4: Configure MPIO for high availability and load balancing

For multi-path based high availability and load balancing, multiple sessions must be manually added to declare the different paths available. For example, if the host has two interfaces connected to iSCSI network and the device has two interfaces connected to iSCSI network, then you need four sessions configured with proper path permutations (only two sessions will be required if each DATA interface and host interface is on a different IP subnet and is not routable).

We recommend that you have at least 8 active parallel sessions between the device and your application host. This can be achieved by enabling 4 network interfaces on your Windows Server system. Use physical network interfaces or virtual interfaces via network virtualization technologies on the hardware or operating system level on your Windows Server host. With the two network interfaces on the device, this configuration would result in 8 active sessions. This configuration helps optimize the device and cloud throughput.

ⓘ Important

We recommend that you do not mix 1 GbE and 10 GbE network interfaces. If you use two network interfaces, both interfaces should be of an identical type.

The following procedure describes how to add sessions when a StorSimple device with two network interfaces is connected to a host with two network interfaces. This gives you only 4 sessions. Use this same procedure with a StorSimple device with two network interfaces connected to a host with four network interfaces. You will need to configure 8 instead of the 4 sessions described here.

To configure MPIO for high availability and load balancing

1. Perform a discovery of the target: in the **iSCSI Initiator Properties** dialog box, on the **Discovery** tab, click **Discover Portal**.
2. In the **Connect to Target** dialog box, enter the IP address of one of the device network interfaces.
3. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.
4. In the **iSCSI Initiator Properties** dialog box, select the **Targets** tab, highlight the discovered target, and then click **Connect**. The **Connect to Target** dialog box appears.
5. In the **Connect to Target** dialog box:

- a. Leave the default selected target setting for **Add this connection** to the list of favorite targets. This makes the device automatically attempt to restart the connection every time this computer restarts.
 - b. Select the **Enable multi-path** check box.
 - c. Click **Advanced**.
6. In the **Advanced Settings** dialog box:
- a. On the **Local Adapter** drop-down list, select **Microsoft iSCSI Initiator**.
 - b. On the **Initiator IP** drop-down list, select the IP address corresponding to the first interface on the host (iSCSI interface).
 - c. On the **Target Portal IP** drop-down list, select the IP address for the first data interface enabled on the device.
 - d. Click **OK** to return to the iSCSI Initiator Properties dialog box.
7. Click **Properties**, and in the **Properties** dialog box, click **Add Session**.
8. In the **Connect to Target** dialog box, select the **Enable multi-path** check box, and then click **Advanced**.
9. In the **Advanced Settings** dialog box:
- a. On the **Local adapter** drop-down list, select **Microsoft iSCSI Initiator**.
 - b. On the **Initiator IP** drop-down list, select the IP address corresponding to the second iSCSI interface on the host.
 - c. On the **Target Portal IP** drop-down list, select the IP address for the second data interface enabled on the device.
 - d. Click **OK** to return to the iSCSI Initiator Properties dialog box. You have now added a second session to the target.
10. Repeat Steps 8-10 to add additional sessions (paths) to the target. With two interfaces on the host and two on the device, you can add a total of four sessions.
11. After adding the desired sessions (paths), in the **iSCSI Initiator Properties** dialog box, select the target and click **Properties**. On the Sessions tab of the **Properties** dialog box, note the four session identifiers that correspond to the possible path permutations. To cancel a session, select the check box next to a session identifier, and then click **Disconnect**.
12. To view devices presented within sessions, select the **Devices** tab. To configure the MPIO policy for a selected device, click **MPIO**. The **Device Details** dialog box appears. On the **MPIO** tab, you can select the appropriate **Load Balance Policy** settings. You can also view the **Active** or **Standby** path type.

Next steps

Learn more about [using the StorSimple Device Manager service to modify your StorSimple device configuration.](#)

Additional resources

Documentation

[MPIO option not available in Disk Management in Windows Server 2019 - Windows Server](#)

Describes a change in Windows Server 2019, in which MPIO option is no longer available in Disk Management.

[iSCSI Target Server Overview](#)

Learn more about: iSCSI Target Server overview

[Get-InitiatorPort \(Storage\)](#)

Use this topic to help manage Windows and Windows Server technologies with Windows PowerShell.

[How to merge checkpoints that have multiple differencing disks - Windows Server](#)

Describes different methods of merging checkpoints and their associated differencing disks into the related virtual machine.

[Unable to access ClusterStorage folder - Windows Server](#)

Describes an issue where you can't access a CSV volume from a passive (non-coordinator) node and receive event ID 5120 or 5142.

[Use live migration without Failover Clustering to move a virtual machine](#)

Gives prerequisites and instructions for doing a live migration in a standalone environment.

[Server-to-server storage replication](#)

How to set up and use Storage Replica for server-to-server replication in Windows Server, including Windows Admin Center and PowerShell.

[Upgrade virtual machine version in Hyper-V on Windows or Windows Server](#)

Gives instructions and considerations for upgrading the version of a virtual machine

[Show 5 more](#)

Configure MPIO on a StorSimple host running CentOS

Article • 08/22/2022 • 14 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article explains the steps required to configure Multipathing IO (MPIO) on your Centos 6.6 host server. The host server is connected to your Microsoft Azure StorSimple device for high availability via iSCSI initiators. It describes in detail the automatic discovery of multipath devices and the specific setup only for StorSimple volumes.

This procedure is applicable to all the models of StorSimple 8000 series devices.

ⓘ Note

This procedure cannot be used for a StorSimple Cloud Appliance. For more information, see how to configure host servers for your cloud appliance.

About multipathing

The multipathing feature allows you to configure multiple I/O paths between a host server and a storage device. These I/O paths are physical SAN connections that can include separate cables, switches, network interfaces, and controllers. Multipathing aggregates the I/O paths, to configure a new device that is associated with all of the aggregated paths.

The purpose of multipathing is two-fold:

- **High availability:** It provides an alternate path if any element of the I/O path (such as a cable, switch, network interface, or controller) fails.

- **Load balancing:** Depending on the configuration of your storage device, it can improve the performance by detecting loads on the I/O paths and dynamically rebalancing those loads.

About multipathing components

Multipathing in Linux consists of kernel components and user-space components as tabulated below.

- **Kernel:** The main component is the *device-mapper* that reroutes I/O and supports failover for paths and path groups.
- **User-space:** These are *multipath-tools* that manage multipathed devices by instructing the device-mapper multipath module what to do. The tools consist of:
 - **Multipath:** lists and configures multipathed devices.
 - **Multipathd:** daemon that executes multipath and monitors the paths.
 - **Devmap-name:** provides a meaningful device-name to udev for devmaps.
 - **Kpartx:** maps linear devmaps to device partitions to make multipath maps partitionable.
 - **Multipath.conf:** configuration file for multipath daemon that is used to overwrite the built-in configuration table.

About the multipath.conf configuration file

The configuration file `/etc/multipath.conf` makes many of the multipathing features user-configurable. The `multipath` command and the kernel daemon `multipathd` use information found in this file. The file is consulted only during the configuration of the multipath devices. Make sure that all changes are made before you run the `multipath` command. If you modify the file afterwards, you will need to stop and start `multipathd` again for the changes to take effect.

The `multipath.conf` has five sections:

- **System level defaults (*defaults*):** You can override system level defaults.
- **Blacklisted devices (*blacklist*):** You can specify the list of devices that should not be controlled by device-mapper.
- **Blacklist exceptions (*blacklist_exceptions*):** You can identify specific devices to be treated as multipath devices even if listed in the blocklist.
- **Storage controller specific settings (*devices*):** You can specify configuration settings that will be applied to devices that have Vendor and Product information.
- **Device specific settings (*multipaths*):** You can use this section to fine-tune the configuration settings for individual LUNs.

Configure multipathing on StorSimple connected to Linux host

A StorSimple device connected to a Linux host can be configured for high availability and load balancing. For example, if the Linux host has two interfaces connected to the SAN and the device has two interfaces connected to the SAN such that these interfaces are on the same subnet, then there will be 4 paths available. However, if each DATA interface on the device and host interface are on a different IP subnet (and not routable), then only 2 paths will be available. You can configure multipathing to automatically discover all the available paths, choose a load-balancing algorithm for those paths, apply specific configuration settings for StorSimple-only volumes, and then enable and verify multipathing.

The following procedure describes how to configure multipathing when a StorSimple device with two network interfaces is connected to a host with two network interfaces.

Prerequisites

This section details the configuration prerequisites for CentOS server and your StorSimple device.

On CentOS host

1. Make sure that your CentOS host has 2 network interfaces enabled. Type:

```
ifconfig
```

The following example shows the output when two network interfaces (`eth0` and `eth1`) are present on the host.

Output

```
[root@centosSS ~]# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:15:5D:A2:33:41
      inet addr:10.126.162.65  Bcast:10.126.163.255  Mask:255.255.252.0
            inet6 addr: 2001:4898:4010:3012:215:5dff:fea2:3341/64 Scope:Global
            inet6 addr: fe80::215:5dff:fea2:3341/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:36536 errors:0 dropped:0 overruns:0 frame:0
              TX packets:6312 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:13994127 (13.3 MiB)  TX bytes:645654 (630.5 KiB)

eth1  Link encap:Ethernet  HWaddr 00:15:5D:A2:33:42
```

```
inet addr:10.126.162.66 Bcast:10.126.163.255 Mask:255.255.252.0
inet6 addr: 2001:4898:4010:3012:215:5dff:fea2:3342/64 Scope:Global
inet6 addr: fe80::215:5dff:fea2:3342/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:25962 errors:0 dropped:0 overruns:0 frame:0
  TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:2597350 (2.4 MiB) TX bytes:754 (754.0 b)

loLink encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:12 errors:0 dropped:0 overruns:0 frame:0
    TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:720 (720.0 b) TX bytes:720 (720.0 b)
```

2. Install *iSCSI-initiator-utils* on your CentOS server. Perform the following steps to install *iSCSI-initiator-utils*.

a. Log on as `root` into your CentOS host.

b. Install the *iSCSI-initiator-utils*. Type:

```
yum install iscsi-initiator-utils
```

c. After the *iSCSI-Initiator-utils* is successfully installed, start the iSCSI service. Type:

```
service iscsid start
```

On occasions, `iscsid` may not actually start and the `--force` option may be needed

d. To ensure that your iSCSI initiator is enabled during boot time, use the `chkconfig` command to enable the service.

```
chkconfig iscsi on
```

e. To verify that it was properly setup, run the command:

```
chkconfig --list | grep iscsi
```

A sample output is shown below.

Output

```
iscsi  0:off  1:off  2:on3:on4:on5:on6:off
iscsid 0:off  1:off  2:on3:on4:on5:on6:off
```

From the above example, you can see that your iSCSI environment will run on boot time on run levels 2, 3, 4, and 5.

3. Install *device-mapper-multipath*. Type:

```
yum install device-mapper-multipath
```

The installation will start. Type Y to continue when prompted for confirmation.

On StorSimple device

Your StorSimple device should have:

- A minimum of two interfaces enabled for iSCSI. To verify that two interfaces are iSCSI-enabled on your StorSimple device, perform the following steps in the Azure classic portal for your StorSimple device:
 1. Log into the classic portal for your StorSimple device.
 2. Select your StorSimple Manager service, click **Devices** and choose the specific StorSimple device. Click **Configure** and verify the network interface settings. A screenshot with two iSCSI-enabled network interfaces is shown below. Here DATA 2 and DATA 3, both 10 GbE interfaces are enabled for iSCSI.

The screenshot shows the configuration interface for the network interface 'data 2'. The interface is currently enabled (YES selected). It has a speed of 10 GbE and is not cloud-enabled (NO selected). The iSCSI setting is also YES. The IP address family is set to IPV4. Below this, there are three input fields for an IPV4 address: IP Address (10.126.162.25), Subnet (255.255.252.0), and Gateway (10.126.172.1).

IPV4	IP Address	10.126.162.25
	Subnet	255.255.252.0
	Gateway	10.126.172.1

network interface: data3

ENABLE	<input checked="" type="button"/> YES	<input type="button"/> NO					
SPEED	10 GbE						
CLOUD ENABLED	<input checked="" type="button"/> YES	<input type="button"/> NO					
iSCSI ENABLED	<input checked="" type="button"/> YES	<input type="button"/> NO					
IP ADDRESS FAMILY	<input checked="" type="button"/> IPV4	<input type="button"/> IPV6	<input type="button"/> BOTH				
IPV4	<table border="1"> <tr> <td>IP Address</td> <td>10.126.162.26</td> </tr> <tr> <td>Subnet</td> <td>255.255.252.0</td> </tr> <tr> <td>Gateway</td> <td>10.126.172.1</td> </tr> </table>	IP Address	10.126.162.26	Subnet	255.255.252.0	Gateway	10.126.172.1
IP Address	10.126.162.26						
Subnet	255.255.252.0						
Gateway	10.126.172.1						

In the Configure page

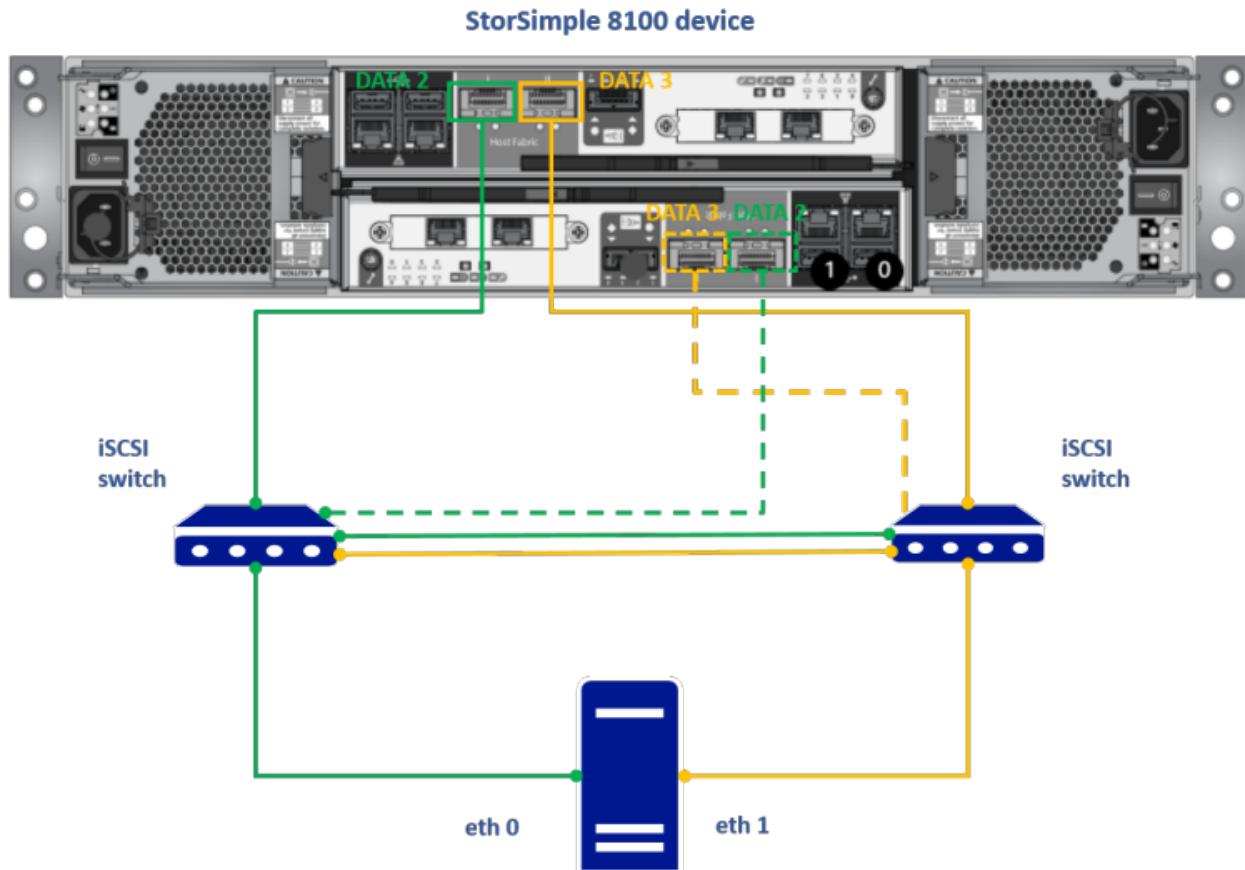
- a. Ensure that both network interfaces are iSCSI-enabled. The **iSCSI enabled** field should be set to **Yes**.
 - b. Ensure that the network interfaces have the same speed, both should be 1 GbE or 10 GbE.
 - c. Note the IPv4 addresses of the iSCSI-enabled interfaces and save for later use on the host.
- The iSCSI interfaces on your StorSimple device should be reachable from the CentOS server. To verify this, you need to provide the IP addresses of your StorSimple iSCSI-enabled network interfaces on your host server. The commands used and the corresponding output with DATA2 (10.126.162.25) and DATA3 (10.126.162.26) is shown below:

Console

```
[root@centosSS ~]# iscsiadm -m discovery -t sendtargets -p
10.126.162.25:3260
10.126.162.25:3260,1 iqn.1991-05.com.microsoft:storsimple8100-
shx0991003g44mt-target
10.126.162.26:3260,1 iqn.1991-05.com.microsoft:storsimple8100-
shx0991003g44mt-target
```

Hardware configuration

We recommend that you connect the two iSCSI network interfaces on separate paths for redundancy. The figure below shows the recommended hardware configuration for high availability and load-balancing multipathing for your CentOS server and StorSimple device.



As shown in the preceding figure:

- Your StorSimple device is in an active-passive configuration with two controllers.
- Two SAN switches are connected to your device controllers.
- Two iSCSI initiators are enabled on your StorSimple device.
- Two network interfaces are enabled on your CentOS host.

The above configuration will yield 4 separate paths between your device and the host if the host and data interfaces are routable.

ⓘ Important

- We recommend that you do not mix 1 GbE and 10 GbE network interfaces for multipathing. When using two network interfaces, both the interfaces should be the identical type.
- On your StorSimple device, DATA0, DATA1, DATA4 and DATA5 are 1 GbE interfaces whereas DATA2 and DATA3 are 10 GbE network interfaces.|

Configuration steps

The configuration steps for multipathing involve configuring the available paths for automatic discovery, specifying the load-balancing algorithm to use, enabling multipathing and finally verifying the configuration. Each of these steps is discussed in detail in the following sections.

Step 1: Configure multipathing for automatic discovery

The multipath-supported devices can be automatically discovered and configured.

1. Initialize `/etc/multipath.conf` file. Type:

```
mpathconf --enable
```

The above command will create a `sample/etc/multipath.conf` file.

2. Start multipath service. Type:

```
service multipathd start
```

You will see the following output:

```
Starting multipathd daemon:
```

3. Enable automatic discovery of multipaths. Type:

```
mpathconf --find_multipaths y
```

This will modify the defaults section of your `multipath.conf` as shown below:

```
config

defaults {
    find_multipaths yes
    user_friendly_names yes
    path_grouping_policy multibus
}
```

Step 2: Configure multipathing for StorSimple volumes

By default, all devices are blocklisted in the multipath.conf file and will be bypassed. You will need to create blocklist exceptions to allow multipathing for volumes from StorSimple devices.

1. Edit the `/etc/multipath.conf` file. Type:

```
vi /etc/multipath.conf
```

2. Locate the `blacklist_exceptions` section in the `multipath.conf` file. Your StorSimple device needs to be listed as a blocklist exception in this section. You can uncomment relevant lines in this file to modify it as shown below (use only the specific model of the device you are using):

```
config

blacklist_exceptions {
    device {
        vendor "MSFT"
        product "STORSIMPLE 8100*"
    }
    device {
        vendor "MSFT"
        product "STORSIMPLE 8600*"
    }
}
```

Step 3: Configure round-robin multipathing

This load-balancing algorithm uses all the available multipaths to the active controller in a balanced, round-robin fashion.

1. Edit the `/etc/multipath.conf` file. Type:

```
vi /etc/multipath.conf
```

2. Under the `defaults` section, set the `path_grouping_policy` to `multibus`. The `path_grouping_policy` specifies the default path grouping policy to apply to unspecified multipaths. The defaults section will look as shown below.

```
config

defaults {
    user_friendly_names yes
    path_grouping_policy multibus
}
```

ⓘ Note

The most common values of `path_grouping_policy` include:

- failover = 1 path per priority group
- multibus = all valid paths in 1 priority group

Step 4: Enable multipathing

1. Restart the `multipathd` daemon. Type:

```
service multipathd restart
```

2. The output will be as shown below:

Output

```
[root@centosSS ~]# service multipathd start
Starting multipathd daemon: [OK]
```

Step 5: Verify multipathing

1. First make sure that iSCSI connection is established with the StorSimple device as follows:

- a. Discover your StorSimple device. Type:

```
iscsiadm -m discovery -t sendtargets -p <IP address of network interface on
the device>:<iSCSI port on StorSimple device>
```

The output when IP address for DATA0 is 10.126.162.25 and port 3260 is opened on the StorSimple device for outbound iSCSI traffic is as shown below:

Output

```
10.126.162.25:3260,1 iqn.1991-05.com.microsoft:storsimple8100-
shx0991003g00dv-target
10.126.162.26:3260,1 iqn.1991-05.com.microsoft:storsimple8100-
shx0991003g00dv-target
```

Copy the IQN of your StorSimple device, `iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target`, from the preceding output.

- b. Connect to the device using target IQN. The StorSimple device is the iSCSI target here. Type:

```
iscsiadm -m node --login -T <IQN of iSCSI target>
```

The following example shows output with a target IQN of `iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target`. The output indicates that you have successfully connected to the two iSCSI-enabled network interfaces on your device.

Output

```
Logging in to [iface: eth0, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.25,3260] (multiple)
Logging in to [iface: eth1, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.25,3260] (multiple)
Logging in to [iface: eth0, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.26,3260] (multiple)
Logging in to [iface: eth1, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.26,3260] (multiple)
Login to [iface: eth0, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.25,3260] successful.
Login to [iface: eth1, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.25,3260] successful.
Login to [iface: eth0, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.26,3260] successful.
Login to [iface: eth1, target: iqn.1991-05.com.microsoft:storsimple8100-shx0991003g00dv-target, portal: 10.126.162.26,3260] successful.
```

If you see only one host interface and two paths here, then you need to enable both the interfaces on host for iSCSI. You can follow the [detailed instructions in Linux documentation](#).

2. A volume is exposed to the CentOS server from the StorSimple device. For more information, see [Step 6: Create a volume](#) via the Azure portal on your StorSimple device.
3. Verify the available paths. Type:

```
multipath -l
```

The following example shows the output for two network interfaces on a StorSimple device connected to a single host network interface with two available

paths.

Output

```
mpathb (36486fd20cc081f8dc3fccb992d45a68) dm-3 MSFT,STORSIMPLE 8100
size=100G features='0' hwhandler='0' wp=rw
`-- policy='round-robin 0' prio=0 status=active
|- 7:0:0:1 sdc 8:32 active undef running
`- 6:0:0:1 sdd 8:48 active undef running
```

The following example shows the output for two network interfaces on a StorSimple device connected to two host network interfaces with four available paths.

Output

```
mpathb (36486fd27a23feba1b096226f11420f6b) dm-2 MSFT,STORSIMPLE 8100
size=100G features='0' hwhandler='0' wp=rw
`-- policy='round-robin 0' prio=0 status=active
|- 17:0:0:0 sdb 8:16 active undef running
|- 15:0:0:0 sdd 8:48 active undef running
|- 14:0:0:0 sdc 8:32 active undef running
`- 16:0:0:0 sde 8:64 active undef running
```

After the paths are configured, refer to the specific instructions on your host operating system (Centos 6.6) to mount and format this volume.

Troubleshoot multipathing

This section provides some helpful tips if you run into any issues during multipathing configuration.

Q. I do not see the changes in `multipath.conf` file taking effect.

A. If you have made any changes to the `multipath.conf` file, you will need to restart the multipathing service. Type the following command:

```
service multipathd restart
```

Q. I have enabled two network interfaces on the StorSimple device and two network interfaces on the host. When I list the available paths, I see only two paths. I expected to see four available paths.

A. Make sure that the two paths are on the same subnet and routable. If the network interfaces are on different VLANs and not routable, you will see only two paths. One way

to verify this is to make sure that you can reach both the host interfaces from a network interface on the StorSimple device. You will need to [contact Microsoft Support](#) as this verification can only be done via a support session.

Q. When I list available paths, I do not see any output.

A. Typically, not seeing any multipathed paths suggests a problem with the multipathing daemon, and it's most likely that any problem here lies in the `multipath.conf` file.

It would also be worth checking that you can actually see some disks after connecting to the target, as no response from the multipath listings could also mean you don't have any disks.

- Use the following command to rescan the SCSI bus:

```
$ rescan-scsi-bus.sh (part of sg3_utils package)
```

- Type the following commands:

```
$ dmesg | grep sd*
```

Or

```
$ fdisk -l
```

These will return details of recently added disks.

- To determine whether it is a StorSimple disk, use the following commands:

```
cat /sys/block/<DISK>/device/model
```

This will return a string, which will determine if it's a StorSimple disk.

A less likely but possible cause could also be stale iscsid pid. Use the following command to log off from the iSCSI sessions:

```
iscsiadm -m node --logout -p <Target_IP>
```

Repeat this command for all the connected network interfaces on the iSCSI target, which is your StorSimple device. Once you have logged off from all the iSCSI sessions, use the iSCSI target IQN to reestablish the iSCSI session. Type the following command:

```
iscsiadm -m node --login -T <TARGET_IQN>
```

Q. I am not sure if my device is allowed.

A. To verify whether your device is allowed, use the following troubleshooting interactive command:

```
Console

multipathd -k
multipathd> show devices
available block devices:
ram0 devnode blacklisted, unmonitored
ram1 devnode blacklisted, unmonitored
ram2 devnode blacklisted, unmonitored
ram3 devnode blacklisted, unmonitored
ram4 devnode blacklisted, unmonitored
ram5 devnode blacklisted, unmonitored
ram6 devnode blacklisted, unmonitored
ram7 devnode blacklisted, unmonitored
ram8 devnode blacklisted, unmonitored
ram9 devnode blacklisted, unmonitored
ram10 devnode blacklisted, unmonitored
ram11 devnode blacklisted, unmonitored
ram12 devnode blacklisted, unmonitored
ram13 devnode blacklisted, unmonitored
ram14 devnode blacklisted, unmonitored
ram15 devnode blacklisted, unmonitored
loop0 devnode blacklisted, unmonitored
loop1 devnode blacklisted, unmonitored
loop2 devnode blacklisted, unmonitored
loop3 devnode blacklisted, unmonitored
loop4 devnode blacklisted, unmonitored
loop5 devnode blacklisted, unmonitored
loop6 devnode blacklisted, unmonitored
loop7 devnode blacklisted, unmonitored
sr0 devnode blacklisted, unmonitored
sda devnode whitelisted, monitored
dm-0 devnode blacklisted, unmonitored
dm-1 devnode blacklisted, unmonitored
dm-2 devnode blacklisted, unmonitored
sdb devnode whitelisted, monitored
sdc devnode whitelisted, monitored
dm-3 devnode blacklisted, unmonitored
```

For more information, go to [troubleshooting for multipathing](#).

List of useful commands

Type	Command	Description
iSCSI	<code>service iscsid start</code>	Start iSCSI service
	<code>service iscsid stop</code>	Stop iSCSI service

Type	Command	Description
	<code>service iscsid restart</code>	Restart iSCSI service
	<code>iscsiadm -m discovery -t sendtargets -p <TARGET_IP></code>	Discover available targets on the specified address
	<code>iscsiadm -m node --login -T <TARGET_IQN></code>	Log in to the iSCSI target
	<code>iscsiadm -m node --logout -p <Target_IP></code>	Log out from the iSCSI target
	<code>cat /etc/iscsi/initiatorname.iscsi</code>	Print iSCSI initiator name
	<code>iscsiadm -m session -s <sessionid> -P 3</code>	Check the state of the iSCSI session and volume discovered on the host
	<code>iscsi -m session</code>	Shows all the iSCSI sessions established between the host and the StorSimple device
Multipathing	<code>service multipathd start</code>	Start multipath daemon
	<code>service multipathd stop</code>	Stop multipath daemon
	<code>service multipathd restart</code>	Restart multipath daemon
	<code>chkconfig multipathd on</code> OR <code>mpathconf -with_chkconfig y</code>	Enable multipath daemon to start at boot time
	<code>multipathd -k</code>	Start the interactive console for troubleshooting
	<code>multipath -l</code>	List multipath connections and devices
	<code>mpathconf --enable</code>	Create a sample mulitpath.conf file in <code>/etc/mulitpath.conf</code>

Next steps

As you are configuring MPIO on Linux host, you may also need to refer to the following CentOS 6.6 documents:

- [Setting up MPIO on CentOS ↗](#)
- [Linux Training Guide ↗](#)

Configure CHAP for your StorSimple device

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This tutorial explains how to configure CHAP for your StorSimple device. The procedure detailed in this article applies to StorSimple 8000 series devices.

CHAP stands for Challenge Handshake Authentication Protocol. It is an authentication scheme used by servers to validate the identity of remote clients. The verification is based on a shared password or secret. CHAP can be one way (unidirectional) or mutual (bidirectional). One way CHAP is when the target authenticates an initiator. In mutual or reverse CHAP, the target authenticates the initiator and then the initiator authenticates the target. Initiator authentication can be implemented without target authentication. However, target authentication can be implemented only if initiator authentication is also implemented.

As a best practice, we recommend that you use CHAP to enhance iSCSI security.

ⓘ Note

Keep in mind that IPSEC is not currently supported on StorSimple devices.

The CHAP settings on the StorSimple device can be configured in the following ways:

- Unidirectional or one-way authentication
- Bidirectional or mutual or reverse authentication

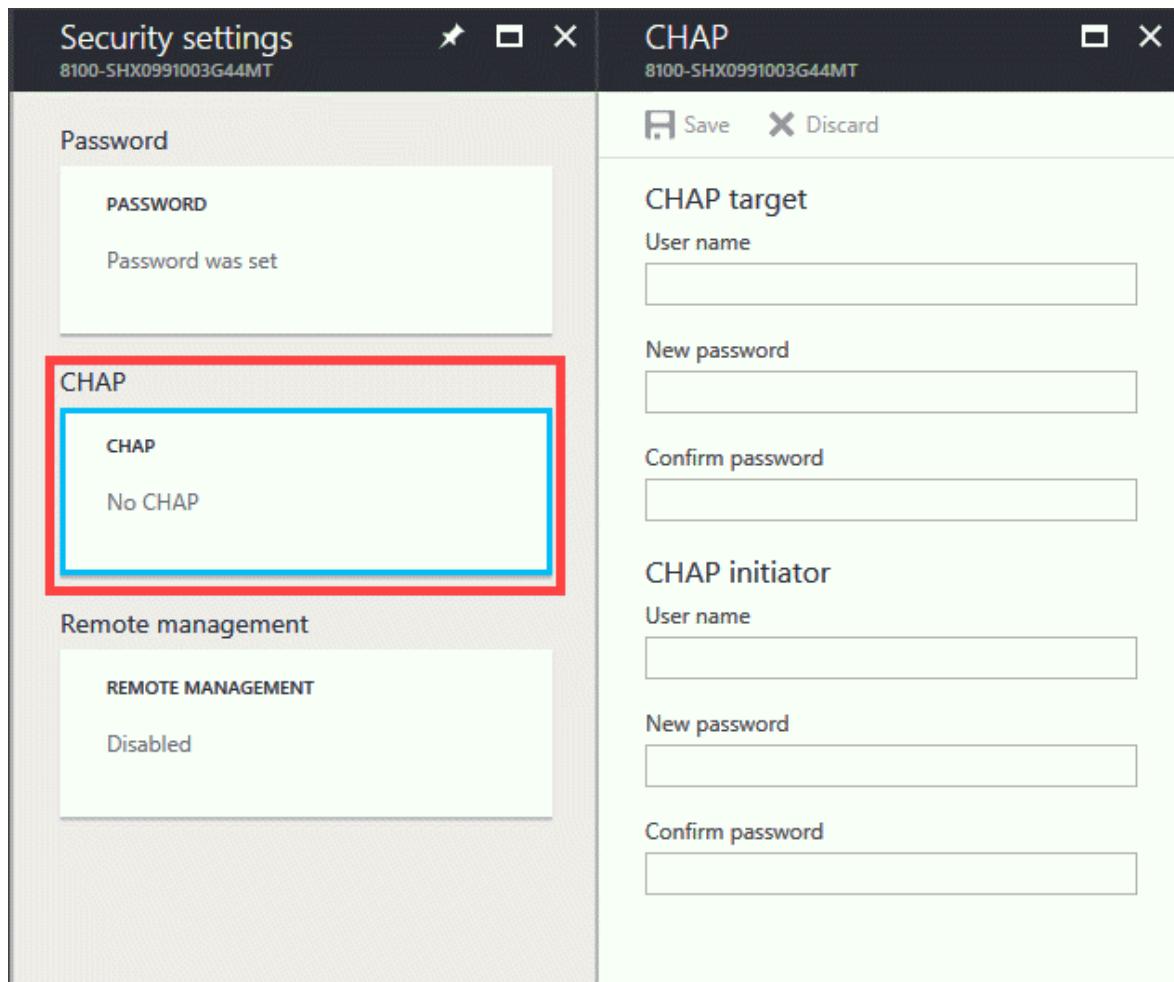
In each of these cases, the portal for the device and the server iSCSI initiator software needs to be configured. The detailed steps for this configuration are described in the following tutorial.

Unidirectional or one-way authentication

In unidirectional authentication, the target authenticates the initiator. This authentication requires that you configure the CHAP initiator settings on the StorSimple device and the iSCSI Initiator software on the host. The detailed procedures for your StorSimple device and Windows host are described next.

To configure your device for one-way authentication

1. In the Azure portal, go to your StorSimple Device Manager service. Click **Devices** and select and click a device you wish to configure CHAP for. Go to **Device settings > Security**. In the **Security settings** blade, click **CHAP**.

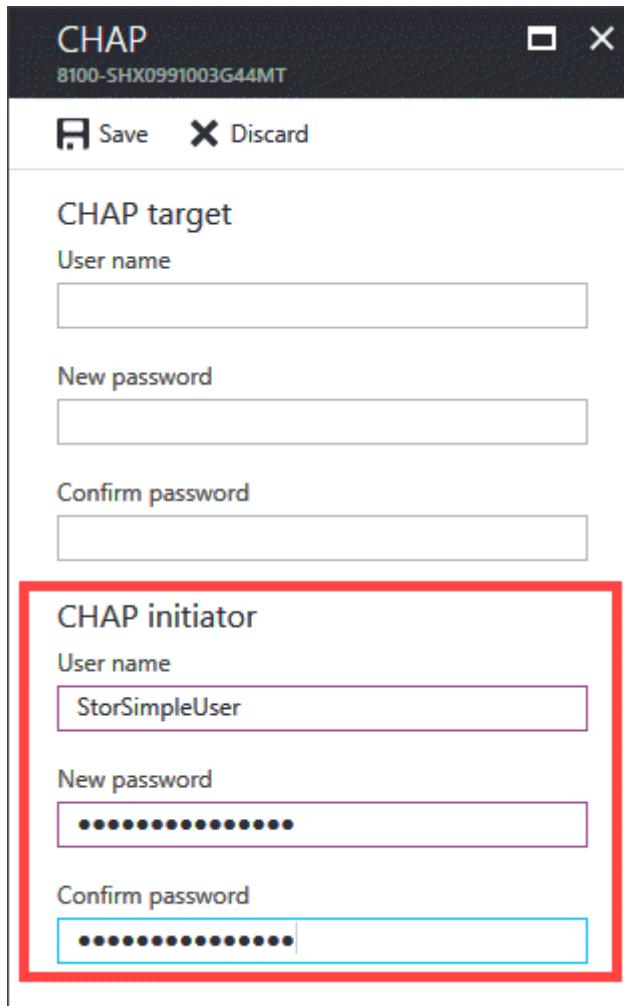


2. In the **CHAP** blade, and in the **CHAP Initiator** section:
 - a. Provide a user name for your CHAP initiator.
 - b. Supply a password for your CHAP initiator.

Important

The CHAP user name must contain fewer than 233 characters. The CHAP password must be between 12 and 16 characters. A longer user name or password results in an authentication failure on the Windows host.

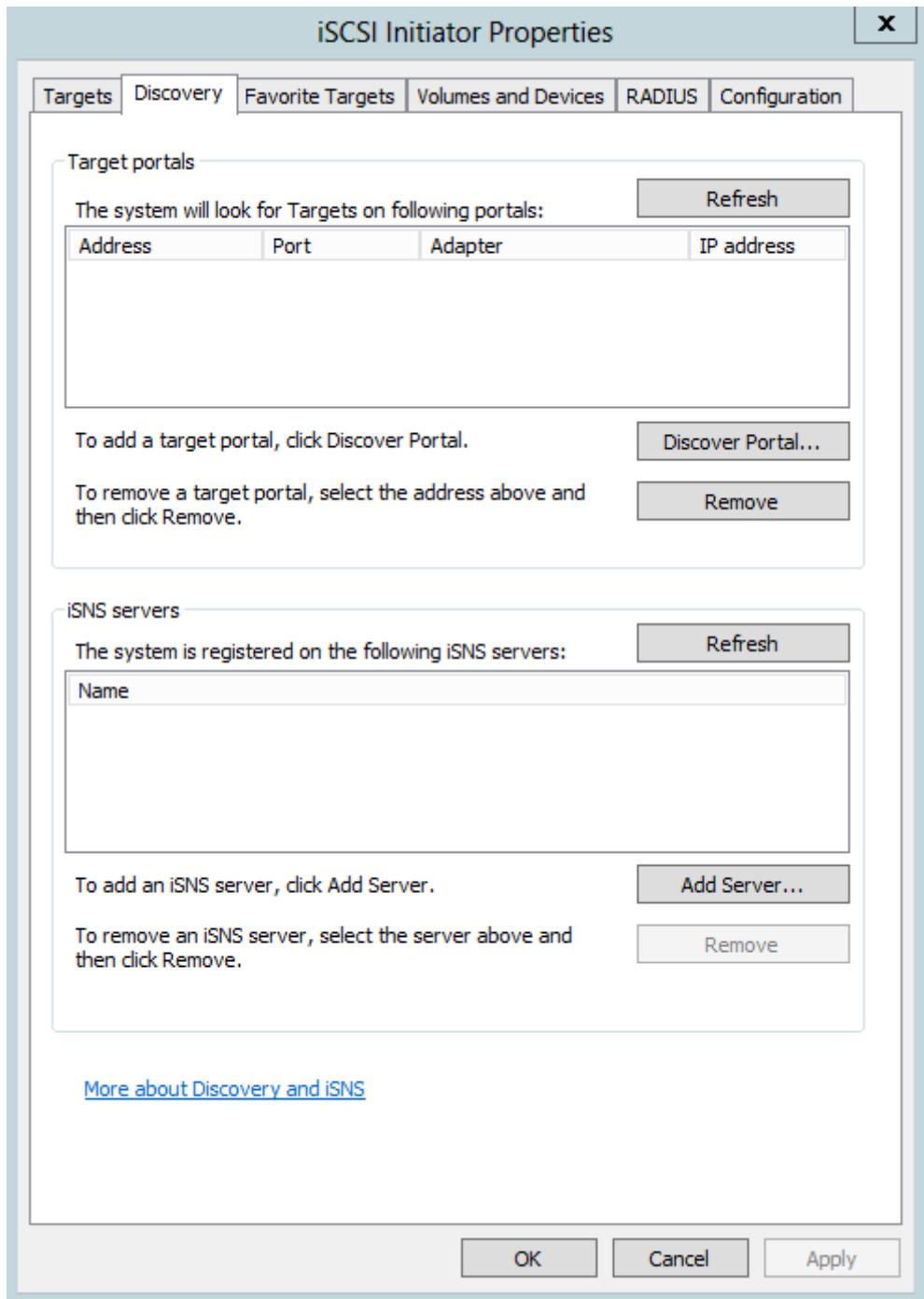
- c. Confirm the password.



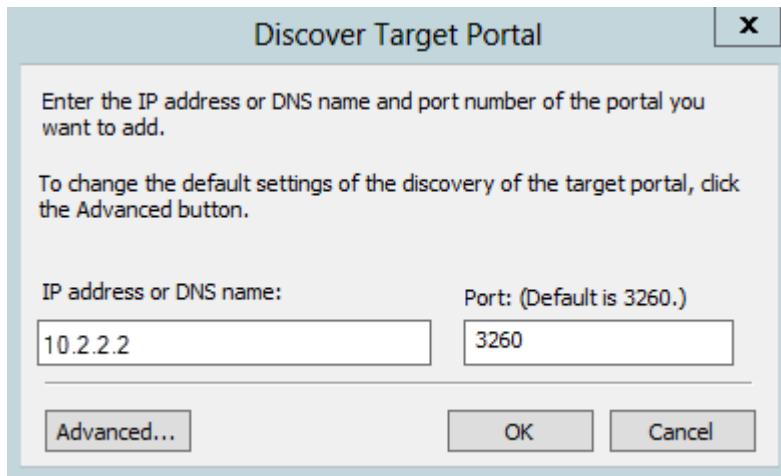
3. Click **Save**. A confirmation message is displayed. Click **OK** to save the changes.

To configure one-way authentication on the Windows host server

1. On the Windows host server, start the iSCSI Initiator.
2. In the iSCSI Initiator Properties window, perform the following steps:
 - a. Click the **Discovery** tab.

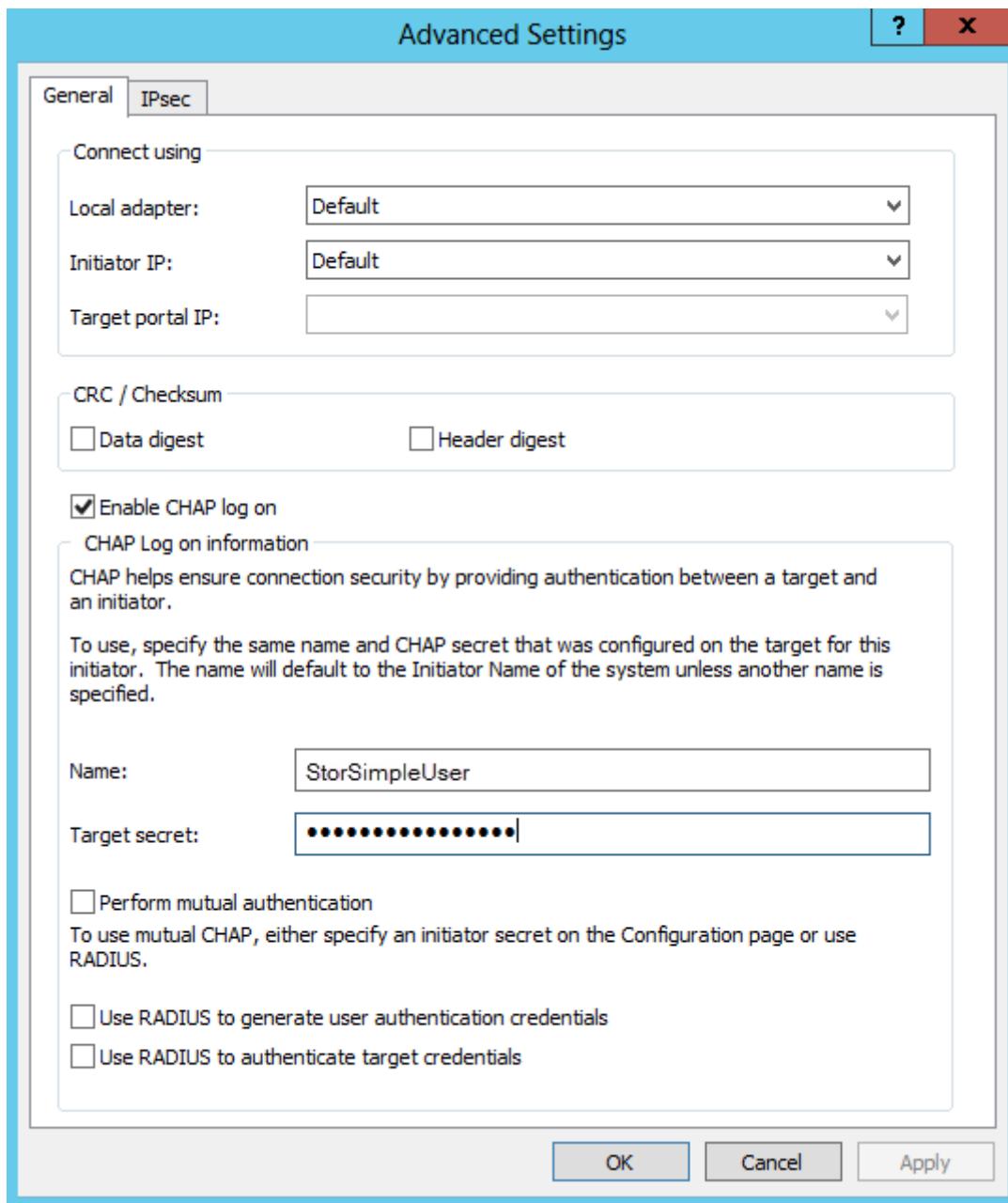


- b. Click **Discover Portal**.
3. In the **Discover Target Portal** dialog box:
 - a. Specify the IP address of your device.
 - b. Click **Advanced**.

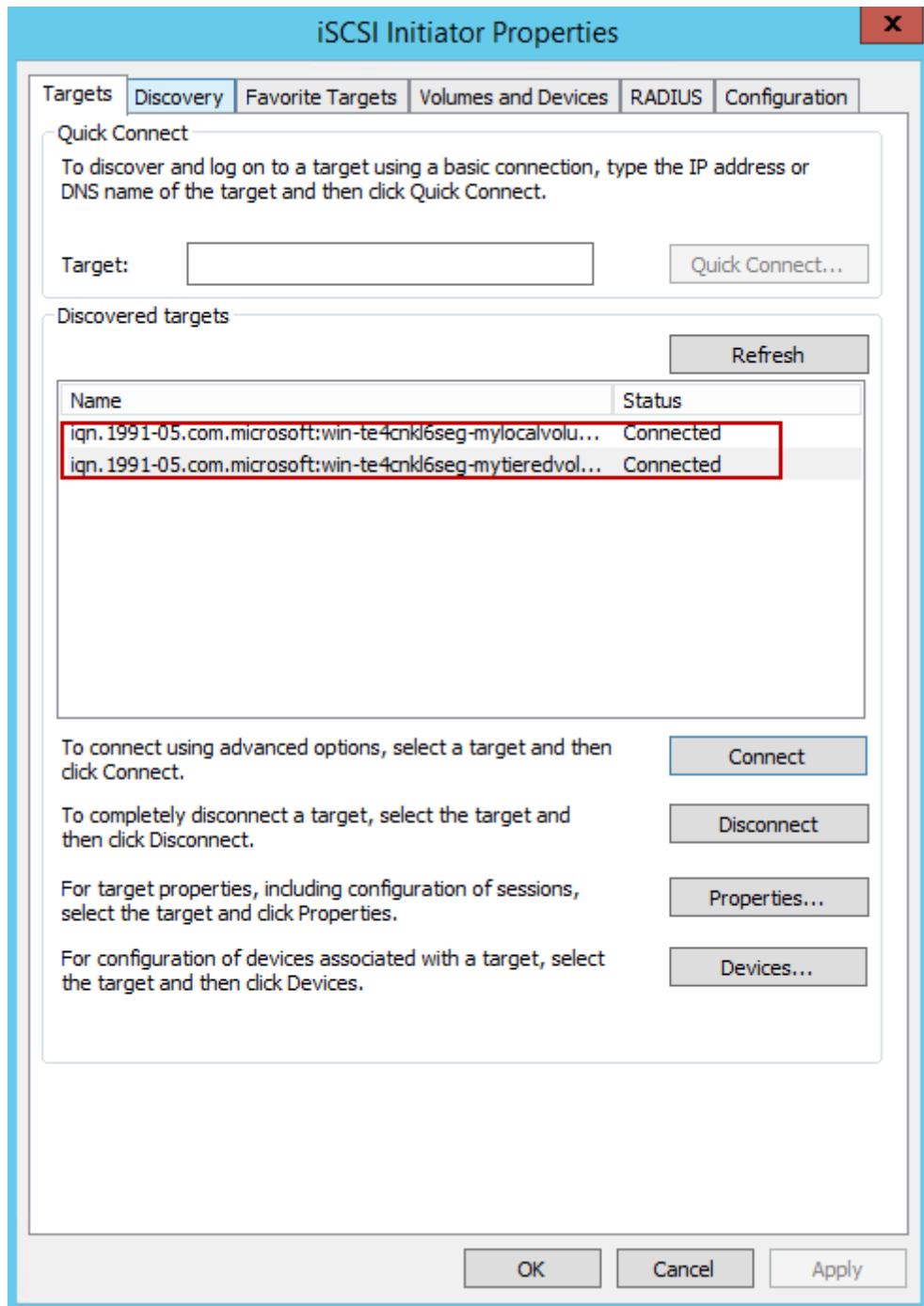


4. In the **Advanced Settings** dialog box:

- a. Select the **Enable CHAP log on** check box.
- b. In the **Name** field, supply the user name that you specified for the CHAP Initiator in the Azure portal.
- c. In the **Target secret** field, supply the password that you specified for the CHAP Initiator in the Azure portal.
- d. Click **OK**.



5. On the **Targets** tab of the **iSCSI Initiator Properties** window, the device status should appear as **Connected**. If you are using a StorSimple 1200 device, then each volume is mounted as an iSCSI target. Hence, steps 3-4 will need to be repeated for each volume.



ⓘ Important

If you change the iSCSI name, the new name is used for new iSCSI sessions. New settings are not used for existing sessions until you log off and log on again.

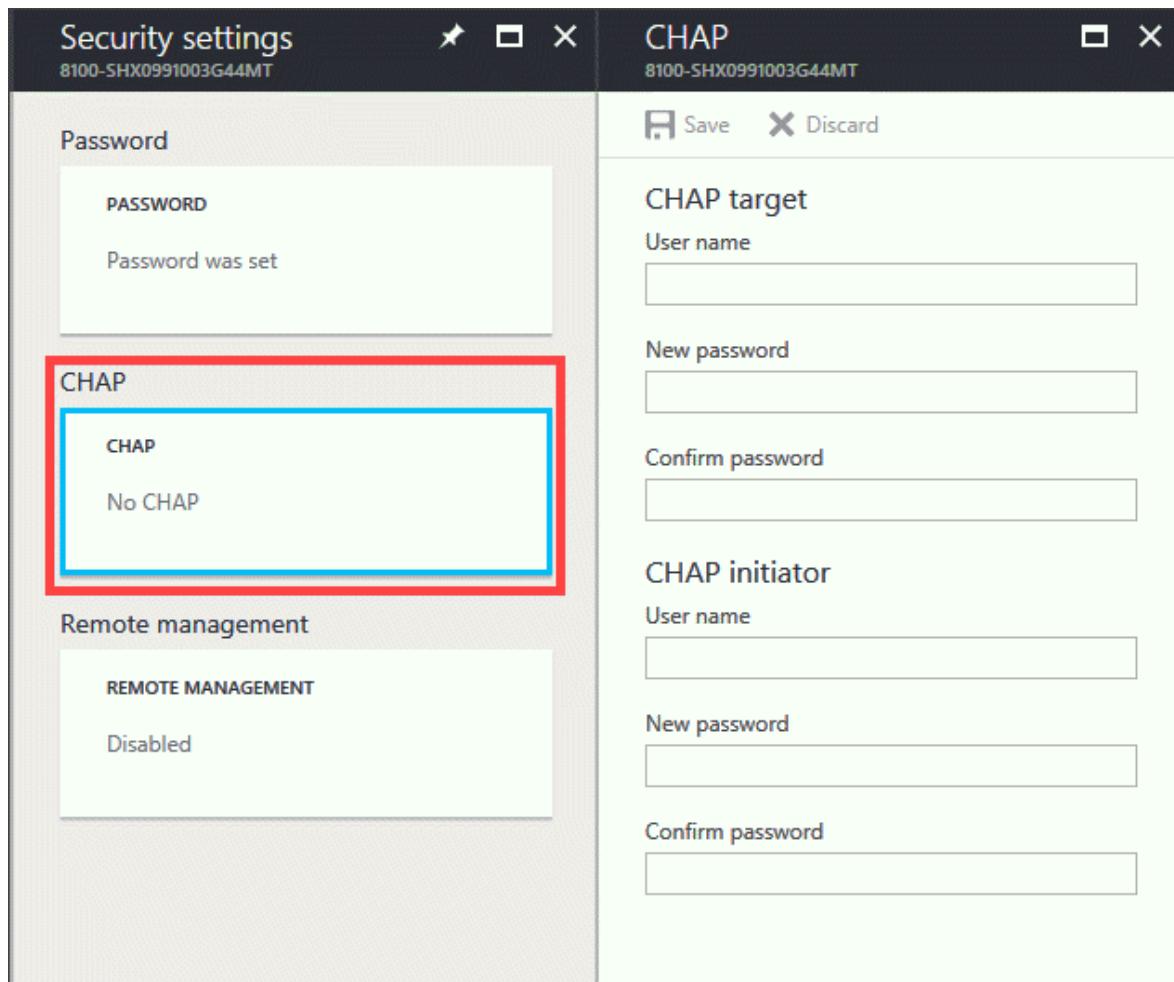
For more information about configuring CHAP on the Windows host server, go to [Additional considerations](#).

Bidirectional or mutual authentication

In bidirectional authentication, the target authenticates the initiator and then the initiator authenticates the target. This procedure requires the user to configure the CHAP initiator settings, reverse CHAP settings on the device, and iSCSI Initiator software on the host. The following procedures describe the steps to configure mutual authentication on the device and on the Windows host.

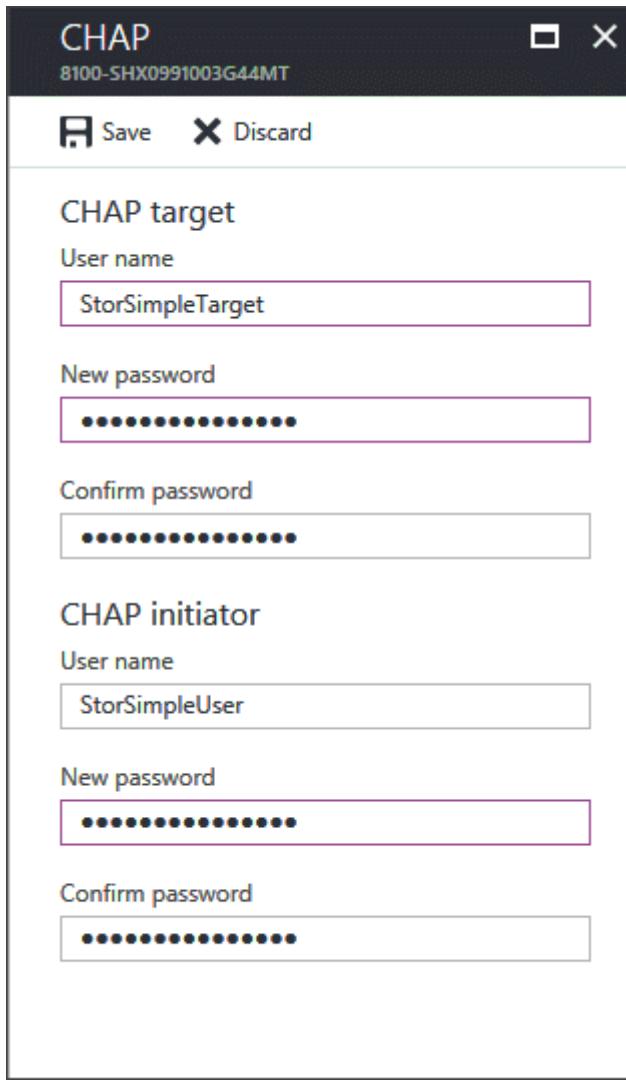
To configure your device for mutual authentication

1. In the Azure portal, go to your StorSimple Device Manager service. Click **Devices** and select and click a device you wish to configure CHAP for. Go to **Device settings > Security**. In the **Security settings** blade, click **CHAP**.



2. Scroll down on this page, and in the **CHAP Target** section:
 - a. Provide a **Reverse CHAP user name** for your device.
 - b. Supply a **Reverse CHAP password** for your device.
 - c. Confirm the password.
3. In the **CHAP Initiator** section:
 - a. Provide a **user name** for your device.
 - b. Provide a **password** for your device.

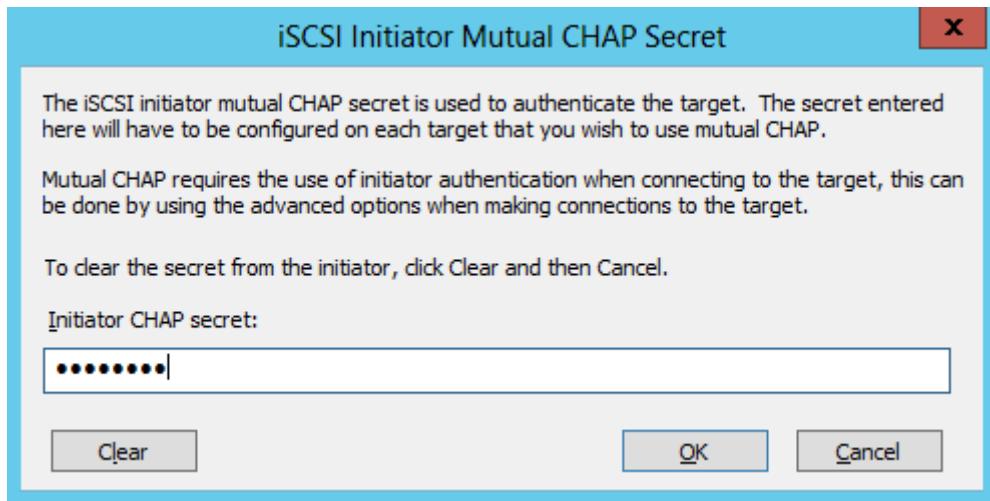
c. Confirm the password.



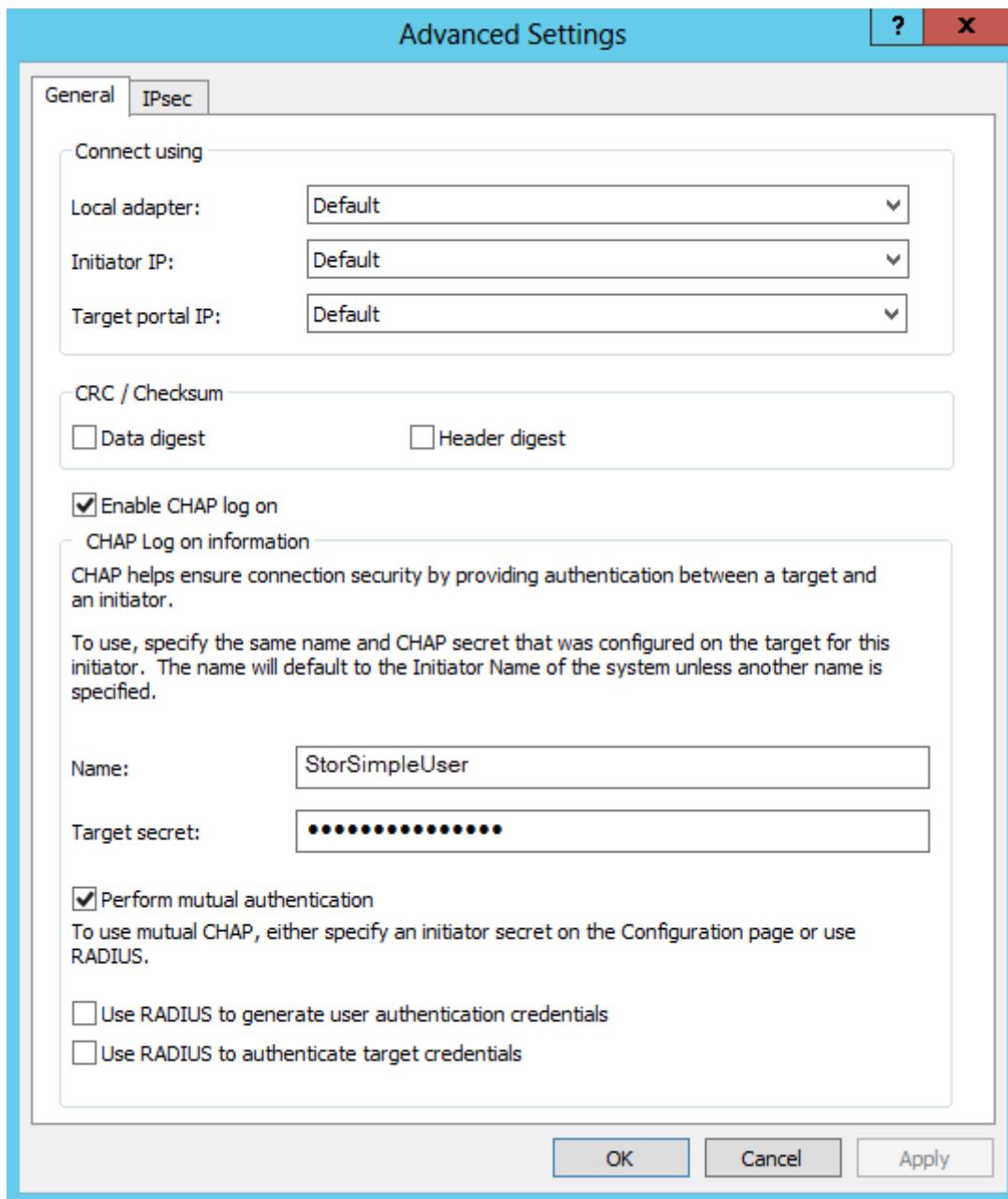
4. Click **Save**. A confirmation message is displayed. Click **OK** to save the changes.

To configure bidirectional authentication on the Windows host server

1. On the Windows host server, start the iSCSI Initiator.
2. In the iSCSI Initiator Properties window, click the **Configuration** tab.
3. Click **CHAP**.
4. In the iSCSI Initiator Mutual CHAP Secret dialog box:
 - a. Type the **Reverse CHAP Password** that you configured in the Azure portal.
 - b. Click **OK**.



5. Click the **Targets** tab.
6. Click the **Connect** button.
7. In the **Connect To Target** dialog box, click **Advanced**.
8. In the **Advanced Properties** dialog box:
 - a. Select the **Enable CHAP log on** check box.
 - b. In the **Name** field, supply the user name that you specified for the CHAP Initiator in the Azure portal.
 - c. In the **Target secret** field, supply the password that you specified for the CHAP Initiator in the Azure portal.
 - d. Select the **Perform mutual authentication** check box.

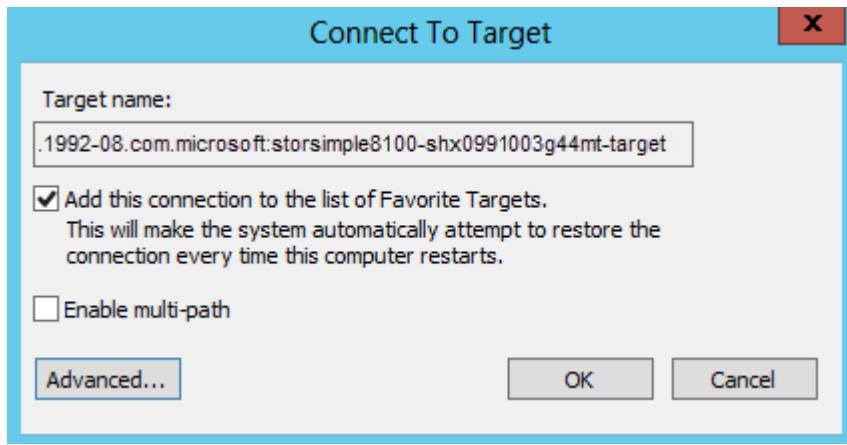


e. Click **OK** to complete the CHAP configuration

For more information about configuring CHAP on the Windows host server, go to [Additional considerations](#).

Additional considerations

The Quick Connect feature does not support connections that have CHAP enabled. When CHAP is enabled, make sure that you use the **Connect** button that is available on the Targets tab to connect to a target.



In the **Connect to Target** dialog box that is presented, select the **Add this connection to the list of Favorite Targets** check box. This selection ensures that every time the computer restarts, an attempt is made to restore the connection to the iSCSI favorite targets.

Errors during configuration

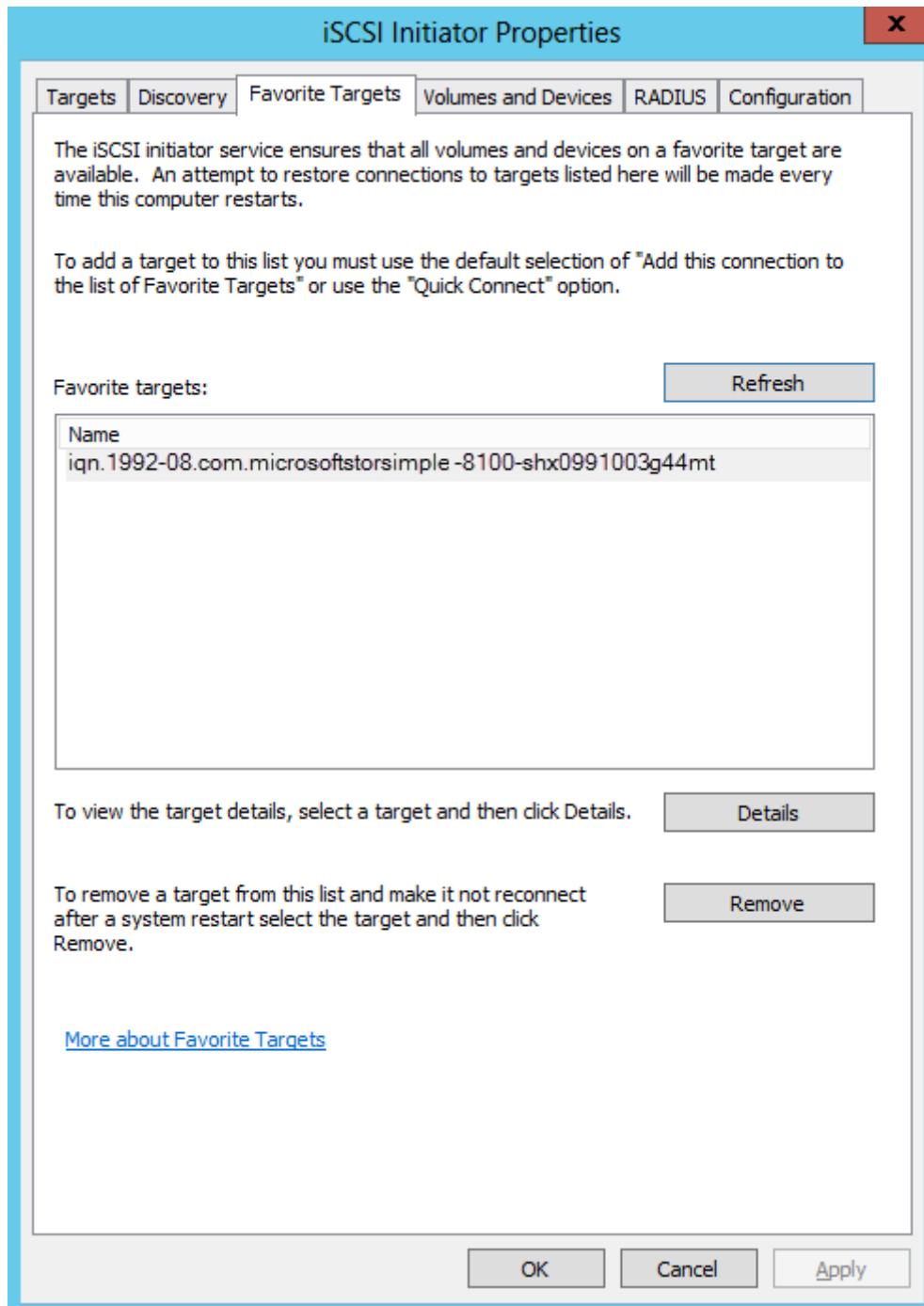
If your CHAP configuration is incorrect, then you are likely to see an **Authentication failure** error message.

Verification of CHAP configuration

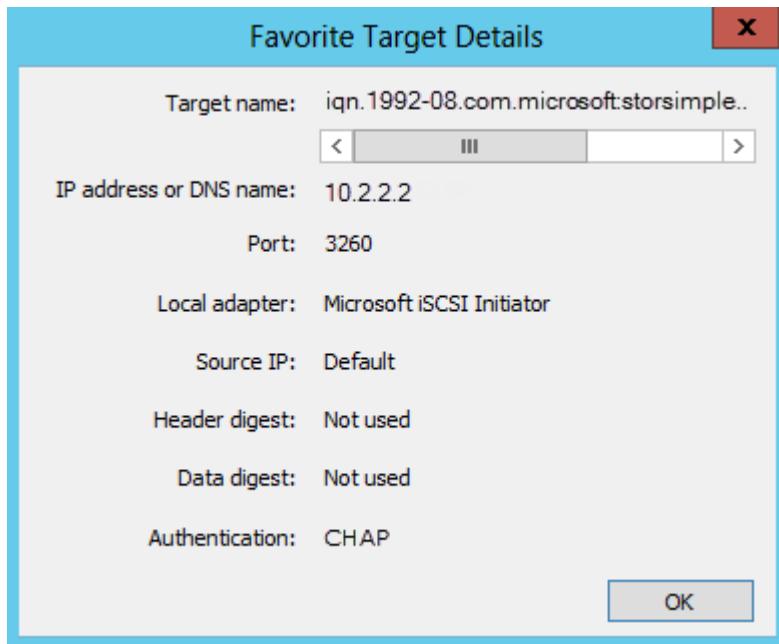
You can verify that CHAP is being used by completing the following steps.

To verify your CHAP configuration

1. Click **Favorite Targets**.
2. Select the target for which you enabled authentication.
3. Click **Details**.



4. In the **Favorite Target Details** dialog box, note the entry in the **Authentication** field. If the configuration was successful, it should say **CHAP**.



Next steps

- Learn more about [StorSimple security](#).
- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use Windows PowerShell for StorSimple to administer your device

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Windows PowerShell for StorSimple provides a command-line interface that you can use to manage your Microsoft Azure StorSimple device. As the name suggests, it is a Windows PowerShell-based, command-line interface that is built in a constrained runspace. From the perspective of the user at the command line, a constrained runspace appears as a restricted version of Windows PowerShell. While maintaining some of the basic capabilities of Windows PowerShell, this interface has other, dedicated cmdlets that are geared towards managing your Microsoft Azure StorSimple device.

This article describes the Windows PowerShell for StorSimple features, including how you can connect to this interface, and contains links to step-by-step procedures or workflows that you can perform using this interface. The workflows include how to register your device, configure the network interface on your device, install updates that require the device to be in maintenance mode, change the device state, and troubleshoot any issues that you may experience.

After reading this article, you will be able to:

- Connect to your StorSimple device using Windows PowerShell for StorSimple.
- Administer your StorSimple device using Windows PowerShell for StorSimple.
- Get help in Windows PowerShell for StorSimple.

ⓘ Note

- Windows PowerShell for StorSimple cmdlets allow you to manage your StorSimple device from a serial console or remotely via Windows PowerShell remoting. For more information about each of the individual cmdlets that can be used in this interface, go to [cmdlet reference for Windows PowerShell for StorSimple](#).
- The Azure PowerShell StorSimple cmdlets are a different collection of cmdlets that allow you to automate StorSimple service-level and migration tasks from the command line. For more information about the Azure PowerShell cmdlets for StorSimple, go to the [Azure StorSimple cmdlet reference](#).

You can access the Windows PowerShell for StorSimple using one of the following methods:

- [Connect to StorSimple device serial console](#)
- [Connect remotely to StorSimple using Windows PowerShell](#)

Connect to Windows PowerShell for StorSimple via the device serial console

You can [download PuTTY](#) or similar terminal emulation software to connect to Windows PowerShell for StorSimple. You need to configure PuTTY specifically to access the Microsoft Azure StorSimple device. The following topics contain detailed steps about how to configure PuTTY and connect to the device. Various menu options in the serial console are also explained.

PuTTY settings

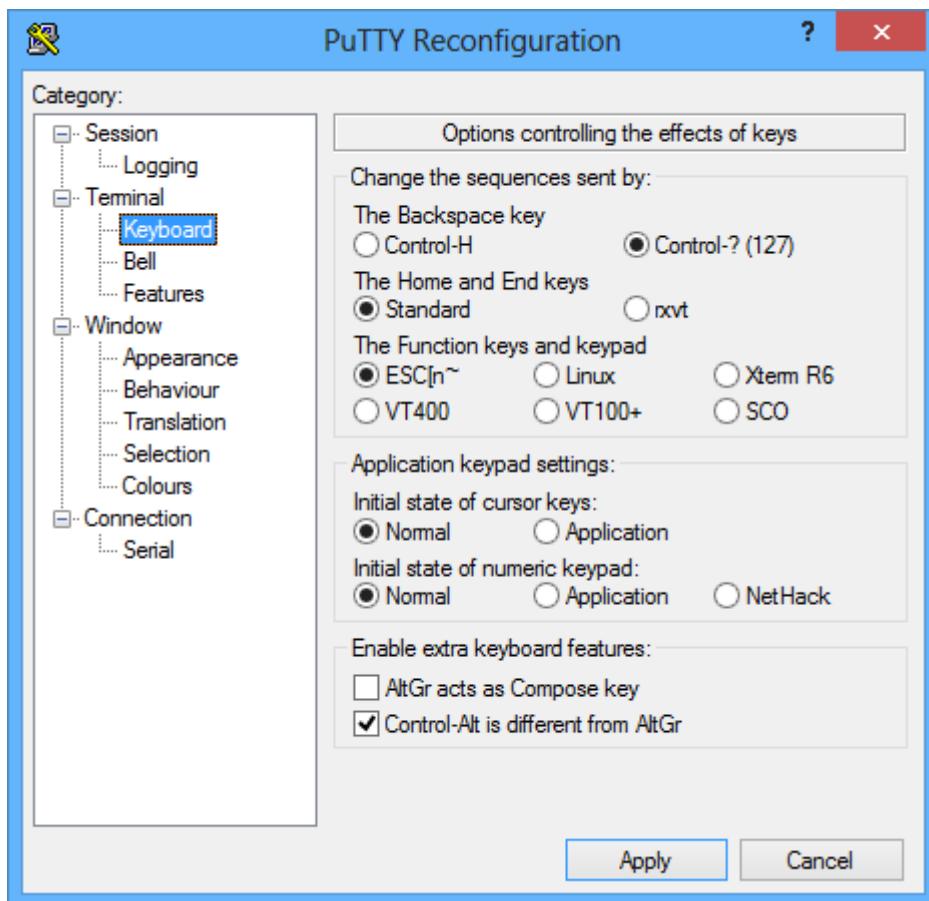
Make sure that you use the following PuTTY settings to connect to the Windows PowerShell interface from the serial console.

To configure PuTTY

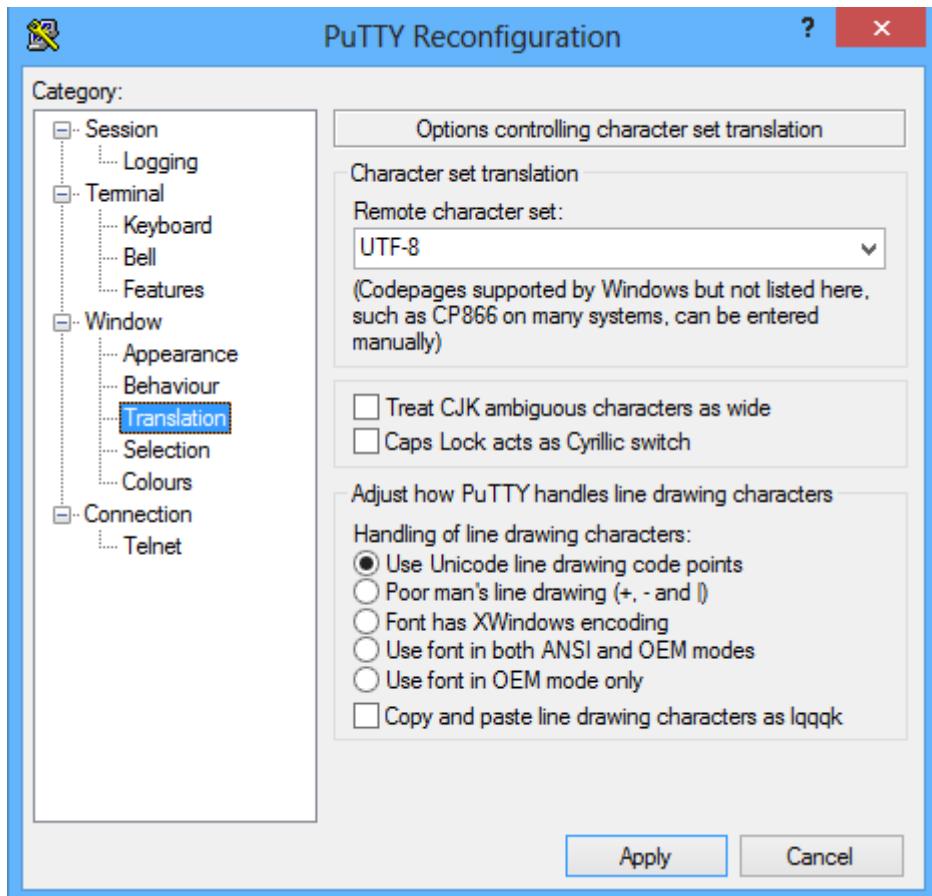
1. In the PuTTY Reconfiguration dialog box, in the **Category** pane, select **Keyboard**.
2. Make sure the following options (the default settings when you start a new session) are selected.

Keyboard item	Select
---------------	--------

Keyboard item	Select
Backspace key	Control-? (127)
Home and End keys	Standard
Function keys and keypad	ESC[n~
Initial state of cursor keys	Normal
Initial state of numeric keypad	Normal
Enable extra keyboard features	Control-Alt is different from AltGr



3. Click **Apply**.
4. In the **Category** pane, select **Translation**.
5. In the **Remote character set** list box, select **UTF-8**.
6. Under **Handling of line drawing characters**, select **Use Unicode line drawing code points**. The following screenshot shows the correct PuTTY selections.

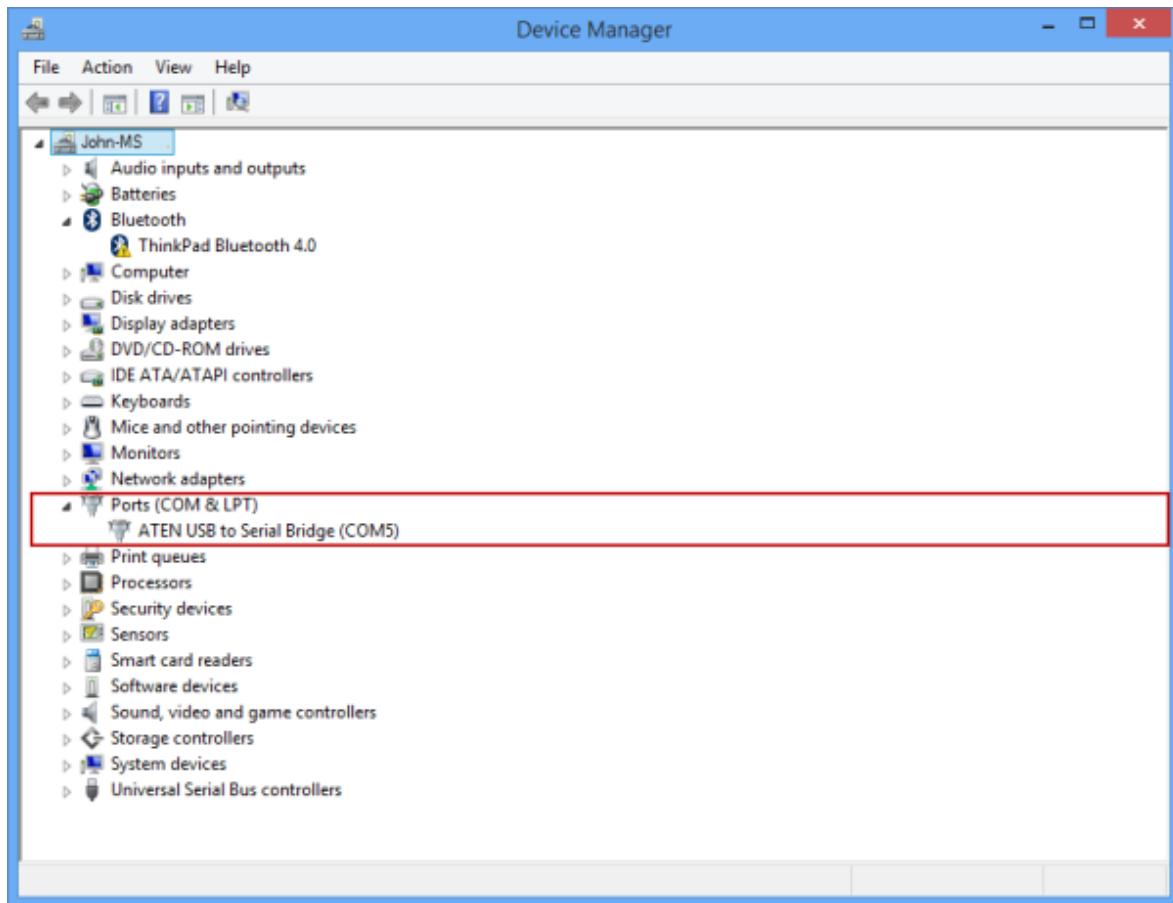


7. Click Apply.

You can now use PuTTY to connect to the device serial console by doing the following steps.

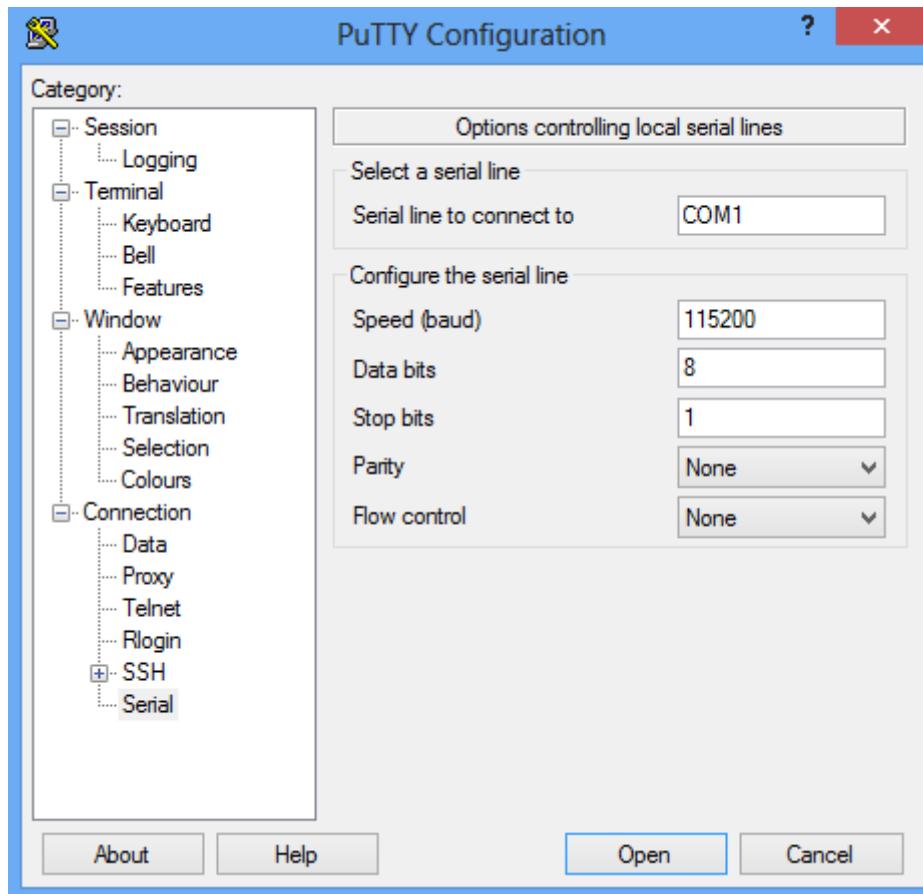
To connect through the serial console

1. Connect your serial cable to the device (directly or through a USB-serial adapter).
2. Open the **Control Panel**, and then open the **Device Manager**.
3. Identify the COM port as shown in the following illustration.



4. Start PuTTY.
5. In the right pane, change the **Connection type** to **Serial**.
6. In the right pane, type the appropriate COM port. Make sure that the serial configuration parameters are set as follows:
 - Speed: 115,200
 - Data bits: 8
 - Stop bits: 1
 - Parity: None
 - Flow control: None

These settings are shown in the following illustration.



(!) Note

If the default flow control setting does not work, try setting the flow control to XON/XOFF.

7. Click **Open** to start a serial session.

About the serial console

When you access the Windows PowerShell interface of your StorSimple device through the serial console, a banner message is presented, followed by menu options.

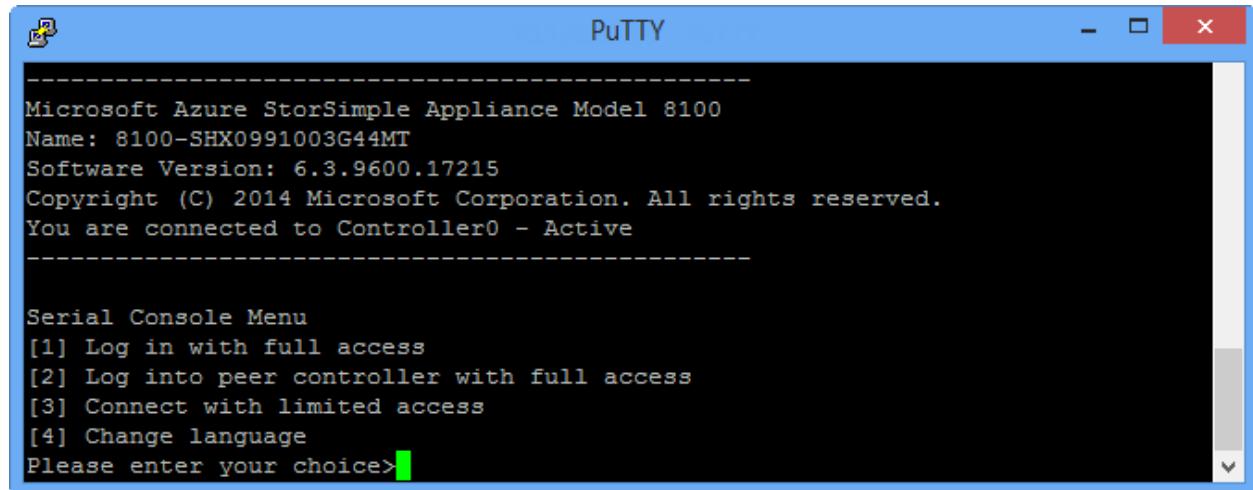
The banner message contains basic StorSimple device information such as the model, name, installed software version, and status of the controller you are accessing. The following image shows an example of a banner message.

```
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17215
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active
```

Important

You can use the banner message to identify whether the controller you are connected to is *Active* or *Passive*.

The following image shows the various runspace options that are available in the serial console menu.



A screenshot of a PuTTY window titled "PuTTY". The window displays the following text:

```
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17215
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active

-----
Serial Console Menu
[1] Log in with full access
[2] Log into peer controller with full access
[3] Connect with limited access
[4] Change language
Please enter your choice>
```

You can choose from the following settings:

1. **Log in with full access.** This option allows you to connect (with the proper credentials) to the **SSAdminConsole** runspace on the local controller. (The local controller is the controller that you are currently accessing through the serial console of your StorSimple device.) This option can also be used to allow Microsoft Support to access unrestricted runspace (a support session) to troubleshoot any possible device issues. After you use option 1 to log on, you can allow the Microsoft Support engineer to access unrestricted runspace by running a specific cmdlet. For details, refer to [Start a support session](#).
2. **Log in to peer controller with full access.** This option is the same as option 1, except that you can connect (with the proper credentials) to the **SSAdminConsole** runspace on the peer controller. Because the StorSimple device is a high availability device with two controllers in an active-passive configuration, peer refers to the other controller in the device that you are accessing through the serial console). Similar to option 1, this option can also be used to allow Microsoft Support to access unrestricted runspace on a peer controller.
3. **Connect with limited access.** This option is used to access Windows PowerShell interface in limited mode. You are not prompted for access credentials. This option connects to a more restricted runspace compared to options 1 and 2. Some of the tasks available through option 1 that *cannot* be performed in this runspace are:

- Reset to the factory settings
- Change the password
- Enable or disable support access
- Apply updates
- Install hotfixes

 **Note**

This is the preferred option if you have forgotten the device administrator password and cannot connect through option 1 or 2.

4. **Change language.** This option allows you to change the display language on the Windows PowerShell interface. The languages supported are English, Japanese, Russian, French, South Korean, Spanish, Italian, German, Chinese, and Portuguese.

Connect remotely to StorSimple using Windows PowerShell for StorSimple

You can use Windows PowerShell remoting to connect to your StorSimple device. When you connect this way, you will not see a menu. (You see a menu only if you use the serial console on the device to connect. Connecting remotely takes you directly to the equivalent of "option 1 – full access" on the serial console.) With Windows PowerShell remoting, you connect to a specific runspace. You can also specify the display language.

The display language is independent of the language that you set by using the **Change Language** option in the serial console menu. Remote PowerShell will automatically pick up the locale of the device you are connecting from if none is specified.

 **Note**

If you are working with Microsoft Azure virtual hosts and StorSimple Cloud Appliances, you can use Windows PowerShell remoting and the virtual host to connect to the cloud appliance. If you have set up a share location on the host on which to save information from the Windows PowerShell session, you should be aware that the *Everyone* principal includes only authenticated users. Therefore, if you have set up the share to allow access by *Everyone* and you connect without specifying credentials, the unauthenticated *Anonymous* principal will be used and

you will see an error. To fix this issue, on the share host you must enable the Guest account and then give the Guest account full access to the share or you must specify valid credentials along with the Windows PowerShell cmdlet.

You can use HTTP or HTTPS to connect via Windows PowerShell remoting. Use the instructions in the following tutorials:

- [Connect remotely using HTTP](#)
- [Connect remotely using HTTPS](#)

Connection security considerations

When you are deciding how to connect to Windows PowerShell for StorSimple, consider the following factors:

- Connecting directly to the device serial console is secure, but connecting to the serial console over network switches is not. Be cautious of the security risk when connecting to device serial over network switches.
- Connecting through an HTTP session might offer more security than connecting through the serial console over network. Although an HTTP session is not the most secure connection method, it is acceptable on trusted networks.
- Connecting through an HTTPS session is the most secure and the recommended option.

Administer your StorSimple device using Windows PowerShell for StorSimple

The following table shows a summary of all the common management tasks and complex workflows that can be performed within the Windows PowerShell interface of your StorSimple device. For more information about each workflow, click the appropriate entry in the table.

Windows PowerShell for StorSimple workflows

If you want to do this ...	Use this procedure.
Register your device	Configure and register the device using Windows PowerShell for StorSimple
Configure web proxy View web proxy settings	Configure web proxy for your StorSimple device

If you want to do this ...	Use this procedure.
Modify DATA 0 network interface settings on your device	Modify DATA 0 network interface for your StorSimple device
Stop a controller Restart or shut down a controller Shut down a device Reset the device to factory default settings	Manage device controllers
Install maintenance mode updates and hotfixes	Update your device
Enter maintenance mode Exit maintenance mode	StorSimple device modes
Create a Support package Decrypt and edit a support package	Create and manage a Support package
Start a Support session	Start a support session in Windows PowerShell for StorSimple

Get Help in Windows PowerShell for StorSimple

In Windows PowerShell for StorSimple, cmdlet Help is available. An online, up-to-date version of this Help is also available, which you can use to update the Help on your system.

Getting Help in this interface is similar to getting Help in Windows PowerShell, and most of the Help-related cmdlets will work. You can find Help for Windows PowerShell online: [Microsoft.PowerShell.Core](#).

To get help for a cmdlet

- To get Help for any cmdlet or function, use the following command: `Get-Help <cmdlet-name>`
- To get online Help for any cmdlet, use the previous cmdlet with the `-Online` parameter: `Get-Help <cmdlet-name> -Online`
- For full Help, you can use the `-Full` parameter, and for examples, use the `-Examples` parameter.

To update Help

You can easily update the Help in the Windows PowerShell interface. Perform the following steps to update the Help on your system.

To update cmdlet Help

1. Start Windows PowerShell with the **Run as administrator** option.
2. At the command prompt, type: `Update-Help`
3. The updated Help files will be installed.
4. After the Help files are installed, type: `Get-Help Get-Command` to display a list of cmdlets for which Help is available.

Note

To get a list of all the available cmdlets in a runspace, log in to the corresponding menu option and run the `Get-Command` cmdlet.

Next steps

If you experience any issues with your StorSimple device when performing one of the above workflows, refer to [Tools for troubleshooting StorSimple deployments](#).

Additional resources

Documentation

[Manage StorSimple 8000 series device controllers](#)

Learn how to stop, restart, shut down, or reset your StorSimple device controllers.

[Deactivate and delete a StorSimple 8000 series device](#)

Learn how to deactivate and delete a StorSimple device that is connected to a StorSimple Device Manager service.

[Connect remotely to your StorSimple device](#)

Explains how to configure your device for remote management and how to connect to Windows PowerShell for StorSimple via HTTP or HTTPS.

[Troubleshoot issues during data copies to your Azure Data Box, Azure Data Box Heavy](#)

Describes how to troubleshoot issues when copying data to Azure Data Box and Azure Data Box

Heavy devices.

[StorSimple 8000 series migration to Azure File Sync](#)

Learn how to migrate a StorSimple 8100 or 8600 appliance to Azure File Sync.

[Tutorial to copy data to Azure Data Box Disk](#)

In this tutorial, learn how to copy data from your host computer to Azure Data Box Disk and then generate checksums to verify data integrity.

[Data migration options from StorSimple 8000 series devices](#)

Provides an overview of the options to migrate data from StorSimple 8000 series.

[Review copy errors in uploads from Azure Data Box, Azure Data Box Heavy devices](#)

Describes review and follow-up for errors during uploads from an Azure Data Box or Azure Data Box Heavy device to the Azure cloud.

[Show 5 more](#)

Manage your StorSimple device controllers

Article • 08/19/2022 • 8 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes the different operations that can be performed on your StorSimple device controllers. The controllers in your StorSimple device are redundant (peer) controllers in an active-passive configuration. At a given time, only one controller is active and is processing all the disk and network operations. The other controller is in a passive mode. If the active controller fails, the passive controller automatically becomes active.

This tutorial includes step-by-step instructions to manage the device controllers by using the:

- **Controllers** blade for your device in the StorSimple Device Manager service.
- Windows PowerShell for StorSimple.

We recommend that you manage the device controllers via the StorSimple Device Manager service. If an action can only be performed by using Windows PowerShell for StorSimple, the tutorial makes a note of it.

After reading this tutorial, you will be able to:

- Restart or shut down a StorSimple device controller
- Shut down a StorSimple device
- Reset your StorSimple device to factory defaults

Restart or shut down a single controller

A controller restart or shutdown is not required as a part of normal system operation. Shutdown operations for a single device controller are common only in cases in which a failed device hardware component requires replacement. A controller restart may also be required in a situation in which performance is affected by excessive memory usage or a malfunctioning controller. You may also need to restart a controller after a successful controller replacement, if you wish to enable and test the replaced controller.

Restarting a device is not disruptive to connected initiators, assuming the passive controller is available. If a passive controller is not available or turned off, then restarting the active controller may result in the disruption of service and downtime.

ⓘ Important

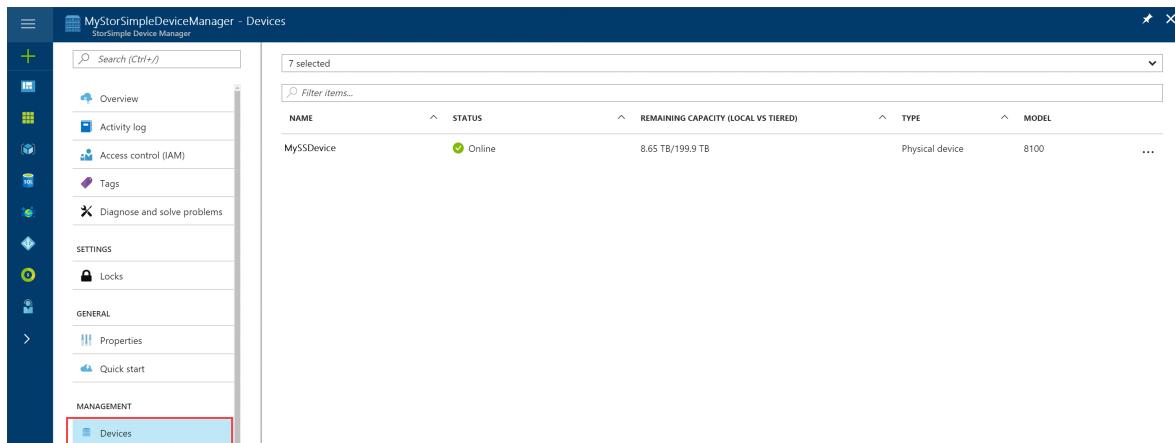
- A running controller should never be physically removed as this would result in a loss of redundancy and an increased risk of downtime.
- The following procedure applies only to the StorSimple physical device. For information about how to start, stop, and restart the StorSimple Cloud Appliance, see [Work with the cloud appliance](#).

You can restart or shut down a single device controller via the Azure portal of the StorSimple Device Manager service or Windows PowerShell for StorSimple.

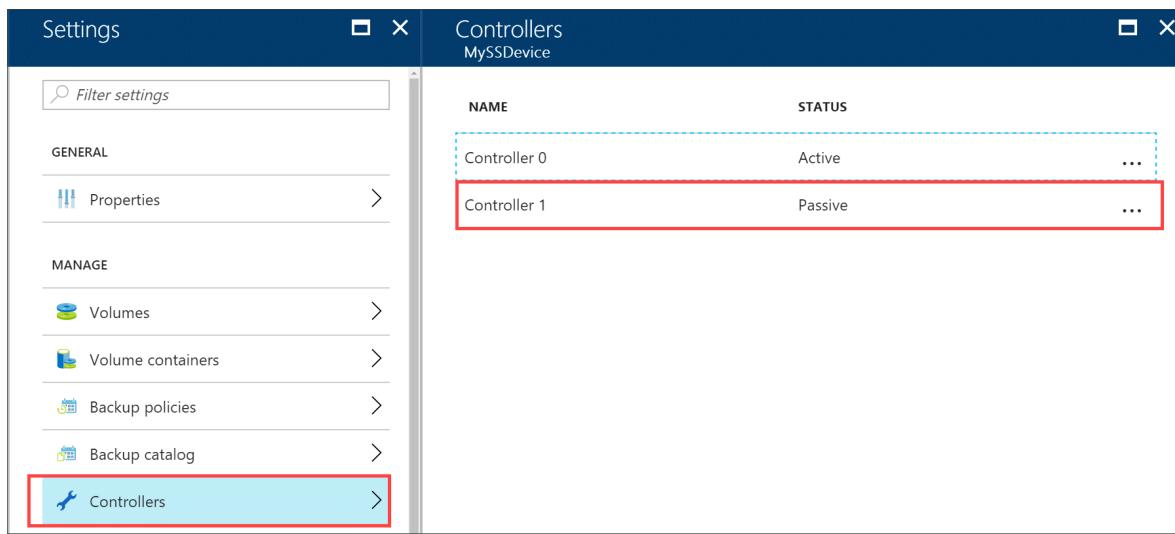
To manage your device controllers from the Azure portal, perform the following steps.

To restart or shut down a controller in Azure portal

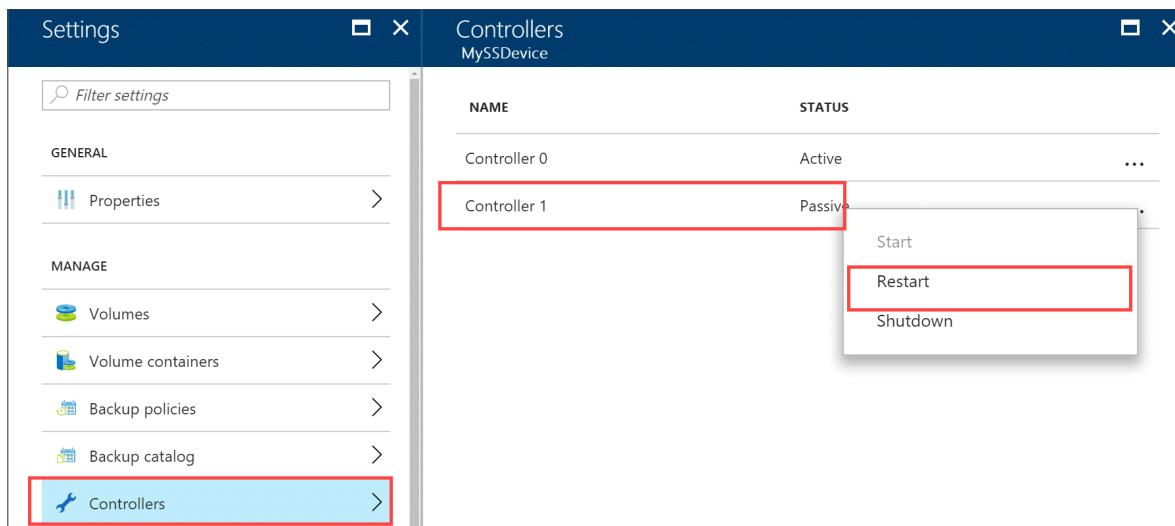
1. In your StorSimple Device Manager service, go to **Devices**. Select your device from the list of devices.



2. Go to **Settings > Controllers**.



3. In the **Controllers** blade, verify that the status of both the controllers on your device is **Healthy**. Select a controller, right-click and then select **Restart** or **Shutdown**.



4. A job is created to restart or shut down the controller and you are presented with applicable warnings, if any. To monitor the restart or shutdown, go to **Service** > **Activity logs** and then filter by parameters specific to your service. If a controller was shut down, then you will need to push the power button to turn on the controller to turn it on.

To restart or shut down a controller in Windows PowerShell for StorSimple

Perform the following steps to shut down or restart a single controller on your StorSimple device from the Windows PowerShell for StorSimple.

1. Access the device via the serial console or a telnet session from a remote computer. To connect to Controller 0 or Controller 1, follow the steps in [Use PuTTY to connect to the device serial console](#).

2. In the serial console menu, choose option 1, **Log in with full access**.
3. In the banner message, make a note of the controller you are connected to (Controller 0 or Controller 1) and whether it is the active or the passive (standby) controller.

- To shut down a single controller, at the prompt, type:

```
Stop-HcsController
```

This shuts down the controller that you are connected to. If you stop the active controller, then the device fails over to the passive controller.

- To restart a controller, at the prompt, type:

```
Restart-HcsController
```

This restarts the controller that you are connected to. If you restart the active controller, it fails over to the passive controller before the restart.

Shut down a StorSimple device

This section explains how to shut down a running or a failed StorSimple device from a remote computer. A device is turned off after both the device controllers are shut down. A device shutdown is done when the device is physically moved, or is taken out of service.

Important

Before you shut down the device, check the health of the device components. Navigate to your device and then click **Settings > Hardware health**. In the **Status and hardware health** blade, verify that the LED status of all the components is green. Only a healthy device has a green status. If your device is being shut down to replace a malfunctioning component, you will see a failed (red) or a degraded (yellow) status for the respective component(s).

To shut down a StorSimple device

1. Use the [restart or shut down a controller](#) procedure to identify and shut down the passive controller on your device. You can perform this operation in the Azure portal or in Windows PowerShell for StorSimple.
2. Repeat the above step to shut down the active controller.

3. You must now look at the back plane of the device. After the two controllers are completely shut down, the status LEDs on both the controllers should be blinking red. If you need to turn off the device completely at this time, flip the power switches on both Power and Cooling Modules (PCMs) to the OFF position. This should turn off the device.

Reset the device to factory default settings

Important

If you need to reset your device to factory default settings, contact Microsoft Support. The procedure described below should be used only in conjunction with Microsoft Support.

This procedure describes how to reset your Microsoft Azure StorSimple device to factory default settings using Windows PowerShell for StorSimple. Resetting a device removes all data and settings from the entire cluster by default.

Perform the following steps to reset your Microsoft Azure StorSimple device to factory default settings:

To reset the device to default settings in Windows PowerShell for StorSimple

1. Access the device through its serial console. Check the banner message to ensure that you are connected to the **Active** controller.
2. In the serial console menu, choose option 1, **Log in with full access**.
3. At the prompt, type the following command to reset the entire cluster, removing all data, metadata, and controller settings:

```
Reset-HcsFactoryDefault
```

To instead reset a single controller, use the [Reset-HcsFactoryDefault](#) cmdlet with the `-scope` parameter.)

The system will reboot multiple times. You will be notified when the reset has successfully completed. Depending on the system model, it can take 45-60 minutes for an 8100 device and 60-90 minutes for an 8600 to finish this process.

Questions and answers about managing device controllers

In this section, we have summarized some of the frequently asked questions regarding managing StorSimple device controllers.

Q. What happens if both the controllers on my device are healthy and turned on and I restart or shut down the active controller?

A. If both the controllers on your device are healthy and turned on, you are prompted for confirmation. You may choose to:

- **Restart the active controller** – You are notified that restarting an active controller caused the device to fail over to the passive controller. The controller restarts.
- **Shut down an active controller** – You are notified that shutting down an active controller results in downtime. You also need to push the power button on the device to turn on the controller.

Q. What happens if the passive controller on my device is unavailable or turned off and I restart or shut down the active controller?

A. If the passive controller on your device is unavailable or turned off, and you choose to:

- **Restart the active controller** – You are notified that continuing the operation will result in a temporary disruption of the service, and you are prompted for confirmation.
- **Shut down an active controller** – You are notified that continuing the operation results in downtime. You also need to push the power button on one or both controllers to turn on the device. You are prompted for confirmation.

Q. When does the controller restart or shutdown fails to progress?

A. Restarting or shutting down a controller may fail if:

- A device update is in progress.
- A controller restart is already in progress.
- A controller shutdown is already in progress.

Q. How can you figure out if a controller was restarted or shut down?

A. You can check the controller status on Controller blade. The controller status will indicate whether a controller is in the process of restarting or shutting down.

Additionally, the **Alerts** blade contain an informational alert if the controller is restarted

or shut down. The controller restart and shutdown operations are also recorded in the activity logs. For more information about activity logs, go to [View the activity logs](#).

Q. Is there any impact to the I/O as a result of controller failover?

A. The TCP connections between initiators and active controller will be reset as a result of controller failover, but will be reestablished when the passive controller assumes operation. There may be a temporary (less than 30 seconds) pause in I/O activity between initiators and the device during the course of this operation.

Q. How do I return my controller to service after it has been shut down and removed?

A. To return a controller to service, you must insert it into the chassis as described in [Replace a controller module on your StorSimple device](#).

Next steps

- If you encounter any issues with your StorSimple device controllers that you cannot resolve by using the procedures listed in this tutorial, [contact Microsoft Support](#).
 - To learn more about using the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).
-

Additional resources

Documentation

[PowerShell for StorSimple device management](#)

Learn how to use Windows PowerShell for StorSimple to manage your StorSimple device.

[Deactivate and delete a StorSimple 8000 series device](#)

Learn how to deactivate and delete a StorSimple device that is connected to a StorSimple Device Manager service.

[Troubleshoot issues during data copies to your Azure Data Box, Azure Data Box Heavy](#)

Describes how to troubleshoot issues when copying data to Azure Data Box and Azure Data Box Heavy devices.

[Troubleshoot share connection failure during data copy to Azure Data Box](#)

Describes how to identify network issues preventing SMB share connections during data copy to an Azure Data Box.

[Connect remotely to your StorSimple device](#)

Explains how to configure your device for remote management and how to connect to Windows PowerShell for StorSimple via HTTP or HTTPS.

[Administer Azure Data Box/Azure Data Box Heavy using local web UI](#)

Describes how to use the local web UI to administer your Data Box and Data Box Heavy devices

[Tutorial to return Azure Data Box](#)

In this tutorial, learn how to return Azure Data Box, including shipping the device, verifying data upload to Azure, and erasing data from Data Box.

[Tutorial: Use data copy service to copy to your device - Azure Data Box](#)

In this tutorial, you learn how to copy data to your Azure Data Box device via the data copy service

[Show 5 more](#)

Configure web proxy for your StorSimple device

Article • 08/19/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial describes how to use Windows PowerShell for StorSimple to configure and view web proxy settings for your StorSimple device. The web proxy settings are used by the StorSimple device when communicating with the cloud. A web proxy server is used to add another layer of security, filter content, cache to ease bandwidth requirements or even help with analytics.

The guidance in this tutorial applies only to StorSimple 8000 series physical devices. Web proxy configuration is not supported on the StorSimple Cloud Appliance (8010 and 8020).

Web proxy is an *optional* configuration for your StorSimple device. You can configure web proxy only via Windows PowerShell for StorSimple. The configuration is a two-step process as follows:

1. You first configure web proxy settings through the setup wizard or Windows PowerShell for StorSimple cmdlets.
2. You then enable the configured web proxy settings via Windows PowerShell for StorSimple cmdlets.

After the web proxy configuration is complete, you can view the configured web proxy settings in both the Microsoft Azure StorSimple Device Manager service and the Windows PowerShell for StorSimple.

After reading this tutorial, you will be able to:

- Configure web proxy by using setup wizard and cmdlets.
- Enable web proxy by using cmdlets.
- View web proxy settings in the Azure portal.
- Troubleshoot errors during web proxy configuration.

Configure web proxy via Windows PowerShell for StorSimple

You use either of the following to configure web proxy settings:

- Setup wizard to guide you through the configuration steps.
- Cmdlets in Windows PowerShell for StorSimple.

Each of these methods is discussed in the following sections.

Configure web proxy via the setup wizard

Use the setup wizard to guide you through the steps for web proxy configuration. Perform the following steps to configure web proxy on your device.

To configure web proxy via the setup wizard

1. In the serial console menu, choose option 1, **Log in with full access** and provide the **device administrator password**. Type the following command to start a setup wizard session:

```
Invoke-HcsSetupWizard
```

2. If this is the first time that you have used the setup wizard for device registration, you need to configure all the required network settings until you reach the web proxy configuration. If your device is already registered, accept all the configured network settings until you reach the web proxy configuration. In the setup wizard, when prompted to configure web proxy settings, type **Yes**.
3. For the **Web Proxy URL**, specify the IP address or the fully qualified domain name (FQDN) of your web proxy server and the TCP port number that you would like your device to use when communicating with the cloud. Use the following format:

```
http://<IP address or FQDN of the web proxy server>:<TCP port number>
```

By default, TCP port number 8080 is specified.

4. Choose the authentication type as **NTLM**, **Basic**, or **None**. Basic is the least secure authentication for the proxy server configuration. NT LAN Manager (NTLM) is a highly secure and complex authentication protocol that uses a three-way messaging system (sometimes four if additional integrity is required) to authenticate a user. The default authentication is NTLM. For more information, see [Basic](#) and [NTLM authentication](#).

Important

In the StorSimple Device Manager service, the device monitoring charts do not work when Basic or NTLM authentication is enabled in the proxy server configuration for the device. For the monitoring charts to work, you need to ensure that authentication is set to NONE.

5. If you enabled the authentication, supply a **Web Proxy Username** and a **Web Proxy Password**. You also need to confirm the password.



If you are registering your device for the first time, continue with the registration. If your device was already registered, the wizard exits. The configured settings are saved.

Web proxy is now enabled. You can skip the [Enable web proxy](#) step and go directly to [View web proxy settings in the Azure portal](#).

Configure web proxy via Windows PowerShell for StorSimple cmdlets

An alternate way to configure web proxy settings is via the Windows PowerShell for StorSimple cmdlets. Perform the following steps to configure web proxy.

To configure web proxy via cmdlets

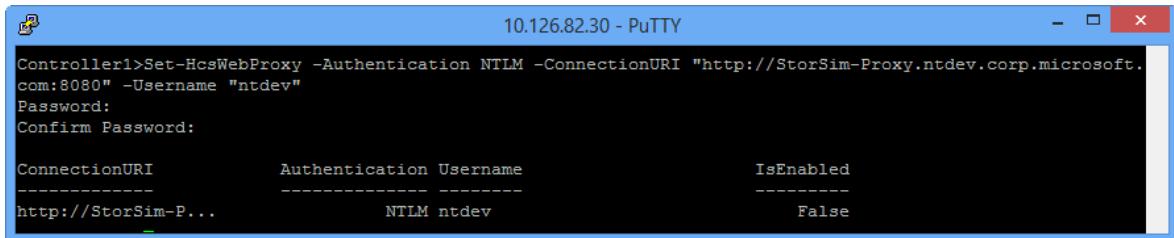
1. In the serial console menu, choose option 1, **Log in with full access**. When prompted, provide the **device administrator password**. The default password is

`Password1.`

2. At the command prompt, type:

```
Set-HcsWebProxy -Authentication NTLM -ConnectionURI "http://<IP address or  
FQDN of web proxy server>:<TCP port number>" -Username "<Username for web  
proxy server>"
```

Provide and confirm the password when prompted.



ConnectionURI	Authentication	Username	IsEnabled
http://StorSim-P...	NTLM	ntdev	False

The web proxy is now configured and needs to be enabled.

Enable web proxy

Web proxy is disabled by default. After you configure the web proxy settings on your StorSimple device, use the Windows PowerShell for StorSimple to enable the web proxy settings.

 **Note**

This step is not required if you used the setup wizard to configure web proxy.
Web proxy is automatically enabled by default after a setup wizard session.

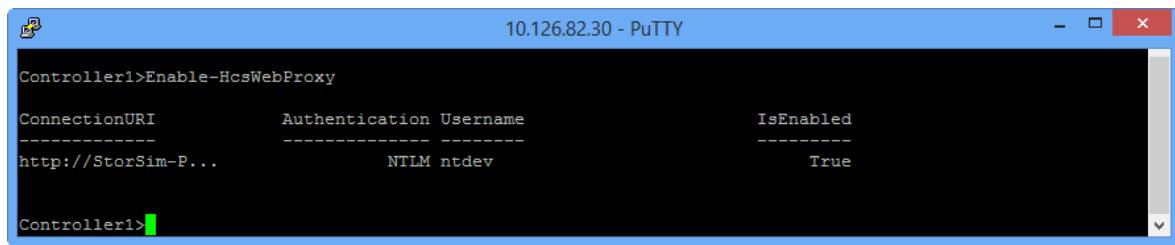
Perform the following steps in Windows PowerShell for StorSimple to enable web proxy on your device:

To enable web proxy

1. In the serial console menu, choose option 1, **Log in with full access**. When prompted, provide the **device administrator password**. The default password is `Password1.`
2. At the command prompt, type:

```
Enable-HcsWebProxy
```

You have now enabled the web proxy configuration on your StorSimple device.



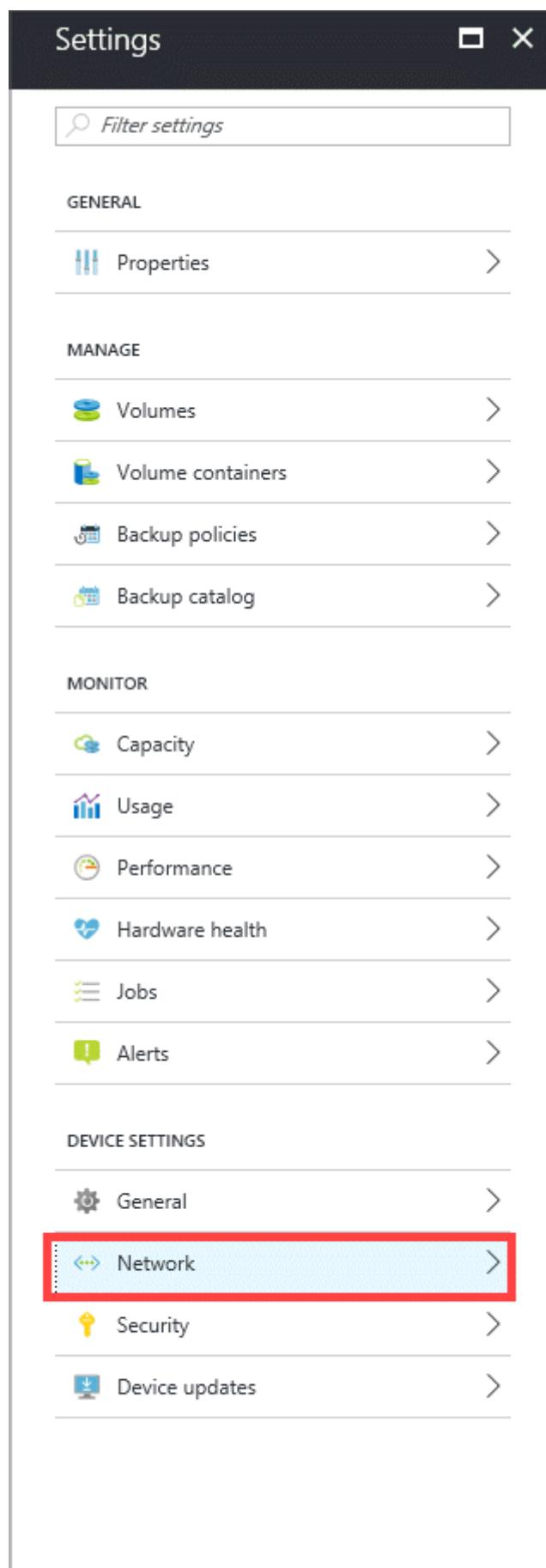
```
Controller1>Enable-HcsWebProxy
ConnectionURI          Authentication Username      IsEnabled
-----                  ----- ----- -----
http://StorSim-P...      NTLM ntdev              True
Controller1>
```

View web proxy settings in the Azure portal

The web proxy settings are configured through the Windows PowerShell interface and cannot be changed from within the portal. You can, however, view these configured settings in the portal. Perform the following steps to view web proxy.

To view web proxy settings

1. Navigate to **StorSimple Device Manager service > Devices**. Select and click a device and then go to **Device settings > Network**.



2. In the **Network** settings blade, click the **Web proxy** tile.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and lists various management options under sections like GENERAL, MANAGE, MONITOR, and DEVICE SETTINGS. The 'Network' option in the DEVICE SETTINGS section is highlighted with a red box. The right window is titled 'Network settings' and displays network interface details for DATA 0 through DATA 5, along with DNS settings and a Web proxy configuration section. The 'Web proxy' section is also highlighted with a red box.

Settings

Filter settings

GENERAL

Properties >

MANAGE

Volumes >

Volume containers >

Backup policies >

Backup catalog >

MONITOR

Capacity >

Usage >

Performance >

Hardware health >

Jobs >

Alerts >

DEVICE SETTINGS

General >

Network >

Security >

Device updates >

Network settings
8100-SHX0991003G44MT

DNS settings

DNS SETTINGS
10.222.118.154

Network interface

DATA 0
10.126.173.90

DATA 1
Configure

DATA 2
Configure

DATA 3
Configure

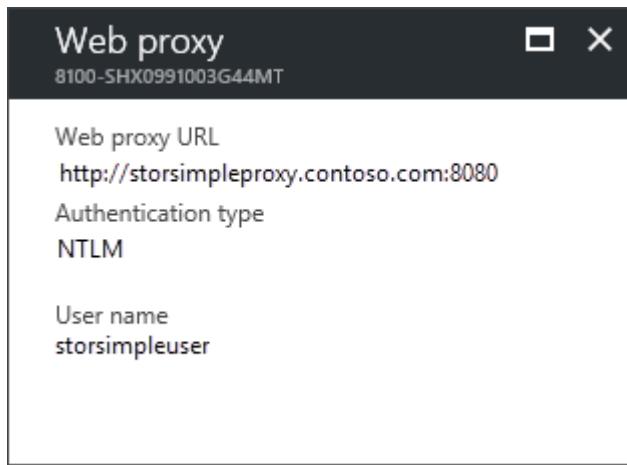
DATA 4
Configure

DATA 5
Configure

Web proxy

WEB PROXY
Not configured

3. In the **Web proxy** blade, review the configured web proxy settings on your StorSimple device.



Errors during web proxy configuration

If the web proxy settings are configured incorrectly, error messages are displayed to the user in Windows PowerShell for StorSimple. The following table explains some of these error messages, their probable causes, and recommended actions.

Serial no.	HRESULT error Code	Possible root cause	Recommended action
1.	0x80070001	Command is run from the passive controller and it is not able to communicate with the active controller.	Run the command on the active controller. To run the command from the passive controller, you must fix the connectivity from passive to active controller. You must engage Microsoft Support if this connectivity is broken.
2.	0x800710dd	Proxy settings are not supported on StorSimple Cloud Appliance. These can only be configured on a StorSimple physical device. - The operation identifier is not valid	Proxy settings are not supported on StorSimple Cloud Appliance. These can only be configured on a StorSimple physical device.
3.	0x80070057	One of the parameters provided for the proxy settings is not valid. - Invalid parameter	The URI is not provided in correct format. Use the following format: <code>http://<IP address or FQDN of the web proxy server>:<TCP port number></code>

Serial no.	HRESULT error Code	Possible root cause	Recommended action
4.	0x800706ba - RPC server not available	The root cause is one of the following: Cluster is not up. Datapath service is not running. The command is run from passive controller and it is not able to communicate with the active controller.	Engage Microsoft Support to ensure that the cluster is up and datapath service is running. Run the command from the active controller. If you want to run the command from the passive controller, you must ensure that the passive controller can communicate with the active controller. You must engage Microsoft Support if this connectivity is broken.
5.	0x800706be - RPC call failed	Cluster is down.	Engage Microsoft Support to ensure that the cluster is up.
6.	0x8007138f - Cluster resource not found	Platform service cluster resource is not found. This can happen when the installation was not proper.	You may need to perform a factory reset on your device. You may need to create a platform resource. Contact Microsoft Support for next steps.
7.	0x8007138c - Cluster resource not online	Platform or datapath cluster resources are not online.	Contact Microsoft Support to help ensure that the datapath and platform service resource are online.

① Note

- The above list of error messages is not exhaustive.
- Errors related to web proxy settings will not be displayed in the Azure portal in your StorSimple Device Manager service. If there is an issue with web proxy after the configuration is completed, the device status will change to **Offline** in the classic portal.|

Next Steps

- If you experience any issues while deploying your device or configuring web proxy settings, refer to [Troubleshoot your StorSimple device deployment](#).
- To learn how to use the StorSimple Device Manager service, go to [Use the StorSimple Device Manager service to administer your StorSimple device](#).

Modify the DATA 0 network interface settings on your StorSimple 8000 series device

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Your Microsoft Azure StorSimple device has six network interfaces, from DATA 0 to DATA 5. The DATA 0 interface is always configured through the Windows PowerShell interface or the serial console, and is automatically cloud-enabled. Note that you cannot configure DATA 0 network interface through the Azure portal.

The DATA 0 interface is first configured through the setup wizard during initial deployment of the StorSimple device. When the device is in an operational mode, you may need to reconfigure DATA 0 settings. This tutorial provides two methods to modify DATA 0 network settings, both through Windows PowerShell for StorSimple.

After reading this tutorial, you will be able to:

- Modify DATA 0 network setting through the setup wizard
- Modify DATA 0 network settings through the `Set-HcsNetInterface` cmdlet

Modify DATA 0 network settings through setup wizard

You can reconfigure DATA 0 network settings by connecting to the Windows PowerShell interface of your StorSimple device and launching a setup wizard session. Perform the following steps to modify DATA 0 settings:

To modify DATA 0 network settings through setup wizard

1. In the serial console menu, choose option 1, **Log in with full access**. When prompted provide the device administrator password. The default password is **Password1**.

2. At the command prompt, type:

```
Invoke-HcsSetupWizard
```

3. A setup wizard appears to help configure the DATA 0 interface of your device. Provide new values for the IP address, gateway, and netmask.

Note

The fixed controllers IPs will need to be reconfigured through the **Network settings** blade of the StorSimple device in the Azure portal. For more information, go to [Modify network interfaces](#).

Modify DATA 0 network settings through Set-HcsNetInterface cmdlet

An alternate way to reconfigure DATA 0 network interface is through the use of the **Set-HcsNetInterface** cmdlet. The cmdlet is executed from the Windows PowerShell interface of your StorSimple device. When using this procedure, the controller fixed IPs can also be configured here. Perform the following steps to modify the DATA 0 settings:

To modify DATA 0 network settings through the Set-HcsNetInterface cmdlet

1. In the serial console menu, choose option 1, **Log in with full access**. When prompted provide the device administrator password. The default password is **Password1**.

2. At the command prompt, type:

```
Set-HCSNetInterface -InterfaceAlias Data0 -IPv4Address <> -IPv4Netmask <> -  
IPv4Gateway <> -Controller0IPv4Address <> -Controller1IPv4Address <> -  
IsiScsiEnabled 1 -IsCloudEnabled 1
```

In the angled brackets, type the following values for DATA 0:

- IPv4 address
- IPv4 gateway
- IPv4 subnet mask
- Fixed IPv4 address for Controller 0
- Fixed IPv4 address for Controller 1

For more information on the use of this cmdlet, go to [Windows PowerShell for StorSimple cmdlet reference](#).

Next steps

- To configure network interfaces other than DATA 0, you can use the [Configure network settings in the Azure portal](#).
- If you experience any issues when configuring your network interfaces, refer to [Troubleshoot deployment issues](#).

Use StorSimple Snapshot Manager to administer your StorSimple solution

Article • 08/22/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

StorSimple Snapshot Manager is a Microsoft Management Console (MMC) snap-in that simplifies data protection and backup management in a Microsoft Azure StorSimple environment. With StorSimple Snapshot Manager, you can manage Microsoft Azure StorSimple data in the data center and in the cloud as a single integrated storage solution, thus simplifying backup processes and reducing costs.

The StorSimple Snapshot Manager central management console enables you to create consistent, point-in-time backup copies of local and cloud data. For example, you can use the console to:

- Configure, back up, and delete volumes.
- Configure volume groups to ensure that backed up data is application-consistent.
- Manage backup policies so that data is backed up on a predetermined schedule.
- Create independent copies of data, which can be stored in the cloud and used for disaster recovery.

This article provides links to tutorials that describe StorSimple Snapshot Manager and how to use it to complete system administration tasks and workflows.

- For more information about StorSimple Snapshot Manager components and architecture, see [What is StorSimple Snapshot Manager?](#)
- To download StorSimple Snapshot Manager, go to [the StorSimple Snapshot Manager download page](#).

- For StorSimple Snapshot Manager deployment procedures, go to [Deploy StorSimple Snapshot Manager](#).

① Note

You cannot use StorSimple Snapshot Manager to manage Microsoft Azure StorSimple Virtual Arrays (also known as StorSimple on-premises virtual devices).

StorSimple Snapshot Manager tasks and workflows

You can use the StorSimple Snapshot Manager to monitor and manage current, scheduled, and completed backup jobs. Additionally, StorSimple Snapshot Manager provides a catalog of up to 64 completed backups. You can use the catalog to find and restore volumes or individual files.

IF YOU WANT TO DO THIS...	USE THIS TUTORIAL...
Learn more about StorSimple Snapshot Manager	What is StorSimple Snapshot Manager?
Install StorSimple Snapshot Manager Reinstall StorSimple Snapshot Manager Remove StorSimple Snapshot Manager	Deploy StorSimple Snapshot Manager
Use StorSimple Snapshot Manager menus and features: <ul style="list-style-type: none">• Menu bar• Tool bar• Scope pane• Results pane• Actions pane• Keyboard navigation and shortcuts	StorSimple Snapshot Manager user interface
Use the common MMC features included in StorSimple Snapshot Manager: <ul style="list-style-type: none">• View• New Window from Here• Refresh• Export List• Help	Use the MMC menu actions in StorSimple Snapshot Manager

IF YOU WANT TO DO THIS...	USE THIS TUTORIAL...
Add or replace a device Connect a device Verify imported volume groups Refresh connected devices Authenticate a device View device details Delete a device configuration Change a device password Replace a failed device	Use StorSimple Snapshot Manager to connect and manage StorSimple devices
Mount volumes View information about volumes Delete a volume Rescan volumes Configure and back up a basic volume Configure and backup a dynamic mirrored volume	Use StorSimple Snapshot Manager to view and manage volumes
View volume groups Create a volume group Back up a volume group Edit a volume group Delete a volume group	Use StorSimple Snapshot Manager to create and manage volume groups
Create a backup policy Edit a backup policy Delete a backup policy	Use StorSimple Snapshot Manager to create and manage backup policies
View and manage scheduled backup jobs View and manage recent backup jobs View and manage currently running backup jobs	Use StorSimple Snapshot Manager to view and manage backup jobs
Restore a volume Clone a volume or volume group Delete a backup Recover a file Restore the StorSimple Snapshot Manager database	Use StorSimple Snapshot Manager to manage the backup catalog

Next steps

[Download StorSimple Snapshot Manager](#).

An introduction to StorSimple Snapshot Manager

Article • 08/22/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

StorSimple Snapshot Manager is a Microsoft Management Console (MMC) snap-in that simplifies data protection and backup management in a Microsoft Azure StorSimple environment. With StorSimple Snapshot Manager, you can manage Microsoft Azure StorSimple data in the data center and in the cloud as a single integrated storage solution, thus simplifying backup processes and reducing costs.

This overview introduces the StorSimple Snapshot Manager, describes its features, and explains its role in Microsoft Azure StorSimple.

For an overview of the entire Microsoft Azure StorSimple system, including the StorSimple device, StorSimple Manager service, StorSimple Snapshot Manager, and StorSimple Adapter for SharePoint, see [StorSimple 8000 series: a hybrid cloud storage solution](#).

ⓘ Note

- You cannot use StorSimple Snapshot Manager to manage Microsoft Azure StorSimple Virtual Arrays (also known as StorSimple on-premises virtual devices).
- If you plan to install StorSimple Update 2 on your StorSimple device, be sure to download the latest version of StorSimple Snapshot Manager and install it **before you install StorSimple Update 2**. The latest version of StorSimple

Snapshot Manager is backward compatible and works with all released versions of Microsoft Azure StorSimple. If you are using the previous version of StorSimple Snapshot Manager, you will need to update it (you do not need to uninstall the previous version before you install the new version).

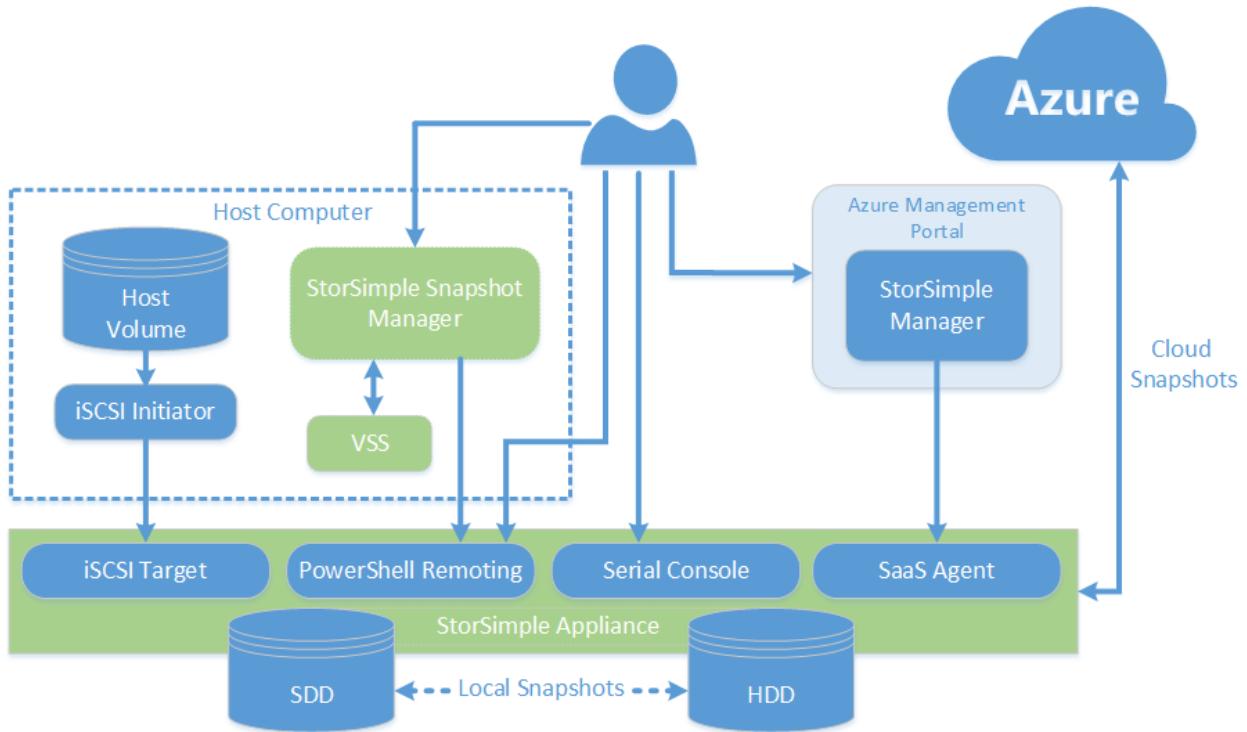
StorSimple Snapshot Manager purpose and architecture

StorSimple Snapshot Manager provides a central management console that you can use to create consistent, point-in-time backup copies of local and cloud data. For example, you can use the console to:

- Configure, back up, and delete volumes.
- Configure volume groups to ensure that backed up data is application-consistent.
- Manage backup policies so that data is backed up on a predetermined schedule.
- Create local and cloud snapshots, which can be stored in the cloud and used for disaster recovery.

The StorSimple Snapshot Manager fetches the list of applications registered with the VSS provider on the host. Then, to create application-consistent backups, it checks the volumes used by an application and suggests volume groups to configure. StorSimple Snapshot Manager uses these volume groups to generate backup copies that are application-consistent. (Application consistency exists when all related files and databases are synchronized and represent the true state of the application at a specific point in time.)

StorSimple Snapshot Manager backups take the form of incremental snapshots, which capture only the changes since the last backup. As a result, backups require less storage and can be created and restored quickly. StorSimple Snapshot Manager uses the Windows Volume Shadow Copy Service (VSS) to ensure that snapshots capture application-consistent data. (For more information, go to the Integration with Windows Volume Shadow Copy Service section.) With StorSimple Snapshot Manager, you can create backup schedules or take immediate backups as needed. If you need to restore data from a backup, StorSimple Snapshot Manager lets you select from a catalog of local or cloud snapshots. Azure StorSimple restores only the data that is needed as it is needed, which prevents delays in data availability during restore operations.)



StorSimple Snapshot Manager architecture

Support for multiple volume types

You can use the StorSimple Snapshot Manager to configure and back up the following types of volumes:

- **Basic volumes** – A basic volume is a single partition on a basic disk.
- **Simple volumes** – A simple volume is a dynamic volume that contains disk space from a single dynamic disk. A simple volume consists of a single region on a disk or multiple regions that are linked together on the same disk. (You can create simple volumes only on dynamic disks.) Simple volumes are not fault tolerant.
- **Dynamic volumes** – A dynamic volume is a volume created on a dynamic disk. Dynamic disks use a database to track information about volumes that are contained on dynamic disks in a computer.
- **Dynamic volumes with mirroring** – Dynamic volumes with mirroring are built on the RAID 1 architecture. With RAID 1, identical data is written on two or more disk, producing a mirrored set. A read request can then be handled by any disk that contains the requested data.
- **Cluster-shared volumes** – With cluster-shared volumes (CSVs), multiple nodes in a failover cluster can simultaneously read or write to the same disk. Failover from one node to another node can occur quickly, without requiring a change in drive ownership or mounting, dismounting, and removing a volume.

Important

Do not mix CSVs and non-CSVs in the same snapshot. Mixing CSVs and non-CSVs in a snapshot is not supported.

You can use StorSimple Snapshot Manager to restore entire volume groups or clone individual volumes and recover individual files.

- [Volumes and volume groups](#)
- [Backup types and backup policies](#)

For more information about StorSimple Snapshot Manager features and how to use them, see [StorSimple Snapshot Manager user interface](#).

Volumes and volume groups

With StorSimple Snapshot Manager, you create volumes and then configure them into volume groups.

StorSimple Snapshot Manager uses volume groups to create backup copies that are application-consistent. Application consistency exists when all related files and databases are synchronized and represent the true state of an application at a specific point in time. Volume groups (which are also known as *consistency groups*) form the basis of a backup or restore job.

Volume groups are not the same as volume containers. A volume container contains one or more volumes that share a cloud storage account and other attributes, such as encryption and bandwidth consumption. A single volume container can contain up to 256 thinly provisioned StorSimple volumes. For more information about volume containers, go to [Manage your volume containers](#). Volume groups are collections of volumes that you configure to facilitate backup operations. If you select two volumes that belong to different volume containers, place them in a single volume group, and then create a backup policy for that volume group, each volume will be backed up in the appropriate volume container, using the appropriate storage account.

Note

All volumes in a volume group must come from a single cloud service provider.

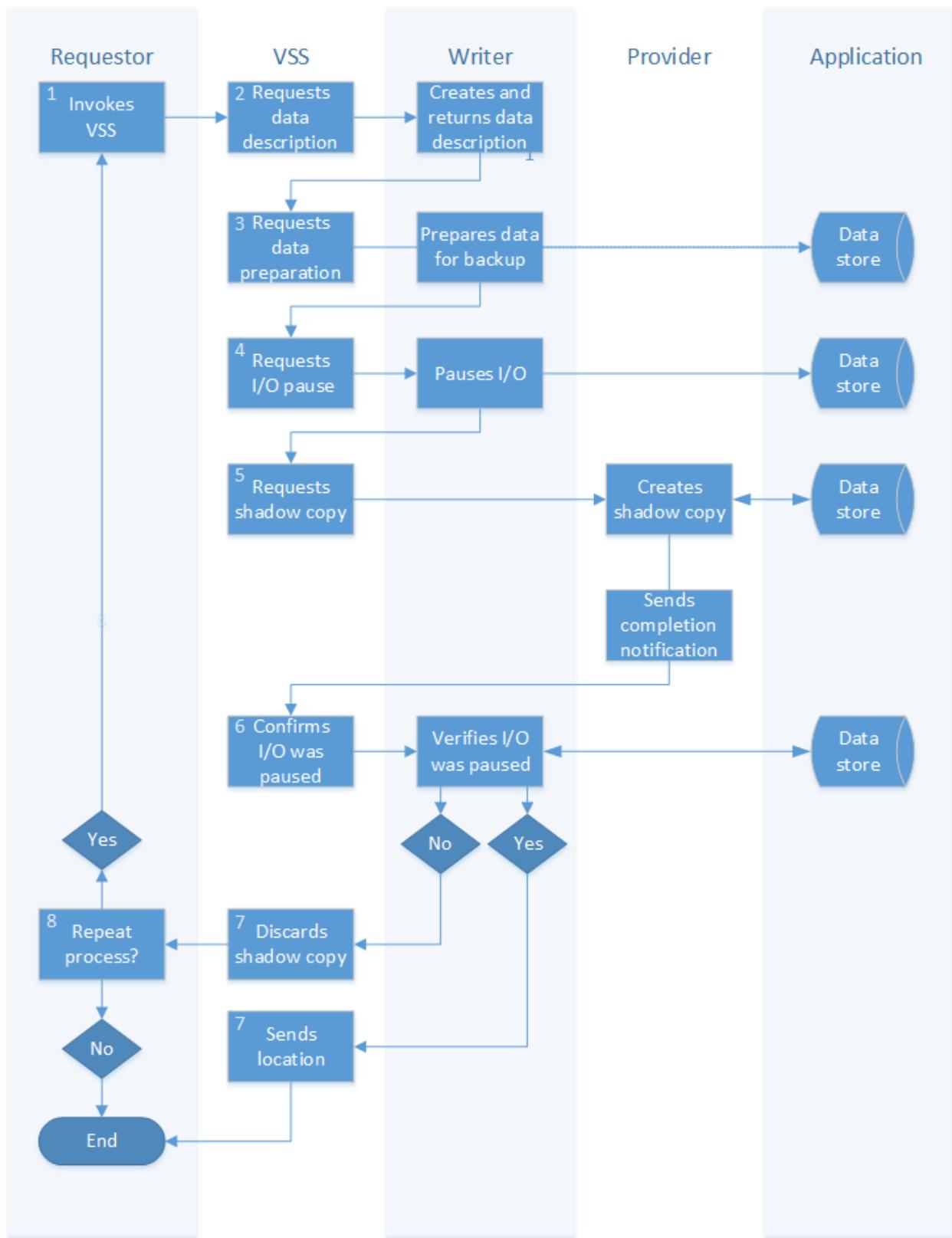
Integration with Windows Volume Shadow Copy Service

StorSimple Snapshot Manager uses the Windows Volume Shadow Copy Service (VSS) to capture application-consistent data. VSS facilitates application consistency by communicating with VSS-aware applications to coordinate the creation of incremental snapshots. VSS ensures that the applications are temporarily inactive, or quiescent, when snapshots are taken.

The StorSimple Snapshot Manager implementation of VSS works with SQL Server and generic NTFS volumes. The process is as follows:

1. A requestor, which is typically a data management and protection solution (such as StorSimple Snapshot Manager) or a backup application, invokes VSS and asks it to gather information from the writer software in the target application.
2. VSS contacts the writer component to retrieve a description of the data. The writer returns the description of the data to be backed up.
3. VSS signals the writer to prepare the application for backup. The writer prepares the data for backup by completing open transactions, updating transaction logs, and so on, and then notifies VSS.
4. VSS instructs the writer to temporarily stop the application's data stores and make sure that no data is written to the volume while the shadow copy is created. This step ensures data consistency, and takes no more than 60 seconds.
5. VSS instructs the provider to create the shadow copy. Providers, which can be software- or hardware-based, manage the volumes that are currently running and create shadow copies of them on demand. The provider creates the shadow copy, and notifies VSS when it is completed.
6. VSS contacts the writer to notify the application that I/O can resume and also to confirm that I/O was paused successfully during shadow copy creation.
7. If the copy was successful, VSS returns the copy's location to the requestor.
8. If data was written while the shadow copy was created, then the backup will be inconsistent. VSS deletes the shadow copy and notifies the requestor. The requestor can either repeat the backup process automatically or notify the administrator to retry it at a later time.

See the following illustration.



Windows Volume Shadow Copy Service process

Backup types and backup policies

With StorSimple Snapshot Manager, you can back up data and store it locally and in the cloud. You can use StorSimple Snapshot Manager to back up data immediately, or you can use a backup policy to create a schedule for taking backups automatically. Backup policies also enable you to specify how many snapshots will be retained.

Backup types

You can use StorSimple Snapshot Manager to create the following types of backups:

- **Local snapshots** – Local snapshots are point-in-time copies of volume data that are stored on the StorSimple device. Typically, this type of backup can be created and restored quickly. You can use a local snapshot as you would a local backup copy.
- **Cloud snapshots** – Cloud snapshots are point-in-time copies of volume data that are stored in the cloud. A cloud snapshot is equivalent to a snapshot replicated on a different, off-site storage system. Cloud snapshots are particularly useful in disaster recovery scenarios.

On-demand and scheduled backups

With StorSimple Snapshot Manager, you can initiate a one-time backup to be created immediately, or you can use a backup policy to schedule recurring backup operations.

A backup policy is a set of automated rules that you can use to schedule regular backups. A backup policy allows you to define the frequency and parameters for taking snapshots of a specific volume group. You can use policies to specify start and expiration dates, times, frequencies, and retention requirements, for both local and cloud snapshots. A policy is applied immediately after you define it.

You can use StorSimple Snapshot Manager to configure or reconfigure backup policies whenever necessary.

You configure the following information for each backup policy that you create:

- **Name** – The unique name of the selected backup policy.
- **Type** – The type of backup policy; either local snapshot or cloud snapshot.
- **Volume group** – The volume group to which the selected backup policy is assigned.
- **Retention** – The number of backup copies to retain. If you check the **All** box, all backup copies are retained until the maximum number of backup copies per volume is reached, at which point the policy will fail and generate an error message. Alternatively, you can specify a number of backups to retain (between 1 and 64).
- **Date** – The date when the backup policy was created.

For information about configuring backup policies, go to [Use StorSimple Snapshot Manager to create and manage backup policies](#).

Backup job monitoring and management

You can use the StorSimple Snapshot Manager to monitor and manage upcoming, scheduled, and completed backup jobs. Additionally, StorSimple Snapshot Manager provides a catalog of up to 64 completed backups. You can use the catalog to find and restore volumes or individual files.

For information about monitoring backup jobs, go to [Use StorSimple Snapshot Manager to view and manage backup jobs](#).

Next steps

- Learn more about [using StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Download [StorSimple Snapshot Manager](#).

Use StorSimple Snapshot Manager user interface to manage backup jobs and backup catalog

Article • 08/22/2022 • 21 minutes to read

⊗ Caution

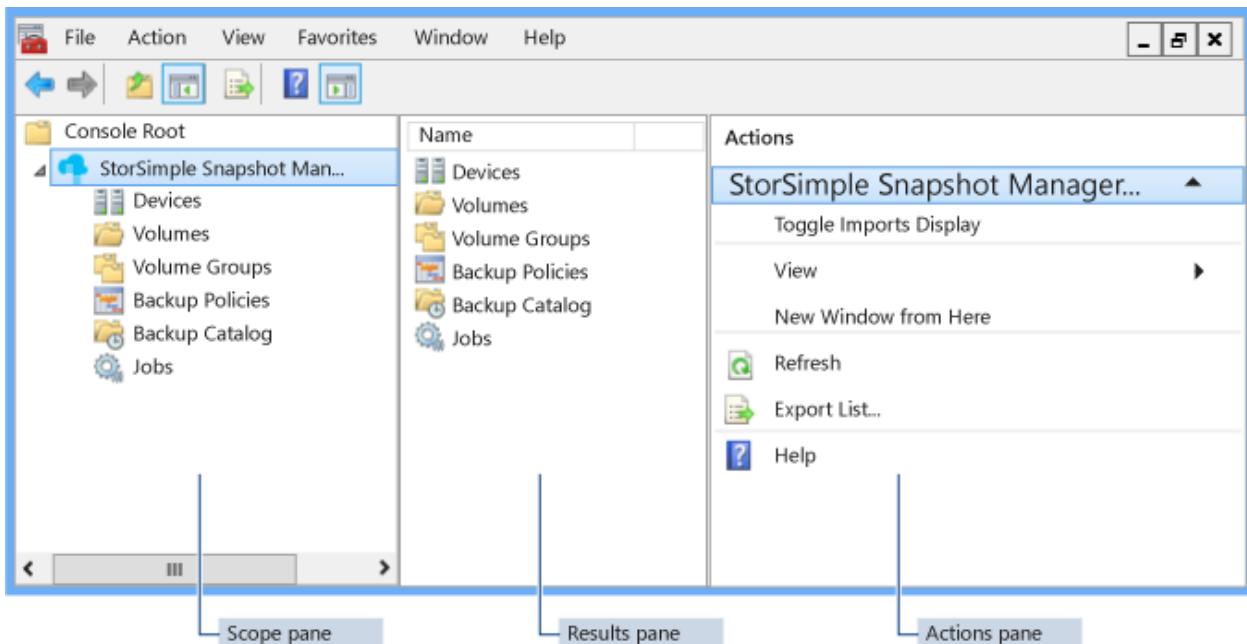
ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Snapshot Manager has an intuitive user interface that you can use to take and manage backups. This tutorial provides an introduction to the user interface, and then explains how to use each of the components. For a detailed description of the StorSimple Snapshot Manager, see [What is StorSimple Snapshot Manager?](#)

Console description

To view the user interface, click the StorSimple Snapshot Manager icon on your desktop. The console window appears, as shown in the following illustration.



The console window has five major elements. Click the appropriate link for a complete description of each element.

- [Menu bar](#)
- [Tool bar](#)
- [Scope pane](#)
- [Results pane](#)
- [Actions pane](#)

Additionally, the StorSimple Snapshot Manager supports [keyboard navigation](#) and a number of [shortcuts](#).

Console accessibility

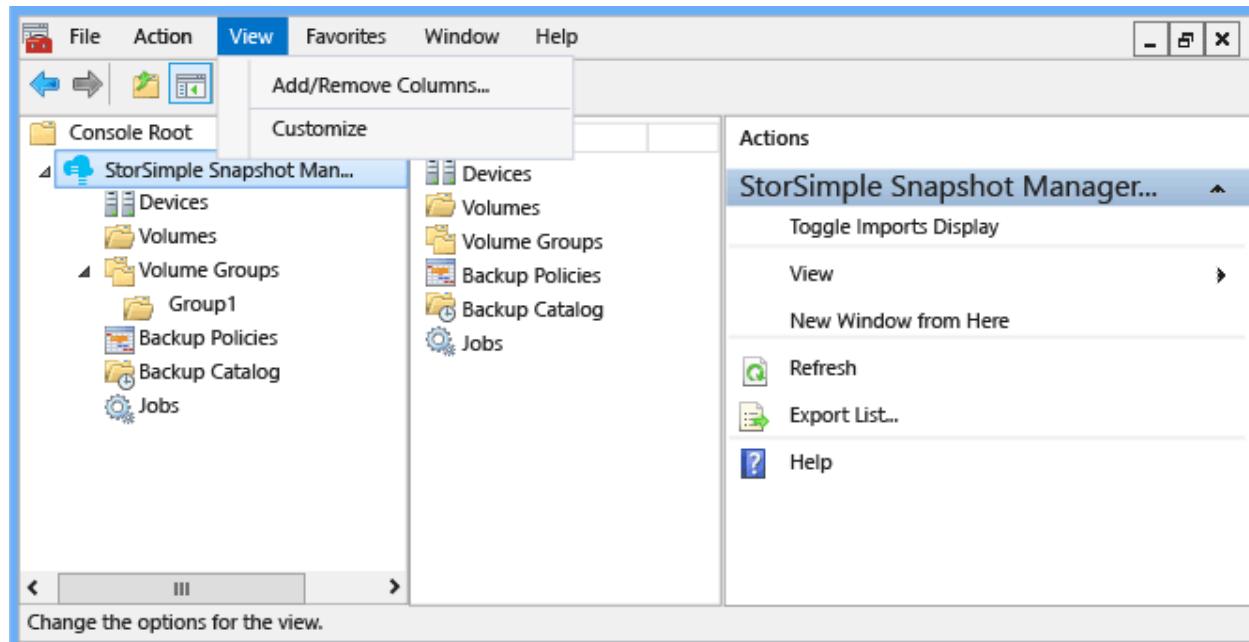
The StorSimple Snapshot Manager user interface supports the accessibility features provided by the Windows operating system and the Microsoft Management Console (MMC), as well as some StorSimple Snapshot Manager-specific keyboard shortcuts.

- For a description of the Windows accessibility features, go to [Keyboard shortcuts for Windows ↗](#).
- For a description of the MMC accessibility features, go to [Accessibility for MMC 3.0](#).
- For a description of the StorSimple Snapshot Manager accessibility features, go to [Keyboard navigation and shortcuts](#).

Menu bar

The menu bar at the top of the console window contains [File](#), [Action](#), [View](#), [Favorites](#), [Window](#), and [Help](#) menus.

Click any item on the menu bar to see a list of available commands on that menu. The following example shows the **View** menu selected on the menu bar.

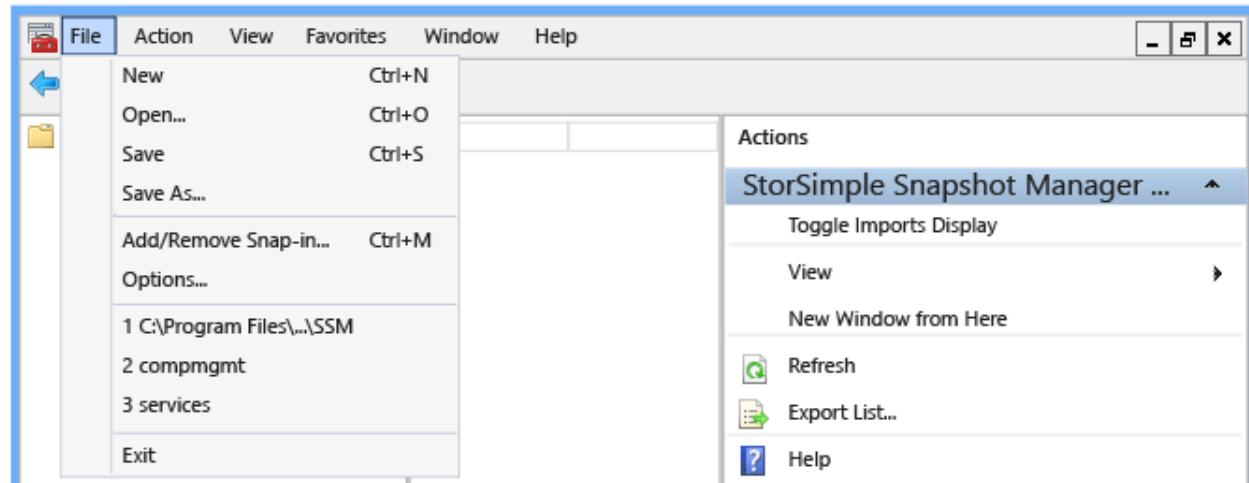


File menu

The **File** menu contains standard Microsoft Management Console (MMC) commands.

Menu access

To view the **File** menu, click **File** on the menu bar. The following menu appears.



Menu description

The following table describes items that appear on the **File** menu.

Menu item	Description
-----------	-------------

Menu item	Description
New	Click New to create a new console based on the StorSimple Snapshot Manager.
Open	Click Open to open an existing console.
Save	Click Save to save the current console.
Save as	Click Save As to create a new, renamed instance of the current console. Use the Save As option to customize a view and save it for later retrieval. For example, you could create StorSimple Snapshot Manager snap-ins that point to specific servers.
Add/Remove Snap-in	Click Add/Remove Snap-in to add or remove snap-ins and to organize nodes in the Scope pane. For more information, go to Add, Remove, and Organize Snap-ins and Extensions in MMC 3.0 .
Options	Click Options to change the console icon, specify user access modes and permissions, or delete console files to increase available disk space.
List of file paths	Click a path in the numbered list to reopen a file that you recently opened.
Exit	Click Exit to close the File menu.

Action menu

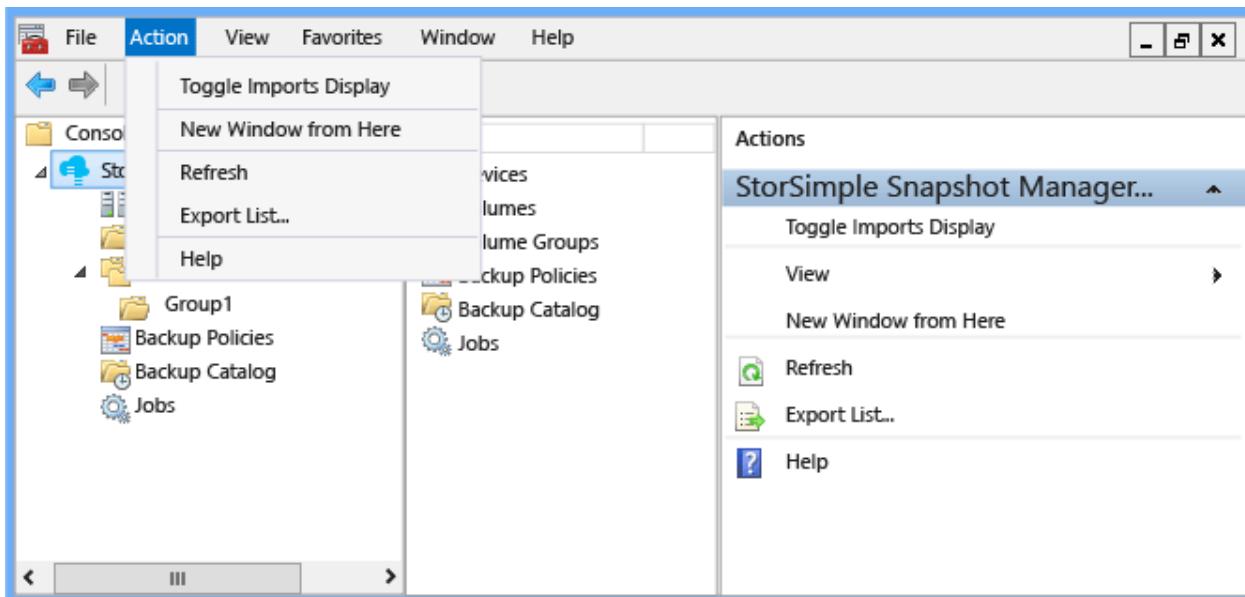
Use the **Action** menu to select from available actions. The items available to you depend on the selection you make in the **Scope** pane or **Results** pane.

Menu access

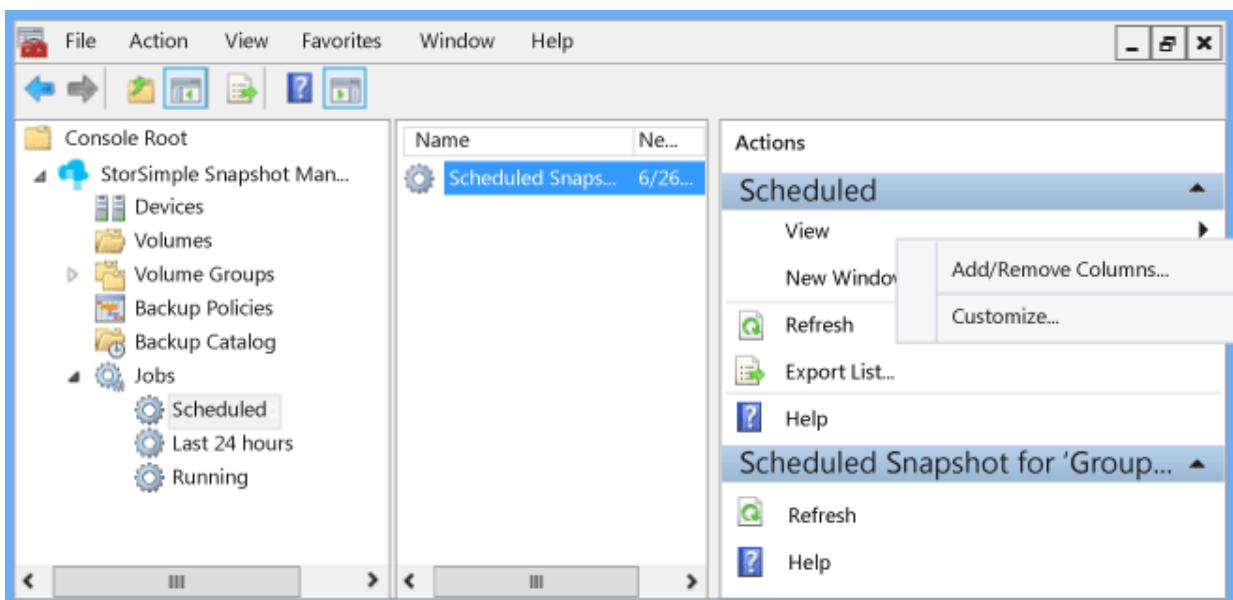
To view the **Action** menu, do one of the following:

- Right-click an item in the **Scope** pane or **Results** pane.
- Select an item in the **Scope** pane or **Results** pane, and then click **Action** on the menu bar.

For example, if you select the top node in the **Scope** pane, and then right-click or click **Action** in the menu bar, the following menu appears.



The **Actions** pane (on the right of the console) contains the same list of actions as the **Action** menu. Additionally, the **Actions** pane contains the **View** menu options, which enable you to create a custom view of the **Results** pane.



Menu description

The following table contains an alphabetical list of StorSimple Snapshot Manager actions.

- The **Action** column lists actions that you can perform on nodes and results.
- The **Navigation** column explains how to display the appropriate **Action** menu so that you can select the action. Some actions appear in multiple **Action** menus. For these actions, select one **Navigation** option from the bulleted list.
- The **Description** column describes how to use each action on the **Action** menu or Actions pane, and explains what it does.

Note

The **Actions** pane and **Action** menus contain additional options, such as **View**, **New Window from here**, **Refresh**, **Export List**, and **Help**. These options are available as a part of the MMC, and are not specific to StorSimple Snapshot Manager. The table includes descriptions of these options.

Action	Navigation	Description
Authenticate	Click the Devices node, and right-click a device in the Results pane.	Click Authenticate to enter the password that you configured for the device.
Clone	Expand Backup Catalog , expand Cloud Snapshots , click a dated backup, and then select a volume in the Results pane.	Click Clone to create a copy of a cloud snapshot and store it in a location that you designate.
Configure a Device	Right-click the Devices node.	Click Configure a Device to configure a single device or multiple devices to connect to the Windows host.
Create Backup Policy	Do one of the following: <ul style="list-style-type: none">• Right-click Backup Policies.• Click or expand Volume Groups, and then right-click a volume group.• Click or expand Backup Catalog, and then right-click a volume group.	Click Create Backup Policy to configure a scheduled backup for a volume group.
Create Volume Group	Do one of the following: <ul style="list-style-type: none">• Click the Volumes node, and then right-click a volume in the Results pane.• Right-click the Volume Groups node.	Click Create Volume Group to assign volumes to a volume group.
Delete	Click a node or result (This item appears on many Action menus and Actions panes.)	Click Delete to delete the node or result that you selected. When the confirmation dialog box appears, confirm or cancel the deletion.
Details	Click the Devices node, and then right-click a device in the Results pane.	Click Details to see the configuration details for a device.

Action	Navigation	Description
Edit	Click Backup Policies , and then right-click a policy in the Results pane.	Click Edit to change the backup schedule for a volume group.
Export List	Click any node or result (This item appears on all Action menus and Actions panes.)	Click Export List to save a list in a comma-separated value (CSV) file. You can then import this file into a spreadsheet application for analysis.
Help	Click any node or result. (This item appears on all Action menus and Actions panes.)	Click Help to open online Help in a separate browser window.
New Window from Here	Click any node or result (This item appears on all Action menus and Actions panes.)	Click New Window from Here to open a new StorSimple Snapshot Manager window.
Refresh	Click any node or result (This item appears on all Action menus and Actions panes.)	Click Refresh to update the currently displayed StorSimple Snapshot Manager window.
Refresh Device	Click the Devices node, and right-click a device in the Results pane.	Click Refresh Device to synchronize a specific connected device with StorSimple Snapshot Manager.
Refresh Devices	Right-click the Devices node.	Click Refresh Devices to synchronize your list of connected devices with StorSimple Snapshot Manager.
Rescan volumes	Right-click the Volumes node.	Click Rescan volumes to update the list of volumes that appears in the Results pane.
Restore	Expand Backup Catalog , expand a volume group, expand Local Snapshots or Cloud Snapshots , and then right-click a backup.	Click Restore to replace the current volume group data with the data from the selected backup.
Take Backup	Do one of the following: <ul style="list-style-type: none"> • Expand Volume Groups, and then right-click a volume group. • Expand Backup Catalog, and then right-click a volume group. 	Click Take Backup to start a backup job immediately.

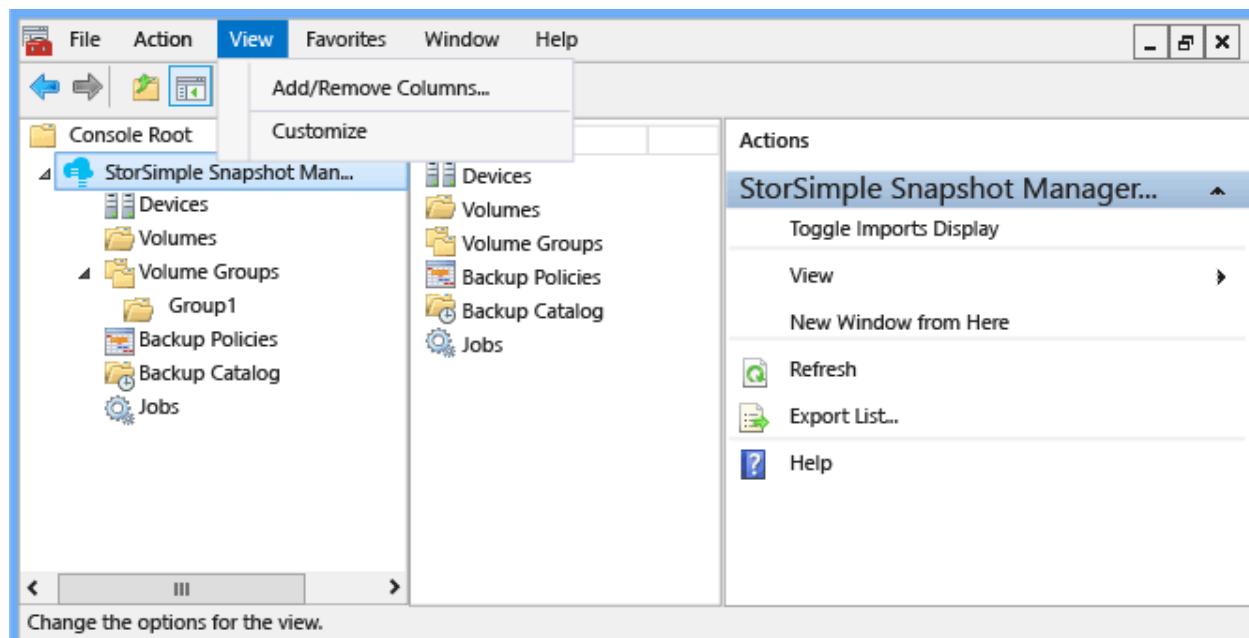
Action	Navigation	Description
Toggle Imports Display	Right-click the top node in the Scope pane (the StorSimple Snapshot Manager node in the examples).	Click Toggle Imports Display to show or hide the volume groups and associated backups that were imported from the StorSimple Device Manager service dashboard.

View menu

Use the **View** menu to create a custom view of the **Results** pane contents. The **View** menu contains **Add/Remove Columns** and **Customize** options.

Menu access

You can access the **View** menu on the menu bar or in the **Actions** pane.



Menu description

The following table describes items that appear on the **View** menu.

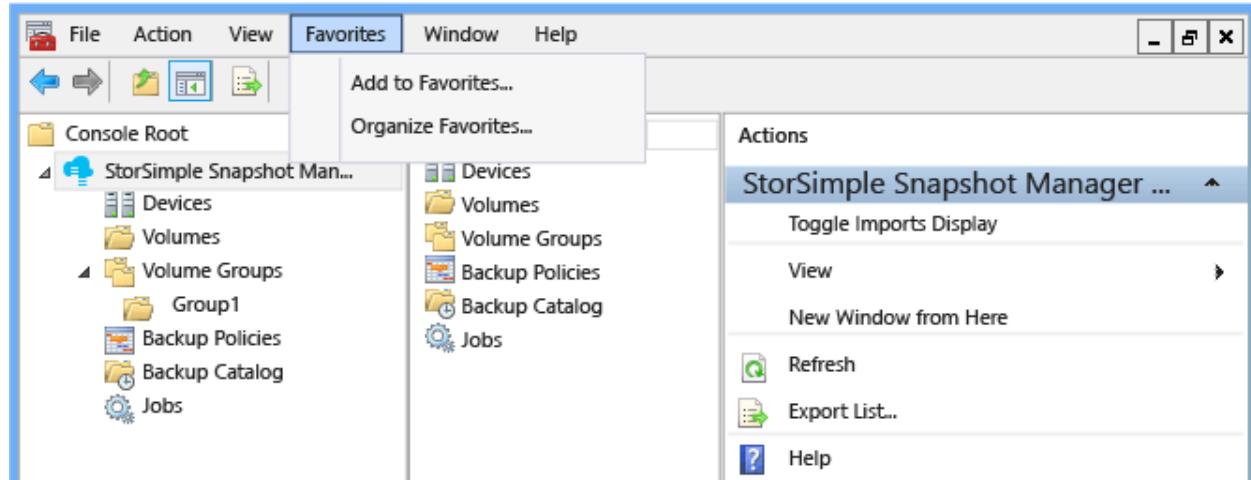
Menu item	Description
Add/Remove Columns	Click Add/Remove Columns to add or remove columns in the Results pane.
Customize	Click Customize to show or hide items in the StorSimple Snapshot Manager console window.

Favorites menu

Use the **Favorites** menu to add, remove, and organize page views and tasks that you use frequently.

Menu access

You can access the **Favorites** menu on the menu bar.



Menu description

The following table describes items that appear on the **Favorites** menu.

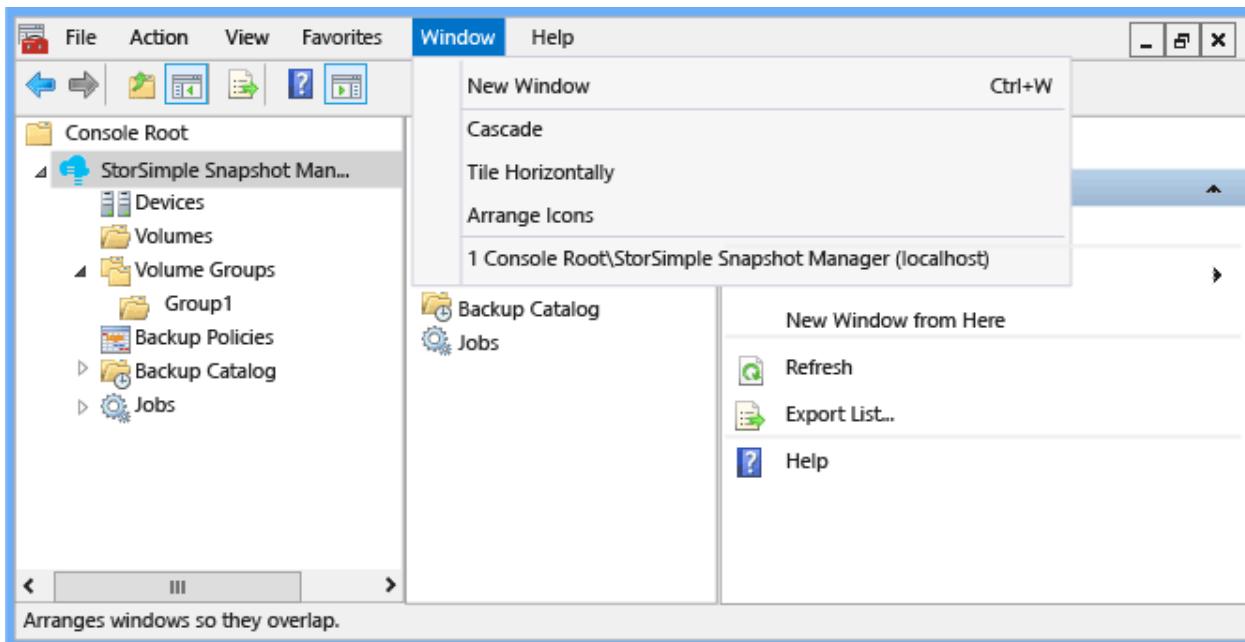
Menu item	Description
Add to Favorites	Click Add to Favorites to add the current view to your list of favorites.
Organize Favorites	Click Organize Favorites to organize the contents of your Favorites folder.

Window menu

Use the **Window** menu to add and rearrange StorSimple Snapshot Manager console windows.

Menu access

You can access the **Window** menu on the menu bar.



The numbered list at the bottom of the menu shows the windows that are currently open. Click any window in that list to bring the window into the foreground.

Menu description

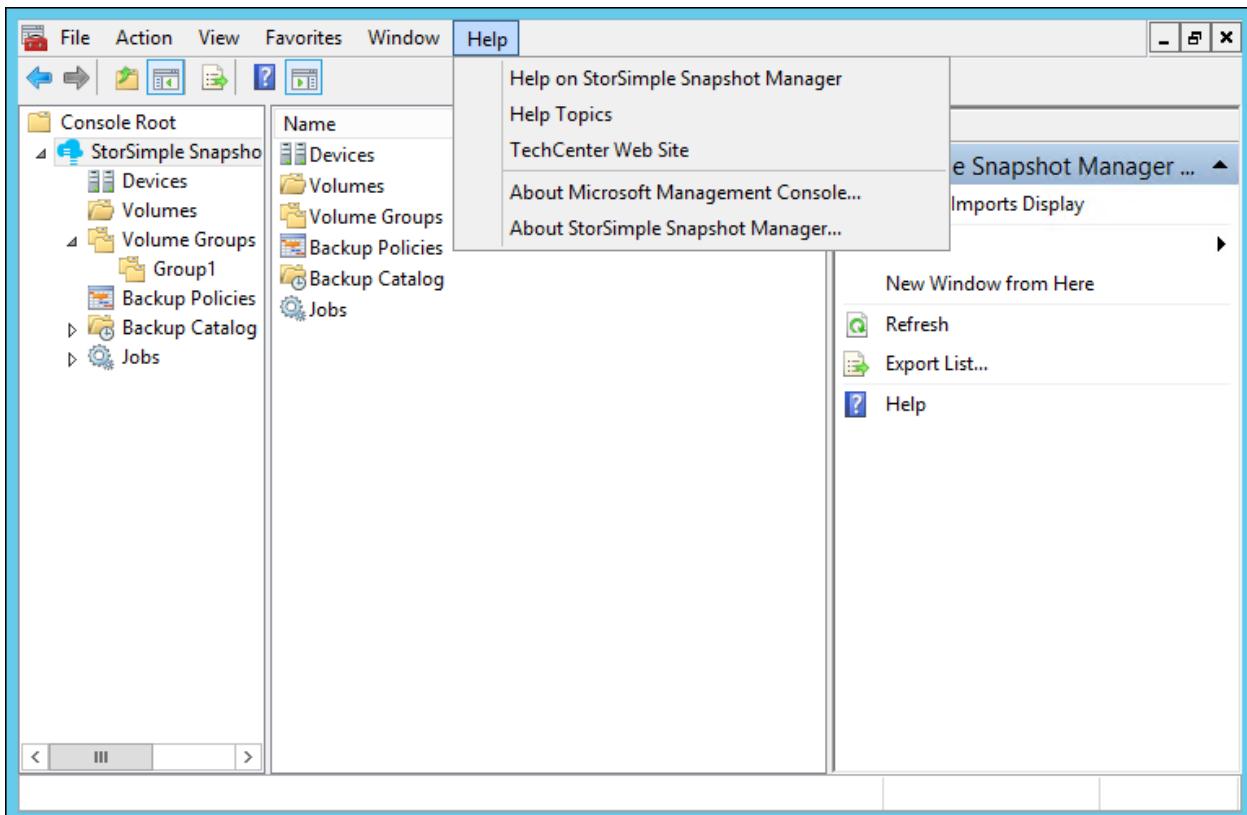
The following table describes the items that appear on the Window menu.

Menu item	Description
New Window	Click New Window to open a new console window (in addition to the existing window).
Cascade	Click Cascade to display the open console windows in a cascading style.
Tile Horizontally	Click Tile Horizontally to display the open console windows in a tile (or grid) format.
Arrange Icons	If you have multiple console windows open and scattered over your desktop, minimize them and then click Arrange Icons to arrange them in a horizontal row on the bottom of your screen.

Help menu

Use the **Help** menu to view available online help for StorSimple Snapshot Manager and the MMC. You can also view information about the MMC and StorSimple Snapshot Manager software versions that are currently installed on your system.

You can access the **Help** menu on the menu bar. You can also access StorSimple Snapshot Manager help topics from the **Actions** pane.



Menu description

The following table describes items that appear on the Help menu.

Menu item	Description
Help on StorSimple Snapshot Manager	Click Help on StorSimple Snapshot Manager to open StorSimple Snapshot Manager help in a separate window.
Help Topics	Click Help Topics to open MMC online help in a separate window.
TechCenter Web Site	Click TechCenter Web Site to open the Microsoft TechNet Tech Center home page in a separate window.
About Microsoft Management Console	Click About Microsoft Management Console to see which version of the Microsoft Management Console is installed on your system.
About StorSimple Snapshot Manager	Click About StorSimple Snapshot Manager to see which version of the snap-in is installed on your system.

Tool bar

The tool bar, located below the menu bar, contains navigation and task icons. Each icon is a shortcut to a specific task.

Icon descriptions

The following table describes the icons that appear on the tool bar.

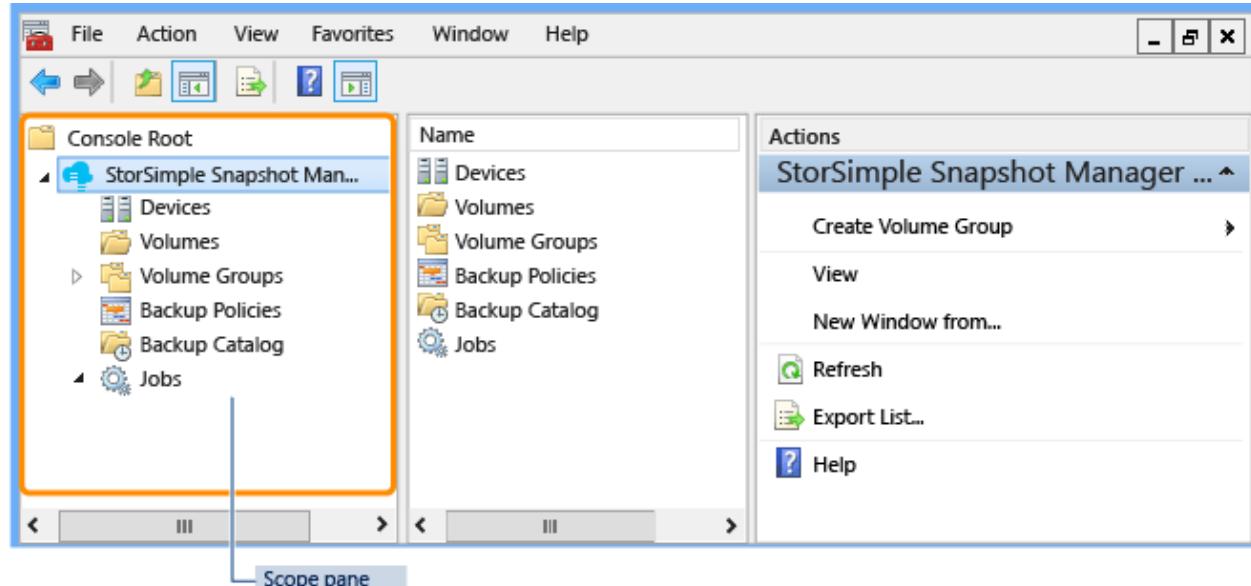
Icon	Description
⬅	Click the left arrow icon to return to the previous page.
➡	Click the right arrow to go to the next page (if the arrow is gray, the action is unavailable).
⬆	Click the up icon to go up one level in the console tree (the Scope pane).
⬇	Click the show/hide console tree icon to show or hide the Scope pane .
CSV	Click the export list icon to export a list to a CSV file that you specify.
?	Click the help icon to open an online MMC help topic.
Actions	Click the show/hide Actions pane icon to show or hide the Actions pane.

Scope pane

The **Scope pane** is the leftmost pane in the StorSimple Snapshot Manager UI. It contains the console (or node) tree and is the primary navigation mechanism for StorSimple Snapshot Manager.

Scope pane structure

The **Scope pane** contains a series of clickable objects (nodes) organized in a tree structure.



- To expand or collapse a node, click the arrow icon next to the node name.
- To view the status or contents of a node, click the node name. The information appears in the **Results** pane.

The **Scope** pane contains the following nodes:

- [Devices node](#)
- [Volumes node](#)
- [Volume Groups node](#)
- [Backup Policies node](#)
- [Backup Catalog node](#)
- [Jobs node](#)

Scope pane tasks

You can use the **Scope** pane to complete an action on a specific node. To select a task, do one of the following:

- Right-click the node, and then select the task from the menu that appears.
- Click the node, and then click **Action** on the menu bar. Select the task from the menu that appears.
- Click the node, and then select the action in the **Actions** pane.

When you select a node and use any of these methods to see a task list, only those actions that can be performed on that node are shown.

Devices node

The **Devices** node represents the StorSimple devices and StorSimple virtual devices that are connected to StorSimple Snapshot Manager. Select this node to connect and configure a device, and import its associated volumes, volume groups, and existing backup copies. Multiple devices can be connected to a single host.

- To expand the node, click the arrow icon next to **Devices**.
- To see a menu of available actions, right-click the **Devices** node or right-click any of the nodes that appear in the expanded view.
- To see a list of configured devices, click **Devices** in the **Scope** pane. The list of devices, together with information about each device, appears in the **Results** pane.

Volumes node

The **Volumes** node represents the drives that correspond to the volumes mounted by the host, including those discovered through iSCSI and those discovered through a device. Use this node to view the list of available volumes and assign individual volumes to volume groups.

- To expand the node, click the arrow icon next to **Volumes**.
- To see a menu of available actions, right-click the **Volumes** node or right-click any of the nodes that appear in the expanded view.
- To see a list of volumes, click **Volumes** in the **Scope** pane. The list of volumes, together with information about each volume, appears in the **Results** pane.

Volume Groups node

Volume groups are also known as consistency groups. Each volume group is a pool of application-related volumes that helps to ensure application consistency during backup operations. Use the **Volume Groups** node to configure these groups and to take interactive backups or create backup schedules.

- To expand the node, click the arrow icon next to **Volume Groups**.
- To see a menu of available actions, right-click the **Volume Groups** node or right-click any of the nodes that appear in the expanded view.
- To see a list of volume groups, click **Volume Groups** in the **Scope** pane. The list of volume groups, together with information about each volume group, appears in the **Results** pane.

Backup Policies node

Backup policies are job schedules for local and cloud snapshots. Use the **Backup Policies** node to specify how often a backup is created and how long a backup should be retained.

- To expand the node, click the arrow icon next to **Backup Policies**.
- To see a menu of available actions, right-click the **Backup Policies** node or right-click any of the nodes that appear in the expanded view.
- To see a list of backup policies, click **Backup Policies** in the **Scope** pane. The list of backup policies, together with information about each policy, appears in the **Results** pane.

Note

You can retain a maximum of 64 backups.

Backup Catalog node

The **Backup Catalog** node contains lists of on-site and off-site backups of Azure StorSimple volumes. This node is organized by volume group, and each volume group container contains separate structures for local snapshots (the **Local Snapshots** node) and cloud snapshots (the **Cloud Snapshots** node). When expanded, each volume group container lists all the successful backups that were taken interactively or by a configured policy.

- To expand the node, click the arrow icon next to **Backup Catalog**.
- To see a menu of available actions, right-click the **Backup Catalog** node or right-click any of the nodes that appear in the expanded view.
- To see a list of backup snapshots, click **Backup Catalog** in the **Scope** pane. The list of snapshots, together with information about each snapshot, appears in the **Results** pane.

Local Snapshots node

The **Local Snapshots** node lists local snapshots for a specific volume group. The node is located under the **Backup Catalog** node in the **Scope** pane. Local snapshots are point-in-time copies of volume data that are stored on the Azure StorSimple device. Typically, this type of backup can be created and restored quickly. You can use a local snapshot as you would a local backup copy.

- To expand the node, click the arrow icon next to **Local Snapshots**.
- To see a menu of available actions, right-click the **Local Snapshots** node or right-click any of the nodes that appear in the expanded view.
- To see a list of local snapshots, click **Local Snapshots** in the **Scope** pane. The list of snapshots, together with information about each snapshot, appears in the **Results** pane.

Cloud Snapshots node

The **Cloud Snapshots** node lists cloud snapshots for a specific volume group. The node is located under the **Backup Catalog** node in the **Scope** pane. Cloud snapshots are point-in-time copies of volume data that are stored in the cloud. A cloud snapshot is equivalent to a snapshot replicated on a different, off-site storage system. Cloud snapshots are particularly useful in disaster recovery scenarios.

- To expand the node, click the arrow icon next to **Cloud Snapshots**.
- To see a menu of available actions, right-click the **Cloud Snapshots** node or right-click any of the nodes that appear in the expanded view.

- To see a list of cloud snapshots, click **Cloud Snapshots** in the **Scope** pane. The list of snapshots, together with information about each snapshot, appears in the **Results** pane.

Jobs node

The **Jobs** node contains information about scheduled, running, and recently completed backup jobs.

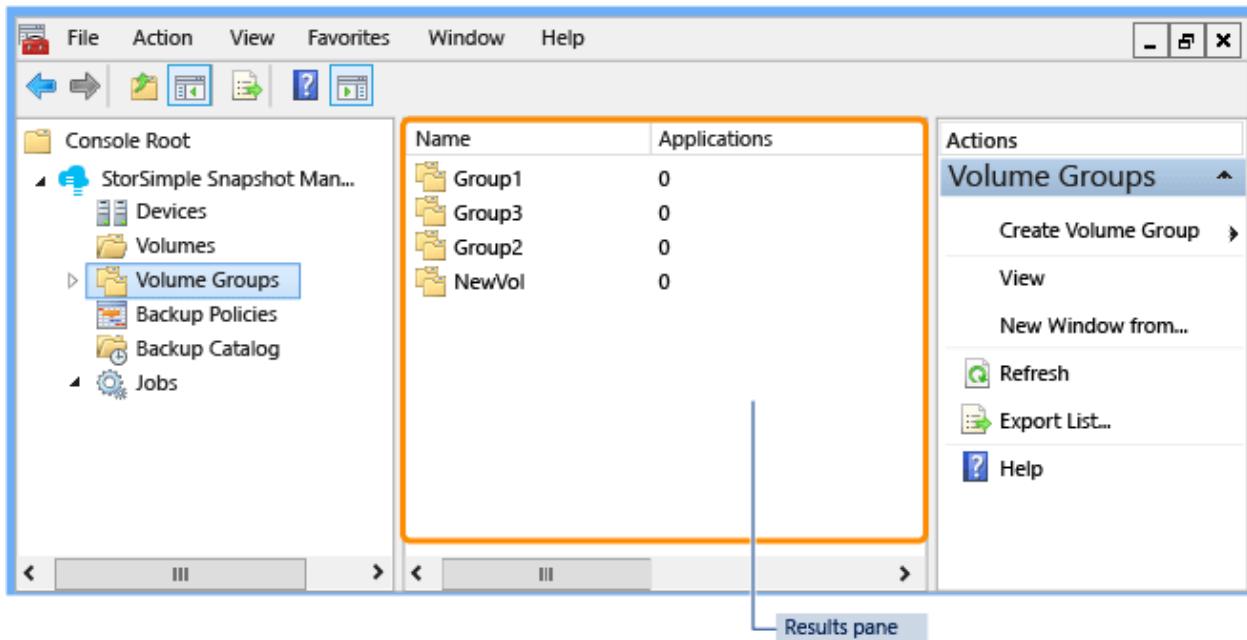
- To expand the node, click the arrow icon next to **Jobs**.
- To see a menu of available actions, right-click the **Jobs** node or right-click any of the nodes that appear in the expanded view.
- To see a list of scheduled jobs, expand the **Jobs** node, and then click **Scheduled**. The list of previously configured jobs and information about each job appears in the **Results** pane.
- To see a list of recently completed jobs, expand the **Jobs** node, and then click **Last 24 Hours**. A list of jobs that were completed in the last 24 hours appears in the **Results** pane. The **Results** pane also contains information about each completed job.
- To see a list of jobs that are currently running, expand the **Jobs** node, and then click **Running**. The list of currently running jobs and information about each job appears in the **Results** pane.

Results pane

The **Results** pane is the center pane in the StorSimple Snapshot Manager UI. It contains lists and detailed status information for the node you selected in the **Scope** pane.

Example

To see the following example, click the **Volume Groups** node in the **Scope** pane. The **Results** pane displays a list of volume groups with details about each group.



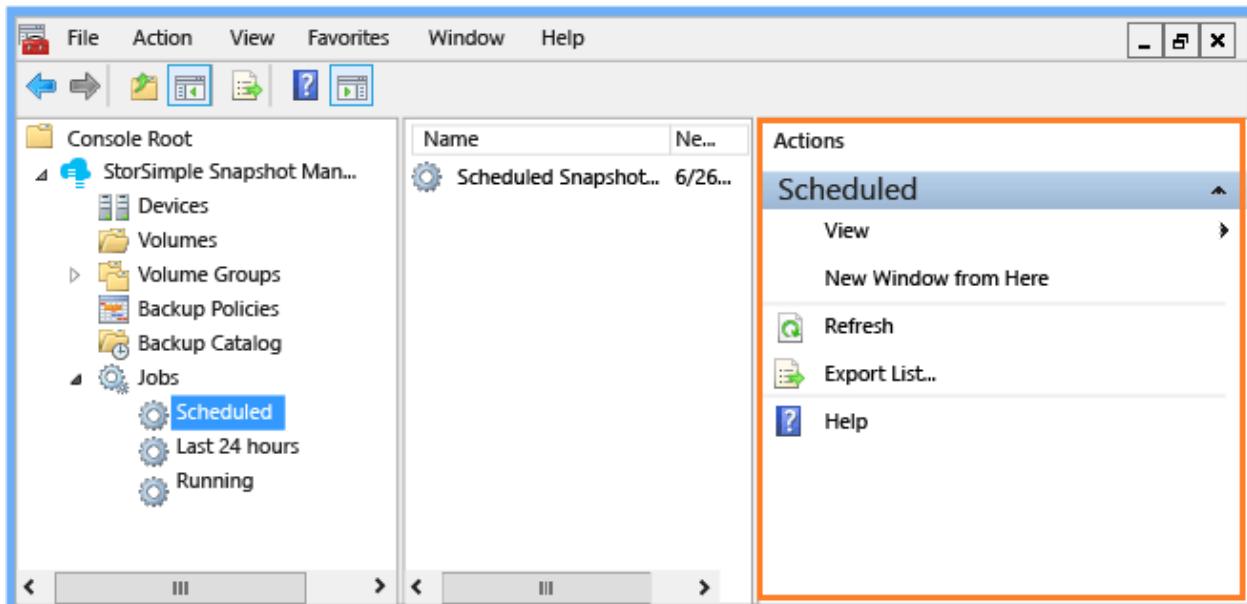
You can configure the details shown in the **Results** pane: right-click a node in the **Scope** pane, click **View**, and then click **Add/Remove Columns**.

Actions pane

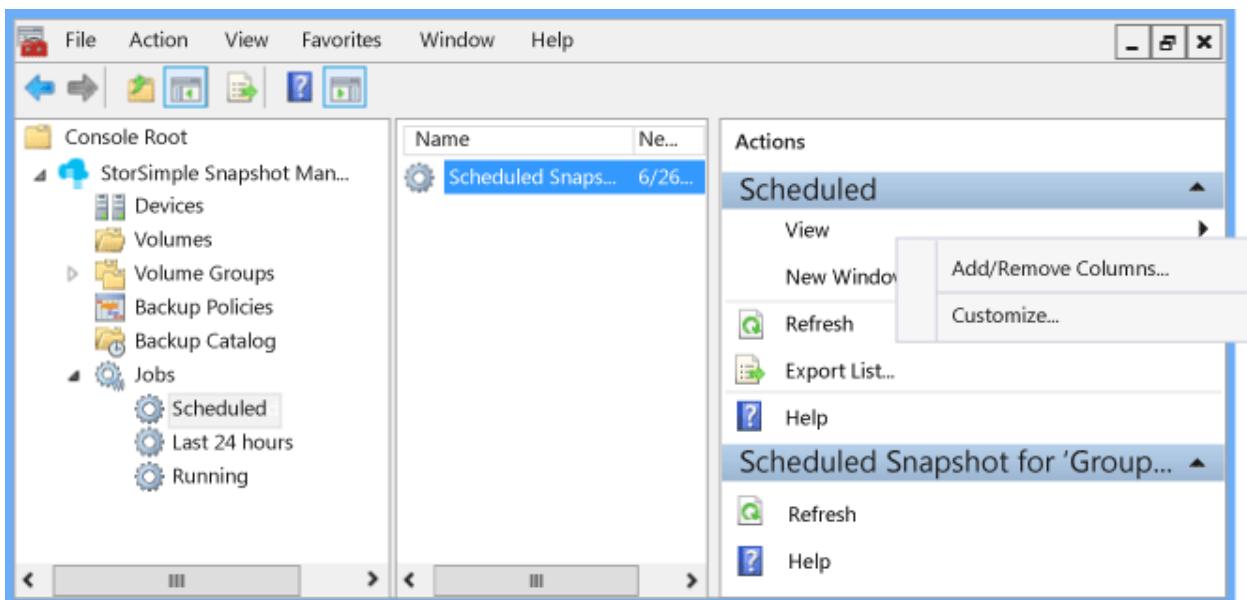
The **Actions** pane is the right pane in the StorSimple Snapshot Manager UI. It contains a menu of operations that you can perform on the node, view, or data that you select in the **Scope** pane or **Results** pane. The **Actions** pane contains the same commands as the **Action** menus that are available for items in the **Scope** pane and **Results** pane. For a description of each action, see the table in the **Action** menu section.

Examples

To see the following example, in the **Scope** pane, expand the **Jobs** node and click **Scheduled**. The **Actions** pane displays the available actions for the **Scheduled** node.



To see more options, in the **Scope** pane, expand the **Jobs** node, click **Scheduled**, and then click a scheduled job in the **Results** pane. The **Actions** pane displays the available actions for the scheduled job, as shown in the following example.



Keyboard navigation and shortcuts

StorSimple Snapshot Manager enables the accessibility features of the Windows operating system and the Microsoft Management Console (MMC). It also includes some keyboard navigation features and shortcuts that are specific to the StorSimple Snapshot Manager, as described in the following sections.

- Keyboard navigation keys
- Menu bar shortcut keys
- Scope pane shortcut keys

Keyboard navigation keys

The following table describes the keys that you can use to navigate the StorSimple Snapshot Manager user interface.

Navigation key	Action
Down arrow key	Use the down arrow key to move vertically to the next item in a menu or pane.
Enter	Press the Enter key to complete an action and then proceed to the next step. For example, you can press Enter to select Next , OK , or Create , and then go to the next step in a wizard.
Esc	Press the Esc key to close a menu or to cancel and close a page.
F1	Press the F1 key to view a help topic for the currently active window.
F5	Press the F5 key to refresh a node.
F6	Press the F6 key to move from the Scope pane to the Results pane.
F10	Press the F10 key to go to the menu bar.
Left arrow key	Use the left arrow key to move horizontally from a menu bar option to the previous option. When you move to the previous item on the menu bar, the action (or context) menu for the previous item appears.
Right arrow key	Use the right arrow key to move horizontally from one menu bar option to the next. When you move to the next item on the menu bar, the action (or context) menu for the new item appears.
Tab key	Use the Tab key to move to the next pane on the console or to the next selection or text box in a page.
Up arrow key	Use the up arrow key to move vertically to the previous item on a menu or pane.

Menu bar shortcut keys

The following table describes the shortcut key combinations for the menu bar. After you press the shortcut keys and the menu opens, you can use menu shortcut keys (the underlined keys on the menu). For more information about the menu bar, go to [Menu bar](#).

Shortcut	Result	Menu Shortcut Key	Result
----------	--------	-------------------	--------

Shortcut	Result	Menu Shortcut Key	Result
ALT+F	Opens the File menu.	N	Opens a new console instance.
	O	Opens the Administrative Tools page.	
	S	Saves the StorSimple Snapshot Manager console.	
	A	Opens the Save As page.	
	M	Opens the Add/Remove Snap-in page.	
	P	Opens the Options page.	
	H	Opens online Help.	
ALT+A	Opens the Action menu.	I	Turns the import display option on and off.
	W	Opens a new StorSimple Snapshot Manager console.	
	F	Updates the StorSimple Snapshot Manager console.	
	L	Opens the Export List page.	
	H	Opens online Help.	
ALT+V	Opens the View menu.	A	Opens the Add/Remove Columns page.
	U	Opens the Customize View page.	
ALT+O	Opens the Favorites menu.	A	Opens the Add to Favorites page.
	O	Opens the Organize Favorites page.	
ALT+W	Opens the Window menu.	N	Opens another StorSimple Snapshot Manager window.
	C	Displays all open console windows in a cascading style.	

Shortcut	Result	Menu Shortcut Key	Result
	T	Displays all open console windows in a grid pattern.	
	I	Arranges icons in a horizontal row at the bottom of your screen.	
ALT+H	Opens the Help menu.	H	Opens online Help.
	T	Opens the Microsoft TechNet Tech Center web page.	
	A	Opens the About Microsoft Management Console page.	

Scope pane shortcut keys

The following tables show the shortcut key combinations for each node in the **Scope** pane.

- [Devices node shortcut keys](#)
- [Volumes node shortcut keys](#)
- [Volume Groups node shortcut keys](#)
- [Backup Policies node shortcut keys](#)
- [Backup Catalog node shortcut keys](#)
- [Jobs node shortcut keys](#)

Devices node shortcut keys

Menu	Result
Shortcut	
C	Opens the Configure a Device page.
D	Refreshes the list of devices and device details.
V	Opens the View menu.
W	Opens a new StorSimple Snapshot Manager console focused on the Details node.
F	Updates the StorSimple Snapshot Manager console.
L	Opens the Export List page.

Menu	Result
Shortcut	
H	Opens online Help.

Volumes node shortcut keys

Menu	Result
Shortcut	
V	Updates the list of volumes.
V (press twice)	Opens the View menu.
W	Opens a new StorSimple Snapshot Manager console focused on the Volumes node.
F	Updates the StorSimple Snapshot Manager console.
L	Opens the Export List page.
H	Opens online Help.

Volume Groups node shortcut keys

Menu	Result
Shortcut	
G	Opens the Create a Volume Group page.
V	Opens the View menu.
W	Opens a new StorSimple Snapshot Manager console focused on the Volume Groups node.
F	Updates the StorSimple Snapshot Manager console.
L	Opens the Export List page.
H	Opens online Help.

Backup Policies node shortcut keys

Menu	Result
Shortcut	
B	Opens the Create a Policy page.

Menu	Result
Shortcut	
V	Opens the View menu.
W	Opens a new StorSimple Snapshot Manager console focused on the Volume Groups node.
F	Updates the StorSimple Snapshot Manager console.
L	Opens the Export List page.
H	Opens online Help.

Backup Catalog node shortcut keys

Menu	Result
Shortcut	
W	Opens a new StorSimple Snapshot Manager console focused on the Volume Groups node.
F	Updates the StorSimple Snapshot Manager console.
H	Opens online Help.

Jobs node shortcut keys

Menu	Shortcut	Result
V		Opens the View menu.
W		Opens a new StorSimple Snapshot Manager console focused on the Jobs node.
F		Updates the StorSimple Snapshot Manager console.
L		Opens the Export List page.
H		Opens online Help

Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to connect and manage devices](#).

Use StorSimple Snapshot Manager to connect and manage StorSimple devices

Article • 08/22/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

You can use nodes in the StorSimple Snapshot Manager **Scope** pane to verify imported StorSimple device data and refresh connected storage devices. Additionally, when you click the **Devices** node, you can see a list of connected devices and corresponding status information in the **Results** pane.

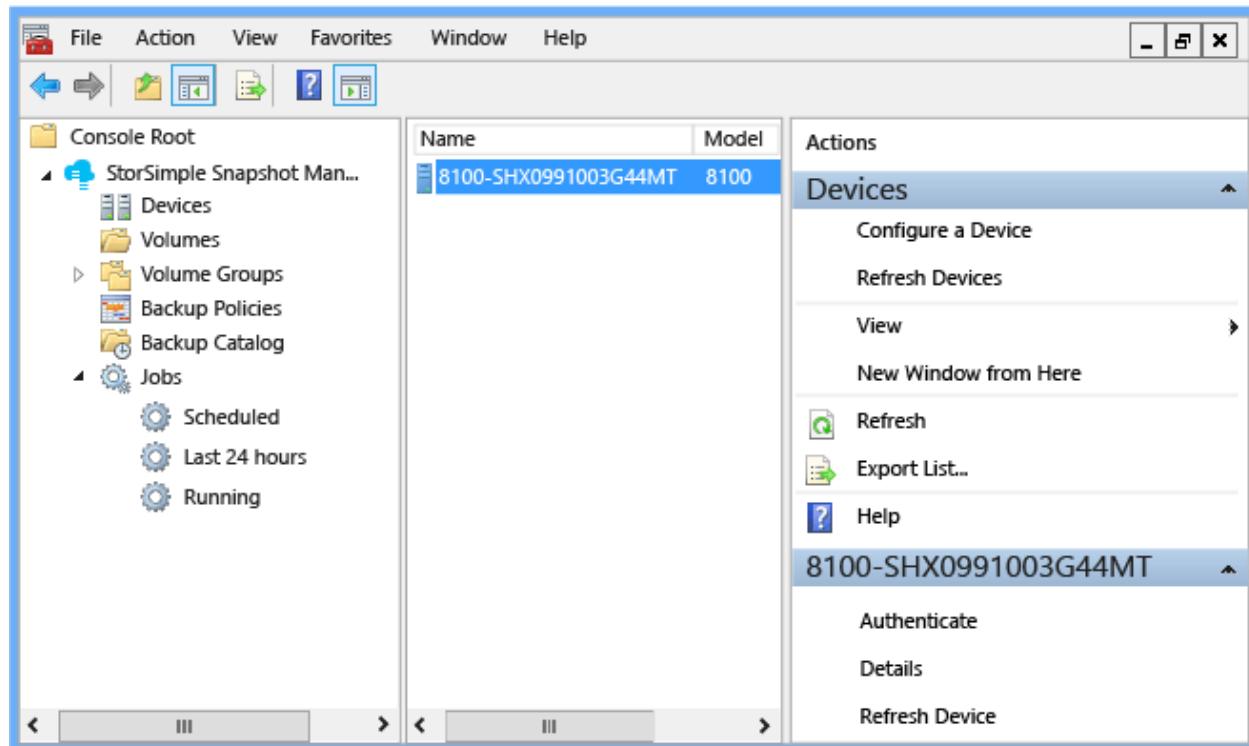


Figure 1: StorSimple Snapshot Manager connected device

Depending on your **View** selections, the **Results** pane shows the following information about each device. (For more information about configuring a view, go to [View menu](#).)

Results column	Description
Name	The name of the device as configured in the Azure classic portal
Model	The model number of the device
Version	The version of the software installed on the device
Status	Whether the device is available
Last Synced	Date and time when the device was last synchronized
Serial No.	The serial number for the device

If you right-click the **Devices** node in the **Scope** pane, you can select from the following actions:

- Add or replace a device
- Connect a device and verify imports
- Refresh connected devices

If you click the **Devices** node and then right-click a device name in the **Results** pane, you can select from the following actions:

- Authenticate a device
- View device details
- Refresh a device
- Delete a device configuration
- Change a device password

 **Note**

All of these actions are also available in the **Actions** pane.

This tutorial explains how to use StorSimple Snapshot Manager to connect and manage devices and perform the following tasks:

- Add or replace a device
- Connect a device and verify imports
- Refresh connected devices
- Authenticate a device
- View device details

- Refresh an individual device
- Delete a device configuration
- Change an expired device password
- Replace a failed device

 **Note**

For general information about using the StorSimple Snapshot Manager interface, go to [StorSimple Snapshot Manager user interface](#).

Add or replace a device

Use the following procedure to add or replace a StorSimple device.

To add or replace a device

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click the **Devices** node, and then click **Configure a device**.
The **Configure a Device** dialog box appears.



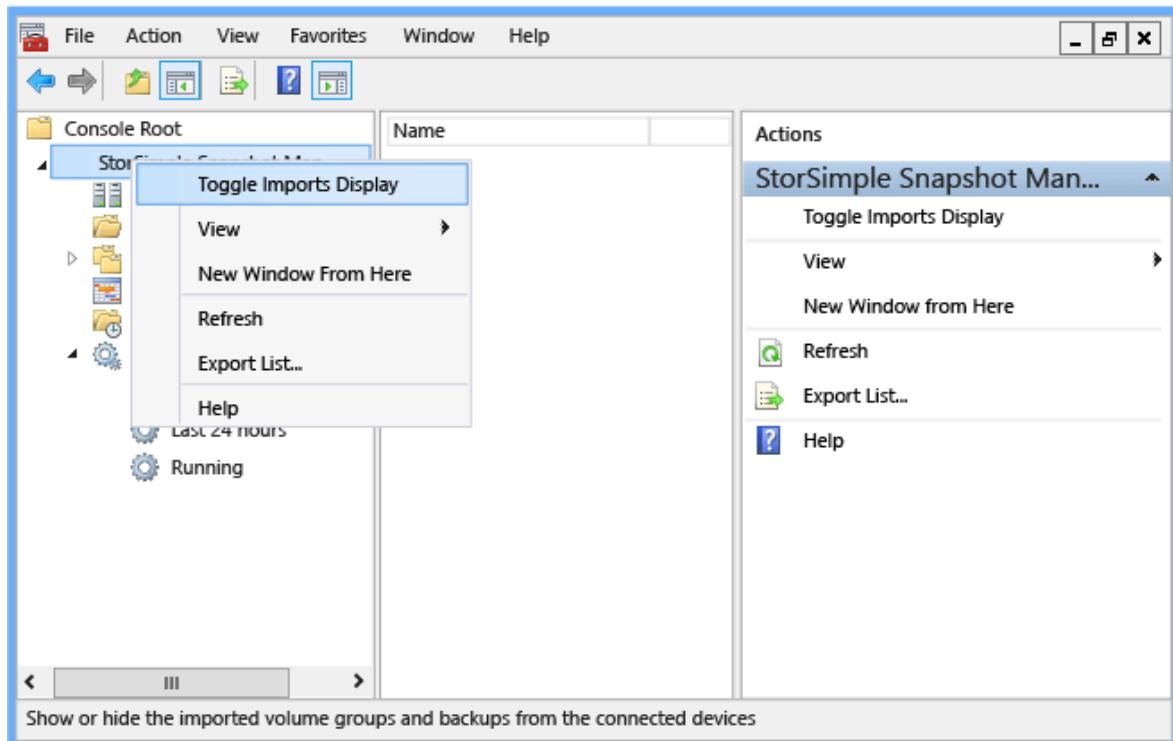
3. In the **Device** drop-down box, select the IP address of the device or virtual device.
4. In the **Password** text box, type the StorSimple Snapshot Manager password that you created for the device in the Azure classic portal. Click **OK**. StorSimple Snapshot Manager searches for the device that you identified.
 - If the device is available, StorSimple Snapshot Manager adds a connection.
 - If the device is unavailable for any reason, StorSimple Snapshot Manager returns an error message. Click **OK** to close the error message, and then click **Cancel** to close the **Configure a Device** dialog box.

Connect a device and verify imports

Use the following procedure to connect a StorSimple device and verify that any existing volume groups that have associated backups are imported.

To connect a device and verify imports

1. To connect a device to StorSimple Snapshot Manager, follow the instructions in Add or replace a device. When it connects to a device, StorSimple Snapshot Manager responds as follows:
 - If the device is unavailable for any reason, StorSimple Snapshot Manager returns an error message.
 - If the device is available, StorSimple Snapshot Manager adds a connection. When you select the device, it appears in the **Results** pane, and the status field indicates that the device is **Available**. StorSimple Snapshot Manager imports any volume groups configured for the device, provided that the volume groups have associated backups. Backup policies are not imported. Volume groups that do not have associated backups are not imported.
2. Click the desktop icon to start StorSimple Snapshot Manager.
3. Right-click the top node in the **Scope** pane, and then click **Toggle Imports Display**.



4. The **Toggle Imports Display** dialog box appears, showing the status of the imported volume groups and backups. Click **OK**.

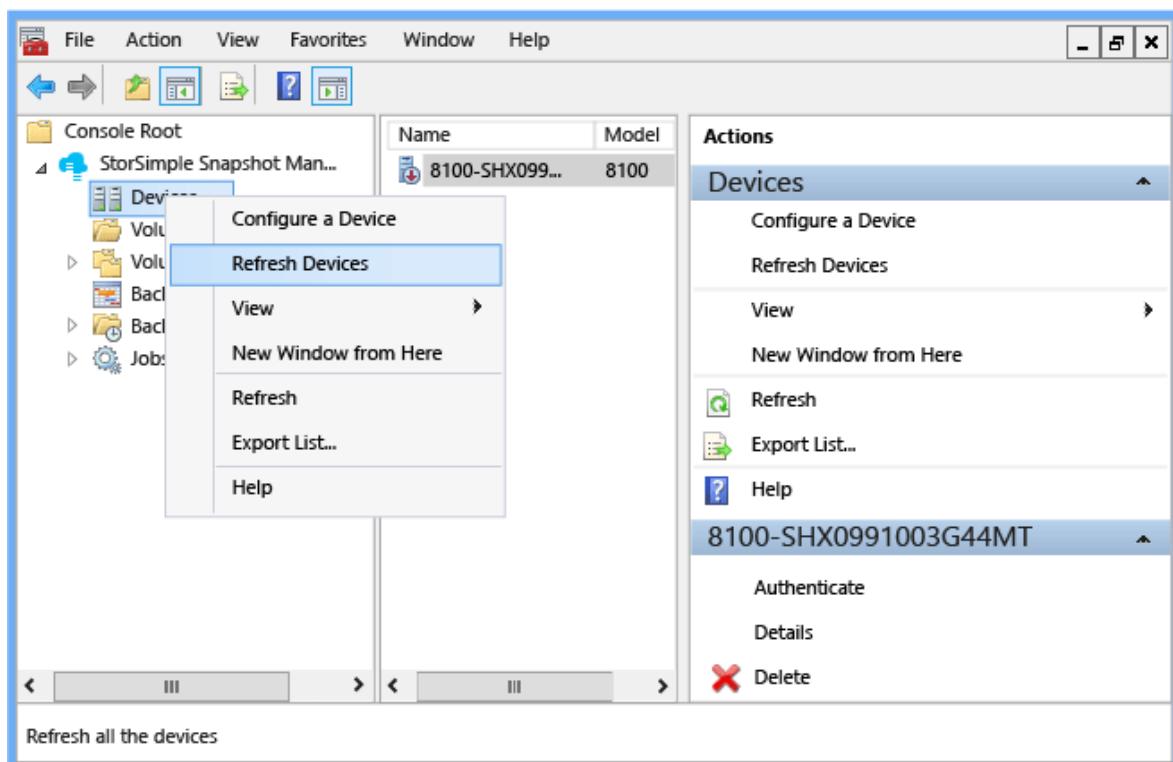
After the volume groups and backups are successfully imported, you can use StorSimple Snapshot Manager to manage them, just as you would manage volume groups and backups that you created and configured with StorSimple Snapshot Manager.

Refresh connected devices

Use the following procedure to synchronize the connected StorSimple devices with StorSimple Snapshot Manager.

To refresh connected devices

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click **Devices**, and then click **Refresh Devices**. This synchronizes the connected devices with StorSimple Snapshot Manager so that you can view the volume groups and backups, including any recent additions.



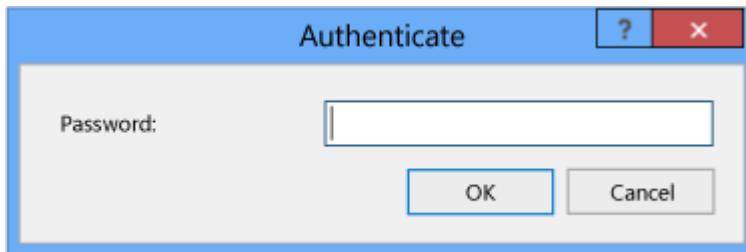
The **Refresh Devices** action retrieves any new volume groups and any associated backups from connected devices. Unlike the **Rescan volumes** action available for the **Volumes** node, **Refresh Devices** does not restore the backup registry.

Authenticate a device

Use the following procedure to authenticate a StorSimple device with StorSimple Snapshot Manager.

To authenticate a device

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click **Devices**.
3. In the **Results** pane, right-click the name of the device, and then click **Authenticate**.
4. The **Authenticate** dialog box appears. Type the device password, and then click **OK**.

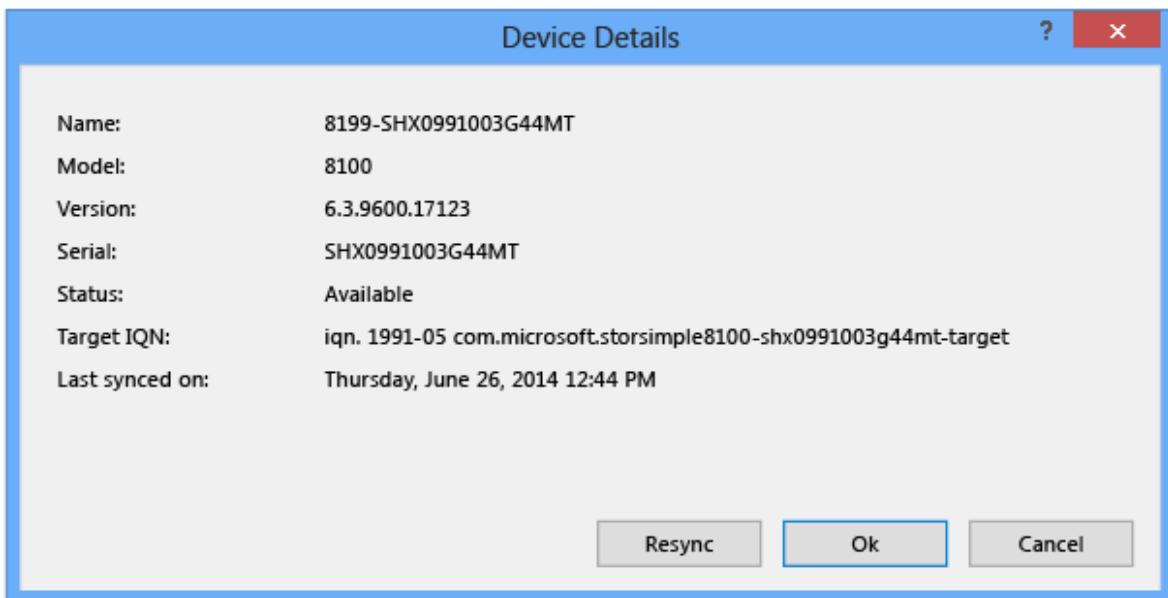


View device details

Use the following procedure to view the details of a StorSimple device and, if necessary, resynchronize the device with StorSimple Snapshot Manager.

To view and resynchronize device details

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click **Devices**.
3. In the **Results** pane, right-click the name of the device, and then click **Details**.
4. The **Device Details** dialog box appears. This box shows the name, model, version, serial number, status, target iSCSI Qualified Name (IQN), and last synchronization date and time.
 - Click **Resync** to synchronize the device.
 - Click **OK** or **Cancel** to close the dialog box.



Refresh an individual device

Use the following procedure to resynchronize an individual StorSimple device with StorSimple Snapshot Manager.

To refresh a device

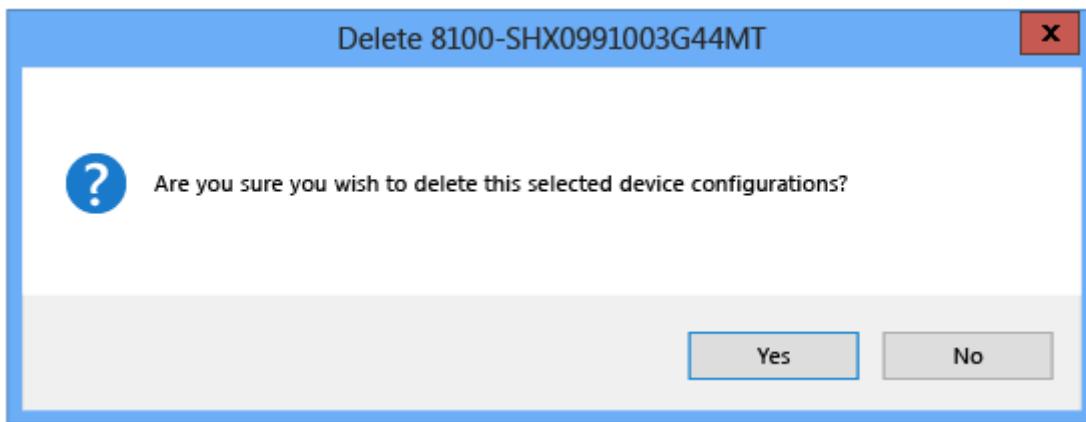
1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click **Devices**.
3. In the **Results** pane, right-click the name of the device, and then click **Refresh Device**. This synchronizes the device with StorSimple Snapshot Manager.

Delete a device configuration

Use the following procedure to delete an individual StorSimple device configuration from StorSimple Snapshot Manager.

To delete a device configuration

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click **Devices**.
3. In the **Results** pane, right-click the name of the device, and then click **Delete**.
4. The following message appears. Click **Yes** to delete the configuration or click **No** to cancel the deletion.



Change an expired device password

You must enter a password to authenticate a StorSimple device with StorSimple Snapshot Manager. You configure this password when you use the Windows PowerShell interface to set up the device. However, the password can expire. If this happens, you can use the Azure classic portal to change the password. Then, because the device was configured in StorSimple Snapshot Manager before the password expired, you must re-authenticate the device in StorSimple Snapshot Manager.

To change the expired password

1. In the Azure classic portal, start the StorSimple Manager service.
2. Click **Devices > Configure** for the device.
3. Scroll down to the StorSimple Snapshot Manager section. Enter a password that is 14-15 characters. Make sure that the password contains a mix of uppercase, lowercase, numeric, and special characters.
4. Re-enter the password to confirm it.
5. Click **Save** at the bottom of the page.

To re-authenticate the device

1. Start StorSimple Snapshot Manager.
2. In the **Scope** pane, click **Devices**. A list of configured devices appears in the **Results** pane.
3. Select the device, right-click, and then click **Authenticate**.
4. In the **Authenticate** window, enter the new password.
5. Select the device, right-click, and select **Refresh device**. This synchronizes the device with StorSimple Snapshot Manager.

Replace a failed device

If a StorSimple device fails and is replaced by a standby (failover) device, use the following steps to connect to the new device and view the associated backups.

To connect to a new device after failover

1. Reconfigure the iSCSI connection to the new device. For instructions, go to "Step 7: Mount, initialize, and format a volume" in [Deploy your on-premises StorSimple device](#).

 **Note**

If the new StorSimple device has the same IP address as the old one, you might be able to connect the old configuration.

1. Stop the Microsoft StorSimple Management Service:
 - a. Start Server Manager.
 - b. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - c. On the **Services** window, select the **Microsoft StorSimple Management Service**.
 - d. In the right pane, under **Microsoft StorSimple Management Service**, click **Stop the service**.
2. Remove the configuration information related to the old device:
 - a. In File Explorer, browse to C:\ProgramData\Microsoft\StorSimple\BACatalog.
 - b. Delete the files in the BACatalog folder.
3. Restart the Microsoft StorSimple Management Service:
 - a. On the Server Manager Dashboard, on the **Tools** menu, select **Services**.
 - b. On the **Services** window, select the **Microsoft StorSimple Management Service**.
 - c. In the right pane, under **Microsoft StorSimple Management Service**, click **Restart the service**.
4. Start StorSimple Snapshot Manager.
5. To configure the new StorSimple device, complete the steps in Step 2: Connect a StorSimple device in [Deploy StorSimple Snapshot Manager](#).
6. Right-click the top-level node in the **Scope** pane (StorSimple Snapshot Manager in the example), and then click **Toggle Imports Display**.
7. A message appears when the imported volume groups and backups are visible in StorSimple Snapshot Manager. Click **OK**.

Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to view and manage volumes](#).

Use StorSimple Snapshot Manager to create and manage backup policies

Article • 08/22/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

A backup policy creates a schedule for backing up volume data locally or in the cloud. When you create a backup policy, you can also specify a retention policy. (You can retain a maximum of 64 snapshots.) For more information about backup policies, see [Backup types in StorSimple 8000 series: a hybrid cloud solution](#).

This tutorial explains how to:

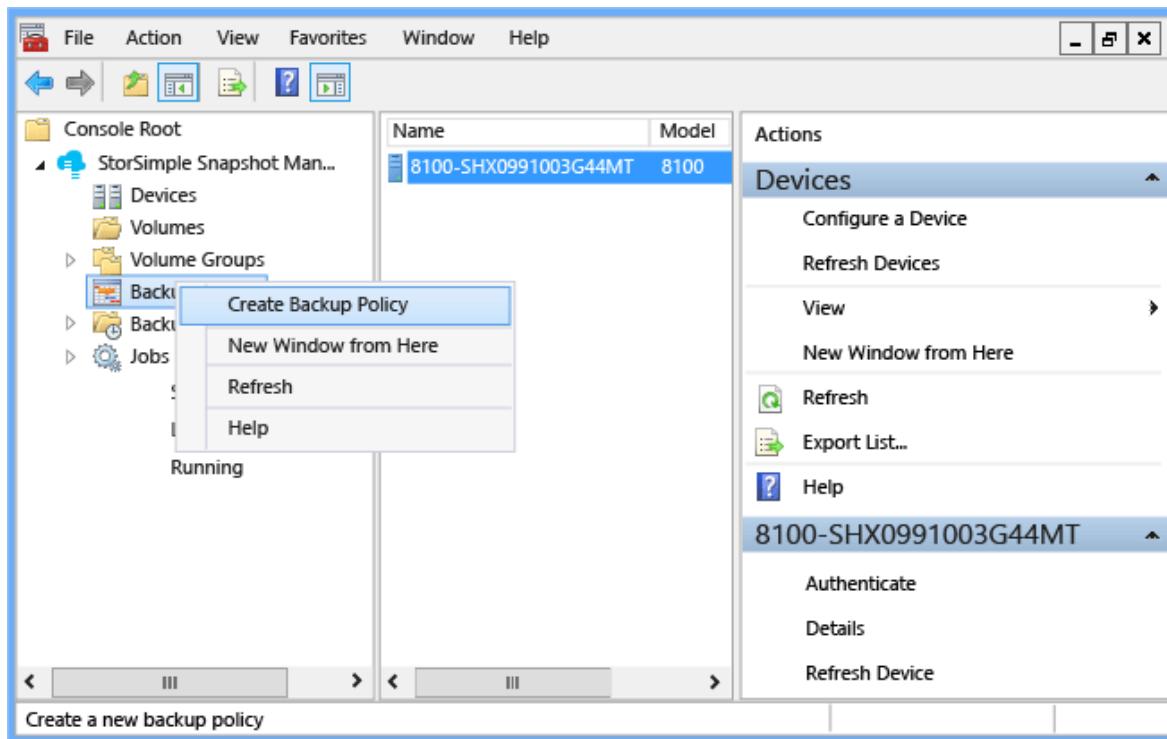
- Create a backup policy
- Edit a backup policy
- Delete a backup policy

Create a backup policy

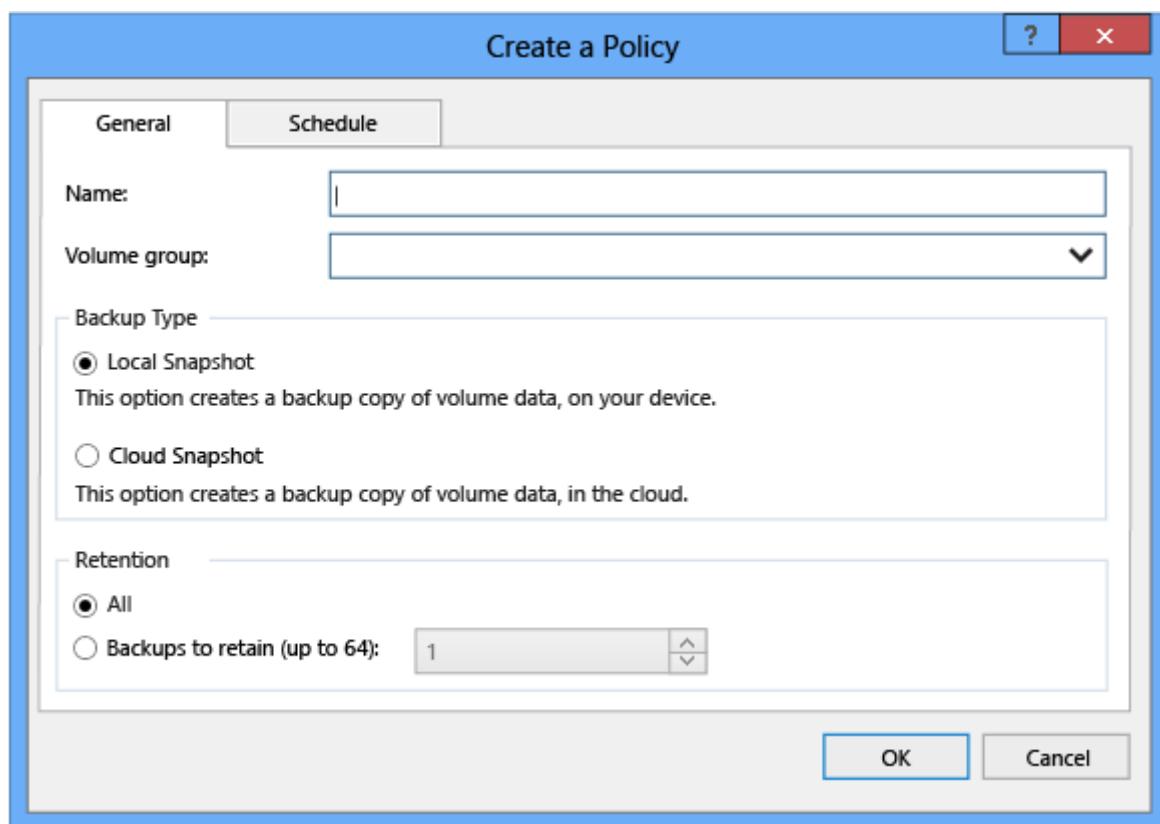
Use the following procedure to create a new backup policy.

To create a backup policy

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click **Backup Policies**, and click **Create Backup Policy**.

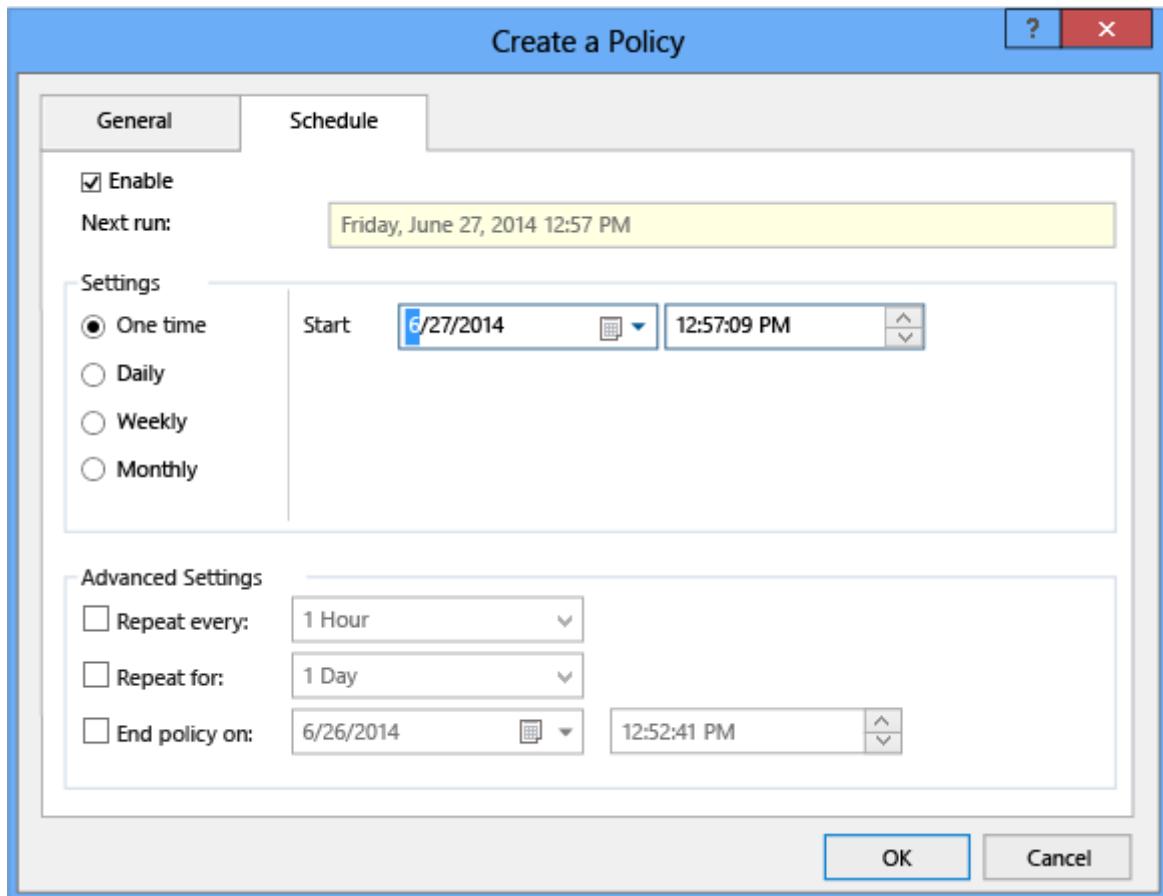


The Create a Policy dialog box appears.



3. On the General tab, complete the following information:
 - a. In the Name text box, type a name for the policy.
 - b. In the Volume group text box, type the name of the volume group associated with the policy.
 - c. Select either Local Snapshot or Cloud Snapshot.
 - d. Select the number of snapshots to retain. If you select All, 64 snapshots will be retained (the maximum).

4. Click the **Schedule** tab.



5. On the **Schedule** tab, complete the following information:

- Click the **Enable** check box to schedule the next backup.
- Under **Settings**, select **One time**, **Daily**, **Weekly**, or **Monthly**.
- In the **Start** text box, click the calendar icon and select a start date.
- Under **Advanced Settings**, you can set optional repeat schedules and an end date.
- Click **OK**.

After you create a backup policy, the following information appears in the **Results** pane:

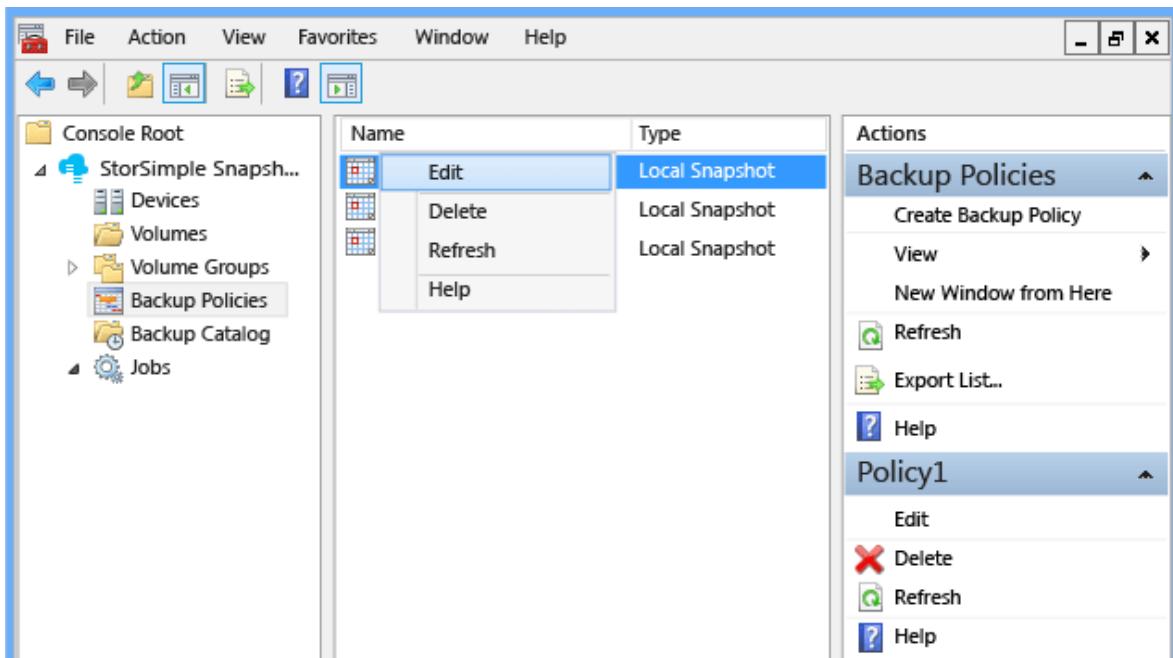
- Name** – the name of backup policy.
- Type** – local snapshot or cloud snapshot.
- Volume Group** – the volume group associated with the policy.
- Retention** – the number of snapshots retained; the maximum is 64.
- Created** – the date that this policy was created.
- Enabled** – whether the policy is currently in effect: **True** indicates that it is in effect; **False** indicates that it is not in effect.

Edit a backup policy

Use the following procedure to edit an existing backup policy.

To edit a backup policy

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the Scope pane, click the **Backup Policies** node. All the backup policies appear in the Results pane.
3. Right-click the policy that you want to edit, and then click **Edit**.



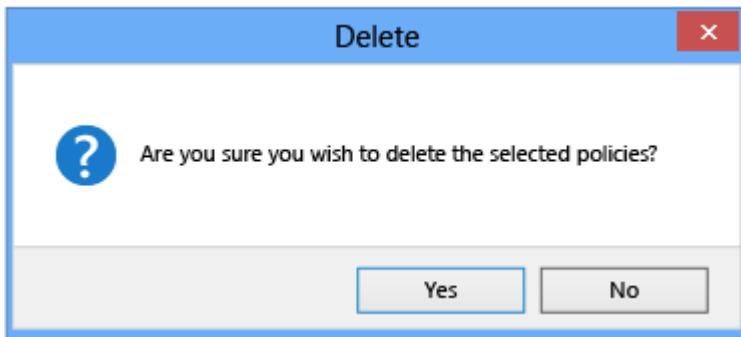
4. When the **Create a Policy** window appears, enter your changes, and then click **OK**.

Delete a backup policy

Use the following procedure to delete a backup policy.

To delete a backup policy

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the Scope pane, click the **Backup Policies** node. All the backup policies appear in the Results pane.
3. Right-click the backup policy that you want to delete, and then click **Delete**.
4. When the confirmation message appears, click **Yes**.



Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to view and manage backup jobs](#).

Use StorSimple Snapshot Manager to create and manage volume groups

Article • 08/22/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

You can use the **Volume Groups** node on the **Scope** pane to assign volumes to volume groups, view information about a volume group, schedule backups, and edit volume groups.

Volume groups are pools of related volumes used to ensure that backups are application-consistent. For more information, see [Volumes and volume groups](#) and [Integration with Windows Volume Shadow Copy Service](#).

ⓘ Important

- All volumes in a volume group must come from a single cloud service provider.
- When you configure volume groups, do not mix cluster-shared volumes (CSVs) and non-CSVs in the same volume group. StorSimple Snapshot Manager does not support a mix of CSVs and non-CSVs in the same snapshot.

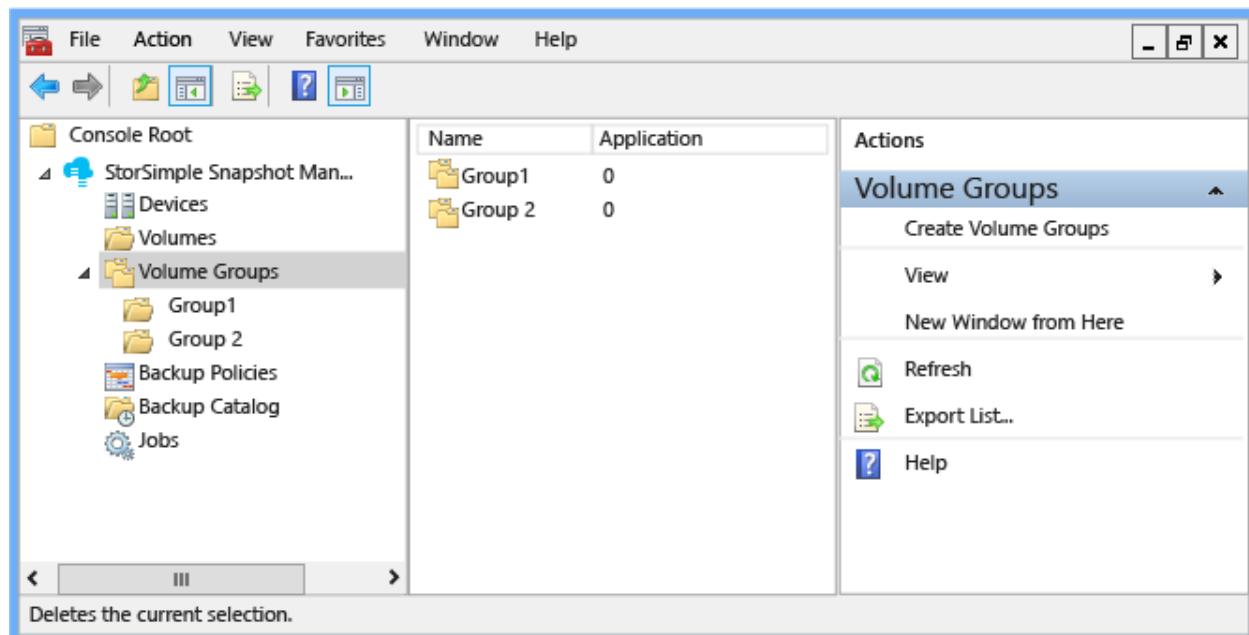


Figure 1: StorSimple Snapshot Manager Volume Groups node

This tutorial explains how you can use StorSimple Snapshot Manager to:

- View information about your volume groups
- Create a volume group
- Back up a volume group
- Edit a volume group
- Delete a volume group

All of these actions are also available on the **Actions** pane.

View volume groups

If you click the **Volume Groups** node, the **Results** pane shows the following information about each volume group, depending on the column selections you make. (The columns in the **Results** pane are configurable. Right-click the **Volumes** node, select **View**, and then select **Add/Remove Columns**.)

Results column	Description
Name	The Name column contains the name of the volume group.
Application	The Applications column shows the number of VSS writers currently installed and running on the Windows host.
Selected	The Selected column shows the number of volumes that are contained in the volume group. A zero (0) indicates that no application is associated with the volumes in the volume group.

Results column	Description
Imported	The Imported column shows the number of imported volumes. When set to True , this column indicates that a volume group was imported from the Azure portal and was not created in StorSimple Snapshot Manager.

① Note

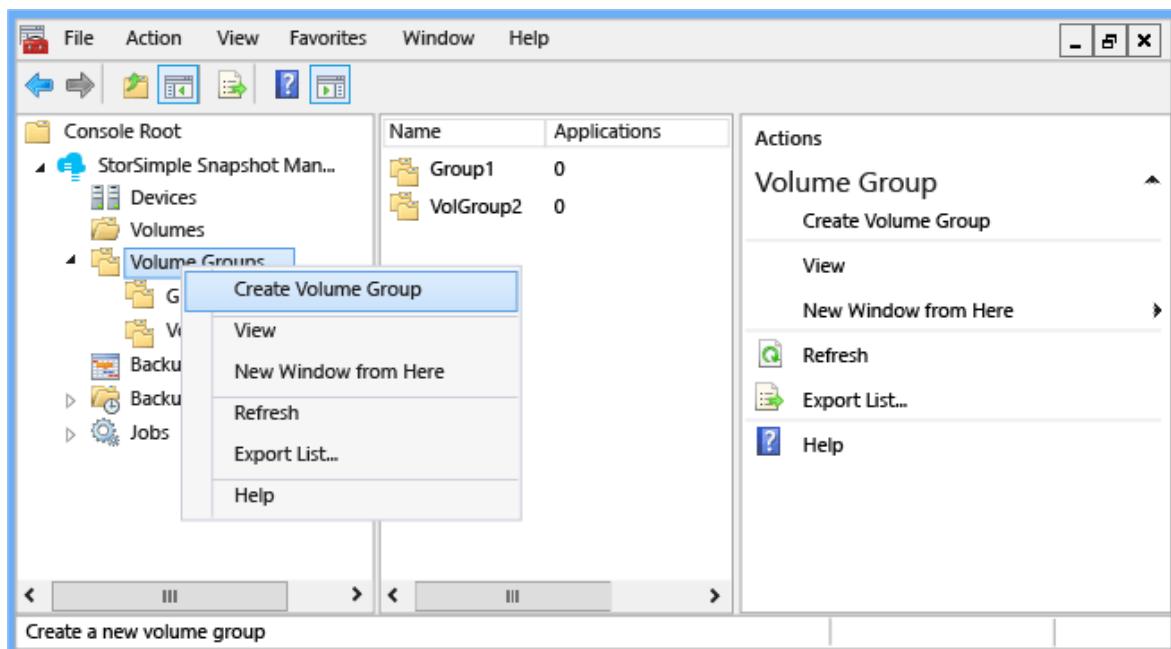
StorSimple Snapshot Manager volume groups are also displayed on the **Backup Policies** tab in the Azure portal.

Create a volume group

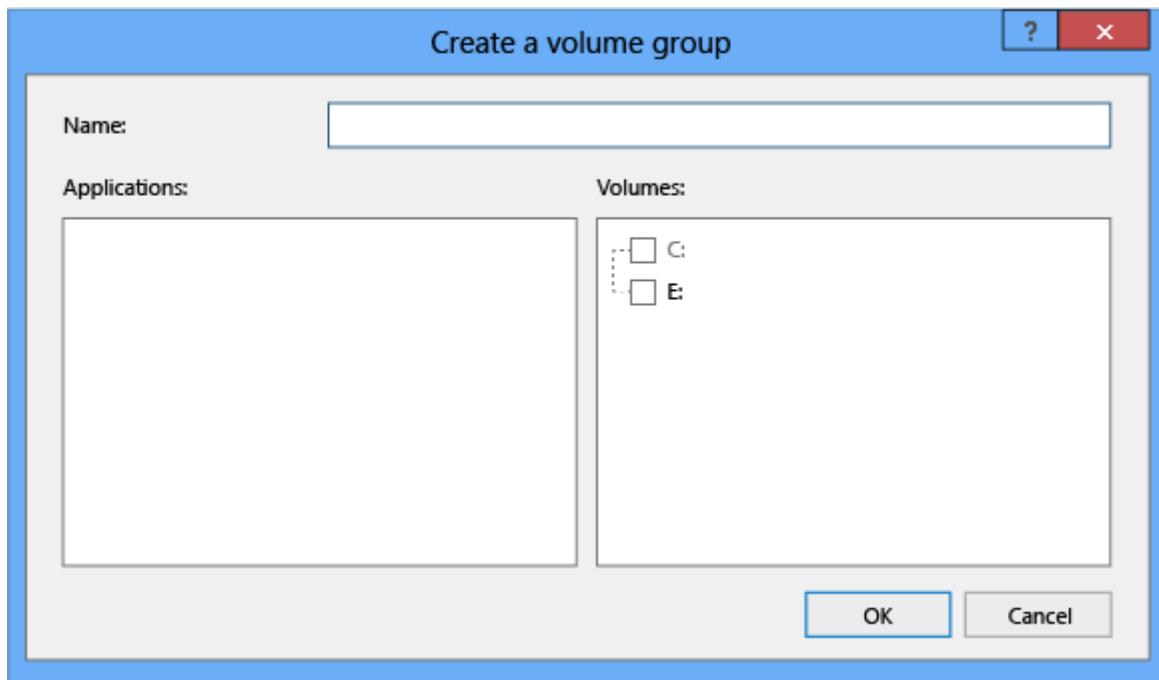
Use the following procedure to create a volume group.

To create a volume group

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click **Volume Groups**, and then click **Create Volume Group**.



The **Create a volume group** dialog box appears.



3. Enter the following information:

- a. In the **Name** box, type a unique name for the new volume group.
- b. In the **Applications** box, select applications associated with the volumes that you will be adding to the volume group.

The **Applications** box lists only those applications that use StorSimple volumes and have VSS writers enabled for them. A VSS writer is enabled only if all the volumes that the writer is aware of are StorSimple volumes. If the Applications box is empty, then no applications that use Azure StorSimple volumes and have supported VSS writers are installed. (Currently, Azure StorSimple supports Microsoft Exchange and SQL Server.) For more information about VSS writers, see [Integration with Windows Volume Shadow Copy Service](#).

If you select an application, all volumes associated with it are automatically selected. Conversely, if you select volumes associated with a specific application, the application is automatically selected in the **Applications** box.

- c. In the **Volumes** box, select StorSimple volumes to add to the volume group.

- You can include volumes with single or multiple partitions. (Multiple partition volumes can be dynamic disks or basic disks with multiple partitions.) A volume that contains multiple partitions is treated as a single unit. Consequently, if you add only one of the partitions to a volume group, all the other partitions are automatically added to that volume group at the same time. After you add a multiple partition volume to a volume group, the multiple partition volume continues to be treated as a single unit.

- You can create empty volume groups by not assigning any volumes to them.
- Do not mix cluster-shared volumes (CSVs) and non-CSVs in the same volume group. StorSimple Snapshot Manager does not support a mix of CSV volumes and non-CSV volumes in the same snapshot.

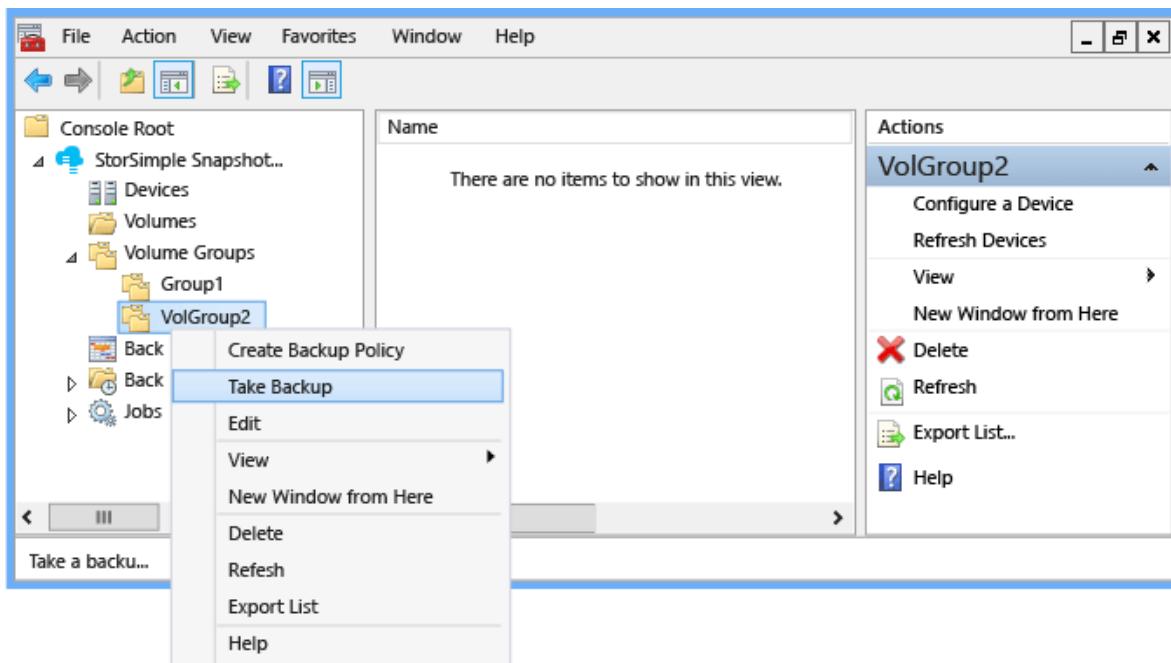
4. Click **OK** to save the volume group.

Back up a volume group

Use the following procedure to back up a volume group.

To back up a volume group

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Volume Groups** node, right-click a volume group name, and then click **Take Backup**.



3. In the **Take Backup** dialog box, select **Local Snapshot** or **Cloud Snapshot**, and then click **Create**.



4. To confirm that the backup is running, expand the **Jobs** node, and then click **Running**. The backup should be listed.
5. To view the completed snapshot, expand the **Backup Catalog** node, expand the volume group name, and then click **Local Snapshot** or **Cloud Snapshot**. The backup will be listed if it finished successfully.

Edit a volume group

Use the following procedure to edit a volume group.

To edit a volume group

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Volume Groups** node, right-click a volume group name, and then click **Edit**.
3. The **Create a volume group** dialog box appears. You can change the **Name**, **Applications**, and **Volumes** entries.
4. Click **OK** to save your changes.

Delete a volume group

Use the following procedure to delete a volume group.

Warning

This also deletes all the backups associated with the volume group.

To delete a volume group

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Volume Groups** node, right-click a volume group name, and then click **Delete**.
3. The **Delete Volume Group** dialog box appears. Type **Confirm** in the text box, and then click **OK**.

The deleted volume group vanishes from the list in the **Results** pane and all backups that are associated with that volume group are deleted from the backup catalog.

Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to create and manage backup policies](#).

Use StorSimple Snapshot Manager to manage the backup catalog

Article • 08/22/2022 • 7 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The primary function of StorSimple Snapshot Manager is to allow you to create application-consistent backup copies of StorSimple volumes in the form of snapshots. Snapshots are then listed in an XML file called a *backup catalog*. The backup catalog organizes snapshots by volume group and then by local snapshot or cloud snapshot.

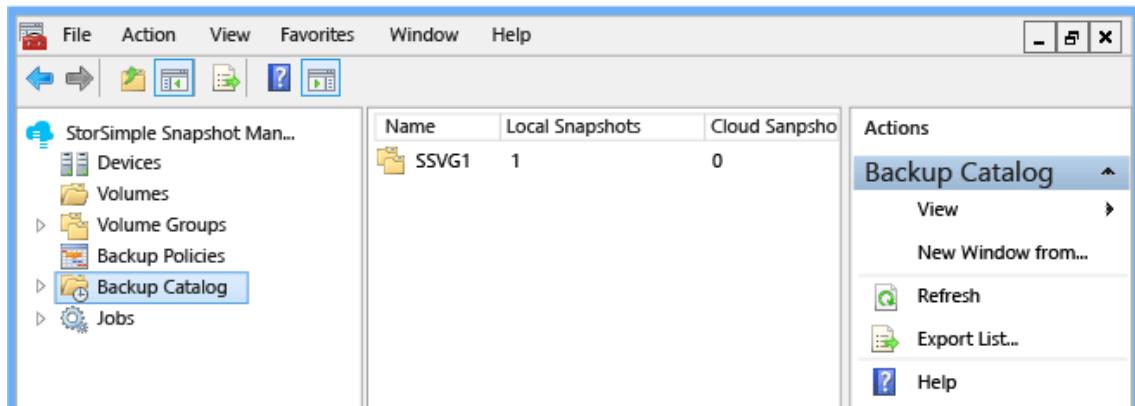
This tutorial describes how you can use the **Backup Catalog** node to complete the following tasks:

- Restore a volume
- Clone a volume or volume group
- Delete a backup
- Recover a file
- Restore the Storsimple Snapshot Manager database

You can view the backup catalog by expanding the **Backup Catalog** node in the **Scope** pane, and then expanding the volume group.

- If you click the volume group name, the **Results** pane shows the number of local snapshots and cloud snapshots available for the volume group.
- If you click **Local Snapshot** or **Cloud Snapshot**, the **Results** pane shows the following information about each backup snapshot (depending on your **View** settings):
 - **Name** – the time the snapshot was taken.

- **Type** – whether this is a local snapshot or a cloud snapshot.
- **Owner** – the content owner.
- **Available** – whether the snapshot is currently available. **True** indicates that the snapshot is available and can be restored; **False** indicates that the snapshot is no longer available.
- **Imported** – whether the backup was imported. **True** indicates that the backup was imported from the StorSimple Device Manager service at the time the device was configured in StorSimple Snapshot Manager; **False** indicates that it was not imported, but was created by StorSimple Snapshot Manager. (You can easily identify an imported volume group because a suffix is added that identifies the device from which the volume group was imported.)



- If you expand **Local Snapshot** or **Cloud Snapshot**, and then click an individual snapshot name, the **Results** pane shows the following information about the snapshot that you selected:
 - **Name** – the volume identified by drive letter.
 - **Local Name** – the local name of the drive (if available).
 - **Device** – the name of the device on which the volume resides.
 - **Available** – whether the snapshot is currently available. **True** indicates that the snapshot is available and can be restored; **False** indicates that the snapshot is no longer available.

Restore a volume

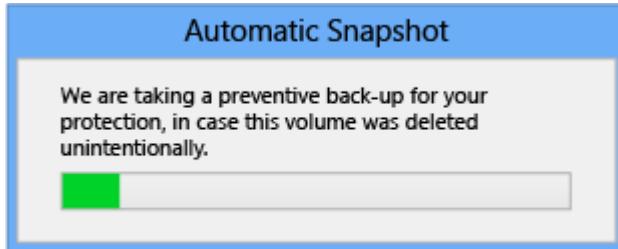
Use the following procedure to restore a volume from backup.

Prerequisites

If you have not already done so, create a volume and volume group, and then delete the volume. By default, StorSimple Snapshot Manager backs up a volume before permitting

it to be deleted. This precaution can prevent data loss if the volume is deleted unintentionally or if the data needs to be recovered for any reason.

StorSimple Snapshot Manager displays the following message while it creates the precautionary backup.

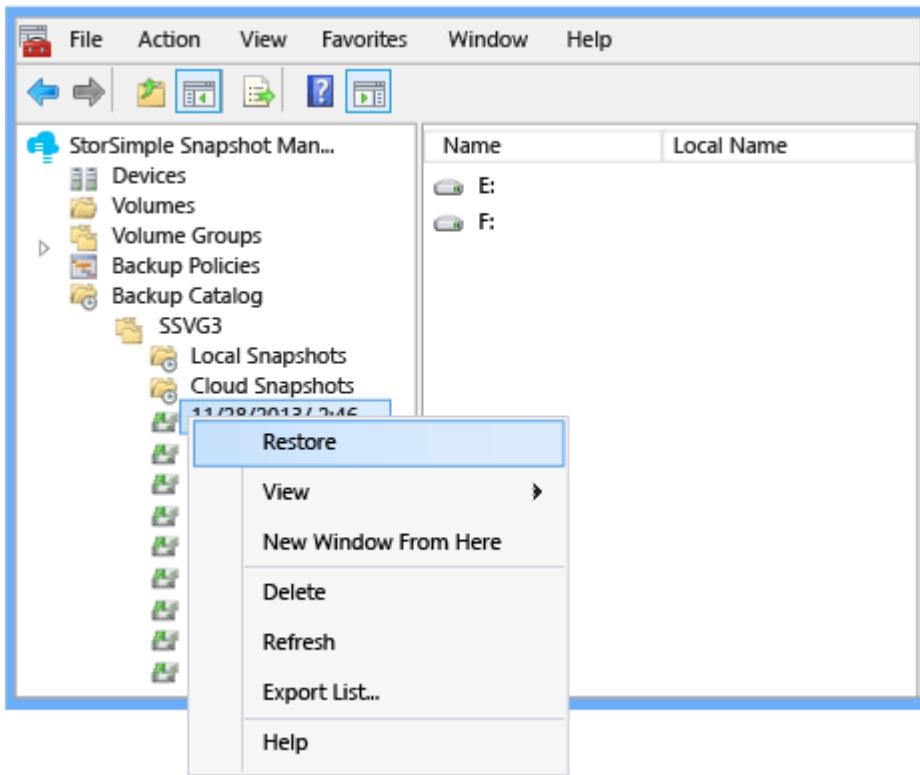


ⓘ Important

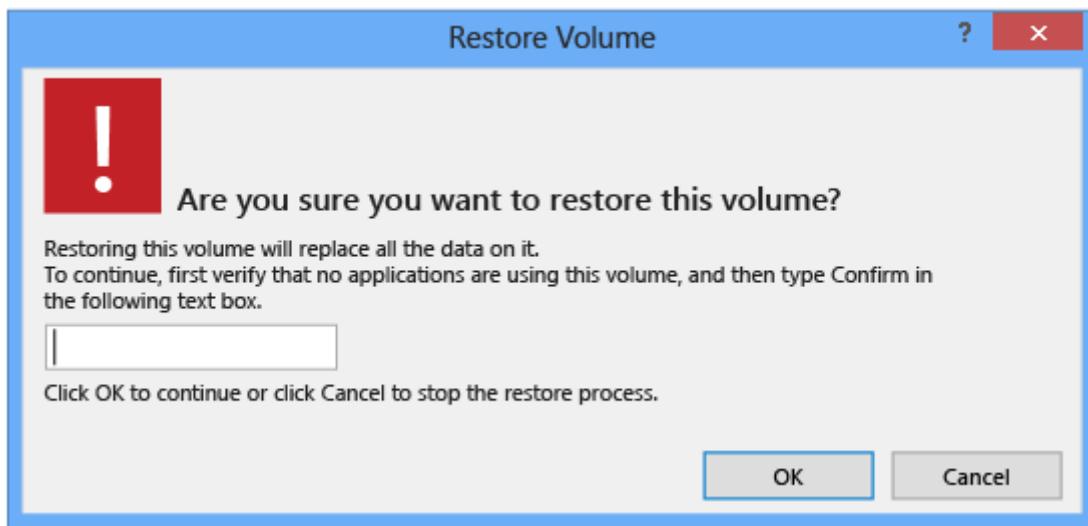
You cannot delete a volume that is part of a volume group. The delete option is unavailable.

To restore a volume

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Backup Catalog** node, expand a volume group, and then click **Local Snapshots** or **Cloud Snapshots**. A list of backup snapshots appears in the **Results** pane.
3. Find the backup that you want to restore, right-click, and then click **Restore**.



4. On the confirmation page, review the details, type **Confirm**, and then click **OK**.
StorSimple Snapshot Manager uses the backup to restore the volume.



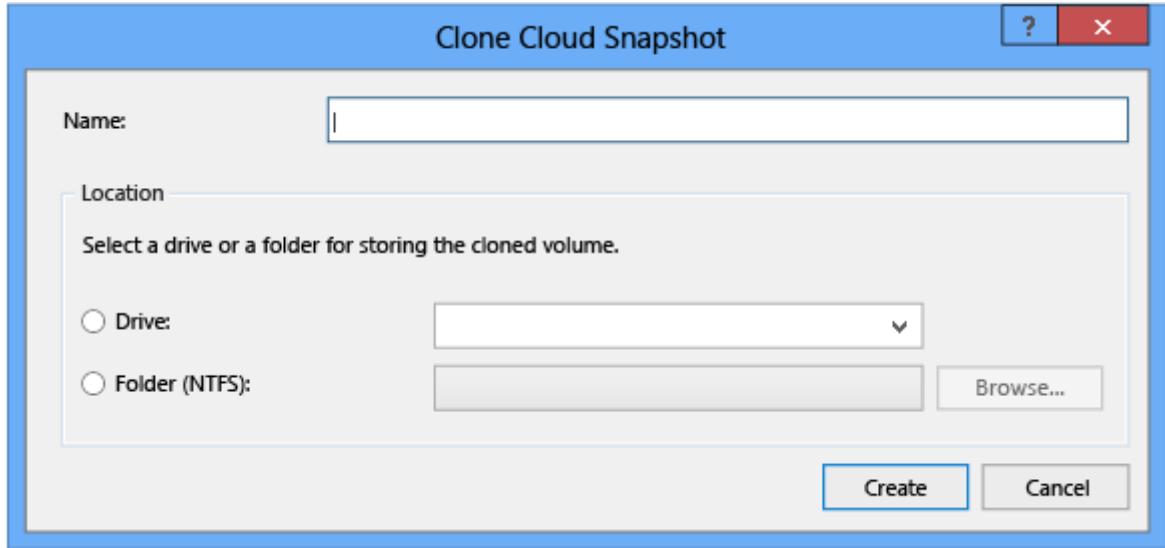
5. You can monitor the restore action as it runs. In the **Scope** pane, expand the **Jobs** node, and then click **Running**. The job details appear in the **Results** pane. When the restore job is finished, the job details are transferred to the **Last 24 hours** list.

Clone a volume or volume group

Use the following procedure to create a duplicate (clone) of a volume or volume group.

To clone a volume or volume group

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Backup Catalog** node, expand a volume group, and then click **Cloud Snapshots**. A list of backups appears in the **Results** pane.
3. Find the volume or volume group that you want to clone, right-click the volume or volume group name, and click **Clone**. The **Clone Cloud Snapshot** dialog box appears.



4. Complete the **Clone Cloud Snapshot** dialog box as follows:
 - a. In the **Name** text box, type a name for the cloned volume. This name will appear in the **Volumes** node.
 - b. (Optional) select **Drive**, and then select a drive letter from the drop-down list.
 - c. (Optional) select **Folder (NTFS)**, and type a folder path or click **Browse** and select a location for the folder.
 - d. Click **Create**.
5. When the cloning process is finished, you must initialize the cloned volume. Start Server Manager, and then start Disk Management. For detailed instructions, see [Mount volumes](#). After it is initialized, the volume will be listed under the **Volumes** node in the **Scope** pane. If you do not see the volume listed, refresh the list of volumes (right-click the **Volumes** node, and then click **Refresh**).

Delete a backup

Use the following procedure to delete a snapshot from the backup catalog.

 **Note**

Deleting a snapshot deletes the backed up data associated with the snapshot. However, the process of cleaning up data from the cloud may take some time.

To delete a backup

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Backup Catalog** node, expand a volume group, and then click **Local Snapshots** or **Cloud Snapshots**. A list of snapshots appears in the **Results** pane.
3. Right-click the snapshot you want to delete, and then click **Delete**.
4. When the confirmation message appears, click **OK**.

Recover a file

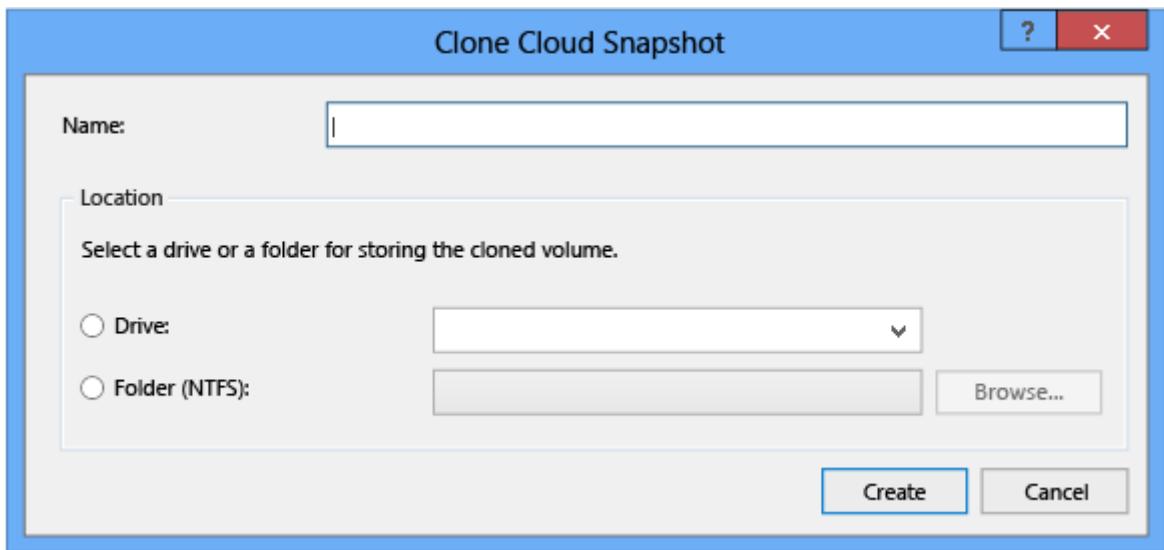
If a file is accidentally deleted from a volume, you can recover the file by retrieving a snapshot that pre-dates the deletion, using the snapshot to create a clone of the volume, and then copying the file from the cloned volume to the original volume.

Prerequisites

Before you begin, make sure that you have a current backup of the volume group. Then, delete a file stored on one of the volumes in that volume group. Finally, use the following steps to restore the deleted file from your backup.

To recover a deleted file

1. Click the StorSimple Snapshot Manager icon on your desktop. The StorSimple Snapshot Manager console window appears.
2. In the **Scope** pane, expand the **Backup Catalog** node, and browse to a snapshot that contains the deleted file. Typically, you should select a snapshot that was created just before the deletion.
3. Find the volume that you want to clone, right-click, and click **Clone**. The **Clone Cloud Snapshot** dialog box appears.



4. Complete the **Clone Cloud Snapshot** dialog box as follows:
 - a. In the **Name** text box, type a name for the cloned volume. This name will appear in the **Volumes** node.
 - b. (Optional) Select **Drive**, and then select a drive letter from the drop-down list.
 - c. (Optional) Select **Folder (NTFS)**, and type a folder path or click **Browse** and select a location for the folder.
 - d. Click **Create**.
5. When the cloning process is finished, you must initialize the cloned volume. Start Server Manager, and then start Disk Management. For detailed instructions, see [Mount volumes](#). After it is initialized, the volume will be listed under the **Volumes** node in the **Scope** pane.

If you do not see the volume listed, refresh the list of volumes (right-click the **Volumes** node, and then click **Refresh**).
6. Open the NTFS folder that contains the cloned volume, expand the **Volumes** node, and then open the cloned volume. Find the file that you want to recover, and copy it to the primary volume.
7. After you restore the file, you can delete the NTFS folder that contains the cloned volume.

Restore the StorSimple Snapshot Manager database

You should regularly back up the StorSimple Snapshot Manager database on the host computer. If a disaster occurs or the host computer fails for any reason, you can then restore it from the backup. Creating the database backup is a manual process.

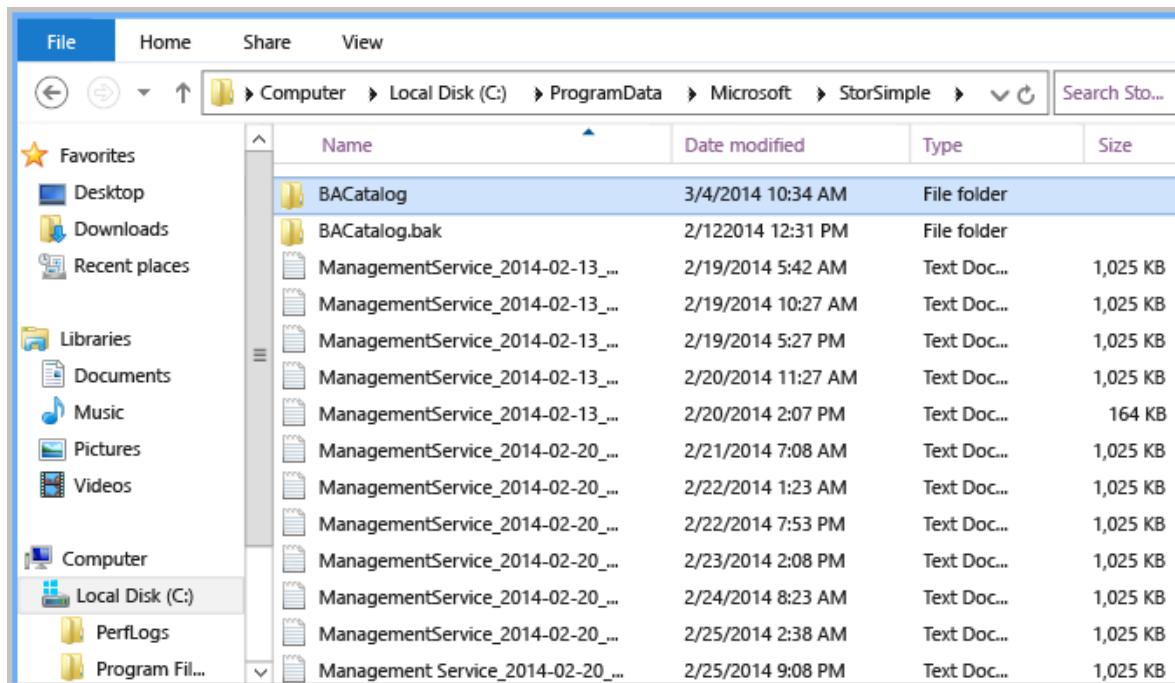
To back up and restore the database

1. Stop the Microsoft StorSimple Management Service:
 - a. Start Server Manager.
 - b. On the Server Manager dashboard, on the **Tools** menu, select **Services**.
 - c. On the **Services** window, select the **Microsoft StorSimple Management Service**.
 - d. In the right pane, under **Microsoft StorSimple Management Service**, click **Stop the service**.
2. On the host computer, browse to
C:\ProgramData\Microsoft\StorSimple\BACatalog.

 **Note**

ProgramData is a hidden folder.

3. Find the catalog XML file, copy the file, and store the copy in a safe location or in the cloud. If the host fails, you can use this backup file to help recover the backup policies that you created in StorSimple Snapshot Manager.



4. Restart the Microsoft StorSimple Management Service:
 - a. On the Server Manager dashboard, on the **Tools** menu, select **Services**.
 - b. On the **Services** window, select the **Microsoft StorSimple Management Service**.
 - c. In the right pane, under **Microsoft StorSimple Management Service**, click **Restart the service**.
5. On the host computer, browse to
C:\ProgramData\Microsoft\StorSimple\BACatalog.

6. Delete the catalog XML file, and replace it with the backup version that you created.
7. Click the desktop StorSimple Snapshot Manager icon to start StorSimple Snapshot Manager.

Next steps

- Learn more about [using StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn more about [StorSimple Snapshot Manager tasks and workflows](#).

Use StorSimple Snapshot Manager to view and manage backup jobs

Article • 08/22/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The **Jobs** node in the **Scope** pane shows the **Scheduled**, **Last 24 hours**, and **Running** backup tasks that you initiated interactively or by a configured policy.

This tutorial explains how you can use the **Jobs** node to display information about scheduled, recent, and currently running backup jobs. (The list of jobs and corresponding information appears in the **Results** pane.) Additionally, you can right-click a listed job and see a context menu that lists available actions.

View scheduled jobs

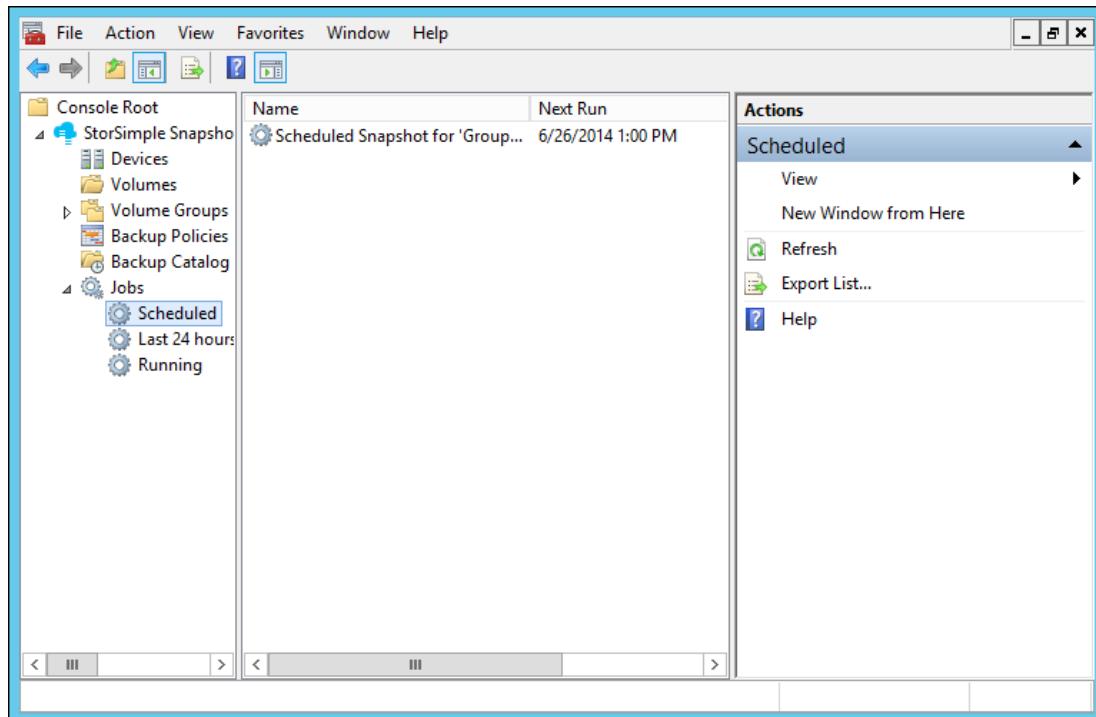
Use the following procedure to view scheduled backup jobs.

To view scheduled jobs

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Jobs** node, and click **Scheduled**. The following information appears in the **Results** pane:
 - **Name** – the name of the scheduled snapshot
 - **Next Run** – the date and time of the next scheduled snapshot
 - **Last Run** – the date and time of the most recent scheduled snapshot

Note

For one-time only snapshots, the **Next Run** and **Last Run** will be the same.



3. To perform additional actions on a specific job, right-click the job name in the **Results** pane and select from the menu options.

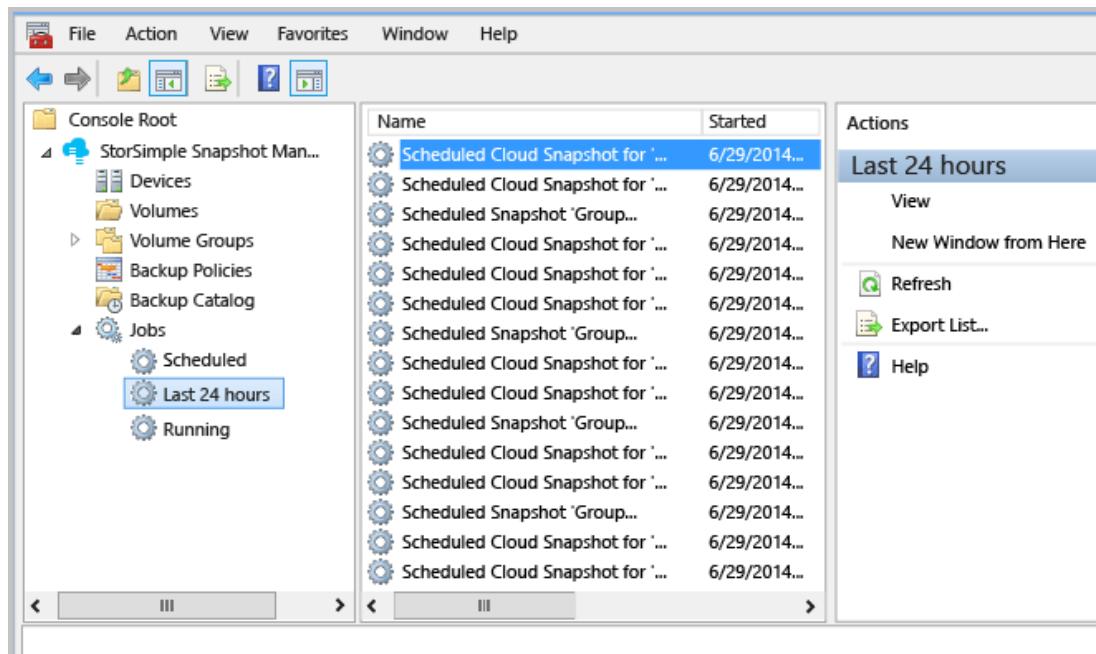
View recent jobs

Use the following procedure to view backup and restore jobs that were completed in the last 24 hours.

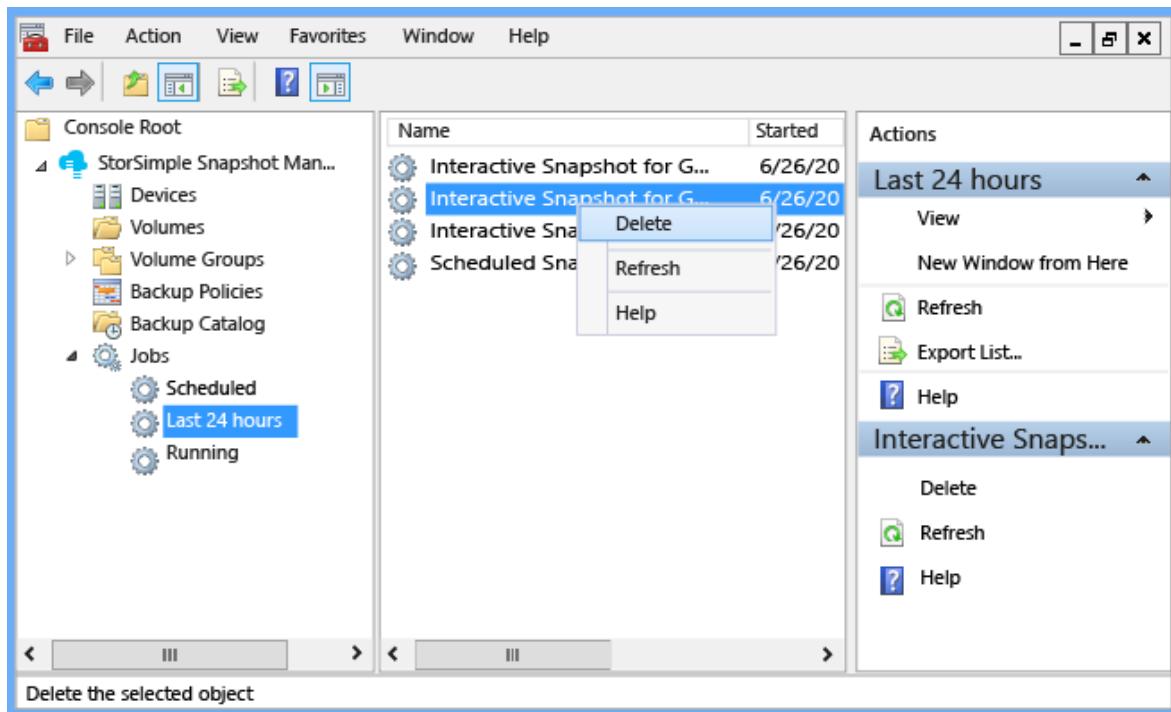
To view recent jobs

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Jobs** node, and click **Last 24 hours**. The **Results** pane shows backup jobs for the last 24 hours (to a maximum of 64 jobs). The following information appears in the **Results** pane, depending on the **View** options you specify:
 - **Name** – the name of the scheduled snapshot.
 - **Started** – the date and time when the snapshot began.

- **Stopped** – the date and time when the snapshot finished or was terminated.
- **Elapsed** – the amount of time between the **Started** and **Stopped** times.
- **Status** – the state of the recently completed job. **Success** indicates that the backup was created successfully. **Failed** indicates that the job did not run successfully.
- **Information** – the reason for the failure.
- **Bytes processed (MB)** – the amount of data from the volume group that was processed (in MBs).



3. To perform additional actions on a specific job, right-click the job name in the Results pane and select from the menu options.



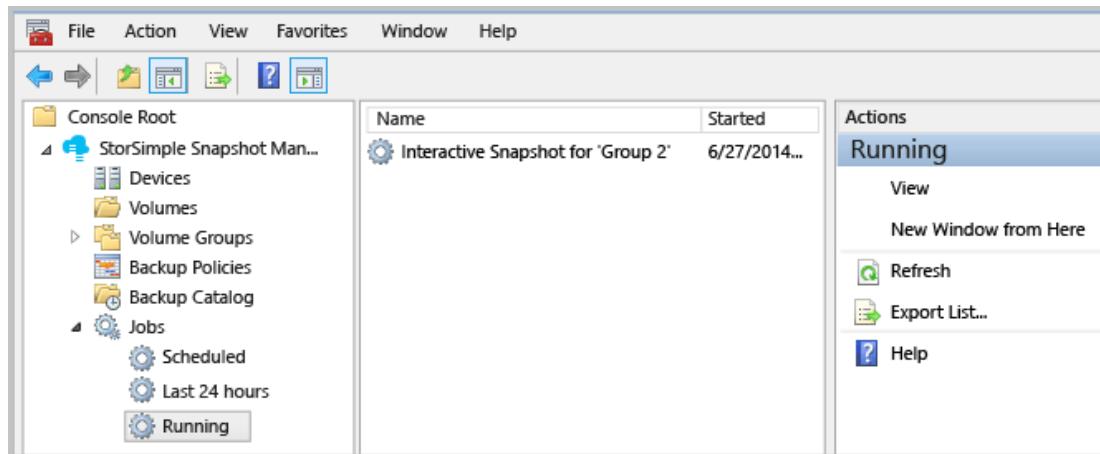
View currently running jobs

Use the following procedure to view jobs that are currently running.

To view currently running jobs

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, expand the **Jobs** node, and click **Running**. Depending on the **View** options you specify, the following information appears in the **Results** pane:
 - **Name** – the name of the scheduled snapshot.
 - **Started** – the date and time when the snapshot began.
 - **Checkpoint** – the current action of the backup.
 - **Status** – the percentage of completion.
 - **Elapsed** – the amount of time that has passed since the backup began.
 - **Average throughput (MB)** – ratio of total bytes of data processed to that of total time taken for processing (MBs).
 - **Bytes processed (MB)** – total bytes of data processed (in MBs).
 - **Bytes written (MB)** – total bytes of data written (in MBs). It includes the data as well as the metadata and hence is typically greater than the Bytes

Processed.



3. To perform additional actions on a specific job, right-click the job name in the **Results** pane and select from the menu options.

Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to manage the backup catalog](#).

Use StorSimple Snapshot Manager to view and manage volumes

Article • 08/22/2022 • 9 minutes to read

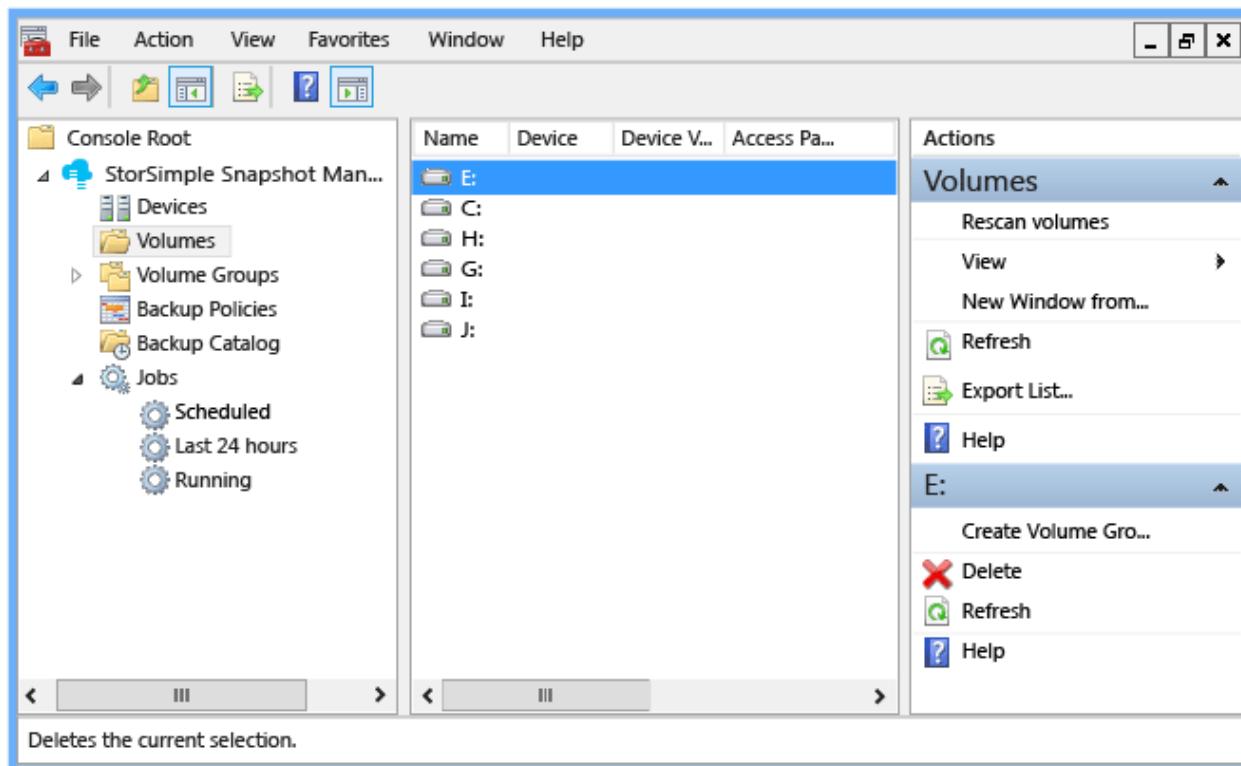
⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

You can use the StorSimple Snapshot Manager **Volumes** node (on the **Scope** pane) to select volumes and view information about them. The volumes are presented as drives that correspond to the volumes mounted by the host. The **Volumes** node shows local volumes and volume types that are supported by StorSimple, including volumes discovered through the use of iSCSI and a device.

For more information about supported volumes, go to [Support for multiple volume types](#).



The **Volumes** node also lets you rescan or delete volumes after StorSimple Snapshot Manager discovers them.

This tutorial explains how you can mount, initialize, and format volumes and then use StorSimple Snapshot Manager to:

- View information about volumes
- Delete volumes
- Rescan volumes
- Configure a basic volume and back it up
- Configure a dynamic mirrored volume and back it up

Note

All of the **Volume** node actions are also available in the **Actions** pane.

Mount volumes

Use the following procedure to mount, initialize, and format StorSimple volumes. This procedure uses Disk Management, a system utility for managing hard disks and the corresponding volumes or partitions. For more information about Disk Management, go to [Disk Management](#) on the Microsoft TechNet website.

To mount volumes

1. On your host computer, start the Microsoft iSCSI initiator.
2. Supply one of the interface IP addresses as the target portal or discovery IP address, and connect to the device. After the device is connected, the volumes will be accessible to your Windows system. For more information about using the Microsoft iSCSI initiator, go to the section “Connecting to an iSCSI target device” in [Installing and Configuring Microsoft iSCSI Initiator](#).
3. Use any of the following options to start Disk Management:
 - Type Diskmgmt.msc in the **Run** box.
 - Start Server Manager, expand the **Storage** node, and then select **Disk Management**.
 - Start **Administrative Tools**, expand the **Computer Management** node, and then select **Disk Management**.

 **Note**

You must use administrator privileges to run Disk Management.

4. Take the volume(s) online:
 - a. In Disk Management, right-click any volume marked **Offline**.
 - b. Click **Reactivate Disk**. The disk should be marked **Online** after the disk is reactivated.
5. Initialize the volume(s):
 - a. Right-click the discovered volumes.
 - b. On the menu, select **Initialize Disk**.
 - c. In the **Initialize Disk** dialog box, select the disks that you want to initialize, and then click **OK**.
6. Format simple volumes:
 - a. Right-click a volume that you want to format.
 - b. On the menu, select **New Simple Volume**.
 - c. Use the New Simple Volume wizard to format the volume:
 - Specify the volume size.
 - Supply a drive letter.
 - Select the NTFS file system.

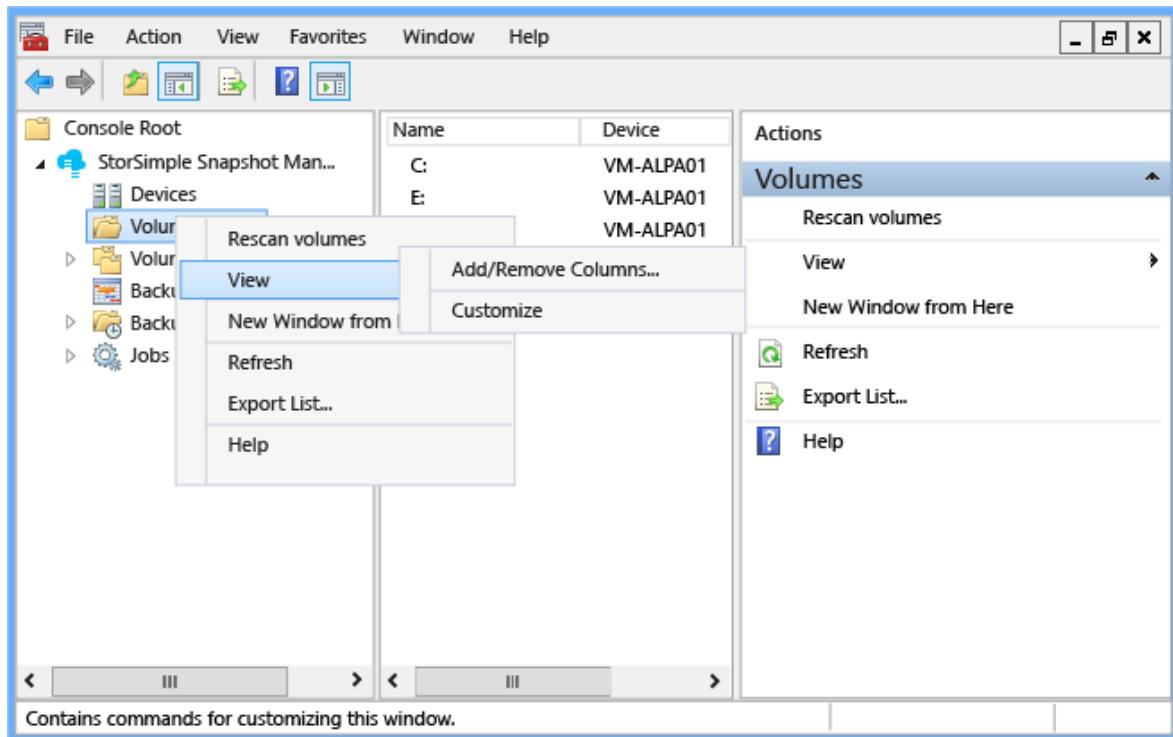
- Specify a 64 KB allocation unit size.
 - Perform a quick format.
7. Format multi-partition volumes. For instructions, go to the section, "Partitions and Volumes" in [Implementing Disk Management](#).

View information about your volumes

Use the following procedure to view information about local and Azure StorSimple volumes.

To view volume information

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click the **Volumes** node. A list of local and mounted volumes, including all Azure StorSimple volumes, appears in the **Results** pane. The columns in the **Results** pane are configurable. (Right-click the **Volumes** node, select **View**, and then select **Add/Remove Columns**.)



Results column	Description
Name	The Name column contains the drive letter assigned to each discovered volume.
Device	The Device column contains the IP address of the device connected to the host computer.

Results column	Description
Device Volume Name	The Device Volume Name column contains the name of the device volume to which the selected volume belongs. This is the volume name defined in the Azure portal for that specific volume.
Access Paths	The Access Paths column displays the access path to the volume. This is the drive letter or mount point at which the volume is accessible on the host computer.

Delete a volume

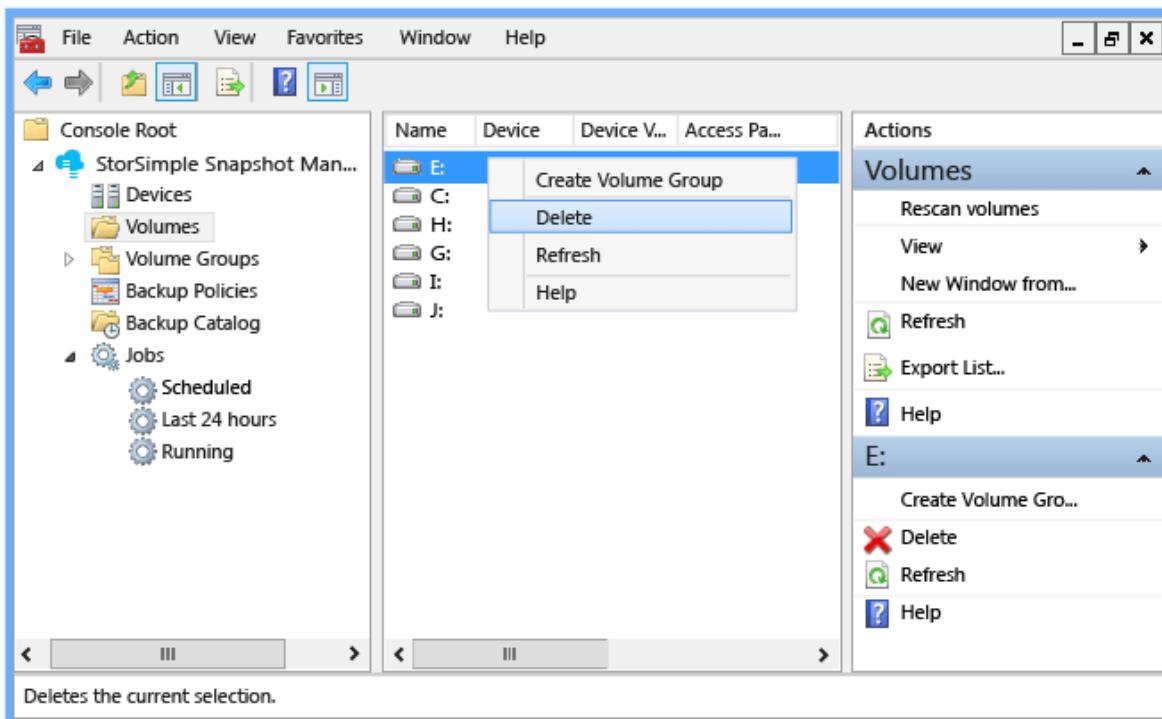
Use the following procedure to delete a volume from StorSimple Snapshot Manager.

Note

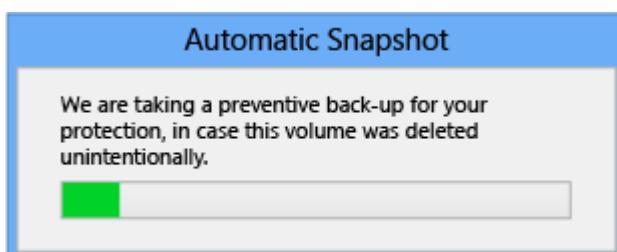
You cannot delete a volume if it is a part of any volume group. (The delete option is not available for volumes that are members of a volume group.) You must delete the entire volume group to delete the volume.

To delete a volume

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, click the **Volumes** node.
3. In the **Results** pane, right-click the volume that you want to delete.
4. On the menu, click **Delete**.



5. The **Delete Volume** dialog box appears. Type **Confirm** in the text box, and then click **OK**.
6. By default, StorSimple Snapshot Manager backs up a volume before deleting it. This precaution can protect you from data loss if the deletion was unintentional. StorSimple Snapshot Manager displays an **Automatic Snapshot** progress message while it backs up the volume.

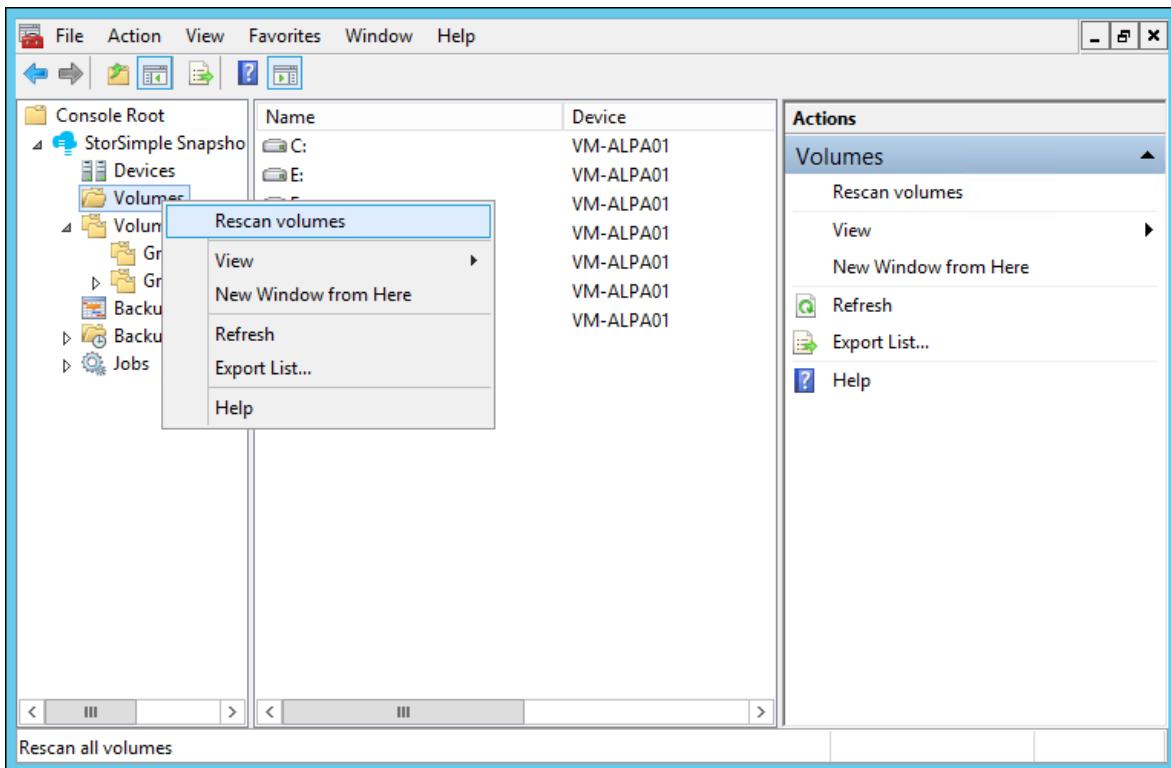


Rescan volumes

Use the following procedure to rescan the volumes connected to StorSimple Snapshot Manager.

To rescan the volumes

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click **Volumes**, and then click **Rescan volumes**.



This procedure synchronizes the volume list with StorSimple Snapshot Manager. Any changes, such as new volumes or deleted volumes, will be reflected in the results.

Configure and back up a basic volume

Use the following procedure to configure a backup of a basic volume, and then either start a backup immediately or create a policy for scheduled backups.

Prerequisites

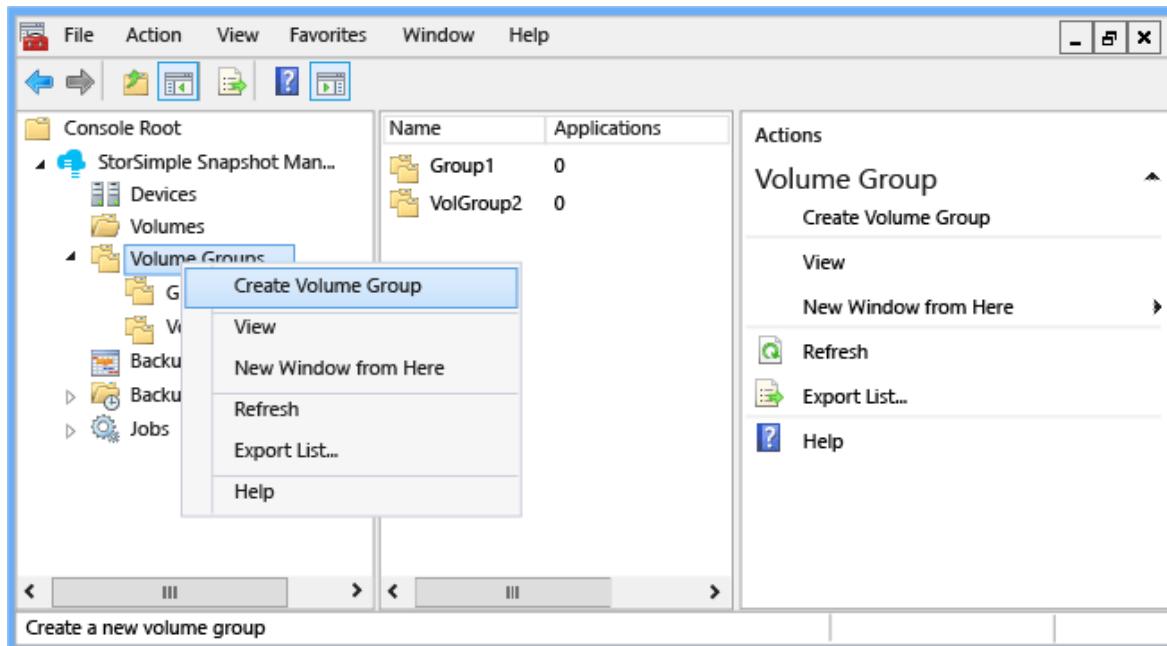
Before you begin:

- Make sure that the StorSimple device and host computer are configured correctly. For more information, go to [Deploy your on-premises StorSimple device](#).
- Install and configure StorSimple Snapshot Manager. For more information, go to [Deploy StorSimple Snapshot Manager](#).

To configure backup of a basic volume

1. Create a basic volume on the StorSimple device.
2. Mount, initialize, and format the volume as described in [Mount volumes](#).

3. Click the StorSimple Snapshot Manager icon on your desktop. The StorSimple Snapshot Manager window appears.
4. In the **Scope** pane, right-click the **Volumes** node, and then select **Rescan volumes**. When the scan is finished, a list of volumes should appear in the **Results** pane.
5. In the **Results** pane, right-click the volume, and then select **Create Volume Group**.



6. In the **Create Volume Group** dialog box, type a name for the volume group, assign volumes to it, and then click **OK**.
7. In the **Scope** pane, expand the **Volume Groups** node. The new volume group should appear under the **Volume Groups** node.
8. Right-click the volume group name.
 - To start an interactive (on-demand) backup job, click **Take Backup**.
 - To schedule an automatic backup, click **Create Backup Policy**. On the **General** page, select a volume group from the list. On the **Schedule** page, enter the schedule details. When you are finished, click **OK**.
9. To confirm that the backup job has started, expand the **Jobs** node in the **Scope** pane, and then click the **Running** node. The list of currently running jobs appears in the **Results** pane.

Configure and back up a dynamic mirrored volume

Complete the following steps to configure backup of a dynamic mirrored volume:

- Step 1: Use Disk Management to create a dynamic mirrored volume.
- Step 2: Use StorSimple Snapshot Manager to configure backup.

Prerequisites

Before you begin:

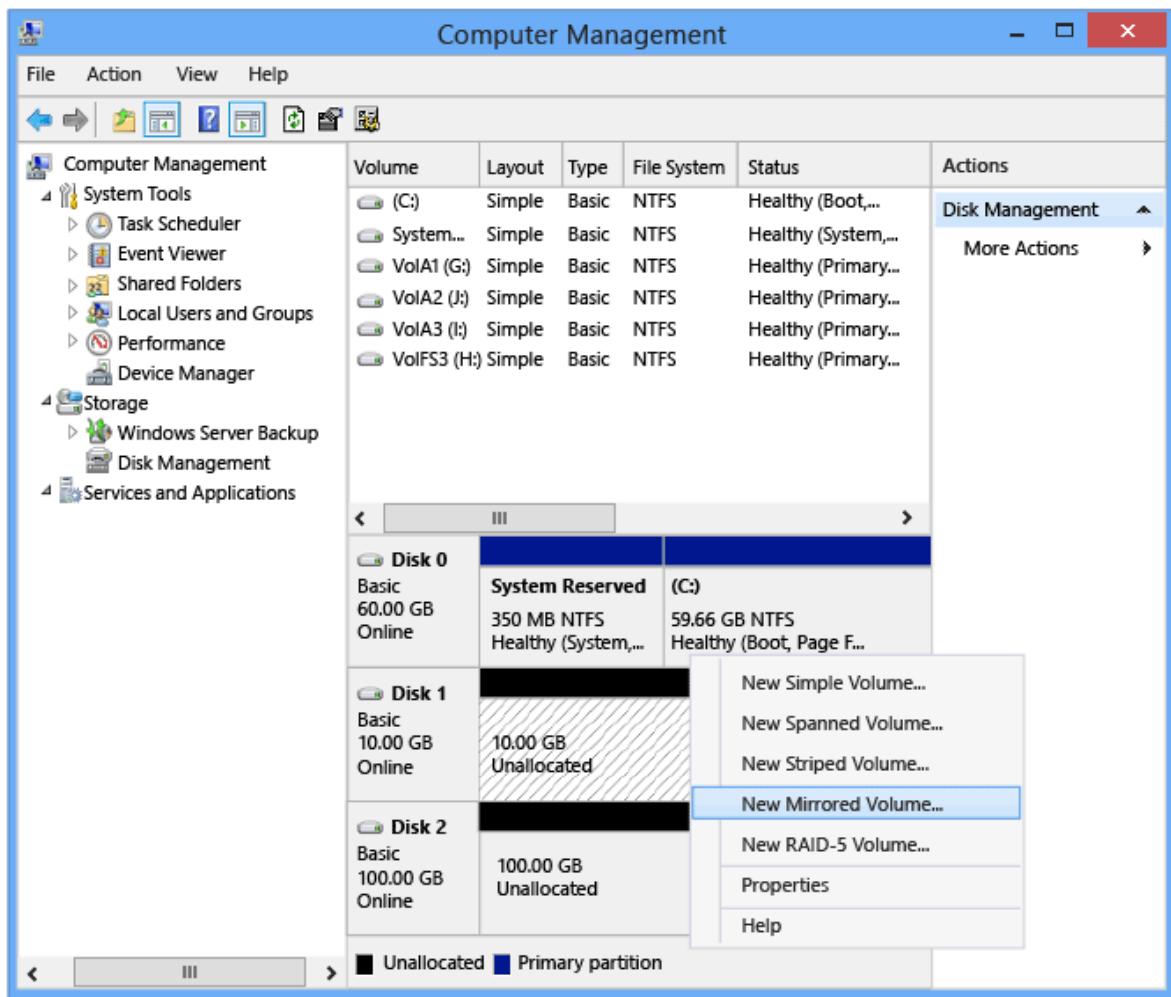
- Make sure that the StorSimple device and host computer are configured correctly. For more information, go to [Deploy your on-premises StorSimple device](#).
- Install and configure StorSimple Snapshot Manager. For more information, go to [Deploy StorSimple Snapshot Manager](#).
- Configure two volumes on the StorSimple device. (In the examples, the available volumes are **Disk 1** and **Disk 2**.)

Step 1: Use Disk Management to create a dynamic mirrored volume

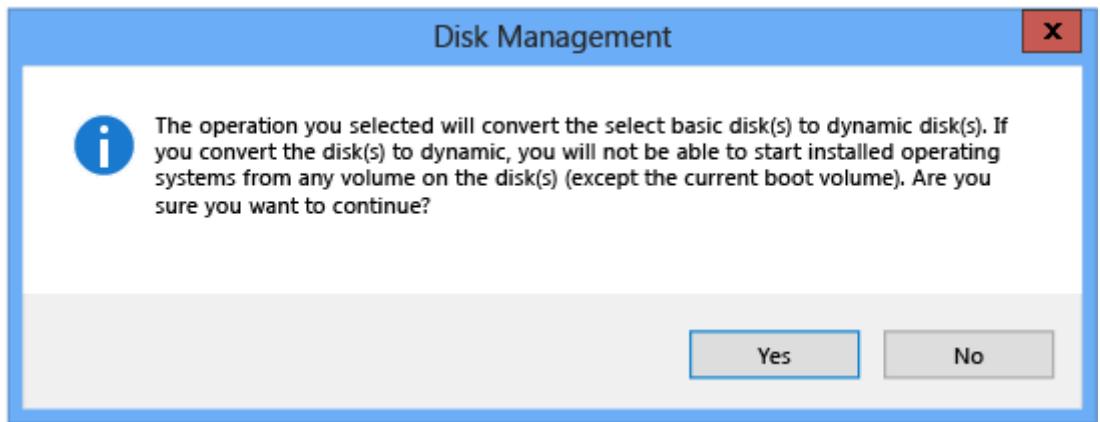
Disk Management is a system utility for managing hard disks and the volumes or partitions that they contain. For more information about Disk Management, go to [Disk Management](#) on the Microsoft TechNet website.

To create a dynamic mirrored volume

1. Use any of the following options to start Disk Management:
 - Open the **Run** box, type **Diskmgmt.msc**, and press Enter.
 - Start Server Manager, expand the **Storage** node, and then select **Disk Management**.
 - Start **Administrative Tools**, expand the **Computer Management** node, and then select **Disk Management**.
2. Make sure that you have two volumes available on the StorSimple device. (In the example, the available volumes are **Disk 1** and **Disk 2**.)
3. In the Disk Management window, in the right column of the lower pane, right-click **Disk 1** and select **New Mirrored Volume**.



4. On the **New Mirrored Volume** wizard page, click **Next**.
5. On the **Select Disks** page, select **Disk 2** in the **Selected** pane, click **Add**, and then click **Next**.
6. On the **Assign Drive Letter or Path** page, accept the defaults, and then click **Next**.
7. On the **Format Volume** page, in the **Allocation Unit Size** box, select **64K**. Select the **Perform a quick format** check box, and then click **Next**.
8. On the **Completing the New Mirrored Volume** page, review your settings, and then click **Finish**.
9. A message appears to indicate that the basic disk will be converted to a dynamic disk. Click **Yes**.



10. In Disk Management, verify that Disk 1 and Disk 2 are shown as dynamic mirrored volumes. (Dynamic should appear in the status column, and the capacity bar color should change to red, indicating a mirrored volume.)

Computer Management						
File Action View Help	System Tools	Volume	Layout	Type	File System	Status
	Task Scheduler	(C:)	Simple	Basic	NTFS	Healthy (Boot,...
	Event Viewer	System...	Simple	Basic	NTFS	Healthy (System,...
	Shared Folders	VolA1 (G:)	Simple	Basic	NTFS	Healthy (Primary...
	Local Users and Groups	VolA2 (J:)	Simple	Basic	NTFS	Healthy (Primary...
	Performance	VolA3 (I:)	Simple	Basic	NTFS	Healthy (Primary...
	Device Manager	VolFS3 (H:)	Simple	Basic	NTFS	Healthy (Primary...
	Disk Management	Disk 0	System Reserved	(C:)	59.66 GB NTFS	Disk Management
		Basic	350 MB NTFS		Healthy (System,...	More Actions
		60.00 GB				
		Online				
	Disk 1	New Volume (E:)				
	Dynamic	10.00 GB				
	10.00 GB					
	Online					
	Disk 2	New Volume (E:)				
	Dynamic	100.00 GB				
	100.00 GB					
	Online					
	Disk 3	VolFS3 (H:)				
	Basic	1024.00 GB				
	1024.00 GB					
	Online					
		Unallocated	Primary partition	Mirrored volume		

Step 2: Use StorSimple Snapshot Manager to configure backup

Use the following procedure to configure a dynamic mirrored volume, and then either start a backup immediately or create a policy for scheduled backups.

To configure backup of a dynamic mirrored volume

1. Click the StorSimple Snapshot Manager icon on your desktop. The StorSimple Snapshot Manager window appears.
2. In the **Scope** pane, right-click the **Volumes** node and select **Rescan volumes**. When the scan is finished, a list of volumes should appear in the **Results** pane. The dynamic mirrored volume is listed as a single volume.
3. In the **Results** pane, right-click the dynamic mirrored volume, and then click **Create Volume Group**.
4. In the **Create Volume Group** dialog box, type a name for the volume group, assign the dynamic mirrored volume to this group, and then click **OK**.
5. In the **Scope** pane, expand the **Volume Groups** node. The new volume group should appear under the **Volume Groups** node.
6. Right-click the volume group name.
 - To start an interactive (on-demand) backup job, click **Take Backup**.
 - To schedule an automatic backup, click **Create Backup Policy**. On the **General** page, select the volume group from the list. On the **Schedule** page, enter the schedule details. When you are finished, click **OK**.
7. You can monitor the backup job as it runs. In the **Scope** pane, expand the **Jobs** node, and then click **Running**. The job details appear in the **Results** pane. When the backup job is finished, the details are transferred to the **Last 24 hours** job list.

Next steps

- Learn how to [use StorSimple Snapshot Manager to administer your StorSimple solution](#).
- Learn how to [use StorSimple Snapshot Manager to create and manage volume groups](#).

Use the MMC menu actions in StorSimple Snapshot Manager

Article • 08/22/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

In StorSimple Snapshot Manager, you will see the following actions listed on all action menus and all variations of the **Actions** pane.

- View
- New Window from Here
- Refresh
- Export List
- Help

These actions are part of the Microsoft Management Console (MMC) and are not specific to StorSimple Snapshot Manager. This tutorial describes these actions and explains how to use each of them in StorSimple Snapshot Manager.

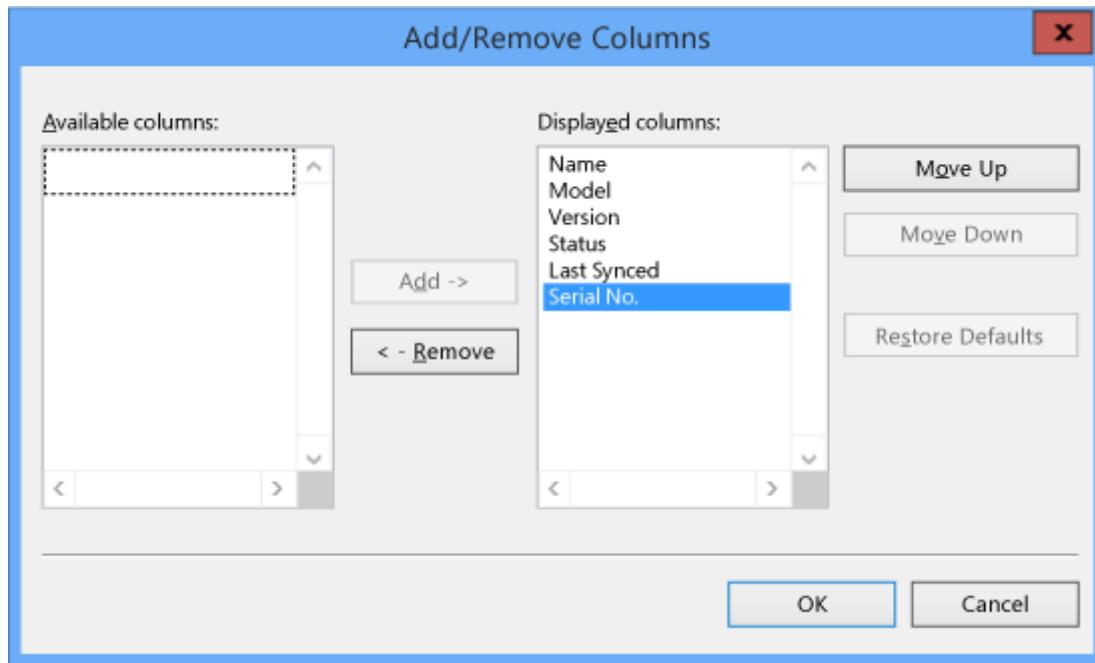
View

You can use the **View** option to change the **Results** pane view and to change the console window view.

To change the Results pane view

1. Click the desktop icon to start StorSimple Snapshot Manager.

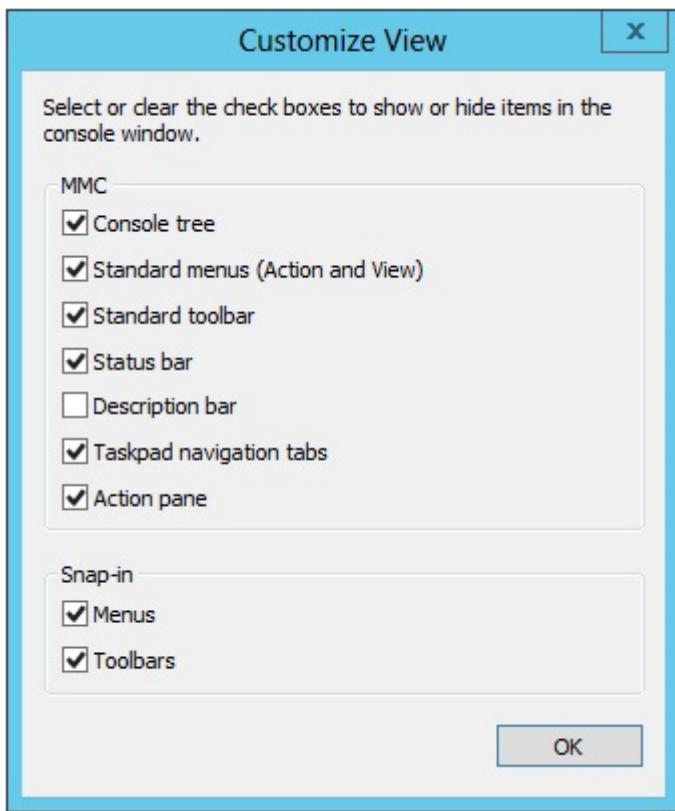
2. In the **Scope** pane, right-click any node or expand the node and right-click an item in the **Results** pane, and then click the **View** option.
3. To add or remove the columns that appear in the **Results** pane, click **Add/Remove Columns**. The **Add/Remove Columns** dialog box appears.



4. Complete the form as follows:
 - Select items from the **Available columns** list and click **Add** to add them to the **Displayed columns** list.
 - Click items in the **Displayed columns** list, and click **Remove** to remove them from the list.
 - Select an item in the **Displayed columns** list and click **Move Up** or **Move Down** to move the item up or down in the list.
 - Click **Restore Defaults** to return to the default **Results** pane configuration.
5. When you are finished with your selections, click **OK**.

To change the console window view

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click any node, click **View**, and then click **Customize**. The **Customize** dialog box appears.



3. Select or clear the check boxes to show or hide items in the console window. When you are finished with your selections, click **OK**.

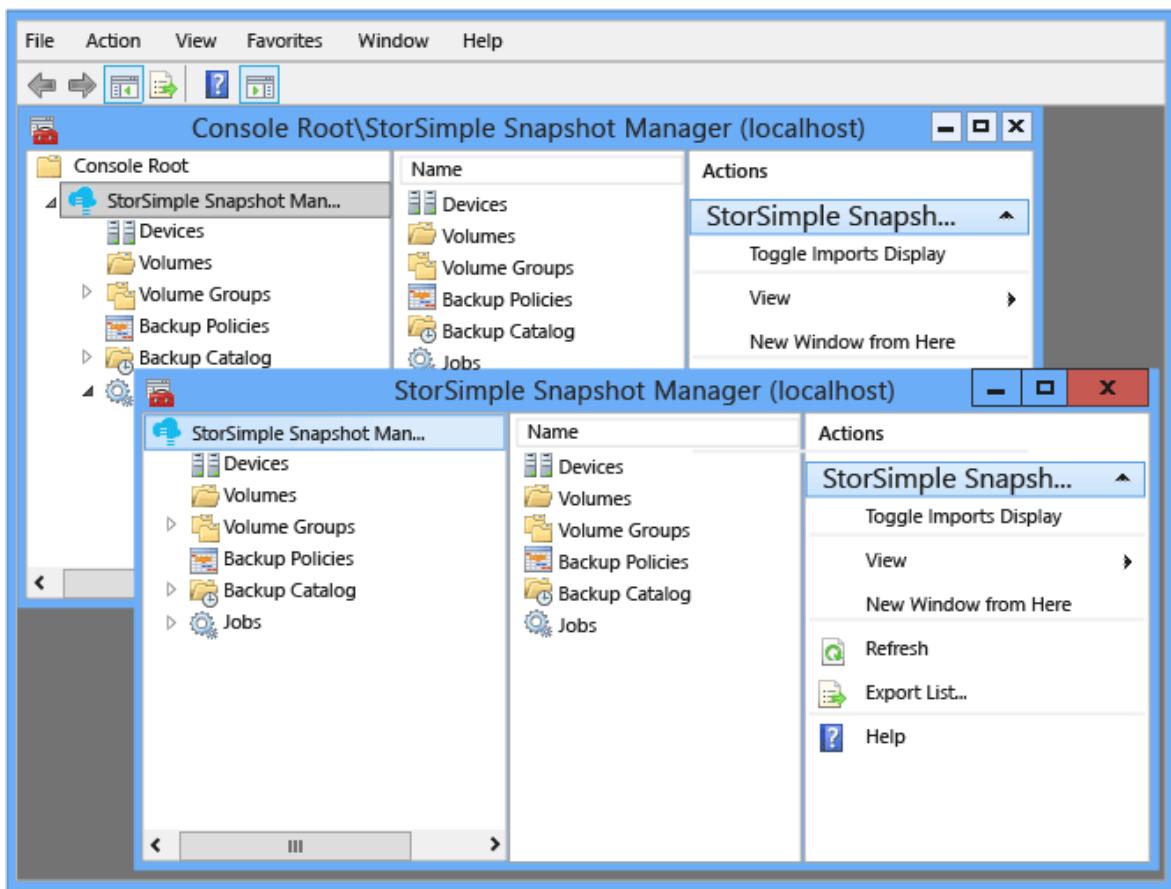
New Window from Here

You can use the **New Window from Here** option to open a new console window.

To open a new console window

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click any node, and then click **New Window from Here**.

A new window appears, showing only the scope that you selected. For example, if you right-click the **Backup Policies** node, the new window will show only the **Backup Policies** node in the **Scope** pane and a list of defined backup policies in the **Results** pane. See the following example.



Refresh

You can use the **Refresh** action to update the console window.

To update the console window

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click any node or expand the node and right-click an item in the **Results** pane, and then click **Refresh**.

Export List

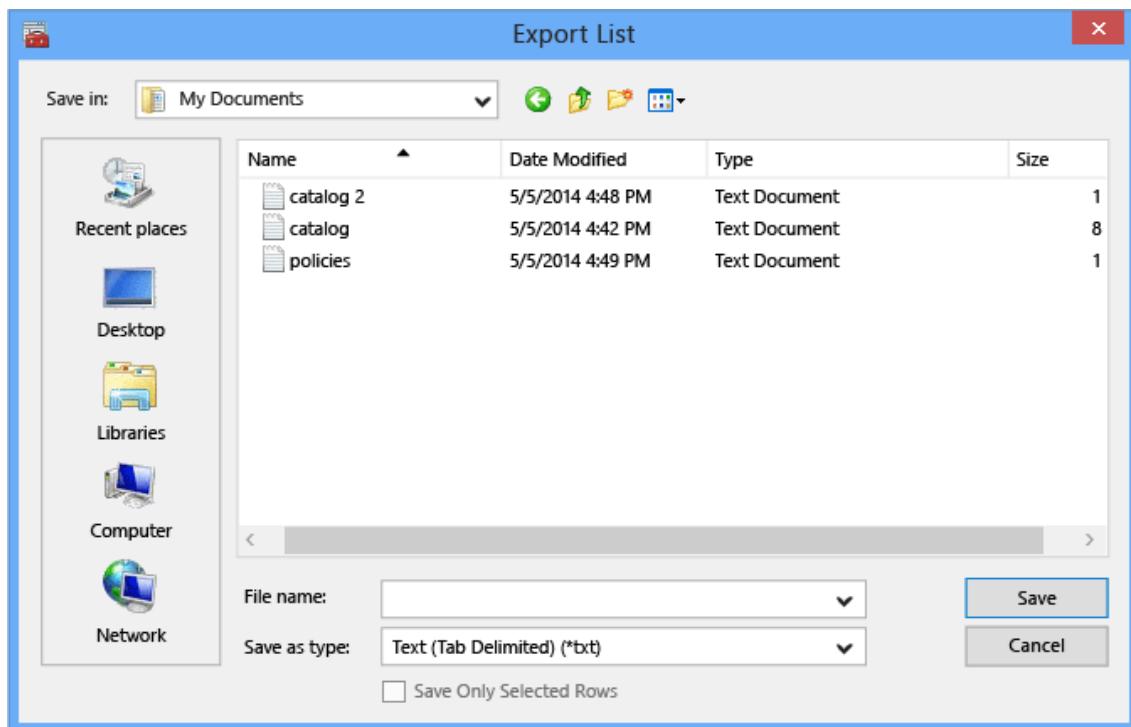
You can use the **Export List** action to save a list in a comma-separated value (CSV) file. For example, you can export the list of backup policies or the backup catalog. You can then import the CSV file into a spreadsheet application for analysis.

To save a list in a comma-separated value (CSV) file

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click any node or expand the node and right-click an item in the **Results** pane, and then click **Export List**.

3. The **Export List** dialog box appears. Complete the form as follows:

- a. In the **File name** box, type a name for the CSV file or click the arrow to select from the drop-down list.
- b. In the **Save as type** box, click the arrow and select a file type from the drop-down list.
- c. To save only selected items, select the rows and then click the **Save Only Selected Rows** check box. To save all exported lists, clear the **Save Only Selected Rows** check box.
- d. Click **Save**.



Help

You can use the **Help** menu to view available online help for StorSimple Snapshot Manager and the MMC.

To view available online help

1. Click the desktop icon to start StorSimple Snapshot Manager.
2. In the **Scope** pane, right-click any node or expand the node and right-click an item in the **Results** pane, and then click **Help**.

Next steps

- Learn more about the StorSimple Snapshot Manager user interface.
- Learn more about [using StorSimple Snapshot Manager to administer your StorSimple solution](#).

Use Azure Resource Manager SDK-based scripts to manage StorSimple devices

Article • 03/31/2023 • 4 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article describes how Azure Resource Manager SDK-based scripts can be used to manage your StorSimple 8000 series device. A sample script is also included to walk you through the steps of configuring your environment to run these scripts.

This article applies to StorSimple 8000 series devices running in Azure portal only.

Sample scripts

The following sample scripts are available to automate various StorSimple jobs.

Table of Azure Resource Manager SDK-based sample scripts

Azure Resource Manager Script	Description
Authorize-ServiceEncryptionRollover.ps1	This script allows you to authorize your StorSimple device to change the service data encryption key.
Create-StorSimpleCloudAppliance.ps1	This script creates an 8010 or an 8020 StorSimple Cloud Appliance. The cloud appliance can then be configured and registered with your StorSimple Data Manager service.
CreateOrUpdate-Volume.ps1	This script creates or modifies StorSimple volumes.

Azure Resource Manager Script	Description
Get-DeviceBackup.ps1	This script lists all the backups for a device registered with your StorSimple Device Manager service.
Get-DeviceBackupPolicy.ps1	This script lists all the backup policies for your StorSimple device.
Get-DeviceJobs.ps1	This script gets all the StorSimple jobs running on your StorSimple Device Manager service.
Get-DeviceUpdateAvailability.ps1	This script scans the Update server and lets you know if updates are available to install on your StorSimple device.
Install-DeviceUpdate.ps1	This script installs the available updates on your StorSimple device.
Manage-CloudSnapshots.ps1	This script starts a manual cloud snapshot and deletes cloud snapshots older than specified retention days.
Monitor-Backups.ps1	This Azure Automation Runbook PowerShell script reports the status of all backup jobs.
Remove-DeviceBackup.ps1	This script deletes a single backup object.
Start-DeviceBackupJob.ps1	This script starts a manual backup on your StorSimple device.
Update-CloudApplianceServiceEncryptionKey.ps1	This script updates the service data encryption key for all the 8010/8020 StorSimple Cloud Appliances registered with your StorSimple Device Manager service.
Verify-BackupScheduleAndBackup.ps1	This script highlights the missing backups after analyzing all the schedules associated with backup policies. It also verifies the backup catalog with the list of available backups.

Configure and run a sample script

This section takes an example script and details the various steps required to run the script.

Prerequisites

Before you begin, ensure that you have:

- Azure PowerShell installed. To install Azure PowerShell modules:
 - In a Windows environment, follow the steps in [Install and configure Azure PowerShell](#). You can install Azure PowerShell on your Windows Server host for your StorSimple if using one.
 - In a Linux or MacOS environment, follow the steps in [Install and configure Azure PowerShell on MacOS or Linux](#).

For more information about using Azure PowerShell, go to [Get started with using Azure PowerShell](#).

Run Azure PowerShell script

The script used in this example lists all the jobs on a StorSimple device. This includes the jobs that succeeded, failed, or are in progress. Perform the following steps to download and run the script.

1. Launch Azure PowerShell. Create a new folder and change directory to the new folder.

```
mkdir C:\scripts\StorSimpleSDKTools  
cd C:\scripts\StorSimpleSDKTools
```

2. [Download NuGet CLI](#) under the folder created in the previous step. There are various versions of *nuget.exe*. Choose the version corresponding to your SDK. Each download link points directly to an .exe file. Be sure to right-click and save the file to your computer rather than running it from the browser.

You can also run the following command to download and store the script in the same folder that you created earlier.

```
wget https://dist.nuget.org/win-x86-commandline/latest/nuget.exe -  
Out C:\scripts\StorSimpleSDKTools\NuGet.exe
```

3. Download the dependent SDK.

```
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.Azure.Management.Storsimple8000series  
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.IdentityModel.Clients.ActiveDirectory -Version 2.28.3  
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.Rest.ClientRuntime.Azure.Authentication -Version 2.2.9-  
preview
```

4. Download the script from the sample GitHub project.

```
wget  
https://raw.githubusercontent.com/anoobbacker/storsimpledevicemgmttools/master/Get-DeviceJobs.ps1 -Out Get-DeviceJobs.ps1
```

5. Run the script. When prompted to authenticate, provide your Azure credentials.
This script should output a filtered list of all the jobs on your StorSimple device.

```
.\Get-StorSimpleJob.ps1 -SubscriptionId [subid] -TenantId [tenant  
id] -DeviceName [name of device] -ResourceGroupName [name of resource  
group] -ManagerName [name of device manager] -FilterByStatus [Filter for  
job status] -FilterByJobType [Filter for job type] -FilterByStartTime  
[Filter for start date time] -FilterByEndTime [Filter for end date  
time]
```

Sample output

The following output is presented when the sample script is run. The output contains all the jobs that ran on a registered device that started on September 25, 2017 and completed by October 2, 2017.

```
-----  
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Scripts\StorSimpleSDKTools> wget  
https://raw.githubusercontent.com/anoobbacker/storsimpledevicemgmttools/master/Get-DeviceJobs.ps1 -Out Get-DeviceJobs.ps1  
PS C:\Scripts\StorSimpleSDKTools> .\Get-DeviceJobs.ps1 -SubscriptionId  
1234ab5c-678d-910e-9fc4-0accc9c0166e -TenantId 12a345bc-67d8-91ef-01ab-
```

```
2c7cd123ef45 -DeviceName 8600-ABC1234567D89EF -ResourceGroupName Contoso -  
ManagerName ContosoDeviceMgr -FilterByStartTime "09/25/2017 08:10:02" -  
FilterByEndTime "10/02/2017 08:10:02"
```

```
Status : Succeeded  
StartTime : 10/2/2017 10:30:02 PM  
EndTime : 10/2/2017 10:31:36 PM  
PercentComplete : 100  
Error :  
JobType : ScheduledBackup  
DataStats :  
Microsoft.Azure.Management.StorSimple8000Series.Models.DataStatistics  
EntityLabel : ss-asr-policy1  
EntityType : Microsoft.StorSimple/managers/devices/backupPolicies  
JobStages :  
DeviceId : /subscriptions/1234ab5c-678d-910e-9fc4-  
0accc9c0166e/resourceGroups/Contoso/providers/Microsoft.Stor  
Simple/managers/ContosoDeviceMgr/devices/8600-  
SHG0997877L71FC  
IsCancellable : True  
BackupType : CloudSnapshot  
SourceDeviceId :  
BackupPointInTime : 1/1/0001 12:00:00 AM  
Id : /subscriptions/1234ab5c-678d-910e-9fc4-  
0accc9c0166e/resourceGroups/Contoso/providers/Microsoft.Stor  
Simple/managers/ContosoDeviceMgr/devices/8600-  
SHG0997877L71FC/jobs/75905c48-b153-4af1-8b21-4b9a2ff9  
825b  
Name : 75905c48-b153-4af1-8b21-4b9a2ff9825b  
Type : Microsoft.StorSimple/managers/devices/jobs  
Kind : Series8000  
-----  
CUT CUT  
-----  
Status : Succeeded  
StartTime : 9/26/2017 5:00:02 PM  
EndTime : 9/26/2017 5:01:20 PM  
PercentComplete : 100  
Error :  
JobType : ScheduledBackup  
DataStats :  
Microsoft.Azure.Management.StorSimple8000Series.Models.DataStatistics  
EntityLabel : 8010 policy  
EntityType : Microsoft.StorSimple/managers/devices/backupPolicies  
JobStages :  
DeviceId : /subscriptions/1234ab5c-678d-910e-9fc4-  
0accc9c0166e/resourceGroups/Contoso/providers/Microsoft.Stor  
Simple/managers/ContosoDeviceMgr/devices/8600-  
ABC1234567D89EF  
IsCancellable : True  
BackupType : CloudSnapshot  
SourceDeviceId :  
BackupPointInTime : 1/1/0001 12:00:00 AM  
Id : /subscriptions/1234ab5c-678d-910e-9fc4-
```

```
0accc9c0166e/resourceGroups/Contoso/providers/Microsoft.Stor
Simple/managers/ContosoDeviceMgr/devices/8600-
ABC1234567D89EF/jobs/3cf8108-db60-4e9a-a8da-6d8fe457
8d2b
Name : 3cf8108-db60-4e9a-a8da-6d8fe4578d2b
Type : Microsoft.StorSimple/managers/devices/jobs
Kind : Series8000
```

```
PS C:\Scripts\StorSimpleSDKTools>
-----
```

Next steps

[Use StorSimple Device Manager service to manage your StorSimple device.](#)

Use Azure Automation runbooks to manage StorSimple devices

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article describes how Azure Automation runbooks are used to manage your StorSimple 8000 series device in Azure portal. A sample runbook is included to walk you through the steps of configuring your environment to execute this runbook.

Configure, add, and run Azure runbook

This section takes an example Windows PowerShell script for StorSimple and details the various steps required to import the script into a runbook and then publish and execute the runbook.

Prerequisites

Before you begin, ensure that you have:

- an active Azure subscription associated with your StorSimple Device Manager service registered with a StorSimple 8000 series device.
- Windows PowerShell 5.0 installed on your computer (Or, your Windows Server host for your StorSimple if using one).

Create automation runbook module in Windows PowerShell

To create an automation module for the StorSimple 8000 series device management, perform the following steps:

1. Launch Windows PowerShell. Create a new folder and change directory to the new folder.

```
PowerShell

mkdir C:\scripts\StorSimpleSDKTools
cd C:\scripts\StorSimpleSDKTools
```

2. Download NuGet CLI [↗](#) under the folder created in the previous step. There are various versions of *nuget.exe*. Choose the version corresponding to your SDK. Each download link points directly to an .exe file. Be sure to right-click and save the file to your computer rather than running it from the browser.

You can also run the following command to download and store the script in the same folder that you created earlier.

```
wget https://dist.nuget.org/win-x86-commandline/latest/nuget.exe -Out C:\scripts\StorSimpleSDKTools\Nuget.exe
```

3. Download the dependent SDK.

```
C:\scripts\StorSimpleSDKTools\Nuget.exe install
Microsoft.Azure.Management.Storsimple8000series
C:\scripts\StorSimpleSDKTools\Nuget.exe install
Microsoft.IdentityModel.Clients.ActiveDirectory -Version 2.28.3
C:\scripts\StorSimpleSDKTools\Nuget.exe install
Microsoft.Rest.ClientRuntime.Azure.Authentication -Version 2.2.9-
preview
```

4. Download the script from the sample GitHub project.

```
wget
https://raw.githubusercontent.com/anoobbacker/storsimpledevicemgmttools
/master/Monitor-Backups.ps1 -Out Monitor-Backups.ps1
```

5. Create an Azure Automation Runbook Module for StorSimple 8000 Series device management. On the Windows PowerShell window, type the following commands:

```
PowerShell
```

```

# set path variables
$downloadDir = "C:\scripts\StorSimpleSDKTools"
$moduleDir =
"$downloadDir\AutomationModule\Microsoft.Azure.Management.StorSimple800
0Series"

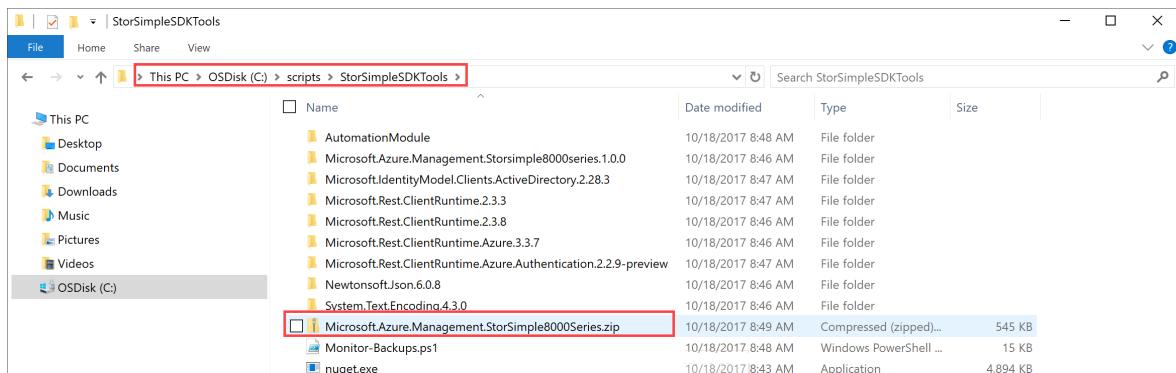
#don't change the folder name
"Microsoft.Azure.Management.StorSimple8000Series"
mkdir "$moduleDir"
Copy-Item
"$downloadDir\Microsoft.IdentityModel.Clients.ActiveDirectory.2.28.3\li
b\net45\Microsoft.IdentityModel.Clients.ActiveDirectory*.dll"
$moduleDir
Copy-Item
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.3.3.7\lib\net452\Micro
soft.Rest.ClientRuntime.Azure*.dll" $moduleDir
Copy-Item
"$downloadDir\Microsoft.Rest.ClientRuntime.2.3.8\lib\net452\Microsoft.R
est.ClientRuntime*.dll" $moduleDir
Copy-Item
"$downloadDir\Newtonsoft.Json.6.0.8\lib\net45\Newtonsoft.Json*.dll"
$moduleDir
Copy-Item
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.Authentication.2.2.9-
preview\lib\net45\Microsoft.Rest.ClientRuntime.Azure.Authentication*.dl
l" $moduleDir
Copy-Item
"$downloadDir\Microsoft.Azure.Management.Storsimple800series.1.0.0\lib
\net452\Microsoft.Azure.Management.Storsimple800series*.dll"
$moduleDir

#Don't change the name of the Archive
compress-Archive -Path "$moduleDir" -DestinationPath
Microsoft.Azure.Management.StorSimple8000Series.zip

```

6. Verify that an automation module zip file is created in

C:\scripts\StorSimpleSDKTools.



7. The following output is presented when the automation module is created via the Windows PowerShell.

PowerShell

```
mkdir C:\scripts\StorSimpleSDKTools
```

Output

```
Directory: C:\scripts
```

Mode	LastWriteTime	Length	Name
-----	-----	-----	-----
d----	10/18/2017 8:43 AM		StorSimpleSDKTools

PowerShell

```
wget https://dist.nuget.org/win-x86-commandline/latest/nuget.exe -Out C:\scripts\StorSimpleSDKTools\NuGet.exe
```

PowerShell

```
C:\scripts\StorSimpleSDKTools\NuGet.exe install Microsoft.Azure.Management.Storsimple8000series
```

Output

```
-----  
CUT          CUT  
-----  
Successfully installed 'Microsoft.Azure.Management.Storsimple8000series  
1.0.0' to C:\scripts\StorSimpleSDKTools  
Executing nuget actions took 1.77 sec
```

PowerShell

```
C:\scripts\StorSimpleSDKTools\NuGet.exe install Microsoft.IdentityModel.Clients.ActiveDirectory -Version 2.28.3
```

Output

```
-----  
CUT          CUT  
-----  
Successfully installed 'Microsoft.IdentityModel.Clients.ActiveDirectory  
2.28.3' to C:\scripts\StorSimpleSDKTools  
Executing nuget actions took 927.64 ms
```

PowerShell

```
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.Rest.ClientRuntime.Azure.Authentication -Version 2.2.9-  
preview
```

Output

```
-----  
CUT          CUT  
-----  
Successfully installed  
'Microsoft.Rest.ClientRuntime.Azure.Authentication 2.2.9-preview' to  
C:\scripts\StorSimpleSDKTools  
Executing nuget actions took 717.48 ms
```

PowerShell

```
wget  
https://raw.githubusercontent.com/anoobbacker/storsimpledevicemgmttools  
/master/Monitor-Backups.ps1 -Out Monitor-Backups.ps1  
# set path variables  
$downloadDir = "C:\scripts\StorSimpleSDKTools"  
$moduleDir =  
"$downloadDir\AutomationModule\Microsoft.Azure.Management.StorSimple800  
0Series"  
#don't change the folder name  
"Microsoft.Azure.Management.StorSimple8000Series"  
mkdir "$moduleDir"
```

Output

```
Directory: C:\scripts\StorSimpleSDKTools\AutomationModule  
  
Mode           LastWriteTime         Length Name  
----           -----          ----- ----  
d----       10/18/2017   8:48 AM          0 Microsoft.Azure.Management.StorSimple8000Series
```

PowerShell

```
Copy-Item  
"$downloadDir\Microsoft.IdentityModel.Clients.ActiveDirectory.2.28.3\li  
b\net45\Microsoft.IdentityModel.Clients.ActiveDirectory*.dll"  
$moduleDir  
Copy-Item  
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.3.3.7\lib\net452\Micro  
soft.Rest.ClientRuntime.Azure*.dll" $moduleDir  
Copy-Item
```

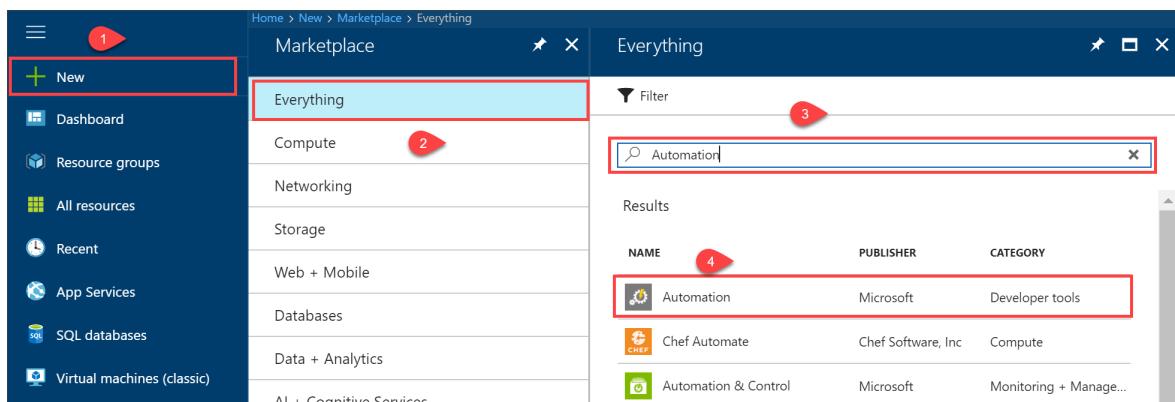
```

"$downloadDir\Microsoft.Rest.ClientRuntime.2.3.8\lib\net452\Microsoft.R
est.ClientRuntime*.dll" $moduleDir
Copy-Item
"$downloadDir\Newtonsoft.Json.6.0.8\lib\net45\Newtonsoft.Json*.dll"
$moduleDir
Copy-Item
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.Authentication.2.2.9-
preview\lib\net45\Microsoft.Rest.ClientRuntime.Azure.Authentication*.dl
l" $moduleDir
Copy-Item
"$downloadDir\Microsoft.Azure.Management.Storsimple8000series.1.0.0\lib
\net452\Microsoft.Azure.Management.Storsimple8000series*.dll"
$moduleDir
#Don't change the name of the Archive
compress-Archive -Path "$moduleDir" -DestinationPath
Microsoft.Azure.Management.StorSimple8000Series.zip

```

Import, publish, and run Automation runbook

1. Create an Azure Run As automation account in the Azure portal. To do so, go to **Azure marketplace > Everything** and then search for **Automation**. Select **Automation accounts**.



2. In the **Add Automation Account** blade:
 - Supply the **Name** of your Automation account.
 - Select the **Subscription** linked to your StorSimple Device Manager service.
 - Create a new resource group or select from an existing resource group.
 - Select a **Location** (if possible the same as where your service is running).
 - Leave the default **Create Run As account** option selected.
 - Optionally check **Pin to dashboard**. Click **Create**.



* Name i

MySSAzAuto



* Subscription

Internal Consumption



* Resource group

Create new Use existing

myssazauto



* Location

South Central US



* Create Azure Run As account i

Yes

No

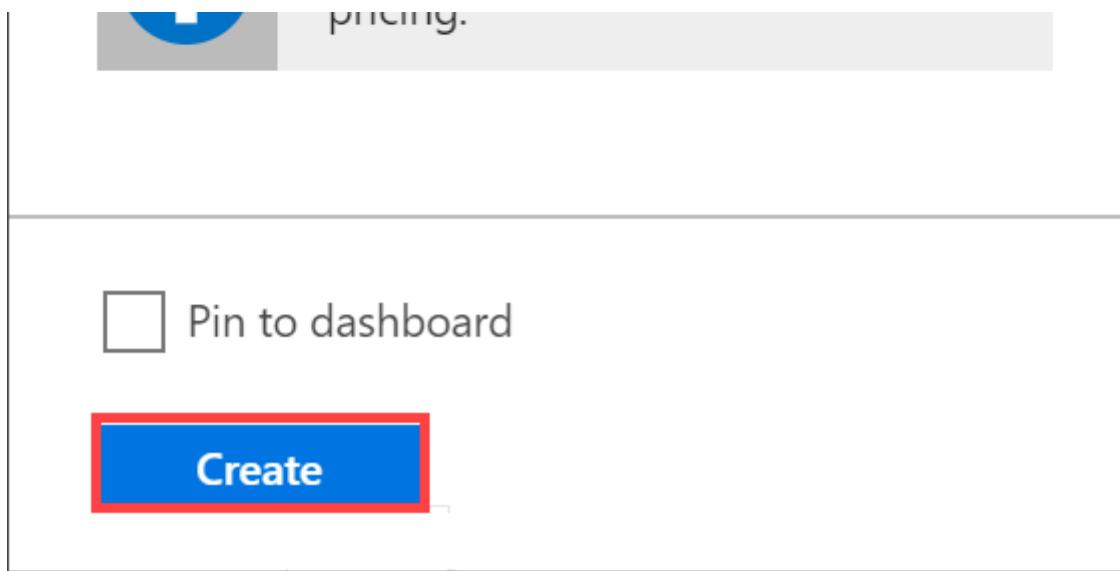


The Run As account feature will
create a Run As account and a
Classic Run As account. [Click here to
learn more about Run As accounts.](#)



Learn more about Automation
pricing





After the automation account is successfully created, you are notified. For more information on how to create an Automation account, go to [Create a Run As account](#).

3. To ensure that the automation account created can access the StorSimple Device Manager service, you need to assign appropriate permissions to the automation account. Go to **Access control** in your StorSimple Device Manager service. Click **+ Add** and provide the name of your Azure Automation Account. **Save** the settings.

A screenshot of the Azure portal showing the 'Access control (IAM)' blade for the resource group 'Contoso'. On the left, there's a sidebar with 'All resources' and a list of resources including 'Contoso', 'Contoso-ResVault', 'ContosoAdsKeyVault1', 'ContosoAG01', 'contosoaasstor simple...', 'contoso-ccnv-01', 'contosocprem01', and 'ContosoDeviceMgr'. The 'ContosoDeviceMgr' item is highlighted with a red box. The main pane shows the 'Access control (IAM)' blade with tabs for 'Overview', 'Activity log', and 'Access control (IAM)', with the last one highlighted with a red box. There are search and filter controls at the top, and a table below showing 123 items (100 Users, 23 Service Principals). One row in the table is highlighted with a red box, showing a contributor named 'AK' with a user icon, 'User' role, and 'Subscription (Inherited)' scope.

4. In the newly created account, go to **Shared Resources > Modules** and click **+ Add module**.
5. In the **Add module** blade, browse to the location of the zipped module, and select and open the module. Click **OK**.



Add Module



Importing a module may take several minutes.

* Upload File (.zip format, 100 MB max size)

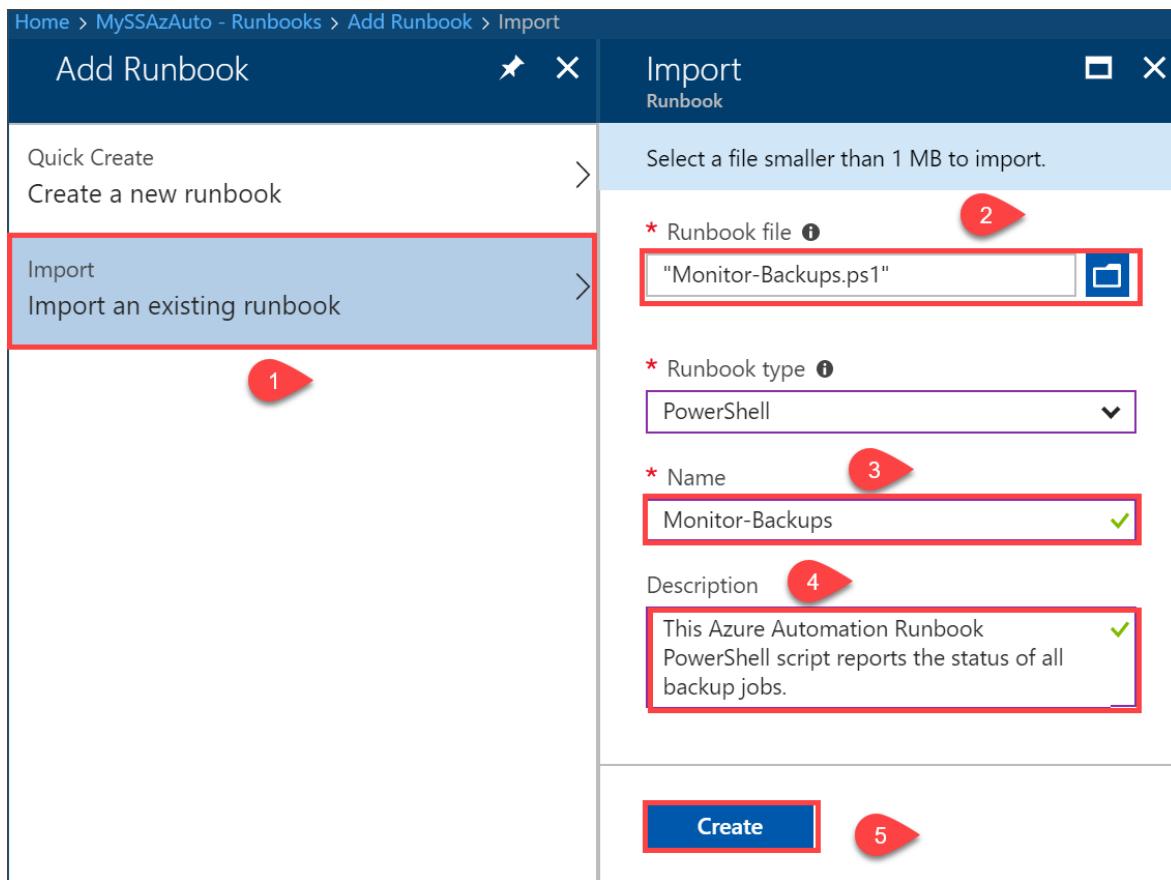
"Microsoft.Azure.Management.StorSim..."

1

2

OK

6. Go to Process Automation > Runbooks and click + Add a runbook. In the Add runbook blade, click Import an existing runbook. Point to the Windows PowerShell script file for the Runbook file. The runbook type is automatically selected. Provide a name and an optional description for the runbook. Click Create.



7. The runbook is added to the list of runbooks. Select and click this runbook.

NAME	AUTHORING STATUS	LAST MODIFIED
AzureAutomationTutorial	✓ Published	10/18/2017, 8:07 AM
AzureAutomationTutorialPython2	✓ Published	10/18/2017, 8:06 AM
AzureAutomationTutorialScript	✓ Published	10/18/2017, 8:06 AM
AzureClassicAutomationTutorial	✓ Published	10/18/2017, 8:06 AM
AzureClassicAutomationTutorialScript	✓ Published	10/18/2017, 8:07 AM
Monitor-Backups	💡 New	10/18/2017, 9:03 AM

8. Edit the runbook and click **Test pane**. Provide the parameters such as name of your StorSimple Device Manager service, name of the StorSimple device and the subscription. **Start** the test. The report is generated when the run is complete. For more information, go to [how to test a runbook](#).

The screenshot shows the Azure Automation Test pane for a PowerShell runbook named 'Test'. On the left, there are sections for 'Parameters' (containing 'RESOURCEGROUPNAME', 'MANAGERNAME', 'DEVICENAME', and 'NUMBEROFDAYSFORREPORT') and 'Run Settings' (set to 'Run on Azure'). A note about using a hybrid runbook worker is present. On the right, a table titled 'Completed' lists backup jobs with columns for 'BackupPolicyName', 'Volumes', 'JobType', 'BackupType', 'Status', 'StartTime', 'EndTime', 'Duration', and 'ErrorMessage'. All jobs show a status of 'Succeeded'.

9. Inspect the output from the runbook in the test pane. If satisfied, close the pane. Click **Publish** and when prompted for confirmation, confirm, and publish the runbook.

The screenshot shows the 'Edit PowerShell Runbook' page with the 'Monitor-Backups' tab selected. The 'Publish' button is highlighted with a red box. Below it, a confirmation dialog box is open, asking 'Publish Runbook' and stating 'This will publish this version of the runbook and override the previously published version. Do you want to proceed?'. Two buttons are visible: 'Yes' (highlighted with a red box) and 'No'.

Next steps

Use StorSimple Device Manager service to manage your StorSimple device.

Additional resources

Training

Module

[Explore Azure Automation with DevOps - Training](#)

Explore Azure Automation with DevOps

StorSimple as a backup target with Veeam

Article • 08/22/2022 • 20 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Azure StorSimple is a hybrid cloud storage solution from Microsoft. StorSimple addresses the complexities of exponential data growth by using an Azure Storage account as an extension of the on-premises solution and automatically tiering data across on-premises storage and cloud storage.

In this article, we discuss StorSimple integration with Veeam, and best practices for integrating both solutions. We also make recommendations on how to set up Veeam to best integrate with StorSimple. We defer to Veeam best practices, backup architects, and administrators for the best way to set up Veeam to meet individual backup requirements and service-level agreements (SLAs).

Although we illustrate configuration steps and key concepts, this article is by no means a step-by-step configuration or installation guide. We assume that the basic components and infrastructure are in working order and ready to support the concepts that we describe.

Who should read this?

The information in this article will be most helpful to backup administrators, storage administrators, and storage architects who have knowledge of storage, Windows Server 2012 R2, Ethernet, cloud services, and Veeam.

Supported versions

- Veeam 9 and later versions
- StorSimple Update 3 and later versions

Why StorSimple as a backup target?

StorSimple is a good choice for a backup target because:

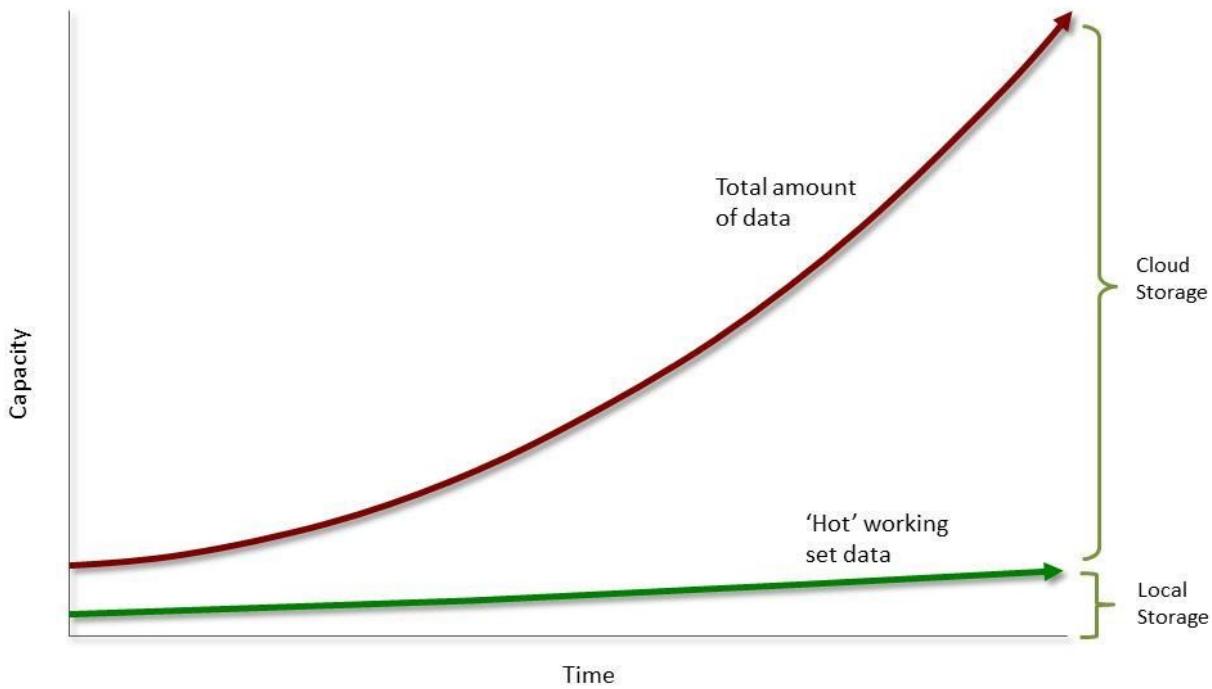
- It provides standard, local storage for backup applications to use as a fast backup destination, without any changes. You also can use StorSimple for a quick restore of recent backups.
- Its cloud tiering is seamlessly integrated with an Azure cloud storage account to use cost-effective Azure Storage.
- It automatically provides offsite storage for disaster recovery.

Key concepts

As with any storage solution, a careful assessment of the solution's storage performance, SLAs, rate of change, and capacity growth needs is critical to success. The main idea is that by introducing a cloud tier, your access times and throughputs to the cloud play a fundamental role in the ability of StorSimple to do its job.

StorSimple is designed to provide storage to applications that operate on a well-defined working set of data (hot data). In this model, the working set of data is stored on the local tiers, and the remaining nonworking/cold/archived set of data is tiered to the cloud. This model is represented in the following figure. The nearly flat green line represents the data stored on the local tiers of the StorSimple device. The red line represents the total amount of data stored on the StorSimple solution across all tiers. The space between the flat green line and the exponential red curve represents the total amount of data stored in the cloud.

StorSimple tiering



With this architecture in mind, you will find that StorSimple is ideally suited to operate as a backup target. You can use StorSimple to:

- Perform your most frequent restores from the local working set of data.
- Use the cloud for offsite disaster recovery and older data, where restores are less frequent.

StorSimple benefits

StorSimple provides an on-premises solution that is seamlessly integrated with Microsoft Azure, by taking advantage of seamless access to on-premises and cloud storage.

StorSimple uses automatic tiering between the on-premises device, which has solid-state device (SSD) and serial-attached SCSI (SAS) storage, and Azure Storage. Automatic tiering keeps frequently accessed data local, on the SSD and SAS tiers. It moves infrequently accessed data to Azure Storage.

StorSimple offers these benefits:

- Unique deduplication and compression algorithms that use the cloud to achieve unprecedented deduplication levels
- High availability
- Geo-replication by using Azure geo-replication
- Azure integration
- Data encryption in the cloud

- Improved disaster recovery and compliance

Although StorSimple presents two main deployment scenarios (primary backup target and secondary backup target), fundamentally, it's a plain, block storage device. StorSimple does all the compression and deduplication. It seamlessly sends and retrieves data between the cloud and the application and file system.

For more information about StorSimple, see [StorSimple 8000 series: Hybrid cloud storage solution](#). Also, you can review the [technical StorSimple 8000 series specifications](#).

Important

Using a StorSimple device as a backup target is supported only for StorSimple 8000 Update 3 and later versions.

Architecture overview

The following tables show the device model-to-architecture initial guidance.

StorSimple capacities for local and cloud storage

Storage capacity	8100	8600
Local storage capacity	< 10 TiB*	< 20 TiB*
Cloud storage capacity	> 200 TiB*	> 500 TiB*

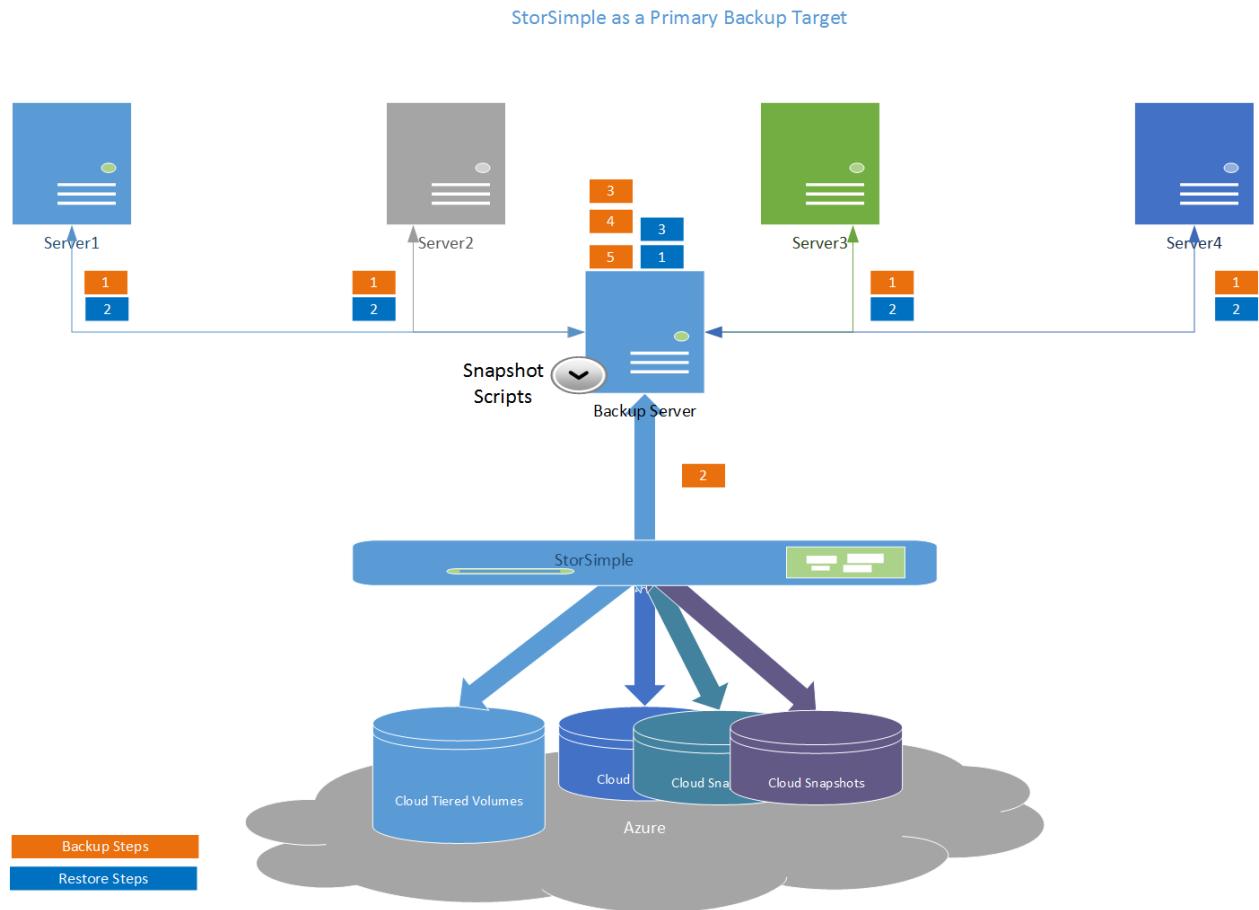
* Storage size assumes no deduplication or compression.

StorSimple capacities for primary and secondary backups

Backup scenario	Local storage capacity	Cloud storage capacity
Primary backup	Recent backups stored on local storage for fast recovery to meet recovery point objective (RPO)	Backup history (RPO) fits in cloud capacity
Secondary backup	Secondary copy of backup data can be stored in cloud capacity	N/A

StorSimple as a primary backup target

In this scenario, StorSimple volumes are presented to the backup application as the sole repository for backups. The following figure shows a solution architecture in which all backups use StorSimple tiered volumes for backups and restores.



Primary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to the StorSimple tiered volumes.
3. The backup server updates the catalog database, and then finishes the backup job.
4. A snapshot script triggers the StorSimple cloud snapshot manager (start or delete).
5. The backup server deletes expired backups based on a retention policy.

Primary target restore logical steps

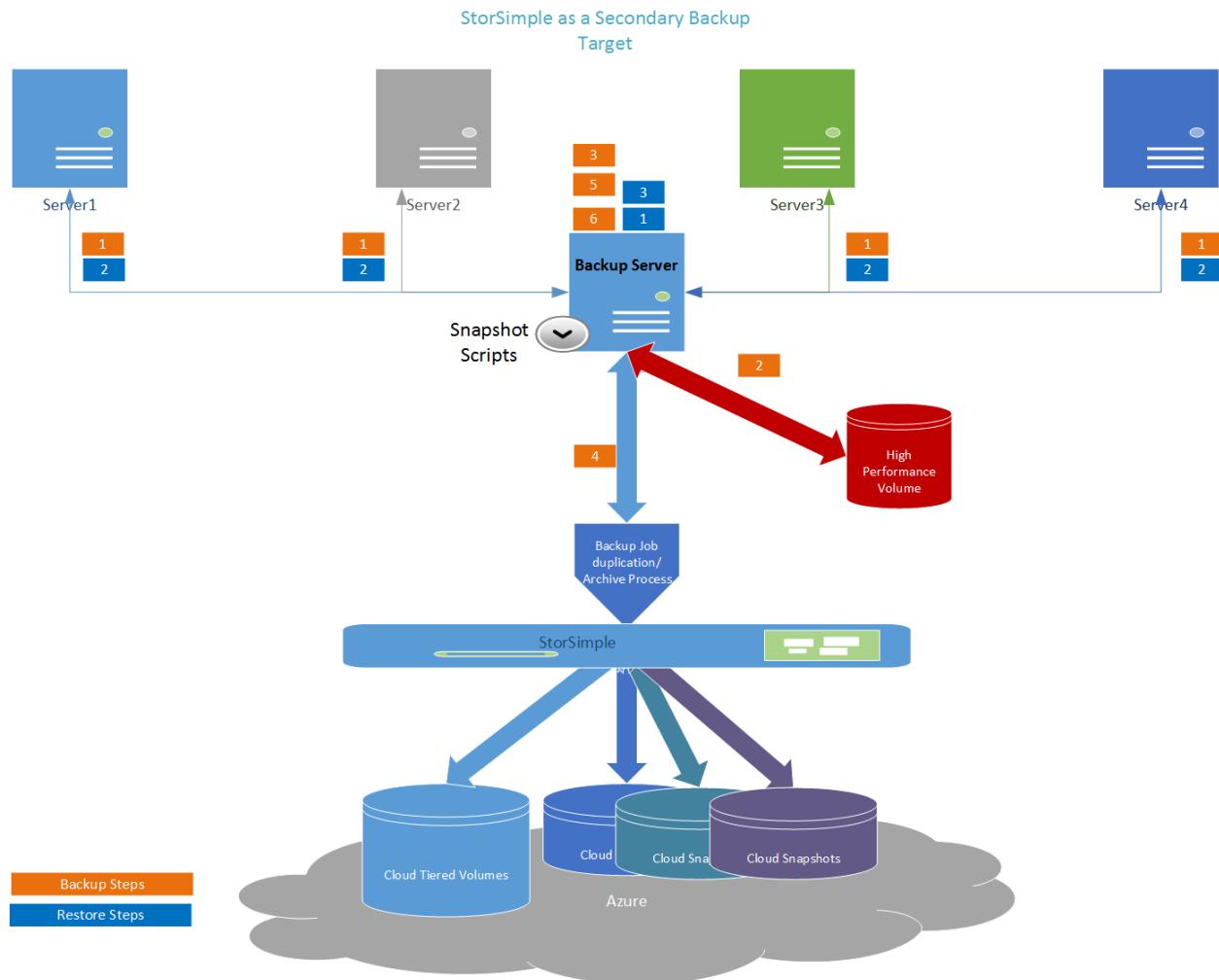
1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

StorSimple as a secondary backup target

In this scenario, StorSimple volumes primarily are used for long-term retention or archiving.

The following figure shows an architecture in which initial backups and restores target a high-performance volume. These backups are copied and archived to a StorSimple tiered volume on a set schedule.

It is important to size your high-performance volume so that it can handle your retention policy capacity and performance requirements.



Secondary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to high-performance storage.
3. The backup server updates the catalog database, and then finishes the backup job.
4. The backup server copies backups to StorSimple based on a retention policy.
5. A snapshot script triggers the StorSimple cloud snapshot manager (start or delete).
6. The backup server deletes expired backups based on a retention policy.

Secondary target restore logical steps

1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

Deploy the solution

Deploying the solution requires three steps:

1. Prepare the network infrastructure.
2. Deploy your StorSimple device as a backup target.
3. Deploy Veeam.

Each step is discussed in detail in the following sections.

Set up the network

Because StorSimple is a solution that is integrated with the Azure cloud, StorSimple requires an active and working connection to the Azure cloud. This connection is used for operations like cloud snapshots, data management, and metadata transfer, and to tier older, less accessed data to Azure cloud storage.

For the solution to perform optimally, we recommend that you follow these networking best practices:

- The link that connects your StorSimple tiering to Azure must meet your bandwidth requirements. Achieve this by applying the necessary Quality of Service (QoS) level to your infrastructure switches to match your RPO and recovery time objective (RTO) SLAs.
- Maximum Azure Blob storage access latencies should be around 80 ms.

Deploy StorSimple

For step-by-step StorSimple deployment guidance, see [Deploy your on-premises StorSimple device](#).

Deploy Veeam

For Veeam installation best practices, see [Veeam Backup & Replication Best Practices](#), and read the user guide at [Veeam Help Center \(Technical Documentation\)](#).

Set up the solution

In this section, we demonstrate some configuration examples. The following examples and recommendations illustrate the most basic and fundamental implementation. This implementation might not apply directly to your specific backup requirements.

Set up StorSimple

StorSimple deployment tasks	Additional comments
Deploy your on-premises StorSimple device.	Supported versions: Update 3 and later versions.
Turn on the backup target.	<p>Use these commands to turn on or turn off backup target mode, and to get status. For more information, see Connect remotely to a StorSimple device.</p> <p>To turn on backup mode: <code>Set-HCSBackupApplianceMode -enable</code>.</p> <p>To turn off backup mode: <code>Set-HCSBackupApplianceMode -disable</code>.</p> <p>To get the current state of backup mode settings: <code>Get-HCSBackupApplianceMode</code>.</p>
Create a common volume container for your volume that stores the backup data. All data in a volume container is deduplicated.	StorSimple volume containers define deduplication domains.
Create StorSimple volumes.	<p>Create volumes with sizes as close to the anticipated usage as possible, because volume size affects cloud snapshot duration time. For information about how to size a volume, read about retention policies.</p> <p>Use StorSimple tiered volumes, and select the Use this volume for less frequently accessed archival data check box.</p> <p>Using only locally pinned volumes is not supported.</p>
Create a unique StorSimple backup policy for all the backup target volumes.	A StorSimple backup policy defines the volume consistency group.
Disable the schedule as the snapshots expire.	Snapshots are triggered as a post-processing operation.

Set up the host backup server storage

Set up the host backup server storage according to these guidelines:

- Don't use spanned volumes (created by Windows Disk Management). Spanned volumes are not supported.
- Format your volumes using NTFS with 64-KB allocation unit size.
- Map the StorSimple volumes directly to the Veeam server.
 - Use iSCSI for physical servers.

Best practices for StorSimple and Veeam

Set up your solution according to the guidelines in the following few sections.

Operating system best practices

- Disable Windows Server encryption and deduplication for the NTFS file system.
- Disable Windows Server defragmentation on the StorSimple volumes.
- Disable Windows Server indexing on the StorSimple volumes.
- Run an antivirus scan at the source host (not against the StorSimple volumes).
- Turn off the default [Windows Server maintenance](#) in Task Manager. Do this in one of the following ways:
 - Turn off the Maintenance configurator in Windows Task Scheduler.
 - Download [PsExec](#) from Windows Sysinternals. After you download PsExec, run Windows PowerShell as an administrator, and type:

PowerShell

```
psexec \\%computername% -s schtasks /change /tn  
"MicrosoftWindowsTaskSchedulerMaintenance Configurator" /disable
```

StorSimple best practices

- Be sure that the StorSimple device is updated to [Update 3 or later](#).
- Isolate iSCSI and cloud traffic. Use dedicated iSCSI connections for traffic between StorSimple and the backup server.
- Be sure that your StorSimple device is a dedicated backup target. Mixed workloads are not supported because they affect your RTO and RPO.

Veeam best practices

- The Veeam database should be local to the server and not reside on a StorSimple volume.
- For disaster recovery, back up the Veeam database on a StorSimple volume.
- We support Veeam full and incremental backups for this solution. We recommend that you do not use synthetic and differential backups.
- Backup data files should contain only the data for a specific job. For example, no media appends across different jobs are allowed.
- Turn off job verification. If necessary, verification should be scheduled after the latest backup job. It is important to understand that this job affects your backup window.
- Turn on media pre-allocation.
- Be sure parallel processing is turned on.
- Turn off compression.
- Turn off deduplication on the backup job.
- Set optimization to **LAN Target**.
- Turn on **Create active full backup** (every 2 weeks).
- On the backup repository, set up **Use per-VM backup files**.
- Set **Use multiple upload streams per job** to 8 (a maximum of 16 is allowed). Adjust this number up or down based on CPU utilization on the StorSimple device.

Retention policies

One of the most common backup retention policy types is a Grandfather, Father, and Son (GFS) policy. In a GFS policy, an incremental backup is performed daily and full backups are done weekly and monthly. This policy results in six StorSimple tiered volumes: one volume contains the weekly, monthly, and yearly full backups; the other five volumes store daily incremental backups.

In the following example, we use a GFS rotation. The example assumes the following:

- Non-deduped or compressed data is used.
- Full backups are 1 TiB each.
- Daily incremental backups are 500 GiB each.
- Four weekly backups are kept for a month.
- Twelve monthly backups are kept for a year.
- One yearly backup is kept for 10 years.

Based on the preceding assumptions, create a 26-TiB StorSimple tiered volume for the monthly and yearly full backups. Create a 5-TiB StorSimple tiered volume for each of the incremental daily backups.

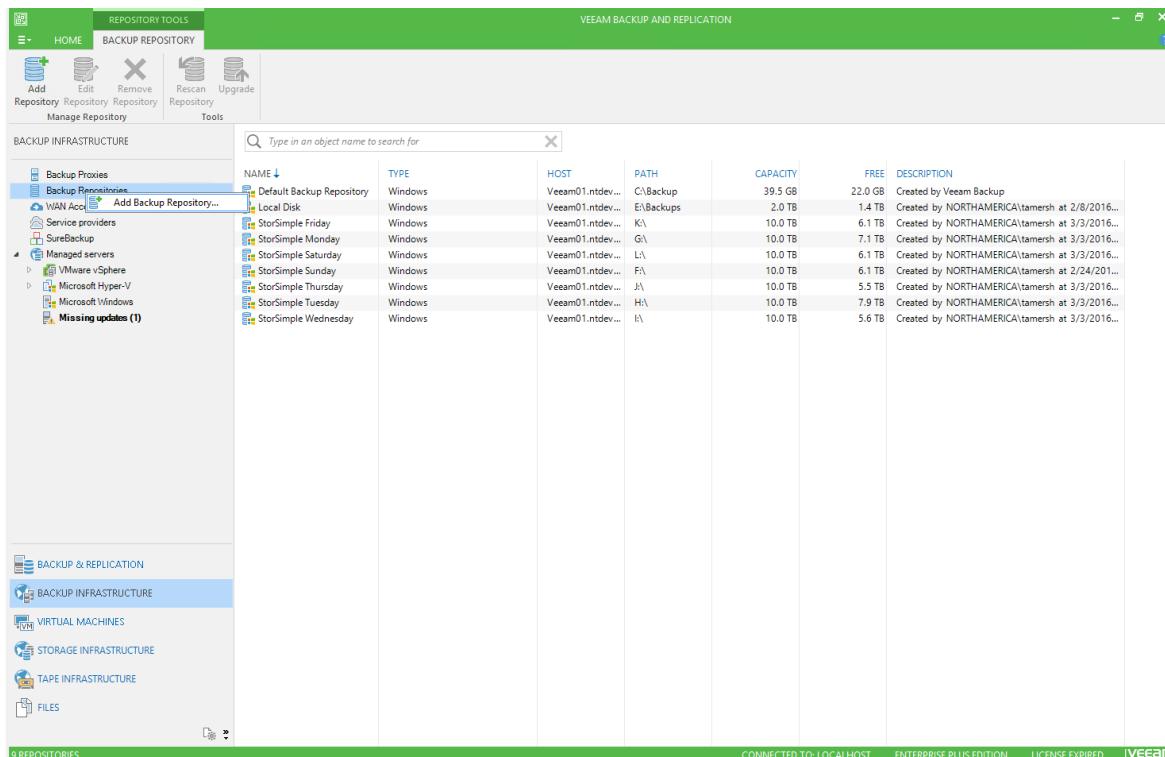
Backup type retention	Size (TiB)	GFS multiplier*	Total capacity (TiB)
Weekly full	1	4	4
Daily incremental	0.5	20 (cycles equal number of weeks per month)	12 (2 for additional quota)
Monthly full	1	12	12
Yearly full	1	10	10
GFS requirement		38	
Additional quota	4		42 total GFS requirement

* The GFS multiplier is the number of copies you need to protect and retain to meet your backup policy requirements.

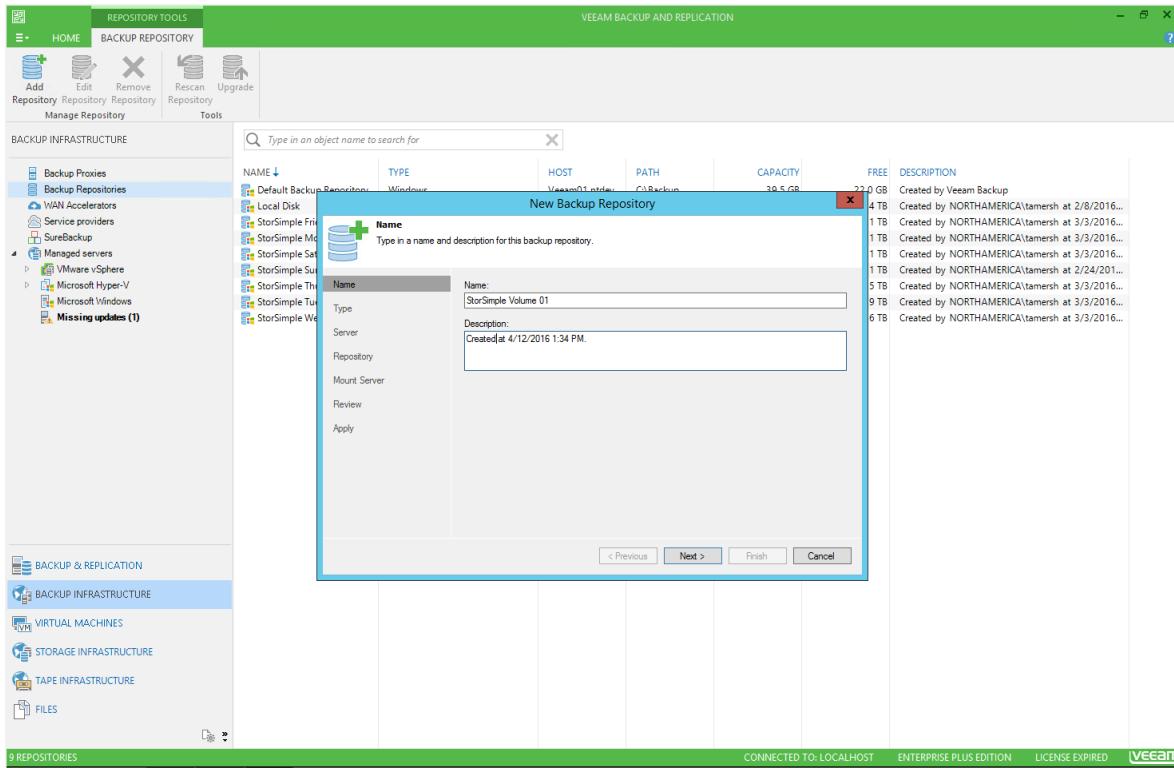
Set up Veeam storage

To set up Veeam storage

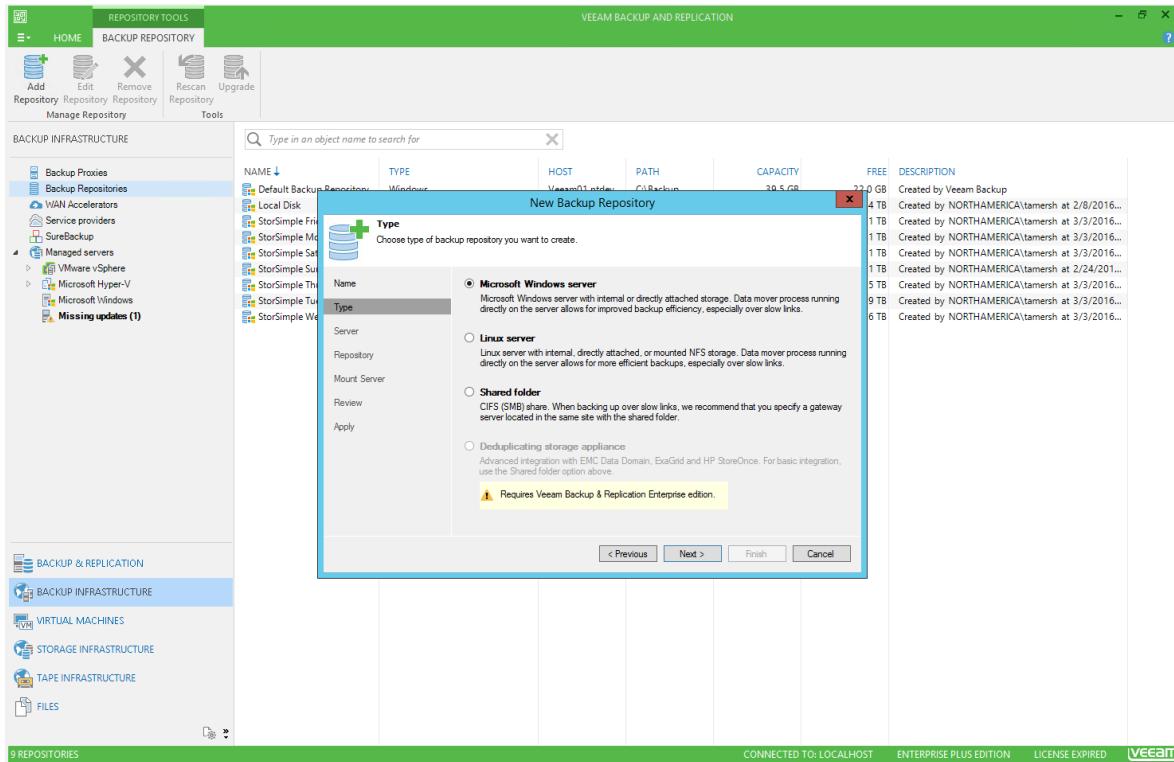
1. In the Veeam Backup and Replication console, in **Repository Tools**, go to **Backup Infrastructure**. Right-click **Backup Repositories**, and then select **Add Backup Repository**.



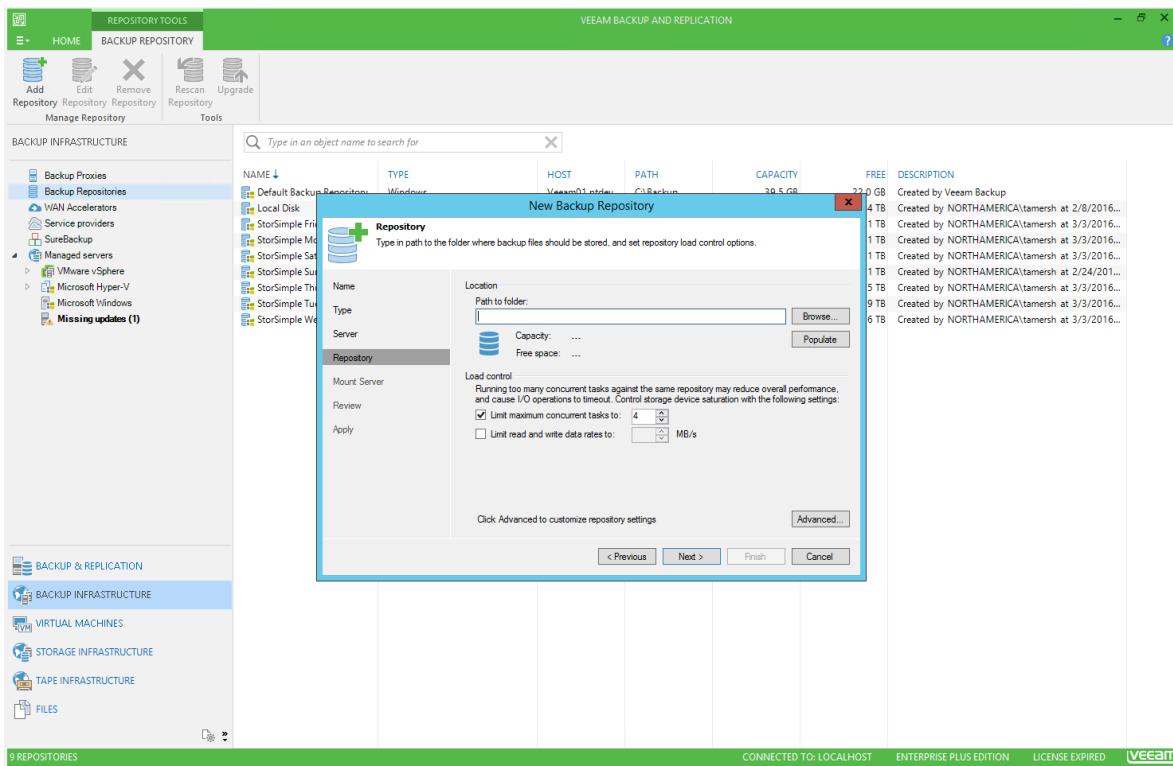
2. In the New Backup Repository dialog box, enter a name and description for the repository. Select Next.



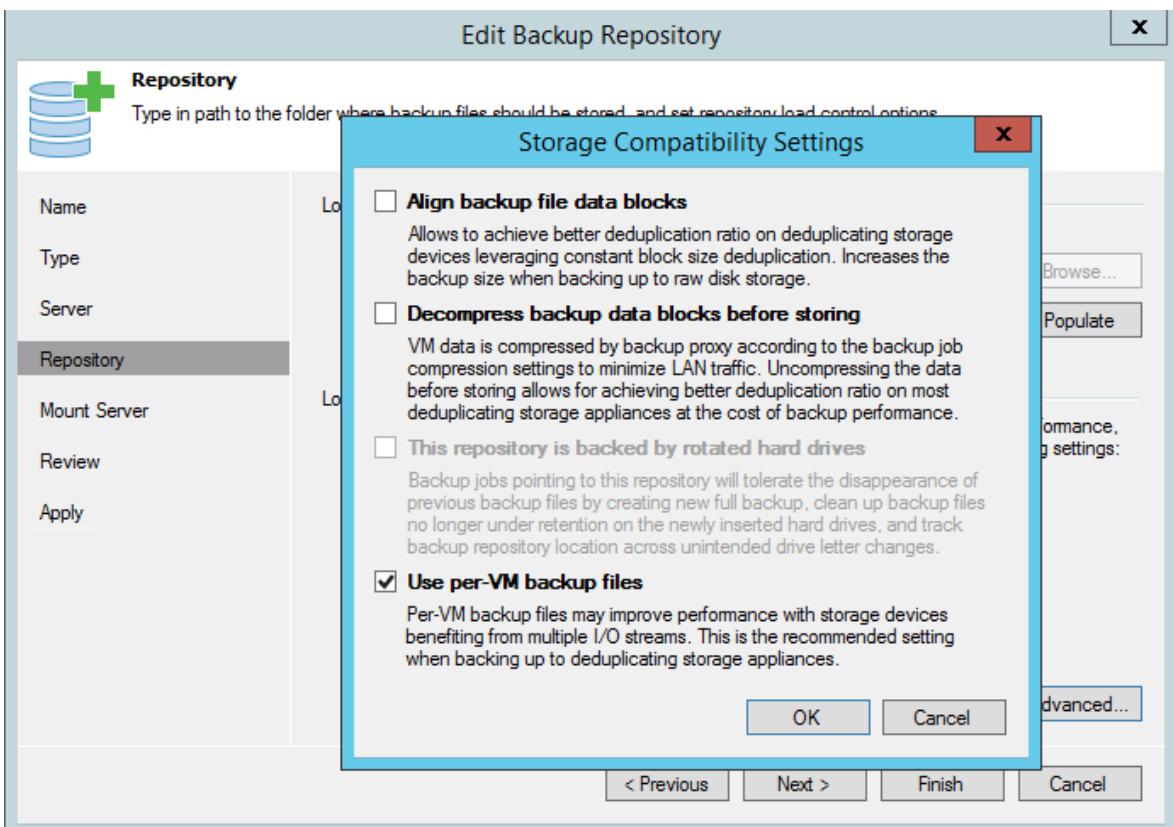
3. For the type, select Microsoft Windows server. Select the Veeam server. Select Next.



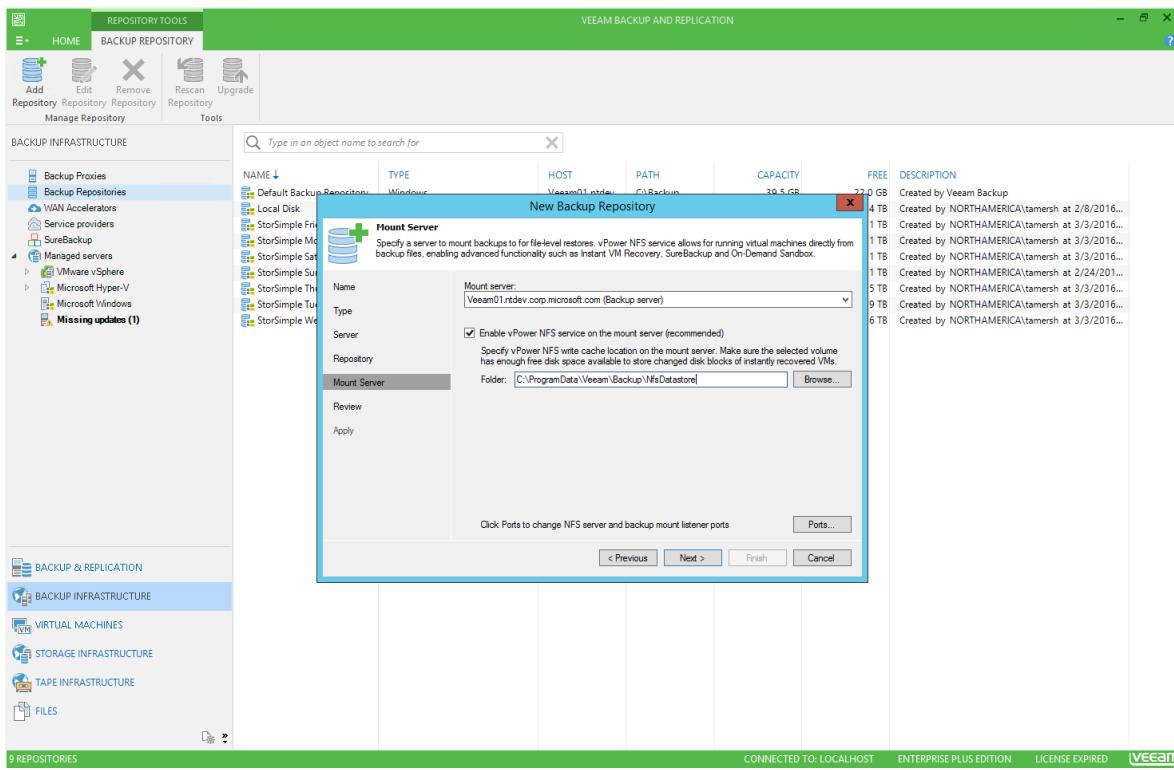
4. To specify Location, browse and select the volume. Select the Limit maximum concurrent tasks to: check box and set the value to 4. This ensures that only four virtual disks are being processed concurrently while each virtual machine (VM) is processed. Select the Advanced button.



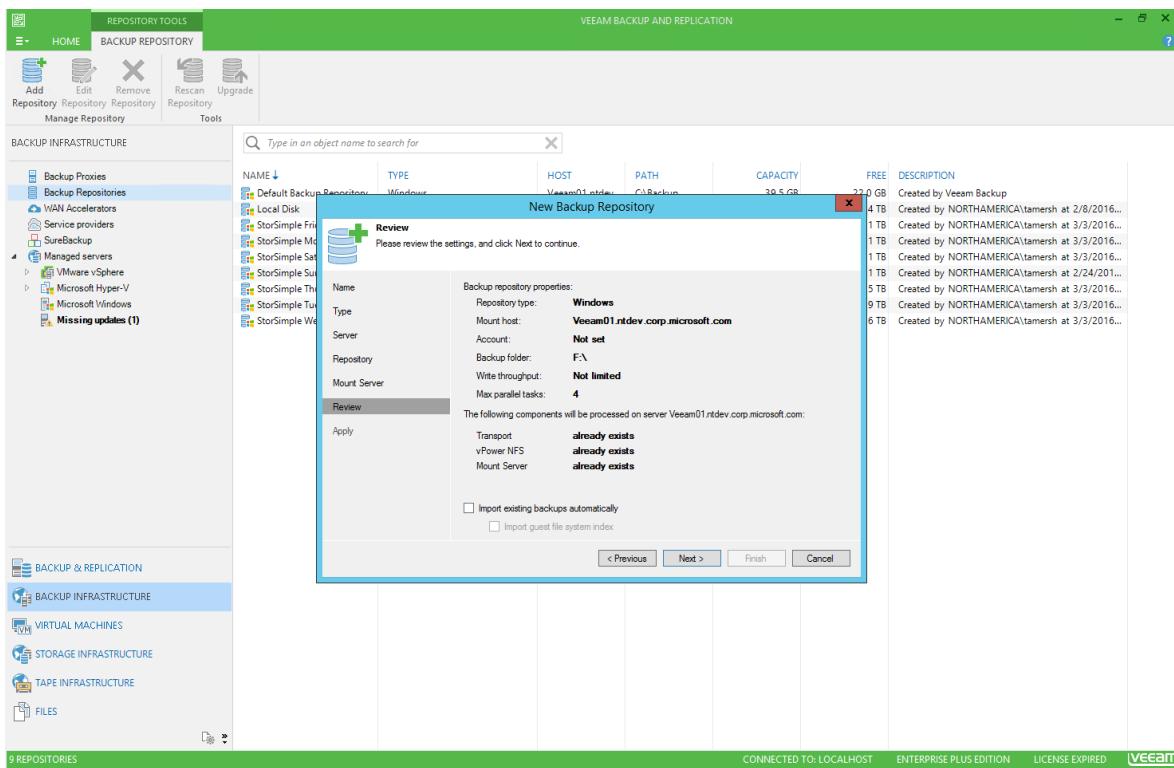
5. In the Storage Compatibility Settings dialog box, select the Use per-VM backup files check box.



6. In the New Backup Repository dialog box, select the Enable vPower NFS service on the mount server (recommended) check box. Select Next.



7. Review the settings, and then select **Next**.



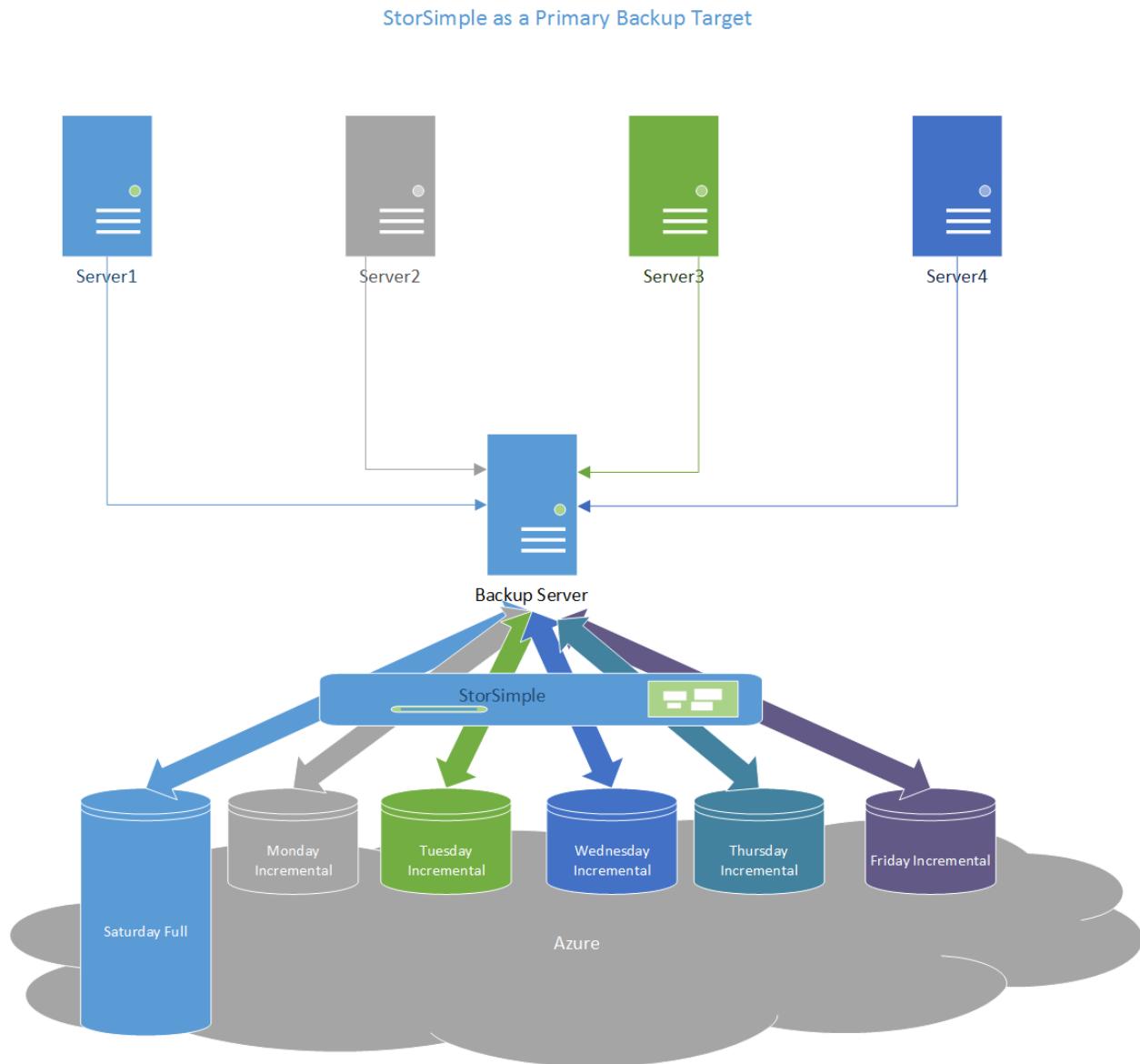
A repository is added to the Veeam server.

Set up StorSimple as a primary backup target

Important

Data restore from a backup that has been tiered to the cloud occurs at cloud speeds.

The following figure shows the mapping of a typical volume to a backup job. In this case, all the weekly backups map to the Saturday full disk, and the incremental backups map to Monday-Friday incremental disks. All the backups and restores are from a StorSimple tiered volume.



StorSimple as a primary backup target GFS schedule example

Here's an example of a GFS rotation schedule for four weeks, monthly, and yearly:

Frequency/backup type	Full	Incremental (days 1-5)
Weekly (weeks 1-4)	Saturday	Monday-Friday

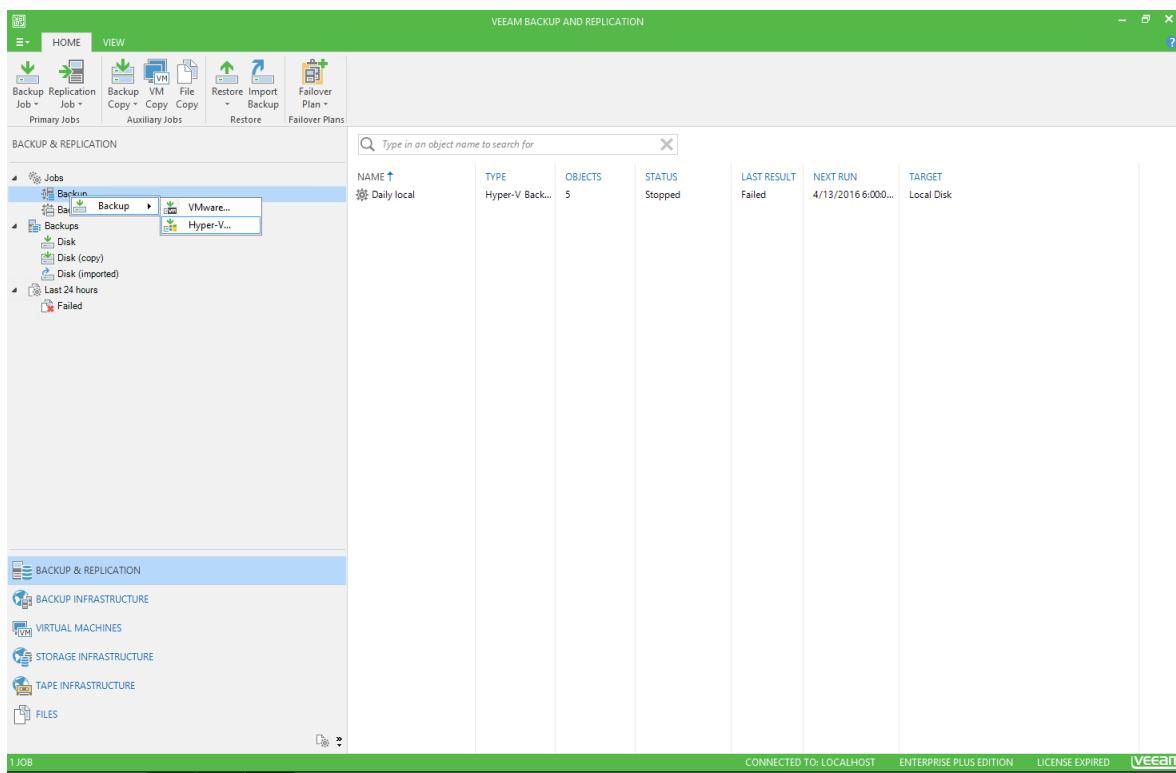
Frequency/backup type	Full	Incremental (days 1-5)
Monthly	Saturday	
Yearly	Saturday	

Assign StorSimple volumes to a Veeam backup job

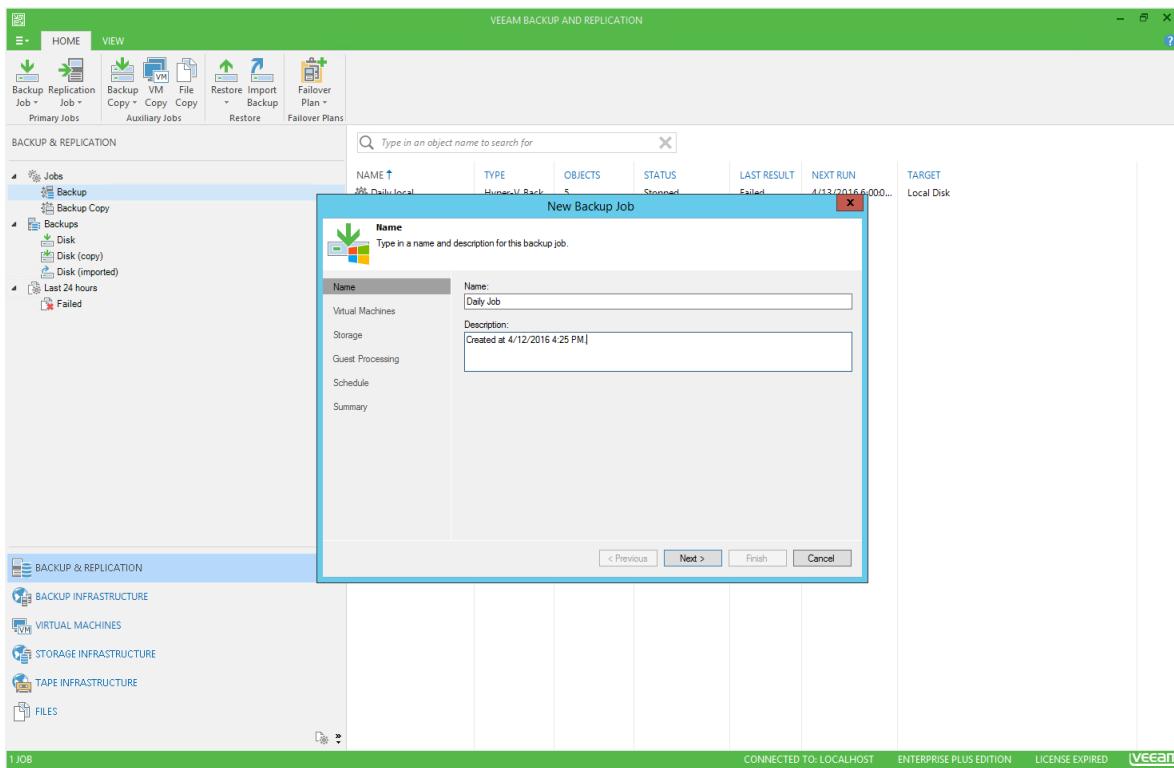
For primary backup target scenario, create a daily job with your primary Veeam StorSimple volume. For a secondary backup target scenario, create a daily job by using Direct Attached Storage (DAS), Network Attached Storage (NAS), or Just a Bunch of Disks (JBOD) storage.

To assign StorSimple volumes to a Veeam backup job

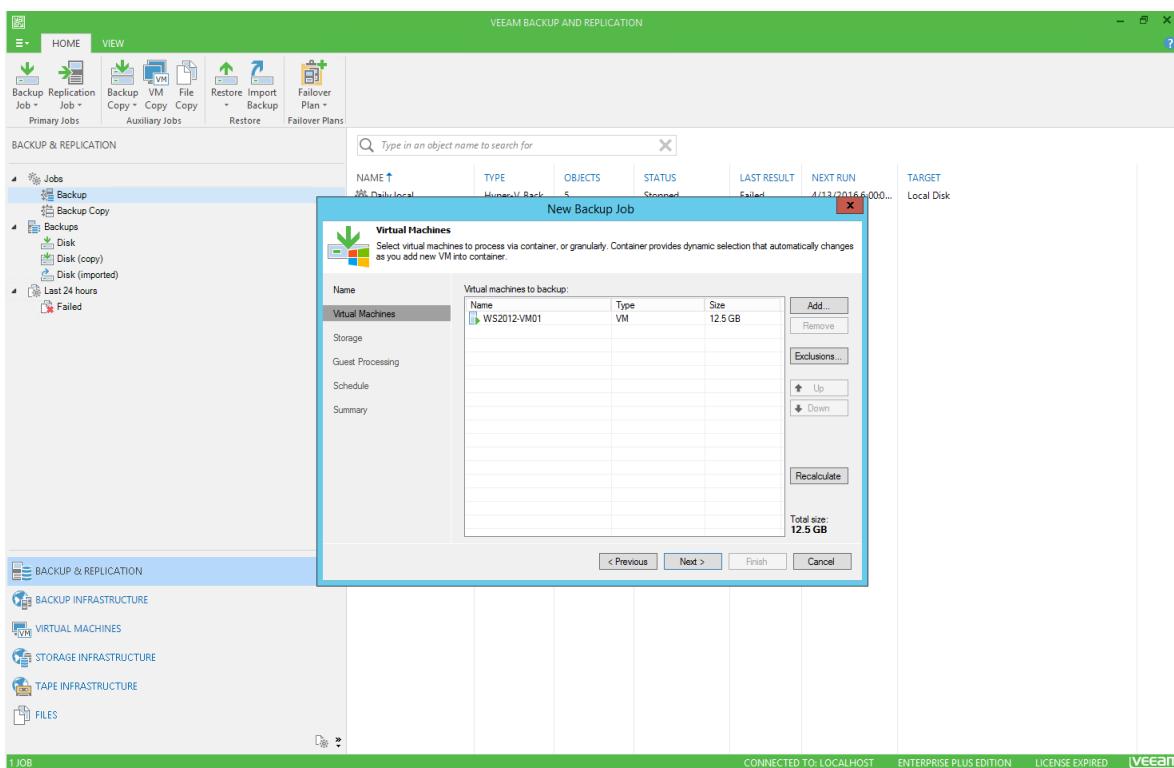
1. In the Veeam Backup and Replication console, select **Backup & Replication**. Right-click **Backup**, and then select **VMware** or **Hyper-V**, depending on your environment.



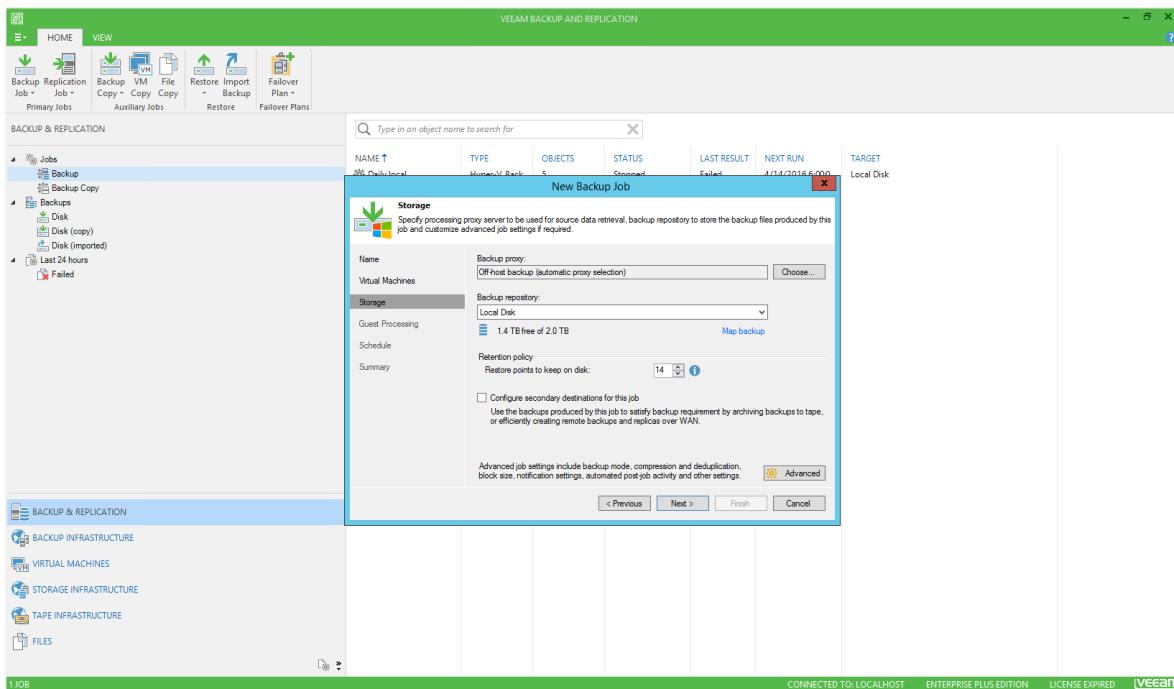
2. In the **New Backup Job** dialog box, enter a name and description for the daily backup job.



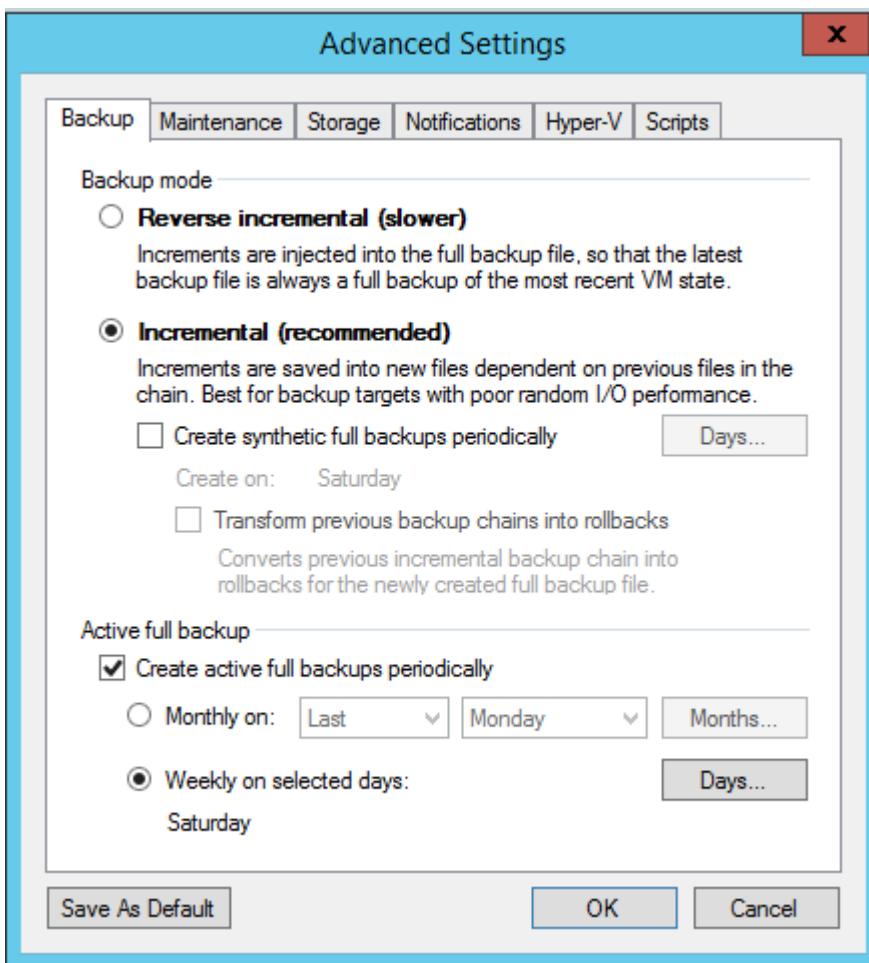
3. Select a virtual machine to back up to.



4. Select the values you want for **Backup proxy** and **Backup repository**. Select a value for **Restore points to keep on disk** according to the RPO and RTO definitions for your environment on locally attached storage. Select **Advanced**.

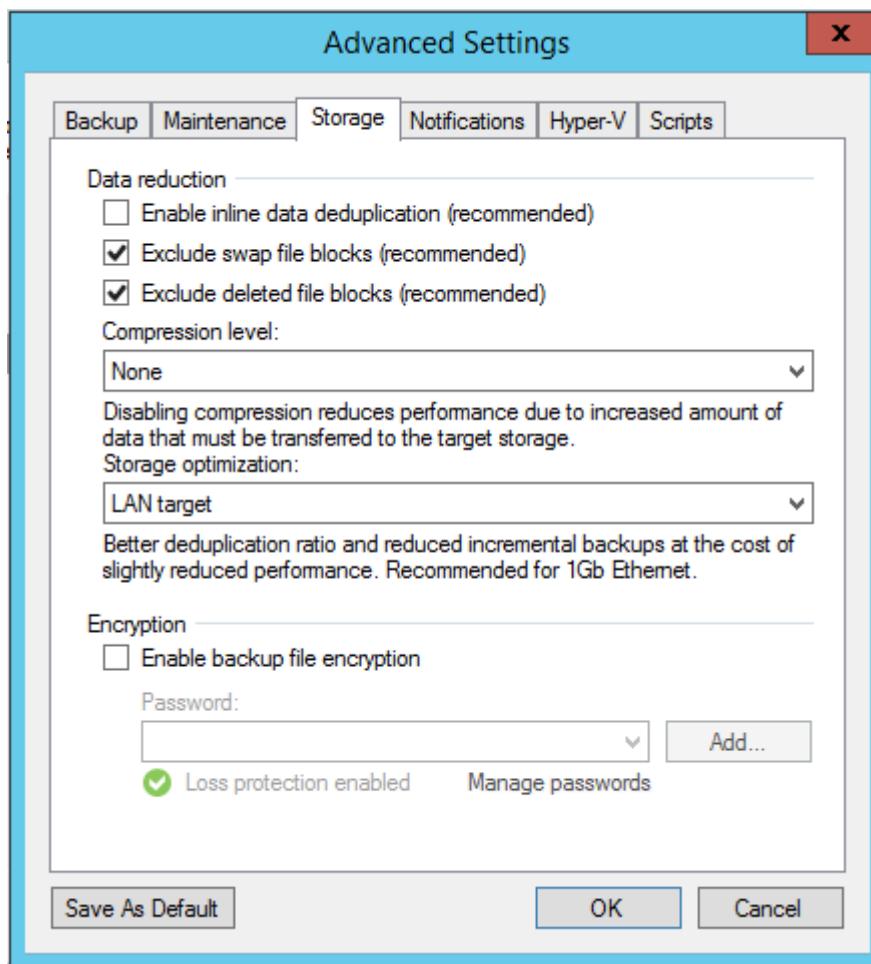


5. In the **Advanced Settings** dialog box, on the **Backup** tab, select **Incremental**. Be sure that the **Create synthetic full backups periodically** check box is cleared. Select the **Create active full backups periodically** check box. Under **Active full backup**, select the **Weekly on selected days** check box for Saturday.



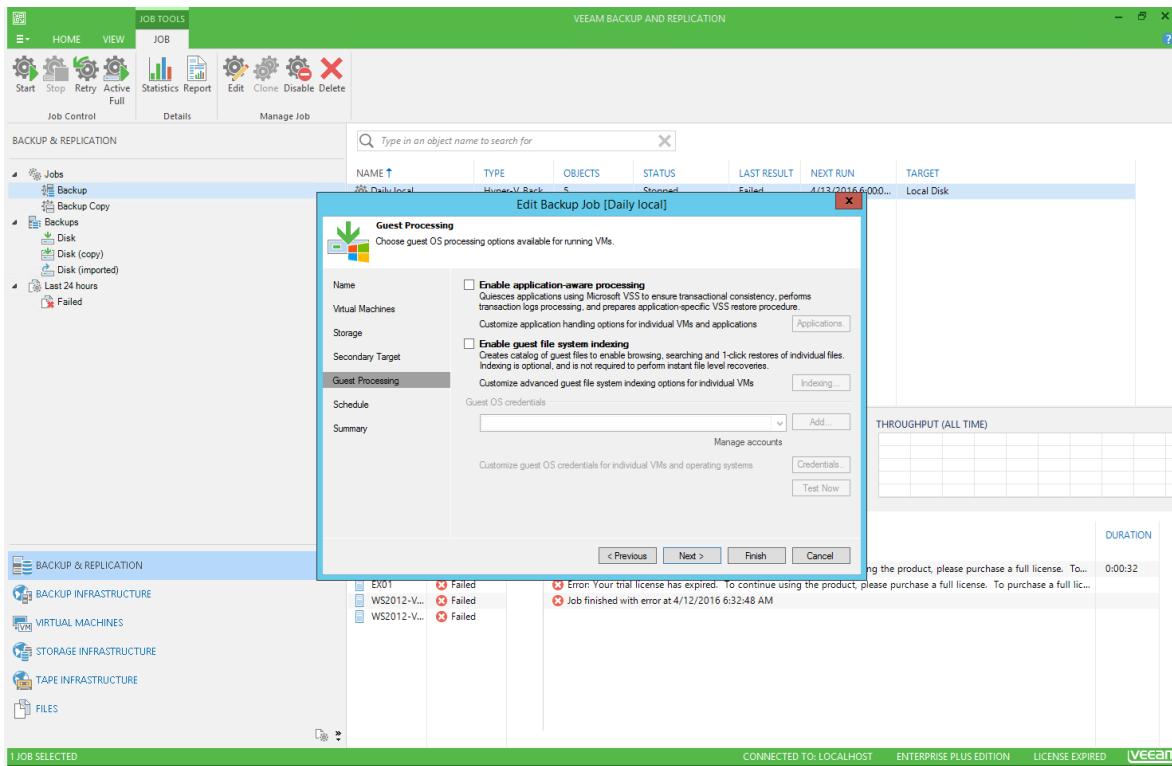
6. On the **Storage** tab, make sure that the **Enable inline data deduplication** check box is cleared. Select the **Exclude swap file blocks** check box, and select the

Exclude deleted file blocks check box. Set Compression level to None. For balanced performance and deduplication, set Storage optimization to LAN target. Select OK.

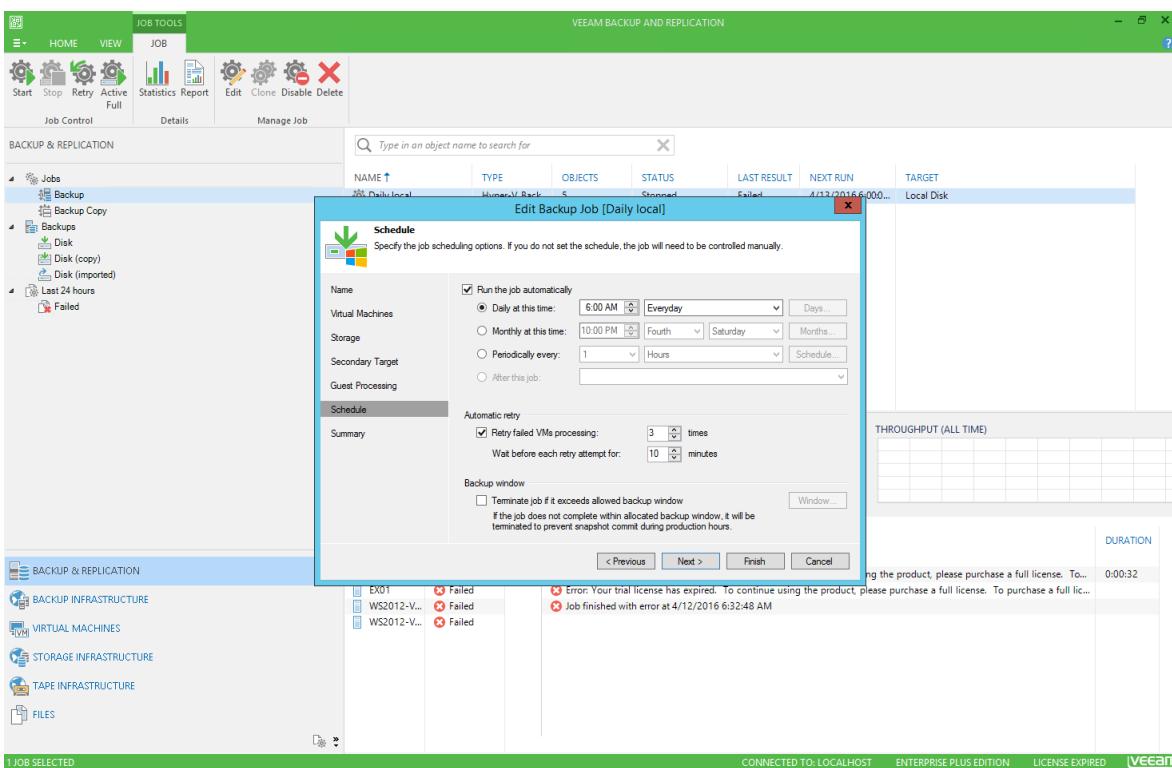


For information about Veeam deduplication and compression settings, see [Data Compression and Deduplication](#).

7. In the **Edit Backup Job** dialog box, you can select the **Enable application-aware processing** check box (optional).



8. Set the schedule to run once daily, at a time you can specify.



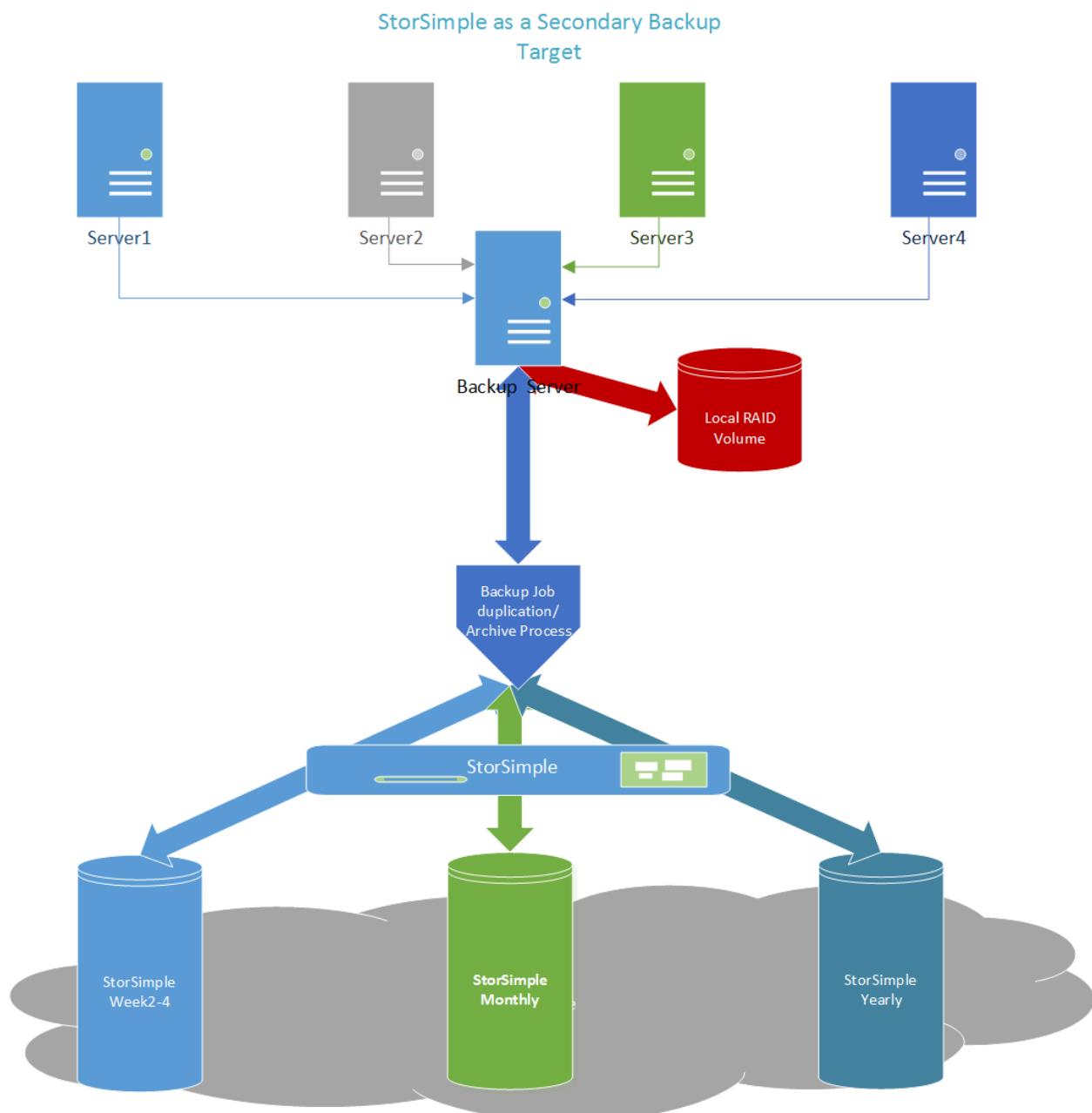
Set up StorSimple as a secondary backup target

Note

Data restores from a backup that has been tiered to the cloud occur at cloud speeds.

In this model, you must have a storage media (other than StorSimple) to serve as a temporary cache. For example, you can use a redundant array of independent disks (RAID) volume to accommodate space, input/output (I/O), and bandwidth. We recommend using RAID 5, 50, and 10.

The following figure shows typical short-term retention local (to the server) volumes and long-term retention archive volumes. In this scenario, all backups run on the local (to the server) RAID volume. These backups are periodically duplicated and archived to an archive volume. It is important to size your local (to the server) RAID volume so that it can handle your short-term retention capacity and performance requirements.



StorSimple as a secondary backup target GFS example

The following table shows how to set up backups to run on the local and StorSimple disks. It includes individual and total capacity requirements.

Backup type and retention	Configured storage	Size (TiB)	GFS multiplier	Total capacity* (TiB)
Week 1 (full and incremental)	Local disk (short-term)	1	1	1
StorSimple weeks 2-4	StorSimple disk (long-term)	1	4	4
Monthly full	StorSimple disk (long-term)	1	12	12
Yearly full	StorSimple disk (long-term)	1	1	1
GFS volumes size requirement				18*

* Total capacity includes 17 TiB of StorSimple disks and 1 TiB of local RAID volume.

GFS example schedule

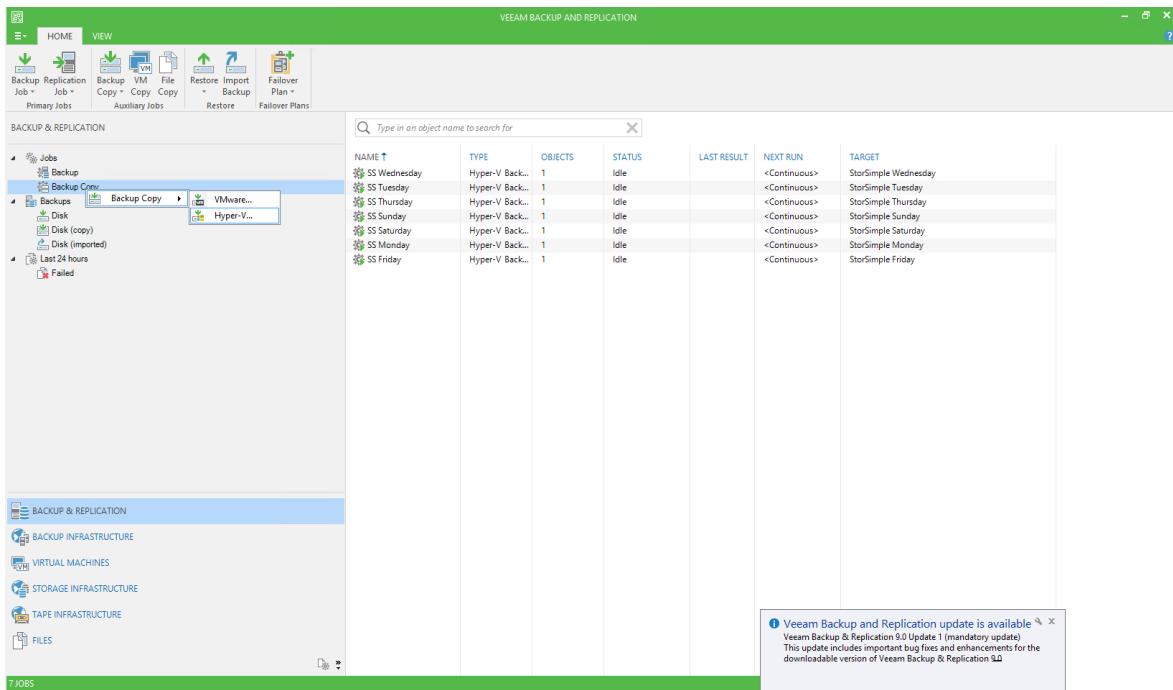
GFS rotation weekly, monthly, and yearly schedule

Week	Full	Incremental day 1	Incremental day 2	Incremental day 3	Incremental day 4	Incremental day 5
Week 1	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume
Week 2	StorSimple weeks 2-4					
Week 3	StorSimple weeks 2-4					
Week 4	StorSimple weeks 2-4					
Monthly	StorSimple monthly					
Yearly	StorSimple yearly					

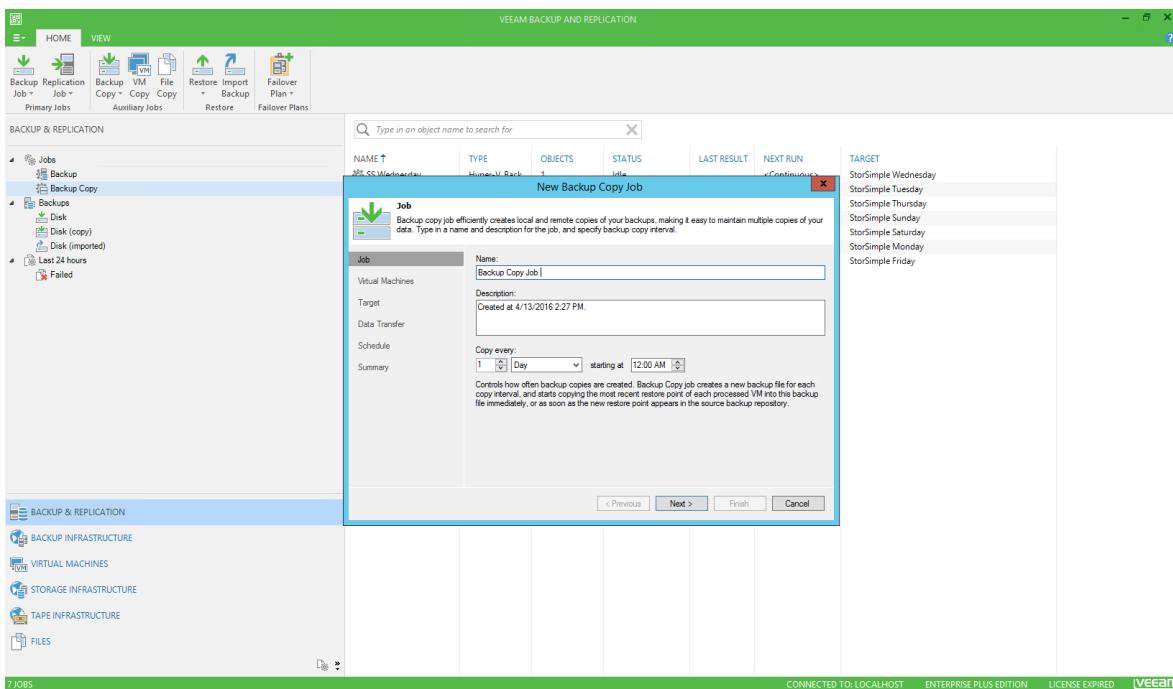
Assign StorSimple volumes to a Veeam copy job

To assign StorSimple volumes to a Veeam copy job

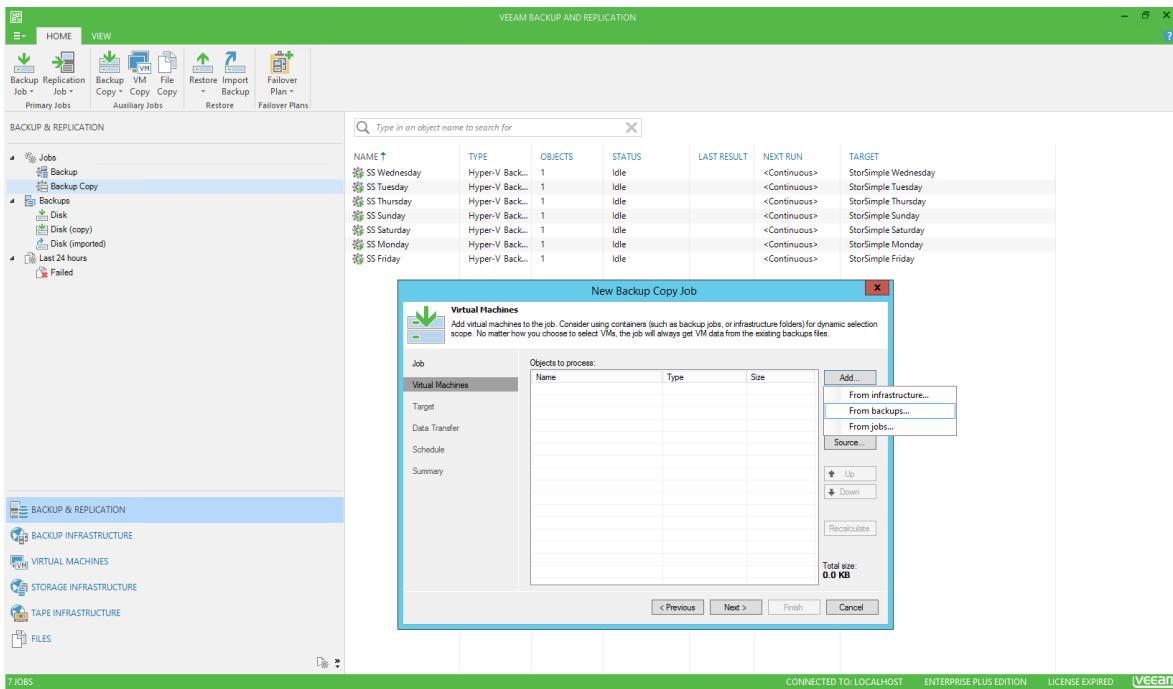
1. In the Veeam Backup and Replication console, select **Backup & Replication**. Right-click **Backup**, and then select **VMware** or **Hyper-V**, depending on your environment.



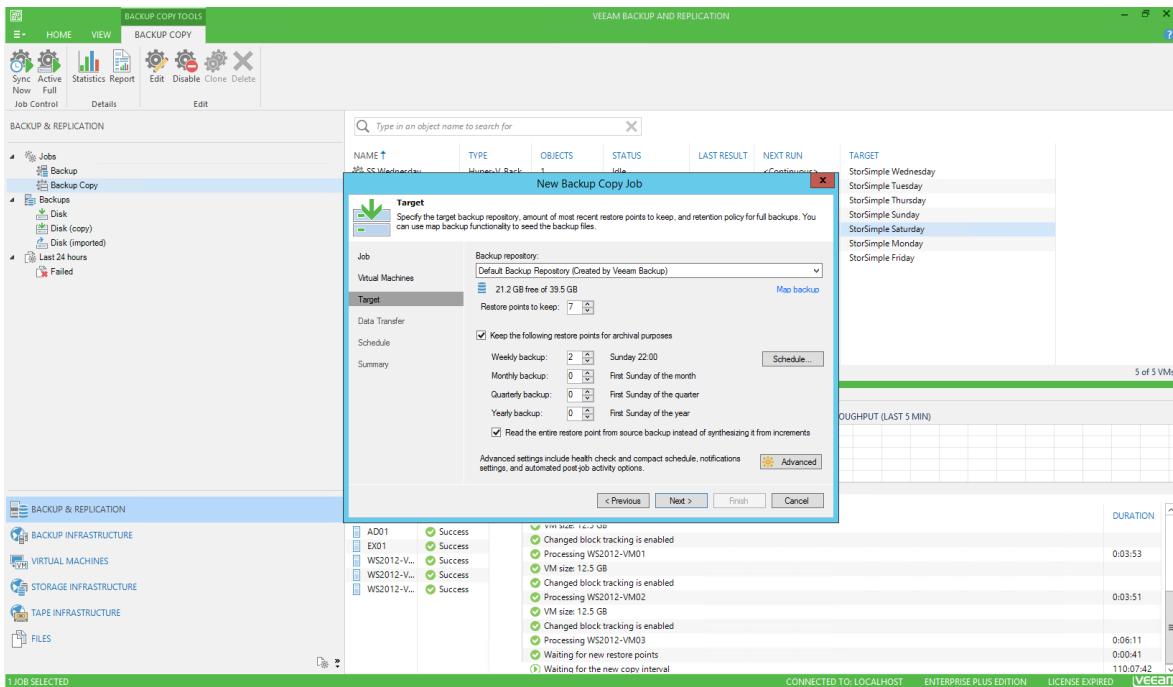
2. In the **New Backup Copy Job** dialog box, enter a name and description for the job.



3. Select the VMs you want to process. Select from backups, and then select the daily backup that you created earlier.

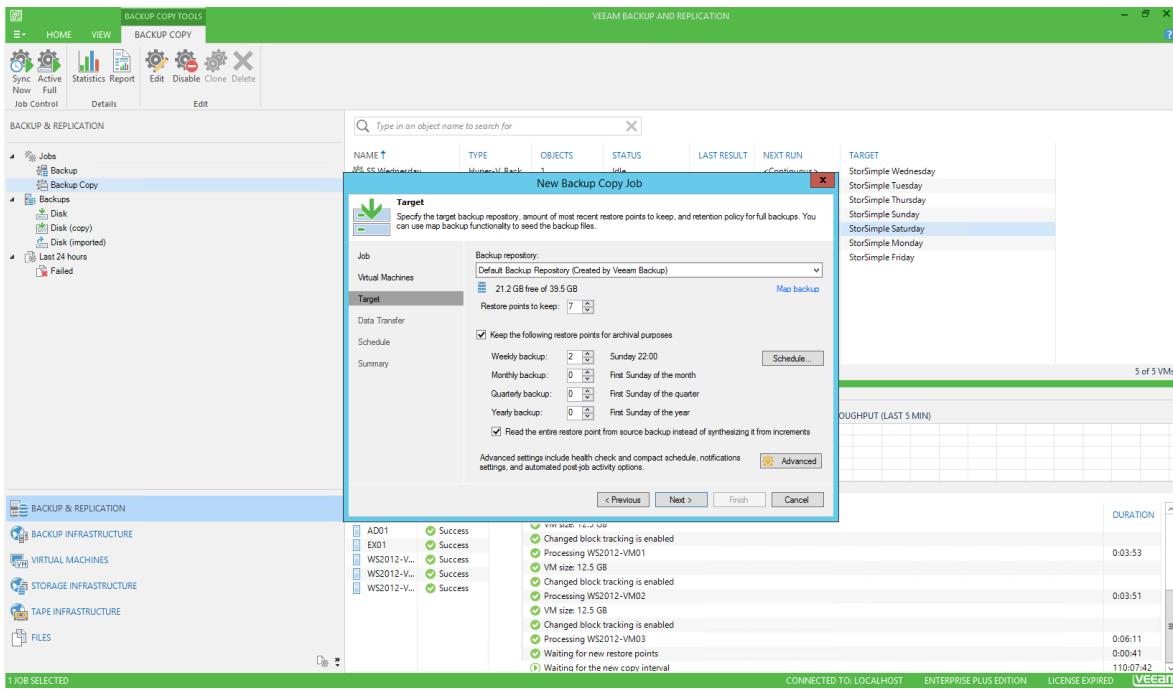


4. Exclude objects from the backup copy job, if needed.
5. Select your backup repository, and set a value for **Restore points to keep**. Be sure to select the **Keep the following restore points for archival purposes** check box. Define the backup frequency, and then select **Advanced**.

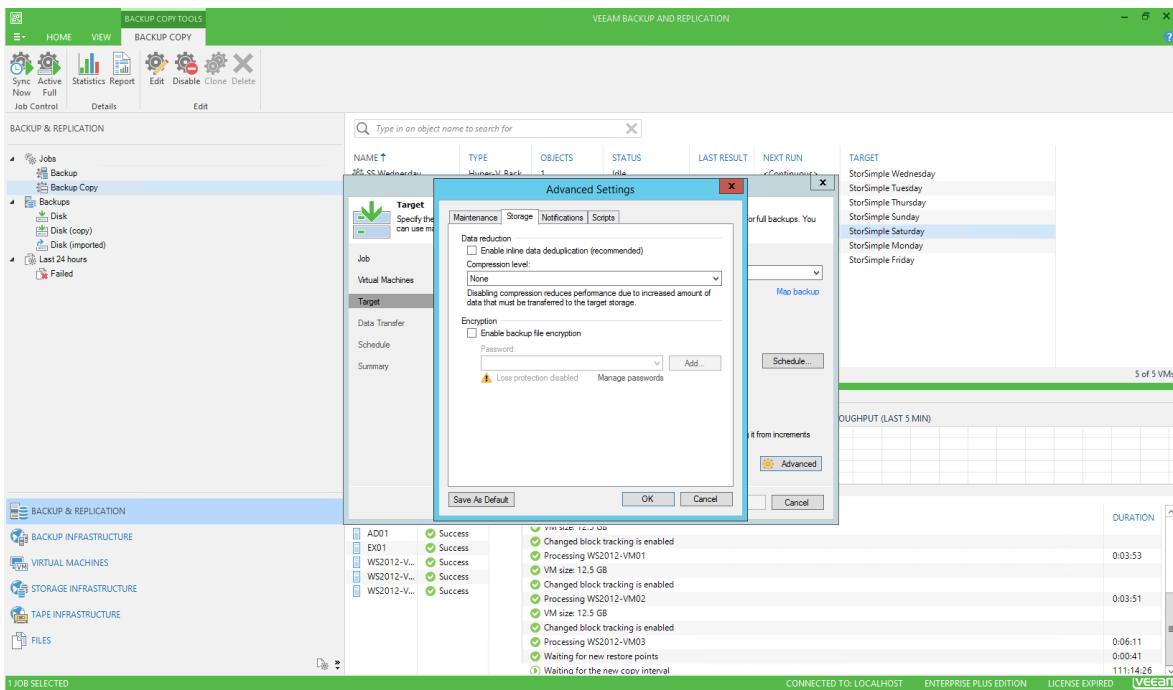


6. Specify the following advanced settings:

- On the **Maintenance** tab, turn off storage level corruption guard.



- On the Storage tab, be sure that deduplication and compression are turned off.



7. Specify that the data transfer is direct.

8. Define the backup copy window schedule according to your needs, and then finish the wizard.

For more information, see [Create backup copy jobs](#).

StorSimple cloud snapshots

StorSimple cloud snapshots protect the data that resides in your StorSimple device. Creating a cloud snapshot is equivalent to shipping local backup tapes to an offsite facility. If you use Azure geo-redundant storage, creating a cloud snapshot is equivalent to shipping backup tapes to multiple sites. If you need to restore a device after a disaster, you might bring another StorSimple device online and do a failover. After the failover, you would be able to access the data (at cloud speeds) from the most recent cloud snapshot.

The following section describes how to create a short script to start and delete StorSimple cloud snapshots during backup post-processing.

 **Note**

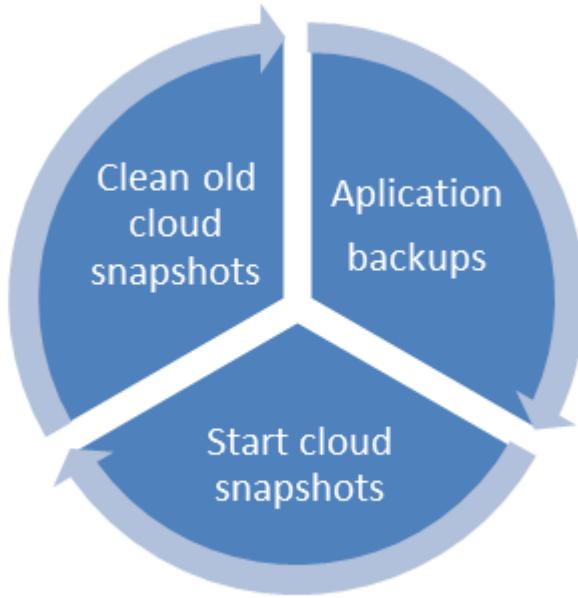
Snapshots that are manually or programmatically created do not follow the StorSimple snapshot expiration policy. These snapshots must be manually or programmatically deleted.

Start and delete cloud snapshots by using a script

 **Note**

Carefully assess the compliance and data retention repercussions before you delete a StorSimple snapshot. For more information about how to run a post-backup script, see the Veeam documentation.

Backup lifecycle



Requirements

- The server that runs the script must have access to Azure cloud resources.
- The user account must have the necessary permissions.
- A StorSimple backup policy with the associated StorSimple volumes must be set up but not turned on.
- You'll need the StorSimple resource name, registration key, device name, and backup policy ID.

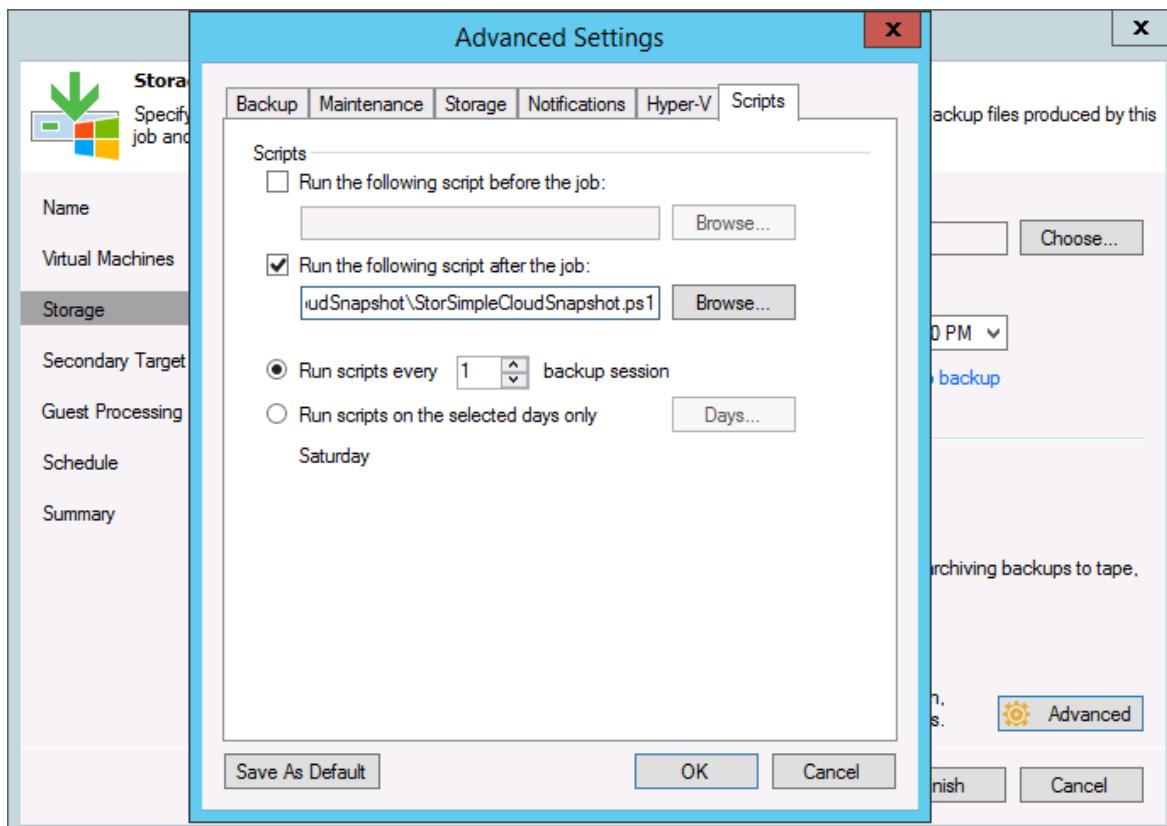
To start or delete a cloud snapshot

1. [Install Azure PowerShell](#).
2. Download and setup [Manage-CloudSnapshots.ps1](#) PowerShell script.
3. On the server that runs the script, run PowerShell as an administrator. Ensure that you run the script with `-WhatIf $true` to see what changes the script will make. Once the validation is complete, pass `-WhatIf $false`. Run the below command:

PowerShell

```
. \Manage-CloudSnapshots.ps1 -SubscriptionId [Subscription Id] -TenantId
[Tenant ID] -ResourceGroupName [Resource Group Name] -ManagerName
[StorSimple Device Manager Name] -DeviceName [device name] -
BackupPolicyName [backup policyname] -RetentionInDays [Retention days]
-WhatIf [$true or $false]
```

4. To add the script to your backup job, edit your Veeam job advanced options.



We recommend that you run your StorSimple cloud snapshot backup policy as a post-processing script at the end of your daily backup job. For more information about how to back up and restore your backup application environment to help you meet your RPO and RTO, please consult with your backup architect.

StorSimple as a restore source

Restores from a StorSimple device work like restores from any block storage device. Restores of data that is tiered to the cloud occurs at cloud speeds. For local data, restores occur at the local disk speed of the device.

With Veeam, you get fast, granular, file-level recovery through StorSimple via the built-in explorer views in the Veeam console. Use the Veeam Explorers to recover individual items, like email messages, Active Directory objects, and SharePoint items from backups. The recovery can be done without on-premises VM disruption. You also can do point-in-time recovery for Azure SQL Database and Oracle databases. Veeam and StorSimple make the process of item-level recovery from Azure fast and easy. For information about how to perform a restore, see the Veeam documentation:

- For [Exchange Server ↗](#)
- For [Active Directory ↗](#)
- For [SQL Server ↗](#)
- For [SharePoint ↗](#)
- For [Oracle ↗](#)

StorSimple failover and disaster recovery

ⓘ Note

For backup target scenarios, StorSimple Cloud Appliance is not supported as a restore target.

A disaster can be caused by a variety of factors. The following table lists common disaster recovery scenarios.

Scenario	Impact	How to recover	Notes
StorSimple device failure	Backup and restore operations are interrupted.	Replace the failed device and perform StorSimple failover and disaster recovery .	If you need to perform a restore after device recovery, full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds. The index and catalog rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier, which might be a time-consuming process.
Veeam server failure	Backup and restore operations are interrupted.	Rebuild the backup server and perform database restore as detailed in Veeam Help Center (Technical Documentation) .	You must rebuild or restore the Veeam server at the disaster recovery site. Restore the database to the most recent point. If the restored Veeam database is not in sync with your latest backup jobs, indexing and cataloging is required. This index and catalog rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier. This makes it further time-intensive.
Site failure that results in the loss of both the backup server and StorSimple	Backup and restore operations are interrupted.	Restore StorSimple first, and then restore Veeam. If you need to perform a restore after device recovery, the full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds.	

References

The following documents were referenced for this article:

- [StorSimple multipath I/O setup](#)

- Storage scenarios: Thin provisioning
- Using GPT drives
- Set up shadow copies for shared folders

Next steps

- Learn more about how to [restore from a backup set](#).
- Learn more about how to perform [device failover and disaster recovery](#).

StorSimple as a backup target with Backup Exec

Article • 08/22/2022 • 19 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Azure StorSimple is a hybrid cloud storage solution from Microsoft. StorSimple addresses the complexities of exponential data growth by using an Azure storage account as an extension of the on-premises solution, and automatically tiering data across on-premises storage and cloud storage.

In this article, we discuss StorSimple integration with Veritas Backup Exec and best practices for integrating both solutions. We also make recommendations on how to set up Backup Exec to best integrate with StorSimple. We defer to Veritas best practices, backup architects, and administrators for the best way to set up Backup Exec to meet individual backup requirements and service-level agreements (SLAs).

Although we illustrate configuration steps and key concepts, this article is by no means a step-by-step configuration or installation guide. We assume that the basic components and infrastructure are in working order and ready to support the concepts that we describe.

Who should read this?

The information in this article will be most helpful to backup administrators, storage administrators, and storage architects who have knowledge of storage, Windows Server 2012 R2, Ethernet, cloud services, and Backup Exec.

Supported versions

- [Backup Exec 16 and later versions ↗](#)
- [StorSimple Update 3 and later versions](#)

Why StorSimple as a backup target?

StorSimple is a good choice for a backup target because:

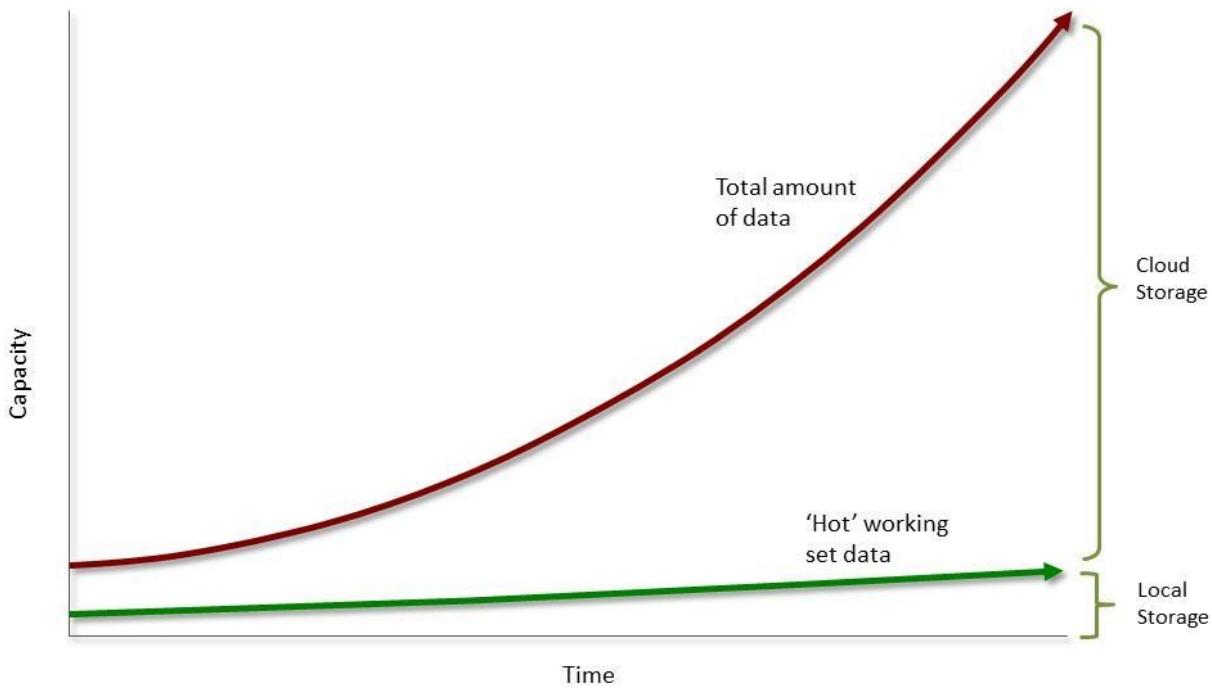
- It provides standard, local storage for backup applications to use as a fast backup destination, without any changes. You also can use StorSimple for a quick restore of recent backups.
- Its cloud tiering is seamlessly integrated with an Azure cloud storage account to use cost-effective Azure Storage.
- It automatically provides offsite storage for disaster recovery.

Key concepts

As with any storage solution, a careful assessment of the solution's storage performance, SLAs, rate of change, and capacity growth needs is critical to success. The main idea is that by introducing a cloud tier, your access times and throughputs to the cloud play a fundamental role in the ability of StorSimple to do its job.

StorSimple is designed to provide storage to applications that operate on a well-defined working set of data (hot data). In this model, the working set of data is stored on the local tiers, and the remaining nonworking/cold/archived set of data is tiered to the cloud. This model is represented in the following figure. The nearly flat green line represents the data stored on the local tiers of the StorSimple device. The red line represents the total amount of data stored on the StorSimple solution across all tiers. The space between the flat green line and the exponential red curve represents the total amount of data stored in the cloud.

StorSimple tiering



With this architecture in mind, you will find that StorSimple is ideally suited to operate as a backup target. You can use StorSimple to:

- Perform your most frequent restores from the local working set of data.
- Use the cloud for offsite disaster recovery and older data, where restores are less frequent.

StorSimple benefits

StorSimple provides an on-premises solution that is seamlessly integrated with Microsoft Azure, by taking advantage of seamless access to on-premises and cloud storage.

StorSimple uses automatic tiering between the on-premises device, which has solid-state device (SSD) and serial-attached SCSI (SAS) storage, and Azure Storage. Automatic tiering keeps frequently accessed data local, on the SSD and SAS tiers. It moves infrequently accessed data to Azure Storage.

StorSimple offers these benefits:

- Unique deduplication and compression algorithms that use the cloud to achieve unprecedented deduplication levels
- High availability
- Geo-replication by using Azure geo-replication
- Azure integration
- Data encryption in the cloud

- Improved disaster recovery and compliance

Although StorSimple presents two main deployment scenarios (primary backup target and secondary backup target), fundamentally, it's a plain, block storage device. StorSimple does all the compression and deduplication. It seamlessly sends and retrieves data between the cloud and the application and file system.

For more information about StorSimple, see [StorSimple 8000 series: Hybrid cloud storage solution](#). Also, you can review the [technical StorSimple 8000 series specifications](#).

Important

Using a StorSimple device as a backup target is supported only for StorSimple 8000 Update 3 and later versions.

Architecture overview

The following tables show the device model-to-architecture initial guidance.

StorSimple capacities for local and cloud storage

Storage capacity	8100	8600
Local storage capacity	< 10 TiB*	< 20 TiB*
Cloud storage capacity	> 200 TiB*	> 500 TiB*

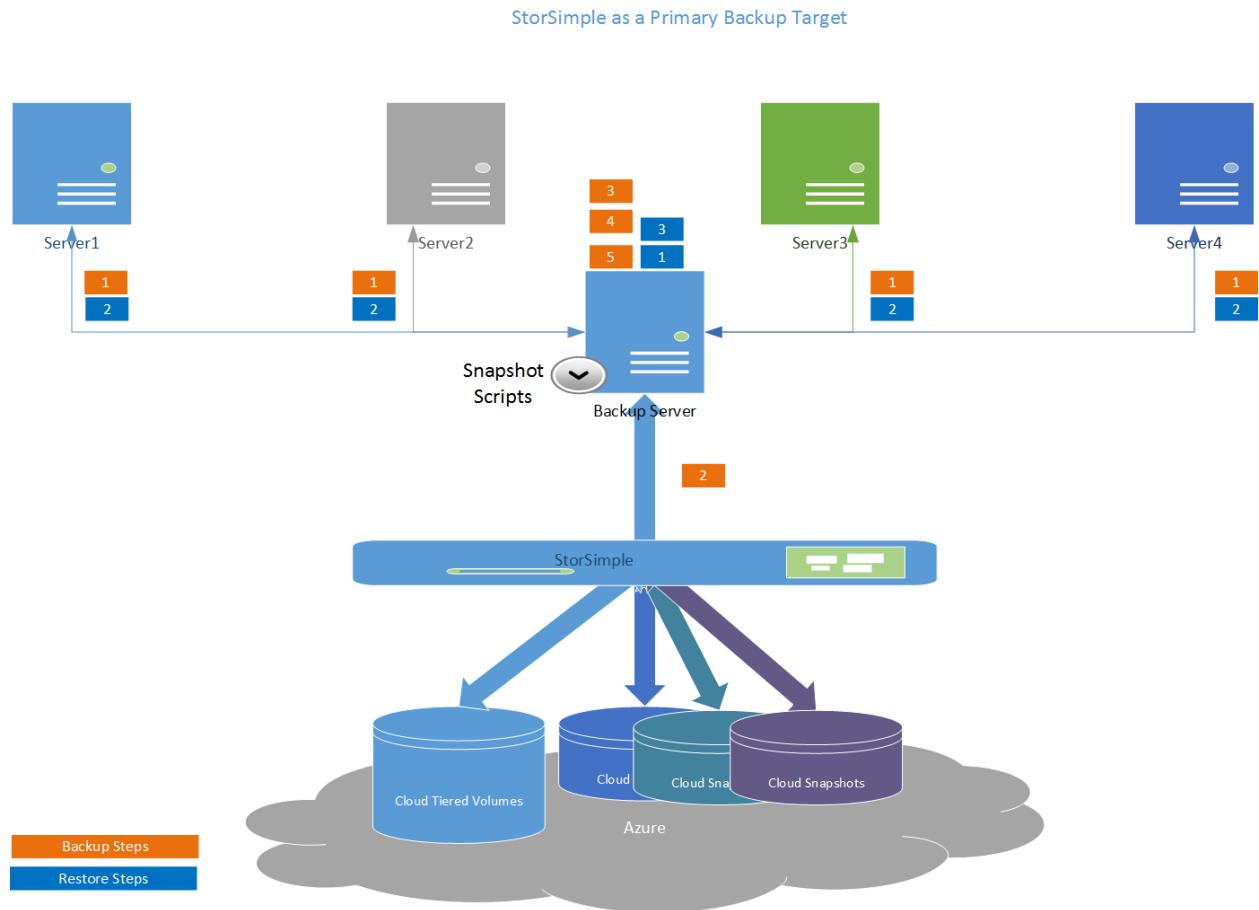
* Storage size assumes no deduplication or compression.

StorSimple capacities for primary and secondary backups

Backup scenario	Local storage capacity	Cloud storage capacity
Primary backup	Recent backups stored on local storage for fast recovery to meet recovery point objective (RPO)	Backup history (RPO) fits in cloud capacity
Secondary backup	Secondary copy of backup data can be stored in cloud capacity	N/A

StorSimple as a primary backup target

In this scenario, StorSimple volumes are presented to the backup application as the sole repository for backups. The following figure shows a solution architecture in which all backups use StorSimple tiered volumes for backups and restores.



Primary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to the StorSimple tiered volumes.
3. The backup server updates the catalog database, and then finishes the backup job.
4. A snapshot script triggers the StorSimple cloud snapshot manager (start or delete).
5. The backup server deletes expired backups based on a retention policy.

Primary target restore logical steps

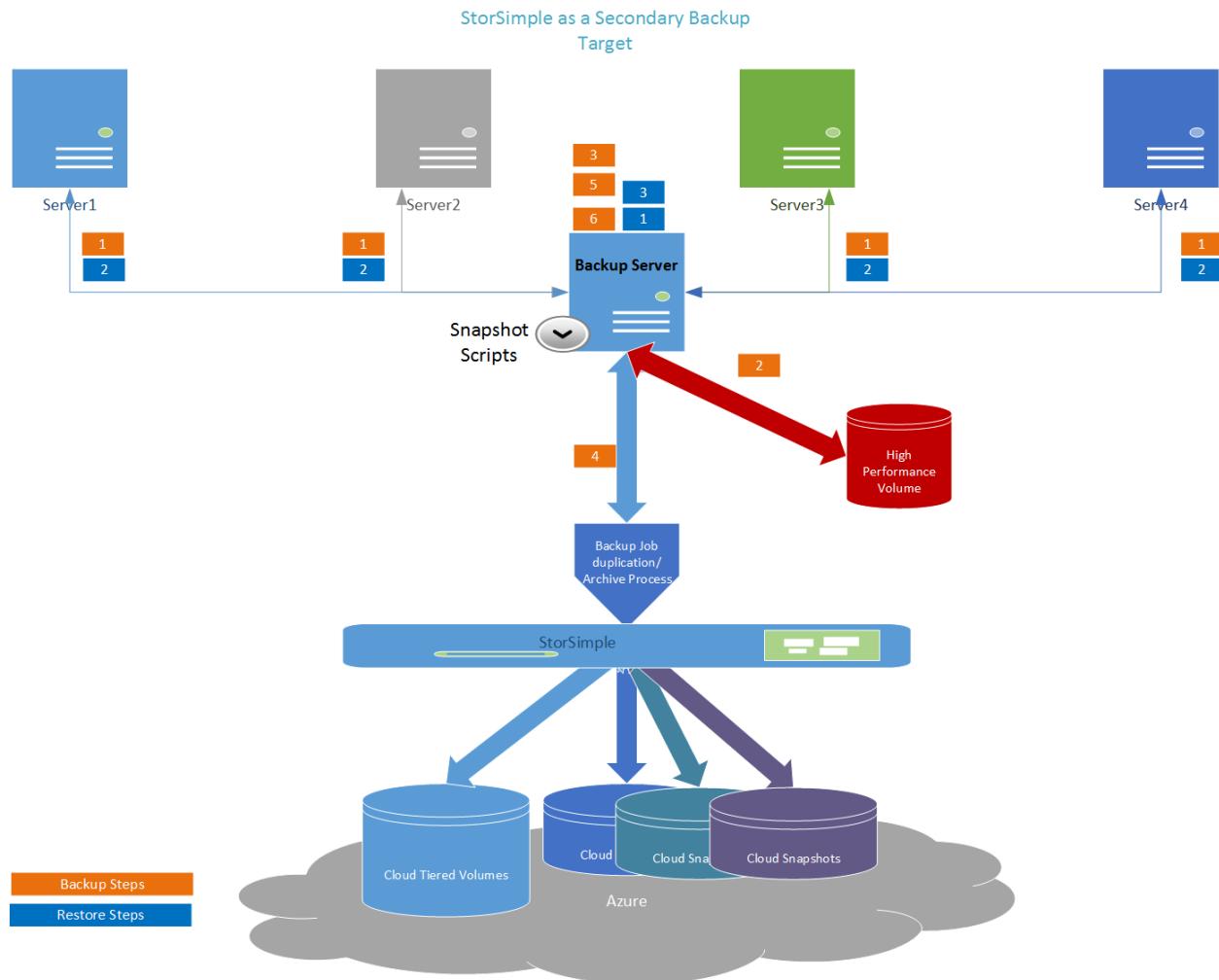
1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

StorSimple as a secondary backup target

In this scenario, StorSimple volumes primarily are used for long-term retention or archiving.

The following figure shows an architecture in which initial backups and restores target a high-performance volume. These backups are copied and archived to a StorSimple tiered volume on a set schedule.

It is important to size your high-performance volume so that it can handle your retention policy capacity and performance requirements.



Secondary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to high-performance storage.
3. The backup server updates the catalog database, and then finishes the backup job.
4. The backup server copies backups to StorSimple based on a retention policy.
5. A snapshot script triggers the StorSimple cloud snapshot manager (start or delete).
6. The backup server deletes expired backups based on a retention policy.

Secondary target restore logical steps

1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

Deploy the solution

Deploying the solution requires three steps:

1. Prepare the network infrastructure.
2. Deploy your StorSimple device as a backup target.
3. Deploy Backup Exec.

Each step is discussed in detail in the following sections.

Set up the network

Because StorSimple is a solution that's integrated with the Azure cloud, StorSimple requires an active and working connection to the Azure cloud. This connection is used for operations like cloud snapshots, management, and metadata transfer, and to tier older, less accessed data to Azure cloud storage.

For the solution to perform optimally, we recommend that you follow these networking best practices:

- The link that connects your StorSimple tiering to Azure must meet your bandwidth requirements. To achieve this, apply the necessary Quality of Service (QoS) level to your infrastructure switches to match your RPO and recovery time objective (RTO) SLAs.
- Maximum Azure Blob storage access latencies should be around 80 ms.

Deploy StorSimple

For a step-by-step StorSimple deployment guidance, see [Deploy your on-premises StorSimple device](#).

Deploy Backup Exec

For Backup Exec installation best practices, see [Best practices for Backup Exec installation](#).

Set up the solution

In this section, we demonstrate some configuration examples. The following examples and recommendations illustrate the most basic and fundamental implementation. This implementation might not apply directly to your specific backup requirements.

Set up StorSimple

StorSimple deployment tasks	Additional comments
Deploy your on-premises StorSimple device.	Supported versions: Update 3 and later versions.
Turn on the backup target.	<p>Use these commands to turn on or turn off backup target mode, and to get status. For more information, see Connect remotely to a StorSimple device.</p> <p>To turn on backup mode: <code>Set-HCSBackupApplianceMode -enable</code>.</p> <p>To turn off backup mode: <code>Set-HCSBackupApplianceMode -disable</code>.</p> <p>To get the current state of backup mode settings: <code>Get-HCSBackupApplianceMode</code>.</p>
Create a common volume container for your volume that stores the backup data. All data in a volume container is deduplicated.	StorSimple volume containers define deduplication domains.
Create StorSimple volumes.	<p>Create volumes with sizes as close to the anticipated usage as possible, because volume size affects cloud snapshot duration time. For information about how to size a volume, read about retention policies.</p> <p>Use StorSimple tiered volumes, and select the Use this volume for less frequently accessed archival data check box.</p> <p>Using only locally pinned volumes is not supported.</p>
Create a unique StorSimple backup policy for all the backup target volumes.	A StorSimple backup policy defines the volume consistency group.
Disable the schedule as the snapshots expire.	Snapshots are triggered as a post-processing operation.

Set up the host backup server storage

Set up the host backup server storage according to these guidelines:

- Don't use spanned volumes (created by Windows Disk Management). Spanned disks are not supported.
- Format your volumes using NTFS with 64-KB allocation size.
- Map the StorSimple volumes directly to the Backup Exec server.
 - Use iSCSI for physical servers.
 - Use pass-through disks for virtual servers.

Best practices for StorSimple and Backup Exec

Set up your solution according to the guidelines in the following sections.

Operating system best practices

- Disable Windows Server encryption and deduplication for the NTFS file system.
- Disable Windows Server defragmentation on the StorSimple volumes.
- Disable Windows Server indexing on the StorSimple volumes.
- Run an antivirus scan at the source host (not against the StorSimple volumes).
- Turn off the default [Windows Server maintenance](#) in Task Manager. Do this in one of the following ways:
 - Turn off the Maintenance configurator in Windows Task Scheduler.
 - Download [PsExec](#) from Windows Sysinternals. After you download PsExec, run Azure PowerShell as an administrator, and type:

PowerShell

```
psexec \\%computername% -s schtasks /change /tn  
"MicrosoftWindowsTaskSchedulerMaintenance Configurator" /disable
```

StorSimple best practices

- Be sure that the StorSimple device is updated to [Update 3 or later](#).
- Isolate iSCSI and cloud traffic. Use dedicated iSCSI connections for traffic between StorSimple and the backup server.
- Be sure that your StorSimple device is a dedicated backup target. Mixed workloads are not supported because they affect your RTO and RPO.

Backup Exec best practices

- Backup Exec must be installed on a local drive of the server, and not on a StorSimple volume.
- Set the Backup Exec storage **concurrent write operations** to the maximum allowed.
 - Set the Backup Exec storage **block and buffer size** to 512 KB.
 - Turn on Backup Exec storage **buffered read and write**.
- StorSimple supports Backup Exec full and incremental backups. We recommend that you not use synthetic and differential backups.
- Backup data files should contain data only for a specific job. For example, no media appends across different jobs are allowed.
- Disable job verification. If necessary, verification should be scheduled after the latest backup job. It is important to understand that this job affects your backup window.
- Select **Storage > Your disk > Details > Properties**. Turn off **Pre-allocate disk space**.

For the latest Backup Exec settings and best practices for implementing these requirements, see [the Veritas website](#) ↗.

Retention policies

One of the most common backup retention policy types is a Grandfather, Father, and Son (GFS) policy. In a GFS policy, an incremental backup is performed daily and full backups are done weekly and monthly. This policy results in six StorSimple tiered volumes. One volume contains the weekly, monthly, and yearly full backups. The other five volumes store daily incremental backups.

In the following example, we use a GFS rotation. The example assumes the following:

- Non-deduped or compressed data is used.
- Full backups are 1 TiB each.
- Daily incremental backups are 500 GiB each.
- Four weekly backups are kept for a month.
- Twelve monthly backups are kept for a year.
- One yearly backup is kept for 10 years.

Based on the preceding assumptions, create a 26-TiB StorSimple tiered volume for the monthly and yearly full backups. Create a 5-TiB StorSimple tiered volume for each of the incremental daily backups.

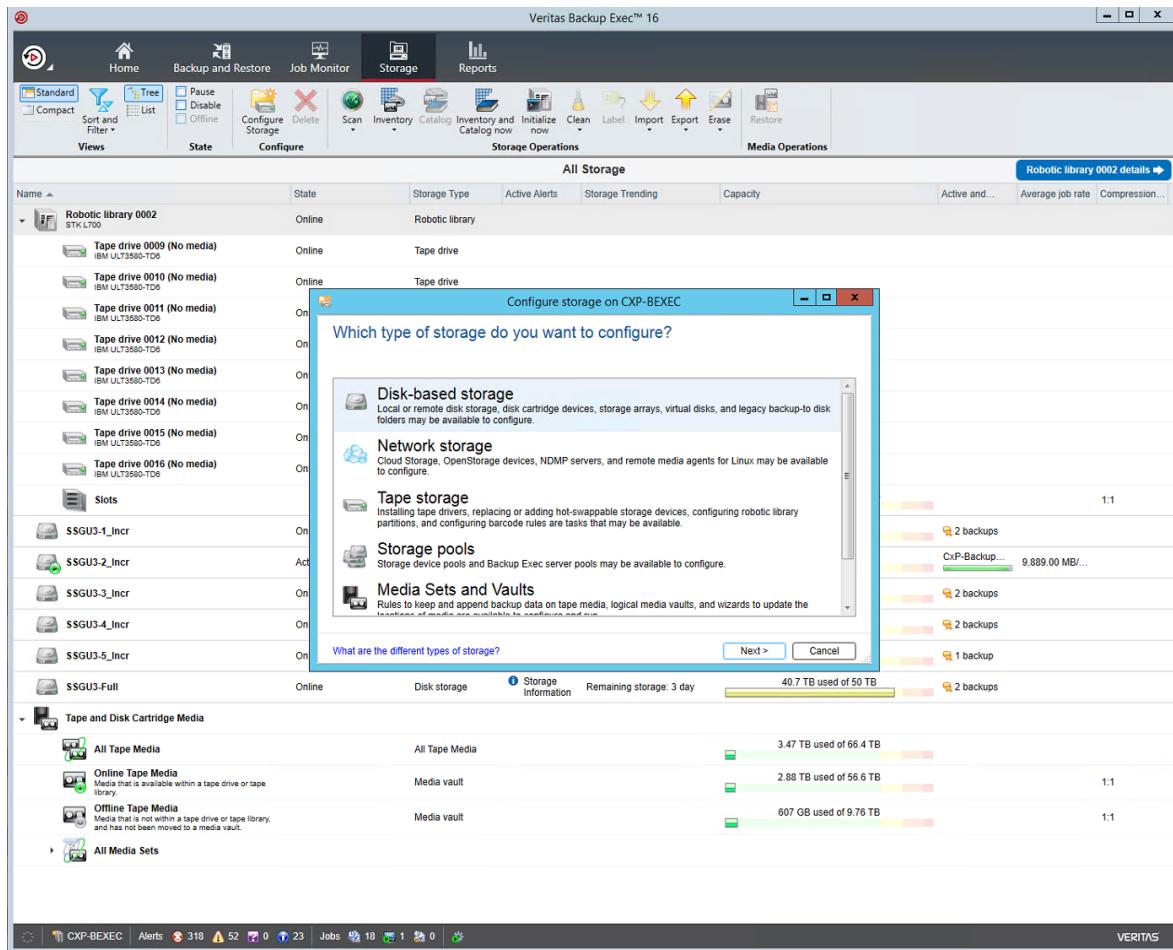
Backup type retention	Size (TiB)	GFS multiplier*	Total capacity (TiB)
Weekly full	1	4	4
Daily incremental	0.5	20 (cycles equal number of weeks per month)	12 (2 for additional quota)
Monthly full	1	12	12
Yearly full	1	10	10
GFS requirement		38	
Additional quota	4		42 total GFS requirement

* The GFS multiplier is the number of copies you need to protect and retain to meet your backup policy requirements.

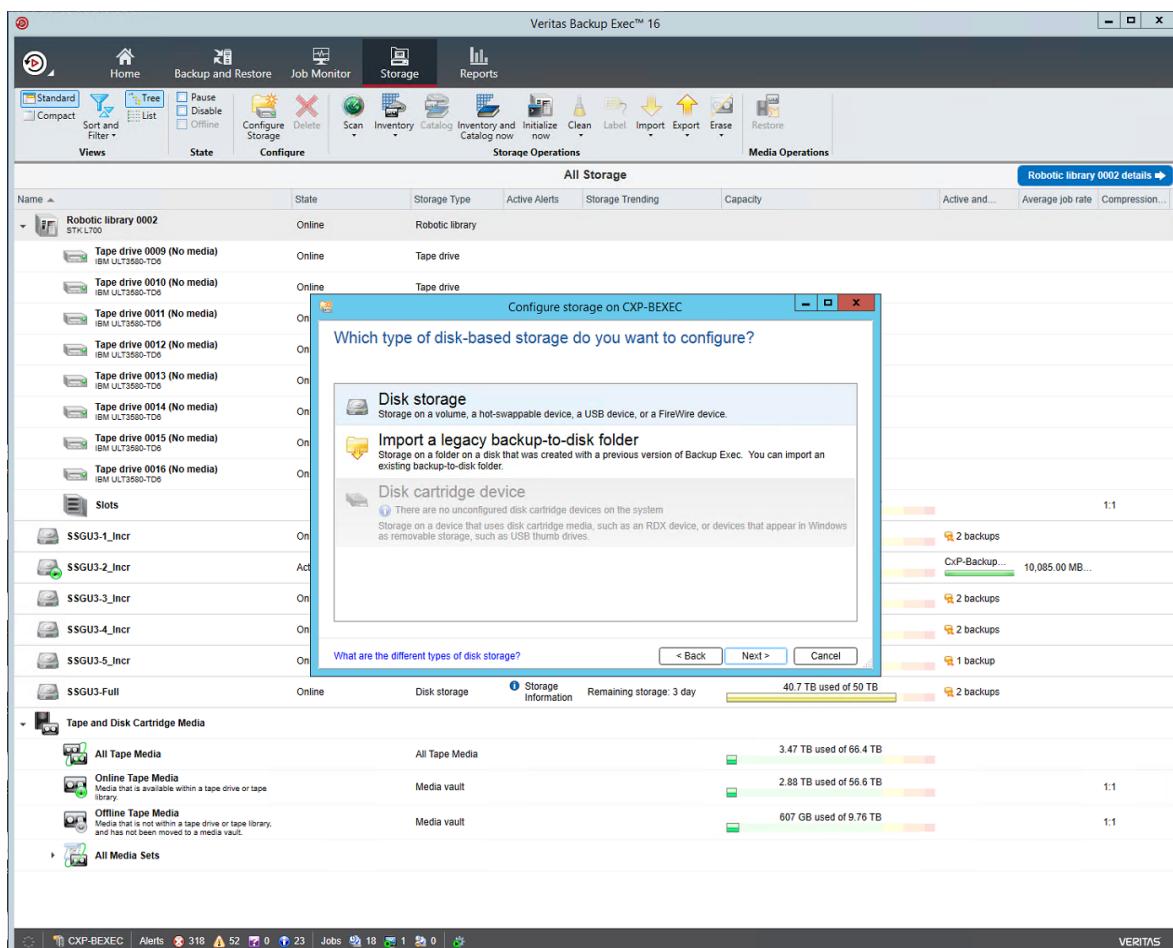
Set up Backup Exec storage

To set up Backup Exec storage

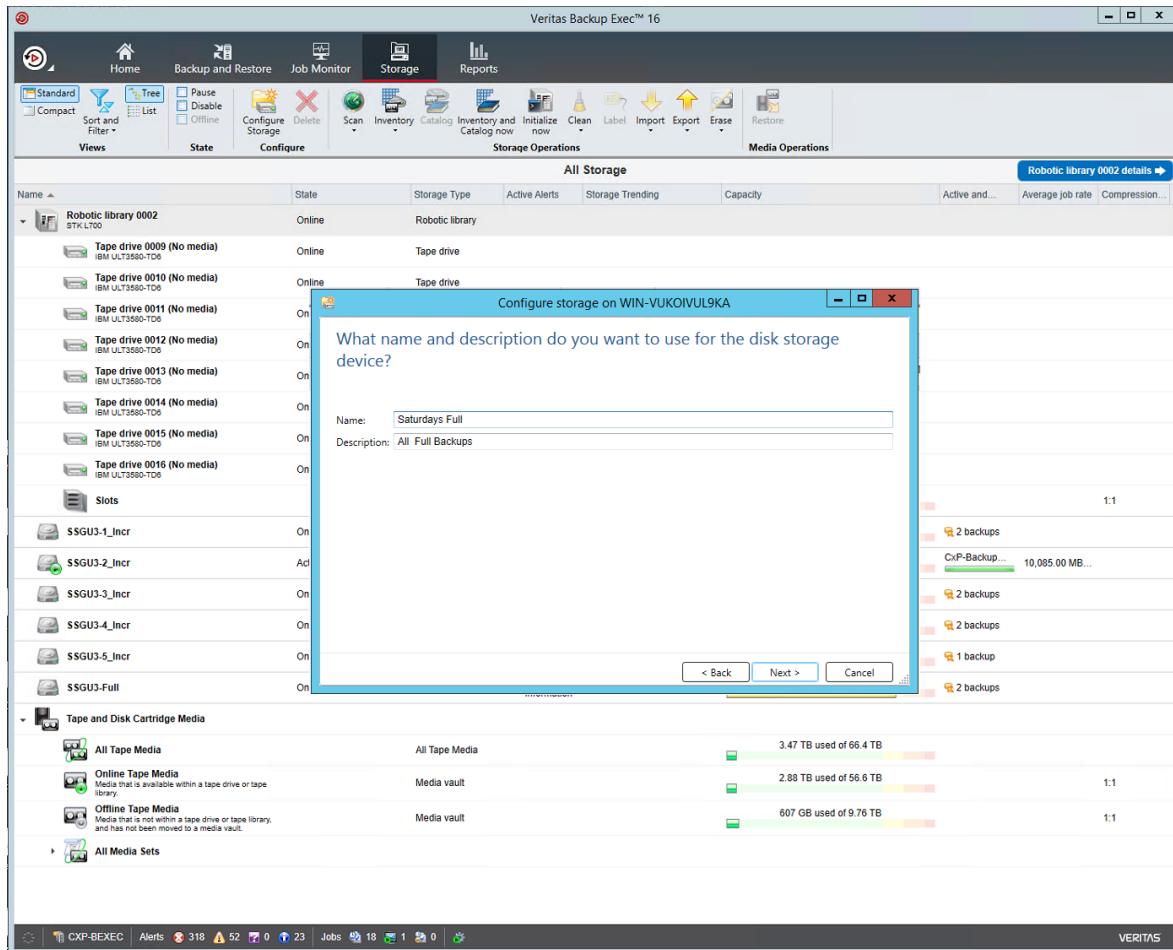
1. In the Backup Exec management console, select **Storage > Configure Storage > Disk-Based Storage > Next**.



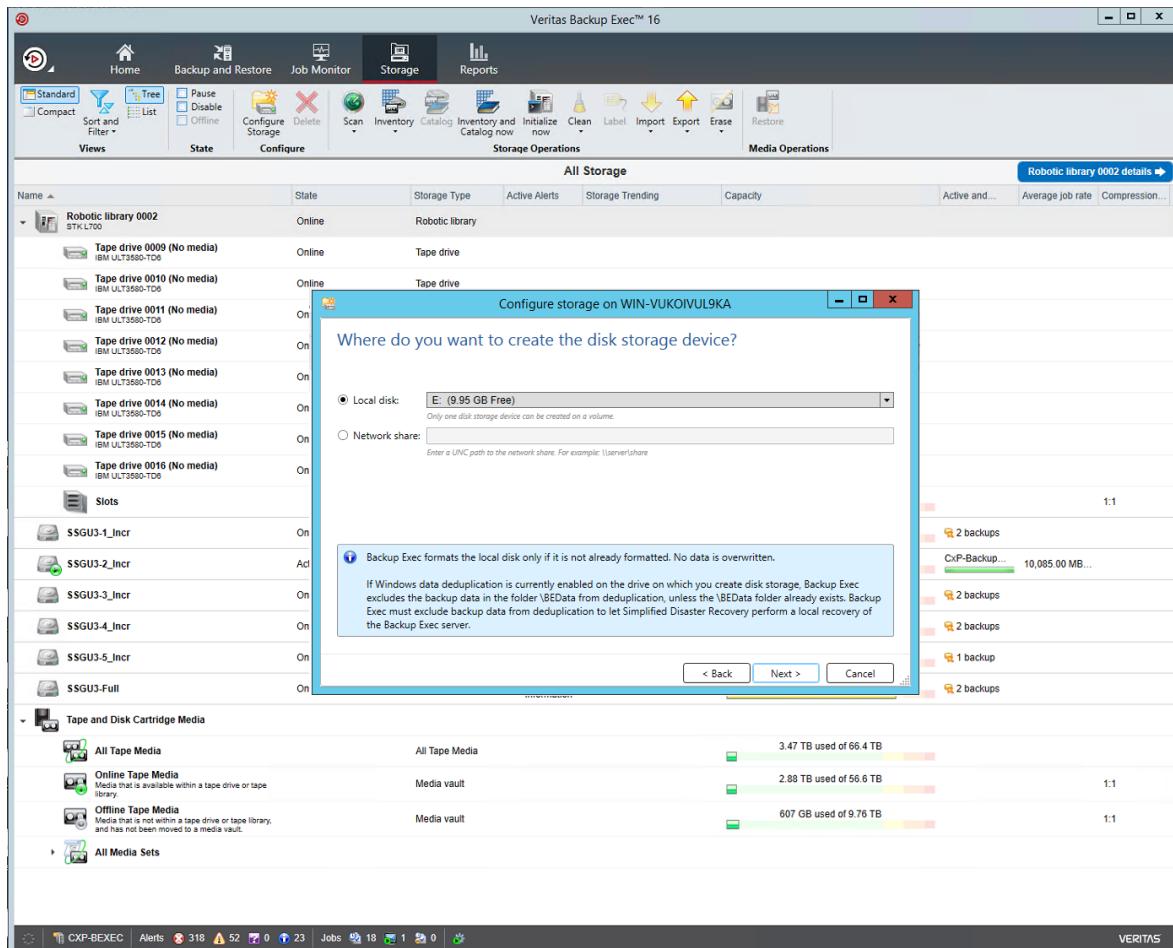
2. Select Disk Storage, and then select Next.



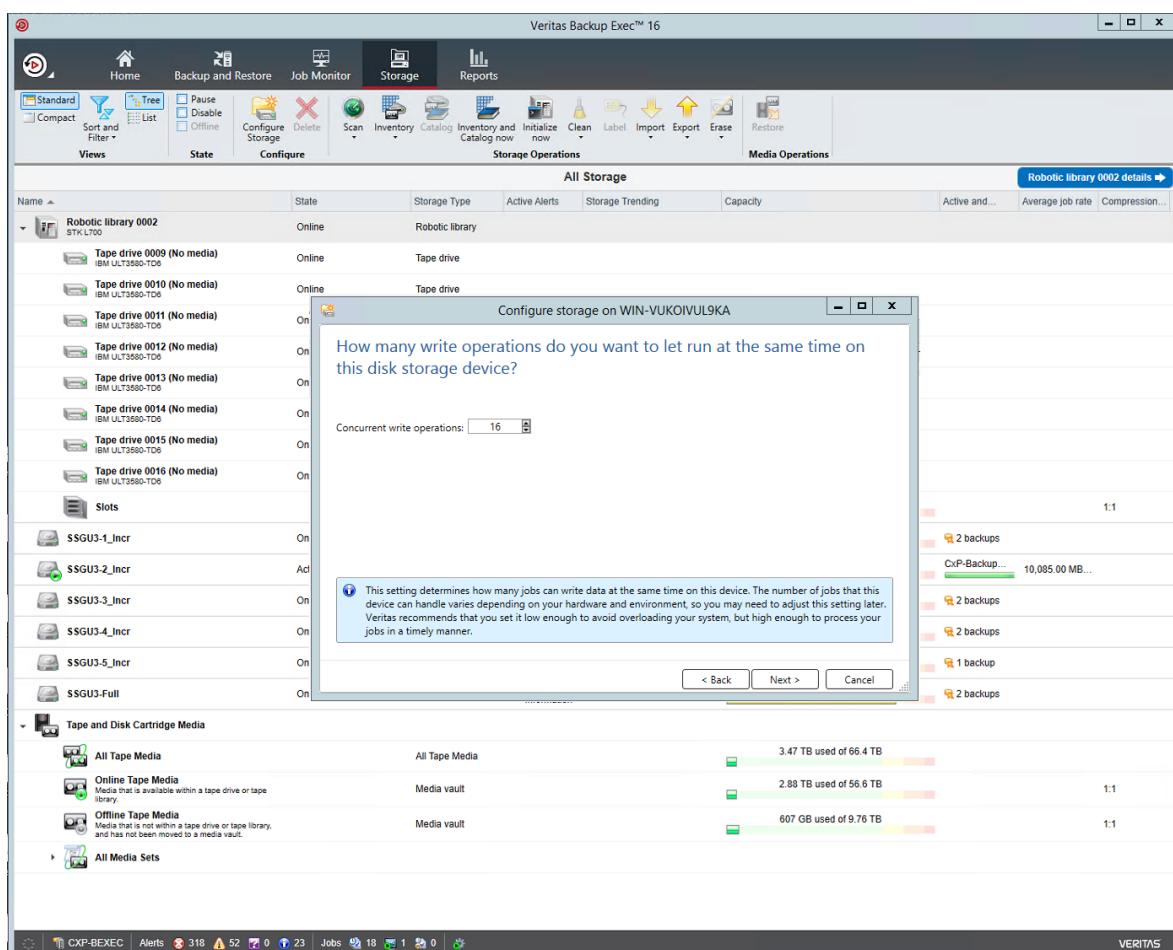
3. Enter a representative name, for example, **Saturday Full**, and a description. Select **Next**.



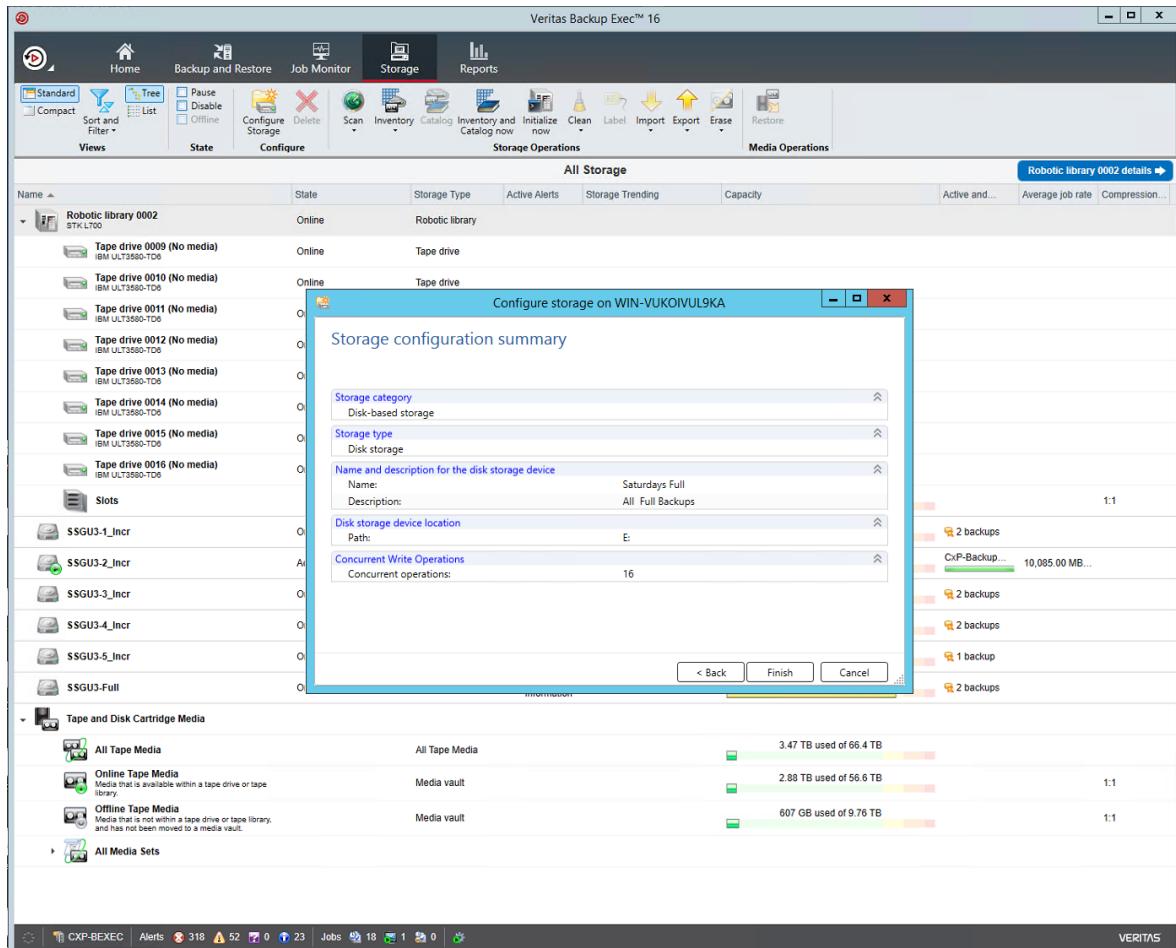
4. Select the disk where you want to create the disk storage device, and then select **Next**.



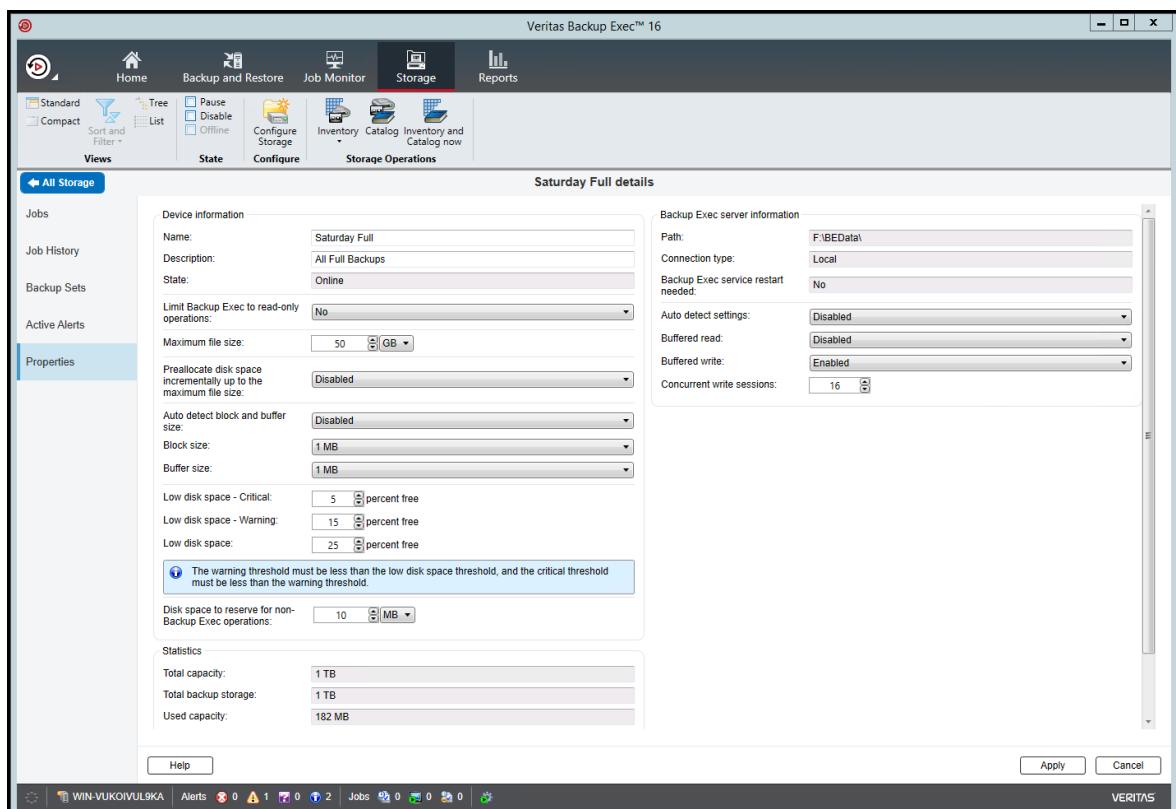
5. Increment the number of write operations to 16, and then select Next.



6. Review the settings, and then select Finish.



7. At the end of each volume assignment, change the storage device settings to match those recommended at [Best practices for StorSimple and Backup Exec](#).



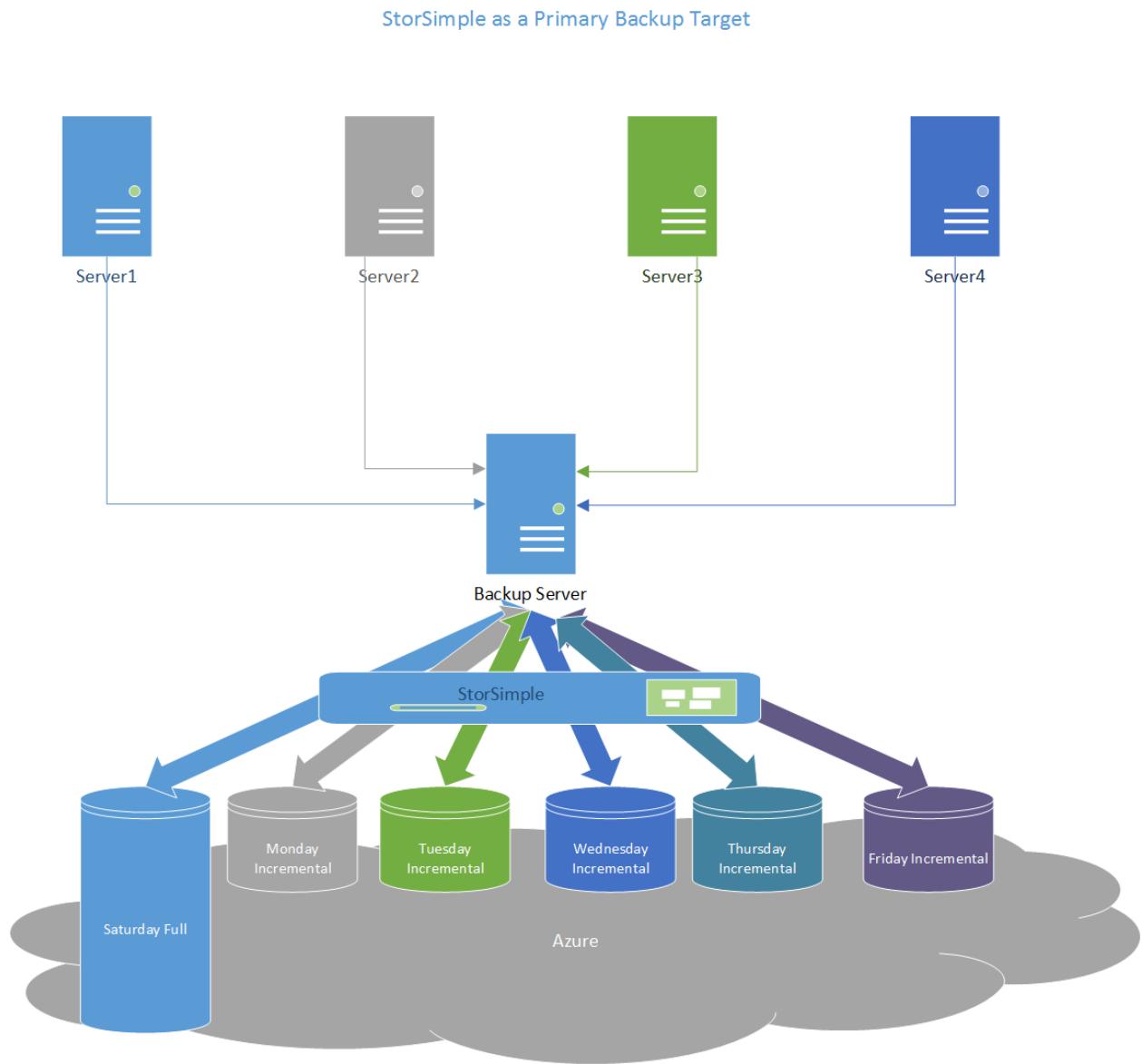
8. Repeat steps 1-7 until you are finished assigning your StorSimple volumes to Backup Exec.

Set up StorSimple as a primary backup target

ⓘ Note

Data restore from a backup that has been tiered to the cloud occurs at cloud speeds.

The following figure shows the mapping of a typical volume to a backup job. In this case, all the weekly backups map to the Saturday full disk, and the incremental backups map to Monday-Friday incremental disks. All the backups and restores are from a StorSimple tiered volume.



StorSimple as a primary backup target GFS schedule example

Here's an example of a GFS rotation schedule for four weeks, monthly, and yearly:

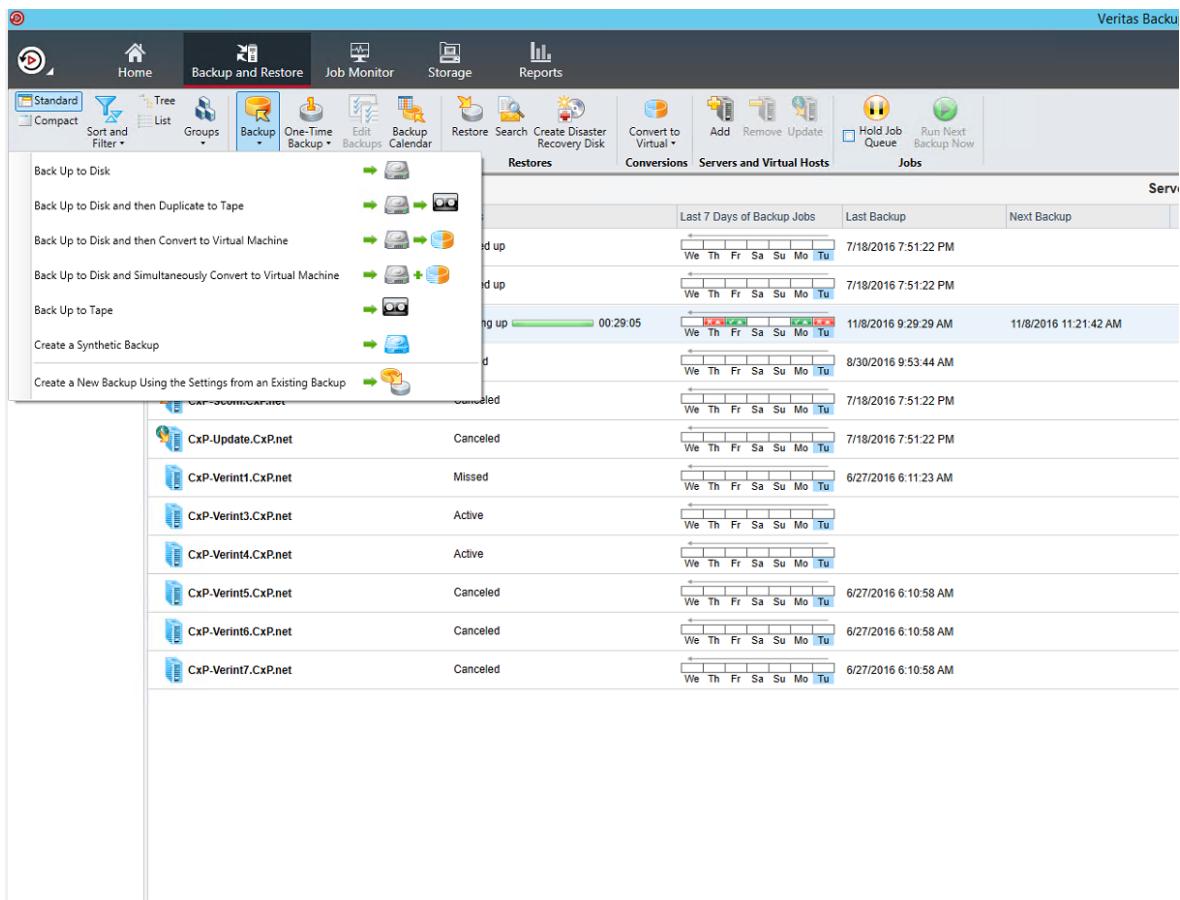
Frequency/backup type	Full	Incremental (days 1-5)
Weekly (weeks 1-4)	Saturday	Monday-Friday
Monthly	Saturday	
Yearly	Saturday	

Assign StorSimple volumes to a Backup Exec backup job

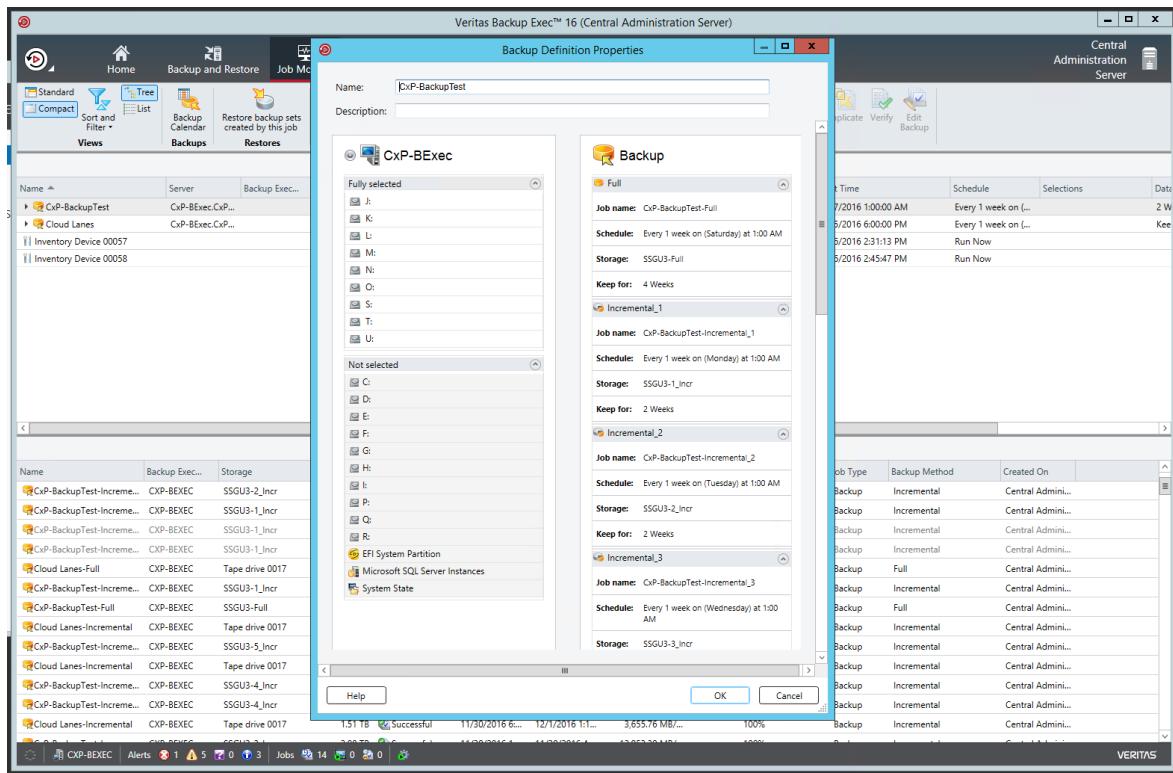
The following sequence assumes that Backup Exec and the target host are configured in accordance with the Backup Exec agent guidelines.

To assign StorSimple volumes to a Backup Exec backup job

1. In the Backup Exec management console, select Host > Backup > Backup to Disk.

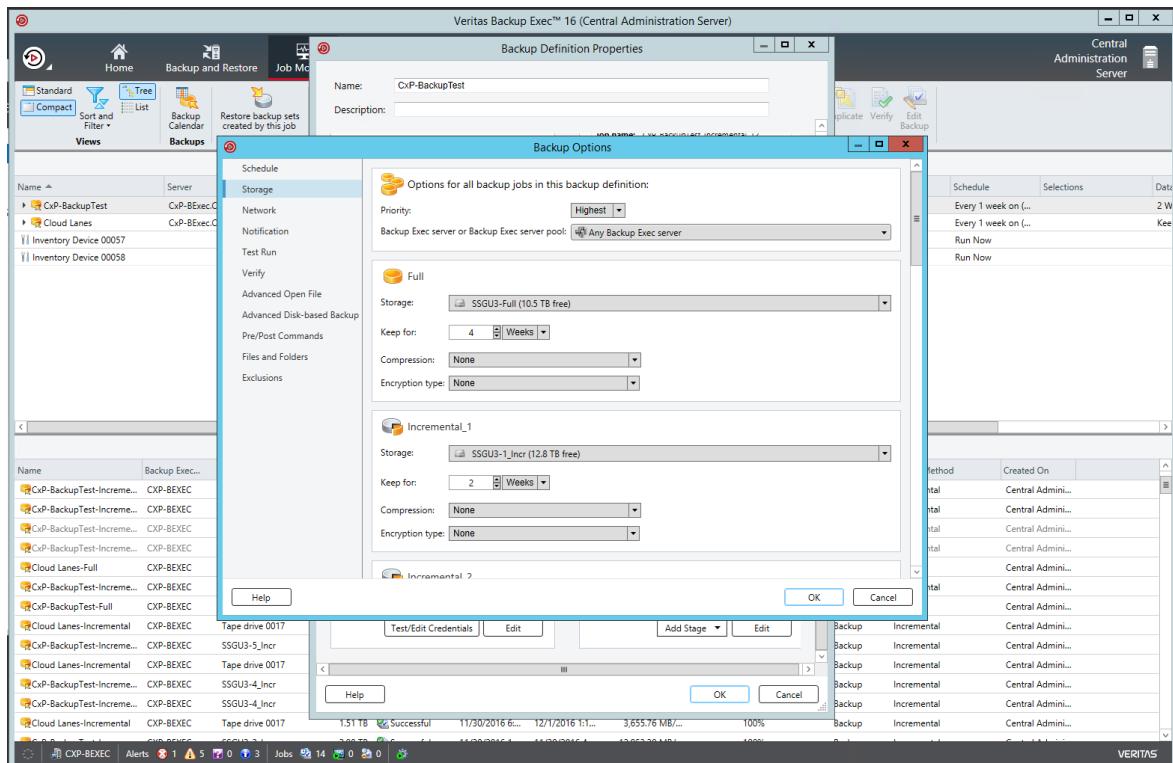


2. In the Backup Definition Properties dialog box, under Backup, select Edit.



3. Set up your full and incremental backups so that they meet your RPO and RTO requirements and conform to Veritas best practices.

4. In the Backup Options dialog box, select Storage.



5. Assign corresponding StorSimple volumes to your backup schedule.

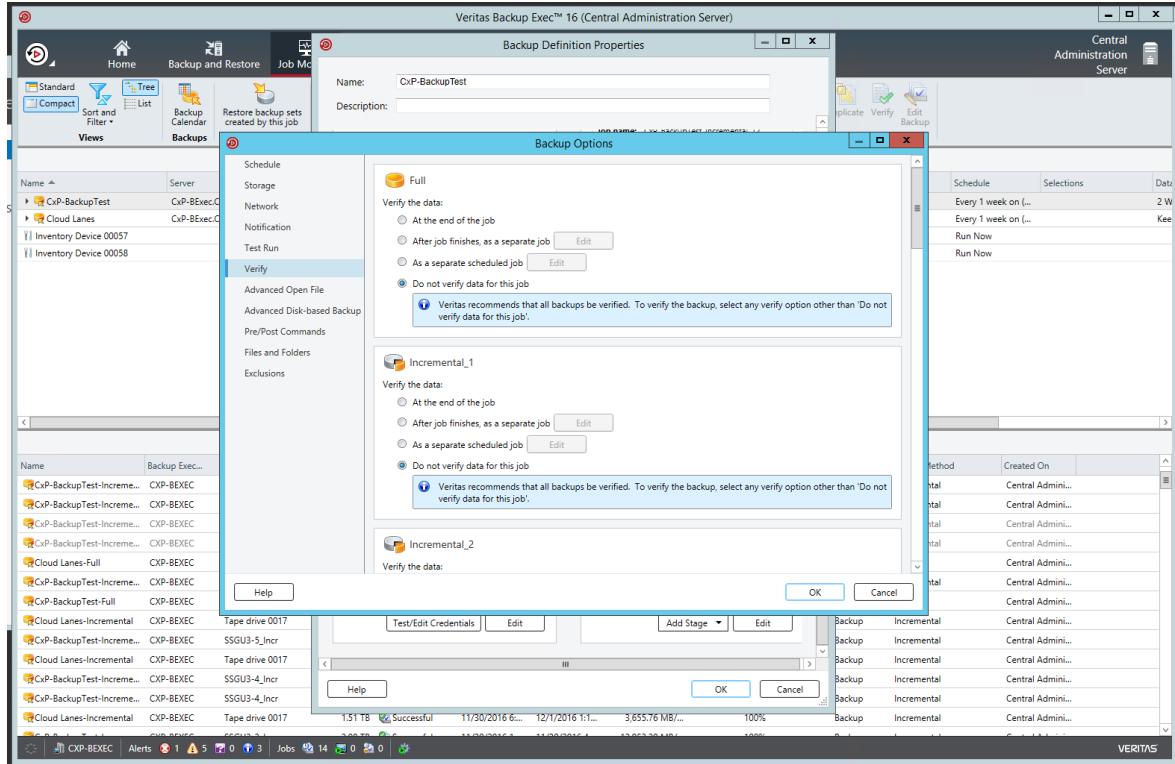
Note

Compression and Encryption type are set to None.

6. Under Verify, select the **Do not verify data for this job** check box. Using this option might affect StorSimple tiering.

! Note

Defragmentation, indexing, and background verification negatively affect the StorSimple tiering.



7. When you've set up the rest of your backup options to meet your requirements, select OK to finish.

Set up StorSimple as a secondary backup target

! Note

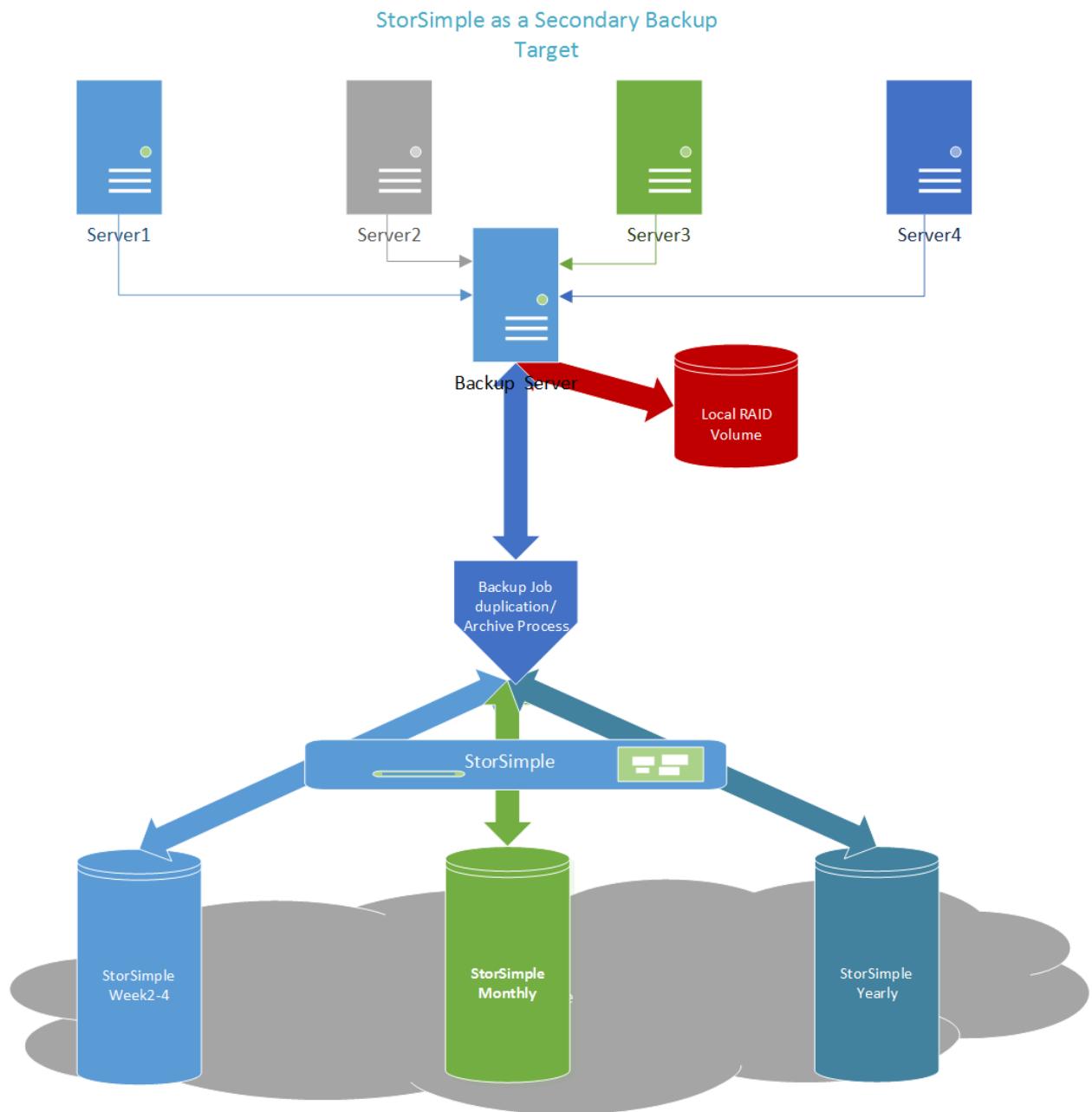
Data restores from a backup that has been tiered to the cloud occur at cloud speeds.

In this model, you must have a storage media (other than StorSimple) to serve as a temporary cache. For example, you can use a redundant array of independent disks

(RAID) volume to accommodate space, input/output (I/O), and bandwidth. We recommend using RAID 5, 50, and 10.

The following figure shows typical short-term retention local (to the server) volumes and long-term retention archives volumes. In this scenario, all backups run on the local (to the server) RAID volume. These backups are periodically duplicated and archived to an archives volume. It is important to size your local (to the server) RAID volume so that it can handle your short-term retention capacity and performance requirements.

StorSimple as a secondary backup target GFS example



The following table shows how to set up backups to run on the local and StorSimple disks. It includes individual and total capacity requirements.

Backup configuration and capacity requirements

Backup type and retention	Configured storage	Size (TiB)	GFS multiplier	Total capacity* (TiB)
Week 1 (full and incremental)	Local disk (short-term)	1	1	1
StorSimple weeks 2-4	StorSimple disk (long-term)	1	4	4
Monthly full	StorSimple disk (long-term)	1	12	12
Yearly full	StorSimple disk (long-term)	1	1	1
GFS volumes size requirement				18*

* Total capacity includes 17 TiB of StorSimple disks and 1 TiB of local RAID volume.

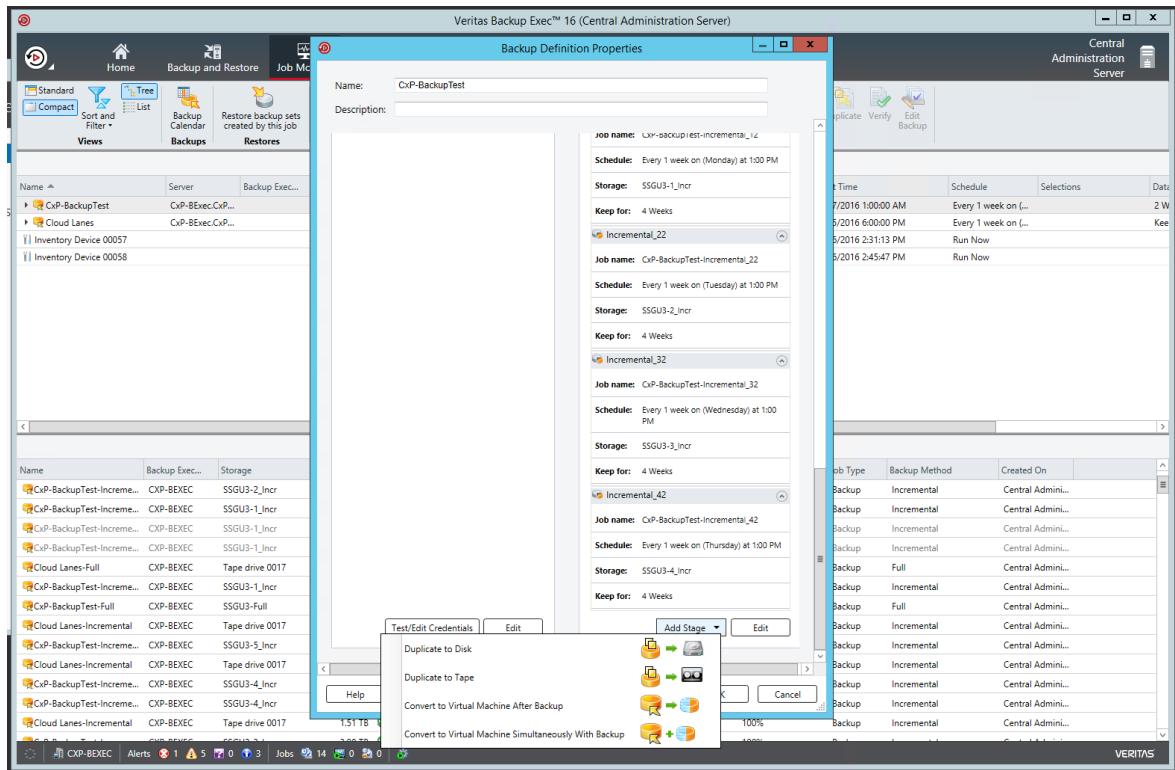
GFS example schedule: GFS rotation weekly, monthly, and yearly schedule

Week	Full	Incremental day 1	Incremental day 2	Incremental day 3	Incremental day 4	Incremental day 5
Week 1	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume
Week 2	StorSimple weeks 2-4					
Week 3	StorSimple weeks 2-4					
Week 4	StorSimple weeks 2-4					
Monthly	StorSimple monthly					
Yearly	StorSimple yearly					

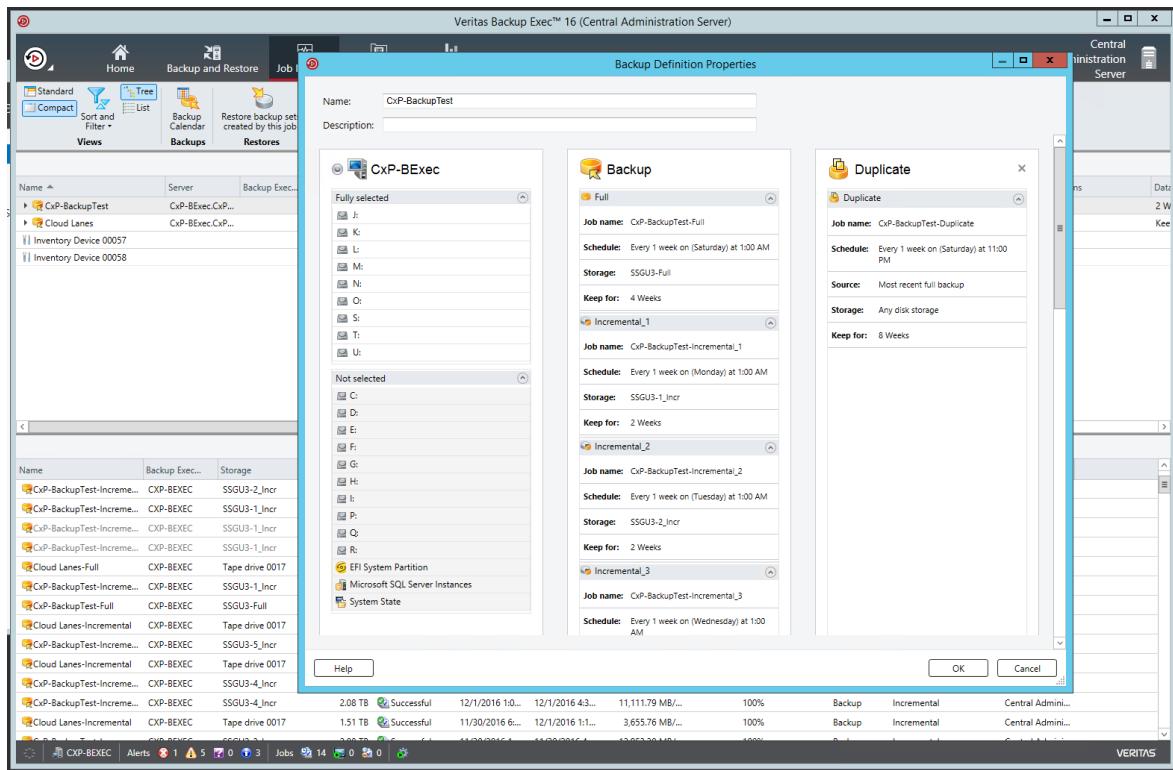
Assign StorSimple volumes to a Backup Exec archive and deduplication job

To assign StorSimple volumes to a Backup Exec archive and duplication job

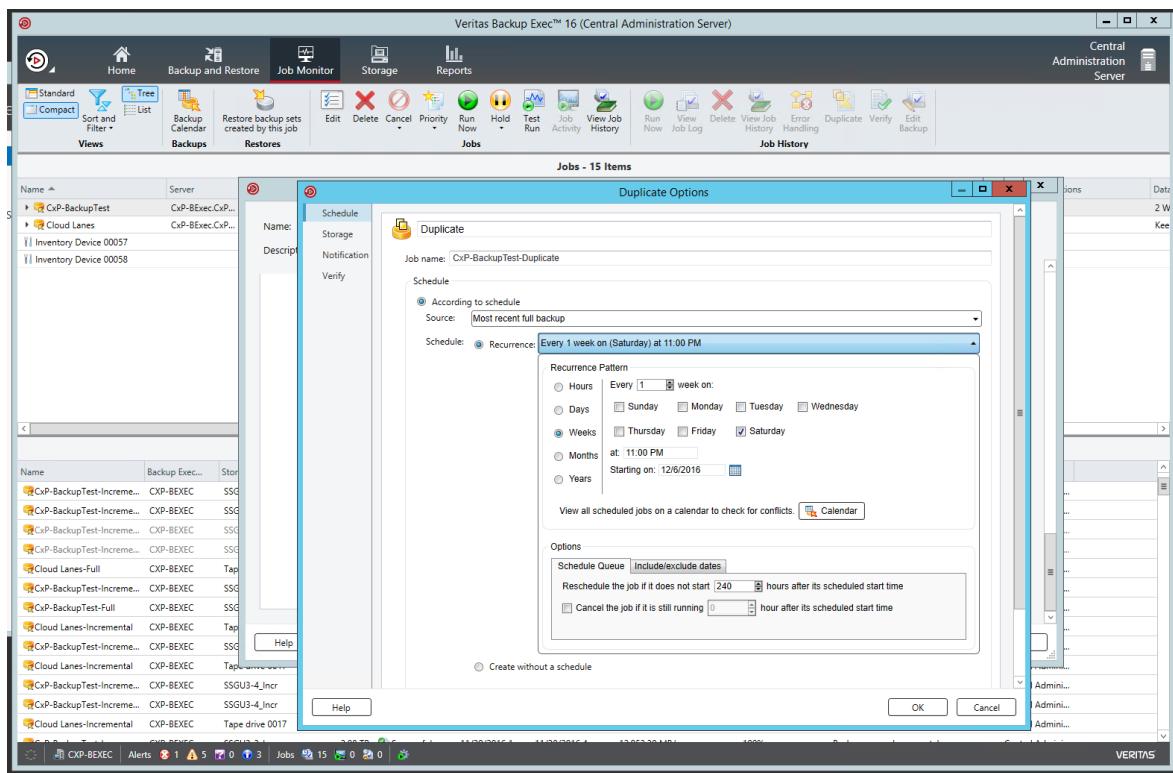
1. In the Backup Exec management console, right-click the job that you want to archive to a StorSimple volume, and then select **Backup Definition Properties > Edit**.



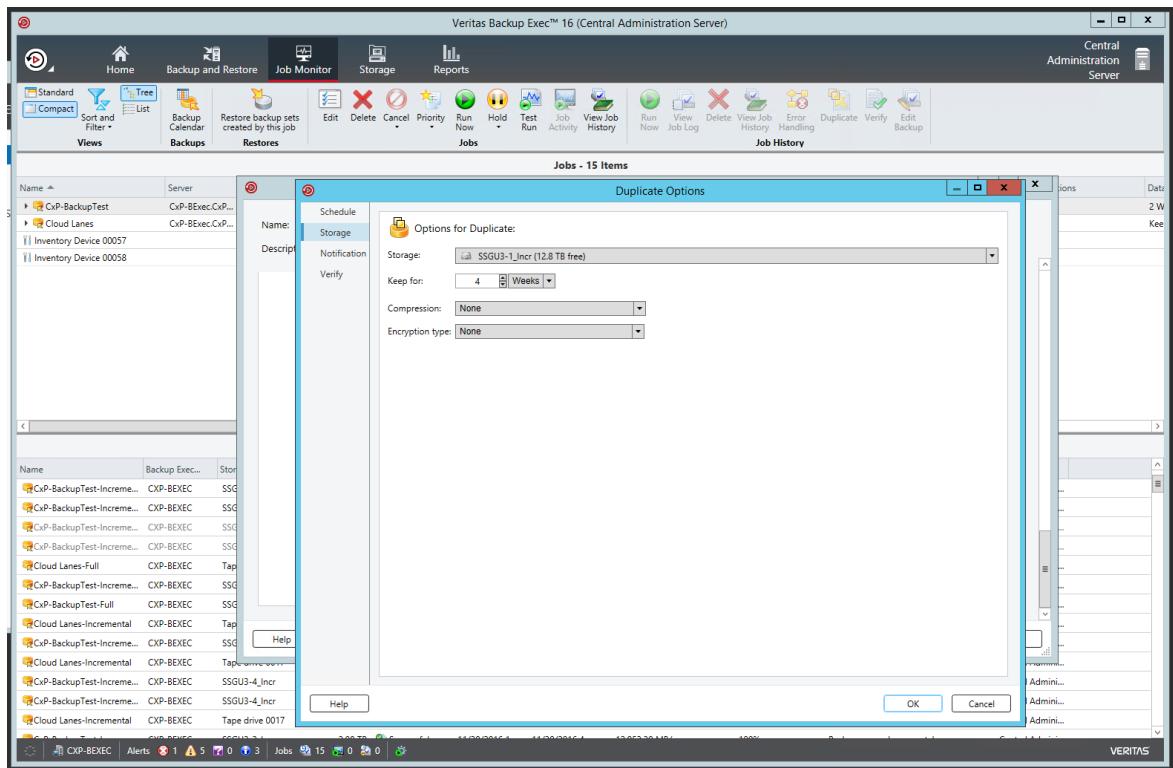
2. Select **Add Stage > Duplicate to Disk > Edit**.



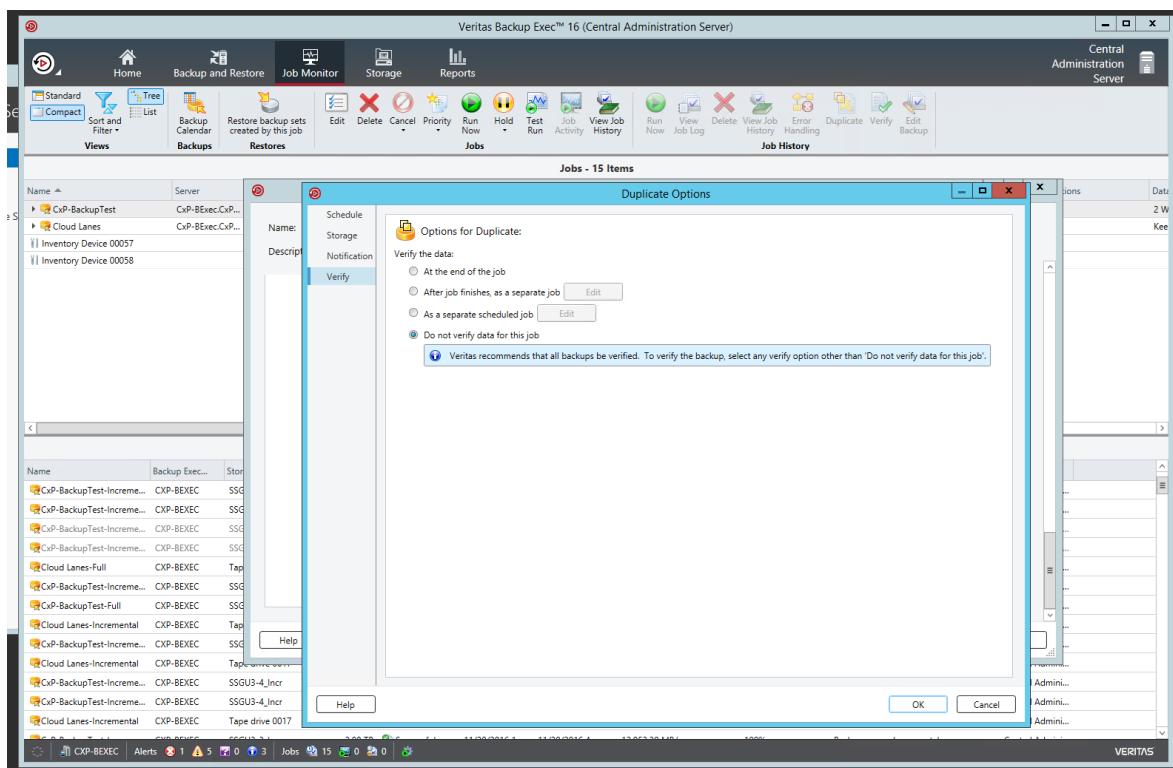
3. In the Duplicate Options dialog box, select the values that you want to use for Source and Schedule.



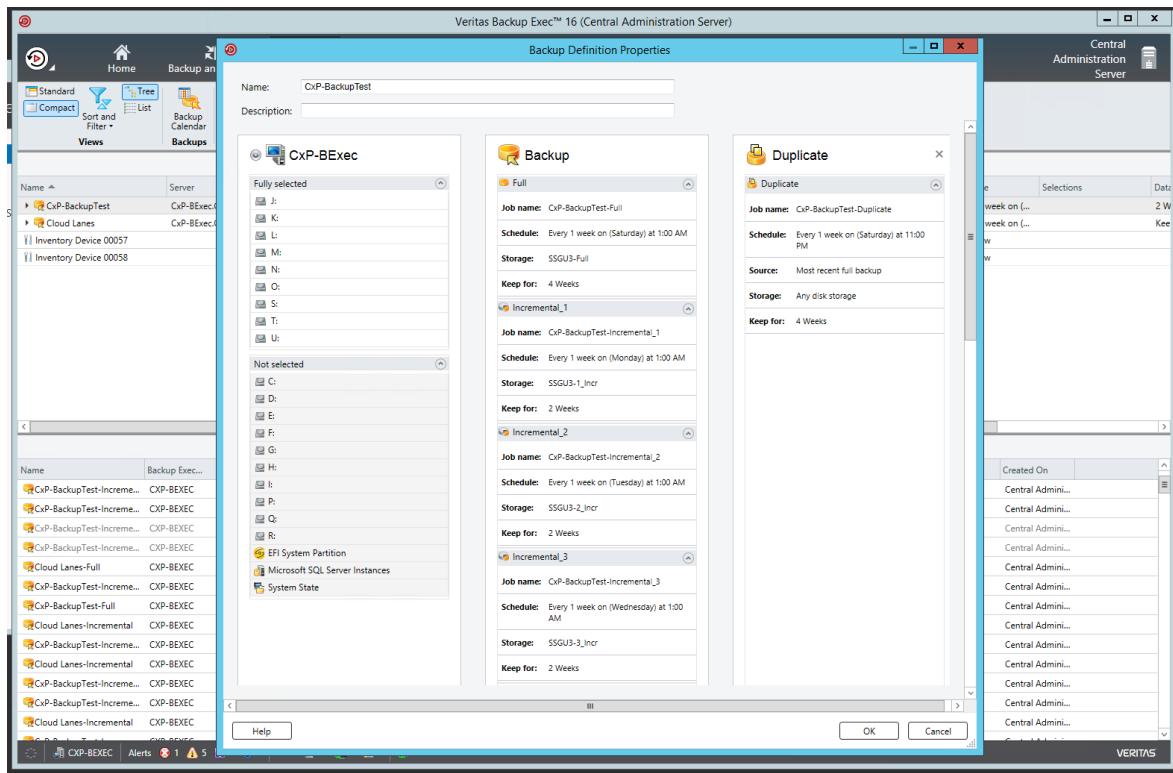
4. In the Storage drop-down list, select the StorSimple volume where you want the archive job to store the data.



5. Select Verify, and then select the Do not verify data for this job check box.



6. Select OK.



7. In the **Backup** column, add a new stage. For the source, use **incremental**. For the target, choose the StorSimple volume where the incremental backup job is archived. Repeat steps 1-6.

StorSimple cloud snapshots

StorSimple cloud snapshots protect the data that resides in your StorSimple device. Creating a cloud snapshot is equivalent to shipping local backup tapes to an offsite facility. If you use Azure geo-redundant storage, creating a cloud snapshot is equivalent to shipping backup tapes to multiple sites. If you need to restore a device after a disaster, you might bring another StorSimple device online and do a failover. After the failover, you would be able to access the data (at cloud speeds) from the most recent cloud snapshot.

The following section describes how to create a short script to start and delete StorSimple cloud snapshots during backup post-processing.

Note

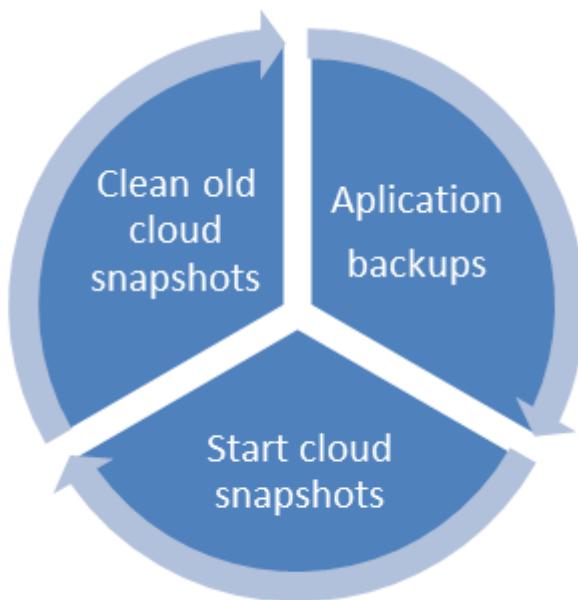
Snapshots that are manually or programmatically created do not follow the StorSimple snapshot expiration policy. These snapshots must be manually or programmatically deleted.

Start and delete cloud snapshots by using a script

Note

Carefully assess the compliance and data retention repercussions before you delete a StorSimple snapshot. For more information about how to run a post-backup script, see the [Backup Exec documentation](#).

Backup lifecycle



Requirements

- The server that runs the script must have access to Azure cloud resources.
- The user account must have the necessary permissions.
- A StorSimple backup policy with the associated StorSimple volumes must be set up but not turned on.
- You'll need the StorSimple resource name, registration key, device name, and backup policy ID.

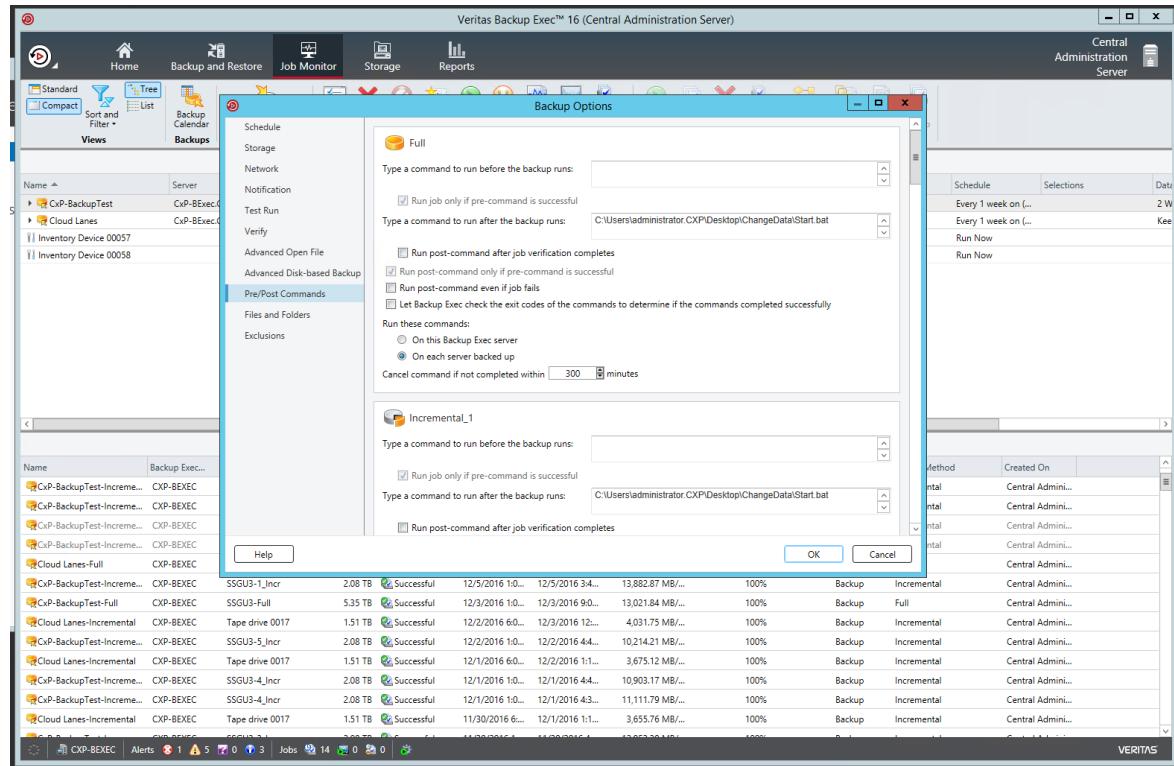
To start or delete a cloud snapshot

1. [Install Azure PowerShell](#).
2. Download and setup [Manage-CloudSnapshots.ps1](#) PowerShell script.
3. On the server that runs the script, run PowerShell as an administrator. Ensure that you run the script with `-WhatIf $true` to see what changes the script will make. Once the validation is complete, pass `-WhatIf $false`. Run the below command:

PowerShell

```
.\Manage-CloudSnapshots.ps1 -SubscriptionId [Subscription Id] -TenantId  
[Tenant ID] -ResourceGroupName [Resource Group Name] -ManagerName  
[StorSimple Device Manager Name] -DeviceName [device name] -  
BackupPolicyName [backup policyname] -RetentionInDays [Retention days]  
-WhatIf [$true or $false]
```

4. Add the script to your backup job in Backup Exec by editing your Backup Exec job options' pre-processing and post-processing commands.



ⓘ Note

We recommend that you run your StorSimple cloud snapshot backup policy as a post-processing script at the end of your daily backup job. For more information about how to back up and restore your backup application environment to help you meet your RPO and RTO, please consult with your backup architect.

StorSimple as a restore source

Restores from a StorSimple device work like restores from any block storage device. Restores of data that is tiered to the cloud occurs at cloud speeds. For local data, restores occur at the local disk speed of the device. For information about how to perform a restore, see the Backup Exec documentation. We recommend that you conform to Backup Exec restore best practices.

StorSimple failover and disaster recovery

ⓘ Note

For backup target scenarios, StorSimple Cloud Appliance is not supported as a restore target.

A disaster can be caused by a variety of factors. The following table lists common disaster recovery scenarios.

Scenario	Impact	How to recover	Notes
StorSimple device failure	Backup and restore operations are interrupted.	Replace the failed device and perform StorSimple failover and disaster recovery .	If you need to perform a restore after device recovery, full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds. The indexing and cataloging rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier, which might be a time-consuming process.
Backup Exec server failure	Backup and restore operations are interrupted.	Rebuild the backup server and perform database restore as detailed in How to do a manual Backup and Restore of Backup Exec (BEDB) database .	You must rebuild or restore the Backup Exec server at the disaster recovery site. Restore the database to the most recent point. If the restored Backup Exec database is not in sync with your latest backup jobs, indexing and cataloging is required. This index and catalog rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier. This makes it further time-intensive.
Site failure that results in the loss of both the backup server and StorSimple	Backup and restore operations are interrupted.	Restore StorSimple first, and then restore Backup Exec. If you need to perform a restore after device recovery, the full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds.	

References

The following documents were referenced for this article:

- [StorSimple multipath I/O setup](#)
- [Storage scenarios: Thin provisioning](#)
- [Using GPT drives](#)
- [Set up shadow copies for shared folders](#)

Next steps

- Learn more about how to [restore from a backup set](#).
 - Learn more about how to perform [device failover and disaster recovery](#).
-

Additional resources

Training

Module

[Introduction to Azure Backup - Training](#)

Evaluate whether Azure Backup is appropriate to use for your backup needs and describe how the features of Azure Backup work to provide backup solutions for your needs.

StorSimple as a backup target with NetBackup

Article • 08/22/2022 • 20 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Azure StorSimple is a hybrid cloud storage solution from Microsoft. StorSimple addresses the complexities of exponential data growth by using an Azure storage account as an extension of the on-premises solution, and automatically tiering data across on-premises storage and cloud storage.

In this article, we discuss StorSimple integration with Veritas NetBackup, and best practices for integrating both solutions. We also make recommendations on how to set up Veritas NetBackup to best integrate with StorSimple. We defer to Veritas best practices, backup architects, and administrators for the best way to set up Veritas NetBackup to meet individual backup requirements and service-level agreements (SLAs).

Although we illustrate configuration steps and key concepts, this article is by no means a step-by-step configuration or installation guide. We assume that the basic components and infrastructure are in working order and ready to support the concepts that we describe.

Who should read this?

The information in this article will be most helpful to backup administrators, storage administrators, and storage architects who have knowledge of storage, Windows Server 2012 R2, Ethernet, cloud services, and Veritas NetBackup.

Supported versions

- NetBackup 7.7.x and later versions
- StorSimple Update 3 and later versions

Why StorSimple as a backup target?

StorSimple is a good choice for a backup target because:

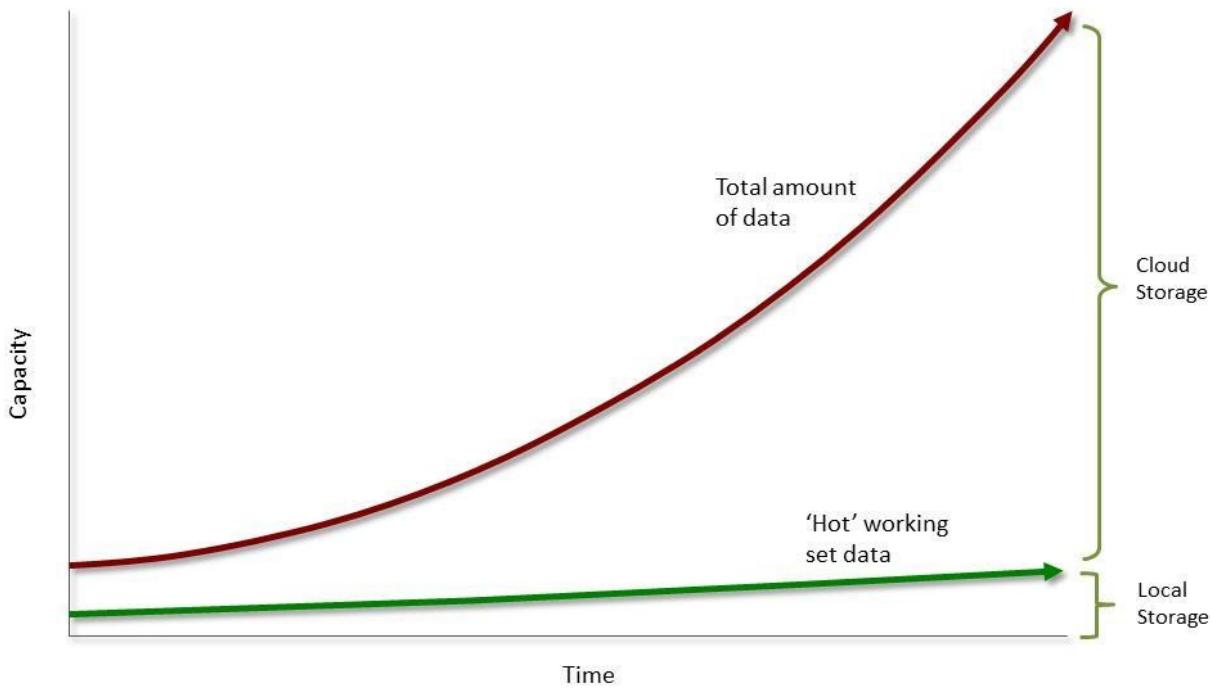
- It provides standard, local storage for backup applications to use as a fast backup destination, without any changes. You also can use StorSimple for a quick restore of recent backups.
- Its cloud tiering is seamlessly integrated with an Azure cloud storage account to use cost-effective Azure Storage.
- It automatically provides offsite storage for disaster recovery.

Key concepts

As with any storage solution, a careful assessment of the solution's storage performance, SLAs, rate of change, and capacity growth needs is critical to success. The main idea is that by introducing a cloud tier, your access times and throughputs to the cloud play a fundamental role in the ability of StorSimple to do its job.

StorSimple is designed to provide storage to applications that operate on a well-defined working set of data (hot data). In this model, the working set of data is stored on the local tiers, and the remaining nonworking/cold/archived set of data is tiered to the cloud. This model is represented in the following figure. The nearly flat green line represents the data stored on the local tiers of the StorSimple device. The red line represents the total amount of data stored on the StorSimple solution across all tiers. The space between the flat green line and the exponential red curve represents the total amount of data stored in the cloud.

StorSimple tiering



With this architecture in mind, you will find that StorSimple is ideally suited to operate as a backup target. You can use StorSimple to:

- Perform your most frequent restores from the local working set of data.
- Use the cloud for offsite disaster recovery and older data, where restores are less frequent.

StorSimple benefits

StorSimple provides an on-premises solution that is seamlessly integrated with Microsoft Azure, by taking advantage of seamless access to on-premises and cloud storage.

StorSimple uses automatic tiering between the on-premises device, which has solid-state device (SSD) and serial-attached SCSI (SAS) storage, and Azure Storage. Automatic tiering keeps frequently accessed data local, on the SSD and SAS tiers. It moves infrequently accessed data to Azure Storage.

StorSimple offers these benefits:

- Unique deduplication and compression algorithms that use the cloud to achieve unprecedented deduplication levels
- High availability
- Geo-replication by using Azure geo-replication
- Azure integration
- Data encryption in the cloud

- Improved disaster recovery and compliance

Although StorSimple presents two main deployment scenarios (primary backup target and secondary backup target), fundamentally, it's a plain, block storage device. StorSimple does all the compression and deduplication. It seamlessly sends and retrieves data between the cloud and the application and file system.

For more information about StorSimple, see [StorSimple 8000 series: Hybrid cloud storage solution](#). Also, you can review the [technical StorSimple 8000 series specifications](#).

Important

Using a StorSimple device as a backup target is supported only for StorSimple 8000 Update 3 and later versions.

Architecture overview

The following tables show the device model-to-architecture initial guidance.

StorSimple capacities for local and cloud storage

Storage capacity	8100	8600
Local storage capacity	< 10 TiB*	< 20 TiB*
Cloud storage capacity	> 200 TiB*	> 500 TiB*

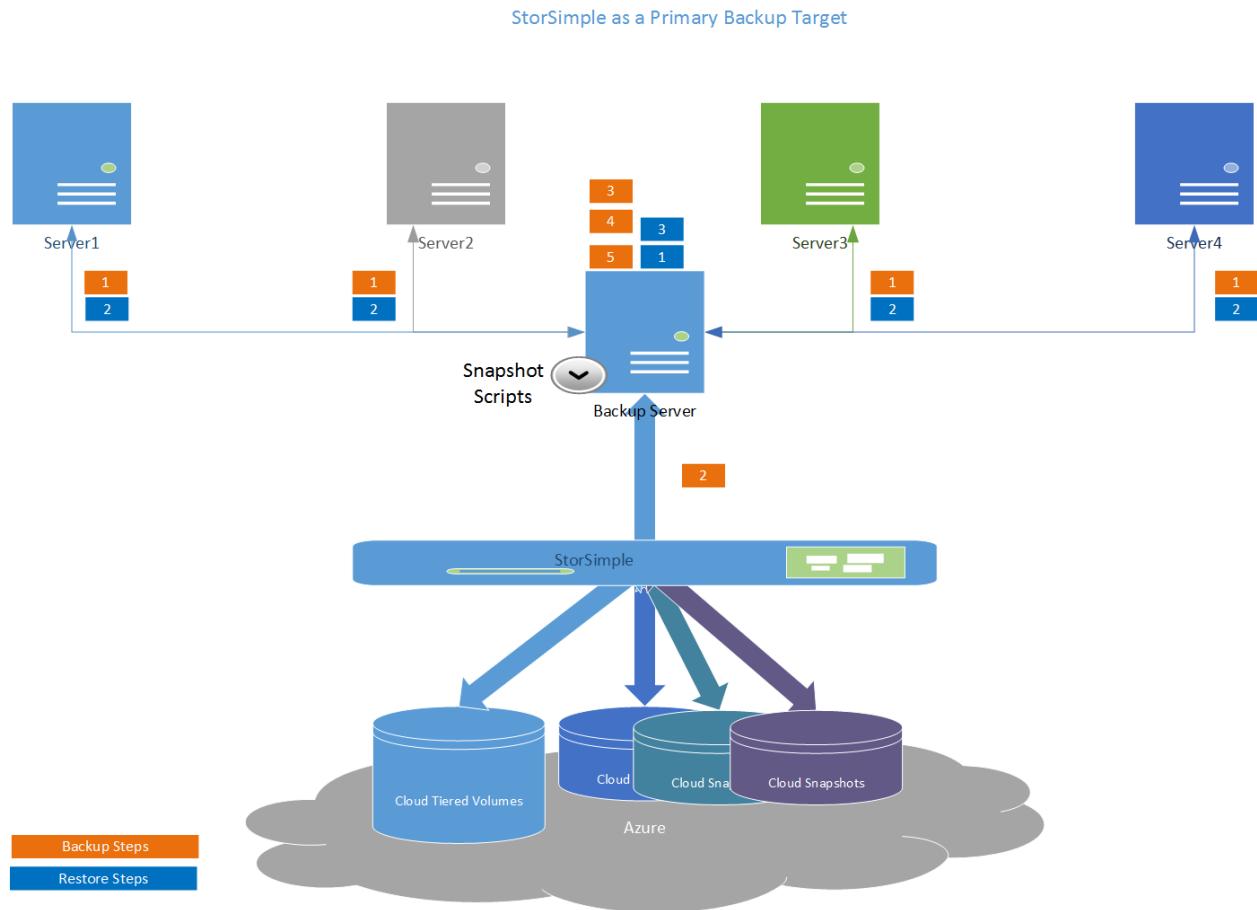
* Storage size assumes no deduplication or compression.

StorSimple capacities for primary and secondary backups

Backup scenario	Local storage capacity	Cloud storage capacity
Primary backup	Recent backups stored on local storage for fast recovery to meet recovery point objective (RPO)	Backup history (RPO) fits in cloud capacity
Secondary backup	Secondary copy of backup data can be stored in cloud capacity	N/A

StorSimple as a primary backup target

In this scenario, StorSimple volumes are presented to the backup application as the sole repository for backups. The following figure shows a solution architecture in which all backups use StorSimple tiered volumes for backups and restores.



Primary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to the StorSimple tiered volumes.
3. The backup server updates the catalog database, and then finishes the backup job.
4. A snapshot script triggers the StorSimple snapshot manager (start or delete).
5. The backup server deletes expired backups based on a retention policy.

Primary target restore logical steps

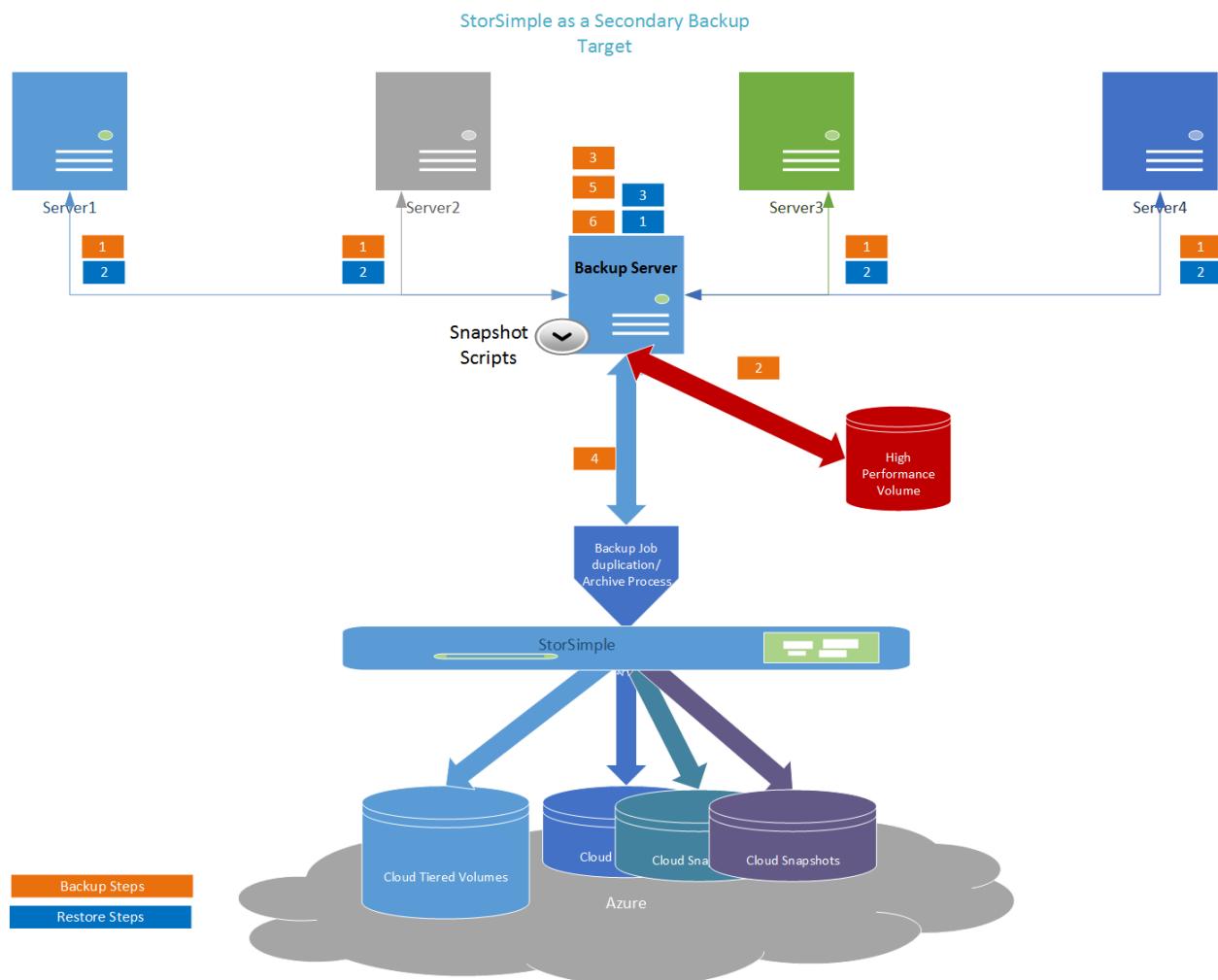
1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

StorSimple as a secondary backup target

In this scenario, StorSimple volumes primarily are used for long-term retention or archiving.

The following figure shows an architecture in which initial backups and restores target a high-performance volume. These backups are copied and archived to a StorSimple tiered volume on a set schedule.

It's important to size your high-performance volume so that it can handle your retention policy capacity and performance requirements.



Secondary target backup logical steps

1. The backup server contacts the target backup agent, and the backup agent transmits data to the backup server.
2. The backup server writes data to high-performance storage.
3. The backup server updates the catalog database, and then finishes the backup job.
4. The backup server copies backups to StorSimple based on a retention policy.
5. A snapshot script triggers the StorSimple snapshot manager (start or delete).
6. The backup server deletes the expired backups based on a retention policy.

Secondary target restore logical steps

1. The backup server starts restoring the appropriate data from the storage repository.
2. The backup agent receives the data from the backup server.
3. The backup server finishes the restore job.

Deploy the solution

Deploying this solution requires three steps:

1. Prepare the network infrastructure.
2. Deploy your StorSimple device as a backup target.
3. Deploy Veritas NetBackup.

Each step is discussed in detail in the following sections.

Set up the network

Because StorSimple is a solution that's integrated with the Azure cloud, StorSimple requires an active and working connection to the Azure cloud. This connection is used for operations like cloud snapshots, data management, and metadata transfer, and to tier older, less accessed data to Azure cloud storage.

For the solution to perform optimally, we recommend that you follow these networking best practices:

- The link that connects the StorSimple tiering to Azure must meet your bandwidth requirements. To achieve this, apply the proper Quality of Service (QoS) level to your infrastructure switches to match your RPO and recovery time objective (RTO) SLAs.
- Maximum Azure Blob storage access latencies should be around 80 ms.

Deploy StorSimple

For step-by-step StorSimple deployment guidance, see [Deploy your on-premises StorSimple device](#).

Deploy NetBackup

For step-by-step NetBackup 7.7.x deployment guidance, see the [NetBackup 7.7.x documentation](#).

Set up the solution

In this section, we demonstrate some configuration examples. The following examples and recommendations illustrate the most basic and fundamental implementation. This implementation might not apply directly to your specific backup requirements.

Set up StorSimple

StorSimple deployment tasks	Additional comments
Deploy your on-premises StorSimple device.	Supported versions: Update 3 and later versions.
Turn on the backup target.	<p>Use these commands to turn on or turn off backup target mode, and to get status. For more information, see Connect remotely to a StorSimple device.</p> <p>To turn on backup mode: <code>Set-HCSBackupApplianceMode -enable</code>.</p> <p>To turn off backup mode: <code>Set-HCSBackupApplianceMode -disable</code>.</p> <p>To get the current state of backup mode settings: <code>Get-HCSBackupApplianceMode</code>.</p>
Create a common volume container for your volume that stores the backup data. All data in a volume container is deduplicated.	StorSimple volume containers define deduplication domains.
Create StorSimple volumes.	<p>Create volumes with sizes as close to the anticipated usage as possible, because volume size affects cloud snapshot duration time. For information about how to size a volume, read about retention policies.</p> <p>Use StorSimple tiered volumes, and select the Use this volume for less frequently accessed archival data check box.</p> <p>Using only locally pinned volumes is not supported.</p>
Create a unique StorSimple backup policy for all the backup target volumes.	A StorSimple backup policy defines the volume consistency group.
Disable the schedule as the snapshots expire.	Snapshots are triggered as a post-processing operation.

Set up the host backup server storage

Set up the host backup server storage according to these guidelines:

- Don't use spanned volumes (created by Windows Disk Management); spanned volumes are not supported.
- Format your volumes using NTFS with 64-KB allocation size.
- Map the StorSimple volumes directly to the NetBackup server.
 - Use iSCSI for physical servers.
 - Use pass-through disks for virtual servers.

Best practices for StorSimple and NetBackup

Set up your solution according to the guidelines in the following few sections.

Operating system best practices

- Disable Windows Server encryption and deduplication for the NTFS file system.
- Disable Windows Server defragmentation on the StorSimple volumes.
- Disable Windows Server indexing on the StorSimple volumes.
- Run an antivirus scan at the source host (not against the StorSimple volumes).
- Turn off the default [Windows Server maintenance](#) in Task Manager. Do this in one of the following ways:
 - Turn off the Maintenance configurator in Windows Task Scheduler.
 - Download [PsExec](#) from Windows Sysinternals. After you download PsExec, run Windows PowerShell as an administrator, and type:

PowerShell

```
psexec \\%computername% -s schtasks /change /tn  
"MicrosoftWindowsTaskSchedulerMaintenance Configurator" /disable
```

StorSimple best practices

- Be sure that the StorSimple device is updated to [Update 3 or later](#).
- Isolate iSCSI and cloud traffic. Use dedicated iSCSI connections for traffic between StorSimple and the backup server.
- Be sure that your StorSimple device is a dedicated backup target. Mixed workloads are not supported because they affect your RTO and RPO.

NetBackup best practices

- The NetBackup database should be local to the server and not reside on a StorSimple volume.
- For disaster recovery, back up the NetBackup database on a StorSimple volume.
- We support NetBackup full and incremental backups (also referred to as differential incremental backups in NetBackup) for this solution. We recommend that you do not use synthetic and cumulative incremental backups.
- Backup data files should contain only the data for a specific job. For example, no media appends across different jobs are allowed.

For the latest NetBackup settings and best practices for implementing these requirements, see the NetBackup documentation at www.veritas.com.

Retention policies

One of the most common backup retention policy types is a Grandfather, Father, and Son (GFS) policy. In a GFS policy, an incremental backup is performed daily and full backups are done weekly and monthly. This policy results in six StorSimple tiered volumes: one volume contains the weekly, monthly, and yearly full backups; the other five volumes store daily incremental backups.

In the following example, we use a GFS rotation. The example assumes the following:

- Non-deduped or compressed data is used.
- Full backups are 1 TiB each.
- Daily incremental backups are 500 GiB each.
- Four weekly backups are kept for a month.
- Twelve monthly backups are kept for a year.
- One yearly backup is kept for 10 years.

Based on the preceding assumptions, create a 26-TiB StorSimple tiered volume for the monthly and yearly full backups. Create a 5-TiB StorSimple tiered volume for each of the incremental daily backups.

Backup type retention	Size (TiB)	GFS multiplier*	Total capacity (TiB)
Weekly full	1	4	4
Daily incremental	0.5	20 (cycles equal number of weeks per month)	12 (2 for additional quota)
Monthly full	1	12	12

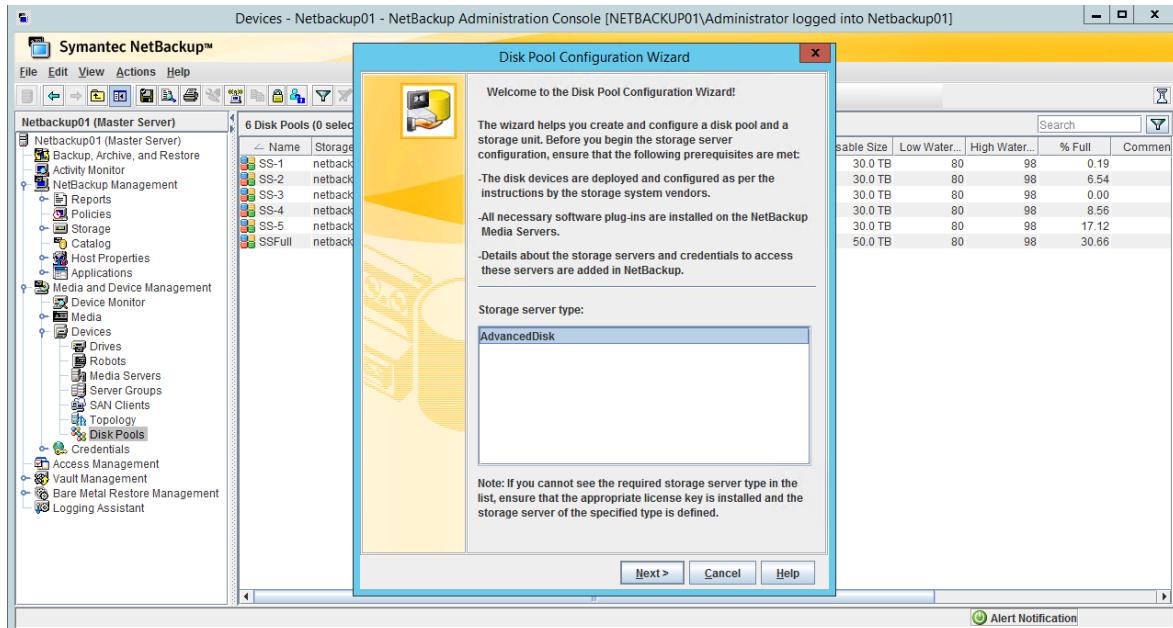
Backup type retention	Size (TiB)	GFS multiplier*	Total capacity (TiB)
Yearly full	1	10	10
GFS requirement		38	
Additional quota	4		42 total GFS requirement

* The GFS multiplier is the number of copies you need to protect and retain to meet your backup policy requirements.

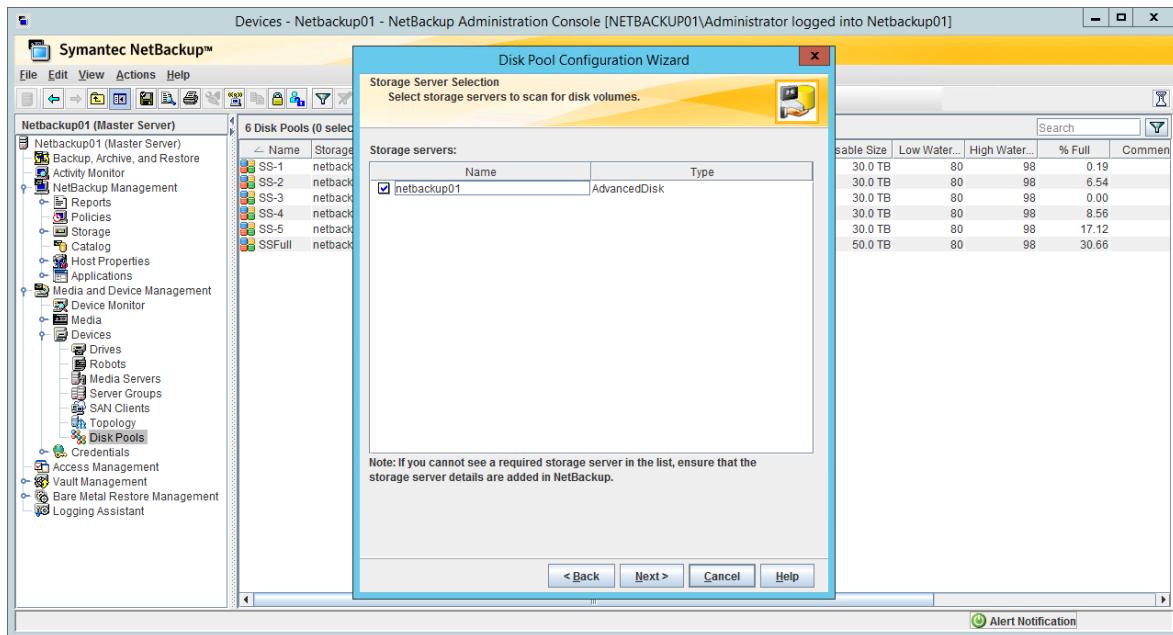
Set up NetBackup storage

To set up NetBackup storage

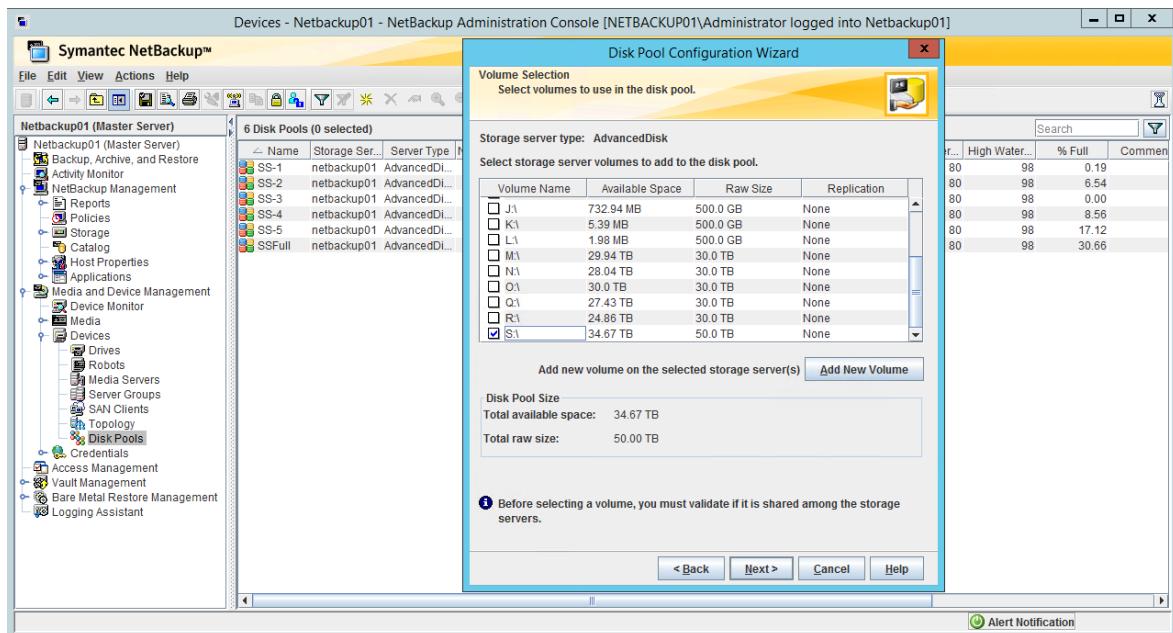
1. In the NetBackup Administration Console, select **Media and Device Management** > **Devices** > **Disk Pools**. In the Disk Pool Configuration Wizard, select the storage server type **AdvancedDisk**, and then select **Next**.



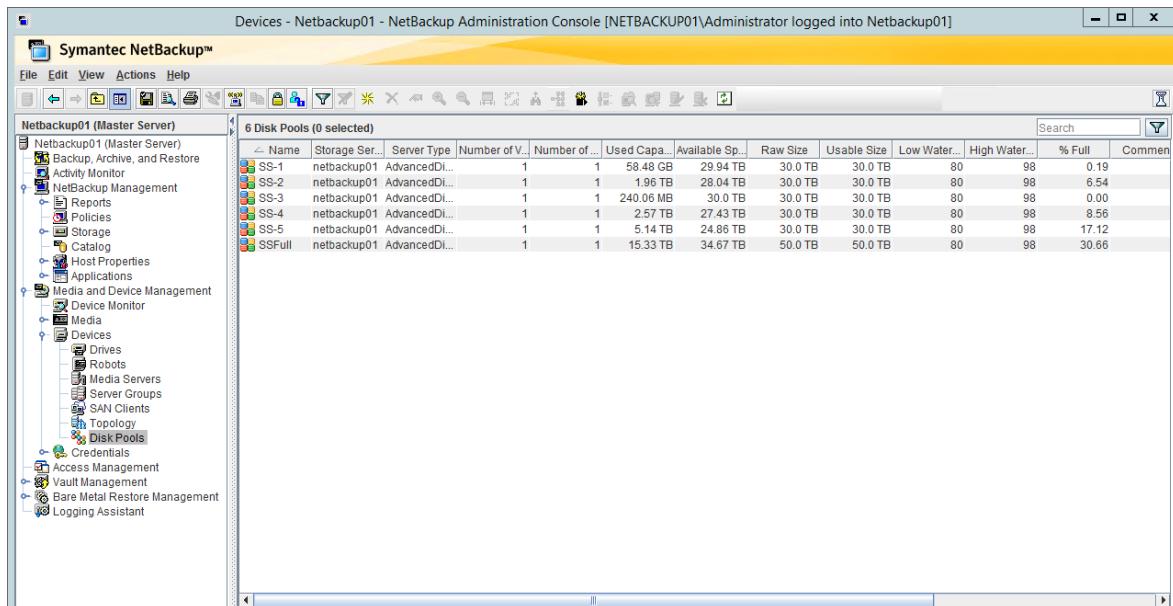
2. Select your server, and then select **Next**.



3. Select your StorSimple volume.



4. Enter a name for the backup target, and then select **Next > Next** to finish the wizard.
5. Review the settings, and then select **Finish**.
6. At the end of each volume assignment, change the storage device settings to match those recommended in [Best practices for StorSimple and NetBackup](#).
7. Repeat steps 1-6 until you are finished assigning your StorSimple volumes.



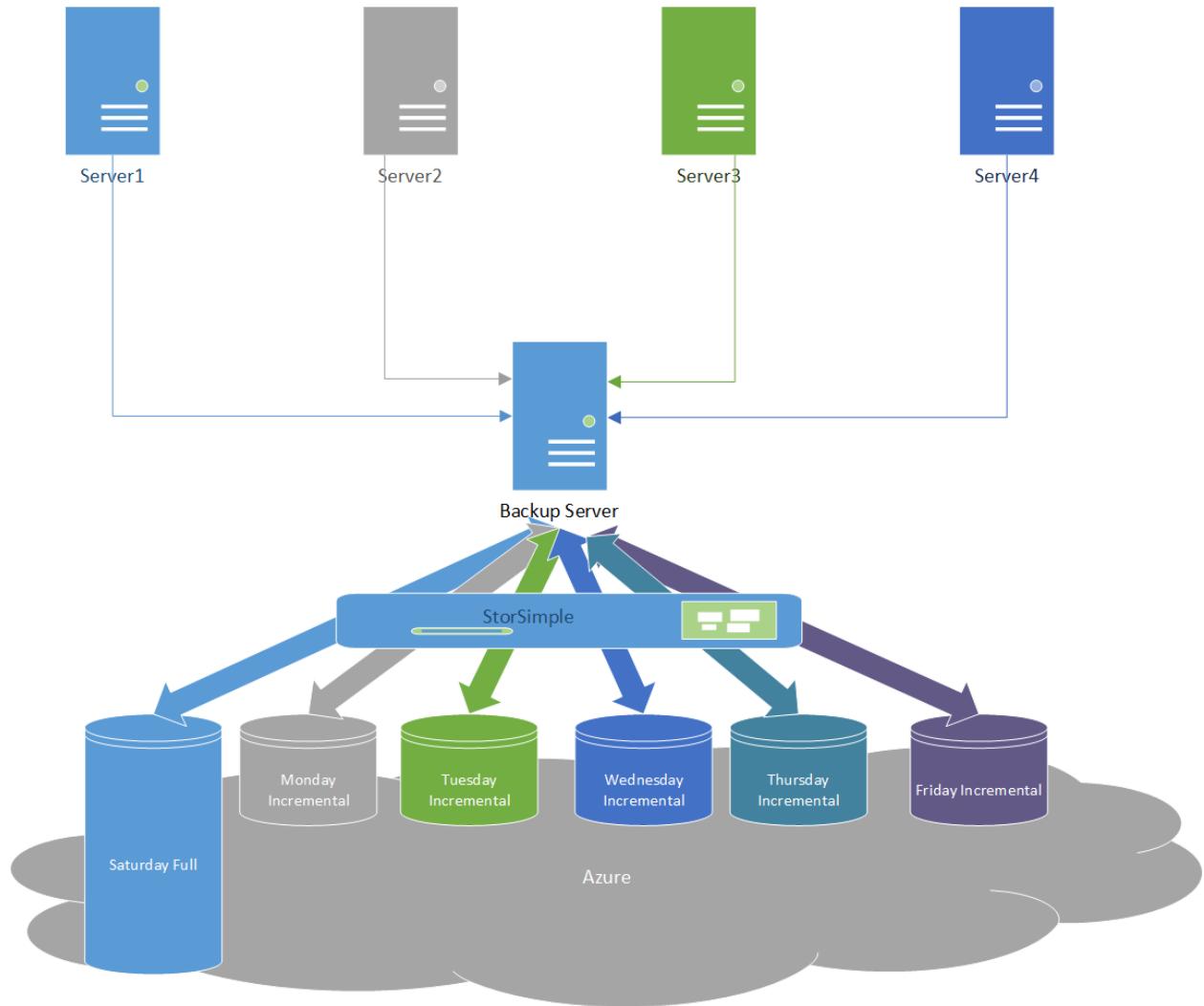
Set up StorSimple as a primary backup target

(!) Note

Data restores from a backup that has been tiered to the cloud occur at cloud speeds.

The following figure shows the mapping of a typical volume to a backup job. In this case, all the weekly backups map to the Saturday full disk, and the incremental backups map to Monday-Friday incremental disks. All the backups and restores are from a StorSimple tiered volume.

StorSimple as a Primary Backup Target



StorSimple as a primary backup target GFS schedule example

Here's an example of a GFS rotation schedule for four weeks, monthly, and yearly:

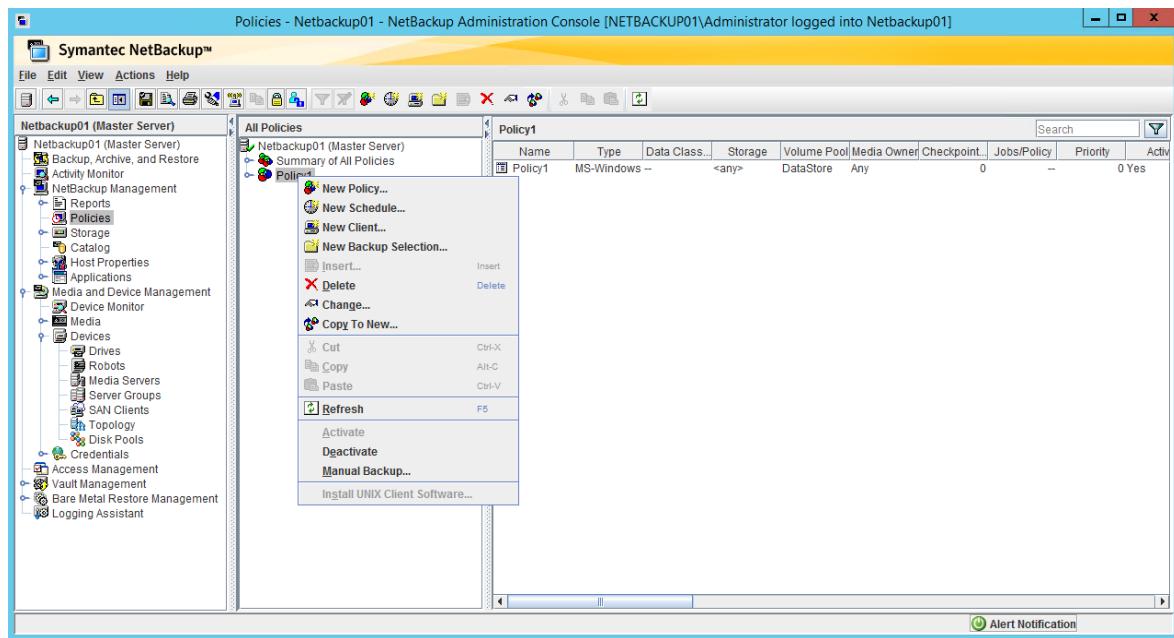
Frequency/backup type	Full	Incremental (days 1-5)
Weekly (weeks 1-4)	Saturday	Monday-Friday
Monthly	Saturday	
Yearly	Saturday	

Assigning StorSimple volumes to a NetBackup backup job

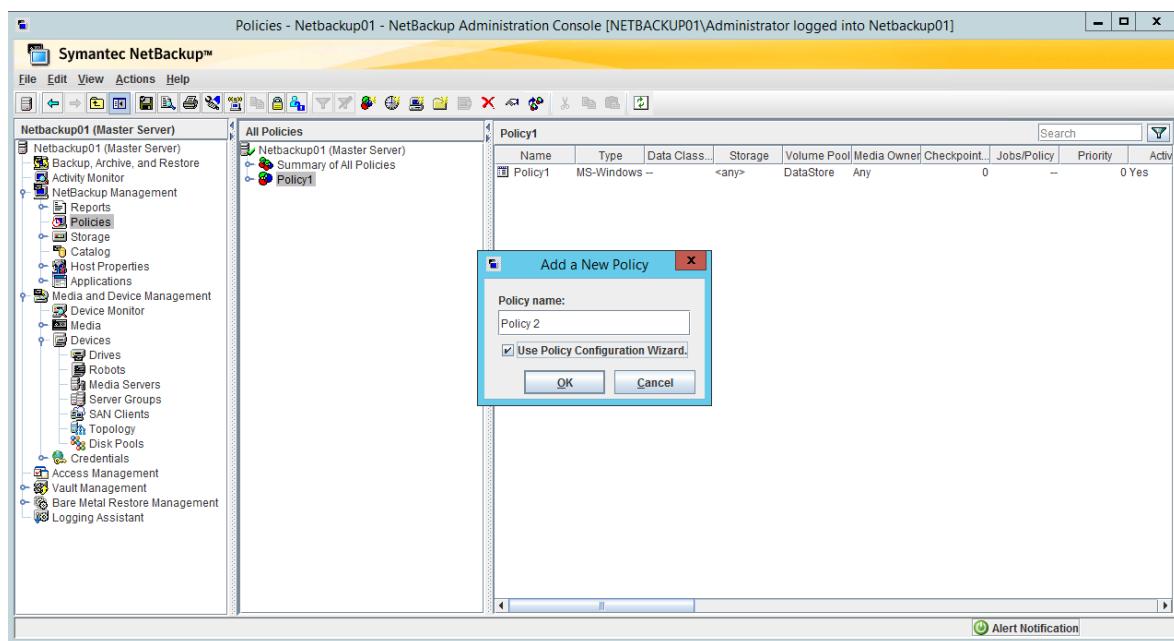
The following sequence assumes that NetBackup and the target host are configured in accordance with the NetBackup agent guidelines.

To assign StorSimple volumes to a NetBackup backup job

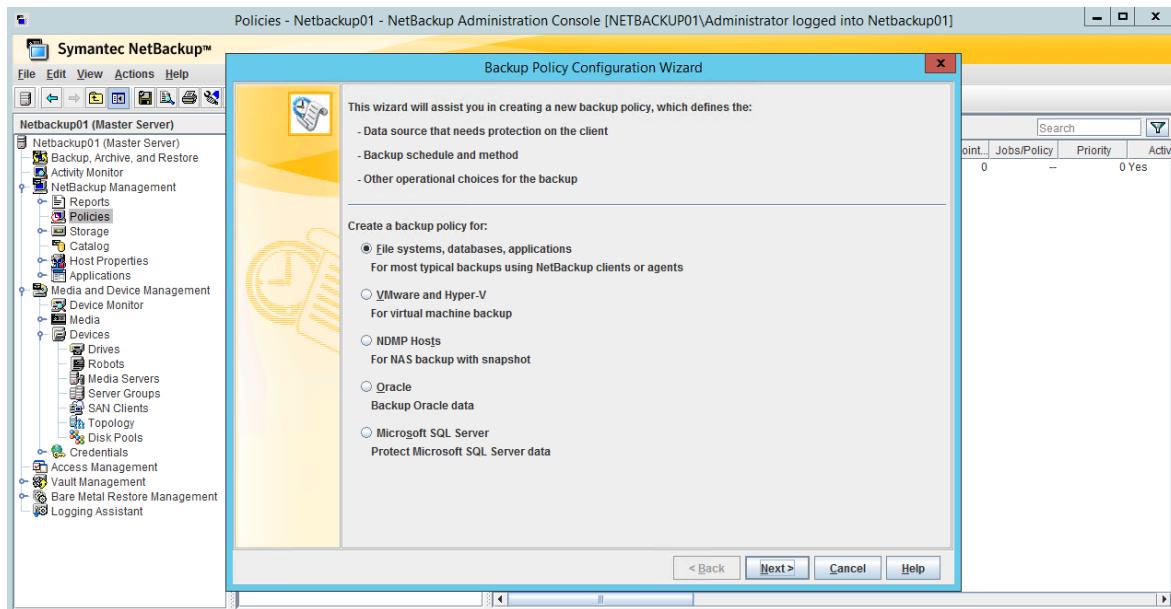
1. In the NetBackup Administration Console, select **NetBackup Management**, right-click **Policies**, and then select **New Policy**.



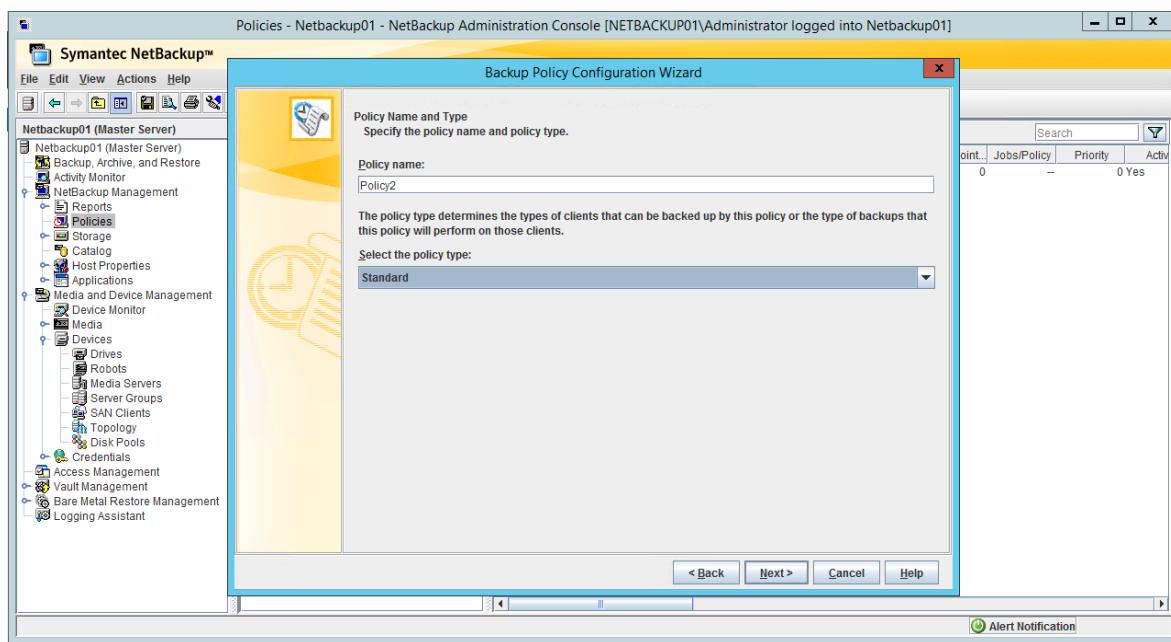
2. In the **Add a New Policy** dialog box, enter a name for the policy, and then select the **Use Policy Configuration Wizard** check box. Select **OK**.



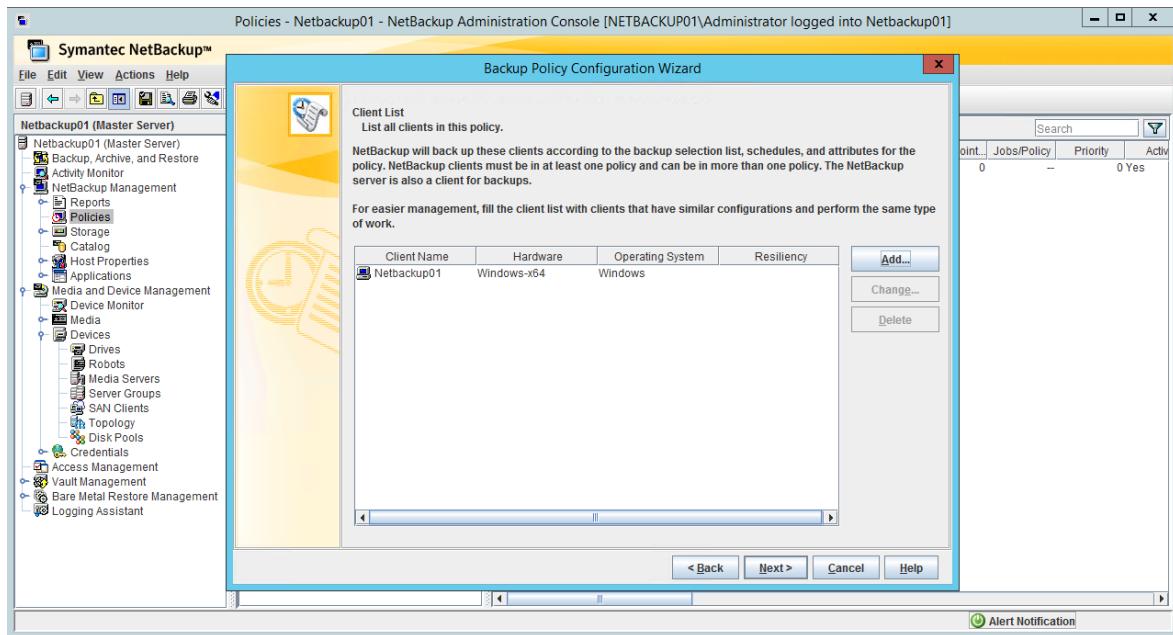
3. In the **Backup Policy Configuration Wizard**, elect the backup type you want, and then select **Next**.



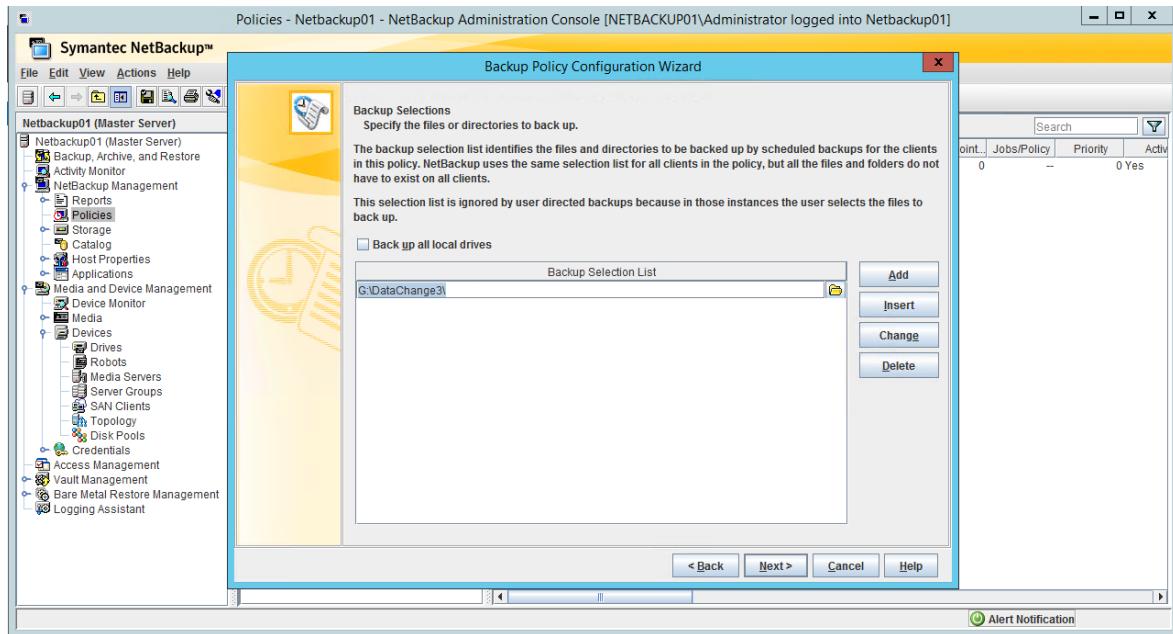
4. To set the policy type, select Standard, and then select Next.



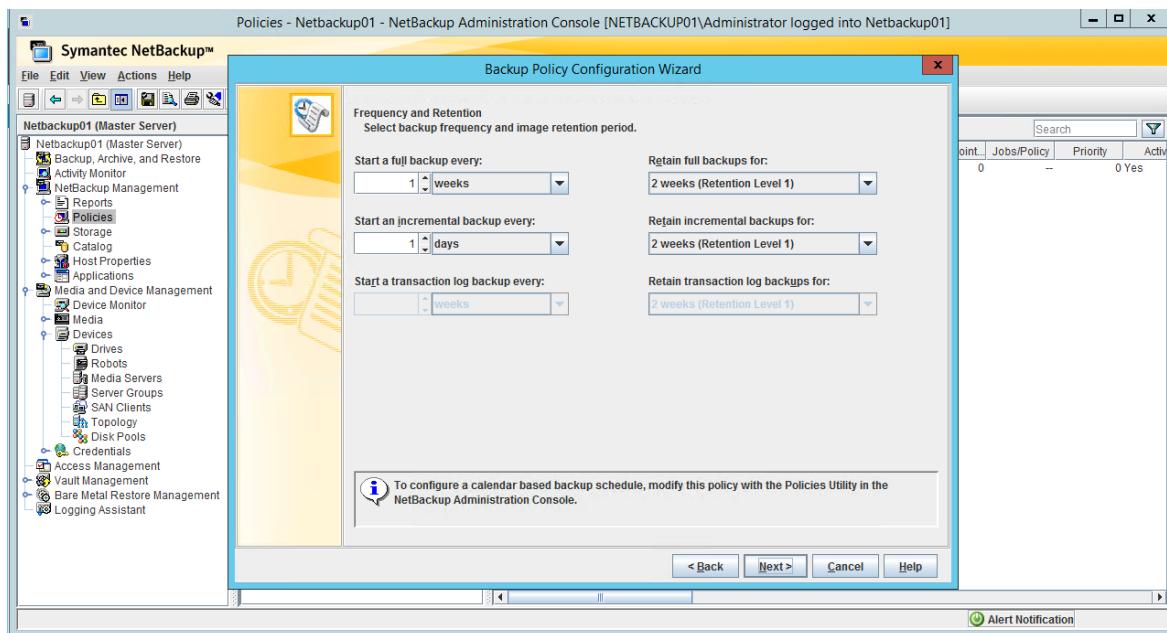
5. Select your host, select the Detect client operating system check box, and then select Add. Select Next.



6. Select the drives you want to back up.



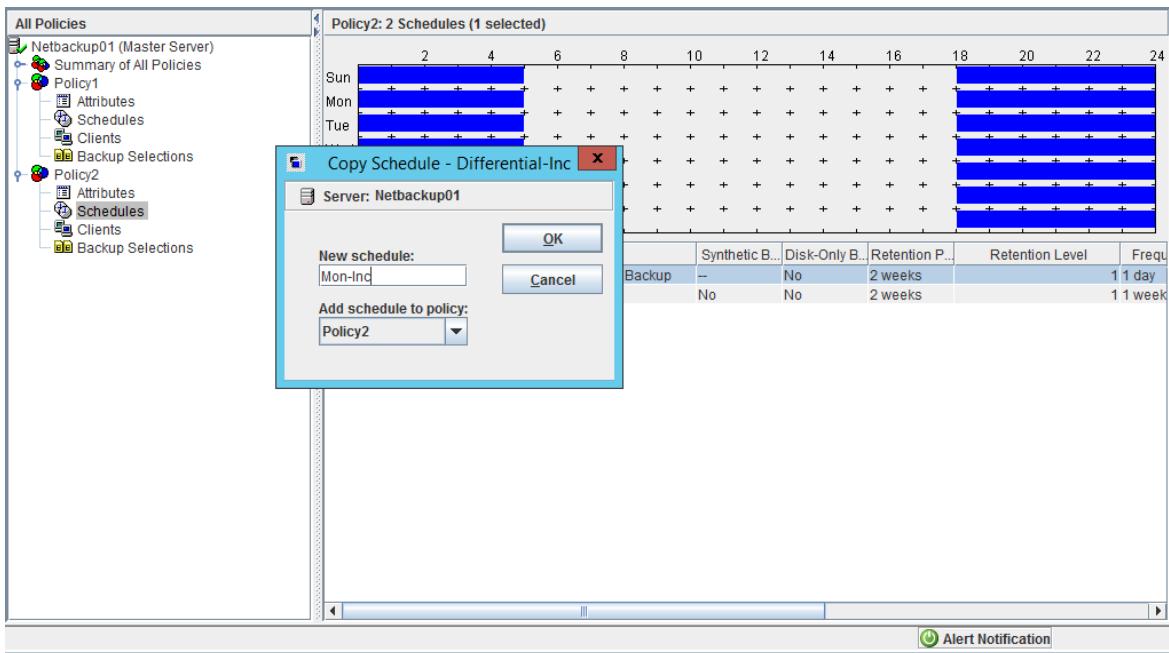
7. Select the frequency and retention values that meet your backup rotation requirements.



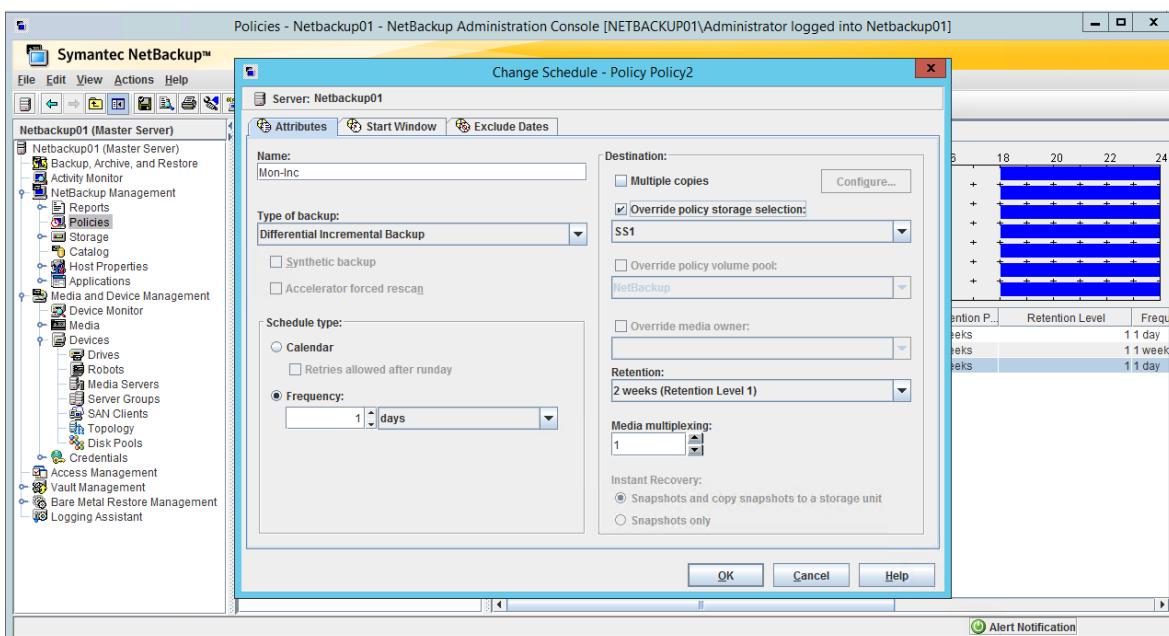
8. Select **Next > Next > Finish**. You can modify the schedule after the policy is created.
9. Select to expand the policy you just created, and then select **Schedules**.

Name	Type	Synthetic B...	Disk-Only B...	Retention P...	Retention Level	Frequ...
Differential-Inc	Differential Incremental Backup	--	No	2 weeks		1 1 day
Full	Full Backup		No	No	2 weeks	1 1 week

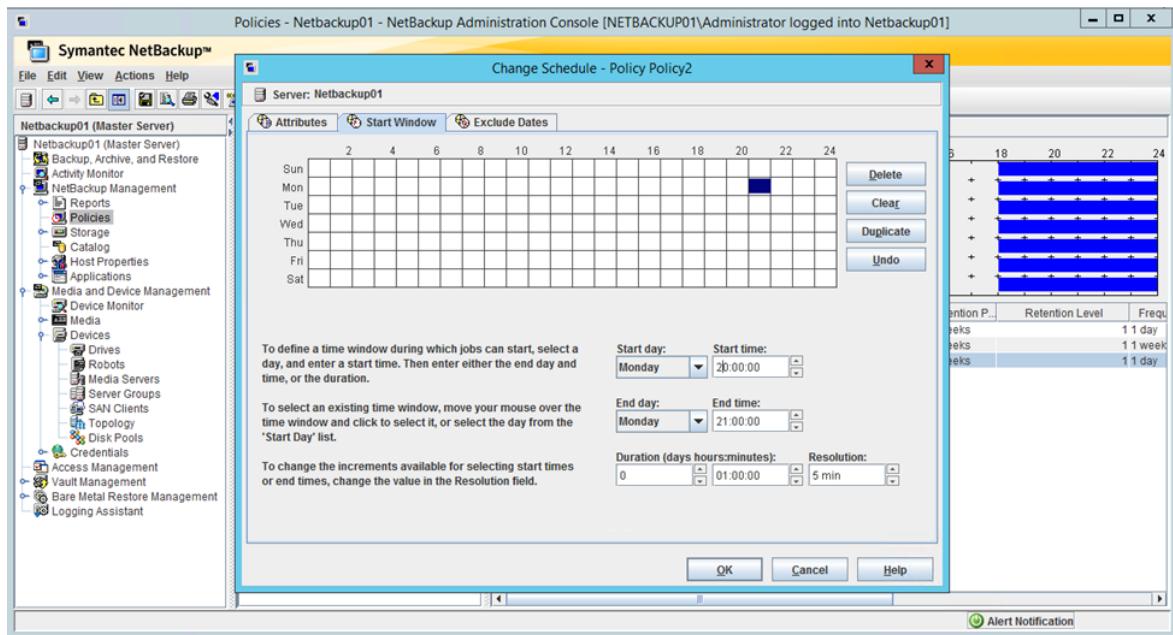
10. Right-click **Differential-Inc**, select **Copy to new**, and then select **OK**.



11. Right-click the newly created schedule, and then select **Change**.
12. On the **Attributes** tab, select the **Override policy storage selection** check box, and then select the volume where Monday incremental backups go.



13. On the **Start Window** tab, select the time window for your backups.

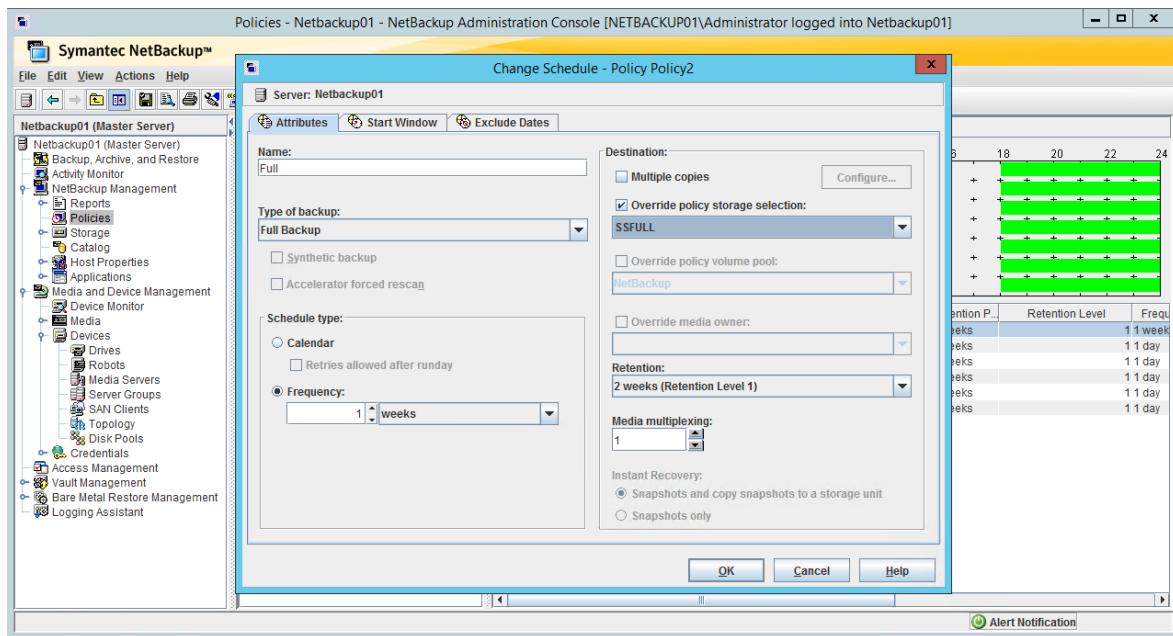


14. Select OK.

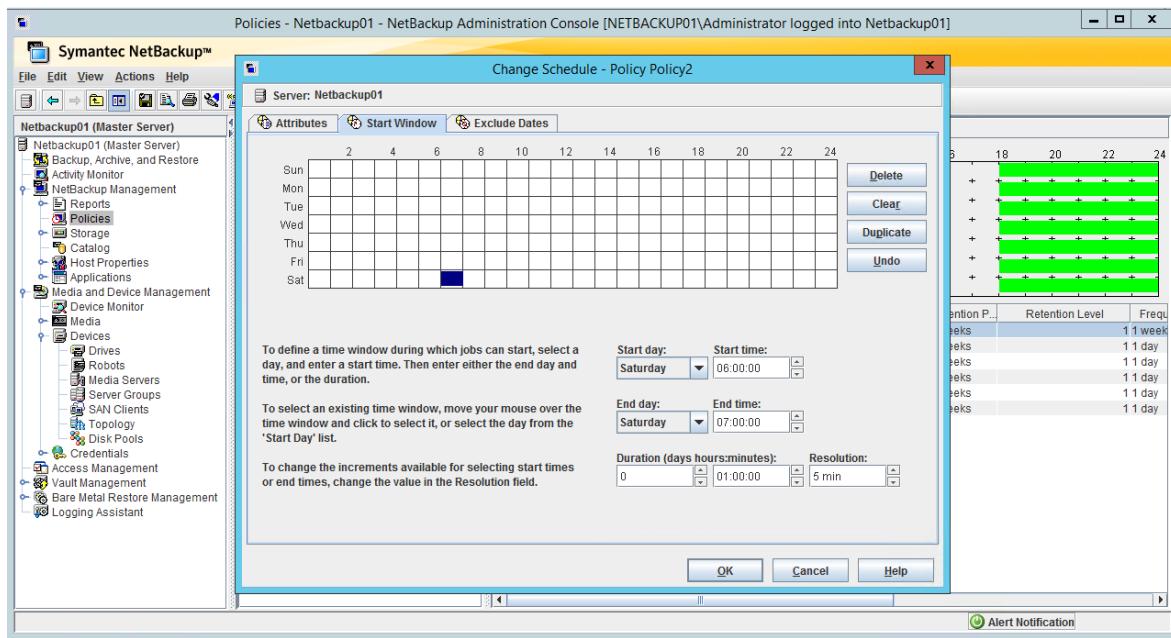
15. Repeat steps 10-14 for each incremental backup. Select the appropriate volume and schedule for each backup you create.

16. Right-click the Differential-Inc schedule, and then delete it.

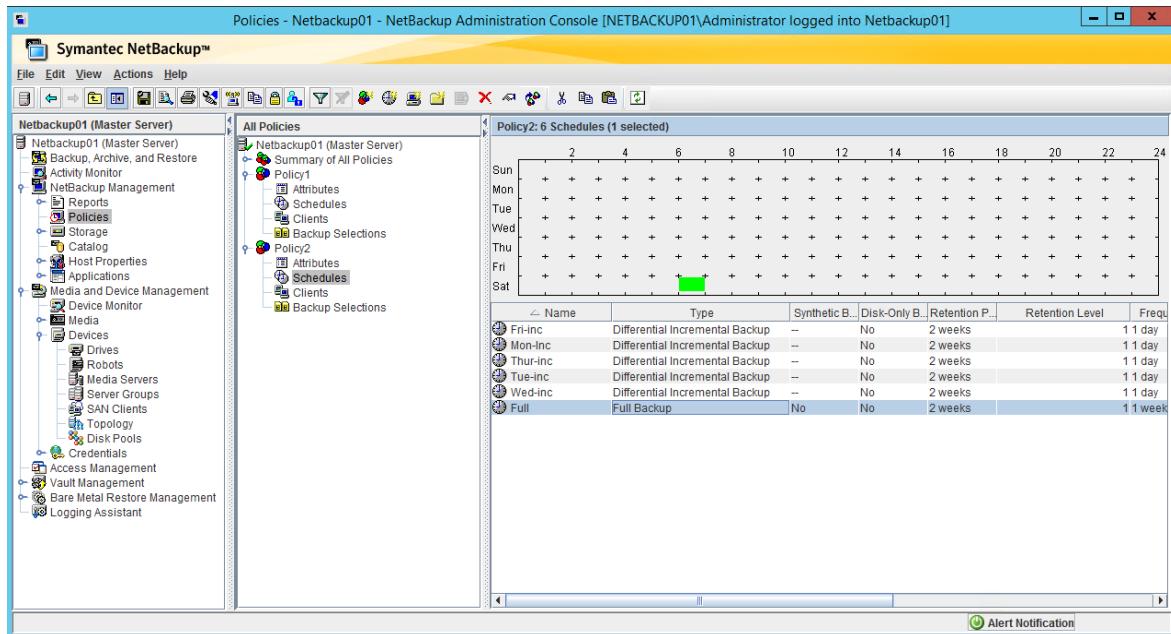
17. Modify your Full schedule to meet your backup needs.



18. Change the start window.



19. The final schedule looks like this:



Set up StorSimple as a secondary backup target

! Note

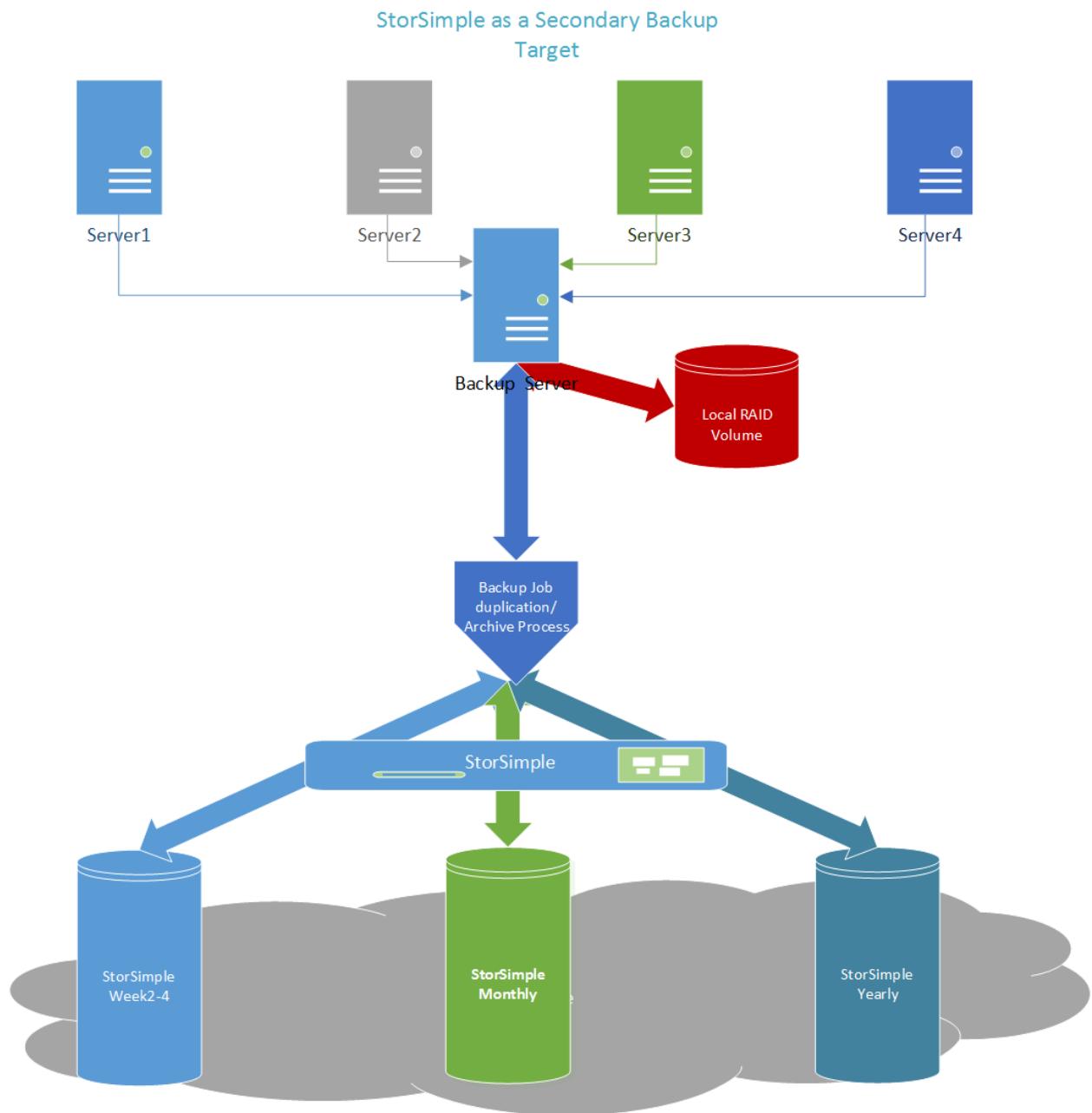
Data restores from a backup that has been tiered to the cloud occur at cloud speeds.

In this model, you must have a storage media (other than StorSimple) to serve as a temporary cache. For example, you can use a redundant array of independent disks

(RAID) volume to accommodate space, input/output (I/O), and bandwidth. We recommend using RAID 5, 50, and 10.

The following figure shows typical short-term retention local (to the server) volumes and long-term retention archives volumes. In this scenario, all backups run on the local (to the server) RAID volume. These backups are periodically duplicated and archived to an archives volume. It is important to size your local (to the server) RAID volume so that it can handle your short-term retention capacity and performance requirements.

StorSimple as a secondary backup target GFS example



The following table shows how to set up backups to run on the local and StorSimple disks. It includes individual and total capacity requirements.

Backup configuration and capacity requirements

Backup type and retention	Configured storage	Size (TiB)	GFS multiplier	Total capacity* (TiB)
Week 1 (full and incremental)	Local disk (short-term)	1	1	1
StorSimple weeks 2-4	StorSimple disk (long-term)	1	4	4
Monthly full	StorSimple disk (long-term)	1	12	12
Yearly full	StorSimple disk (long-term)	1	1	1
GFS volumes size requirement				18*

* Total capacity includes 17 TiB of StorSimple disks and 1 TiB of local RAID volume.

GFS example schedule: GFS rotation weekly, monthly, and yearly schedule

Week	Full	Incremental day 1	Incremental day 2	Incremental day 3	Incremental day 4	Incremental day 5
Week 1	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume	Local RAID volume
Week 2	StorSimple weeks 2-4					
Week 3	StorSimple weeks 2-4					
Week 4	StorSimple weeks 2-4					
Monthly	StorSimple monthly					
Yearly	StorSimple yearly					

Assign StorSimple volumes to a NetBackup archive and duplication job

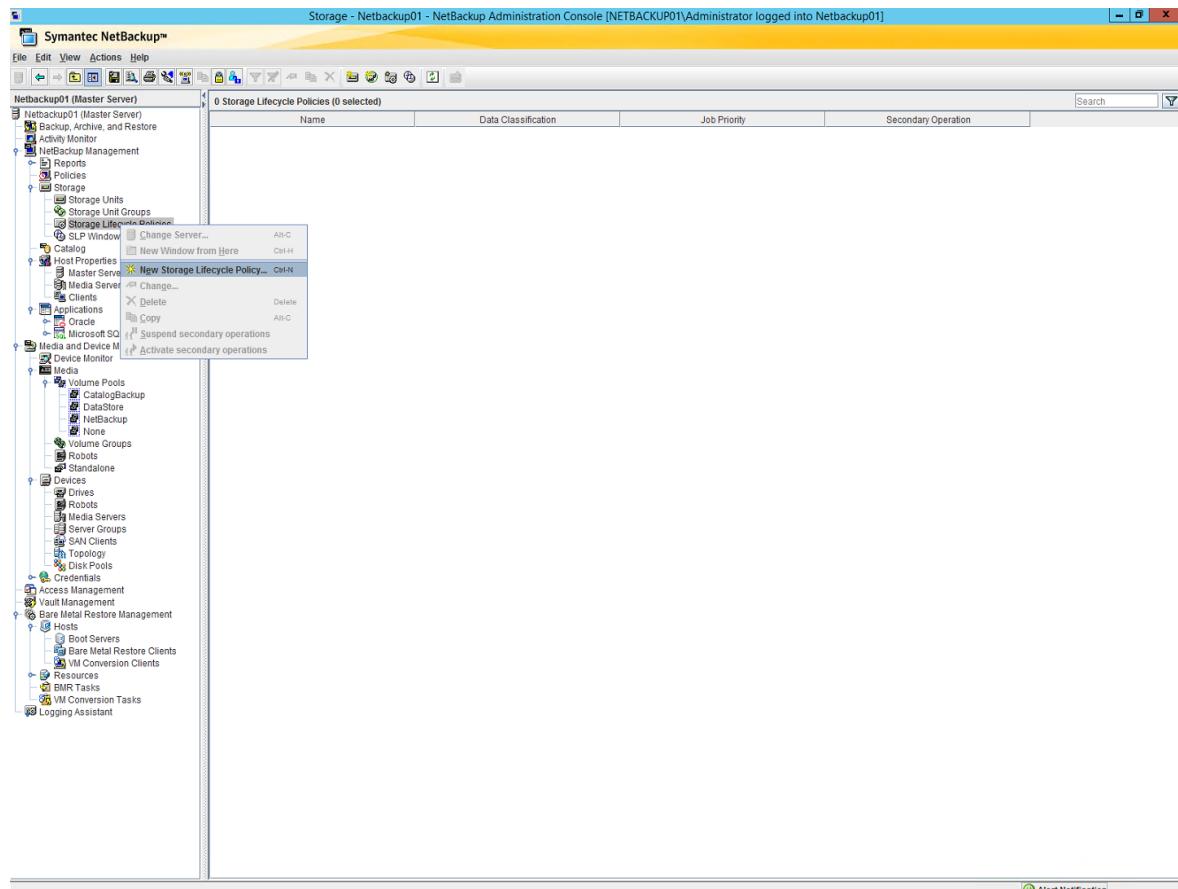
Because NetBackup offers a wide range of options for storage and media management, we recommend that you consult with Veritas or your NetBackup architect to properly assess your storage lifecycle policy (SLP) requirements.

After you've defined the initial disk pools, you need to define three additional storage lifecycle policies, for a total of four policies:

- LocalRAIDVolume
- StorSimpleWeek2-4
- StorSimpleMonthlyFulls
- StorSimpleYearlyFulls

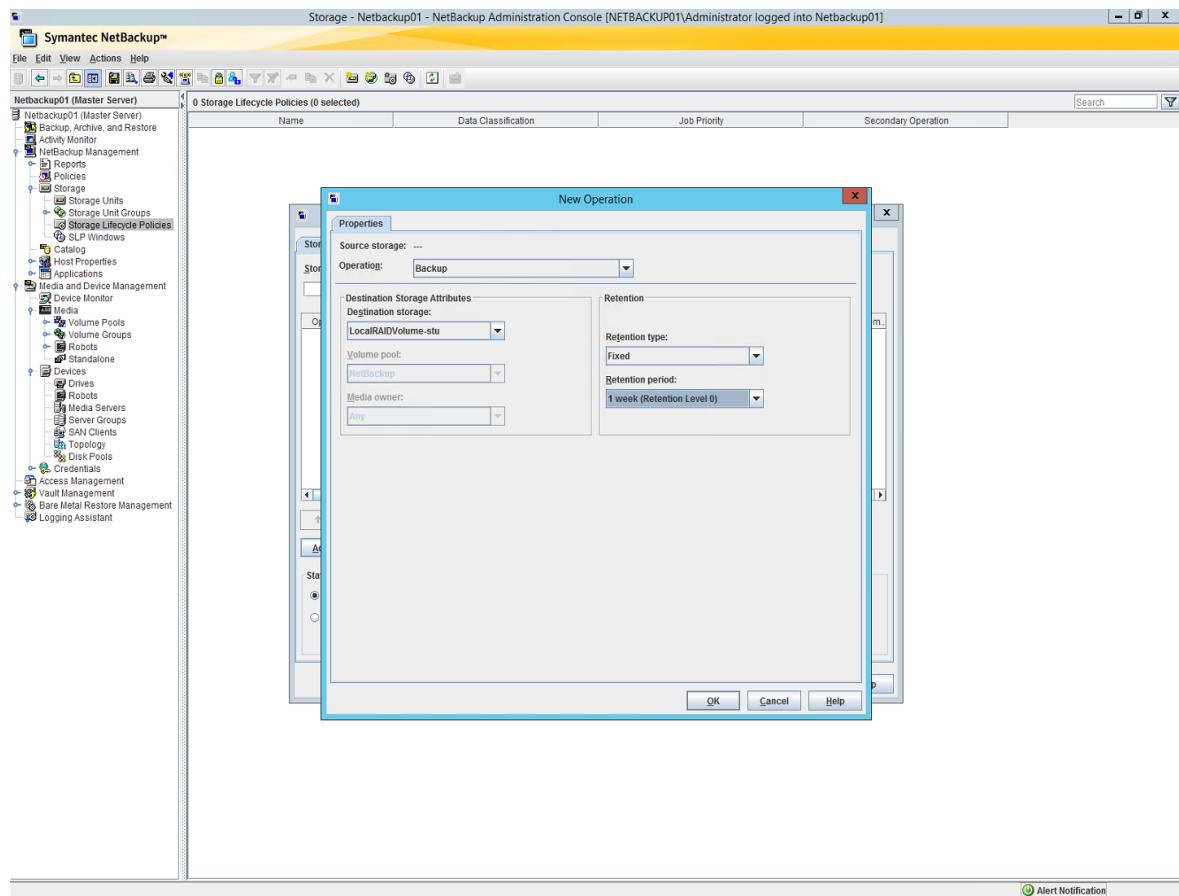
To assign StorSimple volumes to a NetBackup archive and duplication job

1. In the NetBackup Administration Console, select **Storage > Storage Lifecycle Policies > New Storage Lifecycle Policy**.



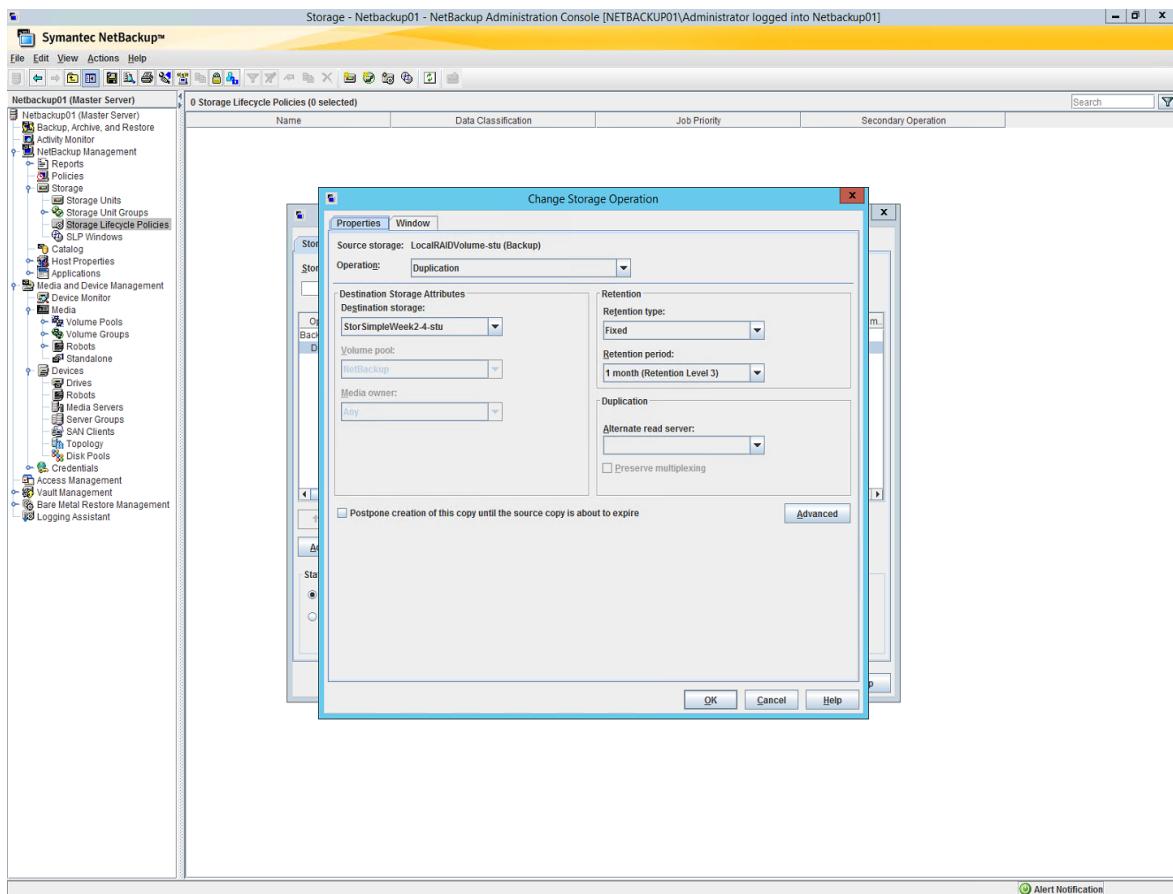
2. Enter a name for the snapshot, and then select Add.

3. In the New Operation dialog box, on the **Properties** tab, for **Operation**, select **Backup**. Select the values you want for **Destination storage**, **Retention type**, and **Retention period**. Select **OK**.

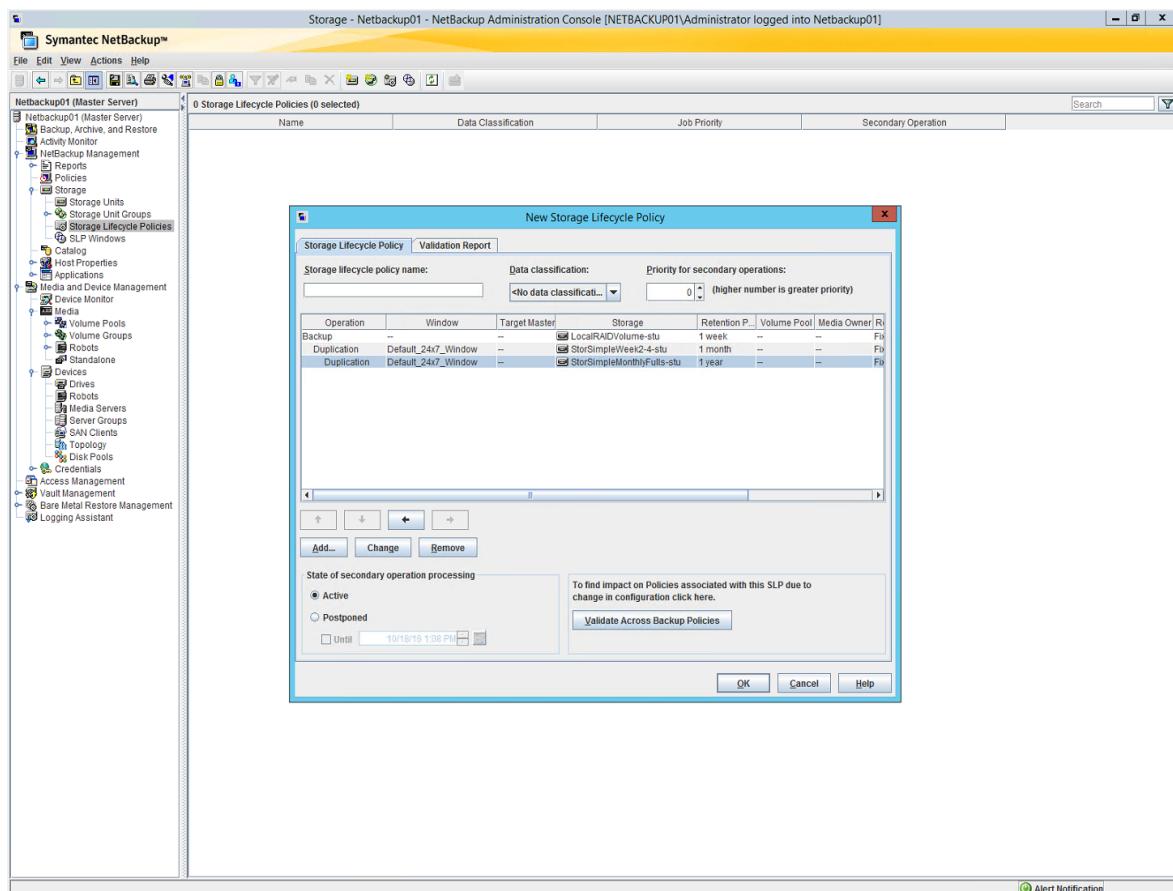


This defines the first backup operation and repository.

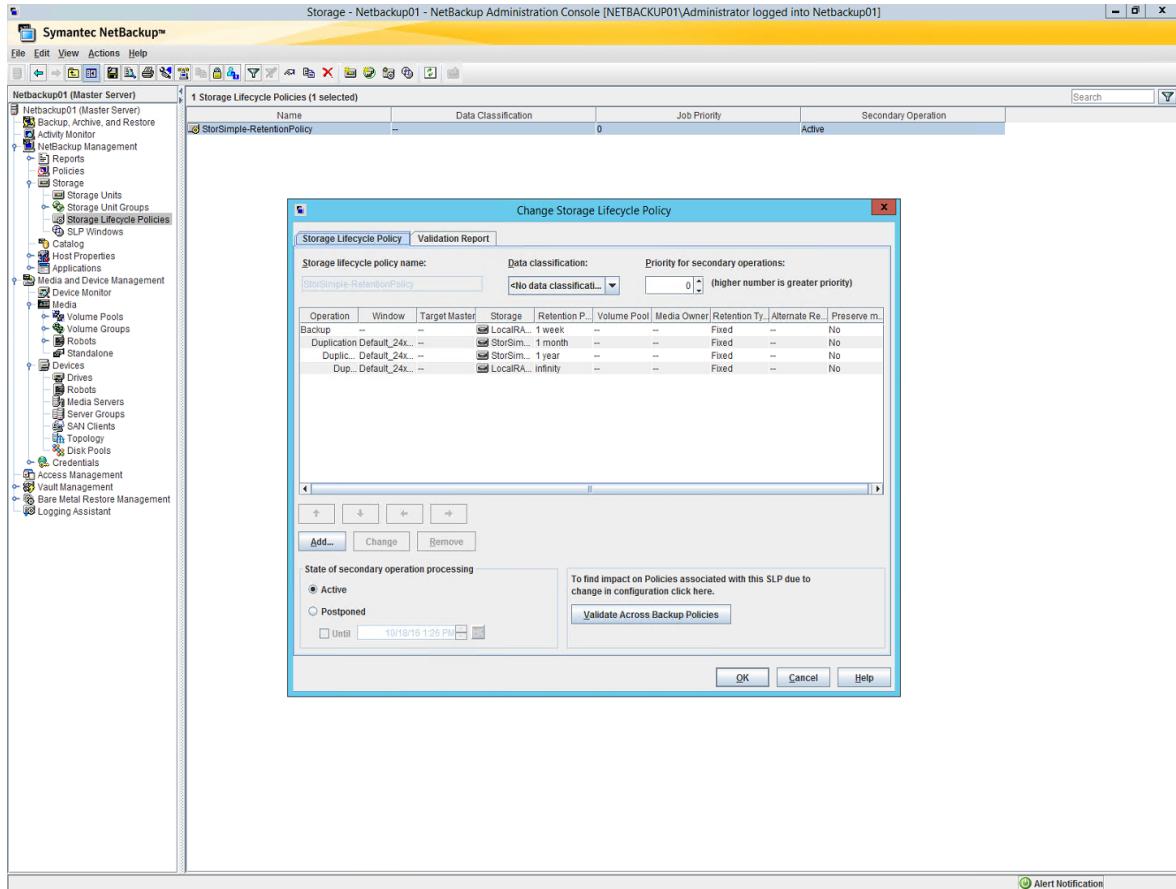
4. Select to highlight the previous operation, and then select **Add**. In the **Change Storage Operation** dialog box, select the values you want for **Destination storage**, **Retention type**, and **Retention period**.



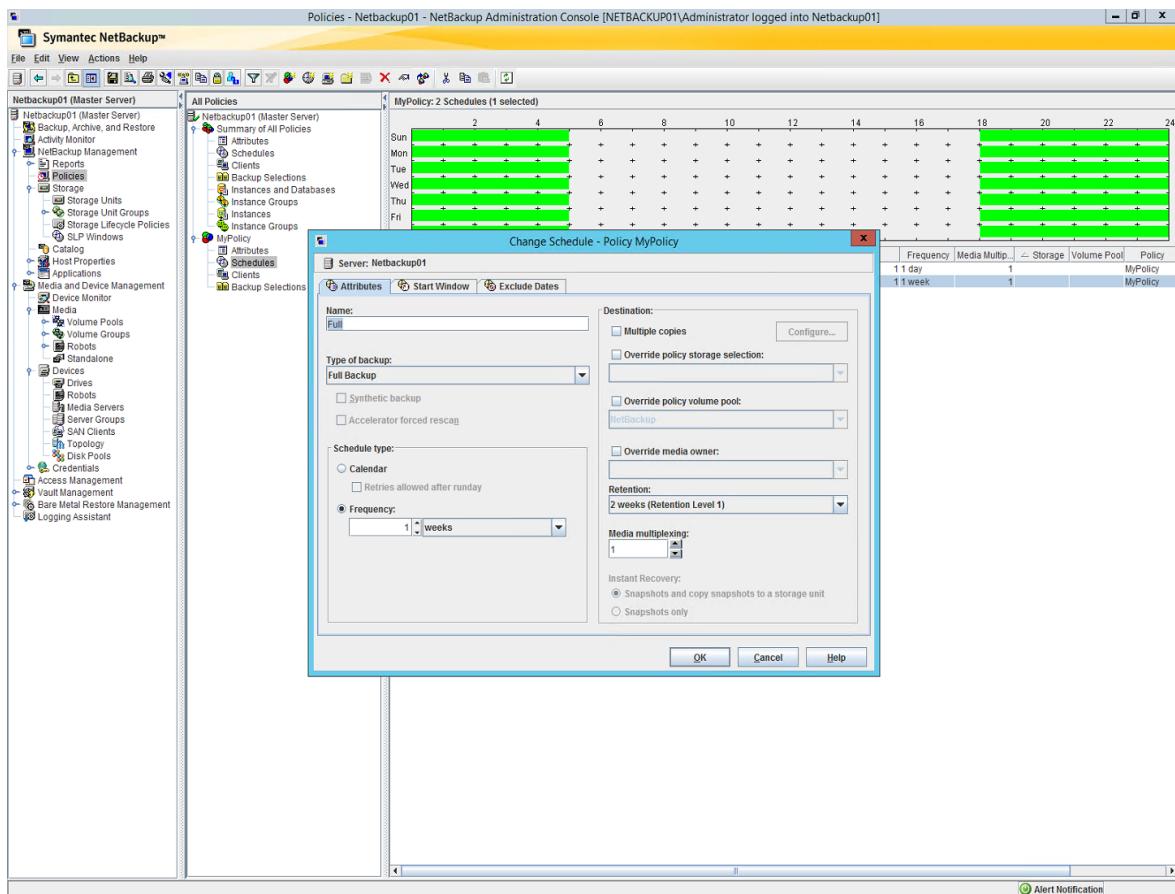
5. Select to highlight the previous operation, and then select **Add**. In the **New Storage Lifecycle Policy** dialog box, add monthly backups for a year.



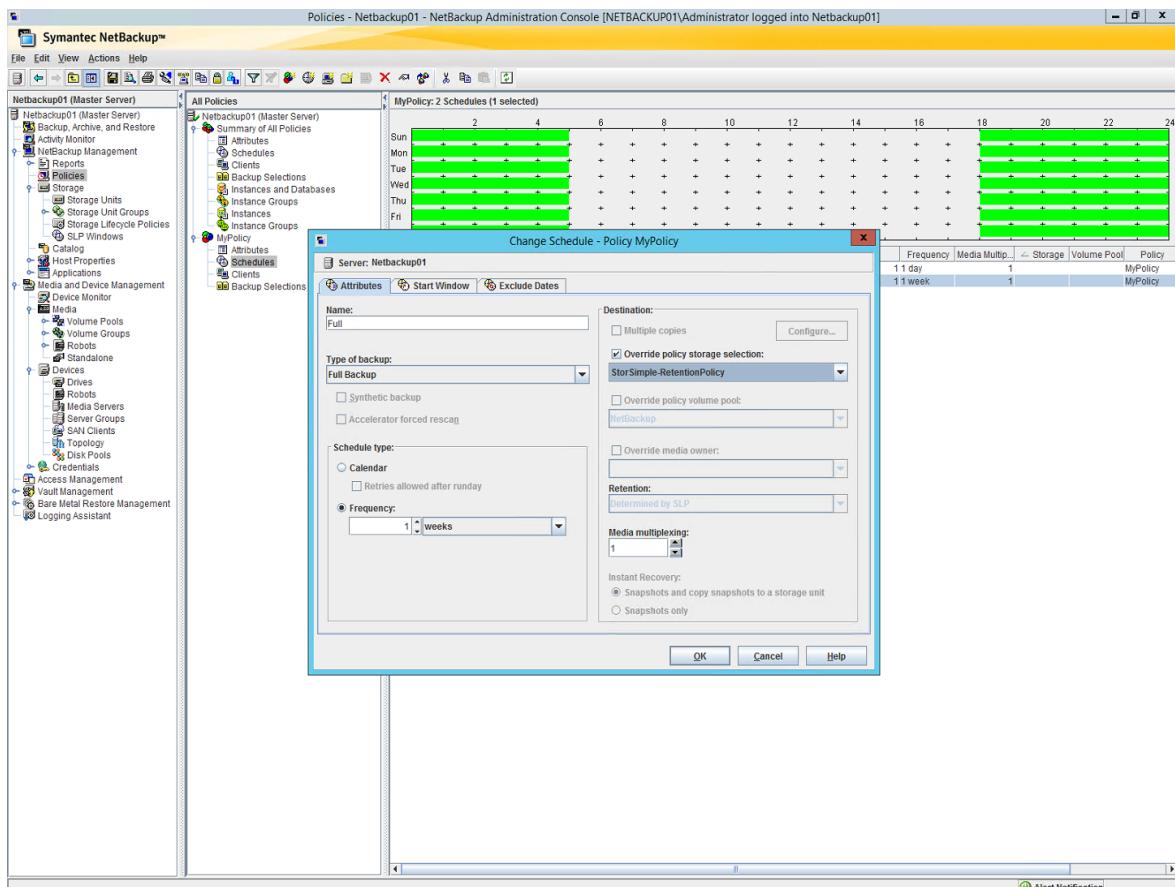
6. Repeat steps 4-5 until you've created the comprehensive SLP retention policy that you need.



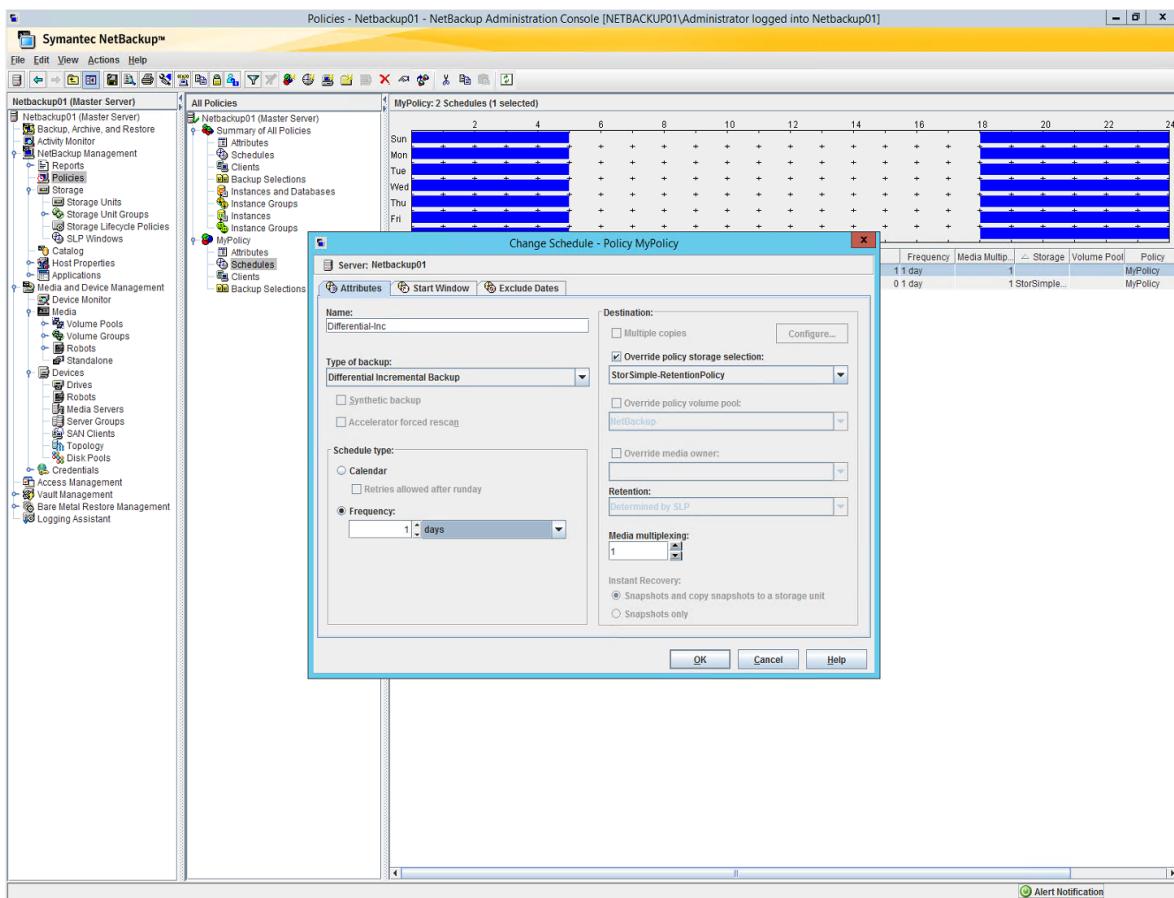
7. When you are finished defining your SLP retention policy, under **Policy**, define a backup policy by following the steps detailed in [Assigning StorSimple volumes to a NetBackup backup job](#).
8. Under **Schedules**, in the **Change Schedule** dialog box, right-click **Full**, and then select **Change**.



9. Select the **Override policy storage selection** check box, and then select the SLP retention policy that you created in steps 1-6.



10. Select **OK**, and then repeat for the incremental backup schedule.



Backup type retention	Size (TiB)	GFS multiplier*	Total capacity (TiB)
Weekly full	1	4	4
Daily incremental	0.5	20 (cycles are equal to the number of weeks per month)	12 (2 for additional quota)
Monthly full	1	12	12
Yearly full	1	10	10
GFS requirement			38
Additional quota	4		42 total GFS requirement

* The GFS multiplier is the number of copies you need to protect and retain to meet your backup policy requirements.

StorSimple cloud snapshots

StorSimple cloud snapshots protect the data that resides in your StorSimple device. Creating a cloud snapshot is equivalent to shipping local backup tapes to an offsite facility. If you use Azure geo-redundant storage, creating a cloud snapshot is equivalent

to shipping backup tapes to multiple sites. If you need to restore a device after a disaster, you might bring another StorSimple device online and do a failover. After the failover, you would be able to access the data (at cloud speeds) from the most recent cloud snapshot.

The following section describes how to create a short script to start and delete StorSimple cloud snapshots during backup post-processing.

 **Note**

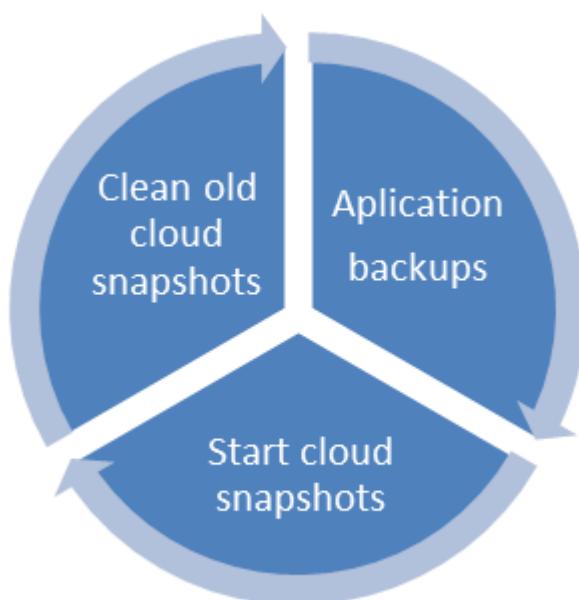
Snapshots that are manually or programmatically created do not follow the StorSimple snapshot expiration policy. These snapshots must be manually or programmatically deleted.

Start and delete cloud snapshots by using a script

 **Note**

Carefully assess the compliance and data retention repercussions before you delete a StorSimple snapshot. For more information about how to run a post-backup script, see the [NetBackup documentation](#).

Backup lifecycle



Requirements

- The server that runs the script must have access to Azure cloud resources.
- The user account must have the necessary permissions.
- A StorSimple backup policy with the associated StorSimple volumes must be set up but not turned on.
- You'll need the StorSimple resource name, registration key, device name, and backup policy ID.

To start or delete a cloud snapshot

1. [Install Azure PowerShell](#).
2. Download and setup [Manage-CloudSnapshots.ps1](#) PowerShell script.
3. On the server that runs the script, run PowerShell as an administrator. Ensure that you run the script with `-WhatIf $true` to see what changes the script will make. Once the validation is complete, pass `-WhatIf $false`. Run the below command:

PowerShell

```
.\Manage-CloudSnapshots.ps1 -SubscriptionId [Subscription Id] -TenantId
[Tenant ID] -ResourceGroupName [Resource Group Name] -ManagerName
[StorSimple Device Manager Name] -DeviceName [device name] -
BackupPolicyName [backup policyname] -RetentionInDays [Retention days]
-WhatIf [$true or $false]
```

4. Add the script to your backup job in NetBackup. To do this, edit your NetBackup job options' pre-processing and post-processing commands.

Note

We recommend that you run your StorSimple cloud snapshot backup policy as a post-processing script at the end of your daily backup job. For more information about how to back up and restore your backup application environment to help you meet your RPO and RTO, please consult with your backup architect.

StorSimple as a restore source

Restores from a StorSimple device work like restores from any block storage device. Restores of data that is tiered to the cloud occurs at cloud speeds. For local data, restores occur at the local disk speed of the device. For information about how to perform a restore, see the [NetBackup documentation](#). We recommend that you conform to NetBackup restore best practices.

StorSimple failover and disaster recovery

ⓘ Note

For backup target scenarios, StorSimple Cloud Appliance is not supported as a restore target.

A disaster can be caused by a variety of factors. The following table lists common disaster recovery scenarios.

Scenario	Impact	How to recover	Notes
StorSimple device failure	Backup and restore operations are interrupted.	Replace the failed device and perform StorSimple failover and disaster recovery .	If you need to perform a restore after device recovery, full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds. The index and catalog rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier, which might be a time-consuming process.
NetBackup server failure	Backup and restore operations are interrupted.	Rebuild the backup server and perform database restore.	You must rebuild or restore the NetBackup server at the disaster recovery site. Restore the database to the most recent point. If the restored NetBackup database is not in sync with your latest backup jobs, indexing and cataloging is required. This index and catalog rescanning process might cause all backup sets to be scanned and pulled from the cloud tier to the local device tier. This makes it further time-intensive.
Site failure that results in the loss of both the backup server and StorSimple	Backup and restore operations are interrupted.	Restore StorSimple first, and then restore NetBackup. If you need to perform a restore after device recovery, the full data working sets are retrieved from the cloud to the new device. All operations are at cloud speeds.	

References

The following documents were referenced for this article:

- StorSimple multipath I/O setup
- Storage scenarios: Thin provisioning
- Using GPT drives
- Set up shadow copies for shared folders

Next steps

- Learn more about how to [restore from a backup set](#).
- Learn more about how to perform [device failover and disaster recovery](#).

Automated Disaster Recovery solution using Azure Site Recovery for file shares hosted on StorSimple

Article • 08/22/2022 • 19 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

ⓘ Note

We recommend that you use the Azure Az PowerShell module to interact with Azure. See [Install Azure PowerShell](#) to get started. To learn how to migrate to the Az PowerShell module, see [Migrate Azure PowerShell from AzureRM to Az](#).

Overview

Microsoft Azure StorSimple is a hybrid cloud storage solution that addresses the complexities of unstructured data commonly associated with file shares. StorSimple uses cloud storage as an extension of the on-premises solution and automatically tiers data across on-premises storage and cloud storage. Integrated data protection, with local and cloud snapshots, eliminates the need for a sprawling storage infrastructure.

[Azure Site Recovery](#) is an Azure-based service that provides disaster recovery (DR) capabilities by orchestrating replication, failover, and recovery of virtual machines. Azure Site Recovery supports a number of replication technologies to consistently replicate, protect, and seamlessly fail over virtual machines and applications to private/public or hosted clouds.

Using Azure Site Recovery, virtual machine replication, and StorSimple cloud snapshot capabilities, you can protect the complete file server environment. In the event of a

disruption, you can use a single click to bring your file shares online in Azure in just a few minutes.

This document explains in detail how you can create a disaster recovery solution for your file shares hosted on StorSimple storage, and perform planned, unplanned, and test failovers using a one-click recovery plan. In essence, it shows how you can modify the Recovery Plan in your Azure Site Recovery vault to enable StorSimple failovers during disaster scenarios. In addition, it describes supported configurations and prerequisites. This document assumes that you are familiar with the basics of Azure Site Recovery and StorSimple architectures.

Supported Azure Site Recovery deployment options

Customers can deploy file servers as physical servers or virtual machines (VMs) running on Hyper-V or VMware, and then create file shares from volumes carved out of StorSimple storage. Azure Site Recovery can protect both physical and virtual deployments to either a secondary site or to Azure. This document covers details of a DR solution with Azure as the recovery site for a file server VM hosted on Hyper-V and with file shares on StorSimple storage. Other scenarios in which the file server VM is on a VMware VM or a physical machine can be implemented similarly.

Prerequisites

Implementing a one-click disaster recovery solution that uses Azure Site Recovery for file shares hosted on StorSimple storage has the following prerequisites:

- On-premises Windows Server 2012 R2 File server VM hosted on Hyper-V or VMware or a physical machine
- StorSimple storage device on-premises registered with Azure StorSimple manager
- StorSimple Cloud Appliance created in the Azure StorSimple manager. The appliance can be kept in a shut-down state.
- File shares hosted on the volumes configured on the StorSimple storage device
- [Azure Site Recovery services vault](#) created in a Microsoft Azure subscription

In addition, if Azure is your recovery site, run the [Azure Virtual Machine Readiness Assessment tool](#) on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery services.

To avoid latency issues (which might result in higher costs), make sure that you create your StorSimple Cloud Appliance, automation account, and storage account(s) in the

same region.

Enable DR for StorSimple file shares

Each component of the on-premises environment needs to be protected to enable complete replication and recovery. This section describes how to:

- Set up Active Directory and DNS replication (optional)
- Use Azure Site Recovery to enable protection of the file server VM
- Enable protection of StorSimple volumes
- Configure the network

Set up Active Directory and DNS replication (optional)

If you want to protect the machines running Active Directory and DNS so that they are available on the DR site, you need to explicitly protect them (so that the file servers are accessible after failover with authentication). There are two recommended options based on the complexity of the customer's on-premises environment.

Option 1

If the customer has a small number of applications, a single domain controller for the entire on-premises site, and will be failing over the entire site, then we recommend using Azure Site Recovery replication to replicate the domain controller machine to a secondary site (this is applicable for both site-to-site and site-to-Azure).

Option 2

If the customer has a large number of applications, is running an Active Directory forest, and will be failing over a few applications at a time, then we recommend setting up an additional domain controller on the DR site (either a secondary site or in Azure).

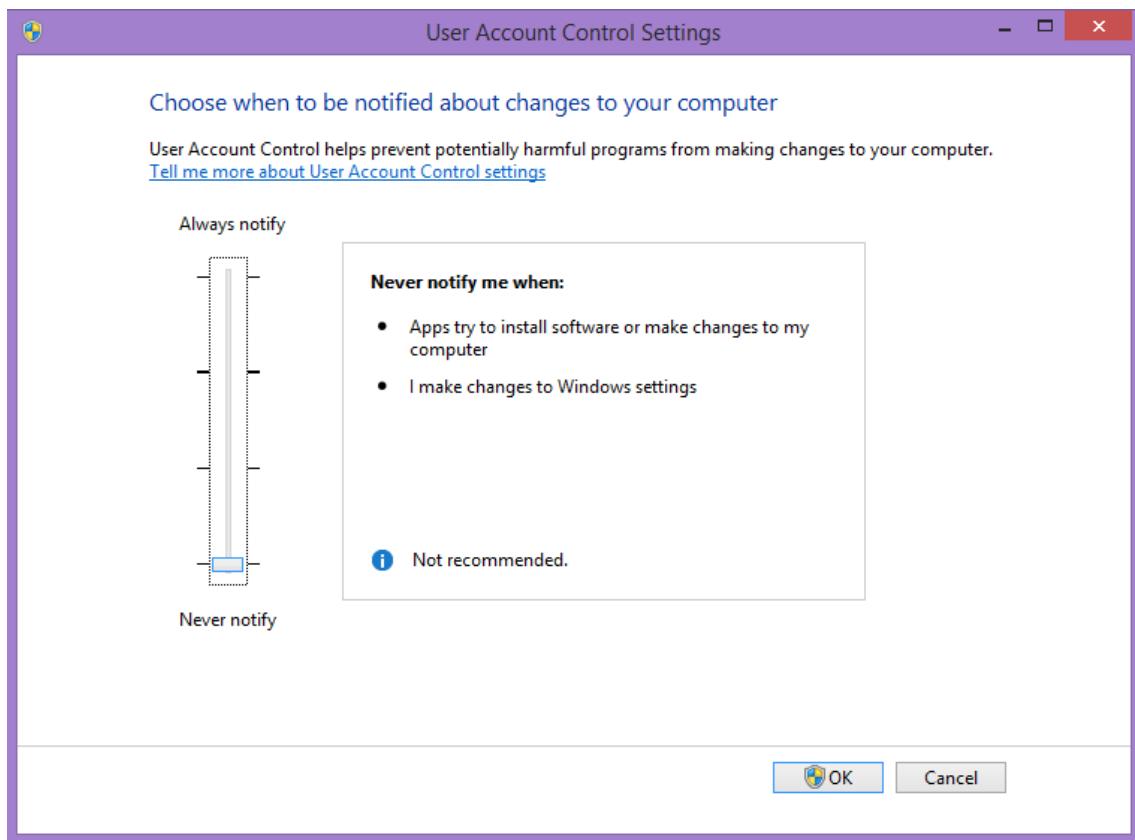
Refer to [Automated DR solution for Active Directory and DNS using Azure Site Recovery](#) for instructions when making a domain controller available on the DR site. For the rest of this document, we assume a domain controller is available on the DR site.

Use Azure Site Recovery to enable protection of the file server VM

This step requires that you prepare the on-premises file server environment, create and prepare an Azure Site Recovery vault, and enable file protection of the VM.

To prepare the on-premises file server environment

1. Set the **User Account Control** to **Never Notify**. This is required so that you can use Azure automation scripts to connect the iSCSI targets after failover by Azure Site Recovery.
 - a. Press the Windows key +Q and search for **UAC**.
 - b. Select **Change User Account Control settings**.
 - c. Drag the bar to the bottom towards **Never Notify**.
 - d. Click **OK** and then select **Yes** when prompted.



2. Install the VM Agent on each of the file server VMs. This is required so that you can run Azure automation scripts on the failed over VMs.
 - a. [Download the agent](#) to `C:\\\\Users\\\\<username>\\\\Downloads`.
 - b. Open Windows PowerShell in Administrator mode (Run as Administrator), and then enter the following command to navigate to the download location:
`cd C:\\\\Users\\\\`

```
<username>\Downloads\WindowsAzureVmAgent.2.6.1198.718.rd\_art\_stable.150  
415-1739.fre.msi
```

① Note

The file name may change depending on the version.

3. Click **Next**.
4. Accept the **Terms of Agreement** and then click **Next**.
5. Click **Finish**.
6. Create file shares using volumes carved out of StorSimple storage. For more information, see [Use the StorSimple Manager service to manage volumes](#).
 - a. On your on-premises VMs, press the Windows key +Q and search for **iSCSI**.
 - b. Select **iSCSI initiator**.
 - c. Select the **Configuration** tab and copy the initiator name.
 - d. Log in to the [Azure portal](#).
 - e. Select the **StorSimple** tab and then select the StorSimple Manager Service that contains the physical device.
 - f. Create volume container(s) and then create volume(s). (These volumes are for the file share(s) on the file server VMs). Copy the initiator name and give an appropriate name for the Access Control Records when you create the volumes.
 - g. Select the **Configure** tab and note down the IP address of the device.
 - h. On your on-premises VMs, go to the **iSCSI initiator** again and enter the IP in the Quick Connect section. Click **Quick Connect** (the device should now be connected).
 - i. Open the Azure portal and select the **Volumes and Devices** tab. Click **Auto Configure**. The volume that you created should appear.
 - j. In the portal, select the **Devices** tab and then select **Create a New Virtual Device**. (This virtual device will be used if a failover occurs). This new virtual device can be kept in an offline state to avoid extra costs. To take the virtual device offline, go to the **Virtual Machines** section on the Portal and shut it down.
 - k. Go back to the on-premises VMs and open Disk Management (press the Windows key + X and select **Disk Management**).
 - l. You will notice some extra disks (depending on the number of volumes you have created). Right-click the first one, select **Initialize Disk**, and select **OK**. Right-click the **Unallocated** section, select **New Simple Volume**, assign it a drive letter, and finish the wizard.

- m. Repeat step I for all the disks. You can now see all the disks on **This PC** in the Windows Explorer.
- n. Use the File and Storage Services role to create file shares on these volumes.

To create and prepare an Azure Site Recovery vault

Refer to the [Azure Site Recovery documentation](#) to get started with Azure Site Recovery before protecting the file server VM.

To enable protection

1. Disconnect the iSCSI target(s) from the on-premises VMs that you want to protect through Azure Site Recovery:
 - a. Press Windows key + Q and search for **iSCSI**.
 - b. Select **Set up iSCSI initiator**.
 - c. Disconnect the StorSimple device that you connected previously. Alternatively, you can switch off the file server for a few minutes when enabling protection.

 **Note**

This will cause the file shares to be temporarily unavailable.

2. [Enable virtual machine protection](#) of the file server VM from the Azure Site Recovery portal.
3. When the initial synchronization begins, you can reconnect the target again. Go to the iSCSI initiator, select the StorSimple device, and click **Connect**.
4. When the synchronization is complete and the status of the VM is **Protected**, select the VM, select the **Configure** tab, and update the network of the VM accordingly (this is the network that the failed over VM(s) will be a part of). If the network doesn't show up, it means that the sync is still going on.

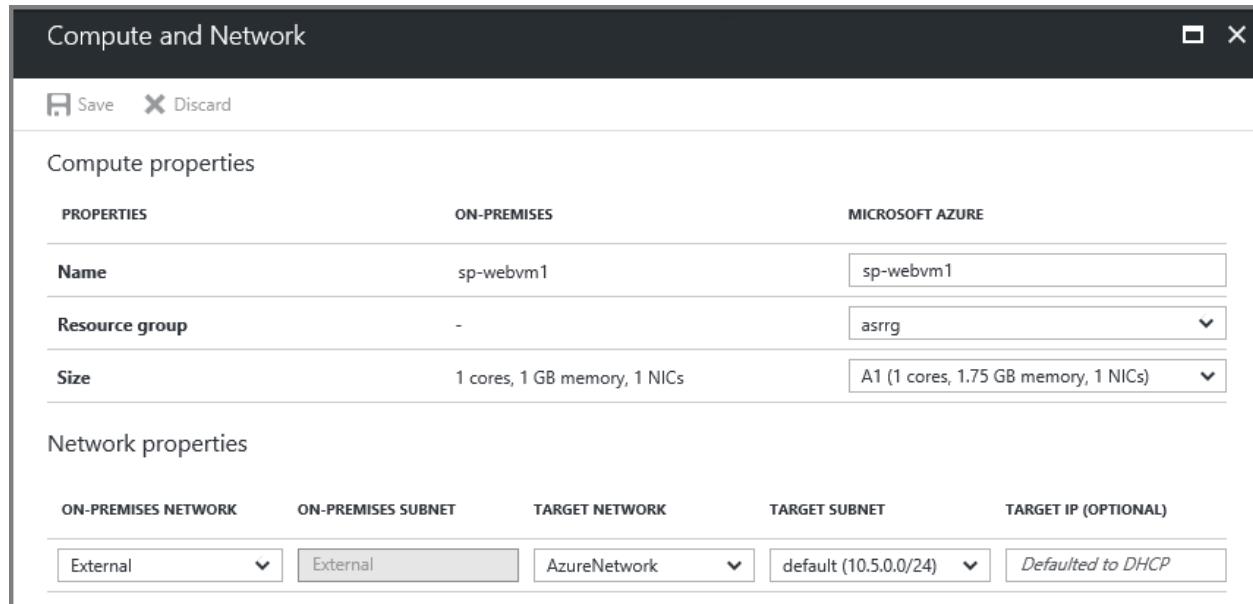
Enable protection of StorSimple volumes

If you have not selected the **Enable a default backup for this volume** option for the StorSimple volumes, go to **Backup Policies** in the StorSimple Manager service, and create a suitable backup policy for all the volumes. We recommend that you set the frequency of backups to the recovery point objective (RPO) that you would like to see for the application.

Configure the network

For the file server VM, configure network settings in Azure Site Recovery so that the VM networks are attached to the correct DR network after failover.

You can select the VM in the **Replicated items** tab to configure the network settings, as shown in the following illustration.



Create a recovery plan

You can create a recovery plan in ASR to automate the failover process of the file shares. If a disruption occurs, you can bring the file shares up in a few minutes with just a single click. To enable this automation, you will need an Azure automation account.

To create an Automation account

1. Go to the Azure portal > **Automation** section.
2. Click **+ Add** button, opens below blade.

Add Automation Account X

* Name i

* Subscription

Select or enter a subscription name

* Resource group i
 Create new Use existing

Select or enter a resource group name

* Location

Select or enter a location

* Create Azure Run As account i

i The Run As account feature will create a Run As account and a Classic Run As account. [Click here to learn more about Run As accounts.](#)

Pin to dashboard

Create

- Name - Enter a new automation account
- Subscription - Choose subscription
- Resource group - Create new/choose existing resource group
- Location - Choose location, keep it in the same geo/region in which the StorSimple Cloud Appliance and Storage Accounts were created.
- Create Azure Run As account - Select Yes option.

3. Go to the Automation account, click **Runbooks > Browse Gallery** to import all the required runbooks into the automation account.
4. Add the following runbooks by finding **Disaster Recovery** tag in the gallery:
 - Clean up of StorSimple volumes after Test Failover (TFO)
 - Failover StorSimple volume containers
 - Mount volumes on StorSimple device after failover
 - Uninstall custom script extension in Azure VM

- Start StorSimple Virtual Appliance

The screenshot shows the 'Browse Gallery' window with a search bar containing 'Disaster recovery'. A red box highlights the search bar and the results list. The results list contains five runbooks, each with a blue icon, a title, a brief description, and metadata (created by, downloads, last updated). The fifth runbook, 'Start StorSimple Virtual Appliance', is also highlighted with a red box.

Runbook Title	Description	Created by	Downloads	Last updated
Cleanup of StorSimple volumes after Test Failover (TFO)	This runbook deletes all the volumes, backups, backup policies temporarily created on the target StorSimple device for TFO scenario using ASR. It also shuts down the StorSimple virtual appliance after TFO.	Sujay Talasila [MSFT]	312	10/25/2016
Failover StorSimple Volume Containers	This runbook performs a failover of the StorSimple volume containers in the context of Azure Site Recovery(ASR) recovery plan.	Sujay Talasila [MSFT]	390	10/25/2016
Mount volumes on StorSimple device after Failover	This runbook creates a script and stores it in an Azure storage account. It then uses the custom VM script extension to run the script from the VM. This script will connect to the iSCSI target and mount the volumes after the failover using ASR (Azure Site Recovery)	Sujay Talasila [MSFT]	455	10/25/2016
Uninstall custom script extension in Azure VM	This runbook uninstalls the custom script extension from the Azure VMs brought up by ASR (Azure Site Recovery) failover. This runbook is to be used in the context of ASR recovery plans for workloads hosted on StorSimple devices.	Sujay Talasila [MSFT]	307	10/25/2016
Start StorSimple Virtual Appliance	This runbook starts the StorSimple virtual appliance in case it is in shut down state. This script is to be used in the context of ASR (Azure Site Recovery) recovery plan for workloads hosted on StorSimple devices.	Sujay Talasila [MSFT]	373	10/24/2016

5. Publish all the scripts by selecting the runbook in the automation account and click **Edit > Publish** and then **Yes** to the verification message. After this step, the **Runbooks** tab will appear as follows:

The screenshot shows the 'Runbooks' list page in the Azure Automation portal. The table lists nine runbooks, all of which are published. The columns are NAME, AUTHORING STATUS, LAST MODIFIED, and TAGS.

NAME	AUTHORING STATUS	LAST MODIFIED	TAGS
AzureAutomationTutorial	✓ Published	5/18/2017 3:05 PM	
AzureAutomationTutorialScript	✓ Published	5/18/2017 3:05 PM	
AzureClassicAutomationTutorial	✓ Published	5/18/2017 3:05 PM	
AzureClassicAutomationTutorialScript	✓ Published	5/18/2017 3:05 PM	
Cleanup-After-Test-Failover	✓ Published	5/19/2017 5:27 PM	
Failover-StorSimple-Volume-Containers	✓ Published	5/19/2017 4:37 PM	
Mount-Volumes-After-Failover	✓ Published	5/19/2017 4:37 PM	
Start-StorSimple-Virtual-Appliance	✓ Published	5/19/2017 4:38 PM	
Uninstall-Custom-Script-Extension	✓ Published	5/19/2017 4:38 PM	

6. In the automation account, click **Variables > Add a variable** and add the following variables. You can choose to encrypt these assets. These variables are recovery plan specific. If your recovery plan, which you will create in the next step, name is

TestPlan, then your variables should be TestPlan-StorSimRegKey, TestPlan-AzureSubscriptionName, and so on.

- **BaseUrl:** The Resource Manager url for the Azure cloud. Get using **Get-AzEnvironment | Select-Object Name, ResourceManagerUrl** cmdlet.
- **RecoveryPlanName-ResourceGroupName:** The Resource Manager group that has the StorSimple resource.
- **RecoveryPlanName-ManagerName:** The StorSimple resource that has the StorSimple device.
- **RecoveryPlanName-DeviceName:** The StorSimple Device that has to be failed over.
- **RecoveryPlanName-DeviceIpAddress:** The IP address of the device (this can be found in the **Devices** tab under StorSimple Device Manager section > **Settings > Network > DNS Settings** group).
- **RecoveryPlanName-VolumeContainers:** A comma-separated string of volume containers present on the device that need to be failed over; for example: volcon1, volcon2, volcon3.
- **RecoveryPlanName-TargetDeviceName:** The StorSimple Cloud Appliance on which the containers are to be failed over.
- **RecoveryPlanName-TargetDeviceIpAddress:** The IP address of the target device (this can be found in the **Virtual Machine** section > **Settings** group > **Networking** tab).
- **RecoveryPlanName-StorageAccountName:** The storage account name in which the script (which has to run on the failed over VM) will be stored. This can be any storage account that has some space to store the script temporarily.
- **RecoveryPlanName-StorageAccountKey:** The access key for the above storage account.
- **RecoveryPlanName-VMGUIDS:** Upon protecting a VM, Azure Site Recovery assigns every VM a unique ID that gives the details of the failed over VM. To obtain the VMGUID, select the **Recovery Services** tab and click **Protected Item > Protection Groups > Machines > Properties**. If you have multiple VMs, then add the GUIDs as a comma-separated string.

For example, if the name of the recovery plan is fileServerpredayRP, then your **Variables**, **Connections** and **Certificates** tab should appear as follows after you add all the assets.

Variables	
NAME	TYPE
BaseUrl	String
fileServerpredayRP-DeviceIpAddress	String
fileServerpredayRP-DeviceName	String
fileServerpredayRP-ManagerName	String
fileServerpredayRP-ResourceGroupName	String
fileServerpredayRP-StorageAccountKey	String
fileServerpredayRP-StorageAccountName	String
fileServerpredayRP-TargetDeviceIpAddress	String
fileServerpredayRP-TargetDeviceName	String
fileServerpredayRP-VMGUIDS	String
fileServerpredayRP-VolumeContainers	String

Connections	
NAME	
AzureClassicRunAsConnection	
AzureRunAsConnection	

Certificates	
NAME	
AzureClassicRunAsCertificate	
AzureRunAsCertificate	

7. Upload StorSimple 8000 series Runbook module in your Automation account. Use the below steps to add a module:

- a. Open powershell, create a new folder & change directory to the folder.

```
mkdir C:\scripts\StorSimpleSDKTools  
cd C:\scripts\StorSimpleSDKTools
```

- b. Download nuget CLI under the same folder in Step1. Various versions of nuget.exe are available on [nuget downloads](#). Each download link points directly to an .exe file, so be sure to right-click and save the file to your computer rather than running it from the browser.

```
wget https://dist.nuget.org/win-x86-commandline/latest/nuget.exe -Out  
C:\scripts\StorSimpleSDKTools\NuGet.exe
```

- c. Download the dependent SDK

```
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.Azure.Management.Storsimple8000series  
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.IdentityModel.Clients.ActiveDirectory -Version 2.28.3  
C:\scripts\StorSimpleSDKTools\NuGet.exe install  
Microsoft.Rest.ClientRuntime.Azure.Authentication -Version 2.2.9-  
preview
```

- d. Create an Azure Automation Runbook Module for StorSimple 8000 Series device management. Use the below commands to create an Automation module zip file.

```
PowerShell  
  
# set path variables  
$downloadDir = "C:\scripts\StorSimpleSDKTools"  
$moduleDir =  
"$downloadDir\AutomationModule\Microsoft.Azure.Management.StorSimple  
8000Series"  
  
#don't change the folder name  
"Microsoft.Azure.Management.StorSimple8000Series"
```

```

mkdir "$moduleDir"

copy
"$downloadDir\Microsoft.IdentityModel.Clients.ActiveDirectory.2.28.3
\lib\net45\Microsoft.IdentityModel.Clients.ActiveDirectory*.dll"
$moduleDir
    copy
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.3.3.7\lib\net452\Mi
crosoft.Rest.ClientRuntime.Azure*.dll" $moduleDir
    copy
"$downloadDir\Microsoft.Rest.ClientRuntime.2.3.8\lib\net452\Microsof
t.Rest.ClientRuntime*.dll" $moduleDir
    copy
"$downloadDir\Newtonsoft.Json.6.0.8\lib\net45\Newtonsoft.Json*.dll"
$moduleDir
    copy
"$downloadDir\Microsoft.Rest.ClientRuntime.Azure.Authentication.2.2.
9-
preview\lib\net45\Microsoft.Rest.ClientRuntime.Azure.Authentication*
.dll" $moduleDir
    copy
"$downloadDir\Microsoft.Azure.Management.Storsimple8000series.1.0.0\
lib\net452\Microsoft.Azure.Management.Storsimple8000series*.dll"
$moduleDir

#Don't change the name of the Archive
compress-Archive -Path "$moduleDir" -DestinationPath
Microsoft.Azure.Management.StorSimple8000Series.zip

```

e. Import the Azure Automation module zip file

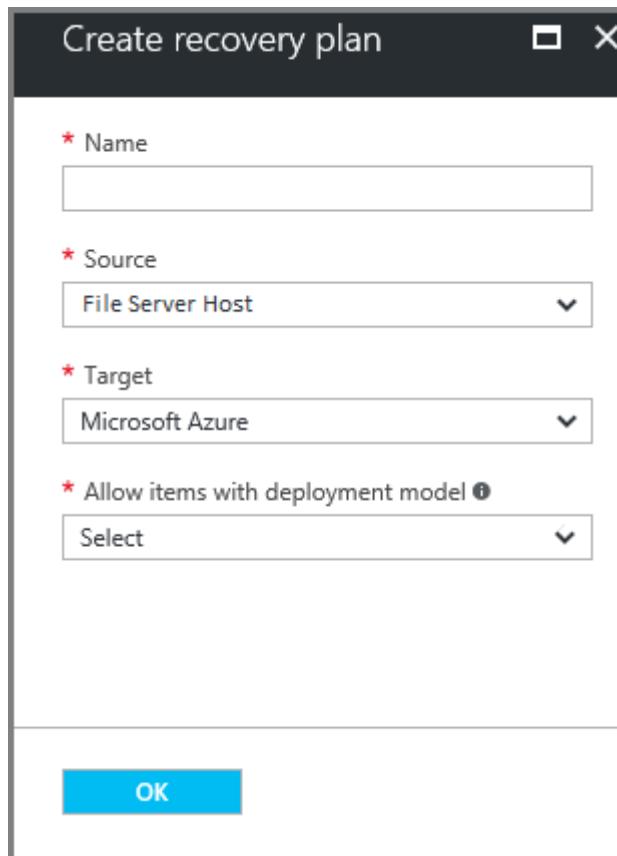
(Microsoft.Azure.Management.StorSimple8000Series.zip) created in above step.

This can be done by selecting the Automation Account, click **Modules** under SHARED RESOURCES and then click **Add a module**.

After you import the StorSimple 8000 series module, the **Modules** tab should appear as follows:

 Add a module	 Update Azure Modules	 Browse gallery	 Refresh
NAME	LAST MODIFIED	STATUS	
Azure	9/16/2017 4:29 AM	Available	
Azure.Storage	9/16/2017 4:36 AM	Available	
AzureRM.Automation	9/16/2017 4:34 AM	Available	
AzureRM.Compute	9/16/2017 4:33 AM	Available	
AzureRM.Profile	9/16/2017 4:33 AM	Available	
AzureRM.Resources	9/16/2017 4:34 AM	Available	
AzureRM.Sql	9/16/2017 4:35 AM	Available	
AzureRM.Storage	9/16/2017 4:35 AM	Available	
Microsoft.Azure.Management.StorSimple8000Series	9/27/2017 6:00 PM	Available	
Microsoft.PowerShell.Core	9/16/2017 4:30 AM	Available	
Microsoft.PowerShell.Diagnostics	9/16/2017 4:30 AM	Available	
Microsoft.PowerShell.Management	9/16/2017 4:31 AM	Available	
Microsoft.PowerShell.Security	9/16/2017 4:31 AM	Available	
Microsoft.PowerShell.Utility	9/16/2017 4:32 AM	Available	
Microsoft.WSMan.Management	9/16/2017 4:32 AM	Available	
Orchestrator.AssetManagement.Cmdlets	9/16/2017 4:36 AM	Available	

8. Go to the **Recovery Services** section and select the Azure Site Recovery vault that you created earlier.
9. Select the **Recovery Plans (Site Recovery)** option from **Manage** group and create a new recovery plan as follows:
 - Click **+ Recover plan** button, opens below blade.



- Enter a recovery plan name, choose Source, Target & Deployment model values.
- Select the VMs from the protection group that you want to include in the recovery plan and click **OK** button.
- Select Recovery plan that you created earlier, click **Customize** button to open the Recovery plan customization view.
- Right click on **All groups shutdown** and click **Add pre action**.
- Opens Insert action blade, enter a name, select **Primary side** option in Where to run option, select Automation account (in which you added the runbooks) and then select the **Failover-StorSimple-Volume-Containers** runbook.
- Right click on **Group 1: Start** and click **Add protected items** option then select the VMs that are to be protected in the recovery plan and Click **Ok** button. Optional, if it's already selected VMs.
- Right click on **Group 1: Start** and click **Post action** option then add all the following scripts:
 - Start-StorSimple-Virtual-Appliance runbook
 - Fail over-StorSimple-volume-containers runbook
 - Mount-volumes-after-failover runbook
 - Uninstall-custom-script-extension runbook

- Add a manual action after the above 4 scripts in the same **Group 1: Post-steps** section. This action is the point at which you can verify that everything is working correctly. This action needs to be added only as a part of Test failover (so only select the **Test Failover** checkbox).
- After the manual action, add the **Cleanup** script using the same procedure that you used for the other runbooks. **Save** the recovery plan.

① Note

When running a test failover, you should verify everything at the manual action step because the StorSimple volumes that had been cloned on the target device will be deleted as a part of the cleanup after the manual action is completed.

The screenshot shows the 'fileServerpredayRP' recovery plan interface. At the top, there are buttons for Group (+), Save, Discard, and Change group. A note says 'This recovery plan contains 1 machine(s.)'. The main table lists the stages and their details:

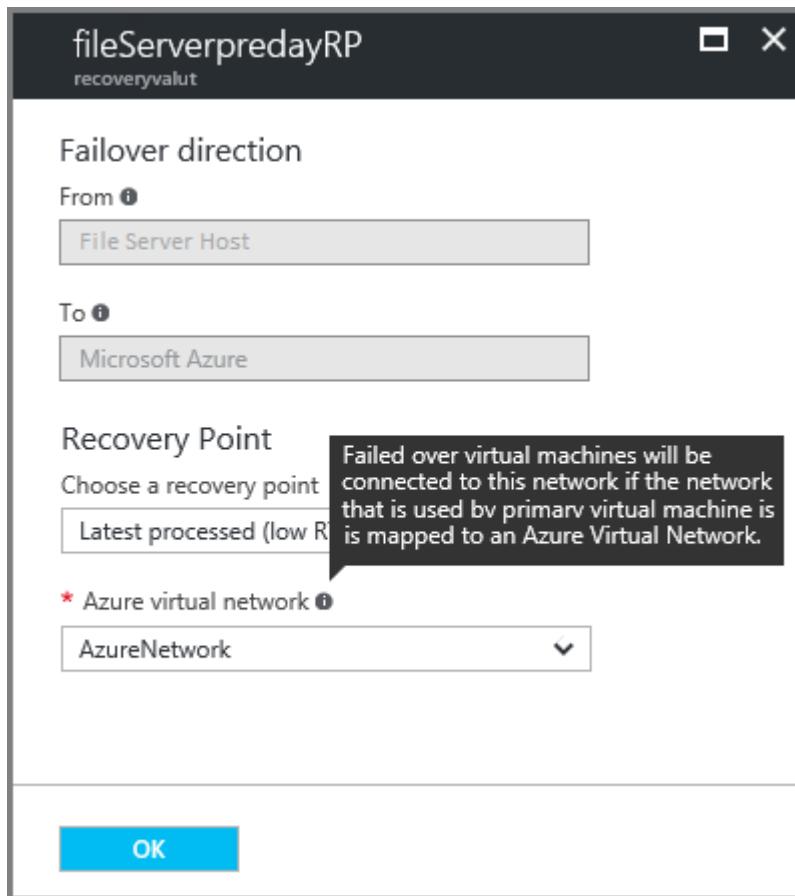
STAGE NAME	DETAILS
▼ All groups shutdown: Pre-steps	1 Step
Script: Failover-StorSimple-Volume-Containers	Script
All groups shutdown	1 machine in 1 group.
▼ All groups failover	
▶ Machines	1 Machine
▼ Group 1: Start	1 Machine
asr-vm-ibiza-1	Machine
▼ Group 1: Post-steps	6 Steps
Script: Start-StorSimple-Virtual-Appliance	Script
Script: Failover-StorSimple-Volume-Containers	Script
Script: Mount-Voumes-After-Failover	Script
Script: Uninstall-Custom-Script-Extension	Script
Manual: TFO Testing	Manual action
Script: Cleanup	Script

Perform a test failover

Refer to the [Active Directory DR Solution](#) companion guide for considerations specific to Active Directory during the test failover. The on-premises setup is not disturbed at all when the test failover occurs. The StorSimple volumes that were attached to the on-premises VM are cloned to the StorSimple Cloud Appliance on Azure. A VM for test purposes is brought up in Azure and the cloned volumes are attached to the VM.

To perform the test failover

1. In the Azure portal, select your Site Recovery vault.
2. Click the recovery plan created for the file server VM.
3. Click **Test Failover**.
4. Select the Azure virtual network to which Azure VMs will be connected after failover occurs.



5. Click **OK** to begin the failover. You can track progress by clicking on the VM to open its properties, or on the **Test failover job** in vault name > **Jobs** > **Site Recovery jobs**.
6. After the failover completes, you should also be able to see the replica Azure machine appear in the Azure portal > **Virtual Machines**. You can perform your validations.

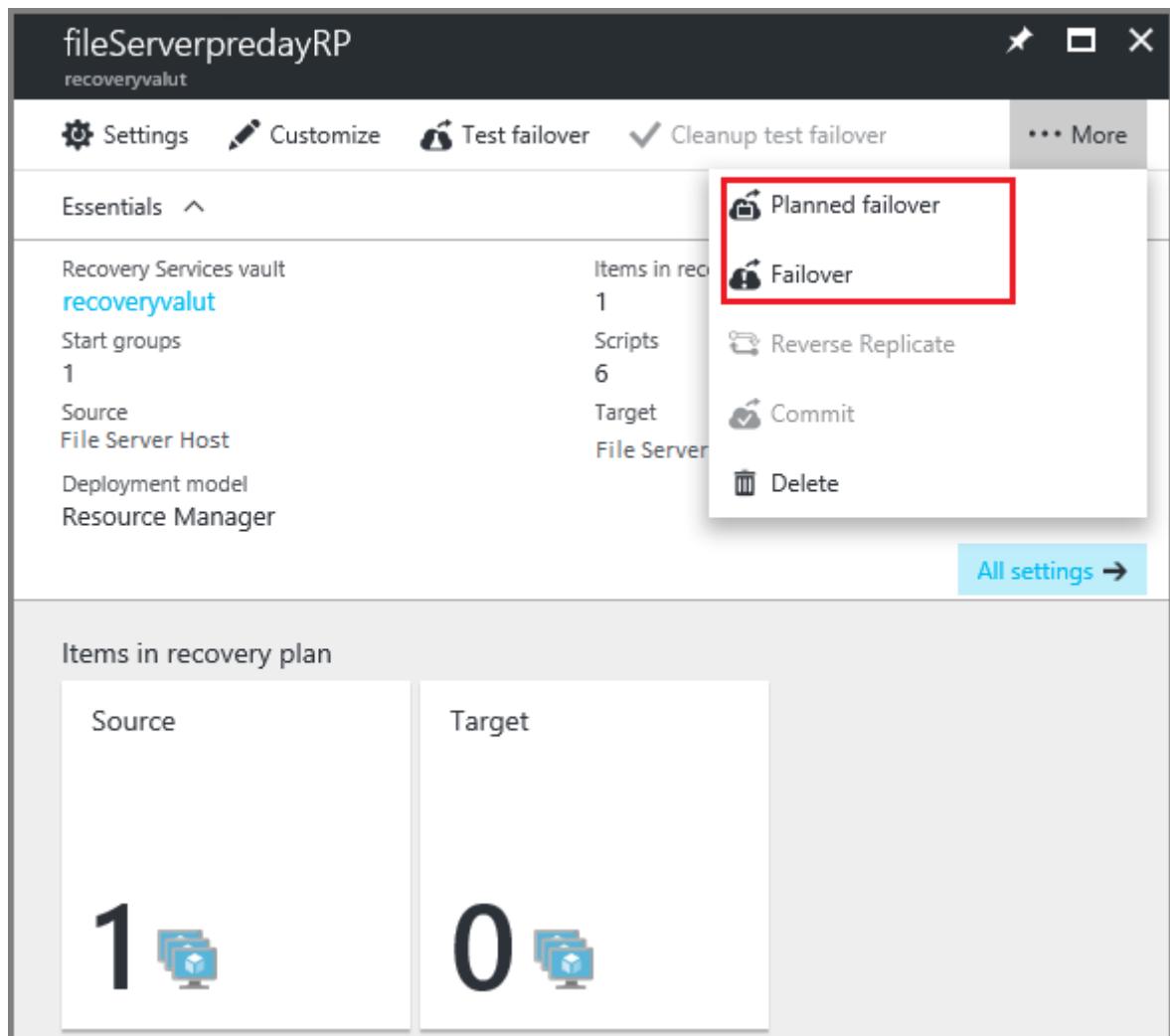
7. After the validations are done, click **Validations Complete**. This will remove the StorSimple Volumes and shut down the StorSimple Cloud Appliance.
8. Once you're done, click **Cleanup test failover** on the recovery plan. In Notes record and save any observations associated with the test failover. This will delete the virtual machine that were created during test failover.

Perform a planned failover

During a planned failover, the on-premises file server VM is shut down gracefully and a cloud backup snapshot of the volumes on StorSimple device is taken. The StorSimple volumes are failed over to the virtual device, a replica VM is brought up on Azure, and the volumes are attached to the VM.

To perform a planned failover

1. In the Azure portal, select **Recovery services vault > Recovery plans (Site Recovery) > recoveryplan_name** created for the file server VM.
2. On the Recovery plan blade, Click **More > Planned failover**.



3. On the **Confirm Planned Failover** blade, choose the source and target locations and select target network and click the check icon ✓ to start the failover process.
4. After replica virtual machines are created they're in a commit pending state. Click **Commit** to commit the failover.
5. After replication is complete, the virtual machines start up at the secondary location.

Perform a failover

During an unplanned failover, the StorSimple volumes are failed over to the virtual device, a replica VM will be brought up on Azure, and the volumes are attached to the VM.

To perform a failover

1. In the Azure portal, select **Recovery services vault** > **Recovery plans (Site Recovery)** > **recoveryplan_name** created for the file server VM.
2. On the Recovery plan blade, Click **More** > **Failover**.
3. On the **Confirm Failover** blade, choose the source and target locations.
4. Select **Shut down virtual machines and synchronize the latest data** to specify that Site Recovery should try to shut down the protected virtual machine and synchronize the data so that the latest version of the data will be failed over.
5. After the failover, the virtual machines are in a commit pending state. Click **Commit** to commit the failover.

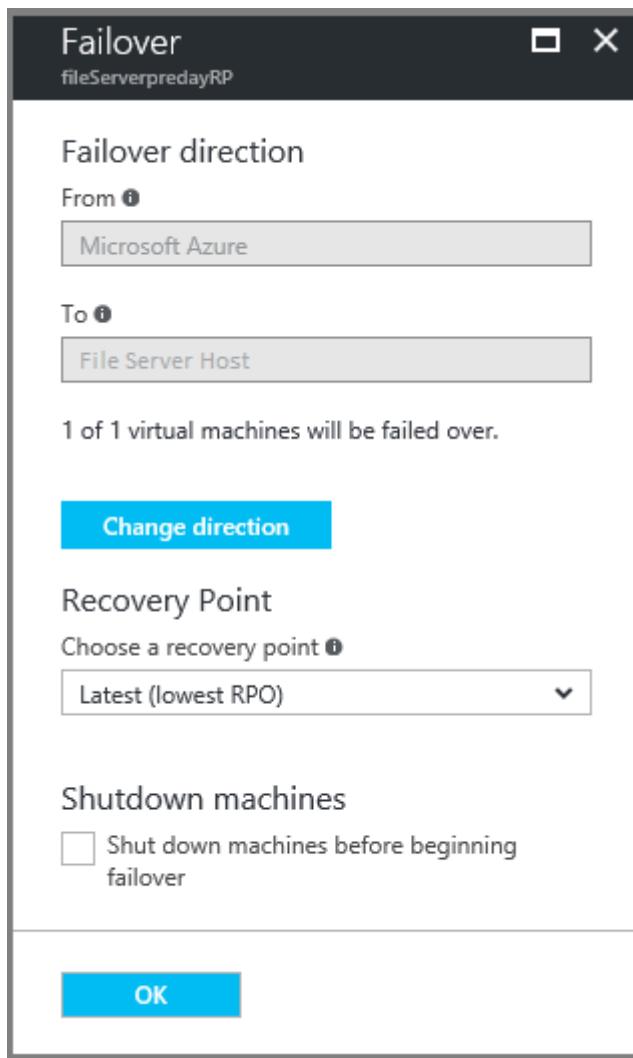
Perform a failback

During a failback, StorSimple volume containers are failed over back to the physical device after a backup is taken.

To perform a failback

1. In the Azure portal, select **Recovery services vault** > **Recovery plans (Site Recovery)** > **recoveryplan_name** created for the file server VM.
2. On the Recovery plan blade, Click **More** > **Planned Failover**.
3. Choose the source and target locations, select the appropriate Data synchronization and VM creation options.

4. Click OK button to start the failback process.



Best Practices

Capacity planning and readiness assessment

Hyper-V site

Use the [User Capacity planner tool](#) to design the server, storage, and network infrastructure for your Hyper-V replica environment.

Azure

You can run the [Azure Virtual Machine Readiness Assessment tool](#) on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery Services. The Readiness Assessment Tool checks VM configurations and warns when configurations are incompatible with Azure. For example, it issues a warning if a C: drive is larger than 127 GB.

Capacity planning is made up of at least two important processes:

- Mapping on-premises Hyper-V VMs to Azure VM sizes (such as A6, A7, A8, and A9).
- Determining the required Internet bandwidth.

Limitations

- Currently, only 1 StorSimple device can be failed over (to a single StorSimple Cloud Appliance). The scenario of a file server that spans several StorSimple devices is not yet supported.
- If you get an error while enabling protection for a VM, make sure that you have disconnected the iSCSI targets.
- All the volume containers that have been grouped together because of backup policies spanning across volume containers will be failed over together.
- All the volumes in the volume containers you have chosen will be failed over.
- Volumes that add up to more than 64 TB can't be failed over because the maximum capacity of a single StorSimple Cloud Appliance is 64 TB.
- If the planned/unplanned failover fails and the VMs are created in Azure, then do not clean up the VMs. Instead, do a fallback. If you delete the VMs then the on-premises VMs cannot be turned on again.
- After a failover, if you are not able to see the volumes, go to the VMs, open Disk Management, rescan the disks, and then bring them online.
- In some instances, the drive letters in the DR site might be different than the letters on-premises. If this occurs, you will need to manually correct the problem after the failover is finished.
- Failover job timeout: The StorSimple script will time out if the failover of volume containers takes more time than the Azure Site Recovery limit per script (currently 120 minutes).
- Backup job timeout: The StorSimple script times out if the backup of volumes takes more time than the Azure Site Recovery limit per script (currently 120 minutes).

 **Important**

Run the backup manually from the Azure portal and then run the recovery plan again.

- Clone job timeout: The StorSimple script times out if the cloning of volumes takes more time than the Azure Site Recovery limit per script (currently 120 minutes).
- Time synchronization error: The StorSimple scripts errors out saying that the backups were unsuccessful even though the backup is successful in the portal. A possible cause for this might be that the StorSimple appliance's time might be out of sync with the current time in the time zone.

ⓘ Important

Sync the appliance time with the current time in the time zone.

- Appliance failover error: The StorSimple script might fail if there is an appliance failover when the recovery plan is running.

ⓘ Important

Rerun the recovery plan after the appliance failover is complete.

Summary

Using Azure Site Recovery, you can create a complete automated disaster recovery plan for a file server VM having file shares hosted on StorSimple storage. You can initiate the failover within seconds from anywhere in the event of a disruption and get the application up and running in a few minutes.

Use the service summary blade for StorSimple 8000 series device

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Device Manager service summary blade provides a summary view of all the devices that are connected to the StorSimple Device Manager service, highlighting those devices that need a system administrator's attention. This tutorial introduces the service summary blade, explains the dashboard content and function, and describes the tasks that you can perform from this page.

The screenshot shows the StorSimple service summary blade. At the top, there are management commands: 'Create cloud appliance', 'Add volume container', 'Add volume', and 'Delete'. Below these, the 'Essentials' section is highlighted with a red box, displaying the resource group 'MySS8000RG', location 'Southeast Asia', and subscription information ('Subscription name: Internal Consumption', 'Subscription ID: 2136cf2e-684f-487b-9fc4-0acc9c0166e'). To the right of this, another red box highlights the capacity summary: 'Capacity PROVISIONED 5.37 TB', 'REMAINING 383.84 TB OR 16.61 TB', and 'Tiered Local'. Below this, a chart titled 'Docs-mySS8000series - Usage - Past 7 days' shows storage usage over time, with three bars at 0 GB each for Primary Tiered Storage, Primary Locally Pinned Storage, and Cloud Storage Used.

Management commands

In the StorSimple service summary blade, you see the options for managing your StorSimple Device Manager service and the StorSimple 8000 series devices registered to this service. You see the management commands across the top of the blade and on the left side.

This screenshot shows the same top navigation bar as the previous one, but without the 'Essentials' section highlighted. It includes the same four management commands: 'Create cloud appliance', 'Add volume container', 'Add volume', and 'Delete'.

Use these options to perform various operations such as add shares or volumes, or monitor the various jobs running on the StorSimple devices.

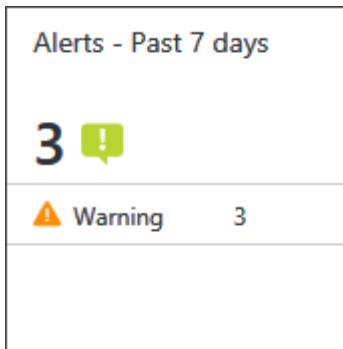
Essentials

The essentials area captures some of the important properties such as, the resource group, location, and subscription in which your StorSimple Device Manager was created.

Essentials ^	
Resource group	Subscription name
MySS8000RG	Internal Consumption
Location	Subscription ID
Southeast Asia	2136cf2e-684f-487b-9fc4-0accc9c0166e

StorSimple Device Manager service summary

- The **Alerts** tile provides a snapshot of all the active alerts across all devices, grouped by alert severity.

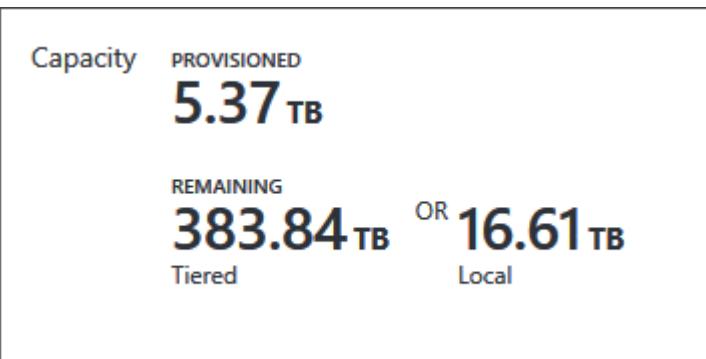


Clicking the tile opens the **Alerts** blade, where you can click an individual alert to view additional details about that alert, including any recommended actions. You can also clear the alert if the issue has been resolved.

The image shows a screenshot of the "Alerts" blade. The blade has a dark header with the title "Alerts". On the left is a vertical toolbar with icons for creating a new alert, viewing device status, and other management functions. The main area has a grid with the following data:

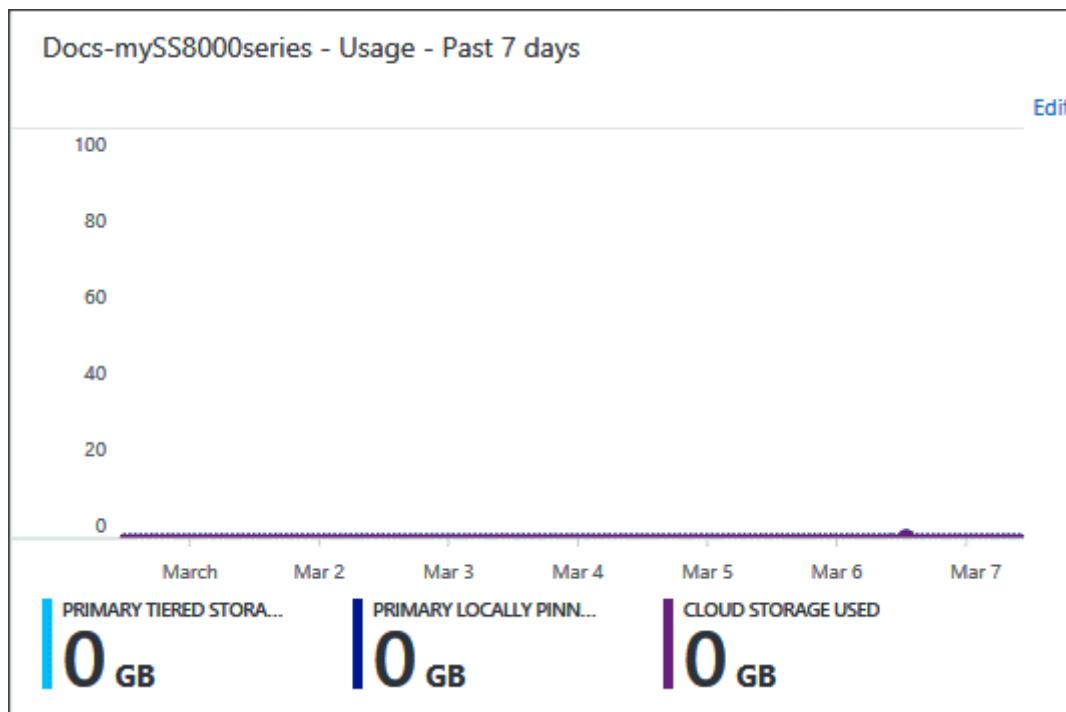
NAME	STATUS	SEVERITY	SOURCE	DURATION
Microsoft Support session has begun	Active	⚠ Warning	8100-SHX0991003G...	2 Hours, 44 Minutes
Unable to automatically check for new updates	Active	⚠ Warning	8100-SHX0991003G...	4 Days, 2 Hours
Microsoft Support session has begun	Active	⚠ Warning	8100-SHX0991003G...	4 Days, 2 Hours

- The **Capacity** tile displays shows the primary storage that is provisioned and remaining across all devices relative to the total storage available across all devices. **Provisioned** refers to the amount of storage that is prepared and allocated for use, **Remaining** refers to the remaining capacity that can be provisioned across all devices.



The **Remaining Tiered** capacity is the available capacity that can be provisioned including cloud, while the **Remaining Local** is the capacity remaining on the disks attached to the StorSimple 8000 series devices.

- In the **Usage** chart, you can see the relevant metrics for your devices. You can view the primary storage used across all devices, and the cloud storage consumed by devices over the past 7 days, the default time period.



To choose a different time scale, use the **Edit** option in the top-right corner of the chart.

Edit chart

Docs-mySS8000series

Time range

Past 7 days

Choose metrics

- Primary Tiered Storage Used
- Primary Locally Pinned Storage Used
- Cloud Storage Used

Save

Docs-mySS8000series - Usage

Docs-mySS8000series



Edit chart

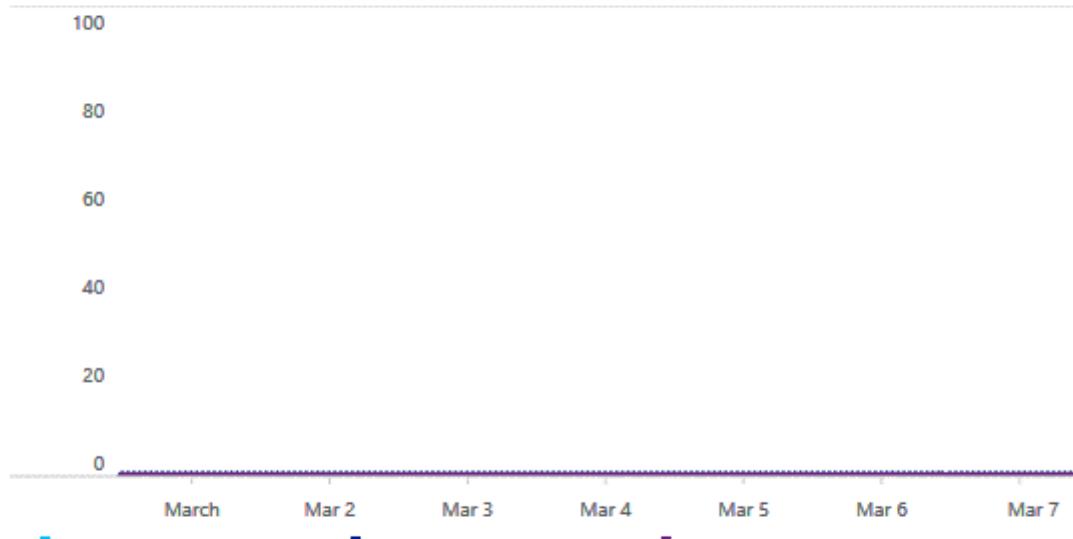
Export data



Cloud storage includes both tiered and backup storage usage. Primary tiered or locally pinned is the actual volumes usage.



Docs-mySS8000series - Usage - Past 7 days



METRIC NAME	CURRENT	GROWTH	RANGE
Primary Tiered Storage Used	0 GB	0 GB	0 GB - 0 GB
Primary Locally Pinned Storage Used	0 GB	0 GB	0 GB - 0 GB
Cloud Storage Used	0 GB	0 GB	0 GB - 0 GB

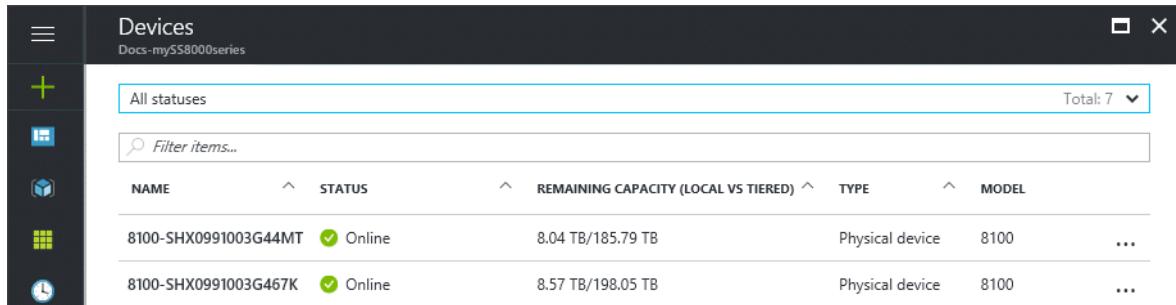
- The **Devices** tile provides a summary of the number of StorSimple 8000 series devices in your StorSimple Device Manager grouped by device status.

Devices

2

Online	2
--------	---

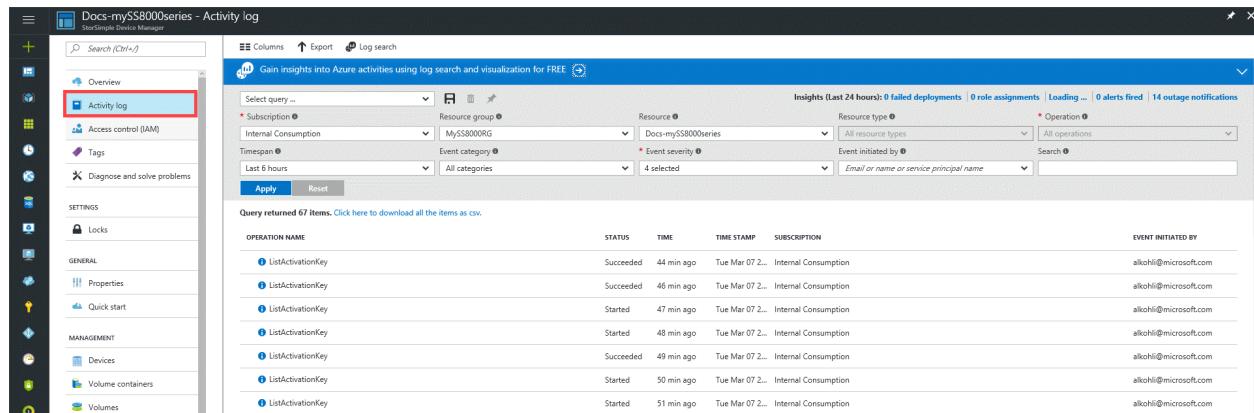
Click this tile to open the **Devices** list blade and then click an individual device to drill into the device summary specific to the device. You can also perform device-specific actions from a given device summary blade. For more information about the device summary blade, go to [Device summary blade](#).



The screenshot shows the 'Devices' list blade for the 'Docs-mySS800series' service. It includes a sidebar with icons for creating new devices, managing access control, and diagnosing problems. The main area displays a table with columns: NAME, STATUS, REMAINING CAPACITY (LOCAL VS TIERED), TYPE, and MODEL. Two devices are listed: '8100-SHX0991003G44MT' and '8100-SHX0991003G467K', both marked as 'Online'. The remaining capacity is 8.04 TB/185.79 TB and 8.57 TB/198.05 TB respectively. The type is 'Physical device' and the model is '8100'.

View the activity logs

To view the various operations carried out within your StorSimple Device Manager, click the **Activity logs** link on the left side of your StorSimple service summary blade. This takes you to the **Activity logs** blade, where you can see a summary of the recent operations carried out.



The screenshot shows the 'Activity log' blade for the 'Docs-mySS800series' service. The left sidebar lists navigation options like Overview, Activity log (which is selected and highlighted in red), Access control (IAM), Tags, and Diagnose and solve problems. The main area features a search bar and filter controls for 'Select query', 'Subscription', 'Resource group', 'Resource', 'Event category', 'Event severity', 'Event initiated by', and 'Time span'. Below these, a table lists 67 recent operations. The columns include OPERATION NAME, STATUS, TIME, TIME STAMP, SUBSCRIPTION, and EVENT INITIATED BY. Most operations are 'ListActivationKey' requests, mostly succeeded or started, with timestamps ranging from 46 min ago to 51 min ago. The 'Event initiated by' column consistently shows 'alkohil@microsoft.com'.

Next steps

- Learn more about how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Use the device summary in StorSimple Device Manager service

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple device summary blade gives you an overview of information for a specific StorSimple device, in contrast to the service summary blade, which gives you information about all the devices included in your Microsoft Azure StorSimple solution.

The device summary blade provides a summary view of a StorSimple 8000 series device that is registered with a given StorSimple Device Manager, highlighting those device issues that need a system administrator's attention. This tutorial introduces the device summary blade, explains the content and function, and describes the tasks that you can perform from this blade.

The device summary blade displays the following information:

The screenshot shows the StorSimple device blade interface. At the top, there's a navigation bar with icons for Settings, Add volume container, Add volume, Fail over, and More. Below this is the 'Essentials' section, which displays device status (Status: Online, Model: 8100), Target IQN (iqn.1991-05.com.microsoft:storsimple8100-...), and Device software version (StorSimple 8000 Series Update 3.0). A blue 'All settings →' button is located at the bottom right of this section. The main content area is divided into several sections: 'Monitoring' (Alerts - Past 7 days: 1 Warning, 1 Device s...; Status and health: Hardwar... OK, Device s... Online; Volumes: 3 Online); 'Usage' (8100-SHX0991003G44MT - Usage - Past 24 hours, showing Primary Tiered Storage, Primary Locally Pinned Storage, and Cloud Storage Used, all measured in GB); and 'Capacity' (PROVISIONED: 3.42 TB, REMAINING: 185.79 TB Tiered OR 8.04 TB Local).

Management command bar

In the StorSimple device blade, you see the options for managing your StorSimple device. You see the management commands across the top of the blade and on the left side. Use these options to add shares or volumes, or update or fail over your device.

Essentials

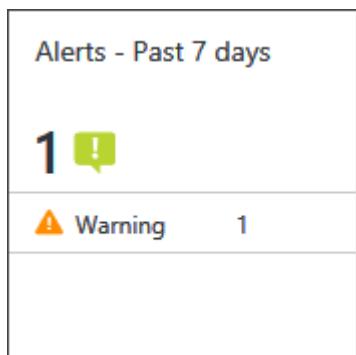
The essentials area captures some of the important properties such as, the status, model, target IQN, and the software version.

Status	Model
Online	8100
Target IQN	Device software version
iqn.1991-05.com.microsoft:storsimple8100-...	StorSimple 8000 Series Update 3.0

[All settings →](#)

Monitoring

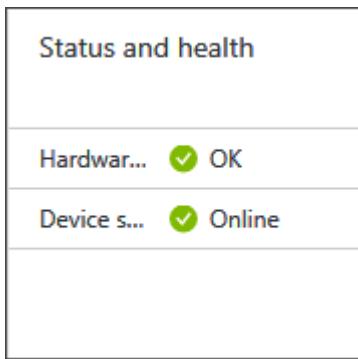
- The **Alerts** tile provides a snapshot of all the active alerts for your device, grouped by alert severity.



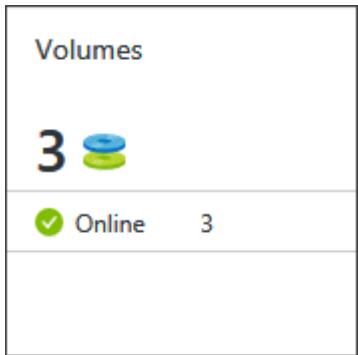
Click the tile to open the **Alerts** blade and then click an individual alert to view additional details about that alert, including any recommended actions. You can also clear the alert if the issue has been resolved.

The blade has a dark header with the word "Alerts". Below the header are four filter dropdowns: "Time range" set to "Past 7 days", "Devices" set to "8100-SHX0991003G44MT", "Severity" set to "All", and "Status" set to "Active". There are "Apply" and "Reset" buttons below the filters. A message says "The query returned 1 items." A search bar labeled "Filter items..." is present. A table follows, with the first row (header) showing columns: NAME, STATUS, SEVERITY, SOURCE, DURATION. The second row (data) contains the alert details: "Microsoft Support session has begun", "Active", "Warning", "8100-SHX0991003G...", and "1 Hour, 14 Minutes". This last row is highlighted with a red rectangle.

- The **Status and health** tile provides insights into the hardware component health for a device including the device status. The device status may be offline, online, deactivated, or ready to set up.



- The **Volumes** tile provides a summary of the number of volumes in your device grouped by status.



Click the tile to open the **Volumes** list blade, and then click on an individual volume to view or modify its properties.

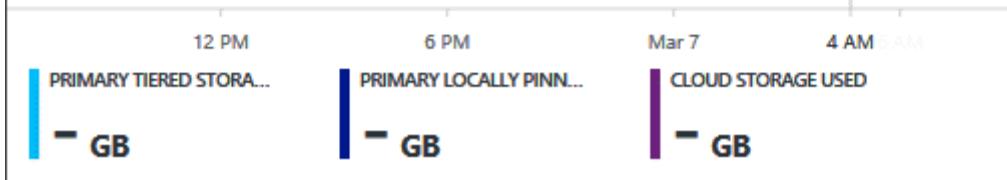
Volumes							
8100-SHX0991003G44MT							
+ Add volume							
<input type="text"/> Filter items...							
NAME	^	STATUS	TYPE	CAPACITY	BACKUP	CONNECTED...	MONITORING
▼ myssvolcont2...							
myssvolarc...	✓ Online	Tiered (Archived)	1000 GB	Enabled	myssacr2	Disabled	...
myssvolsrc...	✓ Online	Tiered	1.95 TB	Enabled	myssacr1	Disabled	...
▼ myvolcont3 (1)							
myvolsql1	✓ Online	Locally pinned	500 GB	Enabled	myssacr1	Disabled	...

For more information, see how to [manage volumes](#).

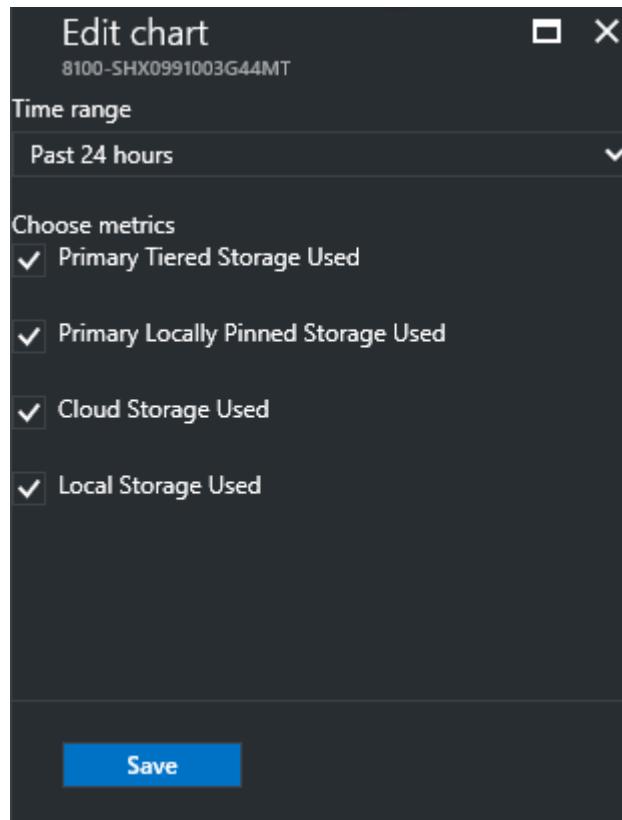
- In the **Usage** chart, you can view the primary storage used across your device, and the cloud storage consumed over the past 7 days, the default time period.

8100-SHX0991003G44MT - Usage - Past 24 hours

Edit



To choose a different time scale, use the **Edit** option in the top-right corner of the chart.



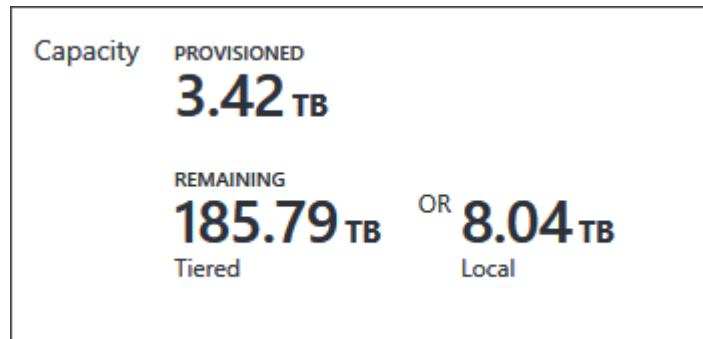
In this chart, you can view metrics for the total primary storage (the amount of data written by hosts to your device) and the total cloud storage consumed by your device over a period of time.

In this context, *primary storage* refers to the total amount of data written by the host, and can be broken down by volume type: *primary tiered storage* includes both locally stored data and data tiered to the cloud. *Primary locally pinned*

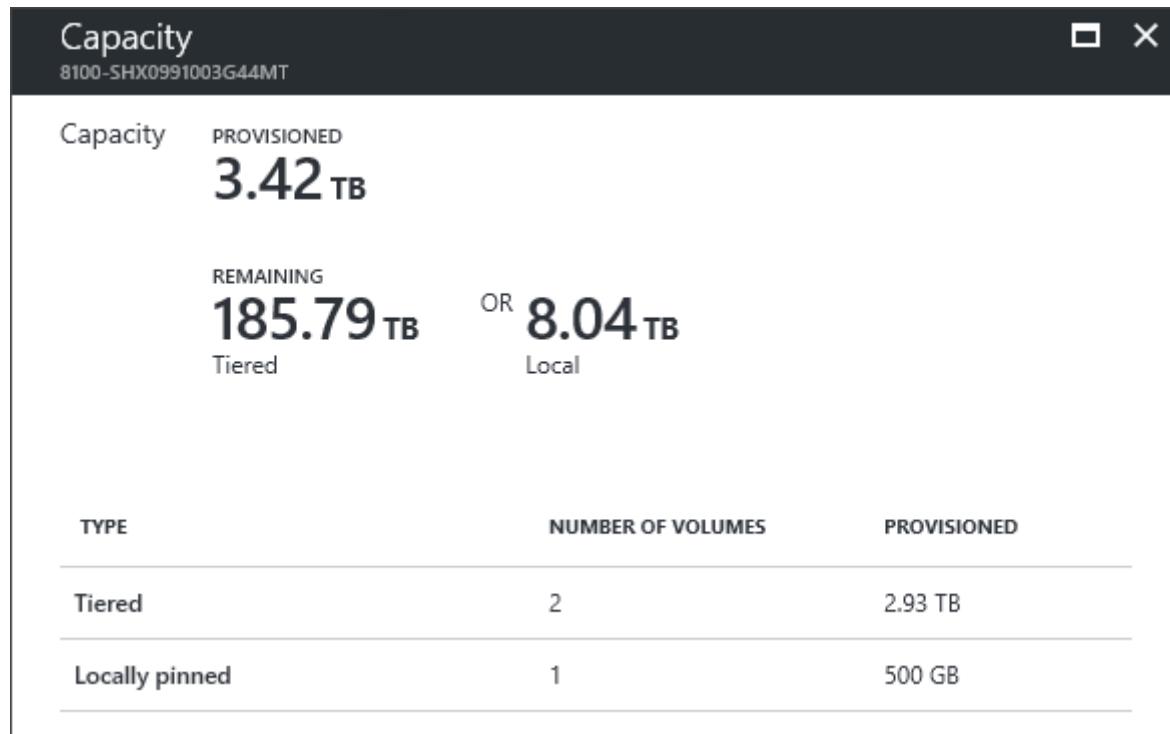
storage includes just data stored locally. *Cloud storage*, on the other hand, is a measurement of the total amount of data stored in the cloud. This storage includes tiered data and backups. The data stored in the cloud is deduplicated and compressed, whereas primary storage indicates the amount of storage used before the data is deduplicated and compressed. (You can compare these two numbers to get an idea of the compression rate.) For both primary and cloud storage, the amounts shown are based on the tracking frequency you configure. For example, if you choose a one week frequency, then the chart shows data for each day in the previous week.

To see the amount of cloud storage consumed over time, select the **CLOUD STORAGE USED** option. To see the total storage that has been written by the host, select the **PRIMARY TIERED STORAGE USED** and **PRIMARY LOCALLY PINNED STORAGE USED** options. For more information, see [Use the StorSimple Device Manager service to monitor your StorSimple device](#).

- The **Capacity** tile displays the primary storage that is provisioned and remaining across the device relative to the total storage available for the same. **Provisioned** refers to the amount of storage that is prepared and allocated for use, **Remaining** refers to the remaining capacity that can be provisioned across this device.



Click this tile to view how the capacity is provisioned across tiered and locally pinned volumes. The **Remaining Tiered** capacity is the available capacity that can be provisioned including cloud, while the **Remaining Local** is the capacity remaining on the disks attached to this device.



Next steps

- Learn more about the StorSimple service summary blade.
- Learn more about [using the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to monitor your StorSimple device

Article • 08/19/2022 • 8 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

You can use the StorSimple Device Manager service to monitor specific devices within your StorSimple solution. You can create custom charts based on I/O performance, capacity utilization, network throughput, and device performance metrics and pin those to the dashboard. For more information, go to [customize your portal dashboard](#).

To view the monitoring information for a specific device, in the Azure portal, select the StorSimple Device Manager service. From the list of devices, select your device and then go to **Monitor**. You can then see the **Capacity**, **Usage**, and **Performance** charts for the selected device.

Capacity

Capacity tracks the provisioned space and the space remaining on the device. The remaining capacity is then displayed as locally pinned or tiered.

The provisioned and remaining capacity is further broken down by tiered and locally pinned volumes. For each volume, the provisioned capacity, and the remaining capacity on the device is displayed.

The screenshot shows three main windows:

- Capacity**: Displays total capacity of 1.58 TB, remaining capacity of 196.28 TB or 8.5 TB, and a table showing the number of volumes and provisioned capacity by type (Tiered and Locally pinned).
- Volumes**: A list of volumes including myssfvol1 (Tiered, 500 GB, Online), myssfvol2 (Tiered (Arc...), 1000 GB, Disabled), and myssvolcont1 (Locally pinned, 100 GB, Online).
- Settings**: A sidebar with sections for GENERAL, MANAGE (Volumes, Volume containers, Backup policies, Backup catalog), and MONITOR (Capacity, Usage, Performance, Health). The Capacity section is highlighted with a red box.

Usage

Usage tracks metrics related to the amount of data storage space that is used by the volumes, volume containers, or device. You can create reports based on the capacity utilization of your primary storage, your cloud storage, or your device storage. Capacity utilization can be measured on a specific volume, a specific volume container, or all volume containers. By default, the usage for past 24 hours is reported. You can edit the chart to change the duration over which the usage is reported by selecting from:

- Past 24 hours
- Past 7 days
- Past 30 days
- Past 90 days
- Past year

Two key metrics, growth and range are reported for the usage charts. Range refers to the maximum value and the minimum values of the usage reported over the selected duration (for instance, Past 7 days).

Growth refers to the increase in usage from the first day to the last day over the selected duration.

Growth and range can also be represented by the following equations:

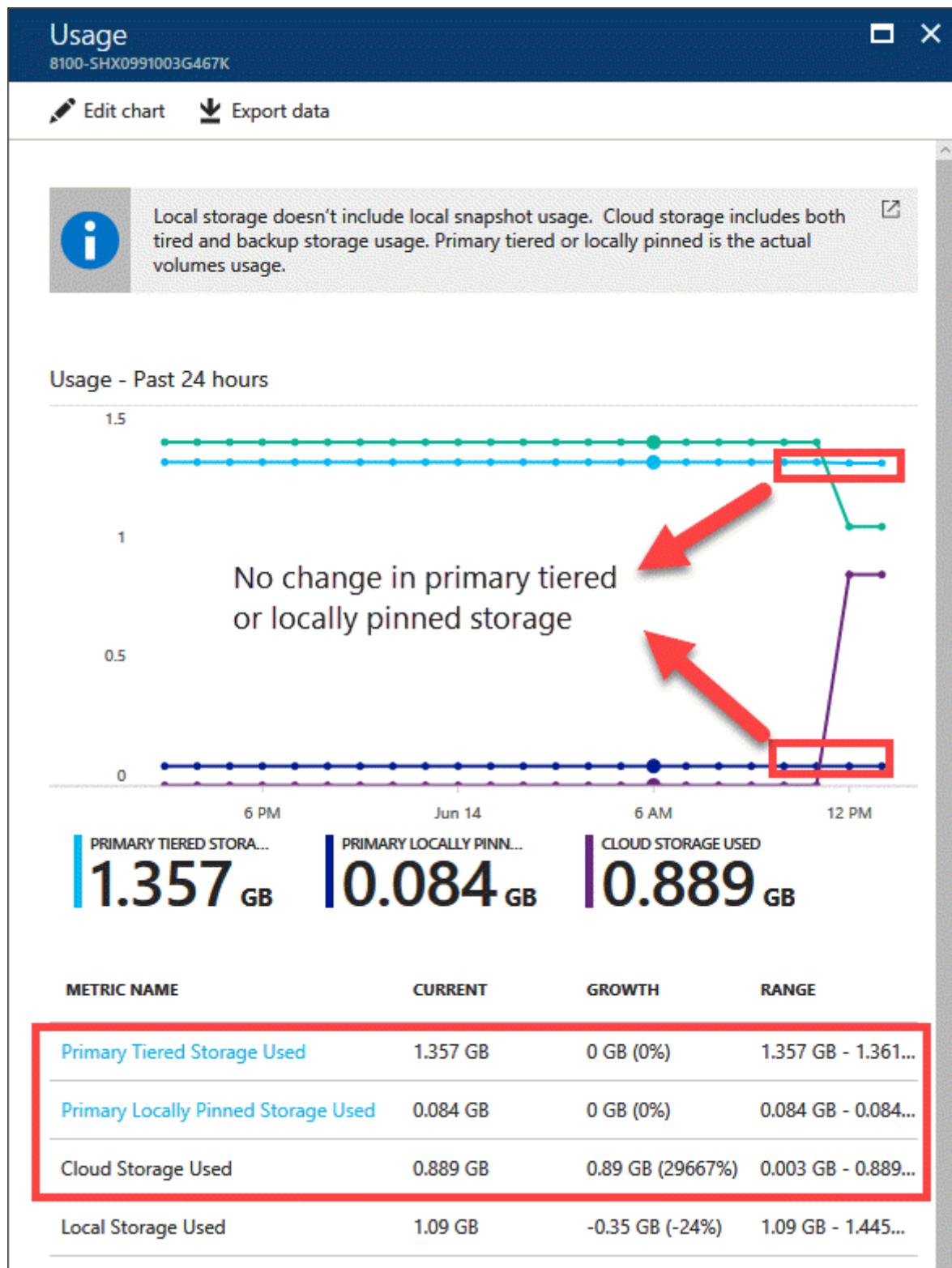
$\text{Range} = \{\text{Usage(minimum)}, \text{Usage(maximum)}\}$ $\text{Growth} = \text{Usage(Last day)} - \text{Usage(first day)}$ $\text{Growth (\%)} = [(\text{Usage(last day)} - \text{Usage(first day)}) / \text{Usage(first day)}] \times 100$

The primary, cloud, and local storage used can be described as follows:

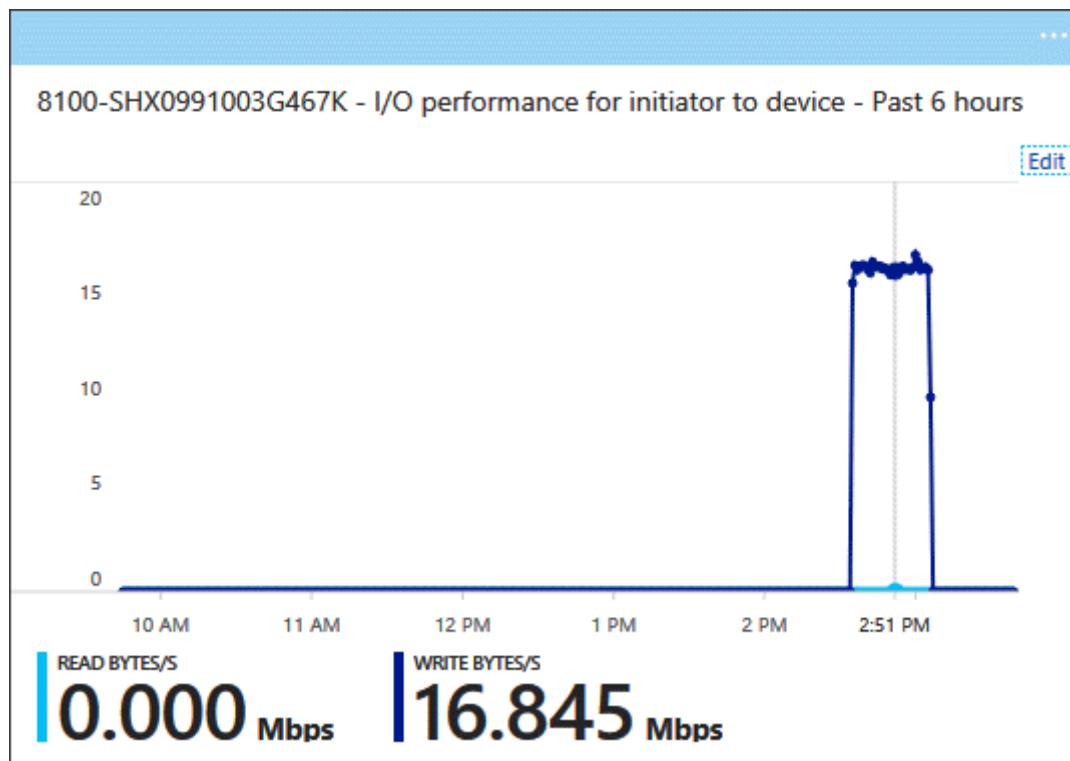
Primary storage usage

These charts show the amount of data written to StorSimple volumes before the data is deduplicated and compressed. You can view the primary storage used by all volumes in a volume container or for a single volume. The primary storage used is further broken down by primary tiered storage used and primary locally pinned storage used.

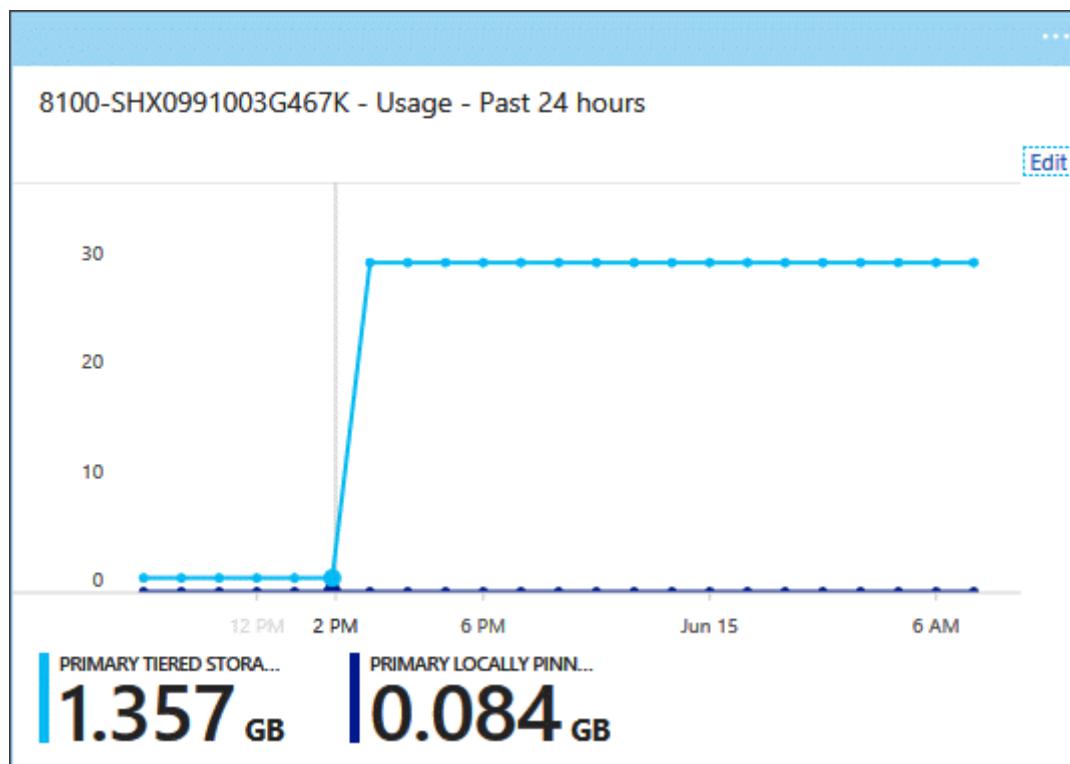
The following charts show the primary storage used for a StorSimple device before and after a cloud snapshot was taken. As this is just volume data, a cloud snapshot should not change the primary storage. As you can see, the chart shows no difference in the primary tiered or locally pinned storage used as a result of taking a cloud snapshot. The cloud snapshot started at around 11:50 pm on that device.



If you now run IO on the host connected to your StorSimple device, you will see an increase in primary tiered storage or primary locally pinned storage used depending upon which volumes (tiered or locally pinned) you write the data to. Here are the primary storage usage charts for a StorSimple device. On this device, the StorSimple host started serving writes at around 2:30 pm on a tiered volume on the device. You can see the peak in the write bytes/s corresponding to the IO running on the host.



If you look at the primary tiered storage used, that has gone up whereas the primary locally pinned usage stays unchanged as there are no writes served to the locally pinned volumes on the device.



If you are running Update 3 or higher, you can break down the primary storage capacity utilization by an individual volume, all volumes, all tiered volumes, and all locally pinned volumes as shown below. Breaking down by all locally pinned volumes will allow you to quickly ascertain how much of the local tier is used up.

Usage
8100-SHX0991003G467K

Edit chart Export data

Local storage doesn't include local snapshot usage. Cloud storage includes both tiered and backup storage usage. Primary tiered or locally pinned is the actual volumes usage.

Usage - Past 7 days

Metric Name	Current	Growth	Range
Primary Tiered Storage Used	1.068 GB	1.07 GB	0 GB - 1.068 GB
Primary Locally Pinned Storage Used	0.084 GB	0.08 GB	0 GB - 0.084 GB
Cloud Storage Used	0.003 GB	0 GB (0%)	0.003 GB - 0.003...
Local Storage Used	1.152 GB	1.15 GB	0 GB - 1.152 GB

Volumes
8100-SHX0991003G467K

+ Add volume

Tiered

NAME	STATUS	TYPE	CAPACI...	BACKUP	CONNECTED HOSTS	MONIT...
myssfsvol1 (2)	Online	Tiered	500 GB	Disabled	myssacr1	Enabled
myssfsvol2	Online	Tiered (Arc...	1000 GB	Enabled	myssacr2	Enabled
myssvolcont1 (0)						

Usage
8100-SHX0991003G467K

Edit chart Export data

Local storage doesn't include local snapshot usage. Cloud storage includes both tiered and backup storage usage. Primary tiered or locally pinned is the actual volumes usage.

Usage - Past 7 days

Metric Name	Current	Growth	Range
Primary Tiered Storage Used	1.068 GB	1.07 GB	0 GB - 1.068 GB
Primary Locally Pinned Storage Used	0.084 GB	0.08 GB	0 GB - 0.084 GB
Cloud Storage Used	0.003 GB	0 GB (0%)	0.003 GB - 0.003...
Local Storage Used	1.152 GB	1.15 GB	0 GB - 1.152 GB

Volumes
8100-SHX0991003G467K

+ Add volume

Locally pinned

NAME	STATUS	TYPE	CAPACI...	BACKUP	CONNECTED HOSTS	MONIT...
myssvc1 (0)						
myssvolcont1 (1)						
myssqlvol1	Online	Locally pin...	100 GB	Disabled	myssacr1	Enabled

You can further click on each of the volumes in the list and see the corresponding usage.

Usage
8100-SHX0991003G467K

Edit chart Export data

Local storage doesn't include local snapshot usage. Cloud storage includes both tiered and backup storage usage. Primary tiered or locally pinned is the actual volumes usage.

Usage - Past 24 hours

Metric Name	Current	Growth	Range
Primary Tiered Storage Used	30.363 GB	29 GB (2131%)	1.357 GB - 30.36...
Primary Locally Pinned Storage Used	0.084 GB	0 GB (0%)	0.084 GB - 0.084...
Cloud Storage Used	29.161 GB	29.16 GB (97200...)	0.005 GB - 29.16...
Local Storage Used	29.516 GB	28.07 GB (1943%)	1.09 GB - 30.452...

Volumes
8100-SHX0991003G467K

+ Add volume

Tiered

NAME	STATUS	TYPE	CAPACI...	BACKUP	CONNECTED HOSTS	MONIT...
myssvc1 (2)	Online	Tiered	500 GB	Enabled	myssacr1	Enabled
myssfsvol1	Online	Tiered	500 GB	Enabled	myssacr1	Enabled
myssfsvol2	Online	Tiered (Arc...	1000 GB	Disabled	myssacr2	Enabled
myssvolcont1 (0)						

myssfsvol1
8100-SHX0991003G467K

Modify Restore Clone Take offline Bring online Delete

Status: Online Capacity: 500 GB
Type: Tiered Backup: Enabled
Monitoring: Enabled
Connected hosts: myssacr1

Associated backup pool: 1 mybupo1

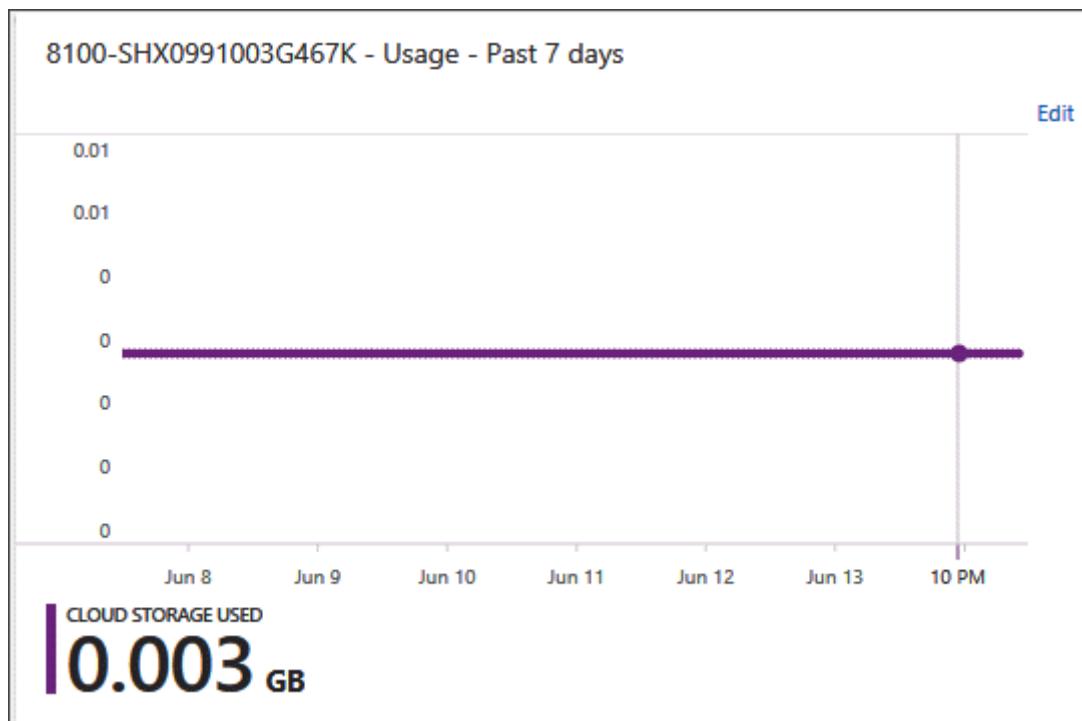
myssfsvol1 - Usage - Past 24 hours

Cloud storage usage

These charts show the amount of cloud storage used. This data is deduplicated and compressed. This amount includes cloud snapshots which might contain data that isn't reflected in any primary volume and is kept for legacy or required retention purposes. You can compare the primary and cloud storage consumption figures to get an idea of the data reduction rate, although the number will not be exact.

The following charts show the cloud storage utilization of a StorSimple device when a cloud snapshot was taken.

- The cloud snapshot started at around 11:50 am on that device and you can see that before the cloud snapshot, there was no cloud storage used.
- Once the cloud snapshot completed, the cloud storage utilization shot up 0.89 GB.
- While the cloud snapshot was in progress, there is also a corresponding peak in the IO from device to cloud.



Usage

8100-SHX0991003G467K



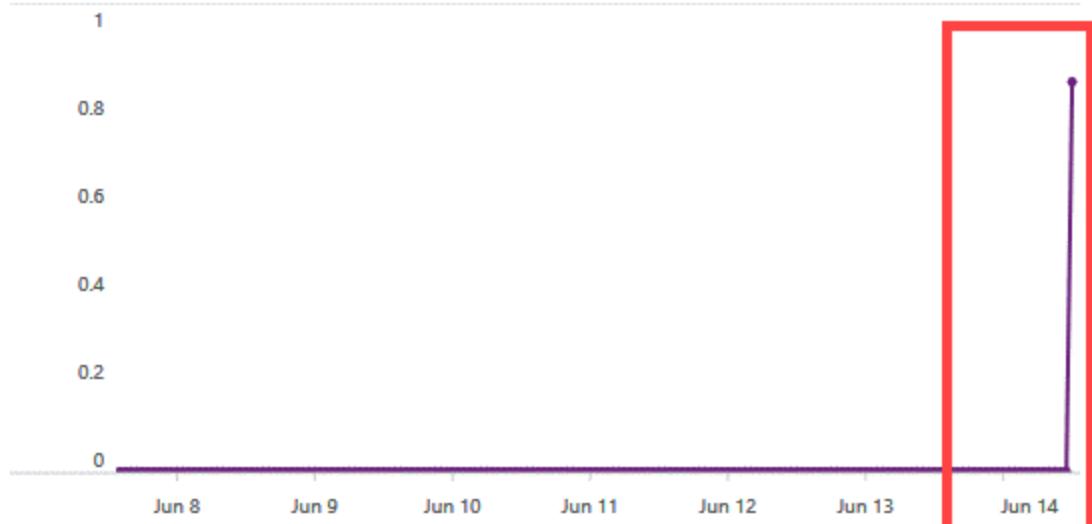
Edit chart

Export data



Local storage doesn't include local snapshot usage. Cloud storage includes both tiered and backup storage usage. Primary tiered or locally pinned is the actual volumes usage.

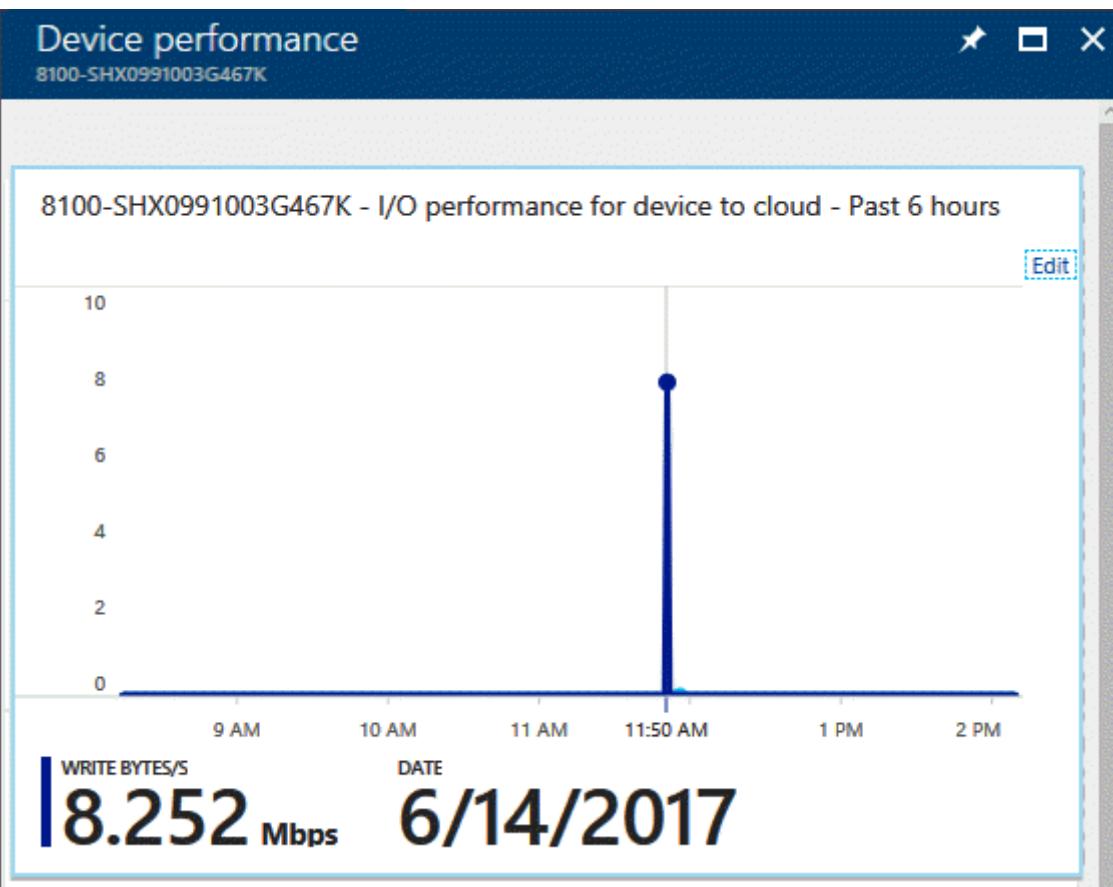
Usage - Past 7 days



CLOUD STORAGE USED

0.889 GB

METRIC NAME	CURRENT	GROWTH	RANGE
Cloud Storage Used	0.889 GB	0.89 GB (29667%)	0.003 GB - 0.889..

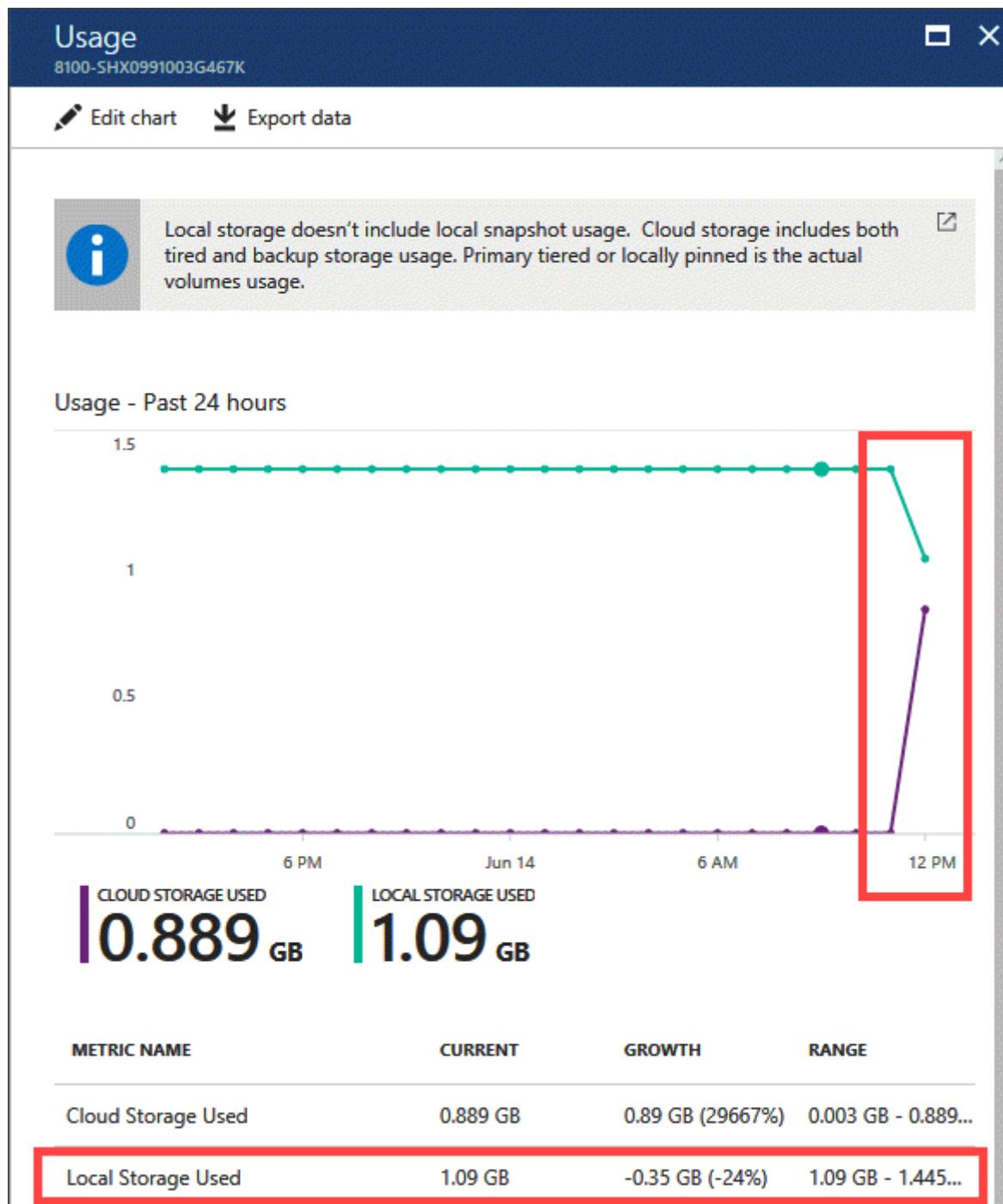


Local storage usage

These charts show the total utilization for the device, which will be more than primary storage usage because it includes the SSD linear tier. This tier contains an amount of data that also exists on the device's other tiers. The capacity in the SSD linear tier is cycled so that when new data comes in, the old data is moved to the HDD tier (at which time it is deduplicated and compressed) and subsequently to the cloud.

Over time, primary storage used and local storage used will most likely increase together until the data begins to be tiered to the cloud. At that point, the local storage used will probably begin to plateau, but the primary storage used will increase as more data is written.

The following charts show the primary storage used for a StorSimple device when a cloud snapshot was taken. The cloud snapshot started at 11:50 am and the local storage started decreasing at that time. The local storage used went down from 1.445 GB to 1.09 GB. This indicates that most likely the uncompressed data in the linear SSD tier was deduplicated, compressed, and moved into the HDD tier. Note that if the device already has a large amount of data in both the SSD and HDD tiers, you may not see this decrease. In this example, the device has a small amount of data.

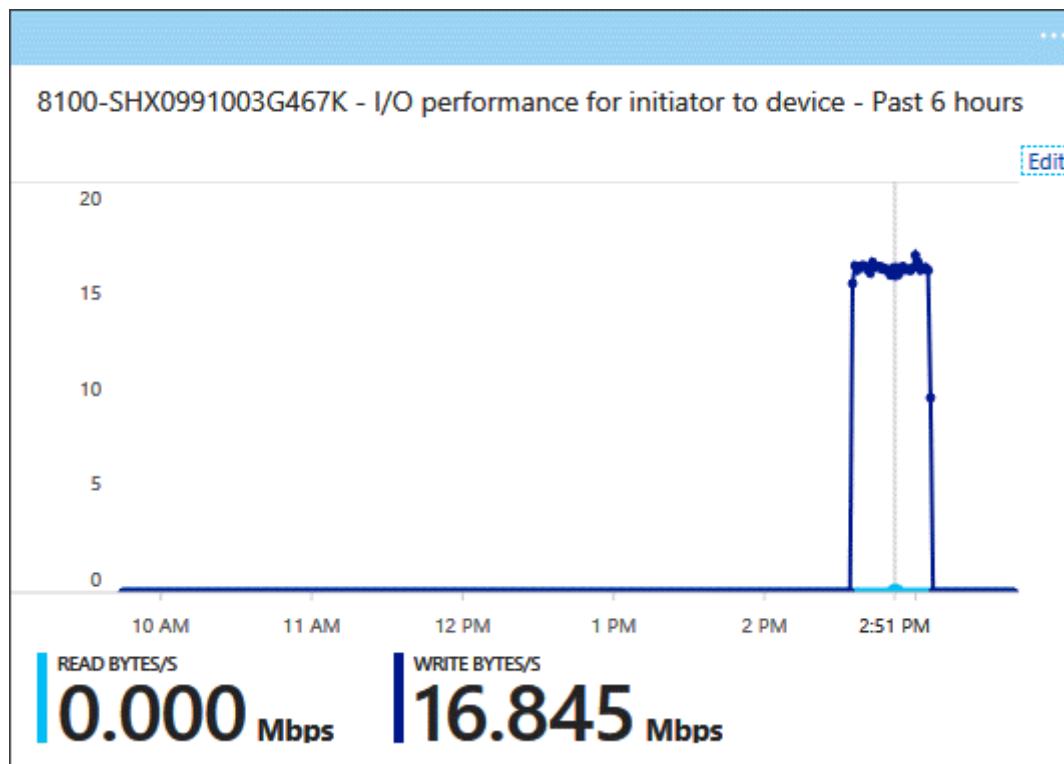


Performance

Performance tracks metrics related to the number of read and write operations between either the iSCSI initiator interfaces on the host server and the device or the device and the cloud. This performance can be measured for a specific volume, a specific volume container, or all volume containers. Performance also includes CPU utilization and Network throughput for the various network interfaces on your device.

I/O performance for initiator to device

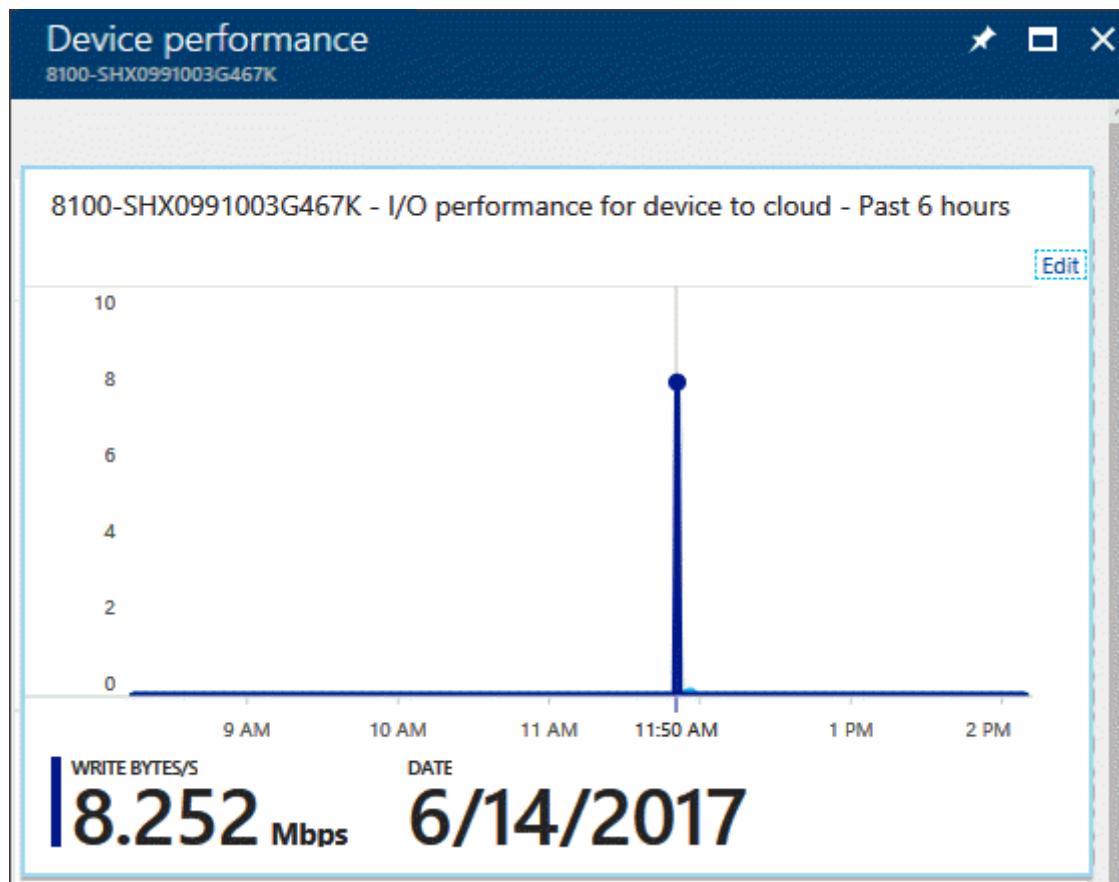
The chart below shows the I/O for the initiator to your device for all the volumes for a production device. The metrics plotted are read and write bytes per second. You can also chart read, write, and outstanding IO, or read and write latencies.



I/O performance for device to cloud

For the same device, the I/O operations are plotted for the data from the device to the cloud for all the volume containers. On this device, the data is only in the linear tier and nothing has spilled to the cloud. There are no read-write operations occurring from device to the cloud. Therefore, the peaks in the chart are at an interval of 5 minutes that corresponds to the frequency at which the heartbeat is checked between the device and the service.

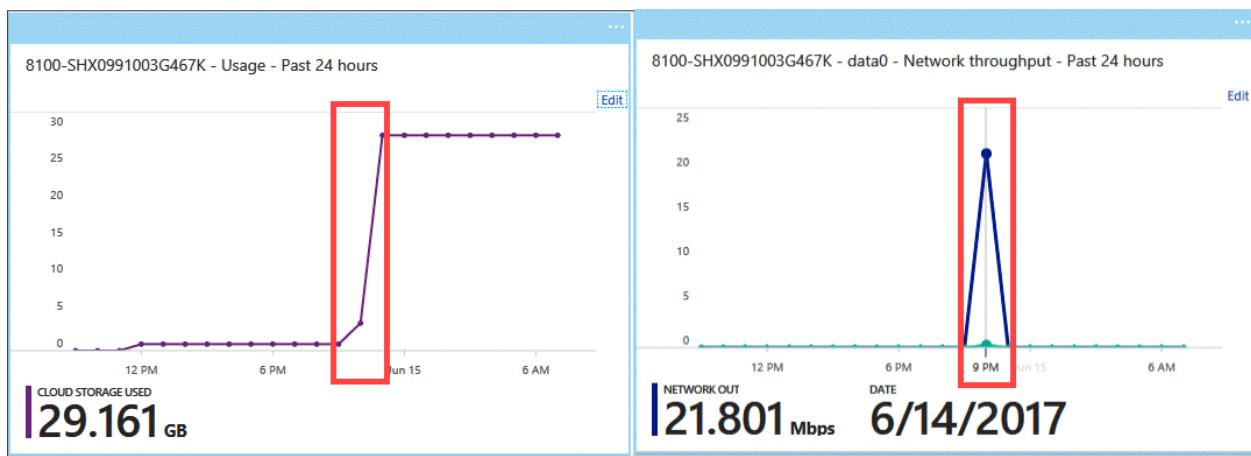
For the same device, a cloud snapshot was taken for volume data starting at 11:50 am. This resulted in data flowing from the device to the cloud. Writes were served to the cloud in this duration. The IO chart shows a peak in the Write Bytes/s corresponding to the time when the snapshot was taken.



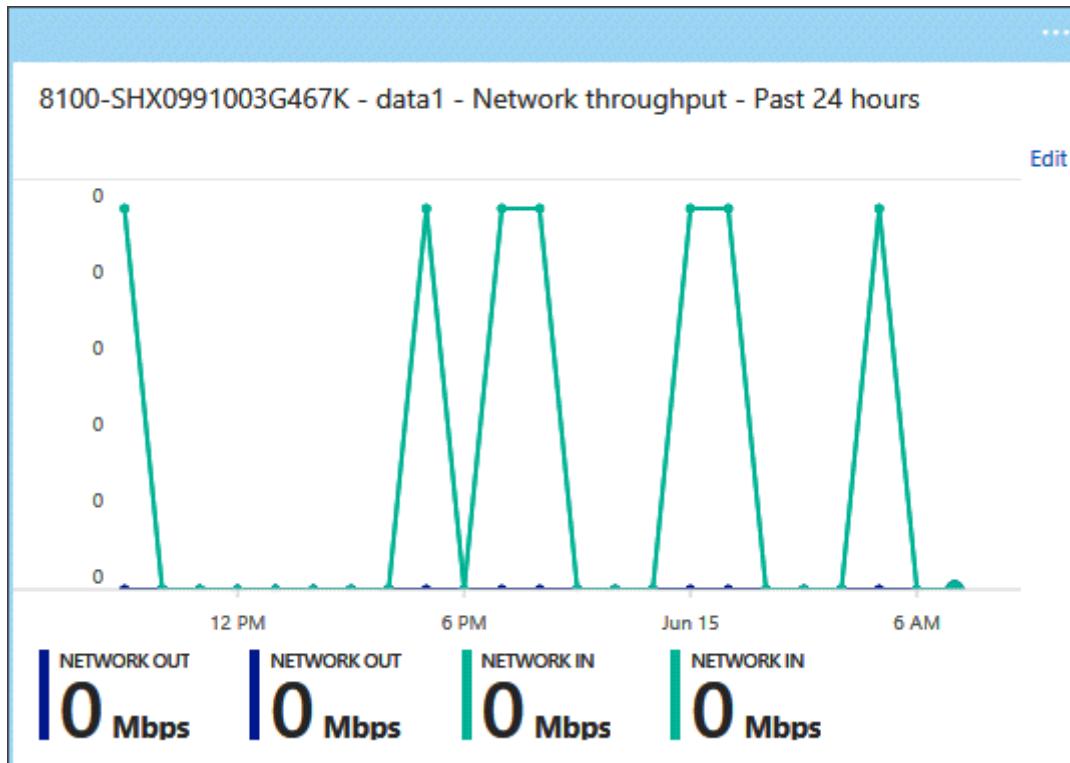
Network throughput for device network interfaces

Network throughput tracks metrics related to the amount of data transferred from the iSCSI initiator network interfaces on the host server and the device and between the device and the cloud. You can monitor this metric for each of the iSCSI network interfaces on your device.

The following charts show the network throughput for the Data 0, 1 1 GbE network on your device, which was both cloud-enabled (default) and iSCSI-enabled. On this device on June 14 at around 9 pm, data was tiered into the cloud (no cloud snapshots were taken at that time which points to tiering being the mechanism to move the data into the cloud) which resulted in IO being served to the cloud. There is a corresponding peak in the network throughput graph for the same time and most of the network traffic is outbound to the cloud.

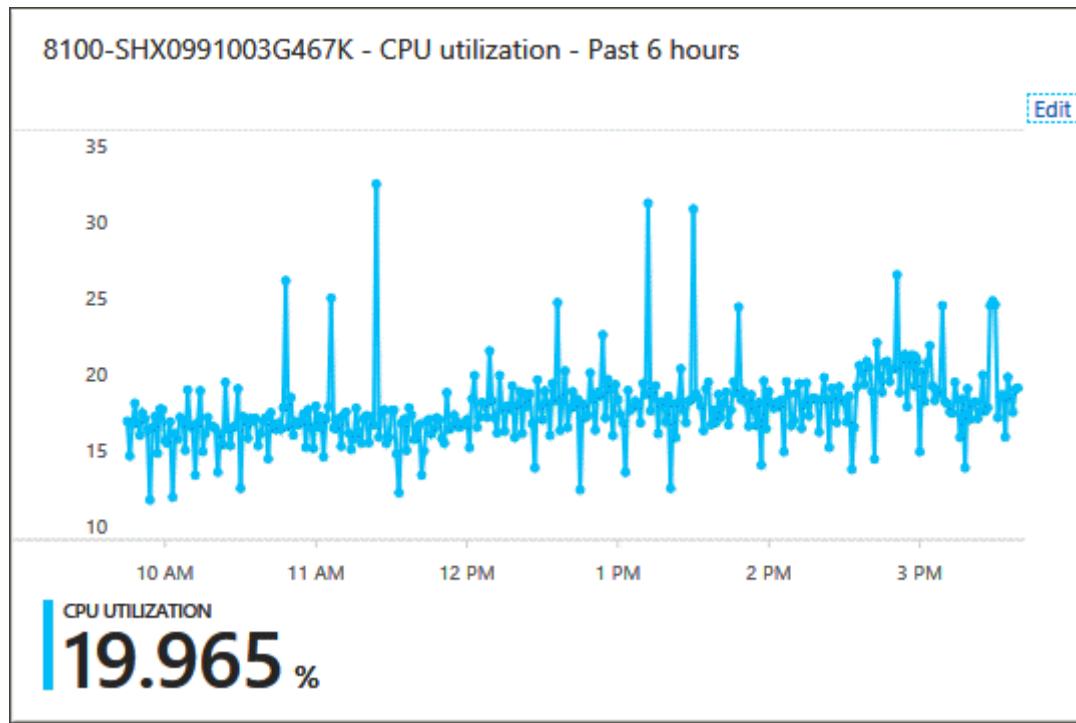


If we look at the Data 1 interface throughput chart, another 1 GbE network interface which was only iSCSI-enabled, then there was virtually no network traffic in this duration.



CPU utilization for device

CPU utilization tracks metrics related to the CPU utilized on your device. The following chart shows the CPU utilization stats for a device in production.



Next steps

- Learn how to [use the StorSimple Device Manager service device dashboard](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Use the StorSimple Device Manager service to view and manage StorSimple alerts

Article • 08/19/2022 • 20 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The **Alerts** blade in the StorSimple Device Manager service provides a way for you to review and clear StorSimple device-related alerts on a real-time basis. From this blade, you can centrally monitor the health issues of your StorSimple devices and the overall Microsoft Azure StorSimple solution.

This tutorial describes common alert conditions, alert severity levels, and how to configure alert notifications. Additionally, it includes alert quick reference tables, which enable you to quickly locate a specific alert and respond appropriately.

The screenshot shows the 'Docs-mySS8000series - Alerts' page in the StorSimple Device Manager. On the left, there's a navigation sidebar with sections like GENERAL, MANAGEMENT, and MONITORING, with 'Alerts' highlighted. The main area has a search bar and filter options for Time range (Past 30 days), Devices (All), Severity (All), and Status (Active). A message says 'The query returned 7 items.' Below is a table with columns: NAME, STATUS, SEVERITY, SOURCE, and DURATION. The table lists seven alerts:

NAME	STATUS	SEVERITY	SOURCE	DURATION
Device failed over to Controller0	Active	Informational	8100-SHX0991003G467K	11 Days, 19 Hours
Device failed over to Controller0	Active	Informational	8100-SHX0991003G44MT	12 Days, 21 Hours
Microsoft Support session has begun	Active	Warning	8100-SHX0991003G44MT	13 Days, 2 Hours
Failed to install updates	Active	Critical	8100-SHX0991003G44MT	13 Days, 16 Hours
Device failed over to Controller1	Active	Informational	8100-SHX0991003G44MT	13 Days, 19 Hours
Unable to automatically check for new updates	Active	Warning	8100-SHX0991003G467K	19 Days, 2 Hours
Microsoft Support session has begun	Active	Warning	8100-SHX0991003G467K	19 Days, 2 Hours

Common alert conditions

Your StorSimple device generates alerts in response to a variety of conditions. The following are the most common types of alert conditions:

- **Hardware issues** – These alerts tell you about the health of your hardware. They let you know if firmware upgrades are needed, if a network interface has issues, or if there is a problem with one of your data drives.
- **Connectivity issues** – These alerts occur when there is difficulty in transferring data. Communication issues can occur during transfer of data to and from the Azure storage account or due to lack of connectivity between the devices and the StorSimple Device Manager service. Communication issues are some of the hardest to fix because there are so many points of failure. You should always first verify that network connectivity and Internet access are available before continuing on to more advanced troubleshooting. For help with troubleshooting, go to [Troubleshoot with the Test-Connection cmdlet](#).
- **Performance issues** – These alerts are caused when your system isn't performing optimally, such as when it is under a heavy load.

In addition, you might see alerts related to security, updates, or job failures.

Alert severity levels

Alerts have different severity levels, depending on the impact that the alert situation will have and the need for a response to the alert. The severity levels are:

- **Critical** – This alert is in response to a condition that is affecting the successful performance of your system. Action is required to ensure that the StorSimple service is not interrupted.
- **Warning** – This condition could become critical if not resolved. You should investigate the situation and take any action required to clear the issue.
- **Information** – This alert contains information that can be useful in tracking and managing your system.

Configure alert settings

You can choose whether you want to be notified by email of alert conditions for each of your StorSimple devices. Additionally, you can identify other alert notification recipients by entering their email addresses in the **Other email recipients** box, separated by semicolons.

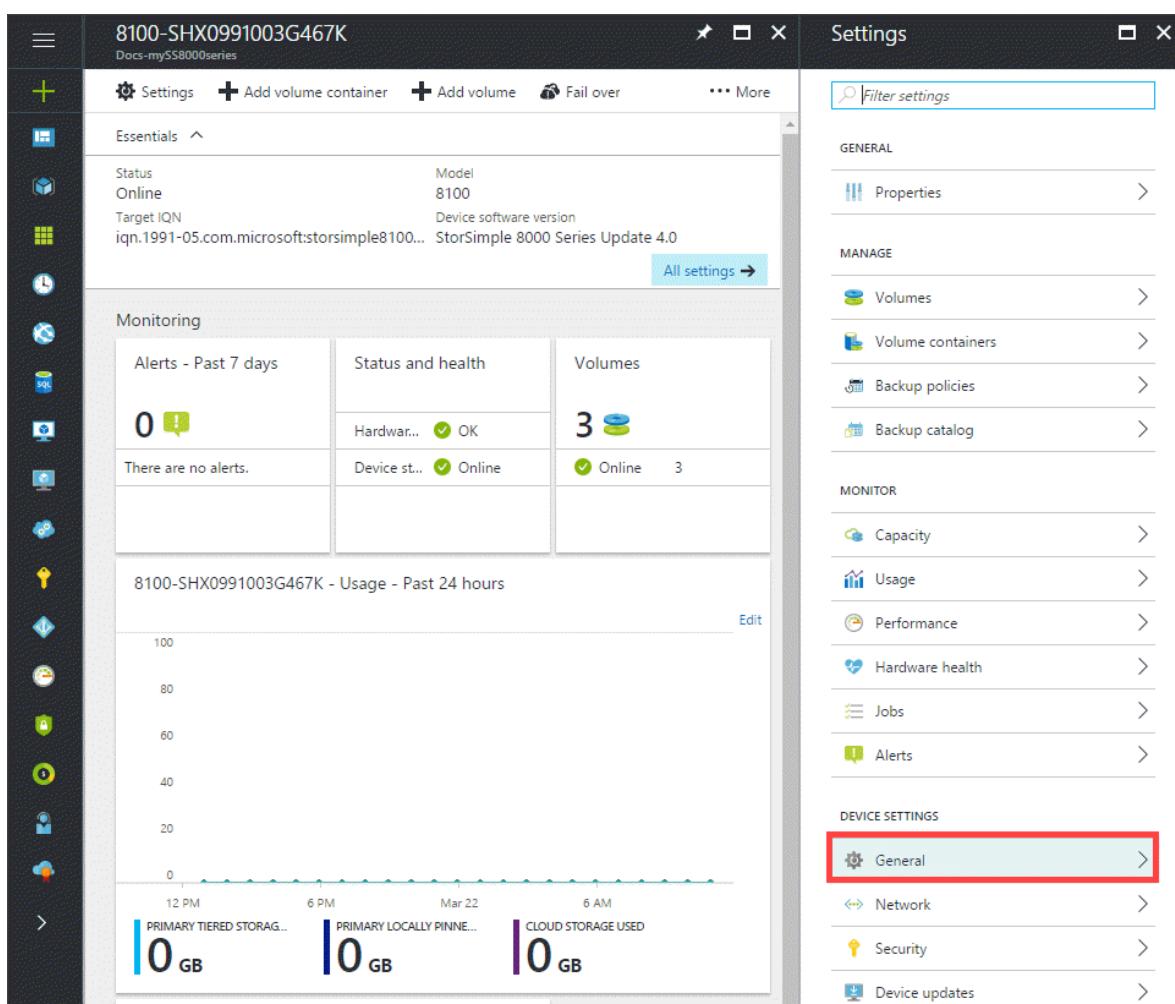
Note

You can enter a maximum of 20 email addresses per device.

After you enable email notification for a device, members of the notification list will receive an email message each time a critical alert occurs. The messages will be sent from *stor simple-alerts-noreply@mail.windowsazure.com* and will describe the alert condition. Recipients can click **Unsubscribe** to remove themselves from the email notification list.

To enable email notification of alerts for a device

1. Go to your StorSimple Device Manager service. From the list of devices, select and click the device that you wish to configure.
2. Go to **Settings > General** for the device.



3. In the **General** settings blade, go to **Alert settings** and set the following:
 - a. In the **Send email notification** field, select **YES**.

- b. In the **Email service administrators** field, select **YES** to have the service administrator and all co-administrators receive the alert notifications.
 - c. In the **Other email recipients** field, enter the email addresses of all other recipients who should receive the alert notifications. Enter names in the format *someone@somewhere.com*. Use semicolons to separate the email addresses. You can configure a maximum of 20 email addresses per device.
4. To send a test email notification, click **Send test email**. The StorSimple Device Manager service will display status messages as it forwards the test notification.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and lists various management options like Properties, Volumes, and Backup catalog. The right window is titled 'General settings' for device 8100-SHX0991003G467K. It includes sections for Device settings (Device name set to 8100-SHX0991003G467K), Time settings (Time zone set to (UTC-08:00) Pacific Standard Time), and Alert settings. The 'Alert settings' section is highlighted with a red box and contains options for enabling email notifications (YES selected), sending emails to service administrators (YES selected), and additional recipients (john@contoso.com;gus@contoso.com, with a checked checkbox). A 'Send Test Email' button is also present.

Filter settings

GENERAL

Properties >

MANAGE

Volumes >

Volume containers >

Backup policies >

Backup catalog >

MONITOR

Capacity >

Usage >

Performance >

Hardware health >

Jobs >

Alerts >

DEVICE SETTINGS

General >

Network >

Security >

Device updates >

Save Discard

Device settings ⓘ

Device name
8100-SHX0991003G467K

Description

Time settings ⓘ

Time zone
(UTC-08:00) Pacific Standard Time

NTP primary
time.windows.com

NTP secondary

Alert settings ⓘ

Enable email notification
 YES NO

Email service administrators ⓘ
 YES NO

Additional email recipients ⓘ
john@contoso.com;gus@contoso.com

Send Test Email

5. You see a notification when the test email is sent.

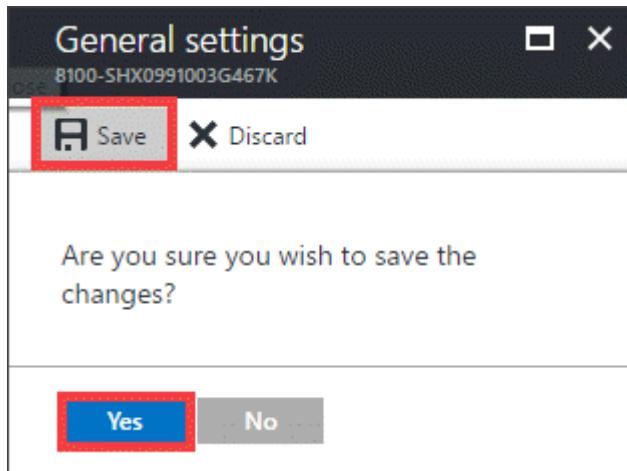
Send Test Alert Email to 'john@contoso.co... 11:58 AM'

Successfully completed the operation.

Note

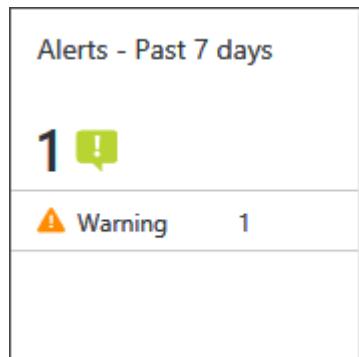
If the test notification message can't be sent, the StorSimple Device Manager service will display an appropriate error message. Wait a few minutes, and then try to send your test notification message again.

- Once you have completed the configuration, click **Save**. When prompted for confirmation, click **Yes**.



View and track alerts

The StorSimple Device Manager service summary blade provides you with a quick glance at the number of alerts on your devices, arranged by severity level.



Clicking the severity level opens the **Alerts** blade. The results include only the alerts that match that severity level.

Clicking an alert in the list provides you with additional details for the alert, including the last time the alert was reported, the number of occurrences of the alert on the device, and the recommended action to resolve the alert. If it is a hardware alert, it will also identify the hardware component.

Device failed over to Controller1

Status: Active

General

Message	Device failed over to Controller1
Recommendation	There was a cluster failover due to an update. This is normal and no action is needed. Once you have acknowledged this alert, please clear it from the alerts page.
Severity	Informational
Device	8100-SHX0991003G44MT

Occurrence

failover reason	Updates
occurrences	2
last observed	3/8/2017 3:51:38 PM ((UTC-08:00) Pacific Time (US & Canada))
first observed	3/8/2017 3:51:38 PM ((UTC-08:00) Pacific Time (US & Canada))

You can copy the alert details to a text file if you need to send the information to Microsoft Support. After you have followed the recommendation and resolved the alert condition on-premises, you should clear the alert from the device by selecting the alert in the **Alerts** blade and clicking **Clear**. To clear multiple alerts, select each alert, click any column except the **Alert** column, and then click **Clear** after you have selected all the alerts to be cleared. Note that some alerts are automatically cleared when the issue is resolved or when the system updates the alert with new information.

When you click **Clear**, you will have the opportunity to provide comments about the alert and the steps that you took to resolve the issue. Some events will be cleared by the system if another event is triggered with new information. In that case, you will see the following message.



Sort and review alerts

You may find it more efficient to run reports on alerts so that you can review and clear them in groups. Additionally, the **Alerts** blade can display up to 250 alerts. If you have

exceeded that number of alerts, not all alerts will be displayed in the default view. You can combine the following fields to customize which alerts are displayed:

- **Status** – You can display either **Active** or **Cleared** alerts. Active alerts are still being triggered on your system, while cleared alerts have been either manually cleared by an administrator or programmatically cleared because the system updated the alert condition with new information.
- **Severity** – You can display alerts of all severity levels (critical, warning, information), or just a certain severity, such as only critical alerts.
- **Source** – You can display alerts from all sources, or limit the alerts to those that come from either the service or one or all of the devices.
- **Time range** – By specifying the **From** and **To** dates and time stamps, you can look at alerts during the time period that you are interested in.

NAME	STATUS	SEVERITY	SOURCE	DURATION
Device failed over to Controller0	Active	Informational	8100-SHX0991003G467K	11 Days, 19 Hours
Device failed over to Controller0	Active	Informational	8100-SHX0991003G44MT	12 Days, 21 Hours
Microsoft Support session has begun	Active	Warning	8100-SHX0991003G44MT	13 Days, 2 Hours
Failed to install updates	Active	Critical	8100-SHX0991003G44MT	13 Days, 16 Hours
Device failed over to Controller1	Active	Informational	8100-SHX0991003G44MT	13 Days, 19 Hours
Unable to automatically check for new updates	Active	Warning	8100-SHX0991003G467K	19 Days, 2 Hours
Microsoft Support session has begun	Active	Warning	8100-SHX0991003G467K	19 Days, 2 Hours

Alerts quick reference

The following tables list some of the Microsoft Azure StorSimple alerts that you might encounter, as well as additional information and recommendations where available. StorSimple device alerts fall into one of the following categories:

- Cloud connectivity alerts
- Cluster alerts
- Disaster recovery alerts
- Hardware alerts
- Job failure alerts
- Locally pinned volume alerts
- Networking alerts
- Performance alerts
- Security alerts

- Support package alerts
- Enclosure environment alerts

Cloud connectivity alerts

Alert text	Event	More information / recommended actions
Connectivity to <cloud credential name> cannot be established.	Cannot connect to the storage account.	<p>It looks like there might be a connectivity issue with your device. Please run the <code>Test-HcsConnection</code> cmdlet from the Windows PowerShell Interface for StorSimple on your device to identify and fix the issue. If the settings are correct, the issue might be with the credentials of the storage account for which the alert was raised. In this case, use the <code>Test-HcsStorageAccountCredential</code> cmdlet to determine if there are issues that you can resolve.</p> <ul style="list-style-type: none"> • Check your network settings. • Check your storage account credentials.
We have not received a heartbeat from your device for the last <number> minutes.	Cannot connect to device.	<p>It looks like there is a connectivity issue with your device. Please use the <code>Test-HcsConnection</code> cmdlet from the Windows PowerShell Interface for StorSimple on your device to identify and fix the issue or contact your network administrator.</p>

StorSimple behavior when cloud connectivity fails

What happens if cloud connectivity fails for my StorSimple device running in production?

If cloud connectivity fails on your StorSimple production device, then depending on the state of your device, the following can occur:

- **For the local data on your device:** For some time, there will be no disruption and reads will continue to be served. However, as the number of outstanding IOs increases and exceeds a limit, the reads could start to fail.

Depending on the amount of data on your device, the writes will also continue to occur for the first few hours after the disruption in the cloud connectivity. The writes will then slow down and eventually start to fail if the cloud connectivity is disrupted for several hours. (There is temporary storage on the device for data that is to be pushed to the cloud. This area is flushed when the data is sent. If

connectivity fails, data in this storage area will not be pushed to the cloud, and IO will fail.)

- **For the data in the cloud:** For most cloud connectivity errors, an error is returned. Once the connectivity is restored, the IOs are resumed without the user having to bring the volume online. In rare instances, user intervention may be required to bring back the volume online from the Azure portal.
- **For cloud snapshots in progress:** The operation is retried a few times within 4-5 hours and if the connectivity is not restored, the cloud snapshots will fail.

Cluster alerts

Alert text	Event	More information / recommended actions
Device failed over to < <i>device name</i> >.	Device is in maintenance mode.	Device failed over due to entering or exiting maintenance mode. This is normal and no action is needed. After you have acknowledged this alert, clear it from the alerts page.
Device failed over to < <i>device name</i> >.	Device firmware or software was just updated.	There was a cluster failover due to an update. This is normal and no action is needed. After you have acknowledged this alert, clear it from the alerts page.
Device failed over to < <i>device name</i> >.	Controller was shut down or restarted.	Device failed over because the active controller was shut down or restarted by an administrator. No action is needed. After you have acknowledged this alert, clear it from the alerts page.
Device failed over to < <i>device name</i> >.	Planned failover.	Verify that this was a planned failover. After you have taken appropriate action, clear this alert from the alerts page.
Device failed over to < <i>device name</i> >.	Unplanned failover.	StorSimple is built to automatically recover from unplanned failovers. If you see a large number of these alerts, contact Microsoft Support.
Device failed over to < <i>device name</i> >.	Other/unknown cause.	If you see a large number of these alerts, contact Microsoft Support. After the issue is resolved, clear this alert from the alerts page.

Alert text	Event	More information / recommended actions
A critical device service reports status as failed.	Datapath service failure.	Contact Microsoft Support for assistance.
Virtual IP address for network interface <DATA #> reports status as failed.	Other/unknown cause.	Sometimes temporary conditions can cause these alerts. If this is the case, then this alert will be automatically cleared after some time. If the issue persists, contact Microsoft Support.
Virtual IP address for network interface <DATA #> reports status as failed.	Interface name: <DATA #> IP address <IP address> cannot be brought online because a duplicate IP address was detected on the network.	Ensure that the duplicate IP address is removed from the network or reconfigure the interface with a different IP address.

Disaster recovery alerts

Alert text	Event	More information / recommended actions
Recovery operations could not restore all of the settings for this service. Device configuration data is in an inconsistent state for some devices.	Data inconsistency detected after disaster recovery.	Encrypted data on the service is not synchronized with that on the device. Authorize the device <device name> from StorSimple Device Manager to start the synchronization process. Use the Windows PowerShell Interface for StorSimple to run the <code>Restore-HcsmEncryptedServiceData</code> cmdlet, providing the old password as an input to this cmdlet to restore the security profile. Then run the <code>Invoke-HcsmServiceDataEncryptionKeyChange</code> cmdlet to update the service data encryption key. After you have taken appropriate action, clear this alert from the alerts page.

Hardware alerts

Alert text	Event	More information / recommended actions
------------	-------	--

Alert text	Event	More information / recommended actions
Hardware component < <i>component ID</i> > reports status as < <i>status</i> >.		Sometimes temporary conditions can cause these alerts. If so, this alert will be automatically cleared after some time. If the issue persists, contact Microsoft Support.
Passive controller malfunctioning.	The passive (secondary) controller is not functioning.	Your device is operational, but one of your controllers is malfunctioning. Try restarting that controller. If the issue is not resolved, contact Microsoft Support.

Job failure alerts

Alert text	Event	More information / recommended actions
Backup of < <i>source volume group ID</i> > failed.	Backup job failed.	Connectivity issues could be preventing the backup operation from successfully completing. If there are no connectivity issues, you may have reached the maximum number of backups. Delete any backups that are no longer needed and retry the operation. After you have taken appropriate action, clear this alert from the alerts page.
Clone of < <i>source backup element IDs</i> > to < <i>destination volume serial numbers</i> > failed.	Clone job failed.	Refresh the backup list to verify that the backup is still valid. If the backup is valid, it is possible that cloud connectivity issues are preventing the clone operation from successfully completing. If there are no connectivity issues, you may have reached the storage limit. Delete any backups that are no longer needed and retry the operation. After you have taken appropriate action to resolve the issue, clear this alert from the alerts page.
< <i>source backup element IDs</i> > failed.	Restore job failed.	Refresh the backup list to verify that the backup is still valid. If the backup is valid, it is possible that cloud connectivity issues are preventing the restore operation from successfully completing. If there are no connectivity issues, you may have reached the storage limit. Delete any backups that are no longer needed and retry the operation. After you have taken appropriate action to resolve the issue, clear this alert from the alerts page.

Locally pinned volume alerts

Alert text	Event	More information / recommended actions
------------	-------	--

Alert text	Event	More information / recommended actions
Creation of local volume < <i>volume name</i> > failed.	The volume creation job has failed. <i><Error message corresponding to the failed error code></i> .	Connectivity issues could be preventing the space creation operation from successfully completing. Locally pinned volumes are thickly provisioned and the process of creating space involves spilling tiered volumes to the cloud. If there are no connectivity issues, you may have exhausted the local space on the device. Determine if space exists on the device before retrying this operation.
Expansion of local volume < <i>volume name</i> > failed.	The volume modification job has failed due to < <i>error message corresponding to the failed error code</i> >.	Connectivity issues could be preventing the volume expansion operation from successfully completing. Locally pinned volumes are thickly provisioned and the process of extending the existing space involves spilling tiered volumes to the cloud. If there are no connectivity issues, you may have exhausted the local space on the device. Determine if space exists on the device before retrying this operation.
Conversion of volume < <i>volume name</i> > failed.	The volume conversion job to convert the volume type from locally pinned to tiered failed.	Conversion of the volume from type locally pinned to tiered could not be completed. Ensure that there are no connectivity issues preventing the operation from completing successfully. For troubleshooting connectivity issues go to Troubleshoot with the Test-HcsmConnection cmdlet . The original locally pinned volume has now been marked as a tiered volume since some of the data from the locally pinned volume has spilled to the cloud during the conversion. The resultant tiered volume is still occupying local space on the device that cannot be reclaimed for future local volumes. Resolve any connectivity issues, clear the alert and convert this volume back to the original locally pinned volume type to ensure all the data is made available locally again.
Conversion of volume < <i>volume name</i> > failed.	The volume conversion job to convert the volume type from tiered to locally pinned failed.	Conversion of the volume from type tiered to locally pinned could not be completed. Ensure that there are no connectivity issues preventing the operation from completing successfully. For troubleshooting connectivity issues go to Troubleshoot with the Test-HcsmConnection cmdlet . The original tiered volume now marked as a locally pinned volume as part of the conversion process continues to have data residing in the cloud, while the thickly provisioned space on the device for this volume can no longer be reclaimed for future local volumes. Resolve any connectivity issues, clear the alert and convert this volume back to the original tiered volume type to ensure local space thickly provisioned on the device can be reclaimed.

Alert text	Event	More information / recommended actions
Nearing local space consumption for local snapshots of < <i>volume group name</i> >	Local snapshots for the backup policy might soon run out of space and be invalidated to avoid host write failures.	Frequent local snapshots alongside a high data churn in the volumes associated with this backup policy group are causing local space on the device to be consumed quickly. Delete any local snapshots that are no longer needed. Also, update your local snapshot schedules for this backup policy to take less frequent local snapshots, and ensure that cloud snapshots are taken regularly. If these actions are not taken, local space for these snapshots might soon be exhausted and the system will automatically delete them to ensure that host writes continue to be processed successfully.
Local snapshots for < <i>volume group name</i> > have been invalidated.	The local snapshots for < <i>volume group name</i> > have been invalidated and then deleted because they were exceeding the local space on the device.	To ensure this does not recur in the future, review the local snapshot schedules for this backup policy and delete any local snapshots that are no longer needed. Frequent local snapshots alongside a high data churn in the volumes associated with this backup policy group might cause local space on the device to be consumed quickly.
Restore of < <i>source backup element IDs</i> > failed.	The restore job has failed.	If you have locally pinned or a mix of locally pinned and tiered volumes in this backup policy, refresh the backup list to verify that the backup is still valid. If the backup is valid, it is possible that cloud connectivity issues are preventing the restore operation from successfully completing. The locally pinned volumes that were being restored as part of this snapshot group do not have all of their data downloaded to the device, and, if you have a mix of tiered and locally pinned volumes in this snapshot group, they will not be in sync with each other. To successfully complete the restore operation, take the volumes in this group offline on the host and retry the restore operation. Note that any modifications to the volume data that were performed during the restore process will be lost.

Networking alerts

Alert text	Event	More information / recommended actions
-------------------	--------------	---

Alert text	Event	More information / recommended actions
Could not start StorSimple service(s).	Datapath error	If the problem persists, contact Microsoft Support.
Duplicate IP address detected for 'Data0'.		The system has detected a conflict for IP address '10.0.0.1'. The network resource 'Data0' on the device <device1> is offline. Ensure that this IP address is not used by any other entity in this network. To troubleshoot network issues, go to Troubleshoot with the Get-NetAdapter cmdlet . Contact your network administrator for help resolving this issue. If the problem persists, contact Microsoft Support.
IPv4 (or IPv6) address for 'Data0' is offline.		The network resource 'Data0' with IP address '10.0.0.1.' and prefix length '22' on the device <device1> is offline. Ensure that the switch ports to which this interface is connected are operational. To troubleshoot network issues, go to Troubleshoot with the Get-NetAdapter cmdlet .
Could not connect to the authentication service.	Datapath error	The URL that is used to authenticate is not reachable. Ensure that your firewall rules include the URL patterns specified for the StorSimple device. For more information on URL patterns in Azure portal, go to https://aka.ms/ss-8000-network-reqs . If using Azure Government Cloud, go to the URL patterns in https://aka.ms/ss8000-gov-network-reqs .

Performance alerts

Alert text	Event	More information / recommended actions
The device load has exceeded <threshold>.	Slower than expected response times.	Your device reports utilization under a heavy input/output load. This could cause your device to not work as well as it should. Review the workloads that you have attached to the device, and determine if there are any that could be moved to another device or that are no longer necessary.
Could not start StorSimple service(s).	Datapath error	If the problem persists, contact Microsoft Support.

Security alerts

Alert text	Event	More information / recommended actions
-------------------	--------------	---

Alert text	Event	More information / recommended actions
Microsoft Support session has begun.	Third-party accessed support session.	Please confirm this access is authorized. After you have taken appropriate action, clear this alert from the alerts page.
Password for <i><element></i> will expire in <i><length of time></i> .	Password expiration is approaching.	Change your password before it expires.
Security configuration information missing for <i><element ID></i> .		The volumes associated with this volume container cannot be used to replicate your StorSimple configuration. To ensure that your data is safely stored, we recommend that you delete the volume container and any volumes associated with the volume container. After you have taken appropriate action, clear this alert from the alerts page.
<i><number></i> login attempts failed for <i><element ID></i> .	Multiple failed logon attempts.	<p>Your device might be under attack or an authorized user is attempting to connect with an incorrect password.</p> <ul style="list-style-type: none"> • Contact your authorized users and verify that these attempts were from a legitimate source. If you continue to see large numbers of failed login attempts, consider disabling remote management and contacting your network administrator. After you have taken appropriate action, clear this alert from the alerts page. • Check that your Snapshot Manager instances are configured with the correct password. After you have taken appropriate action, clear this alert from the alerts page. <p>For more information, go to Change an expired device password.</p>
One or more failures occurred while changing the service data encryption key.		There were errors encountered while changing the service data encryption key. After you have addressed the error conditions, run the <code>Invoke-HcsmServiceDataEncryptionKeyChange</code> cmdlet from the Windows PowerShell Interface for StorSimple on your device to update the service. If this issue persists, contact Microsoft support. After you resolve the issue, clear this alert from the alerts page.

Support package alerts

Alert text	Event	More information / recommended actions
-------------------	--------------	---

Alert text	Event	More information / recommended actions
Creation of support package failed.	StorSimple couldn't generate the package.	Retry this operation. If the issue persists, contact Microsoft Support. After you have resolved the issue, clear this alert from the alerts page.

Enclosure environment alerts

Alert text	Event	More information / recommended actions
Hardware component Ambient temperature sensor reports status as failed.	Enclosure type: Main ambient temperature sensor	This alert is triggered when the ambient outside temperature around StorSimple is above an acceptable range. Check the ambient outside temperature or the airflow from the AC vent in the datacenter. When the temperature returns to normal, the alert is automatically cleared after some time has elapsed. If the issue persists, contact Microsoft support.

Next steps

Learn more about [StorSimple errors and troubleshooting device deployment issues](#).

Use the StorSimple Device Manager service to monitor hardware components and status

Article • 08/19/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article describes the various physical and logical components in your on-premises StorSimple 8000 series device. It also explains how to monitor the device component status by using the **Status and hardware health** blade in the StorSimple Device Manager service.

The **Status and hardware health** blade shows the hardware status of all the StorSimple device components.

Under the list of components for 8100, there are three sections that describe:

- **Shared Components** – These are not part of the controllers, such as disk drives, enclosure, Power and Cooling Module (PCM) components and PCM temperature, line voltage, and line current sensors.
- **Controller 0 Components** – The components that reside on Controller 0, such as controller, SAS expander and connector, controller temperature sensors, and the various network interfaces.
- **Controller 1 Components** – The components that constitute Controller 1, similar to those detailed for Controller 0.

An 8600 device has additional components that correspond to the Extended Bunch of Disks (EBOD) enclosure. Under the list of components, there are five sections. Of these, there are three sections that contain the components in the primary enclosure and are

identical to the ones described for 8100. There are two additional sections for the EBOD enclosure that describe:

- **EBOD Controller 0 Components** – The components that reside on EBOD enclosure 0, such as the EBOD controller, SAS expander and connector, and controller temperature sensors.
- **EBOD Controller 1 Components** – The components that constitute EBOD enclosure 1, similar to those detailed for EBOD enclosure 0.
- **EBOD enclosure Shared Components** – The components present in the EBOD enclosure and PCM that are not part of the EBOD controller.

 **Note**

The hardware status is not available for a StorSimple Cloud Appliance (8010/8020).

Monitor the hardware status

Perform the following steps to view the hardware status of a device component:

1. Navigate to **Devices**, select a specific StorSimple device. Go to **Monitor > Hardware health**.

The screenshot shows two overlapping windows. The left window is titled 'Settings' and lists various management options like Properties, Volumes, and Backup catalog under 'GENERAL' and 'MANAGE'. A red box highlights the 'MONITOR' section, which includes Capacity, Usage, Performance, and Hardware health. Another red box highlights the 'Hardware health' option, which is currently selected and highlighted with a blue background. The right window is titled 'Status and hardware health' and displays device status information. It shows the device ID '8100-SHX0991003G44MT' and its status as 'Online'. Below this, it lists 'HARDWARE COMPONENTS' with three categories: 'CONTROLLER 0 COMPONENTS', 'CONTROLLER 1 COMPONENTS', and 'SHARED COMPONENTS', all of which are marked as 'OK'.

NAME	STATUS
CONTROLLER 0 COMPONENTS	OK
CONTROLLER 1 COMPONENTS	OK
SHARED COMPONENTS	OK

2. Locate the **Hardware components** section and choose from the available components. Simply click the component label to expand the list and view the status of the various device components. See the [detailed component list for the primary enclosure](#) and the [detailed component list for the EBOD enclosure](#).

Status and hardware health X

8100-SHX0991003G44MT

i Device status gets updated every 10 mins. Hardware component health gets updated every 5 mins. There is a lag in updating the latest status here.
To monitor the device go to Settings > Alerts. Ensure that you configure email notifications for alerts to be notified about device issues.

DEVICE STATUS ●

8100-SHX0991003G44MT
Online

HARDWARE COMPONENTS ●

NAME	STATUS
CONTROLLER 0 COMPONENTS	✓ OK
CONTROLLER 1 COMPONENTS	✓ OK
SHARED COMPONENTS	✓ OK

CONTROLLER 0 COMPONENTS X

Filter items...

NAME	STATUS
IO Module Temperat...	✓ OK
CPU Temperature Sen...	✓ OK
DIMM Temperature S...	✓ OK
CPU Exit temperature...	✓ OK
CPU Inlet temperatur...	✓ OK
PCIe Zone temperatur...	✓ OK
Controller [Active]	✓ OK
SAS Expander	✓ OK
SAS Connector 0	✓ OK
SBB Midplane Interco...	✓ OK
Processor Core	✓ OK
Enclosure Electronics...	✓ OK
Enclosure Electronics...	✓ OK
Baseboard Managem...	✓ OK
Ethernet DATA 0	✓ OK
Ethernet DATA 1	✓ OK
Ethernet DATA 2	✓ OK
Ethernet DATA 3	✓ OK
Ethernet DATA 4	✓ OK

3. Use the following color coding scheme to interpret the component status:

- **Green check** – Denotes a healthy component with **OK** status.
- **Yellow** – Denotes a degraded component in **Warning** state.
- **Red exclamation** – Denotes a failed component that has a **Failure** status.
- **White with black text** – Denotes a component that is not present.

The following screenshot shows a device that has components in **OK**, **Warning**, and **Failure** state.

The screenshot displays the 'Status and hardware health' window for a device with the identifier 8100-SHX0991003G44MT. The window includes an informational message about status updates, a 'DEVICE STATUS' section indicating the device is online, and a 'HARDWARE COMPONENTS' table. The 'HARDWARE COMPONENTS' table is highlighted with a red border and contains three rows: 'CONTROLLER 0 COMPONENTS' (OK), 'CONTROLLER 1 COMPONENTS' (Failure), and 'SHARED COMPONENTS' (Warning). The 'SHARED COMPONENTS' row is expanded to show two sub-components: 'NVRAM' and 'cluster', both of which are listed as degraded.

NAME	STATUS
CONTROLLER 0 COMPONENTS	OK
CONTROLLER 1 COMPONENTS	Failure
SHARED COMPONENTS	Warning

Expanding the **Shared components** list, we can see that the NVRAM and the cluster are degraded.

Status and hardware health

8100-SHX0991003G44MT

i Device status gets updated every 10 mins. Hardware component health gets updated every 5 mins. There is a lag in updating the latest status here.

To monitor the device go to Settings > Alerts. Ensure that you configure email notifications for alerts to be notified about device issues.

DEVICE STATUS ⓘ

8100-SHX0991003G44MT
Online

HARDWARE COMPONENTS ⓘ

NAME	STATUS
CONTROLLER 0 COMPONENTS	✓ OK
CONTROLLER 1 COMPONENTS	✗ Failure
SHARED COMPONENTS	⚠ Warning

SHARED COMPONENTS

Enclosure	✓ OK
12V Line Voltage Sen...	✓ OK
5V Line Voltage Sens...	✓ OK
12V Line Voltage Sen...	✓ OK
5V Line Voltage Sens...	✓ OK
12V Line Current Sens...	✓ OK
5V Line Current Senso...	✓ OK
12V Line Current Sens...	✓ OK
5V Line Current Senso...	✓ OK
Enclosure Settings	✓ OK
Metis	✓ OK
Battery in PCM 0	✓ OK
Battery in PCM 1	✓ OK
Cluster	⚠ Warning
Cluster Quorum	✓ OK
HDD Data Space	✓ OK
HDD Management Sp...	✓ OK
HDD Quorum Space	✓ OK
HDD Replacement Sp...	✓ OK
SSD Data Space	✓ OK
SSD NVRAM Space	✓ OK
HDD Storage Pool	✓ OK
SSD Storage Pool	✓ OK
NVRAM	⚠ Warning

Expanding the **Controller 1 components** list, we can see that the cluster node has failed.

Status and hardware health

8100-SHX0991003G44MT

i Device status gets updated every 10 mins. Hardware component health gets updated every 5 mins. There is a lag in updating the latest status here.

To monitor the device go to Settings > Alerts. Ensure that you configure email notifications for alerts to be notified about device issues.

DEVICE STATUS ⓘ

8100-SHX0991003G44MT
Online

HARDWARE COMPONENTS ⓘ

NAME	STATUS
CONTROLLER 0 COMPONENTS	✓ OK
CONTROLLER 1 COMPONENTS	✗ Failure
SHARED COMPONENTS	⚠ Warning

CONTROLLER 1 COMPONENTS

IO Module Temperat...	✓ OK
CPU Temperature Sen...	✓ OK
DIMM Temperature S...	✓ OK
DIMM Temperature S...	✓ OK
DIMM temperature s...	✓ OK
DIMM temperature s...	✓ OK
CPU Exit temperature...	✓ OK
CPU Inlet temperatur...	✓ OK
PCIe Zone temperatur...	✓ OK
Controller	✓ OK
SAS Expander	✓ OK
SAS Connector 0	✓ OK
SBB Midplane Interco...	✓ OK
Processor Core	✓ OK
Enclosure Electronics...	✓ OK
Enclosure Electronics...	✓ OK
Baseboard Managem...	✓ OK
Ethernet DATA 0	✓ OK
Ethernet DATA 1	✓ OK
Ethernet DATA 2	✓ OK
Ethernet DATA 3	✓ OK
Ethernet DATA 4	✓ OK
Ethernet DATA 5	✓ OK
Cluster Node	✗ Failure

4. If you encounter a component that is not in a **Healthy** state, contact Microsoft Support. If alerts are enabled on your device, you will receive an email alert. If you need to replace a failed hardware component, see [StorSimple hardware component replacement](#).

Component list for primary enclosure of StorSimple device

The following table outlines the physical and logical components contained in the primary enclosure (present both in 8100 and 8600) of your on-premises StorSimple device.

Component	Module	Type	Location	Field replaceable unit (FRU)?	Description
Drive in slot [0-11]	Disk Drives	Physical	Shared	Yes	One line is presented for each of the SSD or the HDD drives in the primary enclosure.
Ambient temperature sensor	Enclosure	Physical	Shared	No	Measures the temperature within the chassis.
Mid-plane temperature sensor	Enclosure	Physical	Shared	No	Measures the temperature of the mid-plane.
Audible alarm	Enclosure	Physical	Shared	No	Indicates whether the audible alarm subsystem within the chassis is functional.
Enclosure	Enclosure	Physical	Shared	Yes	Indicates the presence of a chassis.
Enclosure settings	Enclosure	Physical	Shared	No	Refers to the front panel of the chassis.
Line voltage sensors	PCM	Physical	Shared	No	Numerous line voltage sensors have their state displayed, which indicates whether the measured voltage is within tolerance.
Line current sensors	PCM	Physical	Shared	No	Numerous line current sensors have their state displayed, which indicates whether the measured current is within tolerance.

Component	Module	Type	Location	Field replaceable unit (FRU)?	Description
Temperature sensors in PCM	PCM	Physical	Shared	No	Numerous temperature sensors such as Inlet and Hotspot sensors have their state displayed, indicating whether the measured temperature is within tolerance.
Power supply [0-1]	PCM	Physical	Shared	Yes	One line is presented for each of the power supplies in the two PCMs located in the back of the device.
Cooling [0-1]	PCM	Physical	Shared	Yes	One line is presented for each of the four cooling fans residing in the two PCMs.
Battery [0-1]	PCM	Physical	Shared	Yes	One line is presented for each of the backup battery modules that are seated in the PCM.
Metis	N/A	Logical	Shared	N/A	Displays the state of the batteries: whether they need charging and are approaching end-of-life.
Cluster	N/A	Logical	Shared	N/A	Displays the state of the cluster that is created between the two integrated controller modules.
Cluster node	N/A	Logical	Shared	N/A	Indicates the state of the controller as part of the cluster.
Cluster quorum	N/A	Logical		N/A	Indicates the presence of the majority disk membership in the HDD storage pool.
HDD data space	N/A	Logical	Shared	N/A	The storage space that is used for data in the hard disk drive (HDD) storage pool.
HDD management space	N/A	Logical	Shared	N/A	The space reserved in the HDD storage pool for management tasks.
HDD quorum space	N/A	Logical	Shared	N/A	The space reserved in the HDD storage pool for cluster quorum.

Component	Module	Type	Location	Field replaceable unit (FRU)?	Description
HDD replacement space	N/A	Logical	Shared	N/A	The space reserved in the HDD storage pool for controller replacement.
SSD data space	N/A	Logical	Shared	N/A	The storage space used for data in the solid state drive (SSD) storage pool.
SSD NVRAM space	N/A	Logical	Shared	N/A	The storage space in the SSD storage pool that is dedicated for NVRAM logic.
HDD storage pool	N/A	Logical	Shared	N/A	Displays the state of the logical storage pool that is created from device HDDs.
SSD storage pool	N/A	Logical	Shared	N/A	Displays the state of the logical storage pool that is created from device SSDs.
Controller [0-1] [state]	I/O	Physical	Controller	Yes	Displays the state of the controller, and whether it is in active or standby mode within the chassis.
Temperature sensors in controller	I/O	Physical	Controller	No	Numerous temperature sensors such as I/O module, CPU temperature, DIMM and PCIe sensors have their state displayed, which indicates whether or not the temperature encountered is within tolerance.
SAS expander	I/O	Physical	Controller	No	Indicates the state of the serial attached SCSI (SAS) expander, which is used to connect the integrated storage to the controller.
SAS connector [0-1]	I/O	Physical	Controller	No	Indicates the state of each SAS connector, which is used to connect integrated storage to the SAS expander.

Component	Module	Type	Location	Field replaceable unit (FRU)?	Description
SBB mid-plane interconnect	I/O	Physical	Controller	No	Indicates the state of the mid-plane connector, which is used to connect each controller to the mid-plane.
Processor core	I/O	Physical	Controller	No	Indicates the state of the processor cores within each controller.
Enclosure electronics power	I/O	Physical	Controller	No	Indicates the state of the power system used by the enclosure.
Enclosure electronics diagnostics	I/O	Physical	Controller	No	Indicates the state of the diagnostics subsystems provided by the controller.
Baseboard Management Controller (BMC)	I/O	Physical	Controller	No	Indicates the state of the baseboard management controller (BMC), which is a specialized service processor that monitors the hardware device through sensors and communicates with the system administrator via an independent connection.
Ethernet	I/O	Physical	Controller	No	Indicates the state of each of the network interfaces, that is, the management and data ports provided on the controller.
NVRAM	I/O	Physical	Controller	No	Indicates the state of NVRAM, a non-volatile random access memory backed up by the battery that serves to retain application-critical information in the event of power failure.

Component list for EBOD enclosure of StorSimple device

The following table outlines the physical and logical components contained in the EBOD enclosure (only present in 8600 model) of your on-premises StorSimple device.

Component	Module	Type	Location	FRU?	Description
Drive in slot [0-11]	Disk Drives	Physical	Shared	Yes	One line is presented for each of the HDD drives in the front of the EBOD enclosure.
Ambient temperature sensor	Enclosure	Physical	Shared	No	Measures the temperature within the chassis.
Mid-plane temperature sensor	Enclosure	Physical	Shared	No	Measures the temperature of the mid-plane.
Audible alarm	Enclosure	Physical	Shared	No	Indicates whether the audible alarm subsystem within the chassis is functional.
Enclosure	Enclosure	Physical	Shared	Yes	Indicates the presence of a chassis.
Enclosure settings	Enclosure	Physical	Shared	No	Refers to the OPS or the front panel of the chassis.
Line voltage sensors	PCM	Physical	Shared	No	Numerous line voltage sensors have their state displayed, which indicates whether the measured voltage is within tolerance.
Line current sensors	PCM	Physical	Shared	No	Numerous line current sensors have their state displayed, which indicates whether the measured current is within tolerance.
Temperature sensors in PCM	PCM	Physical	Shared	No	Numerous temperature sensors such as Inlet and Hotspot sensors have their state displayed, which indicates whether the measured temperature is within tolerance.
Power supply [0-1]	PCM	Physical	Shared	Yes	One line is presented for each of the power supplies in the two PCMs located in the back of the device.
Cooling [0-1]	PCM	Physical	Shared	Yes	One line is presented for each of the four cooling fans residing in the two PCMs.

Component	Module	Type	Location	FRU?	Description
Local storage [HDD]	N/A	Logical	Shared	N/A	Displays the state of the logical storage pool that is created from device HDDs.
Controller [0-1] [state]	I/O	Physical	Controller	Yes	Displays the state of the controllers in the EBOD module.
Temperature sensors in EBOD	I/O	Physical	Controller	No	Numerous temperature sensors from each controller have their state displayed, which indicates whether the temperature encountered is within tolerance.
SAS expander	I/O	Physical	Controller	No	Indicates the state of the SAS expander, which is used to connect the integrated storage to the controller.
SAS connector [0-2]	I/O	Physical	Controller	No	Indicates the state of each SAS connector, which is used to connect integrated storage to the SAS expander.
SBB mid-plane interconnect	I/O	Physical	Controller	No	Indicates the state of the mid-plane connector, which is used to connect each controller to the mid-plane.
Enclosure electronics power	I/O	Physical	Controller	No	Indicates the state of the power system used by the enclosure.
Enclosure electronics diagnostics	I/O	Physical	Controller	No	Indicates the state of the diagnostics subsystems provided by the controller.
Connection to device controller	I/O	Physical	Controller	No	Indicates the state of the connection between the EBOD I/O module and the device controller.

Next steps

- To use the StorSimple Device Manager service to administer your device, go to [use the StorSimple Device Manager service to administer your StorSimple device](#).
- If you need to troubleshoot a device component that has a degraded or failed status, refer to [StorSimple monitoring indicators](#).
- To replace a failed hardware component, see [StorSimple hardware component replacement](#).

- If you continue to experience device issues, [contact Microsoft Support](#).

Use StorSimple monitoring indicators to manage your device

Article • 08/22/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Your StorSimple device includes light-emitting diodes (LEDs) and alarms that you can use to monitor the modules and overall status of the StorSimple device. The monitoring indicators can be found on the hardware components of the device's primary enclosure and the EBOD enclosure. The monitoring indicators can be either LEDs or audible alarms.

There are three LED states used to indicate the status of a module: green, flashing green to red-amber, or red-amber.

- Green LEDs represent a healthy operating status.
- Flashing green to red-amber LEDs represent the presence of non-critical conditions that might require user intervention.
- Red-amber LEDs indicate that there is a critical fault present within the module.

The remainder of this article describes the various monitoring indicator LEDs, their locations on the StorSimple device, the device status based on the LED states, and any associated audible alarms.

Front panel indicator LEDs

The front panel, also known as the *operations panel* or *ops panel*, displays the aggregate status of all the modules in the system. The front panel is identical on the StorSimple primary and the EBOD enclosure, and is illustrated below.



The front panel contains the following indicators:

1. Mute button
2. Power indicator LED (green/red-amber)
3. Module fault indicator LED (ON red-amber/OFF)
4. Logical fault indicator LED (ON red-amber/OFF)
5. Unit ID display

The major difference between the front panel LEDs for the device and those for the EBOD enclosure is the **System Unit Identification Number** shown on the LED display. The default unit ID displayed on the device is **00**, whereas the default unit ID displayed on the EBOD enclosure is **01**. This allows you to quickly differentiate between the device and the EBOD enclosure when the device is turned on. If your device is turned off, use the information provided in [Turn on a new device](#) to differentiate the device from the EBOD enclosure.

Front panel LED status

Use the following table to identify the status indicated by the LEDs on the front panel for the device or the EBOD enclosure.

System power	Module fault	Logical fault	Alarm	Status
Red-amber	OFF	OFF	N/A	AC power lost, operating on backup power, or AC power ON and the controller modules were removed.
Green	ON	ON	N/A	Ops panel power on (5s) test state
Green	OFF	OFF	N/A	Power on, all functions good
Green	ON	N/A	PCM fault LEDs, fan fault LEDs	Any PCM fault, fan fault, over or under temperature

System power	Module fault	Logical fault	Alarm	Status
Green	ON	N/A	I/O module LEDs	Any controller module fault
Green	ON	N/A	N/A	Enclosure logic fault
Green	Flash	N/A	Module status LED on controller module. PCM fault LEDs, fan fault LEDs	Unknown controller module type installed, I2C bus failure, controller module vital product data (VPD) configuration error

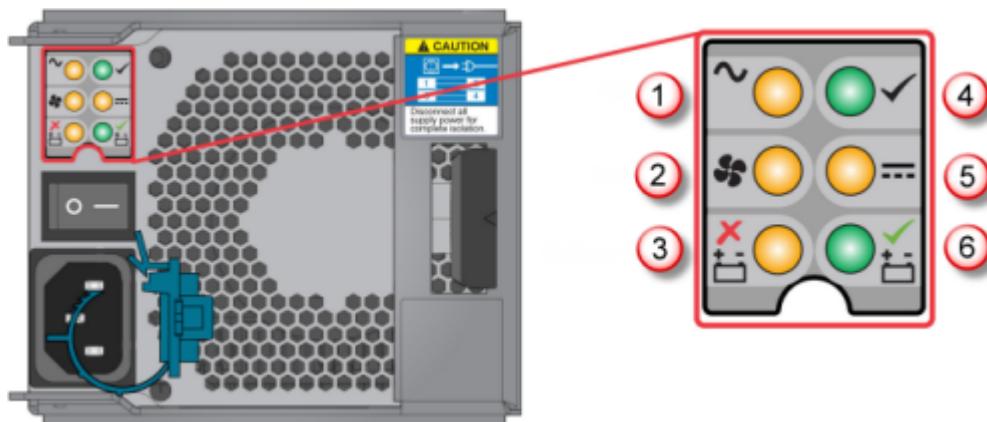
Power cooling module (PCM) indicator LEDs

Power cooling module (PCM) indicator LEDs can be found on the back of the primary enclosure or EBOD enclosure on each PCM module. This topic discusses how to use the following LEDs to monitor the status of your StorSimple device.

- PCM LEDs for the primary enclosure
- PCM LEDs for the EBOD enclosure

PCM LEDs for the primary enclosure

The StorSimple device has a 764W PCM module with an additional battery. The following illustration shows the LED panel for the device.



LED legend:

1. AC power failure
2. Fan failure
3. Battery fault
4. PCM OK
5. DC failure
6. Battery good

The status of the PCM is indicated on the LED panel. The device PCM LED panel has six LEDs. Four of these LEDs display the status of the power supply and the fan. The remaining two LEDs indicate the status of the backup battery module in the PCM. You can use the following tables to determine the status of the PCM.

PCM indicator LEDs for power supply and fan

Status	PCM OK (green)	AC fail (amber)	Fan fail (amber)	DC fail (amber)
No AC power (to enclosure)	OFF	OFF	OFF	OFF
No AC power (this PCM only)	OFF	ON	OFF	ON
AC present PCM ON - OK	ON	OFF	OFF	OFF
PCM fail (fan fail)	OFF	OFF	ON	N/A
PCM fault (over amp, over voltage, over current)	OFF	ON	ON	ON
PCM (fan out of tolerance)	ON	OFF	OFF	ON
Standby mode	Flashing	OFF	OFF	OFF
PCM firmware download	OFF	Flashing	Flashing	Flashing

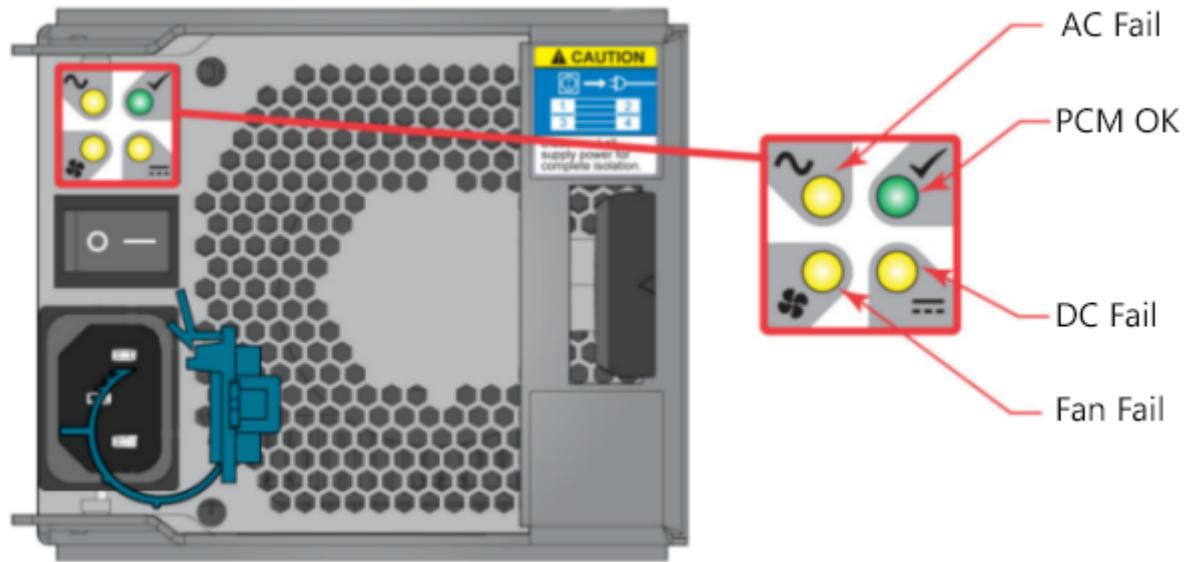
PCM indicator LEDs for the backup battery

Status	Battery good (green)	Battery fault (amber)
Battery not present	OFF	OFF
Battery present and charged	ON	OFF
Battery charging or maintenance discharge	Flashing	OFF
Battery "soft" fault (recoverable)	OFF	Flashing
Battery "hard" fault (non-recoverable)	OFF	ON
Battery disarmed	Flashing	OFF

PCM LEDs for the EBOD enclosure

The EBOD enclosure has a 580W PCM and no additional battery. The PCM panel for the EBOD enclosure has indicator LEDs only for the power supplies and the fan. The

following illustration shows these LEDs.



You can use the following table to determine the status of the PCM.

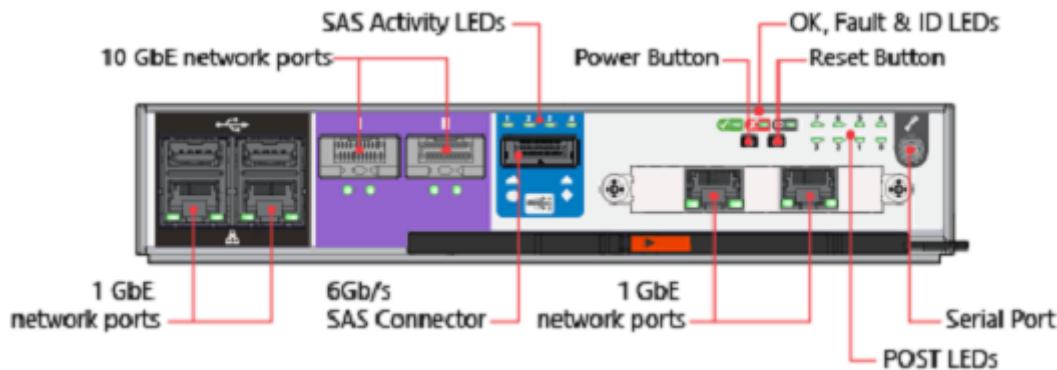
Status	PCM OK (green)	AC fail (amber)	Fan fail (amber)	DC fail (amber)
No AC power (to enclosure)	OFF	OFF	OFF	OFF
No AC power (this PCM only)	OFF	ON	OFF	ON
AC present PCM ON – OK	ON	OFF	OFF	OFF
PCM fail (fan fail)	OFF	OFF	ON	X
PCM fault (over amp, over voltage, over current)	OFF	ON	ON	ON
PCM (fan out of tolerance)	ON	OFF	OFF	ON
Standby mode	Flashing	OFF	OFF	OFF
PCM firmware download	OFF	Flashing	Flashing	Flashing

Controller module indicator LEDs

The StorSimple device contains LEDs for the primary controller and the EBOD controller modules.

Monitoring LEDs for the primary controller

The following illustration helps you identify the LEDs on the primary controller. (All of the components are listed to aid in orientation.)



Use the following table to determine whether the controller module is operating correctly.

Controller indicator LEDs

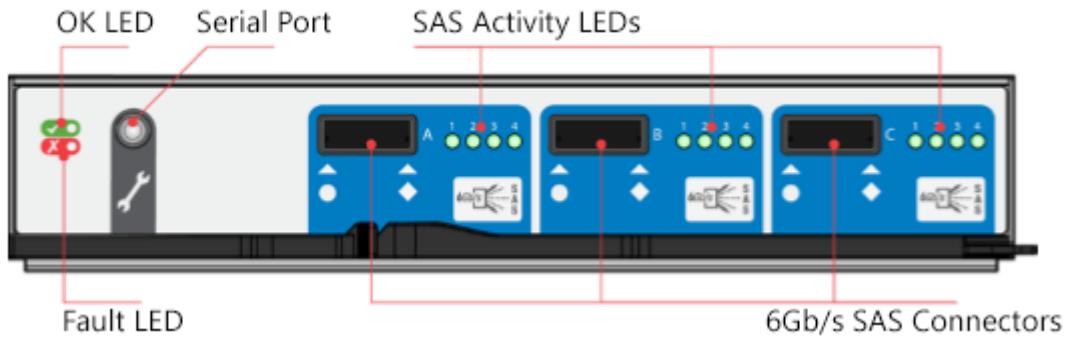
LED	Description
ID LED (blue)	Indicates that the module is being identified. If the blue LED is blinking on a running controller, then the controller is the active controller and the other one is the standby controller. For more information, see Identify the active controller on your device .
Fault LED (amber)	Indicates a fault in the controller.
OK LED (green)	Steady green indicates that the controller is OK. Flashing green indicates a controller VPD configuration error.
SAS activity LEDs (green)	Steady green indicates a connection with no current activity. Flashing green indicates the connection has ongoing activity.
Ethernet status LEDs	Right side indicates link/network activity: (steady green) link active, (flashing green) network activity. Left side indicates network speed: (yellow) 1000 Mb/s, (green) 100 Mb/s, and (OFF) 10 Mb/s. Depending on the component model, this light might blink even if the network interface is not enabled.
POST LEDs	Indicates the boot progress when the controller is turned on. If the StorSimple device fails to boot, this LED will help Microsoft Support identify the point in the boot process at which the failure occurred.

Important

If the fault LED is lit, there is a problem with the controller module that might be resolved by restarting the controller. Please contact Microsoft Support if restarting the controller does not resolve this issue.

Monitoring LEDs for the EBOD (EBOD enclosure)

Each of the 6 Gb/s SAS EBOD controllers has LEDs that indicate its status as shown in the following illustration.



Use the following table to determine whether the EBOD controller module is operating normally.

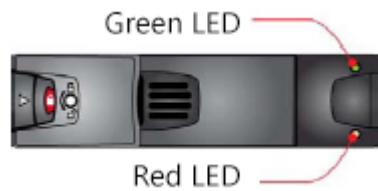
EBOD controller module indicator LEDs

Status	I/O module OK (green)	I/O module fault (amber)	Host port activity (green)
Controller module OK	ON	OFF	-
Controller module fault	OFF	ON	-
No external host port connection	-	-	OFF
External host port connection – no activity	-	-	ON
External host port connection – activity	-	-	Flashing
Controller module metadata error	Flashing	-	-

Disk drive indicator LEDs for the primary enclosure and EBOD enclosure

The StorSimple device has disk drives located in both the primary enclosure and the EBOD enclosure. Each disk drive contains monitoring indicator LEDs, as described in this section.

For the disk drives, the drive status is indicated by a green LED and a red-amber LED mounted on the front of each drive carrier module. The following illustration shows these LEDs.



Use the following table to determine the state of each disk drive, which in turn affects the overall front panel LED status.

Disk drive indicator LEDs for the EBOD enclosure

Status	Activity OK LED (green)	Fault LED (red-amber)	Associated ops panel LED
No drive installed	OFF	OFF	None
Drive installed and operational	Flashing on/off with activity	X	None
SCSI Enclosure Services (SES) device identity set	ON	Flashing 1 second on/1 second off	None
SES device fault bit set	ON	ON	Logical fault (red)
Power control circuit failure	OFF	ON	Module fault (red)

Audible alarms

A StorSimple device contains audible alarms associated with both the primary enclosure and the EBOD enclosure. An audible alarm is located on the front panel (also known as the ops panel) of both enclosures. The audible alarm indicates when a fault condition is present. The following conditions will activate the alarm:

- Fan fault or failure
- Voltage out of range
- Over or under temperature condition
- Thermal overrun
- System fault
- Logical fault
- Power supply fault

- Removal of a power cooling module (PCM)

The following table describes the various alarm states.

Alarm states

Alarm state	Action	Action with mute button pressed
S0	Normal mode: silent	Beep twice
S1	Fault mode: 1 second on/1 second off	Transition to S2 or S3 (see notes)
S2	Remind mode: intermittent beep	None
S3	Muted mode: silent	None
S4	Critical fault mode: continuous alarm	Not available: mute not active

ⓘ Note

- In alarm state S1, if you do not press mute within 2 minutes, the state automatically transitions to S2 or S3.
- Alarm states S1 to S4 return to S0 after the fault condition is cleared.
- Critical fault state S4 can be entered from any other state.

You can mute the audible alarm by pressing the mute button on the ops panel. Automatic muting will occur after two minutes if the mute switch is not manually operated. When the alarm is muted, it will continue to sound with short intermittent beeps to indicate that a problem still exists. The alarm will be silent when all the problems are cleared.

The following table describes the various alarm conditions.

Alarm conditions

Status	Severity	Alarm	Ops panel LED
PCM alert – loss of DC power from a single PCM	Fault – no loss of redundancy	S1	Module fault
PCM alert – loss of DC power from a single PCM	Fault – loss of redundancy	S1	Module fault

Status	Severity	Alarm	Ops panel LED
PCM fan fail	Fault – loss of redundancy	S1	Module fault
SBB module detected PCM fault	Fault	S1	Module fault
PCM removed	Configuration error	None	Module fault
Enclosure configuration error	Fault – critical	S1	Module fault
Low warning temperature alert	Warning	S1	Module fault
High warning temperature alert	Warning	S1	Module fault
Over temperature alarm	Fault – critical	S1	Module fault
I2C bus failure	Fault – loss of redundancy	S1	Module fault
Ops panel communication error (I2C)	Fault – critical	S1	Module fault
Controller error	Fault – critical	S1	Module fault
SBB interface module fault	Fault – critical	S1	Module fault
SBB interface module fault – No functioning modules remaining	Fault – critical	S4	Module fault
SBB interface module removed	Warning	None	Module fault
Drive power control fault	Warning – no loss of drive power	S1	Module fault
Drive power control fault	Fault – critical; loss of drive power	S1	Module fault
Drive removed	Warning	None	Module fault

Status	Severity	Alarm	Ops panel LED
Insufficient power available	Warning	none	Module fault

Next steps

Learn more about [StorSimple hardware components and status](#).

Troubleshoot StorSimple device deployment issues

Article • 08/19/2022 • 28 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article provides helpful troubleshooting guidance for your Microsoft Azure StorSimple deployment. It describes common issues, possible causes, and recommended steps to help you resolve problems that you might experience when you configure StorSimple.

This information applies to both the StorSimple 8000 series physical device and the StorSimple Cloud Appliance.

ⓘ Note

Device configuration-related issues that you may face can occur when you deploy the device for the first time, or they can occur later, when the device is operational. This article focuses on troubleshooting first-time deployment issues. To troubleshoot an operational device, go to [Use the Diagnostics tool to troubleshoot an operational device](#).

This article also describes the tools for troubleshooting StorSimple deployments and provides a step-by-step troubleshooting example.

First-time deployment issues

If you run into an issue when deploying your device for the first time, consider the following guidance:

- If you are troubleshooting a physical device, make sure that the hardware has been installed and configured as described in [Install your StorSimple 8100 device](#) or [Install your StorSimple 8600 device](#).
- Check prerequisites for deployment. Make sure that you have all the information described in the [deployment configuration checklist](#).
- Review the StorSimple Release Notes to see if the problem is described. The release notes include workarounds for known installation problems.

During device deployment, the most common issues that users face occur when they run the setup wizard and when they register the device via Windows PowerShell for StorSimple. (You use Windows PowerShell for StorSimple to register and configure your StorSimple device. For more information on device registration, see [Step 3: Configure and register your device through Windows PowerShell for StorSimple](#)).

The following sections can help you resolve issues that you come across when you configure the StorSimple device for the first time.

First-time setup wizard process

The following steps summarize the setup wizard process. For detailed setup information, see [Deploy your on-premises StorSimple device](#).

1. Run the [Invoke-HcsSetupWizard](#) cmdlet to start the setup wizard that will guide you through the remaining steps.
2. Configure the network: the setup wizard lets you configure network settings for the DATA 0 network interface on your StorSimple device. The following settings are included:
 - Virtual IP (VIP), subnet mask, and gateway – The [Set-HcsNetInterface](#) cmdlet is executed in the background. It configures the IP address, subnet mask, and gateway for the DATA 0 network interface on your StorSimple device.
 - Primary DNS server – The [Set-HcsDnsClientServerAddress](#) cmdlet is executed in the background. It configures the DNS settings for your StorSimple solution.
 - NTP server – The [Set-HcsNtpClientServerAddress](#) cmdlet is executed in the background. It configures the NTP server settings for your StorSimple solution.

- Optional web proxy – The [Set-HcsWebProxy](#) cmdlet is executed in the background. It sets and enables the web proxy configuration for your StorSimple solution.

3. Set up the password: the next step is to set up the device administrator password. The device administrator password is used to log on to your device. The default device password is **Password1**.

ⓘ Important

Passwords are collected before registration, but applied only after you successfully register the device. If there is a failure to apply a password, you will be prompted to supply the password again until the required passwords (that meet the complexity requirements) are collected.

4. Register the device: the final step is to register the device with the StorSimple Device Manager service running in Microsoft Azure. The registration requires you to [get the service registration key](#) from the Azure portal, and provide it in the setup wizard. After the device is successfully registered, a service data encryption key is provided to you. Be sure to keep this encryption key in a safe location because it will be required to register all future devices with the service.

Common errors during device deployment

The following tables list common errors you might come across when you:

- Configure the required network settings.
- Configure the optional web proxy settings.
- Set up the device administrator password.
- Register the device.

Errors during the required network settings

No.	Error message	Possible causes	Recommended action
1	Invoke-HcsSetupWizard: This command can only be run on the active controller.	Configuration was being performed on the passive controller.	Run this command from the active controller. For more information, see Identify an active controller on your device .

No.	Error message	Possible causes	Recommended action
2	Invoke-HcsSetupWizard: Device not ready.	There are issues with the network connectivity on DATA 0.	Check the physical network connectivity on DATA 0.
3	Invoke-HcsSetupWizard: There is an IP address conflict with another system on the network (Exception from HRESULT: 0x80070263).	The IP supplied for DATA 0 was already in use by another system.	Provide a new IP that is not in use.
4	Invoke-HcsSetupWizard: A cluster resource failed. (Exception from HRESULT: 0x800713AE).	Duplicate VIP. The supplied IP is already in use.	Provide a new IP that is not in use.
5	Invoke-HcsSetupWizard: Invalid IPv4 address.	The IP address is provided in an incorrect format.	Check the format and supply your IP address again. For more information, see Ipv4 Addressing .
6	Invoke-HcsSetupWizard: Invalid IPv6 address.	The IP address is provided in an incorrect format.	Check the format and supply your IP address again. For more information, see Ipv6 Addressing .
7	Invoke-HcsSetupWizard: There are no more endpoints available from the endpoint mapper. (Exception from HRESULT: 0x800706D9)	The cluster functionality is not working.	Contact Microsoft Support for next steps.

Errors during the optional web proxy settings

No.	Error message	Possible causes	Recommended action
1	Invoke-HcsSetupWizard: Invalid parameter (Exception from HRESULT: 0x80070057)	One of the parameters provided for the proxy settings is not valid.	The URI is not provided in the correct format. Use the following format: <code>http://<IP address or FQDN of the web proxy server>:<TCP port number></code>

No.	Error message	Possible causes	Recommended action
2	Invoke-HcsSetupWizard: RPC server not available (Exception from HRESULT: 0x800706ba)	The root cause is one of the following: 1. The cluster is not up. 2. The passive controller cannot communicate with the active controller, and the command is run from passive controller.	Depending on the root cause: 1. Contact Microsoft Support to make sure that the cluster is up. 2. Run the command from the active controller. If you want to run the command from the passive controller, you will need to ensure that the passive controller can communicate with the active controller. You will need to contact Microsoft Support if this connectivity is broken.
3	Invoke-HcsSetupWizard: RPC call failed (Exception from HRESULT: 0x800706be)	Cluster is down.	Contact Microsoft Support to make sure that the cluster is up.
4	Invoke-HcsSetupWizard: Cluster resource not found (Exception from HRESULT: 0x8007138f)	The cluster resource is not found. This can happen when the installation was not correct.	You may need to reset the device to the factory default settings. Contact Microsoft Support to create a cluster resource.
5	Invoke-HcsSetupWizard: Cluster resource not online (Exception from HRESULT: 0x8007138c)	Cluster resources are not online.	Contact Microsoft Support for next steps.

Errors related to device administrator password

The default device administrator password is **Password1**. This password expires after the first logon; therefore, you will need to use the setup wizard to change it. You must provide a new device administrator password when you register the device for the first time.

Make sure that your passwords meet the following requirements:

- Your device administrator password should be from 8 to 15 characters long.
- Passwords should contain three of the following character types: lowercase, uppercase, numeric, and special.
- Your password cannot be the same as the last 24 passwords.

In addition, keep in mind that passwords expire every year, and can be changed only after you successfully register the device. If the registration fails for any reason, the passwords will not be changed.

For more information on device administrator password, go to [Use the StorSimple Device Manager service to change your StorSimple password](#).

You may encounter one or more of the following errors when setting up the device administrator and StorSimple Snapshot Manager passwords.

No.	Error message	Recommended action
1	The password exceeds the maximum length.	Your device administrator password must be between 8 and 15 characters long.
2	The password does not meet the required length.	Your device administrator password must be between 8 and 15 characters long.
3	The password must contain lowercase characters.	Passwords must contain 3 of the following 4 character types: lowercase, uppercase, numeric, and special. Make sure that your password meets these requirements.
4	The password must contain numeric characters.	Passwords must contain 3 of the following 4 character types: lowercase, uppercase, numeric, and special. Make sure that your password meets these requirements.
5	The password must contain special characters.	Passwords must contain 3 of the following 4 character types: lowercase, uppercase, numeric, and special. Make sure that your password meets these requirements.

No.	Error message	Recommended action
6	The password must contain 3 of the following 4 character types: uppercase, lowercase, numeric, and special.	Your password does not contain the required types of characters. Make sure that your password meets these requirements.
7	Parameter does not match confirmation.	Make sure that your password meets all requirements and that you entered it correctly.
8	Your password cannot match the default.	The default password is <i>Password1</i> . You need to change this password after you log on for the first time.
9	The password you have entered does not match the device password. Please retype the password.	Check the password and type it again.

Passwords are collected before the device is registered, but are applied only after successful registration. The password recovery workflow requires the device to be registered.

Important

In general, if an attempt to apply a password fails, then the software repeatedly attempts to collect the password until it is successful. In rare instances, the password cannot be applied. In this situation, you can register the device and proceed, however the passwords will not be changed. You can change the device administrator password after the registration from the Azure portal.

You can reset the password in the Azure portal via the StorSimple Device Manager service. For more information, go to [Change the device administrator password](#).

Errors during device registration

You use the StorSimple Device Manager service running in Microsoft Azure to register the device. You could encounter one or more of the following issues during device registration.

No.	Error message	Possible causes	Recommended action
-----	---------------	-----------------	--------------------

No.	Error message	Possible causes	Recommended action
1	Error 350027: Failed to register the device with the StorSimple Device Manager.		Wait for a few minutes and then try the operation again. If the issue persists, contact Microsoft Support .
2	Error 350013: An error has occurred in registering the device. This could be due to incorrect service registration key.		Please register the device again with the correct service registration key. For more information, see Get the service registration key .
3	Error 350063: Authentication to StorSimple Device Manager service passed but registration failed. Please retry the operation after some time.	This error indicates that authentication with ACS has passed but the register call made to the service has failed. This could be a result of a sporadic network glitch.	If the issue persists, please contact Microsoft Support .
4	Error 350049: The service could not be reached during registration.	When the call is made to the service, a web exception is received. In some cases, this may get fixed by retrying the operation later.	Please check your IP address and DNS name and then retry the operation. If the problem persists, contact Microsoft Support .
5	Error 350031: The device has already been registered.		No action necessary.
6	Error 350016: Device Registration failed.		Please make sure the registration key is correct.
7	Invoke-HcsSetupWizard: An error has occurred while registering your device; this could be due to incorrect IP address or DNS name. Please check your network settings and try again. If the problem persists, contact Microsoft Support . (Error 350050)	Ensure that your device can ping the outside network. If you do not have connectivity to outside network, the registration may fail with this error. This error may be a combination of one or more of the following: <ul style="list-style-type: none">• Incorrect IP• Incorrect subnet• Incorrect gateway• Incorrect DNS settings	See the steps in the Step-by-step troubleshooting example .

No.	Error message	Possible causes	Recommended action
8	Invoke-HcsSetupWizard: The current operation failed due to an internal service error [0x1FBE2]. Please retry the operation after some time. If the issue persists, please contact Microsoft Support.	This is a generic error thrown for all user invisible errors from service or agent. The most common reason may be that the ACS authentication has failed. A possible cause for the failure is that there are issues with the NTP server configuration and time on the device is not set correctly.	Correct the time (if there are issues) and then retry the registration operation. If you use the Set-HcsSystem -Timezone command to adjust the time zone, capitalize each word in the time zone (for example "Pacific Standard Time"). If this issue persists, contact Microsoft Support for next steps.
9	Warning: Could not activate the device. Your device administrator and StorSimple Snapshot Manager passwords have not been changed.	If the registration fails, the device administrator and StorSimple Snapshot Manager passwords are not changed.	

Tools for troubleshooting StorSimple deployments

StorSimple includes several tools that you can use to troubleshoot your StorSimple solution. These tools include:

- Support packages and device logs.
- Cmdlets designed for troubleshooting.

Support packages and device logs available for troubleshooting

A support package contains all the relevant logs that can assist the Microsoft Support team with troubleshooting device issues. You can use Windows PowerShell for StorSimple to generate an encrypted support package that you can then share with support personnel.

To view the logs or the contents of the support package

1. Use Windows PowerShell for StorSimple to generate a support package as described in [Create and manage a support package](#).

2. Download the decryption script [locally](#) on your client computer.
3. Use this [step-by-step procedure](#) to open and decrypt the support package.
4. The decrypted support package logs are in etw/etvx format. You can perform the following steps to view these files in Windows Event Viewer:
 - a. Run the `eventvwr` command on your Windows client to start the Event Viewer.
 - b. In the **Actions** pane, click **Open Saved Log** and point to the log files in etvx/etw format (the support package). You can now view the file. After you open the file, you can right-click and save the file as text.

 **Important**

You can also use the **Get-WinEvent** cmdlet to open these files in Windows PowerShell. For more information, see [Get-WinEvent](#) in the Windows PowerShell cmdlet reference documentation.

5. When the logs open in Event Viewer, look for the following logs that contain issues related to the device configuration:
 - hcs_pfconfig/Operational Log
 - hcs_pfconfig/Config
6. In the log files, search for strings related to the cmdlets called by the setup wizard. See [First-time setup wizard process](#) for a list of these cmdlets.
7. If you are not able to figure out the cause of the problem, you can [contact Microsoft Support](#) for next steps. Use the steps in [Create a support request](#) when you contact Microsoft Support for assistance.

Cmdlets available for troubleshooting

Use the following Windows PowerShell cmdlets to detect connectivity errors.

- `Get-NetAdapter`: Use this cmdlet to detect the health of network interfaces.
- `Test-Connection`: Use this cmdlet to check the network connectivity inside and outside of the network.
- `Test-HcsConnection`: Use this cmdlet to check the connectivity of a successfully registered device.
- `Sync-HcsTime`: Use this cmdlet to display device time and force a time sync with the NTP server.

- `Enable-HcsPing` and `Disable-HcsPing`: Use these cmdlets to allow the hosts to ping the network interfaces on your StorSimple device. By default, the StorSimple network interfaces do not respond to ping requests.
- `Trace-HcsRoute`: Use this cmdlet as a route tracing tool. It sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Since `Trace-HcsRoute` shows the degree of packet loss at any given router or link, you can pinpoint which routers or links might be causing network problems.
- `Get-HcsRoutingTable`: Use this cmdlet to display the local IP routing table.

Troubleshoot with the Get-NetAdapter cmdlet

When you configure network interfaces for a first-time device deployment, the hardware status is not available in the StorSimple Device Manager service UI because the device is not yet registered with the service. Additionally, the **Hardware health** blade may not always correctly reflect the state of the device, especially if there are issues that affect service synchronization. In these situations, you can use the `Get-NetAdapter` cmdlet to determine the health and status of your network interfaces.

To see a list of all the network adapters on your device

1. Start Windows PowerShell for StorSimple, and then type `Get-NetAdapter`.
2. Use the output of the `Get-NetAdapter` cmdlet and the following guidelines to understand the status of your network interface.
 - If the interface is healthy and enabled, the `ifIndex` status is shown as **Up**.
 - If the interface is healthy but is not physically connected (by a network cable), the `ifIndex` is shown as **Disabled**.
 - If the interface is healthy but not enabled, the `ifIndex` status is shown as **NotPresent**.
 - If the interface does not exist, it does not appear in this list. The StorSimple Device Manager service UI will still show this interface in a failed state.

For more information on how to use this cmdlet, go to [Get-NetAdapter](#) in the Windows PowerShell cmdlet reference.

The following sections show samples of output from the `Get-NetAdapter` cmdlet.

In these samples, controller 0 was the passive controller, and was configured as follows:

- DATA 0, DATA 1, DATA 2, and DATA 3 network interfaces existed on the device.

- DATA 4 and DATA 5 network interface cards were not present; therefore, they are not listed in the output.
- DATA 0 was enabled.

Controller 1 was the active controller, and was configured as follows:

- DATA 0, DATA 1, DATA 2, DATA 3, DATA 4, and DATA 5 network interfaces existed on the device.
- DATA 0 was enabled.

Sample output – controller 0

The following sample data is the output from controller 0 (the passive controller). DATA 1, DATA 2, and DATA 3 are not connected. DATA 4 and DATA 5 are not listed because they are not present on the device.

Output			
Controller0>Get-NetAdapter			
Name	InterfaceDescription	ifIndex	
Status			
---	-----	-----	--
---	-----	-----	--
DATA3	Mellanox ConnectX-3 Ethernet Adapter #2	17	
NotPresent			
DATA2	Mellanox ConnectX-3 Ethernet Adapter	14	
NotPresent			
Ethernet 2	HCS VNIC	13	Up
DATA1	Intel(R) 82574L Gigabit Network Co...#2	16	
NotPresent			
DATA0	Intel(R) 82574L Gigabit Network Conn...	15	Up

Sample output – controller 1

The following sample data is the output from controller 1 (the active controller). Only the DATA 0 network interface on the device is configured and working.

Output			
Controller1>Get-NetAdapter			
Name	InterfaceDescription	ifIndex	
Status			
---	-----	-----	--
---	-----	-----	--
DATA3	Mellanox ConnectX-3 Ethernet Adapter	18	
NotPresent			
DATA2	Mellanox ConnectX-3 Ethernet Adapter #2	19	
NotPresent			
DATA1	Intel(R) 82574L Gigabit Network Co...#2	16	

NotPresent				
DATA0	Intel(R) 82574L Gigabit Network Conn...	15	Up	
Ethernet 2	HCS VNIC	13	Up	
DATA5	Intel(R) Gigabit ET Dual Port Server...	14		
NotPresent				
DATA4	Intel(R) Gigabit ET Dual Port Serv...#2	17		
NotPresent				

Troubleshoot with the Test-Connection cmdlet

You can use the `Test-Connection` cmdlet to determine whether your StorSimple device can connect to the outside network. If all the networking parameters, including the DNS, are configured correctly in the setup wizard, you can use the `Test-Connection` cmdlet to ping a known address outside of the network, such as outlook.com.

If the ping cmdlet is disabled, you should enable ping for use in troubleshooting connectivity issues.

See the following samples of output from the `Test-Connection` cmdlet.

ⓘ Note

In the first sample, the device is configured with an incorrect DNS. In the second sample, the DNS is correct.

Sample output – incorrect DNS

The following sample does not include any output for the IPV4 and IPV6 addresses, which indicates the DNS is not resolved. There is no connectivity to the outside network, and a correct DNS needs to be supplied.

Output			
Source	Destination	IPV4Address	IPV6Address
-----	-----	-----	-----
HCSNODE0	outlook.com		

Sample output – correct DNS

In the following sample, the DNS returns the IPV4 address, indicating that the DNS is configured correctly. The output confirms that there is connectivity to the outside

network.

Output			
Source	Destination	IPV4Address	IPV6Address
-----	-----	-----	-----
HCSNODE0	outlook.com	132.245.92.194	

Troubleshoot with the Test-HcsmConnection cmdlet

Use the `Test-HcsmConnection` cmdlet for a device that is already connected to and registered with your StorSimple Device Manager service. This cmdlet helps you verify the connectivity between a registered device and the corresponding StorSimple Device Manager service. You can run this command on Windows PowerShell for StorSimple.

To run the Test-HcsmConnection cmdlet

1. Make sure that the device is registered.
2. Check the device status. If the device is deactivated, in maintenance mode, or offline, you might see one of the following errors:
 - `ErrorCode.CiDDeviceDecommissioned`: Indicates the device is deactivated.
 - `ErrorCode.DeviceNotReady`: Indicates the device is in maintenance mode.
 - `ErrorCode.DeviceNotReady`: Indicates the device is not online.
3. Verify that the StorSimple Device Manager service is running (use the [Get-ClusterResource](#) cmdlet). If the service is not running, you might see the following errors:
 - `ErrorCode.CiSApplianceAgentNotOnline`
 - `ErrorCode.CisPowershellScriptHcsError`: Indicates that there was an exception when you ran `Get-ClusterResource`.
4. Check the Access Control Service (ACS) token. If it throws a web exception, it might be the result of a gateway problem, a missing proxy authentication, an incorrect DNS, or an authentication failure. You might see the following errors:

- ErrorCode.CiSApplianceGateway: Indicates an HttpStatusCode.BadGateway exception: the name resolver service could not resolve the host name.
- ErrorCode.CiSApplianceProxy: Indicates an HttpStatusCode.ProxyAuthenticationRequired exception (HTTP status code 407): the client could not authenticate with the proxy server.
- ErrorCode.CiSApplianceDNSError: Indicates a WebExceptionStatus.NameResolutionFailure exception: The name resolver service could not resolve the host name.
- ErrorCode.CiSApplianceACSError: Indicates that the service returned an authentication error, but there is connectivity.

If it does not throw a web exception, check for ErrorCode.CiSApplianceFailure, which indicates the appliance failed.

5. Check the cloud service connectivity. If the service throws a web exception, you might see the following errors:

- ErrorCode.CiSApplianceGateway: Indicates an HttpStatusCode.BadGateway exception: an intermediate proxy server received a bad request from another proxy or from the original server.
- ErrorCode.CiSApplianceProxy: Indicates an HttpStatusCode.ProxyAuthenticationRequired exception (HTTP status code 407): the client could not authenticate with the proxy server.
- ErrorCode.CiSApplianceDNSError: Indicates a WebExceptionStatus.NameResolutionFailure exception: the name resolver service could not resolve the host name.
- ErrorCode.CiSApplianceACSError: Indicates the service returned an authentication error, but there is connectivity.

If it does not throw a web exception, check for ErrorCode.CiSApplianceSaasServiceError, which indicates a problem with the StorSimple Device Manager service.

6. Check Azure Service Bus connectivity. ErrorCode.CiSApplianceServiceBusError indicates that the device cannot connect to the Service Bus.

The log files CiSCommandletLog0Curr.errlog and CiSAgentsvc0Curr.errlog will have more information, such as exception details.

For more information about how to use the cmdlet, go to [Test-HcsmConnection](#) in the Windows PowerShell reference documentation.

ⓘ Important

You can run this cmdlet for both the active and the passive controller.

See the following samples of output from the `Test-HcsmConnection` cmdlet.

Sample output – successfully registered device running StorSimple Update 3

Output

```
Controller1>Test-HcsmConnection

Checking device registration state ... Success
Device registered successfully

Checking primary NTP server [time.windows.com] ... Success

Checking web proxy ... NOT SET

Checking primary IPv4 DNS server [10.222.118.154] ... Success
Checking primary IPv6 DNS server ... NOT SET
Checking secondary IPv4 DNS server [10.222.120.24] ... Success
Checking secondary IPv6 DNS server ... NOT SET

Checking device online ... Success

Checking device authentication ... This will take a few minutes.
Checking device authentication ... Success

Checking connectivity from device to service ... This will take a few
minutes.

Checking connectivity from device to service ... Success

Checking connectivity from service to device ... Success

Checking connectivity to Microsoft Update servers ... Success
Controller1>
```

Sample output – offline device

This sample is from a device that has a status of **Offline** in the Azure portal.

Output

```
Checking device registrationstate: Success  
Device is registered successfully  
Checking connectivity from device to SaaS.. Failure
```

The device could not connect using the current web proxy configuration. There could be an issue with the web proxy configuration or a network connectivity problem. In this case, you should make sure that your web proxy settings are correct and your web proxy servers are online and reachable.

Troubleshoot with the Sync-HcsTime cmdlet

Use this cmdlet to display the device time. If the device time has an offset with the NTP server, you can then use this cmdlet to force-synchronize the time with your NTP server.

- If the offset between the device and NTP server is greater than 5 minutes, you will see a warning.
- If the offset exceeds 15 minutes, then the device will go offline. You can still use this cmdlet to force a time sync.
- However, if the offset exceeds 15 hours, then you will not be able to force-sync the time and an error message will be shown.

Sample output – forced time sync using Sync-HcsTime

Output

```
Controller0>Sync-HcsTime  
The current device time is 4/24/2015 4:05:40 PM UTC.  
  
Time difference between NTP server and appliance is 00.0824069 seconds. Do  
you want to resync time with NTP server?  
[Y] Yes [N] No (Default is "Y"): Y  
Controller0>
```

Troubleshoot with the Enable-HcsPing and Disable-HcsPing cmdlets

Use these cmdlets to ensure that the network interfaces on your device respond to ICMP ping requests. By default, the StorSimple network interfaces do not respond to ping requests. Using this cmdlet is the easiest way to know if your device is online and reachable.

Sample output – Enable-HcsPing and Disable-HcsPing

Output

```
Controller0>
Controller0>Enable-HcsPing
Successfully enabled ping.
Controller0>
Controller0>
Controller0>Disable-HcsPing
Successfully disabled ping.
Controller0>
```

Troubleshoot with the Trace-HcsRoute cmdlet

Use this cmdlet as a route tracing tool. It sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Because the cmdlet shows the degree of packet loss at any given router or link, you can pinpoint which routers or links might be causing network problems.

Sample output showing how to trace the route of a packet with Trace-HcsRoute

Output

```
Controller0>Trace-HcsRoute -Target 10.126.174.25

Tracing route to contoso.com [10.126.174.25]
over a maximum of 30 hops:
    0  HCSNode0 [10.126.173.90]
    1  contoso.com [10.126.174.25]

Computing statistics for 25 seconds...
              Source to Here   This Node/Link
Hop  RTT      Lost/Sent = Pct  Lost/Sent = Pct  Address
    0          0/ 100 =  0%      0/ 100 =  0%  HCSNode0 [10.126.173.90]
                                         | 
    1     0ms      0/ 100 =  0%      0/ 100 =  0%  contoso.com
[10.126.174.25]

Trace complete.
```

Troubleshoot with the Get-HcsRoutingTable cmdlet

Use this cmdlet to view the routing table for your StorSimple device. A routing table is a set of rules that can help determine where data packets traveling over an Internet

Protocol (IP) network will be directed.

The routing table shows the interfaces and the gateway that routes the data to the specified networks. It also gives the routing metric, which is the decision maker for the path taken to reach a particular destination. The lower the routing metric, the higher the preference.

For example, suppose you have two network interfaces, DATA 2 and DATA 3, connected to the Internet. If the routing metrics for DATA 2 and DATA 3 are 15 and 261 respectively, then DATA 2, with the lower routing metric, is the preferred interface used to reach the Internet.

If you are running Update 1 on your StorSimple device, your DATA 0 network interface has the highest preference for the cloud traffic. With this configuration, even if there are other cloud-enabled interfaces, most of the cloud traffic would be routed through DATA 0.

If you run the `Get-HcsRoutingTable` cmdlet without specifying any parameters (as the following example shows), the cmdlet will output both IPv4 and IPv6 routing tables.

Alternatively, you can specify `Get-HcsRoutingTable -IPv4` or `Get-HcsRoutingTable -IPv6` to get a relevant routing table.

Output

```
Controller0>
Controller0>Get-HcsRoutingTable
=====
Interface List
 14...00 50 cc 79 63 40 .....Intel(R) 82574L Gigabit Network Connection
 12...02 9a 0a 5b 98 1f .....Microsoft Failover Cluster Virtual Adapter
 13...28 18 78 bc 4b 85 .....HCS VNIC
 1.....Software Loopback Interface 1
 21...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 22...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0        0.0.0.0  192.168.111.100  192.168.111.101
15
          127.0.0.0      255.0.0.0    On-link       127.0.0.1    306
          127.0.0.1  255.255.255.255    On-link       127.0.0.1    306
        127.255.255.255  255.255.255.255    On-link       127.0.0.1    306
          169.254.0.0      255.255.0.0    On-link     169.254.1.235    261
          169.254.1.235  255.255.255.255    On-link     169.254.1.235
261
        169.254.255.255  255.255.255.255    On-link     169.254.1.235    261
```

```

        192.168.111.0    255.255.255.0      On-link    192.168.111.101
266
    192.168.111.101  255.255.255.255      On-link    192.168.111.101  266
    192.168.111.255  255.255.255.255      On-link    192.168.111.101  266
        224.0.0.0       240.0.0.0       On-link     127.0.0.1      306
        224.0.0.0       240.0.0.0       On-link     169.254.1.235  261
        224.0.0.0       240.0.0.0       On-link    192.168.111.101  266
    255.255.255.255  255.255.255.255      On-link     127.0.0.1      306
    255.255.255.255  255.255.255.255      On-link     169.254.1.235  261
    255.255.255.255  255.255.255.255      On-link    192.168.111.101  266
=====
Persistent Routes:
  Network Address          Netmask   Gateway Address  Metric
        0.0.0.0            0.0.0.0   192.168.111.100    5
=====

IPv6 Route Table
=====
Active Routes:
  If Metric Network Destination      Gateway
    1    306  ::1/128                On-link
   13    276 fd99:4c5b:5525:d80b::/64 On-link
   13    276 fd99:4c5b:5525:d80b::1/128
                                On-link
   13    276 fd99:4c5b:5525:d80b::3/128
                                On-link
   13    276 fe80::/64              On-link
   12    261 fe80::/64              On-link
   13    276 fe80::17a:4eba:7c80:727f/128
                                On-link
   12    261 fe80::fc97:1a53:e81a:3454/128
                                On-link
    1    306 ff00::/8               On-link
   13    276 ff00::/8               On-link
   12    261 ff00::/8               On-link
   14    266 ff00::/8               On-link
=====

Persistent Routes:
  None
Controller0>

```

Step-by-step StorSimple troubleshooting example

The following example shows step-by-step troubleshooting of a StorSimple deployment. In the example scenario, device registration fails with an error message indicating that the network settings or the DNS name is incorrect.

The error message returned is:

Output

```
Invoke-HcsSetupWizard: An error has occurred while registering the device.  
This could be due to incorrect IP address or DNS name. Please check your  
network settings and try again. If the problems persist, contact Microsoft  
Support.
```

```
+CategoryInfo: Not specified
```

```
+FullyQualifiedErrorID: CiSClientCommunicationErrors,
```

```
Microsoft.HCS.Management.PowerShell.Cmdlets.InvokeHcsSetupWizardCommand
```

The error could be caused by any of the following issues:

- Incorrect hardware installation
- Faulty network interface(s)
- Incorrect IP address, subnet mask, gateway, primary DNS server, or web proxy
- Incorrect registration key
- Incorrect firewall settings

To locate and fix the device registration problem

1. Check your device configuration: on the active controller, run `Invoke-HcsSetupWizard`.

(!) Note

The setup wizard must run on the active controller. To verify that you are connected to the active controller, look at the banner presented in the serial console. The banner indicates whether you are connected to controller 0 or controller 1, and whether the controller is active or passive. For more information, go to [Identify an active controller on your device](#).

2. Make sure that the device is cabled correctly: check the network cabling on the device back plane. The cabling is specific to the device model. For more information, go to [Install your StorSimple 8100 device](#) or [Install your StorSimple 8600 device](#).

(!) Note

If you are using 10 GbE network ports, you will need to use the provided QSFP-SFP adapters and SFP cables. For more information, see the [list of cables, switches, and transceivers recommended for the 10 GbE ports](#).

3. Verify the health of the network interface:

- Use the Get-NetAdapter cmdlet to detect the health of the network interfaces for DATA 0.
- If the link isn't functioning, the `ifindex` status will indicate that the interface is down. You will then need to check the network connection of the port to the appliance and to the switch. You will also need to rule out bad cables.
- If you suspect that DATA 0 port on the active controller has failed, you can confirm that by connecting to DATA 0 port on the controller 1. Disconnect the network cable from the back of the device from controller 0, connect the cable to controller 1, and then run the Get-NetAdapter cmdlet again.

If DATA 0 port on a controller fails, [contact Microsoft Support](#) for next steps. You might need to replace the controller on your system.

4. Verify the connectivity to the switch:

- Make sure that DATA 0 network interfaces on controller 0 and controller 1 in your primary enclosure are on the same subnet.
- Check the hub or router. Typically, you should connect both controllers to the same hub or router.
- Make sure that the switches you use for the connection have DATA 0 for both controllers in the same vLAN.

5. Eliminate any user errors:

- Run the setup wizard again (run `Invoke-HcsSetupWizard`), and enter the values again to make sure that there are no errors.
- Verify the registration key used. The same registration key can be used to connect multiple devices to a StorSimple Device Manager service. Use the procedure in [Get the service registration key](#) to ensure that you are using the correct registration key.

Important

If you have multiple services running, you will need to ensure that the registration key for the appropriate service is used to register the device. If you have registered a device with the wrong StorSimple Device Manager service, you will need to [contact Microsoft Support](#) for next steps. You may have to perform a factory reset of the device (which could result in data loss) to then connect it to the intended service.

6. Use the Test-Connection cmdlet to verify that you have connectivity to the outside network. For more information, go to [Troubleshoot with the Test-Connection cmdlet](#).
7. Check for firewall interference. If you have verified that the virtual IP (VIP), subnet, gateway, and DNS settings are all correct, and you still see connectivity issues, it's possible that your firewall is blocking communication between your device and the outside network. Ensure that ports 80 and 443 are available on your StorSimple device for outbound communication. For more information, see [Networking requirements for your StorSimple device](#).
8. Look at the logs. Go to [Support packages and device logs available for troubleshooting](#).
9. If the preceding steps do not solve the problem, [contact Microsoft Support](#) for assistance.

Next steps

Learn how to use the Diagnostics tool to troubleshoot a StorSimple device.

Use the StorSimple Diagnostics Tool to troubleshoot 8000 series device issues

Article • 08/19/2022 • 13 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The StorSimple Diagnostics tool diagnoses issues related to system, performance, network, and hardware component health for a StorSimple device. The diagnostics tool can be used in various scenarios. These scenarios include workload planning, deploying a StorSimple device, assessing the network environment, and determining the performance of an operational device. This article provides an overview of the diagnostics tool and describes how the tool can be used with a StorSimple device.

The diagnostics tool is primarily intended for StorSimple 8000 series on-premises devices (8100 and 8600).

Run diagnostics tool

This tool can be run via the Windows PowerShell interface of your StorSimple device. There are two ways to access the local interface of your device:

- [Use PuTTY to connect to the device serial console.](#)
- [Remotely access the tool via the Windows PowerShell for StorSimple.](#)

In this article, we assume that you have connected to the device serial console via PuTTY.

To run the diagnostics tool

Once you have connected to the Windows PowerShell interface of the device, perform the following steps to run the cmdlet.

1. Log on to the device serial console by following the steps in [Use PuTTY to connect to the device serial console](#).
2. Type the following command:

```
Invoke-HcsDiagnostics
```

If the scope parameter is not specified, the cmdlet executes all the diagnostic tests. These tests include system, hardware component health, network, and performance.

To run only a specific test, specify the scope parameter. For instance, to run only the network test, type

```
Invoke-HcsDiagnostics -Scope Network
```

3. Select and copy the output from the PuTTY window into a text file for further analysis.

Scenarios to use the diagnostics tool

Use the diagnostics tool to troubleshoot the network, performance, system, and hardware health of the system. Here are some possible scenarios:

- **Device offline** - Your StorSimple 8000 series device is offline. However, from the Windows PowerShell interface, it seems that both the controllers are up and running.
 - You can use this tool to then determine the network state.

ⓘ Note

Do not use this tool to assess performance and network settings on a device before the registration (or configuring via setup wizard). A valid IP is assigned to the device during setup wizard and registration. You can run this cmdlet, on a device that is not registered, for hardware health and system. Use the scope parameter, for example:

```
Invoke-HcsDiagnostics -Scope Hardware
```

```
Invoke-HcsDiagnostics -Scope System
```

- **Persistent device issues** - You are experiencing device issues that seem to persist. For instance, registration is failing. You could also be experiencing device issues after the device is successfully registered and operational for a while.
 - In this case, use this tool for preliminary troubleshooting before you log a service request with Microsoft Support. We recommend that you run this tool and capture the output of this tool. You can then provide this output to Support to expedite troubleshooting.
 - If there are any hardware component or cluster failures, you should log in a Support request.
- **Low device performance** - Your StorSimple device is slow.
 - In this case, run this cmdlet with scope parameter set to performance. Analyze the output. You get the cloud read-write latencies. Use the reported latencies as maximum achievable target, factor in some overhead for the internal data processing, and then deploy the workloads on the system. For more information, go to [Use the network test to troubleshoot device performance](#).

Diagnostics test and sample outputs

Hardware test

This test determines the status of the hardware components, the USM firmware, and the disk firmware running on your system.

- The hardware components reported are those components that failed the test or are not present in the system.
- The USM firmware and disk firmware versions are reported for the Controller 0, Controller 1, and shared components in your system. For a complete list of hardware components, go to:
 - [Components in primary enclosure](#)
 - [Components in EBOD enclosure](#)

 **Note**

If the hardware test reports failed components, log in a service request with Microsoft Support.

Sample output of hardware test run on an 8100 device

Here is a sample output from a StorSimple 8100 device. In the 8100 model device, the EBOD enclosure is not present. Hence, the EBOD controller components are not reported.

```
Controller0>Invoke-HcsDiagnostics -Scope Hardware  
Running hardware diagnostics ...
```

```
-----  
Hardware components failed or not present  
-----
```

Type	State	Controller	Index
EnclosureId	-----	-----	-----
---	-----	-----	-----
...rVipResource	NotPresent	None	1
None			
...rVipResource	NotPresent	None	2
None			
...rVipResource	NotPresent	None	3
None			
...rVipResource	NotPresent	None	4
None			
...rVipResource	NotPresent	None	5
None			
...rVipResource	NotPresent	None	6
None			
...rVipResource	NotPresent	None	7
None			
...rVipResource	NotPresent	None	8
None			
...rVipResource	NotPresent	None	9
None			
...rVipResource	NotPresent	None	10
None			
...rVipResource	NotPresent	None	11
None			

```
Firmware information
```

```
-----  
TalladegaController : ActiveBIOS:0.45.0010  
                    BackupBIOS:0.45.0006  
                    MainCPLD:17.0.000b  
                    ActiveBMCRoot:2.0.001F  
                    BackupBMCRoot:2.0.001F  
                    BMCKeepalive:2.0.0002  
                    LsiFirmware:20.00.04.00  
                    LsiBios:07.37.00.00  
                    Battery1Firmware:06.2C  
                    Battery2Firmware:06.2C  
                    DomFirmware:X231600  
                    CanisterFirmware:3.5.0.56
```

```
CanisterBootloader:5.03
CanisterConfigCRC:0x9134777A
CanisterVPDStructure:0x06
CanisterGEMCPLD:0x19
CanisterVPDCRC:0x142F7DC2
MidplaneVPDStructure:0x0C
MidplaneVPDCRC:0xA6BD4F64
MidplaneCPLD:0x10
PCM1Firmware:1.00|1.05
PCM1VPDStructure:0x05
PCM1VPDCRC:0x41BEF99C
PCM2Firmware:1.00|1.05
PCM2VPDStructure:0x05
PCM2VPDCRC:0x41BEF99C

EbodController      :
DisksFirmware       : SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
TalladegaController : ActiveBIOS:0.45.0010
                      BackupBIOS:0.45.0006
                      MainCPLD:17.0.000b
                      ActiveBMCRoot:2.0.001F
                      BackupBMCRoot:2.0.001F
                      BMCBoot:2.0.0002
                      LsiFirmware:20.00.04.00
                      LsiBios:07.37.00.00
                      Battery1Firmware:06.2C
                      Battery2Firmware:06.2C
                      DomFirmware:X231600
                      CanisterFirmware:3.5.0.56
                      CanisterBootloader:5.03
                      CanisterConfigCRC:0x9134777A
                      CanisterVPDStructure:0x06
                      CanisterGEMCPLD:0x19
                      CanisterVPDCRC:0x142F7DC2
                      MidplaneVPDStructure:0x0C
                      MidplaneVPDCRC:0xA6BD4F64
                      MidplaneCPLD:0x10
                      PCM1Firmware:1.00|1.05
                      PCM1VPDStructure:0x05
                      PCM1VPDCRC:0x41BEF99C
                      PCM2Firmware:1.00|1.05
                      PCM2VPDStructure:0x05
                      PCM2VPDCRC:0x41BEF99C
```

```
EbodController      : 
DisksFirmware      : SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      SmrtStor:TXA2D20400GA6XYR:KZ50
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
                      WD:WD4001FYYG-01SL3:VR08
```

System test

This test reports the system information, the updates available, the cluster information, and the service information for your device.

- The system information includes the model, device serial number, time zone, controller status, and the detailed software version running on the system. To understand the various system parameters reported as the output, go to [Interpreting system information](#).
- The update availability reports whether the regular and maintenance modes are available and their associated package names. If `RegularUpdates` and `MaintenanceModeUpdates` are `false`, this indicates that the updates are not available. Your device is up-to-date.
- The cluster information contains the information on various logical components of all the HCS cluster groups and their respective statuses. If you see an offline cluster group in this section of the report, [contact Microsoft Support](#).
- The service information includes the names and statuses of all the HCS and CiS services running on your device. This information is helpful for the Microsoft Support in troubleshooting the device issue.

Sample output of system test run on an 8100 device

Here is a sample output of the system test run on an 8100 device.

```
Controller0>Invoke-HcsDiagnostics -Scope System
Running system diagnostics ...

-----
System information
-----
Controller0:

InstanceId : 7382407f-a56b-4622-8f3f-756fe04cf38
Name : 8100-SHX0991003G467K
Model : 8100
SerialNumber : SHX0991003G467K
TimeZone : (UTC-08:00) Pacific Time (US & Canada)
CurrentController : Controller0
ActiveController : Controller0
Controller0Status : Normal
Controller1Status : Normal
SystemMode : Normal
FriendlySoftwareVersion : StorSimple 8000 Series Update 4.0
HcsSoftwareVersion : 6.3.9600.17820
ApiVersion : 9.0.0.0
VhdVersion : 6.3.9600.17759
OSVersion : 6.3.9600.0
CisAgentVersion : 1.0.9441.0
MdsAgentVersion : 35.2.2.0
Lsisas2Version : 2.0.78.0
Capacity : 219902325555200
RemoteManagementMode : Disabled
FipsMode : Enabled

Controller1:
InstanceId : 7382407f-a56b-4622-8f3f-756fe04cf38
Name : 8100-SHX0991003G467K
Model : 8100
SerialNumber : SHX0991003G467K
TimeZone :
CurrentController : Controller0
ActiveController : Controller0
Controller0Status : Normal
Controller1Status : Normal
SystemMode : Normal
FriendlySoftwareVersion : StorSimple 8000 Series Update 4.0
HcsSoftwareVersion : 6.3.9600.17820
ApiVersion : 9.0.0.0
VhdVersion : 6.3.9600.17759
OSVersion : 6.3.9600.0
CisAgentVersion : 1.0.9441.0
MdsAgentVersion : 35.2.2.0
Lsisas2Version : 2.0.78.0
Capacity : 219902325555200
RemoteManagementMode : HttpsAndHttpEnabled
FipsMode : Enabled
```

Update availability

```

-----
RegularUpdates : False
MaintenanceModeUpdates : False
RegularUpdatesTitle : {}
MaintenanceModeUpdatesTitle : {}

Cluster information
-----
Name           State OwnerGroup
-----
ApplicationHostRLUA   Online HCS Cluster Group
Data0v4          Online HCS Cluster Group
HCS Vnic Resource Online HCS Cluster Group
hcs_cloud_connectivity_... Online HCS Cluster Group
hcs_controller_replacement Online HCS Cluster Group
hcs_datapath_service  Online HCS Cluster Group
hcs_management_service Online HCS Cluster Group
hcs_nvram_service    Online HCS Cluster Group
hcs_passive_datapath Online HCS Passive Cluster Group
hcs_platform_service Online HCS Cluster Group
hcs_saas_agent_service Online HCS Cluster Group
HddDataClusterDisk  Online HCS Cluster Group
HddMgmtClusterDisk  Online HCS Cluster Group
HddReplClusterDisk  Online HCS Cluster Group
iSCSI Target Server Online HCS Cluster Group
NvramClusterDisk   Online HCS Cluster Group
SSAdminRLUA       Online HCS Cluster Group
SsdDataClusterDisk Online HCS Cluster Group
SsdNvramClusterDisk Online HCS Cluster Group

Service information
-----
Name           Status DisplayName
-----
CiAgentSvc     Stopped CiS Service Agent
hcs_cloud_connectivity_... Running
hcs_cloud_connectivity_... Running
hcs_controller_replacement Running HCS Controller
Replace...
hcs_datapath_service Running HCS Datapath Service
hcs_management_service Running HCS Management Service
hcs_minishell    Running hcs_minishell
HCS_NVRAM_Service Running HCS NVRAM Service
hcs_passive_datapath Stopped HCS Passive Datapath
S...
hcs_platform_service Running HCS Platform Monitor
S...
hcs_saas_agent_service Running hcs_saas_agent_service
hcs_startup      Stopped hcs_startup
-----
```

Network test

This test validates the status of the network interfaces, ports, DNS and NTP server connectivity, TLS/SSL certificate, storage account credentials, connectivity to the Update servers, and web proxy connectivity on your StorSimple device.

Sample output of network test when only DATA0 is enabled

Here is a sample output of the 8100 device. You can see in the output that:

- Only DATA 0 and DATA 1 network interfaces are enabled and configured.
- DATA 2 - 5 are not enabled in the portal.
- The DNS server configuration is valid and the device can connect via the DNS server.
- The NTP server connectivity is also fine.
- Ports 80 and 443 are open. However, port 9354 is blocked. Based on the [system network requirements](#), you need to open this port for the service bus communication.
- The TLS/SSL certification is valid.
- The device can connect to the storage account: *myss8000storageacct*.
- The connectivity to Update servers is valid.
- The web proxy is not configured on this device.

Sample output of network test when DATA0 and DATA1 are enabled

```
Controller0>Invoke-HcsDiagnostics -Scope Network
Running network diagnostics ....
-----
Validating networks ....
Name          Entity      Result      Details
----          ----      -----
Network interface Data0      Valid
Network interface Data1      Valid
Network interface Data2      Not enabled
Network interface Data3      Not enabled
Network interface Data4      Not enabled
Network interface Data5      Not enabled
DNS           10.222.118.154  Valid
NTP            time.windows.com  Valid
Port           80          Open
Port           443         Open
Port           9354        Blocked
SSL certificate https://myss8000... Valid
Storage account ... myss8000storageacct Valid
URL            http://download.... Valid
URL            http://download.... Valid
```

Web proxy not...	Not enabled	Web proxy is

Performance test

This test reports the cloud performance via the cloud read-write latencies for your device. This tool can be used to establish a baseline of the cloud performance that you can achieve with StorSimple. The tool reports the maximum performance (best case scenario for read-write latencies) that you can get for your connection.

As the tool reports the maximum achievable performance, we can use the reported read-write latencies as targets when deploying the workloads.

The test simulates the blob sizes associated with the different volume types on the device. Regular tiered and backups of locally pinned volumes use a 64 KB blob size. Tiered volumes with archive option checked use 512 KB blob data size. If your device has tiered and locally pinned volumes configured, only the test corresponding to 64 KB blob data size is run.

To use this tool, perform the following steps:

1. First, create a mix of tiered volumes and tiered volumes with archived option checked. This action ensures that the tool runs the tests for both 64 KB and 512 KB blob sizes.
2. Run the cmdlet after you have created and configured the volumes. Type:

```
Invoke-HcsDiagnostics -Scope Performance
```

3. Make a note of the read-write latencies reported by the tool. This test can take several minutes to run before it reports the results.
4. If the connection latencies are all under the expected range, then the latencies reported by the tool can be used as maximum achievable target when deploying the workloads. Factor in some overhead for internal data processing.

If the read-write latencies reported by the diagnostics tool are high:

- a. Configure Storage Analytics for blob services and analyze the output to understand the latencies for the Azure storage account. For detailed instructions, go to [enable and configure Storage Analytics](#). If those latencies are also high and comparable to the numbers you received from the StorSimple Diagnostics tool, then you need to log a service request with Azure storage.

- b. If the storage account latencies are low, contact your network administrator to investigate any latency issues in your network.

Sample output of performance test run on an 8100 device

```
Controller0>Invoke-HcsDiagnostics -Scope Performance
Running performance diagnostics...
-----
Cloud performance: writing blobs
Cloud write latency: 194 ms using credential 'myss8000storageacct', blob
size '64KB'
Cloud performance: reading blobs..
Cloud read latency: 544 ms using credential 'myss8000storageacct', blob size
'64KB'
Cloud performance: writing blobs.
Cloud write latency: 369 ms using credential 'myss8000storageacct', blob
size '512KB'
Cloud performance: reading blobs...
Cloud read latency: 4924 ms using credential 'myss8000storageacct', blob
size '512KB'
-----
Controller0>
```

Appendix: interpreting system information

Here is a table describing what the various Windows PowerShell parameters in the system information map to.

PowerShell Parameter	Description
Instance ID	Every controller has a unique identifier or a GUID associated with it.
Name	The friendly name of the device as configured through the Azure portal during device deployment. The default friendly name is the device serial number.
Model	The model of your StorSimple 8000 series device. The model can be 8100 or 8600.

PowerShell Parameter	Description
SerialNumber	The device serial number is assigned at the factory and is 15 characters long. For instance, 8600-SHX0991003G44HT indicates: 8600 – Is the device model. SHX – Is the manufacturing site. 0991003 - Is a specific product. G44HT- the last 5 digits are incremented to create unique serial numbers. This may not be a sequential set.
TimeZone	The device time zone as configured in the Azure portal during device deployment.
CurrentController	The controller that you are connected to through the Windows PowerShell interface of your StorSimple device.
ActiveController	The controller that is active on your device and is controlling all the network and disk operations. This can be Controller 0 or Controller 1.
Controller0Status	The status of Controller 0 on your device. The controller status can be normal, in recovery mode, or unreachable.
Controller1Status	The status of Controller 1 on your device. The controller status can be normal, in recovery mode, or unreachable.
SystemMode	The overall status of your StorSimple device. The device status can be normal, maintenance, or decommissioned (corresponds to deactivated in the Azure portal).
FriendlySoftwareVersion	The friendly string that corresponds to the device software version. For a system running Update 4, the friendly software version would be StorSimple 8000 Series Update 4.0.
HcsSoftwareVersion	The HCS software version running on your device. For instance, the HCS software version corresponding to StorSimple 8000 Series Update 4.0 is 6.3.9600.17820.
ApiVersion	The software version of the Windows PowerShell API of the HCS device.
VhdVersion	The software version of the factory image that the device was shipped with. If you reset your device to factory defaults, then it runs this software version.
OSVersion	The software version of the Windows Server operating system running on the device. The StorSimple device is based off the Windows Server 2012 R2 that corresponds to 6.3.9600.

PowerShell Parameter	Description
CisAgentVersion	The version for your Cis agent running on your StorSimple device. This agent helps communicate with the StorSimple Manager service running in Azure.
MdsAgentVersion	The version corresponding to the Mds agent running on your StorSimple device. This agent moves data to the Monitoring and Diagnostics Service (MDS).
Lsisas2Version	The version corresponding to the LSI drivers on your StorSimple device.
Capacity	The total capacity of the device in bytes.
RemoteManagementMode	Indicates whether the device can be remotely managed via its Windows PowerShell interface.
FipsMode	Indicates whether the United States Federal Information Processing Standard (FIPS) mode is enabled on your device. The FIPS 140 standard defines cryptographic algorithms approved for use by US Federal government computer systems for the protection of sensitive data. For devices running Update 4 or later, FIPS mode is enabled by default.

Next steps

- Learn the [syntax of the Invoke-HcsDiagnostics cmdlet](#).
- Learn more about how to [troubleshoot deployment issues](#) on your StorSimple device.

Troubleshoot an operational StorSimple device

Article • 08/22/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

ⓘ Note

The classic portal for StorSimple is deprecated. Your StorSimple Device Managers will automatically move to the new Azure portal as per the deprecation schedule. You will receive an email and a portal notification for this move. This document will also be retired soon. For any questions regarding the move, see [FAQ: Move to Azure portal](#).

Overview

This article provides helpful troubleshooting guidance for resolving configuration issues that you might encounter after your StorSimple device is deployed and operational. It describes common issues, possible causes, and recommended steps to help you resolve problems that you might experience when you run Microsoft Azure StorSimple. This information applies to both the StorSimple on-premises physical device and the StorSimple virtual device.

At the end of this article you can find a list of error codes that you might encounter during Microsoft Azure StorSimple operation, as well as steps you can take to resolve the errors.

Setup wizard process for operational devices

You use the setup wizard ([Invoke-HcsSetupWizard](#)) to check the device configuration and take corrective action if necessary.

When you run the setup wizard on a previously configured and operational device, the process flow is different. You can change only the following entries:

- IP address, subnet mask, and gateway
- Primary DNS server
- Primary NTP server
- Optional web proxy configuration

The setup wizard does not perform the operations related to password collection and device registration.

Errors that occur during subsequent runs of the setup wizard

The following table describes the errors that you might encounter when you run the setup wizard on an operational device, possible causes for the errors, and recommended actions to resolve them.

No.	Error message or condition	Possible causes	Recommended action
1	Error 350032: This device has already been deactivated.	You will see this error if you run the setup wizard on a device that is deactivated.	Contact Microsoft Support for next steps. A deactivated device cannot be put in service. A factory reset may be required before the device can be activated again.
2	Invoke-HcsSetupWizard : ERROR_INVALID_FUNCTION(Exception from HRESULT: 0x80070001)	The DNS server update is failing. DNS settings are global settings and are applied across all the enabled network interfaces.	Enable the interface and apply the DNS settings again. This may disrupt the network for other enabled interfaces because these settings are global.
3	The device appears to be online in the StorSimple Manager service portal, but when you try to complete the minimum setup and save the configuration, the operation fails.	During initial setup, the web proxy was not configured, even though there was an actual proxy server in place.	Use the Test-HcsConnection cmdlet to locate the error. Contact Microsoft Support if you are unable to correct the problem.

No.	Error message or condition	Possible causes	Recommended action
4	Invoke-HcsSetupWizard: Value does not fall within the expected range.	<p>An incorrect subnet mask produces this error. Possible causes are:</p> <ul style="list-style-type: none"> • The subnet mask is missing or empty. • The Ipv6 prefix format is incorrect. • The interface is cloud-enabled, but the gateway is missing or incorrect. <p>Note that DATA 0 is automatically cloud-enabled if configured through the setup wizard.</p>	To determine the problem, use subnet 0.0.0.0 or 256.256.256.256, and then look at the output. Enter correct values for the subnet mask, gateway, and Ipv6 prefix, as needed.

Error codes

Errors are listed in numeric order.

Error Number	Error text or description	Recommended user action
10502	An error was encountered while accessing your storage account.	Wait for a few minutes and then try again. If the error persists, please Contact Microsoft Support for next steps.
40017	The backup operation has failed as a volume specified in the backup policy was not found on the device.	Retry the backup operation, if the error persists, contact Microsoft Support for next steps.
40018	The backup operation has failed as none of the volumes specified in the backup policy were found on the device.	Retry the backup operation, if the error persists, contact Microsoft Support for next steps.
390061	The system is busy or unavailable.	Wait for a few minutes and then try again. If the error persists, please Contact Microsoft Support for next steps.

Error Number	Error text or description	Recommended user action
390143	An error has occurred with error code 390143. (Unknown error.)	If the error persists, please contact Microsoft Support for next steps.

Next steps

If you are unable to resolve the problem, [contact Microsoft Support](#) for assistance.

Replace a hardware component on your StorSimple 8000 series device

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The hardware component replacement tutorials describe the hardware components of your Microsoft Azure StorSimple 8000 series device and the steps necessary to remove and replace them. This article describes the safety icons, provides pointers to the detailed tutorials, and lists the components that are replaceable.

ⓘ Important

Before attempting to remove or replace any StorSimple component, make sure that you review the [safety icon conventions](#) and other [safety precautions](#).

Safety icon conventions

The following table describes the safety icons used in these tutorials. Pay close attention to these safety icons as you go through the steps to remove and replace device components.

Icon	Text	Additional information
	DANGER!	Indicates a hazardous situation that, if not avoided, will result in death or serious injury. This signal word is limited to the most extreme situations.
	WARNING!	Indicates a hazardous situation that, if not avoided, could result in death or serious injury.

Icon	Text	Additional information
	CAUTION!	Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.
	NOTICE:	Indicates information considered important, but not hazard-related.
	Electrical Shock Hazard	Indicates high voltage.
	Heavy Weight	
	No User Serviceable Parts	Do not access unless properly trained.
	Read All Instructions First	
	Tip Hazard	

Before you begin

Familiarize yourself with the safety information about your device and safety icons used in this tutorial. Go to [Safely install and operate your StorSimple device](#) for complete information. Be sure to review the [Safety precautions](#) before you handle your StorSimple device.

Before you attempt to replace a component, consider the following information.



- Ground yourself properly by using an electrostatic discharge or antistatic mat when handling modules and components of your StorSimple device.
- Do not touch any circuitry. Use the supplied handles and guides while handling components that may have exposed circuitry.



When you replace a module, **NEVER leave an empty bay in the rear of the enclosure.** Obtain a replacement or blank module before removing the problem part.

Hardware component replacement procedures

Your StorSimple 8000 series device consists of several plug-in modules in the primary and/or EBOD enclosures. The 8100 has a single primary enclosure, whereas the 8600 is a dual enclosure device with a primary enclosure and an EBOD enclosure.

The main hardware components in your device are summarized in the following tables. Click the link in the **Replacement procedure** column to go to the associated tutorial.

Components	# Present	Plug-in module?	Replacement procedure
Chassis	1	No	Replace the chassis on your StorSimple device
Primary controllers	2	Yes	Replace a controller module on your StorSimple device
764W Power and Cooling Modules (PCMs)	2	Yes	Replace a Power and Cooling Module on your StorSimple device
Backup battery	2	Yes	Replace the backup battery module on your StorSimple device
Disk drives	12	Yes	Replace a disk drive on your StorSimple device

Table 1 Hardware components in the primary enclosure

The primary enclosure and the EBOD enclosure differ in their I/O modules. Additionally, the PCMs have different wattage. The PCMs in the primary enclosure are 764 W, whereas those in the EBOD enclosure are 580 W. The PCMs in the primary enclosure also contain a backup battery module.

Components	# Present	Plug-in module?	Replacement procedure
Chassis	1	No	Replace the chassis on your StorSimple device
EBOD controllers	2	Yes	Replace an EBOD controller on your StorSimple device
580W Power and Cooling Modules (PCMs)	2	Yes	Replace a Power and Cooling Module on your StorSimple device
Disk drives	12	Yes	Replace a disk drive on your StorSimple device

Table 2 Hardware components in the EBOD enclosure

The plug-in modules on the device are highlighted in the following front and rear diagrams. You can use these diagrams to determine the location of the various plug-in modules if a replacement is required. The front diagram shows the disk drives, and the rear diagrams of the EBOD enclosure and the primary enclosure show the plug-in modules.

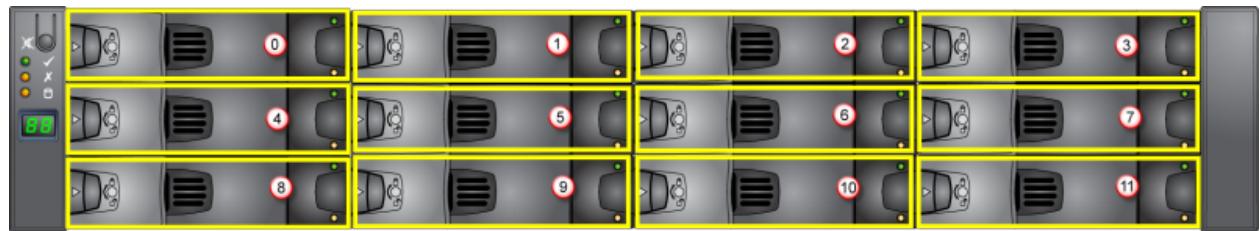


Figure 1 Front of the device

Label	Description
0 - 11	Disk drives (total of 12)

Both the primary enclosure and the EBOD enclosure have drive carrier modules. The chassis houses twelve 3.5" disk drives arranged in a 3 by 4 format.

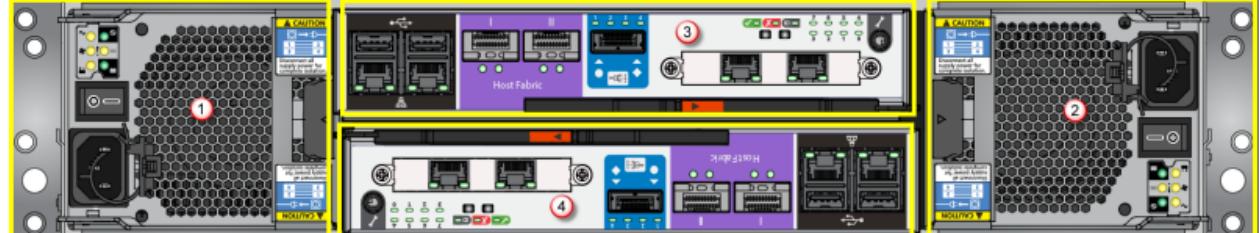


Figure 2 Back of the primary enclosure

Label	Description
1	PCM 0
2	PCM 1
3	Controller 0
4	Controller 1

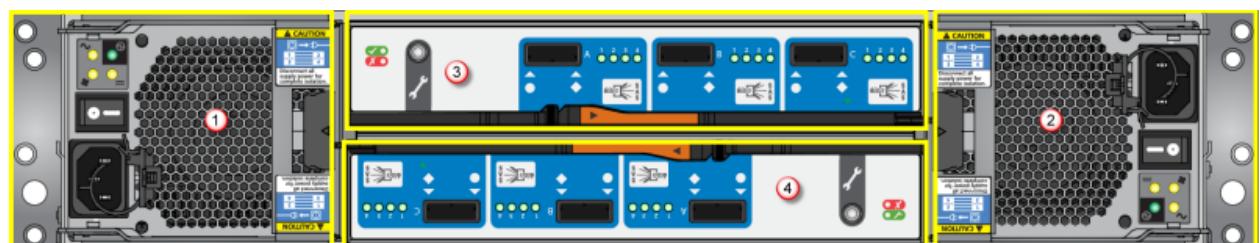


Figure 3 Back of the EBOD enclosure

Label	Description
1	PCM 0
2	PCM 1
3	EBOD Controller 0
4	EBOD Controller 1

Field replaceable units

The following field replaceable units (FRUs) are available for your StorSimple device:

- Chassis (including the integrated operations panel)
- 764 W AC PCM
- 580 W AC PCM
- Hard disk drive with drive carrier module
- Controller module
- EBOD controller module
- Backup battery module
- Rack mounting rail kit

Please [contact Microsoft Support](#) to order any of these replacement units.

Next steps

Review all [safety information](#) before you attempt to replace a StorSimple hardware component.

Replace a controller module on your StorSimple device

Article • 08/19/2022 • 11 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to remove and replace one or both controller modules in a StorSimple device. It also discusses the underlying logic for the single and dual controller replacement scenarios.

ⓘ Note

Prior to performing a controller replacement, we recommend that you always update your controller firmware to the latest version.

To prevent damage to your StorSimple device, do not eject the controller until the LEDs are showing as one of the following:

- All lights are OFF.
- LED 3,  , and  are flashing, and LED 0 and LED 7 are ON.

The following table shows the supported controller replacement scenarios.

Case	Replacement scenario	Applicable procedure
1	One controller is in a failed state, the other controller is healthy and active.	Single controller replacement , which describes the logic behind a single controller replacement , as well as the replacement steps .

Case	Replacement scenario	Applicable procedure
2	Both the controllers have failed and require replacement. The chassis, disks, and disk enclosure are healthy.	Dual controller replacement , which describes the logic behind a dual controller replacement, as well as the replacement steps.
3	Controllers from the same device or from different devices are swapped. The chassis, disks, and disk enclosures are healthy.	A slot mismatch alert message will appear.
4	One controller is missing and the other controller fails.	Dual controller replacement , which describes the logic behind a dual controller replacement, as well as the replacement steps.
5	One or both controllers have failed. You cannot access the device through the serial console or Windows PowerShell remoting.	Contact Microsoft Support for a manual controller replacement procedure.
6	<p>The controllers have a different build version, which may be due to:</p> <ul style="list-style-type: none"> • Controllers have a different software version. • Controllers have a different firmware version. 	<p>If the controller software versions are different, the replacement logic detects that and updates the software version on the replacement controller.</p> <p>If the controller firmware versions are different and the old firmware version is not automatically upgradeable, an alert message will appear in the Azure portal. You should scan for updates and install the firmware updates.</p> <p>If the controller firmware versions are different and the old firmware version is automatically upgradeable, the controller replacement logic will detect this, and after the controller starts, the firmware will be automatically updated.</p>

You need to remove a controller module if it has failed. One or both the controller modules can fail, which can result in a single controller replacement or dual controller replacement. For replacement procedures and the logic behind them, see the following:

- [Replace a single controller](#)
- [Replace both controllers](#)
- [Remove a controller](#)
- [Insert a controller](#)
- [Identify the active controller on your device](#)

Important

Before removing and replacing a controller, review the safety information in [StorSimple hardware component replacement](#).

Replace a single controller

When one of the two controllers on the Microsoft Azure StorSimple device has failed, is malfunctioning, or is missing, you need to replace a single controller.

Single controller replacement logic

In a single controller replacement, you should first remove the failed controller. (The remaining controller in the device is the active controller.) When you insert the replacement controller, the following actions occur:

1. The replacement controller immediately starts communicating with the StorSimple device.
2. A snapshot of the virtual hard disk (VHD) for the active controller is copied on the replacement controller.
3. The snapshot is modified so that when the replacement controller starts from this VHD, it will be recognized as a standby controller.
4. When the modifications are complete, the replacement controller will start as the standby controller.
5. When both the controllers are running, the cluster comes online.

Single controller replacement steps

Complete the following steps if one of the controllers in your Microsoft Azure StorSimple device fails. (The other controller must be active and running. If both controllers fail or malfunction, go to [dual controller replacement steps](#).)

Note

It can take 30 – 45 minutes for the controller to restart and completely recover from the single controller replacement procedure. The total time for the entire procedure, including attaching the cables, is approximately 2 hours.

To remove a single failed controller module

1. In the Azure portal, go to the StorSimple Device Manager service, click **Devices**, and then click the name of the device that you want to monitor.
2. Go to **Monitor > Hardware health**. The status of either Controller 0 or Controller 1 should be red, which indicates a failure.

 **Note**

The failed controller in a single controller replacement is always a standby controller.

3. Use Figure 1 and the following table to locate the failed controller module.

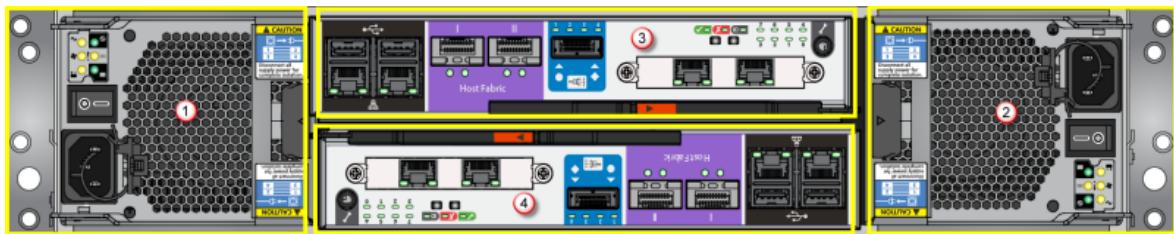


Figure 1 Back of StorSimple device

Label	Description
1	PCM 0
2	PCM 1
3	Controller 0
4	Controller 1

4. On the failed controller, remove all the connected network cables from the data ports. If you are using an 8600 model, also remove the SAS cables that connect the controller to the EBOD controller.
5. Follow the steps in [remove a controller](#) to remove the failed controller.
6. Install the factory replacement in the same slot from which the failed controller was removed. This triggers the single controller replacement logic. For more information, see [single controller replacement logic](#).
7. While the single controller replacement logic progresses in the background, reconnect the cables. Take care to connect all the cables exactly the same way that

they were connected before the replacement.

8. After the controller restarts, check the **Controller status** and the **Cluster status** in the Azure portal to verify that the controller is back to a healthy state and is in standby mode.

 **Note**

If you are monitoring the device through the serial console, you may see multiple restarts while the controller is recovering from the replacement procedure. When the serial console menu is presented, then you know that the replacement is complete. If the menu does not appear within two hours of starting the controller replacement, please [contact Microsoft Support](#).

Starting Update 4, you can also use the cmdlet `Get-HCSControllerReplacementStatus` in the Windows PowerShell interface of the device to monitor the status of the controller replacement process.

Replace both controllers

When both controllers on the Microsoft Azure StorSimple device have failed, are malfunctioning, or are missing, you need to replace both controllers.

Dual controller replacement logic

In a dual controller replacement, you first remove both failed controllers and then insert replacements. When the two replacement controllers are inserted, the following actions occur:

1. The replacement controller in slot 0 checks the following:
 - a. Is it using current versions of the firmware and software?
 - b. Is it a part of the cluster?
 - c. Is the peer controller running and is it clustered?

If none of these conditions are true, the controller looks for the latest daily backup (located in the **nonDOMstorage** on drive S). The controller copies the latest snapshot of the VHD from the backup.

2. The controller in slot 0 uses the snapshot to image itself.

3. Meanwhile, the controller in slot 1 waits for controller 0 to complete the imaging and start.
4. After controller 0 starts, controller 1 detects the cluster created by controller 0, which triggers the single controller replacement logic. For more information, see [single controller replacement logic](#).
5. Afterwards, both controllers will be running and the cluster will come online.

ⓘ Important

Following a dual controller replacement, after the StorSimple device is configured, it is essential that you take a manual backup of the device. Daily device configuration backups are not triggered until after 24 hours have elapsed. Work with [Microsoft Support](#) to make a manual backup of your device.

Dual controller replacement steps

This workflow is required when both of the controllers in your Microsoft Azure StorSimple device have failed. This could happen in a datacenter in which the cooling system stops working, and as a result, both the controllers fail within a short period of time. Depending on whether the StorSimple device is turned off or on, and whether you are using an 8600 or an 8100 model, a different set of steps is required.

ⓘ Important

It can take 45 minutes to 1 hour for the controller to restart and completely recover from a dual controller replacement procedure. The total time for the entire procedure, including attaching the cables, is approximately 2.5 hours.

To replace both controller modules

1. If the device is turned off, skip this step and proceed to the next step. If the device is turned on, turn off the device.
 - a. If you are using an 8600 model, turn off the primary enclosure first, and then turn off the EBOD enclosure.
 - b. Wait until the device has shut down completely. All the LEDs in the back of the device will be off.

2. Remove all the network cables that are connected to the data ports. If you are using an 8600 model, also remove the SAS cables that connect the primary enclosure to the EBOD enclosure.
3. Remove both controllers from the StorSimple device. For more information, see [remove a controller](#).
4. Insert the factory replacement for Controller 0 first, and then insert Controller 1. For more information, see [insert a controller](#). This triggers the dual controller replacement logic. For more information, see [dual controller replacement logic](#).
5. While the controller replacement logic progresses in the background, reconnect the cables. Take care to connect all the cables exactly the same way that they were connected before the replacement. See the detailed instructions for your model in the Cable your device section of [install your StorSimple 8100 device](#) or [install your StorSimple 8600 device](#).
6. Turn on the StorSimple device. If you are using an 8600 model:
 - a. Make sure that the EBOD enclosure is turned on first.
 - b. Wait until the EBOD enclosure is running.
 - c. Turn on the primary enclosure.
 - d. After the first controller restarts and is in a healthy state, the system will be running.

 **Note**

If you are monitoring the device through the serial console, you may see multiple restarts while the controller is recovering from the replacement procedure. When the serial console menu appears, then you know that the replacement is complete. If the menu does not appear within 2.5 hours of starting the controller replacement, please [contact Microsoft Support](#).

Remove a controller

Use the following procedure to remove a faulty controller module from your StorSimple device.

 **Note**

The following illustrations are for controller 0. For controller 1, these would be reversed.

To remove a controller module

1. Grasp the module latch between your thumb and forefinger.
2. Gently squeeze your thumb and forefinger together to release the controller latch.

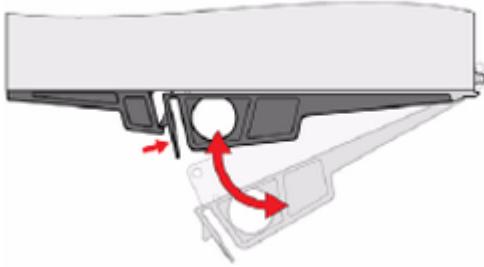


Figure 2 Releasing controller latch

3. Use the latch as a handle to slide the controller out of the chassis.

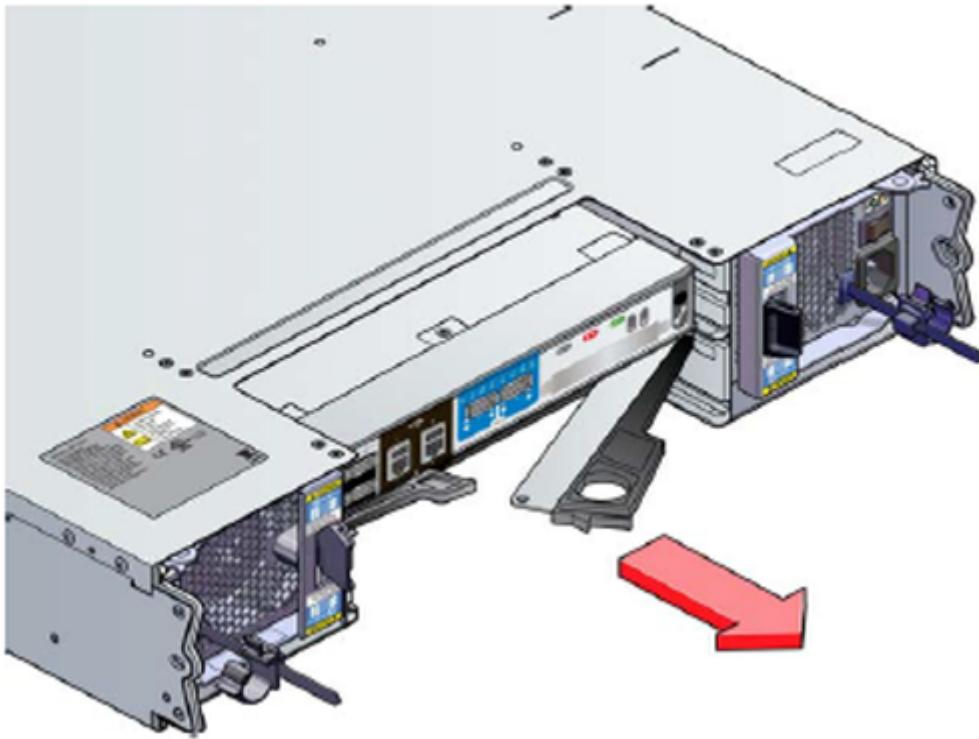


Figure 3 Sliding the controller out of the chassis

Insert a controller

Use the following procedure to install a factory-supplied controller module after you remove a faulty module from your StorSimple device.

To install a controller module

1. Check to see if there is any damage to the interface connectors. Do not install the module if any of the connector pins are damaged or bent.
2. Slide the controller module into the chassis while the latch is fully released.

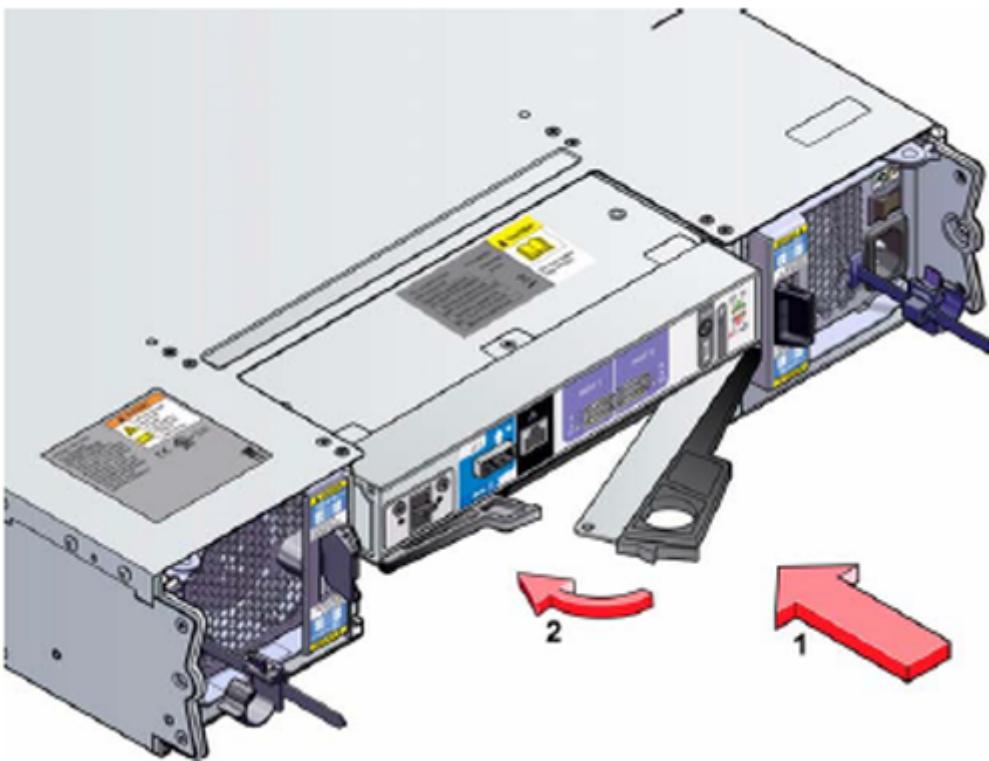


Figure 4 Sliding controller into the chassis

3. With the controller module inserted, begin closing the latch while continuing to push the controller module into the chassis. The latch will engage to guide the controller into place.

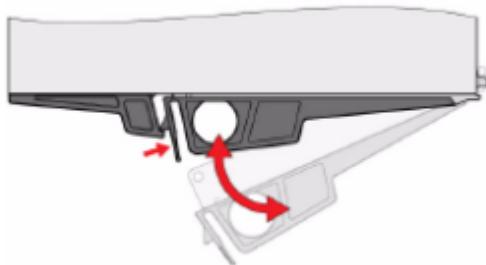


Figure 5 Closing the controller latch

4. You're done when the latch snaps into place. The **OK** LED should now be on.

! **Note**

It can take up to 5 minutes for the controller and the LED to activate.

5. To verify that the replacement is successful, in the Azure portal, go to your device and then navigate to **Monitor > Hardware health**, and make sure that both controller 0 and controller 1 are healthy (status is green).

Identify the active controller on your device

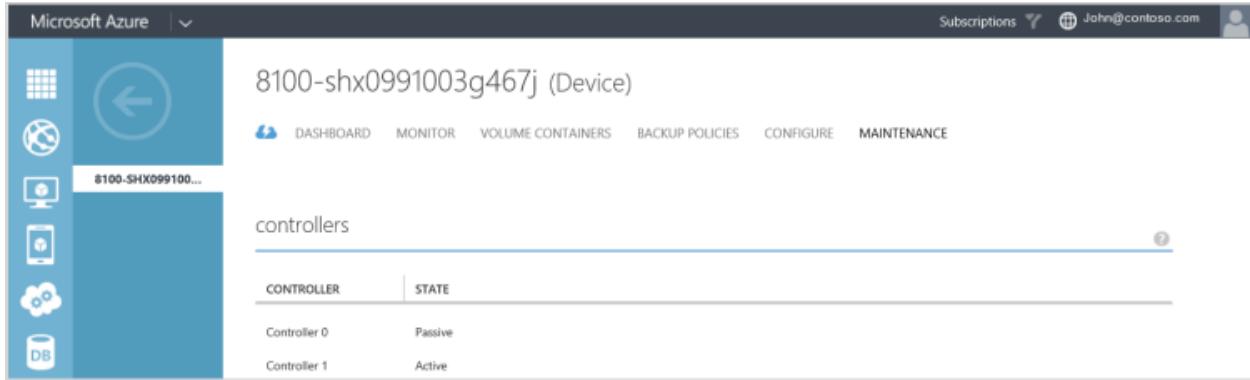
There are many situations, such as first-time device registration or controller replacement, that require you to locate the active controller on a StorSimple device. The active controller processes all the disk firmware and networking operations. You can use any of the following methods to identify the active controller:

- [Use the Azure portal to identify the active controller](#)
- [Use Windows PowerShell for StorSimple to identify the active controller](#)
- [Check the physical device to identify the active controller](#)

Each of these procedures is described next.

Use the Azure portal to identify the active controller

In the Azure portal, navigate to your device and then to **Monitor > Hardware health**, and scroll to the **Controllers** section. Here you can verify which controller is active.

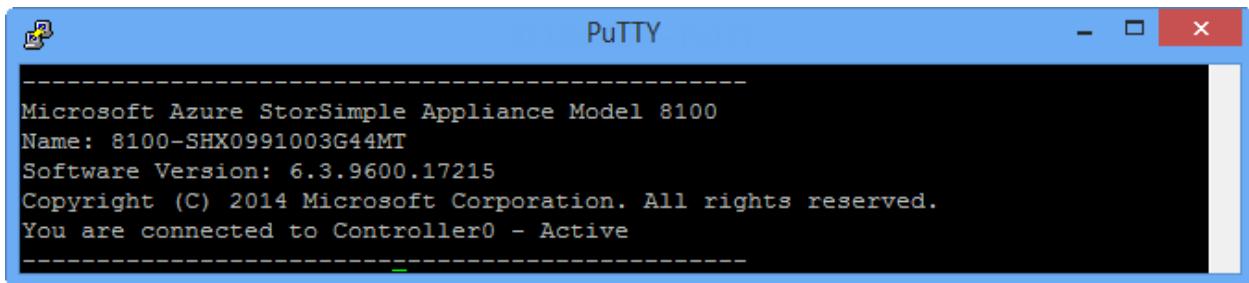


CONTROLLER	STATE
Controller 0	Passive
Controller 1	Active

Figure 6 Azure portal showing the active controller

Use Windows PowerShell for StorSimple to identify the active controller

When you access your device through the serial console, a banner message is presented. The banner message contains basic device information such as the model, name, installed software version, and status of the controller you are accessing. The following image shows an example of a banner message:



```
PuTTY
-----
Microsoft Azure StorSimple Appliance Model 8100
Name: 8100-SHX0991003G44MT
Software Version: 6.3.9600.17215
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Active
```

Figure 7 Banner message showing controller 0 as Active

You can use the banner message to determine whether the controller you are connected to is active or passive.

Check the physical device to identify the active controller

To identify the active controller on your device, locate the blue LED above the DATA 5 port on the back of the primary enclosure.

If this LED is blinking, the controller is active and the other controller is in standby mode. Use the following diagram and table as an aid.

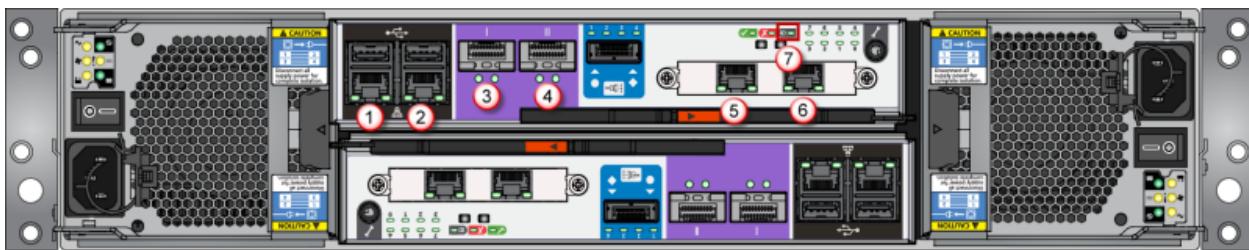


Figure 8 Back of primary enclosure with data ports and monitoring LEDs

Label	Description
1-6	DATA 0 – 5 network ports
7	Blue LED

Next steps

Learn more about [StorSimple hardware component replacement](#).

Replace an EBOD controller on your StorSimple device

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to replace a faulty EBOD controller module on your Microsoft Azure StorSimple device. To replace an EBOD controller module, you need to:

- Remove the faulty EBOD controller
- Install a new EBOD controller

Consider the following information before you begin:

- Blank EBOD modules must be inserted into all unused slots. The enclosure will not cool properly if a slot is left open.
- The EBOD controller is hot-swappable and can be removed or replaced. Do not remove a failed module until you have a replacement. When you initiate the replacement process, you must finish it within 10 minutes.

ⓘ Important

Before attempting to remove or replace any StorSimple component, make sure that you review the [safety icon conventions](#) and other [safety precautions](#).

Remove an EBOD controller

Before replacing the failed EBOD controller module in your StorSimple device, make sure that the other EBOD controller module is active and running. The following

procedure and table explain how to remove the EBOD controller module.

To remove an EBOD module

1. Open the Azure portal.
2. Go to your device and navigate to **Settings > Hardware health**, and verify that the status of the LED for the active EBOD controller module is green and the LED for the failed EBOD controller module is red.
3. Locate the failed EBOD controller module at the back of the device.
4. Remove the cables that connect the EBOD controller module to the controller before taking the EBOD module out of the system.
5. Make a note of the exact SAS port of the EBOD controller module that was connected to the controller. You will be required to restore the system to this configuration after you replace the EBOD module.

! Note

Typically, this will be Port A, which is labeled as **Host in** in the following diagram.

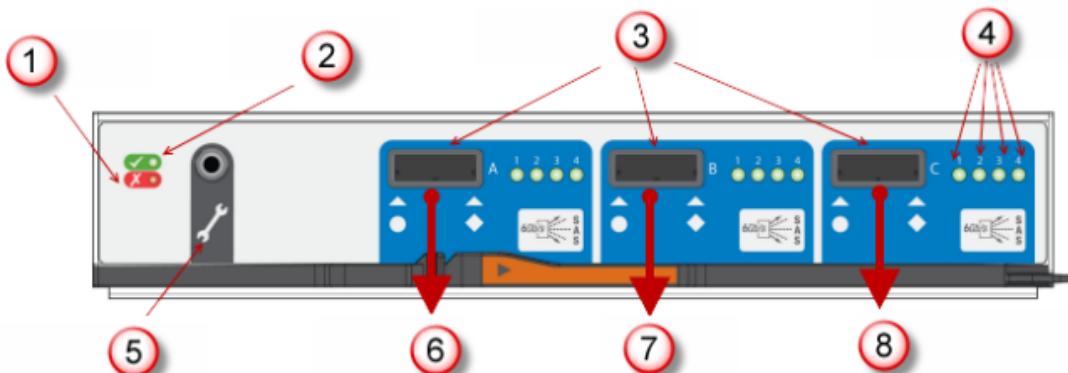


Figure 1 Back of EBOD module

Label	Description
1	Fault LED
2	Power LED
3	SAS connectors
4	SAS LEDs

Label	Description
5	Serial ports for factory use only
6	Port A (Host in)
7	Port B (Host out)
8	Port C (Factory use only)

Install a new EBOD controller

The following procedure and table explain how to install an EBOD controller module in your StorSimple device.

To install an EBOD controller

1. Check the EBOD device for damage, especially to the interface connector. Do not install the new EBOD controller if any pins are bent.
2. With the latches in the open position, slide the module into the enclosure until the latches engage.

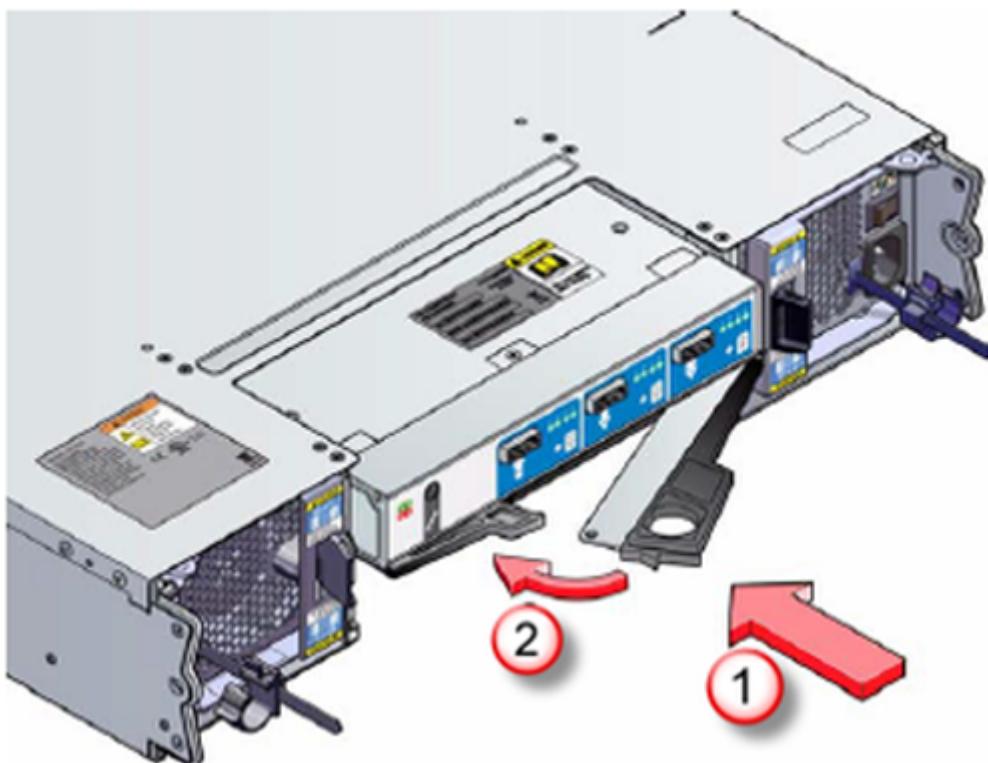


Figure 2 Installing the EBOD controller module

3. Close the latch. You should hear a click as the latch engages.

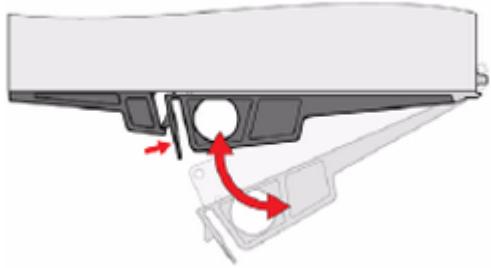


Figure 3 Closing the EBOD module latch

- Reconnect the cables. Use the exact configuration that was present before the replacement. See the following diagram and table for details about how to connect the cables.

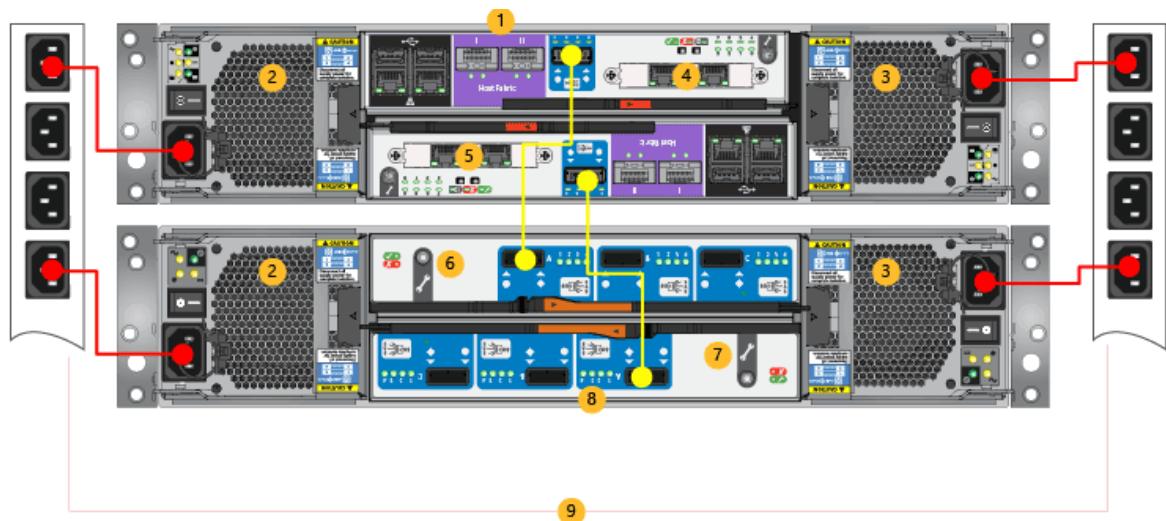


Figure 4. Reconnecting cables

Label	Description
1	Primary enclosure
2	PCM 0
3	PCM 1
4	Controller 0
5	Controller 1
6	EBOD controller 0
7	EBOD controller 1
8	EBOD enclosure
9	Power Distribution Units

Next steps

Learn more about [StorSimple hardware component replacement](#).

Replace a Power and Cooling Module on your StorSimple device

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The Power and Cooling Module (PCM) in your Microsoft Azure StorSimple device consists of a power supply and cooling fans that are controlled through the primary and EBOD enclosures. There is only one model of PCM that is certified for each enclosure. The primary enclosure is certified for a 764 W PCM and the EBOD enclosure is certified for a 580 W PCM. Although the PCMs for the primary enclosure and the EBOD enclosure are different, the replacement procedure is identical.

This tutorial explains how to:

- Remove a PCM
- Install a replacement PCM

ⓘ Important

Before removing and replacing a PCM, review the safety information in [StorSimple hardware component replacement](#).

Before you replace a PCM

Be aware of the following important issues before you replace your PCM:

- If the power supply of the PCM fails, leave the faulty module installed, but remove the power cord. The fan will continue to receive power from the enclosure and

continue to provide proper cooling. If the fan fails, the PCM needs to be replaced immediately.

- Before removing the PCM, disconnect the power from the PCM by turning off the main switch (where present) or by physically removing the power cord. This provides a warning to your system that a power shutdown is imminent.
- Make sure that the other PCM is functional for continued system operation before replacing the faulty PCM. A faulty PCM must be replaced by a fully operational PCM as soon as possible.
- PCM module replacement takes only few minutes to complete, but it must be completed within 10 minutes of removing the failed PCM to prevent overheating.
- Note that the replacement 764 W PCM modules shipped from the factory do not contain the backup battery module. You will need to remove the battery from your faulty PCM and then insert it into the replacement module prior to performing the replacement. For more information, see how to [remove and insert a backup battery module](#).

Remove a PCM

Follow these instructions when you are ready to remove a Power and Cooling Module (PCM) from your Microsoft Azure StorSimple device.

Note

Before you remove your PCM, verify that you have a correct replacement (764 W for the primary enclosure or 580 W for the EBOD enclosure).

To remove a PCM

1. In the Azure classic portal, click **Settings > Monitor > Hardware health**. Check the status of the PCM components under **Shared components** to identify which PCM has failed:
 - If a power supply in PCM 0 has failed, the status of **Power Supply in PCM 0** will be red.
 - If a power supply in PCM 1 has failed, the status of **Power Supply in PCM 1** will be red.
 - If the fan in PCM 1 has failed, the status of either **Cooling 0 for PCM 0** or **Cooling 1 for PCM 0** will be red.

2. Locate the failed PCM on the back of the primary enclosure. If you are running an 8600 model, identify the primary enclosure by looking at the System Unit Identification Number shown on the front panel LED display. The default Unit ID displayed on the primary enclosure is **00**, whereas the default Unit ID displayed on the EBOD enclosure is **01**. The following diagram and table explain the front panel of the LED display.

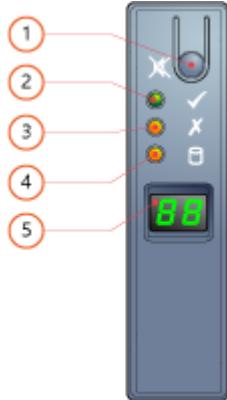


Figure 1 Front panel of the device

Label	Description
1	Mute button
2	System power
3	Module fault
4	Logical fault
5	Unit ID display

3. The monitoring indicator LEDs in the back of the primary enclosure can also be used to identify the faulty PCM. See the following diagram and table to understand how to use the LEDs to locate the faulty PCM. For example, if the LED corresponding to the **Fan Fail** is lit, the fan has failed. Likewise, if the LED corresponding to **AC Fail** is lit, the power supply has failed.

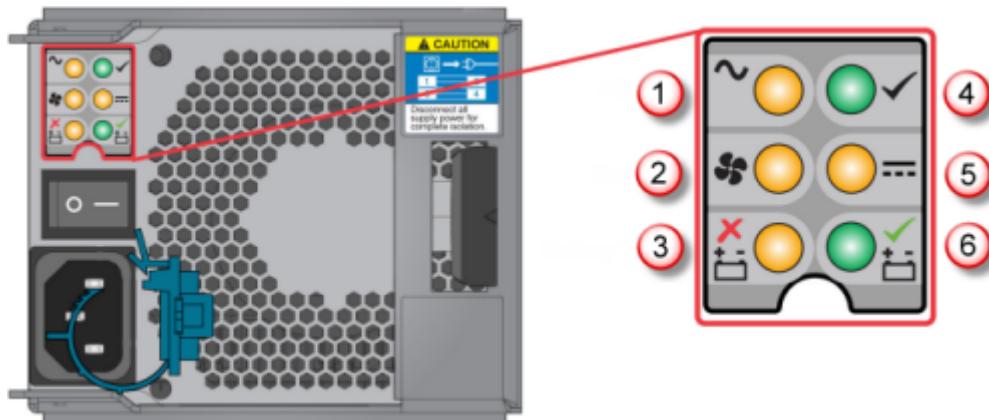


Figure 2 Back of PCM with indicator LEDs

Label	Description
1	AC power failure
2	Fan failure
3	Battery fault
4	PCM OK
5	DC power failure
6	Battery healthy

4. Refer to the following diagram of the back of the StorSimple device to locate the failed PCM module. PCM 0 is on the left and PCM 1 is on the right. The table that follows explains the modules.

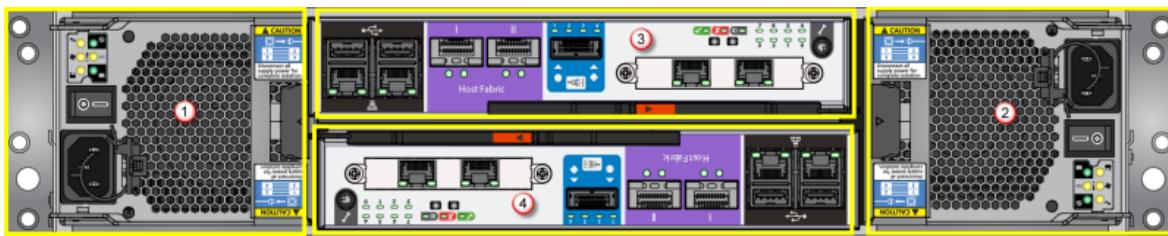


Figure 3 Back of device with plug-in modules

Label	Description
1	PCM 0
2	PCM 1
3	Controller 0
4	Controller 1

5. Turn off the faulty PCM and disconnect the power supply cord. You can now remove the PCM.
6. Grasp the latch and the side of the PCM handle between your thumb and forefinger, and squeeze them together to open the handle.

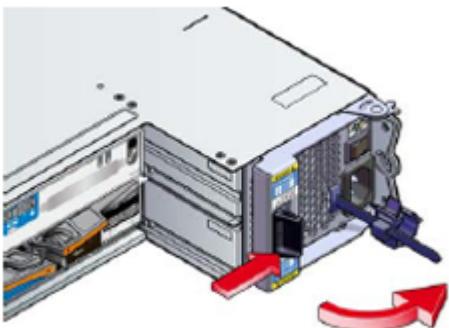


Figure 4 Opening the PCM handle

7. Grip the handle and remove the PCM.

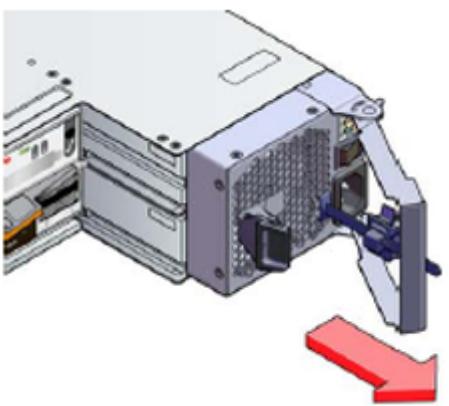


Figure 5 Removing the PCM

Install a replacement PCM

Follow these instructions to install a PCM in your StorSimple device. Ensure that you have inserted the backup battery module prior to installing the replacement PCM (applies to 764 W PCMs only). For more information, see how to [remove and insert a backup battery module](#).

To install a PCM

1. Verify that you have the correct replacement PCM for this enclosure. The primary enclosure needs a 764 W PCM and the EBOD enclosure needs a 580 W PCM. You should not attempt to use the 580 W PCM in the Primary enclosure, or the 764 W PCM in the EBOD enclosure. The following image shows where to identify this information on the label that is affixed to the PCM.



Figure 6 PCM label

- Check for damage to the enclosure, paying particular attention to the connectors.

(!) Note

Do not install the module if any connector pins are bent.

- With the PCM handle in the open position, slide the module into the enclosure.

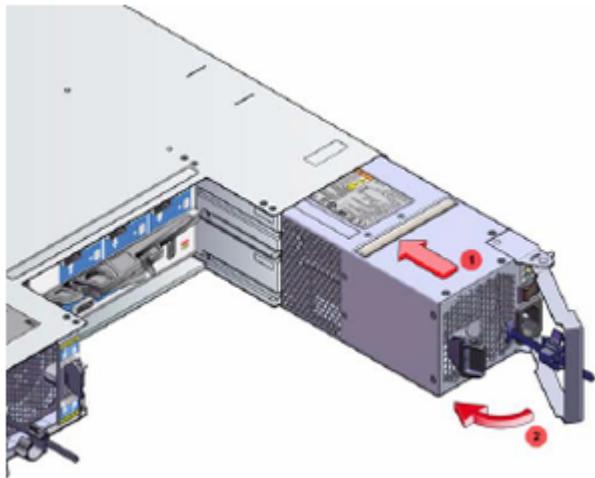


Figure 7 Installing the PCM

- Manually close the PCM handle. You should hear a click as the handle latch engages.

(!) Note

To ensure that the connector pins have engaged, you can gently tug on the handle without releasing the latch. If the PCM slides out, it implies that the latch was closed before the connectors engaged.

5. Connect the power cables to the power source and to the PCM.
6. Secure the strain relief bales.
7. Turn on the PCM.
8. Verify that the replacement was successful: in the Azure portal of your StorSimple Device Manager service, navigate to your device and then to **Settings > Monitor > Hardware health**. Under the **Shared components**, the status of the PCM should be green.

 **Note**

It may take a few minutes for the replacement PCM to completely initialize.

Next steps

Learn more about [StorSimple hardware component replacement](#).

Replace a disk drive on your StorSimple 8000 series device

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how you can remove and replace a malfunctioning or failed hard disk drive on a Microsoft Azure StorSimple device. To replace a disk drive, you need to:

- Disengage the antitamper lock
- Remove the disk drive
- Install the replacement disk drive

ⓘ Important

Before removing and replacing a disk drive, review the safety information in [StorSimple hardware component replacement](#).

Disengage the antitamper lock

This procedure explains how the antitamper locks on your StorSimple device can be engaged or disengaged when you replace the disk drives. The antitamper locks are fitted in the drive carrier handles, and they are accessed through a small aperture in the latch section of the handle. Drives are supplied with the locks set to the locked position.

To unlock the antitamper lock

1. Carefully insert the lock key (a "tamperproof" T10 screwdriver that Microsoft provided) into the aperture in the handle and into its socket.

If the antitamper lock is activated, the red indicator is visible in the aperture.

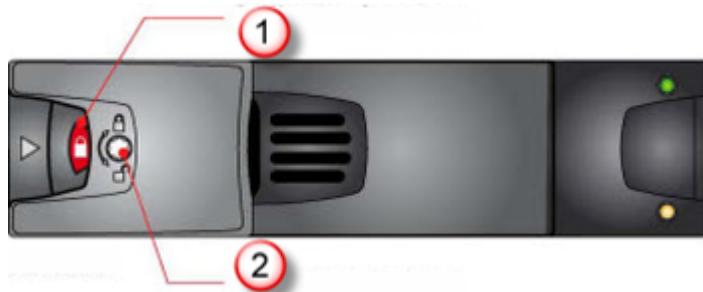


Figure 1 Anti-tamper lock engaged

Label	Description
1	Indicator aperture
2	Antitamper lock

2. Rotate the key in an anticlockwise direction until the red indicator is not visible in the aperture above the key.
3. Remove the key.



Figure 2 Unlocked disk drive

4. The disk drive can now be removed.

Follow the steps in reverse to engage the lock.

Remove the disk drive

Your StorSimple device supports a RAID 10-like storage spaces configuration. This implies that it can operate normally with one failed disk, solid-state drive (SSD), or hard disk drive (HDD).

Important

- If your system has more than one failed disk, do not remove more than one SSD or HDD from the system at any point in time. Doing so could result in loss of data.
- Make sure that you place a replacement SSD in a slot that previously contained an SSD. Similarly, place a replacement HDD in a slot that previously contained an HDD.
- In the Azure portal, slots are numbered from 0 – 11. Therefore, if the portal shows that a disk in slot 2 has failed, on the device, look for the failed disk in the third slot from the top left.

Drives can be removed and replaced while the system is operating.

To remove a drive

1. To identify the failed disk, in the Azure portal, go to your device **Settings > Hardware health**. Because a disk can fail in the primary enclosure and/or in an EBOD enclosure (if you are using a 8600 model), look at the status of the disks under **Shared components** and under **EBOD shared components**. A failed disk in either enclosure will be shown with a red status.
2. Locate the drives in the front of the primary enclosure or the EBOD enclosure.
3. If the disk is unlocked, proceed to the next step. If the disk is locked, unlock it by following the procedure in [Disengage the antitamper lock](#).
4. Press the black latch on the drive carrier module and pull the drive carrier handle out and away from the front of the chassis.

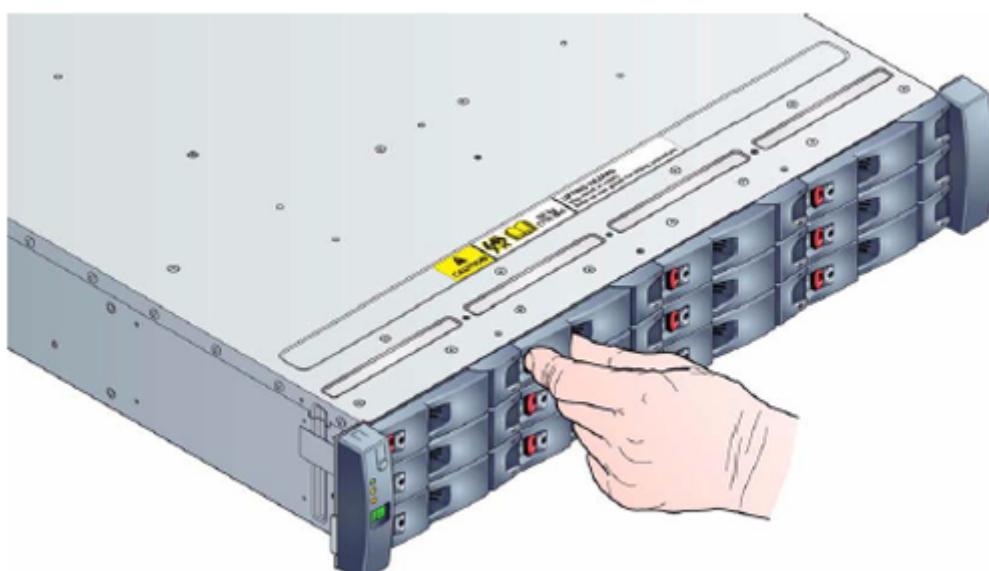


Figure 3 Releasing the drive handle

5. When the drive carrier handle is fully extended, slide the drive carrier out of the chassis.

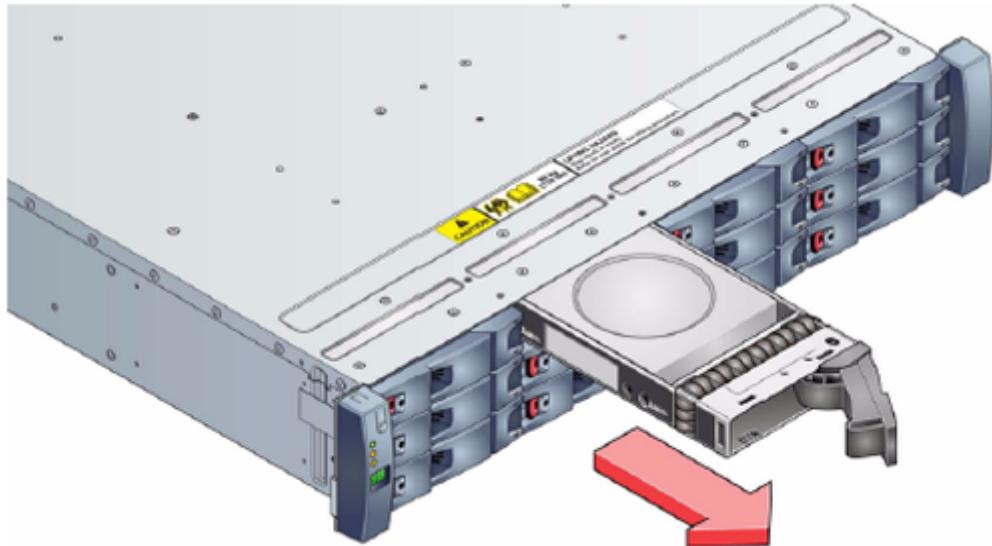


Figure 4 Sliding the disk drive out of the carrier

Install the replacement disk drive

After a drive has failed in your StorSimple device and you have removed it, follow this procedure to replace it with a new drive.

To insert a drive

1. Ensure the drive carrier handle is fully extended, as shown in the following image.



Figure 5 Drive with handle extended

2. Slide the drive carrier all the way into the chassis.

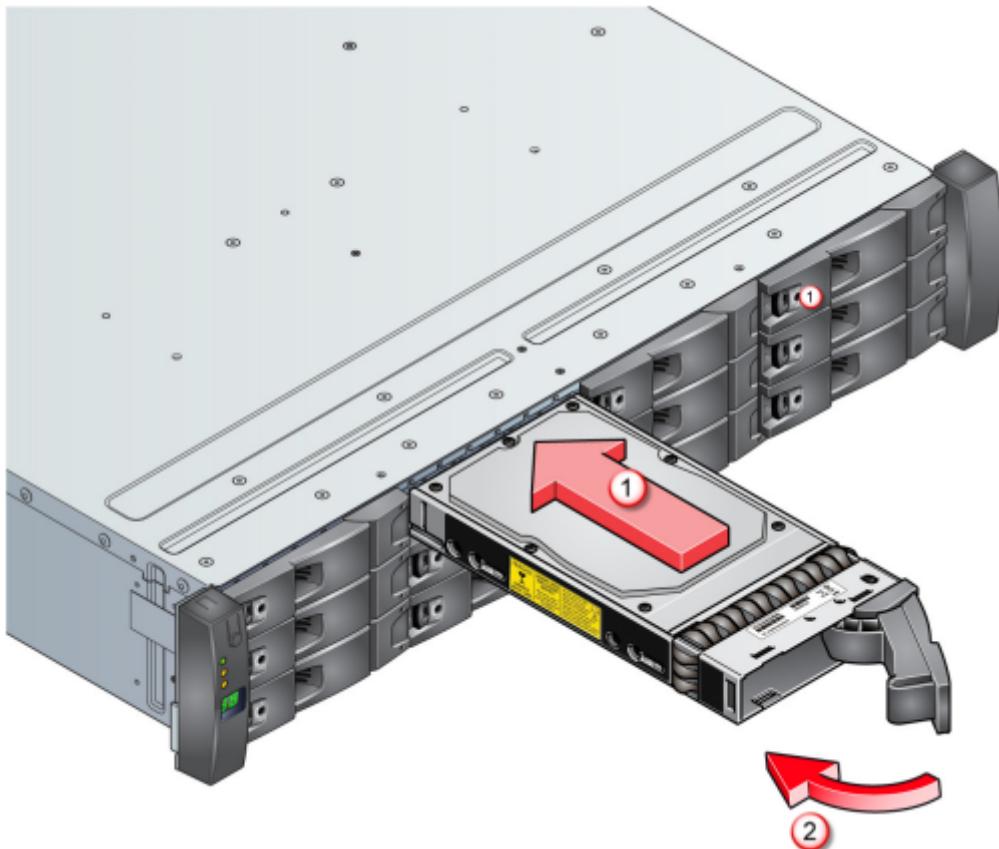


Figure 6 Sliding the drive carrier into the chassis

3. With the drive carrier inserted, close the drive carrier handle while continuing to push the drive carrier into the chassis, until the drive carrier handle snaps into a locked position.
4. Use the lock key that was provided by Microsoft (tamperproof Torx screwdriver) to secure the carrier handle into place by turning the lock screw a quarter turn clockwise.
5. Verify that the replacement was successful and the drive is operational. Access the Azure portal and navigate to **Device settings > Hardware health**. Under **Shared components** or **EBOD shared components**, the drive status should be green, indicating that it is healthy.

(!) Note

It may take several hours for the disk status to turn green after the replacement.

Next steps

Learn more about [StorSimple hardware component replacement](#).

Replace the backup battery module on your StorSimple device

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The primary enclosure Power and Cooling Module (PCM) on your Microsoft Azure StorSimple device has an additional battery pack. This pack provides power so that the StorSimple device can save data if there is loss of AC power to the primary enclosure. This battery pack is referred to as the *backup battery module*. The backup battery module exists only for the primary enclosure in your StorSimple device (the EBOD enclosure does not contain a backup battery module).

This tutorial explains how to:

- Remove the backup battery module
- Install a new backup battery module
- Maintain the backup battery module

ⓘ Important

Before removing and replacing a backup battery module, review the safety information in the [Introduction to StorSimple hardware component replacement](#).

Remove the backup battery module

The backup battery module for your StorSimple device is a field-replaceable unit. Before it is installed in the PCM, the battery module should be stored in its original packaging.

Perform the following steps to remove the backup battery.

To remove the backup battery module

1. In the Azure portal, go to your StorSimple Device Manager service blade. Go to **Devices** and then select your device from the list of devices. Navigate to **Monitor** > **Hardware health**. Under **Shared Components**, look at the status of the battery.
2. Identify the PCM in which the battery has failed. Figure 1 shows the back of the StorSimple device.

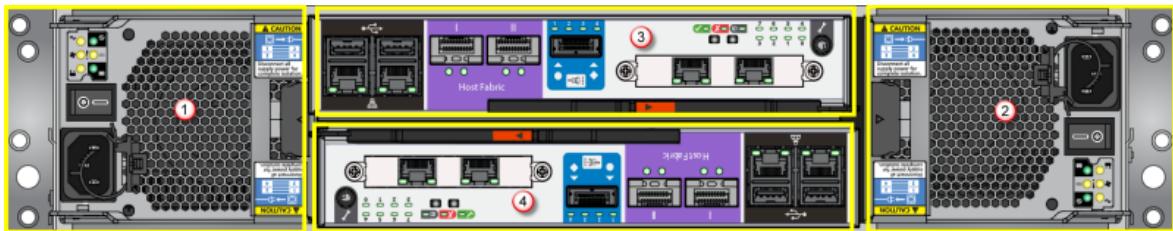


Figure 1 Back of primary device showing PCM and controller modules

Label	Description
1	PCM 0
2	PCM 1
3	Controller 0
4	Controller 1

As shown by number 3 in the Figure 2, the monitoring indicator LED on PCM 0 that corresponds to **Battery Fault** should be lit.

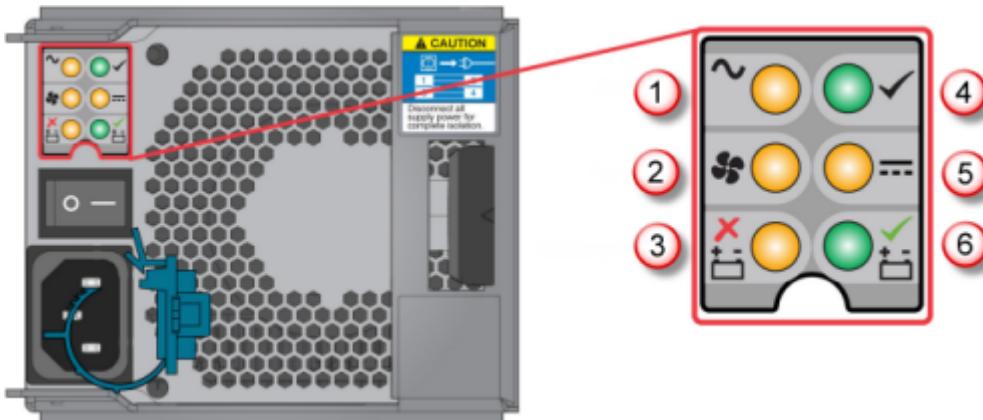


Figure 2 Back of PCM showing the monitoring indicator LEDs

Label	Description

Label	Description
1	AC power failure
2	Fan failure
3	Battery fault
4	PCM OK
5	DC power failure
6	Battery healthy

3. To remove the PCM with a failed battery, follow the steps in [Remove a PCM](#).
4. With the PCM removed, lift and rotate the battery module handle upward as indicated in the following figure, and pull it up to remove the battery.

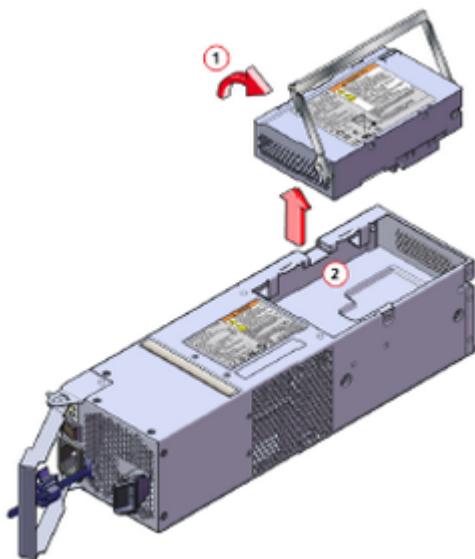


Figure 3 Removing the battery from the PCM

5. Place the module in the field-replaceable unit packaging.
6. Return the defective unit to Microsoft for proper servicing and handling.

Install a new backup battery module

Perform the following steps to install the replacement battery module in the PCM in the primary enclosure of your StorSimple device.

To install the battery module

1. Place the backup battery module in the proper orientation in the PCM.

2. Press down the battery module handle all the way to seat the connector.
3. Replace the PCM in the primary enclosure by following the guidelines in [Replace a Power and Cooling Module on your StorSimple device](#).
4. After the replacement is complete, go to your device and then go to **Monitor > Hardware health** in the Azure portal. Verify the status of the battery to make sure that the installation was successful. A green status indicates that the battery is healthy.

Maintain the backup battery module

In your StorSimple device, the backup battery module provides power to the controller during a power loss event. It allows the StorSimple device to save critical data prior to shutting down in a controlled manner. With two fully charged batteries in the PCMs, the system can handle two consecutive loss events.

In the Azure portal, the **Hardware health** under the **Monitor** blade indicates whether the battery is malfunctioning or the end-of-life is approaching. The battery status is indicated by **Battery in PCM 0** or **Battery in PCM 1** under **Shared Components**. This blade will show a **DEGRADED** state for end-of-life approaching, and **FAILED** for end-of-life reached.

Note

The battery can report **FAILED** when it simply needs to be charged.

If the **DEGRADED** state appears, we recommend the following course of action:

- The system may have experienced a recent power loss or the batteries may be undergoing periodic maintenance. Observe the system for 12 hours before proceeding.
 - If the state is still **DEGRADED** after 12 hours of continuous connection to AC power with the controllers and PCMs running, then the battery needs to be replaced. Please [contact Microsoft Support](#) for a replacement backup battery module.
 - If the state becomes **OK** after 12 hours, the battery is operational, and it only needed a maintenance charge.
- If there has not been an associated loss of AC power and the PCM is turned on and connected to AC power, the battery needs to be replaced. [Contact Microsoft Support](#) to order a replacement backup battery module.

 **Important**

Dispose of the failed battery according to national and regional regulations.

Next steps

Learn more about [StorSimple hardware component replacement](#).

Replace the chassis on your StorSimple device

Article • 08/19/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to remove and replace a chassis in a StorSimple 8000 series device. The StorSimple 8100 model is a single enclosure device (one chassis), whereas the 8600 is a dual enclosure device (two chassis). For an 8600 model, there are potentially two chassis that could fail in the device: the chassis for the primary enclosure or the chassis for the EBOD enclosure.

In either case, the replacement chassis that is shipped by Microsoft is empty. No Power and Cooling Modules (PCMs), controller modules, solid state disk drives (SSDs), hard disk drives (HDDs), or EBOD modules will be included.

ⓘ Important

Before removing and replacing the chassis, review the safety information in [StorSimple hardware component replacement](#).

Remove the chassis

Perform the following steps to remove the chassis on your StorSimple device.

To remove a chassis

1. Make sure that the StorSimple device is shut down and disconnected from all the power sources.
2. Remove all the network and SAS cables, if applicable.
3. Remove the unit from the rack.
4. Remove each of the drives and note the slots from which they are removed. For more information, see [Remove the disk drive](#).
5. On the EBOD enclosure (if this is the chassis that failed), remove the EBOD controller modules. For more information, see [Remove an EBOD controller](#).

On the primary enclosure (if this is the chassis that failed), remove the controllers and note the slots from which they are removed. For more information, see [Remove a controller](#).

Install the chassis

Perform the following steps to install the chassis on your StorSimple device.

To install a chassis

1. Mount the chassis in the rack. For more information, see [Rack-mount your StorSimple 8100 device](#) or [Rack-mount your StorSimple 8600 device](#).
2. After the chassis is mounted in the rack, install the controller modules in the same positions that they were previously installed in.
3. Install the drives in the same positions and slots that they were previously installed in.

 **Note**

We recommend that you install the SSDs in the slots first, and then install the HDDs.

4. With the device mounted in the rack and the components installed, connect your device to the appropriate power sources, and turn on the device. For details, see [Cable your StorSimple 8100 device](#) or [Cable your StorSimple 8600 device](#).

Next steps

Learn more about [StorSimple hardware component replacement](#).

Contact Microsoft Support

Article • 08/19/2022 • 4 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The StorSimple Device Manager provides the capability to [log a new support request](#) within the service summary blade. If you encounter any issues with your StorSimple solution, you can create a service request for technical support. In an online session with your support engineer, you may also need to start a support session on your StorSimple device. This article walks you through:

- How to create a support request.
- How to manage a support request lifecycle from within the portal.
- How to start a support session in the Windows PowerShell interface of your StorSimple device.

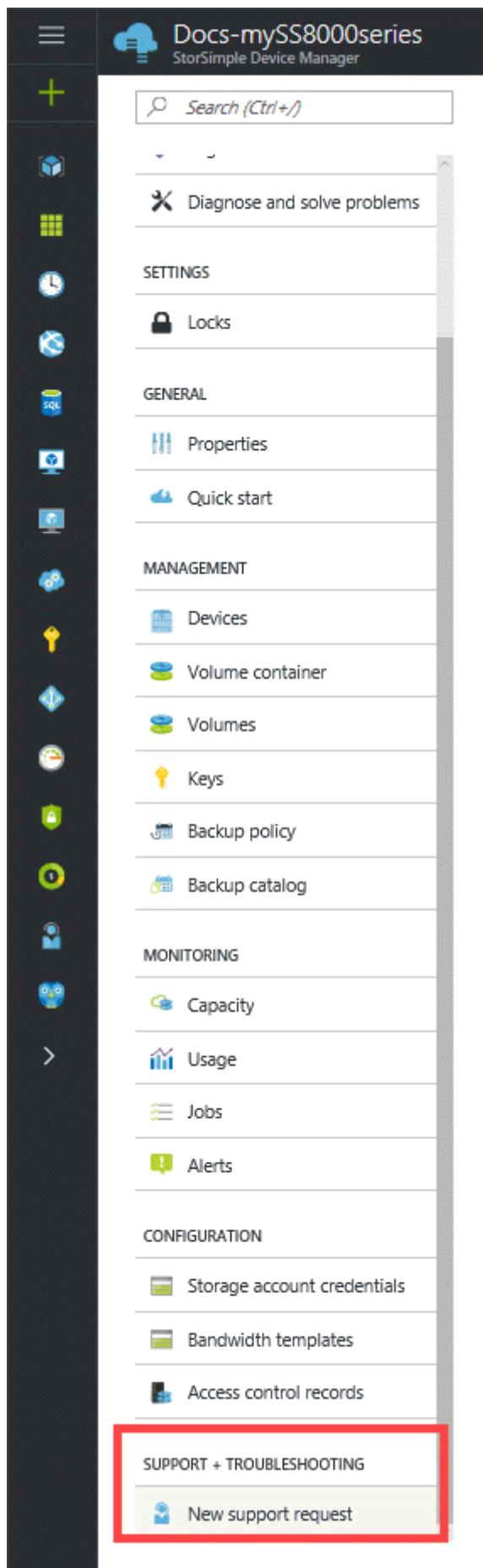
Review the [StorSimple 8000 Series Support SLAs and information](#) before you create a Support request.

Create a support request

Depending upon your [support plan](#), you can create support tickets for an issue on your StorSimple device directly from the StorSimple Device Manager service summary blade. Perform the following steps to create a support request:

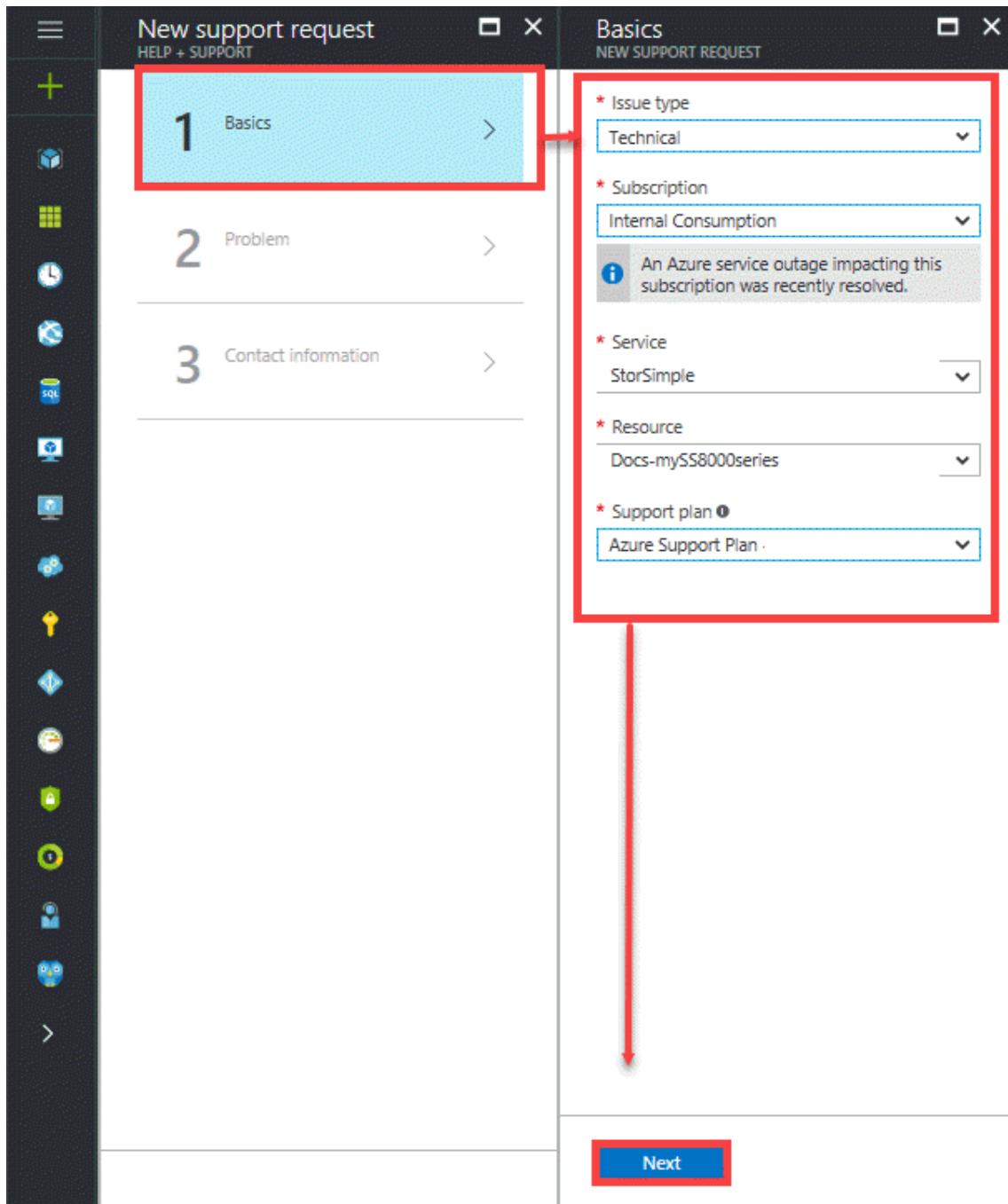
To create a support request

1. Go to your StorSimple Device Manager service. In the service summary blade settings, go to **SUPPORT + TROUBLESHOOTING** section and then click **New support request**.



2. In the **New support request** blade, select **Basics**. In the **Basics** blade, do the following steps:
 - a. From the **Issue type** drop-down list , select **Technical**.

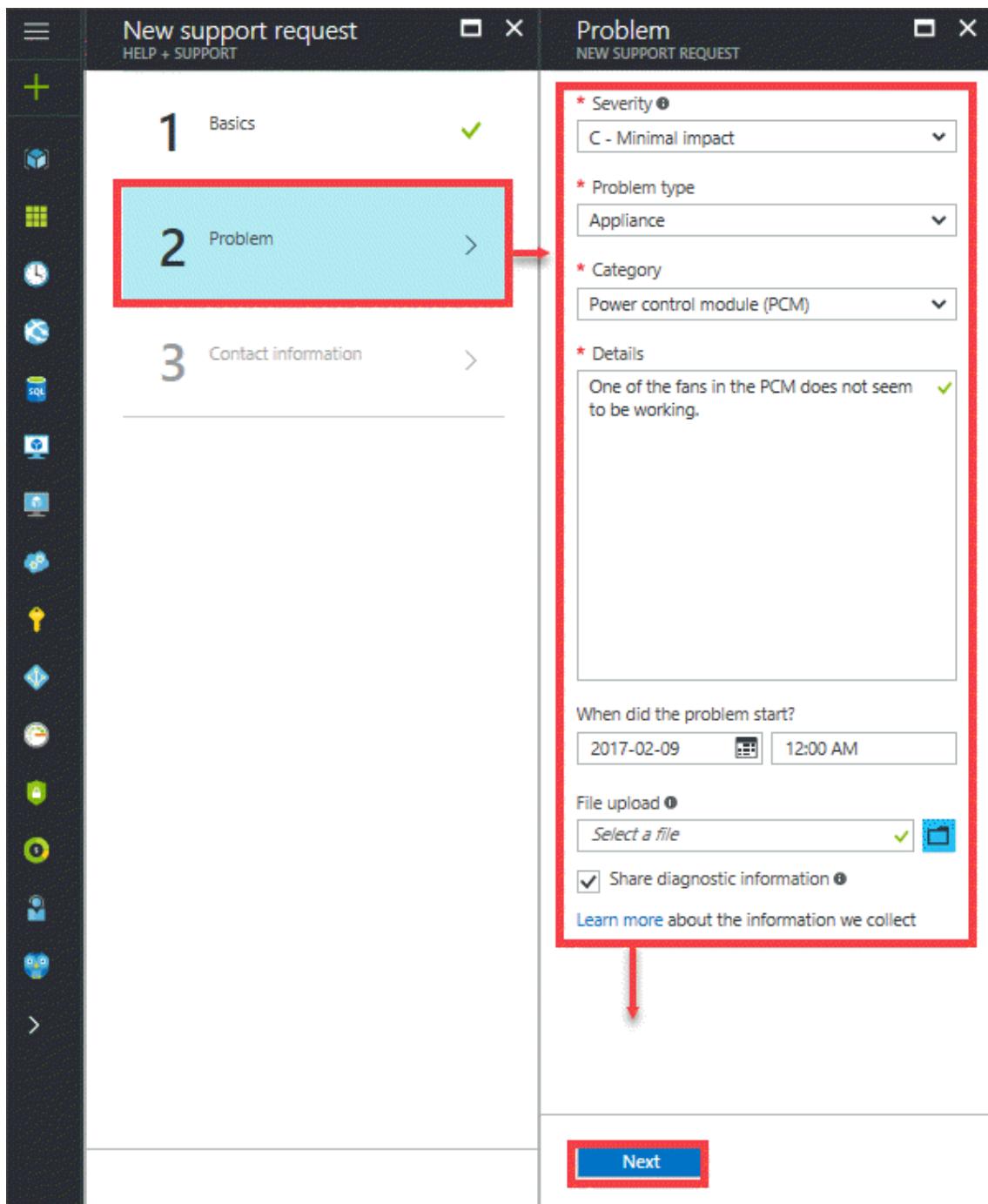
- b. The current **Subscription**, **Service type**, and the **Resource** (StorSimple Device Manager service) are automatically chosen.
- c. Select a **Support plan** from the drop-down list if you have multiple plans associated with your subscription. You need a paid support plan to enable Technical Support.
- d. Click **Next**.



- 3. In the **New support request** blade, select **Step 2 Problem**. In the **Problem** blade, do the following steps:
 - a. Choose the **Severity**.

- b. Specify if the issue is related to the appliance or the StorSimple Device Manager service.
- c. Choose a **Category** for this issue and provide more **Details** about the issue.
- d. Provide the start date and time for the problem.
- e. In the **File upload**, click the folder icon to browse to your support package.
- f. Check **Share diagnostic information**.

g. Click **Next**.

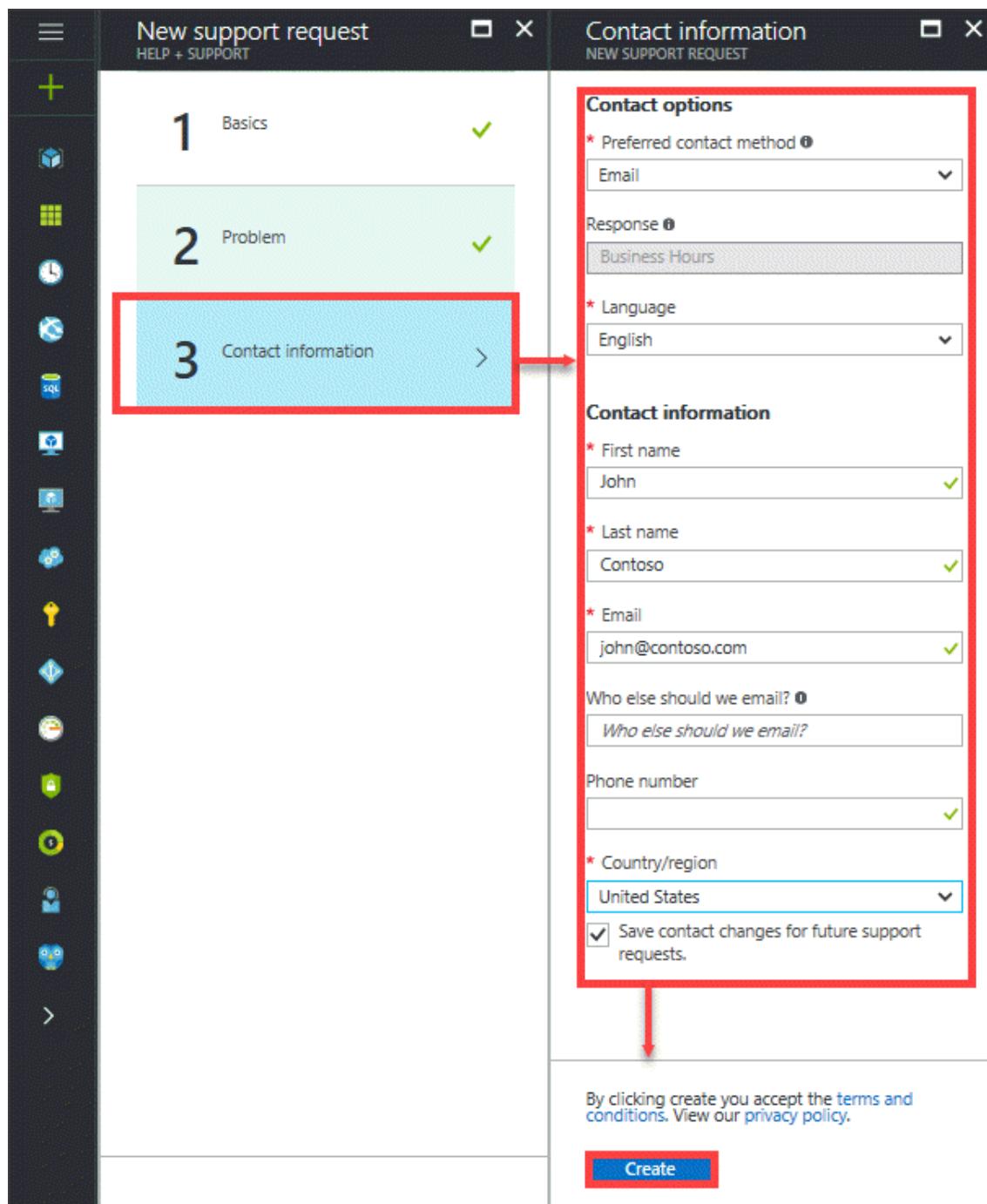


4. In the **New support request** blade, click **Step 3 Contact information**. In the **Contact information** blade, do the following steps:

- a. In the **Contact options**, provide your preferred contact method (phone or email) and the language. The response time is automatically selected based on your subscription plan.

- b. In the Contact information, provide your name, email, optional contact, country/region. Select the **Save contact changes for future support requests** check box.

- c. Click **Create**.



The screenshot shows the Microsoft Support 'New support request' interface. On the left, there's a vertical toolbar with various icons. The main window has a header 'New support request' and 'HELP + SUPPORT'. It displays a three-step process: '1 Basics' (marked with a green checkmark), '2 Problem' (marked with a green checkmark), and '3 Contact information' (highlighted with a red box). A red arrow points from the 'Contact information' box to the right panel, which is titled 'Contact information' and 'NEW SUPPORT REQUEST'. This panel contains two sections: 'Contact options' and 'Contact information'. The 'Contact options' section includes fields for 'Preferred contact method' (set to 'Email'), 'Response' (set to 'Business Hours'), and 'Language' (set to 'English'). The 'Contact information' section includes fields for 'First name' (set to 'John'), 'Last name' (set to 'Contoso'), 'Email' (set to 'john@contoso.com'), and 'Who else should we email?' (empty). It also includes fields for 'Phone number' (empty) and 'Country/region' (set to 'United States'). A checked checkbox at the bottom of this section says 'Save contact changes for future support requests.' At the bottom of the right panel, there's a note about accepting terms and conditions and a 'Create' button.

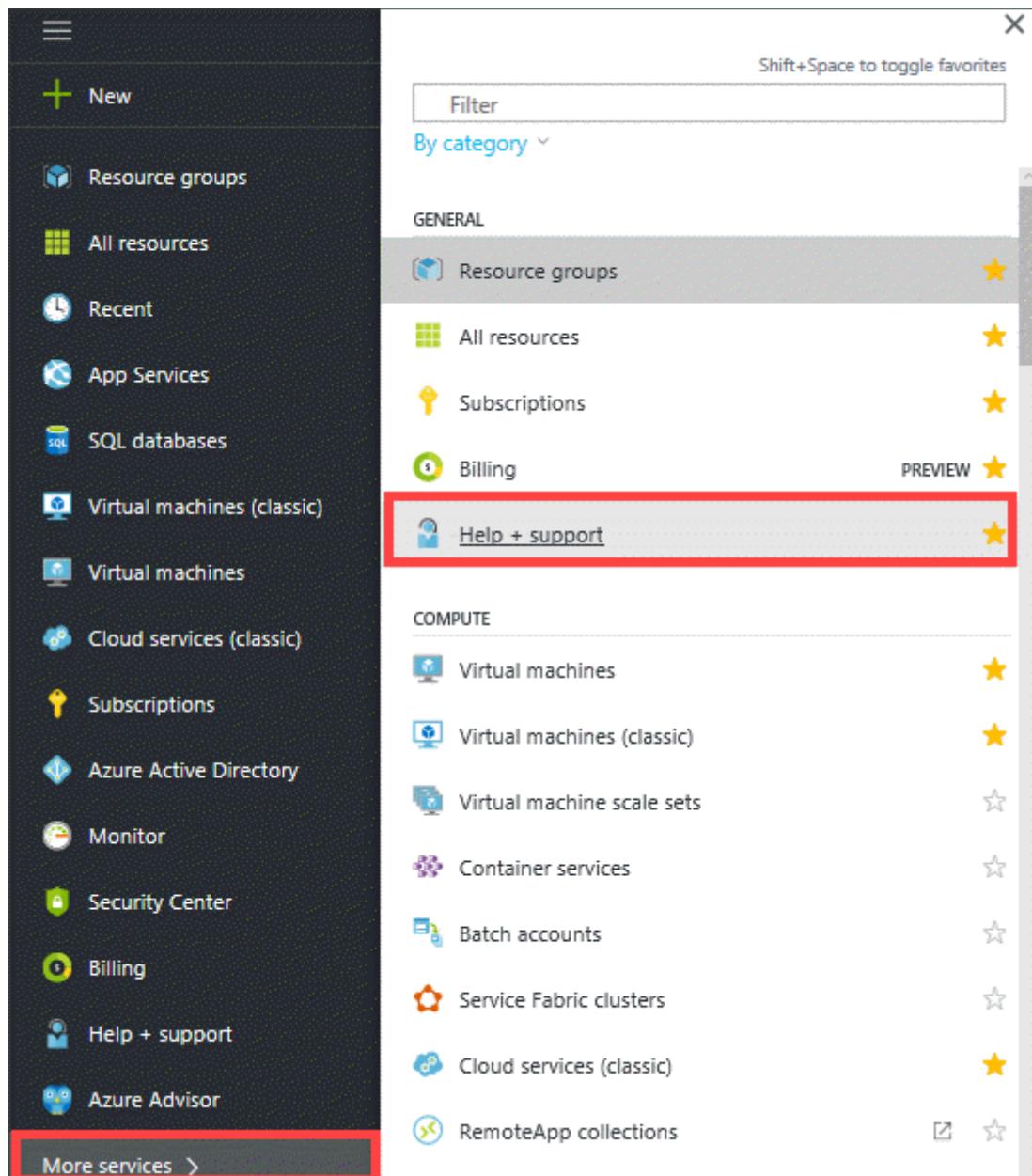
Microsoft Support will use this information to reach out to you for further information, diagnosis, and resolution. After you have submitted your request, a Support engineer will contact you as soon as possible to proceed with your request.

Manage a support request

After creating a support ticket, you can manage the lifecycle of the ticket from within the portal.

To manage your support requests

1. To get to the help and support page, navigate to **Browse > Help + support**.



2. A tabular listing of All the support requests is displayed in the **Help + support** blade.

The screenshot shows the Azure Help + support portal. On the left, there's a sidebar with various icons and links like Overview, Get started, Documentation, Billing FAQ, Support plans, and Community. The main area has sections for 'Recent support requests' and 'Community'. A specific support request for 'One of the fans in the PCM does not seem to be working.' is highlighted with a red border. The request details include ID: 117020915297847, Resource Type: StorSimple, Updated: 47 min ago, Subscription: Internal Consumption, and Status: Open.

3. Select and click a support request. You can view the status and the details for this request. Click **+ New message** if you want to follow up on this request.

This screenshot shows the details of the support request from the previous step. The 'New message' button is highlighted with a red box. In the message pane, a message is being typed: 'Hi, I am following up on my service request. I wanted to report an additional detail about the problem.' The 'Send' button is also highlighted with a red box.

Start a support session in Windows PowerShell for StorSimple

To troubleshoot any issues that you might experience with the StorSimple device, you will need to engage with the Microsoft Support team. Microsoft Support may need to use a support session to log on to your device.

Perform the following steps to start a support session:

To start a support session

1. Access the device directly by using the serial console or through a telnet session from a remote computer. To do this, follow the steps in [Use PuTTY to connect to the device serial console](#).
2. In the session that opens, press the **Enter** key to get a command prompt.
3. In the serial console menu, select option 1, **Log in with full access**.
4. At the prompt, type the following password:

```
 Password1
```

5. At the prompt, type the following command:

```
 Enable-HcsSupportAccess
```

6. An encrypted string will be presented to you. Copy this string into a text editor such as Notepad.
7. Save this string and send it in an email message to Microsoft Support.

Important

You can disable support access by running `Disable-HcsSupportAccess`. The StorSimple device will also attempt to disable support access 8 hours after the session was initiated. It is a best practice to change your StorSimple device credentials after initiating a support session.

Next steps

Learn how to [diagnose and solve problems related to your StorSimple 8000 series device](#)

Create and manage a support package for StorSimple 8000 series

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

A StorSimple support package is an easy-to-use mechanism that collects all relevant logs to assist Microsoft Support with troubleshooting any StorSimple device issues. The collected logs are encrypted and compressed.

This tutorial includes step-by-step instructions to create and manage the support package for your StorSimple 8000 series device. If you are working with a StorSimple Virtual Array, go to [generate a log package](#).

Create a support package

In some cases, you'll need to manually create the support package through Windows PowerShell for StorSimple. For example:

- If you need to remove sensitive information from your log files prior to sharing with Microsoft Support.
- If you are having difficulty uploading the package due to connectivity issues.

You can share your manually generated support package with Microsoft Support over email. Perform the following steps to create a support package in Windows PowerShell for StorSimple.

To create a support package in Windows PowerShell for StorSimple

1. To start a Windows PowerShell session as an administrator on the remote computer that's used to connect to your StorSimple device, enter the following command:

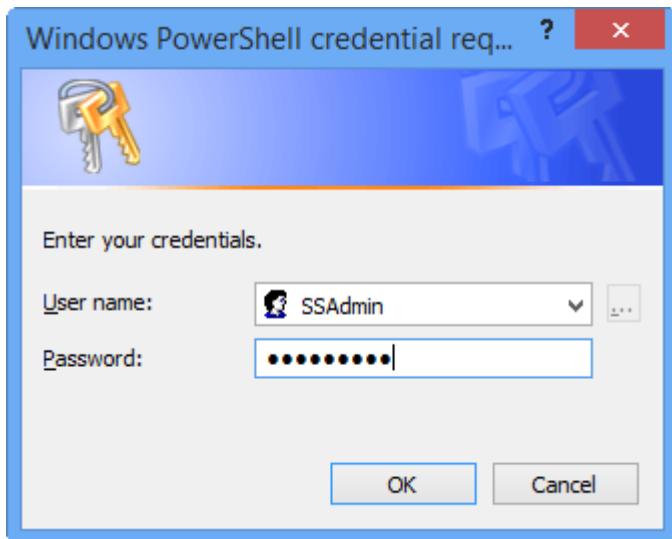
```
Start PowerShell
```

2. In the Windows PowerShell session, connect to the SSAdmin Console of your device:

- a. At the command prompt, enter:

```
$MS = New-PSSession -ComputerName <IP address for DATA 0> -Credential  
SSAdmin -ConfigurationName "SSAdminConsole"
```

- b. In the dialog box that opens, enter your device administrator password. The default password is *Password1*.



- c. Select OK.

- d. At the command prompt, enter:

```
Enter-PSSession $MS
```

3. In the session that opens, enter the appropriate command.

- For network shares that are password protected, enter:

```
Export-HcsSupportPackage -Path <\IP address\location of the shared  
folder> -Include Default -Credential domainname\username
```

You'll be prompted for a password and an encryption passphrase (because the support package is encrypted). A support package is then created in the default folder (Device name appended with current date and time).

- For shares that are not password protected, you do not need the `-Credential` parameter. Enter the following:

```
Export-HcsSupportPackage
```

The support package is created for both controllers in the default folder. The package is an encrypted, compressed file that can be sent to Microsoft Support for troubleshooting. For more information, see [Contact Microsoft Support](#).

The Export-HcsSupportPackage cmdlet parameters

You can use the following parameters with the Export-HcsSupportPackage cmdlet.

Parameter	Required/Optional	Description
<code>-Path</code>	Required	Use to provide the location of the network shared folder in which the support package is placed.
<code>-EncryptionPassphrase</code>	Required	Use to provide a passphrase to help encrypt the support package.
<code>-Credential</code>	Optional	Use to supply access credentials for the network shared folder.
<code>-Force</code>	Optional	Use to skip the encryption passphrase confirmation step.
<code>-PackageTag</code>	Optional	Use to specify a directory under <i>Path</i> in which the support package is placed. The default is [device name]-[current date and time:yyyy-MM-dd-HH-mm-ss].
<code>-Scope</code>	Optional	Specify as Cluster (default) to create a support package for both controllers. If you want to create a package only for the current controller, specify Controller .

Edit a support package

After you have generated a support package, you might need to edit the package to remove sensitive information. This can include volume names, device IP addresses, and backup names from the log files.

 **Important**

You can only edit a support package that was generated through Windows PowerShell for StorSimple. You can't edit a package created in the Azure portal with StorSimple Device Manager service.

To edit a support package before uploading it on the Microsoft Support site, first decrypt the support package, edit the files, and then re-encrypt it. Perform the following steps.

To edit a support package in Windows PowerShell for StorSimple

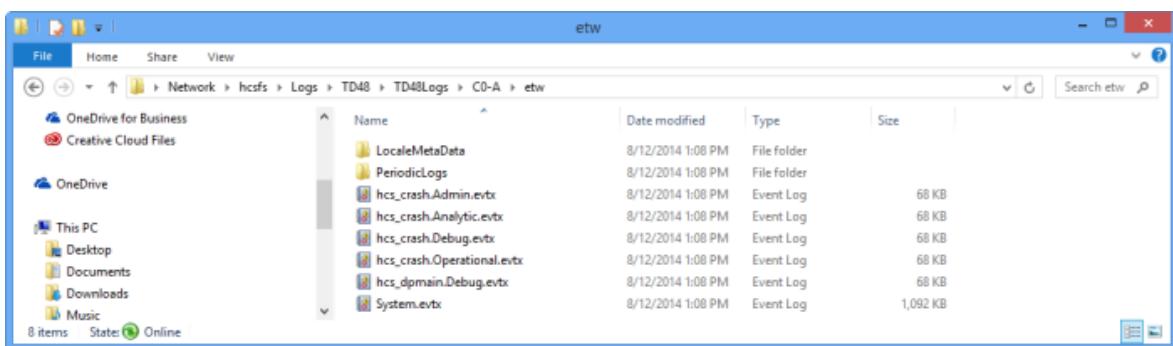
1. Generate a support package as described earlier, in [To create a support package in Windows PowerShell for StorSimple](#).
2. [Download the script](#) locally on your client.
3. Import the Windows PowerShell module. Specify the path to the local folder in which you downloaded the script. To import the module, enter:

```
Import-Module <Path to the folder that contains the Windows PowerShell  
script>
```

4. All the files are .aes files that are compressed and encrypted. To decompress and decrypt files, enter:

```
Open-HcsSupportPackage <Path to the folder that contains support package  
files>
```

Note that the actual file extensions are now displayed for all the files.



5. When you're prompted for the encryption passphrase, enter the passphrase that you used when the support package was created.

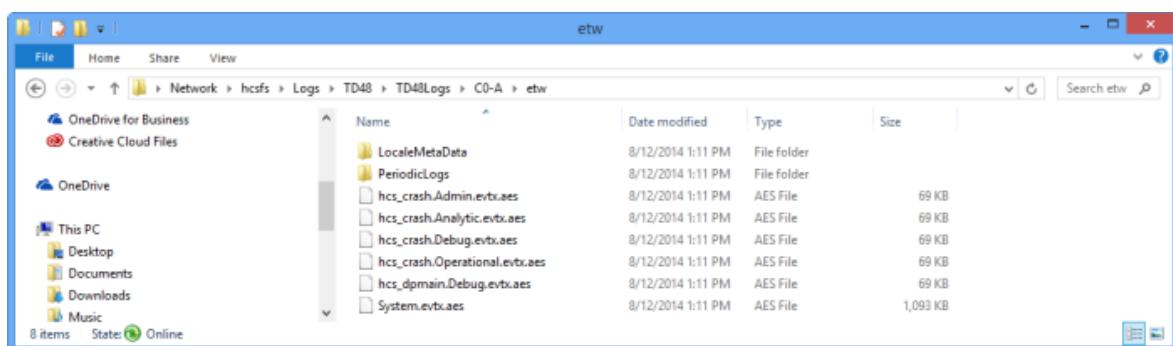
PowerShell

```
cmdlet Open-HcsSupportPackage at command pipeline position 1
```

Supply values for the following parameters:EncryptionPassphrase: ****

6. Browse to the folder that contains the log files. Because the log files are now decompressed and decrypted, these will have original file extensions. Modify these files to remove any customer-specific information, such as volume names and device IP addresses, and save the files.
7. Close the files to compress them with gzip and encrypt them with AES-256. This is for speed and security in transferring the support package over a network. To compress and encrypt files, enter the following:

```
Close-HcsSupportPackage <Path to the folder that contains support package  
files>
```



8. When prompted, provide an encryption passphrase for the modified support package.

PowerShell

```
cmdlet Close-HcsSupportPackage at command pipeline position 1  
Supply values for the following parameters:EncryptionPassphrase: ****
```

9. Write down the new passphrase, so that you can share it with Microsoft Support when requested.

Example: Editing files in a support package on a password-protected share

The following example shows how to decrypt, edit, and re-encrypt a support package.

PowerShell

```
PS C:\WINDOWS\system32> Import-Module  
C:\Users\Default\StorSimple\SupportPackage\HCSSupportPackageTools.psm1  
PS C:\WINDOWS\system32> Open-HcsSupportPackage
```

```
\hcsfs\Logs\TD48\TD48Logs\C0-A\etw

cmdlet Open-HcsSupportPackage at command pipeline position 1

Supply values for the following parameters:

EncryptionPassphrase: ****

PS C:\WINDOWS\system32> Close-HcsSupportPackage
\hcsfs\Logs\TD48\TD48Logs\C0-A\etw

cmdlet Close-HcsSupportPackage at command pipeline position 1

Supply values for the following parameters:

EncryptionPassphrase: ****

PS C:\WINDOWS\system32>
```

Next steps

- Learn about the [information collected in the Support package](#) ↗
- Learn how to [use support packages and device logs to troubleshoot your device deployment](#).
- Learn how to [use the StorSimple Device Manager service to administer your StorSimple device](#).

Migrate subscriptions and storage accounts associated with StorSimple Device Manager service

Article • 08/19/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

You may need to move your StorSimple service to a new enrollment or to a new subscription. These migration scenarios are either account changes or datacenter changes. Use the following table to understand which of these scenarios are supported including the detailed steps to move.

Account changes

Can you move ...	Supported	Downtime	Azure Support process	Approach

Can you move ...	Supported	Downtime	Azure Support process	Approach
An entire subscription (includes StorSimple service and storage accounts) to another enrollment?	Yes	No	<p>Enrollment Transfer</p> <p>Use :</p> <ul style="list-style-type: none"> • When you purchase a new Azure commitment under a new agreement. • You want to migrate all accounts and subscriptions from the old enrollment to the new. This includes all the Azure services under the old subscription. 	<p>Step 1: Open an Azure Enterprise Operation Support ticket.</p> <ul style="list-style-type: none"> • Go to https://aka.ms/AzureEntSupport. • Select Enrollment Administration and then select Transfer from one enrollment to a new enrollment. <p>Step 2: Provide the requested information</p> <p>Include:</p> <ul style="list-style-type: none"> • source enrollment number • destination enrollment number • transfer effective date
StorSimple service from an existing account to a new enrollment?	Yes	No	<p>Account Transfer</p> <p>Use:</p> <ul style="list-style-type: none"> • When you do not want a full enrollment transfer. • You only want to move specific accounts to a new enrollment. 	<p>Step 1: Open an Azure Enterprise Operation Support ticket.</p> <ul style="list-style-type: none"> • Go to https://aka.ms/AzureEntSupport. • Select Enrollment Administration and then select Transfer an EA Account to a new enrollment. <p>Step 2: Provide the requested information</p> <p>Include:</p> <ul style="list-style-type: none"> • source enrollment number • destination enrollment number • transfer effective date

Can you move ...	Supported	Downtime	Azure Support process	Approach
StorSimple service from one subscription to another subscription?	No	Yes	None, manual process	<ul style="list-style-type: none"> Migrate data off the StorSimple device. Perform a factory reset of the device, this deletes any local data on the device. Register the device with the new subscription to a StorSimple Device Manager service. Migrate the data back to the device.
Can I transfer ownership of an Azure subscription to another directory?	Yes	No	Associate an existing subscription to your Azure AD directory	Refer To associate an existing subscription to your Azure AD directory . It might take up to 10 minutes for everything to show up properly.
StorSimple device from one StorSimple Device Manager service to another service in a different region?	No	Yes	None, manual process	Same as above.
Storage account to a new subscription or resource group?	Yes	No	Move storage account to different subscription or resource group	After the move, if the storage account access keys are updated, the user will need to configure the access keys manually for the migrated storage account through the StorSimple Device Manager service.

Can you move ...	Supported	Downtime	Azure Support process	Approach
Classic storage account to an Azure Resource Manager storage account	Yes	No	Migrate from classic to Azure Resource Manager	<ul style="list-style-type: none"> For detailed instructions on how to migrate a storage account from classic to Azure Resource Manager, go to Migrate a classic storage account. If the storage account access keys are updated after migration, the user will need to synchronize the access keys for the migrated storage account through the StorSimple Device Manager service. This is to ensure the StorSimple devices continue to function normally and are able to tier primary/backup data to Azure. For detailed instructions on synchronizing access keys, go to Rotation workflow. In the case of a StorSimple Cloud Appliance, if the classic storage account is migrated but the underlying virtual machine still stays in classic, the appliance should function properly. If the underlying virtual machine for the cloud appliance is migrated, then the deactivate and delete functionality will not work. You must create a new StorSimple Cloud Appliances in the Azure portal and then fail over from the older cloud appliances. You cannot create a StorSimple Cloud Appliance in the new Azure portal using a classic storage account, they need to have an Azure Resource Manager storage account. For more information, go to Deploy and manage a StorSimple Cloud Appliance.

Datacenter changes

Can you move ...	Supported	Downtime	Azure Support process	Approach
-------------------------	------------------	-----------------	------------------------------	-----------------

Can you move ...	Supported	Downtime	Azure Support process	Approach
A StorSimple service from one Azure datacenter to another?	No	Yes	None, manual process	<ul style="list-style-type: none"> • Migrate data off the StorSimple device. • Perform a factory reset of the device, this deletes any local data on the device. • Register the device with the new subscription to a new StorSimple Device Manager service. • Migrate the data back to the device.
A storage account from one Azure datacenter to another?	No	Yes	None, manual process	Same as above.

Next steps

- [Deploy StorSimple Device Manager service](#)
- [Deploy StorSimple 8000 series device in Azure portal](#)

Options to migrate data from StorSimple 8000 series

Article • 08/19/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Migration options

There are two main migration paths, cloud-side or on-premises:

Cloud-side migrations

There are two Azure offerings you can migrate to from StorSimple: Azure Files and Azure Blob Storage. Alternatively, you can migrate your data to another cloud location of your choice. However, you must migrate your data into either Azure Files or Azure Blob Storage. Then you can migrate to a location of your choice. Azure can't assist with migrations to external services.

- **Azure file shares**

If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. Optionally, you can also make use of Azure File Sync and create an on-premises cache of your Azure file shares. Backup, cloud tiering, and multi-site sync are also highly utilized features that match or exceed previous StorSimple capabilities. To migrate to Azure Files, see [StorSimple 8100 and 8600 migration to Azure File Sync](#).

- **Azure Blob Storage**

If you don't want to preserve file and folder metadata, ACLs, or backups, and SMB access isn't important, then Azure Blob Storage may fit your needs. Specifically, the archive tier can provide long-term, cost efficient offline storage, if only the raw data needs to be preserved.

The StorSimple Data Manager can be used to move the latest StorSimple volume backup into a blob container. The Data Manager has a dedicated migration service built-in, that allows you to split your StorSimple volumes into several Azure file shares, move all required backups, and preserves file fidelity to its best ability. To use this migration path, see [StorSimple 8100 and 8600 migration to Azure File Sync](#).

If neither of the Azure offerings are suitable for your data, you can migrate your data from either Azure Files or Azure Blob Storage to a location of your choice. RoboCopy or AzCopy can be helpful to accomplish such a move out. Check with the vendor of your choice to find the best possible migration path for data located in either Azure file shares or Azure blob containers.

On-premises recall and copy

If you want to maintain an on-premises solution, it's generally better to first migrate cloud-side into a number of Azure file shares, then copy from the Azure file shares back to on-premises. Migrating cloud-side first is quicker and allows you to retain backups. This method would only require a final RoboCopy `/MIR` from the StorSimple appliance before cutting over users and apps to the new on-premises storage location.

Any file access against your StorSimple volume will cause the StorSimple appliance to either serve it from local cache or recall it from the cloud, on-demand. Theoretically, a RoboCopy run would sequentially recall all content and move it to a target storage device with SMB protocol capabilities. While this option can work, it will be slow. Furthermore, it has a chance to interrupt your business operations. The StorSimple appliances have a limited cache. Running RoboCopy will fill the cache and displace previously cached files that might be important to users or applications. Subsequent access to these files competes for space, network, and compute abilities of your StorSimple appliance and may result in a degraded experience.

Migration - Frequently asked questions

Q. What happens to the data I have stored in Azure - beyond the end-of-life date?

A. Data loss! Your data is stored in a proprietary format in Azure storage accounts. It will remain there beyond the end-of-life date, until you delete it. However, you will no longer be able to interpret the data once the StorSimple cloud service is turned off.

Q. What happens to the data I have stored locally on my StorSimple device - beyond the end-of-life date?

A. You lose all data stored locally on your StorSimple device. Your StorSimple appliance has a limited, local cache capacity. Once the StorSimple cloud service is shut down, you won't be able to access tiered files that your local appliance only holds a cloud reference for. For a limited amount of time, it is likely but not guaranteed that you still have access to the files stored in the appliances local cache. However, you should never assume that even the locally cached files remain available past the end-of-life date. Eventually, the appliance will stop working when it is no longer able to reach the cloud service. To migrate and preserve your data, see [StorSimple 8100 and 8600 migration to Azure File Sync](#).

Q. What happens if I want to keep my StorSimple 8000 series appliance - beyond the end-of-life date?

A. Depending on your contractual obligations, you may keep the appliance hardware. Microsoft won't request leased devices to be returned. The device will stop working. Microsoft won't provide hardware and software support. The StorSimple service won't work. Migration is required for business continuity before the end-of-life date. To migrate and preserve your data, see [StorSimple 8100 and 8600 migration to Azure File Sync](#).

Q. How long does it take to complete a migration?

A. The time to migrate depends on several factors. We often default to considering bandwidth as the most limiting factor in a migration - and that can be true. But the ability to enumerate a namespace can influence the total time to copy even more for larger namespaces with smaller files. Consider that copying 1 TiB of small files will take considerably longer than copying 1 TiB of fewer but larger files. Assuming that all other variables remain the same. Other factors are the structure of your StorSimple deployment. That will determine how many migration jobs you can run in parallel.

Next steps

- Migrate data from a StorSimple 8000 series with the dedicated migration service.

Options to migrate data from StorSimple 5000-7000 series

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

ⓘ Important

On July 9, 2019 the StorSimple 5000/7000 series will reach end of support (EOS) status. We recommend that StorSimple 5000/7000 series customers migrate to one of the alternatives described in the document.

StorSimple 5000-7000 series is reaching [end of Support](#) in July 2019. The customers who are running StorSimple 5000-7000 series have an option to upgrade to other Azure first party hybrid services. This article describes the Azure hybrid options available to migrate data.

Migration options

The customers using StorSimple 5000-7000 series have Azure or third-party options.

Azure options

Upgrade to StorSimple 8000 Series

Upgrade to StorSimple 8000 series and thus continue on the StorSimple platform. This upgrade path requires customers to replace their 5000-7000 series devices with an 8000 series. The data is migrated from the 5000-7000 series device by using the migration tool. Once the migration is successfully complete, the StorSimple 8000 series devices will continue to tier data to Azure Blob Storage.

For more information on how to migrate data using a StorSimple 8000 series, go to [Migrate data from StorSimple 5000-7000 series to 8000 series device](#).

Migrate to Azure File Sync

This brand new migration option enables customers to store their organization's file shares in the Azure Files. These files shares are then centralized for on-premises access using Azure File Sync (AFS). AFS can be deployed on a Windows Server host. The actual data migration is then performed as a host copy or using the migration tool.

For more information on how to migrate data to Azure File Sync, go to [Migrate data from StorSimple 5000-7000 series to Azure File Sync](#).

Migrate to Azure NetApp Files

StorSimple 5000-7000 Series customers can migrate to Azure NetApp Files (ANF) paired with NetApp Global File Cache (GFC) to continue storing critical data in Azure while maintaining content at remote sites. Customers can streamline and simplify IT storage and infrastructure by centralizing unstructured data in Microsoft Azure using Azure NetApp Files to provide fast local and geographically distributed access with NetApp Global File Cache.

For an overview of capabilities, deployment methodologies, and migration, see [Reference Architecture: Globally Distributed Enterprise File Sharing with Azure NetApp Files and NetApp Global File Cache](#), from NetApp.

Third-party options

Migrate to Panzura Freedom NAS

StorSimple 5000-7000 customers can choose to migrate to Panzura Freedom NAS to keep their data in Azure. Panzura Freedom solution provides a NAS solution that spans datacenters, offices, public and private clouds. The solution enables local, hybrid, and in-cloud data workflows for NFS, SMB, and mobile clients.

This migration is supported by Panzura and customers can get started by requesting migration support from the [Panzura website](#).

Migrate to Cohesity

Cohesity enables you to migrate data from your current StorSimple 5000–7000 to the Cohesity Data Platform on Azure. The Cohesity Data Platform is a software-defined web-scale solution that consolidates files, backups, objects, and VMs onto a single cloud-native solution. After migration to the Data Platform, you can manage, protect, and provision data and apps from cloud to core through a single pane of glass. With Cohesity, start with as few as three nodes.

Learn more on [migration to the Cohesity Data Platform ↗](#).

Migrate to Nasuni

Nasuni makes it easy for StorSimple 5000-7000 customers to migrate and keep their data in Azure. Nasuni is a leading Azure-based NAS storage solution, giving customers the performance and security they expect from on-prem solutions, with cloud economics and scale. In addition to high performance file storage, Nasuni and Azure handle backup and DR, while allowing you to share and collaborate on your data around the globe with centralized file storage management.

Nasuni has the experience to make your migration easy – get started today:
<https://www.nasuni.com/blog-migrating-off-storsimple/> ↗

Migration - Frequently asked questions

Q. When do the StorSimple 5000 and 7000 series devices reach end of service?

A. StorSimple 5000-7000 series reach [end of service ↗](#) in July 2019. The end of service implies that Microsoft will no longer be able to provide support for both hardware and software of these devices after July 2019. We strongly recommend that you start formulating a plan to migrate the data from your devices now.

Q. What happens to the data I have stored in Azure?

A. You can continue to use the data in Azure once you migrate it to a newer service.

Q. What happens to the data I have stored locally on my StorSimple device?

A. The data that is on the local device can be copied to the newer service as described in the migration documents.

Q. What happens if I want to keep my StorSimple 5000/7000 series appliance?

A. While the services might continue to work, Microsoft will no longer be able to provide hardware and software support. Migration is strongly recommended for business continuity.

Q. What options are available to migrate data from StorSimple 5000-7000 series devices?

A. Depending on their scenario, StorSimple 5000-7000 series users have the following migration options.

- **Upgrade to 8000 series:** Use this option when you want to continue on StorSimple platform.
- **Migrate to Azure File Sync:** Use this option when you want to switch to Azure native format. You can use Azure File Sync for centralized management of file shares.

You can contact Microsoft Support to discuss migration options not listed here.

Q. Is migration to other storage solutions supported?

A. Yes. Migration to other storage solutions using host copy of the data is supported.

Q. Is migration supported by Microsoft?

A. Migrating from 5000 or 7000 series is a fully supported operation. In fact, Microsoft recommends reaching out to Support before you start migration. Migration is currently an assisted operation. If you intend to migrate data from your StorSimple 5000-7000 series device, [Open a Support ticket](#).

Q. What is the pricing model for both the migration options?

A. Cost of migration varies depending on the option you choose. While migration itself is free, if you decide to upgrade to a StorSimple 8000 series, there will be the cost of the hardware device.

Similarly, when using Azure File Sync, the subscription fees for the service may apply. In each case, customers will also have to pay ongoing storage costs. Refer to the following

for an estimate:

- [StorSimple pricing ↗](#)
- [AFS pricing ↗](#)

Q. How long does it take to complete a migration?

A. The time to migrate data depends on the amount of the data and the upgrade option selected.

Q. What is the End of Support date for StorSimple 8000 series?

A. The End of Support date for StorSimple 8000 series is published [here ↗](#).

Next steps

- [Migrate data from a StorSimple 5000-7000 series to an 8000 series device.](#)
- [Migrate data from a StorSimple 5000-7000 series to Azure File Sync](#)

Migrate data from StorSimple 5000-7000 series to 8000 series device

Article • 08/19/2022 • 8 minutes to read

Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Important

- On July 31, 2019 the StorSimple 5000/7000 series will reach end of support (EOS) status. We recommend that StorSimple 5000/7000 series customers migrate to one of the alternatives described in the document.
- Migration is currently an assisted operation. If you intend to migrate data from your StorSimple 5000-7000 series device to an 8000 series device, you need to schedule migration with Microsoft Support. Microsoft Support will then enable your subscription for migration. For more information, see how to [Open a Support ticket](#).
- After you file the service request, it may take couple of weeks to execute the migration plan and actually start the migration.
- Before you contact Microsoft Support, be sure to review and complete the [Migration prerequisites](#) indicated in the article.

Overview

This article introduces the migration feature that allows the StorSimple 5000-7000 series customers to migrate their data to StorSimple 8000 series physical device or an 8010/8020 cloud appliance. This article also links to a downloadable step-by-step walkthrough of the steps required to migrate data from a 5000-7000 series legacy device to an 8000 series physical or cloud appliance.

This article is applicable for both the on-premises 8000 series device as well as the StorSimple Cloud Appliance.

Migration feature versus host-side migration

You can move your data using the migration feature or by performing a host-side migration. This section describes the specifics of each method including the pros and cons. Use this information to figure out which method you want to pursue to migrate your data.

The migration feature simulates a disaster recovery (DR) process from 7000/5000 series to 8000 series. This feature allows you to migrate the data from 5000/7000 series format to 8000 series format on Azure. The migration process is initiated using the StorSimple Migration tool. The tool starts the download and the conversion of backup metadata on the 8000 series device and then uses the latest backup to expose the volumes on the device.

Pros	Cons
The migration process preserves the history of backups that were taken on 5000/7000 series.	When users try to access the data, this migration will download the data from Azure thus incurring data download costs.
No data is migrated on the host side.	The process needs downtime between the start of the backup and latest backup being surfaced on the 8000 series (can be estimated using the migration tool).
This process preserves all the policies, bandwidth templates, encryption, and other settings on 8000 series devices.	User access will bring back only the data accessed by the users and will not rehydrate the entire dataset.
This process requires additional time to convert all the older backups in Azure which is done asynchronously without impacting production	Migration can only be done at a cloud configuration level. Individual volumes in a cloud configuration cannot be migrated separately

A host-side migration allows setting up of 8000 series independently and copying the data from 5000/7000 series device to 8000 series device. This is equivalent to migrating data from one storage device to another. A variety of tools such as Diskboss, robocopy are used to copy the data.

Pros	Cons
------	------

Pros	Cons
Migration can be approached in a phased manner on a volume-by-volume basis.	Previous backups (taken on 5000/7000 series) will not be available on the 8000 series device.
Allows for consolidation of data into one storage account on Azure.	First backup to the cloud on 8000 series will take a longer time as all the data on 8000 series needs to be backed up to Azure.
Following a successful migration, all the data is local on the appliance. There are no latencies when accessing the data.	Azure storage consumption will increase until the data is deleted from the 5000/7000 device.
	If the 7000/5000 series device has a large amount of data, during migration this data needs to be downloaded from Azure which will incur costs and latencies related to downloading data from Azure

This article focuses only on the migration feature from 5000/7000 to 8000 series device. For more information on host-side migration, go to [Migration from other storage devices](#).

Migration prerequisites

Here are the migration prerequisites for your legacy 5000 or 7000 series device and the 8000 series StorSimple device.

ⓘ Important

Review and complete the migration prerequisites before you file a service request with Microsoft Support.

For the 5000/7000 series device (source)

Before you begin migration, ensure that:

- You have your 5000 or 7000 series source device; the device can be live or down.

ⓘ Important

We recommend that you have serial access to this device throughout the migration process. Should there be any device issues, serial access can help

with troubleshooting.

- Your 5000 or 7000 series source device is running software version v2.1.1.518 or later. Earlier versions are not supported.
- To verify the version that your 5000 or 7000 series is running, look at the top-right corner of your Web UI. This should display the software version that your device is running. For migration, your 5000 or 7000 series should be running v2.1.1.518.



Welcome, admin | [Log Out](#) | [Invite a Friend to a Free Trial](#)
10.2.31.160 | MyStorSimple | v2.1.1 (build 2.1.1.518)

- If your live device is not running v2.1.1.518 or later, please upgrade your system to the required minimal version. You may need to work with Microsoft Support to help you perform the upgrade.
- If you are running v2.1.1.518, go to web UI to see if there are any notifications for registry restore failures. If registry restore had failed, run registry restore. You may need to work with Microsoft Support to help you restore your registry.
- If you have a down device that was not running v2.1.1.518, perform a failover to a replacement device that is running v2.1.1.518. For detailed instructions, refer to DR of your 5000/7000 series StorSimple device.
- Back up the data for your device by taking a cloud snapshot.
- Check for any other active backup jobs that are running on the source device. This includes the jobs on the StorSimple Data Protection Console host. Wait for the current jobs to complete.

For the 8000 series physical device (target)

Before you begin migration, ensure that:

- Your target 8000 series device is registered and running. For more information, see how to [Deploy your StorSimple device with StorSimple Manager service](#).
- Your 8000 series device has the latest StorSimple 8000 Series Update 5 installed and is running 6.3.9600.17845 or later version. If your device does not have the latest updates installed, you need to install the latest updates before you can proceed with migration. For more information, see how to [Install latest update on your 8000 series device](#).
- Your Azure subscription is enabled for migration. If your subscription is not enabled, contact Microsoft Support to enable your subscription for migration.

For the 8010/8020 cloud appliance (target)

Before you begin migration, ensure:

- Your target cloud appliance is registered and running. For more information, see how to [Deploy and manage StorSimple Cloud Appliance](#).
- Your cloud appliance is running the latest StorSimple 8000 Series Update 5 software version 6.3.9600.17845. If your cloud appliance is not running Update 5, create a new Update 5 cloud appliance before you proceed with migration. For more information, see how to [Create a 8010/8020 cloud appliance](#).

For the computer running StorSimple Migration tool

StorSimple Migration tool is a UI-based tool that enables you to migrate data from a StorSimple 5000-7000 series to an 8000 series device. To install the StorSimple Migration tool, use a computer that meets the following requirements.

The computer has Internet connectivity and:

- Is running the following operating system
 - Windows 10.
 - Windows Server 2012 R2 (or higher) to install StorSimple Migration tool.
- Has .NET 4.5.2 installed.
- Has a minimum of 5 GB of free space to install and use the tool.

Tip

If your StorSimple device is connected to a Windows Server host, you can install the migration tool on the Windows Server host computer.

To install StorSimple Migration tool

Perform the following steps to install StorSimple Migration tool on your computer.

1. Copy the folder *StorSimple8000SeriesMigrationTool* to your Windows computer.
Make sure that the drive where the software is copied has sufficient space.

Open the tool config file *StorSimple8000SeriesMigrationTool.exe.config* in the folder.
Here is the snippet of the file.

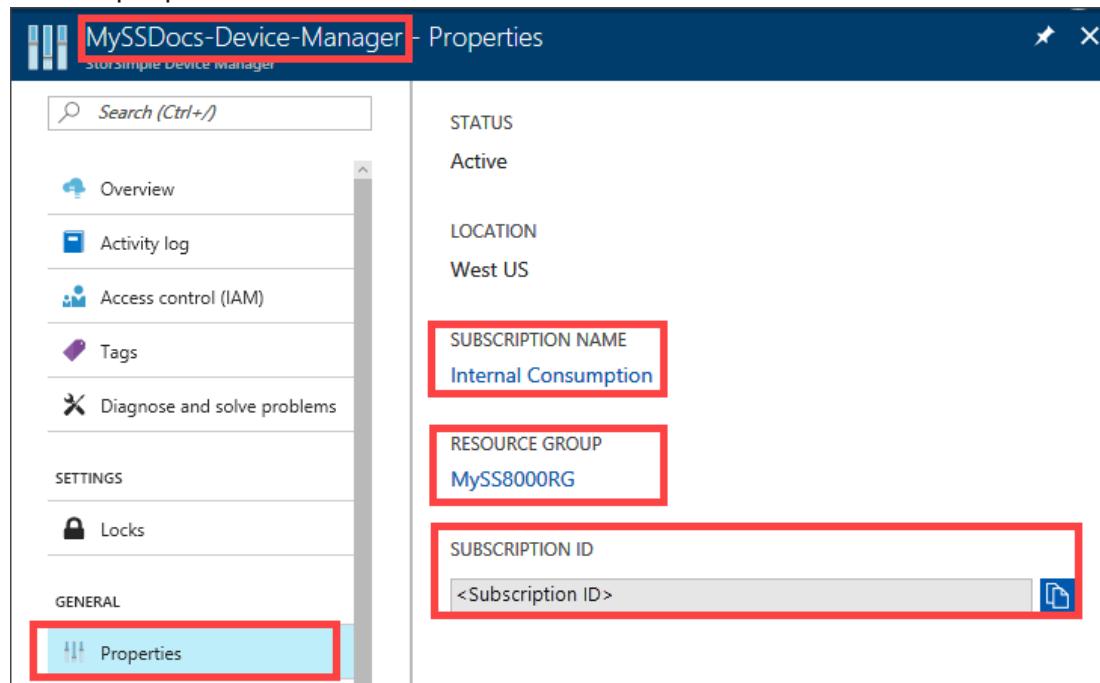
XML

```
<add key="UserName" value="username@xyz.com" />
<add key="SubscriptionName" value="YourSubscriptionName" />
<add key="SubscriptionId" value="YourSubscriptionId" />
```

```
<add key="TenantId" value="YourTenantId" />
<add key="ResourceName" value="YourResourceName" />
<add key="ResourceGroupName" value="YourResourceGroupName" />
```

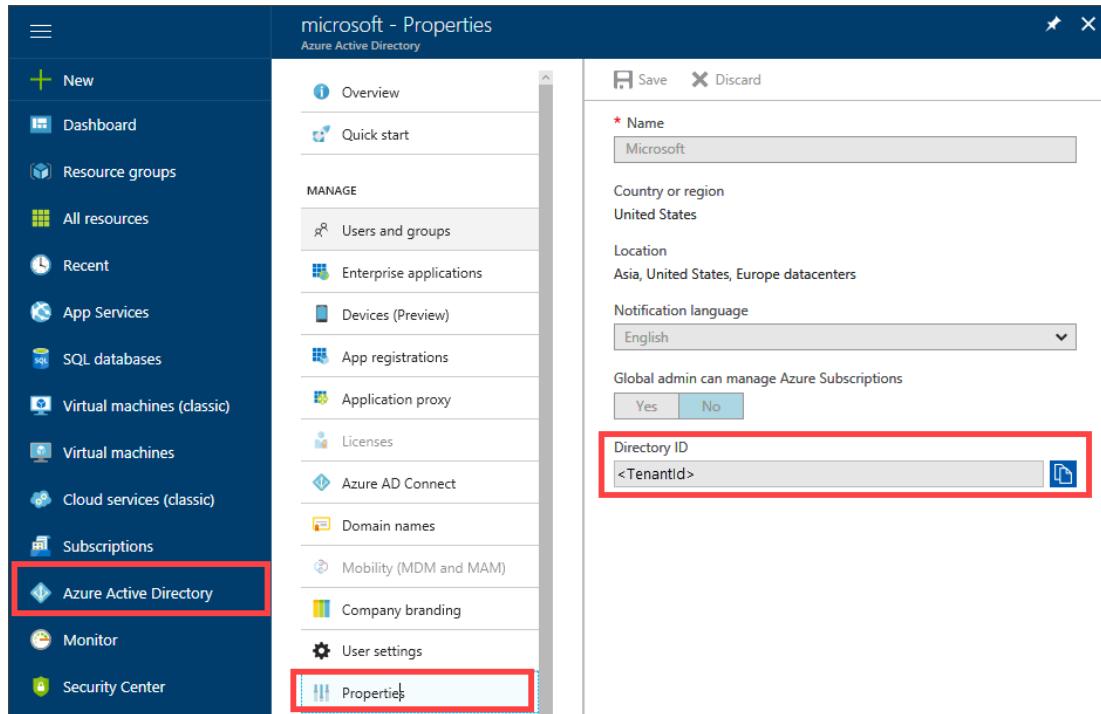
2. Edit the values corresponding to the keys and replace with:

- `UserName` – User name to log in to Azure portal.
- `SubscriptionName` and `SubscriptionId` – Name and ID for your Azure subscription. In your StorSimple Device Manager service landing page, under **General**, click **Properties**. Copy the Subscription name and Subscription ID associated with your service.
- `ResourceName` – Name of your StorSimple Device Manager service in the Azure portal. Also shown under service properties.
- `ResourceGroup` – Name of the resource group associated with your StorSimple Device Manager service in the Azure portal. Also shown under service properties.



- `TenantId` – Azure Active Directory Tenant ID in Azure portal. Log in to Microsoft Azure as an administrator. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in

the Directory ID box.



3. Save the changes made to the config file.
4. Run the *StorSimple8000SeriesMigrationTool.exe* to launch the tool. When prompted for credentials, provide the credentials associated with your subscription in Azure portal.
5. The StorSimple Migration tool UI is displayed.

Next steps

Download the step-by-step instructions on how to [Migrate data from a StorSimple 5000-7000 series to an 8000 series device](#).

Install Update 5.1 on your StorSimple device

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to install Update 5.1 on a StorSimple device running an earlier software version via the Azure portal or the hotfix method.

Update 5.1 includes non-disruptive security updates that can be applied through the Azure portal or by the hotfix method.

If you apply Update 5.1 from the Azure portal, manual and automatic pre-checks are done to determine the device health in terms of hardware state and network connectivity. These pre-checks occur only when you apply the updates from the Azure portal.

If you'd rather use the hotfix method, we strongly recommend that you install Update 5 first using the instructions in [Install Update 5 on your StorSimple device](#). Then follow the steps in [Install Update 5.1 as a hotfix](#), below, to install Update 5.1.

The security updates in Update 5.1 take about 30 minutes to install.

ⓘ Important

- Update 5.1 is a mandatory update and should be installed immediately. For more information, see [Update 5.1 release notes](#).
- Update 5 is a minimally supported version.

Note

- We recommend that you install the software and other regular updates via the Azure portal.
- If you plan to install using the hotfix method, you must contact **Microsoft Support** before you begin the installation.

Preparing for updates

You will need to perform the following steps before you scan and apply the update:

1. Take a cloud snapshot of the device data.
2. Ensure that your controller fixed IPs are routable and can connect to the Internet.
These fixed IPs will be used to service updates to your device. You can test this by running the following cmdlet on each controller from the Windows PowerShell interface of the device:

```
Test-Connection -Source <Fixed IP of your device controller> -Destination <Any IP or computer name outside of datacenter network>
```

Sample output for Test-Connection when fixed IPs can connect to the Internet

```
Output

Controller0>Test-Connection -Source 10.126.173.91 -Destination bing.com

Source      Destination      IPV4Address      IPV6Address
-----
HCSNODE0    bing.com        204.79.197.200
HCSNODE0    bing.com        204.79.197.200
HCSNODE0    bing.com        204.79.197.200
HCSNODE0    bing.com        204.79.197.200

Controller0>Test-Connection -Source 10.126.173.91 -Destination
204.79.197.200

Source      Destination      IPV4Address      IPV6Address
-----
HCSNODE0    204.79.197.200  204.79.197.200
HCSNODE0    204.79.197.200  204.79.197.200
HCSNODE0    204.79.197.200  204.79.197.200
HCSNODE0    204.79.197.200  204.79.197.200
```

After you have successfully completed these manual pre-checks, you can proceed to scan and install the updates.

Install Update 5.1 through the Azure portal

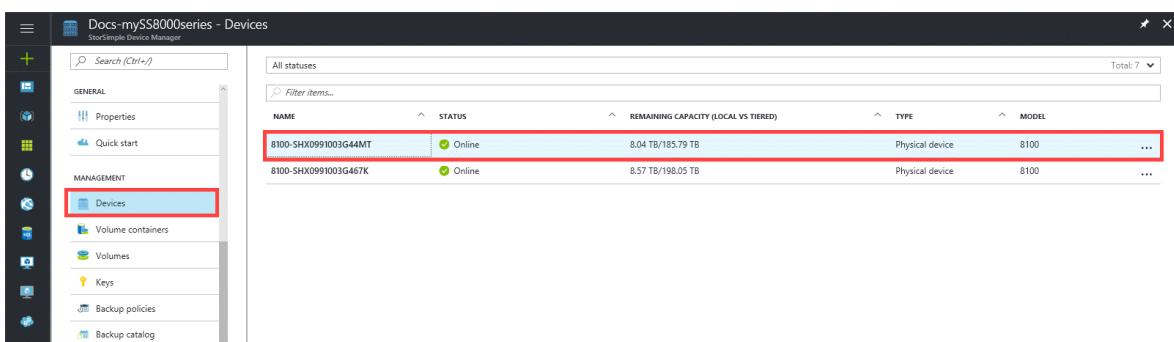
Perform the following steps to update your device to [Update 5.1](#).

Note

Microsoft pulls additional diagnostic information from the device. As a result, when our operations team identifies devices that are having problems, we are better equipped to collect information from the device and diagnose issues.

To install an update from the Azure portal

1. On the StorSimple service page, select your device.



The screenshot shows the 'Devices' section of the StorSimple Device Manager. The left sidebar has a 'Devices' icon highlighted with a red box. The main area displays a table with two rows of device information:

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.04 TB/185.79 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100

2. Navigate to **Device settings > Device updates**.

The screenshot shows the Microsoft StorSimple 8000 Series Management Portal. On the left, a vertical toolbar contains icons for various management functions like Settings, Add volume container, Add volume, Fail over, and More. The main pane displays device details: Status (Online), Model (8100), Target IQN (iqn.1991-05.com.microsoft:storsimple8100...), and Device software version (StorSimple 8000 Series Update 5). Below this is a Monitoring section with three cards: Alerts - Past 7 days (1 Warning, 1 OK), Status and health (Hardware OK, Device status Online), and Volumes (3 Online). A chart titled "8100-SHX0991003G44MT - Usage - Past 24 hours" shows storage usage over time, with three segments: PRIMARY TIERED STORAGE (0 GB), PRIMARY LOCALLY PINNED (0 GB), and CLOUD STORAGE USED (0 GB). At the bottom, capacity information is shown: Capacity (PROVISIONED 3.42 TB) and REMAINING (105 TB). The right pane is titled "Settings" and lists various configuration options under sections like GENERAL, MANAGE, MONITOR, and DEVICE SETTINGS. The "Device updates" option is highlighted with a red box.

3. A notification appears if new updates are available. Alternatively, in the **Device updates** blade, click **Scan Updates**. A job is created to scan for available updates. You are notified when the job completes successfully.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and contains a navigation menu with sections: GENERAL, MANAGE, MONITOR, and DEVICE SETTINGS. Under DEVICE SETTINGS, the 'Device updates' link is highlighted with a red box. The right window is titled 'Device updates' and shows a summary of the device's software version (StorSimple 8000 Series Update 5.0) and last update date (Tue Mar 03 2020). It also features a message box indicating new regular updates are available, with a red box around the 'Install updates' button.

Device updates

8100-SHX0991003G44MT

Scan Install updates

New regular updates are available.
Click 'Install updates'.

Installed software version
StorSimple 8000 Series Update 5.0
(6.3 9600.17845)

Last updated on
Tue Mar 03 2020

Filter settings

GENERAL

Properties >

MANAGE

Volumes >

Volume containers >

Backup policies >

Backup catalog >

MONITOR

Capacity >

Usage >

Performance >

Hardware health >

Jobs >

Alerts >

DEVICE SETTINGS

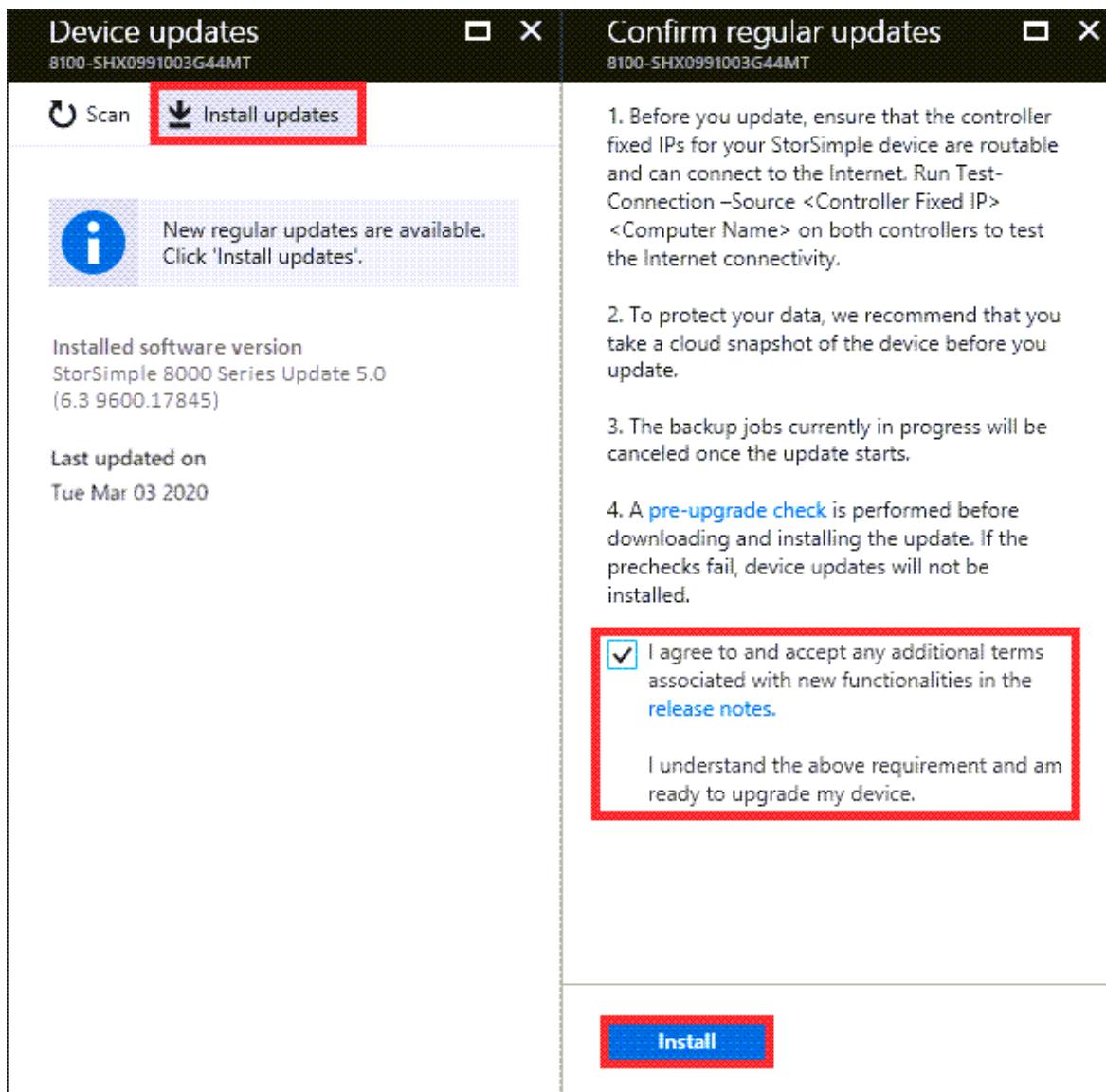
General >

Network >

Security >

Device updates >

4. We recommend that you review the release notes before you apply an update on your device. To apply updates, click **Install updates**. In the **Confirm regular updates** blade, review the prerequisites to complete before you apply updates. Select the checkbox to indicate that you are ready to update the device and then click **Install**.



5. A set of prerequisite checks starts. These checks include:

- **Controller health checks** to verify that both the device controllers are healthy and online.
- **Hardware component health checks** to verify that all the hardware components on your StorSimple device are healthy.
- **DATA 0 checks** to verify that DATA 0 is enabled on your device. If this interface is not enabled, you must enable it and then retry.

The update is downloaded and installed only if all the checks are successfully completed. You are notified when the checks are in progress. If the prechecks fail, then you will be provided with the reasons for failure. Address those issues and then retry the operation. You may need to contact Microsoft Support if you cannot address these issues by yourself.

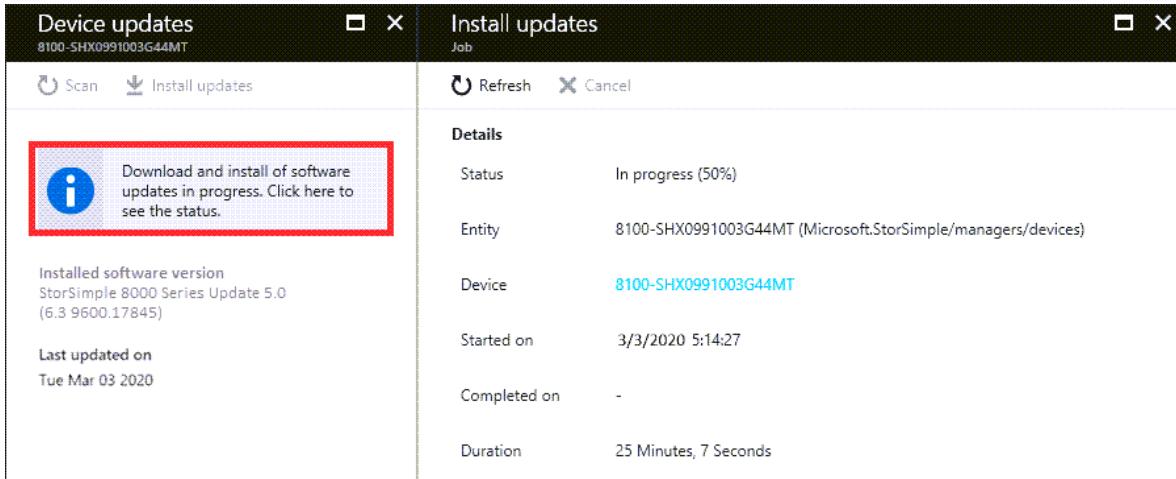
6. After the prechecks are successfully completed, an update job is created. You are notified when the update job is successfully created.

 Starting software updates job on devi... 10:39 AM

Successfully completed the operation.

The update is then applied on your device.

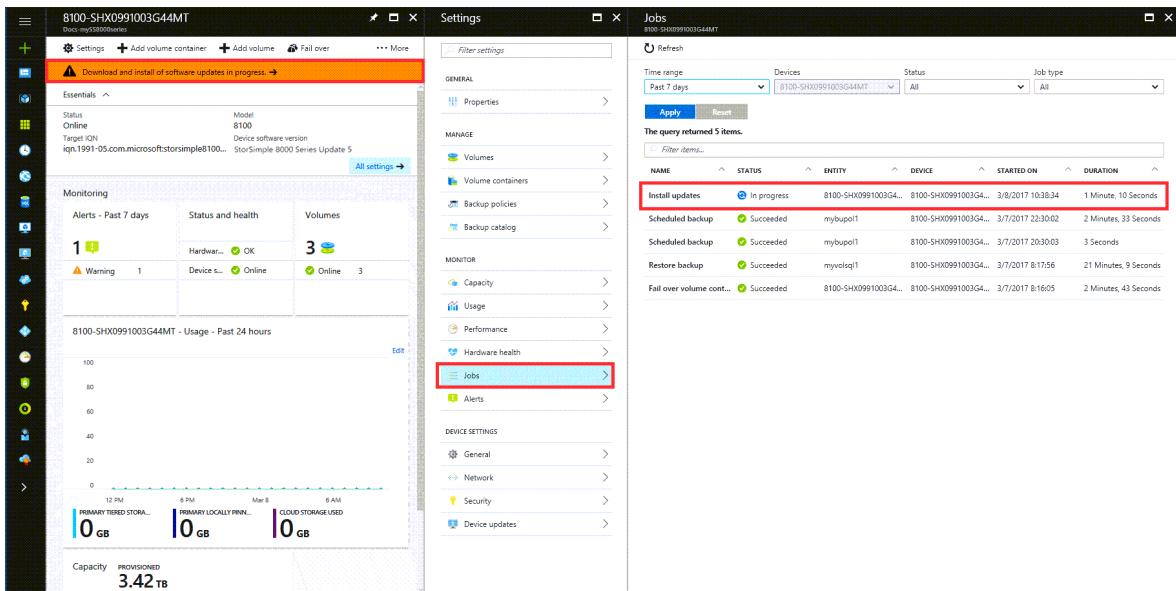
7. The update takes a few hours to complete. Select the update job and click **Details** to view the details of the job at any time.



The screenshot shows two overlapping windows. The left window is titled 'Device updates' and shows a status message: 'Download and install of software updates in progress. Click here to see the status.' It also displays the 'Installed software version' as 'StorSimple 8000 Series Update 5.0 (6.3 9600.17845)' and the 'Last updated on' date as 'Tue Mar 03 2020'. The right window is titled 'Install updates Job' and provides detailed information about the current job:

Details
Status: In progress (50%)
Entity: 8100-SHX0991003G44MT (Microsoft.StorSimple/managers/devices)
Device: 8100-SHX0991003G44MT
Started on: 3/3/2020 5:14:27
Completed on: -
Duration: 25 Minutes, 7 Seconds

You can also monitor the progress of the update job from **Device settings > Jobs**. On the **Jobs** blade, you can see the update progress.



The screenshot shows the 'Device settings' interface with the 'Jobs' blade selected. The 'Install updates' job is listed in the 'Jobs' table, which includes columns for Name, Status, Entity, Device, Started On, and Duration. The 'Install updates' job is shown as 'In progress'.

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Install updates	In progress	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/8/2017 10:38:34	1 Minute, 10 Seconds
Scheduled backup	Succeeded	mybackup1	8100-SHX0991003G44MT	3/7/2017 22:30:02	2 Minutes, 33 Seconds
Restore backup	Succeeded	myvsql1	8100-SHX0991003G44MT	3/7/2017 8:17:56	21 Minutes, 9 Seconds
Fall over volume cont...	Succeeded	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/7/2017 8:16:05	2 Minutes, 43 Seconds

8. After the job is complete, navigate to the **Device settings > Device updates**. The software version should now be updated.

Verify that your device is running **StorSimple 8000 Series Update 5.1 (6.3.9600.17885)** and the **Last updated date** is today's date.

Install Update 5.1 as a hotfix

If you want to install Update 5.1 as a hotfix, do these steps before you begin the installation:

- Install Update 5 before you install Update 5.1. For instructions, see [Install Update 5 on your StorSimple device](#).
- Before you begin the hotfix installation, contact [Microsoft Support](#).

The hotfix method involves the following steps:

1. Download the hotfix from the Microsoft Update Catalog.
2. Install and verify the regular mode hotfix.
3. Install and verify the maintenance mode hotfix.

Download updates for your device

You must download and install the following hotfixes to the suggested folders in the prescribed order.

Order	KB	Description	Update type	Install time	Install in folder
1.	KB4542887	Software update Download both <i>HcsSoftwareUpdate.exe</i> and <i>CisMSDAgent.exe</i>	Regular Non-disruptive	~ 25 mins	FirstOrderUpdate
3. ^{1, 2}	KB4037263	Disk firmware	Maintenance Disruptive	~ 30 mins	ThirdOrderUpdate

¹ There are no second order updates in Update 5.1.

² Install the third order updates if you didn't install disk firmware updates on top of the hotfix updates for Update 5.

Perform the following steps to download and install the hotfixes.

Download hotfixes

To download the hotfixes, see [To download hotfixes](#).

Install and verify device updates

Install the device updates in KB4542887 by following the steps in [To install and verify regular mode hotfixes](#) in [Install Update 5 on your StorSimple device](#).

ⓘ Important

If you haven't yet contacted **Microsoft Support**, you must do that now, before you install the hotfixes.

Follow the steps to install first order updates. There are no second order updates in Update 5.1.

For Update 5.1, check for these software versions after installing:

- FriendlySoftwareVersion: StorSimple 8000 Series Update 5.1
- HcsSoftwareVersion: 6.3.9600.17885
- CisAgentVersion: 1.0.9777.0
- MdsAgentVersion: 35.2.2.0
- Lsisas2Version: 2.0.78.00

Install and verify disk firmware updates

If you didn't install disk firmware updates when you installed Update 5, install the disk firmware updates in KB4037263 by following the steps in [To install and verify regular mode hotfixes](#) in [Install Update 5 on your StorSimple device](#).

You don't need to install disk firmware updates if you're running these firmware versions: `XMGJ`, `XGEG`, `KZ50`, `F6C2`, `VR08`, `N003`, `0107`.

To verify whether you need the disk firmware updates, run the `Get-HcsFirmwareVersion` cmdlet.

Next steps

Learn more about the [Update 5.1 release](#).

Install Update 5 on your StorSimple device\

Article • 08/19/2022 • 18 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to install Update 5 on a StorSimple device running an earlier software version via the Azure portal and using the hotfix method. The hotfix method is used when you are trying to install Update 5 on a device running pre-Update 3 versions. The hotfix method is also used when a gateway is configured on a network interface other than DATA 0 of the StorSimple device and you are trying to update from a pre-Update 1 software version.

Update 5 includes device software, Storport and Spaceport, OS security updates and OS updates, and disk firmware updates. The device software, Spaceport, Storport, security, and other OS updates are non-disruptive updates. The non-disruptive or regular updates can be applied via the Azure portal or via the hotfix method. The disk firmware updates are disruptive updates and are applied when the device is in maintenance mode via the hotfix method using the Windows PowerShell interface of the device.

ⓘ Important

- Update 5 is a mandatory update and should be installed immediately. For more information, see [Update 5 release notes](#).
- A set of manual and automatic pre-checks are done prior to the install to determine the device health in terms of hardware state and network connectivity. These pre-checks are performed only if you apply the updates from the Azure portal.

- We strongly recommend that when updating a device running versions prior to Update 3, you install the updates using hotfix method. If you encounter any issues, [log a support ticket](#).
- We recommend that you install the software and other regular updates via the Azure portal. You should only go to the Windows PowerShell interface of the device (to install updates) if the pre-update gateway check fails in the portal. Depending upon the version you are updating from, the updates may take 4 hours (or greater) to install. The maintenance mode updates must be installed via the Windows PowerShell interface of the device. As maintenance mode updates are disruptive updates, these result in a down time for your device.
- If running the optional StorSimple Snapshot Manager, ensure that you have upgraded your Snapshot Manager version to Update 5 prior to updating the device.

Preparing for updates

You will need to perform the following steps before you scan and apply the update:

1. Take a cloud snapshot of the device data.
2. Ensure that your controller fixed IPs are routable and can connect to the Internet. These fixed IPs will be used to service updates to your device. You can test this by running the following cmdlet on each controller from the Windows PowerShell interface of the device:

```
Test-Connection -Source <Fixed IP of your device controller> -Destination <Any IP or computer name outside of datacenter network>
```

Sample output for Test-Connection when fixed IPs can connect to the Internet

Output

Source	Destination	IPV4Address	IPV6Address
<hr/>			
HCSNODE0	bing.com	204.79.197.200	

```
Controller0>Test-Connection -Source 10.126.173.91 -Destination  
204.79.197.200
```

Source	Destination	IPV4Address	IPV6Address
HCSNODE0	204.79.197.200	204.79.197.200	

After you have successfully completed these manual pre-checks, you can proceed to scan and install the updates.

Install Update 5 via the Azure portal

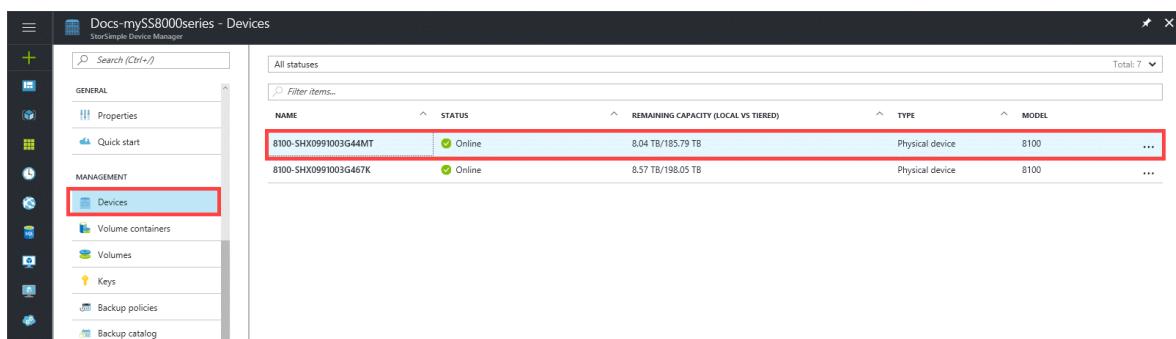
Perform the following steps to update your device to [Update 5](#).

Note

Microsoft pulls additional diagnostic information from the device. As a result, when our operations team identifies devices that are having problems, we are better equipped to collect information from the device and diagnose issues.

To install an update from the Azure portal

1. On the StorSimple service page, select your device.



The screenshot shows the 'Devices' section of the StorSimple Device Manager. The left sidebar has a 'Devices' button highlighted with a red box. The main area displays a table with two rows of device information:

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.04 TB/185.79 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100

2. Navigate to **Device settings > Device updates**.

The screenshot shows the Microsoft StorSimple 8000 Series Management Portal. On the left, there's a vertical toolbar with various icons. The main area displays device details (8100-SHX0991003G44MT, Model 8100, Target IQN iqn.1991-05.com.microsoft:stor simple8100...), monitoring information (Alerts - Past 7 days: 1 Warning, Status and health: Hardwar... OK, Volumes: 3 Online), and usage statistics (Usage - Past 24 hours: PRIMARY TIERED STORA... 0 GB, PRIMARY LOCALLY PINNED 0 GB, CLOUD STORAGE USED 0 GB, Capacity PROVISIONED 3.42 TB). On the right, the 'Settings' blade is open, showing sections for GENERAL (Properties), MANAGE (Volumes, Volume containers, Backup policies, Backup catalog), MONITOR (Capacity, Usage, Performance, Hardware health, Jobs, Alerts), DEVICE SETTINGS (General, Network, Security), and a highlighted section for Device updates.

3. A notification appears if new updates are available. Alternatively, in the **Device updates** blade, click **Scan Updates**. A job is created to scan for available updates. You are notified when the job completes successfully.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and lists various management and monitoring options. The right window is titled 'Device updates' and displays information about available software updates.

Settings Window:

- GENERAL: Properties
- MANAGE: Volumes, Volume containers, Backup policies, Backup catalog
- MONITOR: Capacity, Usage, Performance, Hardware health, Jobs, Alerts
- DEVICE SETTINGS: General, Network, Security, Device updates

Device updates Window:

- Scan, Install updates
- New regular updates are available. Click 'Install updates.'
- Installed software version: StorSimple 8000 Series Update 4.0 (6.3.9600.17820)
- Last updated on: -

4. We recommend that you review the release notes before you apply an update on your device. To apply updates, click **Install updates**. In the **Confirm regular updates** blade, review the prerequisites to complete before you apply updates. Select the checkbox to indicate that you are ready to update the device and then click **Install**.

<p>Device updates 8100-SHX0991003G44MT</p> <p> Scan Install updates</p> <p>i New regular updates are available. Click 'Install updates'.</p> <p>Installed software version StorSimple 8000 Series Update 4.0 (6.3.9600.17820)</p> <p>Last updated on -</p>	<p>Confirm regular updates 8100-SHX0991003G44MT</p> <ol style="list-style-type: none"> 1. Before you update, ensure that the controller fixed IPs for your StorSimple device are routable and can connect to the Internet. Run Test-Connection -Source <Controller Fixed IP> <Computer Name> on both controllers to test the Internet connectivity. 2. To protect your data, we recommend that you take a cloud snapshot of the device before you update. 3. The backup jobs currently in progress will be canceled once the update starts. 4. A pre-upgrade check is performed before downloading and installing the update. If the prechecks fail, device updates will not be installed. <p><input checked="" type="checkbox"/> I agree to and accept any additional terms associated with new functionalities in the release notes.</p> <p>I understand the above requirement and am ready to upgrade my device.</p> <p>Install</p>
---	---

5. A set of prerequisite checks starts. These checks include:

- **Controller health checks** to verify that both the device controllers are healthy and online.
- **Hardware component health checks** to verify that all the hardware components on your StorSimple device are healthy.
- **DATA 0 checks** to verify that DATA 0 is enabled on your device. If this interface is not enabled, you must enable it and then retry.

The update is downloaded and installed only if all the checks are successfully completed. You are notified when the checks are in progress. If the prechecks fail, then you will be provided with the reasons for failure. Address those issues and then retry the operation. You may need to contact Microsoft Support if you cannot address these issues by yourself.

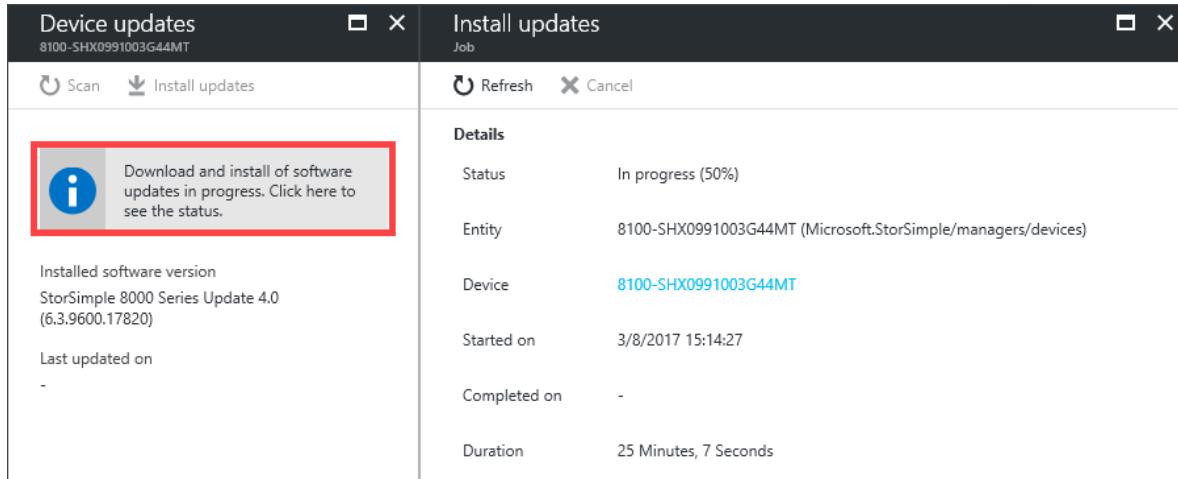
6. After the prechecks are successfully completed, an update job is created. You are notified when the update job is successfully created.

 Starting software updates job on devi... 10:39 AM

Successfully completed the operation.

The update is then applied on your device.

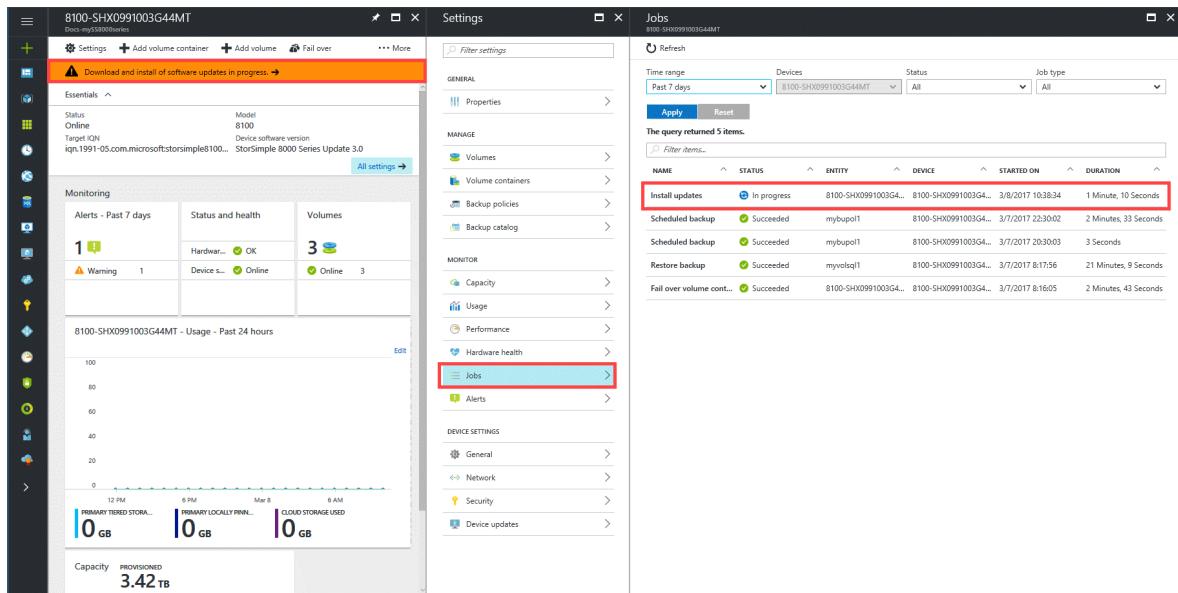
7. The update takes a few hours to complete. Select the update job and click **Details** to view the details of the job at any time.



The screenshot shows two overlapping windows. The left window is titled 'Device updates' and shows a message: 'Download and install of software updates in progress. Click here to see the status.' The right window is titled 'Install updates Job' and displays the following details:

Details	
Status	In progress (50%)
Entity	8100-SHX0991003G44MT (Microsoft.StorSimple/managers/devices)
Device	8100-SHX0991003G44MT
Started on	3/8/2017 15:14:27
Completed on	-
Duration	25 Minutes, 7 Seconds

You can also monitor the progress of the update job from **Device settings > Jobs**. On the **Jobs** blade, you can see the update progress.



The screenshot shows the 'Device settings' interface with the 'Jobs' blade selected. A red box highlights the 'Jobs' link in the navigation menu. The main pane displays a table of jobs:

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Install updates	In progress	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/8/2017 10:38:34	1 Minute, 10 Seconds
Scheduled backup	Succeeded	mybu101	8100-SHX0991003G44MT	3/7/2017 22:30:02	2 Minutes, 33 Seconds
Scheduled backup	Succeeded	mybu101	8100-SHX0991003G44MT	3/7/2017 20:30:03	3 Seconds
Restore backup	Succeeded	myvsql1	8100-SHX0991003G44MT	3/7/2017 8:17:56	21 Minutes, 9 Seconds
Fall over volume cont...	Succeeded	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/7/2017 8:16:05	2 Minutes, 43 Seconds

8. After the job is complete, navigate to the **Device settings > Device updates**. The software version should now be updated.

Verify that your device is running **StorSimple 8000 Series Update 5 (6.3.9600.17845)**. The **Last updated date** should be modified.

You will now see that the Maintenance mode updates are available (this message might continue to be displayed for up to 24 hours after you install the updates). The steps to install maintenance mode update are detailed in the next section.

Install maintenance mode updates via Windows PowerShell for StorSimple

When you apply maintenance mode updates to StorSimple device, all I/O requests are paused. Services such as non-volatile random access memory (NVRAM) or the clustering service are stopped. Both controllers reboot when you enter or exit this mode. When you exit this mode, all the services resume and are healthy. (This may take a few minutes.)

ⓘ Important

- Before entering maintenance mode, verify that both device controllers are healthy in the Azure portal. If the controller is not healthy, [Contact Microsoft Support](#) for the next steps.
- When you are in maintenance mode, you need to first update one controller and then the other controller.

1. Use PuTTY to connect to the serial console. Follow the detailed instructions in [Use PuTTy to connect to the serial console](#). At the command prompt, press **Enter**. Select Option 1, **Log in with full access**.
2. To place the controller in maintenance mode, type:

```
Enter-HcsMaintenanceMode
```

Both the controllers restart into maintenance mode.

3. Install your maintenance mode updates. Type:

```
Start-HcsUpdate
```

You are prompted for confirmation. After you confirm the updates, they are installed on the controller that you are currently accessing. After the updates are installed, the controller restarts.

4. Monitor the status of updates. Sign in to the peer controller as the current controller is updating and is not able to process any other commands. Type:

```
Get-HcsUpdateStatus
```

If the `RunInProgress` is `True`, the update is still in progress. If `RunInProgress` is `False`, it indicates that the update has completed.

5. After the disk firmware updates are successfully applied and the updated controller has restarted, verify the disk firmware version. On the updated controller, type:

```
Get-HcsFirmwareVersion
```

The expected disk firmware versions are: XMGJ, XGEG, KZ50, F6C2, VR08, N003, 0107

6. Exit the maintenance mode. Type the following command for each device controller:

```
Exit-HcsMaintenanceMode
```

The controllers restart when you exit maintenance mode.

7. Return to the Azure portal. The portal may not show that you installed the maintenance mode updates for 24 hours.

Install Update 5 as a hotfix

The software versions that can be upgraded using the hotfix method are:

- Update 0.1, 0.2, 0.3
- Update 1, 1.1, 1.2
- Update 2, 2.1, 2.2
- Update 3, 3.1
- Update 4

Note

The recommended method to install Update 5 is via the Azure portal when trying to update from Update 3 and later version. When updating a device running versions prior to Update 3, use this procedure. You can also use this procedure if you fail the gateway check when trying to install the updates through the Azure portal. The check fails when you have a gateway assigned to a non-DATA 0 network interface and your device is running a software version earlier than Update 1.

The hotfix method involves the following three steps:

1. Download the hotfixes from the Microsoft Update Catalog.
2. Install and verify the regular mode hotfixes.
3. Install and verify the maintenance mode hotfix.

Download updates for your device

You must download and install the following hotfixes in the prescribed order and the suggested folders:

Order	KB	Description	Update type	Install time	Install in folder
1.	KB4037264	Software update Download both <i>HcsSoftwareUpdate.exe</i> and <i>CisMSDAgent.exe</i>	Regular Non-disruptive	~ 25 mins	FirstOrderUpdate

If updating from a device running Update 4, you only need to install the OS cumulative updates as second order updates.

Order	KB	Description	Update type	Install time	Install in folder
2A.	KB4025336	OS cumulative updates package Download Windows Server 2012 R2 version	Regular Non-disruptive	-	SecondOrderUpdate

If installing from a device running Update 3 or earlier, install the following in addition to the cumulative updates.

Order	KB	Description	Update type	Install time	Install in folder
2B.	KB4011841 KB4011842	LSI driver and firmware updates USM firmware update (version 3.38)	Regular Non-disruptive	~ 3 hrs (includes 2A. + 2B. + 2C.)	SecondOrderUpdate
2C.	KB3139398 KB3142030 KB3108381 KB3153704 KB3174644 KB3139914	OS security updates package Download Windows Server 2012 R2 version	Regular Non-disruptive	-	SecondOrderUpdate
2D.	KB3146621 KB3103616 KB3121261 KB3123538	OS updates package Download Windows Server 2012 R2 version	Regular Non-disruptive	-	SecondOrderUpdate

You may also need to install disk firmware updates on top of all the updates shown in the preceding tables. You can verify whether you need the disk firmware updates by running the `Get-HcsFirmwareVersion` cmdlet. If you are running these firmware versions: XMGJ, XGEG, KZ50, F6C2, VR08, N003, 0107, then you do not need to install these updates.

Order	KB	Description	Update type	Install time	Install in folder
3.	KB4037263	Disk firmware	Maintenance	~ 30 mins	ThirdOrderUpdate

ⓘ Important

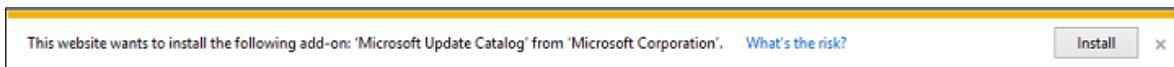
- If updating from Update 4, the total install time is close to 4 hours.
- Before using this procedure to apply the update, make sure that both the device controllers are online and all the hardware components are healthy.

Perform the following steps to download and install the hotfixes.

To download hotfixes

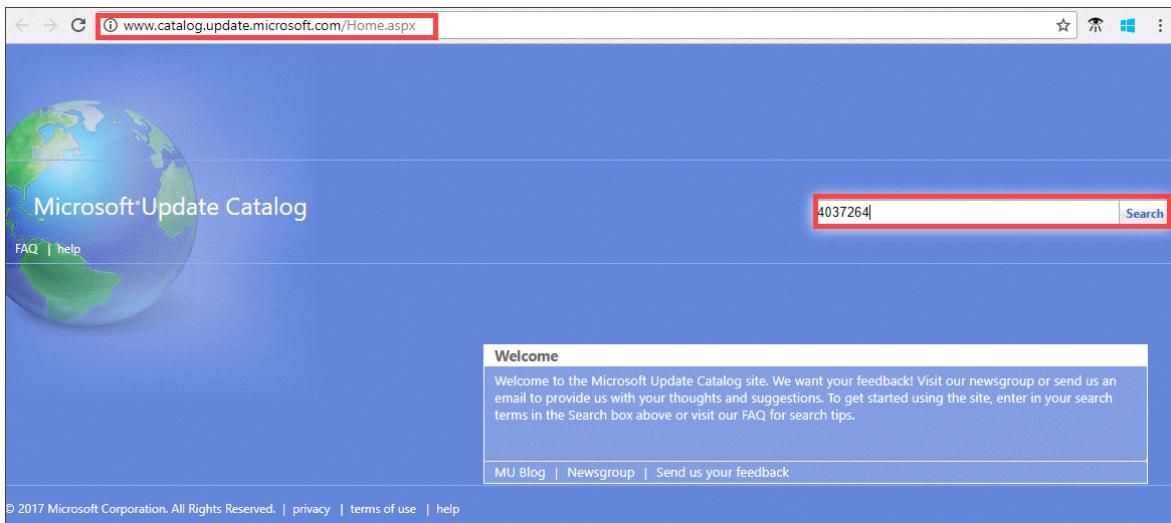
Perform the following steps to download the software update from the Microsoft Update Catalog.

1. Start Internet Explorer and navigate to <http://catalog.update.microsoft.com>.
2. If this is your first time using the Microsoft Update Catalog on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.



3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download, for example **4037264**, and then click **Search**.

The hotfix listing appears, for example, **Cumulative Software Bundle Update 5.0 for StorSimple 8000 Series**.



4. Click **Download**. Specify or **Browse** to a local location where you want the downloads to appear. Click the files to download to the specified location and folder. The folder can also be copied to a network share that is reachable from the device.
5. Search for any additional hotfixes listed in the table above (**4037266**), and download the corresponding files to the specific folders as listed in the preceding table.

Note

The hotfixes must be accessible from both controllers to detect any potential error messages from the peer controller.

The hotfixes must be copied in 3 separate folders. For example, the device software/Cis/MDS agent update can be copied in *FirstOrderUpdate* folder, all the other non-disruptive updates could be copied in the *SecondOrderUpdate* folder, and maintenance mode updates copied in *ThirdOrderUpdate* folder.

To install and verify regular mode hotfixes

Perform the following steps to install and verify regular-mode hotfixes. If you already installed them using the Azure portal, skip ahead to [install and verify maintenance mode hotfixes](#).

1. To install the hotfixes, access the Windows PowerShell interface on your StorSimple device serial console. Follow the detailed instructions in [Use PuTTy to connect to the serial console](#). At the command prompt, press **Enter**.

2. Select option 1, **Log in with full access**. We recommend that you install the hotfix on the passive controller first.

3. To install the hotfix, at the command prompt, type:

```
Start-HcsHotfix -Path <path to update file> -Credential <credentials in  
domain\username format>
```

Use IP rather than DNS in share path in the above command. The credential parameter is used only if you are accessing an authenticated share.

We recommend that you use the credential parameter to access shares. Even shares that are open to "everyone" are typically not open to unauthenticated users.

4. Supply the password when prompted. A sample output for installing the first order updates is shown below. For the first order update, you need to point to the specific file.

 **Note**

You should install the *HcsSoftwareUpdate.exe* first. After this install has completed, then install *CisMdsAgentUpdate.exe*.

Output

```
Controller0>Start-HcsHotfix -Path \\10.100.100.100\share  
\FirstOrderUpdate\HcsSoftwareUpdate.exe -Credential contoso\John
```

Confirm

This operation starts the hotfix installation and could reboot one or both of the controllers. If the device is serving I/Os, these will not be disrupted. Are you sure you want to continue?
[Y] Yes [N] No [?] Help (default is "Y"): Y

5. Type **Y** when prompted to confirm the hotfix installation.

6. Monitor the update by using the `Get-HcsUpdateStatus` cmdlet. The update will first complete on the passive controller. Once the passive controller is updated, there will be a failover and the update will then get applied on the other controller. The update is complete when both the controllers are updated.

The following sample output shows the update in progress. The `RunInProgress` is `True` when the update is in progress.

```
Controller0>Get-HcsUpdateStatus  
RunInprogress      : True  
LastHotfixTimestamp :  
LastUpdateTimestamp : 07/28/2017 2:04:02 AM  
Controller0Events   :  
Controller1Events   :
```

The following sample output indicates that the update is finished. The `RunInProgress` is `False` when the update is complete.

```
Controller0>Get-HcsUpdateStatus  
RunInprogress      : False  
LastHotfixTimestamp : 07/28/2017 9:15:55 AM  
LastUpdateTimestamp : 07/28/2017 9:06:07 AM  
Controller0Events   :  
Controller1Events   :
```

ⓘ Note

Occasionally, the cmdlet reports `False` when the update is still in progress. To ensure that the hotfix is complete, wait for a few minutes, rerun this command and verify that the `RunInProgress` is `False`. If it is, then the hotfix has completed.

7. After the software update is complete, verify the system software versions. Type:

```
Get-HcsSystem
```

You should see the following versions:

- `FriendlySoftwareVersion: StorSimple 8000 Series Update 5.0`
- `HcsSoftwareVersion: 6.3.9600.17845`

If the version number does not change after applying the update, it indicates that the hotfix has failed to apply. Should you see this, please contact [Microsoft Support](#) for further assistance.

ⓘ Important

You must restart the active controller via the `Restart-HcsController` cmdlet before applying the next update.

8. Repeat steps 3-6 to install the `CisMDSAgentupdate.exe` agent downloaded to your `FirstOrderUpdate` folder.

9. Repeat steps 3-6 to install the second order updates.

 **Note**

For second order updates, multiple updates can be installed by just running the `Start-HcsHotfix` cmdlet and pointing to the folder where second order updates are located. The cmdlet will execute all the updates available in the folder. If an update is already installed, the update logic will detect that and not apply that update.

After all the hotfixes are installed, use the `Get-HcsSystem` cmdlet. The versions should be:

- `CisAgentVersion: 1.0.9724.0`
- `MdsAgentVersion: 35.2.2.0`
- `Lsisas2Version: 2.0.78.00`

To install and verify maintenance mode hotfixes

Use KB4037263 to install disk firmware updates. These are disruptive updates and take around 30 minutes to complete. You can choose to install these in a planned maintenance window by connecting to the device serial console.

 **Note**

If your disk firmware is already up-to-date, you won't need to install these updates. Run the `Get-HcsUpdateAvailability` cmdlet from the device serial console to check if updates are available and whether the updates are disruptive (maintenance mode) or non-disruptive (regular mode) updates.

To install the disk firmware updates, follow the instructions below.

1. Place the device in the maintenance mode.

! Note

Do not use Windows PowerShell remoting when connecting to a device in maintenance mode. Instead run this cmdlet on the device controller when connected through the device serial console.

To place the controller in maintenance mode, type:

```
Enter-HcsMaintenanceMode
```

A sample output is shown below.

Output

```
Controller0>Enter-HcsMaintenanceMode  
Checking device state...
```

In maintenance mode, your device will not service IOs and will be disconnected from the Microsoft Azure StorSimple Manager service. Entering maintenance mode will end the current session and reboot both controllers, which takes a few minutes to complete. Are you sure you want to enter maintenance mode?
[Y] Yes [N] No (Default is "Y"): Y

```
-----MAINTENANCE MODE-----  
Microsoft Azure StorSimple Appliance Model 8600  
Name: Update4-8600-mystorsimple  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller0 - Passive  
-----
```

```
Serial Console Menu  
[1] Log in with full access  
[2] Log into peer controller with full access  
[3] Connect with limited access  
[4] Change language  
Please enter your choice>
```

Both the controllers then restart into maintenance mode.

2. To install the disk firmware update, type:

```
Start-HcsHotfix -Path <path to update file> -Credential <credentials in  
domain\username format>
```

A sample output is shown below.

Output

```
Controller1>Start-HcsHotfix -Path  
\\10.100.100.100\share\ThirdOrderUpdates\ -Credential contoso\john  
Enter Password:  
WARNING: In maintenance mode, hotfixes should be installed on each  
controller sequentially. After the hotfix is installed on this  
controller, install it on the peer controller.  
Confirm  
This operation starts a hotfix installation and could reboot one or  
both of the controllers. By installing new updates you agree to, and  
accept any additional terms associated with, the new functionality  
listed in the release notes (https://go.microsoft.com/fwlink/?LinkID=613790). Are you sure you want to continue?  
[Y] Yes [N] No (Default is "Y"): Y  
WARNING: Installation is currently in progress. This operation can take  
several minutes to complete.
```

3. Monitor the install progress using `Get-HcsUpdateStatus` command. The update is complete when the `RunInProgress` changes to `False`.
4. After the installation is complete, the controller on which the maintenance mode hotfix was installed restarts. Sign in as option 1, **Log in with full access**, and verify the disk firmware version. Type:

```
Get-HcsFirmwareVersion
```

The expected disk firmware versions are:

```
XMGJ, XGEG, KZ50, F6C2, VR08, N003, 0107
```

A sample output is shown below.

Output

```
-----MAINTENANCE MODE-----  
Microsoft Azure StorSimple Appliance Model 8600  
Name: Update4-8600-mystorsimple  
Software Version: 6.3.9600.17845  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller1  
-----
```

```
Controller1>Get-HcsFirmwareVersion  
  
Controller0 : TalladegaFirmware  
ActiveBIOS:0.45.0010  
    BackupBIOS:0.45.0006  
    MainCPLD:17.0.000b  
    ActiveBMCRoot:2.0.001F  
    BackupBMCRoot:2.0.001F  
    BMCBoot:2.0.0002
```

```
LsiFirmware:20.00.04.00
LsiBios:07.37.00.00
Battery1Firmware:06.2C
Battery2Firmware:06.2C
DomFirmware:X231600
CanisterFirmware:3.5.0.56
CanisterBootloader:5.03
CanisterConfigCRC:0x9134777A
CanisterVPDStructure:0x06
CanisterGEMCPLD:0x19
CanisterVPDCRC:0x142F7DC2
MidplaneVPDStructure:0x0C
MidplaneVPDCRC:0xA6BD4F64
MidplaneCPLD:0x10
PCM1Firmware:1.00|1.05
PCM1VPDStructure:0x05
PCM1VPDCRC:0x41BEF99C
PCM2Firmware:1.00|1.05
PCM2VPDStructure:0x05
PCM2VPDCRC:0x41BEF99C
```

EbodFirmware

```
CanisterFirmware:3.5.0.56
CanisterBootloader:5.03
CanisterConfigCRC:0xB23150F8
CanisterVPDStructure:0x06
CanisterGEMCPLD:0x14
CanisterVPDCRC:0xBA55828
MidplaneVPDStructure:0x0C
MidplaneVPDCRC:0xA6BD4F64
MidplaneCPLD:0x10
PCM1Firmware:3.11
PCM1VPDStructure:0x03
PCM1VPDCRC:0x6B58AD13
PCM2Firmware:3.11
PCM2VPDStructure:0x03
PCM2VPDCRC:0x6B58AD13
```

DisksFirmware

```
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08
```

Run the `Get-HcsFirmwareVersion` command on the second controller to verify that the software version has been updated. You can then exit the maintenance mode. To do so, type the following command for each device controller:

```
Exit-HcsMaintenanceMode
```

5. The controllers restart when you exit maintenance mode. After the disk firmware updates are successfully applied and the device has exited maintenance mode, return to the Azure portal. Note that the portal might not show that you installed the maintenance mode updates for 24 hours.

Troubleshooting update failures

What if you see a notification that the pre-upgrade checks have failed?

If a pre-check fails, make sure that you have looked at the detailed notification bar at the bottom of the page. This provides guidance as to which pre-check has failed. For instance, you receive a notification that the controller health check and hardware component health check have failed. Go to **Monitor > Hardware health**. You need to make sure that both controllers are healthy and online. You also need to make sure that all the hardware components in the StorSimple device are shown to be healthy in this blade. You can then try to install updates. If you are not able to fix the hardware component issues, then you will need to contact Microsoft Support for next steps.

What if you receive a "Could not install updates" error message, and the recommendation is to refer to the update troubleshooting guide to determine the cause of the failure?

One likely cause for this could be that you do not have connectivity to the Microsoft Update servers. This is a manual check that needs to be performed. If you lose connectivity to the update server, your update job would fail. You can check the connectivity by running the following cmdlet from the Windows PowerShell interface of your StorSimple device:

```
Test-Connection -Source <Fixed IP of your device controller> -Destination <Any IP  
or computer name outside of datacenter>
```

Run the cmdlet on both controllers.

If you have verified the connectivity exists, and you continue to see this issue, please contact Microsoft Support for next steps.

What if you see an update failure when updating your device to Update 4 and both the controllers are running Update 4?

Starting Update 4, if both the controllers are running the same software version and if there is an update failure, the controllers do not go into recovery mode. This situation can arise if the device software hotfix (1st order update) is applied to both the controllers successfully but other hotfixes (2nd order and 3rd order) are yet to be applied. Starting Update 4, the controllers will go into recovery mode only if the two controllers are running different software versions.

If the user sees an update failure when both controllers are running Update 4, we recommend that they wait a few minutes and then retry updating. If the retry does not succeed, then they should contact Microsoft Support.

Next steps

Learn more about the [Update 5 release](#).

Install Update 4 on your StorSimple device

Article • 08/19/2022 • 16 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This tutorial explains how to install Update 4 on a StorSimple device running an earlier software version via the Azure portal and using the hotfix method. The hotfix method is used when a gateway is configured on a network interface other than DATA 0 of the StorSimple device and you are trying to update from a pre-Update 1 software version.

Update 4 includes device software, USM firmware, LSI driver and firmware, Storport and Spaceport, OS security updates, and a host of other OS updates. The device software, USM firmware, Spaceport, Storport, and other OS updates are non-disruptive updates. The non-disruptive or regular updates can be applied via the Azure portal or via the hotfix method. The disk firmware updates are disruptive updates and can only be applied via the hotfix method using the Windows PowerShell interface of the device.

ⓘ Important

- A set of manual and automatic pre-checks are done prior to the install to determine the device health in terms of hardware state and network connectivity. These pre-checks are performed only if you apply the updates from the Azure portal.
- We recommend that you install the software and other regular updates via the Azure portal. You should only go to the Windows PowerShell interface of the device (to install updates) if the pre-update gateway check fails in the portal. Depending upon the version you are updating from, the updates may

take 4 hours (or greater) to install. The maintenance mode updates must also be installed via the Windows PowerShell interface of the device. As maintenance mode updates are disruptive updates, these will result in a down time for your device.

- If running the optional StorSimple Snapshot Manager, ensure that you have upgraded your Snapshot Manager version to Update 4 prior to updating the device.

Preparing for updates

You will need to perform the following steps before you scan and apply the update:

1. Take a cloud snapshot of the device data.
2. Ensure that your controller fixed IPs are routable and can connect to the Internet. These fixed IPs will be used to service updates to your device. You can test this by running the following cmdlet on each controller from the Windows PowerShell interface of the device:

```
Test-Connection -Source <Fixed IP of your device controller> -Destination <Any IP or computer name outside of datacenter network>
```

Sample output for Test-Connection when fixed IPs can connect to the Internet

Output

```
Controller0>Test-Connection -Source 10.126.173.91 -Destination bing.com
```

Source	Destination	IPV4Address	IPV6Address
HCSNODE0	bing.com	204.79.197.200	

```
Controller0>Test-Connection -Source 10.126.173.91 -Destination  
204.79.197.200
```

Source	Destination	IPV4Address	IPV6Address
HCSNODE0	204.79.197.200	204.79.197.200	

After you have successfully completed these manual pre-checks, you can proceed to scan and install the updates.

Install Update 4 via the Azure portal

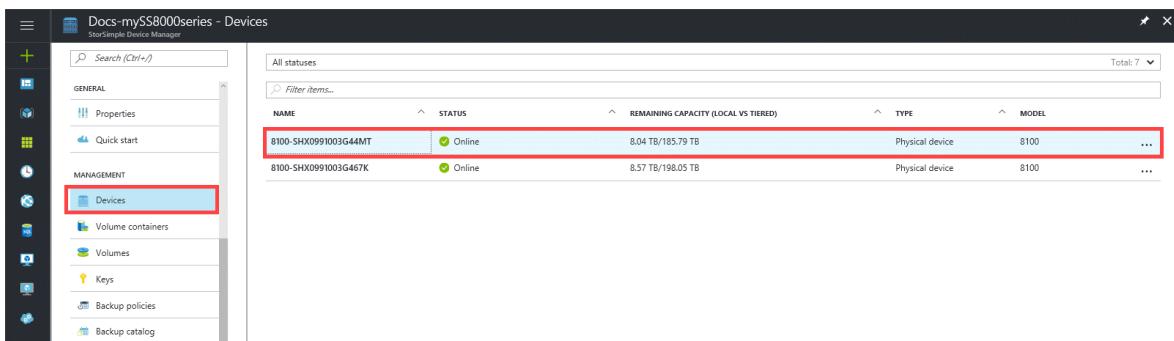
Perform the following steps to update your device to [Update 4](#).

Note

Microsoft pulls additional diagnostic information from the device. As a result, when our operations team identifies devices that are having problems, we are better equipped to collect information from the device and diagnose issues.

To install an update from the Azure portal

1. On the StorSimple service page, select your device.



The screenshot shows the 'Devices' section of the StorSimple Device Manager. The left sidebar has a 'Devices' item highlighted with a red box. The main area displays a table with two rows of device information:

NAME	STATUS	REMAINING CAPACITY (LOCAL VS TIERED)	TYPE	MODEL
8100-SHX0991003G44MT	Online	8.04 TB/185.79 TB	Physical device	8100
8100-SHX0991003G467K	Online	8.57 TB/198.05 TB	Physical device	8100

2. Navigate to **Device settings > Device updates**.

The screenshot shows the Microsoft StorSimple 8000 Series Management Portal. On the left, there's a vertical toolbar with various icons. The main area displays device details (8100-SHX0991003G44MT, Model 8100, Target IQN iqn.1991-05.com.microsoft:stor simple8100...), monitoring information (Alerts - Past 7 days: 1 Warning, Status and health: Hardwar... OK, Volumes: 3 Online), and usage statistics (Usage - Past 24 hours: PRIMARY TIERED STORA... 0 GB, PRIMARY LOCALLY PINNED 0 GB, CLOUD STORAGE USED 0 GB, Capacity PROVISIONED 3.42 TB). On the right, the 'Settings' blade is open, showing sections for GENERAL (Properties), MANAGE (Volumes, Volume containers, Backup policies, Backup catalog), MONITOR (Capacity, Usage, Performance, Hardware health, Jobs, Alerts), DEVICE SETTINGS (General, Network, Security), and a highlighted section for Device updates.

3. A notification appears if new updates are available. Alternatively, in the **Device updates** blade, click **Scan Updates**. A job is created to scan for available updates. You are notified when the job completes successfully.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and lists various management and monitoring options. The right window is titled 'Device updates' and displays information about available software updates.

Settings Window (Left):

- GENERAL
 - Properties
- MANAGE
 - Volumes
 - Volume containers
 - Backup policies
 - Backup catalog
- MONITOR
 - Capacity
 - Usage
 - Performance
 - Hardware health
 - Jobs
 - Alerts
- DEVICE SETTINGS
 - General
 - Network
 - Security
 - Device updates

Device updates Window (Right):

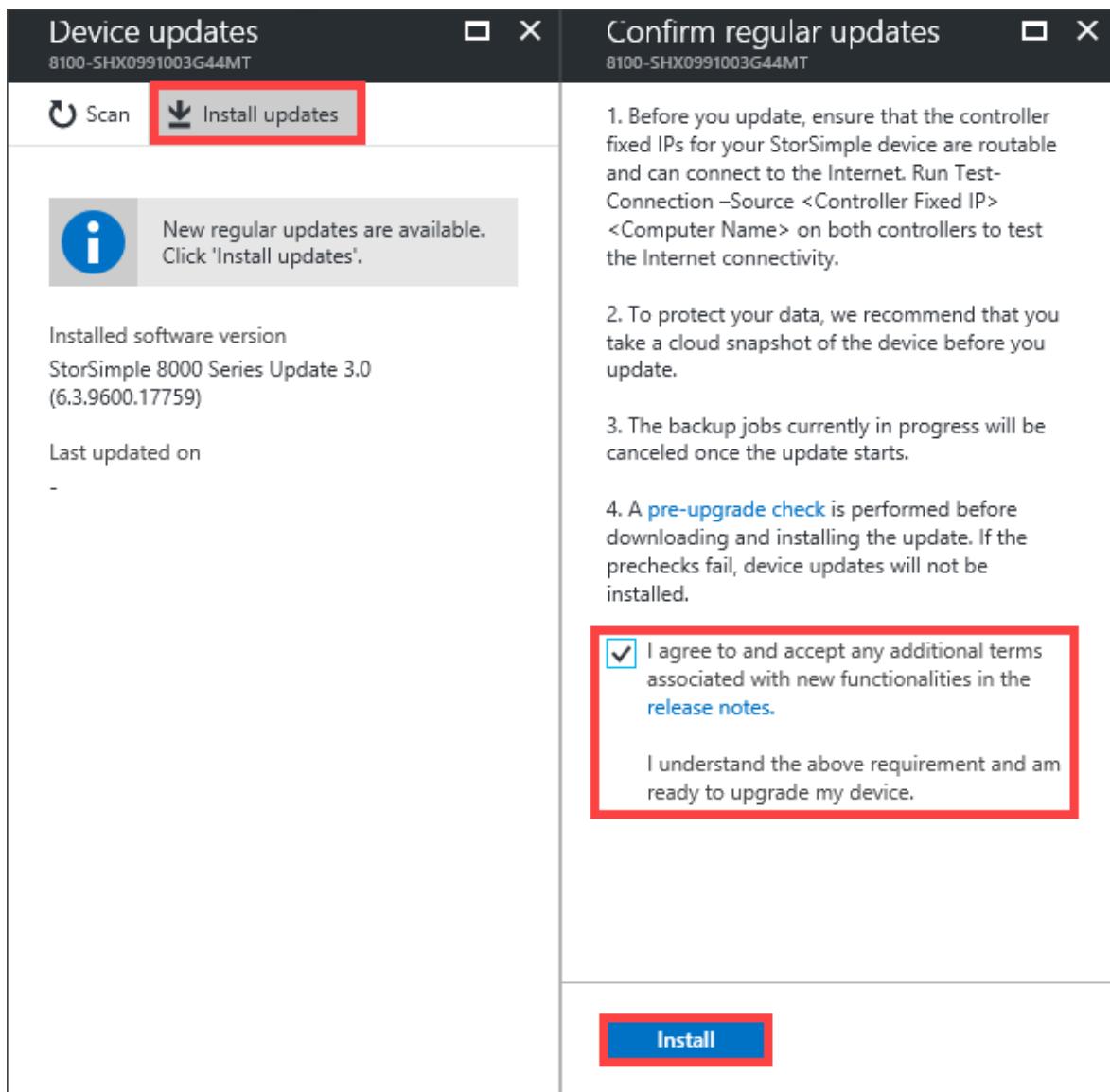
- Scan
- Install updates

New regular updates are available.
Click 'Install updates'.

Installed software version
StorSimple 8000 Series Update 3.0
(6.3.9600.17759)

Last updated on
-

4. We recommend that you review the release notes before you apply an update on your device. To apply updates, click **Install updates**. In the **Confirm regular updates** blade, review the prerequisites to complete before you apply updates. Select the checkbox to indicate that you are ready to update the device and then click **Install**.



5. A set of prerequisite checks starts. These checks include:

- **Controller health checks** to verify that both the device controllers are healthy and online.
- **Hardware component health checks** to verify that all the hardware components on your StorSimple device are healthy.
- **DATA 0 checks** to verify that DATA 0 is enabled on your device. If this interface is not enabled, you must enable it and then retry.

The update is downloaded and installed only if all the checks are successfully completed. You are notified when the checks are in progress. If the prechecks fail, then you will be provided with the reasons for failure. Address those issues and then retry the operation. You may need to contact Microsoft Support if you cannot address these issues by yourself.

6. After the prechecks are successfully completed, an update job is created. You are notified when the update job is successfully created.



Starting software updates job on devi... 10:39 AM

Successfully completed the operation.

The update is then applied on your device.

7. The update takes a few hours to complete. Select the update job and click **Details** to view the details of the job at any time.

The screenshot shows two overlapping windows. The left window is titled 'Device updates' and shows a message: 'Download and install of software updates in progress. Click here to see the status.' The right window is titled 'Install updates' and displays the following details:

Details	
Status	In progress (50%)
Entity	8100-SHX0991003G44MT (Microsoft.StorSimple/managers/devices)
Device	8100-SHX0991003G44MT
Started on	3/8/2017 15:14:27
Completed on	-
Duration	25 Minutes, 7 Seconds

You can also monitor the progress of the update job from **Device settings > Jobs**. On the **Jobs** blade, you can see the update progress.

The screenshot shows the 'Device settings' interface with the 'Jobs' blade selected. A red box highlights the 'Jobs' link in the navigation menu. The 'Jobs' table lists the following tasks:

NAME	STATUS	ENTITY	DEVICE	STARTED ON	DURATION
Install updates	In progress	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/8/2017 10:38:34	1 Minute, 10 Seconds
Scheduled backup	Succeeded	mybupoi1	8100-SHX0991003G44MT	3/7/2017 22:30:02	2 Minutes, 33 Seconds
Scheduled backup	Succeeded	mybupoi1	8100-SHX0991003G44MT	3/7/2017 20:30:03	3 Seconds
Restore backup	Succeeded	myvoql1	8100-SHX0991003G44MT	3/7/2017 8:17:56	21 Minutes, 9 Seconds
Fall over volume cont...	Succeeded	8100-SHX0991003G44MT	8100-SHX0991003G44MT	3/7/2017 8:16:05	2 Minutes, 43 Seconds

8. After the job is complete, navigate to the **Device settings > Device updates**. The software version should now be updated.

The screenshot shows two windows side-by-side. The left window is titled 'Settings' and lists various management options like Properties, Volumes, and Device updates. The right window is titled 'Device updates' and shows a message about new regular updates available, along with the installed software version (StorSimple 8000 Series Update 4.0) and last update date (Wed Mar 08 2017). The 'Device updates' option in the Settings menu is highlighted with a red box.

Settings

Filter settings

GENERAL

- Properties >

MANAGE

- Volumes >
- Volume containers >
- Backup policies >
- Backup catalog >

MONITOR

- Capacity >
- Usage >
- Performance >
- Hardware health >
- Jobs >
- Alerts >

DEVICE SETTINGS

- General >
- Network >
- Security >
- Device updates > (highlighted with a red box)

Device updates

8100-SHX0991003G44MT

Scan Install updates

New regular updates are available. Click 'Install updates'.

Installed software version
StorSimple 8000 Series Update 4.0
(6.3.9600.17820)

Last updated on
Wed Mar 08 2017

Verify that your device is running **StorSimple 8000 Series Update 4 (6.3.9600.17820)**.
The **Last updated date** should also be modified.

- You will now see that the Maintenance mode updates are available (this message might continue to be displayed for up to 24 hours after you install the updates). Maintenance mode updates are disruptive updates that result in device downtime and can only be applied via the Windows PowerShell interface of your device.

- Download the maintenance mode updates by using the steps listed in [to download hotfixes](#) to search for and download KB4011837, which installs disk firmware updates (the other updates should already be installed by now). Follow the steps listed in [install and verify maintenance mode hotfixes](#) to install the maintenance mode updates.

Install Update 4 as a hotfix

The recommended method to install Update 4 is via the Azure portal.

Use this procedure if you fail the gateway check when trying to install the updates through the Azure portal. The check fails as you have a gateway assigned to a non-DATA 0 network interface and your device is running a software version prior to Update 1.

The software versions that can be upgraded using the hotfix method are:

- Update 0.1, 0.2, 0.3
- Update 1, 1.1, 1.2
- Update 2, 2.1, 2.2
- Update 3, 3.1

The hotfix method involves the following three steps:

1. Download the hotfixes from the Microsoft Update Catalog.
2. Install and verify the regular mode hotfixes.
3. Install and verify the maintenance mode hotfix.

Download updates for your device

You must download and install the following hotfixes in the prescribed order and the suggested folders:

Order	KB	Description	Update type	Install time	Install in folder
1.	KB4011839	Software update	Regular Non-disruptive	~ 25 mins	FirstOrderUpdate

Order	KB	Description	Update type	Install time	Install in folder
2A.	KB4011841 KB4011842	LSI driver and firmware updates USM firmware update (version 3.38)	Regular Non-disruptive	~ 3 hrs (includes 2A. + 2B. + 2C.)	SecondOrderUpdate
2B.	KB3139398, KB3108381 KB3205400, KB3142030 KB3197873, KB3197873 KB3192392, KB3153704 KB3174644, KB3139914	OS security updates package Download Windows Server 2012 R2	Regular Non-disruptive	-	SecondOrderUpdate
2C.	KB3210083, KB3103616 KB3146621, KB3121261 KB3123538	OS updates package Download Windows Server 2012 R2	Regular Non-disruptive	-	SecondOrderUpdate

You may also need to install disk firmware updates on top of all the updates shown in the preceding tables. You can verify whether you need the disk firmware updates by running the `Get-HcsFirmwareVersion` cmdlet. If you are running these firmware versions: `XMGJ`, `XGEG`, `KZ50`, `F6C2`, `VR08`, `N002`, `0106`, then you do not need to install these updates.

Order	KB	Description	Update type	Install time	Install in folder
3.	KB3121899	Disk firmware	Maintenance Disruptive	~ 30 mins	ThirdOrderUpdate

ⓘ Important

- This procedure needs to be performed only once to apply Update 4. You can use the Azure portal to apply subsequent updates.
- If updating from Update 3 or 3.1, the total install time is close to 4 hours.

- Before using this procedure to apply the update, make sure that both the device controllers are online and all the hardware components are healthy.

Perform the following steps to download and install the hotfixes.

To download hotfixes

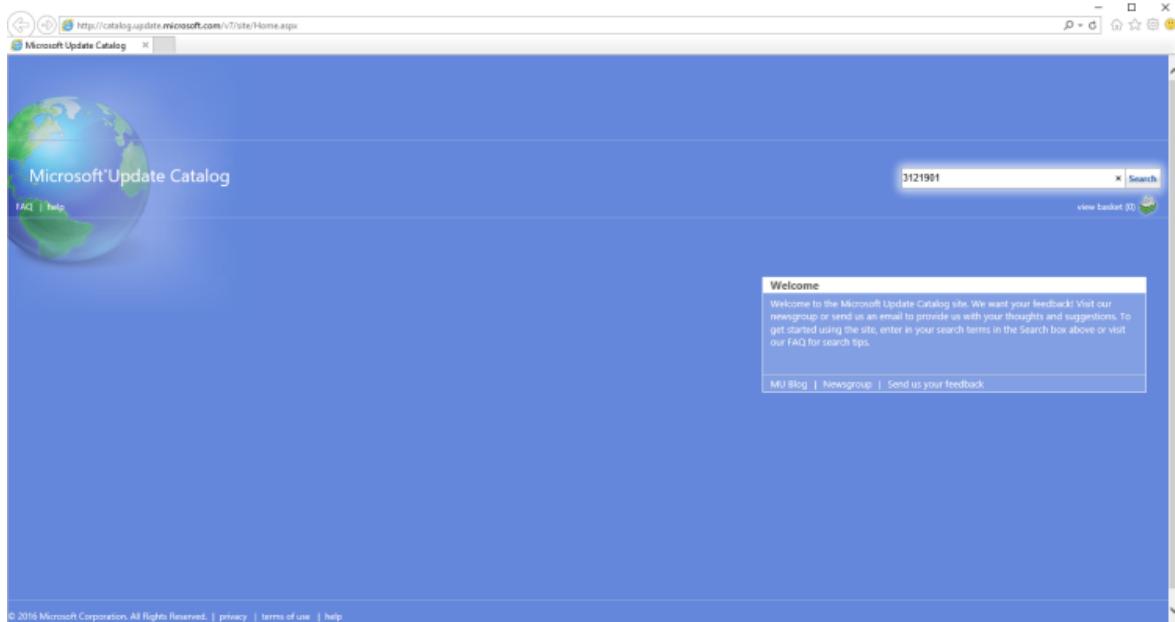
Perform the following steps to download the software update from the Microsoft Update Catalog.

1. Start Internet Explorer and navigate to <http://catalog.update.microsoft.com>.
2. If this is your first time using the Microsoft Update Catalog on this computer, click **Install** when prompted to install the Microsoft Update Catalog add-on.



3. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix you want to download, for example **4011839**, and then click **Search**.

The hotfix listing appears, for example, **Cumulative Software Bundle Update 4.0 for StorSimple 8000 Series**.



4. Click **Download**. Specify or **Browse** to a local location where you want the downloads to appear. Click the files to download to the specified location and folder. The folder can also be copied to a network share that is reachable from the device.

5. Search for any additional hotfixes listed in the table above ([4011841](#)), and download the corresponding files to the specific folders as listed in the preceding table.

 **Note**

The hotfixes must be accessible from both controllers to detect any potential error messages from the peer controller.

The hotfixes must be copied in 3 separate folders. For example, the device software/Cis/MDS agent update can be copied in *FirstOrderUpdate* folder, all the other non-disruptive updates could be copied in the *SecondOrderUpdate* folder, and maintenance mode updates copied in *ThirdOrderUpdate* folder.

To install and verify regular mode hotfixes

Perform the following steps to install and verify regular-mode hotfixes. If you already installed them using the Azure classic portal, skip ahead to [install and verify maintenance mode hotfixes](#).

1. To install the hotfixes, access the Windows PowerShell interface on your StorSimple device serial console. Follow the detailed instructions in [Use PuTTy to connect to the serial console](#). At the command prompt, press **Enter**.
2. Select option 1, **Log in with full access**. We recommend that you install the hotfix on the passive controller first.
3. To install the hotfix, at the command prompt, type:

```
Start-HcsHotfix -Path <path to update file> -Credential <credentials in  
domain\username format>
```

Use IP rather than DNS in share path in the above command. The credential parameter is used only if you are accessing an authenticated share.

We recommend that you use the credential parameter to access shares. Even shares that are open to “everyone” are typically not open to unauthenticated users.

Supply the password when prompted.

A sample output for installing the first order updates is shown below. For the first order update, you need to point to the specific file.

Output

```
Controller0>Start-HcsHotfix -Path \\10.100.100.100\share  
\FirstOrderUpdate\HcsSoftwareUpdate.exe -Credential contoso\John
```

Confirm

This operation starts the hotfix installation and could reboot one or both of the controllers. If the device is serving I/Os, these will not be disrupted. Are you sure you want to continue?

[Y] Yes [N] No [?] Help (default is "Y"): Y

4. Type **Y** when prompted to confirm the hotfix installation.
5. Monitor the update by using the `Get-HcsUpdateStatus` cmdlet. The update will first complete on the passive controller. Once the passive controller is updated, there will be a failover and the update will then get applied on the other controller. The update is complete when both the controllers are updated.

The following sample output shows the update in progress. The `RunInprogress` will be `True` when the update is in progress.

```
Controller0>Get-HcsUpdateStatus  
RunInprogress      : True  
LastHotfixTimestamp :  
LastUpdateTimestamp : 02/03/2017 2:04:02 AM  
Controller0Events   :  
Controller1Events   :
```

The following sample output indicates that the update is finished. The `RunInProgress` will be `False` when the update has completed.

```
Controller0>Get-HcsUpdateStatus  
RunInprogress      : False  
LastHotfixTimestamp : 02/03/2017 9:15:55 AM  
LastUpdateTimestamp : 02/03/2017 9:06:07 AM  
Controller0Events   :  
Controller1Events   :
```

ⓘ Note

Occasionally, the cmdlet reports `False` when the update is still in progress. To ensure that the hotfix is complete, wait for a few minutes, rerun this command and verify that the `RunInProgress` is `False`. If it is, then the hotfix has completed.

6. After the software update is complete, verify the system software versions. Type:

```
Get-HcsSystem
```

You should see the following versions:

- `FriendlySoftwareVersion: StorSimple 8000 Series Update 4.0`
- `HcsSoftwareVersion: 6.3.9600.17820`

If the version number does not change after applying the update, it indicates that the hotfix has failed to apply. Should you see this, please contact [Microsoft Support](#) for further assistance.

Important

You must restart the active controller via the `Restart-HcsController` cmdlet before applying the next update.

7. Repeat steps 3-5 to install the Cis/MDS agent downloaded to your *FirstOrderUpdate* folder.

8. Repeat steps 3-5 to install the second order updates. **For second order updates, multiple updates can be installed by just running the `Start-HcsHotfix` cmdlet and pointing to the folder where second order updates are located. The cmdlet will execute all the updates available in the folder.** If an update is already installed, the update logic will detect that and not apply that update.

After all the hotfixes are installed, use the `Get-HcsSystem` cmdlet. The versions should be:

- `CisAgentVersion: 1.0.9441.0`
- `MdsAgentVersion: 35.2.2.0`
- `Lsisas2Version: 2.0.78.00`

To install and verify maintenance mode hotfixes

Use KB4011837 to install disk firmware updates. These are disruptive updates and take around 30 minutes to complete. You can choose to install these in a planned maintenance window by connecting to the device serial console.

Note that if your disk firmware is already up-to-date, you won't need to install these updates. Run the `Get-HcsUpdateAvailability` cmdlet from the device serial console to check if updates are available and whether the updates are disruptive (maintenance mode) or non-disruptive (regular mode) updates.

To install the disk firmware updates, follow the instructions below.

1. Place the device in the maintenance mode. **Note that you should not use Windows PowerShell remoting when connecting to a device in maintenance mode. Instead run this cmdlet on the device controller when connected through the device serial console.** Type:

```
Enter-HcsMaintenanceMode
```

A sample output is shown below.

```
Output

Controller0>Enter-HcsMaintenanceMode
Checking device state...

In maintenance mode, your device will not service IOs and will be
disconnected from the Microsoft Azure StorSimple Manager service.
Entering maintenance mode will end the current session and reboot both
controllers, which takes a few minutes to complete. Are you sure you
want to enter maintenance mode?
[Y] Yes [N] No (Default is "Y"): Y

-----MAINTENANCE MODE-----
Microsoft Azure StorSimple Appliance Model 8600
Name: Update4-8600-mystorsimple
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
You are connected to Controller0 - Passive
-----

Serial Console Menu
[1] Log in with full access
[2] Log into peer controller with full access
[3] Connect with limited access
[4] Change language
Please enter your choice>
```

Both the controllers then restart into maintenance mode.

2. To install the disk firmware update, type:

```
Start-HcsHotfix -Path <path to update file> -Credential <credentials in  
domain\username format>
```

A sample output is shown below.

Output

```
Controller1>Start-HcsHotfix -Path  
\\"10.100.100.100\\share\\ThirdOrderUpdates\\ -Credential contoso\\john  
Enter Password:  
WARNING: In maintenance mode, hotfixes should be installed on each  
controller sequentially. After the hotfix is installed on this  
controller, install it on the peer controller.  
Confirm  
This operation starts a hotfix installation and could reboot one or  
both of the controllers. By installing new updates you agree to, and  
accept any additional terms associated with, the new functionality  
listed in the release notes (https://go.microsoft.com/fwlink/?LinkID=613790). Are you sure you want to continue?  
[Y] Yes [N] No (Default is "Y"): Y  
WARNING: Installation is currently in progress. This operation can take  
several minutes to complete.
```

3. Monitor the install progress using `Get-HcsUpdateStatus` command. The update is complete when the `RunInProgress` changes to `False`.
4. After the installation is complete, the controller on which the maintenance mode hotfix was installed restarts. Sign in as option 1, **Log in with full access**, and verify the disk firmware version. Type:

```
Get-HcsFirmwareVersion
```

The expected disk firmware versions are:

```
XMGJ, XGEG, KZ50, F6C2, VR08, N002, 0106
```

A sample output is shown below.

Output

```
-----MAINTENANCE MODE-----  
Microsoft Azure StorSimple Appliance Model 8600  
Name: Update4-8600-mystorsimple  
Software Version: 6.3.9600.17820  
Copyright (C) 2014 Microsoft Corporation. All rights reserved.  
You are connected to Controller1  
-----
```

```
Controller1>Get-HcsFirmwareVersion
```

Controller0 : TalladegaFirmware
ActiveBIOS:0.45.0010
BackupBIOS:0.45.0006
MainCPLD:17.0.000b
ActiveBMCRoot:2.0.001F
BackupBMCRoot:2.0.001F
BMCCBoot:2.0.0002
LsiFirmware:20.00.04.00
LsiBios:07.37.00.00
Battery1Firmware:06.2C
Battery2Firmware:06.2C
DomFirmware:X231600
CanisterFirmware:3.5.0.56
CanisterBootloader:5.03
CanisterConfigCRC:0x9134777A
CanisterVPDStructure:0x06
CanisterGEMCPLD:0x19
CanisterVPDCRC:0x142F7DC2
MidplaneVPDStructure:0x0C
MidplaneVPDCRC:0xA6BD4F64
MidplaneCPLD:0x10
PCM1Firmware:1.00|1.05
PCM1VPDStructure:0x05
PCM1VPDCRC:0x41BEF99C
PCM2Firmware:1.00|1.05
PCM2VPDStructure:0x05
PCM2VPDCRC:0x41BEF99C

EbodFirmware
CanisterFirmware:3.5.0.56
CanisterBootloader:5.03
CanisterConfigCRC:0xB23150F8
CanisterVPDStructure:0x06
CanisterGEMCPLD:0x14
CanisterVPDCRC:0xBAE55828
MidplaneVPDStructure:0x0C
MidplaneVPDCRC:0xA6BD4F64
MidplaneCPLD:0x10
PCM1Firmware:3.11
PCM1VPDStructure:0x03
PCM1VPDCRC:0x6B58AD13
PCM2Firmware:3.11
PCM2VPDStructure:0x03
PCM2VPDCRC:0x6B58AD13

DisksFirmware
SmrtStor:TXA2D20800GA6XYR:KZ50
SmrtStor:TXA2D20800GA6XYR:KZ50
SmrtStor:TXA2D20800GA6XYR:KZ50
SmrtStor:TXA2D20800GA6XYR:KZ50
SmrtStor:TXA2D20800GA6XYR:KZ50
WD:WD4001FYYG-01SL3:VR08
WD:WD4001FYYG-01SL3:VR08
WD:WD4001FYYG-01SL3:VR08

```
WD:WD4001FYYG-01SL3:VR08  
WD:WD4001FYYG-01SL3:VR08
```

Run the `Get-HcsFirmwareVersion` command on the second controller to verify that the software version has been updated. You can then exit the maintenance mode. To do so, type the following command for each device controller:

```
Exit-HcsMaintenanceMode
```

5. The controllers restart when you exit maintenance mode. After the disk firmware updates are successfully applied and the device has exited maintenance mode, return to the Azure classic portal. Note that the portal might not show that you installed the maintenance mode updates for 24 hours.

Troubleshooting update failures

What if you see a notification that the pre-upgrade checks have failed?

If a pre-check fails, make sure that you have looked at the detailed notification bar at the bottom of the page. This provides guidance as to which pre-check has failed. The following illustration shows an instance in which such a notification appears. In this case, the controller health check and hardware component health check have failed. Under the **Hardware Status** section, you can see that both **Controller 0** and **Controller 1** components need attention.

The screenshot shows the Microsoft Azure StorSimple device management interface. On the left is a vertical toolbar with various icons. The main area displays the device details for '8100-shx0991003g00b4 (Device)'. Under the 'CONTROLLERS' section, there are two entries: 'Controller 0' (Passive) and 'Controller 1' (Active). The 'hardware status' section shows three components under 'COMPONENTS': 'SHARED COMPONENTS' (Healthy), 'CONTROLLER 0 COMPONENTS' (Needs Attention), and 'CONTROLLER 1 COMPONENTS' (Needs Attention). A message at the bottom indicates 'Pre-upgrade checks failed' with two error items: 'Controller health check Failed' and 'Hardware component health check Failed'. The 'software updates' section includes a 'CREATE AND UPLOAD SUPPORT PACKAGE' button. At the bottom, there are 'NEW', 'INSTALL UPDATES', and help icons.

You will need to make sure that both controllers are healthy and online. You will also need to make sure that all the hardware components in the StorSimple device are shown to be healthy on the Maintenance page. You can then try to install updates. If you are not able to fix the hardware component issues, then you will need to contact Microsoft Support for next steps.

What if you receive a "Could not install updates" error message, and the recommendation is to refer to the update troubleshooting guide to determine the cause of the failure?

One likely cause for this could be that you do not have connectivity to the Microsoft Update servers. This is a manual check that needs to be performed. If you lose connectivity to the update server, your update job would fail. You can check the connectivity by running the following cmdlet from the Windows PowerShell interface of your StorSimple device:

```
Test-Connection -Source <Fixed IP of your device controller> -Destination <Any IP or computer name outside of datacenter>
```

Run the cmdlet on both controllers.

If you have verified the connectivity exists, and you continue to see this issue, please contact Microsoft Support for next steps.

What if you see an update failure when updating your device to Update 4 and both the controllers are running Update 4?

Starting Update 4, if both the controllers are running the same software version and if there is an update failure, the controllers do not go into recovery mode. This situation can arise if the device software hotfix (1st order update) is applied to both the controllers successfully but other hotfixes (2nd order and 3rd order) are yet to be applied. Starting Update 4, the controllers will go into recovery mode only if the two controllers are running different software versions.

If the user sees an update failure when both controllers are running Update 4, we recommend that they wait a few minutes and then retry updating. If the retry does not succeed, then they should contact Microsoft Support.

Next steps

Learn more about the [Update 4 release](#).

StorSimple 8000 Series Update 5.2 release notes

Article • 09/27/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe new features and identify critical open issues for StorSimple 8000 Series Update 5.2. They also contain a list of the StorSimple software updates included in this release.

The release notes are continuously updated. As critical issues are discovered, they're added to the update. Before you deploy StorSimple 8000 Series, carefully review the information contained in these release notes.

Update 5.2 corresponds to software version 6.3.9600.17886.

ⓘ Important

- Update 5.2 is a mandatory security update. It must be installed immediately to ensure the operation of the device. Microsoft implements a phased rollout, so your new release might not detect all available updates. To ensure a complete update to 5.2, wait a few days and then scan for updates again.
- If you're not notified about Update 5.2 via a banner in the Azure portal UI, contact Microsoft Support.

What's new in Update 5.2

- **Automatic remediation for failed backups caused by a device controller left active for long periods.** When a device controller is continuously active for a long period (more than a year), scheduled and manually triggered backups may fail. No alert or other notification is raised in the Azure portal. The only way to recover is to initiate a controller failover. Update 5.2 detects this condition and remediates it by initiating a controller failover. An alert informs the customer.
- **Reliability issue fixed in backup code path** without which a backup could be corrupted in a rare scenario.
- **Issue with Local Only volume conversion fixed.** In earlier releases, Local Only volume conversion might get stuck if the system restarts at a specific window of the conversion.
- **SHA 256 hashing algorithm is supported for the remote management certificate.** Remote management certificates are used while connecting to the PowerShell interface of the appliance, or during a Support session using remote PowerShell over Single Sockets Layer (SSL). Earlier releases use an SHA 128 hashing algorithm, which is considered weak. Update 5.2 uses SHA 256, which is considered more secure.

Install Update 5.2

Use the following steps to install Update 5.2:

1. [Connect to Windows PowerShell on the StorSimple 8000 series device](#), or connect directly to the appliance via serial cable.
2. Use [Start-HcsUpdate](#) to update the device. For detailed steps, see [Install regular updates via Windows PowerShell](#). This update is non-disruptive.
3. If `Start-HcsUpdate` doesn't work because of firewall issues, contact Microsoft Support.

Verify the updates

To verify Update 5.2, check for these software versions after installation:

- FriendlySoftwareVersion: StorSimple 8000 Series Update 5.2
- HcsSoftwareVersion: 6.3.9600.17886
- CisAgentVersion: 1.0.9777.0
- MdsAgentVersion: 35.2.2.0

- Lsisas2Version: 2.0.78.00

Next steps

Install StorSimple 8000 Series Update 5.2. Steps to install Update 5.2 are largely the same as for installation of Update 5.1. For more information, see detailed steps in [Installing via the hotfix method](#).

StorSimple 8000 Series Update 5.1 release notes

Article • 08/22/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 5.1. They also contain a list of the StorSimple software updates included in this release.

Update 5.1 can be applied to any StorSimple device running Update 5. If you're are using a version lower than 5, apply Update 5 first, and then apply Update 5.1. The device version associated with Update 5.1 is 6.3.9600.17885.

Review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- Update 5.1 is a mandatory update and must be installed immediately to ensure the operation of the device. Update 5.0 is a minimally supported version.
- Update 5.1 has security updates that take about 30 minutes to install. For more information, see how to [Apply Update 5.1](#).

What's new in Update 5.1

The following key improvements and bug fixes have been made in Update 5.1:

- **TLS 1.2** - This StorSimple update will enforce TLS 1.2 on all clients. TLS 1.2 is a mandatory update for all StorSimple 8000 series devices.

If you see the following warning, you must update the software on the device before proceeding:

One or more StorSimple devices are running an older software version. The latest available update for TLS 1.2 is a mandatory update and should be installed immediately on these devices. TLS 1.2 is used for all Azure portal communication and without this update, the device won't be able to communicate with the StorSimple service.

Known issues in Update 5.1 from previous releases

There are no new known issues in Update 5.1. For a list of issues carried over to Update 5.1 from previous releases, go to [Update 3 release notes](#).

StorSimple Cloud Appliance updates in Update 5.1

This update cannot be applied to the StorSimple Cloud Appliance (also known as the virtual device). You will need to create new cloud appliances using the Update 5.1 image. For information on how to create a StorSimple Cloud Appliance, go to [Deploy and manage a StorSimple Cloud Appliance](#).

Next step

Learn how to [install Update 5.1](#) on your StorSimple device.

StorSimple 8000 Series Update 5 release notes

Article • 08/22/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 5. They also contain a list of the StorSimple software updates included in this release.

Update 5 can be applied to any StorSimple device running Update 0.1 through Update 4. The device version associated with Update 5 is 6.3.9600.17845.

Review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- Update 5 is a mandatory update and must be installed immediately. For more information, see how to [Apply Update 5](#).
- Update 5 has device software, disk firmware, OS security, and other OS updates. It takes approximately 4 hours to install this update. Disk firmware update is a disruptive update and results in a downtime for your device. We recommend that you apply Update 5 to keep your device up-to-date.
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Wait a few days, and then scan for updates again as these updates will become available soon.

What's new in Update 5

The following key improvements and bug fixes have been made in Update 5.

- **Use of Azure Active Directory (AAD) to authenticate with StorSimple Device Manager service** – From Update 5 onwards, Azure Active Directory is used to authenticate with the StorSimple Device Manager service. The old authentication mechanism will be deprecated by December 2017. All the users must include the new authentication URLs in their firewall rules. For more information, go to [authentication URLs listed in the networking requirements for your StorSimple device](#).

If the authentication URL is not included in the firewall rules, the users will see a critical alert that their StorSimple device could not authenticate with the service. If the users see this alert, they need to include the new authentication URL. For more information, go to [StorSimple networking alerts](#).

- **New version of StorSimple Snapshot Manager** - A new version of StorSimple Snapshot Manager is released with Update 5 and is compatible with all the StorSimple devices that are running Update 4 or later. We recommend that you update to this version. The previous version of StorSimple Snapshot Manager is used for StorSimple devices that are running Update 3 or earlier. [Download the appropriate version of StorSimple Snapshot Manager](#) and refer to [deploy StorSimple Snapshot Manager](#).

Issues fixed in Update 5

The following table provides a summary of issues that were fixed in Update 5.

No	Feature	Issue	Applies to physical device	Applies to virtual device
1	Windows PowerShell remoting	In the previous release, a user would receive an error while trying to establish a remote connection to the StorSimple Cloud Appliance via Windows PowerShell. This issue was root-caused and fixed in this release.	No	Yes
2	Bandwidth templates	In earlier release, there was an issue with bandwidth templates that resulted in lower bandwidth than what the device was configured for. This issue is resolved in this release.	Yes	Yes

No	Feature	Issue	Applies to physical device	Applies to virtual device
3	Failover	In previous release, when a device with a large number of volumes was failed over to another device running Update 4, the process would fail when trying to apply the access control records. This issue is fixed in this release.	Yes	Yes

Known issues in Update 5 from previous releases

There are no new known issues in Update 5. For a list of issues carried over to Update 5 from previous releases, go to [Update 3 release notes](#).

Serial-attached SCSI (SAS) controller and firmware updates in Update 5

This release has SAS controller and LSI driver and firmware updates. For more information on how to install these updates, see [install Update 5](#) on your StorSimple device.

StorSimple Cloud Appliance updates in Update 5

This update cannot be applied to the StorSimple Cloud Appliance (also known as the virtual device). New cloud appliances need to be created using the Update 5 image. For information on how to create a StorSimple Cloud Appliance, go to [Deploy and manage a StorSimple Cloud Appliance](#).

Next step

Learn how to [install Update 5](#) on your StorSimple device.

StorSimple 8000 Series Update 4 release notes

Article • 08/22/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 4. They also contain a list of the StorSimple software updates included in this release.

Update 4 can be applied to any StorSimple device running Release (GA) or Update 0.1 through Update 3.1. The device version associated with Update 4 is 6.3.9600.17820.

Please review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- Update 4 has device software, USM firmware, LSI driver and firmware, disk firmware, Storport and Spaceport, security, and other OS updates. It takes approximately 4 hours to install this update. Disk firmware update is a disruptive update and results in a downtime for your device. We recommend that you apply Update 4 to keep your device up-to-date.
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Wait a few days, and then scan for updates again as these will become available soon.

What's new in Update 4

The following key improvements and bug fixes have been made in Update 4.

- **Smarter automated space reclamation algorithms** – In Update 4, the automated space reclamation algorithms are enhanced to adjust the space reclamation cycles based on the expected reclaimed space available in the cloud.
- **Performance enhancements for locally pinned volumes** – Update 4 has improved the performance of locally pinned volumes in scenarios that have high data ingestion (data comparable to volume size).
- **Heatmap-based restore** - In the earlier releases, following a disaster recovery (DR), the data was restored from the cloud based on the access patterns resulting in a slow performance.

A new feature is implemented in Update 4 that tracks frequently accessed data to create a heatmap when the device is in use prior to DR (Most used data chunks have high heat whereas less used chunks have low heat). After DR, StorSimple uses the heatmap to automatically restore and rehydrate the data from the cloud.

All the restores are now heatmap based restores. For more information on how to query and cancel heatmap based restore and rehydration jobs, go to [Windows PowerShell for StorSimple cmdlet reference](#).

- **StorSimple Diagnostics tool** – In Update 4, a StorSimple Diagnostics tool is being released to allow for easy diagnosing and troubleshooting of issues related to system, network, performance, and hardware component health. This tool is run via the Windows PowerShell for StorSimple. For more information, go to [troubleshoot using StorSimple Diagnostics tool](#).
- **UI-based StorSimple Migration tool** - Prior to this release, migration of data from 5000-7000 series required the users to execute a part of the migration workflow using the Azure PowerShell interface. In this release, an easy-to-use UI-based StorSimple Migration tool is made available for Support to facilitate the same migration workflow. This tool would also allow for the consolidation of recovery buckets.
- **FIPS-related changes** - This release onwards, FIPS is enabled by default on all the StorSimple 8000 series devices for both the Microsoft Azure Government and Azure public cloud accounts.
- **Update changes** - In this release, bugs related to update failures have been fixed.

- **Alert for disk failures** - A new alert that warns the user of impending disk failures is added in this release. If you encounter this alert, contact Microsoft Support to ship a replacement disk. For more information, go to [hardware alerts on your StorSimple device](#).
- **Controller replacement changes** - A cmdlet that allows the user to query the status of the controller replacement process is added in this release. For more information, go to the [cmdlet to query controller replacement status](#).

Issues fixed in Update 4

The following table provides a summary of issues that were fixed in Update 4.

No	Feature	Issue	Applies to physical device	Applies to virtual device
1	Failover	In the earlier release, after the failover, there was an issue related to cleanup observed at the customer site. This issue is fixed in this release.	Yes	Yes
2	Locally pinned volumes	In the previous release, there was an issue related to volume creation for locally pinned volumes that would result in volume creation failures. This issue was root-caused and fixed in this release.	Yes	No
3	Support package	In previous release, there were issues related to Support package that would result in a System.OutOfMemory exception or other errors resulting in a Support package creation failure. These bugs are fixed in this release.	Yes	Yes
4	Monitoring	In previous release, there was an issue related to monitoring charts for locally pinned volumes where consumption was shown in EB. This bug is resolved in this release.	Yes	Yes
5	Migration	In previous release, there were several issues related to the reliability of migration from 5000-7000 series to 8000 series devices. These issues have been addressed in this release.	Yes	Yes

No	Feature	Issue	Applies to physical device	Applies to virtual device
6	Update	<p>In previous releases, if there was an update failure, the controllers would go into recovery mode and hence the user could not proceed with the update and would need to contact Microsoft Support.</p> <p>This behavior was changed in this release. If the user has an update failure after both the controllers are running the same version (Update 4), the controllers do not go into recovery mode. If the user encounters this failure, we recommend that they wait for a bit and then retry the update. The retry could succeed. If the retry fails, then they should contact Microsoft Support.</p>	Yes	Yes

Known issues in Update 4 from previous releases

There are no new known issues in Update 4. For a list of issues carried over to Update 4 from previous releases, go to [Update 3 release notes](#).

Serial-attached SCSI (SAS) controller and firmware updates in Update 4

This release has SAS controller and LSI driver and firmware updates. For more information on how to install these updates, see [Install Update 4](#) on your StorSimple device.

Virtual device updates in Update 4

This update cannot be applied to the StorSimple Cloud Appliance (also known as the virtual device). New virtual devices will need to be created.

Next step

Learn how to [Install Update 4](#) on your StorSimple device.

Update 3 release notes for your StorSimple 8000 series device

Article • 08/22/2022 • 9 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 3. They also contain a list of the StorSimple software updates included in this release.

Update 3 can be applied to any StorSimple device running Release (GA) or Update 0.1 through Update 2.2. The device version associated with Update 3 is 6.3.9600.17759.

Please review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- Update 3 has device software, LSI driver and firmware, and Storport and Spaceport updates. It takes approximately 1.5-2 hours to install this update.
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Wait a few days, and then scan for updates again as these will become available soon.

What's new in Update 3

The following key improvements and bug fixes have been made in Update 3.

- **Automated space reclamation changes** – Starting Update 3, the space reclamation algorithms run on the standby controller of the system resulting in faster execution. For more information on the ports that are required to work with space reclamation, refer to the [StorSimple networking requirements](#).
- **Performance enhancements** – Update 3 has improved read-write performance to the cloud.
- **Migration-related improvements** – In this release, several bug fixes and improvements were done for the Migration feature from 5000/7000 series devices to 8000 series devices. For more information on how to use the migration feature, go to [Migration from 5000/7000 series device to 8000 series device](#).
- **Monitoring related fixes** - In this release, bugs related to monitoring charts, service dashboard, and device dashboard were fixed.

Issues fixed in Update 3

The following tables provides a summary of issues that were fixed in Update 3.

No	Feature	Issue	Applies to physical device	Applies to virtual device
1	Host-side data migration	In the earlier release, the StorSimple Cloud Appliance was going offline during a host-side data migration. This issue is fixed in this release.	No	Yes
2	Locally pinned volumes	In the previous release, there were issues related to I/O failures, volume conversion failures, and datapath failures for locally pinned volumes. These issues were root-caused and fixed in this release.	Yes	No
3	Monitoring	There were multiple issues related to reporting units and monitoring as well as device dashboard charts where incorrect information was displayed for locally pinned volumes. These issues are fixed in this release.	Yes	No
4	Heavy writes I/O	When using StorSimple for workloads involving heavy writes, the user would run into an infrequent bug where the working set was being tiered into the cloud. This bug is fixed in this release.	Yes	Yes
5	Backup	In certain rare instances, in the previous versions of software, when user took a backup of a remote clone, they would run into cloud errors and the operation would error out. In this release, the issue is fixed and the operation completes successfully.	Yes	Yes
6	Backup policy	In certain rare instances, in the earlier releases of software, there was a bug related to the deletion of backup policy. This issue is fixed in this release.	Yes	Yes

Known issues in Update 3

The following table provides a summary of known issues in this release.

No.	Feature	Issue	Comments / workaround	Applies to physical device	Applies to virtual device
1	Disk quorum	In rare instances, if the majority of disks in the EBOD enclosure of an 8600 device are disconnected resulting in no disk quorum, then the storage pool will go offline. It will stay offline even if the disks are reconnected.	You will need to reboot the device. If the issue persists, please contact Microsoft Support for next steps.	Yes	No
2	Incorrect controller ID	When a controller replacement is performed, controller 0 may show up as controller 1. During controller replacement, when the image is loaded from the peer node, the controller ID can show up initially as the peer controller's ID. In rare instances, this behavior may also be seen after a system reboot.	No user action is required. This situation will resolve itself after the controller replacement is complete.	Yes	No

No.	Feature	Issue	Comments / workaround	Applies to physical device	Applies to virtual device
3	Storage accounts	Using the Storage service to delete the storage account is an unsupported scenario. This will lead to a situation in which user data cannot be retrieved.		Yes	Yes
4	Device failover	Multiple failovers of a volume container from the same source device to different target devices is not supported. Failover from a single dead device to multiple devices will make the volume containers on the first failed over device lose data ownership. After such a failover, these volume containers will appear or behave differently when you view them in the Azure classic portal.		Yes	No
5	Installation	During StorSimple Adapter for SharePoint installation, you need to provide a device IP in order for the install to finish successfully.		Yes	No
6	Web proxy	If your web proxy configuration has HTTPS as the specified protocol, then your device-to-service communication will be affected and the device will go offline. Support packages will also be generated in the process, consuming significant resources on your device.	Make sure that the web proxy URL has HTTP as the specified protocol. For more information, go to Configure web proxy for your device .	Yes	No
7	Web proxy	If you configure and enable web proxy on a registered device, then you will need to restart the active controller on your device.		Yes	No
8	High cloud latency and high I/O workload	When your StorSimple device encounters a combination of very high cloud latencies (order of seconds) and high I/O workload, the device volumes go into a degraded state and the I/Os may fail with a "device not ready" error.	You will need to manually reboot the device controllers or perform a device failover to recover from this situation.	Yes	No
9	Azure PowerShell	When you use the StorSimple cmdlet <code>Get-AzureStorSimpleStorageAccountCredential</code> <code>Select-Object -First 1 -Wait</code> to select the first object so that you can create a new <code>VolumeContainer</code> object, the cmdlet returns all the objects.	Wrap the cmdlet in parentheses as follows: <code>(Get-AzureStorSimpleStorageAccountCredential)</code> <code>Select-Object -First 1 -Wait</code>	Yes	Yes
10	Migration	When multiple volume containers are passed for migration, the ETA for latest backup is accurate only for the first volume container. Additionally, parallel migration will start after the first 4 backups in the first volume container are migrated.	We recommend that you migrate one volume container at a time.	Yes	No

No.	Feature	Issue	Comments / workaround	Applies to physical device	Applies to virtual device
11	Migration	After the restore, volumes are not added to the backup policy or the virtual disk group.	You will need to add these volumes to a backup policy in order to create backups.	Yes	Yes
12	Migration	After the migration is complete, the 5000/7000 series device must not access the migrated data containers.	We recommend that you delete the migrated data containers after the migration is complete and committed.	Yes	No
13	Clone and DR	A StorSimple device running Update 1 cannot clone or perform disaster recovery to a device running pre-update 1 software.	You will need to update the target device to Update 1 to allow these operations	Yes	Yes
14	Migration	Configuration backup for migration may fail on a 5000-7000 series device when there are volume groups with no associated volumes.	Delete all the empty volume groups with no associated volumes and then retry the configuration backup.	Yes	No
15	Azure PowerShell cmdlets and locally pinned volumes	You cannot create a locally pinned volume via Azure PowerShell cmdlets. (Any volume you create via Azure PowerShell will be tiered.)	Always use the StorSimple Manager service to configure locally pinned volumes.	Yes	No
16	Space available for locally pinned volumes	If you delete a locally pinned volume, the space available for new volumes may not be updated immediately. The StorSimple Manager service updates the local space available approximately every hour.	Wait for an hour before you try to create the new volume.	Yes	No
17	Locally pinned volumes	Your restore job exposes the temporary snapshot backup in the Backup Catalog, but only for the duration of the restore job. Additionally, it exposes a virtual disk group with prefix tmpCollection on the Backup Policies page, but only for the duration of the restore job.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No
18	Locally pinned volumes	If you cancel a restore job and a controller failover occurs immediately afterwards, the restore job will show Failed instead of Canceled . If a restore job fails and a controller failover occurs immediately afterwards, the restore job will show Canceled instead of Failed .	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No
19	Locally pinned volumes	If you cancel a restore job or if a restore fails and then a controller failover occurs, an additional restore job appears on the Jobs page.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No

No.	Feature	Issue	Comments / workaround	Applies to physical device	Applies to virtual device
20	Locally pinned volumes	If you try to convert a tiered volume (created and cloned with Update 1.2 or earlier) to a locally pinned volume and your device is running out of space or there is a cloud outage, then the clone(s) can be corrupted.	This problem occurs only with volumes that were created and cloned with pre-Update 2.1 software. This should be an infrequent scenario.		
21	Volume conversion	Do not update the ACRs attached to a volume while a volume conversion is in progress (tiered to locally pinned or vice versa). Updating the ACRs could result in data corruption.	If needed, update the ACRs prior to the volume conversion and do not make any further ACR updates while the conversion is in progress.		
22	Updates	When applying Update 3, the Maintenance page in the Azure classic portal will display the following message related to Update 2 - "StorSimple 8000 series Update 2 includes the ability for Microsoft to proactively collect log information from your device when we detect potential problems". This is misleading as it indicates that the device is being updated to Update 2. After the device is successfully updated to Update 3, this message will disappear.	This behavior will be fixed in a future release.	Yes	No

Controller and firmware updates in Update 3

This release has LSI driver and firmware updates. For more information on how to install the LSI driver and firmware updates, see [Install Update 3](#) on your StorSimple device.

Virtual device updates in Update 3

This update cannot be applied to the StorSimple Cloud Appliance (also known as the virtual device). New virtual devices will need to be created.

Next step

Learn how to [install Update 3](#) on your StorSimple device.

StorSimple 8000 Series Update 2.2 release notes

Article • 08/23/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 2.2. They also contain a list of the StorSimple software updates included in this release.

Update 2.2 can be applied to any StorSimple device running Release (GA) or Update 0.1 through Update 2.1. The device version associated with Update 2.2 is 6.3.9600.17708.

Review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- Update 2.2 has software only updates. It takes approximately 1.5-2 hours to install this update.
- If you are running Update 2.1, we recommend that you apply Update 2.2 as soon as possible.
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Wait a few days, and then scan for updates again as these will become available soon.

What's new in Update 2.2

The following key improvements have been made in Update 2.2.

- **Automated space reclamation optimization** – When data is deleted on thinly provisioned volumes, the unused storage blocks need to be reclaimed. This release has improved the space reclamation process from the cloud resulting in the unused space becoming available faster as compared to the previous versions.
- **Snapshot performance enhancements** – Update 2.2 has improved the time to process a cloud snapshot in certain scenarios where large volumes are being used and there's minimal to no data churn. A scenario that would benefit from this enhancement would be the archive volumes.
- **Hardening of Support package gathering** – There have been improvements in the way the Support package is gathered and uploaded in this release.
- **Update reliability improvements** – This release has bug fixes that result in an improved Update reliability.

Issues fixed in Update 2.2

The following table provides a summary of issues that were fixed in Updates 2.2 and 2.1.

No	Feature	Issue	Applies to physical device	Applies to virtual device
1	Host performance	In the earlier release, host-side performance issues were observed during the creation of a locally pinned volume and during the conversion of a tiered volume to a locally pinned volume. These issues are fixed in this release thereby resulting in an improvement in the host performance during the volume creation and conversion procedures.	Yes	No
2	Locally pinned volumes	In rare instances, the system would crash when creating a locally pinned volume. This bug has been fixed in this release.	Yes	No
3	Tiering	There were sporadic crashes when the metadata for the StorSimple Cloud Appliances (8010 and 8020) tiered to the cloud. This issue is fixed in this release.	No	Yes
4	Snapshot creation	There were issues related to the creation of incremental snapshots in scenarios with large volumes and minimal to no data churn. These issues are fixed in this release.	Yes	Yes
5	Openstack authentication	When using Openstack as the cloud service provider, the user would run into an infrequent bug related to the authentication where the JSON parser resulted in a crash. This bug is fixed in this release.	Yes	No
6	Host-side copy	In earlier versions of software, an infrequent bug related to the ODX timing was seen when copying the data from one volume to another volume. This would result in a controller failover and the system could potentially go into Recovery mode. This bug is fixed in this release.	Yes	No
7	Windows Management Instrumentation (WMI)	In the previous versions of software, there were several instances of web proxy failure with the exception "<ManagementException> Provider load failure". This bug was attributed to a WMI memory leak and is now fixed.	Yes	No
8	Update	In certain rare instances, in the previous versions of software, the user received a "C:\Windows\Temp\PowerShellHcsscripterror" when trying to scan or install updates. This issue is fixed in this release.	Yes	Yes
9	Support package	In this release, there have been improvements to the way the Support package is gathered and uploaded.	Yes	Yes

Known issues in Update 2.2

The following table provides a summary of known issues in this release.

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
1	Disk quorum	In rare instances, if most disks in the EBOD enclosure of an 8600 device are disconnected resulting in no disk quorum, then the storage pool will go offline. It will stay offline even if the disks are reconnected.	You'll need to reboot the device. If the issue persists, please contact Microsoft Support for next steps.	Yes	No
2	Incorrect controller ID	When a controller replacement is performed, controller 0 may show up as controller 1. During controller replacement, when the image is loaded from the peer node, the controller ID can show up initially as the peer controller's ID. In rare instances, this behavior may also be seen after a system reboot.	No user action is required. This situation will resolve itself after the controller replacement is complete.	Yes	No
3	Storage accounts	Using the Storage service to delete the storage account is an unsupported scenario. This will lead to a situation in which user data can't be retrieved.		Yes	Yes
4	Device failover	Multiple failovers of a volume container from the same source device to different target devices isn't supported. Failover from a single dead device to multiple devices will make the volume containers on the first failed over device lose data ownership. After such a failover, these volume containers will appear or behave differently when you view them in the Azure classic portal.		Yes	No
5	Installation	During StorSimple Adapter for SharePoint installation, you need to provide a device IP in order for the install to finish successfully.		Yes	No
6	Web proxy	If your web proxy configuration has HTTPS as the specified protocol, then your device-to-service communication will be affected and the device will go offline. Support packages will also be generated in the process, consuming significant resources on your device.	Make sure that the web proxy URL has HTTP as the specified protocol. For more information, go to Configure web proxy for your device .	Yes	No
7	Web proxy	If you configure and enable web proxy on a registered device, then you'll need to restart the active controller on your device.		Yes	No
8	High cloud latency and high I/O workload	When your StorSimple device encounters a combination of high cloud latencies (order of seconds) and high I/O workload, the device volumes go into a degraded state, and the I/Os may fail with a "device not ready" error.	You'll need to manually reboot the device controllers or perform a device failover to recover from this situation.	Yes	No

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
9	Azure PowerShell	When you use the StorSimple cmdlet <code>Get-AzureStorSimpleStorageAccountCredential</code> <code>Select-Object -First 1 -Wait</code> to select the first object so that you can create a new <code>VolumeContainer</code> object, the cmdlet returns all the objects.	Wrap the cmdlet in parentheses as follows: <code>(Get-AzureStorSimpleStorageAccountCredential)</code> <code>Select-Object -First 1 -Wait</code>	Yes	Yes
10	Migration	When multiple volume containers are passed for migration, the ETA for latest backup is accurate only for the first volume container. Additionally, parallel migration will start after the first four backups in the first volume container are migrated.	We recommend that you migrate one volume container at a time.	Yes	No
11	Migration	After the restore, volumes aren't added to the backup policy or the virtual disk group.	You'll need to add these volumes to a backup policy in order to create backups.	Yes	Yes
12	Migration	After the migration is complete, the 5000/7000 series device must not access the migrated data containers.	We recommend that you delete the migrated data containers after the migration is complete and committed.	Yes	No
13	Clone and DR	A StorSimple device running Update 1 can't clone or perform disaster recovery to a device running pre-update 1 software.	You'll need to update the target device to Update 1 to allow these operations	Yes	Yes
14	Migration	Configuration backup for migration may fail on a 5000-7000 series device when there are volume groups with no associated volumes.	Delete all the empty volume groups with no associated volumes and then retry the configuration backup.	Yes	No
15	Azure PowerShell cmdlets and locally pinned volumes	You can't create a locally pinned volume via Azure PowerShell cmdlets. (Any volume you create via Azure PowerShell will be tiered.)	Always use the StorSimple Manager service to configure locally pinned volumes.	Yes	No
16	Space available for locally pinned volumes	If you delete a locally pinned volume, the space available for new volumes may not be updated immediately. The StorSimple Manager service updates the local space available approximately every hour.	Wait for an hour before you try to create the new volume.	Yes	No
17	Locally pinned volumes	Your restore job exposes the temporary snapshot backup in the Backup Catalog, but only during the restore job. Additionally, it exposes a virtual disk group with prefix <code>tmpCollection</code> on the Backup Policies page, but only during the restore job.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior won't occur. No user intervention is required.	Yes	No

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
18	Locally pinned volumes	If you cancel a restore job and a controller failover occurs immediately afterwards, the restore job will show Failed instead of Canceled . If a restore job fails and a controller failover occurs immediately afterwards, the restore job will show Canceled instead of Failed .	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior won't occur. No user intervention is required.	Yes	No
19	Locally pinned volumes	If you cancel a restore job or if a restore fails and then a controller failover occurs, an additional restore job appears on the Jobs page.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior won't occur. No user intervention is required.	Yes	No
20	Locally pinned volumes	If you try to convert a tiered volume (created and cloned with Update 1.2 or earlier) to a locally pinned volume and your device is running out of space or there's a cloud outage, then the clone(s) can be corrupted.	This problem occurs only with volumes that were created and cloned with pre-Update 2.1 software. This should be an infrequent scenario.		
21	Volume conversion	Don't update the ACRs attached to a volume while a volume conversion is in progress (tiered to locally pinned or vice versa). Updating the ACRs could result in data corruption.	If needed, update the ACRs prior to the volume conversion and don't make any further ACR updates while the conversion is in progress.		

Controller and firmware updates in Update 2.2

This release has software-only updates. However, if you're updating from a version prior to Update 2, you'll need to install driver, Storport, Spaceport, and (in some cases) disk firmware updates on your device.

For more information on how to install the driver, Storport, Spaceport, and disk firmware updates, see [install Update 2.2](#) on your StorSimple device.

Virtual device updates in Update 2.2

This update can't be applied to the virtual device. New virtual devices will need to be created.

Next step

Learn how to [install Update 2.2](#) on your StorSimple device.

StorSimple 8000 Series Update 2 release notes

Article • 08/23/2022 • 9 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 2. They also contain a list of the StorSimple software, driver, and disk firmware updates included in this release.

Update 2 can be applied to any StorSimple device running Release (GA) or Update 0.1 through Update 1.2. The device version associated with Update 2 is 6.3.9600.17673.

Please review the information contained in the release notes before you deploy the update in your StorSimple solution.

ⓘ Important

- It takes approximately 4-7 hours to install this update (including the Windows updates).
- Update 2 has software, LSI driver, and SSD firmware updates.
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Wait a few days, and then scan for updates again as these will become available soon.

What's new in Update 2

Update 2 introduces the following new features.

- **Locally pinned volumes** – In previous releases of the StorSimple 8000 series, blocks of data were tiered to the cloud based on usage. There was no way to guarantee that blocks would stay on local. In Update 2, when you create a volume, you can designate a volume as locally pinned, and primary data from that volume will not be tiered to the cloud. Snapshots of locally pinned volumes will still be copied to the cloud for backup so that the cloud can be used for data mobility and disaster recovery purposes. Additionally, you can change the volume type (that is, convert tiered volumes to locally pinned volumes and convert locally pinned volumes to tiered).
- **StorSimple virtual device improvements** – Previously, the StorSimple 8000 series positioned the virtual device as a disaster recovery or development/test solution. There was only one model of virtual device (model 1100). Update 2 introduces two virtual device models:

- 8010 (formerly called the 1100) – No change; has a capacity of 30 TB and uses Azure standard storage.
- 8020 – Has a capacity of 64 TB and uses Azure Premium storage for improved performance.

There is a single VHD for both virtual device models (8010/8020). When you first start the virtual device, it detects the platform parameters and applies the correct model version.

- **Networking Improvements** – Update 2 contains the following networking improvements:
 - Multiple NICs can be enabled for the cloud so that failover can occur if a NIC fails.
 - Routing improvements, with fixed metrics for cloud enabled blocks.
 - Online retry of failed resources before a failover.
 - New alerts for service failures.
- **Updating Improvements** – In Update 1.2 and earlier, the StorSimple 8000 series was updated via two channels: Windows Update for clustering, iSCSI, and so on, and Microsoft Update for binaries and firmware. Update 2 uses Microsoft Update for all update packages. This should lead to less time patching or doing failovers.
- **Firmware updates** – The following firmware updates are included:
 - LSI: lsi_sas2.sys Product Version 2.00.72.10
 - SSD only (no HDD updates): XMGG, XGEG, KZ50, F6C2, and VR08
- **Proactive Support** – Update 2 enables Microsoft to pull additional diagnostic information from the device. When our operations team identifies devices that are having problems, we are better equipped to collect information from the device and diagnose issues. **By accepting Update 2, you allow us to provide this proactive support.**

Issues fixed in Update 2

The following table provides a summary of issues that were fixed in Updates 2.

No.	Feature	Issue	Applies to physical device	Applies to virtual device
1	Network interfaces	After an upgrade to Update 1, the StorSimple Manager service reported that the Data2 and Data3 ports failed on one controller. This issue has been fixed.	Yes	No
2	Updates	After an upgrade to Update 1, audible alarm alerts occurred in the Azure classic portal on multiple devices. This issue has been fixed.	Yes	No
3	Openstack authentication	When using Openstack as your cloud service provider, you could receive an error that your cloud authentication string was too long. This has been fixed.	Yes	No

Known issues in Update 2

The following table provides a summary of known issues in this release.

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
1	Disk quorum	In rare instances, if the majority of disks in the EBOD enclosure of an 8600 device are disconnected resulting in no disk quorum, then the storage pool will go offline. It will stay offline even if the disks are reconnected.	You will need to reboot the device. If the issue persists, please contact Microsoft Support for next steps.	Yes	No
2	Incorrect controller ID	When a controller replacement is performed, controller 0 may show up as controller 1. During controller replacement, when the image is loaded from the peer node, the controller ID can show up initially as the peer controller's ID. In rare instances, this behavior may also be seen after a system reboot.	No user action is required. This situation will resolve itself after the controller replacement is complete.	Yes	No
3	Storage accounts	Using the Storage service to delete the storage account is an unsupported scenario. This will lead to a situation in which user data cannot be retrieved.		Yes	Yes
4	Device failover	Multiple failovers of a volume container from the same source device to different target devices is not supported. Failover from a single dead device to multiple devices will make the volume containers on the first failed over device lose data ownership. After such a failover, these volume containers will appear or behave differently when you view them in the Azure classic portal.		Yes	No
5	Installation	During StorSimple Adapter for SharePoint installation, you need to provide a device IP in order for the install to finish successfully.		Yes	No
6	Web proxy	If your web proxy configuration has HTTPS as the specified protocol, then your device-to-service communication will be affected and the device will go offline. Support packages will also be generated in the process, consuming significant resources on your device.	Make sure that the web proxy URL has HTTP as the specified protocol. For more information, go to Configure web proxy for your device .	Yes	No
7	Web proxy	If you configure and enable web proxy on a registered device, then you will need to restart the active controller on your device.		Yes	No
8	High cloud latency and high I/O workload	When your StorSimple device encounters a combination of very high cloud latencies (order of seconds) and high I/O workload, the device volumes go into a degraded state and the I/Os may fail with a "device not ready" error.	You will need to manually reboot the device controllers or perform a device failover to recover from this situation.	Yes	No

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
9	Azure PowerShell	When you use the StorSimple cmdlet <code>Get-AzureStorSimpleStorageAccountCredential</code> <code>Select-Object -First 1 -Wait</code> to select the first object so that you can create a new <code>VolumeContainer</code> object, the cmdlet returns all the objects.	Wrap the cmdlet in parentheses as follows: <code>(Get-AzureStorSimpleStorageAccountCredential)</code> <code>Select-Object -First 1 -Wait</code>	Yes	Yes
10	Migration	When multiple volume containers are passed for migration, the ETA for latest backup is accurate only for the first volume container. Additionally, parallel migration will start after the first 4 backups in the first volume container are migrated.	We recommend that you migrate one volume container at a time.	Yes	No
11	Migration	After the restore, volumes are not added to the backup policy or the virtual disk group.	You will need to add these volumes to a backup policy in order to create backups.	Yes	Yes
12	Migration	After the migration is complete, the 5000/7000 series device must not access the migrated data containers.	We recommend that you delete the migrated data containers after the migration is complete and committed.	Yes	No
13	Clone and DR	A StorSimple device running Update 1 cannot clone or perform disaster recovery to a device running pre-update 1 software.	You will need to update the target device to Update 1 to allow these operations	Yes	Yes
14	Migration	Configuration backup for migration may fail on a 5000-7000 series device when there are volume groups with no associated volumes.	Delete all the empty volume groups with no associated volumes and then retry the configuration backup.	Yes	No
15	Azure PowerShell cmdlets and locally pinned volumes	You cannot create a locally pinned volume via Azure PowerShell cmdlets. (Any volume you create via Azure PowerShell will be tiered.)	Always use the StorSimple Manager service to configure locally pinned volumes.	Yes	No
16	Space available for locally pinned volumes	If you delete a locally pinned volume, the space available for new volumes may not be updated immediately. The StorSimple Manager service updates the local space available approximately every hour.	Wait for an hour before you try to create the new volume.	Yes	No
17	Locally pinned volumes	Your restore job exposes the temporary snapshot backup in the Backup Catalog, but only for the duration of the restore job. Additionally, it exposes a virtual disk group with prefix <code>tmpCollection</code> on the Backup Policies page, but only for the duration of the restore job.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No

No.	Feature	Issue	Comments / work around	Applies to physical device	Applies to virtual device
18	Locally pinned volumes	If you cancel a restore job and a controller failover occurs immediately afterwards, the restore job will show Failed instead of Canceled . If a restore job fails and a controller failover occurs immediately afterwards, the restore job will show Canceled instead of Failed .	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No
19	Locally pinned volumes	If you cancel a restore job or if a restore fails and then a controller failover occurs, an additional restore job appears on the Jobs page.	This behavior can occur if your restore job has only locally pinned volumes or a mix of locally pinned and tiered volumes. If the restore job includes only tiered volumes, then this behavior will not occur. No user intervention is required.	Yes	No
20	Locally pinned volumes	If you try to convert a tiered volume (created and cloned with Update 1.2 or earlier) to a locally pinned volume and your device is running out of space or there is a cloud outage, then the clone(s) can be corrupted.	This problem occurs only with volumes that were created and cloned with pre-Update 2 software. This should be an infrequent scenario.		
21	Volume conversion	Do not update the ACRs attached to a volume while a volume conversion is in progress (tiered to locally pinned or vice versa). Updating the ACRs could result in data corruption.	If needed, update the ACRs prior to the volume conversion and do not make any further ACR updates while the conversion is in progress.		

Controller and firmware updates in Update 2

This release updates the driver and the disk firmware on your device.

- For more information about the LSI firmware update, see Microsoft Knowledge base article 3121900.
- For more information about the disk firmware update, see Microsoft Knowledge base article 3121899.

Virtual device updates in Update 2

This update cannot be applied to the virtual device. New virtual devices will need to be created.

Next step

Learn how to [install Update 2](#) on your StorSimple device.

Update 1.2 release notes for your StorSimple 8000 series device

Article • 08/23/2022 • 10 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes describe the new features and identify the critical open issues for StorSimple 8000 Series Update 1.2. They also contain a list of the StorSimple software, driver and disk firmware updates included in this release.

Update 1.2 can be applied to any StorSimple device running Release (GA), Update 0.1, Update 0.2, or Update 0.3 software. Update 1.2 is not available if your device is running Update 1 or Update 1.1. If your device is running Release (GA), please [contact Microsoft Support](#) to assist you with installing this update.

The following table lists the device software versions corresponding to Updates 1, 1.1, and 1.2.

If running update ...	this is your device software version.
Update 1.2	6.3.9600.17584
Update 1.1	6.3.9600.17521
Update 1.0	6.3.9600.17491

Please review the information contained in the release notes before you deploy the update in your StorSimple solution. For more information, see how to [install Update 1.2 on your StorSimple device](#).

ⓘ Important

- It takes approximately 5-10 hours to install this update (including the Windows Updates).
- Update 1.2 has software, LSI driver and disk firmware updates. To install, follow the instructions in [install Update 1.2 on your StorSimple device](#).
- For new releases, you may not see updates immediately because we do a phased rollout of the updates. Scan for updates in a few days again as these will become available soon.

What's new in Update 1.2

These features were first released with Update 1 that was made available to a limited set of users. With the Update 1.2 release, most of the StorSimple users would see the following new features and improvements:

- **Migration from 5000-7000 series to 8000 series devices** – This release introduces a new migration feature that allows the StorSimple 5000-7000 series appliance users to migrate their data to a StorSimple 8000 series physical appliance or a virtual appliance. The migration feature has two key value propositions:
 - **Business continuity**, by enabling migration of existing data on 5000-7000 series appliances to 8000 series appliances.
 - **Improved feature offerings of the 8000 series appliances**, such as efficient centralized management of multiple appliances through StorSimple Manager service, better class of hardware and updated firmware, virtual appliances, data mobility, and features in the future roadmap.
- Refer to the [migration guide](#) for details on how to migrate a StorSimple 5000-7000 series to an 8000 series device.
- **Availability in the Azure Government Portal** – StorSimple is now available in the Azure Government portal. See how to [deploy a StorSimple device in the Azure Government Portal](#).
- **Support for other cloud service providers** – The other cloud service providers supported are Amazon S3, Amazon S3 with RRS, HP, and OpenStack (beta).
- **Update to latest Storage APIs** – With this release, StorSimple has been updated to the latest Azure Storage service APIs. StorSimple 8000 series devices that are running pre-Update 1 software versions (Release, 0.1, 0.2, and 0.3) are using versions of the Azure Storage Service APIs older than July 17, 2009. As stated in the updated [announcement about removal of Storage service versions](#), by August 1, 2016, these APIs will be deprecated. It is imperative that you apply the StorSimple 8000 Series Update 1 prior to August 1, 2016. If you fail to do so, StorSimple devices will stop functioning correctly.
- **Support for Zone Redundant Storage (ZRS)** – With the upgrade to the latest version of the Storage APIs, the StorSimple 8000 series will support Zone Redundant Storage (ZRS) in addition to Locally Redundant Storage (LRS) and Geo-redundant Storage (GRS). Refer to this [article on Azure Storage redundancy options](#) for ZRS details.
- **Enhanced initial deployment and update experience** – In this release, the installation and update processes have been enhanced. The installation through the setup wizard is improved to provide feedback to the user if the network configuration and firewall settings are incorrect. Additional diagnostic cmdlets have been provided to help you with troubleshooting networking of the device. See the [troubleshooting deployment article](#) for more information about the new diagnostic cmdlets used for troubleshooting.

Issues fixed in Update 1.2

The following table provides a summary of issues that were fixed in Updates 1.2, 1.1, and 1.

No.	Feature	Issue	Fixed in Update	Applies to physical device	Applies to virtual device

No.	Feature	Issue	Fixed in Update	Applies to physical device	Applies to virtual device
1	Windows PowerShell for StorSimple	When a user remotely accessed the StorSimple device by using Windows PowerShell for StorSimple and then started the setup wizard, a crash occurred as soon as Data 0 IP was input. This bug is now fixed in Update 1.	Update 1	Yes	Yes
2	Factory reset	In some instances, when you performed a factory reset, the StorSimple device became stuck and displayed this message: Reset to factory is in progress (phase 8) . This happened if you pressed CTRL+C while the cmdlet was in progress. This bug is now fixed.	Update 1	Yes	No
3	Factory reset	After a failed dual controller factory reset, you were allowed to proceed with device registration. This resulted in an unsupported system configuration. In Update 1, an error message is shown and registration is blocked on a device that has a failed factory reset.	Update 1	Yes	No
4	Factory reset	In some instances, false positive mismatch alerts were raised. Incorrect mismatch alerts will no longer be generated on devices running Update 1.	Update 1	Yes	No
5	Factory reset	If a factory reset was interrupted prior to completion, the device entered recovery mode and did not allow you to access Windows PowerShell for StorSimple. This bug is now fixed.	Update 1	Yes	No
6	Disaster recovery	A disaster recovery (DR) bug was fixed wherein DR would fail during the discovery of backups on the target device.	Update 1	Yes	Yes
7	Monitoring LEDs	In certain instances, monitoring LEDs at the back of appliance did not indicate correct status. The blue LED was turned off. DATA 0 and DATA 1 LEDs were flashing even when these interfaces were not configured. The issue has been fixed and monitoring LEDs now indicate the correct status.	Update 1	Yes	No
8	Monitoring LEDs	In certain instances, after applying Update 1, the blue light on the active controller turned off thereby making it hard to identify the active controller. This issue has been fixed in this patch release.	Update 1.2	Yes	No
9	Network interfaces	In previous versions, a StorSimple device configured with a non-routable gateway could go offline. In this release, the routing metric for Data 0 has been made the lowest; therefore, even if other network interfaces are cloud-enabled, all the cloud traffic from the device will be routed via Data 0.	Update 1	Yes	Yes
10	Backups	A bug in Update 1 which caused backups to fail after 24 days has been fixed in the patch release Update 1.1.	Update 1.1	Yes	Yes
11	Backups	A bug in previous versions resulted in poor performance for cloud snapshots with low change rates. This bug has been fixed in this patch release.	Update 1.2	Yes	Yes
12	Updates	A bug in Update 1 that reported a failed upgrade and caused the controllers to go into Recovery mode, has been fixed in this patch release.	Update 1.2	Yes	Yes

Known issues in Update 1.2

The following table provides a summary of known issues in this release.

No.	Feature	Issue	Comments/workaround	Applies to physical device	Applies to virtual device
1	Disk quorum	In rare instances, if the majority of disks in the EBOD enclosure of an 8600 device are disconnected resulting in no disk quorum, then the storage pool will be offline. It will stay offline even if the disks are reconnected.	You will need to reboot the device. If the issue persists, please contact Microsoft Support for next steps.	Yes	No
2	Incorrect controller ID	When a controller replacement is performed, controller 0 may show up as controller 1. During controller replacement, when the image is loaded from the peer node, the controller ID can show up initially as the peer controller's ID. In rare instances, this behavior may also be seen after a system reboot.	No user action is required. This situation will resolve itself after the controller replacement is complete.	Yes	No
3	Storage accounts	Using the Storage service to delete the storage account is an unsupported scenario. This will lead to a situation in which user data cannot be retrieved.	Yes		Yes
4	Device failover	Multiple failovers of a volume container from the same source device to different target devices is not supported. Device failover from a single dead device to multiple devices will make the volume containers on the first failed over device lose data ownership. After such a failover, these volume containers will appear or behave differently when you view them in the Azure classic portal.		Yes	No
5	Installation	During StorSimple Adapter for SharePoint installation, you need to provide a device IP in order for the install to finish successfully.		Yes	No
6	Web proxy	If your web proxy configuration has HTTPS as the specified protocol, then your device-to-service communication will be affected and the device will go offline. Support packages will also be generated in the process, consuming significant resources on your device.	Make sure that the web proxy URL has HTTP as the specified protocol. For more information, go to Configure web proxy for your device .	Yes	No
7	Web proxy	If you configure and enable web proxy on a registered device, then you will need to restart the active controller on your device.		Yes	No

No.	Feature	Issue	Comments/workaround	Applies to physical device	Applies to virtual device
8	High cloud latency and high I/O workload	When your StorSimple device encounters a combination of very high cloud latencies (order of seconds) and high I/O workload, the device volumes go into a degraded state and the I/Os may fail with a "device not ready" error.	You will need to manually reboot the device controllers or perform a device failover to recover from this situation.	Yes	No
9	Azure PowerShell	When you use the StorSimple cmdlet <code>Get-AzureStorSimpleStorageAccountCredential Select-Object -First 1 -Wait</code> to select the first object so that you can create a new <code>VolumeContainer</code> object, the cmdlet returns all the objects.	Wrap the cmdlet in parentheses as follows: <code>(Get-AzureStorSimpleStorageAccountCredential) Select-Object -First 1 -Wait</code>	Yes	Yes
10	Migration	When multiple volume containers are passed for migration, the ETA for latest backup is accurate only for the first volume container. Additionally, parallel migration will start after the first 4 backups in the first volume container are migrated.	We recommend that you migrate one volume container at a time.	Yes	No
11	Migration	After the restore, volumes are not added to the backup policy or the virtual disk group.	You will need to add these volumes to a backup policy in order to create backups.	Yes	Yes
12	Migration	After the migration is complete, the 5000/7000 series device must not access the migrated data containers.	We recommend that you delete the migrated data containers after the migration is complete and committed.	Yes	No
13	Clone and DR	A StorSimple device running Update 1 cannot clone or perform Disaster Recovery to a device running pre-update 1 software.	You will need to update the target device to Update 1 to allow these operations	Yes	Yes
14	Migration	Configuration backup for migration may fail on a 5000-7000 series device when there are volume groups with no associated volumes.	Delete all the empty volume groups with no associated volumes and then retry the configuration backup.	Yes	No

Physical device updates in Update 1.2

If patch update 1.2 is applied to a physical device (running versions prior to Update 1), the software version will change to 6.3.9600.17584.

Controller and firmware updates in Update 1.2

This release updates the driver and the disk firmware on your device.

- For more information about the SAS controller update, see [Update 1 for LSI SAS controllers in Microsoft Azure StorSimple Appliance](#).
- For more information about the disk firmware update, see [Disk firmware Update 1 for Microsoft Azure StorSimple Appliance](#).

Virtual device updates in Update 1.2

This update cannot be applied to the virtual device. New virtual devices will need to be created.

Next steps

- [Install Update 1.2 on your device.](#)

StorSimple documentation

Learn how to use Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

About StorSimple

OVERVIEW

[Compare StorSimple with Azure File Sync and Data Box Edge](#)

StorSimple Virtual Array

OVERVIEW

[What is StorSimple Virtual Array?](#)

GET STARTED

[Review requirements](#)

StorSimple 8000 Series

OVERVIEW

[What is StorSimple 8000 Series?](#)

GET STARTED

[Review requirements](#)

StorSimple Data Manager

OVERVIEW

[What is StorSimple Data Manager?](#)

GET STARTED

[Manage in the Azure portal](#)

StorSimple for Cloud Solutions Providers Program

OVERVIEW

[What is the StorSimple for Cloud Solutions Providers Program?](#)

GET STARTED

[Deploy](#)

StorSimple documentation

Learn how to use Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

About StorSimple

OVERVIEW

[Compare StorSimple with Azure File Sync and Data Box Edge](#)

StorSimple Virtual Array

OVERVIEW

[What is StorSimple Virtual Array?](#)

GET STARTED

[Review requirements](#)

StorSimple 8000 Series

OVERVIEW

[What is StorSimple 8000 Series?](#)

GET STARTED

[Review requirements](#)

StorSimple Data Manager

OVERVIEW

[What is StorSimple Data Manager?](#)

GET STARTED

[Manage in the Azure portal](#)

StorSimple for Cloud Solutions Providers Program

OVERVIEW

[What is the StorSimple for Cloud Solutions Providers Program?](#)

GET STARTED

[Deploy](#)

StorSimple documentation

Learn how to use Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

About StorSimple

OVERVIEW

[Compare StorSimple with Azure File Sync and Data Box Edge](#)

StorSimple Virtual Array

OVERVIEW

[What is StorSimple Virtual Array?](#)

GET STARTED

[Review requirements](#)

StorSimple 8000 Series

OVERVIEW

[What is StorSimple 8000 Series?](#)

GET STARTED

[Review requirements](#)

StorSimple Data Manager

OVERVIEW

[What is StorSimple Data Manager?](#)

GET STARTED

[Manage in the Azure portal](#)

StorSimple for Cloud Solutions Providers Program

OVERVIEW

[What is the StorSimple for Cloud Solutions Providers Program?](#)

GET STARTED

[Deploy](#)

StorSimple documentation

Learn how to use Azure StorSimple, an integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

About StorSimple

OVERVIEW

[Compare StorSimple with Azure File Sync and Data Box Edge](#)

StorSimple Virtual Array

OVERVIEW

[What is StorSimple Virtual Array?](#)

GET STARTED

[Review requirements](#)

StorSimple 8000 Series

OVERVIEW

[What is StorSimple 8000 Series?](#)

GET STARTED

[Review requirements](#)

StorSimple Data Manager

OVERVIEW

[What is StorSimple Data Manager?](#)

GET STARTED

[Manage in the Azure portal](#)

StorSimple for Cloud Solutions Providers Program

OVERVIEW

[What is the StorSimple for Cloud Solutions Providers Program?](#)

GET STARTED

[Deploy](#)

HCS

Reference

{{Manually Enter Description Here}}

HCS

Disable-HcsNetInterface	Disables a network interface.
Disable-HcsRemoteManagement	Disables Windows PowerShell remote management.
Disable-HcsSupportAccess	Disables support access to this device.
Disable-HcsWebProxy	Disables the web proxy for the device.
Enable-HcsNetInterface	Enables a network interface.
Enable-HcsRemoteManagement	Enables remote Windows PowerShell management.
Enable-HcsSupportAccess	Enables access to this device for Customer Service and Support.
Enable-HcsWebProxy	Enables the web proxy.
Enter-HcsMaintenanceMode	Puts a device into maintenance mode.
Enter-HcsSupportSession	Used by Microsoft Support to enter into an unrestricted PowerShell runspace on the device for troubleshooting purposes.
Exit-HcsMaintenanceMode	Takes a device out of maintenance mode.
Export-HcsSupportPackage	Bundles logs into a single .zip file.
Get-HcsDnsClientServerAddress	Gets the server addresses that a Domain Name System (DNS) client device is configured to use.
Get-HcsFirmwareVersion	Gets the firmware versions of devices and displays the results.
Get-HcsNetInterface	Gets configuration information for a network interface.
Get-HcsNtpClientServerAddress	Gets URLs of the NTP servers for this device.
Get-HcsRemoteManagementCert	Gets the certificate for remote management.
Get-HcsSupportAccess	Gets the encrypted password that Customer Service and Support uses to access the device.

Get-HcsSystem	Gets system information about this StorSimple device.
Get-HcsUpdateAvailability	Scans for updates.
Get-HcsUpdateStatus	Gets the current status of updates.
Get-HcsWebProxy	Gets the web proxy configuration.
Get-HcsWuaVersion	Gets the version of the Windows Update Agent.
Invoke-HcsSetupWizard	Performs initial configuration and device registration.
Restart-HcsController	Restarts a controller.
Set-HcsDnsClientServerAddress	Sets the server addresses for a Domain Name System (DNS) client device.
Set-HcsNetInterface	Sets the configuration for a single network interface by alias.
Set-HcsNtpClientServerAddress	Sets the NTP URLs for this device.
Set-HcsPassword	Sets the password for a user account.
Set-HcsRemoteManagementCert	Generates the certificate for remote management.
Set-HcsSystem	Modifies settings for your StorSimple instance.
Set-HcsWebProxy	Sets the web proxy configuration.
Start-HcsFirmwareCheck	Checks whether a device needs a firmware update.
Start-HcsHotfix	Installs a hotfix on a StorSimple device.
Start-HcsUpdate	Installs updates.
Stop-HcsController	Stops a controller.
Test-HcsNtp	Attempts to synchronize the time to the NTP server.

Microsoft.StorSimple resource types

Article • 12/28/2022 • 2 minutes to read

This article lists the available versions for each resource type.

For a list of changes in each API version, see [change log](#)

Resource types and versions

Types	Versions
managers	2017-06-01 2016-10-01
managers/accessControlRecords	2017-06-01 2016-10-01
managers/bandwidthSettings	2017-06-01
managers/certificates	2016-10-01
managers/devices/alertSettings	2017-06-01 2016-10-01
managers/devices/backupPolicies	2017-06-01
managers/devices/backupPolicies/schedules	2017-06-01
managers/devices/backupScheduleGroups	2016-10-01
managers/devices/chapSettings	2016-10-01
managers/devices/fileservers	2016-10-01
managers/devices/fileservers/shares	2016-10-01
managers/devices/iscsiservers	2016-10-01
managers/devices/iscsiservers/disks	2016-10-01
managers/devices/timeSettings	2017-06-01
managers/devices/volumeContainers	2017-06-01
managers/devices/volumeContainers/volumes	2017-06-01
managers/extendedInformation	2017-06-01 2016-10-01

Types	Versions
managers/storageAccountCredentials	2017-06-01 2016-10-01
managers/storageDomains	2016-10-01

StorSimple Data Manager overview

Article • 08/19/2022 • 5 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Microsoft Azure StorSimple uses cloud storage as an extension of the on-premises solution and automatically tiers data across on-premises storage and the cloud. Data is stored in the cloud in a deduped and compressed format for maximum efficiency. As the data is stored in StorSimple format, it isn't readily consumable by other cloud applications that you may want to use.

The StorSimple Data Manager allows you to copy your StorSimple data to Azure file shares or Azure blob storage. This article focuses on the former.

In some scenarios, Azure blob storage can be the right choice, if file and folder structure, metadata, and backups are not important for you to preserve. The remainder of this article provides an overview of the StorSimple Data Manager. It also explains how you can use this service to write applications that use StorSimple data and other Azure services in the cloud.

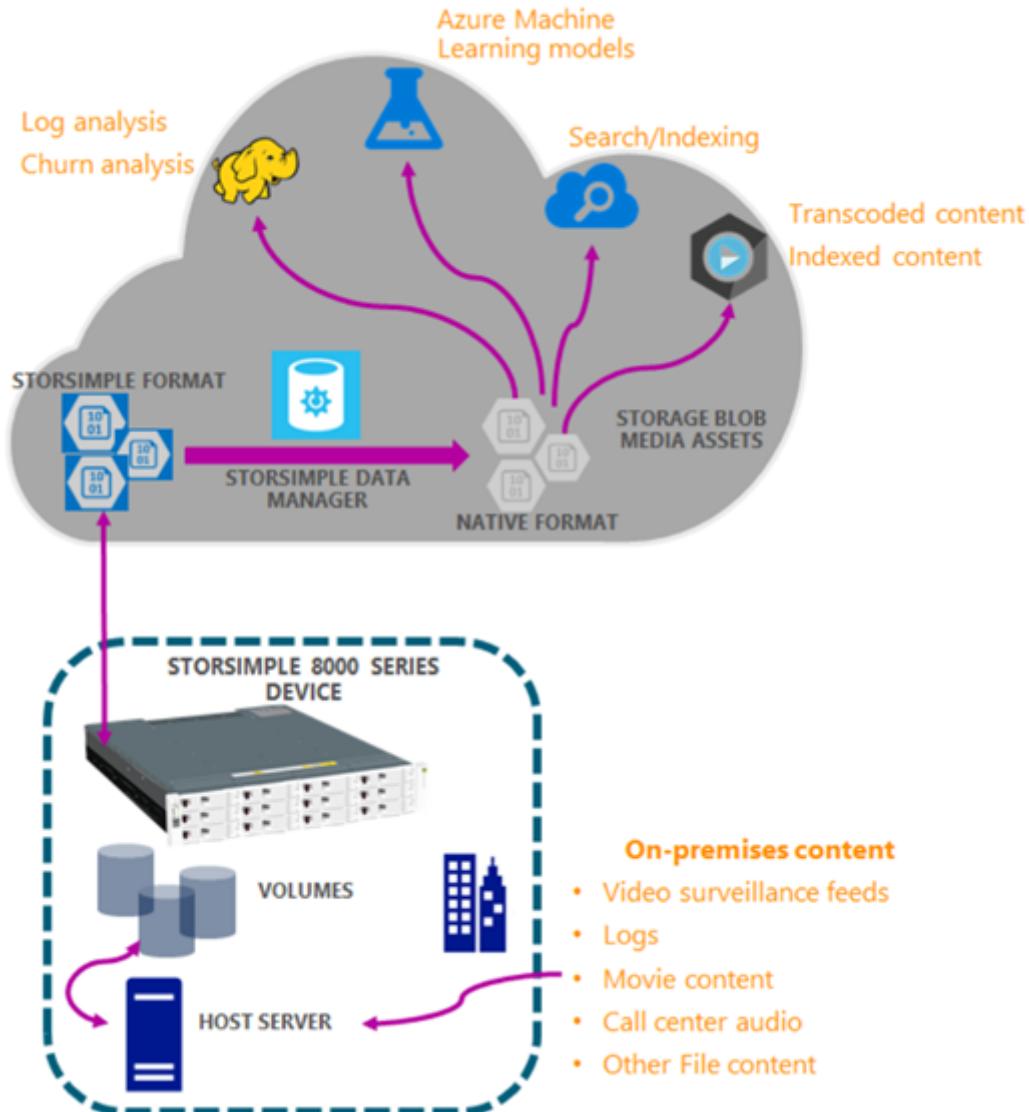
ⓘ Important

To learn how to use the Data Manager to migrate and preserve your data, see [StorSimple 8100 and 8600 migration to Azure File Sync](#).

Functional overview

The StorSimple Data Manager service identifies StorSimple data in the cloud from a StorSimple 8000 series on-premises device. The StorSimple data in the cloud is

deduped, compressed StorSimple format. The Data Manager service provides APIs to extract the StorSimple format data and transform it into other formats such as Azure blobs and Azure Files. This transformed data is then consumed by Azure HDInsight and Azure Media services. The data transformation enables these services to operate on the transformed StorSimple data from StorSimple 8000 series on-premises device. This flow is illustrated in the following diagram.



Data Manager use cases

The primary use case for a Data Manager is the build-in migration service to leave the StorSimple platform.

Choosing a region

The region of your Data Manager is not very important for copy performance. The Data Manager itself orchestrates migrations. It is far more important to choose the correct region for your job definitions (migration jobs) within your Data Manager.

Choose a region for your job definition that is either the same or near the region that contains the StorSimple storage account for your StorSimple source volumes.

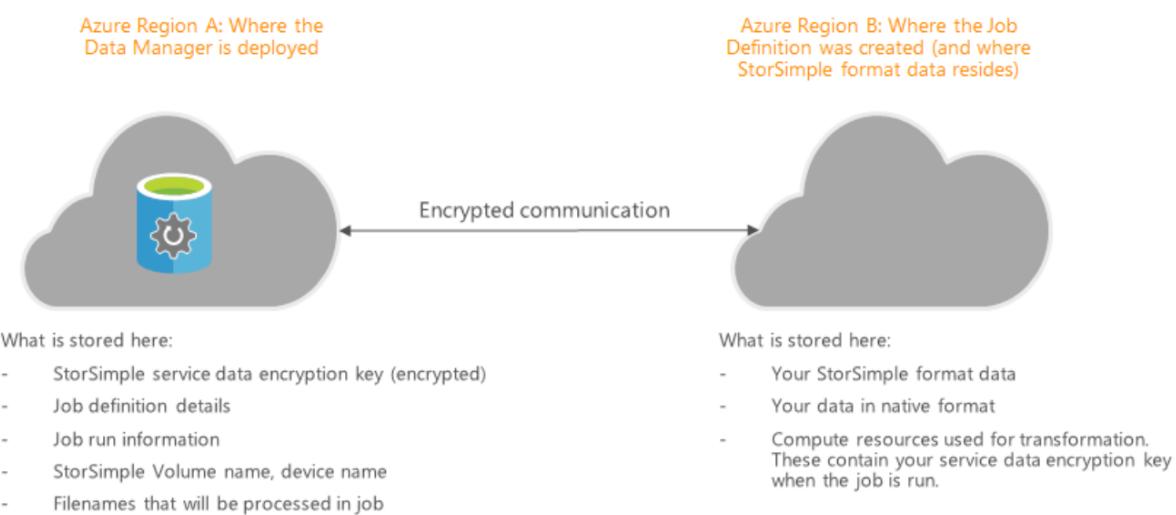
Security considerations

The StorSimple Data Manager needs the service data encryption key to transform from StorSimple format to native format. The service data encryption key is generated when the first device registers with the StorSimple service. For more information on this key, go to [StorSimple security](#).

The service data encryption key provided as an input is stored in a key vault that is created when you create a Data Manager. The vault resides in the same Azure region as your StorSimple Data Manager. This key is deleted when you delete your Data Manager service.

This key is used by the compute resources to perform the transformation. These compute resources are located in the same Azure region as your job definition. This region may, or may not be the same as the region where you bring up your Data Manager.

If your Data Manager region is different from your job definition region, it is important that you understand what data/metadata resides in each of these regions. The following diagram illustrates the effect of having different regions for Data Manager and job definition.



Managing personal information

The StorSimple Data Manager does not collect or display any personal information. For more information, review the Microsoft Privacy policy at [Trust Center](#).

Known limitations

StorSimple Data Manager has different limitations, based on the storage you are moving your data into. The following items prevent a migration regardless of target storage:

- Only NTFS volumes from your StorSimple appliance are supported.
- The service doesn't work with volumes that are BitLocker encrypted.
- The service can't copy data from a corrupted StorSimple backup.
- Special networking options, such as firewalls or private endpoint-only communication can't be enabled on either the source storage account where StorSimple backups are stored, nor on the target storage account that holds your Azure file shares.

Target an Azure file share

There are also limitations on what can be stored in Azure file shares. It's important to understand them before a migration. *File fidelity* refers to the multitude of attributes, timestamps, and data that compose a file. In a migration, file fidelity is a measure of how well the information on the source (StorSimple volume) can be translated (migrated) to the target (Azure file share). [Azure Files supports a subset](#) of the [NTFS file properties](#). ACLs, common metadata, and some timestamps will be migrated. The following items won't prevent a migration but will cause per-item issues during a migration:

- Timestamps: File change time won't be set - it is currently read-only over the REST protocol. Last access timestamp on a file won't be moved, it currently isn't a supported attribute on files stored in an Azure file share.
- [Alternate Data Streams](#) can't be stored in Azure file shares. Files holding Alternate Data Streams will be copied, but Alternate Data Streams are stripped from the file in the process.
- Symbolic links, hard links, junctions, and reparse points are skipped during a migration. The migration copy logs will list each skipped item and a reason.
- EFS encrypted files will fail to copy. Copy logs will show the item failed to copy with *Access is denied*.
- Corrupt files are skipped. The copy logs may list different errors for each item that is corrupt on the StorSimple disk: *The request failed due to a fatal device hardware error* or *The file or directory is corrupted or unreadable* or *The access control list (ACL) structure is invalid*.
- A single file can't be larger than 4 TiB or it'll be skipped in the migration.
- File path lengths must be equal to or fewer than 2048 characters. Files and folders with longer paths will be skipped.

Target an Azure blob container

- Blob transfer limitations:
 - You can't migrate your backup history. Only the latest StorSimple volume backup can be used as a source.
 - File path lengths need to be fewer than 256 characters else the job will fail.
 - Maximum supported file size for a blob is 4.7 TiB.
 - Most recent available backup set will be used.
 - File metadata is not uploaded with the file content.
 - Uploaded blobs are of the Block Blob type. Thus, any uploaded VHD or VHDX can't be used in Azure Virtual Machines.

Next steps

[Use StorSimple Data Manager UI to transform your data.](#)

Additional resources

Documentation

[Tutorial to return Azure Data Box](#)

In this tutorial, learn how to return Azure Data Box, including shipping the device, verifying data upload to Azure, and erasing data from Data Box.

[Microsoft Azure Data Box system requirements](#)

Learn about important system requirements for your Azure Data Box and for clients that connect to the Data Box.

[Data migration options from StorSimple 8000 series devices](#)

Provides an overview of the options to migrate data from StorSimple 8000 series.

[StorSimple 8000 series migration to Azure File Sync](#)

Learn how to migrate a StorSimple 8100 or 8600 appliance to Azure File Sync.

[Tutorial to order Azure Data Box](#)

In this tutorial, learn about Azure Data Box, a hybrid solution that allows you to import on-premises data into Azure, and how to order Azure Data Box.

[Manage Azure Data Box, Azure Data Box Heavy via Azure portal](#)

Describes how to use the Azure portal to administer your Azure Data Box and Azure Data Box Heavy.

[Tutorial to export data from Azure Data Box](#)

Learn the deployment prerequisites and how to export data from an Azure Data Box

Azure Data Box, Azure Data Box Heavy FAQ

Contains frequently asked questions and answers for Azure Data Box and Azure Data Box Heavy, a cloud solution that enables you to transfer large amounts of data into Azure.

[Show 5 more](#)

Manage the StorSimple Data Manager service in Azure portal

Article • 12/08/2021 • 6 minutes to read

⊗ Caution

StorSimple 8000 series will reach its end-of-life in December 2022. Microsoft provides a **dedicated migration service** for StorSimple 8000 series volumes and their backups. It is imperative that you stop any new StorSimple deployments and begin planning your migration now.

The StorSimple Data Manager contains a dedicated migration service for your StorSimple volumes and their backups. If you want to preserve your file and folder structure, ACLs, timestamps, attributes, and backups, then Azure Files is the ideal choice. [Review the migration guide](#).

The remainder of this article focuses on how to use the Data Manager when blob storage is the target.

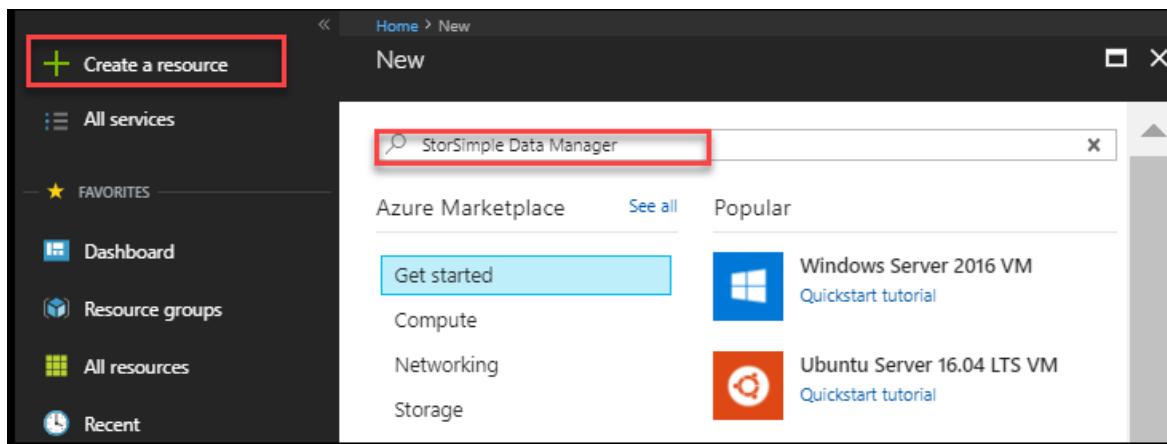
Use StorSimple Data Transformation

The StorSimple Data Manager is the resource within which data transformation is instantiated. The Data Transformation service lets you transform data from the StorSimple format to native format in blobs or Azure Files. To transform the StorSimple native format data, you need to specify the details about your StorSimple 8000 series device and the data of interest that you want to transform.

Create a StorSimple Data Manager service

Perform the following steps to create a StorSimple Data Manager service.

1. Use your Microsoft account credentials to log on to the [Azure portal](#).
2. Click **+ Create a resource** and search for StorSimple Data Manager.

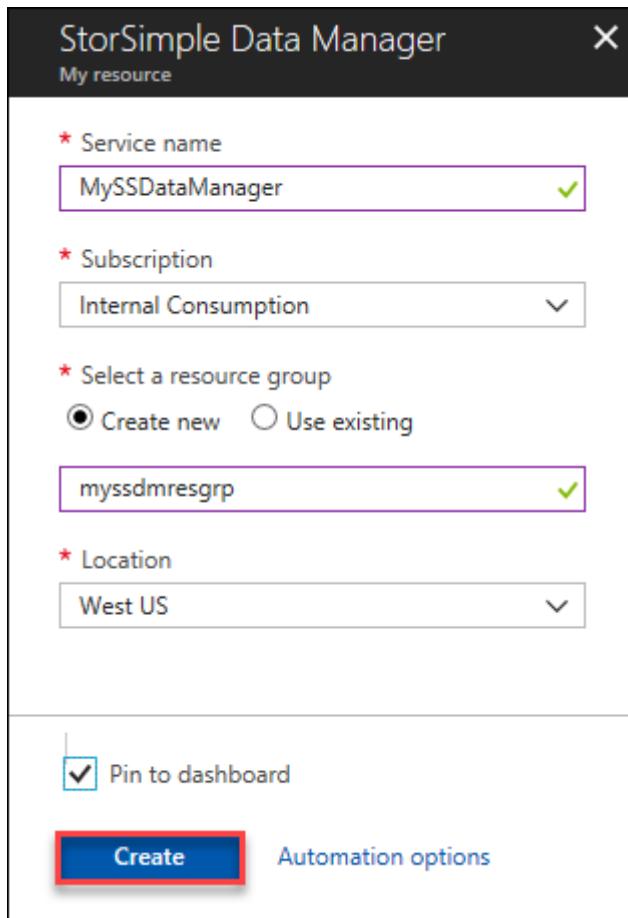


3. Click StorSimple Data Manager and then click **Create**.

NAME	PUBLISHER	CATEGORY
StorSimple Data Manager	Microsoft	Storage

4. For the new service, specify the following:

- Provide a unique **Service name** for your StorSimple Data Manager. This is a friendly name that can be used to identify the service. The name can have between 3 and 24 characters that can be letters, numbers, and hyphens. The name must start and end with a letter or a number.
- Choose a **Subscription** from the dropdown list. The subscription is linked to your billing account. This field is automatically populated (and not selectable) if you have only one subscription.
- Select an existing resource group or create a new group. For more information, see [Azure resource groups](#).
- Specify the **Location** for your service that houses your storage accounts and your StorSimple Data Manager service. Your StorSimple Device Manager service, Data Manager service, and the associated storage account should all be in the supported regions.
- To get a link to this service on your dashboard, select **Pin to dashboard**.
- Click **Create**.



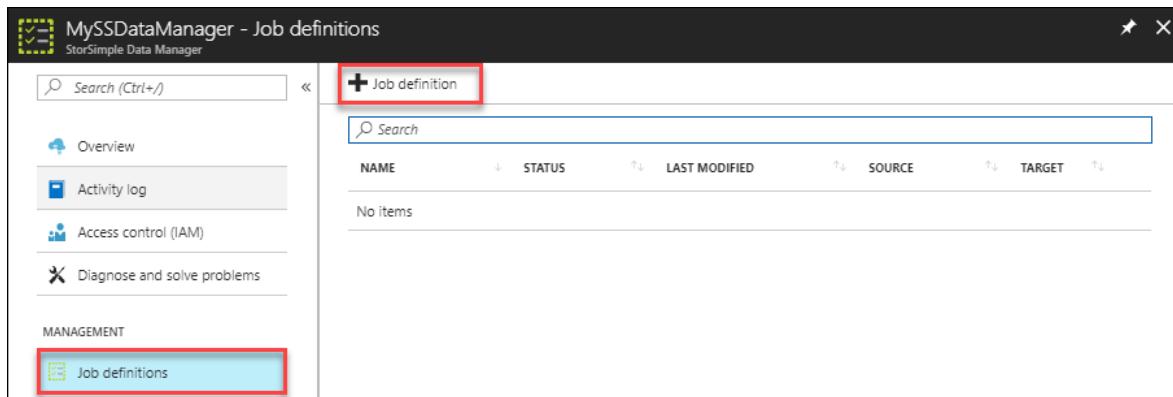
The service creation takes a few minutes. You see a notification after the service is successfully created and the new service is displayed.

Create a data transformation job definition

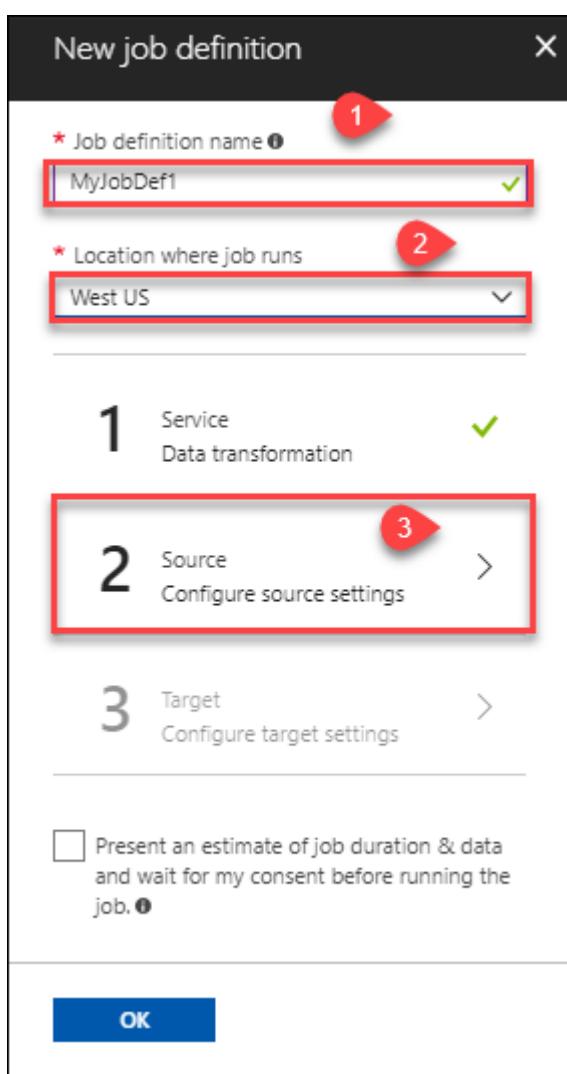
Within a StorSimple Data Manager service, you need to create a data transformation job definition. A job definition specifies details of the StorSimple data that you are interested in moving into a storage account in the native format. Once you create a job definition, then you can run this job again with different runtime settings.

Perform the following steps to create a job definition.

1. Navigate to the service that you created. Go to **Management > Job definitions**.
2. Click **+ Job definition**.



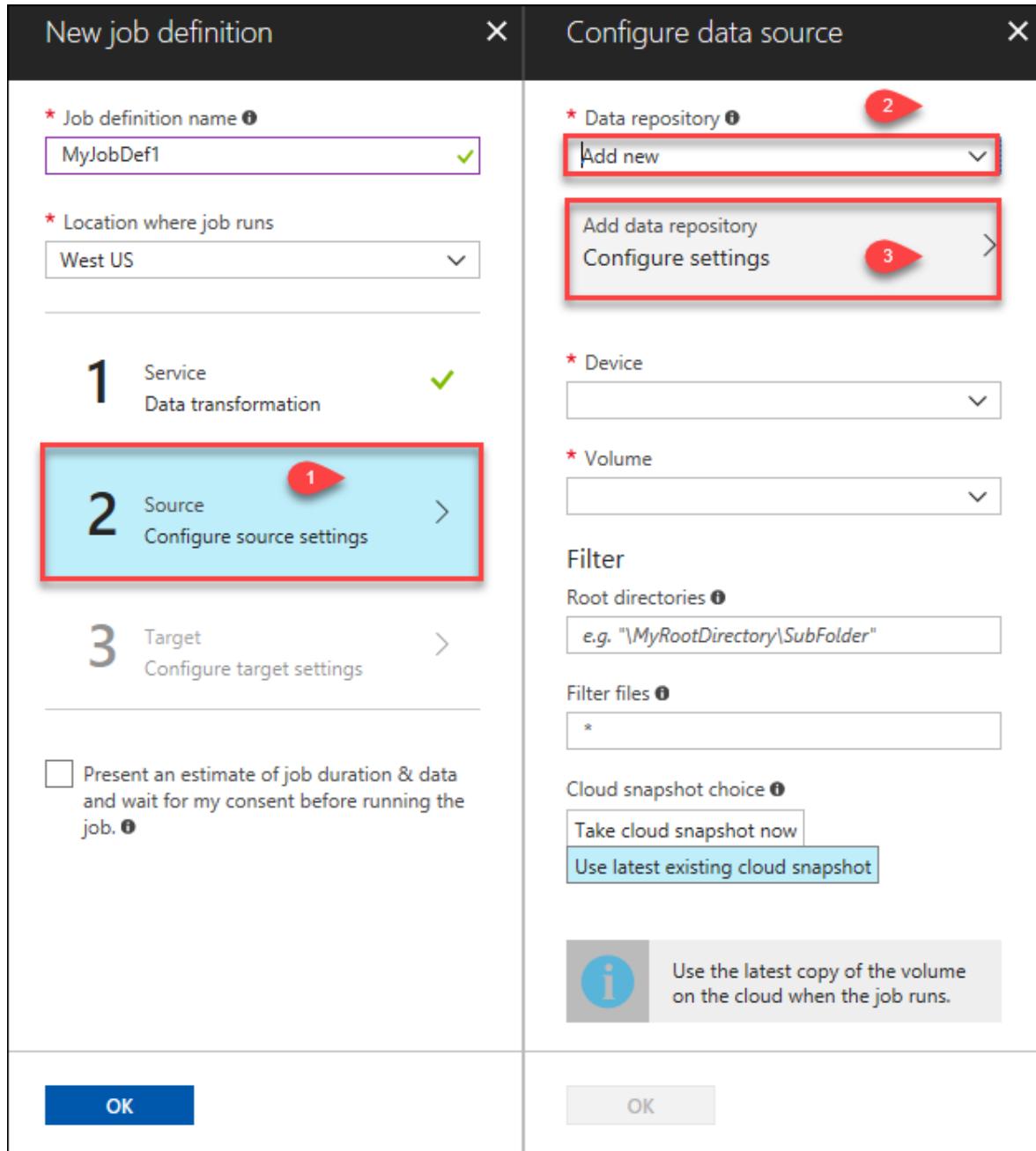
3. Provide a name for your job definition. The name can be between 3 and 63 characters. The name can contain uppercase and lowercase letters, numbers, and hyphens.
4. Specify a location where your job runs. This location can be different than the location where the service is deployed.
5. Click **Source** to specify the source data repository.



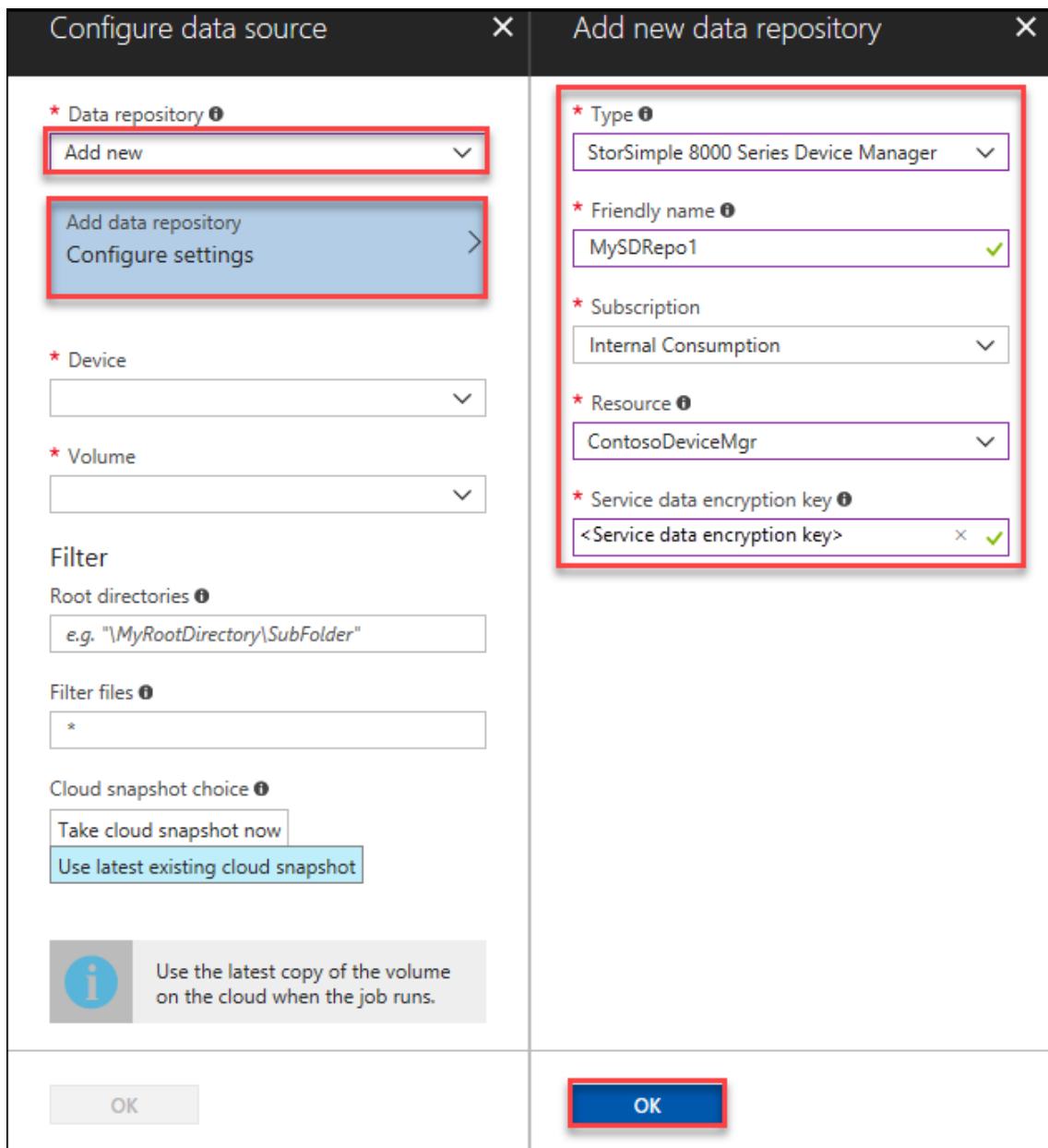
6. Since this is a new Data Manager service, no data repositories are configured. In **Configure data source**, specify the details of your StorSimple 8000 series device

and the data of interest.

To add your StorSimple Device Manager as a data repository, click **Add new** in the data repository dropdown and then click **Add Data Repository**.



- a. Choose **StorSimple 8000 series Manager** as the data repository type.
- b. Enter a friendly name for your source data repository.
- c. From the dropdown list, choose a subscription associated with your StorSimple Device Manager service.
- d. Provide the name of the StorSimple Device Manager for the **Resource**.
- e. Enter the **Service data encryption key** for the StorSimple Device Manager service.

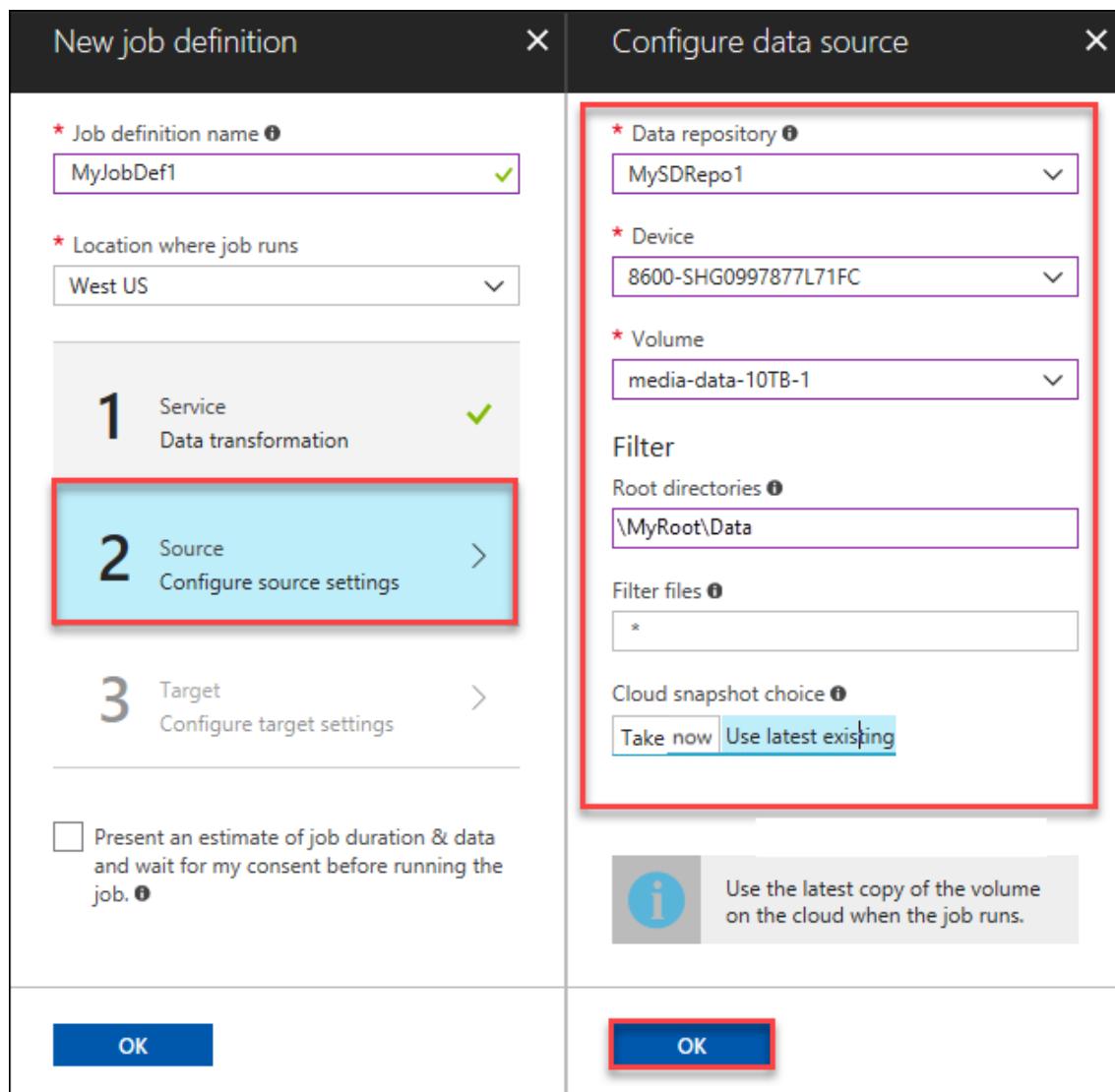


Click **OK** when done. This saves your data repository. Reuse this StorSimple Device Manager in other job definitions without entering these parameters again. It takes a few seconds after you click **OK** for the newly created source data repository to show up in the dropdown.

7. From the dropdown list for **Data repository**, select the data repository you created.
 - a. Enter the name of the StorSimple 8000 series device that contains the data of interest.
 - b. Specify the name of the volume residing on the StorSimple device that has your data of interest.
 - c. In the **Filter** subsection, enter the root directory that contains your data of interest in `\MyRootDirectory\Data` format. Drive letters such `\C:\Data` are not supported. You can also add any file filters here.

d. The data transformation service only works on the latest snapshot of the data that is pushed up to Azure.

e. Click **OK**.



8. Next, the target data repository needs to be configured. Choose storage accounts to put files into blobs in that account. In the dropdown, select **Add new** and then **Configure settings**.

9. Select the type of target repository you want to add and the other parameters associated with the repository.

If you select a Storage account type target, you can specify a friendly name, subscription (choose the same as that of the service or other), and a storage

account.

New job definition	Configure target settings	Add new data repository
<p>* Job definition name <input type="text" value="MyJobDef1"/> ✓</p> <p>* Location where job runs <input type="text" value="West US"/> ✓</p> <p>1 Service Data transformation</p> <p>2 Source MySDRepo1</p> <p>3 Target <input type="button" value="Configure target settings"/> ></p> <p><input type="checkbox"/> Present an estimate of job duration & data and wait for my consent before running the job. <small>(1)</small></p>	<p>* Target repository <input type="text" value="Add new"/> <small>(2)</small></p> <p>Add data repository <input type="button" value="Configure settings"/> > <small>(3)</small></p>	<p>* Type <input type="text" value="Storage account"/> <small>(4)</small></p> <p>* Friendly name <input type="text" value="MyTDrepo1"/> ✓</p> <p>Subscription <small>(5)</small></p> <p>* Storage account <input type="text" value="myssstoracct"/> <small>(6)</small></p> <p>Location <input type="text" value="Southeast Asia"/></p>
<input type="button" value="OK"/>	<input type="button" value="OK"/>	<input type="button" value="OK"/> <small>(7)</small>

A storage queue is created when the job runs. This queue is populated with messages about transformed blobs as they are ready. The name of this queue is the same as the name of the job definition.

10. After you add the data repository, wait a couple minutes.

- a. Select the repository you created as the target from the dropdown list in the **Target account name**.
- b. Choose the storage type as blobs or files. Specify the name of the storage container where the transformed data resides. Click **OK**.

Configure target settings X

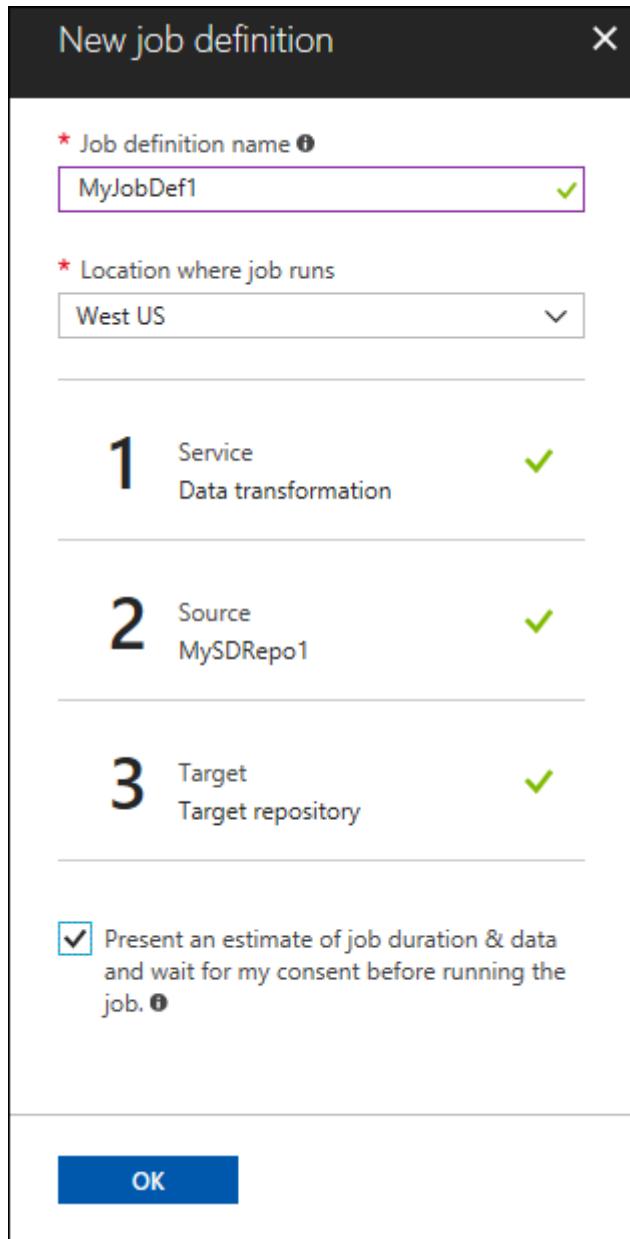
* Target repository

Storage type
 Blobs Files

* Storage container ✓

11. You can also check the option to present an estimate of job duration before you run the job. Click **OK** to create the job definition. Your job definition is now

complete. You can use this job definition multiple times via the UI with different runtime settings.



The newly created job definition is added to the list of job definitions for this service.

Run the job definition

Whenever you need to move data from StorSimple to the storage account that you have specified in the job definition, you need to run it. At runtime, some parameters can be specified differently. The steps are as follows:

1. Select your StorSimple Data Manager service and go to **Management > Job definitions**. Select and click the job definition that you want to run.

The screenshot shows the 'Job definitions' section of the MySSDataManager interface. On the left, there's a navigation bar with links like Overview, Activity log, Access control (IAM), Diagnose and solve problems, and Management (with 'Job definitions' highlighted). The main area displays a table of job definitions with columns for Name, Status, Last Modified, Source, Target, and an ellipsis button. Two entries are listed: 'MyJobDef1' (Active, 12/15/2017 8:34 AM, MySDRepo1, MyTDrepo1) and 'MyJobDef2' (Active, 12/15/2017 8:44 AM, MySDRepo1, MyDMSMediaAcct).

2. Click Run Now.

This screenshot shows the details for the 'MyJobDef1' job definition. It includes a header with 'Run now' and 'Delete' buttons, and a table with job metadata: Data source (MySDRepo1), Device & volumes (8600-StorSimple, media-data-10TB...), Data target (MyTDrepo1), and Last modified (12/15/2017 8:34:13 AM).

3. Click Run settings to modify any settings that you might want to change for this job run. Click OK and then click Run to launch your job.

The screenshot shows the 'Run job definition' dialog. It has fields for 'Data service' (DataTransformation) and 'Job definition name' (MyJobDef1). A 'Run settings' button is highlighted with a red box (1). To the right, a 'Run now' dialog is open, containing settings for 'Device' (8600-StorSimple), 'Volume' (media-data-10TB-1), 'Root directory' (\MyRoot\DMs), 'Filter files' (*), 'Cloud snapshot choice' (Take backup now / Use latest cloud snapshot), and a checked checkbox for presenting an estimate before running (2). At the bottom, there are 'Run' and 'OK' buttons, both highlighted with red boxes (3 and 4 respectively).

4. To monitor this job, go to **Jobs** in your StorSimple Data Manager. In addition to monitoring in the **Jobs** blade, you can also listen on the storage queue where a message is added every time a file is moved from StorSimple to the storage account.

The screenshot shows the 'MySSDataManager - Jobs' interface. On the left, there's a navigation bar with links like Overview, Activity log, Access control (IAM), Diagnose and solve problems, Job definitions, Data repositories, Locks, Usage (with a red circle '1'), and Jobs (with a red box and red circle '1'). The main area is a table titled 'Search' with columns: STATUS, STARTED ON, DURATION, JOB DEFINITION, SERVICE, and DATA PROCESSED. A single row is shown, highlighted with a red box and red circle '2': STATUS is 'In progress', STARTED ON is '12/15/2017 8:37 AM', DURATION is '1 minute, 36 seconds', JOB DEFINITION is 'MyJobDef1', SERVICE is 'Data transformation', and DATA PROCESSED is '0 Bytes'. There's also a '...' button at the end of the row.

View logs after job completion

After completion of a job, you can view the status of the job. Job status can be **Succeeded**, **Partially Succeeded** and **Failed**. You can view the list of files that were successfully copied and files that failed to be copied. These lists are available in a container called "**storsimple-data-manager-joblogs**" within your target storage account. Within this container, you can look for a folder with the same name as your job definition. Within this, a folder will be created for every job run which will contain your lists. The name of this folder will be the GUID of the job, which you can get from the job details page. Alternatively, in most cases you will see a link for the copy logs within the jobs page itself. There are 2 set of csv files that you will see in this folder. All files that start with **copiedfilelist...** will contain the list of successfully copied files. All files that start with **failedfilelist...** contain files that were not able to be copied, along with an error message.

Next steps

[Use .NET SDK to launch StorSimple Data Manager jobs.](#)

Use the .NET SDK to initiate data transformation

Article • 08/23/2022 • 4 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

This article explains how you can use the data transformation feature within the StorSimple Data Manager service to transform StorSimple device data. The transformed data is then consumed by other Azure services in the cloud.

You can launch a data transformation job in two ways:

- Use the .NET SDK
- Use Azure Automation runbook

This article details how to create a sample .NET console application to initiate a data transformation job and then track it for completion. To learn more about how to initiate data transformation via Automation, go to [Use Azure Automation runbook to trigger data transformation jobs](#).

Prerequisites

Before you begin, ensure that you have:

- A computer running:
 - Visual Studio 2012, 2013, 2015, or 2017.
 - Azure PowerShell. [Download Azure PowerShell](#).

- A correctly configured job definition in StorSimple Data Manager within a resource group.
- All the required dlls. Download these dlls from the [GitHub repository](#).
- [Get-ConfigurationParams.ps1](#) script from the GitHub repository.

Step-by-step procedure

Perform the following steps to use .NET to launch a data transformation job.

1. To retrieve the configuration parameters, do the following steps:
 - a. Download the `Get-ConfigurationParams.ps1` from the GitHub repository script in `C:\DataTransformation` location.
 - b. Run the `Get-ConfigurationParams.ps1` script from the GitHub repository. Type the following command:

```
C:\DataTransformation\Get-ConfigurationParams.ps1 -SubscriptionName
"AzureSubscriptionName" -ActiveDirectoryKey "AnyRandomPassword" -
AppName "ApplicationName"
```

You can pass in any values for the ActiveDirectoryKey and AppName.

2. This script outputs the following values:

- Client ID
- Tenant ID
- Active Directory key (same as the one entered above)
- Subscription ID

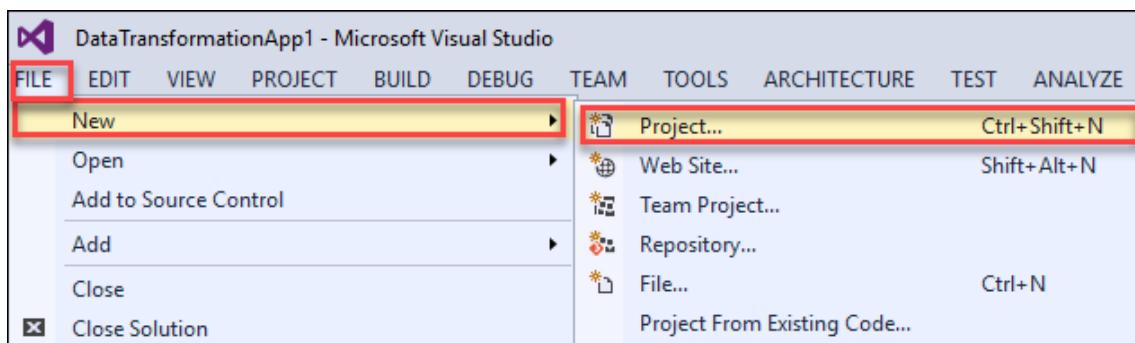
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\DataTransformation\Get-ConfigurationParams.ps1 -SubscriptionName "Internal Consumption"
-ActiveDirectoryKey "Password1234" -AppName "MyApp"
#####
+ Subscription Id: 2136cfze-684f-487b-9fc4-0acc9c0166e
#####
+ Tenant Id: 72f988bf-86f1-41af-91ab-2d7cd011db47
#####
+ Client Id: ade8d114-c517-4f6f-ad13-fa4b96343bce
#####
+ ActiveDirectoryKey: Password1234
PS C:\DataTransformation\Get-ConfigurationParams.ps1 -SubscriptionName "Internal Consumption"
-ActiveDirectoryKey "Password1234" -AppName "MyApp"
```

3. Using Visual Studio 2012, 2013 or 2015, create a C# .NET console application.

- a. Launch **Visual Studio 2012/2013/2015**.

b. Select File > New > Project.

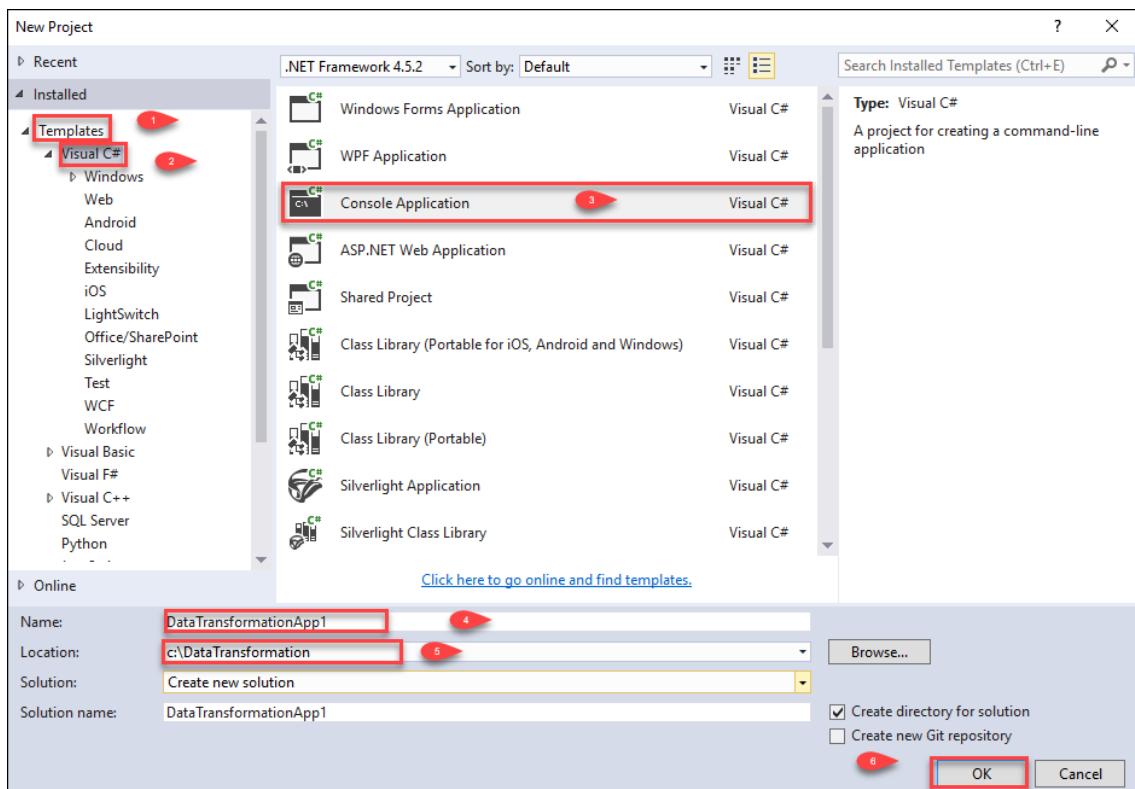


c. Select Installed > Templates > Visual C# > Console Application.

d. Enter DataTransformationApp for the Name.

e. Select C:\DataTransformation for the Location.

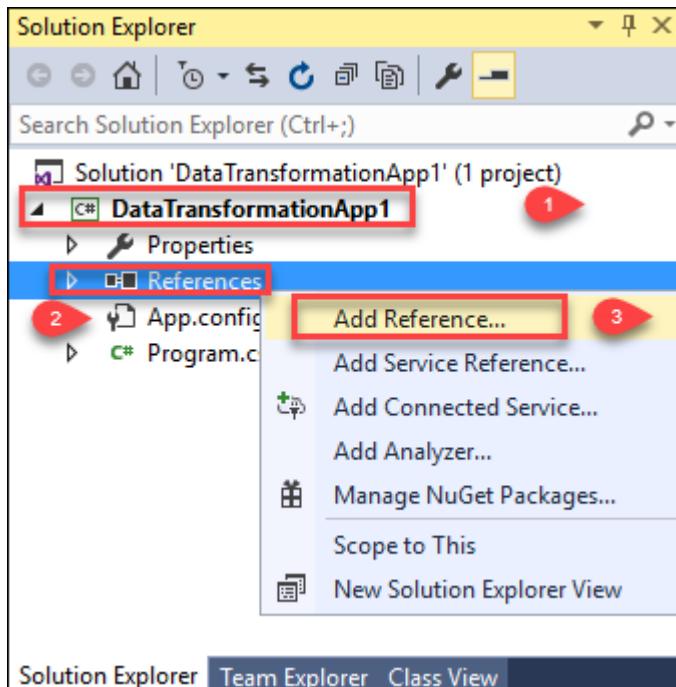
f. Click OK to create the project.



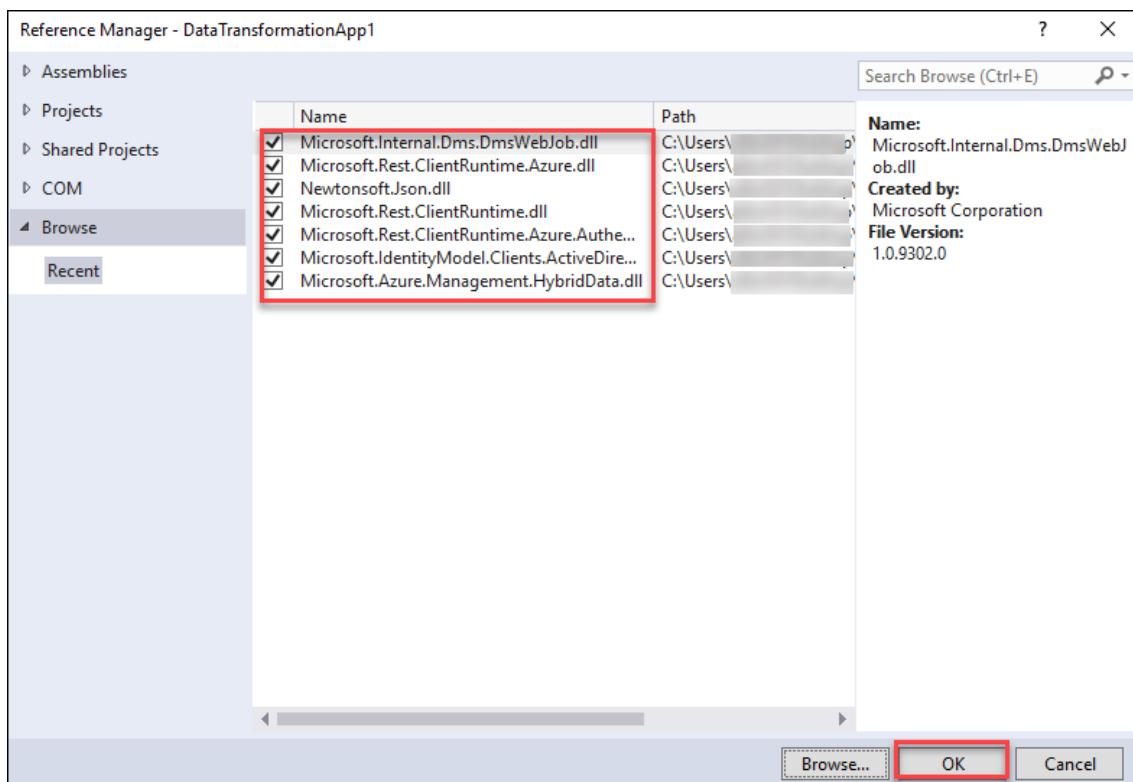
4. Now, add all dlls present in the [dlls folder](#) as References in the project that you created. To add the dll files, perform the following:

a. In Visual Studio, go to View > Solution Explorer.

b. Click the arrow to the left of Data Transformation App project. Click References and then right-click to Add Reference.



- c. Browse to the location of the packages folder, select all the dlls and click Add, and then click OK.



5. Add the following **using** statements to the source file (Program.cs) in the project.

```
using System;
using System.Collections.Generic;
using System.Threading;
using Microsoft.Azure.Management.HybridData.Models;
using Microsoft.Internal.Dms.DmsWebJob;
using Microsoft.Internal.Dms.DmsWebJob.Contracts;
```

6. The following code initializes the data transformation job instance. Add this in the **Main** method. Replace the values of configuration parameters as obtained earlier. Plug in the values of **Resource Group Name** and **ResourceName**. The **ResourceGroupName** is the associated with the StorSimple Data Manager on which the job definition was configured. The **ResourceName** is the name of your StorSimple Data Manager service.

```
// Setup the configuration parameters.  
var configParams = new ConfigurationParams  
{  
    ClientId = "client-id",  
    TenantId = "tenant-id",  
    ActiveDirectoryKey = "active-directory-key",  
    SubscriptionId = "subscription-id",  
    ResourceGroupName = "resource-group-name",  
    ResourceName = "resource-name"  
};  
  
// Initialize the Data Transformation Job instance.  
DataTransformationJob dataTransformationJob = new  
DataTransformationJob(configParams);
```

7. Specify the parameters with which the job definition needs to be run

```
string jobDefinitionName = "job-definition-name";  
  
DataTransformationInput dataTransformationInput =  
dataTransformationJob.GetJobDefinitionParameters(jobDefinitionName);
```

(OR)

If you want to change the job definition parameters during run time, then add the following code:

```
string jobDefinitionName = "job-definition-name";  
// Must start with a '\'  
var rootDirectories = new List<string> {@"\root"};  
  
// Name of the volume on the StorSimple device.  
var volumeNames = new List<string> {"volume-name"};
```

```
var dataTransformationInput = new DataTransformationInput
{
    // If you require the latest existing backup to be picked else use
    TakeNow to trigger a new backup.
    BackupChoice = BackupChoice.UseExistingLatest.ToString(),
    // Name of the StorSimple device.
    DeviceName = "device-name",
    // Name of the container in Azure storage where the files will be
    placed after execution.
    ContainerName = "container-name",
    // File name filter (search pattern) to be applied on files under
    the root directory. * - Match all files.
    FileNameFilter = "*",
    // List of root directories.
    RootDirectories = rootDirectories,
    // Name of the volume on StorSimple device on which the relevant
    data is present.
    VolumeNames = volumeNames
};
```

8. After the initialization, add the following code to trigger a data transformation job on the job definition. Plug in the appropriate **Job Definition Name**.

```
// Trigger a job, retrieve the jobId and the retry interval for
polling.
int retryAfter;
string jobId = dataTransformationJob.RunJobAsync(jobDefinitionName,
dataTransformationInput, out retryAfter);
Console.WriteLine("jobid: ", jobId);
Console.ReadLine();
```

Once the code is pasted, build the solution. Here is a screenshot of the code snippet to initialize the data transformation job instance.

```

Program.cs # X DataTransformationApp1
namespace DataTransformationApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            // Setup the configuration parameters.
            var configParams = new ConfigurationParams
            {
                ClientId = "client-id",
                TenantId = "tenant-id",
                ActiveDirectoryKey = "active-directory-key",
                SubscriptionId = "subscription-id",
                ResourceGroupName = "resource-group-name",
                ResourceName = "resource-name"
            };

            // Initialize the Data Transformation Job instance.
            DataTransformationJob dataTransformationJob = new DataTransformationJob(configParams);

            string jobDefinitionName = "MyJobDef3";
            DataTransformationInput dataTransformationInput = dataTransformationJob.GetJobDefinitionParameters(jobDefinitionName);
        }
    }
}

100 % < 
Output
Show output from: Build
1>----- Build started: Project: DataTransformationApp1, Configuration: Debug Any CPU -----
1> DataTransformationApp1 -> c:\DataTransformation\DataTransformationApp1\bin\Debug\DataTransformationApp1.exe
===== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped =====
Build succeeded

```

9. This job transforms the data that matches the root directory and file filters within the StorSimple volume and puts it into the specified container/file share. When a file is transformed, a message is added to a storage queue (in the same storage account as the container/file share) with the same name as the job definition. This message can be used as a trigger to initiate any further processing of the file.
10. Once the job has been triggered, you can use the following code to track the job for completion. It is not mandatory to add this code for the job run.

```

Job jobDetails = null;

// Poll the job.
do
{
    jobDetails = dataTransformationJob.GetJob(jobDefinitionName,
    jobId);

    // Wait before polling for the status again.
    Thread.Sleep(TimeSpan.FromSeconds(retryAfter));

} while (jobDetails.Status == JobStatus.InProgress);

// Completion status of the job.
Console.WriteLine("JobStatus: {0}", jobDetails.Status);

// To hold the console before exiting.
Console.Read();

```

Here is a screenshot of the entire code sample used to trigger the job using .NET.

```
Program.cs  X
DataTransformationApp1
DataTransformationApp1.Program
using System;
using System.Collections.Generic;
using System.Threading;
using Microsoft.Azure.Management.HybridData.Models;
using Microsoft.Internal.Dms.DmsWebJob;
using Microsoft.Internal.Dms.DmsWebJob.Contracts;

namespace DataTransformationApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            // Setup the configuration parameters.
            var configParams = new ConfigurationParams
            {
                ClientId = "REDACTED",
                TenantId = "REDACTED",
                ActiveDirectoryKey = "Password1234",
                SubscriptionId = "REDACTED",
                ResourceGroupName = "myssdmsrg",
                ResourceName = "MySSDataManager"
            };

            // Initialize the Data Transformation Job instance.
            DataTransformationJob dataTransformationJob = new DataTransformationJob(configParams);

            string jobDefinitionName = "MyJobDef3";

            DataTransformationInput dataTransformationInput = dataTransformationJob.GetJobDefinitionParameters(jobDefinitionName);

            // Trigger a job, retrieve the jobId and the retry interval for polling.
            int retryAfter;
            string jobId = dataTransformationJob.RunJobAsync(jobDefinitionName,
                dataTransformationInput, out retryAfter);

            Job jobDetails = null;

            // Poll the job.
            do
            {
                jobDetails = dataTransformationJob.GetJob(jobDefinitionName, jobId);

                // Wait before polling for the status again.
                Thread.Sleep(TimeSpan.FromSeconds(retryAfter));
            }
        }
    }
}

// Output
Show output from: Build
1> DataTransformationApp1 -> c:\DataTransformation\DataTransformationApp1\bin\Debug\DataTransformationApp1.exe
===== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped =====
Build succeeded
```

Next steps

Use StorSimple Data Manager UI to transform your data.

Additional resources

Training

Certification

[Microsoft Certified: Azure Enterprise Data Analyst Associate - Certifications](#)

Azure enterprise data analysts perform advanced data analytics at scale, such as cleaning and transforming data, designing and building enterprise data models, incorporating advanced analytics capabilities, integrating with IT infrastructure, and applying development lifecycle practices.

Use Azure Automation to trigger a job

Article • 08/23/2022 • 3 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

This article explains how you can use the data transformation feature within the StorSimple Data Manager service to transform StorSimple device data. You can launch a data transformation job in two ways:

- Use the .NET SDK
- Use Azure Automation runbook

This article details how to create an Azure Automation runbook and then use it to initiate a data transformation job. To learn more about how to initiate data transformation via .NET SDK, go to [Use .NET SDK to trigger data transformation jobs](#).

Prerequisites

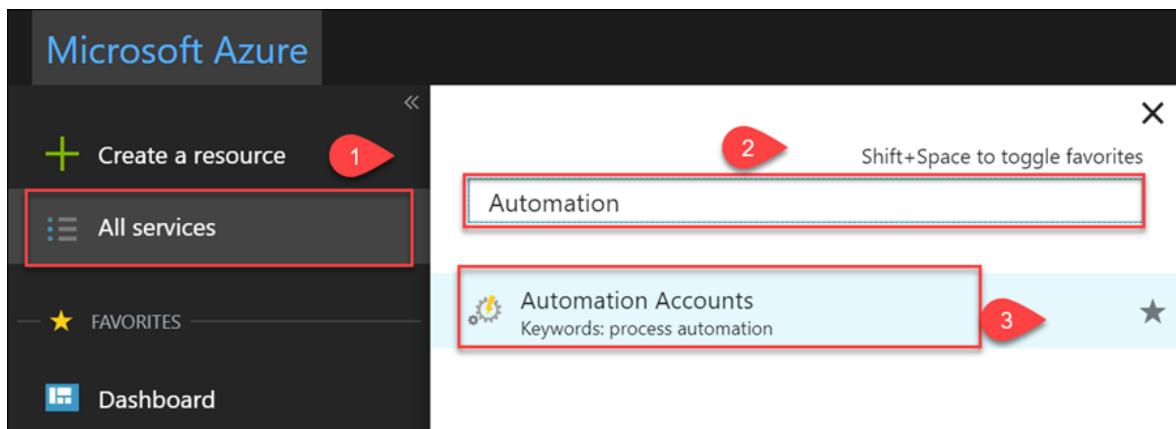
Before you begin, ensure that you have:

- Azure PowerShell installed on the client computer. [Download Azure PowerShell](#).
- A correctly configured job definition in a StorSimple Data Manager service within a resource group.
- Download [DataTransformationApp.zip](#) file from the GitHub repository.
- Download [Trigger-DataTransformation-Job.ps1](#) script from the GitHub repository.

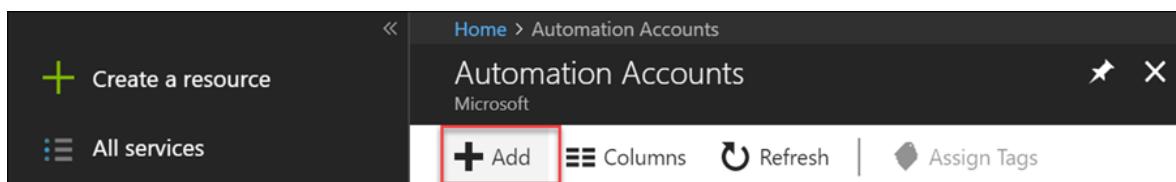
Step-by-step procedure

Set up the Automation account

1. Create an Azure Run As automation account in the Azure portal. To do so, go to **Azure marketplace > Everything** and then search for **Automation**. Select **Automation accounts**.



2. To add a new automation account, click **+ Add**.



3. In the **Add Automation**:

- a. Supply the **Name** of your automation account.
- b. Select the **Subscription** linked to your StorSimple Data Manager service.
- c. Create a new resource group or select from an existing resource group.
- d. Select a **Location**.
- e. Leave the default **Create Run As account** option selected.
- f. To get a link for quick access on the dashboard, check **Pin to dashboard**. Click **Create**.

A screenshot of the 'Add Automation Account' dialog box. The title is 'Add Automation Account'. The form contains two required fields: 'Name' (1) with the value 'myssdmsautoacct' and a green checkmark, and 'Subscription' (2) with the value 'Internal Consumption'. Both fields are highlighted with red boxes.

* Resource group 3

Create new Use existing

myssdmsrsg ✓

* Location 4

Japan East ▼

* Create Azure Run As account 1



The Run As account feature will create a Run As account and a Classic Run As account. [Click here to learn more about Run As accounts.](#)



Learn more about Automation pricing. ↗

Pin to dashboard

5

After the automation account is successfully created, you are notified.

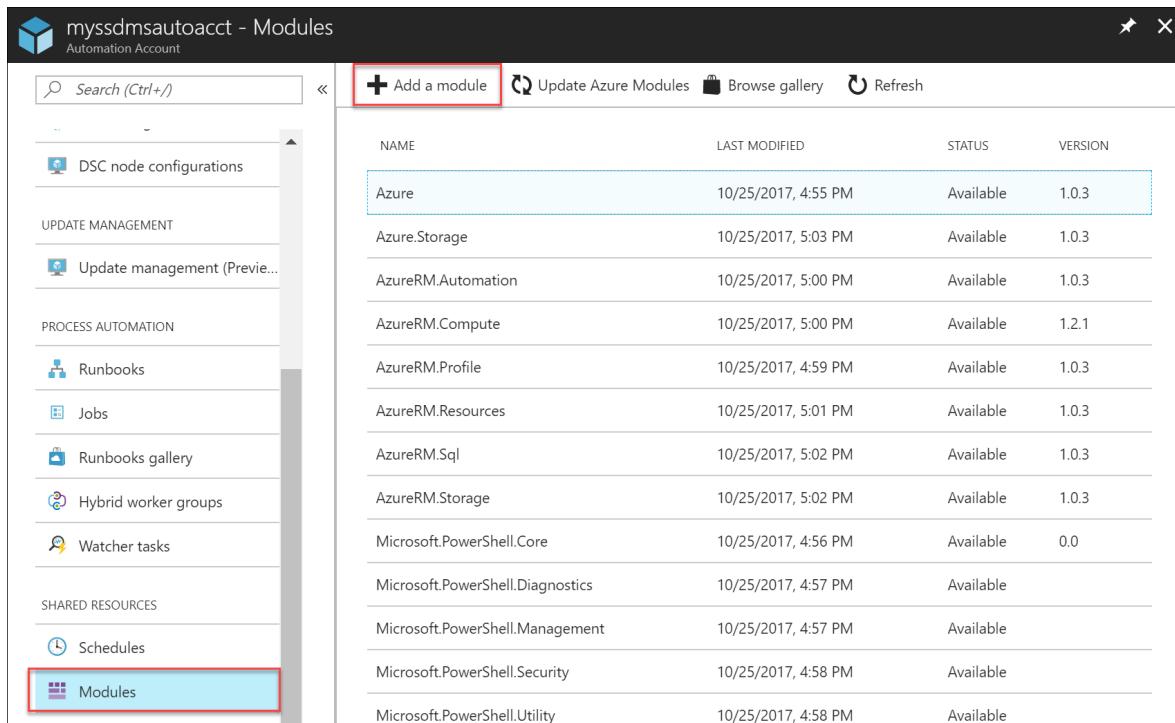


New Azure Run As account (service princip...10:14 AM X

Azure Run As account (service principal) for account 'myssdmsautoacct' was created successfully and assigned the Contributor role to this user at the subscription level.

For more information, go to [Create a Run As account](#).

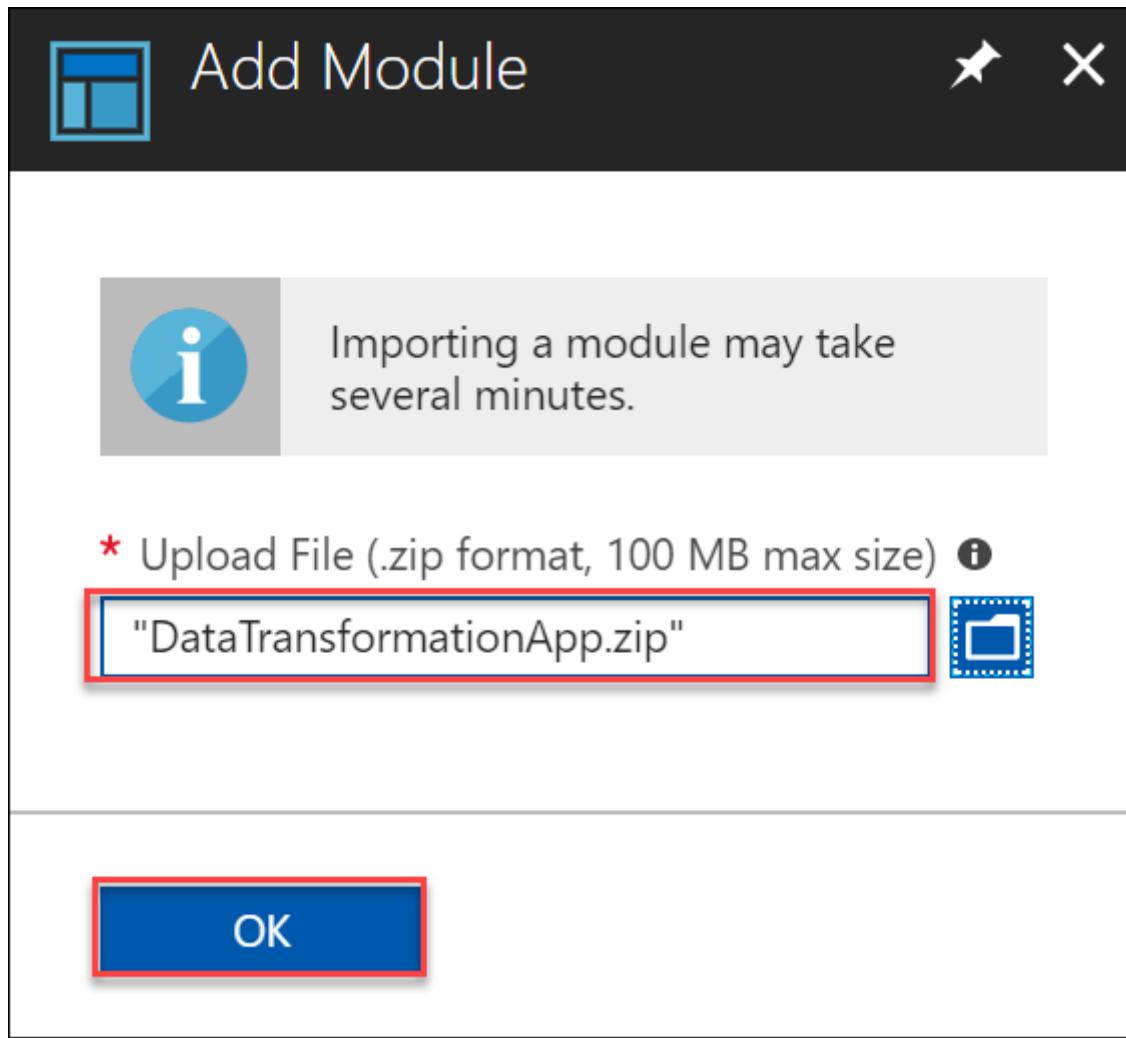
4. In the newly created account, go to **Shared Resources > Modules** and click **+ Add module**.



The screenshot shows the 'myssdmsautoacct - Modules' page in the Azure portal. On the left, there's a navigation menu with links like 'DSC node configurations', 'UPDATE MANAGEMENT', 'PROCESS AUTOMATION', 'Runbooks', 'Jobs', 'Runbooks gallery', 'Hybrid worker groups', 'Watcher tasks', 'SHARED RESOURCES', 'Schedules', and 'Modules'. The 'Modules' link is highlighted with a red box. The main area displays a table of modules with columns: NAME, LAST MODIFIED, STATUS, and VERSION. The table lists various Azure-related modules such as 'Azure', 'Azure.Storage', 'AzureRM.Automation', etc., all marked as 'Available' with version 1.0.3 or 1.0.0.

NAME	LAST MODIFIED	STATUS	VERSION
Azure	10/25/2017, 4:55 PM	Available	1.0.3
Azure.Storage	10/25/2017, 5:03 PM	Available	1.0.3
AzureRM.Automation	10/25/2017, 5:00 PM	Available	1.0.3
AzureRM.Compute	10/25/2017, 5:00 PM	Available	1.2.1
AzureRM.Profile	10/25/2017, 4:59 PM	Available	1.0.3
AzureRM.Resources	10/25/2017, 5:01 PM	Available	1.0.3
AzureRM.Sql	10/25/2017, 5:02 PM	Available	1.0.3
AzureRM.Storage	10/25/2017, 5:02 PM	Available	1.0.3
Microsoft.PowerShell.Core	10/25/2017, 4:56 PM	Available	0.0
Microsoft.PowerShell.Diagnostics	10/25/2017, 4:57 PM	Available	
Microsoft.PowerShell.Management	10/25/2017, 4:57 PM	Available	
Microsoft.PowerShell.Security	10/25/2017, 4:58 PM	Available	
Microsoft.PowerShell.Utility	10/25/2017, 4:58 PM	Available	

5. Browse to the location of `DataTransformationApp.zip` file from your local computer, and select and open the module. Click **OK** to import the module.



When Azure Automation imports a module to your account, it extracts metadata about the module. This operation may take a couple of minutes.

NAME	LAST MODIFIED	STATUS	VERSION
Azure	10/25/2017, 4:55 PM	Available	1.0.3
Azure.Storage	10/25/2017, 5:03 PM	Available	1.0.3
AzureRM.Automation	10/25/2017, 5:00 PM	Available	1.0.3
AzureRM.Compute	10/25/2017, 5:00 PM	Available	1.2.1
AzureRM.Profile	10/25/2017, 4:59 PM	Available	1.0.3
AzureRM.Resources	10/25/2017, 5:01 PM	Available	1.0.3
AzureRM.Sql	10/25/2017, 5:02 PM	Available	1.0.3
AzureRM.Storage	10/25/2017, 5:02 PM	Available	1.0.3
DataTransformationApp	12/12/2017, 10:17 AM	Importing	
Microsoft.PowerShell.Core	10/25/2017, 4:56 PM	Available	0.0
Microsoft.PowerShell.Diagnostics	10/25/2017, 4:57 PM	Available	
Microsoft.PowerShell.Management	10/25/2017, 4:57 PM	Available	

6. You receive a notification that the module is being deployed and another notification when the process is complete. The status in **Modules** changes to **Available**.

NAME	LAST MODIFIED	STATUS	VERSION
Azure	10/25/2017, 4:55 PM	Available	1.0.3
Azure.Storage	10/25/2017, 5:03 PM	Available	1.0.3
AzureRM.Automation	10/25/2017, 5:00 PM	Available	1.0.3
AzureRM.Compute	10/25/2017, 5:00 PM	Available	1.2.1
AzureRM.Profile	10/25/2017, 4:59 PM	Available	1.0.3
AzureRM.Resources	10/25/2017, 5:01 PM	Available	1.0.3
AzureRM.Sql	10/25/2017, 5:02 PM	Available	1.0.3
AzureRM.Storage	10/25/2017, 5:02 PM	Available	1.0.3
DataTransformationApp	12/12/2017, 10:18 AM	Available	1.0.0.0
Microsoft.PowerShell.Core	10/25/2017, 4:56 PM	Available	0.0
Microsoft.PowerShell.Diagnostics	10/25/2017, 4:57 PM	Available	
Microsoft.PowerShell.Management	10/25/2017, 4:57 PM	Available	
Microsoft.PowerShell.Security	10/25/2017, 4:58 PM	Available	

Import, publish, and run Automation runbook

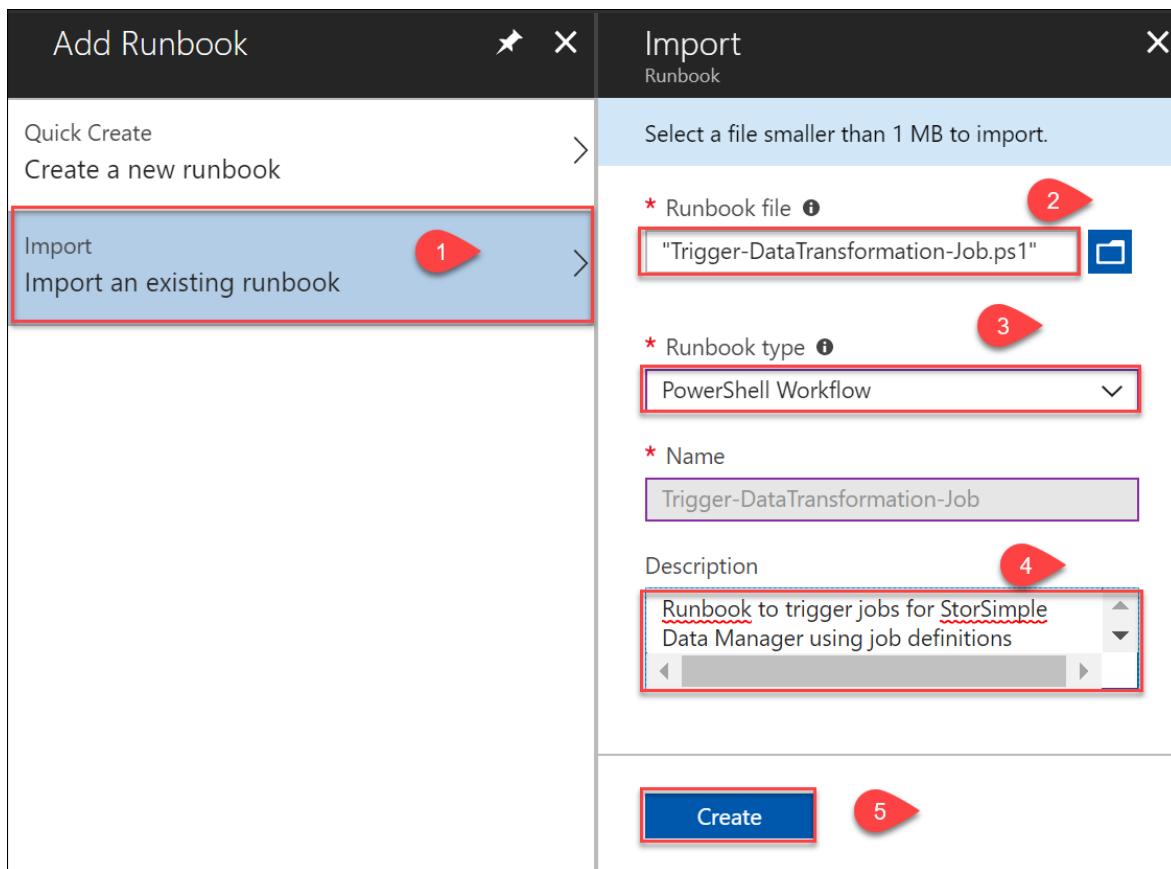
Perform the following steps to import, publish, and run the runbook to trigger job definition.

1. In the Azure portal, open your Automation account. Go to **Process Automation > Runbooks** and click **+ Add a runbook**.

NAME	AUTHORING STATUS	LAST MODIFIED
AzureAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialPython2	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM

2. In **Add runbook**, click **Import an existing runbook**.

3. Point to the Azure PowerShell script file `Trigger-DataTransformation-Job.ps1` for the **Runbook file**. The runbook type is automatically selected. Provide a name and an optional description for the runbook. Click **Create**.



4. The new runbook appears in the list of runbooks for the Automation account. Select and click this runbook.

NAME	AUTHORING STATUS	LAST MODIFIED
AzureAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialPython2	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM
Trigger-DataTransformation-Job	★ New	12/12/2017, 10:27 AM

5. Edit the runbook and click **Test** pane.

6. Provide the parameters such as the name of your StorSimple Data Manager service, the associated resource group and the job definition name. **Start** the test. The report is generated when the run is complete. For more information, go to how to [test a runbook](#).





test

Trigger-DataTransformation-Job

Start

Stop

Suspend

Re

Parameters

*** RESOURCEGROUPNAME** ⓘ

myssdmsresgrp

*Mandatory, String**** DATAMANAGERNAME** ⓘ

MySSDMS1

*Mandatory, String**** JOBDEFINITIONNAME** ⓘ

MyJD1

*Mandatory, String*

Run Settings

Run on Azure ⓘ



Using a hybrid runbook worker can increase test performance.

[Learn more](#)

Activity-level tracing

This configuration is available only for

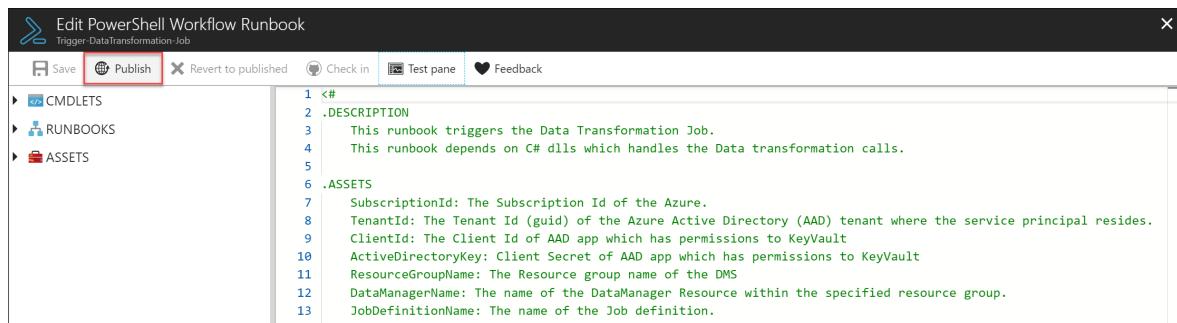
graphical runbooks.

Trace level

None Basic Detailed

7. Inspect the output from the runbook in the test pane. If satisfied, close the pane.

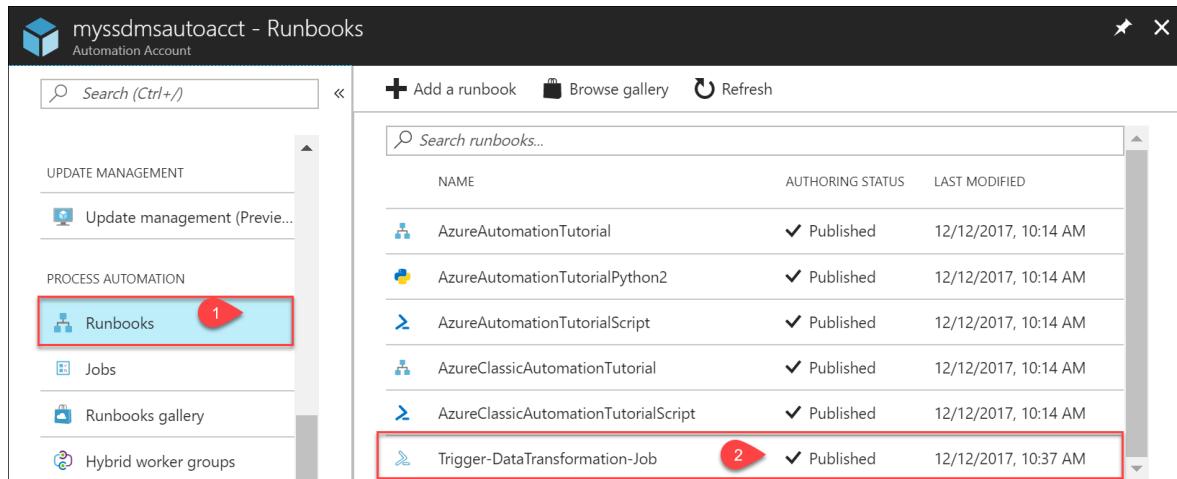
Click **Publish** and when prompted for confirmation, confirm, and publish the runbook.



```
<#>
.DESCRIPTION
    This runbook triggers the Data Transformation Job.
    This runbook depends on C# dlls which handles the Data transformation calls.

.ASSETS
SubscriptionId: The Subscription Id of the Azure.
TenantId: The Tenant Id (guid) of the Azure Active Directory (AAD) tenant where the service principal resides.
ClientId: The Client Id of AAD app which has permissions to KeyVault
ActiveDirectoryKey: Client Secret of AAD app which has permissions to KeyVault
ResourceGroupName: The Resource group name of the DMS
DataManagerName: The name of the DataManager Resource within the specified resource group.
JobDefinitionName: The name of the Job definition.
```

8. Go back to **Runbooks** and select the newly created runbook.



The screenshot shows the 'Runbooks' blade in the Azure portal. On the left, there's a navigation menu with 'Runbooks' selected (marked with a red arrow 1). The main area lists several runbooks with their names, authoring status, and last modified date. One runbook, 'Trigger-DataTransformation-Job', is highlighted with a red box and a red arrow 2, indicating it's the newly created runbook.

NAME	AUTHORING STATUS	LAST MODIFIED
AzureAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialPython2	✓ Published	12/12/2017, 10:14 AM
AzureAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorial	✓ Published	12/12/2017, 10:14 AM
AzureClassicAutomationTutorialScript	✓ Published	12/12/2017, 10:14 AM
Trigger-DataTransformation-Job	✓ Published	12/12/2017, 10:37 AM

9. Start the runbook. In **Start runbook**, enter all the parameters. Click **OK** to submit and start the data transformation job.

10. To monitor the job progress in Azure portal, go to **Jobs** in your StorSimple Data Manager service. Select and click the job to view the job details.

The screenshot shows the StorSimple Data Manager interface. On the left, there's a navigation sidebar with sections like Overview, Activity log, Access control (IAM), Diagnose and solve problems, MANAGEMENT (Job definitions, Data repositories, Locks), and MONITORING (Usage). The 'Jobs' item under MONITORING is highlighted with a red box. The main area is a table titled 'Search' with columns: STATUS, STARTED ON, DURATION, JOB DEFINITION, SERVICE, and DATA PROCESSED. It lists four jobs: one In progress (myjd3), one Canceled (myjd4), one Failed (myjd2), and one Succeeded (myjd1). The 'Jobs' section in the sidebar and the first row of the table are also highlighted with red boxes.

STATUS	STARTED ON	DURATION	JOB DEFINITION	SERVICE	DATA PROCESSED
In progress	12/21/2017, 6:57 PM	1 minute, 45 seconds	myjd3	Data transformation	0 Bytes
Canceled	12/21/2017, 5:48 PM	6 minutes, 23 seconds	myjd4	Data transformation	0 Bytes
Failed	12/21/2017, 5:45 PM	34 minutes, 29 seconds	myjd2	Data transformation	0 Bytes
Succeeded	12/20/2017, 2:10 PM	43 minutes, 43 seconds	myjd1	Data transformation	1.25 GB

Next steps

Use StorSimple Data Manager UI to transform your data.

Change a blob path from the default path

Article • 09/21/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

When the StorSimple Data Manager service transforms the data, by default it places the transformed blobs in a storage container as specified during the creation of the target repository. As the blobs arrive at this location, you may want to move these blobs to an alternate location. This article describes how to set up an Azure function to rename a default blob file path and hence move the blobs to a different location.

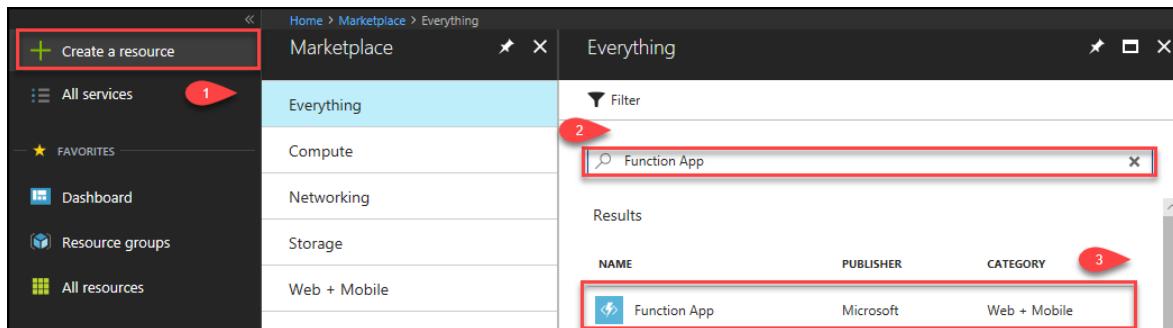
Prerequisites

Ensure that you have a correctly configured job definition in your StorSimple Data Manager service.

Create an Azure function

To create an Azure function, perform the following steps:

1. Go to the [Azure portal](#).
2. Click **+ Create a resource**. In the **Search** box, type **Function App** and press **Enter**. Select and click **Function app** in the list of apps displayed.



3. Click **Create**.

Function App
Microsoft

Write any function in minutes – whether to run a simple job that cleans up a database or build a more complex architecture. Creating functions is easier than ever before, whatever your chosen OS, platform, or development method.

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)

PUBLISHER	Microsoft
USEFUL LINKS	Documentation Solution Overview Pricing Details

Create

4. On the **Function App** configuration blade, perform the following steps:

- Provide a unique **App name**.
- From the dropdown list, select the **Subscription**. This subscription should be the same as the one associated with your StorSimple Data Manager service.
- Select **Create new resource group**.
- For the **Hosting Plan** dropdown list, select **Consumption Plan**.
- Specify a location where your function runs. You want the same region where the StorSimple Data Manager service and the storage account associated with the job definition, are located.
- Select an existing storage account or create a new storage account. A storage account is used internally for the function.

Function App

Create

* App name
RenameBlob .azurewebsites.net

* Subscription
Microsoft Azure Internal Consumption

* Resource Group
 Create new Use existing
RenameBlobRG

* OS Windows Linux (Preview)

* Hosting Plan
Consumption Plan

* Location
West US

* Storage
 Create new Use existing
renameblob8f06

Application Insights On Off

Pin to dashboard

Create **Automation options**

g. Click **Create**. The function app is created.

RenameBlob
Function Apps

"RenameBlob"

Microsoft Azure Internal Consumption

Function Apps

RenameBlob

Functions

Proxies

Slots (preview)

Overview Platform features

Status Running Subscription Microsoft Azure Internal Consumption Resource group RenameBlobRG URL <https://renameblob.azurewebsites.net>

Subscription ID <Subscription ID> Location West US App Service plan / pricing tier WestUSPlan (Consumption)

Configured features

5. Select **Functions**, and click **+ New function**.

The screenshot shows the Azure Functions portal interface. At the top, it says "RenameBlob" and "Function Apps". On the left, there's a sidebar with a search bar containing "RenameBlob", a dropdown for "Microsoft Azure Internal Consumption", and a tree view showing "Function Apps" and "RenameBlob" (which is expanded, with "Functions" highlighted by a red box). On the right, there's a "Functions" section with a search bar, a table header for "NAME" and "STATUS", and a message "No results". In the top right corner of the main area, there's a "New function" button with a plus sign, also highlighted by a red box.

6. Select **C#** for the language. In the array of template tiles, select **C#** in the **QueueTrigger-CSharp** tile.

7. In the **Queue trigger**:

a. Enter a **Name** for your function.

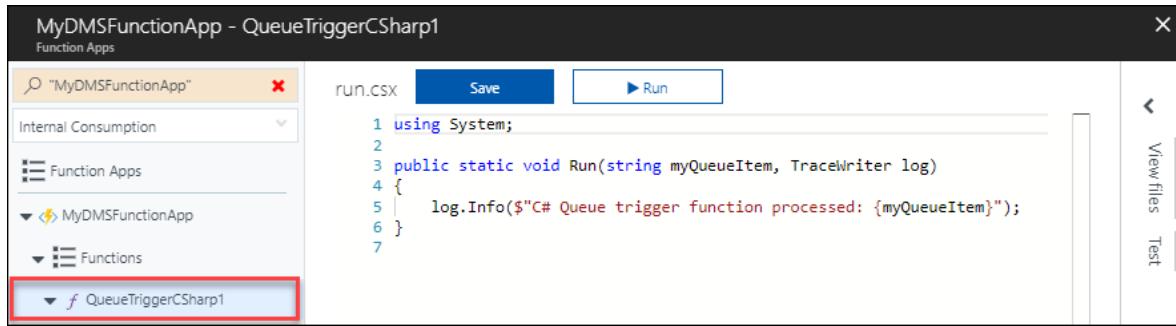
b. In the **Queue name** box, type your data transformation job definition name.

c. Under **Storage account connection**, click **new**. From the list of storage accounts, select the account associated with your job definition. Make a note of the connection name (highlighted). The name is required later in the Azure function.

The screenshot shows the "New Function" dialog for a "Queue trigger". The "Language" is set to "C#". The "Name" field contains "QueueTriggerCSharp1". The "Queue name" field contains "myjobdef3". The "Storage account connection" field contains "stor simple dms_STORAGE", which is highlighted with a yellow background. At the bottom, there are "Create" and "Cancel" buttons, with the "Create" button highlighted by a red box.

d. Click **Create**. The Function is created.

8. In the Function window, run .csx file.



Perform the following steps.

a. Paste the following code:

```
C#
```

```
using System;
using System.Configuration;
using Microsoft.WindowsAzure.Storage.Blob;
using Microsoft.WindowsAzure.Storage.Queue;
using Microsoft.WindowsAzure.Storage;
using System.Collections.Generic;
using System.Linq;

public static void Run(QueueItem myQueueItem, TraceWriter log)
{
    CloudStorageAccount storageAccount =
CloudStorageAccount.Parse(ConfigurationManager.AppSettings[ "STORAGE_
CONNECTIONNAME" ]);

    string storageAccUriEndswith = "windows.net/";
    string uri = myQueueItem.TargetLocation.Replace("%20", " ");
    log.Info($"Blob Uri: {uri}");

    // Remove storage account uri string
    uri = uri.Substring(uri.IndexOf(storageAccUriEndswith) +
storageAccUriEndswith.Length);

    string containerName = uri.Substring(0, uri.IndexOf("/"));

    // Remove container name string
    uri = uri.Substring(containerName.Length + 1);

    // Current blob path
    string blobName = uri;

    string volumeName = uri.Substring(containerName.Length + 1);
    volumeName = uri.Substring(0, uri.IndexOf("/"));

    // Remove volume name string
```

```

uri = uri.Substring(volumeName.Length + 1);

    string newContainerName = uri.Substring(0,
uri.IndexOf("/").ToLower());
    string newBlobName = uri.Substring(newContainerName.Length + 1);

    log.Info($"Container name: {containerName}");
    log.Info($"Volume name: {volumeName}");
    log.Info($"New container name: {newContainerName}");

    log.Info($"Blob name: {blobName}");
    log.Info($"New blob name: {newBlobName}");

    // Create the blob client.
    CloudBlobClient blobClient =
storageAccount.CreateCloudBlobClient();

    // Container reference
    CloudBlobContainer container =
blobClient.GetContainerReference(containerName);
    CloudBlobContainer newContainer =
blobClient.GetContainerReference(newContainerName);
    newContainer.CreateIfNotExists();

    if(!container.Exists())
{
    log.Info($"Container - {containerName} not exists");
    return;
}

    if(!newContainer.Exists())
{
    log.Info($"Container - {newContainerName} not exists");
    return;
}

CloudBlockBlob blob = container.GetBlockBlobReference(blobName);
if (!blob.Exists())
{
    // Skip to copy the blob to new container, if source blob
doesn't exist
    log.Info($"The specified blob does not exist.");
    log.Info($"Blob Uri: {blob.Uri}");
    return;
}

    CloudBlockBlob blobCopy =
newContainer.GetBlockBlobReference(newBlobName);
    if (!blobCopy.Exists())
{
    blobCopy.StartCopy(blob);
    // Delete old blob, after copy to new container
    blob.DeleteIfExists();
    log.Info($"Blob file path renamed completed successfully");
}

```

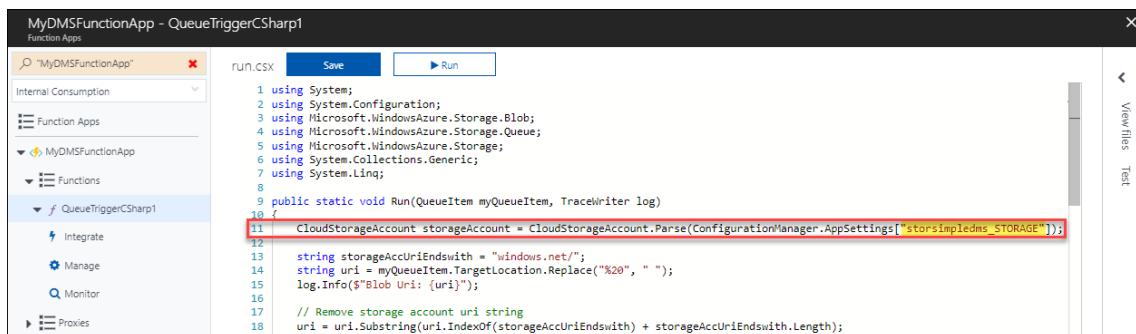
```

        else
    {
        log.Info($"Blob file path renamed already done");
        // Delete old blob, if already exists.
        blob.DeleteIfExists();
    }
}

public class QueueItem
{
    public string SourceLocation {get;set;}
    public long SizeInBytes {get;set;}
    public string Status {get;set;}
    public string JobID {get;set;}
    public string TargetLocation {get; set;}
}

```

- b. Replace **STORAGE_CONNECTIONNAME** on line 11 with your storage account connection (refer step 7c).



- c. Save the function.

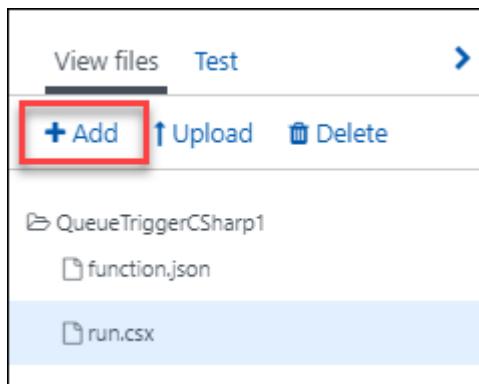


9. To complete the function, add one more file by doing the following steps:

- a. Click **View files**.



b. Click + Add.

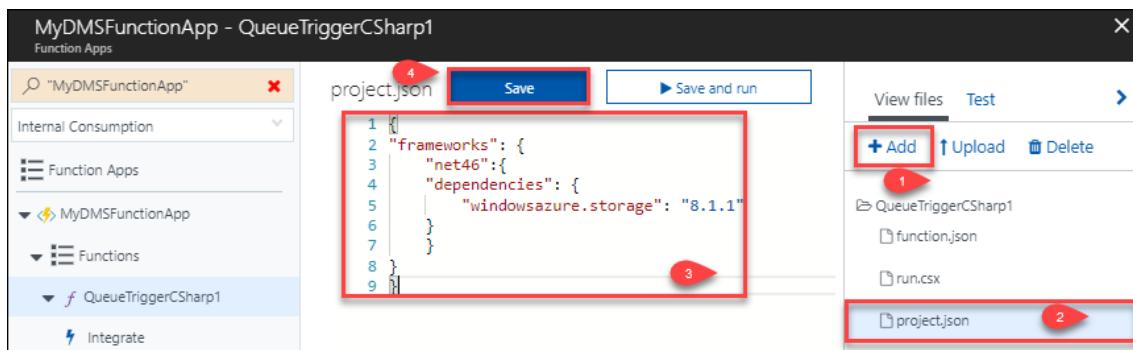


c. Type **project.json**, and then press **Enter**. In the **project.json** file, paste the following code:

A screenshot of a code editor window titled 'JSON'. It contains the following JSON code:

```
{
  "frameworks": {
    "net46": {
      "dependencies": {
        "windowsazure.storage": "8.1.1"
      }
    }
  }
}
```

d. Click **Save**.



You have created an Azure function. This function is triggered each time a new blob is generated by the data transformation job.

Next steps

Use StorSimple Data Manager UI to transform your data

What is StorSimple for Cloud Solutions Providers Program?

Article • 08/23/2022 • 2 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

Microsoft Azure StorSimple is a unique approach to enterprise storage with true hybrid cloud storage capabilities. It empowers the customers to take advantage of economical cloud storage for the inactive data, while keeping their mission-critical data on-premises for the highest levels of performance.

StorSimple Virtual Array for Cloud Solutions Provider (CSP) enables partners to capitalize on this opportunity. The partners own the end-to-end customer lifecycle with direct provisioning, billing, and support of Microsoft's cloud services. In short, the partners can now transact the StorSimple along with their services to customers.

For more information about StorSimple for CSP, visit the [Azure CSP overview](#) page.

For more information on billing, pricing, incentives, and getting support in CSP, go to [StorSimple in CSP: FAQ](#).

Deploy and manage StorSimple for CSP

StorSimple for CSP is available as a usage-based service in all the markets where the StorSimple is available today. StorSimple for CSP uses the Azure portal and the StorSimple Device Manager service. A CSP partner can create a StorSimple Device Manager to manage StorSimple Virtual Arrays, shares, volumes, and backups. You can administer all the virtual arrays registered to your StorSimple Device Manager service via the Azure portal.

For more information, go to [Deploy and manage your StorSimple Virtual Array for CSP](#).

Next steps

- If you have more questions regarding the StorSimple in CSP, go to [StorSimple for CSP: Frequently asked questions](#).
- If you are ready to deploy your StorSimple, go to [Deploy your StorSimple for CSP](#).

Deploy StorSimple Virtual Array for Cloud Solution Provider Program

Article • 08/23/2022 • 3 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

StorSimple Virtual Array can be deployed by the Cloud Solution Provider (CSP) partners for their customers. A CSP partner can create a StorSimple Device Manager service. This service can then be used to deploy and manage StorSimple Virtual Array and the associated shares, volumes, and backups.

This article describes how a CSP partner can add a customer or a new subscription to an existing customer and then create a service to deploy a StorSimple Virtual Array in CSP.

Prerequisites

Before you begin, ensure that:

- You are enrolled under the CSP program.
- You have valid [Partner Center](#) login credentials. The credentials enable you to sign in to the Partner portal to add new customers, search for customers, or navigate to a customer account from the Partner dashboard. The CSP can function as a StorSimple administrator on behalf of the customer in the Azure portal.

Add a customer

If you add a customer, a subscription is automatically created. To add a customer (and automatically create a subscription), perform the following steps in the Partner portal.

1. Go to the [Partner Center](https://partnercenter.microsoft.com/en-us/partner/home) and sign in using your CSP credentials. Click Dashboard.

The screenshot shows the Microsoft Partner Center homepage. At the top, there's a navigation bar with links for Microsoft Partner Center, Programs, How-to, Support, and Find a Partner. To the right of the navigation is a user profile section with an email address (azstorsimplepartner@te...). Below the navigation, there's a main content area titled "Find a Microsoft partner" with a sub-section "Syndicate your business solutions to Microsoft customers, increasing your pipeline of qualified referrals." A "Find a Partner" button is visible. On the right side of the main content area, there's a photograph of two people working together at a laptop. At the bottom of the main content area, there are two buttons: "Enroll now" and "Sign in to Partner Center". Below this, there's a section titled "Achieve new heights with the Cloud Solution Provider program" with three sub-sections: "Be your customers' hero", "The sky's the limit", and "One-stop shopping". Each sub-section has a brief description and a "Learn more" link.

2. In the left-pane, click **Customers**. In the right-pane, click **Add customers**. Enter the details of the customer. Click **Next: Subscriptions** to create a customer subscription.

The screenshot shows the "Add customer" form on the Microsoft Partner Center. The left pane displays a navigation path: New customer > Account info > Company > Country/region > Review > Confirmation. The right pane is divided into sections: "New customer" (with sub-links for Account info, Subscriptions, Review, Confirmation) and "Account info". The "Account info" section includes fields for Company (Contoso), Primary domain name (.onmicrosoft.com), Address line 1 (555, Maple Way), Address line 2, City (Sunnyvale), State/Province (California), ZIP/Postal code (98888), First name (Gus), Last name (Poland), Email address (Gus.Poland@contoso.com), and Phone number (1-555-555-0100). At the bottom of the form are "Next: Subscriptions" and "Cancel" buttons, with "Next: Subscriptions" highlighted by a red box.

3. Select Microsoft Azure offer. Scroll to the bottom of the page and click **Review**.

The screenshot shows the Microsoft Partner Center interface for creating a new customer. The top navigation bar includes links for Microsoft Partner Center, Programs, How-to, Support, Find a Partner, and Dashboard. The user is currently on the 'New customer' section, specifically the 'Subscriptions' step. On the left, there's a sidebar with links for Account info, Subscriptions, Review, and Confirmation. The main content area is titled 'New subscription' and shows a 'Top offers' section with a checked checkbox for 'Microsoft Azure' under the 'Usage-based' category. To the right, there's a 'Catalog' section with filters for Enterprise, Small business, and Government, and a list of other subscription options like Azure Active Directory Basic, Premium, and P2, as well as Azure Information Protection Premium P2, Azure Rights Management Premium, and Dynamics 365 Enterprise Edition Plan 1 - Add-On for CRM Basic (Qualified Offer). A small note on the right side says 'Microsoft Azure: Azure Cloud Solution Provider offer for Partner and Resellers'.

4. Review the information and click **Submit**.

The screenshot shows the Microsoft Partner Center 'Review' page. The top navigation bar is identical to the previous screenshot. The main content is divided into two sections: 'Account info' and 'Subscriptions'. The 'Account info' section contains fields for Company (Contoso, 555, Maple Way, Sunnyvale, CA 98888, ContosoCSP@microsoft.com), Primary contact info (F.NameOfAdmin, F.NameOfAdmin, admin@ContosoCSP.com, 6506932202), and a 'Review' message asking to check the accuracy of the information before submitting. The 'Subscriptions' section shows an 'Enterprise' selection for 'Microsoft Azure' under the 'Usage-based' category. At the bottom, there are 'Submit' and 'Cancel' buttons, with 'Submit' being highlighted with a red border.

5. Save the confirmation information for future reference.

New customer

Confirmation

We have received your order. It may take a few minutes to process. To see this order, view this customer's subscriptions. Be sure to copy the following customer and subscription information for your records.

Setup info

Microsoft ID	2ffa3ce9-71a8-4b39-88bf-8fc4c9480e21
Admin user account	admin@ContosoCSP.onmicrosoft.com
Password	GJQQsIFP5

Please copy and store this password. After you leave this page, you can't view this password again.

Account info

Company	Contoso 1023 Enterprise Way Sunnyvale CA 94089 ContosoCSP.onmicrosoft.com
Primary contact info	F.NameOfAdmin F.NameOfAdmin admin@ContosoCSP.com 6506932202

Subscriptions

Enterprise:	Usage-based 7D2A8DA7-5B40-4A3D-A66F-CEF22516A8D6
-------------	---

Done

- Find or navigate to the customer you just added. Click the **Company name** to drill down into the details.

Customers

Contoso

Company name	Primary domain name	Relationship	Service alerts
Contoso	ContosoCSP.onmicrosoft.com	Cloud Reseller	
Microsoft ID:	2ffa3ce9-71a8-4b39-88bf-8fc4c9480e21	Add subscriptions	View subscriptions
Subscriptions:		Users and licenses	
Licenses:		Office 365	Microsoft Azure Management Portal
Administrator services:		Either the customer has no billable subscriptions or the first billing cycle hasn't occurred yet.	
Service costs	Preview		

- In the left-pane, select **Service management**. In the right-pane, under **Administer services**, click **Microsoft Azure Management Portal** to sign in as an Azure administrator for your customer.

The screenshot shows the Microsoft Partner Center dashboard for a customer named Contoso. On the left, there's a sidebar with links like Subscriptions, Customer insights, Users and licenses, and Service management (which is highlighted with a red box). The main area has tabs for Service management, Administer services, and Service health. Under Service management, there's a section for Office 365 with a link to the Microsoft Azure Management Portal (also highlighted with a red box). The Service health section lists several services with their status: Dynamics CRM Online (normal), Exchange Online (normal), Identity Service (normal), Microsoft Dynamics Marketing (normal), and Mobile Device Management (normal).

8. To create a StorSimple Device Manager, click + New and search for or navigate to **StorSimple Virtual Device Series**. For more information, go to [Deploy a StorSimple Device Manager service](#).

The screenshot shows the Microsoft Azure Marketplace search results. A search bar at the top right contains the text "StorSimple Virtual Device Series". The results table has columns for NAME, PUBLISHER, and CATEGORY. One result is highlighted with a red box: "StorSimple Virtual Device Series" by Microsoft, categorized under Storage. On the left, there's a sidebar with a "+ New" button highlighted with a red box, and a list of categories including Everything, Compute, Networking, and Storage (which is also highlighted with a red box).

Add a subscription

In some instances, you may have an existing customer, and you need to add a subscription. To add a subscription to an existing customer, perform the following steps in the Partner portal.

1. Go to the [Partner Center](#) and sign in using your CSP credentials. Click Dashboard.

The screenshot shows the Microsoft Partner Center homepage. At the top, there's a search bar with the URL 'partnercenter.microsoft.com/en-us/partner/home'. Below the search bar is a blue navigation bar with links for 'Microsoft Partner Center', 'Programs', 'How-to', 'Support', 'Find a Partner', and 'Dashboard'. A red box highlights the 'Dashboard' link. The main content area features a heading 'Find a Microsoft partner' and a sub-headline 'Syndicate your business solutions to Microsoft customers, increasing your pipeline of qualified referrals.' Below this is a 'Find a Partner' button. To the right is a photograph of two people working on a laptop together. Below the photo are 'Enroll now' and 'Sign in to Partner Center' buttons. Further down, there's a section titled 'Achieve new heights with the Cloud Solution Provider program' with three sub-sections: 'Be your customers' hero', 'The sky's the limit', and 'One-stop shopping', each with a brief description and a 'Learn more' link.

2. In the left-pane, click **Customers**. Find or navigate to the customer you want to add a subscription to. Click the icon to expand the row for the company name for your customer. In the details, click **Add subscriptions**.

The screenshot shows the 'Customers' page in the Microsoft Partner Center. The left sidebar has links for 'Overview', 'Customers', 'Support requests', 'Service Health', 'Referrals', 'Billing', 'Pricing and offers', 'Product Analytics', 'Microsoft Azure spending', 'Account settings', 'Notification center', and 'Activity Log'. The main area shows a table of customers with columns for 'Company name', 'Primary domain name', 'Relationship', and 'Service alerts'. One row for 'Contoso' is highlighted with a red box around its name. Below the table, under the 'Contoso' row, are sections for 'Microsoft ID', 'Subscriptions', 'Licenses', 'Administer services', and 'Service costs'. The 'Subscriptions' section contains a red box around the 'Add subscriptions' button. A red box also highlights the 'Edit' icon in the top right corner of the customer row.

3. Check **Microsoft Azure** for the **Top offers** in the subscription and click **Submit**. This creates a new subscription.

The screenshot shows the Microsoft Partner Center interface. In the left sidebar, 'Subscriptions' is selected, and 'New subscription' is highlighted with a red box. The main content area shows 'Top offers' with 'Microsoft Azure' selected (indicated by a checked checkbox) and 'Usage-based' pricing. A 'Catalog' section below lists 'Enterprise', 'Small business', and 'Government' options. Under 'Small business', 'Office 365 Business', 'Office 365 Business Essentials', and 'Office 365 Business Premium' are listed. At the bottom are 'Submit' and 'Cancel' buttons.

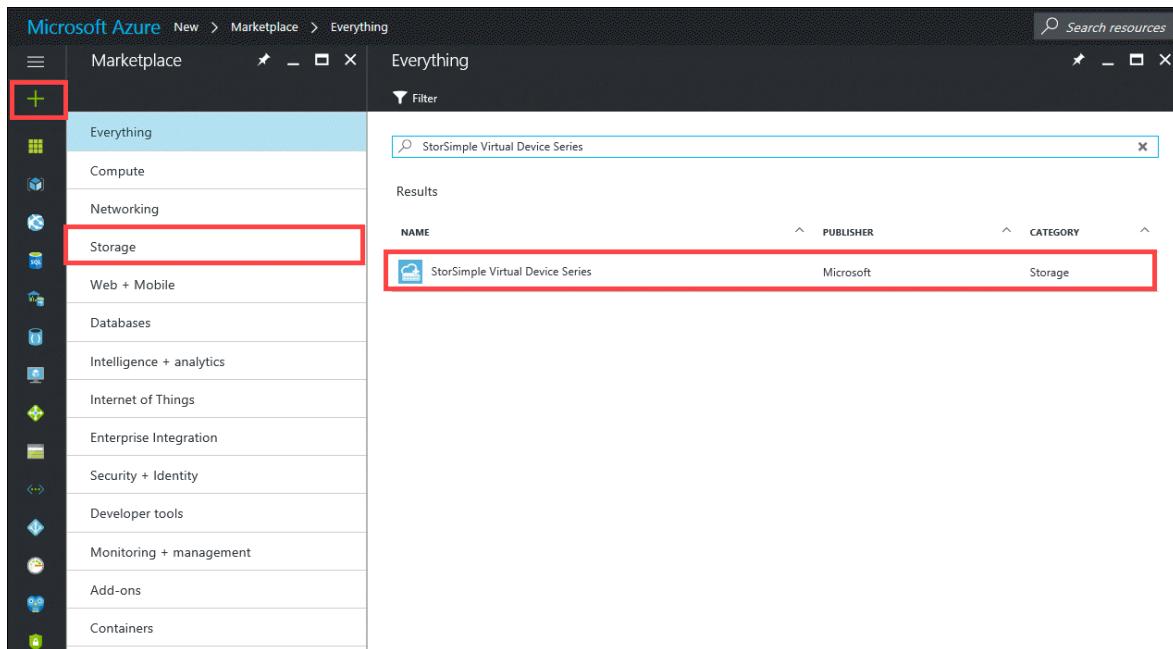
4. After a new subscription is created, click <-- Customers in the left-pane to return to the **Customers** page. Search for the customer for whom you just created a subscription. Click the **Company name** to drill down into the details.

The screenshot shows the 'Customers' page in the Microsoft Partner Center. The left sidebar has 'Overview' selected and 'Customers' highlighted with a red box. The main content area shows a table of customers. One row for 'Contoso' is selected, with its company name 'ContosoCSP.onmicrosoft.com' highlighted with a red box. Other columns include Primary domain name, Relationship, and Service alerts. Buttons for 'Add customer' and 'Request a reseller relationship' are at the top of the table. A search bar at the top right contains 'ContosoCSP'.

5. In the left-pane, select **Service management**. In the right-pane, under **Administer services**, click **Microsoft Azure Management Portal** to sign in as an Azure administrator for your customer.

The screenshot shows the 'Service management' page in the Microsoft Partner Center. The left sidebar has 'Subscriptions' selected and 'Service management' highlighted with a red box. The main content area shows 'Administer services' with a link to 'Microsoft Azure Management Portal' highlighted with a red box. To the right, there's a 'Service health' section listing various Microsoft services with their status and severity.

6. To create a StorSimple Device Manager, click **+ New** and search for or navigate to **StorSimple Virtual Device Series**. For more information, go to [Deploy a StorSimple Device Manager service](#).



Next steps

- If you have more questions regarding the StorSimple in CSP, go to [StorSimple in CSP: Frequently asked questions](#).
- If you are ready to deploy your StorSimple, go to [Deploy your StorSimple in CSP](#).

StorSimple Virtual Array Update 0.4 release notes

Article • 08/19/2022 • 6 minutes to read

⊗ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

Overview

The following release notes identify the critical open issues and the resolved issues for Microsoft Azure StorSimple Virtual Array updates.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your StorSimple Virtual Array, carefully review the information contained in the release notes.

Update 0.4 corresponds to the software version 10.0.10289.0.

ⓘ Note

Updates are disruptive and restart your device. If I/O are in progress, the device incurs downtime.

What's new in the Update 0.4

Update 0.4 is primarily a bug-fix build coupled with a few enhancements. In this version, several bugs resulting in backup failures in the previous version have been addressed. The main enhancements and bug-fixes are as follows:

- **Backup performance enhancements** - This release has made several key enhancements to improve the backup performance. As a result, the backups that

involve a large number of files see a significant reduction in the time to complete, for full and incremental backups.

- **Enhanced restore performance** - This release contains enhancements that significantly improve the restore performance when using large number of files. If using 2 - 4 million files, we recommend that you provision a virtual array with 16 GB RAM to see the improvements. When using less than 2 million files, the minimum requirement for the virtual machine continues to be 8 GB RAM.
- **Improvements to Support package** - The improvements include logging in the statistics for disk, CPU, memory, network, and cloud into the Support package thereby improving the process of diagnosing/debugging device issues.
- **Limit locally pinned iSCSI volumes to 200 GB** - For locally pinned volumes, we recommend that you limit to a 200 GB iSCSI volume on your StorSimple Virtual Array. The local reservation for tiered volumes continues to be 10 % of the provisioned volume size but is capped at 200 GB.
- **Backup-related bug fixes** - In previous versions of software, there were issues related to backups that would cause backup failures. These bugs have been addressed in this release.

Issues fixed in the Update 0.4

The following table provides a summary of issues fixed in this release.

No.	Feature	Issue
1	Backup performance	In the earlier releases, the backups involving large number of files would take a long time to complete (in the order of days). In this release, both the full and incremental backups see a significant reduction in the time to completion.
2	Support package	Disk, CPU, memory, network, and cloud statistics are now logged in to the Support logs making the Support packages very effective in troubleshooting any device issues.
3	Backup	In earlier releases, long running backups could result in a space crunch on the device resulting in backup failures. This bug is addressed in this release by allowing no more than 5 backups to queue at one time.

No.	Feature	Issue
4	iSCSI	In earlier releases, the local reservation for tiered or locally pinned volumes was 10% of the provisioned volume size. In this release, the local reservation for all iSCSI volumes (locally pinned or tiered) is limited to 10 % with a maximum of up to 200 GB (for tiered volumes larger than 2 TB) thereby freeing up more space on the local disk. We recommend that the locally pinned volumes in this release be limited to 200 GB.

Known issues in the Update 0.4

The following table provides a summary of known issues for the StorSimple Virtual Array and includes the issues release-noted from the previous releases.

No.	Feature	Issue	Workaround/comments
1.	Updates	The virtual devices created in the preview release cannot be updated to a supported General Availability version.	These virtual devices must be failed over for the General Availability release using a disaster recovery (DR) workflow.
2.	Provisioned data disk	Once you have provisioned a data disk of a certain specified size and created the corresponding StorSimple virtual device, you must not expand or shrink the data disk. Attempting to do results in a loss of all the data in the local tiers of the device.	
3.	Group policy	When a device is domain-joined, applying a group policy can adversely affect the device operation.	Ensure that your virtual array is in its own organizational unit (OU) for Active Directory and no group policy objects (GPO) are applied to it.
4.	Local web UI	If enhanced security features are enabled in Internet Explorer (IE ESC), some local web UI pages such as Troubleshooting or Maintenance may not work properly. Buttons on these pages may also not work.	Turn off enhanced security features in Internet Explorer.
5.	Local web UI	In a Hyper-V virtual machine, the network interfaces in the web UI are displayed as 10 Gbps interfaces.	This behavior is a reflection of Hyper-V. Hyper-V always shows 10 Gbps for virtual network adapters.

No.	Feature	Issue	Workaround/comments
6.	Tiered volumes or shares	Byte range locking for applications that work with the StorSimple tiered volumes is not supported. If byte range locking is enabled, StorSimple tiering does not work.	<p>Recommended measures include:</p> <p>Turn off byte range locking in your application logic.</p> <p>Choose to put data for this application in locally pinned volumes as opposed to tiered volumes.</p> <p><i>Caveat:</i> When using locally pinned volumes and byte range locking is enabled, the locally pinned volume can be online even before the restore is complete. In such instances, if a restore is in progress, then you must wait for the restore to complete.</p>
7.	Tiered shares	Working with large files could result in slow tier out.	When working with large files, we recommend that the largest file is smaller than 3% of the share size.
8.	Used capacity for shares	You may see share consumption when there is no data on the share. This is because the used capacity for shares includes metadata.	
9.	Disaster recovery	You can only perform the disaster recovery of a file server to the same domain as that of the source device. Disaster recovery to a target device in another domain is not supported in this release.	This is implemented in a later release.
10.	Azure PowerShell	The StorSimple virtual devices cannot be managed through the Azure PowerShell in this release.	All the management of the virtual devices should be done through the Azure classic portal and the local web UI.
11.	Password change	The virtual array device console only accepts input in en-US keyboard format.	
12.	CHAP	CHAP credentials once created cannot be removed. Additionally, if you modify the CHAP credentials, you need to take the volumes offline and then bring them online for the change to take effect.	This issue is addressed in a later release.

No.	Feature	Issue	Workaround/comments
13.	iSCSI server	The 'Used storage' displayed for an iSCSI volume may be different in the StorSimple Manager service and the iSCSI host.	The iSCSI host has the filesystem view. The device sees the blocks allocated when the volume was at the maximum size.
14.	File server	If a file in a folder has an Alternate Data Stream (ADS) associated with it, the ADS is not backed up or restored via disaster recovery, clone, and Item Level Recovery.	
15.	File server	Symbolic links are not supported.	
16.	File server	Files protected by Windows Encrypting File System (EFS) when copied over or stored on the StorSimple Virtual Array file server result in an unsupported configuration.	

Next step

[Install Update 0.4](#) on your StorSimple Virtual Array.

References

Looking for an older release note? Go to:

- [StorSimple Virtual Array Update 0.3 Release Notes](#)
- [StorSimple Virtual Array Update 0.1 and 0.2 Release Notes](#)
- [StorSimple Virtual Array General Availability Release Notes](#)

StorSimple for Cloud Solutions Provider Program: Frequently Asked Questions

FAQ

Overview

Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

The following are questions and answers that you might have as a StorSimple partner when you deploy or manage a StorSimple Virtual Array in Azure portal.

StorSimple and CSP model

What does it mean to have StorSimple as a part of the Cloud Solutions Provider (CSP) program?

StorSimple for CSP enables our CSP partners to resell StorSimple Virtual Array to their customers. This model enables the CSP partners to own the end-to-end customer lifecycle with direct provisioning, billing, and support of Microsoft's cloud services.

For more information, go to [StorSimple in CSP program](#).

Is StorSimple a usage-based or based on seat licenses like Microsoft 365 and Enterprise Mobility Suite (EMS)?

StorSimple is a usage-based service. Customers who procure StorSimple Virtual Array via the CSP route pay for the usage of virtual array and Azure, billed as separate line-items in the CSP bill.

Is the StorSimple business model similar to that of other services such as the Microsoft 365 and the Enterprise Mobility Suite?

Yes. The model is a wholesale discount model just like other usage-based services in Azure. The wholesale discount for StorSimple is similar to that of other Azure services. This model provides our CSP partners an opportunity to sell more and drive Azure consumption via StorSimple Virtual Array.

Which StorSimple SKUs are available at launch?

The same SKUs that are available with the standalone StorSimple services.

Is there any difference between the StorSimple directly purchased from Microsoft under EA and StorSimple as a part of CSP?

No. Under CSP, customers can also purchase other services offered by the CSP partner along with StorSimple Virtual Array (SVA) under one invoice. Do note that for procuring the StorSimple 8000 series physical device, customers still need to go through the EA route.

In which markets, is StorSimple available for CSP at launch?

StorSimple Virtual Array for CSP is available in all the markets where StorSimple is available today. For more information, go to the [list of regions where StorSimple is available](#).

What kind of solutions can a partner deliver with StorSimple and CSP?

There are multiple solutions:

- The partners can resell StorSimple Virtual Array.
- The partners can deliver solutions built around StorSimple and other Azure services or third-party software. For more information, review some possible [solutions that exist around StorSimple](#).
- They can also discover new business models by delivering managed services.

What are the incentives available for StorSimple CSP partners? Do I qualify for any CSP program incentives?

For information on incentives, go to [CSP program incentives](#).

Deploy and manage StorSimple as a partner

How can I administer StorSimple Virtual Array in CSP?

You can add StorSimple Virtual Array subscriptions to your customers' account through the Partner Center. Additionally, you can use the Azure portal to add users to the subscriptions.

Is the Azure portal approach the same as other services for CSP?

Yes. With StorSimple Virtual Array for CSP, the best way for partners to access the Azure portal should be via the [Partner Center](#) where they can manage customers and subscriptions. To manage StorSimple subscriptions, the partner or customer (depending on permissions granted) should log in to the Azure portal.

Is Microsoft shipping a new portal for StorSimple for CSP?

No. You will be able to administer StorSimple Virtual Array in CSP through the Azure portal.

I have provisioned a standalone StorSimple subscription for my customer. Do I have to use the Azure portal to administer my device?

Yes.

Is the Microsoft Account team compensated as a result of sales of StorSimple through CSP?

Yes. The partner sales executive and the customer account team for the end customer will be compensated for CSP sales. The partners are expected to take the lead in selling their differentiated value and offerings.

Support for StorSimple and CSP

Are there any forums to get additional support for CSP partners to deploy and manage StorSimple?

You can visit the StorSimple in CSP forum to get answers to some commonly asked questions. You would need to join the [Azure Advisors Yammer group](#) first. Next search for and join the group - **StorSimple Partner Advisors**.

How does the Support work for StorSimple for CSP?

The support model for StorSimple in CSP is the same as that of other Azure services in CSP. For more information, go to [Customer Support for CSP](#).

For more information about StorSimple for CSP, go to:

- [Microsoft Cloud Solution Provider Program](#)
- [Partner Center](#)

Next steps

If you are ready to deploy your StorSimple, go to [Deploy your StorSimple in CSP](#).

StorSimple solution support

Article • 08/19/2022 • 7 minutes to read

✖ Caution

ACTION REQUIRED: StorSimple Data Manager, StorSimple Device Manager, StorSimple 1200, and StorSimple 8000 have reached their end of support. End of support details were published in 2019 on the [Microsoft Lifecycle Policy](#) and [Azure Communications](#) pages. Additional notifications were also sent via email and posted on the [Azure portal](#) and [StorSimple documentation site](#). Contact [Microsoft Support](#) for additional details.

StorSimple support

Microsoft offers flexible support options for StorSimple enterprise storage customers. We're deeply committed to delivering a high-quality support experience that allows you to maximize the impact of your investment in the StorSimple solution and Microsoft Azure. As a StorSimple customer, you receive:

- 24x7 ability to submit support tickets through the Azure portal.
- Help desk access for general support queries and deep technical assistance.
- Local language support where available.
- Alert provisioning and management for health and performance insights.
- Access to software updates covering major, minor, and maintenance fixes.
- Support for StorSimple 8000 Series Storage Arrays and StorSimple Virtual Arrays in a single package.

StorSimple support plans

Support feature	STANDARD ¹	PREMIUM ¹
Billing and subscription management	✓	✓
Azure portal ticket submission	✓	✓
Online support portal access	✓	✓
Alert provisioning and management	✓	✓

Support feature	STANDARD ¹	PREMIUM ¹
Helpdesk initial response time 24x7 support ticket submission	Severity A: Within 2 hours	Severity A: Within 60 mins
Initial response time based on Severity ²	Severity B: Within 4 hours Severity C: Within 8 hours	Severity B: Within 2 hours Severity C: Within 4 hours
Phone support (call back)	✓	✓
Advanced parts replacement (StorSimple 8000 series only) ³	Next business day ⁴	Within 4 hours
On-site field services engineer (StorSimple 8000 series only) ³	Not available	Within 4 hours
StorSimple Virtual Array ⁵	✓	✓
Instances of StorSimple Virtual Array ⁵	No limit	No limit

HARDWARE AND SOFTWARE WARRANTY

Hardware parts replacement (StorSimple 8000 series only) ⁶

Free software updates

¹ Support provided to customer until next EA anniversary. Customers must renew support at EA anniversary to be eligible for StorSimple support. Contact Microsoft for geographical coverage. Premium coverage may vary by city. Contact Microsoft account/sales team for geographical coverage before purchasing StorSimple Premium Support.

² Severity defined as follows:

- Severity A: Significant loss or degradation of services
- Severity B: Moderate loss or degradation but work can continue in an impaired manner
- Severity C: Substantially functioning with minor or no impediments to system functionality

Microsoft may downgrade the severity level of a Severity A case if the customer is unable to provide adequate resources or responses to enable Microsoft to continue with problem resolution. Expected response time based on 24x7 support in English for Severity A, local business hours for Severity B and C.

³ Service begins only after root cause identification is complete and Microsoft recommended a path for problem resolution.

⁴ Next business day parts delivery is performed on a best-effort basis and may be subject to delays.

⁵ Customers using only StorSimple Virtual Arrays must purchase either StorSimple Standard or Premium support plans. Contact your Microsoft account/sales team to purchase StorSimple support.

⁶ To expedite hardware warranty claims, replacement parts are shipped to the customer before receiving defective parts. Customer is responsible for timely return shipment of defective parts.

If your support contract has expired, be aware, depending on how long the support contract has been expired, it may take up to three weeks after the renewal processing has completed before a part is delivered as the local stocking location for your contract won't be stocked with replacement parts for your device until after your contract is processed.

Local language support

In addition to English, local language support is provided in the following languages during business hours: Spanish, Portuguese, Japanese, Korean, Taiwanese, and Traditional Chinese.

Support scope

Support for billing and subscription management-related issues is available at all support levels. In order to receive StorSimple support, customer must be actively enrolled for either StorSimple Standard or Premium support plans. StorSimple support team will be responsible for resolving all issues that impact the StorSimple solution. In order to receive support for Azure-related issues that aren't directly related to StorSimple, customer needs to be enrolled in an appropriate Azure support plan. Refer [here](#) for details. The support team refers non-StorSimple support cases to the Azure team for followup based on customer entitlements for Azure support.

SEVERITY	CUSTOMER'S SITUATION	EXPECTED MICROSOFT RESPONSE ²	EXPECTED CUSTOMER RESPONSE

SEVERITY	CUSTOMER'S SITUATION	EXPECTED MICROSOFT RESPONSE ²	EXPECTED CUSTOMER RESPONSE
A	<p>Critical business impact:</p> <ul style="list-style-type: none"> Customers business has significant loss or degradation of services.¹ Needs immediate attention. 	<p>Initial response:¹</p> <ul style="list-style-type: none"> One hour or less for Premium. Two hours or less for Standard. Continuous effort all day, every day. 	<ul style="list-style-type: none"> Allocation of appropriate resources to sustain continuous effort all day, every day. Accurate contact information for case owner.
B	<p>Moderate business impact:</p> <ul style="list-style-type: none"> Customer's business has moderate loss or degradation of services, but work can reasonably continue in an impaired manner. 	<p>Initial response:¹</p> <ul style="list-style-type: none"> Two hours or less for Premium. Four hours or less for Standard. 	<ul style="list-style-type: none"> Allocation of appropriate resources to sustain continuous effort during business hours unless customer requests to opt out of 24x7. Accurate contact information for case owner.
C	<p>Minimum business impact:</p> <ul style="list-style-type: none"> Customer's business is substantially functioning with minor or no impediments to services. 	<p>Initial response:¹</p> <ul style="list-style-type: none"> Four hours or less for Premium. Eight hours or less for Standard. 	<ul style="list-style-type: none"> Accurate contact information for case owner

¹ Microsoft may downgrade the severity level of a Severity A case if the customer isn't able to provide adequate resources or responses to enable Microsoft to continue with problem resolution efforts.

² Expected response times are based on 24x7 support in English for Severity A and local business hours for Severity B and C, and local business hours support in the remaining local languages: Japanese, Taiwanese, Traditional Chinese, and Korean.

Cancellation policy

In order to receive StorSimple support, customer must purchase Standard or Premium support plans for the duration of the subscription term. Cancellation doesn't result in a prorated refund. StorSimple support plans are reduction eligible at EA anniversary. However, Microsoft is unable to provide support to StorSimple customers without valid support contracts.

Renewal policy

Upon the purchase of StorSimple 8000 Series Storage Arrays, support is provided through the next EA anniversary. Customer must renew StorSimple support at EA anniversary. StorSimple support plan orders are coterminous. Customers are notified via e-mail about impending support expiry for StorSimple 8000 Series Storage Arrays and are expected to follow up with the Microsoft account/sales teams or their Microsoft Licensing Solution Partner (LSP) to renew StorSimple support.

Standard Azure support doesn't cover StorSimple hardware support. If you're covered under Premier or Unified Microsoft support, you must still purchase Standard StorSimple support renewal. StorSimple support renewal can be aligned with EA anniversary date by acquiring the required support SKU with the license quantity equal to the number of the appliances and the unit quantity ordered being the remaining number of months of support needed until the EA anniversary date if all the units have the same support contract expiration date. If the units have different support contract expiration dates, each appliance must be covered with one support SKU with the unit quantity ordered being the remaining number of months of support needed until the EA anniversary date per each appliance.

StorSimple 8000 Series Storage Arrays support is provided based on how the StorSimple array was purchased.

Support SKUs	Subscription Model	ASAP + Model
--------------	--------------------	--------------

Support SKUs	Subscription Model	ASAP + Model
Standard support	Included.	<ul style="list-style-type: none"> • Provided to customers with initial purchase through the next EA anniversary. • Customer must purchase support in subsequent years as no replacement hardware parts can be dispatched without an active StorSimple support contract.
<p>[CWZ-00023]</p> <p><i>AzureStorSimple</i> <i>ShrdSvr ALNG</i> <i>SubsVL MVL</i> <i>StdSpprt</i></p>		
Premium* support	<p>Since standard support is automatically included with Subscription, refer to the Standard to Premium Upgrade.</p> <p>[CWZ-00024]</p> <p><i>AzureStorSimple</i> <i>ShrdSvr ALNG</i> <i>SubsVL MVL</i> <i>PremSpprt</i></p>	<ul style="list-style-type: none"> • Customers covered by Microsoft Premier support contracts should refer to the standard to premium upgrade. • Customers who aren't covered by a Microsoft Premier contract and wish to have Premium StorSimple Support should purchase this SKU at renewal time.

Support SKUs	Subscription Model	ASAP + Model
Standard to Premium** upgrade [CWZ- 00025] <i>AzureStorSimple ShrdSvr ALNG SubsVL MVL Spprt-StepuptoPrem</i>	Customers covered by Microsoft Premier Support contract at the time of StorSimple purchase are automatically upgraded to Premium StorSimple support free of charge for the duration of the time they remain covered by Premier support. If customers acquire Premier Support later, a free StorSimple support upgrade can be obtained by requesting it via SSSupOps@microsoft.com .	<ul style="list-style-type: none"> Customers covered by Microsoft Premier Support contract can purchase the Standard Support SKU [CWZ-00023] and the StorSimple Standard Support contract will be automatically upgraded, at no additional charges, for the duration of the time they remain covered by Premier support.
	Non-Premier customers can purchase the StorSimple Standard to Premium upgrade SKU [CWZ-00025] anytime during the Enterprise Agreement(EA) contract.	<ul style="list-style-type: none"> If customers acquire Premier Support later, a free StorSimple support upgrade can be obtained by requesting it via SSSupOps@microsoft.com. Non-Premier customers covered by StorSimple Standard support can purchase the Premium upgrade SKU [CWZ-00025] anytime during the Enterprise Agreement(EA) contract. Next year, when renewing Support contract, customers should purchase directly the Premium Support SKU [CWZ-00024] and not just the upgrade SKU [CWZ-00025].

* Premium coverage isn't available in all locations. Contact Microsoft at SSSupOps@microsoft.com for geographical coverage before purchasing StorSimple Premium Support.

** The StorSimple appliance must be deployed in a region where the customer is covered by Premier support in order to be eligible for a free upgrade to premium StorSimple support.

ASAP+ customers can switch to subscription model where standard support is included. Use the StorSimple pricing calculator for subscription pricing and contact SSSupOps@microsoft.com for any questions. Switching is one way only from ASAP+ to Subscription.