Configuring Customer-Provided Azure Tenant for the Nasuni Filer

Version 7.10
March 2018
Last modified: March 13, 2018

Document Information

Configuring Customer-Provided Azure Tenant for the Nasuni Filer
Version 7.10
March 2018

Copyright

Notice

Trademarks

Contacting Nasuni Corporation

Nasuni Corporation
One Marina Park Drive
Boston, MA 02210

Telephone: 1-857-444-8500
Sales: 1-800-208-3418
http://www.nasuni.com
Email: info@nasuni.com

Technical Support

Telephone: 1-888-6NASUNI (888-662-7864)
Email: support@nasuni.com
Technical Support is available 24/7/365 for full production customers.

Contents

Preface

Audience

This guide is intended for the IT administrator or person responsible for installing the Nasuni Filer or the Nasuni Management Console in a customer-provided Microsoft Azure tenant.

What's in this Book

This guide contains the following chapters:

- Chapter 1, "General Information," on page 1 gives general information about how the Nasuni Filer operates, and specifications on what a platform requires to run the Nasuni Filer.
- Chapter 2, "Installing in customer-provided Microsoft Azure tenant," on page 7 explains how to install the Nasuni Filer or the Nasuni Management Console in a customer-provided Microsoft Azure tenant.

Text Conventions

The following text conventions are used in this document:

Convention	Description
1. Number	Used to indicate a step in a task.
• Bullet	Used for items in a list without any particular order.
Bold	Used to give emphasis to a word. Also used for named graphical elements.
Italics	Used to represent options or parameters.
Underline	Used for hyperlinks, such as links to Web sites.
`Monospace`	Used to indicate pathnames, filenames, folder names, typed information, and code.

Product Documentation

Electronic Publications

Extensive documentation is available for all aspects of installing, configuring, and operating the Nasuni Filer. The latest version of each of the following documents is available in PDF format at http://www.nasuni.com/support/documentation.

- *Hardware Getting Started Guide*: For setting up the Nasuni Filer on the Nasuni Filer hardware appliance.
  To download this guide for the NF-60, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_HW_GS_Guide_NF-60.pdf

  To download this guide for the NF-200, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_HW_GS_Guide_NF-200.pdf

  To download this guide for the NF-400, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_HW_GS_Guide_NF-400.pdf

  To download this guide for the NF-440, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_HW_GS_Guide_NF-440.pdf

  To download this guide for the NF-600, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_HW_GS_Guide_NF-600.pdf

- *Installing the Nasuni Filer on Virtual Platforms*: For installing the Nasuni Filer on a virtual machine within a corporate network. To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Installing-on-Virtual.pdf

- *Installing the Nasuni Filer on the Azure Platform*: For installing the Nasuni Filer on the Microsoft Azure cloud virtual machine. To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Installing-on-Azure.pdf

- *Installing the Nasuni Filer on the EC2 Platform*: For installing the Nasuni Filer on the Amazon EC2 cloud virtual machine. To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Installing-on-EC2.pdf

- *Initial Configuration Guide*: For configuring and deploying the Nasuni Filer after the initial installation on the hardware appliance or virtual machine. To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_Initial_Configuration_Guide.pdf

- *Administration Guide*: For managing unified storage using the Nasuni Filer.
  To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_Administration_Guide.pdf

- *Nasuni Management Console Guide*: For managing multiple Nasuni Filers.
  To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/NMCGuide.pdf

- *Nasuni Management Console Quick Start Guide*: To quickly get started using the Nasuni Management Console to manage multiple Nasuni Filers. To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/NMCQuickStartGuide.pdf

- *Using Multiple Protocols*: Discusses scenarios requiring particular access to data, and how different combinations of protocols can help provide the access that clients need.
  To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/UsingMultipleProtocols.pdf

- *Third-Party Licensing Guide*: Listing of third-party software used in the Nasuni Filer.
  To download this guide, visit:

  http://info.nasuni.com/hubfs/Nasuni.com-assets/Support-Docs/Nasuni_Filer_Third-Party_Licensing_Guide.pdf

Release Notes for Nasuni Documentation Set

Date (As Of)	Changes
2018-03-12	Clarified supported instance types, in *Installing the Nasuni Filer on the EC2 Platform*. Added procedures for accessing software through Azure Marketplace, in *Configuring Customer-Provided Azure Tenant*. Updated screen shots and procedures for SSL certificates, in *Administration Guide*. Updated screen shot, in *Configuring Customer-Provided Azure Tenant*. Fixed incorrect screen shot, in *DFS Configuration Guide*. Added procedure for removing Revit Worksharing Monitor, in *Revit Configuration Guide*.
2018-02-28	Added information about time to generate an encryption key, in *Best Practices Guide*, *Encryption Key Best Practices*, *NMC Guide*, *Recovery Guide*, and *Administration Guide*. Added considerations about MTU on the EC2 platform, in *Installing the Nasuni Filer on the EC2 Platform*. Noted that enabling "Snapshot Directory Access" prevents directories from being deleted, in *NMC Guide*, *Administration Guide,* and *Best Practices Guide*. Clarified behavior of Security indication when permission of remote volume is set to Disabled, in *NMC Guide*. Noted that you cannot create an internal link to folders created by using the "%U" wildcard, in several documents. Clarified the relative size of the COW disk, in *Cache Configuration Guide* and *Installing on Virtual*. Added tip on hard links with Linux and Mac OS X clients using global locking with CIFS, in *Administration Guide*. Updated default number of cores to 4, in *Initial Configuration Guide* and *Installing on Virtual*. Added tip on case-sensitive volumes and multiple volume protocols, in *Administration Guide*. Added tip on using Windows “net use” command, in *Administration Guide* and *Initial Configuration Guide*.

Date (As Of)	Changes
	Added details of the suggested usage, in *Revit Configuration Guide*. Clarified how Auto Cache works, in *Administration Guide* and *NMC Guide*. Specified that the user names for CIFS Administrative Users should not have the leading domain, in *Administration Guide*. Added tip about Embedded Host Client for installing the Nasuni Filer into VMware ESXi using the vSphere Web interface, in *Installing on Virtual*. Added description of backup keys, which enable recovery of Nasuni Filers that don't have owned volumes or snapshots, in *Administration Guide* and *Recovery Guide*. Updated procedure for installing Nasuni Filer and NMC on Microsoft Azure platform, in *Configuring Customer-Provided Azure Tenant for the Nasuni Filer*. Added the Device ID and Logged In fields to the Mobile Licenses table, in *NMC Guide*. Added description of Prioritize Snapshot feature, in *NMC Guide* and *Administration Guide*. Created tip for error when installing to non-default location on Hyper-V, in *Installing on Virtual*.
2017-11-15	Clarified when the file syncs occur related to Global Locking, in *Cache Configuration Guide*, *Best Practices Guide*, *Global Locking Guide*, and *Administration Guide*. Clarified processing when a Nasuni Filer goes under the control of a Nasuni Management Console, in *NMC Guide* and *Administration Guide*. Added details about how certain types of loads can affect syncs, in *NMC Guide*, *Merge Conflicts Guide*, and *Administration Guide*. Warned that downloading large files from the NMC can take a long time, in *NMC Guide*. Added warning against saving encryption key files to volume, in *Best Practices Guide*, *NMC Guide*, *Recovery Guide*, and *Administration Guide*. Updated copyright, trademark, disclaimer, and liability statements, in most documents. Updated maximum Azure disk size to 4,095 GiB, in *Best Practices Guide*, *Cache Configuration Guide*, *Initial Configuration Guide*, *Resizing Cache Guide*, *Installing on Virtual Platforms*, and *Suggestions for VM Installation*.

Date (As Of)	Changes
2017-10-31	Added procedure for possible notification during snapshot or sync, in *NMC Guide* and *Administration Guide*. Added details about the Clam AntiVirus (ClamAV®) open-source antivirus engine, in *Best Practices Guide*, *NMC Guide*, *Third-Party Licensing Guide*, and *Administration Guide*. New screenshots, in *Installing the Nasuni Filer on the EC2 Platform*. Added reminders to keep COW disk in proportion to cache disk when changing the size of the cache disk, in *Cache Configuration* and several other documents. Selecting the "Secure transfer required" feature for an Azure Storage account does not affect the operation of the Nasuni Filer, in *Configuring Customer-Provided Azure Storage for the Nasuni Filer* and *Installing Nasuni Filer on Customer-Provided Azure Storage Getting Started Guide*. Corrected the default number of cores for a Nasuni Filer, in *Best Practices Guide*, *Initial Configuration Guide*, and *Installing on Virtual Platforms*. Clarified the processing for recovery after resetting the administrative account, in *Recovery Guide*, *Administration Guide*, and *NMC Guide*. Clarified the prerequisites for performing the Side Load procedure, in *Recovery Guide*, *Administration Guide*, and *Side Load Guide*. Clarified the default outbound Quality of Service, in *Best Practices Guide*, *Cache Configuration Guide*, *Administration Guide*, and *NMC Guide*. Added material about enabling Auditing to help mitigate ransomware, in *Best Practices Guide*, *Administration Guide*, and *NMC Guide*. Clarified meaning of Restrict Anonymous setting for CIFS, in *Administration Guide* and *NMC Guide*.
2017-09-29	Added material on Cloud I/O and Cloud Credentials, in *Administration Guide* and *NMC Guide*. Added discussion of chunk size and related topics, in *Best Practices Guide*, *Cache Configuration Guide*, *Administration Guide*, and *NMC Guide*. Rewrote section on General CIFS Settings to clarify processing in different situations, in *Administration Guide* and *NMC Guide*. Added details about how long notifications are retained, in *Administration Guide* and *NMC Guide*.

Date (As Of)	Changes
	Added procedure for obtaining JSON format of shares configuration in NMC, in *NMC Guide*. Clarified use of DFS for failover, in *DFS Configuration and Best Practices Guide*. Reconciled the recovery procedures, in *Administration Guide* and *Recovery Guide*. Removed mentions of default volume and default CIFS share, in *Best Practices Guide*, *Best Practices Guide*, and *Administration Guide*. Clarified best use cases for Side Load procedure, in *Side Load Feature*. Added warnings against restoring a virtual machine from a virtual machine snapshot or backup, in *Cache Configuration Guide* and *Installing on Virtual Platforms*. Added information about how permissions affect the ability to download files, in *Administration Guide* and *NMC Guide*. Added procedure for SMB3 encryption, in *Administration Guide*, *Security Features*, and *NMC Guide*. Added instructions for “Snapshot ran out of internal space” error, in *Administration Guide* and *Best Practices Guide*. Updated the supported Cleversafe/IBM Cloud Object Storage version to 3.8.3. Added details of the use of encryption keys with remote volumes, in *Encryption Key Best Practices*. Clarified details of NTFS Exclusive Mode and NTFS Compatible Mode, in *Administration Guide* and others.
2017-08-31	Formatting and pagination, in *Data API* doc. Clarified NMC procedure for changing SMB protocol. Added procedure for installing NMC using Azure Resource Manager, in *Installing the Nasuni Filer on the Azure Platform*. Clarified that displayed size might differ from external size indications, in Administration Guide and other documents. Clarified the distinction between “private cloud”, “customer-controlled public cloud”, “BYOC”, and “public cloud” in many docs. Changed name of *Private-Cloud-Getting-Started-Guide-Azure* to *GS-Guide-for-Azure-BYOC*. Added link to NASUNI-FILER-MIB for SNMP support, in *Administration Guide*.

Date (As Of)	Changes
	Added NTFS Exclusive Mode to available permissions for volume, in *Administration Guide* and other documents. Created *Upgrading Nasuni Filers to Use Case-Insensitive Volumes* procedure. Clarified that changes to the Snapshot Retention setting go into effect when the next snapshot occurs, and that it is normal to temporarily see more snapshots than the Snapshot Retention setting would suggest, in *Administration Guide* and *NMC Guide*. Added detailed instructions in volume creation procedures about preferring case-insensitive CIFS volumes, in *Administration Guide*, *Best Practices Guide*, and *Worksheets for Configuring NMC*, *Nasuni Filers*, *Volumes*, *and Shares*. Added best practices for handling historical SIDs before adding data, in *Administration Guide*, *Best Practices Guide*, and *NMC Guide*. Removed references to `fsck`, since it is unnecessary with OS7, in *Administration Guide*, *NMC Guide*, *Recovery Guide*, *Installing on Virtual*.

Chapter 1: General Information

Overview

This chapter includes general information about the Nasuni Filer, as well as technical specifications.

In this chapter

Nasuni NAS

Nasuni delivers an advanced storage solution using a cloud infrastructure. The core technology is a next-generation storage controller – the Nasuni Filer – that offers the security and performance of traditional storage, while adding unlimited scalability, automatic offsite protection, and global multi-site access to files. The Nasuni system is managed through a single, small-footprint point of control within the enterprise's data center.

The Nasuni Filer is an on-premises storage device supporting NFS, CIFS, FTP/SFTP, iSCSI, and HTTP/REST protocols. The Nasuni Filer is fully integrated with Active Directory, LDAP, Distributed File System (DFS), and Windows Previous Versions. It includes a high-performance cache and takes periodic snapshots that enable file-level restores. Its reach and capacity far exceed those of a traditional controller, however, because it does not rely only on memory and local disk to manage its data: it has the entire capacity of the cloud at its disposal. All data is deduplicated, compressed, and encrypted before storage.

Several choices are available for the back-end cloud storage component, including the following:

- Your own public cloud service from Microsoft Azure Blob Storage or Amazon AWS S3.
- Private cloud products, including Cleversafe, IBM Cloud Object Storage, EMC ViPR/ECS, and EMC Atmos.

The choices for the back-end cloud storage component are part of each customer license. Each volume has only one back-end cloud storage component.

Multi-site access enables organizations with several locations to work on a single set of shared data. Nasuni's architecture allows multiple storage controllers to have live access to the same volume of data. Organizations benefit by having a simple, safe, and secure way to share data across any number of sites. Nasuni's multi-site access enables capabilities that include:

- Secure data distribution to remote office/branch office (ROBO).
- Remote offices forwarding data to a central point.
- Two-way synchronized read-write.

Multi-site access does away with cumbersome replication schemes and slow WAN optimizers.

Nasuni Filer

Nasuni's NAS is delivered through the Nasuni Filer, a storage controller that runs in your data center and provides primary storage with built-in backup, offsite protection, and multi-site access. With your Nasuni Filer, you manage your volumes and performance using the Web-based Nasuni Filer user interface.

The Nasuni Filer is available as a virtual appliance, as a hardware appliance, and as a Microsoft Azure and Amazon EC2 virtual appliance.

Nasuni Management Console

The Nasuni Management Console enables you to monitor and manage many Nasuni Filers from one central appliance. Using the Nasuni Management Console, you can view the status of all of your managed Nasuni Filers, as well as configure their settings. Using the Nasuni Management Console, you can ensure consistent settings on all your Nasuni Filers.

> ***Note:*** *If a Nasuni Filer loses internet connectivity with the Nasuni Management Console, the Nasuni Filer can still leave the Nasuni Management Console.*

Key Terms

The following terms are helpful in understanding the Nasuni Filer:

- **Nasuni Filer**: The storage controller in your data center that integrates with your infrastructure

via CIFS, NFS, iSCSI, FTP/SFTP, or HTTPS/REST protocols. The Nasuni Filer can be mapped as a network drive.

- **Nasuni Filer user interface**: The Web-based graphical user interface with which you configure and manage the Nasuni Filer. The Nasuni Filer user interface is accessible with supported Web browsers including Mozilla Firefox, Internet Explorer, Safari, and Google Chrome.
- **Nasuni Management Console (NMC)**: The Web-accessible appliance with which you can configure and manage multiple Nasuni Filers. The Nasuni Management Console is accessible with supported Web browsers including Mozilla Firefox, Internet Explorer, Apple Safari, and Google Chrome.
- **Cloud storage**: Internet-based, highly protected, unlimited storage.
- **Volume**: A set of files and directories (CIFS, NFS, and FTP/SFTP) or blocks of data (iSCSI).
- **Share/export**: An access point to a folder on a volume that can be shared or exported on your network. Access to a CIFS share can be customized on a user-level or group-level basis. You can create many shares or exports on a volume, for different purposes or audiences.
- **Cache**: The local storage of the Nasuni Filer. All data and metadata that is accessed regularly is kept locally in the cache. If requested data is not locally resident, it is staged into the cache and provided for the request.
- **Snapshot**: A snapshot is a complete picture of your volume at a specific point in time. Snapshots offer data protection by enabling you to recover data deleted in error or to restore an entire file system. After a snapshot has been taken and is sent to cloud storage, it is not possible to modify that snapshot.

Nasuni Filer Specifications

This section contains specifications for configuring the Nasuni Filer.

General Specifications

The following table lists general specifications for the Nasuni Filer.

Description	Value
Maximum number of owned volumes per Nasuni Filer.	8
Maximum number of files in the Nasuni Service.	Unlimited
Maximum capacity of files in the Nasuni Service.	Unlimited (might be restricted by license)
Default cache size on disk.	250 GB (VM only)
Default snapshot period.	1 hour (after last snapshot)
Maximum file size.	Available cache space at time of write
Number of cache volumes supported.	1
Minimum memory required.	4 GiB (VM only)

Supported Web Browsers

The Nasuni Filer supports the following Web browsers:

Browser	Version
Mozilla Firefox	Latest
Internet Explorer	Latest two versions
Google Chrome	Latest
Apple Safari	Latest

Supported Windows Operating Systems

The Nasuni Filer provides file sharing services to the following Windows operating systems:

Server Operating Systems

Operating System	Version	Service Packs
Windows Server 2008 R2	Standard	N/A
Windows Server 2012	Standard	N/A
Windows Server 2012 R2	Standard	N/A

Desktop Operating Systems

Operating System	Version	Service Packs
Windows 7	Professional	1
Windows 8.1	Professional	N/A
Windows 10	Professional	N/A

Initial, Recommended, and Minimum Memory

The memory allocation for a virtual machine platform (VM) is set and changed in the hypervisor. The memory allocation that is first set is the "initial memory allocation".

The "recommended memory allocation" is a suggested amount of memory. If the VM has less than the "recommended memory allocation", an alert informs the customer of the situation.

There is also a "minimum memory allocation". If the VM has less than the "minimum memory allocation", then the software does not run.

> ***Tip:*** *For both the Nasuni Filer and the NMC, it might be necessary to increase the memory allocation above the recommended memory allocation, depending on the workload.*

For the Nasuni Filer, these values are:

- Initial memory allocation: 8 GiB
- Recommended memory allocation: 8 GiB
- Minimum memory allocation: 4 GiB

  Note: *The document preview feature of Nasuni Web Access requires a minimum of 8 GiB and version OS7 of the Nasuni Filer base operating system.*

For the NMC, these values are:

- Initial memory allocation: 6 GiB
- Recommended memory allocation: 6 GiB
- Minimum memory allocation: 2 GiB

Chapter 2: Installing in customer-provided Microsoft Azure tenant

Overview

This chapter explains how to perform the initial installation of the Nasuni Filer or the Nasuni Management Console in a customer-provided Microsoft Azure tenant.

For additional information on the initial configuration of the Nasuni Filer, see the *Nasuni Filer Initial Configuration Guide* and the *Nasuni Filer Administration Guide*.

For additional information on the initial configuration of the Nasuni Management Console, see the *Nasuni Management Console Guide*.

> ***Note:*** *The Microsoft Azure tenant vendor changes their interfaces occasionally with little notice to the users. The exact screens and text on these platforms might change at any time. For complete information, see https://account.windowsazure.com/Home/Index.*

Platforms for Nasuni Filer and Nasuni Management Console

You can install the Nasuni Filer and the Nasuni Management Console on a variety of platforms. Extensive documentation is available for all aspects of installing, configuring, and operating the Nasuni Filer. See "Product Documentation" on page vii.

Supported platforms include:

- The Nasuni Filer hardware appliance.
- A virtual machine within a corporate network.
- The Microsoft Azure cloud virtual machine.
- The Amazon EC2 cloud virtual machine.

Installing software from Azure Marketplace

You can install the software for the Nasuni Filer or the Nasuni Management Console on a virtual machine by using the corresponding installation software, which is available from on the Azure Marketplace.

The Azure Marketplace images for both the NMC and the Nasuni Edge Appliance contain the underlying OS disks, and is automatically sized to 16 GB at launch.

The Azure Marketplace image for the Nasuni Edge Appliance includes a 1 TB cache disk. Optionally, you can expand the cache after creating the virtual machine.

The Nasuni Edge Appliance automatically uses the Azure temp storage disk as the Copy-on-Write (COW) disk, so it is unnecessary to manually attach a Copy-on-Write (COW) disk.

> ***Tip:*** *To install software by downloading the software from Nasuni, see "Installing software by downloading" on page 9.*

> ***Important:*** *You must create and maintain your own Microsoft Azure account. Nasuni does not have access to your Microsoft Azure account. To create a Microsoft Azure account, visit the Microsoft Azure site at https://azure.microsoft.com/.*

> ***Important:*** *To access Active Directory-enabled volumes, the Nasuni Filer must have access to the same Active Directory domains as the other Nasuni Filers connected to the volume. This requires either access to a Domain Controller running in Azure or the necessary network connectivity, such as a VPN connection or Azure ExpressRoute, to an on-premises Domain Controller. Azure Active Directory is not currently supported.*
> *Similarly, to access LDAP-enabled volumes, the Nasuni Filer must be able to access LDAP and Kerberos in the same LDAP domain*
> *You cannot enable both Active Directory and LDAP Directory Services for a Nasuni Filer.*

To install software from the Azure Marketplace, follow these steps:

1. Log in to the Azure Portal at https://portal.azure.com/. The Microsoft Azure dashboard page appears.

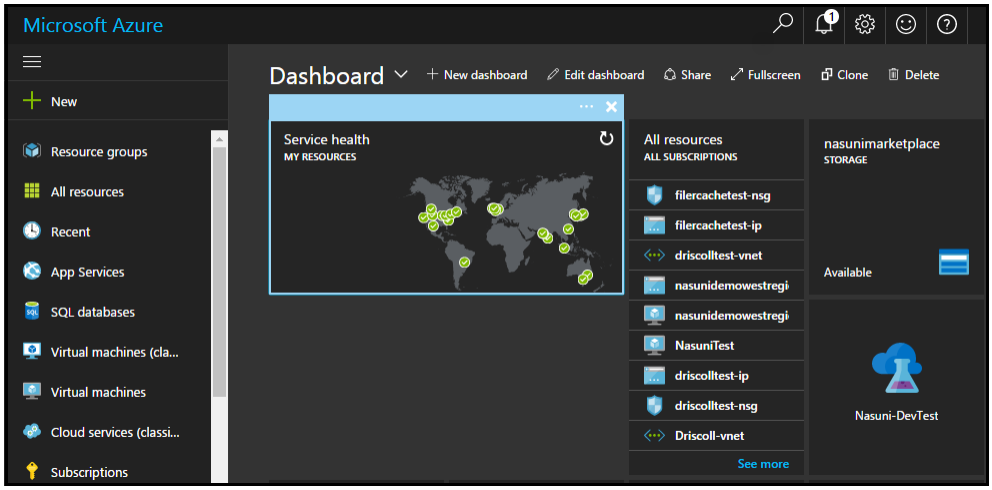

Figure 2-1: Microsoft Azure dashboard page.

2. On the top left of the page, click **New** or "**Create a resource**". The **New** pane appears.

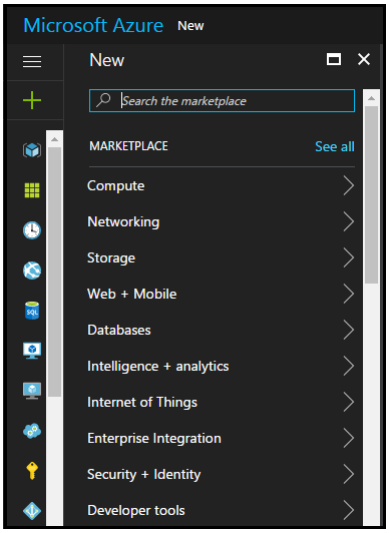

Figure 2-2: New pane.

3. In the "**Search the marketplace**" text box, type `Nasuni`, then select either **Nasuni NMC** or **Nasuni Edge Appliance** from the drop-down menu. The "**Bring Your Own License enabled**" pane appears.

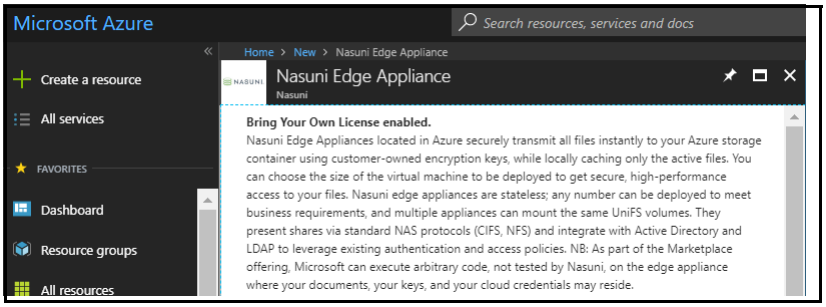

Figure 2-3: "Bring Your Own License enabled".

Review the information on this pane.

4. From the "**Select a deployment model**" drop-down box, select "**Resource Manager**".
5. Continue with "Creating virtual machine" on page 19.

Installing software by downloading

You can install the software for the Nasuni Filer or the Nasuni Management Console on a virtual machine by downloading the corresponding installation software, which is available from Nasuni.

> ***Important:*** *You must create and maintain your own Microsoft Azure account. Nasuni does not have access to your Microsoft Azure account. To create a Microsoft Azure account, visit the Microsoft Azure site at https://azure.microsoft.com/.*

> ***Important:*** *To access Active Directory-enabled volumes, the Nasuni Filer must have access to the same Active Directory domains as the other Nasuni Filers connected to the volume.*

This requires either access to a Domain Controller running in Azure or the necessary network connectivity, such as a VPN connection or Azure ExpressRoute, to an on-premises Domain Controller. Azure Active Directory is not currently supported. Similarly, to access LDAP-enabled volumes, the Nasuni Filer must be able to access LDAP and Kerberos in the same LDAP domain
You cannot enable both Active Directory and LDAP Directory Services for a Nasuni Filer.

To download software for the Nasuni Filer or the NMC, follow these steps:

1. If you do not have a Nasuni account already, go to the Nasuni evaluation Web site at http://www.nasuni.com/demo/. The **Demo** page appears.

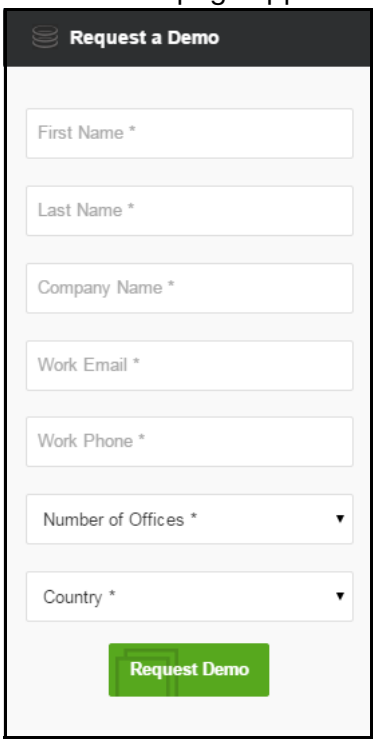

Figure 2-4: Excerpt from "Request a Demo" page.

Enter the required information, then click **Request Demo**.

Note: *The email address that you enter is used for authentication with the Nasuni Service.*
The Nasuni staff will contact you with registration material to obtain your Nasuni account.

2. When you have your Nasuni account credentials, log in to your Nasuni account web site (https://account.nasuni.com/) and click **Downloads**. The **Downloads** page appears.

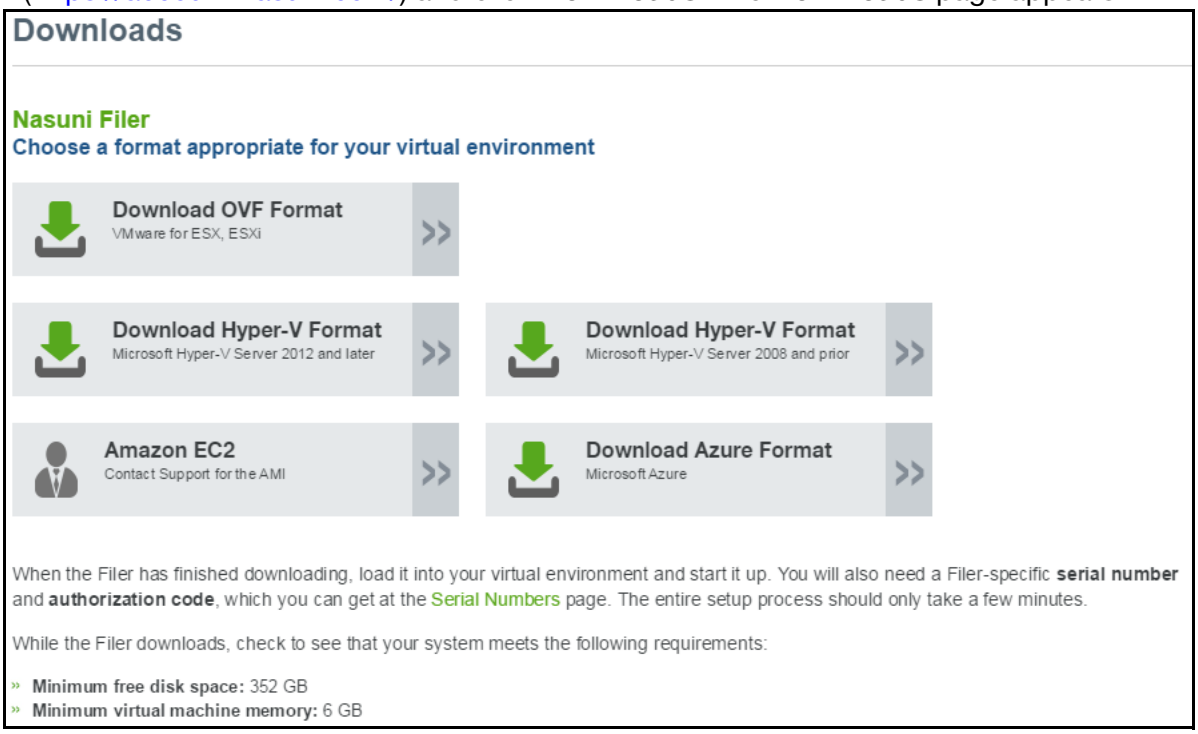

Figure 2-5: Nasuni Filer downloads.

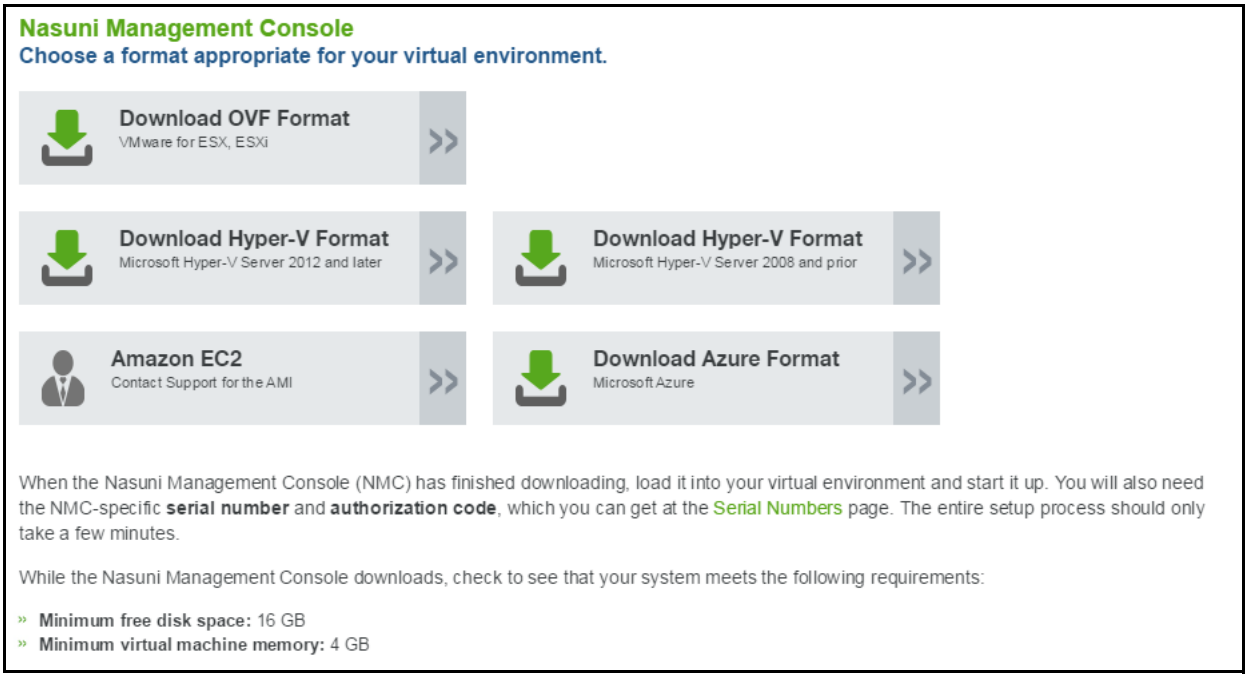

Figure 2-6: NMC downloads.

3. Select the appropriate format of the Nasuni Filer software or of the Nasuni Management Console software. For the Microsoft Azure cloud virtual machine, select Microsoft Azure format.
4. Download the Nasuni software `.zip` file to a location on your local drive.
   The amount of time to download the software file depends on your Internet connection. The Nasuni Filer `.zip` file is approximately 900 MB in size. The NMC `.zip` file is approximately 900 MB in size.
5. Unzip the Nasuni software file to a convenient directory.
6. Continue with "Creating an Azure storage account (using Azure Portal)" on page 13 or "Creating an Azure storage account (using Azure Resource Manager and PowerShell)" on page 22.

Creating an Azure storage account (using Azure Portal)

Important: *You must have at least one subscription for this purpose.*

Note: *Selecting the "Secure transfer required" feature for an Azure Storage account does not affect the operation of the Nasuni Filer.*

Tip: *You can download the Azure Storage Explorer, a tool for configuring and maintaining Microsoft Azure accounts, at https://azure.microsoft.com/en-us/features/storage-explorer/.*

This procedure uses the Azure Portal.

Creating a new storage account

If you do not already have a storage account in Microsoft Azure, create a storage account in Microsoft Azure by following these steps:

1. Log in to the Azure Portal at https://portal.azure.com/. The Microsoft Azure dashboard page appears.

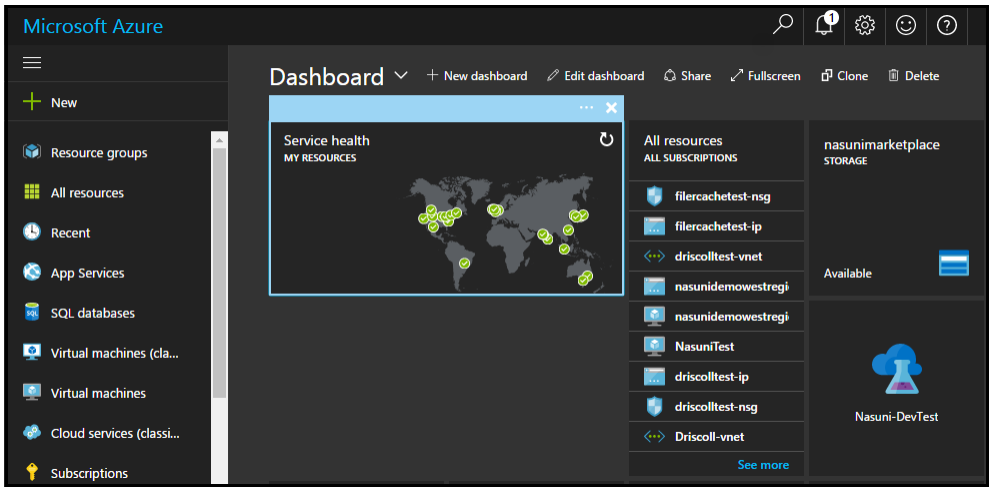

Figure 2-7: Microsoft Azure dashboard page.

2. On the top left of the page, click **New** or "**Create a resource**". The **New** pane appears.

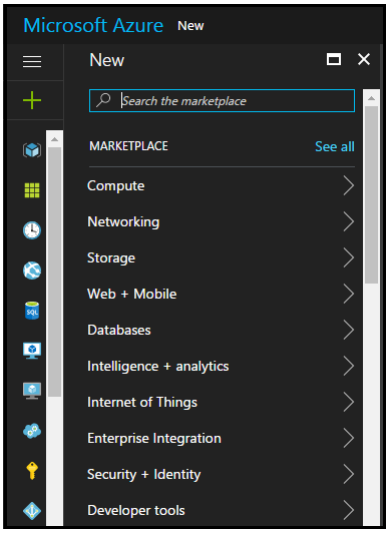

Figure 2-8: New pane.

3. Click **Storage**, then click "**Storage account - blob, file, table, queue**". The "**Create storage account**" pane appears.

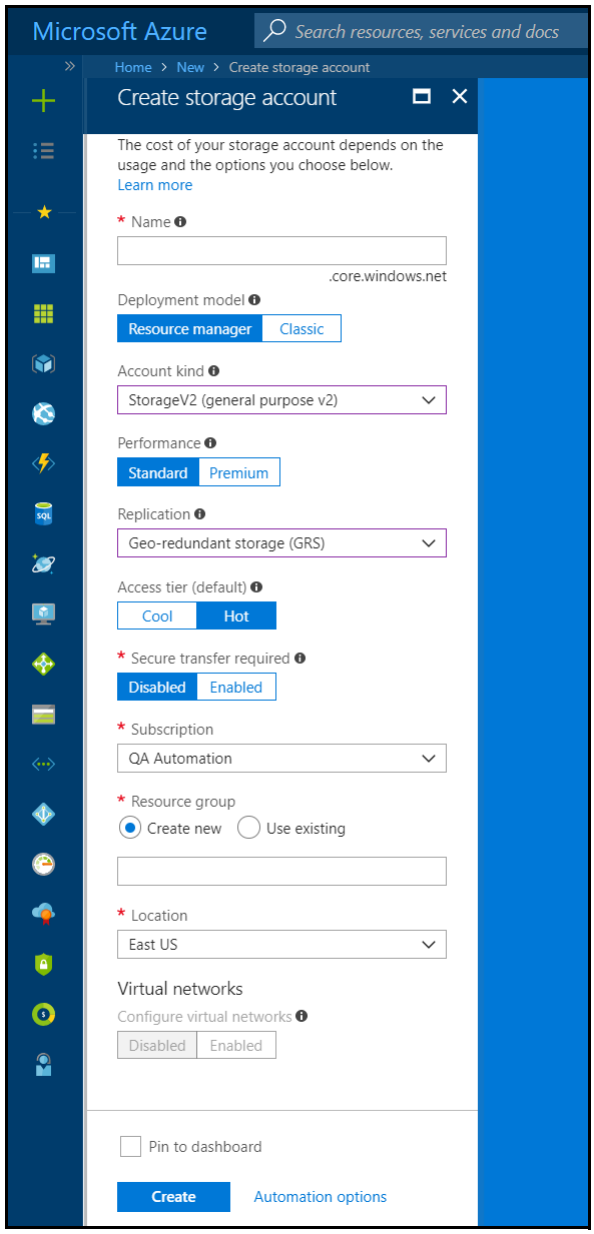

Figure 2-9: "Create storage account" pane.

4. In the **Name** text box, enter a descriptive name to use in the URL of the storage account. The name must be at least 3 characters long and at most 24 characters long, using only numbers and lowercase letters. This name will be appended with "`.core.windows.net`" to form the complete URL for the storage account. The storage account name must be globally unique.
5. For the "**Deployment model**", select "**Resource Manager**".
6. From the "**Account kind**" drop-down list, select "**StorageV2 (general purpose v2)**".
7. For the **Performance**, select **Standard**.

8. From the **Replication** drop-down list, select the type of replication that you prefer.

   Tip: *Nasuni recommends "Geo-redundant storage (GRS)". Also, see https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/.*

   Tip: *Legal requirements or your organization's policies may require data placement in a specific region, or prevent replication outside the region.*

9. For the "**Access tier**", select **Hot** for production data.
10. If your security policy requires it, enable "**Secure transfer required**".
11. If there is more than one subscription, from the **Subscription** drop-down list, select the subscription to use for this storage account.
12. To select an existing **Resource Group**, click "**Use existing**" and then select an existing Resource Group.
    Alternatively, create a new Resource Group by clicking "**Create new**" and then entering a name for the new Resource Group.
13. From the **Location** drop-down list, select the location for the storage account. By selecting the appropriate location, you can locate your cloud storage closest to where it will be used.

    Note: *If you choose "Resource Manager" as the "Deployment model" and "Blob storage" as the "Account kind", some Locations might not be available. In this case, select either "General Purpose" as the "Account kind" or "Classic" as the "Deployment model".*

    Tip: *Legal requirements or your organization's policies may require data placement in a specific region, or prevent replication outside the region.*

14. For "**Virtual networks (Preview)**, select **Disabled**.
15. To pin this storage account to the Microsoft Azure dashboard, select "**Pin to dashboard**".
16. Click **Create**.
    The storage account starts being created. When the storage account is created, click **Storage Accounts** in the left-hand list. The new storage account appears in the list of storage accounts.

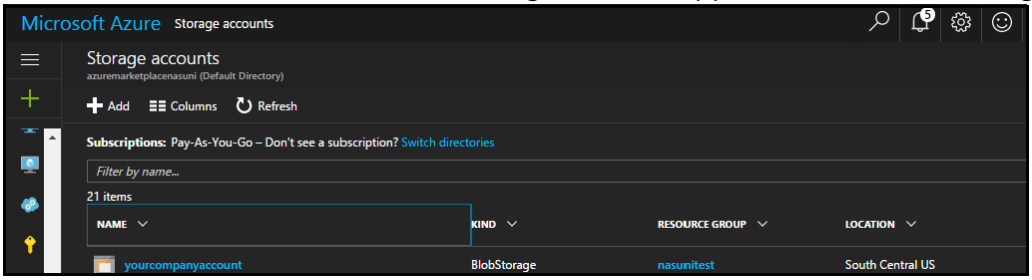

Figure 2-10: Storage account pane.

17. Click the name of your storage account. The pane for your storage account settings appears.

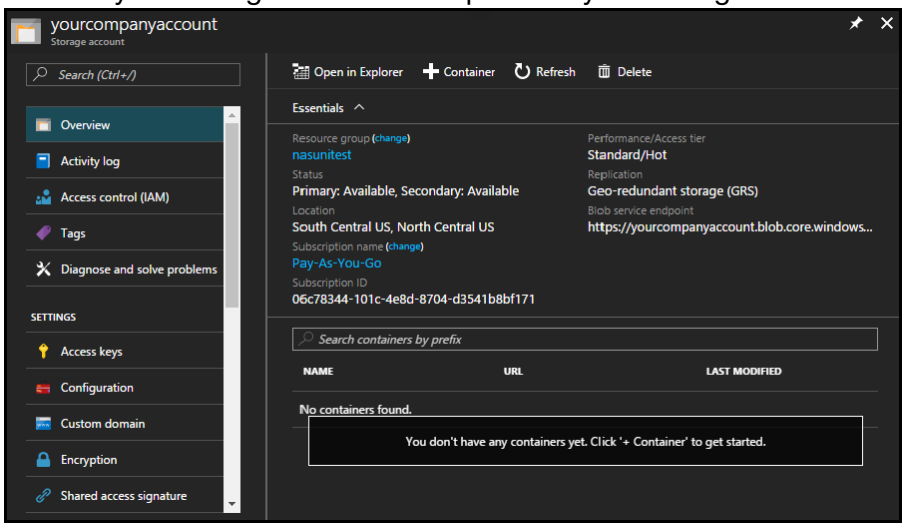

Figure 2-11: Storage account settings pane.

Creating a new container

To create a new container, follow this procedure:

1. In the left-hand pane, click “**Storage accounts**”. A list of available storage account appears.
2. In the list of available storage accounts, click your storage account. The overview of your storage account appears.
3. In the list under your storage account name, click **Containers**. The **Containers** pane appears.
4. Click “**+ Container**”. The “**New container**” pane appears.
5. Enter a **Name** for the new container that is between 3 and 63 characters long, beginning with a number or a lowercase letter, and consisting of numbers, lowercase letters, and hyphens. Hyphens must be preceded and followed by non-hyphens.
6. From the “**Public access level**” drop-down list, select “**Private (no anonymous access)**”.
7. Click **OK**. The container is created and appears in the list of containers.

Copying Nasuni software to container

To copy Nasuni software to the container, follow this procedure:

1. From the list of containers, select the container. A pane of information about the container appears.
2. Click **Upload**. The “**Upload blob**” pane appears.
3. Navigate to the `.vhd` file that you downloaded in “Installing software by downloading” on page 9 above.

4. To upload the file even if a file of the same name already exists in this location, select "**Overwrite if files already exist**".
5. Click **Upload**.
   The `.vhd` file is uploaded to the container.

   Tip: *This can take a few minutes to complete, depending on your Internet speed. When complete, the file appears in the list for the container.*

Creating image of installation software

To create an image of the installation software, follow this procedure:

1. In the left-hand pane, click **Images**. The **Images** pane appears.
2. Click "**+ Add**". The "**Create image**" pane appears.
3. Enter a **Name** for this image. The name must begin with a letter or a number; end with a letter, a number, or an underscore; and contain only letters, numbers, underscores, periods, or hyphens.
4. From the **Subscription** drop-down list, select your subscription.
5. For the "**Resource group**", select "**Use existing**", then, from the drop-down list, select the resource group.
6. From the **Location** drop-down list, select the location.
7. For the "**OS disk**", select **Linux**.
8. For "**Storage blob**", click **Browse**, then navigate to the storage account, container, and file uploaded in "Copying Nasuni software to container" on page 17 above.
9. From the "**Account type**" drop-down list, select "**Premium (SSD)**", or the choice most appropriate for your performance requirements.
10. From the "**Host caching**" drop-down list, select "**Read/write**".
11. To pin this image to the Microsoft Azure dashboard, select "**Pin to dashboard**".
12. Click **Create**. The image is created and appears in the list of images. If the image does not appear in the list after it is created, refresh the page.
13. Click the newly created image in the list of images. The **Image** pane appears.
14. Click "**+ Create VM**". The "**Create virtual machine**" pane appears.
15. Continue with "Creating virtual machine" on page 19.

Creating virtual machine

To create a virtual machine, follow this procedure:

1. Enter a **Name** for this virtual machine. The name must be 1 to 15 characters long. Non-ASCII and special characters are not allowed.
2. From the "**VM disk type**" drop-down list, select **SSD**, or the choice most appropriate for your performance requirements.
3. Enter a "**User name**" for the user of this virtual machine.

   Note: *This value is not used and does not provide access to the virtual machine.*
4. If available, for "**Authentication type**", select **Password**.
5. Enter a **Password** for this user. Passwords must be at least 13 characters, and satisfy complexity requirements.

   Note: *This value is not used and does not provide access to the virtual machine.*
6. Confirm the password.

   Note: *This value is not used and does not provide access to the virtual machine.*
7. If there is more than one subscription, from the **Subscription** drop-down list, select the subscription to use.
8. For the "**Resource group**", select "**Create new**" or "**Use existing**", then, from the drop-down list, select the resource group.
9. From the **Location** drop-down list, select the location.
10. Click **OK**. The "**Choose a size**" pane appears.
11. Select a virtual machine size appropriate for your workload. If you installed software using the Azure Marketplace, several compatible instances are published in the Azure Marketplace as defaults, but might not be optimal for your workload.
    Depending on your **VM disk type** selection (SSD or HDD), an informational message might indicate incompatibility between the virtual machine size selected and the **VM disk type** selected. Select another virtual machine size, or change the **VM disk type** to match the virtual machine size.

    Tip: *Consult with Nasuni for assistance determining the appropriate virtual machine size.*
12. Click **Select**. The **Settings** pane appears. Use the newly provided values, or adjust the settings to use existing network resources in your resource group. Validate the Network security group (firewall) details to match your organization security requirements and planned Nasuni usage.
13. From the "**High availability**" drop-down list, select **None**.
14. For "**Use managed disks**", select **Yes**.
15. By default, a public IP is created for the new instance. If a public IP is not required, edit the "**Virtual network**" and **Subnet** values, and, for "**Public IP address**", select **None**.

16. Click "**Network security group (firewall)**". The "**Create network security group**" pane appears.
    On the "**Create network security group**" pane, click "**+ Add an inbound rule**". The "**Add inbound security rule**" pane appears.
    Change the "**Port ranges**" to `8443` for a Nasuni Filer virtual machine, or to `443` for a NMC virtual machine.
    By default, the Marketplace virtual machine includes a Network security group that includes all of the required ports for Nasuni Edge Appliance or NMC operations. For example, if you don't plan to use iSCSI or NFS, you could remove those ports from the network security group.
    Change the **Name** to "**Filer_Mgmt**" or "**NMC_Mgmt**", as appropriate.
    Click **OK**. The new inbound rule is created.
    Click **OK**. The "**Create network security group**" pane closes.
17. Ensure that "**Auto-shutdown**" is set to **Off**.
18. For **Monitoring**, configuring monitoring to match your desired monitoring settings.
19. On the **Settings** pane, click **OK**. The **Summary** pane appears. Configuration parameters are validated.
20. Click **OK**. The deployment begins. When the deployment is finished, the new virtual machine appears in the list of virtual machines ("**Virtual machines**" in left-most pane).
21. If you installed software using the Azure Marketplace, continue with "Installing the Nasuni Filer" on page 24.

Adding the cache disk

If you installed software by downloading software, continue with this section.

To add the cache disk, follow this procedure:

1. In the left-most pane, click "**Virtual machines**", then click the new virtual machine in the list. The virtual machine pane opens.
2. Click **Stop** to stop the virtual machine. A dialog box appears. Click **Yes**. The virtual machine stops.
3. From the list directly under the name of the virtual machine, click **Disks**. The **Disks** pane appears.
4. Click "**+ Add data disk**". In the "**Data disks**" area, new blank fields appear.
5. From the top of the **Name** drop-down list, click "**Create disk**". The "**Create managed disk**" pane appears.
6. Enter a **Name** for the disk. The name must begin with a letter or a number; end with a letter, a number, or an underscore; and contain only letters, numbers, underscores, periods, or hyphens.
7. For "**Resource group**", select "**Use existing**", then, from the drop-down list, select the resource group.

8. From the “**Account type**” drop-down list, select “**Premium (SSD)**”.
9. From the “**Source type**” drop-down list, select **None**.
10. In the “**Size GiB**” field, enter the appropriate disk size, such as `1023`.

    Note: *Contact Nasuni Support if you require a cache size that exceeds the limits of a single Azure virtual disk.*

11. Click **Create**. The configuration is validated, and the disk is created. The new disk appears in the list of “**Data disks**”.
12. For the disk just created, from the “**Host Caching**” drop-down list, select “**Read/write**”.
13. Click **Save**. The disk is updated. The new disk appears in the list of “**Data disks**”.

Starting the virtual machine

To start the virtual machine, follow this procedure:

1. From the list in the left-most pane, click “**Virtual machines**”. The “**Virtual machines**” pane appears.
2. From the “Virtual machines” list, click the virtual machine created in “Creating virtual machine” on page 19 above. The **Overview** pane for this virtual machine appears.
3. To launch the virtual machine, click **Start**.

Accessing the Nasuni Filer or NMC

To access the newly installed Nasuni Filer or NMC, follow this procedure:

1. From the list in the left-most pane, click “**Virtual machines**”. The “**Virtual machines**” pane appears.
2. From the “**Virtual machines**” list, click the virtual machine created in “Creating virtual machine” on page 19 above. The **Overview** pane for this virtual machine appears.
3. Copy the “**Public IP address**”.
4. Open a new browser window.
5. To access the Nasuni Filer, enter the address in this form: `https://<Public IP address>:8443`. The Nasuni Filer user interface should appear.
6. To access the NMC, enter the address `https://<Public IP address>`. The Nasuni Management Console should appear.

Creating an Azure storage account (using Azure Resource Manager and PowerShell)

Important: *You must have at least one subscription for this purpose.*

Note: *Confirm with Nasuni Sales or Support that your Nasuni account is configured to work with your existing Microsoft Azure account.*

Note: *Selecting the "Secure transfer required" feature for an Azure Storage account does not affect the operation of the Nasuni Filer.*

Tip: *Run PowerShell as an Administrator.*

This procedure uses the Azure Resource Manager and PowerShell.

If you do not already have a storage account in Microsoft Azure, create a storage account in Microsoft Azure by following these steps:

1. Install Azure PowerShell, which is used to enter commands for Azure Resource Manager, by following these steps:
   a. From https://www.microsoft.com/en-us/download/details.aspx?id=50395, install PowerShell.
   b. Using PowerShell, install the Azure PowerShell module by entering this command:

      ```
      Install-Module -Name AzureRM -Scope CurrentUser
      ```

      This command installs the Azure Resource Manager (ARM) PowerShell module from https://www.powershellgallery.com/ (PowerShell Gallery), which is a central, publicly accessible repository for modules and scripts.
2. Create an ARM Resource Group, by following these steps:
   a. Authenticate to Microsoft Azure using the following command:

      ```
      Add-AzureRmAccount;
      ```

   b. Create a Resource Group using the following commands:

      ```
      $ResourceGroup = @{
      Name = '<name_of_resource_group>';
      Location = '<location>';
      Force = $true;
      }
      New-AzureRmResourceGroup @ResourceGroup;
      ```

      where `<name_of_resource_group>` is the name of the Resource Group you are creating; and `<location>` is the Azure Region where the resource should be deployed, such as "Central US". Use the `Get-AzureLocation` command to obtain an authoritative list of Azure Regions.

3. Create a Storage Account, by using the following command:

```
New-AzureRmStorageAccount
   -ResourceGroupName "<name_of_resource_group>"
   -AccountName "<name_of_storage_account>"
   -Location "<location>"
   -Type "<replication>"
```

   where `<name_of_resource_group>` is the name of the Resource Group;
   `<name_of_storage_account>` is the name of the Storage Account you are creating;
   `<location>` is the Azure Region where the resource should be deployed, such as “Central US”;
   `<replication>` is the replication policy for the storage Account (Nasuni recommends “Standard_GRS”).
   Use the `Get-AzureLocation` command to obtain an authoritative list of Azure Regions.

4. Authenticate to the Azure Blob Storage Service, by following these steps:

   a. Obtain the Storage Account authentication keys using the following command:

```
$Keys = Get-AzureRmStorageAccountKey
   -ResourceGroupName <name_of_resource_group>
   -Name <name_of_storage_account>;
```

   where `<name_of_resource_group>` is the name of the Resource Group;
   `<name_of_storage_account>` is the name of the Storage Account you are creating.

   b. Use the Azure.Storage module to create a Storage Authentication Context:

```
$StorageContext = New-AzureStorageContext
   -StorageAccountName <name_of_storage_account>
   -StorageAccountKey $Keys[0].Value;
```

   where `<name_of_storage_account>` is the name of the storage account.

5. Record this Microsoft Azure Storage Account Name for use in configuring the Azure credentials for the Nasuni Filer.

   Note: *Do not create a container in your storage account. The Nasuni Filer creates containers automatically. Containers created outside the Nasuni Filer are not useable.*

6. Obtain the Microsoft Azure Primary Access Key, by using the following example to command:

```
Get-AzureRMStorageAccountKey
   -ResourceGroupName "<name_of_resource_group>"
   -Name "<name_of_storage_account>"
    | Where-Object {$_.KeyName -eq 'key1'}
```

   where `<name_of_resource_group>` is the name of the Resource Group;
   `<name_of_storage_account>` is the name of the Storage Account you created.

7. Record the Microsoft Azure Primary Access Key for use in configuring the Azure credentials for the Nasuni Filer.

Installing the Nasuni Filer

Note: *Confirm with Nasuni Sales or Support that your Nasuni account is configured to work with your existing Microsoft Azure account.*

The installation procedure for the Nasuni Filer depends on the platform that you have chosen. As mentioned above, supported platforms for the Nasuni Filer include the following:

- The Nasuni Filer hardware appliance: No installation is necessary.
- A virtual machine within a corporate network: If installing on a VMware ESXi or Microsoft Hyper-V platform, see the *Installing the Nasuni Filer on Virtual Platforms* document on www.nasuni.com/resource-center/support-documentation/.

  Note: *Nasuni supports VMware ESXi 5.5 and above.*
- The Microsoft Azure public cloud virtual machine: If installing on a Microsoft Azure public cloud platform, see the *Installing the Nasuni Filer on the Azure Platform* document on www.nasuni.com/resource-center/support-documentation/.
- The Amazon EC2 public cloud virtual machine: If installing on an Amazon EC2 public cloud platform, see the *Installing the Nasuni Filer on the EC2 Platform* document on www.nasuni.com/resource-center/support-documentation/

To install the Nasuni Filer on other platforms, please contact Nasuni Technical Support.

All installation procedures result in an initial IP address for the Nasuni Filer. In your web browser, enter the following in the address bar and press **Enter**:

```
https://<IP address>:8443
```

where `<IP address>` is the IP address.

It may take a few minutes before the new Nasuni Filer is available. For more details, see the *Nasuni Filer Administration Guide.*

Installing the Nasuni Management Console (NMC)

> ***Note:*** *Confirm with Nasuni Sales or Support that your Nasuni account is configured to work with your existing Microsoft Azure account.*

To install the Nasuni Management Console (NMC), unzip the NMC installation file to a convenient directory.

See the installation procedure in the Nasuni Management Console Guide on www.nasuni.com/resource-center/support-documentation/.

It may take a few minutes before the new Nasuni Management Console is available.

Configuring Microsoft Azure credentials on a Nasuni Filer

Note: *Port 443 (HTTPS) must be open outbound from the Nasuni Filer to Microsoft Azure.*

Note: *If you change Microsoft Azure credentials, update them on the Nasuni Filer or NMC, to retain access to data.*

To configure credentials using the NMC, see "Configuring Microsoft Azure credentials on the NMC" on page 30.

To configure Microsoft Azure credentials:

1. On the Nasuni Filer, click **Configuration**, then select **Cloud Credentials** from the menu. The **User Provided Cloud Credentials** page displays a list of cloud credentials.

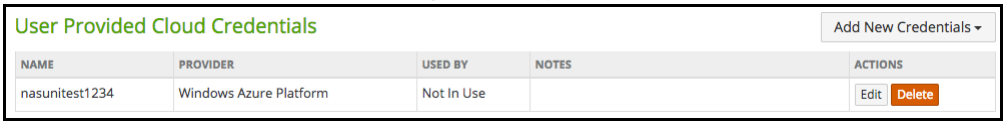

Figure 2-12: Cloud Credentials page.

The following information appears for each set of credentials in the list:

- **Name**: The name of the set of credentials.
- **Provider**: The cloud provider.
- **Used by**: The volumes that use the cloud credentials.
- **Notes**: Information provided by the user about the connection with the cloud provider.
- **Actions**: Actions available for each set of credentials.

2. To add new credentials, click **Add New Credentials** and select the platform. Alternatively, to edit existing credentials, click **Edit** for the credentials to edit.

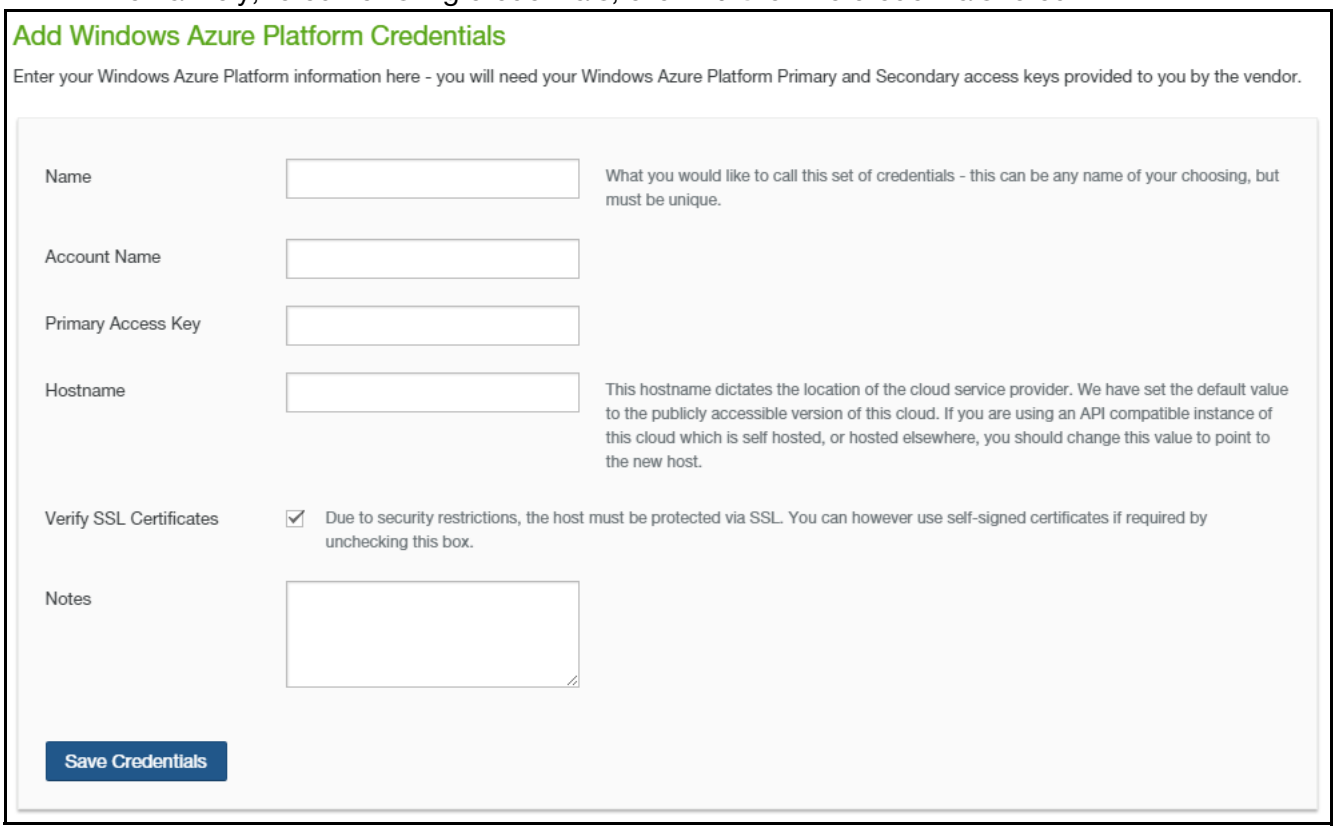

Figure 2-13: Add Windows Azure Platform Credentials page.

3. Enter the credentials for Microsoft Azure, including the following:
   - **Name**: A name for this set of credentials, which is used for display purposes.
   - **Account Name**: The Microsoft Azure Storage Account Name for this set of credentials.
   - **Primary Access Key**: The Microsoft Azure Primary Access Key for this set of credentials.
   - **Hostname**: The hostname for the location of the cloud service provider. Use the default setting: `blob.core.windows.net`
   - **Verify SSL Certificates**: Use the default **On** setting.
   - **Notes**: Optional information to save.

   Tip: *Be careful changing existing credentials. The connection between the Nasuni Filer and the container could become invalid, causing loss of data access. Credential editing is to update access after changes to the account name or the access key on the Microsoft Azure system.*

4. Click **Save Credentials**.

At this point, you can begin adding volumes to the Nasuni Filer. Volume creation, volume connection and credentials verification can each take up to 2 minutes.

Adding a volume to Nasuni Filer

Adding a volume to a Nasuni Filer in a customer-provided Microsoft Azure tenant is slightly different from the usual method of adding a volume.

First, you select the cloud provider. In this case, select Windows Azure.

After selecting the cloud provider, you select the credentials. If “Automatically Provisioned” is available, and you select “Automatically Provisioned”, then you can select the region. However, if you select previously entered credentials (see “Configuring Microsoft Azure credentials on a Nasuni Filer” on page 26), you cannot select the region, because the region is tied to the credentials. With Microsoft Azure, each storage account is tied to a single specific region (such as “Central US”). For this reason, if you have Microsoft Azure as the single cloud provider, and you want volumes in multiple regions, you must have multiple Microsoft Azure storage accounts.

To add a new volume, follow these steps:

1. Click **Volumes**, then click **Add New Volume**. The **Add New Volume** page appears.

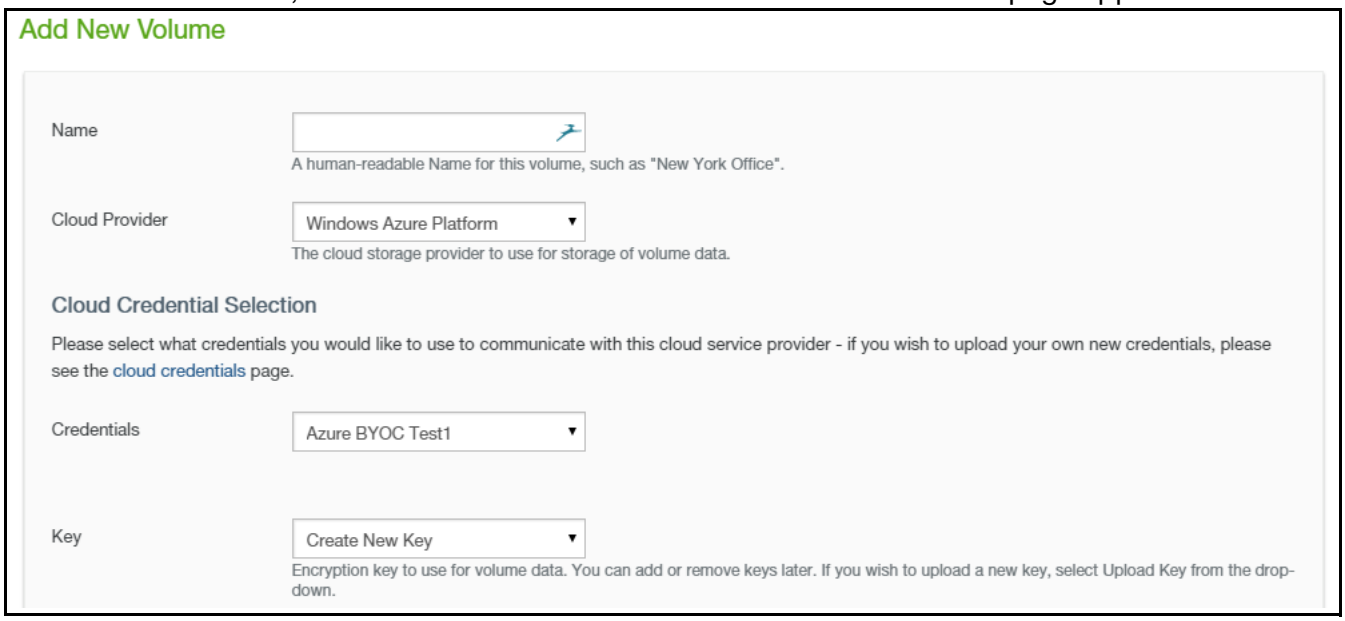

Figure 2-14: Add New Volume page.

Note: *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. Enter a human-readable name for the volume in the **Name** text box, for example, “New York Office”. The name you enter is automatically applied as the encryption key name in the **Keyname** text box.

   Note: *For iSCSI volumes, the iSCSI volume name is used to generate the target name. This includes changing any upper-case letters to lower-case, and changing any non-ASCII symbols to their hex code.*

3. Select a **Cloud Provider** from the drop-down list. In this case, select Windows Azure Platform. Available credentials appear.
4. From the **Credentials** drop-down list, select the credentials that you created in step 3 on page 27 of the previous section.

   Note: *Note that the Azure regions drop-down list is not available, because the region is defined at the time of the creation of the storage account.*

5. Continue with the rest of the **Add New Volume** page, as usual.

For more details, see the *Nasuni Filer Administration Guide.*

Configuring Microsoft Azure credentials on the NMC

Note: *If you change Microsoft Azure credentials, update them on the Nasuni Filer or NMC, to retain access to data.*

To configure Microsoft Azure credentials:

1. Open the Nasuni Management Console (NMC).
2. Click **Account**, then select **Cloud Credentials** from the menu. The **Cloud Credentials** page displays a list of cloud credentials.

Figure 2-15: Cloud Credentials page.

The following information appears for each set of credentials in the list:

- **Name**: The name of the set of credentials.
- **Filer**: The name of the Nasuni Filer.
- **Volumes**: The volumes that use the cloud credentials.
- **Cloud**: The type of cloud.
- **Actions**: Actions available for each set of credentials.

3. To add new credentials, click **Add New Credentials** and select the platform.
   Alternatively, to edit existing credentials, click **Edit Credentials** for the credentials to edit.

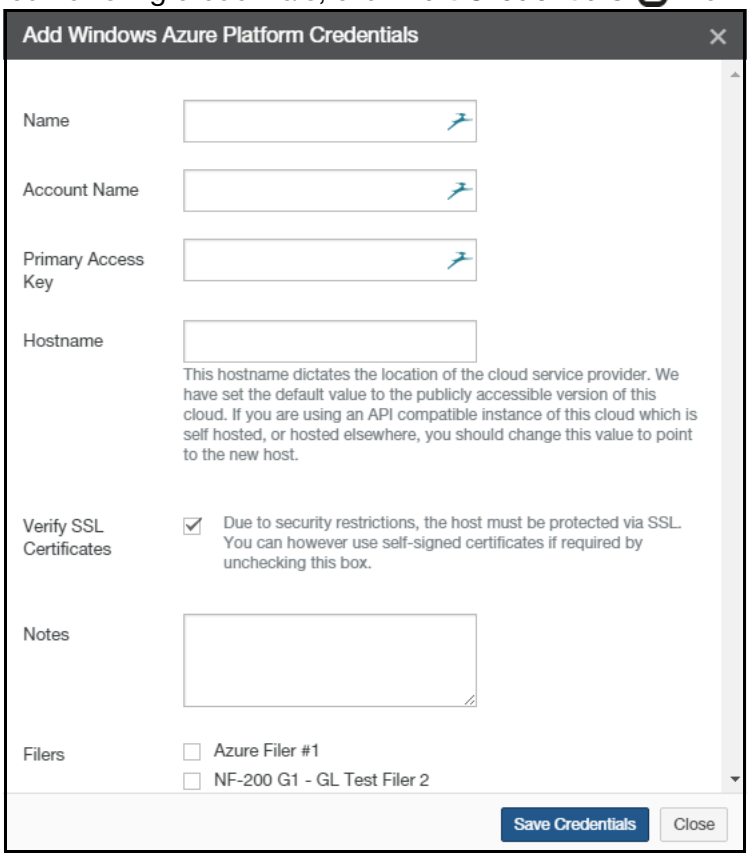

Figure 2-16: Add Windows Azure Platform Credentials page.

4. Enter the credentials for Microsoft Azure, including the following:
   - **Name**: A name for this set of credentials, which is used for display purposes.
   - **Account Name**: The Microsoft Azure Account Name for this set of credentials.
   - **Primary Access Key**: The Microsoft Azure Primary Access Key for this set of credentials.
   - **Hostname**: The hostname for the location of the cloud service provider. Use the default setting: `blob.core.windows.net`
   - **Verify SSL Certificates**: Use the default **On** setting.
   - **Notes**: Optional information to save.
   - **Filers**: The target Nasuni Filers.

   Tip: *Be careful changing existing credentials. The connection between the Nasuni Filer and the container could become invalid, causing loss of data access. Only change credentials after changes to the account name or the access key on the Microsoft Azure system.*

   Tip: *After defining one set of cloud credentials, you can use the Copy action to copy cloud credentials for one Nasuni Filer to other Nasuni Filers.*

5. Click **Save Credentials**.

Configuring the Nasuni Filer

You now use the *Nasuni Filer Initial Configuration Guide* and the *Nasuni Filer Administration Guide* to complete the configuration of the Nasuni Filer.

After the Nasuni Filer is running, if you need Nasuni Technical Support to help you with your Microsoft Azure instance, enable the Remote Support Service on the **Services** menu.

If directed by Nasuni Customer Support, to enable or disable Nasuni's compression and deduplication, or to adjust the chunk size, this is possible using the **Volume** page.

To enable or disable Nasuni's compression and deduplication, or to adjust the chunk size, follow these steps:

1. From the **Volume** list, select the volume. The **Volume** page for the volume appears, including the **Cloud I/O** area.

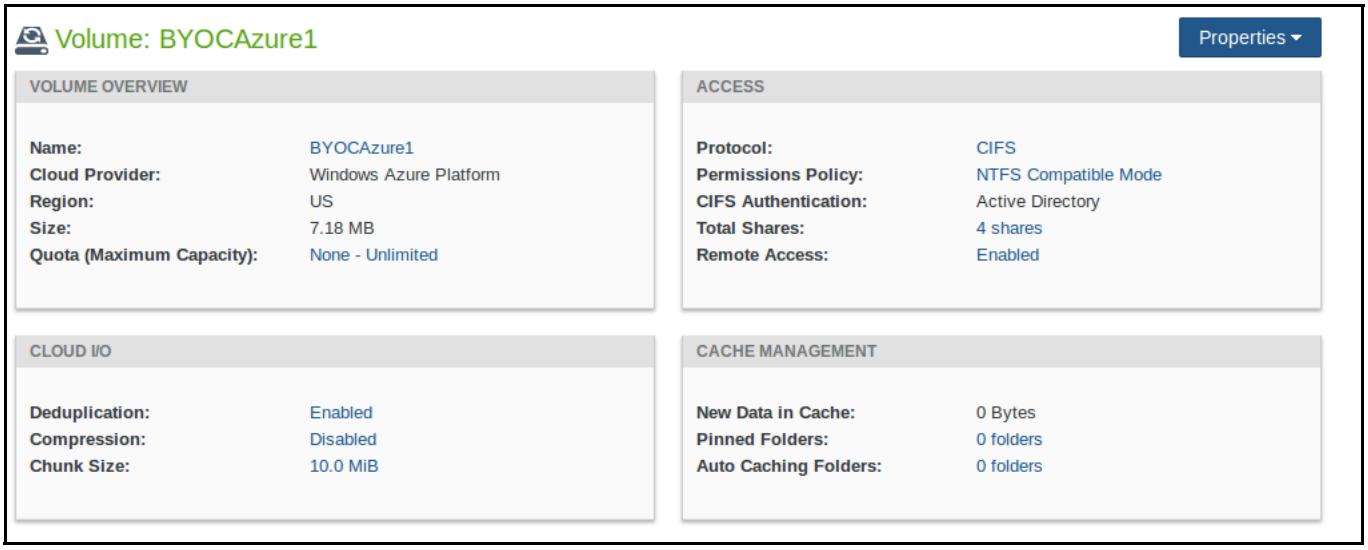

Figure 2-17: Cloud I/O area on the Volume page.

2. To enable or disable deduplication, enable or disable compression, or change the chunk size, click the current value. The **Change Volume Cloud I/O** dialog box appears.

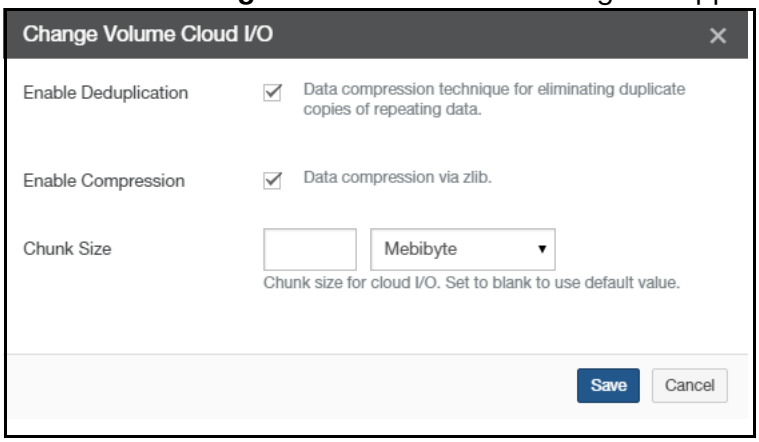

Figure 2-18: Change Volume Cloud I/O dialog box.

3. Select or deselect deduplication and compression.

4. Enter the chunk size, and select the units from the drop-down menu. To use the default chunk size, leave the text box blank.

   Warning: *Contact Nasuni Support before changing the chunk size.*

5. Click **Save** to save your settings.

Configuring the Nasuni Management Console

You now use the *Nasuni Management Console Guide* to complete the configuration of the Nasuni Management Console.

After the Nasuni Management Console is running, if you need Nasuni Technical Support to help you with your Microsoft Azure instance, enable the Remote Support Service on the **Console Settings** menu.

If directed by Nasuni Customer Support, to enable or disable Nasuni's compression and deduplication, or to adjust the chunk size for a volume, this is possible using the **Volume Cloud I/O** page.

To enable or disable Nasuni's compression and deduplication, or to adjust the chunk size, follow these steps:

1. Click **Volume**, then select **Cloud I/O**. The **Volume Cloud I/O** page for the volume appears.

   The following information appears for each volume in the list:

   - **Name**: The name of the volume.
   - **Filer**: The name of the Nasuni Filer for the volume.
   - **Deduplication**: The state of deduplication for this volume.
   - **Compression**: The state of compression for this volume.
   - **Chunk Size**: The chunk size for this volume.
   - **Actions**: Actions available for each volume.

2. For the volume to change, click **Edit** . The **Change Volume Cloud I/O** dialog box appears.
3. Select or deselect deduplication and compression.
4. Enter the chunk size, and select the units from the drop-down menu.

   Warning: *Contact Nasuni Support before changing the chunk size.*

5. Click **Save** to save your settings.

Performance

For the Nasuni Filer, industry-standard NAS and SAN interfaces are not designed to be hosted on remote sites and attached over the public Internet. Nasuni recommends using only Mobile Access (iOS and Android devices), Web Access, and Nasuni Desktop Client over long distances. Nasuni also recommends only using the NAS and SAN protocols from clients that are hosted in the same infrastructure “near” the Nasuni Filer.

For the Nasuni Management Console, since all access is browser-based, there are no specific performance concerns.

Adding a static IP address to an existing Nasuni Filer (using Azure Resource Manager and PowerShell)

Important: *You must have at least one subscription for this purpose.*

Note: *Confirm with Nasuni Sales or Support that your Nasuni account is configured to work with your existing Microsoft Azure account.*

Tip: *Run PowerShell as an Administrator.*

You can add a static IP address to an existing Nasuni Filer. This procedure uses the Azure Resource Manager and PowerShell. For details, see https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-static-private-ip-arm-ps.

To add a static IP address to an existing Nasuni Filer, follow these steps:

1. In Azure PowerShell, enter the following commands:

```
$nic=Get-AzureRmNetworkInterface -Name <NICname>
   -ResourceGroupName <RGname>
$nic.IpConfigurations[0].PrivateIpAllocationMethod = "Static"
$nic.IpConfigurations[0].PrivateIpAddress = "<privateip>"
Set-AzureRmNetworkInterface -NetworkInterface $nic
```

   where

   `<NICname>` is the name you are giving to the network interface controller (NIC);

   `<RGname>` is the name you are giving to the resource group;

   `<privateip>` is the private IP address for the static network IP.

Index

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W