Monitoring Microsoft Azure

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Microsoft Azure is Microsoft's cloud computing platform, providing a wide variety of services you can use without purchasing and provisioning your own hardware. Azure enables the rapid development of solutions and provides the resources to accomplish tasks that may not be feasible in an on-premises environment. Azure's compute, storage, network, and application services allow you to focus on building great solutions without the need to worry about how the physical infrastructure is assembled. Some of the Azure services in the cloud computing platform is mentioned below:

- **Compute services** This includes the Microsoft Azure Cloud Services (web and worker roles), Azure Virtual Machines, Azure Websites, and Azure Mobile Services.
- **Data services** This includes Microsoft Azure Storage (comprised of the Blob, Queue, Table, and Azure Files services), Azure SQL Database, and the Redis Cache.
- **Application services** This includes services that you can use to help build and operate your applications, such as the Azure Active Directory, Service Bus for connecting distributed systems, HDInsight for processing big data, the Azure Scheduler, and Azure Media Services.
- **Network services** This includes Azure features such as Virtual Networks, the Azure Content Delivery Network, and the Azure Traffic Manager.

An online management portal provides the easiest way to manage the resources you deploy into Azure. You can use this to create virtual networks, use cloud services, set up VMs, set up storage accounts, define websites, and so on. In order to deploy and manage the resources to the Azure portal, you would require a subscription.

Since many mission-critical applications these days are deployed on Microsoft Azure, the user experience with these applications depends upon the continuous availability and superlative performance of the Microsoft Azure cloud platform. To ensure this, eG Enterprise Suite now offers a specialized monitoring model for Microsoft Azure. This model provides in-depth insights into the health of a single subscription registered with the cloud platform, and in the process, proactively alerts administrators to potential issues that may cause performance bottlenecks, so that administrators can resolve the issues before end users start complaining.

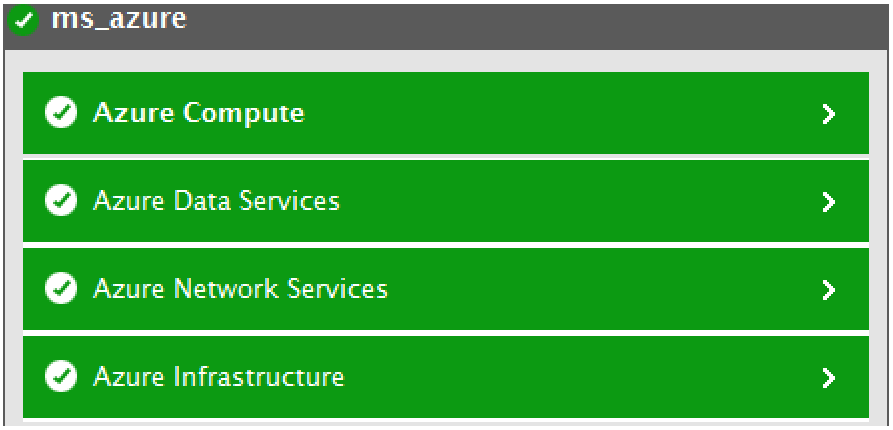


Figure 1.1: The layer model of Microsoft Azure

Each layer of Figure 1.1 is mapped to a variety of tests each of which report a wealth of performance metrics related to the Microsoft Azure. Using these metrics administrators can find quick and accurate answers to the following queries:

- Is the Azure cloud available?
- How well the cloud responds to user requests?
- How many cores, storage accounts, cloud services, virtual and local network sites are monitored for each subscription ID?
- What is the current state of the storage account?
- Are the cloud services available? How many errors were encountered by the cloud services?
- What is the current state of each Azure database?
- How well the resources are utilized in the Azure databases?
- How many Azure databases are currently powered off, added, deleted etc?
- What is the current state of each Azure Virtual Machine?
- How many Azure virtual Machines were added, registered, powered on, powered off etc?
- Do the Azure Virtual machines have sufficient resources?
- How many errors are encountered by the Azure web sites and what is the current state of each Azure web site?

Chapter 2: How does eG Enterprise Monitor the Microsoft Azure?

eG Enterprise employs an agentless approach to monitor the target Microsoft Azure cloud. This approach requires that the eG agent be deployed on a remote host in the environment. To collect the metrics of interest from the Azure cloud, this eG agent uses the REST APIs. Using the REST APIs the eG agent can securely communicate with the Microsoft Azure cloud if the pre-requisites mentioned in the next section are fulfilled.

2.1 Pre-Requisites for Monitoring the Microsoft Azure (ARM)

The eG agent collects metrics from the target Microsoft Azure cloud in an *agentless* manner only.

In order to collect metrics from the target Microsoft Azure cloud, the eG agent communicates with the target Microsoft Azure cloud using Java API calls. To collect the required metrics, the eG agent requires the following:

- Directory ID of the target Microsoft Azure cloud;
- Access token in the form of an Application ID and Client secret.

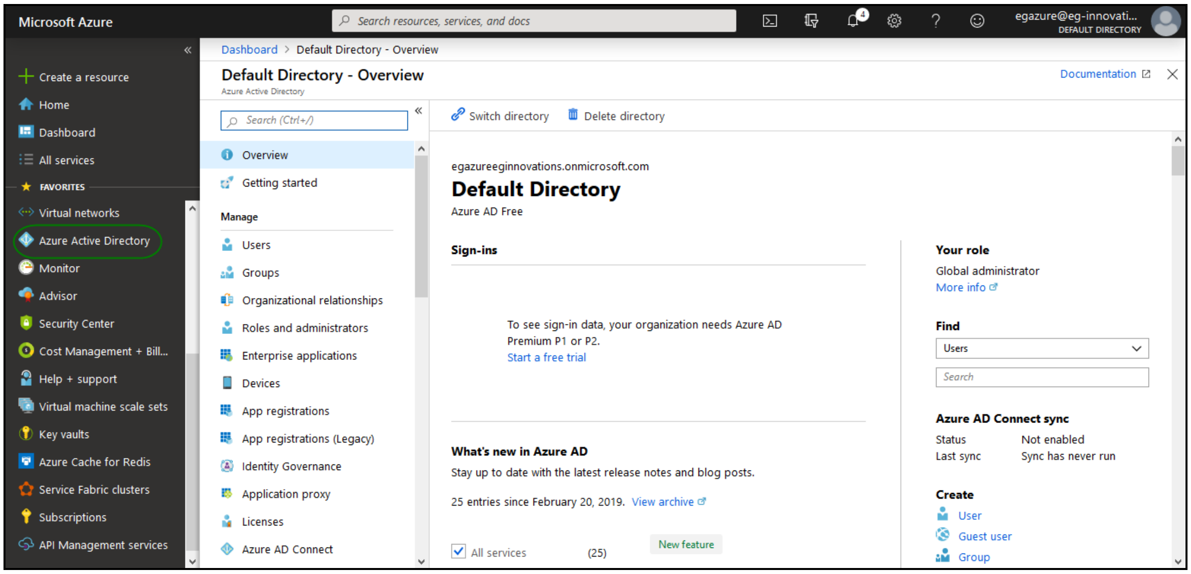
2.1.1 Broad Steps to Determine the Tenant ID and the Access Token

- Create a Web Application in the Active Directory of the target Microsoft Azure.
- Figure out the Tenant ID, the Application ID and Key value associated with the Application ID.
- Grant the required privileges to the Web Application from the Subscription of the target Microsoft Azure.

2.1.1.1 Creating a Web Application

To create the Web Application, do the following:

- Login to the Microsoft Azure portal using *https://portal.azure.com* with valid credentials.
- Click on **Azure Active Directory** icon in the leftmost pane (see 2.1).



egazureeginnovations.onmicrosoft.com

Default Directory

Azure AD Free

To see sign-in data, your organization needs Azure AD Premium P1 or P2. Start a free trial

Global administrator

Status	Not enabled
Last sync	Sync has never run

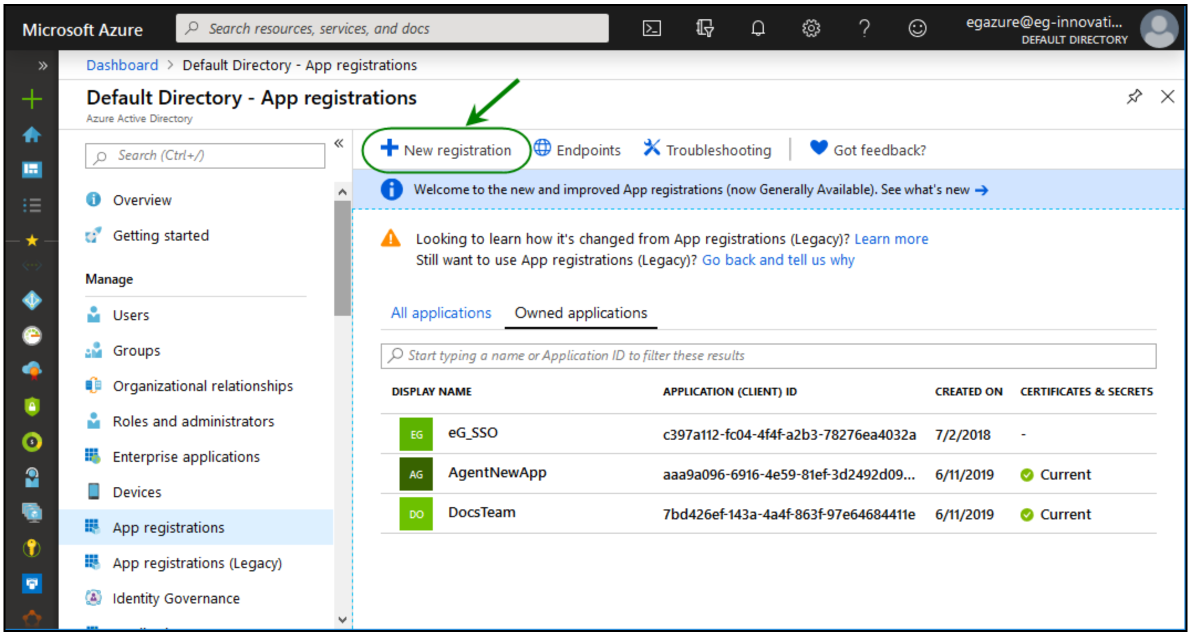
What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

25 entries since February 20, 2019. View archive

Figure 2.1: Selecting the Azure Active Directory option

- Click the **App Registrations** in the panel that appears when the Azure Active Directory is clicked. Figure 2.2 will then appear.



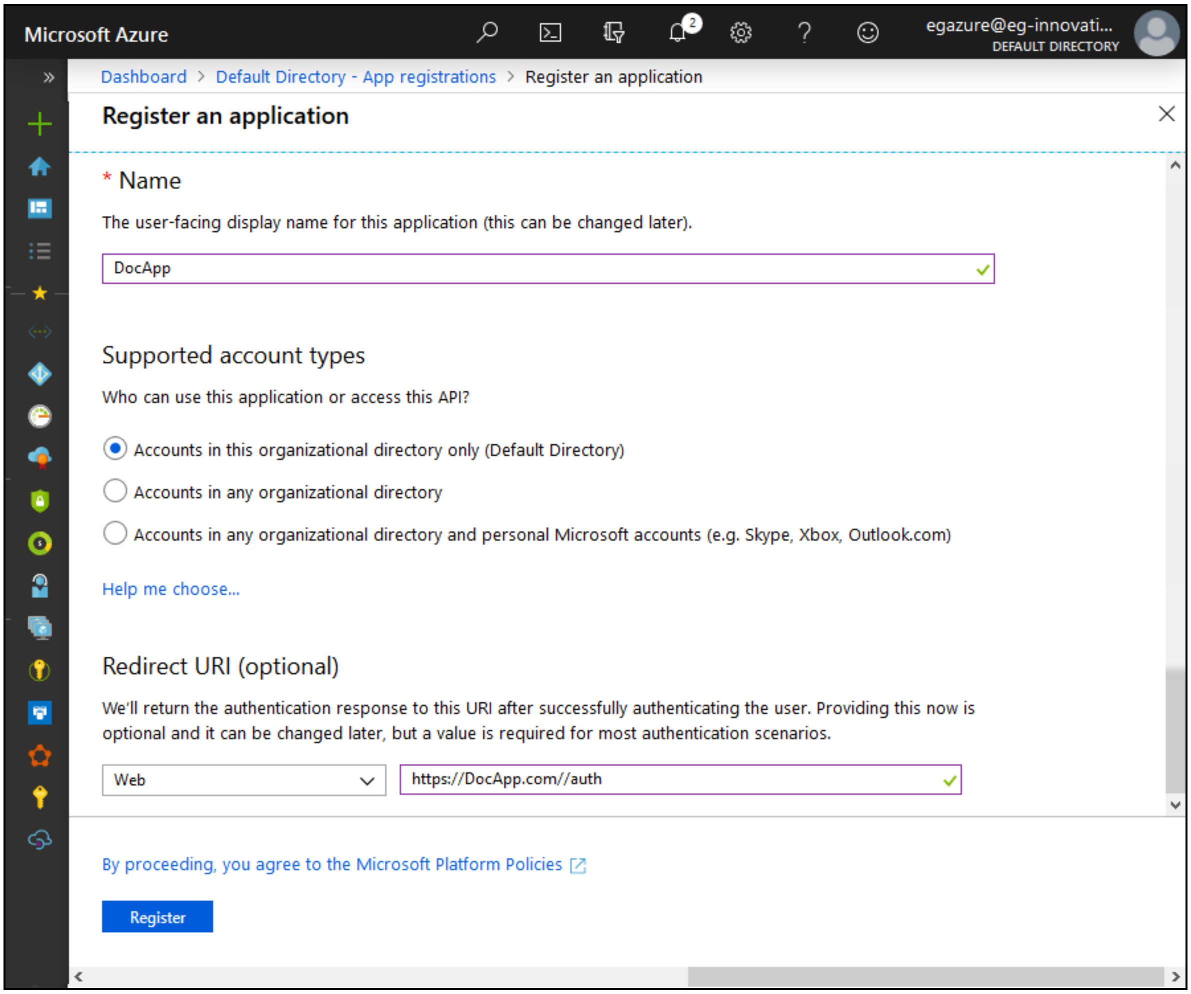
Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS
EG eG_SSO	c397a112-fc04-4f4f-a2b3-78276ea4032a	7/2/2018	-
AG AgentNewApp	aaa9a096-6916-4e59-81ef-3d2492d09...	6/11/2019	✓ Current
DO DocsTeam	7bd426ef-143a-4a4f-863f-97e64684411e	6/11/2019	✓ Current

Figure 2.2: Registering new application

- Click the **New application registration** in Figure 2.2. The **Register an application** will then appear as shown in Figure 2.3.


Microsoft Azure
egazure@eg-innovati...
DEFAULT DIRECTORY
Dashboard > Default Directory - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

DocApp ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://DocApp.com//auth ✓

By proceeding, you agree to the Microsoft Platform Policies

Figure 2.3: Specifying the details of the new web application

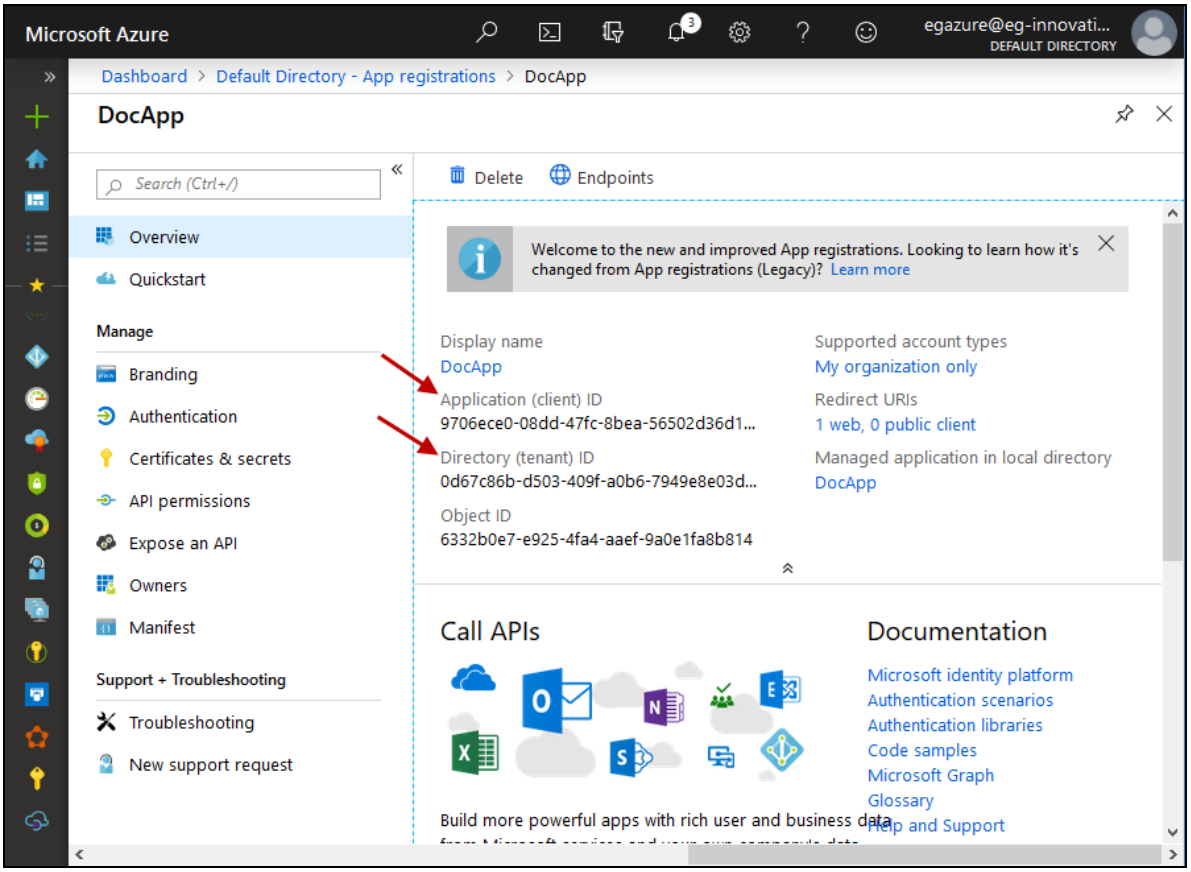
- In Figure 2.3, specify the following:
  - The name of the web application in the **Name** text box,
  - Select the type of the account from the **Supported account types** section.

Supported account types	Description
Accounts in this organizational directory only	Select this option if you're building a line-of-business (LOB) application. This option is not available if you're not registering the application in a directory. This option maps to Azure AD only single-tenant. This is the default option unless you're registering the app outside of a directory. In cases where the app is registered

Supported account types	Description
	outside of a directory, the default is Azure AD multi-tenant and personal Microsoft accounts.
Accounts in any organizational directory	Select this option if you would like to target all business and educational customers. This option maps to an Azure AD only multi-tenant. If you registered the app as Azure AD only single-tenant, you can update it to be Azure AD multi-tenant and back to single-tenant through the Authentication blade.
Accounts in any organizational directory and personal Microsoft accounts	Select this option to target the widest set of customers. This option maps to Azure AD multi-tenant and personal Microsoft accounts. If you registered the app as Azure AD multi-tenant and personal Microsoft accounts, you cannot change this in the UI. Instead, you must use the application manifest editor to change the supported account types.

  - Then, select the type of app you are building, Web or Public client (mobile & desktop), and then enter the redirect URI (or reply URL) for your application in the **Redirect URI** text box. For web applications, provide the base URL of your app. For example, *http://localhost:31544* might be the URL for a web app running on your local machine. Users would use this URL to sign in to a web client application. For public client applications, provide the URL used by Azure AD to return token responses. Enter a value specific to your application, such as *https://DocApp.com//auth*.

- Clicking the **Register** button in Figure 2.3 will create the **Web Application**. Then, the **Overview** page of the created application will appear as shown in Figure 2.4.



Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Display name: DocApp

Application (client) ID: 9706ece0-08dd-47fc-8bea-56502d36d1...

Directory (tenant) ID: 0d67c86b-d503-409f-a0b6-7949e8e03d...

Object ID: 6332b0e7-e925-4fa4-aaef-9a0e1fa8b814

Supported account types: My organization only

Redirect URIs: 1 web, 0 public client

Managed application in local directory: DocApp

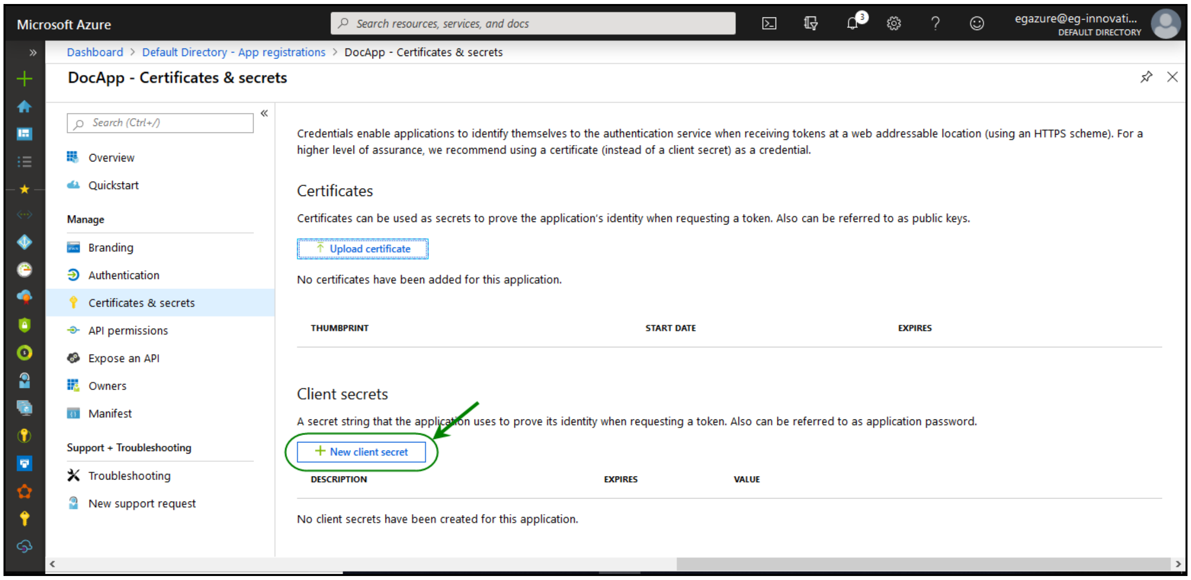
Build more powerful apps with rich user and business data

Figure 2.4: The successfully created web application

From the **Overview** page, you can obtain the **Application ID** and **Directory ID** (see Figure 4). Copy the **Application ID** and the **Directory ID** and paste them against the **CLIENT ID** and **TENANT ID** text boxes while configuring the tests associated with the Microsoft Azure that is to be monitored.

2.1.1.2 Obtaining the Client Secret

For the eG agent to obtain metrics from the target Microsoft Azure, it is necessary to provide the client secret associated with the created Web Application. For this, click on the **Certificates & secrets** option under the **Manage** node as shown in Figure 2.4. This will invoke Figure 2.5.



Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

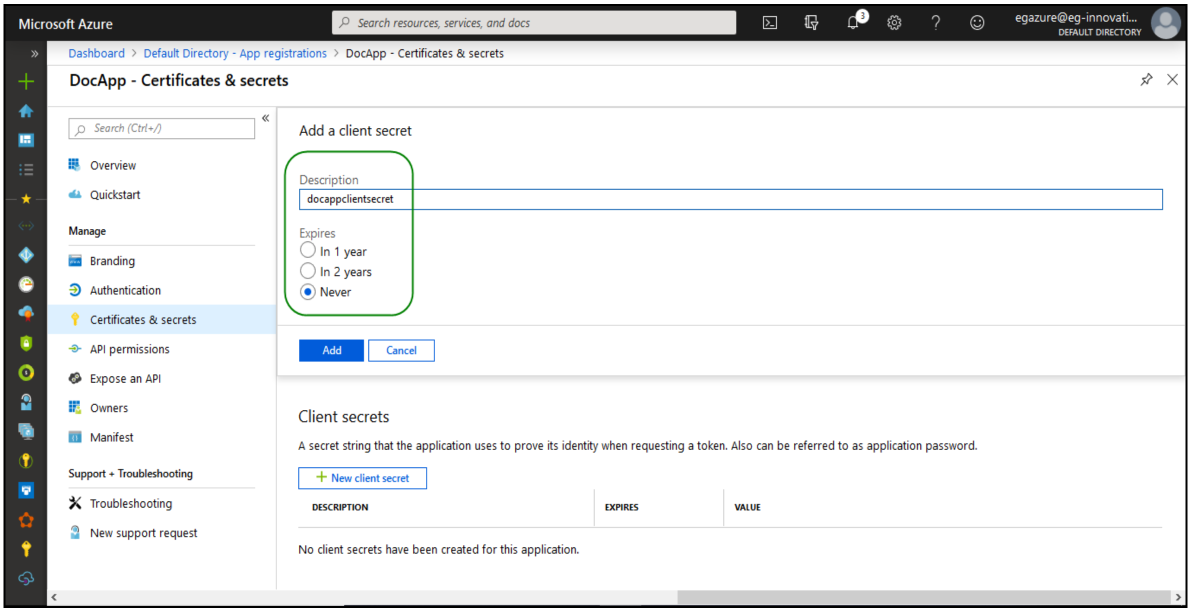
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

No client secrets have been created for this application.

Figure 2.5: Creating New Client Secret

Clicking on the **New client secret** button in Figure 2.5 will invoke Figure 2.6. Specify the description of the client secret in the **Description** text box and choose an expiry period from the **EXPIRES** section as shown in Figure 2.6.



Add a client secret

Description: docappclientsecret

Expires
○ In 1 year
○ In 2 years
● Never

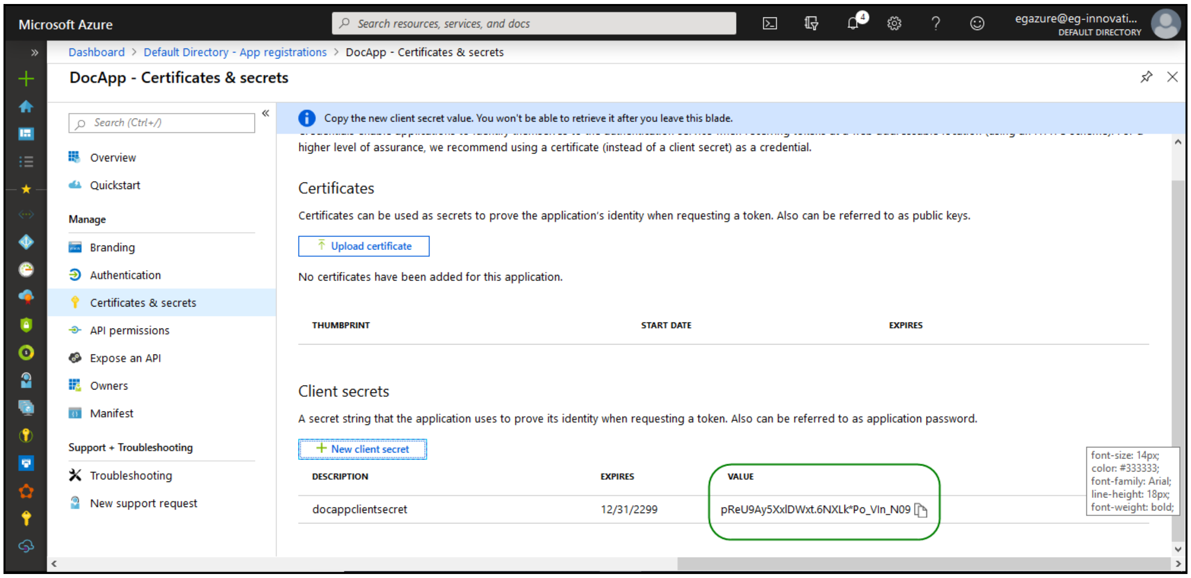
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

No client secrets have been created for this application.

Figure 2.6: Adding the client secret

Clicking the **Add** button in Figure 2.6 will display a client secret value in the **Value** section as shown in Figure 2.7.



Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE
docappclientsecret	12/31/2299	pReU9Ay5XxlDWxt.6NXLk*Po_Vln_N09

font-size: 14px;
color: #333333;
font-family: Arial;
line-height: 18px;
font-weight: bold;

Figure 2.7: Generating the client secret value for the web application

Note that the **Value** will disappear once you leave this page, so make sure that you copy the new client secret value in the clipboard by clicking the 📋 icon. Otherwise, you may need to generate a new client secret value. The client secret value has to be specified against the **CLIENT PASSWORD** field in the test configuration page.

2.1.1.3 Granting the Reader privilege to the Web Application

Once the web application is created, the web application should be granted *Reader* privilege on the Subscription associated with the Azure Active Directory. To grant the *Reader* privilege, do the following:

- Click on **All services** option in the leftmost pane as shown in Figure 9.

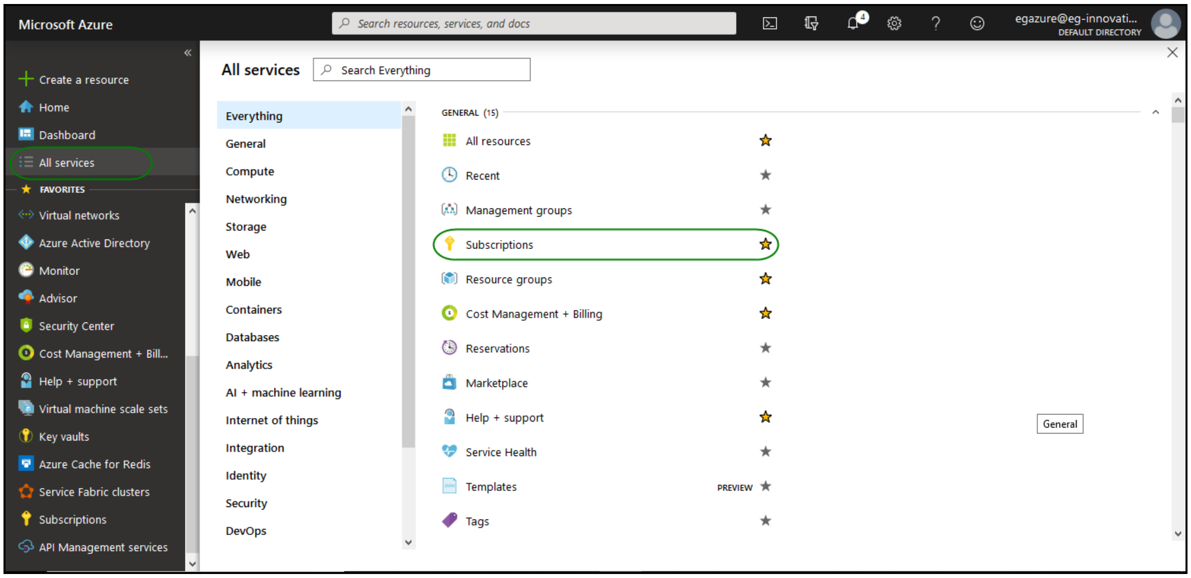


Figure 2.8: Clicking the All services option

- A context-sensitive menu sequence then appears in the right panel. Clicking the **Subscriptions** label from this panel in Figure 2.8 opens another context sensitive panel to the right. This will list all the subscriptions associated with your Azure account.

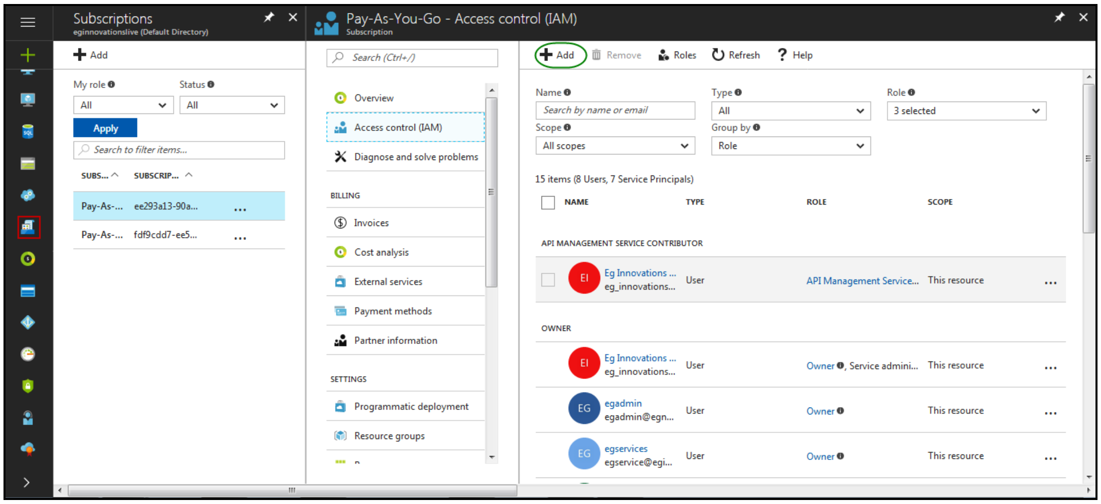
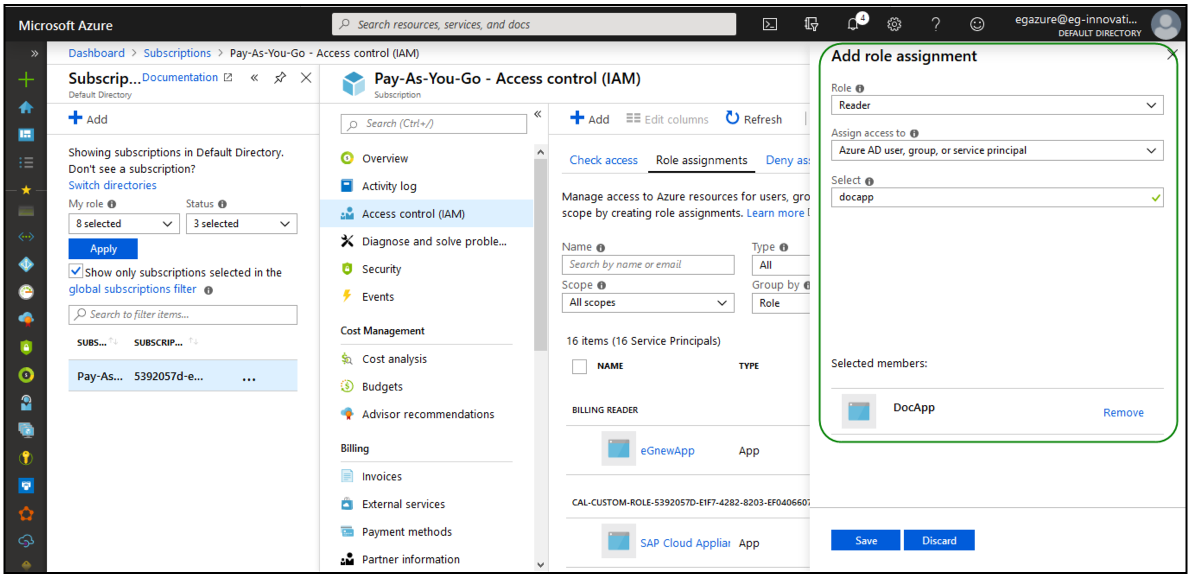


Figure 2.9: Adding the Subscription

Select the subscription that is associated with the target Microsoft Azure and click the **Access Control (IAM)**. In the next panel, click the **Add** button (seeFigure 2.9). In Figure 2.10 that appears, choose the *Reader* role from the **Role** list. In the **Select** text box, type the first few alphabets of the web application that you have created. Your selection will then appear as shown in Figure 2.10.



Add role assignment

Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: docapp

Selected members:

DocApp

Pay-As-You-Go - Access control (IAM)

Manage access to Azure resources for users, gro scope by creating role assignments. Learn more

Showing subscriptions in Default Directory. Don't see a subscription? Switch directories

My role: 8 selected

Status: 3 selected

☑ Show only subscriptions selected in the global subscriptions filter

16 items (16 Service Principals)

NAME	TYPE
BILLING READER	
eGnewApp	App
CAL-CUSTOM-ROLE-5392057D-E1F7-4282-8203-EF0406607	
SAP Cloud Applia	App

Figure 2.10: Granting the Reader role to the created web application

Clicking the **Save** button in Figure 2.10 will save your changes.

2.2 Pre-Requisites for Monitoring the Microsoft Azure (Classic)

To enable the eG agent to monitor the target Microsoft Azure cloud, the following pre-requisites need to be fulfilled:

The Subscription ID of the target Microsoft Azure cloud.

The Management Certificate. This certificate is required to authenticate the REST API calls. Note that the Management Certificate should be associated with the subscription of the target Microsoft Azure cloud. You could either create a management certificate on your own and associate it with your subscription or you could ask Windows Azure platform to create a management certificate for you and associate it with your subscription. If you are creating your own Management Certificate, then you need to follow the below-mentioned steps elaborately:

- Create a Keystore
- Export the Management Certificate i.e., Create a Management Certificate
- Upload the Certificate

2.2.1 Creating a Keystore

In order to create a keystore, a keytool is required. A keytool is a key and certificate management utility. It allows users to administer their own public/private key pairs and associated certificates for use in self-authentication (where the user authenticates himself/herself to other users/services) or data integrity and authentication services, using digital signatures. It also allows users to cache the public keys (in the form of certificates) of their communicating peers.

A certificate is a digitally signed statement from one entity (person, company, etc.), saying that the public key (and some other information) of some other entity has a particular value. (See Certificates.) When data is digitally signed, the signature can be verified to check the data integrity and authenticity. Integrity means that the data has not been modified or tampered with, and authenticity means the data indeed comes from whoever claims to have created and signed it.

The keytool also enables users to administer secret keys used in symmetric encryption/decryption (e.g. DES). The keytool stores the keys and certificates in a keystore.

For example, if you wish to create a keystore with the name WindowsAzureKeyStore.jks, then you have to run the keytoo utility from the command prompt of the target Microsoft Azure. By default, the keytool utility will be available in the *<eG_Agent_Install Directory>\java\jre7\bin* folder. Follow the steps given below to create a keystore using the keytool utility:

From the command prompt of the eG agent install directory, execute the keytool utility using the following commnd:

```
<eG_Agent_Install_Directory>\java\jre7\bin>keytool -genkeypair -alias mydomain -keyalg
RSA -keystore WindowsAzureKeyStore.jks -keysize 2048 -storepass "test123"
```

Once you have executed this command, you will be requested to provide your personal details as explained below:

```
What is your first and last name?

    [Unknown]: Sam Jose

What is the name of your organizational unit?

    [Unknown]: IT

What is the name of your organiation?

    [Unknown]: eG Innovations

What is the name of your City or Locality?

    [Unknown]: Chennai

What is the name of your State or Province?
```

```
    [Unknown]: Tamil Nadu
What is the two-letter country code for this unit?
    [Unknown]: IN
```

Once you have entered all the personal details, you will be prompted to verify if the give credentials are correct.

```
Is CN=Sam Jose, OU=IT, O=eG Innovations, L= Chennai, ST=Tamil Nadu, C=IN correct?
    [no]: yes
```

If you have confirmed your personal details, you will be prompted to provide the password for the domain.

```
Enter key password for <mydomain>
    (Return if password is same as keystore password):
```

The keystore is now created successfully and can be used to create a Management Certificate.

2.2.2 Creating a Management Certificate

To export or create a Management Certificate, you would be required to use the keytool command once again. To create a certificate named WindowsAzureSMAPI.cer in the location of your choice say for example, D:\, execute the following command from the *command prompt of the eG_Agent_Install_Directory*.

```
<eG_Agent_Install_Directory>\java\jre7\bin>keytool -v -export -file
D:\WindowsAzureSMAPI.cer -keystore WindowsAzureKeyStore.jks -alias mydomain
```

Once this command is executed, you will be prompted to provide the keystore password.

```
Enter keystore password: ********
```

The certificate file will be created and stored in the *D:\WindowsAzureSMAIP.cer* location of the eG_Agent_Install_Directory.

2.2.3 Uploading the Management Certificate

Once the Keystore and the Management Certificate are created, you need to upload this certificate to the Windows Azure Portal. To upload the certificate, do the following:

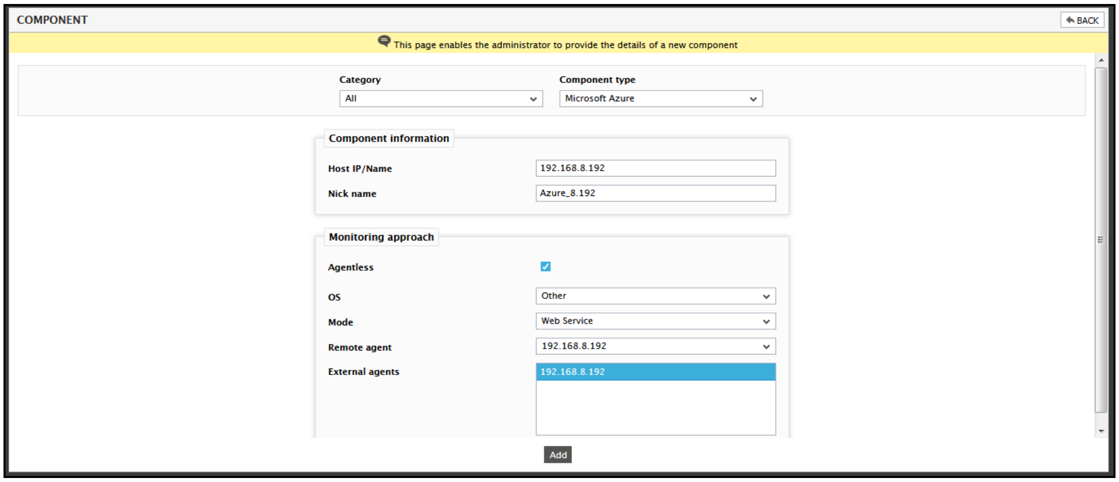
- Login into Windows Azure Portal at https://manage.windowsazure.com
- Click on the **SETTINGS** tab and then the **MANAGEMENT CERTIFICATES** tab and upload this *WindowsAzureSMAPI.cer* file.

Once the Management Certificate is uploaded to the target Microsoft Azure and the keystore is available in your eG_Agent_Install_Directory, then the communication between the eG agent and the target Microsoft Azure cloud will be secure and the metrics will be collected through secure communication. This way, the eG agent can collect the required metrics while monitoring the target Microsoft Azure cloud.

2.3 Managing the Microsoft Azure

The eG Enterprise cannot automatically discover the Microsoft Azure. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Microsoft Azure, do the following:

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover Microsoft Azure. You need to manually add the server using the **COMPONENTS** page (see Figure 2.11) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Microsoft Azure

Component information

Host IP/Name: 192.168.8.192

Nick name: Azure_8.192

Monitoring approach

Agentless: ☑

OS: Other

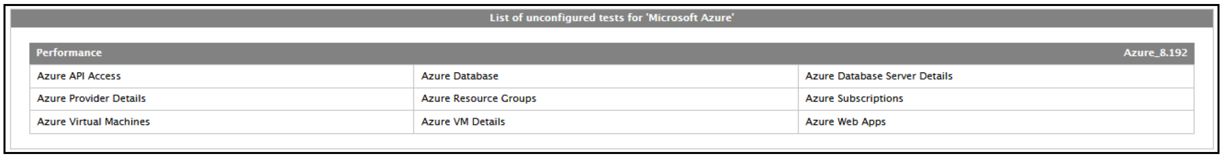
Mode: Web Service

Remote agent: 192.168.8.192

External agents: 192.168.8.192

Figure 2.11: Adding a Microsoft Azure

3. Specify the Host IP and the **Nick name** of the Microsoft Azure in Figure 2.11. The Microsoft Azure can only be monitored in Agentless manner. Then click the **Add** button to register the changes.
4. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.12.



List of unconfigured tests for 'Microsoft Azure'

Performance		Azure_8.192
Azure API Access	Azure Database	Azure Database Server Details
Azure Provider Details	Azure Resource Groups	Azure Subscriptions
Azure Virtual Machines	Azure VM Details	Azure Web Apps

Figure 2.12: List of Unconfigured tests to be configured for the IBM Integration Bus server

5. Click on the **Azure Database** test to configure it. To know how to configure the test, Click here. The remaining tests will be configured automatically.

6. Once the tests are configured, signout of the eG administrative interface.

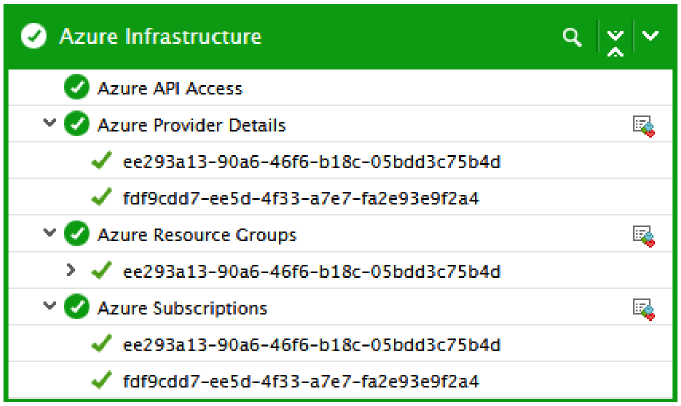
Chapter 3: Monitoring the Microsoft Azure

Microsoft Azure is a cloud computing platform and infrastructure, created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed and Microsoft partner hosted datacenters. Since many mission-critical applications these days are deployed on Microsoft Azure, the user experience with these applications depends upon the continuous availability and superlative performance of the Microsoft Azure cloud platform. To ensure this, eG now offers a specialized monitoring model for Microsoft Azure.

This chapter deep dives into every layer of the Microsoft Azure monitoring model, the tests mapped to each layer, and the measures every test reports.

3.1 Azure Infrastructure Layer

This layer throws light on how well the Azure cloud responds to user requests, the resource allocation to the subscription, the accessibility of the Azure cloud from an external perspective etc.



Azure Infrastructure

Azure API Access

Azure Provider Details

ee293a13-90a6-46f6-b18c-05bdd3c75b4d

fdf9cdd7-ee5d-4f33-a7e7-fa2e93e9f2a4

Azure Resource Groups

ee293a13-90a6-46f6-b18c-05bdd3c75b4d

Azure Subscriptions

ee293a13-90a6-46f6-b18c-05bdd3c75b4d

fdf9cdd7-ee5d-4f33-a7e7-fa2e93e9f2a4

Figure 3.1: The Azure Infrastructure layer

The sections discussed below will provide more information on these tests and the measures reported by them.

3.1.1 Azure API Access Test

The Azure Resource Manager provides a consistent management layer for the tasks performed through Azure PowerShell, Azure CLI, Azure portal, REST API, and development tools. All the tools use a common set of operations. These tools can be chosen and used in a hassle free manner. The Azure Resource Manager communicates with the development tools using the Azure Resource manager API. The API passes requests from the tools to the Resource Manager service, which authenticates and authorizes the requests. Resource Manager then routes the requests to the appropriate resource providers. If the Resource Manager API is not accessible, then the tools hosted on the Azure may not be available. Therefore it is necessary to periodically check the accessibility of the Resource manager API. The **Azure API Access** test helps administrators in this regard.

This test helps administrators figure out whether/not the API is accessible.

Target of the Test : Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each cloud service of the target Microsoft Azure being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Is API accessible?	Indicates whether/not the API is accessible.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Yes</td><td>1</td></tr>
<tr><td>No</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not the API is accessible. The graph of this measure however, represents the status of a server using the numeric equivalents only i.e., 0 or 1.
</td></tr>
</table>

3.1.2 Azure Provider Details Test

A resource provider is a service that supplies the resources you can deploy and manage through the Resource Manager. Each resource provider offers operations for working with the resources that are deployed. By default, most of the resource providers are automatically registered with the subscription. Alternately, the administrator can also register a resource provider to a subscription. If the resource providers are not available or are not registered with the subscription, the resources corresponding to those resource providers may not be accessible. To avoid this, it is necessary to keep track on the count of resource provides that were registered and those that were not registered. The **Azure Provider Details** test helps administrators in this regard!

For each subscription on the Microsoft Azure cloud, this test reports the total number of resource providers available, the count of the resource providers that are registered and are not registered. In addition, this test also reports the number of resource providers that are unregistered from the subscription. This way, administrators can figure out the resource providers that were unregistered from the subscription and can proactively hide the resources that cannot be accessed without the corresponding resource provider.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each subscription on the target Microsoft Azure being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test

Measurement	Description	Measurement Unit	Interpretation
Total providers	Indicates the total number of resource providers to which this subscription can be registered with.	Number	

Measurement	Description	Measurement Unit	Interpretation
Number of registered providers	Indicates the number of resource providers to which this subscription is registered with.	Number	The detailed diagnosis of this measure lists the names of the resource providers that were registered for each subscription.
Number of not registered providers	Indicates the number of resource providers to which this subscription is not registered with.	Number	The detailed diagnosis of this measure lists the names of the resource providers that were not registered with each subscription.
Number of registering providers	Indicates the number of resource providers to which this subscription is currently being registered.	Number	The detailed diagnosis of this measure lists the resource providers that were being registered with each subscription.
Number of unregistered providers	Indicates the number of resource providers from which this subscription is unregistered.	Number	The detailed diagnosis of this measure lists the resource providers that were unregistered with each subscription.
Number of unregistering providers	Indicates the number of resource providers from which this subscription is currently being unregistered.	Number	The detailed diagnosis of this measure lists the number of resource providers that were being unregistered from this subscription.

3.1.3 Azure Resource Groups Test

A resource is a manageable item that is available through Azure. A few common resources are a virtual machine, storage account, web app, database, virtual network etc. A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that the administrator wants to manage as a group. The resources in the resource group share the same lifecycle i.e., they are deployed, updated and deleted together. The Azure ARM can maintain multiple resource groups and though a resource can be migrated from one resource group to another the resource cannot exist in more than one group at a time. Often, failure of a resource group leads to the inaccessibility of the resources in that group. To avoid this, it is necessary to monitor the state of the resource groups round the clock! The **Azure Resource Groups** test helps in this regard!

This test auto-discovers the resource groups in a Microsoft Azure Resource Manager and reveals the current state of each resource group. This test also reveals the number of resources in each of the resource group. Using this test, administrators can figure out the exact resources residing in the resource groups and the location of those resources.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each *Subscription ID:Resource group* of the target Microsoft Azure being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures made by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of this resource group.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Succeeded</td><td>1</td></tr><tr><td>Unknown</td><td>0</td></tr></table><b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current state of this resource group. The graph of this measure however, represents the status of a server using the numeric equivalents only i.e., 0 or 1.</td></tr>
<tr><td>Number of resources</td><td>Indicates the number of resources in this resource group.</td><td>Number</td><td>The detailed diagnosis of this measure lists the name of each resource in the resource group, the type of the resource and the location of the resource.</td></tr>
</table>

3.1.4 Azure Subscriptions Test

An Azure subscription is the basic unit where all resources are contained. It also defines several limits within Azure, such as number of cores, resources, etc.

In target environments where critical applications are to be hosted on Microsoft Azure, it becomes a necessity to create a Microsoft Azure subscription. Once the subscription is created, monitoring the count of the allocated resources within the subscription may pose a challenge to the administrators. In order to help administrators to keep track of the resources allocated to the subscription and the resources that remain inactive and are not available for use, the eG Enterprise suite provides you with the **Azure Subscriptions** test.

This test helps administrators to figure out the state of each subscription and the total number of resources allocated to each subscription, the number of geographic locations of allocated to each subscription, etc. Using this test, administrators can figure out the number of inactive resources on each subscription. This way, resources that are seldom used can be identified.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each subscription of the target Microsoft Azure being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of this subscription.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>1</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current state of this subscription. The graph of this measure however, is represented using the numeric equivalents only - 0 or 1.</td></tr>
<tr><td>Number of GEO locations</td><td>Indicates the number of geographic locations allocated to this subscription.</td><td>Number</td><td>The detailed diagnosis of this measure lists the name of the geographic locations that are allocated to each subscription.</td></tr>
<tr><td>Total number of resources</td><td>Indicates the total number of resources that can be allocated to this subscription.</td><td>Number</td><td></td></tr>
<tr><td>Number of active resources</td><td>Indicates the number of resources that are currently active on this subscription.</td><td>Number</td><td>The detailed diagnosis of this measure lists the name of the resource provider and the name of the resources provided through each resource provider that are active for each subscription.</td></tr>
<tr><td>Number of inactive resources</td><td>Indicates the number of resources that are currently inactive on this subscription.</td><td>Number</td><td>The detailed diagnosis of this measure lists the name of the resource provider and the name of the resources provided through each resource provider that are inactive for each subscription.</td></tr>
<tr><td>Other resources</td><td>Indicates the number of resources that are</td><td>Number</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	currently in other states on this subscription.		
Active resource groups	Indicates the number of resource groups that currently active on this subscription.	Number	

3.1.5 Azure Connection (classic) Test

This test reports the availability of the Microsoft Azure cloud and also helps administrators figure out how well the cloud responds to user requests. Using this test, administrators can very well figure out the poor responsiveness of the cloud to user requests.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID -** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text

box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **DD FREQUENCY -** Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Availability:	Indicates whether/not the Microsoft Azure cloud is available.	Percent	The value 100 indicates that the cloud is available. The value 0 for this measure indicates that the cloud is not available.
Response time:	Indicates the time taken by the cloud to respond to client requests.	Secs	Ideally, the value of this measure should be low. A high value or a steady increase in the value of this measure is a cause for concern, as it

Measurement	Description	Measurement Unit	Interpretation
			indicates poor responsiveness. This can be caused by factors such as a bottleneck in the cloud or a configuration problem.

3.1.6 Azure Subscriptions (classic) Test

A Microsoft Azure subscription grants you access to Microsoft Azure services and to the Microsoft Azure Platform Management Portal.

A Microsoft Azure subscription has two aspects:

- The Microsoft Azure account, through which resource usage is reported and services are billed.
- The subscription itself, which governs access to and use of the Microsoft Azure services that are subscribed to. The subscription holder manages services (Microsoft Azure, Azure SQL database, Azure Storage etc) through the Microsoft Azure Platform Management Portal.

In target environments where critical applications are to be hosted on Microsoft Azure, it becomes a necessity to create a Microsoft Azure subscription. Once the subscription is created, monitoring the utilization of the allocated resources within the subscription may pose a challenge to the administrators. In order to help administrators to keep track of the resources allocated to the subscription and the resources utilized, the eG Enterprise suite provides you with the **Azure Subscriptions (classic)** test.

This test helps administrators to figure out the maximum amount of resources i.e., cores, virtual machines, storage accounts, cloud services etc allocated to the Azure Subscription and also helps to detect irregularities in the allocation of the resources, if any.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID-** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

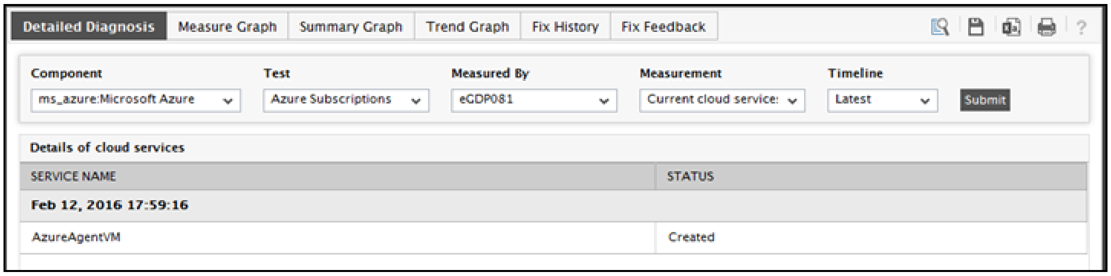
   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Max cores:	Indicates the maximum number of cores that can be allocated to the subscription.	Number	
Current cores:	Indicates the number of cores that are currently utilized in the subscription.	Number	If the value of this measure is equal to the Max cores measure, then it indicates that no more cores in the subscription can be utilized. Administrators are therefore alerted to monitor the high utilization of the cores.
Core utilization:	Indicates the percentage of cores utilized in the subscription.	Percent	A value close to 100 indicates that the subscription ID is running out of cores.
Max storage accounts:	Indicates the maximum number of storage accounts that can be allocated to the subscription.	Number	
Current storage accounts:	Indicates the number of storage accounts that are currently utilized in the subscription.	Number	If the value of this measure is equal to the Max storage accounts measure, then it indicates that no more storage accounts can be utilized in the subscription. The detailed diagnosis of this measure if enabled, lists the storage accounts associated with the subscription.
Storage accounts utilization:	Indicates the percentage of storage accounts utilized in the subscription.	Percent	A value close to 100 indicates that the subscription is running out of storage accounts.
Max cloud services:	Indicates the maximum number of cloud services that can be allocated to the subscription ID.	Number	

Measurement	Description	Measurement Unit	Interpretation
Current cloud services:	Indicates the number of cloud services that are currently utilized in the subscription.	Number	If the value of this measure is equal to Max cloud services, then it indicates that all the allocated cloud services are already utilized. The detailed diagnosis of this measure if enabled, lists the cloud services that were created for the subscription.
Cloud services utilization	Indicates the percentage of cloud services utilized in the subscription.	Percent	A value close to 100 indicates that the subscription is running short of cloud services.
Max virtual network sites:	Indicates the maximum number of virtual network sites that can be allocated to the subscription.	Number	
Current virtual network sites:	Indicates the number of virtual network sites that are currently allocated to the subscription.	Number	If the value of this measure is equal to the Max virtual network sites, then it indicates that no more virtual network sites can be utilized in the subscription.
Virtual network sites utilization:	Indicates the percentage of virtual network sites utilized in the subscription.	Percent	A value close to 100 indicates that the subscription is running out of virtual network sites.
Max local network sites:	Indicates the maximum number of local network sites that can be allocated to the subscription.	Number	
Max DNS servers:	Indicates the maximum number of DNS servers that can be allocated to the subscription.	Number	

The detailed diagnosis of the *Current cloud services* measure if enabled, lists the cloud services that were created in the subscription.



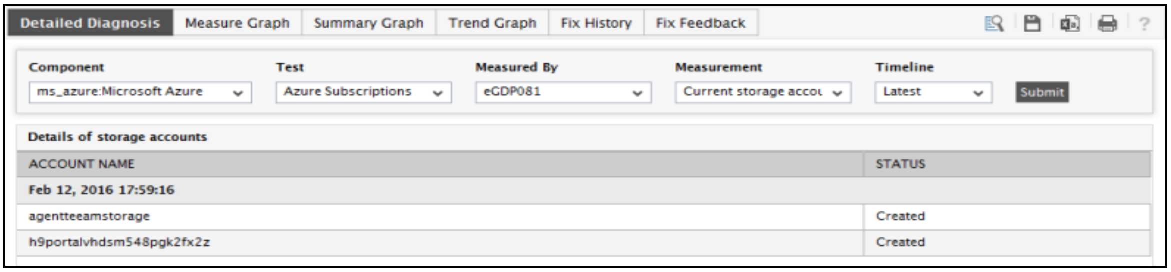
Component: ms_azure:Microsoft Azure
Test: Azure Subscriptions
Measured By: eGDP081
Measurement: Current cloud service:
Timeline: Latest

Details of cloud services

SERVICE NAME	STATUS
Feb 12, 2016 17:59:16	
AzureAgentVM	Created

Figure 3.2: The detailed diagnosis of the *Current cloud services* measure

The detailed diagnosis of the *Current storage accounts* measure if enabled, lists the storage accounts that were created in the subscription.



Component: ms_azure:Microsoft Azure
Test: Azure Subscriptions
Measured By: eGDP081
Measurement: Current storage accou
Timeline: Latest

Details of storage accounts

ACCOUNT NAME	STATUS
Feb 12, 2016 17:59:16	
agentteeamstorage	Created
h9portalvhdsm548pgk2fx2z	Created

Figure 3.3: The detailed diagnosis of the *Current storage accounts* measure

3.1.7 Azure Web Access (classic) Test

The details of the **Azure Web Access (classic)** test that emulates a user accessing the Microsoft Azure cloud are provided below. Since this test can be executed from a location external to the Microsoft Azure, this test presents an unbiased external perspective of the state of the Microsoft Azure cloud.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for every URL being monitored

First-level descriptor: URL available in the target Microsoft Azure

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **PORT-** The port to which the specified **HOST** listens
4. **URL -** This test emulates a user accessing a specific web site(s) on the target Azure cloud to determine the availability and responsiveness of the cloud. To enable this emulation, you need to configure the test with the URL of the web site that it should access. Specify this URL against the URL parameter. If required, you can even configure multiple URLs – one each for every web site that the test should attempt to access. If each URL configured requires special permissions for logging in, then, you need to configure the test with separate credentials for logging into every URL. Likewise, you need to provide instructions to the test on how to validate the content returned by every URL, and also set an encoding format for each URL. To enable administrators to easily configure the above per URL, eG Enterprise provides a special interface. To access this interface, click on the encircled '+' button alongside the URL text box in the test configuration page. Alternatively, you can even click on the encircled '+' button adjacent to the URL parameter in the test configuration page. To know how to use this special interface, refer to Section 2.2.1.1. of this document.
5. **COOKIEFILE -** Whether any cookies being returned by the web server need to be saved locally and returned with subsequent requests
6. **PROXYHOST -** The host on which a web proxy server is running (in case a proxy server is to be used)
7. **PROXYPORT -** The port number on which the web proxy server is listening
8. **PROXYUSERNAME -** The user name of the proxy server
9. **PROXYPASSWORD -** The password of the proxy server
10. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
11. **TIMEOUT -** Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default *TIMEOUT* period is 30 seconds.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Web availability:	Indicates whether the Azure cloud was able to respond successfully to the query made by the	Percent	Availability failures could be caused by several factors such as the web server process(es) being down, the web server being misconfigured, a network failure, etc. Temporary unavailability may also occur if

Measurement	Description	Measurement Unit	Interpretation
	test.		the web server is overloaded. Availability is determined based on the response code returned by the server. A response code between 200 to 300 indicates that the server is available.
Total response time:	Indicates the time taken by the cloud to respond to the requests it receives.	Secs	Response time being high denotes a problem. Poor response times may be due to the server being overloaded or misconfigured. If the URL accessed involves the generation of dynamic content by the server, backend problems (e.g., an overload at the application server or a database failure) can also result in an increase in response time.
TCP connection availability:	Indicates whether the test managed to establish a TCP connection to the cloud.	Percent	Failure to establish a TCP connection may imply that either the web server process is not up, or that the process is not operating correctly. In some cases of extreme overload, the failure to establish a TCP connection may be a transient condition. As the load subsides, the server may start functioning properly again.
TCP connect time:	Quantifies the time for establishing a TCP connection to the web server host.	Secs	Typically, the TCP connection establishment must be very small (of the order of a few milliseconds). Since TCP connection establishment is handled at the OS-level, rather than by the application, an increase in this value signifies a system-level bottleneck on the host that supports the web server.
Server response time:	Indicates the time period between when the connection was established and when the server sent back a HTTP response header to the client.	Secs	While the total response time may depend on several factors, the server response time is typically, a very good indicator of a server bottleneck (e.g., because all the available server threads or processes are in use).
Content validity:	Validates whether	Percent	A value of 100% indicates that the content

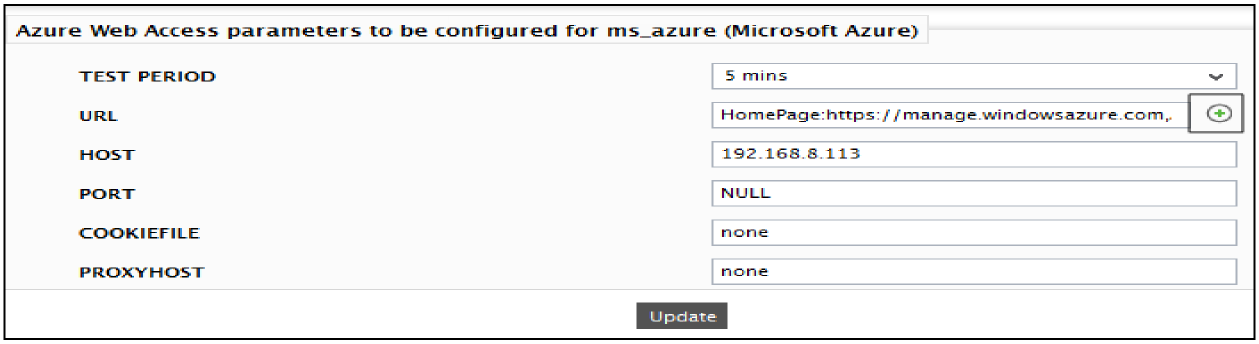
Measurement	Description	Measurement Unit	Interpretation
	the server was successful in executing the request made to it.		returned by the test is valid. A value of 0% indicates that the content may not be valid. This capability for content validation is especially important for multi-tier web applications. For example, a user may not be able to login to the web site but the server may reply back with a valid HTML page where in the error message, say, "Invalid Login" is reported. In this case, the availability will be 100 % (since we got a valid HTML response). If the test is configured such that the content parameter should exclude the string "Invalid Login," in the above scenario content validity would have a value 0.
Response code:	Indicates the response code returned by the server for the simulated request.	Number	A value between 200 and 300 indicates a good response. A 4xx value indicates a problem with the requested content (eg., page not found). A 5xx value indicates a server error.
Content length:	Indicates the size of the content returned by the cloud.	Kbytes	Typically the content length returned by the server for a specific URL should be the same across time. Any change in this metric may indicate the need for further investigation on the server side.
Data transfer time:	Indicates the time taken for a data transfer between the drive and the host system.	Secs	Data transfer time being high denotes a problem.
DNS availability:	Indicates whether the DNS server was able to respond successfully to the request made to it.	Percent	While the value 100 for this measure indicates that the DNS server is available and successfully responded to the request, the value 0 indicates that the DNS server is unavailable or is not responding to requests. Availability failures could be caused by many reasons such as a network failure. Sometimes, the DNS server may be

Measurement	Description	Measurement Unit	Interpretation
			reachable through basic network testing, but may not respond to DNS queries from clients. **Note:** This measure will be able to report a value only if the URL parameter of the test is configured with a domain name-based URL – eg., http://www.eginnovations.com, http://www.eBooks.com. If the URL parameter is configured with an IP-based URL instead – eg., http://192.168.10.21:80, http://192.168.10.34:7077 – then, this measure will not report any value. This is because, to report the availability of the DNS server, the test attempts to connect to the DNS server and resolve the domain name in the URL to its IP address. If the test is able to perform domain name – IP address resolution successfully, it reports the value 100 for this measure. If the resolution fails, the test reports the value 0. In case of an IP-based URL naturally, the test will not be able to find any domain name to resolve. The test therefore will not report any value for this measure in that case.

3.1.7.1 Configuring URLs for Monitoring

By default, the Azure Web Access test will be configured with the URL of the home page of the target Azure cloud being monitored. To configure additional URLs, do the following:

1. Click on the encircled '+' button alongside the URL text box in Figure 3.4.

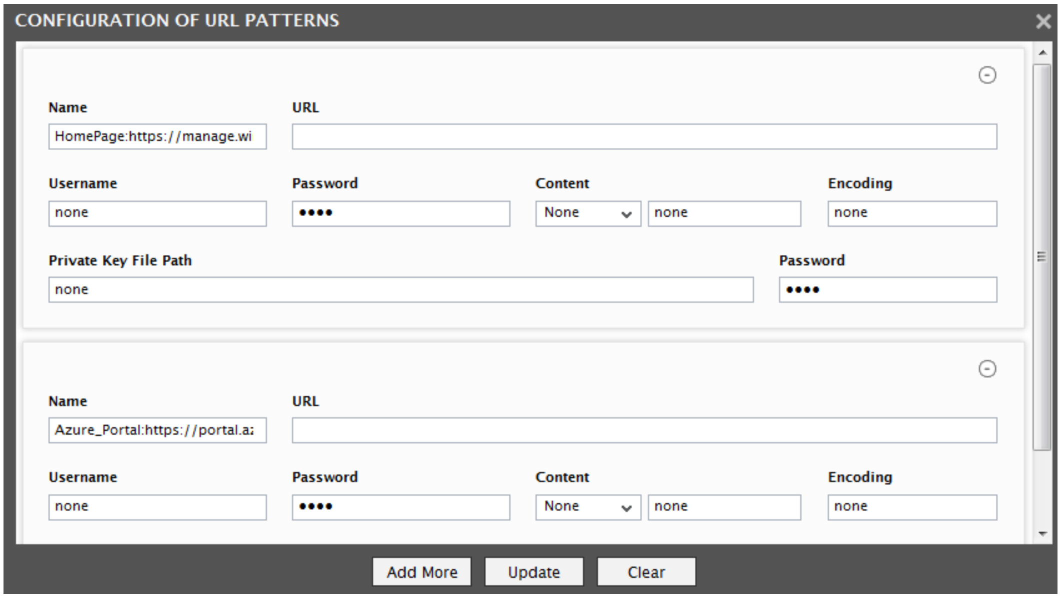


Azure Web Access parameters to be configured for ms_azure (Microsoft Azure)

TEST PERIOD	5 mins
URL	HomePage:https://manage.windowsazure.com,
HOST	192.168.8.113
PORT	NULL
COOKIEFILE	none
PROXYHOST	none

Figure 3.4: Configuring the Azure Web Access test

2. Figure 3.5 then appears. To add another URL, click the Add More button in Figure 3.5.



CONFIGURATION OF URL PATTERNS

Name	HomePage:https://manage.wi
URL	
Username	none
Password	••••
Content	None; none
Encoding	none
Private Key File Path	none
Password	••••

Name	Azure_Portal:https://portal.a:
URL	
Username	none
Password	••••
Content	None; none
Encoding	none

Figure 3.5: Configuring multiple URLs

3. Another URL specification section will appear. Specify the following in that section:

- **Name:** Specify a unique name by which the URL you will be specifying shortly will be referred to across the eG user interface. This is the name that will appear as the descriptor of this test.
- **URL:** Enter the URL of the web page that this test should access.
- **Username** and **Password:** These parameters are to be set only if a specific user name / password has to be specified to login to the web page (i.e., **URL**) that you have configured for

monitoring. In this case, provide valid login credentials using the **Username** and **Password** text boxes. If the web server on which **Azure Web Access** test executes supports 'Anonymous user access', then these parameters will take either of the following values:

- A valid **Username** and **Password** for the configured **URL**
- *none* in both the **Username** and **Password** text boxes of the configured **URL**, if no user authorization is required
- Some web servers however, support NTLM (Integrated Windows) authentication, where valid login credentials are mandatory. In other words, a none specification will not be supported by such web servers. Therefore, in this case, against each configured **URL**, you will have to provide a valid **Username** in the format: *domainname\username*, followed by a valid **Password**.
- Please be sure to check if your web site requires HTTP authentication while configuring this parameter. HTTP authentication typically involves a separate pop-up window when you try to access the page. Many sites use HTTP POST for obtaining the user name and password and validating the user login. In such cases, the username and password have to be provided as part of the POST information.

- **Content:** The **Content** parameter has to be configured with an instruction:value pair that will be used to validate the content being returned by the test. If the Content value is *None*, no validation is performed. On the other hand, if you pick the *Include* option from the **Content** list, it indicates to the test that for the content returned by the web server to be valid, the content must include the specified value (a simple string search is done in this case). This value should be specified in the adjacent text box. Similarly, if the *Exclude* option is chosen from the **Content** drop-down, it indicates to the test that the server's output is valid if it does not contain the value specified in the adjacent text box. The *Include* or *Exclude* value you specify in the text box can include wildcard characters. For example, an *Include* instruction can be **Home page**.
- **Encoding:** Sometimes the eG agent has to parse the **URL** content with specific encoding other than the default (ISO-8859-1) encoding. In such a case, specify the type of encoding using which the eG agent can parse the **URL** content in the **Encoding** text box. By default, this value is *none*.
- **Private Key File Path** and **Password:** SSL-enabled web sites are typically secured by a private key, public key, or a public-private key pair. If the web page configured for this test is SSL-enabled – i.e., if an HTTPS URL is specified against URL – and the contents of this web page can only be accessed using a private key, then the full path to the private key file will have to be provided against Private key file path and the password of the private key file

should be specified against Password. If no such private key protects the contents of the configured URL, then set the Private key file path and its Password to *none*.

4. Similarly, you can add multiple URL specifications. To remove a URL specification, click on the encircled '-' button corresponding to it. To clear all URL specifications, click the **Clear** button in Figure 3.5. To update all the changes you made, click the **Update** button.
5. Once **Update** is clicked, you will return to the test configuration page. The **URL** text box in the test configuration page will display just the **Names** – i.e., the unique display names – that you may have configured for the multiple URLs, as a comma-separated list. To view the complete URL specification, click the encircled ''+' button alongside the **URL** text box, once again.

3.2 Azure Network Services Layer

This layer helps administrators to keep track on the number of virtual networks available in the Azure cloud for each subscription.

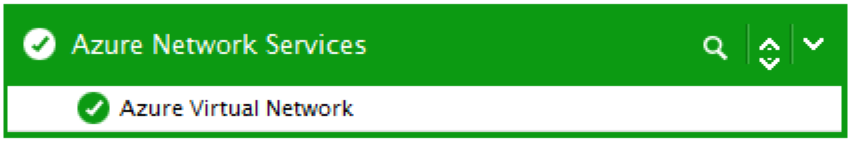


Figure 3.6: The Azure Network Services layer

The forthcoming section will discuss in detail about the test and the measures reported by the test.

3.2.1 Azure Virtual Network (classic) Test

An Azure virtual network (VNet) is a representation of your own network in the Azure cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. You can fully control the IP address blocks, DNS settings, security policies, and route tables within this network. You can also further segment your VNet into subnets and launch Azure IaaS virtual machines (VMs) and/or Cloud services (PaaS role instances). Additonally, you can connect the virtual network to your on-premises network using one of the connectivity options available in Azure. In essence, you can expand your network to Azure, with complete control on IP address blocks with the benefit of enterprise scale Azure provides. Following are the benefits of virtual networks in an environment:

- **Isolation.** VNets are completely isolated from one another. That allows you to create disjoint networks for development, testing, and production that use the same CIDR address blocks.
- **Access to the public Internet.** All IaaS VMs and PaaS role instances in a VNet can access the public Internet by default. You can control access by using Network Security Groups (NSGs).
- **Access to VMs within the VNet**. PaaS role instances and IaaS VMs can be launched in the same virtual network and they can connect to each other using private IP addresses even if they are in different subnets without the need to configure a gateway or use public IP addresses.
- **Name resolution.** Azure provides internal name resolution for IaaS VMs and PaaS role instances deployed in your VNet. You can also deploy your own DNS servers and configure the VNet to use them.
- **Security.** Traffic entering and exiting the virtual machines and PaaS role instances in a VNet can be controlled using Network Security groups.
- **Connectivity.** VNets can be connected to each other, and even to your on- premises datacenter, by using a site-to-site VPN connection, or ExpressRoute connection. To learn more about VPN gateways, visit About VPN gateways.

If the virtual networks experience a sudden slowdown or are rendered inaccessible, the virtual machines and cloud services associated with the virtual networks will not be accessible thus causing setback to the user experience. To avoid such setbacks, it is essential for the administrators to figure out the count and the status of the virtual networks in the target environment. The **Azure Virtual Network (classic)** test helps administrators in this regard!.

This test helps administrators to figure out the number of virtual networks available in the target Microsoft Azure cloud . The detailed diagnosis of the test will list the status of each virtual network in the cloud. This way, administrators can figure out the virtual networks that are currently down/inaccessible.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

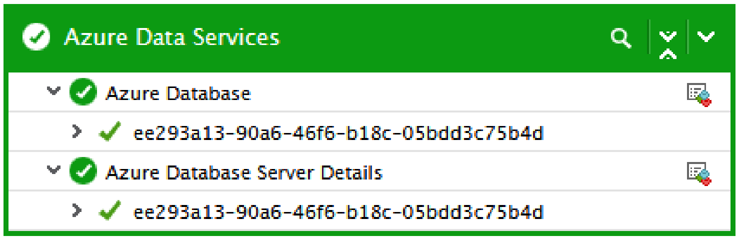
   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Virtual network:	Indicates the number of virtual networks that were configured for the subscription.	Number	The detailed diagnosis of this measure if enabled, lists the Name, Status, Location, Subnet name, Subnet address space, Address prefix and ID.

3.3 Azure Data Services Layer

This layer helps administrators analyze the current state and resource utilization of each database, the numerical statistics of the databases that were added, removed, registered on the cloud etc. This layer also depicts the status of different storage accounts and helps them figure out the storage services that are unavailable and error prone.



Azure Data Services
- Azure Database
  - ee293a13-90a6-46f6-b18c-05bdd3c75b4d
- Azure Database Server Details
  - ee293a13-90a6-46f6-b18c-05bdd3c75b4d

Figure 3.7: The Azure Data Services layer

The sections discussed below will provide more information on these tests and the measures reported by them.

3.3.1 Azure Database Test

Microsoft Windows Azure SQL Database is similar to an on-premise Microsoft SQL Server and extends the SQL Server database capability to the cloud. Azure SQL Database lets you provision and deploy relational database solutions to the cloud, including many benefits such as, rapid provisioning, scalable, high availability and minimal maintenance overhead.

Maintaining Azure SQL database on the cloud is easy to manage, with less effort, because of the complete infrastructure provided by Microsoft System Center. Though the Azure SQL database can be easily managed and can be included as a resource in a resource group, it is also essential to keep track on the day-to-day performance of the Azure SQL database. To achieve this, administrators may use the **Azure Database** test.

For each Azure SQL database instance in a resource group, this test reports the current state and also the resource utilization. Using this test, administrators can identify the Azure SQL database instance that is improperly sized with CPU, memory and I/O resources.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each *Subscription ID: Resource Group: Azure SQL Database logical server: Azure SQL Database instance* of the target Microsoft Azure being monitored

Descriptor: Azure SQL Database instance

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures made by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this database instance.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>0</td><td>Unknown</td></tr><tr><td>1</td><td>Online</td></tr></table>
<b>Note:</b>
By default, this measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of this database instance. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 or 1.
The detailed diagnosis of this measure if enabled, lists the location of the database instance, the edition, the date on which the instance was created, the collation of the database instance, the default secondary location of the instance and the service level objective of the instance.</td></tr>
<tr><td>Maximum database size</td><td>Indicates the maximum size allocated to this database instance.</td><td>MB</td><td></td></tr>
<tr><td>CPU utilization</td><td>Indicates the average percentage of CPU utilized by this database instance.</td><td>Percent</td><td></td></tr>
<tr><td>Data IO percentage</td><td>Indicates the percentage of physical data that was read from this database instance.</td><td>Percent</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Log IO percentage	Indicates the percentage of logs written to this database instance.	Percent	
Storage utilization	Indicates the percentage of space utilized in this database instance.	Percent	A value close to 100 for this measure denotes that the database instance is running short of space.
Total database size	Indicates the amount of memory utilized by this database instance.	MB	A high value for this measure is a cause of concern, If the value of this measure is close to the *Maximum database size*, then administrators should either increase the memory limit of the database or free up the available resources.
Workers percentage	Indicates the percentage of worker threads that are currently running on this database instance.	Percentage	
Sessions percentage	Indicates the percentage of sessions that are currently opened and used by the clients on this database instance.	Percentage	
DTU limit	Indicates the maximum number of resources i.e., Database Transaction Units allocated to this database instance.	Number	
DTU used	Indicates the number of Database Transaction Units utilized by this database instance.	Number	
DTU percentage	Indicates the percentage of Database Transaction Units utilized by this database instance.	Percentage	A value close to 100 is an alert to the administrator to increase the DTUs allocated to the database instance.
Successful	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
connections	successful connections to this database instance.		
Failed connections	Indicates the number of connections that failed to establish on this database instance.	Number	
Blocked by firewall	Indicates the number of connections that were terminated on this database instance due to the blocking activity of the firewall.	Number	
Deadlock connections	Indicates the number of connections that experienced deadlock on this database instance.	Number	Ideally, the value of this measure should be zero. If a sudden/gradual increase in the value of this measure is noticed, then, administrators should query the database to identify when exactly the deadlocks occurred.

3.3.2 Azure Database Server Details Test

An Azure SQL database is a managed database in Microsoft Azure that is created within an Azure resource group with a defined set of compute and storage resources for different workloads. An Azure SQL database is associated with an Azure SQL Database logical server, which is created within a specific Azure region. A logical server acts as a central administrative point for multiple databases, including SQL elastic pools logins, firewall rules, auditing rules, threat detection policies, and failover groups. A logical server can be in a different region than its resource group. The logical server must exist before you can create the Azure SQL database. All databases on a server are created within the same region as the logical server.

A logical server is a parent resource for databases, elastic pools, and data warehouses. It also provides the scope for database quota and DTU quota for the resources it contains (such as 45,000 DTU) and therefore is a high-order element of the identity of databases, elastic pools, and data warehouses for Azure resource management purposes. If the Azure logical server is not ready, then the Azure databases associated with the logical server and the resource group may not be accessible causing inconvenience to the users accessing the resources from such resource groups.

Therefore, it is necessary to periodically monitor the state of the Azure logical server. The **Azure Database Server Details** test helps you in this regard!

For each Azure SQL Database logical server being monitored, this test reports the current state of the server and the number of Azure SQL databases associated with the logical server. In addition, this test reports the number of Database Transaction Units allocated to the SQL databases associated with the logical server and the maximum number of DTUs that can be allocated to the SQL databases.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each *Subscription ID: Resource Group: Azure SQL Database logical server* of the target Microsoft Azure being monitored

Descriptor: Azure SQL Database logical server

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameters	Description
	• The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures made by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>State</td><td>Indicates the current status of this Azure SQL Database logical server.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Ready</td><td>1</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of this database instance. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 or 1.
The detailed diagnosis of this measure if enabled, lists the location of the database instance, the version of the SQL installed and the Fully Qualified Domain Name of the server.</td></tr>
<tr><td>Number of databases</td><td>Indicates the number of databases instances associated with this Azure SQL Database logical server.</td><td>Number</td><td>The detailed diagnosis of this measure lists the name of the database instances created on the database server.</td></tr>
<tr><td>Current DTUs</td><td>Indicates the number of</td><td>Number</td><td>For a single Azure SQL database at a</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	Database Transaction Units allocated to the database instances associated with this Azure SQL Database logical server.		specific performance level within a service tier, Microsoft guarantees a certain level of resources for that database (independent of any other database in the Azure cloud) and providing a predictable level of performance. This amount of resources is calculated as a number of Database Transaction Units or DTUs, and is a blended measure of CPU, memory, I/O (data and transaction log I/O).
Maximum DTUs	Indicates the maximum number of Database Transactions Units that can be allocated to the database instances associated with this Azure SQL Database logical server.	Number	

3.3.3 Azure Database (classic) Test

Microsoft Windows Azure SQL Database is similar to an on-premise Microsoft SQL Server and extends the SQL Server database capability to the cloud. Azure SQL Database lets you provision and deploy relational database solutions to the cloud, including many benefits such as, rapid provisioning, scalable, high availability and minimal maintenance overhead.

Maintaining Azure SQL database on the cloud is easy to manage, with less effort, because of the complete infrastructure provided by Microsoft System Center. Though the Azure SQL database can be easily managed, it is also essential to keep track on the day-to-day performance of the Azure SQL database. To achieve this, administrators may use the **Azure Database (classic)** test.

For each Azure SQL database instance, this test reports the current state and also the resource utilization. Using this test, administrators can identify the Azure SQL database that is improperly sized with CPU, memory and I/O resources.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each Azure SQL Database instance of the target Microsoft Azure being monitored

Descriptor: Azure SQL Database instance

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **DATABASE NAME -** Specify the name of the database to which the target Microsoft Azure is connected to.
8. **USERNAME -** Specify the name of the user who is authorized to access the database to which the target Microsoft Azure is connected to.
9. **PASSWORD -** Specify the password corresponding to the *USERNAME* here.

10. **CONFIRM PASSWORD -** Confirm the password by retyping it here.

11. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.

12. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability.
    - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this database instance.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Created</td><td>1</td></tr>
<tr><td>Limited</td><td>2</td></tr>
<tr><td>Offline</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current status of this database instance. The graph of this measure however, represents the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			status of a server using the numeric equivalents only - 0 to 2. The detailed diagnosis of this measure if enabled, lists the Server name on which the database instance is hosted, the location of the server, status of the server and the current edition of the server.
Total size	Indicates the maximum size allocated to this database instance.	MB	
Used size:	Indicates the amount of space that is already utilized in this database instance.	MB	If the value of this measure is close to the Total size measure, then it indicates that the database instance is running short of space. Administrators should either clean the database or provide additional resources.
Free size	Indicates the amount of space that is available for use in this database instance.	MB	A high value is desired for this measure.
Storage utilization	Indicates the percentage of space utilized in this database instance.	Percent	A value close to 100 for this measure denotes that the database instance is running short of space.
CPU utilization	Indicates the average percentage of CPU utilized by the service of this database instance.	Percent	
Avg physical data reads utilization	Indicates the percentage of physical data that is read from this database instance.	Percent	
Avg log writes utilization	Indicates the percentage of logs written to this database instance.	Percent	

Measurement	Description	Measurement Unit	Interpretation
Avg memory utilization	Indicates the percentage of memory utilized by this database instance.	Percent	A high value for this measure is a cause of concern, If the value of this measure is close to 100, then administrators should either increase the memory limit of the database or free up the available resources.
Successful connections	Indicates the number of successful connections to this database instance.	Number	
Failed connections:	Indicates the number of connections that failed to establish on this database instance.	Number	
Terminated connections	Indicates the number of connections that were terminated on this database instance.	Number	
Deadlock connections	Indicates the number of connections that experienced deadlock on this database instance.	Number	Ideally, the value of this measure should be zero. If a sudden/gradual increase in the value of this measure is noticed, then administrators should query the database to identify when exactly the deadlocks occurred.
Throttled connections	Indicates the number of connections that were throttled on this database instance.	Number	Throttling is a mechanism used by Azure SQL Database to prevent the server from becoming overloaded and unresponsive. It ensures that all users receive an appropriate share of resources and that no one monopolizes resources; Azure SQL Database may close or "throttle" subscriber connections under certain conditions. Too many connections that were throttled may often lead to performance bottleneck. Therefore, the value of this measure should be zero.
Throttling long	Indicates the number of	Number	A low value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
transaction	long running transactions on this database instance.		A sudden/gradual increase in the value of this measure may decrease the performance of the database as the database locks will be retained by the transactions.

3.3.4 Azure Database Status (classic) Test

This test enables administrators to determine how many Azure databases were registered with the Azure cloud and how many are currently powered on/powered off. In addition, this test helps administrators to determine how many Azure databases were currently added and how many databases were removed. Using this test, administrators can instantly identify the powered off databases i.e., unavailable databases and start investigating the exact reason behind the powered off status of the databases.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH** - In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft

Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

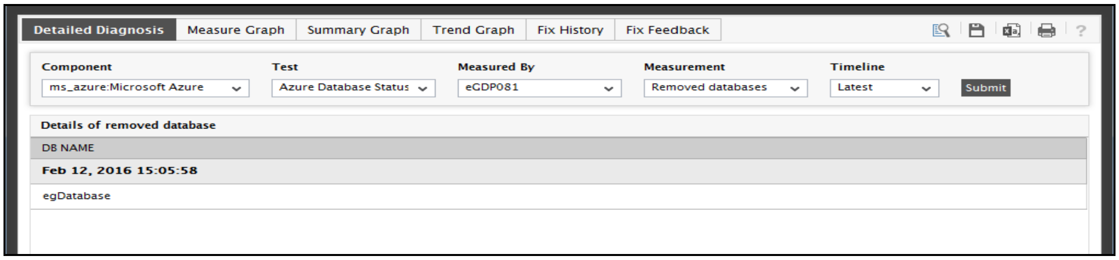
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test

Measurement	Description	Measurement Unit	Interpretation
Registered databases	Indicates the number of database instances registered on the Azure cloud.	Number	The detailed diagnosis of this measure if enabled, lists the database instances that were recently registered.
Powered on	Indicates the number of	Number	The detailed diagnosis of this measure

Measurement	Description	Measurement Unit	Interpretation
databases	database instances that are currently powered-on on the Azure cloud.		if enabled, lists the database instances that were powered on recently.
Powered off databases	Indicates the number of database instances that are currently powered off on the Azure cloud.	Number	The detailed diagnosis of this measure if enabled, lists the database instances that were powered off recently.
Added databases	Indicates the number of database instances that were added during the last measurement period.	Number	The detailed diagnosis of this measure if enabled, lists the database instances that were recently added.
Removed databases	Indicates the number of database instances that were removed from the Azure cloud during the last measurement period.	Number	The detailed diagnosis of this measure if enabled, lists the database instances that were removed recently.

The detailed diagnosis of the *Removed databases* measure if enabled, lists the databases that were removed from the Azure cloud as shown in Figure 3.8.



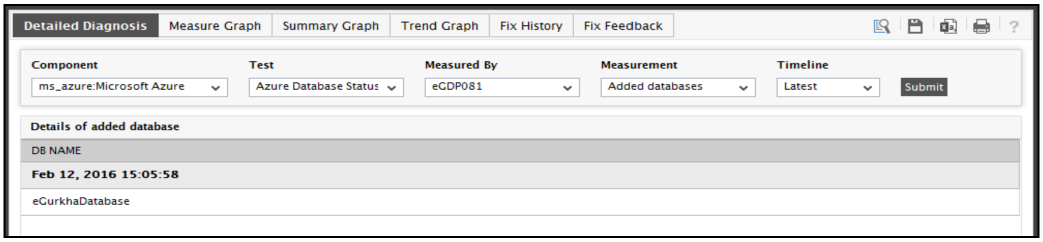
Component: ms_azure:Microsoft Azure
Test: Azure Database Status
Measured By: eGDP081
Measurement: Removed databases
Timeline: Latest

Details of removed database

DB NAME
Feb 12, 2016 15:05:58
egDatabase

Figure 3.8: The detailed diagnosis of the Removed databases measure

The detailed diagnosis of the *Added databases* measure lists the databases that were added to the Azure cloud as shown in Figure 3.9.



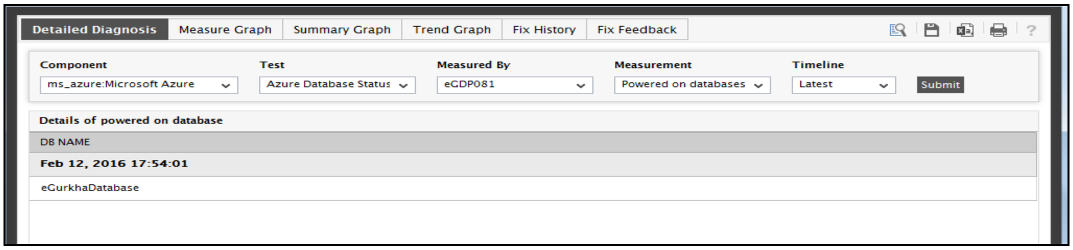
Component: ms_azure:Microsoft Azure
Test: Azure Database Status
Measured By: eGDP081
Measurement: Added databases
Timeline: Latest

Details of added database

DB NAME
Feb 12, 2016 15:05:58
eGurkhaDatabase

Figure 3.9: The detailed diagnosis of the Added databases measure

The detailed diagnosis of the *Powered on databases* measure(see Figure 3.10) lists the databases that were powered on on the Azure cloud.



Component	Test	Measured By	Measurement	Timeline
ms_azure:Microsoft Azure	Azure Database Status	eGDP081	Powered on databases	Latest

Details of powered on database

DB NAME
Feb 12, 2016 17:54:01
eGurkhaDatabase

Figure 3.10: The detailed diagnosis of the Powered on databases measure

3.3.5 Azure Database Firewall (classic) Test

This test reports the current state of each firewall rule applied on the Azure SQL database of the target Azure cloud. Using this test, administrators can figure out if their database is safe or prone to vulnerabilities.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each firewall rule set on the Azure SQL database of the target Microsoft Azure being monitored

First-level descriptor: Azure SQL Database

Second-level descriptor: Firewall rule

1. **TEST PERIOD -** How often should the test be executed
2. **HOST–** The host for which the test is being configured
3. **SUBSCRIPTION ID-** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a

management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD** - Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of this firewall rule applied on this Azure SQL Database.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Limited</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the firewall rule applied on he Azure SQL Database. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 2.</td></tr>
</table>

3.3.6 Azure Storage (classic) Test

Microsoft Azure Storage is developed to enable new scenarios for applications requiring scalable, durable, and highly available storage for their data. Azure Storage is massively scalable, so you can store and process hundreds of terabytes of data to support the big data scenarios required by scientific, financial analysis, and media applications. Azure Storage is currently designed to store tens of trillions of unique customer objects, and handles millions of requests per second on average. Azure Storage is elastic, so you can design applications for a large global audience, and scale those applications as needed - both in terms of the amount of data stored and the number of requests made against it. Azure Storage uses an auto-partitioning system that automatically load-balances your data based on traffic. This means that as the demands on your application grow, Azure Storage automatically allocates the appropriate resources to meet them. Azure Storage is accessible from anywhere in the world, from any type of application, whether it's running in the cloud, on the desktop, on an on-premises server, or on a mobile or tablet device. An Azure storage account is a secure account that gives you access to services in Azure Storage. For a single subscription, you can create upto 100 uniquely named storage accounts.

Azure Storage also supports redundancy so that high read availability of data within the storage can be achieved. There are three different redundancy options available to the users namely:

- **Locally Redundant Storage (LRS)**: All data in the storage account is made durable by replicating transactions synchronously to three different storage nodes within the same region.
- **Geo Redundant Storage (GRS)**: This is the default option for redundancy when a storage account is created. Like LRS, transactions are replicated synchronously to three storage nodes within the primary region chosen for creating the storage account. However, the transaction is also queued for asynchronous replication to another secondary region (hundreds of miles away from the primary) where data is again made durable by replicating it to three more storage nodes there.
- **Read Access - Geo Redundant Storage (RA-GRS)**: For a GRS storage account, the ability to turn on read only access to a storage account's data in the secondary region has been introduced in limited preview. Since replication to the secondary region is done asynchronously, this provides an eventual consistent version of the data to read from.

If the Azure storage account/Azure Storage is taken offline or is not accessible even for a few minutes, then millions of user requests may not be serviced causing hardship to the users. To avoid such discrepancies, you need to figure out the current state of the storage account and if the storage account supports redundancy, then you may need to figure out the status of the primary as well as the secondary regions. The **Azure Storage (classic)** Test helps you exactly in this regard!

For each storage account in the Azure storage, this test helps administrators to figure out the whether the storage account is online or offline. If the storage account is online, then administrators can figure out the current status of the storage account. In addition, if the storage account is redundant across regions, then you can figure out the status of the primary region as well as the secondary region.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each storage account on the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH** - In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.

8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Current status</td><td>Indicates the current state of this storage account.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Creating</td><td>1</td></tr>
<tr><td>Created</td><td>2</td></tr>
<tr><td>Deleting</td><td>3</td></tr>
<tr><td>Deleted</td><td>4</td></tr>
<tr><td>Changing</td><td>5</td></tr>
<tr><td>Resolving DNS</td><td>6</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Measure Values listed in the table above to indicate the current state of this storage account. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 6.</td></tr>
<tr><td>Primary status</td><td>Indicates the availability of the primary storage region in this storage account.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Available</td><td>1</td></tr>
<tr><td>Created</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the primary storage region in this storage account. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>Secondary status</td><td>Indicates the availability of the secondary storage region in this storage account.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Available</td><td>1</td></tr>
<tr><td>Created</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>above to indicate the secondary storage region in this storage account. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>Status</td><td>Indicates whether this storage account is online or offline.</td><td></td><td>This measure will report Online if the Current Status measure reports a value Created, Primary Status and Secondary Status values are Available.
The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Online</td><td>1</td></tr><tr><td>Offline</td><td>2</td></tr></table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate whether this storage account is online or offline. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 2.</td></tr>
</table>

3.3.7 Azure Storage Performance (classic) Test

Azure Storage provides the flexibility and hyper-scale needed to store and retrieve large amounts of data. The Azure storage stores all information relating to the Azure websites, cloud services, virtual machines etc and ensures prompt availability of data. If the Azure storage is unavailable or is error-prone too often, then the Azure cloud will not be accessible by the users causing inconvenience to them. Therefore it is essential to monitor the Azure storage and the **Azure Storage Performance (classic)** test helps administrators exactly in this regard!

This test monitors the Azure storage accounts in the target Azure cloud and reports the availability of the storage. In addition, this test helps administrators to figure out the error-prone storage accounts and the errors encountered by the storage accounts. Using this test, administrators can also figure out the latencies of the storage accounts to process the requests.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each storage account on the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **METRICS TABLE NAME** - All metrics data for each of the storage services is stored in three tables reserved for the storage service: one table for hourly transaction information, one table for minute transaction information, and another table for capacity information. Transaction and minute transaction information consists of request and response data, and capacity information consists of storage usage data. To extract metrics related to the performance of the storage in the target Microsoft Azure cloud, the eG agent queries the *$MetricsHourPrimaryTransactionsTable* table. By default, specify none against this parameter. If the Microsoft Azure cloud administrators have changed the locations of the *$MetricsHourPrimaryTransactionsTable* table or if the data in the table is stored elsewhere, then provide the name of such table in this text box.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Availability	Indicates the availability of this storage, in percent.	Percent	
Total requests	Indicates the total number of requests made to this storage.	Number	
Total ingress	Indicates the amount of ingress data in this storage.	MB	The value of this measure includes the ingress from an external client to the Azure as well as ingress within Azure.
Total egress	Indicates the amount of egress data in this storage.	MB	The value of this measure includes the egress from an external client to the Azure as well as egress within Azure.
Total billable requests	Indicates the number of billable requests received by this storage.	Number	Every request made to an account's storage service is either billable or non-billable. Storage Analytics logs each individual request made to a service, including a status message that indicates how the request was handled. Similarly, Storage Analytics stores metrics for both a service and the API operations of that service, including the percentages and count of certain status messages. Together, these features can help you analyze your billable requests, make improvements on your application,

Measurement	Description	Measurement Unit	Interpretation
			and diagnose issues with requests to your services.
Avg E2E latency	Indicates the average end to end latency of successful requests made to this storage.	msecs	A low value is desired for this measure.
Avg server latency	Indicates the average latency used by this storage to process a successful request.	msecs	A low value is desired for this measure.
Successful requests percent	Indicates the percentage of successful requests made to this storage.	Percent	Ideally, the value of this measure should be high.
Successful requests	Indicates the number of successful requests made to this storage.	Number	A high value is desired for this measure.
Throttling error percent	Indicates the percentage of requests made to this storage that failed with throttling errors.	Percent	Ideally, the value of this measure should be zero.
Timeout error	Indicates the percentage of requests made to this storage that failed with timeout errors.	Percent	Ideally, the value of this measure should be zero.
Server other error percent	Indicates the percentage of requests made to this storage that failed with status code 500.	Percent	Internal Server Error where the storage error code is not Timeout. Ideally, the value of this measure should be zero.
Client other error percent	Indicates the percentage of requests made to this storage that failed with errors such as NotFound, Precondition Failed etc.	Percent	Most 3XX and 4XX failures fall under this category. Ideally, the value of this measure should be zero.
Authorization error percent:	Indicates the percentage of requests made to this	Percent	Ideally, the value of this measure should be zero.

Measurement	Description	Measurement Unit	Interpretation
	storage that failed with authorization errors.		
Network error percent	Indicates the percentage of requests made to this storage that failed with network errors.	Percent	Ideally, the value of this measure should be zero.
Successful anonymous requests	Indicates the number of anonymous requests that were successfully made to this storage.	Number	These will also include all conditional GET requests that did not return because the condition did not succeed. These are billable requests and counted for availability.
Successful SAS requests	Indicates the number of successful shared access signature requests made to this storage.	Number	These will also include all conditional GET requests that did not return because the condition did not succeed. These are billable requests and counted for availability.
Throttling error	Indicates the number of authenticated requests that returned ServerBusy status i.e., that returned status code 503.	Number	These are not billable and are not counted for availability. Ideally, the value of this measure should be zero.
Anonymous throttling error	Indicates the number of anonymous requests that returned ServerBusy status i.e., that returned status code 503.	Number	These are not billable and are not counted for availability. Ideally, the value of this measure should be zero.
SAS throttling error	Indicates the number of Shared Access Signature requests that returned ServerBusy status i.e., that returned status code 503.	Number	These are not billable and are not counted for availability. Ideally, the value of this measure should be zero.
Client timeout error	Indicates the total number of authenticated requests that timed out.	Number	These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”.

Measurement	Description	Measurement Unit	Interpretation
			This happens when timeout value provided is not sufficient for the IO over the network. For example, if the read/write/etc. request completes in the expected time on the server but it takes a long time to return to the client due to network latency, this is considered as a client timeout. Any other timeout will be deemed as ServerTimeout. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Anonymous client timeout error	Indicates the number of anonymous errors that timed out.	Number	These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”. This happens when timeout value provided is not sufficient for the IO of the network. For example, if the read/write/etc. request completes in the expected time on the server but it takes a long time to return to the client due to network latency, this is considered as a client timeout. Any other timeout will be deemed as AnonymousServerTimeout. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
SAS client timeout error	Indicates the number of Shared Access Signature requests that timed out.	Number	These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”. This happens when timeout value

Measurement	Description	Measurement Unit	Interpretation
			provided is not sufficient for the IO of the network. For example, if the read/write/etc. request completes in the expected time on the server but it takes a long time to return to the client due to network latency, this is considered as a client timeout. Any other timeout will be deemed as SASServerTimeout. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Server timeout error	Indicates the total number of authenticated requests that timed out.	Number	The requests may time out due to the storage service taking too long to respond to the request. The time taken by service excludes the time to read/write from/to client over the network. These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”. These are not billable requests and counted against availability. Ideally, the value of this measure should be zero.
Anonymous server timeout error	Indicates the total number of anonymous requests that timed out.	Number	The requests may time out due to the storage service taking too long to respond to the request. The time taken by service excludes the time to read/write from/to client over the network. These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”.

Measurement	Description	Measurement Unit	Interpretation
			These are not billable requests and counted against availability. Ideally, the value of this measure should be zero.
SAS server timeout error	Indicates the total number of Shared Access Signature requests that timed out.	Number	The requests may time out due to the storage service taking too long to respond to the request. The time taken by service excludes the time to read/write from/to client over the network. These are seen as timeout errors or Http Status code 500 with Storage error code as “Timeout”. These are not billable requests and counted against availability. Ideally, the value of this measure should be zero.
Client other error	Indicates the number of authenticated requests that failed as expected.	Number	The requests may be expected to fail when the resources already exits or when the resources fail. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
SAS client other error:	Indicates the number of Shared Access Signature requests that failed as expected.	Number	The requests may be expected to fail when the resources already exits or when the resources fail. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Anonymous client other error:	Indicates the number of anonymous requests that failed precondition	Number	These are billable requests and counted for availability. Ideally, the value of this measure should

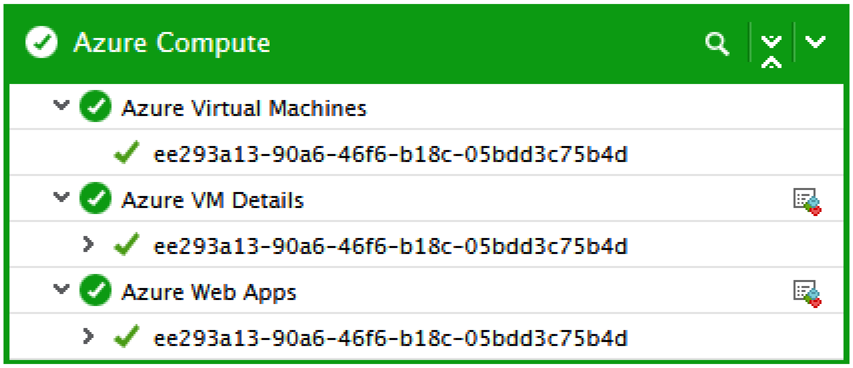
Measurement	Description	Measurement Unit	Interpretation
	checks.		be zero.
Server other error	Indicates the total number of authenticated requests that failed due to unknown server errors.	Number	These are typically Http Status code 500 with Storage error code other than Timeout. These are not billable requests and counted against availability. Ideally, the value of this measure should be zero.
Anonymous server other error	Indicates the total number of anonymous requests that failed due to unknown server errors.	Number	These are typically Http Status code 500 with Storage error code other than Timeout. These are not billable requests and counted against availability. Ideally, the value of this measure should be zero.
SAS server other error	Indicates the total number of Shared Access Signature requests that failed due to unknown server errors.	Number	These are typically Http Status code 500 with Storage error code other than Timeout. These are not billable requests and counted against availability.
Authorization error	Indicates the total number of authentication requests that failed due to authorization errors.	Number	A good example for such errors is write requests from users to logs under $logs. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Anonymous authorization error	Indicates the total number of anonymous requests that failed due to authorization errors.	Number	A good example of authentication error occurance is when only authenticated write requests are allowed against all write requests in the storage. These are billable requests and counted for availability.
SAS authorization	Indicates the number of	Number	Example: write requests using SAS

Measurement	Description	Measurement Unit	Interpretation
error	Shared Access Signature requests that failed due to authorization errors.		when only read access was provided Authorization error. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Network error	Indicates the number of authenticated requests that failed due to network errors.	Number	Network errors occur when a user prematurely closes the connection before the timeout expires or if there are problems in any of the intermediate switches. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Anonymous network error	Indicates the number of anonymous requests that failed due to network errors.	Number	Network errors occur when a user prematurely closes the connection before the timeout expires or if there are problems in any of the intermediate switches. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
SAS network error	Indicates the number of Shared Access Signature requests that failed due to network errors.	Number	Network errors occur when a user prematurely closes the connection before the timeout expires or if there are problems in any of the intermediate switches. These are billable requests and counted for availability. Ideally, the value of this measure should be zero.
Ingress bandwidth	Indicates the amount of	MBs	

Measurement	Description	Measurement Unit	Interpretation
	bandwidth utilized for transferring ingress data requests per second to this storage.		
Egress bandwidth	Indicates the amount of egress data utilized per second in this storage.	MBs	

3.4 Azure Compute Layer

This layer depicts the status of each cloud service, virtual machine and Azure website hosted on the Azure cloud. This layer also helps administrators to figure out the websites that are over-utilizing the resources allocated to them. In addition, this layer also throws light on the logs and log tables that store information related to various events triggered on the cloud.



Azure Compute
Azure Virtual Machines
ee293a13-90a6-46f6-b18c-05bdd3c75b4d
Azure VM Details
ee293a13-90a6-46f6-b18c-05bdd3c75b4d
Azure Web Apps
ee293a13-90a6-46f6-b18c-05bdd3c75b4d

Figure 3.11: The Azure Compute layer

The following sections provide more information on these tests and the measures reported by them.

3.4.1 Azure Virtual Machines Test

Azure Virtual Machines is one of several types of on-demand, scalable computing resources that Azure offers. An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the virtual machine.

Azure Virtual Machines lets you create and use virtual machines in the cloud. Providing what's known as Infrastructure as a Service (IaaS), virtual machine technology can be used in variety of ways. Some examples are:

Virtual machines (VMs) for development and test. Development groups commonly use VMs because they offer a quick, easy way to create a computer with specific configurations required to code and test an application. Azure Virtual Machines provides a straightforward and economical way to create these VMs, use them, then delete them when they're no longer needed.

Running applications in the cloud. It makes economic sense to run some applications in the public cloud. One example is an application that has large spikes in demand. Although you could equip your own data center with enough hardware to handle peak demand, that hardware might be underutilized much of the time. Running this application on Azure lets you pay for extra VMs only when you need them and shut them down when you don't. Or, suppose you're a start-up that needs on-demand computing resources quickly and with no commitment. Once again, Azure can be the right choice.

Extending your own datacenter into the public cloud. When you use Azure Virtual Network, your organization can create a virtual network (VNET) that's an extension of your own on-premises network and add VMs to that VNET. This allows running applications such as SharePoint, SQL Server and others on an Azure VM. This approach might be easier to deploy or less expensive than running them in VMs your own datacenter.

Disaster recovery. Rather than paying continuously for a backup datacenter that's rarely used, IaaS-based disaster recovery lets you pay for the computing resources you need only when you really need them. For example, if your primary datacenter goes down, you can create VMs running on Azure to run essential applications, then shut them down when they're no longer needed.

When multiple virtual machines are deployed through the Azure Resource Manager on the Azure cloud, administrators may often want to closely monitor the count of the VMs that are registered on the cloud and the VMs that were removed from the cloud. The Azure Virtual Machines test helps administrators in this regard.

This test auto-discovers the Azure subscriptions in a virtual environment and for each subscription, this test monitors the VMs that were deployed through the Azure Resource Manager and reports the numerical statistics of the VMs that were registered, added, removed, powered on and powered off etc.

Note:

The metrics of this test does not include the count of the virtual machines deployed using the Azure classic mode.

Target of the Test : Microsoft Azure

Agent deploying the test : A remote agent

Output of the test: One set of results for each subscription subscribed on the target Microsoft Azure being monitored

First level Descriptor: Subscription ID

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Registered VMs	Indicates the number of virtual machines that were currently registered	Number	The detailed diagnosis of this measure if enabled, lists the names of the virtual machines, the location of the virtual

Measurement	Description	Measurement Unit	Interpretation
	on this cloud.		machine, the Public IP address, the Internal IP address and the Operating system of the virtual machine.
Poweredon VMs	Indicates the number of virtual machines that are currently powered on.	Number	The detailed diagnosis of this measure lists the name of the virtual machine, the location of the virtual machine, the Public IP address, the Internal IP address and the Operating system of the virtual machine.
Poweredoff VMs	Indicates the number of virtual machines that are currently powered off.	Number	The detailed diagnosis of this measure lists the name of the virtual machine, the location of the virtual machine, the Public IP address, the Internal IP address and the Operating system of the virtual machine.
Added VMs	Indicates the number of virtual machines that were newly added to the cloud during the last measurement period	Number	The detailed diagnosis of this measure lists the name of the virtual machine, the location of the virtual machine and the Operating system of the virtual machine.
Removed VMs	Indicates the number of virtual machines that were removed from the cloud during the last measurement period.	Number	The detailed diagnosis of this measure lists the name of the virtual machine, the location of the virtual machine and the Operating system of the virtual machine.
Other VMs	Indicates the number of virtual machines that were in disconnected or invalid or inaccessible state during the last measurement period.	Number	The detailed diagnosis of this measure lists the name of the virtual machine, the state of the virtual machine and the location of the virtual machine.

3.4.2 Azure VM Details Test

This test auto-discovers the virtual machines on the target Microsoft Azure, and for each VM, it reveals in-depth metrics such as status, memory utilization, CPU utilization, disk I/O measures, etc.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each Subscription: Resource Group: VM on the target Microsoft Azure being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Tenant ID	Specify the Directory ID of the Azure Active Directory that is associated with the subscription of the target Microsoft Azure. To know how to determine the Directory ID, refer to Section **2.1**.
Client ID and Client Password	The eG agent communicates with the target Microsoft Azure using JAVA API calls. To collect the required metrics, the eG agent requires an Access token in the form of an Application ID and the client secret value. To know more about determining the Application ID and the key refer to Section **2.1.1**. Specify the Application ID of the created Web Application in the Client ID text box and the client secret value in the Client Password text box.
Diagnostic Measures	
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of this virtual machine.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Provisioning succeeded</td><td>1</td></tr>
<tr><td>Running</td><td>2</td></tr>
<tr><td>Updating</td><td>3</td></tr>
<tr><td>Deallocating</td><td>4</td></tr>
<tr><td>Starting</td><td>5</td></tr>
<tr><td>Stopped</td><td>6</td></tr>
<tr><td>Deallocated</td><td>7</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current state of this virtual machine. The graph of this measure however, is represented using the numeric equivalents only - 1 to 7.</td></tr>
<tr><td>Provisioning status</td><td>Indicates provisioning status of this virtual machine.</td><td>Number</td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Succeeded</td><td>1</td></tr>
<tr><td>Updating</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			above to indicate the current state of this virtual machine. The graph of this measure however, is represented using the numeric equivalents only - 1 or 2.
Total cores	Indicates the total number of cores in this virtual machine.	Number	
Configured memory	Indicates the amount of memory that is configured for this VM.	GB	
Maximum disk size	Indicates the maximum size of the disk allocated to this VM.	GB	
Temporary disk size	Indicates the size of the 'temporary disk' allocated to this VM.	GB	
Maximum data disk	Indicates the maximum number of the 'Data disks' attached to this VM.	Number	
Maximum IOPS	Indicates the maximum number of I/O operations that are allowed for this VM.	Number	
CPU utilization	Indicates the percentage of CPU utilized by this VM.	Percent	
Network in	Indicates the amount of data received by this VM through all network interfaces.	MB	
Network out	Indicates the amount of data sent out through all the network interfaces by this VM.	MB	
Disk read data	Indicates the amount of	MB	

Measurement	Description	Measurement Unit	Interpretation
	data read from the disk of this VM during the last measurement period.		
Disk write data	Indicates the amount of data written to the disk of this VM during the last measurement period.	MB	
Disk read operation	Indicates the rate at which data was read from the disk of this VM during the last measurement period.	Operations/sec	
Disk write operation	Indicates the rate at which data was written from the disk of this VM during the last measurement period.	Operations/sec	
Total IOPS	Indicates the total number of I/O Operations per second on this VM.	Number	
Interrupt time	Indicates the percentage of time that the processor of this VM spent receiving and servicing hardware interrupts during the last measurement period.	Percentage	The value of this measure is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards, and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended during interrupts. Most system clocks interrupt the processor every 10 milliseconds, creating a background of interrupt activity.
Processor time	Indicates the percentage of time that the processor of this VM is executing application or operating system processes other	Percentage	The value of this measure is a primary indicator of processor activity. It is calculated by measuring the time that the processor spends executing the thread of the Idle process in each

Measurement	Description	Measurement Unit	Interpretation
	than Idle threads.		sample interval, and subtracting that value from 100%. Each processor has an Idle thread which consumes cycles when no other threads are ready to run.
User time	Indicates the percentage of non-idle processor time that is spent in user mode by the processor of this VM.	Percentage	User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. The alternative, privileged mode, is designed for operating system components and allows direct access to hardware and all memory. The operating system switches application threads to privileged mode to obtain operating system services.
Privileged time	Indicates the percentage of non-idle processor time spent in privileged mode by the processor of this VM.	Percentage	Privileged mode is a processing mode designed for operating system components and hardware-manipulating drivers. It allows direct access to hardware and all memory. The alternative, user mode, is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. The operating system switches application threads to privileged mode to obtain operating system services. % Privileged Time includes time spent servicing interrupts and DPCs. A high rate of privileged time might be attributable to a large number of interrupts generated by a failing device.
Processor frequency	Indicates the frequency at which the processor of this VM operates.	Number	
Parking status	Indicates the number of CPU cores that were	Number	

Measurement	Description	Measurement Unit	Interpretation
	parked for the processor of this VM.		
Page Faults	Indicates the rate at which page faults by the threads executing in this process of this VM are occurring.	Faults/sec	A page fault occurs when a thread refers to a virtual memory page that is not in its working set in main memory. This does not cause the page to be fetched from disk if it is on the standby list and hence already in main memory, or if it is in use by another process with whom the page is shared.
Handle in use	Indicates the number of handles that are currently utilized by the processor of this VM.	Number	
Private bytes	Indicates the amount of data bytes that the processes of the processor associated with this VM has allocated that cannot be shared with other processes.	MB	
Working set	Indicates the current number of bytes in the working set of the processes of the processor of this VM.	Number	The working set is the set of memory pages touched recently by the threads in the process. If free memory in the VM is above a certain threshold, pages are left in the working set of a process even if they are not in use. When free memory falls below a certain threshold, pages are trimmed from working sets. If they are needed, they are then soft-faulted back into the working set before they leave main memory.
Working set - private	Indicates the number of bytes in the working set that are not shared and cannot be shared by other	Number	

Measurement	Description	Measurement Unit	Interpretation
	processes of the processor of this VM.		
Processes	Indicates the number of system processes in this VM at the time of data collection.	Number	
Threads	Indicates the number of system threads in this VM at the time of data collection.	Number	
Context switches	Indicates the rate at which context switches occurred on this VM.	Switches/sec	A context switch occurs when the kernel switches the processor from one thread to another. A context switch might also occur when a thread with a higher priority than the running thread becomes ready or when a running thread must wait for some reason (such as an I/O operation). The Thread\Context Switches/sec counter value increases when the thread gets or loses the time of the processor.
Available bytes	Indicates the amount of physical memory, in bytes, that is immediately available for allocation to a process or for use by this VM.	MB	
Committed bytes in use	Indicates the amount of physical memory that is in use for which space has been reserved in the paging file so that it can be written to disk allocated to this VM.	MB	
Cache faults	Indicates the rate at which faults occur when a page sought in the file system	Faults/sec	

Measurement	Description	Measurement Unit	Interpretation
	cache is not found and must be retrieved from elsewhere in memory (a soft fault) or from disk (a hard fault) of this VM.		
Page reads	Indicates the rate at which the disk of this VM was read to resolve hard page faults.	Pages/sec	Hard page faults occur when a process references a page in virtual memory that is not in its working set or elsewhere in physical memory, and must be retrieved from disk. This measure is a primary indicator of the kinds of faults that cause system-wide delays. It includes read operations to satisfy faults in the file system cache (usually requested by applications) and in noncached mapped memory files. Compare the value of Page Reads/sec to the value of Pages Input/sec to find an average of how many pages were read during each read operation.
Pages read and written to disk	Indicates the rate at which pages are read from or written to disk of this VM to resolve hard page faults.	Pages/sec	
Memory paged pool size	Indicates the size of the paged pool which is an area of system memory (physical memory) for objects that can be written to disk of this VM when they are not being used.	MB	
Non- paged pool kernel memory size	Indicates the size of the nonpaged pool which is an area of system memory (physical memory) for objects that cannot be written to disk of this VM, but must remain in physical	MB	

Measurement	Description	Measurement Unit	Interpretation
	memory as long as they are allocated.		
Committed bytes	Indicates the amount of committed virtual memory allocated to this VM.	MB	
Page Faults	Indicates the average number of pages faulted per second.	Faults/sec	
Transition faults	Indicates the rate at which page faults are resolved by recovering pages that were being used by another process sharing the page, or were on the modified page list or the standby list, or were being written to disk of this VM at the time of the page fault.	Faults/sec	
Disk read bytes	Indicates the amount of data read from the disk of this VM.	MB	
Disk write bytes	Indicates the amount of data written to the disk of this VM.	MB	
Connection failures	Indicates the number of times the TCP connection to this VM failed.	Number	This measure is calculated based on the number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state along with the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Segments sent	Indicates the rate at which TCP Segments were sent from this VM.	Segments/sec	The value of this measure includes those segemtns sent from current connections, but excludes those containing only retransmitted bytes.

Measurement	Description	Measurement Unit	Interpretation
Segments retransmitted	Indicates the rate at which segments containing one or more previously transmitted bytes were retransmitted by this VM.	Segments/sec	
Connections reset	Indicates the number of times that TCP connections from this VM have made a direct transition to the CLOSED state from either the ESTABLISHED or CLOSE-WAIT state.	Number	
Segments received	Indicates the rate at which segments were received by this VM, including those received in error.	Segments/sec	The value of this measure includes segments received on currently established connections.
Connections established	Indicates the number of TCP connections established on this VM.	Number	

3.4.3 Azure Web Access Test

The details of the Azure Web Access test that emulates a user accessing the Microsoft Azure cloud are provided below. Since this test can be executed from a location external to the Microsoft Azure, this test presents an unbiased external perspective of the state of the Microsoft Azure cloud.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for every URL being monitored

First-level descriptor: URL available in the target Microsoft Azure

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured

3. **PORT**- The port to which the specified *HOST* listens
4. **URL** - This test emulates a user accessing a specific web site(s) on the target Azure cloud to determine the availability and responsiveness of the cloud. To enable this emulation, you need to configure the test with the URL of the web site that it should access. Specify this URL against the URL parameter. If required, you can even configure multiple URLs – one each for every web site that the test should attempt to access. If each URL configured requires special permissions for logging in, then, you need to configure the test with separate credentials for logging into every URL. Likewise, you need to provide instructions to the test on how to validate the content returned by every URL, and also set an encoding format for each URL. To enable administrators to easily configure the above per URL, eG Enterprise provides a special interface. To access this interface, click on the encircled '+' button alongside the URL text box in the test configuration page. Alternatively, you can even click on the encircled '+' button adjacent to the URL parameter in the test configuration page. To know how to use this special interface, refer to Section 2.2.1.1. of this document.
5. **COOKIEFILE** - Whether any cookies being returned by the web server need to be saved locally and returned with subsequent requests
6. **PROXYHOST** - The host on which a web proxy server is running (in case a proxy server is to be used)
7. **PROXYPORT** - The port number on which the web proxy server is listening
8. **PROXYUSERNAME** - The user name of the proxy server
9. **PROXYPASSWORD** - The password of the proxy server
10. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
11. **TIMEOUT** - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default *TIMEOUT* period is 30 seconds.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Web availability	Indicates whether the Azure cloud was able to respond successfully to the query made by the test.	Percent	Availability failures could be caused by several factors such as the web server process(es) being down, the web server being misconfigured, a network failure, etc. Temporary unavailability may also occur if the web server is overloaded. Availability is determined based on the response code returned by the server. A response code

Measurement	Description	Measurement Unit	Interpretation
			between 200 to 300 indicates that the server is available.
Total response time	Indicates the time taken by the cloud to respond to the requests it receives.	Secs	Response time being high denotes a problem. Poor response times may be due to the server being overloaded or misconfigured. If the URL accessed involves the generation of dynamic content by the server, backend problems (e.g., an overload at the application server or a database failure) can also result in an increase in response time.
TCP connection availability	Indicates whether the test managed to establish a TCP connection to the cloud.	Percent	Failure to establish a TCP connection may imply that either the web server process is not up, or that the process is not operating correctly. In some cases of extreme overload, the failure to establish a TCP connection may be a transient condition. As the load subsides, the server may start functioning properly again.
TCP connect time	Quantifies the time for establishing a TCP connection to the web server host.	Secs	Typically, the TCP connection establishment must be very small (of the order of a few milliseconds). Since TCP connection establishment is handled at the OS-level, rather than by the application, an increase in this value signifies a system-level bottleneck on the host that supports the web server.
Server response time	Indicates the time period between when the connection was established and when the server sent back a HTTP response header to the client.	Secs	While the total response time may depend on several factors, the server response time is typically, a very good indicator of a server bottleneck (e.g., because all the available server threads or processes are in use).
Content validity	Validates whether the server was successful in executing the request	Percent	A value of 100% indicates that the content returned by the test is valid. A value of 0% indicates that the content may not be valid. This capability for content validation is

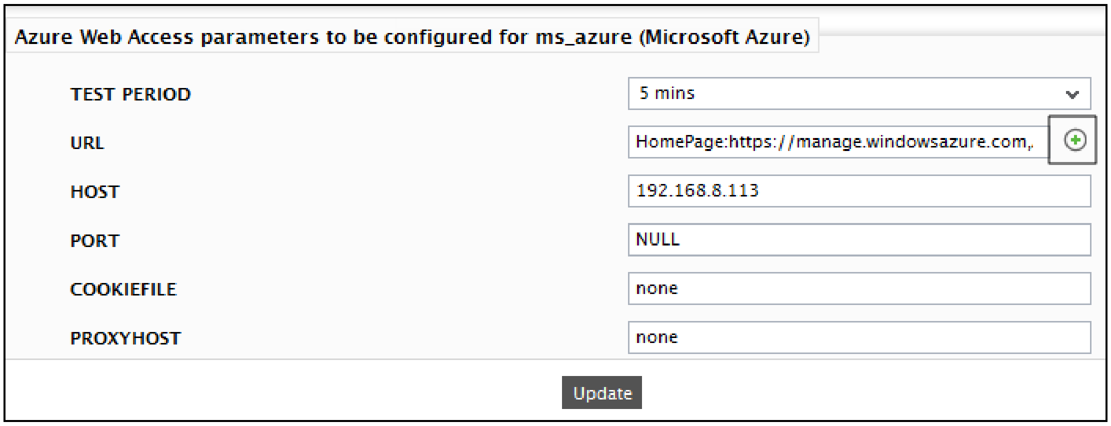
Measurement	Description	Measurement Unit	Interpretation
	made to it.		especially important for multi-tier web applications. For example, a user may not be able to login to the web site but the server may reply back with a valid HTML page where in the error message, say, "Invalid Login" is reported. In this case, the availability will be 100 % (since we got a valid HTML response). If the test is configured such that the content parameter should exclude the string "Invalid Login," in the above scenario content validity would have a value 0.
Response code	Indicates the response code returned by the server for the simulated request.	Number	A value between 200 and 300 indicates a good response. A 4xx value indicates a problem with the requested content (eg., page not found). A 5xx value indicates a server error.
Content length	Indicates the size of the content returned by the cloud.	Kbytes	Typically the content length returned by the server for a specific URL should be the same across time. Any change in this metric may indicate the need for further investigation on the server side.
Data transfer time	Indicates the time taken for a data transfer between the drive and the host system.	Secs	Data transfer time being high denotes a problem..
DNS availability	Indicates whether the DNS server was able to respond successfully to the request made to it.	Percent	While the value 100 for this measure indicates that the DNS server is available and successfully responded to the request, the value 0 indicates that the DNS server is unavailable or is not responding to requests. Availability failures could be caused by many reasons such as a network failure. Sometimes, the DNS server may be reachable through basic network testing, but may not respond to DNS queries from clients. **Note:**

Measurement	Description	Measurement Unit	Interpretation
			This measure will be able to report a value only if the URL parameter of the test is configured with a domain name-based URL – eg., http://www.eginnovations.com, http://www.eBooks.com. If the URL parameter is configured with an IP-based URL instead – eg., http://192.168.10.21:80, http://192.168.10.34:7077 – then, this measure will not report any value. This is because, to report the availability of the DNS server, the test attempts to connect to the DNS server and resolve the domain name in the URL to its IP address. If the test is able to perform domain name – IP address resolution successfully, it reports the value 100 for this measure. If the resolution fails, the test reports the value 0. In case of an IP-based URL naturally, the test will not be able to find any domain name to resolve. The test therefore will not report any value for this measure in that case.

3.4.3.1 Configuring URLs for Monitoring

By default, the Azure Web Access test will be configured with the URL of the home page of the target Azure cloud being monitored. To configure additional URLs, do the following:

1. Click on the encircled '+' button alongside the URL text box in Figure 3.12.

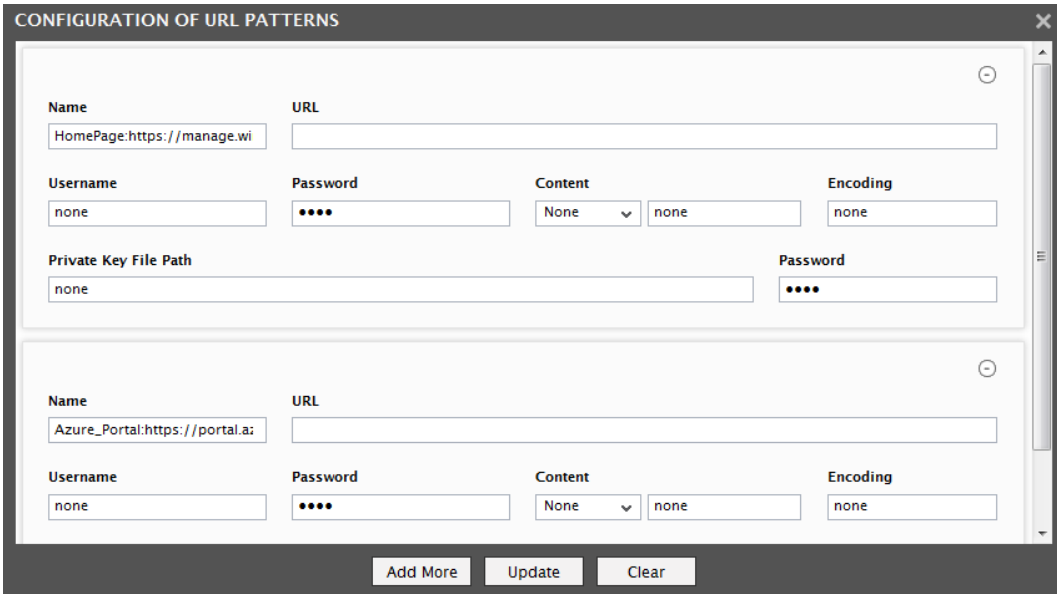


Azure Web Access parameters to be configured for ms_azure (Microsoft Azure)

TEST PERIOD	5 mins
URL	HomePage:https://manage.windowsazure.com,.
HOST	192.168.8.113
PORT	NULL
COOKIEFILE	none
PROXYHOST	none

Figure 3.12: Configuring the Azure Web Access test

2. Figure 3.13 then appears. To add another URL, click the Add More button in Figure 3.13.



CONFIGURATION OF URL PATTERNS

Name: HomePage:https://manage.wi
URL:
Username: none
Password: ••••
Content: None | none
Encoding: none
Private Key File Path: none
Password: ••••

Name: Azure_Portal:https://portal.az
URL:
Username: none
Password: ••••
Content: None | none
Encoding: none

Figure 3.13: Configuring multiple URLs

3. Another URL specification section will appear. Specify the following in that section:

- **Name:** Specify a unique name by which the URL you will be specifying shortly will be referred to across the eG user interface. This is the name that will appear as the descriptor of this test.
- **URL:** Enter the URL of the web page that this test should access.
- **Username** and **Password:** These parameters are to be set only if a specific user name / password has to be specified to login to the web page (i.e., **URL**) that you have configured for monitoring. In this case, provide valid login credentials using the **Username** and **Password** text boxes. If the web server on which **Azure Web Access** test executes supports 'Anonymous user access', then these parameters will take either of the following values:
  - A valid **Username** and **Password** for the configured **URL**
  - *none* in both the **Username** and **Password** text boxes of the configured **URL**, if no user authorization is required
  - Some web servers however, support NTLM (Integrated Windows) authentication, where valid login credentials are mandatory. In other words, a none specification will not be supported by such web servers. Therefore, in this case, against each configured **URL**,

you will have to provide a valid **Username** in the format: *domainname\username*, followed by a valid **Password**.

- Please be sure to check if your web site requires HTTP authentication while configuring this parameter. HTTP authentication typically involves a separate pop-up window when you try to access the page. Many sites use HTTP POST for obtaining the user name and password and validating the user login. In such cases, the username and password have to be provided as part of the POST information.

- **Content:** The **Content** parameter has to be configured with an instruction:value pair that will be used to validate the content being returned by the test. If the Content value is *None*, no validation is performed. On the other hand, if you pick the *Include* option from the **Content** list, it indicates to the test that for the content returned by the web server to be valid, the content must include the specified value (a simple string search is done in this case). This value should be specified in the adjacent text box. Similarly, if the *Exclude* option is chosen from the **Content** drop-down, it indicates to the test that the server's output is valid if it does not contain the value specified in the adjacent text box. The *Include* or *Exclude* value you specify in the text box can include wildcard characters. For example, an *Include* instruction can be **Home page**.

- **Encoding:** Sometimes the eG agent has to parse the **URL** content with specific encoding other than the default (ISO-8859-1) encoding. In such a case, specify the type of encoding using which the eG agent can parse the **URL** content in the **Encoding** text box. By default, this value is *none*.

- **Private Key File Path** and **Password:** SSL-enabled web sites are typically secured by a private key, public key, or a public-private key pair. If the web page configured for this test is SSL-enabled – i.e., if an HTTPS URL is specified against URL – and the contents of this web page can only be accessed using a private key, then the full path to the private key file will have to be provided against Private key file path and the password of the private key file should be specified against Password. If no such private key protects the contents of the configured URL, then set the Private key file path and its Password to *none*.

4. Similarly, you can add multiple URL specifications. To remove a URL specification, click on the encircled '-' button corresponding to it. To clear all URL specifications, click the **Clear** button in Figure 3.13. To update all the changes you made, click the **Update** button.

5. Once **Update** is clicked, you will return to the test configuration page. The **URL** text box in the test configuration page will display just the **Names** – i.e., the unique display names – that you may have configured for the multiple URLs, as a comma-separated list. To view the complete URL specification, click the encircled ''+' button alongside the **URL** text box, once again.

3.4.4 Azure Cloud Service (classic) Test

For each cloud service, this test reports the current status, deployment status and CPU utilization on the Azure cloud. In addition, this test helps administrators figure out the Disk I/O and network traffic through each cloud service. This way, administrators can identify the cloud service that is utilized the most in the Azure cloud.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each cloud service of the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID** - Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH** - In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD** - Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Service status</td><td>Indicates the current status of this cloud service.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Created</td><td>1</td></tr>
<tr><td>Creating</td><td>2</td></tr>
<tr><td>Deleting</td><td>3</td></tr>
<tr><td>Deleted</td><td>4</td></tr>
<tr><td>Changing</td><td>5</td></tr>
<tr><td>Resolving DNS</td><td>6</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current status of this cloud service. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 6.</td></tr>
<tr><td>Deployment slot</td><td>Indicates the deployment environment of this cloud service.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Staging</td><td>1</td></tr>
<tr><td>Production</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the deployment environment of this cloud service. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>Deployment status</td><td>Indicates the current deployment status of this cloud service.</td><td>Number</td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Suspended</td><td>2</td></tr>
<tr><td>RunningTransitioning</td><td>3</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>SuspendedTransitioning</td><td>4</td></tr><tr><td>Starting</td><td>5</td></tr><tr><td>Suspending</td><td>6</td></tr><tr><td>Deploying</td><td>7</td></tr><tr><td>Deleting</td><td>8</td></tr><tr><td>Unknown</td><td>0</td></tr></table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current deployment status of this cloud service. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 8.</td></tr>
<tr><td>Disk reads</td><td>Indicates the rate at which data is read from the disk allocated to this cloud service.</td><td>MB/Sec</td><td></td></tr>
<tr><td>Disk writes</td><td>Indicates the rate at which data is written to the disk allocated to this cloud service.</td><td>MB/Sec</td><td></td></tr>
<tr><td>Incoming network traffic</td><td>Indicates the amount of incoming network traffic i.e., the amount of data received by all the network interfaces connected to this cloud service.</td><td>MB</td><td></td></tr>
<tr><td>Outgoing network traffic</td><td>Indicates the amount of outgoing network traffic i.e., the amount of data</td><td>MB</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	sent through all the network interfaces connected to this cloud service.		
CPU utilization	Indicates the percentage of CPU utilized by this cloud service.	Percent	
Total instances	Indicates the total number of instances that are currently running on this cloud service.	Number	The detailed diagnosis of this measure if enabled, lists the role name, instance name, instance status, instance size, IP Address and the power status of the cloud service.

3.4.5 Azure Virtual Machine (classic) Test

Azure Virtual Machines is one of several types of on-demand, scalable computing resources that Azure offers. An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the virtual machine. Azure Virtual Machines lets you create and use virtual machines in the cloud.

Azure Virtual Machines lets you create and use virtual machines in the cloud. Providing what's known as Infrastructure as a Service (IaaS), virtual machine technology can be used in variety of ways. Some examples are:

Virtual machines (VMs) for development and test. Development groups commonly use VMs because they offer a quick, easy way to create a computer with specific configurations required to code and test an application. Azure Virtual Machines provides a straightforward and economical way to create these VMs, use them, then delete them when they're no longer needed.

Running applications in the cloud. It makes economic sense to run some applications in the public cloud. One example is an application that has large spikes in demand. Although you could equip your own data center with enough hardware to handle peak demand, that hardware might be underutilized much of the time. Running this application on Azure lets you pay for extra VMs only when you need them and shut them down when you don't. Or, suppose you're a start-up that needs on-demand computing resources quickly and with no commitment. Once again, Azure can be the right choice.

Extending your own datacenter into the public cloud. When you use Azure Virtual Network, your organization can create a virtual network (VNET) that's an extension of your own on-premises network and add VMs to that VNET. This allows running applications such as SharePoint, SQL Server and others on an Azure VM. This approach might be easier to deploy or less expensive than running them in VMs your own datacenter.

Disaster recovery. Rather than paying continuously for a backup datacenter that's rarely used, IaaS-based disaster recovery lets you pay for the computing resources you need only when you really need them. For example, if your primary datacenter goes down, you can create VMs running on Azure to run essential applications, then shut them down when they're no longer needed.

When multiple virtual machines are hosted on the Azure cloud, administrators may often want to figure out if each virtual machine in the cloud is used optimally. In order to closely monitor the virtual machine and figure out the resource utilization of each virtual machine, administrators can use the **Azure Virtual Machine (classic)** test.

This test monitors the current state and the amount of resources that each virtual machine on the Azure cloud is taking up. Using the metrics reported by this test, administrators can determine which virtual machine in the cloud is taking up most CPU, which virtual machine is generating the most network traffic, which virtual machine has the maximum IOPS, etc.

Note:

eG Enterprise *cannot* auto-discover and monitor the Virtual Machines deployed through the Azure Resource Manager whereas Virtual Machines deployed in Azure Classic mode can be monitored.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each virtual machine of the target Microsoft Azure being monitored

First level Descriptor: Virtual Machine

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured

3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.

4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.

8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this virtual machine.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>RoleStateUnknown</td><td>1</td></tr>
<tr><td>CreatingVM</td><td>2</td></tr>
<tr><td>StartingVM</td><td>3</td></tr>
<tr><td>CreatingRole</td><td>4</td></tr>
<tr><td>StartingRole</td><td>5</td></tr>
<tr><td>Running</td><td>6</td></tr>
<tr><td>BusyRole</td><td>7</td></tr>
<tr><td>StoppingRole</td><td>8</td></tr>
<tr><td>StoppedRole</td><td>9</td></tr>
<tr><td>StoppingVM</td><td>10</td></tr>
<tr><td>StoppedVM</td><td>11</td></tr>
<tr><td>RestartingRole</td><td>12</td></tr>
<tr><td>CyclingRole</td><td>13</td></tr>
<tr><td>FailedStartingRole</td><td>14</td></tr>
<tr><td>FailedStartingVM</td><td>15</td></tr>
<tr><td>UnresponsiveRole</td><td>16</td></tr>
<tr><td>StoppedDeallocated</td><td>17</td></tr>
<tr><td>Offline</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current status of this virtual machine. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 17.
The detailed diagnosis of this measure if</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			enabled, lists the operating system that is running on the virtual machine, the size of the role instance, the location of the virtual machine, the virtual disk name, the host cache and the media link.
Disk reads	Indicates the rate at which data is read from the disks of this virtual machine.	MB/sec	A high value of this measure indicates that the disks are experiencing high I/O activity.
Disk writes	Indicates the rate at which data is written from the disks of this virtual machine.	MB/sec	
Incoming network traffic	Indicates the amount of data bytes received by all the network interfaces connected to this virtual machine.	MB	Comparing the value of this measure across the virtual machines will help you to identify the virtual machine that is hogged with incoming network data.
Outgoing network traffic	Indicates the amount of data bytes sent through all the network interfaces connected to this virtual machine.	MB	Comparing the value of this measure across the virtual machines will help you to identify the virtual machine through which maximum amount of data traffic passes through.
CPU utilization	Indicates the average percentage of CPU utilized by this virtual machine.	Percent	A very high value of this measure indicates that the VM is currently utilizing high memory resources.
Total core	Indicates the total number of CPU cores allocated to this virtual machine.	Number	
Configured memory	Indicates the amount of memory that is configured for this virtual machine.	GB	
Maximum disk size:	Indicates the maximum	GB	

Measurement	Description	Measurement Unit	Interpretation
	amount of disk space allocated for this virtual machine.		
Temporary disk size	Indicates the amount of temporary disk space that is allocated for this virtual machine.	GB	
Maximum data disk	Indicates the maximum number of data disks allocated to this virtual machine.	Number	
Maximum IOPS	Indicates the maximum amount of data space allocated for IOPS on this virtual machine.	GB	

3.4.6 Azure Web Apps (classic) Test

Azure Websites is a managed cloud service that allows you to deploy a web application and make it available to your customers on the Internet in a very short amount of time. You don't directly support the VMs on which your website runs; they are managed for you. By hosting the websites on the cloud, administrators can be freed from managing the physical infrastructure required to run the websites. Though the website is hosted on the Azure cloud through the Azure Resource Manager, it is important for an administrator to constantly monitor the availability and resource utilization of the websites. The **Azure Web Apps** test helps administrators in this regard.

By constantly monitoring the website hosted on the cloud, administrators can figure out the availability of the website, runtime availability of the website, erroneous websites and the websites that are over-utilizing the resources allocated to them. This way, administrators can be assured of the availability of the websites.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each website hosted on the target Microsoft Azure being monitored

Descriptor: Website

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID -** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **DD FREQUENCY -** Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option

against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

- The eG manager license should allow the detailed diagnosis capability.
- Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current state of this website.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Running / 1 Stopped / 2 Unknown / 0 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of this website. The graph of this measure however, is represented using the numeric equivalents only - 0 to 2. The detailed diagnosis of this measure if enabled, lists the Webspacename, the status, of the webspace, region, location and the URL that is used to hit the website.
Availability status	Indicates the current availability of management information		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>of this website.</td><td></td><td>
<table>
<tr><th>Numeric Value</th><th>Measure Value</th><th>Description</th></tr>
<tr><td>1</td><td>Normal</td><td>Indicates that the site is currently running and the management information of the site is available.</td></tr>
<tr><td>2</td><td>Limited</td><td>Indicates that only partial management information of the site is available and the detailed information is unavailable.</td></tr>
<tr><td>0</td><td>Unknown</td><td>Indicates that the management information is unknown.</td></tr>
</table>
<p><b>Note:</b></p>
<p>By default, this measure reports the Measure Values listed in the table above to indicate the current availability of management information of this website. The graph of this measure however, is represented using the numeric equivalents only - 0 to 2.</p>
</td></tr>
<tr><td>Compute mode</td><td>Indicates the compute mode of this website.</td><td></td><td>
<p>The values reported by this measure and its numeric equivalents are mentioned in the table below:</p>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Shared</td><td>1</td></tr>
<tr><td>Dedicated</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<p><b>Note:</b></p>
<p>By default, this measure reports the</p>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Measure Values listed in the table above to indicate the compute mode of this website. The graph of this measure however, is represented using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>Is site enabled?</td><td>Indicates whether/not this website is enabled.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>True</td><td>1</td></tr>
<tr><td>False</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate whether/not this website is enabled. The graph of this measure however, is represented using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>Runtime availability</td><td>Indicates the runtime availability of this website.</td><td>Number</td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Degraded</td><td>2</td></tr>
<tr><td>Not Available</td><td>3</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the runtime availability of this website. The graph of this measure</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>however, is represented using the numeric equivalents only - 0 to 3.</td></tr>
<tr><td>Site mode</td><td>Indicates the current mode of this website.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Free</td><td>1</td></tr>
<tr><td>Shared</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the runtime availability of this website. The graph of this measure however, is represented using the numeric equivalents only - 0 to 2.</td></tr>
<tr><td>CPU time</td><td>Indicates the amount of time the CPU is actually executing instructions for this website.</td><td>Secs</td><td></td></tr>
<tr><td>Data in</td><td>Indicates the rate at which the data enters this website.</td><td>Mbps</td><td></td></tr>
<tr><td>Data out</td><td>Indicates the rate at which data is sent from this website.</td><td>Mbps</td><td></td></tr>
<tr><td>Local data reads</td><td>Indicates the amount of local data read from this website.</td><td>MB</td><td></td></tr>
<tr><td>Local data writes</td><td>Indicates the rate at which data is written to this website.</td><td>MB</td><td></td></tr>
<tr><td>Network data reads</td><td>Indicates the rate at</td><td>Mbps</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	which network data is read from this website.		
Network data writes	Indicates the rate at which network data is written to this website.	Mbps	
Stop requests	Indicates the number of stop requests received by this website.	Number	
Memory usage	Indicates the amount of memory used by this website.	MB	
File system storage	Indicates the amount of memory used to store file system of this website.	MB	
Incoming requests	Indicates the amount of bytes utilized by the incoming requests of this website.	MB	Comparing the value of this measure across websites will reveal the website that is handling maximum number of incoming requests.
Incoming request response	Indicates the amount of bytes utilized for sending response to the incoming requests of this website.	MB	
Outgoing requests	Indicates the amount of bytes utilized for sending the outgoing requests from this website.	MB	Comparing the value of this measure across websites will reveal the website that is handling the maximum number of outgoing requests.
Outgoing request response	Indicates the amount of bytes utilized for receiving a response from the outgoing requests of this website.	MB	
Total requests	Indicates the total number of requests to this website.	Number	

Measurement	Description	Measurement Unit	Interpretation
Http 2xx	Indicates the number of HTTP 2xx errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 3xx	Indicates the number of HTTP 3xx errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 401	Indicates the number of HTTP 401 errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 403	Indicates the number of HTTP 403 errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 404	Indicates the number of HTTP 404 errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 406	Indicates the number of HTTP 406 errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http 4xx	Indicates the total number of HTTP 4xx errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Http server errors	Indicates the number of HTTP server errors encountered by this website.	Number	Ideally, the value of this measure should be zero.
Memory working set	Indicates the amount of physical memory required for the working set of this website.	MB	

Measurement	Description	Measurement Unit	Interpretation
Average memory working set	Indicates the average amount of memory required for the working set of this website.	MB	
Average response time	Indicates the average time taken by this website to respond to requests.	Secs	A high value for this measure indicates that the website is taking too long to respond.
Http error percent	Indicates the percentage of HTTP errors encountered by this website.	Percent	Ideally, the value of this measure should be zero. A high value for this measure indicates that the website is prone to errors. Comparing the value of this measure across websites will reveal the website that is more prone to errors.

3.4.7 Azure VM Status (classic) Test

This test enables administrators to determine how many virtual machines were registered with the Azure cloud and how many are currently powered on/powered off. In addition, this test helps administrators to determine how many virtual machines were currently added and how many virtual machines were removed. Using this test, administrators can also instantly identify the virtual machines that are inaccessible or disconnected.

Note:

eG Enterprise *cannot* auto-discover and monitor the Virtual Machines deployed through the Azure Resource Manager whereas Virtual Machines deployed in Azure Classic Mode can be monitored.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST–** The host for which the test is being configured
3. **SUBSCRIPTION ID -** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.

   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures

should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Registered VMs	Indicates the number of virtual machines that were currently registered on this cloud.	Number	The detailed diagnosis of this measure if enabled, lists the names of the virtual machines, the location of the virtual machine, the Public IP address, the Internal IP address and the Operating system of the virtual machine.
Powered on VMs	Indicates the number of virtual machines that are currently powered on.	Number	
Powered off VMs	Indicates the number of virtual machines that are currently powered off,	Number	
Added VMs	Indicates the number of virtual machines that are currently added to the cloud.	Number	
Removed VMs	Indicates the number of virtual machines that are currently removed from the cloud.	Number	
Other VMs	Indicates the number of virtual machines that are in disconnected or invalid or inaccessible state.	Number	

3.4.8 Azure Web Audit Logs (classic) Test

For each Azure website hosted on the Azure cloud, this test reports the number of information events that were generated when the test was executed the last time.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each Azure website hosted on the target Microsoft Azure being monitored

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID-** Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **SHOW INFO DD -** By default, this flag is set to **No**, indicating that by default, the test does not generate detailed measures for information events, so as to conserve storage space. If you want the test to generate and store detailed measures for information events, set the **SHOW INFO DD** flag to **Yes**.
8. **DD FREQUENCY -** Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can

modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.

9. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Information	Indicates the number of information events that were generated for this website during the last execution of the test.	Number	A change in value of this measure may indicate infrequent but successful operations performed by one or more applications. Please check the Audit Logs available in the Azure storage for more details.

3.4.9 Web Apps/VM Diagnostics - WAD (classic) Test

Azure Diagnostics is the capability within Azure that enables the collection of diagnostic data on a deployed application. You can use the diagnostics extension from a number of different sources. Currently supported are Azure Cloud Service Web and Worker Roles, Azure Virtual Machines running Microsoft Windows and Service Fabric.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each *Storage account:cloud service* of the target Microsoft Azure being monitored

First-level Descriptor: Storage account

Second-level Descriptor: Cloud service

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH -** In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks.*
5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable

the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability. • Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test

Measurement	Description	Measurement Unit	Interpretation
Total errors	Indicates the total number of errors encountered by this cloud service.	Number	Ideally, the value of this measure should be zero.
Requests	Indicates the total number of requests made to this cloud service.	Number	
Processor time	Indicates the percentage of time taken to process the requests for this cloud service.	Percent	A high value for this measure may indicate performance bottlenecks or may indicate that the cloud service is inaccessible.
Total bytes	Indicates the total number of bytes in this cloud service.	Number	
Queued requests	Indicates the number of requests that are queued to this cloud service.	Number	
Rejected requests	Indicates the number of requests that were rejected to this cloud service during the last execution of the test.	Number	
Available memory	Indicates the amount of memory that is available for this cloud service.	MB	
ISAPI extension	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
requests	ISAPI extension requests received on this cloud service.		

3.4.10 InfrastructureLogs - WAD (classic) Test

To enable administrators to rapidly capture the information events generated by the *WADDiagnosticInfrastructureLogsTable* available in the Azure storage, and troubleshoot issues that occur, the **InfrastructureLogs - WAD (classic)** test can be used.

This test monitors the *WADDiagnosticInfrastructureLogsTable* and reports the count and details of errors and warning events captured by that log.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for the target Microsoft Azure being monitored

1. **TEST PERIOD** - How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH** - In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text

box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.
6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
7. **SHOW INFO DD -** By default, this flag is set to **No**, indicating that by default, the test does not generate detailed measures for information events, so as to conserve storage space. If you want the test to generate and store detailed measures for information events, set the **SHOW INFO DD** flag to **Yes**.
8. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
9. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Information	Indicates the number of WAD diagnostics infrastructure log information events generated for this	Number	The detailed diagnosis of this measure if enabled, lists the Role name, PID and the detailed message. Please check the

Measurement	Description	Measurement Unit	Interpretation
	storage instance during the last execution of the test.		WADDiagnosticInfrastructureLogsTable available in the Azure storage for more details.

3.4.11 EventLogs - WAD (classic) Test

To enable administrators to rapidly capture error/warning events generated by the WADWindowsEventLogsTable available in the Azure storage, and troubleshoot issues that occur, the **EventLogs - WAD (classic)** test will be of much use.

This test monitors the *WADWindowsEventLogsTable* and reports the count and details of errors and warning events captured by that log.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Azure* as the *Component type*, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the Test: Microsoft Azure

Agent deploying the test: A remote agent

Output of the test: One set of results for each *Storage account:Cloud service:EventType* of the target Microsoft Azure being monitored

First-level Descriptor: Storage account

Second-level Descriptor: Cloud service

Third-level Descriptor: Event Type

1. **TEST PERIOD -** How often should the test be executed
2. **HOST**– The host for which the test is being configured
3. **SUBSCRIPTION ID**- Specify the GUID which uniquely identifies your subscription to the target Microsoft Azure that is to be monitored.
4. **CERTIFICATE PATH** - In order to collect metrics from the target Microsoft Azure, the eG agent communicates via the Microsoft Azure Service Management API Requests. By default, a

management certificate is required to authenticate the Microsoft Azure Service Management API Requests. The Management certificate should be associated with the subscription ID. The management certificate can be created on your own or you can request the Microsoft Azure portal to create a certificate on behalf of you. Prior to creating a management certificate, you have to create a keystore. The steps for creating a management certificate and the keystore is discussed elaborately in Section 1.1. The created keystore will reside in the *<JAVA_INSTALL_DIR>\jre7\bin* folder. Specify the exact path to the keystore file in this text box. If you have requested Microsoft Azure portal to create the management certificate, then, specify the exact path on which you have stored the keystore file. For example, if the keystore file created is *WindowsAzureKeyStore.jks* and if you have stored it in D:\Azure folder, then specify the **CERTIFICATE PATH** as *D:\Azure\WindowsAzureKeyStore.jks*.

5. **CERTIFICATE PASSWORD -** Specify the password that is provided while creating the keystore in this text box.

6. **CONFIRM PASSWORD -** Confirm the password by retyping it here.

7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.

8. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option.
   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability.
   - Both the bad and normal frequencies configured for the detailed diagnosis measures should not be 0.

Measures reported by the test:

Measurement	Description	Measurement Unit	Interpretation
Information	Indicates the number of WAD windows	Number	A change in value of this measure may indicate infrequent but successful

Measurement	Description	Measurement Unit	Interpretation
	information events of this type that were generated during the last execution of the test.		operations. Please check the WADWindowsEventLogsTable available in the Azure storage for more details.
Error	Indicates the number of WAD windows error events of this type that were generated during the last execution of the test.	Number	A very low value (zero) is desired for this measure, as it indicates good health. An increasing trend or a high value indicates the existence of problems. Please check the WADWindowsEventLogsTable available in the Azure storage for more details.
Warning	Indicates the number of WAD windows warnings of this type that were generated.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems. Please check the WADWindowsEventLogsTable available in the Azure storage for more details.
Critical	Indicates the number of WAD windows critical error events of this type that were generated when the test was last executed.	Number	This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems. A very low value (zero) indicates that the service is in a healthy state and is running smoothly without any potential problems. An increasing trend or high value indicates the existence of fatal/irrepairable problems. Please check the WADWindowsEventLogsTable available in the Azure storage for more details.
Verbose	Indicates the number of verbose events of this type that were generated when the test was last	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better.

Measurement	Description	Measurement Unit	Interpretation
	executed.		This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems. Please check the WADWindowsEventLogsTable available in the Azure storage for more details.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.