Quest

Foglight® for Cloud Migration 6.3.0

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

their respective owners.

Legend

WARNING: **A WARNING icon indicates a potential for property damage, personal injury, or death.**

CAUTION: **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight for Cloud Migration User Guide
Updated - 2023
Foglight Version - 6.3.0
Cartridge Version - 6.3.0

Contents

1

Using Foglight for Cloud Migration

Foglight® for Cloud Migration supports Cloud Model for any cloud. It finds the best target cloud tiers for the virtual machines you selected, and adds the virtual machines to migration plan. After configured monitored Rapid Recovery core server and with an available Azure account, Foglight for Cloud Migration helps you to migrate the selected VMware virtual machines to Azure cloud.

This section introduces you to the Foglight for Cloud Migration environment, and provides you with essential information.

For more information, see the following topics:

- Installation requirements
- Dashboard location and UI elements

Installation requirements

Foglight for Cloud Migration comes installed on Foglight Evolve and can be installed on a Foglight Management Server.

Foglight for Cloud Migration requires the following cartridges for data collection:

- *OptimizerAutomation-5.8.3.car*
- *Optimizer-5_8_3.car*
- *CommonAnalytics-5.8.3.car*
- *Virtual-VMware-Lite-5.8.3.car*
- *Virtual-HyperV-Lite-5.8.3.car*
- *Protect-1_9_0.car*
- *Cloud-Migration-5_8_3.car*

While Foglight Evolve comes with these cartridges pre-installed and enabled, a stand-alone Foglight release requires that these components be installed on the Foglight Management Server. For more information about installing Foglight for Cloud Migration, and for details about system requirements and version compatibility, see the *Foglight Cloud Migration Release Notes*.

Dashboard location and UI elements

After installing Foglight for Cloud Migration, the **Cloud Migration** dashboard appears in the Foglight Management Server.

To access the Cloud Migration dashboard:

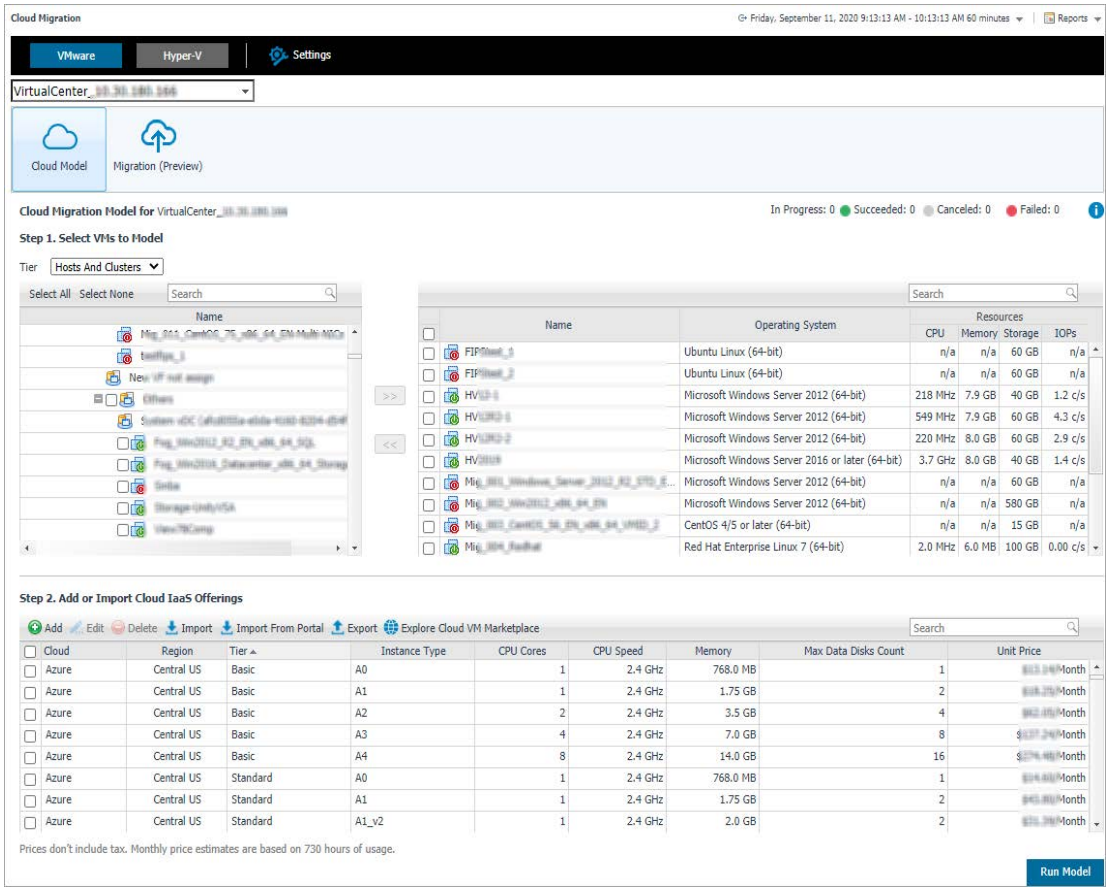
1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Dashboards*, click **Cloud Migration**.

The **Cloud Migration** dashboard opens.

Figure 1. Cloud Migration dashboard



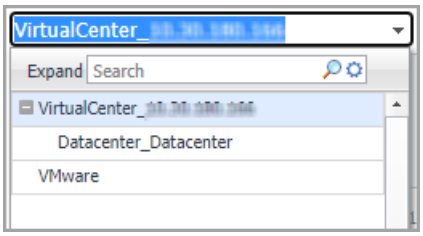
The **Cloud Migration** dashboard consists of the following UI elements:

- Group selector
- Action bar
- Menu bar
- Migration status bar
- Quick view

Group selector

The Group selector is located at the top of the dashboard and allows you to select the virtual environment that you want to monitor.

Figure 2. Group Selector



Action bar

The actions bar at the top of the screens contains the following options, Domain switcher and Settings.

Figure 3. Action bar

Domain switcher

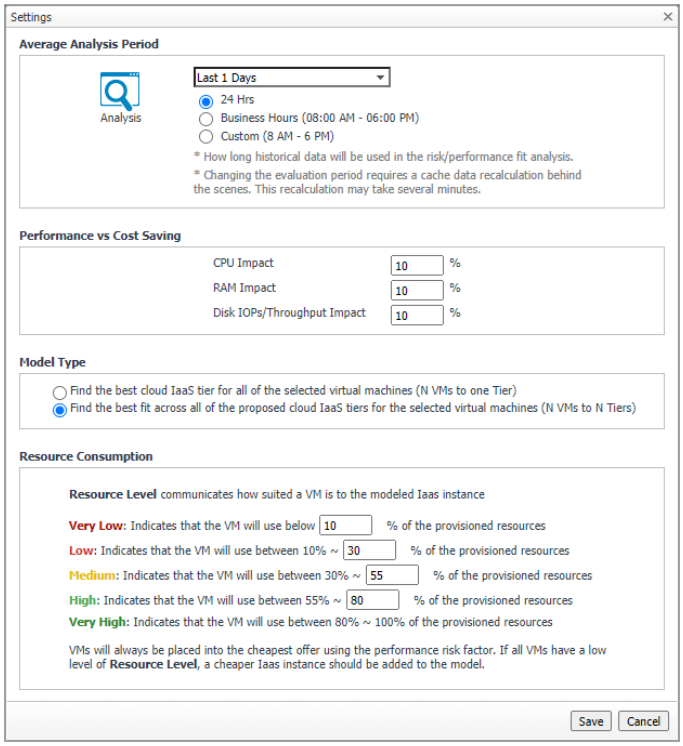
Click the domain switcher to switch between VMware environment and Hyper-V environment.

NOTE: For Hyper-V environment, only Cloud Model features are supported.

Settings

Click the Settings button. A Settings dialog box opens.

Figure 4. Settings



- **Average Analysis Period**

  Specify the *Average Analysis Period* and select the analysis time range for Cloud Model. The *Average Analysis Period* includes the following options: Last 1 Day, Last 3 Days, Last 7 Days, Last 30 Days, Last 90 Days, and Last 180 Days. The analysis time range includes the following options: 24 Hrs, Business Hours (08:00 AM - 06:00 PM), and Custom (8 AM - 6 PM).

- **Performance vs Cost Saving**

  Specify the CPU Impact, RAM Impact, and Disk IOPs/Throughput Impact. The default values are 10%.

  NOTE: If the virtual machines that have been selected for migration must always perform at their peak, enter 0% against each of CPU, Memory, Disk and Network. If Cost is the most important factor and performance is not a concern, enter 100 against CPU, Memory, Disk and Network; that way, no matter how often the virtual machine will exceed the destinations available resources it will always be included in the cloud model recommendation and costs calculation.

- **Model Type**

  Select either of the following option:

  - Find the best cloud IaaS tier for all of the selected virtual machines (N VMs to one Tier): Move all VMs to the same tier.
  - Find the best fit across all of the proposed cloud IaaS tiers for the selected virtual machines (N VMs to N Tiers): Moves all VMs to different tiers.

- **Resource Consumption**

  Resource Level communicates how suited a VM is to the modeled IaaS instance. The values can be modified.

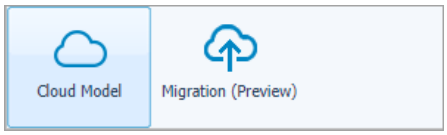
  - Very Low: Indicates that the VM will use below *10*% of the provisioned resources.
  - Low: Indicates that the VM will use between *10*% - *30*% of the provisioned resources.
  - Medium: Indicates that the VM will use between *30*% - *55*% of the provisioned resources.
  - High: Indicates that the VM will use between *55*% - *80*% of the provisioned resources.
  - Very High: Indicates that the VM will use between *80*% - *100*% of the provisioned resources.

  VMs will always be placed into the cheapest offer using the performance risk factor. If all VMs have a low level of Resource Level, a cheaper IaaS instance should be added to the model.

Menu bar

The Menu bar contains the following two tabs: Cloud Model and Cloud Migration (Technical Preview).

Figure 5. Menu bar



Migration status bar

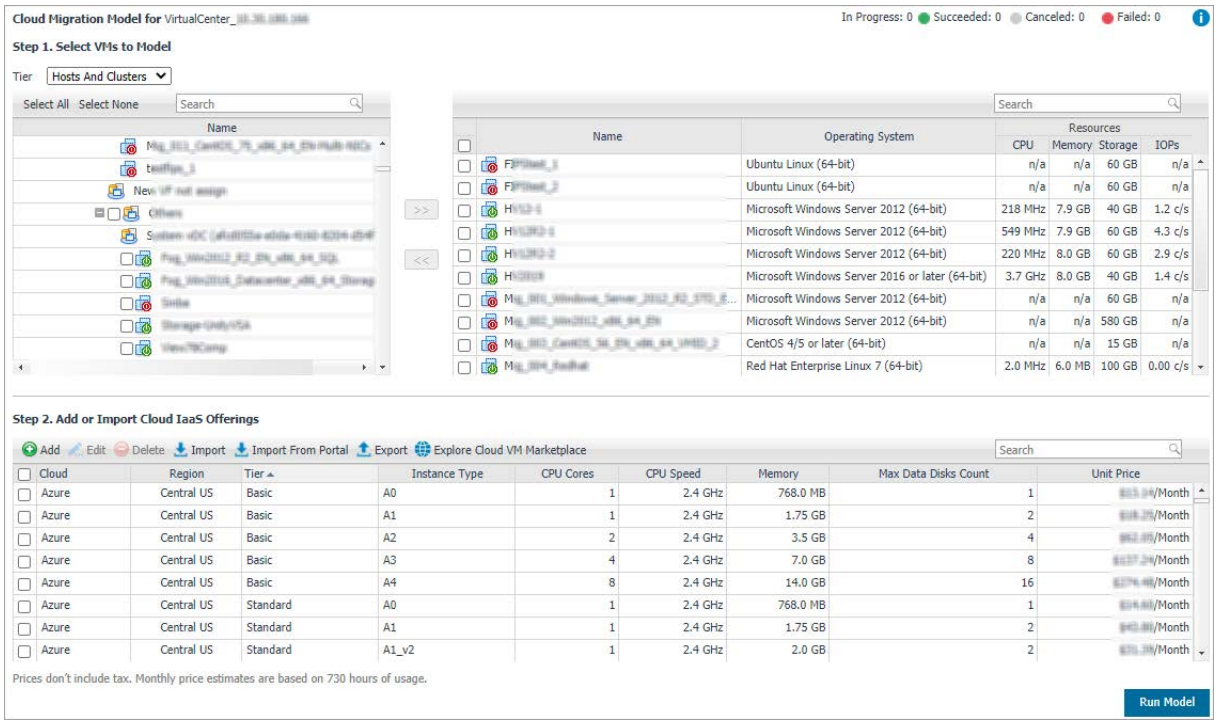
Displays the migration status, including In Progress, Succeeded, Canceled, and Failed.

Figure 6. Migration status bar

Quick view

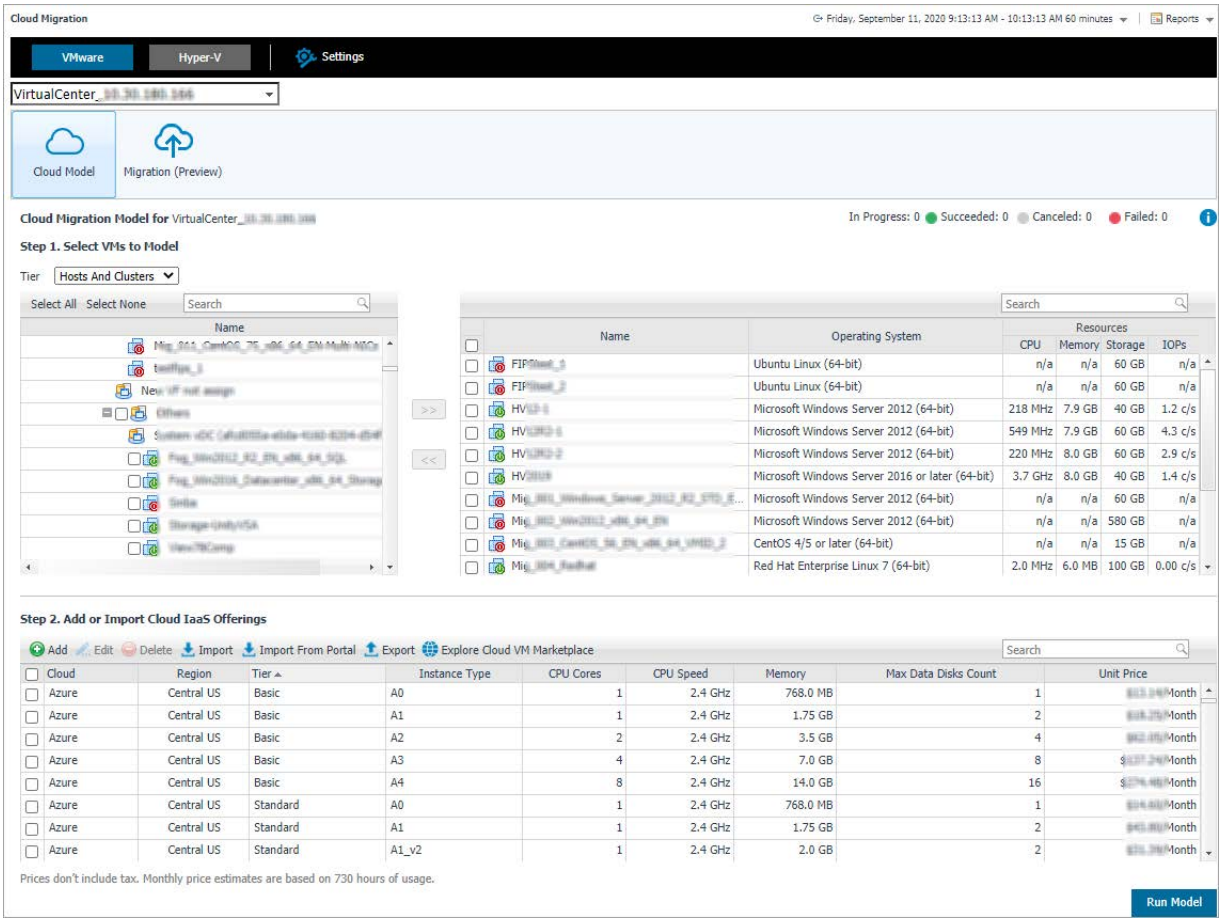
The quick view is located on the lower part of the Cloud Migration dashboard, which is updated based on the tab selected on the Menu bar.

Figure 7. Quick view for Cloud Model tab



2

Cloud Model



The *Cloud Model* view helps you understand costs and impacts caused by migrating virtual machine workloads to any MSP, Cloud, or IaaS offering. Simply enter the proposed destinations that are under review, like Azure A2 Small, select the virtual machines that have been designated for a cloud migration and input the level of acceptable performance impact for CPU, Memory, Disk IO, and Network. Select the cloud IaaS offering, select the virtual machines to be modeled, and then click **Run Model**. The *Cloud Model* view includes the following elements:

- *Select VMs to Model*: Supports to select Tiers between *Hosts and Clusters* and VMs and Templates, lists available virtual machines in the selected virtual center or datacenter, and provides the capability to search or filter VMs as needed.
- *Cloud Instances pane*: Allow to add or edit the hardware specification and unit cost of your proposed IaaS subscriptions, such as Azure, AWS EC2, Google cloud. IaaS subscriptions are supported to import or export as a .CSV file.

  NOTE: Currently, Cloud Migration only supports the following regions for Google Cloud: Council Bluffs, Iowa, USA (us-central1), Moncks Corner, South Carolina, USA (us-east1), Ashburn, Northern Virginia, USA (us-east4), Dalles, Oregon, USA (us-west1), Los Angeles, California, USA (us-west2), Salt Lake City, Utah, USA (us-west3), Las Vegas, Nevada, and USA (us-west4).

- *Recommendation pane*: Lists migration recommendations and resources consumption analysis. In addition, this pane shows migration impacts caused by restricted hardware resources, including C*PU Demand, Memory Consumed, Disk IOPs, Disk Size, Disk Throughput,* and *Cost Estimation* information.
- *Run Model button*: Click this button to start the recommendation consumption analysis based on historical performance metrics for the specified values (including selected virtual machines, performance impacts, selected Cloud Instances, and the modeling scenario).

  NOTE: The management server must have an Internet connection enabled to run the Cloud Model, because *Network Traffic Cost* and *Cloud Disk Cost* data need to be collected.

To access the *Cloud Model* view:

1. On the navigation panel, under **Dashboards**, click **Cloud Migration**.

   The *Cloud Migration* dashboard opens.
2. Use the Group selector located at the top of the dashboard to select the virtual environment that you want to monitor.
3. On the Menu bar, click the **Cloud Model** tab.

   The *Cloud Model* view appears at the bottom of the *Cloud Migration* dashboard.

Cloud Instances pane

The Cloud Instance table locates in the middle of the *Cloud Model* view offers the following menus:

- The Add button: Provides the functionality to add a new Cloud instance. For more information, see Adding a Cloud instance on page 12.
- The Edit button: Provides the functionality to edit existing Cloud instances. For more information, see Editing existing Cloud instance on page 12.
- The Delete button: Provides the functionality to delete existing Cloud instances. For more information, see Delete existing Cloud instance(s) on page 13.
- The Import button: Provides the functionality that helps you easily import Cloud instances in batches, as needed. For more information, see Importing Cloud instances on page 13.
- The Import From Portal button: Provides the functionality that helps you easily import Cloud instances from the portal, as needed. For more information, see Importing Cloud Models from Portal on page 13.
- The Export button: Provides the functionality that helps you easily import Cloud instances in batches, as needed. For more information, see Exporting Cloud instances on page 13.
- The Run Model button: Provides the functionality that starts the analysis. For more information, see Running Cloud Model on page 13.
- Cloud instance table: Lists all cloud instances that are available in the selected virtual center or datacenter.

Description	Lists the detailed information about all Cloud instances that are available in the selected vCenter or datacenter.
Data displayed	• **Cloud**. The provider name of the Cloud instance. • **Region**. The region of the Cloud instance. • **Tier**. The name of tier. • **Instance Type**. The type of Cloud instance. • **CPU Cores**. The number of CPU cores. • **CPU Speed**. The CPU speed. • **Memory**. The memory size. • **Max Data Disks Count**. The number of the data disks. • **Unit Price**. The unit price per month.

Adding a Cloud instance

To add a new Cloud instance:

1 In the Cloud Instance pane, click **Add**.

The **Add Cloud Model** dialog box opens.

2 In the **Add Cloud Model** dialog box, specify the following values, as needed.

- Cloud: Select the provider name of the Cloud instance.
- Region: Select the region of the Cloud instance
- Tier: Select the name of the Cloud tier.
- Instance Type: Type the type of the Cloud instance.
- CPU Cores: Type the number of CPU cores available in the Cloud instance.
- CPU Speed: Type the CPU speed. The unit is one of the following: GHz (default option), MHz, and THz.
- Memory: Type the physical memory. The unit is one of the following: GB (default option), MB, and TB.
- Max Data Disks Count: Type the number of the data disks.
- Unit Price per Month($): Type the unit price per month.

3 Click **Save**.

The *Cloud Instance* table refreshes automatically and the new Cloud instance is added into this table.

Editing existing Cloud instance

To edit an existing Cloud instance:

1 In the Cloud Instance pane, select a Cloud instance that you want to edit, and then click **Edit**.

The **Edit Cloud Model** dialog box opens.

2 In the **Edit Cloud Model** dialog box, modify the following values, as needed.

- Cloud: Select the provider name of the Cloud instance.
- Region: Select the region of the Cloud instance
- Tier: Select the name of the Cloud tier.
- Instance Type: Type the type of the Cloud instance.
- CPU Cores: Type the number of CPU cores available in the Cloud instance.
- CPU Speed: Type the CPU speed. The unit is one of the following: GHz (default option), MHz, and THz.
- Memory: Type the physical memory. The unit is one of the following: GB (default option), MB, and TB.
- Max Data Disks Count: Type the number of the data disks.
- Unit Price per Month($): Type the unit price per month.

3 Click **Save**.

The *Cloud Instance* table refreshes automatically and the Cloud instance is updated.

Delete existing Cloud instance(s)

To delete existing Cloud instance(s):

1 In the Cloud Instance pane, select one or more Cloud instances that you want to delete, and then click **Delete**.

The **Confirm Delete Cloud Models Dialog** box opens.

2 In the Confirm Delete Cloud Models dialog box, click **Delete**.

The *Cloud Instance* table refreshes automatically and the selected Cloud instances are removed.

Importing Cloud instances

To import Cloud instances:

1 In the Cloud Instance pane, click **Import**.

The **Import Host Models** dialog box opens.

2 In the Import Host Models dialog box, click **Choose File**.

3 In the prompted dialog box, browse to select a .csv file, and then click **Open**.

4 Click **Import**.

The *Cloud Instance* table refreshes automatically and imported Cloud instances are added into this table.

Importing Cloud Models from Portal

To import Cloud models from the portal:

1 In the Cloud Instance pane, click **Import From Portal**.

The **Import Cloud Models From Portal** dialog box opens.

2 In the Import Cloud Models From Portal dialog box, select a cloud provider and a region, the instances table refreshes automatically.

3 In the instances table, select the cloud models as needed, and then click **Save**.

The *Cloud Instance* table refreshes automatically and imported Cloud instances are added into this table.

Exporting Cloud instances

To export Cloud instances:

1 In the Cloud Instance pane, click **Export**.

The existing Cloud instances are downloaded as a .csv file automatically.

Running Cloud Model

To run Cloud model:

1 In the Cloud Model view, **Select VMs to Model**.

Select the VMs that you want to migrate to the Cloud instance, and then click >>.

2 **Add or Import Cloud IaaS Offerings**.

3 Set the following fields in **Setting**. See Settings on page 7 for more information.

   a Select time range for analysis in the **Average Analysis Period** area.

   b Specify the values in the **Performance vs Cost Saving** area.

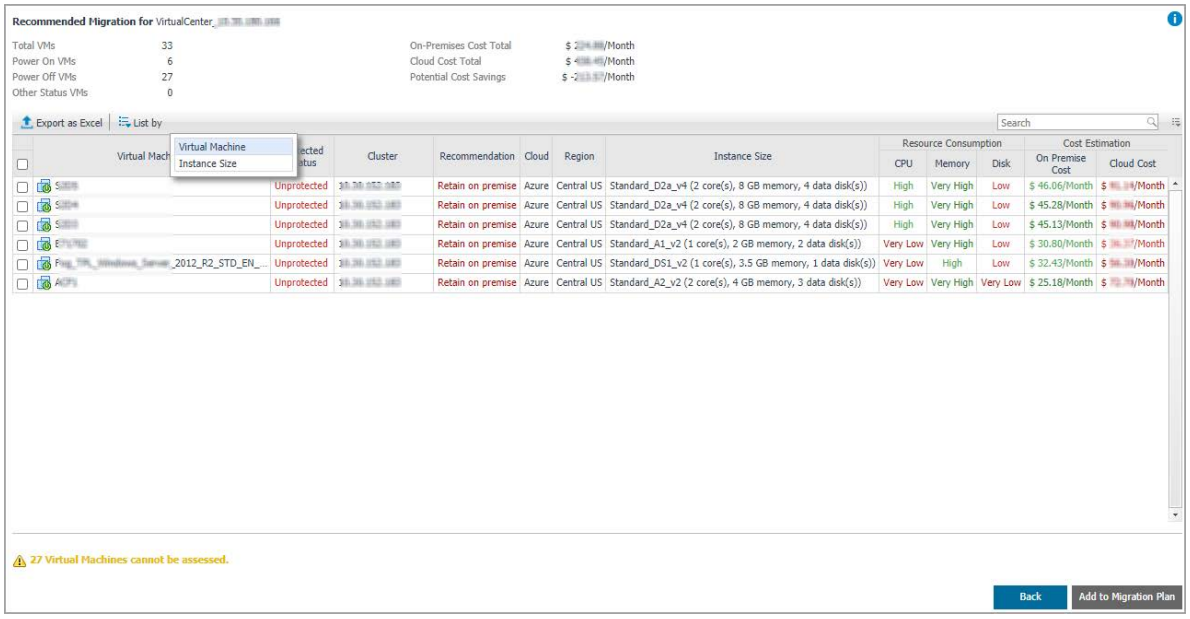
   c Select **Model Type**.

   d Set **Resource Consumption**.

4 Click **Run Model**.

   The Foglight for Cloud Migration runs the analysis and shows recommended values in the Cloud Migration *Recommendation* pane. For more information, see Recommendation pane.

Recommendation pane



The Recommendation pane locates on the bottom of the *Cloud Model* view. The default view is listed by Virtual Machine, which includes two sections:

- A summary for the assessed virtual machines.

  Lists the total number of virtual machines assessed, the number of Power-on, Power-off, and other status virtual machines, and some cost information.

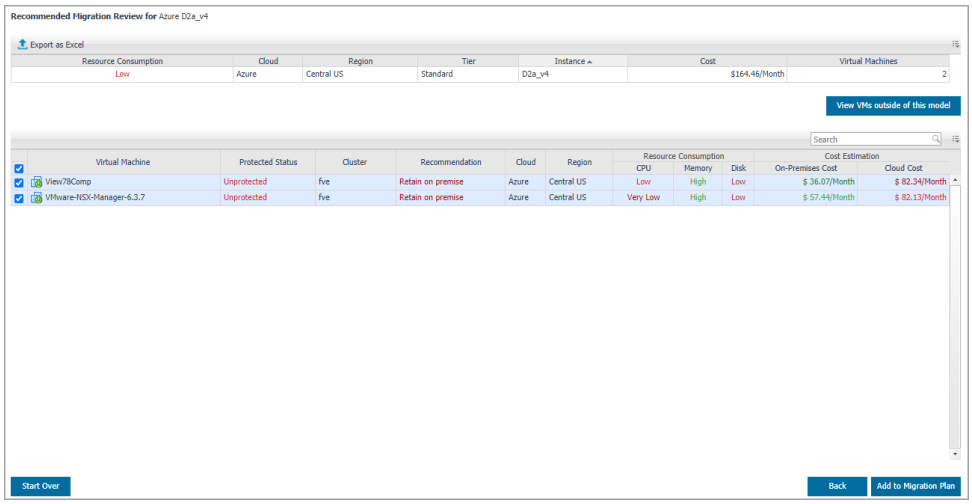
- A Recommended Migration table.

  Indicates how suited a VM is to the modeled IaaS instance. For the values descriptions, see Resource Consumption on page 8.

  - **Export as Excel**: Click the button to export the model review result into an Excel file.
  - **List by** function: Click **List by** to sort the model review result by *Virtual Machine* or *Instance Size*.
    - *List by Virtual Machine* view is the default view. Shows the detailed information for the modeling VMs, including *Protected Status*, *Cluster*, *Recommendation*, *Cloud*, *Region*, *Instance Size*, *Resource Consumption*, and *Cost Estimation*.

Select the VMs and click **Add to Migration Plan**. Click **Back** will return to the *Cloud Model* view.

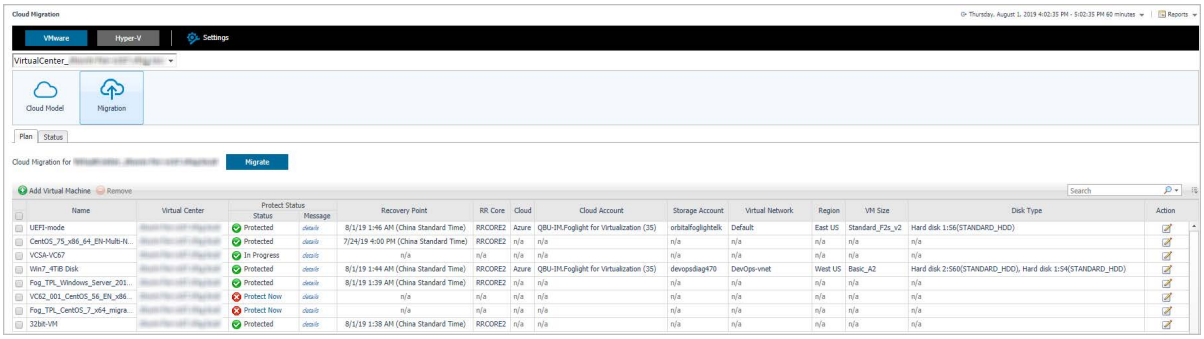
- *List by Instance Size* view sorts the modeling VMs by different instance size. Clicking *Review Model* in *Explore Outcome* column, a *Recommended Migration Review for* the selected instance size view will be displayed.



  - Clicking **View VMs outside of this model**, a new page opens and shows the VMs that are not suitable for the proposed cloud options.
  - Clicking **Start Over** will return to the *Cloud Model* view.
  - Clicking **Back** will return to the *List by Instance Size* view.
  - Select the VMs and click **Add to Migration Plan**.

3

Cloud Migration



NOTE: The Migration feature is a technical preview release.

The *Migration* view lists the virtual machines planned for migration and the migration statuses of the virtual machines.

NOTE: To migrate the virtual machines to the cloud, ensure the following two prerequisites:
1. Have monitored a Rapid Recovery 6.3 Server in this FMS.
2. Have configured an Azure Cloud Account in Rapid Recovery core server you monitored.

The *Migration* view includes the following elements:

- Plan tab: Shows a list of virtual machines that planned to migrate.
- Status tab: Shows a detail status of all the migration tasks.

To access the *Migration* view:

1. On the navigation panel, under **Dashboards**, click **Cloud Migration**.

   The *Cloud Migration* dashboard opens.
2. Use the Group selector located at the top of the dashboard to select the virtual environment that you want to monitor.
3. On the Menu bar, click the **Migration** tab.

   The *Migration* view appears at the bottom of the *Cloud Migration* dashboard.

Foglight for Cloud Migration supports migrate VMware virtual machines to Azure. With the help of Rapid Recovery, Foglight for Cloud Migration finds the best cloud tiers for virtual machines, and calls Rapid Recovery to migrate virtual machines to cloud.

NOTE: Offline migration is not supported. The management server must have an Internet connection enabled to migrate VMs.

Setup Rapid Recovery Server

Before migrating VMs to Azure cloud, set up a Rapid Recovery server.

Installing a Rapid Recovery server

For more information, see *About installing the Rapid Recovery Core* in *Rapid Recovery 6.3 Installation and Upgrade Guide.*

Setup a repository

Before protecting any machines, you must create a repository in a storage location designated for your Rapid Recovery Core. For information about repositories, see *Understanding repositories* in *Rapid Recovery 6.3 User Guide*.

Protecting virtual machines

To protect one or more agentless ESXi virtual machines (VMs), do the following:

NOTE: Quest recommends that VMware Tools be installed on virtual machines (VMs) you want to protect on vSphere or ESXi hosts. When VMware Tools are installed on a VM using a Windows operating system (OS), the backups that the Rapid Recovery Core captures use Microsoft Volume Shadow Services (VSS). For information on the behavior of agentless VMs with or without VMware Tools, see *Benefits of installing hypervisor tools for agentless protection* in *Rapid Recovery 6.3 User Guide*.

1. From the Rapid Recovery Core Console button bar, click the **Protect** drop-down menu, and then select

   Protect Multiple Machines.

   The *Protect Multiple Machines Wizard* opens.

2. On the Welcome page, select either of the follow installation options:

   - If you do not have multiple repositories defined for this Core, or you do not need to establish encryption, select **Typical**.
   - If you have multiple repositories defined, or you want to establish encryption, select **Advanced (show optional steps)**.

     Optionally, if you do not want to see the Welcome page for the Protect Machine Wizard in the future, select the option **Skip this Welcome page the next time the wizard opens**.

3. Click **Next.**
4. On the *Connection* page of the wizard, from the **Source** drop-down list, select **vCenter/ESXi**.
5. Enter the host information and logon credentials as described in the following table.

   Table 1. vCenter/ESXi connection settings

Text Box	Description
Host	The name or IP address of the virtual host.
Port	The port used to connect to the virtual host. The default setting is 443.

Table 1. vCenter/ESXi connection settings

Text Box	Description
User name	The user name used to connect to this machine.For example, Administrator (or, if the machine is in a domain, [domain name]\Administrator). Enter the user name or, to use a set of credentials saved to Credentials Vault, use the drop-down list and select a user name. Optionally, to save your credentials to Credentials Vault, click the plus sign next to the text box. For more information, see *Credentials Vault* in *Rapid Recovery 6.3 User Guide*.
Password	The secure password used to connect to this virtual host.

6 Ensure that **Use Rapid Snap for Virtual host-based protection** is selected. (This option is selected by default).

7 Click **Next**.

8 On the *Select Machines* page, select the VMs you want to protect. You can use the drop-down menu to display a tree of **Hosts and Clusters** or of **VMs and Templates** exactly as they appear in your vCenter/ESXi environment.

CAUTION: Quest recommends that you limit agentless protection to no more than 200 VMs at once. For example, do not select more than 200 VMs when using the Protect Multiple Machines Wizard. Protecting more than 200 VMs results in slow performance. There is no limit to how many VMs a Core can agentlessly protect over time. For example, you could protect 200 VMs today and another 200 VMs tomorrow.

NOTE: VMware Changed Block Tracking (CBT) must be enabled on each of the VMs you want to protect. If it is not enabled, Rapid Recovery automatically enables CBT to ensure protection.

9 If you want to automatically protect new VMs when they are added to the host, select **Auto protect new machines**, and then complete the following steps.

a Click **Next**.

b On the *Auto Protection* page, select any containers in which you expect to add new machines.

NOTE: You may need to switch between views of **Hosts and Clusters** and **VMs and Templates**.

c Click **Next.**

d On the Protection Rules page, select any of the following options:

Table 2. ESXi and vCenter agentless protection options

Option	Description
Protect machine if it is orphaned by this Core	Allows the Core protect a machine that was previously protected but was then removed from protection because the hypervisor became unreachable. This option is selected by default.
Protect machine if it already has recovery points	Shows existing recovery points alongside the new recovery points after protection. This option is selected by default.
Protect machine agentlessly if it is already protected with the Rapid Recovery Agent	If a Core detects that a machine is already protected by the Rapid Recovery Agent, this option permits duplicate protection (both agentlessly and with the Agent). The protected VM must be powered on and VMware Tools must be installed. This option is selected by default.
Protect machine if it is paired with a different Core	Protects the VM with this Core and discontinues protection from the other Core.

Table 2. ESXi and vCenter agentless protection options

Option	Description
Delete old VMware snapshots in order to enable Changed Block Tracking	Allows the Core delete previous VMware snapshots, including snapshots created by a user or another program, if required to enable Changed Block Tracking (CBT).
Save rules	Saves the selected rules to use for future VM agentless protection on this hypervisor host. These rules apply to machines protected automatically or by using the Protect Multiple Machines wizard.

10 Click **Next**.

11 On the *Protection* page, select the appropriate protection schedule settings as described below:

- To use the default protection schedule, in the **Schedule Settings** option, select Default protection (hourly snapshots of all volumes).

  With a default protection schedule, the Core takes snapshots of all volumes on the protected machine once every hour. To change the protection settings at any time after you close the wizard, including choosing which volumes to protect, go to the Summary page for the specific protected machine.

- To define a different protection schedule, in the **Schedule Settings** option, select **Custom protection**.

  Schedule options are added to the wizard workflow.

12 Proceed with your configuration as follows:

- If you specified default protection, then click **Next** and continue to Step 14 to the ABM Settings page.
- If you specified custom protection, then click **Next** and continue to the next step to configure a protection schedule.

13 On the *Protection Schedule* page, define a custom protection schedule and then click **Next**. For details on defining a custom protection schedule, see *Creating custom protection schedules in Simple Mode* in *Rapid Recovery 6.3 User Guide.*

14 Optionally, on the ABM Settings page, select **Enable Active Block Mapping**, and then complete the following information:

Table 3. Active Block Mapping settings

Option	Description
Enable Active Block Mapping	Allows you to enable or disable the ABM feature.
Enable swap file blocks exclusion	Excludes the content of system files, such as pagefile.sys, hyberfill.sys, and swapfile.sys, from the backup.
Exclude subdirectories	Allows you to exclude specific files by specifying '<file name>' or '<folder>\<subfolder>\<file name>'. Only the files will be excluded. The folders or subfolders that contained excluded files are included in the mount point, with no contents. **NOTE:** This option may affect the performance of the “determining data” phase of transfers.
+ Add	If you opted to exclude subdirectories, click **Add** and enter the location in the Path table for each item you want to exclude.

For more information, see *Understanding Active Block Mapping* in *Rapid Recovery 6.3 User Guide*.

NOTE: Active Block Mapping only supports NTFS file systems.

15 Click **Next**.

16 Proceed with your configuration as follows:

- If you selected a *Typical* configuration for the Protect Machine Wizard in Step 2 and specified default protection, then click **Finish** to confirm your choices, close the wizard, and protect the machine you specified.
- If you selected *Advanced* configuration for the Protect Machine Wizard in Step 2, and default protection, then click **Next** to see repository and encryption options.

17 On the *Repository* page, select the repository you want to use to store recovery points for this machine, and then click **Next**.

18 If you want to use encryption keys for data stored in the repository, on the *Encryption* page select **Encrypt the data at rest in a repository**, and then do either of the following:

- To select an existing encryption key to apply to all new data stored in your repository, select **Encrypt data using Core-based encryption with an existing key**, and from the **Select encryption key** drop-down menu, select the encryption key.
- To define a new encryption key at this time to apply to all future data stored in your repository, select **Encrypt data using Core-based encryption with a new key**, and then enter information about the key as described in the table below:

Table 4. Define new encryption key

Text Box	Description
Name	Enter a name for the encryption key. Encryption key names must contain between 1 and 64 alphanumeric characters. Do not use prohibited characters or prohibited phrases.
Description	Enter a descriptive comment for the encryption key. This information appears in the Description field when viewing a list of encryption keys in the Rapid Recovery. Descriptions may contain up to 254 characters. Best practice is to avoid using prohibited characters and prohibited phrases.
Passphrase	Enter a passphrase used to control access. Best practice is to avoid using prohibited characters. Record the passphrase in a secure location. Quest Data Protection Support cannot recover a passphrase. Once you create an encryption key and apply it to one or more protected machines, you cannot recover data if you lose the passphrase.
Confirm passphrase	Re-enter the passphrase. It is used to confirm the passphrase entry.

19 Click **Finish** to save and apply your settings.

NOTE: The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) transfers to the repository indicated in your Rapid Recovery Core following the schedule you defined, unless you specified that the Core should initially pause protection. For information on pausing and resuming protection, see *Pausing and resuming protection* in *Rapid Recovery 6.3 User Guide*.

For more information, see *Protecting vCenter/ESXi virtual machines using agentless protection* in *Rapid Recovery 6.3 User Guide*.

Configuring Cloud account

Before you move data between Azure and your Core, you must add cloud provider account information to the Rapid Recovery Core Console. This information identifies the cloud account in the Core Console while caching the connection information securely. This process then allows Rapid Recovery Core connect to the cloud account to perform the operations you specify.

To add a cloud account, do the following:

1 Creating an Azure storage account. For more information, see *Creating an Azure storage account* in *Rapid Recovery 6.3 User Guide*.

2 Creating an Azure Active Directory web application. For more information, see *Creating an Azure Active Directory web application* in *Rapid Recovery 6.3 User Guide.*

3 Adding a cloud account.

a On the Rapid Recovery Core Console icon bar, click the (More) icon, and then select **Cloud Accounts**.

The *Cloud Accounts* page appears.

b On the *Cloud Accounts* page, click **+ Add New Account**.

The *Add New Account* dialog box opens.

c Select **Microsoft Azure Resource Management (for Virtual Export)** from the Cloud type drop-down list.

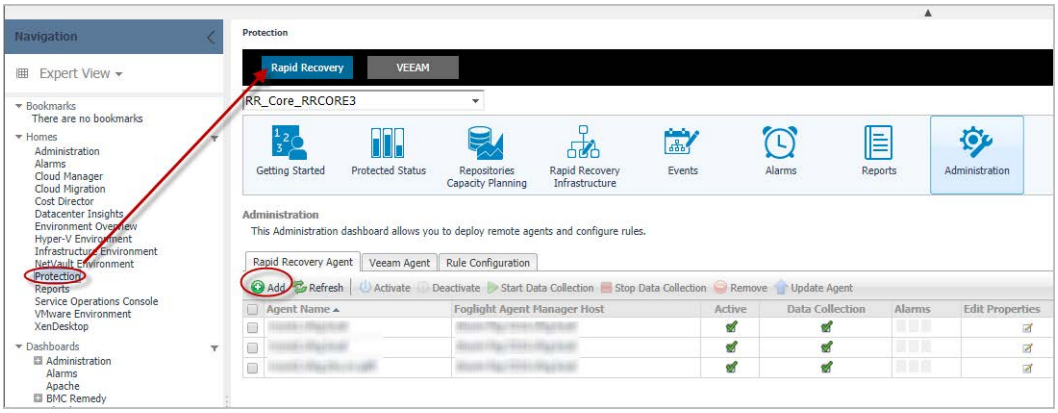
d Enter the details described in the following table.

Text Box	Description
Display name	Enter a display name for this cloud account to display on the Rapid Recovery Core Console; for example, Azure Cloud Account 1.
Region	Select the appropriate region for your Azure account. For example, select from Azure Global Cloud, Azure China Cloud, Azure German Cloud, Azure US Government Cloud, and so on.
Tenant ID	Enter the tenant ID precisely. This is an alphanumeric string (also called the Directory ID) associated with your Azure Active Directory application. To obtain this value from the Azure UI, select **Azure Active Directory > Properties > Directory ID**.
Application ID	Enter the application ID for your Azure AD application precisely. To obtain this value from the Azure UI, select **Azure Active Directory > App registrations**, select your application, and from the Settings pane, copy the **Application ID**.
Secret key	Enter the secret key for this account. You must obtain this value from the Azure when you set up the key. If you do not record it, you must create a new secret key. From the Azure UI, to see or create secret keys, select **Azure Active Directory > App registrations**, select your application, click **Settings**, and from the Settings pane, click **Keys.**
Subscription ID	Enter the subscription ID for your Azure account precisely. To obtain this value from the Azure UI, select **All services**, click **Subscriptions**, and from the appropriate subscription, copy the **Subscription ID**.

For more information, see *Adding a cloud account* in *Rapid Recovery 6.3 User Guide.*

Monitoring Rapid Recovery Server

To collect Rapid Recovery Server data in Foglight, create a Rapid Recovery agent in Foglight first. To create a Rapid Recovery agent, go to ***Homes*** > ***Protection*** > ***Rapid Recovery*** > ***Administration***.



For more information, see *Administration Tab > Creating Rapid Recovery Agent* in *Foglight Protect Dashboard Guide.*

Monitoring vCenter

To do cloud modeling, the vm performance metric, CPU, Memory, Storage, and other information are required. Create a VMware Performance agent to collect vCenter data.

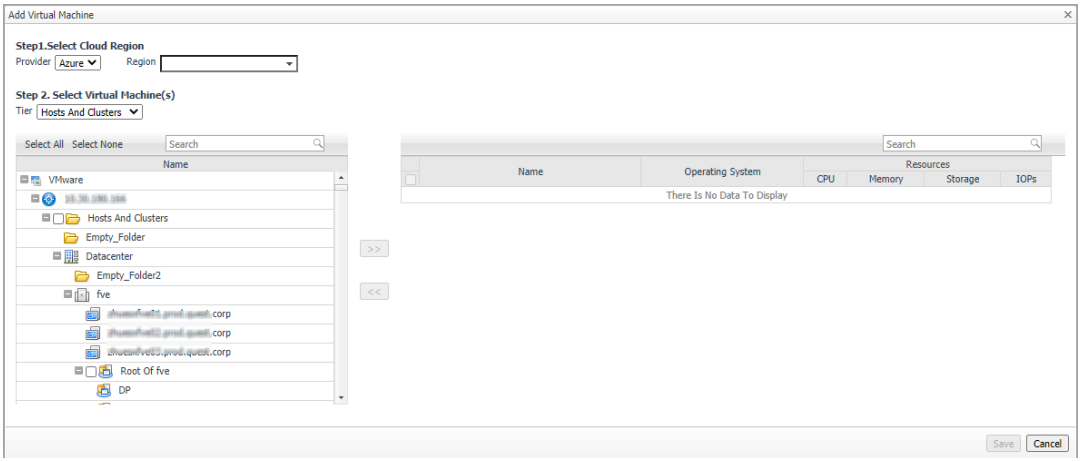
IMPORTANT:
1. Before creating your first VMware Performance agent, you must configure a Virtual Center user with sufficient privileges. For more information, see *Enabling VMware Performance Agents to Collect Data from a Virtual Center* in the *Foglight for VMware Installation Guide*.
2. If the protected vCenter in rapid recovery is using IP, ensure that the vCenter is monitored by the same IP. However, if the protected vCenter in rapid recovery is using FQDN, ensure that the vCenter is monitored by the same FQDN.

For more information, see *Using Foglight for VMware > Interacting with Foglight for VMware > Configuring monitoring agents for data collection* in *Foglight for VMware User and Reference Guide*.

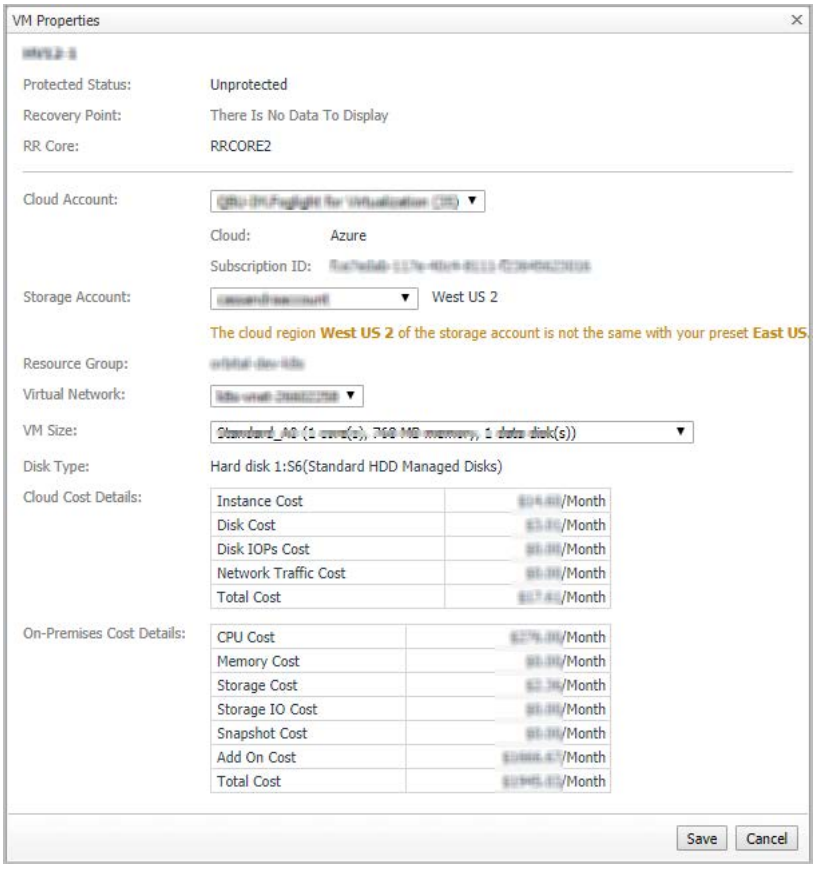
Modeling Virtual machines

To model virtual machines, do the following:

1 Click **Add Virtual Machine**, an **Add Virtual Machine** tree selector will open for users to select cloud region and virtual machines. Click **Save** and the selected virtual machine will be listed in the Plan table.



2 Click the icon will open a *VM Properties* dialog box. Configure the VM Properties in this page.



3 After selecting the Storage Account, the system will find the best VM size for this VM. Users can also select another VM Size manually.

Preparing Virtual Machines

Before migrating on-premises virtual machines to Azure cloud, prepare the virtual machines first.

Preparing Windows virtual machines

1 Set Windows configurations for Azure.

2 Check the Windows services.

3 Update remote-desktop registry settings.

4 Configure Windows Firewall rules.

5 Verify the VM.

Install Windows updates.

6 Complete the recommended configurations.

For detailed information, see *Set Windows configurations for Azure*.

Preparing Linux virtual machines

1 Prepare the various endorsed Linux distributions for Azure:

- CentOS-based Distributions. See *Prepare a CentOS-based virtual machine for Azure*.
- Debian Linux. See *Prepare a Debian VHD for Azure*.
- Oracle Linux. See *Prepare an Oracle Linux virtual machine for Azure*.
- Red Hat Enterprise Linux. See *Prepare a Red Hat-based virtual machine for Azure*.
- SLES & openSUSE. See *Prepare a SLES or openSUSE virtual machine for Azure*.
- Ubuntu. See *Prepare an Ubuntu virtual machine for Azure*.

2 General Linux Installation Notes.

Installing kernel modules without Hyper-V.

3 Linux Kernel Requirements.

4 The Azure Linux Agent.

5 General Linux System Requirements.

For detailed information, see *General Linux System Requirements*.

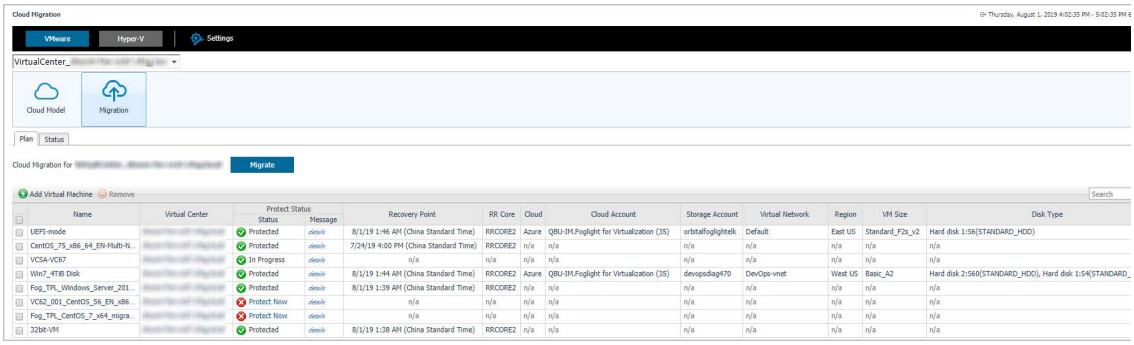
Migrating Virtual Machines

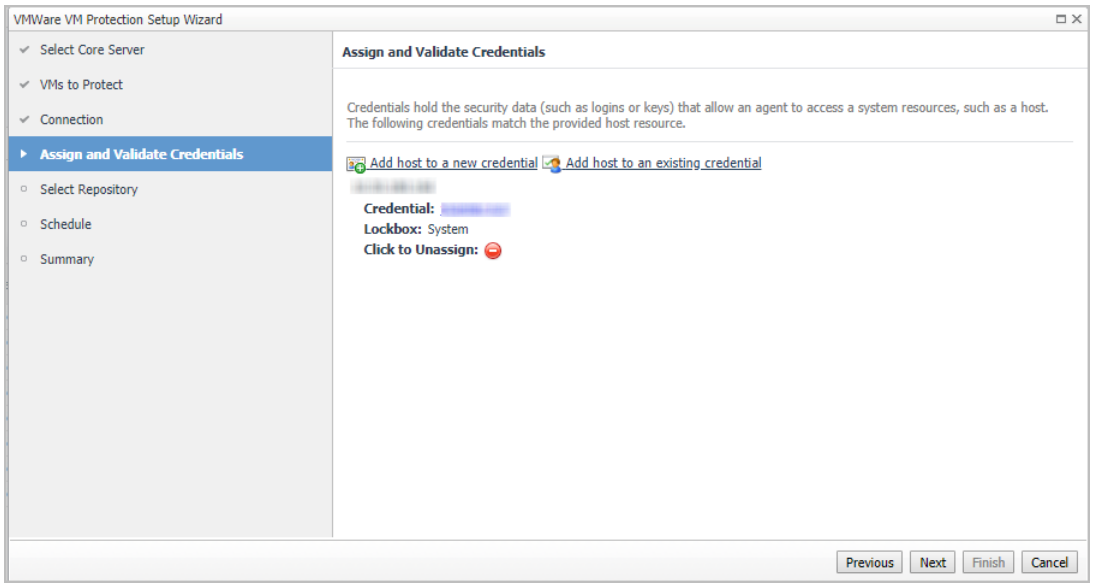
Before migrating virtual machines to Azure, you need to protect the virtual machines and ensure that the virtual machines have taken recovery points.

1 If the virtual machines are not protected, protect them on *Migration* > *Plan* tab. Protect virtual machines.

Click **Protect Now** to popup *VMWare VM Protection Setup Wizard*.

NOTE: The Credential should have administration role.

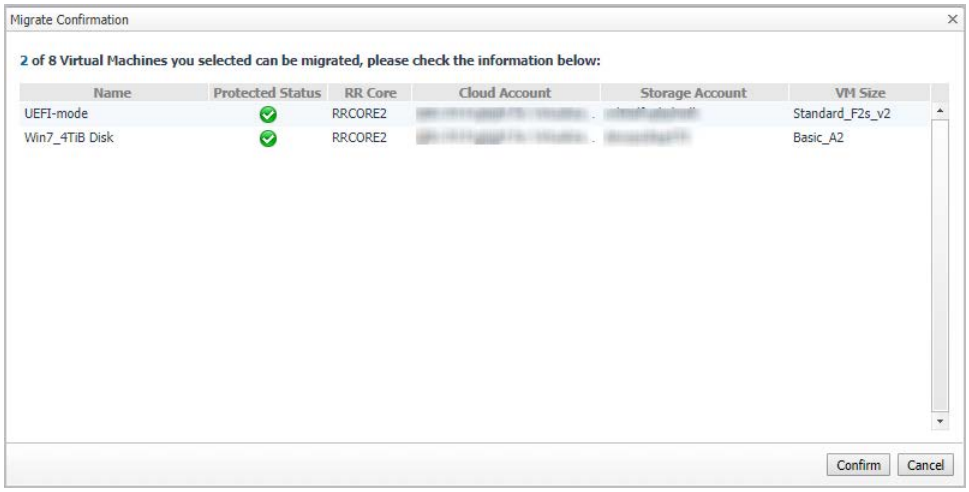




2 Take a Recovery Point. You need to Force a Recovery Point after preparing the virtual machine. See *Forcing a snapshot* in *Rapid Recovery 6.3 User Guide*.

3 Check Recovery Point. Ensure that current recovery point includes the VM preparation.

4 Migrate the virtual machines. Select the VMs and click **Migration** button. Then, click **Confirm** on the *Migration Confirmation* popup dialog box.

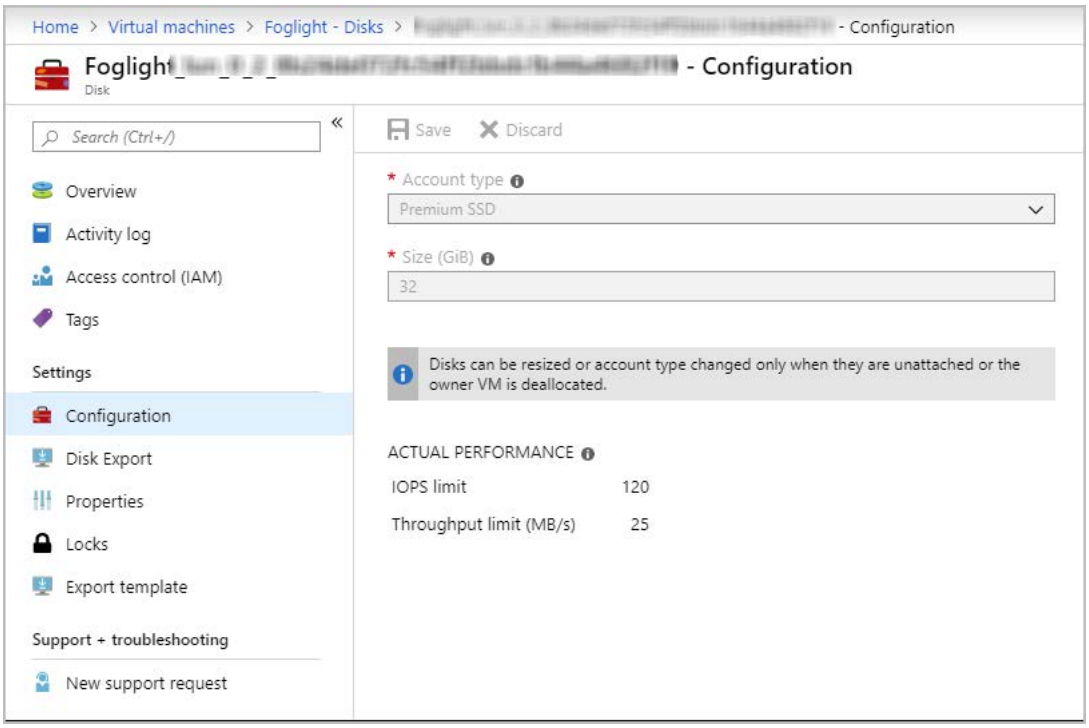


Configuring Virtual machines on Azure

1 Change disk type or size.

Currently, Rapid recovery does not allow to specify the disk type or size for migration. All disk types will be HDD after migrated to Azure.

Users will have to manually change the disk type or size according to recommendation after migrated to Azure.

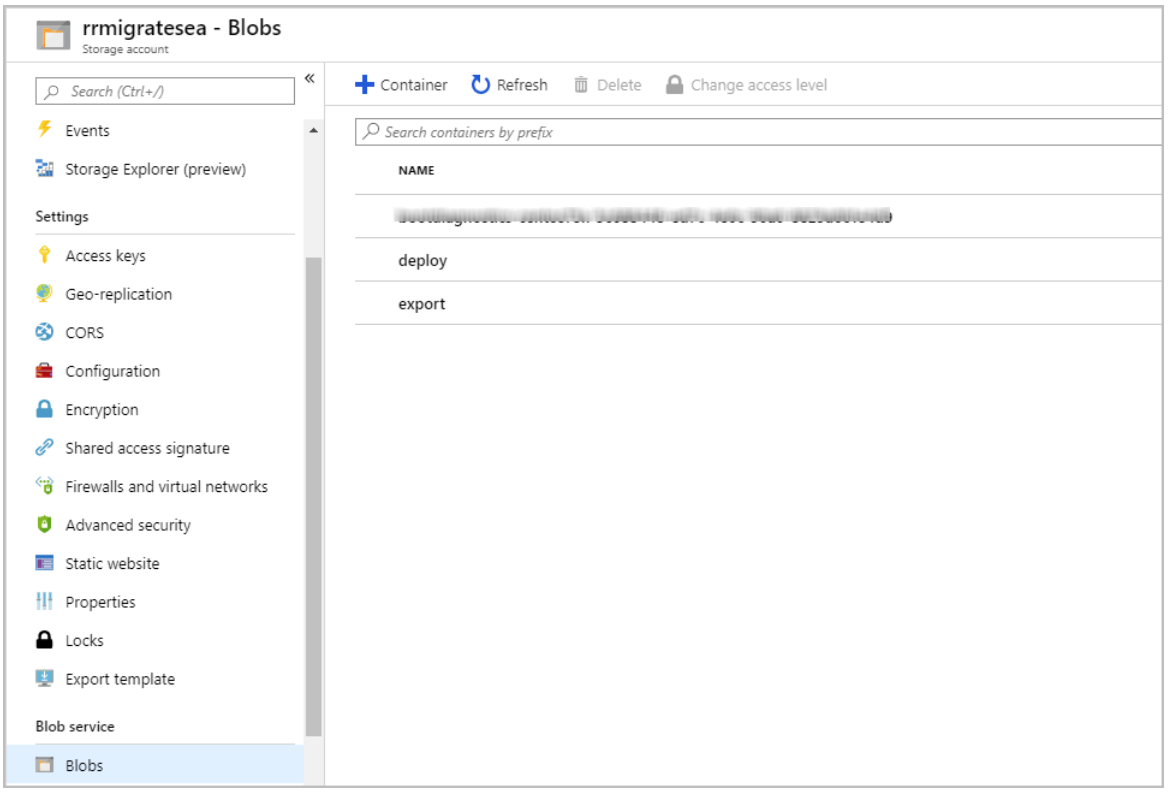


2 Add more NICs for virtual machines.

Only one NIC will be created for the migrated VM in Azure by default. If the virtual machine needs multi-NICs, manually add more NICs for them (depending on VM size).

Deleting VHD files

Azure Blobs storage is used to store the VHD files temporarily. When VM migration is completed, you can delete the VHD files on the Azure Blobs storage. The files are default saved in “export” and “deploy” containers under the storage account you used to migrate.



Limitations

Currently some VMs or disks are not supported for migration, including:

- VMs with UEFI boot
- VMs with 32-bit operating system
- VMs with 4 TiB disks or above
- VMs with RDM disks
- VMs with NFS/SMB volumes mounted as volumes
- VMs with encrypted disks/volumes

The VMs with the following features require manual operation:

- VMs will be migrated to standard HDD managed disks in Azure by default, users can change the disk type or size in Azure manually after migration.
- If the VMs have multiple NICs, only one NIC will be created for the migrated VM in Azure by default. Users can add more NICs manually after migration.

Supported Operating systems

Table 5. Microsoft Windows operating systems

OS Version	VM Export to Azure
7 SP1	Limited*
8	Limited*
8.1	Limited*
10	Yes 1
Server 2008 R2 SP1	Yes 1
Server 2012	Yes 1
Server 2012 R2	Yes 1
Server 2016	Yes 1
Server 2019**	Yes 1

Windows support notes:

* VM export to Azure works only for x64 editions of operating systems listed. EFI is not supported. Azure VMs do not support Generation 2 Hyper-V VM features.
  For more information about these features, see *Generation 2 Virtual Machine Overview* in the Microsoft Technet article

** Rapid Recovery does not support protection of ReFS volumes running on Windows Server 2019. For more information, see the topic *Support for Windows Server 2019* in *Rapid Recovery 6.3 Release Notes*.

Table 6. Linux operating systems

OS Version	VM Export to Azure
Red Hat Enterprise Linux (RHEL) 6.3 - 6.10	Yes
RHEL 7.0 - 7.6	Yes
CentOS Linux 6.3 - 6.10	Yes
CentOS Linux 7.0 - 7.6	Yes
Debian Linux 7	Limited
Debian Linux 8	Yes
Debian Linux 9	Yes
Oracle Linux 6.3 - 6.10	Yes
Oracle Linux 7.0 - 7.6	Yes
Ubuntu Linux 12.10, 13.04, 13.10	Limited**
Ubuntu Linux 14.04 LTS	Yes
Ubuntu Linux 14.10, 15.04, 15.10	Limited**
Ubuntu Linux 16.04 LTS, 16.10	Yes
Ubuntu Linux 17.04 LTS	Limited**
Ubuntu Linux 17.10	Yes
Ubuntu Linux 18.04 LTS	Yes
Ubuntu Linux 18.10	Yes
SUSE Linux Enterprise Server (SLES) 11 SP2 (or later SP)	Yes
SLES 12, 12 SP1, 12 SP2, 12 SP3	Yes*

Linux support notes:

* B-tree file system (BTRFS) is supported only on operating systems with kernel version 3.7 or later. The earliest

versions of compliant operating systems include Ubuntu 14.04, Debian 8, CentOS/Oracle Linux/RHEL 7, and SLES 12.

** This OS distribution has reached end of life, and is therefore no longer tested. Support for this OS is therefore limited.

For more information on Windows and Linux supported by Rapid Recovery, see *Rapid Recovery release 6.3 operating system installation and compatibility matrix*.

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit https://www.quest.com/.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.