Foglight™ Evolve 6.3.0

Azure Virtual Machine Deployment Guide

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 Evolve Azure Virtual Machine Deployment Guide
Updated - May 2023
Foglight Version - 6.3.0
Software Version - 6.3.0

Contents

1

Deploying and Monitoring Virtual Appliance

This guide provides instructions for deploying and monitoring the Foglight™ for Virtualization, Enterprise Edition appliance on Microsoft Azure (hereafter called Foglight-FVE-Azure-vApp).

For more information, see the following topics:

- Deploying virtual machine through Azure portal
- Accessing Management Server console
- Creating monitored agent

Deploying virtual machine through Azure portal

Before monitoring the Foglight-FVE-Azure-vApp, make sure to deploy your virtual machine on Microsoft Azure.

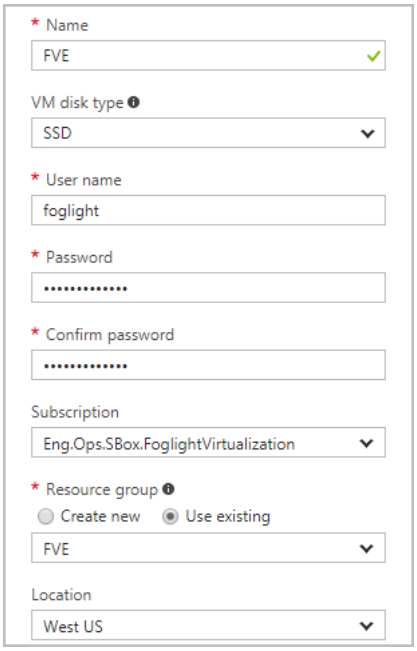
To deploy the virtual machine through the Azure portal:

1. Log into the Azure portal.
2. On the left navigation panel, select **New.**

   The *New MARKETPLACE* view opens.
3. In the *New MARKETPLACE* view, type "*foglight evolve*" in the search box, and then select *Foglight Evolve* from the search result.

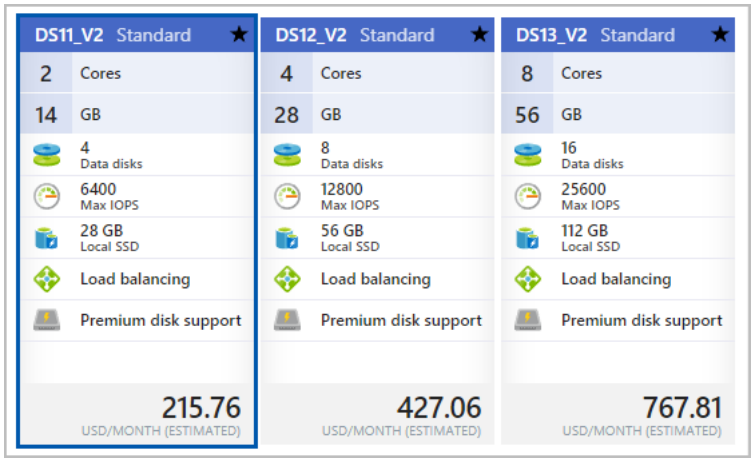
   TheFoglight Evolveview opens.
4. In the *Foglight Evolve* view, click **Create**.

   The *Create virtual machine* view opens.
5. In the *Basics* step, specify the following information, and then click **OK**.



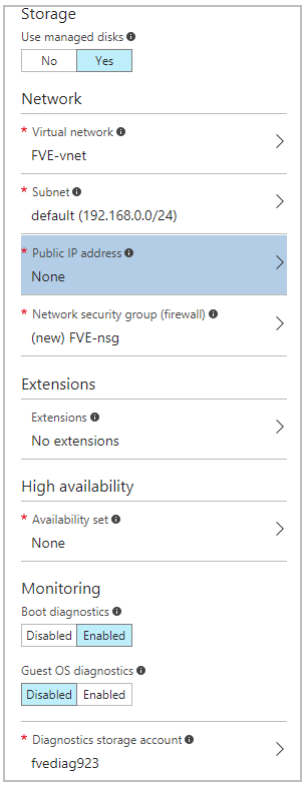
- *Name* (mandatory): Specify the name of the virtual machine.
- *VM disk type*: Indicate the disk type of the virtual machine. Quest recommends selecting *SSD* for this field.
    - SSD: Premium disks (SSD) are backed by solid state drives and offer consistent, low-latency performance. They provide the best balance between price and performance, and are ideal for I/O-intensive applications and production workloads.
    - HDD: Standard disks (HDD) are backed by magnetic drives and are preferable for applications where data is accessed infrequently.
- *Password* (mandatory): Specify the password of the virtual machine.
- *Confirm password* (mandatory): Type your password again.
- *Subscription*: Select your subscription from the drop-down list.
- *Resource group* (mandatory): A resource group is a collection of resources that share the same lifecycle, permissions, and policies. Do either of the following:
    - Select *Create new*, and then specify the name of this new resource group.
    - Select *Use existing*, and then select an existing resource group from the drop-down list.
- *Location*: Indicate in which the virtual machine is located.

6 In the *Size* step, select any of the following, and then click **Select**.



- *DS11_V2:* Select this option for an environment that includes less than 1000 VMs.
- *DS12_V2:* Select this option for an environment that includes less than 3000 VMs.
- *DS13_V2:* Select this option for an environment that includes more than 3000 VMs.

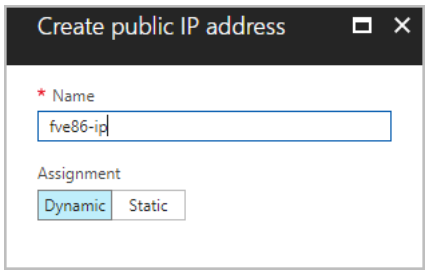
7 In the *Settings* step, specify the following information, and then click **OK**.



- *Storage:* Enable this feature to have Azure automatically manage the availability of disks to provide data redundancy and fault tolerance, without creating and managing storage accounts on your own.
- *Storage account* (available for non-managed disks only): Disks for Azure virtual machines are created in storage accounts. Create a new storage account or select an existing account.
- *Network:*
  - *Virtual network* (mandatory): Virtual networks are logically isolated from each other in Azure. You can create a new virtual network or select an existing one. Virtual machines in the same virtual network can access each other by default.

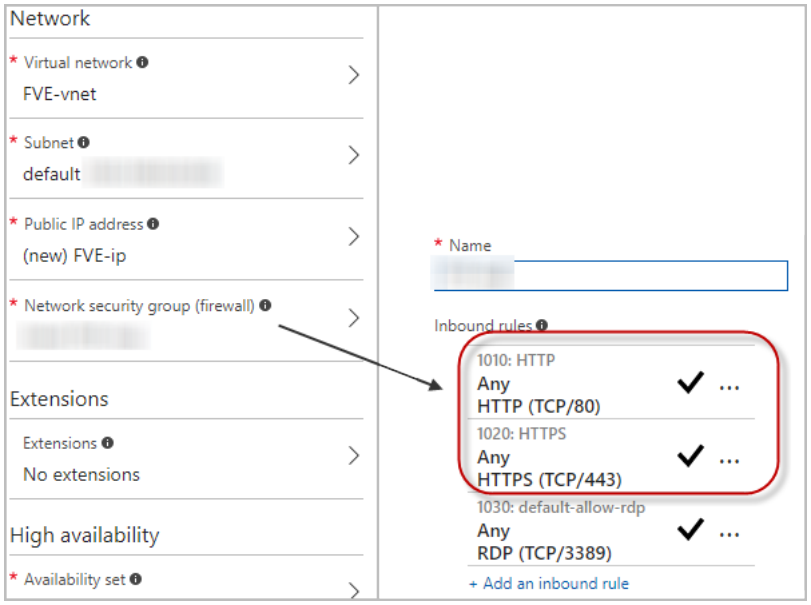
- *Subnet* (mandatory): A subnet is a range of IP addresses in your virtual network, which can be used to isolate virtual machines from each other or from the Internet.
- *Public IP address* (mandatory): Use a public IP address if you want to communicate with the virtual machine from outside the virtual network.

  To create a new public IP address, specify the name of IP address, select dynamic or static alignment, and then click **OK**.



- *Network security group (firewall)* (mandatory): A network security group is a set of firewall rules that control traffic to and from your virtual machine.

NOTE: Ensure that HTTP (TCP/80) and HTTPS(TCP/443) ports in the *Inbound rules* area are enabled.



- *Extensions*: Add new features, like configuration management or anti-virus protection, to your virtual machine using extensions.
- *Availability set* (mandatory): To provide redundancy to your application, we recommend that you group two or more virtual machines in an availability set.
- *Boot diagnostics*: Enable this feature to capture serial console output and screenshots of the virtual machine running on a host to help diagnose startup issue.
- *Guest OS diagnostics*: Enable this feature to get metrics every minute for your virtual machine. You can use them to create alerts and stay informed on your application.
- *Diagnostics storage account* (mandatory): Metrics are written to a storage account so you can analyze them with your own tools.

8 In the *Purchase* step, review the summarized information, and then click **Purchase**.

The virtual machine is now being deployed on Microsoft Azure.

Accessing Management Server console

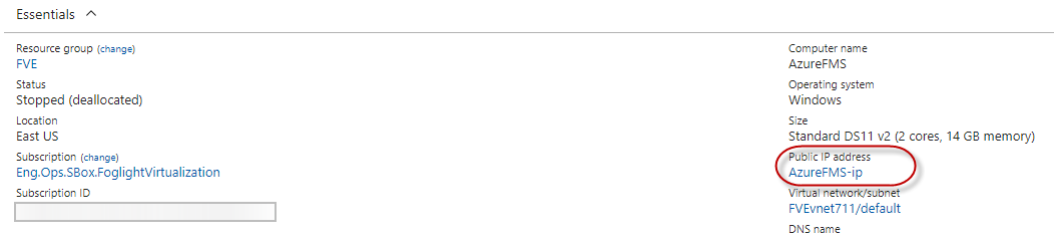
After deploying your virtual machine(s) on Microsoft Azure, enter `http://<public-IP-address>` in your Internet browser to open the management server console.

IMPORTANT: The default credentials for the Management Server console are: **Username**: *foglight*. **Password**: *foglight*.

To find the public IP address:

1. Log into the Azure portal.
2. On the left navigation panel, select **Virtual Machines**, and then browse to select your virtual machine.
3. Click your virtual machine.

   The *Overview* view of this virtual machine opens by default.
4. Check the value of *Public IP address* in the *Essentials* area.



Creating monitored agent

The monitored agent(s) can be any of the following types:

- AWS Cloud agent: For more information, see Creating an AWS agent on page 9.
- Azure Performance agent: For more information, see Creating Azure Performance Agent on page 11.
- On-Premises agent: To create and monitor On-Premises agents, make sure to set up external Foglight Agent Manager in your private network before creating an agent. For more information about how to set up Foglight Agent Manager, refer to Installing external Agent Managers.
  - VMware agent: For instructions about how to create a VMware agent, visit Configuring monitoring agents for data collection.
  - Hyper-V agent: For instructions about how to create a Hyper-V agent, visit Configuring monitoring agents.
  - Rapid Recovery agent: For instructions about how to create a Rapid Recovery agent, visit Creating Rapid Recovery Agent.

Creating an AWS agent

Each AWS Agent monitors the assets inside the selected region. To monitor an AWS environment, AWS Identity and Access (IAM) users need use Access Keys to secure REST or HTTP query protocol requests. Create an IAM user with the following privileges to use the Foglight Evolve:

- *AmazonSSMFullAccess*
- *AmazonEC2ReadOnlyAccess*
- *IAMReadOnlyAccess*
- *AWSHealthFullAccess*

To collect EC2 Memory metrics and Linux Volume metrics, make sure to assign the following privileges for an IAM user when creating the EC2 instance that is to be launched and monitored:

- *AmazonEC2RoleforSSM*
- *CloudWatchFullAccess*

A complete setup includes the following two steps:

1 Get the authentication information through AWS Management Console. For more information, see Getting authentication information through console on page 10.

2 Create an AWS Agent on the Foglight Management Server. For more information, see Creating an AWS Agent on page 11.

Getting authentication information through console

To create and retrieve a user's Access Keys through the AWS IAM console:

1 Log into the AWS IAM console at: https://console.aws.amazon.com/iam/.

2 Click **IAM** under the *Security, Identity & Compliance* column.

3 On the left navigation panel, click **Users**.

The *Resource Groups* view opens on the right.

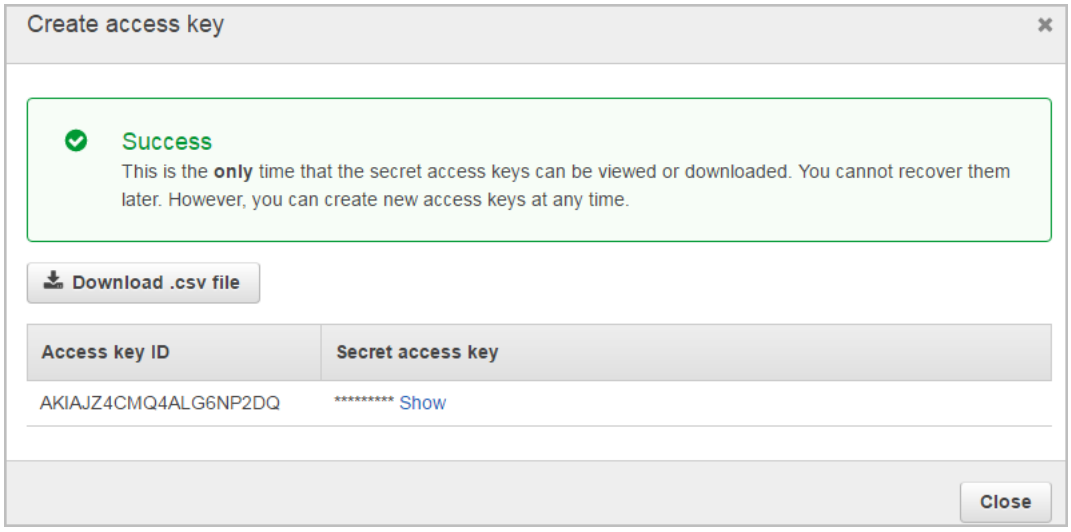
4 In the *Resource Groups* view, click the user which Access Key is to be retrieved.

The *User Summary* view opens.

5 In the *User Summary* view, click **Security credentials**, then the *Sign-in credentials* view opens.

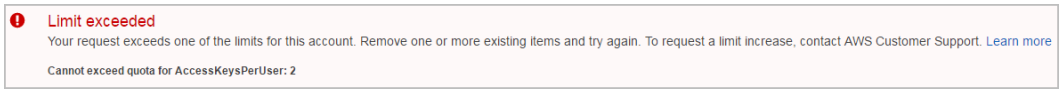
6 In the *Access keys* area, click **Create access key**.

The **Create access key** dialog box appears and shows the access key and Secret access key.



7 Click **Download .csv file** to keep the access key and secret access key somewhere safe.

8 (Optional) If you see the *Limit exceed* message, click the ✖ button next to the **Status** column to delete an access key that is not being used. Then repeat Step 6 to create and retrieve a new access key.



Creating an AWS Agent

To create an AWS agent:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

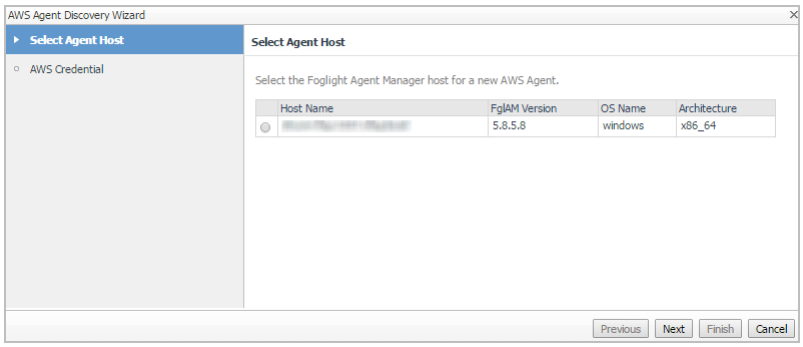
To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 In the **Cloud Manager** dashboard, click **Administration**, and then click **Add** or **Create AWS Agent**.

The **Agent Setup Wizard** dialog box opens.



5 In the *Select Agent Host* view, select the agent manager on which the new agent is to be deployed, and then click **Next**.

6 In the *AWS Credential* view, specify the following values, as needed, then click **Finish**.

- *Account Id*: The display name of this account.
- *Access Key*: The access key retrieved in Getting authentication information through console.
- *Secret Key*: The secrete access key retrieved in Getting authentication information through console.

The new AWS Agent is created, and its data is to be displayed on the **Monitoring** tab after a few minutes.

Creating Azure Performance Agent

Each Azure Performance Agent monitors the subscriptions inside the same Azure Active Directory (AD). To collect the Azure data, you need register an application in Azure AD, and this application needs be granted the following privileges for all subscriptions to be monitored by Foglight Evolve:

- *Reader*
- *Storage Account Contributor*

To fully enable the monitoring of Azure environment, Foglight Evolve requires to create an Azure Performance Agent that is to be authenticated using *Azure Active Directory ID (Tenant ID)*, *Application ID*, and *Access Key*.

A complete setup includes the following two steps:

1 Get the authentication information using Azure Command Line Interface (CLI). For more information, see Getting authentication information through CLI on page 12.

Or

Get the authentication information through the Azure portal. For more information, see Getting authentication information through Azure portal on page 12.

2 Create an Azure Performance Agent on the Foglight Management Server. For more information, see Creating Azure Performance Agent on page 14.

Getting authentication information through CLI

To get Tenant ID, Application ID, and Access Key through CLI:

NOTE: Ensure that Azure CLI has been installed in the environment. For details about how to install Azure CLI, visit Install Azure CLI 2.0.

1 Run the `azure login` command to log into the Azure account.

2 Run the `azure config mode arm` command to set CLI as the Azure Resource Manager (ARM) mode.

3 Run the `azure account show` command to get the value of *Tenant ID* that is used for Creating Azure Performance Agent. Make sure to keep this *Tenant ID* somewhere safe.

4 Run the following command to create an Active Directory (AD) application. The value of *password* is the *Access Key* to be used for Creating Azure Performance Agent. Make sure to keep this *password* somewhere safe.

```
azure ad app create --name "FoglightAzureMonitoringAuth" --home-page
"http://app.quest.com" --identifier-uris "http://app.quest.com" --password
"Passwrod"
```

After executing this command, the returned *AppId* value is the *Application ID* to be used in Step 5 and for Creating Azure Performance Agent. Make sure to keep this *AppId* somewhere safe.

5 Create a Service Principal by:

1 Running the `azure ad sp create {app-id}` command, if your Azure CLI version is lower than 0.10.2.

2 Running the `azure ad sp create -a {app-id}` command, if your Azure CLI version is 0.10.2 or later.

6 Run the following command to grant the Reader permission for the subscription to be monitored.

NOTE: The value of *objectId* is the Object Id returned after executing the command in Step 5, and the value of *subscription-Id* represents the subscription to be monitored.

```
azure role assignment create --objectId {object-Id} --roleName Reader --subscription
{subscription-Id}
```

Getting authentication information through Azure portal

To get Tenant ID, Application ID, and Access Key through the Azure portal:

1 Log into the Azure portal.

2 On the left navigation panel, select **Azure Active Directory.**

The *Azure Active Directory* view that belongs to your account opens.

3 In the A*zure Active Directory* view, select **MANAGE > Properties**, and then click to copy the *Directory ID* that is also known as *Tenant ID*.

4 In the A*zure Active Directory* view, select **MANAGE > App registrations**, and then click **New application registration**.

The *App registrations* > *Create* view opens.

5 Type the following information, as needed, and then click **Create**.

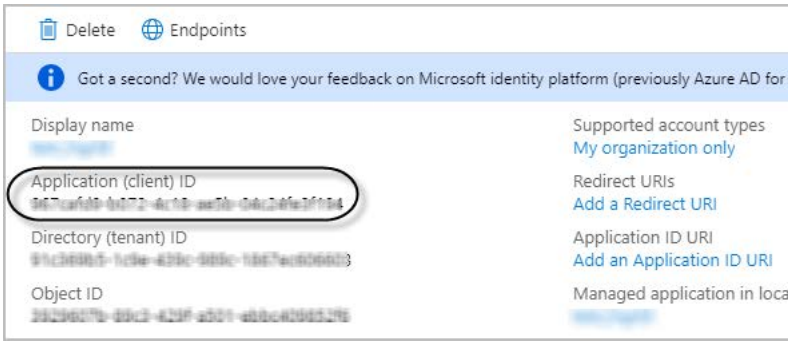
- *Name*: type the name of the application.
- *Application type*: select Web app / API.

- *Sign-on URL*: type the URL address where users can sign in and use the application.

The *App registrations* > *Create* view closes and the *App registrations* list is refreshed automatically.

6 In the *App registrations* list, select the application created in Step 7.

Keep the *Application ID* displayed in the Application details view somewhere safe.

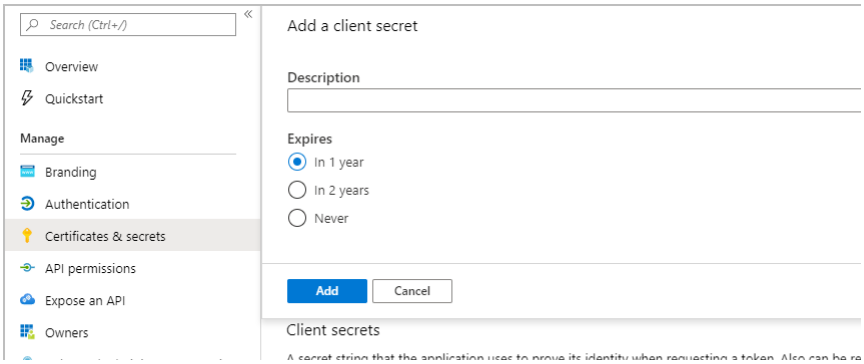


7 In the Application details view, click **All settings**. The *Settings* view opens on the right view.

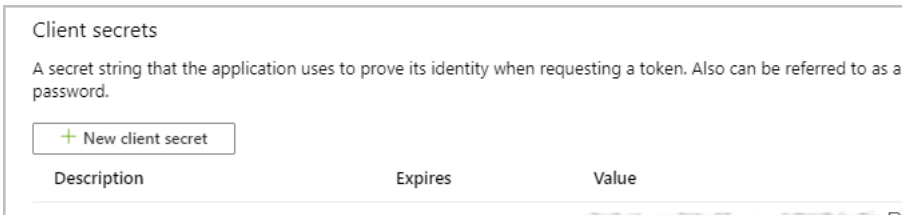
8 In the *Settings* view, click **Keys**.

The *Keys* view opens.

9 In the *Keys* view, specify the values of *DESCRIPTION* and *EXPIRES*, and then click **Save**.



10 Keep the key value as prompted.

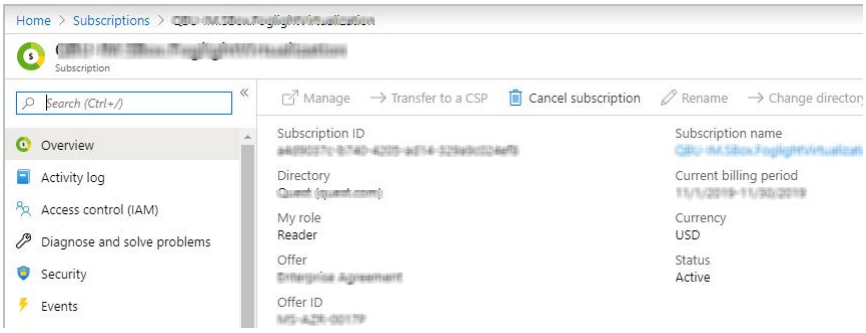


11 Click **Microsoft Azure** on the top right corner, to return the default dashboard that appears once logged into the Azure portal.

12 On the left navigation panel, click **Subscriptions**.

The *Subscriptions* view opens.

13 In the *Subscriptions* view, click the subscription that you want to monitor, then the Subscriptions details view opens.



14 In the Subscription details view, click **Access control (IAM)**, then *Access control (IAM) view* opens on the right.

15 Click **Add**. The *Add Permissions* view opens.

16 In the Add Permissions view, select *Reader* from the **Role** drop-down list, search for the application created in Step 7, and then click **Save**.

17 Repeat Step 11 to Step 16, to assign the *Storage Account Contributor* role to the application created in Step 7.

Repeat this procedure if there are multiple applications to be monitored.

> **NOTE: Diagnostics settings** must be enabled to collect metrics for both ARM-deployed virtual machines and standard Storage Account. For more information, visit How to enable metrics using the Azure portal.

Creating Azure Performance Agent

To create an Azure Performance Agent:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

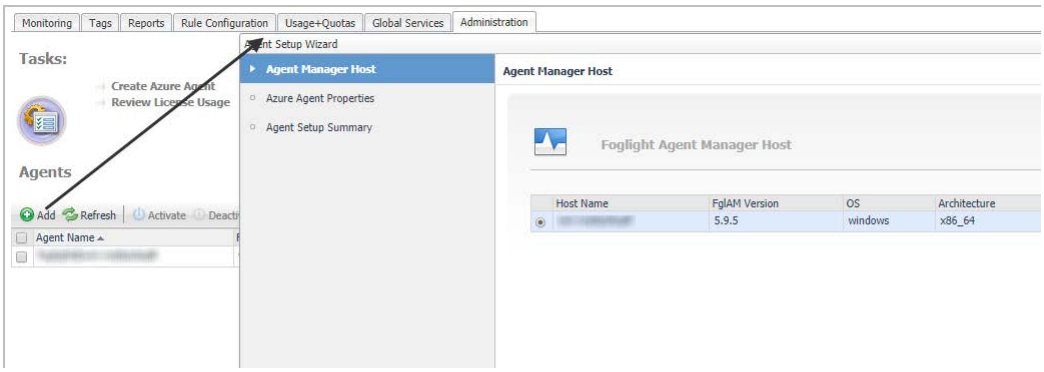
To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 In the **Cloud Manager** dashboard, click **Administration**, and then click **Add**.

The **Agent Setup Wizard** dialog box opens.



5 In the *Agent Manager Host* view, select the agent manager on which the new agent is to be deployed, and then click **Next**.

6 In the *Azure Agent Properties* view, specify the following values, as needed, then click **Next**.

- *Tenant Directory ID* *: The value of *Tenant ID* retrieved in Getting authentication information through CLI or Getting authentication information through Azure portal.
- *Tenant Alias Name*: The display name that identifies your Tenant
- *Application ID* *: The value of *Application ID* retrieved in Getting authentication information through CLI or Getting authentication information through Azure portal.
- *Access Key* *: The value of *Access Key* retrieved in Getting authentication information through CLI or Getting authentication information through Azure portal.

7 In the *Agent Setup Summary* view, confirm the agent information, and then click **Finish**.

The new Azure Performance Agent is created, and its data is to be displayed on the **Monitoring** tab after a few minutes.

About Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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.