NASUNI®

Installing the Nasuni Filer on the Azure Platform

Version 7.10
February 2018
Last modified: February 9, 2018

Document Information

Installing the Nasuni Filer on the Azure Platform
Version 7.10
February 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 on the Microsoft Azure platform.

What's in this Book

This guide contains the following chapters:

- Chapter 1, "Installing on the Microsoft Azure Platform," on page 7 explains how to install the Nasuni Filer or the Nasuni Management Console on the Microsoft Azure platform.
- Chapter 2, "Controlling the Microsoft Azure Instance," on page 29 explains how to control the Nasuni Filer or the Nasuni Management Console from the Microsoft Azure platform.
- Chapter 3, "Uninstalling the Microsoft Azure Instance," on page 31 explains how to remove the Nasuni Filer or the Nasuni Management Console from your system if you are upgrading or replacing your hardware.

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
2018-02-07	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*. 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*.

Date (As Of)	Changes
	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*.
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*.

Date (As Of)	Changes
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*. 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*.

Date (As Of)	Changes
	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*. 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: Installing on the Microsoft Azure Platform

Overview

This chapter explains how to perform the initial installation of the Nasuni Filer or the Nasuni Management Console on the Microsoft Azure platform.

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

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

> ***Note:*** *The vendor changes their interfaces occasionally with little notice to the users. The exact screens and text on these platforms might change at any time.*

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.*

Specifying a static IP address (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 create an Azure cloud service with a specified static IP address, and then deploy the new Nasuni Filer in that service. This procedure uses the Azure Resource Manager and PowerShell. For details, see https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-reserved-private-ip.

If you do not already have a service in Microsoft Azure, create a service 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 a cloud service, by using the following command:

   ```
   New-AzureService -ServiceName <servicename> -Location "<location>"
      $image = Get-AzureVMImage
      | ?{_.ImageName –like “<name_of_storage_account>”}
      New-AzureVMConfig -Name <vmname>
      -InstanceSize Basic_A3 -ImageName $image.ImageName `
      | Add-AzureProvisioningConfig -Linux -AdminUsername <adminuser>
       -Password <password> `
      | Set-AzureSubnet -SubnetNames <subnetname> `
      | Set-AzureStaticVNetIP -IPAddress <privateIP> `
      | New-AzureVM -ServiceName “<servicename>” -VNetName <vnetname>
   ```

   where

   `<servicename>` is the name of the service you are creating;

   `<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);

   `<name_of_storage_account>` is the name of the Storage Account you are creating;

   `<vmname>` is the name of the virtual machine you are creating;

   `<adminuser>` is the username of the administrator;

   `<password>` is the password of the administrator user;

   `<subnetname>` is the name of the subnet for the static network;

`<privateip>` is the private IP address for the static network IP;
`<servicname>` is the name of the service;
`<vnetname>` is the name of the vnet containing the IP address.
After the cloud service is created, you can deploy the Nasuni Filer using the Microsoft Azure public cloud virtual machine platform.

Deploying Nasuni Management Console (NMC) on the Azure Portal

Installing the Nasuni Management Console requires the corresponding Microsoft Azure VHD, 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 Windows Azure Management Portal at https://manage.windowsazure.com/*.*
>
> ***Important:*** *To access Active Directory-enabled volumes, the Nasuni Filer must be connected to an Active Directory server in the same Active Directory forest. This requires part of your Active Directory infrastructure to also be running on the Microsoft Azure platform. In particular, you must create and configure a Virtual Network for the virtual machine to join. Similarly, to access LDAP-enabled volumes, the Nasuni Filer must be able to access LDAP and Kerberos in the same LDAP domain.*
>
> ***Important:*** *Before beginning this procedure there must be an existing primary resource group, a primary virtual network for this virtual machine, and a primary subnet*
>
> ***Tip:*** *During this procedure, if the expected items do not appear, click the Subscriptions Filter icon near the top right of the dashboard, then select all the subscriptions that might include the item.*

Obtaining software

To obtain the NMC software, follow these steps:

1. Obtain the Microsoft Azure VHD file for the NMC from Nasuni by following these steps:

   a. If you do not have a Nasuni account already, go to the Nasuni evaluation Web site at https://www.nasuni.com/evaluate. The **Evaluate** page appears.

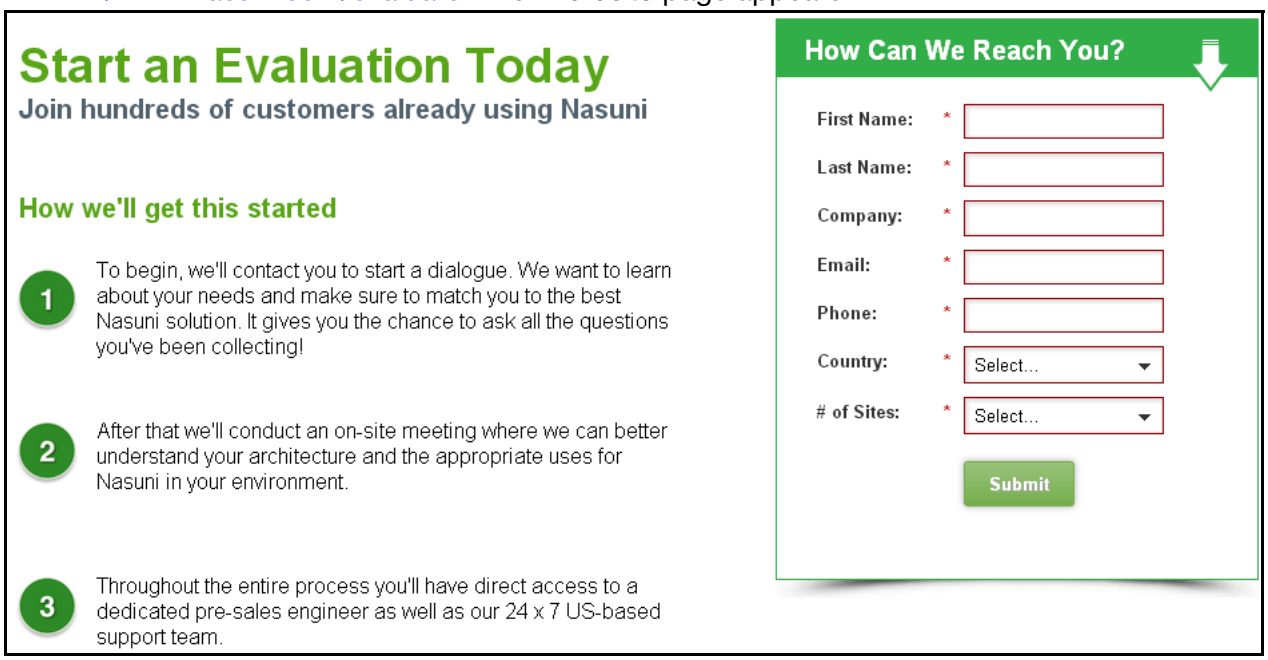

Figure 1-1: "Evaluate" page.

   Enter your **First Name**, **Last Name**, **Company** name, **Work Email** address, **Work Phone** number, **State**, and **Country**. Click **Submit**.

   Note: *The email address that you enter is used for authentication with Nasuni.*

   A member of the Nasuni staff will contact you with registration material to obtain your Nasuni account.

   b. Log in to your Nasuni account web site (https://account.nasuni.com/) and click **Downloads**. The **Downloads** page appears.

   c. In the **Nasuni Management Console** area, select the Azure format.

   d. Download the Nasuni Management Console software `.zip` file to your local drive.

   The amount of time to download the software file depends on your Internet connection. The file is approximately 17 GB in size.

   e. Unzip the software file to a convenient directory.

   Tip: *Since you must type the complete path to the extracted contents in a later step, the shorter the path, the better.*

   f. If the extracted file does not have the extension `.vhd`, change the extension to `.vhd`.

Installing and Configuring Azure Resource Manager PowerShell

For more information on the Azure PowerShell, see http://www.windowsazure.com/en-us/documentation/articles/install-configure-powershell/.

To install and configure the Azure Resource Manager (ARM) PowerShell module, follow these steps:

1. Launch PowerShell as Administrator.
2. Enter the following command:

   ```
   Install-Module AzureRM
   ```

   This command installs the Azure Resource Manager module from the PowerShell gallery.

   a. If prompted to download and install the latest version of NuGet, select **Yes**.

   b. If prompted to install modules from an untrusted repository, select **Yes**.
   PowerShell spends some time installing packages in the PowerShell window.
3. Enter the following command:

   ```
   Set-ExecutionPolicy Unrestricted
   ```

   This sets the execution policy. Loads all configuration files and runs all scripts.

   a. If prompted to allow the policy change, select **Yes**.
4. Enter the following command:

   ```
   Import-Module AzureRM
   ```

   This loads the AzureRM module into your PowerShell session.
5. Enter the following command:

   ```
   Login-AzureRmAccount
   ```

   a. Log in with the credentials for the Azure account.

   b. Select **Yes** for enabling data collection.

   c. Validate that the account and Subscription Names are correct.

Configuring ARM Storage Account and Uploading NMC Software

To configure the Azure Resource Manager storage account and upload the NMC software, follow these steps:

1. Open Azure Resource Manager in your preferred browser.

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

   a. To use the Azure Portal aka Azure Resource Manager (ARM), log in to https://portal.azure.com/, then continue with step b on page 21.
   Alternatively, to use the Azure Classic Portal aka Service Management model, log in to the Windows Azure Management Portal at https://manage.windowsazure.com/ . The Windows Azure dashboard page appears.

      i. On the bottom left of the page, click **New**. The **New** pane appears.

      ii. Click **Data Services**. On the menu that appears, click **Storage**, and then click **Quick Create**. The storage account quick create form appears.

      iii. In the **URL** 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 numbers and lowercase letters.

      iv. From the "**Account kind**" drop-down list, select "**General Purpose**".

      v. From the **Location/Affinity Group** drop-down list, select the location or affinity group for the storage account. By selecting the appropriate affinity group, you can locate your cloud services in the same data center as your storage.

      vi. From the **Subscription** drop-down list, select the subscription to use for this storage account.

      vii. To replicate your data to another location at no extra cost, select the **Enable Geo-Replication** check box. This is selected by default. If legal requirements or your organization's policies forbid moving your data to another location, clear the check box.

      viii. Click **Create Storage Account**.
      The storage account is created and appears in the **Storage** list on the Windows Azure dashboard.

      ix. Click the name of the storage account in the list. The page for the new storage account appears.

      x. Click **Dashboard**. The dashboard for this storage account appears. Note the **Endpoint** URL of the **Blobs** service.
      Continue with step 3 on page 15.

   b. To create a storage account at https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), follow these steps:

      i. On the top left of the page, click **New**. The **New** pane appears.

      ii. Click **Data + Storage**. On the **Data + Storage** pane, click "**Storage account**", and then, at the bottom of the page, click **Create**. The "**Storage account**" creation form appears.

      iii. In the **Storage** 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 numbers and lowercase letters, such as "`organizationfilers`".

iv. Click "**Pricing tier**". The "**Choose your pricing tier**" pane appears. Select the pricing tier, then click **Select**.

Tip: *Nasuni recommends "Geo-Redundant Replication" with Windows Azure. 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.*

v. Click **Resource Group**, then either create a new resource group or use an existing resource group.

vi. Click **Subscription**, then select the subscription to use for this storage account.

vii. Click **Account kind**, then select **General Purpose**.

viii. Click **Location**, then select the location for the storage account.

ix. Click **Diagnostics**, then select either **Off** or **On**.

x. Ensure that "**Pin to dashboard**" is selected.

xi. Click **Create**.
The storage account is created and appears on the Windows Azure dashboard.

xii. Click the name of the storage account. The page for the new storage account appears.

xiii. Click **Blobs**. The "**Blob service**" pane for this storage account appears. Note the "**Primary blob service endpoint**" URL.
Continue with step 3 on page 15.

3. If you do not already have a container in your storage account, create a container within your storage account by following these steps:

Note: *This container can house all of the Nasuni Filers and the NMC, or separate containers can be created for each instance.*

a. On https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), continue with step b on page 16
Alternatively, to use https://manage.windowsazure.com/ (for the Azure Classic Portal aka Service Management model), follow these steps..

i. On the Windows Azure dashboard page, click **Storage** in the left-hand column. A list of storage accounts appears.

ii. Click the name of the storage account you just created. The dashboard for this storage account appears. Near the top of the dashboard, click **Containers**. A list of containers for this storage account appears.

iii. At the bottom of the page, click **Add**. The **New container** dialog box appears.

iv. In the **Name** text box, enter a descriptive name for this container. The name must be at least 3 characters long and at most 63 characters long, using only numbers, hyphens, and

lowercase letters. The name must start with a letter or a number, and cannot contain two consecutive hyphens.

v. From the **Access** drop-down list, select the type of access for this container, from the following choices:

- **Private**: The container is private and can be accessed only by the account owner. This is the default.
- **Public Blob**: Anyone can read the blobs in the container, but only the account owner can read the container properties and metadata.
- **Public Container**: Anyone can read the blobs, container properties, and metadata.

vi. Click the checkmark in the lower right corner of the dialog box.
The new container is created in the storage account, and appears in the list of containers.

vii. Continue with step c on page 16.

b. To create a container within your storage account at https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), follow these steps:

i. On the Windows Azure dashboard page, click the name of the storage account you just created. The dashboard for this storage account appears. Near the top of the dashboard, click **Containers**. A list of containers for this storage account appears.

ii. Click **Add**. The **Add a container** pane appears.

iii. In the **Name** text box, enter a descriptive name for this container. The name must be at least 3 characters long and at most 63 characters long, using only numbers, hyphens, and lowercase letters. The name must start with a letter or a number, and cannot contain two consecutive hyphens.

iv. From the **Access type** drop-down list, select the type of access for this container, from the following choices:

- **Private**: The container is private and can be accessed only by the account owner. This is the default.
- **Blob**: Anyone can read the blobs in the container, but only the account owner can read the container properties and metadata.
- **Container**: Anyone can read the blobs, container properties, and metadata.

v. Click **OK**.
The new container is created in the storage account, and appears in the list of containers.

c. Select the new blob that you created.

i. Select **Upload**.

ii. Change the **Blob type** to “Page Blob”.

4. Use the Windows Azure PowerShell, or a comparable utility, to prepare and upload the VHD file, by following these steps:

   Note: *Other tools are available to prepare and upload the VHD file. The steps here are for using the Windows Azure PowerShell.*

   a. Download and install the Windows Azure PowerShell, or comparable utility, from http://www.windowsazure.com/en-us/documentation/articles/install-configure-powershell/.

   b. Enter the following command:

      ```
      Get-AzurePublishSettingsFile
      ```

      This command opens a browser window and automatically downloads a `.publishsettings` file. Save this file to a convenient directory.

      Tip: *Since you must type the complete path to this file in a later step, the shorter the path, the better.*

   c. Enter the following command:

      ```
      Import-AzurePublishSettingsFile <PathToPublishsettingsFile>
      ```

      where `<PathToPublishsettingsFile>` is the full path to the `.publishsettings` file.

   d. Enter the following command:

      ```
      Select-AzureSubscription -SubscriptionName <SubscriptionName>
      ```

      where `<SubscriptionName>` is the subscription name of the storage account. This ensures that the storage account and the subscription are consistent.

   e. Enter the following command:

      ```
      Add-AzureRmVhd -ResourceGroupName <ResourceGroup>
       -Destination <EndpointURL>/<ContainerName>/<VHDName>
       -LocalFilePath <PathToLocalVHDFile>
      ```

      where
      `<ResourceGroupName>` is the name of the resource group from step v on page 15;
      `<EndpointURL>` is the Endpoint URL for the storage account you created in step 2 on page 14, including the extension;
      `<ContainerName>` is the name of the container you created in step 3 on page 15, including the extension;
      `<VHDName>` is the name you want to give to the name of the VHD when it is in the container, including the extension;

      Tip: *After the VHD file has been uploaded, it cannot be renamed. Ensure that your naming conventions are addressed before uploading the VHD file.*

      `<PathToLocalVHDFile>` is the full path and file name, including the extension, of the `.vhd` file that you extracted in step f on page 12.

The Windows Azure PowerShell begins calculating the MD5 hash of the `.vhd` file. This can take several minutes. A countdown provides an estimate of the time until finished.

The `.vhd` file is copied to the container in the storage account.

f. Verify that the `.vhd` file is in the container by navigating to the container and clicking the container name. The `.vhd` file appears in the list with the new name assigned in step e on page 17.

5. Use the Windows Azure PowerShell, or a comparable utility, to deploy the NMC, by following these steps:

   a. Enter the following command:

   ```
   New-AzureRmResourceGroupDeployment -Name <nmcname>
    -ResourceGroupName <resourcegroupname>
    -TemplateUri <template>
   ```

   where
   `<nmcname>` is the name of the NMC for this environment;
   `<resourcegroupname>` is the name of the resource group for this environment.
   `<template>` is the Azure template `https://raw.githubusercontent.com/azure/azure-quickstart-templates/master/201-vm-specialized-vhd-existing-vnet/azuredeploy.json`

   b. A wizard prompts for the following information:

   - **vmName**: Name of the NMC in the Azure Virtual Machines view. This can match the name given during step a on page 18.
   - **osType**: Use “Linux” without the quotes.
   - **osDiskVhdUri**: Path to the uploaded VHD from step e on page 17. If you are unsure, the notification of the upload includes the path. After completion of the upload, the URL can be copied from the VHD blob properties.
   - **vmSize**: VM size, as listed here: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general
   - **existingVirtualNetworkName**: Virtual Network name of your Azure virtual network where the NMC is to reside.
   - **existingVirtualNetworkResourceGroup**: Resource group where the virtual network above is located.
   - **subnetName**: Subnet name located within the virtual network above.
   - **dnsNameForPublicIP**: Creates the hostname for the `.cloudapp.azure.com` domain, rather than your domain’s explicit domain information. The script fails if it is not unique, however, it is not required for proper functionality.

   After the script completes successfully, the new virtual machine should be assigned to the Primary Resource Group.

Launching the Azure VM

Installing the Nasuni Filer requires the corresponding Microsoft Azure VHD, 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 Windows Azure Management Portal at https://manage.windowsazure.com/*.*
>
> ***Important:*** *To access Active Directory-enabled volumes, the Nasuni Filer must be connected to an Active Directory server in the same Active Directory forest. This requires part of your Active Directory infrastructure to also be running on the Microsoft Azure platform. In particular, you must create and configure a Virtual Network for the virtual machine to join. Similarly, to access LDAP-enabled volumes, the Nasuni Filer must be able to access LDAP and Kerberos in the same LDAP domain.*
>
> ***Tip:*** *During this procedure, if the expected items do not appear, click the Subscriptions Filter icon near the top right of the dashboard, then select all the subscriptions that might include the item.*

To launch the VM:

1. Obtain the Microsoft Azure VHD file from Nasuni by following these steps:
   a. If you do not have a Nasuni account already, go to the Nasuni evaluation Web site at https://www.nasuni.com/evaluate. The **Evaluate** page appears.

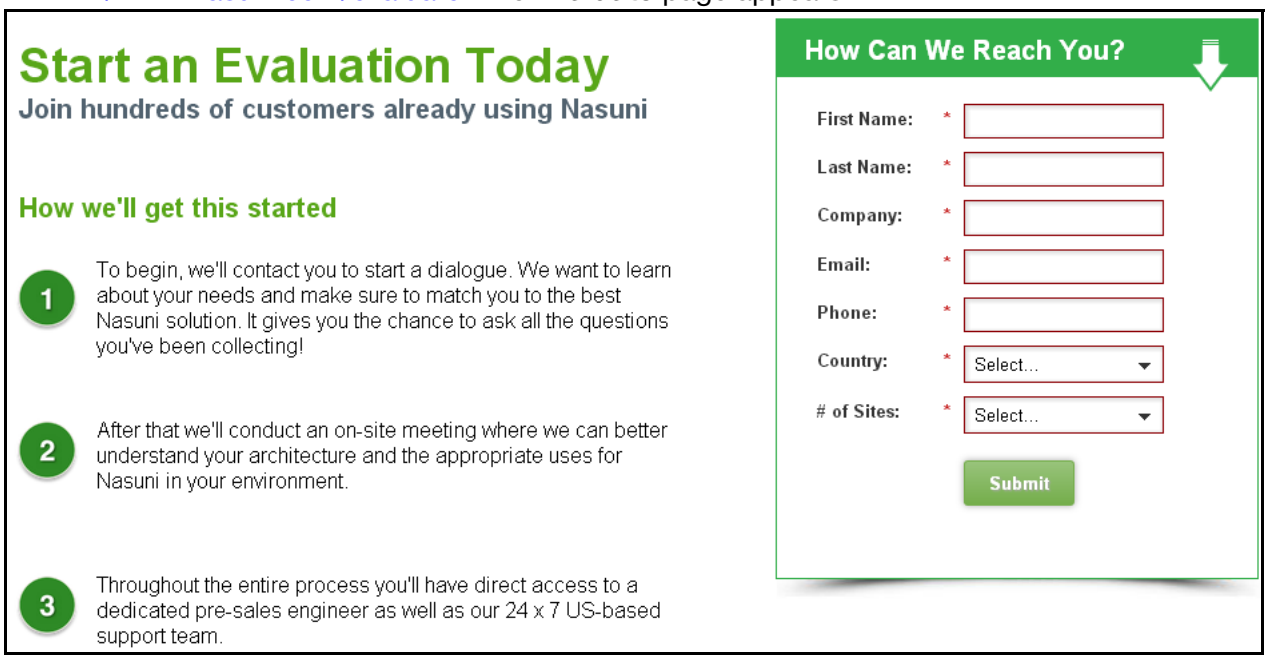

Figure 1-2: "Evaluate" page.

Enter your **First Name**, **Last Name**, **Company** name, **Work Email** address, **Work Phone** number, **State**, and **Country**. Click **Submit**.

Note: *The email address that you enter is used for authentication with Nasuni.*

A member of the Nasuni staff will contact you with registration material to obtain your Nasuni account.

b. Log in to your Nasuni account web site (https://account.nasuni.com/) and click **Downloads**. The **Downloads** page appears.

c. Select the Azure format.

d. Download the Nasuni Filer 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 file is approximately 300 MB in size.

e. Unzip the Nasuni Filer software file to a convenient directory.

Tip: *Since you must type the complete path to the extracted contents in a later step, the shorter the path, the better.*

f. If the extracted file does not have the extension `.vhd`, change the extension to `.vhd`.

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

a. Log in to the Windows Azure Management Portal at https://manage.windowsazure.com/ for the Azure Classic Portal aka Service Management model. The Windows Azure dashboard page appears.
Alternatively, log in to https://portal.azure.com/ for the Azure Portal aka Azure Resource Manager (ARM). Continue with step b on page 21.

i. On the bottom left of the page, click **New**. The **New** pane appears.

ii. Click **Data Services**. On the menu that appears, click **Storage**, and then click **Quick Create**. The storage account quick create form appears.

iii. In the **URL** 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 numbers and lowercase letters.

iv. From the **Location/Affinity Group** drop-down list, select the location or affinity group for the storage account. By selecting the appropriate affinity group, you can locate your cloud services in the same data center as your storage.

v. From the **Subscription** drop-down list, select the subscription to use for this storage account.

vi. To replicate your data to another location at no extra cost, select the **Enable Geo-Replication** check box. This is selected by default. If legal requirements or your organization's policies forbid moving your data to another location, clear the check box.

vii. Click **Create Storage Account**.
The storage account is created and appears in the **Storage** list on the Windows Azure dashboard.

viii. Click the name of the storage account in the list. The page for the new storage account appears.

ix. Click **Dashboard**. The dashboard for this storage account appears. Note the **Endpoint** URL of the **Blobs** service.
Continue with step 3 on page 22.

b. To create a storage account at https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), follow these steps:

i. On the top left of the page, click **New**. The **New** pane appears.

ii. Click **Data + Storage**. On the **Data + Storage** pane, click "**Storage account**", and then, at the bottom of the page, click **Create**. The "**Storage account**" creation form appears.

iii. In the **Storage** 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 numbers and lowercase letters.

iv. Click "**Pricing tier**". The "**Choose your pricing tier**" pane appears. Select the pricing tier, then click **Select**.

Tip: *Nasuni recommends "Geo-Redundant Replication" with Windows Azure. 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.*

v. Click **Resource Group**, then either create a new resource group or use an existing resource group.

vi. Click **Subscription**, then select the subscription to use for this storage account.

vii. Click **Location**, then select the location for the storage account.

viii. Click **Diagnostics**, then select either **Off** or **On**.

ix. Ensure that "**Pin to dashboard**" is selected.

x. Click **Create**.
The storage account is created and appears on the Windows Azure dashboard.

xi. Click the name of the storage account. The page for the new storage account appears.

xii. Click **Blobs**. The "**Blob service**" pane for this storage account appears. Note the "**Primary blob service endpoint**" URL.
Continue with step 3 on page 22.

3. If you do not already have a container in your storage account, create a container within your storage account by following these steps:

   a. On https://manage.windowsazure.com/ (for the Azure Classic Portal aka Service Management model), follow these steps.
   Alternatively, to use https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), continue with step b on page 22.

      i. On the Windows Azure dashboard page, click **Storage** in the left-hand column. A list of storage accounts appears.

      ii. Click the name of the storage account you just created. The dashboard for this storage account appears. Near the top of the dashboard, click **Containers**. A list of containers for this storage account appears.

      iii. At the bottom of the page, click **Add**. The **New container** dialog box appears.

      iv. In the **Name** text box, enter a descriptive name for this container. The name must be at least 3 characters long and at most 63 characters long, using only numbers, hyphens, and lowercase letters. The name must start with a letter or a number, and cannot contain two consecutive hyphens.

      v. From the **Access** drop-down list, select the type of access for this container, from the following choices:

         - **Private**: The container is private and can be accessed only by the account owner. This is the default.
         - **Public Blob**: Anyone can read the blobs in the container, but only the account owner can read the container properties and metadata.
         - **Public Container**: Anyone can read the blobs, container properties, and metadata.

      vi. Click the checkmark in the lower right corner of the dialog box.
      The new container is created in the storage account, and appears in the list of containers.

      vii. Continue with step 4 on page 23.

   b. To create a container within your storage account at https://portal.azure.com/ (for the Azure Portal aka Azure Resource Manager (ARM)), follow these steps:

      i. On the Windows Azure dashboard page, click the name of the storage account you just created. The dashboard for this storage account appears. Near the top of the dashboard, click **Containers**. A list of containers for this storage account appears.

      ii. Click **Add**. The **Add a container** pane appears.

      iii. In the **Name** text box, enter a descriptive name for this container. The name must be at least 3 characters long and at most 63 characters long, using only numbers, hyphens, and lowercase letters. The name must start with a letter or a number, and cannot contain two consecutive hyphens.

iv. From the **Access type** drop-down list, select the type of access for this container, from the following choices:

- **Private**: The container is private and can be accessed only by the account owner. This is the default.
- **Blob**: Anyone can read the blobs in the container, but only the account owner can read the container properties and metadata.
- **Container**: Anyone can read the blobs, container properties, and metadata.

v. Click **OK**.
The new container is created in the storage account, and appears in the list of containers.

vi. Continue with step 4 on page 23.

4. Use the Windows Azure PowerShell, or a comparable utility, to prepare and upload the VHD file, by following these steps:

   Note: *Other tools are available to prepare and upload the VHD file. The steps here are for using the Windows Azure PowerShell.*

   a. Download and install the Windows Azure PowerShell, or comparable utility, from http://www.windowsazure.com/en-us/documentation/articles/install-configure-powershell/.

   b. Type the following command:

      ```
      Get-AzurePublishSettingsFile
      ```

      This command opens a browser window and automatically downloads a `.publishsettings` file. Save this file to a convenient directory.

      Tip: *Since you must type the complete path to this file in a later step, the shorter the path, the better.*

   c. Type the following command:

      ```
      Import-AzurePublishSettingsFile <PathToPublishsettingsFile>
      ```

      where `<PathToPublishsettingsFile>` is the full path to the `.publishsettings` file.

   d. Type the following command:

      ```
      Select-AzureSubscription -SubscriptionName <SubscriptionName>
      ```

      where `<SubscriptionName>` is the subscription name of the storage account. This ensures that the storage account and the subscription are consistent.

e. Type the following command:

```
Add-AzureVhd -Destination <EndpointURL>/<ContainerName>/<VHDName>
 -LocalFilePath <PathToLocalVHDFile>
```

where
`<EndpointURL>` is the Endpoint URL for the storage account you created in step 2, including the extension;
`<ContainerName>` is the name of the container you created in step 3, including the extension;
`<VHDName>` is the name you want to give to the name of the VHD when it is in the container, including the extension; and
`<PathToLocalVHDFile>` is the full path and file name, including the extension, of the `.vhd` file that you extracted in step 1.

The Windows Azure PowerShell begins calculating the MD5 hash of the `.vhd` file. This can take several minutes. A countdown provides an estimate of the time until finished.

The `.vhd` file is copied to the container in the storage account.

f. Verify that the `.vhd` file is in the container by navigating to the container and clicking the container name. The `.vhd` file appears in the list with the new name assigned in step e.

5. Create an image from this `.vhd` file by following these steps:

a. On https://manage.windowsazure.com/ (for the Azure Classic Portal aka Service Management model), follow these steps.

b. On the Windows Azure dashboard page, click **Virtual Machines** in the left-hand column. A list of **Virtual Machine Instances** appears.

Tip: *If the expected items do not appear, click the Subscriptions Filter icon near the top right of the dashboard, then select all the subscriptions that might include the item.*

c. Near the top of the dashboard, click **Images**. A list of images appears.

d. At the bottom of the page, click **Create**. The **Create an image from a VHD** dialog box appears.

e. In the **Name** text box, enter a descriptive name for this image. The name must be at least 1 character long and at most 100 characters long, using only numbers, hyphens, underscores, and lowercase letters. The name must start with a letter, and must end with a letter or a number.

f. In the **Description** text box, enter a description for this image. The description must have fewer than 150 characters.

g. Click in the VHD URL box, then navigate to the storage account, container, and `.vhd` file. Click **Open**.

h. From the **Operating System Family** drop-down list, select **Linux**.

i. Select the "**I have run waagent -deprovision on the virtual machine**" check box.

j. Click the checkmark in the lower right corner of the dialog box.
The new image is created, and appears in the list of images.

6. Create the virtual machine by following these steps:

   Important: *To access Active Directory-enabled volumes, before performing this step, ensure that there is Virtual Network for the virtual machine to join.*

   a. On the Windows Azure dashboard page, click **Virtual Machines** in the left-hand column. A list of **Virtual Machine Instances** appears.

   b. At the bottom of the page, click **New**. The **New** pane appears.

   c. Click **Virtual Machine**. On the menu that appears, click **From Gallery**.

   d. The **Virtual machine image selection** page appears.

   e. Click **My Images**. A list of available images appears. Select the image that you created in step 5. Then click the right-arrow at the bottom right of the page. The **Virtual machine configuration** page appears.

   f. In the **Virtual Machine Name** text box, enter a descriptive name for this virtual machine. The name must be at least 3 characters long and at most 15 characters long, using only numbers, hyphens, and lowercase letters. The name must start with a letter, and must end with a letter or a number.

   g. For the **Tier**, select **Standard**, which is recommended for production workloads. For more information, see https://azure.microsoft.com/en-us/pricing/details/virtual-machines/#Linux.

   h. From the **Size** drop-down list, select the size of the virtual machine. Select a virtual machine with at least 4 cores and at least 6 GB of memory.

      Tip: *This is the minimum configuration. Larger values might be necessary.*

   i. In the **New User Name** text box, enter a user name. The user name must be at least 4 characters. This user name is not actually used, so it can have any allowed value.

   j. Click the right-arrow at the bottom right of the page. The next **Virtual machine configuration** page appears.

   k. Accept the default values of the **Cloud Service**, **Cloud Service DNS Name** (based on the **Virtual Machine Name** in step f), and the **Availability Set**.
   To access Active Directory-enabled volumes, from the **Region/Affinity Group/Virtual Network** drop-down list, select the appropriate value. If you are not accessing Active-Directory-enabled volumes, accept the default value of the **Region/Affinity Group/Virtual Network**.

   l. Use the list of **Endpoints** to configure port security. For each port or protocol, enter the following information:

      - **Name**: The name of the protocol. Select from the drop-down list or enter name.
      - **Protocol**: From the drop-down list, select **TCP** or **UDP**.
      - **Public Port**: Enter or accept the public port number.

- **Private Port**: Enter or accept the private port number.

  Warning: *Running the Nasuni Filer or NMC on the Microsoft Azure platform is similar to running these systems outside of your business. Unused ports should not be exposed to the public Internet, including the SSH port, port 222. Minimally, the following ports should be exposed to the hosts that access them:*
  Outbound*: Microsoft Azure does not enable restricting outbound traffic. Nasuni recommends allowing outgoing traffic on all ports to all hosts for the Nasuni Filer and NMC.*
  Inbound*: Here are recommendations for the following ports:*

  - **Port 222 SSH**: Close this port. If Nasuni Customer Support requests you to open this port, open this port temporarily to all clients/ranges.
  - **Port 443 TCP**: Used for Web Access as well as Mobile Access (iOS and Android devices). If these features are in use, Nasuni recommends opening this port to all clients/ranges. Note that these features must be enabled on the Nasuni Filer.
  - **Port 8443 TCP**: Used to administer the Nasuni Filer and Nasuni Management Console. Open to clients that need to use the Nasuni administration interface.
  - **Ports 139 and 445 TCP**: Open to clients that need to use SMB/CIFS.
  - **Ports 111, 662, 875, 892, 2049, and 32803 TCP or UDP**: Open to clients that need to use NFS.
  - **Port 3260 TCP**: Open to clients that need to use iSCSI.
  - **Port 161 UDP**: Open to clients that need to use SNMP.

m. Click the right-arrow in the lower right corner of the dialog box. The next **Virtual machine configuration** page appears.

n. Accept all defaults. Click the checkmark in the lower right corner of the dialog box.

7. The new virtual machine is created, and appears in the list of virtual machines. The state should become Running.
   Details of the instance include **Status**, **Subscription**, **Location**, and **DNS Name**.

8. Note the **DNS Name** address, which is of the format `<VMName>.cloudapp.net`, where `<VMName>` is the name of the VM.

9. If installing a Nasuni Filer, attach a cache disk to the virtual machine by following these steps:

   a. On the Windows Azure dashboard page, click **Virtual Machines** in the left-hand column. A list of **Virtual Machine Instances** appears.

   b. At the bottom of the page, click **Attach**. From the drop-down list, select **Attach empty disk**. The "**Attach an empty disk to the virtual machine**" dialog box appears.

   c. In the **Size (GB)** text box, enter the size of the new disk in GB. For typical instances (at least 4 cores and at least 6 GB of memory), Nasuni recommends no larger than 1023 GB.

d. Host caching can improve performance under some circumstances. Select the **Host Cache Preference** from the following choices:

- **None**: Do not use host caching.
- **Read Only**: Use host caching only for read operations.
- **Read/Write**: Use host caching for both read and write operations. Nasuni recommends enabling **Read/Write** host caching.

e. Click the checkmark in the lower right corner of the dialog box.
The cache disk is attached to the virtual machine. This might take 10 minutes to complete. The state should become Running.

> ***Note:*** *When installing a Nasuni Filer, the Nasuni Filer 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.*

10. In your web browser, enter the following in the address bar and press **Enter**:

```
https://<DNS Name>
```

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

11. The Nasuni Filer or Nasuni Management Console is now installed and ready to access using the DNS Name address from step 8 on page 26.

Configuring the Nasuni Filer on Microsoft Azure

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

During this configuration, do not change any of the network settings. Leave the network interface/ configuration as DHCP and the traffic group as General. Only a single interface and traffic group are supported on Microsoft Azure images.

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.

Configuring the Nasuni Management Console on Microsoft Azure

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

During this configuration, do not change any of the network settings. Leave the network interface/ configuration as DHCP and the traffic group as General. Only a single interface and traffic group are supported on Microsoft Azure images.

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.

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.

Chapter 2: Controlling the Microsoft Azure Instance

Overview

Virtual platforms offer the ability to control various aspects of your Nasuni Filer or Nasuni Management Console. This chapter presents procedures for these control functions. Because these controls depend on third-party virtual platforms, you should follow the procedures for your specific virtual platform.

> ***Note:*** *The vendor changes their interfaces occasionally with little notice to the users. The exact screens and text on these platforms might change at any time.*

Status of the Microsoft Azure instance

On the virtual platform, you can view the status of the Microsoft Azure instance of the Nasuni Filer or Nasuni Management Console. On the Windows Azure dashboard, click **Virtual Machines** in the left column, then select the virtual machine from the list. The virtual machine page appears. Click **Dashboard**.

Information appears, including graphs of activity, status, DNS name, public virtual IP address, and details about the disks.

Shutting down the Microsoft Azure instance

On the virtual platform, you can shut down the Microsoft Azure instance of the Nasuni Filer or Nasuni Management Console.

> ***Note:*** *You can also shut down the Nasuni Filer or Nasuni Management Console using the* **Shutdown** *or* **Power** *button available on every page.*

To shut down the Microsoft Azure instance, follow these steps:

1. Log in to the Windows Azure Management Portal at https://manage.windowsazure.com/. The Windows Azure dashboard page appears.

2. Click **Virtual Machines** in the left-hand column. The **Virtual Machines Instances** screen appears.
3. Select the instance.
4. At the bottom of the screen, select **Shut Down**. The state changes to Stopping, then to Stopped.
   The virtual machine shuts down.

Starting the Microsoft Azure Instance

On the virtual platform, you can start a stopped Microsoft Azure instance of the Nasuni Filer or Nasuni Management Console.

To start a stopped Microsoft Azure instance, follow these steps:

1. Log in to the Windows Azure Management Portal at https://manage.windowsazure.com/. The Windows Azure dashboard page appears.
2. Click **Virtual Machines** in the left-hand column. The **Virtual Machines Instances** screen appears.
3. Select the instance.
4. At the bottom of the screen, select **Start**. The state changes to Starting, then to Running.
   The virtual machine starts.

Chapter 3: Uninstalling the Microsoft Azure Instance

Overview

This chapter explains how to uninstall the Nasuni Filer or Nasuni Management Console from the Microsoft Azure platform. You might need to uninstall the Nasuni Filer or Nasuni Management Console if you are upgrading the system hardware.

> ***Note:*** *The vendor changes their interfaces occasionally with little notice to the users. The exact screens and text on these platforms might change at any time.*

Uninstalling the Nasuni Filer or Nasuni Management Console

To uninstall the Nasuni Filer or Nasuni Management Console on the Microsoft Azure platform:

1. Log in to the Windows Azure Management Portal at https://manage.windowsazure.com/. The Windows Azure dashboard page appears.
2. Click **Virtual Machines** in the left-hand column. The **Virtual Machines Instances** screen appears.
3. Select the instance.
4. At the bottom of the screen, select **Delete**.

   > ***Caution:*** *Deleting a Nasuni Filer deletes the Microsoft Azure instance and all data in it. Any data not preserved via a snapshot is permanently lost*

5. A dialog appears asking if you are sure you want to delete the virtual machine. Click **Yes**. The virtual machine is uninstalled.

6. Deleting the virtual machine does not delete the data disks associated with the virtual machine. To delete the data disks, follow these steps:

   a. On the Virtual Machines page, click **Disks** at the top of the page.

   b. A list of disks appear. Select the disk to delete from the list. The **Attached To** entry should be blank.

   c. At the bottom of the screen, click **Delete**. Two menu choices appear: "**Delete the associated VHD**" and "**Retain the associated VHD**". Select "**Delete the associated VHD**".

   d. A dialog appears asking if you are sure you want to delete the disk. Click **Yes**.

   e. If there are more data disks to delete, continue with step b above.

   The selected disks and selected VHDs are deleted.

Index

N

P

R

S

T

U

V

W