Monitoring Microsoft Azure

Microsoft: Azure PowerPack version 123

Table of Contents

Introduction to Monitoring Microsoft Azure **6**
What Does the Microsoft: Azure PowerPack Monitor? 6
What are Azure Locations? 10
Installing the Microsoft: Azure PowerPack 11
Configuration and Credentials for Monitoring Azure **13**
Configuring an Azure Active Directory Application 14
Creating an Active Directory Application in the Azure Portal 14
Adding Microsoft Graph API Permissions to the Application 16
Generating the Secret Key 18
Locating the Application ID and Tenant ID 19
Locating the Subscription ID 19
Adding Reader Access to the Active Directory Application 20
Setting Up a Proxy Server 22
Network Requirements 23
Creating an Azure Credential for Use in Guided Discovery 23
Testing the Azure Credential Using the Credential Tester Panel 26
Creating a SOAP/XML Credential for Azure 27
Load-Balancing an Account with Multiple Subscriptions 29
Filtering Virtual Machine Discovery 29
Testing the Azure Credential 30
Creating a SOAP/XML Credential for Azure in the Skylar One Classic User Interface 31
Load-Balancing an Account with Multiple Subscriptions 33
Testing the Azure Credential in the Skylar One Classic User Interface 33
Discovering Azure Services and Devices **35**
Discovering Microsoft Azure Devices Using Guided Discovery 35
Discovering Microsoft Azure Devices in the Classic Skylar One User Interface 38
Creating an Azure Virtual Device for Discovery 38
Aligning the Azure Dynamic Applications 39
Discovering Azure Component Devices 39
Viewing Azure Component Devices 40
Relationships Between Component Devices 42
Monitoring Azure Unified Alerts **46**
Prerequisites for Configuring Azure Unified Alerts 46
Azure Unified Alert Event Policies 47

Enabling the "Microsoft: Azure Unified Alerts Performance" Dynamic Application 48
Viewing Azure Unified Alert Counts 48
Azure Run Book Actions and Automations 50
Azure Run Book Automation Permissions 50
About the Azure Run Book Actions and Automations 51
Disabling VMs or Storage Disks by VM Tag 52
Run Book Automation Policy: Disable and Discover from IP 52
Run Book Automation Policy: Disable Storage Disks 53
Configuration Steps 54
Modifying the Parameters of the "Disable By VM Tag" Run Book Action 54
Enabling the "Component Device Record Created" Event Policy 55
Enabling the Run Book Automation Policies 55
Preserving Automation Changes 56
Disabling Databricks by Tag 56
Run Book Automation Policy: Disable Databricks 56
Configuration Steps 57
Modifying the Parameters of the "Disable By Databrick Tag" Run Book Action 57
Enabling the "Component Device Record Created" Event Policy (Discover from IP Only) 59
Enabling the Run Book Automation Policies 59
Preserving Automation Changes 60
Discovering VMs and Merging Physical Devices with Components 60
Run Book Automation Policy: Discover from IP 60
Run Book Automation Policy: Merge with VM 61
Configuration Steps 61
Modifying the Parameters of the Run Book Actions 62
Enabling the "Component Device Record Created" Event Policy (Discover from IP Only) 64
Enabling the "Device Record Created" Event Policy 64
Enabling the Run Book Policies 65
Preserving Automation Changes 66
Vanishing Terminated or Terminating VM Instances 67
Enabling the Run Book Automation Policies 68
Preserving Automation Changes 68
Azure Dashboards 69
Device Dashboards 69
Microsoft: Azure Batch Account 69

Microsoft: Azure Cache for Redis 70
Microsoft: Azure Key Vault 70
Microsoft: Azure Kubernetes Cluster 70
Microsoft: Azure MySQL Server 71
Microsoft: Azure PostgreSQL Server 71
Microsoft: Azure Service Bus Namespace 71
Microsoft: Azure WAF on CDN Policy 71
Key Metrics Collected by the Microsoft: Azure PowerPack 73
Azure Active Directory Tenant Service 75
Azure API Management 76
Azure App Service 81
Azure Application Gateway Service 83
Azure Automation Service 85
Azure Backup Policies Service 86
Azure Batch Service 87
Azure Cache for Redis 91
Azure Container Instances 94
Azure Container Registry 96
Azure Content Delivery Network 98
Azure CosmosDB Service 101
Azure Data Factory 104
Azure Database for MySQL 106
Azure Database for PostgreSQL 109
Azure Databricks Service 112
Azure DNS Service 113
Azure Event Grid 113
Azure ExpressRoute Service 119
Azure Fabric Capacity Service 123
Azure Firewall Service 123
Azure Front Door Service 126
Azure Function App Service Plan 127
Azure Functions 128
Azure HDInsight Service 128
Azure Key Vault 132
Azure Kubernetes Service (AKS) 134

Azure Load Balancer Service 136
Azure Logic App Service 138
Azure Managed Disks Service 140
Azure Network Security Group Service 140
Azure OpenAI Service 145
Azure Recovery Service Vault 147
Azure Resource Group Service 148
Azure Resource List Services 148
Azure Service Bus (Relay) 149
Azure Site Recovery 152
Azure SQL Managed Instance Service 154
Azure SQL Servers Service 156
Azure Storage Service 158
Azure Traffic Manager Service 164
Azure Virtual Desktop Host Pool Service 166
Azure Virtual Machines Service 168
Azure Virtual Network Service 172
Azure VM Scale Sets Service 177
Azure Web Application Firewall (WAF) 183
Other Supported Services 186

Chapter 1

Introduction to Monitoring Microsoft Azure

Overview

This manual describes how to monitor Microsoft Azure resources that are managed with Azure Resource Manager (ARM) in Skylar One using the "Microsoft: Azure" PowerPack.

This chapter covers the following topics:

What Does the Microsoft: Azure PowerPack Monitor? *6*

Installing the Microsoft: Azure PowerPack *11*

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What Does the Microsoft: Azure PowerPack Monitor?

To monitor Microsoft Azure resources using Skylar One, you must install the "Microsoft: Azure" PowerPack. This PowerPack enables you to discover, model, and collect data about Azure resources.

The "Microsoft: Azure" PowerPack includes:

- Dynamic Applications to discover, model, and monitor performance metrics and/or collect configuration data for the following Azure resources:
    - Active Directory tenants
    - Archive storage
    - API Management
    - Application gateways
    - Application services
    - Azure API Apps
    - Azure Blob storage
    - Azure Cache for Redis
    - Azure Container Instances
    - Azure Container Registry
    - Azure Data Factory
    - Azure Database for MySQL
    - Azure Database for PostgreSQL
    - Azure Databricks
    - Azure Event Grid
    - Azure Firewall
    - Azure Functions
    - Azure Kubernetes Services (AKS)
    - Azure Service Buses (Relay)
    - Batch Accounts
    - Content Delivery Networks
    - Cosmos DB accounts
    - Data Science virtual machines
    - Disk storage
    - DNS zones
    - ExpressRoute circuits
    - ExpressRoute Direct
    - ExpressRoute gateways
    - Fabric capacities

    - Front Door services
    - Function apps
    - Key Vaults
    - Load balancers
    - Managed storage disks
    - Network security groups
    - OpenAI resources
    - Queue storage
    - Recovery Services vaults
    - Resource groups
    - Site recovery configurations
    - Spot virtual machines
    - SQL databases
    - SQL managed instances
    - SQL servers
    - Storage accounts
    - Table storage
    - Traffic Manager profiles
    - Virtual machine scale sets
    - Virtual machines
    - Virtual network subnets
    - Virtual network gateways
    - Virtual networks
    - VPN gateways
    - Web apps
    - Web Application Firewalls (WAF)
- Device Classes for each Azure data center location and all of the Azure resources Skylar One monitors
- Event Policies and corresponding alerts that are triggered when Azure resources meet certain status criteria
- Example credentials you can use as templates to create SOAP/XML credentials to connect to Azure
- A Credential Test to ensure that your Azure credential works as expected

- Run Book Action and Automation policies that can automate certain Azure monitoring processes
- Limited monitoring is available for services based on the Azure Resource List and Azure Resource Health APIs. The services are modeled as device components which can be used for CMDB syncing. The PowerPack collects availability information and uses it for alerts, and aligns Azure alerts to the related service. There is no performance monitoring, so all the device components created by the "Microsoft: Azure Resource List Discovery" Dynamic Application are non-billable. The services included are:
    - Azure Analysis Services
    - Azure Arc
    - Azure Bastion
    - Azure Cognitive Services
    - Azure Data Lake Storage
    - Azure Database for MariaDB
    - Azure Database for MySQL Flexible Server
    - Azure Database for PostgreSQL Flexible Server
    - Azure Database Migration Service
    - Azure Dedicated Host
    - Azure Digital Twins
    - Azure IoT Hub
    - Azure Purview
    - Azure Service Fabric
    - Azure Spring Cloud
    - Azure Stream Analytics
    - Azure Synapse Analytics
    - Data Lake Analytics
    - Event Hubs
    - HDInsight
    - Log Analytics
    - Media Services
    - Microsoft Purview
    - Mobile Apps

- Notification Hubs
- Power BI Embedded

What are Azure Locations?

An Azure location is an individual data center located in a specific geographic locale. The Dynamic Applications in the "Microsoft: Azure" PowerPack create a "location" component device for each discovered data center location.

The PowerPack supports the following Azure data center locations:

- Australia Central (Canberra)
- Australia Central 2 (Canberra)
- Australia East (New South Wales)
- Australia Southeast (Victoria)
- Brazil South (Sao Paulo)
- Canada Central (Toronto)
- Canada East (Quebec)
- Central India (Pune)
- Central US (Iowa)
- China East (Shanghai)
- China East 2 (Shanghai)
- China North (Beijing)
- China North 2 (Beijing)
- East Asia (Hong Kong)
- East US (Virginia)
- East US 2 (Virginia)
- France Central (Paris)
- France South (Marseille)
- Japan East (Saitama)
- Japan West (Osaka)
- Korea Central (Seoul)
- Korea South (Busan)
- North Central US (Illinois)
- North Europe (Ireland)
- South Central US (Texas)
- South India (Chennai)
- Southeast Asia (Singapore)

- UK South (London)
- UK West (Cardiff)
- US DoD Central (for Microsoft Azure Government only)
- US DoD East (for Microsoft Azure Government only)
- US Gov Arizona (for Microsoft Azure Government only)
- US Gov Iowa (for Microsoft Azure Government only)
- US Gov Texas (for Microsoft Azure Government only)
- US Gov Virginia (for Microsoft Azure Government only)
- West Central US
- West Europe (Netherlands)
- West India (Mumbai)
- West US (California)
- West US 2 (Washington)
- West US 3 (Arizona)

Installing the Microsoft: Azure PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Microsoft: Azure" PowerPack.

NOTE: The following instructions describe how to install the "Microsoft: Azure" PowerPack for the first time. If you are upgrading to the latest version from a previous version, see the corresponding "Microsoft: Azure" PowerPack Release Notes for release-specific upgrade instructions.

TIP: By default, when you install a new version of a PowerPack, it overwrites all content from that PowerPack that is already installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting on the **Behavior Settings** page (System > Settings > Behavior) to prevent the new version of the PowerPack from overwriting local changes for some commonly customized fields.

NOTE: For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).

3. Click the **[Actions]** menu and select *Import PowerPack*. The **Import PowerPack** modal appears.
4. Click **[Browse]** and go to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack appears on the **PowerPacks** page.

> **NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack does not appear on the **PowerPacks** page. However, the imported PowerPack appears in the **Imported PowerPacks** modal. This modal appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Credentials for Monitoring Azure

Overview

The following sections describe how to configure Microsoft Azure resources for monitoring by Skylar One using the "Microsoft: Azure" PowerPack:

> **NOTE:** The "Microsoft: Azure" PowerPack can monitor Microsoft Azure resources, Microsoft Azure Government resources, and Microsoft Azure resources in the China region.

This chapter covers the following topics:

Configuring an Azure Active Directory Application *14*

Network Requirements *23*

Creating an Azure Credential for Use in Guided Discovery *23*

Creating a SOAP/XML Credential for Azure *27*

Configuring an Azure Active Directory Application

To create a SOAP/XML credential that allows Skylar One to access Microsoft Azure, you must provide the following information about an Azure application that is already registered with an Azure AD tenant:

- Application ID
- Subscription ID (if monitoring a single subscription)
- Tenant ID
- Secret key

To capture the above information, you must first create (or already have) an application that is registered with Azure Active Directory. The registered application must have Reader access in the subscription. You can then enter the required information about the application when configuring the SOAP/XML credential in Skylar One. The registered application and the ScienceLogic credential allow Skylar One to retrieve information from Microsoft Azure.

TIP: For details on registering an Azure application, see https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app.

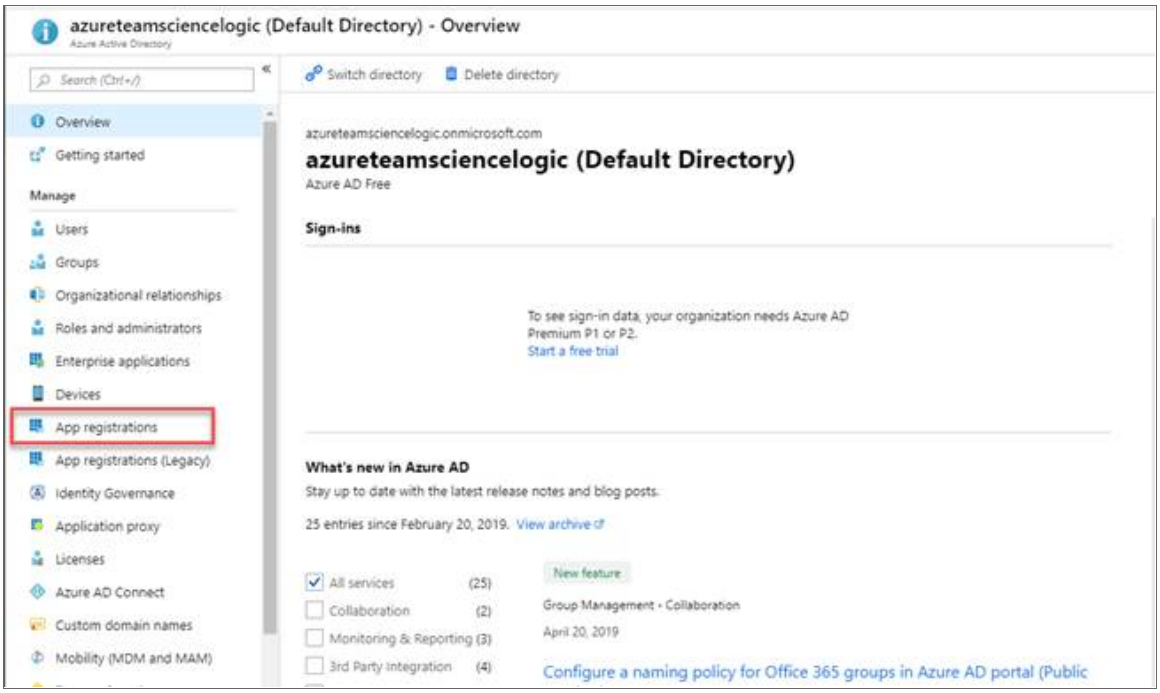
Creating an Active Directory Application in the Azure Portal

When configuring a SOAP/XML credential in Skylar One, you must provide the application ID, subscription ID, tenant ID, and secret key of an application that is registered with Azure Active Directory. You will use this registered application to authenticate your Azure account.

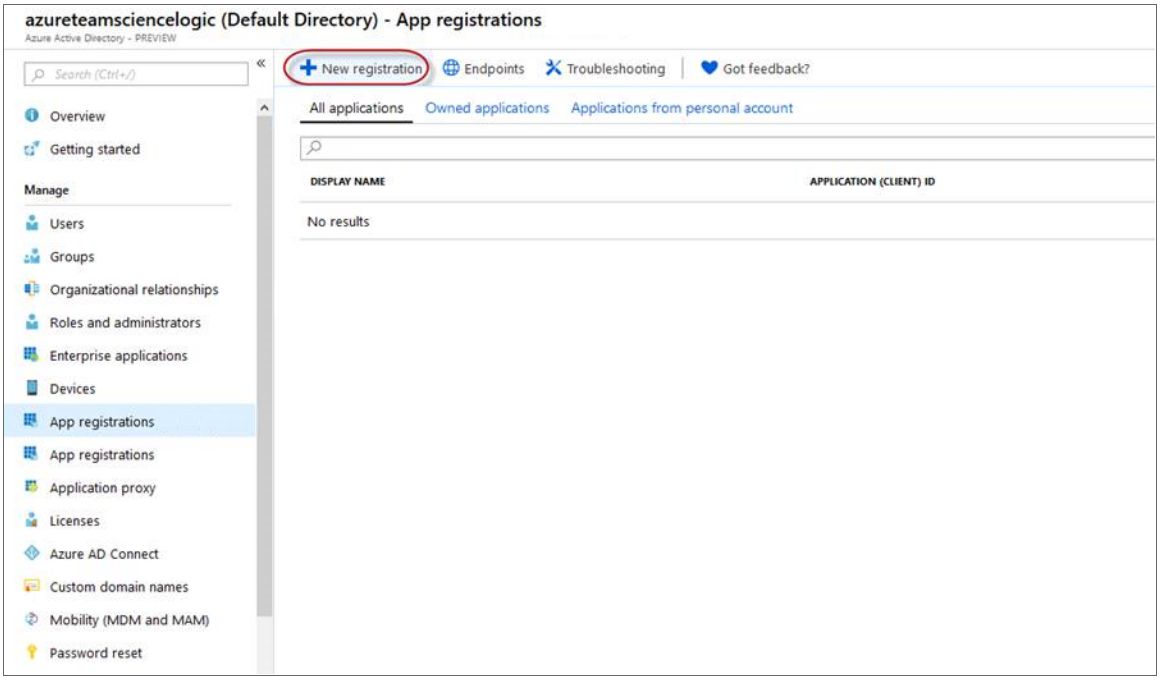
NOTE: You must have Service Administrator rights to create an Azure Active Directory application.

To create an application in Azure and register it with Azure Active Directory:

1. Log in to the Azure portal (https://portal.azure.com) and type "active directory" in the ***Search*** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **[App registrations]**. The **App registrations** page appears:

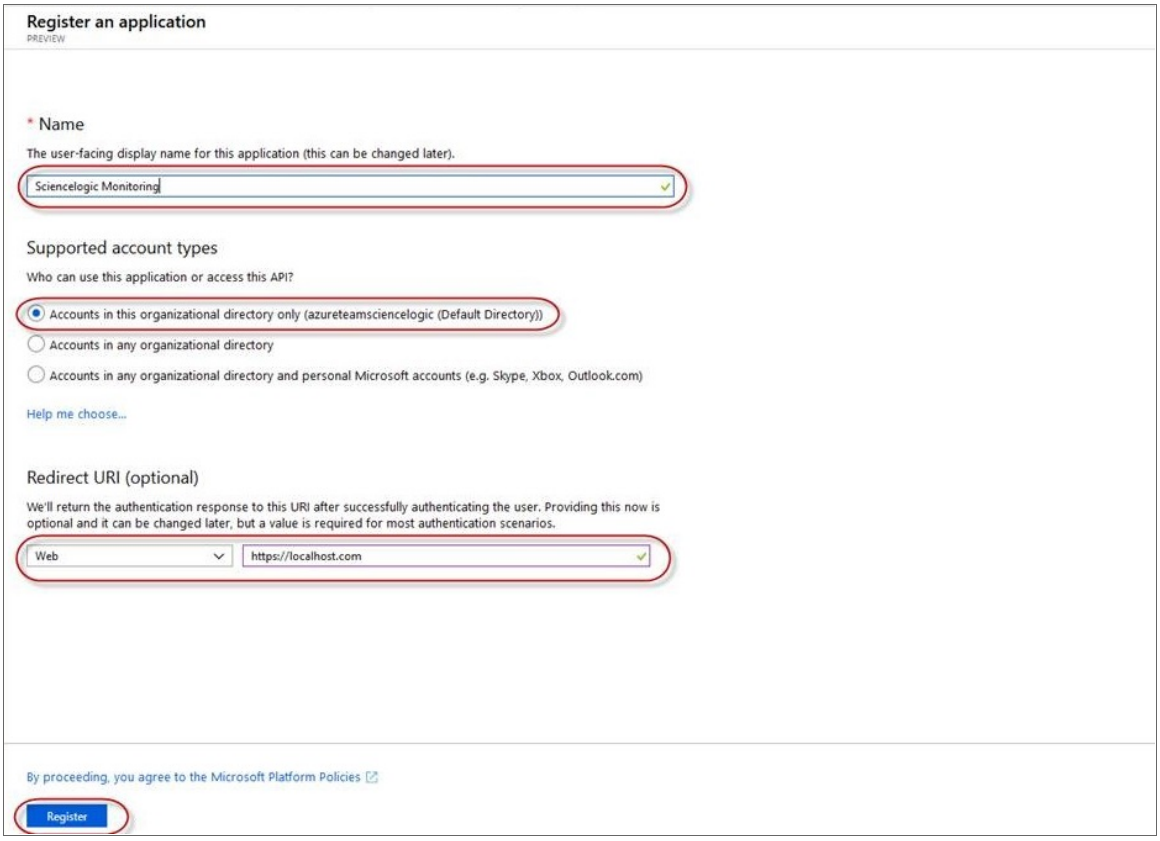


3. Click the **[New registration]** button.



4. When the **Register an application page** appears, enter your application's registration information:
   - ***Name***. Type a name for the application.
   - ***Supported account types***. Select *Accounts in this organizational directory only*.

- ***Redirect URI (optional)***. Select *Web* in the drop-down menu and type a valid URL.



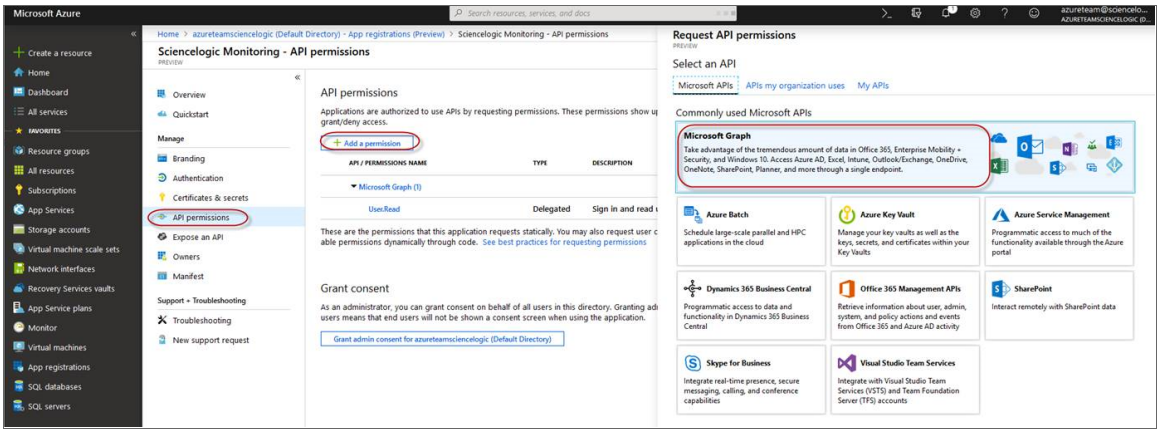
5. Click the **[Register]**button. A message appears confirming that your application was added.

Adding Microsoft Graph API Permissions to the Application

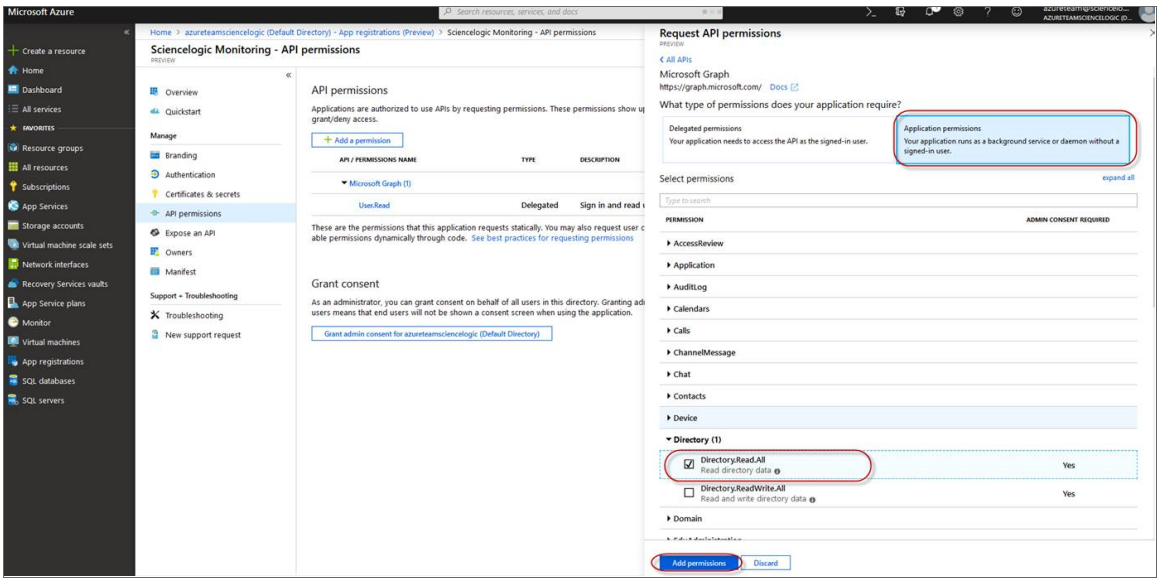
By default, any new application has Microsoft Graph API permission. At a minimum, the Microsoft Graph APIs must have permission to directly read data.

To add the Microsoft Graph APIs:

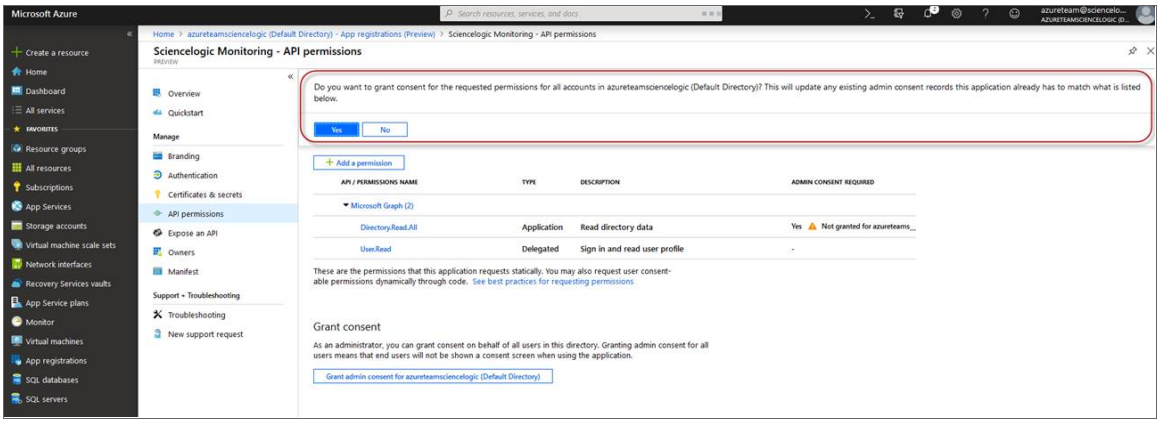
1. Log in to the Azure portal (https://portal.azure.com) and type "active directory" in the ***Search*** field at the top of the window.
2. Click **[App registrations]**, and then click on the name of the Azure Active Directory application you will use to authenticate your Azure account.
3. Click **[API Permissions]**, and then click **[Add a permission]**. Next, select the *Microsoft Graph* option.



4. In the **Request API permissions** pane, under Select permissions, click the arrow next to **Directory** to open the submenu and select the checkbox for ***Directory.Read.all*** permission.



5. After you have added the Read directory data permission, in the **API permissions** page, click the **[Add Permissions]** button.
6. Click **[Grant admin consent for [Directory Name]]**.
7. A pop-up window appears asking if you grant consent for the required permissions for all accounts in your directory. Click **[Yes]**.

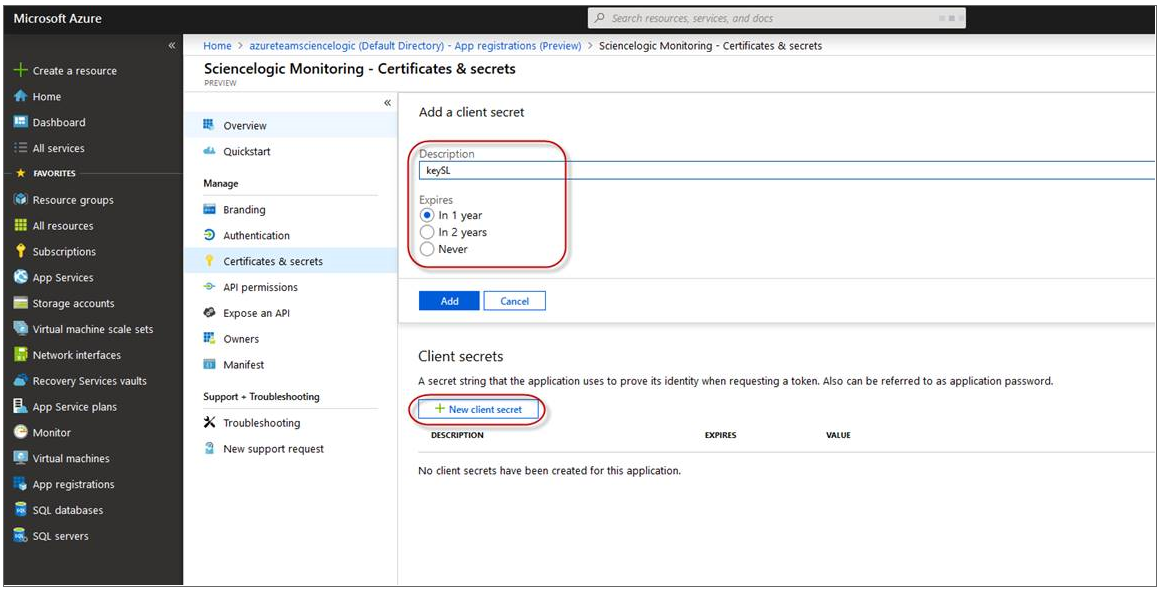


Generating the Secret Key

When configuring a SOAP/XML credential for Azure in Skylar One, you need to provide a secret key for the Azure Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. Log in to the Azure portal (https://portal.azure.com) and type "active directory" in the ***Search*** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **[App registrations]**.
3. Select the app and then click **[Certificates & secrets]**.
4. In the **Client secrets** pane, click **[+ New client secret]**.



5. In the **Add a client secret** pane, type a name in the ***Description*** field and select a duration in the ***Expires*** field.

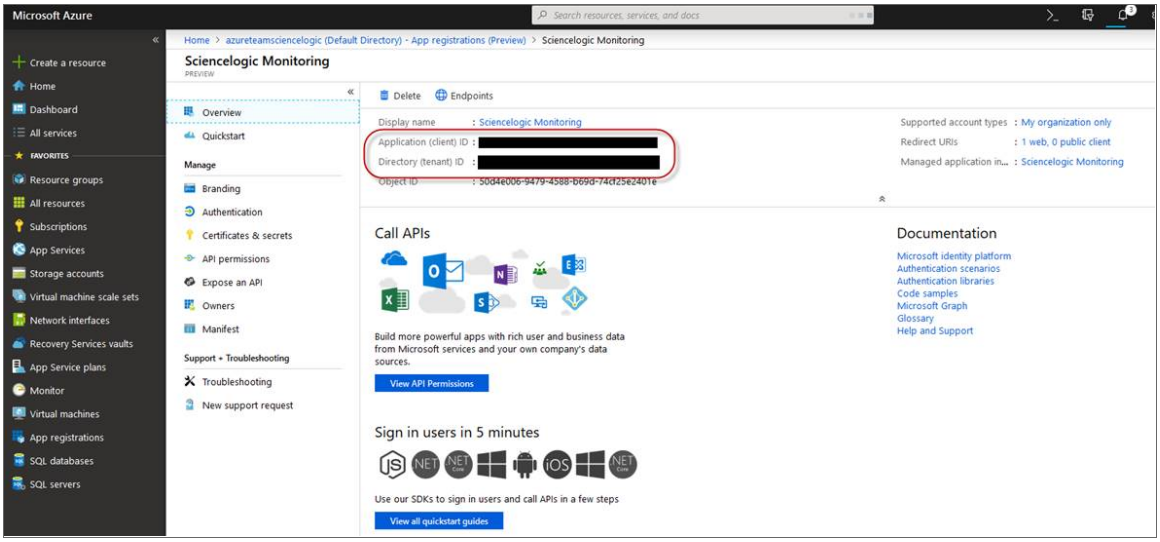
6. Click **[Add]** to generate the secret key. A new key value displays in the **Client secrets** pane.
7. Copy and save the key value.

Locating the Application ID and Tenant ID

When configuring a SOAP/XML credential for Azure in Skylar One, you need to provide the Application ID of the Azure Active Directory application you will use to authenticate your Azure account.

To locate the Application ID:

1. Log in to the Azure portal (https://portal.azure.com) and type "active directory" in the ***Search*** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations**.
3. Click the name of the Active Directory application you will use to authenticate your Azure account. The Application ID and Tenant ID appear in the **Overview** section.



4. Copy and save the values in the corresponding credential fields.

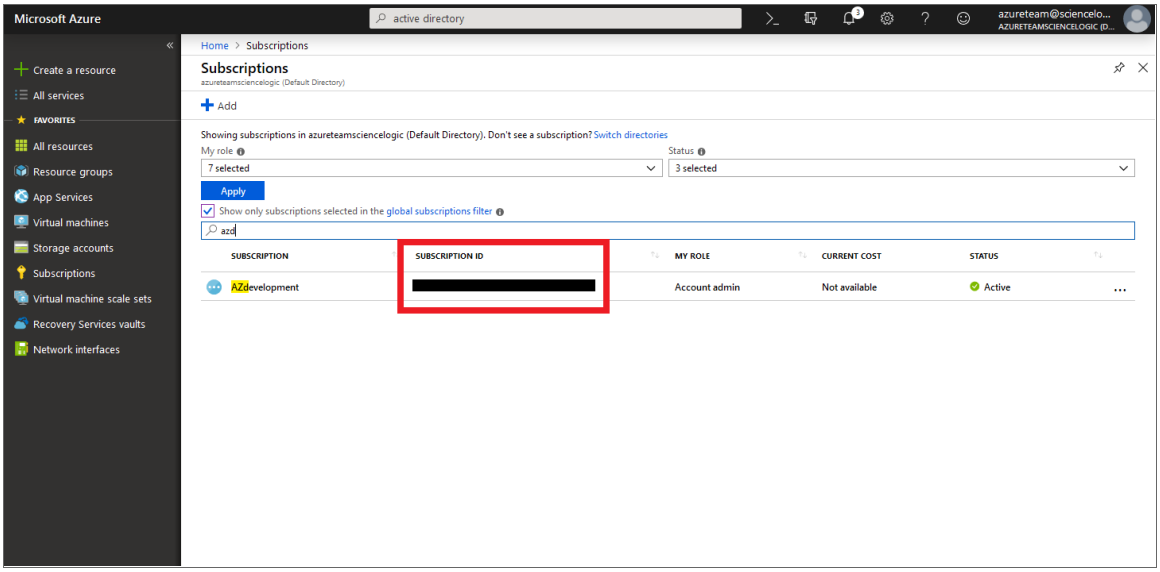
Locating the Subscription ID

If you are monitoring only a single Azure subscription, you must provide the Subscription ID of the Azure Active Directory application you will use to authenticate your account when you configure your SOAP/XML credential for Azure in Skylar One.

> **NOTE:** If you are monitoring an account with multiple child subscriptions, you can skip this section.

To locate the Subscription ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Subscriptions]**.
2. Copy and save the ***Subscription ID*** of the subscription where you created the Azure Active Directory application you will use to authenticate your account.

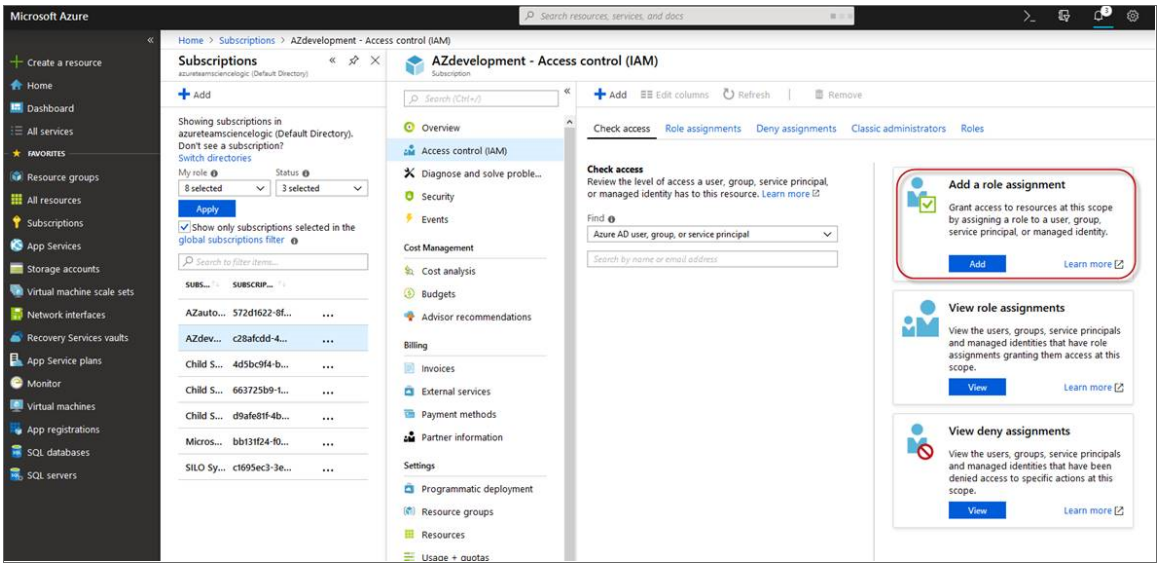


Adding Reader Access to the Active Directory Application

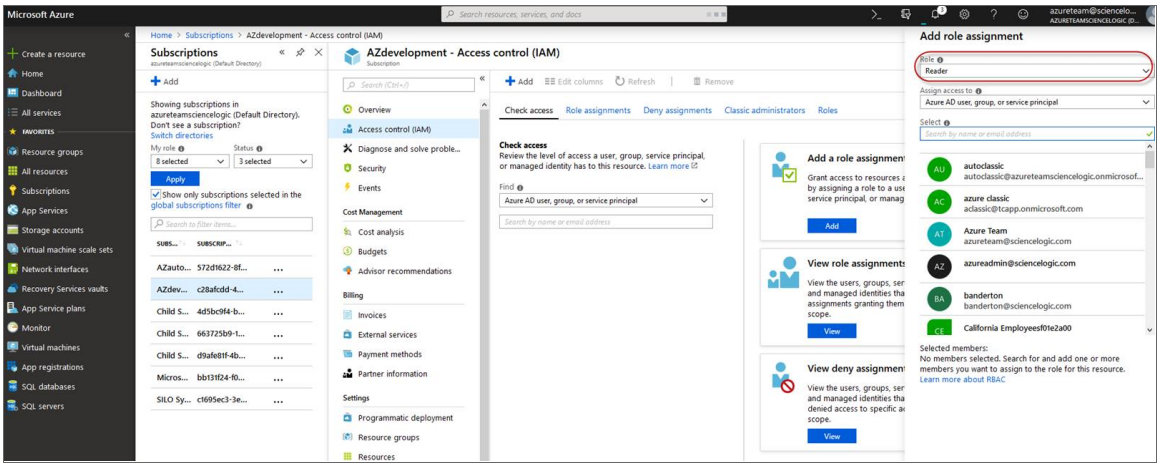
To allow ScienceLogic to access your Azure account, you must specify the type of access the user whose information you will use in your SOAP/XML credential has to the Active Directory application used to authenticate your account. Use the ***Reader*** access role, which is a read-only user that can view everything but cannot make changes.

To specify the access role to the Azure Active Directory application:

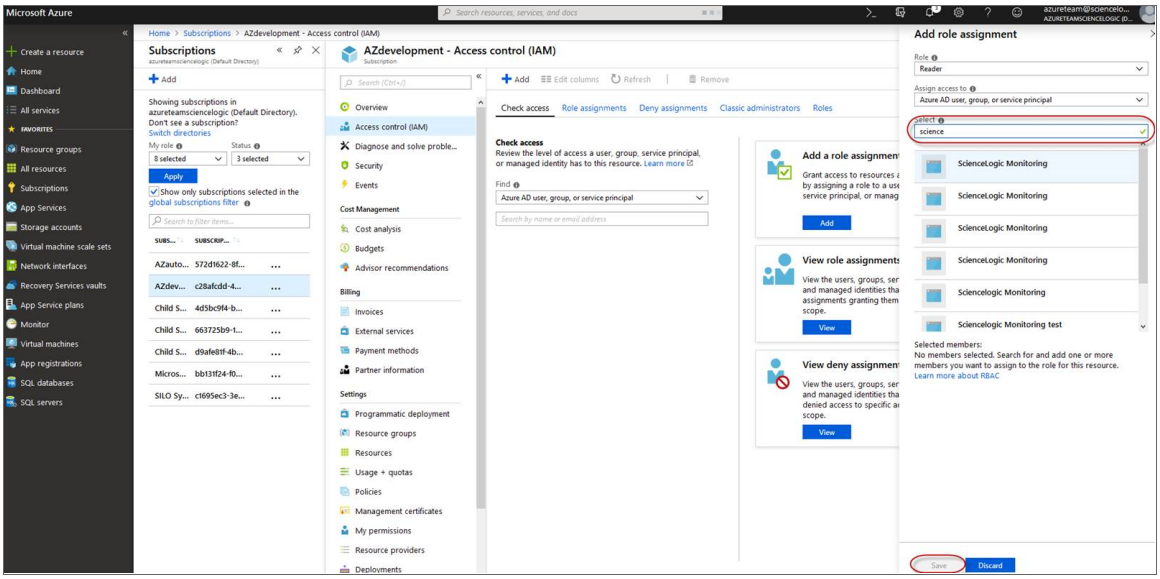
1. In the left pane of the Azure portal (https://portal.azure.com), click **[Subscriptions]**.
2. Click the name of your subscription, and then click **[Access control (IAM)]**.
3. In the **Access Control (IAM)** pane, click the **[Add]** button in the **Add a role assignment** section.



4. In the **Add a role assignment** pane, select *Reader* in the ***Role*** field.



5. In the ***Select*** field, type the name of the Azure Active Directory application you will use to authenticate your account.



6. Select the application from the search results and click **[Save]**.

Setting Up a Proxy Server

Depending on your needs, you can optionally enable Skylar One to connect to Azure through a third-party proxy server such as SQUID. With this configuration, Skylar One connects to the proxy server, which then connects to Azure. Azure relays information to the proxy server and Skylar One then retrieves that information from the proxy.

> **NOTE:** You can connect to Azure via a proxy server regardless of whether you are monitoring a single subscription or an account with multiple child subscriptions. You can connect to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure China region via a proxy server.

> **NOTE:** The "Microsoft: Azure" PowerPack is certified to work with SQUID version 3.5.12 proxy servers.

If you choose to use a proxy server, configure the third-party proxy server based on the third-party documentation. Depending on the type of authentication you require, you might need to specify a user name and password for the proxy server configuration. Also, make a note of the port you opened for the configuration, as this information is needed when creating the SOAP/XML credential.

Network Requirements

You must allow access to the following URLs so the Skylar One Data Collector can communicate with the Azure APIs:

- Commercial Portal (portal.azure.com)
  - https://management.core.windows.net/
  - https://management.azure.com
  - https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token
  - https://graph.microsoft.com/v1.0/
  - https://batch.core.windows.net/
  - https://*.batch.azure.com
  - https://*.table.core.windows.net
- US Government Portal (portal.azure.us)
  - https://management.core.usgovcloudapi.net/
  - https://batch.core.usgovcloudapi.net
  - https://*.batch.usgovcloudapi.net
  - https://management.usgovcloudapi.net/
  - https://graph.microsoft.us
  - https://login.microsoftonline.us/{tenant_id}/oauth2/v2.0/token
  - https://*.table.core.usgovcloudapi.net
- China Portal (portal.azure.cn)
  - https://management.core.chinacloudapi.cn
  - https://batch.core.chinacloudapi.cn/
  - https://*.batch.chinacloudapi.cn
  - https://management.chinacloudapi.cn
  - https://login.chinacloudapi.cn/{tenant_id}/oauth2/v2.0/token
  - https://microsoftgraph.chinacloudapi.cn
  - https://*.table.core.chinacloudapi.cn

Creating an Azure Credential for Use in Guided Discovery

To configure Skylar One to monitor Microsoft Azure, you must first create an Azure credential. This credential allows the Dynamic Applications in the "Microsoft: Azure" PowerPack to connect with the Azure

Active Directory Application.

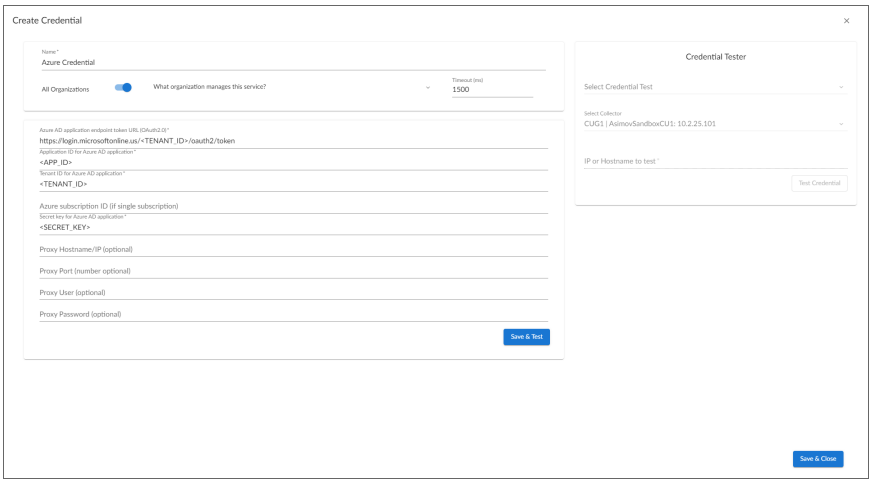
Skylar One includes an Azure credential type that you can use to connect with the Azure service during guided discovery. This credential type uses field names and terminology that are specific to the Azure service.

NOTE: Alternatively, you could monitor Azure using a generic SOAP/XML credential that does not include Azure-specific fields. For more information, see the section on *Creating a SOAP/XML Credential for Azure*.

NOTE: Currently, this process does not support discovery for Government or China accounts because the required HTTP headers cannot be added. ScienceLogic recommends creating the credentials for these accounts using the generic *SOAP/XML credential for Azure.*

To define an Azure-specific credential:

1. Go to the **Credentials** page (System > Manage > Credentials).
2. Click the **[Create New]** button and then select *Create Azure Credential*. The **Create Credential** modal page appears:



3. Supply values in the following fields:
   - ***Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Time, in milliseconds, after which Skylar One will stop trying to communicate with the device from which you want to retrieve data.
   - ***Azure AD application endpoint token URL (OAuth2.0)***. The AD application endpoint token URL for the Azure Active Directory application.
   - ***Application ID for Azure AD application***. The Application ID for the Azure Active Directory application.
   - ***Tenant ID for Azure AD application***. The Tenant ID for the Azure Active Directory application.
   - ***Azure subscription ID (if single subscription)***. The subscription ID for the Azure Active Directory application. This field is required only if you are monitoring a single Azure subscription.
   - ***Secret key for Azure AD application***. The secret key for the Azure Active Directory application.

   <u>Proxy Settings</u>

   If you use a proxy server in front of the Azure Active Directory applications you want to communicate with, enter values in these fields. Otherwise, you can skip these fields.

- ***Proxy Hostname/IP***. The host name or IP address of the proxy server.
- ***Proxy Port***. Port on the proxy server to which you will connect.
- ***Proxy User***. Username to use to access the proxy server.
- ***Proxy Password***. Password to use to access the proxy server.

4. Click **[Save & Close]**.

> **NOTE:** If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the *Testing the Azure Credential* section.

Testing the Azure Credential Using the Credential Tester Panel

The "Microsoft: Azure" PowerPack includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that Skylar One can execute on demand to validate whether a credential works as expected.

To test the Azure credential using the Credential Tester panel:

1. After *defining an Azure credential*, click the **[Save & Test]** button. This activates the Credential Tester fields.
2. In the Credential Tester panel, supply values in the following fields:
   - ***Select Credential Test***. Select a credential test to run. This drop-down list includes the *ScienceLogic Default Credential Tests*, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
   - ***Select Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
   - ***IP or Hostname to test***. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
3. Click the **[Run Test]** button to run the credential test. The **Testing Credential** window appears.

   The **Testing Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

   - ***Step***. The name of the step.
   - ***Description***. A description of the action performed during the step.
   - ***Log Message***. The result of the step for this execution of the credential test.
   - ***Status***. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).

- ***Step Tip***. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

Creating a SOAP/XML Credential for Azure

If you want to create a SOAP/XML credential without Azure-specific fields, note the application ID, subscription ID, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account. This credential allows the Dynamic Applications in the "Microsoft: Azure" PowerPack to communicate with your Azure subscriptions.

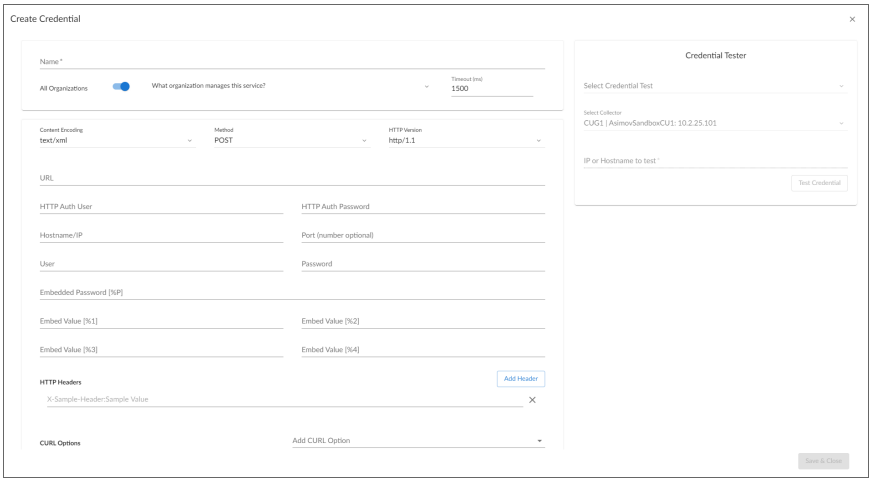
If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure Chinese region.

The "Microsoft: Azure" PowerPack includes multiple sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - China**, for users who connect to an Azure data center in a Chinese region
- **Azure Credential Gov Example**, for users who subscribe to Microsoft Azure Government
- **Azure Credential Proxy Example**, for users who connect to Azure through a third-party proxy server
- **Azure Credential - Example**, for all other users.

To create a SOAP/XML credential for Azure:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the sample credential you want to use, click its actions icon (⋮) and select ***Duplicate***. A copy of the credential appears.
3. Click the actions icon (⋮) for the credential copy and select ***Edit***. The **Edit Credential** modal page appears.



4. Supply values in the following fields:
    - ***Name***. Type a new name for the Azure credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (ms)***. Type "120".
    - ***Content Encoding***. Select *text/xml*.
    - ***Method***. Select *POST*.
    - ***HTTP Version***. Select *HTTP/1.1*.
    - ***URL***. Type the tenant ID in the appropriate place in the URL provided in the sample credential.
    - ***HTTP Auth User***. Leave this field blank.
    - ***HTTP Auth Password***. Leave this field blank.

    Proxy Settings

    - ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
    - ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.
    - ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
    - ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

    SOAP Options

    - ***Embedded Password [%P]***. Type the secret key for the Azure Active Directory application.
    - ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
    - ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
    - ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
    - ***Embed Value [%4]***. Leave this field blank.

    HTTP Headers

    - ***HTTP Headers***. Leave this field blank, unless one of the following scenarios applies to you:
        - If you are using Microsoft Azure Government, this field contains the text "AZGOV".
        - If you are monitoring Microsoft Azure resources in China, this field contains the text "AZCHINA".
        - If you would like to enable extended logging, enter "LOGGING" in to a header field. The log file is located at `/data/logs/azure.log` in the data collector.

- SSL certification verification is enabled by default, but you can disable it in a header field by entering "VERIFY:FALSE".
- If you want to filter which Azure virtual machines Skylar One discovers based on power state or Azure tags, you can add several different headers to do so. For more information, see the section on *Filtering Virtual Machine Discovery*.

cURL Options

- ***CURL Options***. Do not make any selections in this field.

5. Click **[Save & Close]**.

> **NOTE:** If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the *Testing the Azure Credential Using the Credential Tester Panel* section.

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

- The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.
- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
  - Perform all of the steps in the section on *Configuring an Azure Active Directory Application*.
  - Align each subscription in the group with the same application that you registered with Azure AD.
  - In the credential, enter the application ID in the ***Embed Value [%1]*** field.
  - In the credential, leave the ***Embed Value [%3]*** field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions. The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Filtering Virtual Machine Discovery

Beginning in version 122 of the "Microsoft: Azure" PowerPack, you can filter which Azure virtual machines Skylar One discovers based on power state or Azure tags. To configure this filtering, add one or more of

the headers described below to the ***HTTP Headers*** field of the SOAP/XML Azure credential used for discovery.

- ***Filter-PowerStates***. Type "all" or a comma-separated list of the power states you want Skylar One to discover: "Starting", "Running", "Stopping", "Stopped", "Deallocating", "Deallocated", or "Unknown". For example: "Filter-PowerStates: all".
- ***Filter-Mode***. Use this header together with "Filter-Tags". Type "Include" or "Exclude" to determine how "Filter-Tags" is applied. For example: "Filter-Mode: Include".
- ***Filter-Tags***. Type one or more Azure tag key/value pairs, separated by commas, in the format "tag=value". In "Include" mode, discovery skips any virtual machine that does not have a matching tag. In "Exclude" mode, discovery skips any virtual machine that has a matching tag. If your tag list does not fit in a single header, add a second "Filter-Tags" header. Skylar One combines the tag/value pairs from every "Filter-Tags" header into a single filter. For example: "Filter-Tags: Vendor=Databricks,Environment=Dev".

If you do not add any of these headers to the credential, the "Microsoft: Azure Virtual Machine Discovery" Dynamic Application discovers only virtual machines in the "Running" power state.

CAUTION: If you add the "Filter-PowerStates" header, you must give it a value. An empty "Filter-PowerStates" header filters out every virtual machine. This means that Skylar One cannot discover any virtual machines.

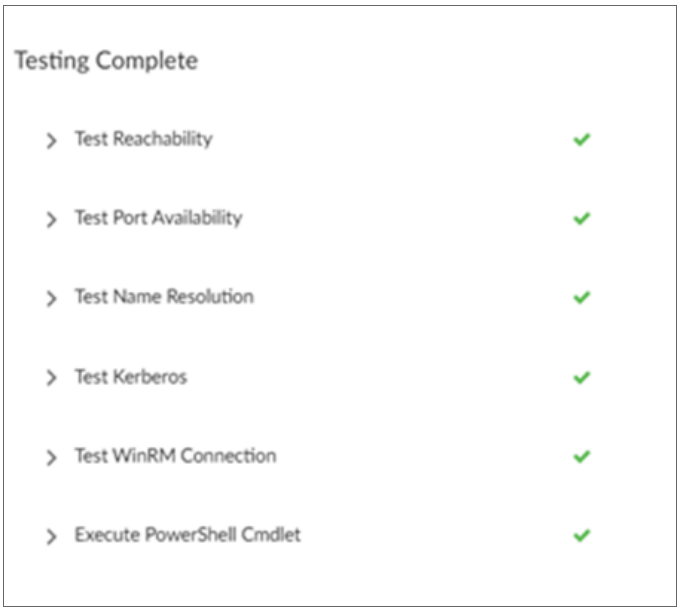
IMPORTANT: If you add or change these headers after Skylar One has already discovered a virtual machine, the existing component device is not deleted even if the new filter now excludes it. Instead, it remains modeled and reports as unavailable.

Testing the Azure Credential

You can test a credential from the **Credentials** page using a predefined credential test.

To run a credential test from the **Credentials** page:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the actions icon (⋮) of the credential that you want to test, and then select *Edit/Test*.
3. The **Credential Tester** modal page appears. Fill out the following fields on this page:
   - ***Select Credential Test***. Select a credential test to run. This drop-down list includes the *ScienceLogic Default Credential Tests*, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
   - ***IP or Hostname to Test***. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
4. Click the **[Test Credential]** button to run the credential test. The Credential Test starts and the Testing Completed modal displays the results.



The **Testing Completed** window displays a log entry for each step in the credential test. The steps performed are different for each credential test.

Creating a SOAP/XML Credential for Azure in the Skylar One Classic User Interface

After you note the application ID, subscription ID, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in Skylar One. This credential allows the Dynamic Applications in the "Microsoft: Azure" PowerPack to communicate with your Azure subscriptions.

If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to Microsoft Azure, Microsoft Azure Government, and the Microsoft Azure Chinese region.

The "Microsoft: Azure" PowerPack includes multiple sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - China**, for users who connect to an Azure data center in a Chinese region
- **Azure Credential Gov Example**, for users who subscribe to Microsoft Azure Government
- **Azure Credential Proxy Example**, for users who connect to Azure through a third-party proxy server
- **Azure Credential - Example**, for all other users.

To create a SOAP/XML credential for Azure:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential you want to use and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:

   Basic Settings

- ***Profile Name***. Type a new name for the Azure credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the tenant ID in the appropriate place in the URL provided in the sample credential.
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.
- ***Timeout (seconds)***. Type "120".

Proxy Settings

- ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.
- ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

- ***CURL Options***. Do not make any selections in this field.

SOAP Options

- ***Embedded Password [%P]***. Type the secret key for the Azure Active Directory application.
- ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
- ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- ***Embed Value [%4]***. Leave this field blank.

HTTP Headers

- ***HTTP Headers***. Leave this field blank, unless one of the following scenarios applies to you:
- If you are using Microsoft Azure Government, this field contains the text "AZGOV".
- If you are monitoring Microsoft Azure resources in China, this field contains the text "AZCHINA".
- If you would like to enable extended logging, enter "LOGGING" in to a header field. The log file is located at `/data/logs/azure.log` in the data collector.
- SSL certification verification is enabled by default, but you can disable it in a header field by entering "VERIFY:FALSE".

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

- The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.
- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
  - Perform all of the steps in the section on *Configuring an Azure Active Directory Application*.
  - Align each subscription in the group with the same application that you registered with Azure AD.
  - In the credential, enter the application ID in the ***Embed Value [%1]*** field.
  - In the credential, leave the ***Embed Value [%3]*** field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions. The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Testing the Azure Credential in the Skylar One Classic User Interface

The "Microsoft: Azure" PowerPack includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that Skylar One can execute on demand to validate whether a credential works as expected.

The "Azure Credential Test - ARM" can be used to test a SOAP/XML credential for monitoring Azure using the Dynamic Applications in the "Microsoft: Azure" PowerPack. The "Azure Credential Test - ARM" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Azure endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Azure endpoint.
- ***Make connection to Azure account***. Attempts to connect to the Azure service using the account specified in the credential.
- ***Validate Azure Microsoft Graph Permission***. Verifies that the Azure Active Directory application has Microsoft Graph API permissions.

- *Validate Azure subscription assignments*. Verifies that the Azure Active Directory application is assigned to the subscription.

To test the Azure credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Locate the **Azure Credential Test - ARM** and click its lightning bolt icon ( ). The **Credential Tester** modal page appears:
3. Supply values in the following fields:
    - *Test Type*. This field is pre-populated with the credential test you selected.
    - *Credential*. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
    - *Hostname/IP*. Leave this field blank.
    - *Collector*. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:
    - *Step*. The name of the step.
    - *Description*. A description of the action performed during the step.
    - *Log Message*. The result of the step for this credential test.
    - *Status*. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).
    - *Step Tip*. Mouse over the question mark icon ( ) to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".

Chapter 3

Discovering Azure Services and Devices

Overview

The following sections describe how to discover Microsoft Azure resources for monitoring by Skylar One using the "Microsoft: Azure" PowerPack.

This chapter covers the following topics:

Discovering Microsoft Azure Devices Using Guided Discovery *35*

Discovering Microsoft Azure Devices in the Classic Skylar One User Interface *38*

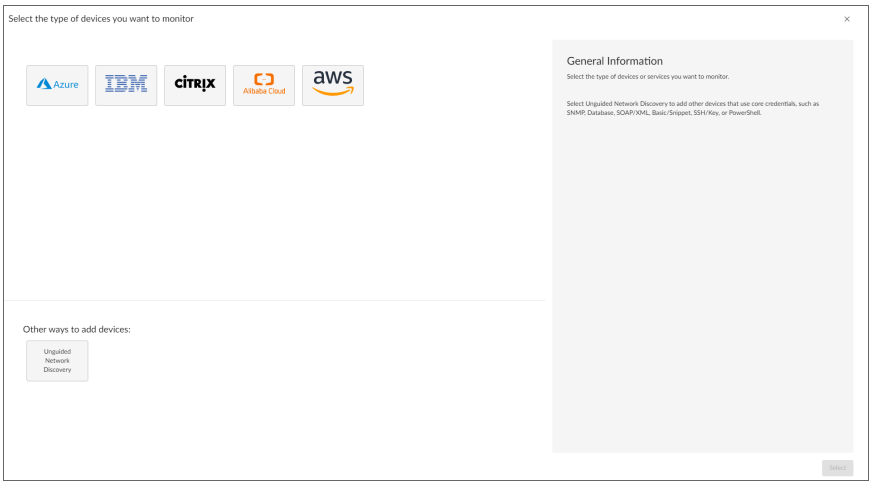
Viewing Azure Component Devices *40*

Discovering Microsoft Azure Devices Using Guided Discovery

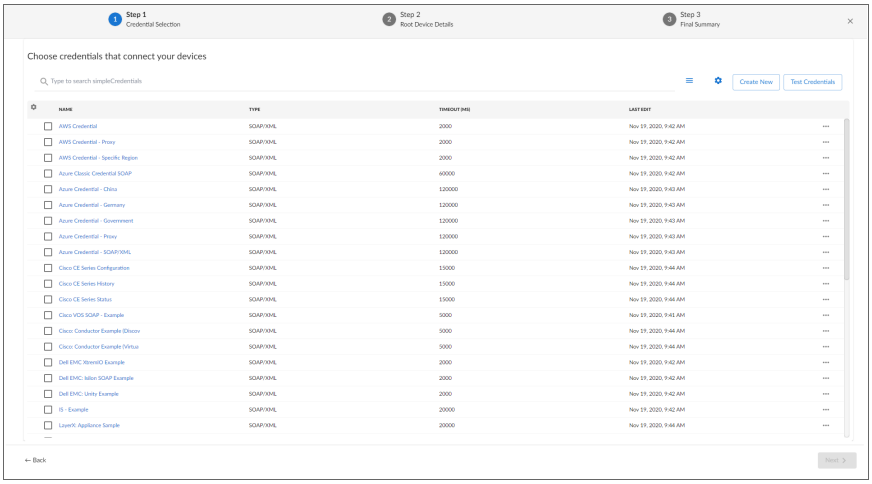
You can use the universal discovery framework process in Skylar One that guides you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you pick a discovery type based on the type of devices you want to monitor. It includes a button for Microsoft Azure.

To run a guided discovery for Microsoft Azure:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.

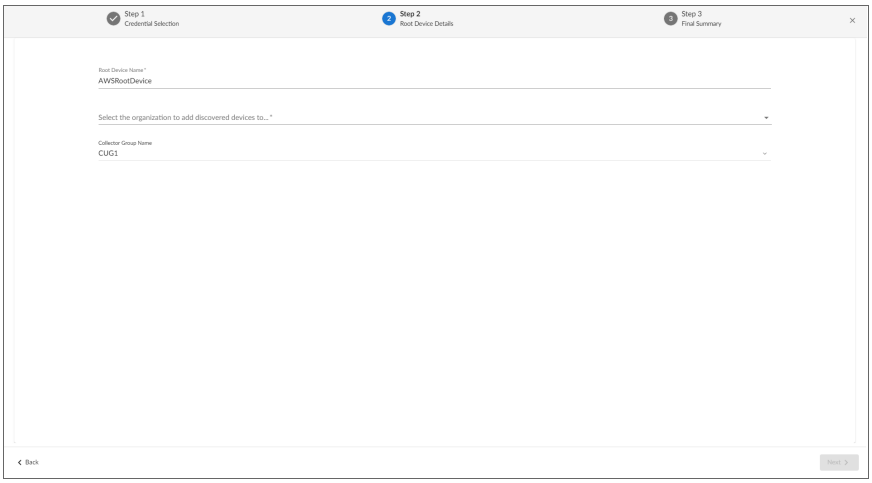


2. Click the **Microsoft Azure** button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Credential Selection** page appears.

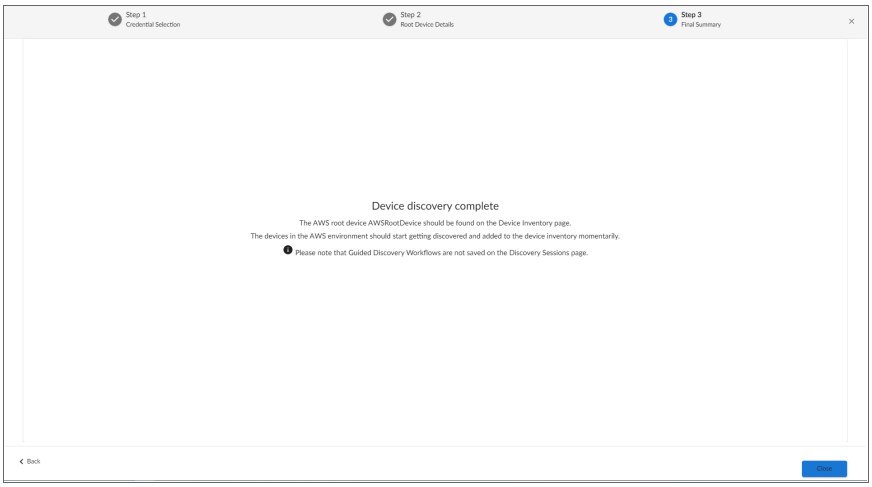


NOTE: During the guided discovery process, you cannot click **[Next]** until the required fields are filled on the page, nor can you skip to future steps. However, you can revisit previous steps that you have already completed.

4. On the **Credential Selection** page of the guided discovery process, select the Azure credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.



5. Complete the following fields:
   - ***Root Device Name***. Type the name of the root device for the Microsoft Azure root device you want to monitor.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
   - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.
6. Click **[Next]**. Skylar One creates the Microsoft Azure root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.



7. Click **[Close]**.

NOTE: The results of a guided discovery do not display on the **Discovery Sessions** page (Devices > Discovery Sessions).

Discovering Microsoft Azure Devices in the Classic Skylar One User Interface

If you are using the classic Skylar One user interface, or you do not want to use *the guided discovery workflow to discover your Azure devices*, you can discover your Azure devices using an alternative method. In this scenario, you create a virtual device representing your Azure service and then manually align a discovery Dynamic Application to that virtual device. The following sections describe that process.

Creating an Azure Virtual Device for Discovery

Because the Azure service does not have a static IP address, you cannot use standard discovery to locate Azure devices. Instead, you must create a ***virtual device*** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by Skylar One. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Azure service:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Enter values in the following fields:
   - ***Device Name***. Enter a name for the device. For example, "Azure Cloud".
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits which users can view and edit it. Typically, only members of that organization can view and edit the device.
   - ***Device Class***. Select *Microsoft | Azure Services*.
   - ***Collector***. Select the collector group that will monitor the device.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how Skylar One monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For more information, see the section on *Load-Balancing an Account with Multiple Subscriptions*.

4. Click **[Add]** to create the virtual device.

Aligning the Azure Dynamic Applications

The Dynamic Applications in the "Microsoft: Azure" PowerPack are divided into the following types:

- ***Discovery***. These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll Azure for performance metrics.

When configuring Skylar One to monitor Azure services, you can manually align Dynamic Applications to discover Azure component devices.

Discovering Azure Component Devices

To discover all the components of your Azure platform, you must manually align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device.

> **TIP:** When monitoring an account with multiple child subscriptions, ScienceLogic recommends that you first review your device capacity and load limits to determine the best method for implementation before discovery. For more information, see the section on *Load-Balancing an Account with Multiple Subscriptions*.

To manually align the "Microsoft: Azure Account Discovery" Dynamic Application:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Click the wrench icon (🔧) for your Azure virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the actions icon and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:
    - In the ***Dynamic Applications*** field, select *Microsoft: Azure Account Discovery*.
    - In the ***Credentials*** field, select the credential you created for your Azure service.
6. Click **[Save]** to align the Dynamic Application with the Azure virtual device.

When you align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device, Skylar One does one of the following, depending on your subscription model:

- If you are monitoring an account with multiple child subscriptions, Skylar One creates a root component device representing the Azure account and one or more child component devices representing all of your Azure subscriptions.
- If you are monitoring a single subscription, Skylar One creates a root component device representing your Azure subscription.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how Skylar One monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For more information, see the section on *Load-Balancing an Account with Multiple Subscriptions*.

Skylar One then automatically aligns several other Dynamic Applications to the subscription component devices. These additional Dynamic Applications discover and create component devices for Active Directory tenants, Traffic Manager profiles, and each location used by the Azure account. Under each location, Skylar One then discovers component devices relevant to the Azure service.

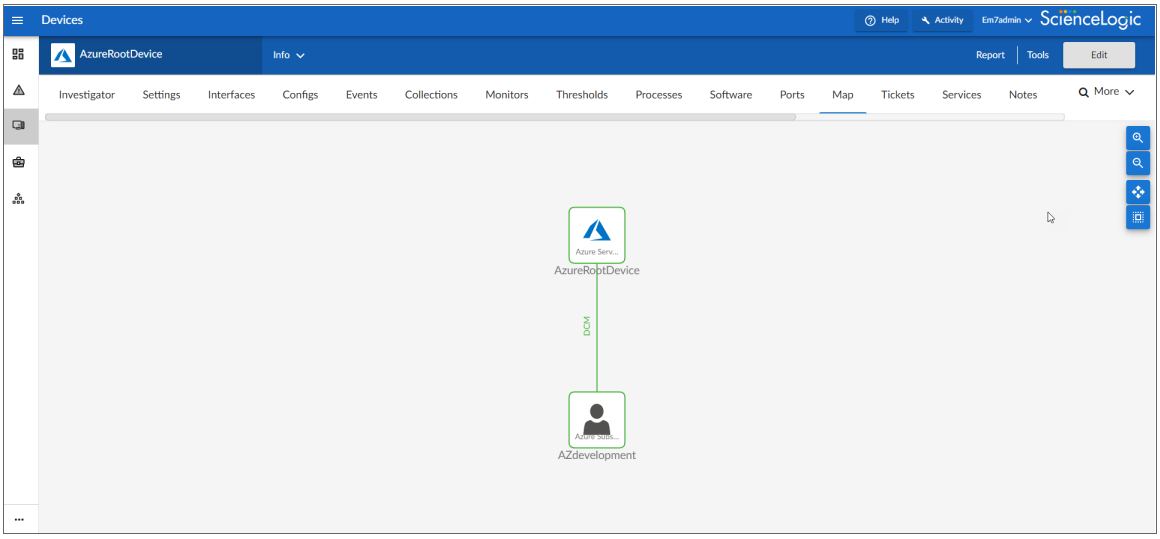
NOTE: Skylar One might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

NOTE: When discovering a large number of component devices, such as when discovering an account with multiple child subscriptions, the discovery process can cause the appearance of numerous critical events with the message, "`Large backlog of asynchronous jobs detected`". This will occur only during the initial discovery session.

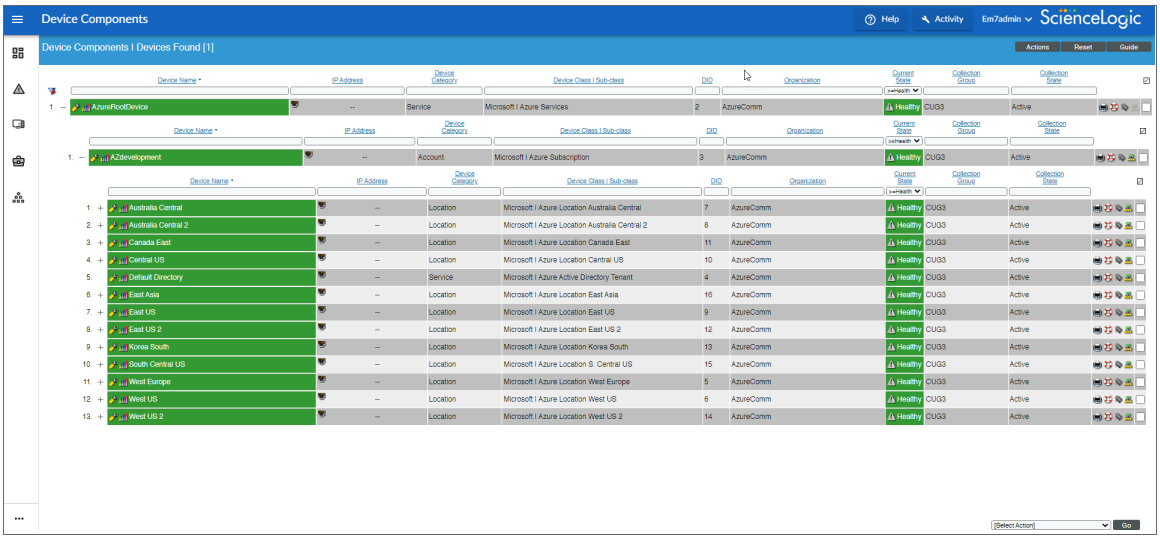
Viewing Azure Component Devices

In addition to the **Devices** page, you can view the Azure service and all associated component devices in the following places in the user interface:

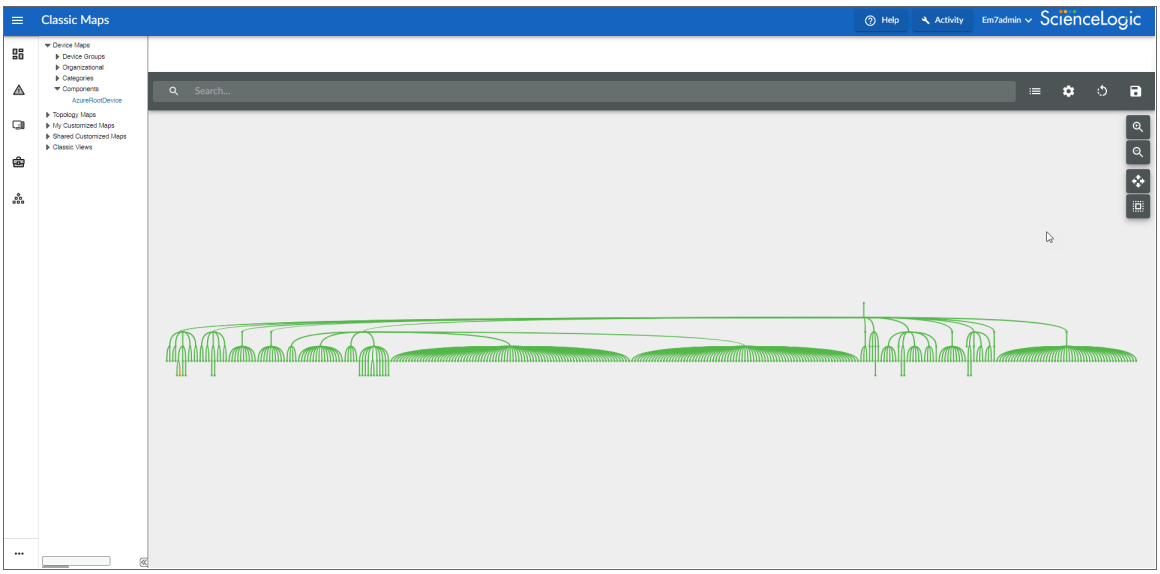
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. If you double-click any of the listed devices, the page reloads and makes that device the primary device.



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by Skylar One. This page uses an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an Azure service, find the Azure service and click its plus icon (**+**).



- Use the **Component Map** page (Classic Maps > Device Maps > Components) to view devices by root node and see the relationships between root nodes, parent components, and child components in a map. You can use this map to visualize and manage root nodes and their components. Skylar One automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for an Azure service, go to the **Component Map** page and select the map from the list in the left navigation bar. To learn more about the **Component Map** page, see the ***Maps*** manual.



Relationships Between Component Devices

In addition to parent/child relationships between component devices, Skylar One also creates relationships between the following component devices:

- API Apps and Resource Groups
- API Management and System Topics
- App Configuration and System Topics
- App Service and System Topics
- Apps and Resource Groups
- Application Gateways and Resource Groups
- Application Gateways and Virtual Network Subnets
- Azure Automation and Resources Groups
- Azure CosmosDB and Resource Groups
- Azure CosmosDB and Virtual Networks
- Azure CosmosDB and Virtual Network Subnets
- Azure Maps and System Topics
- Azure Policies and System Topics
- Azure Subscriptions and System Topics
- Azure Traffic Managers and Traffic Managers
- Batch Accounts and Key Vaults
- Batch Accounts and Resource Groups
- Batch Accounts and Storage Groups
- Blob Storage and System Topics
- CDN Profiles and Resource Groups
- Communication Services and System Topics
- Container Instances and Resource Groups
- Container Registries and Resource Groups
- Container Registries and System Topics
- Data Lakes and Resource Groups
- Data Lakes and Storage Accounts
- Databricks and Resource Groups
- Databricks and Storage Accounts
- Event Grids and Resource Groups
- Event Hubs and System Topics
- HDInsight Clusters and Storage Groups

- HDInsight Clusters and Virtual Networks
- HDInsight Clusters and Resource Groups
- Health Data Services and System Topics
- Host Pools and Resource Groups
- Host Pools and Virtual Machines
- IoT Hubs and System Topics
- Key Vaults and Resource Groups
- Key Vaults and System Topics
- Key Vaults and Virtual Networks
- Key Vault Rules and Subnets
- Kubernetes Agent Pools and Subnets
- Kubernetes Services and System Topics
- Load Balancers and Resource Groups
- Logic Apps and Resource Groups
- Machine Learning Services and System Topics
- Managed Disks and Resource Groups
- Managed Disks and Virtual Machines
- Media Services and System Topics
- Network Security Groups and Resource Groups
- Network Security Groups and Virtual Network Subnets
- PostgreSQL Servers and Resource Groups
- PostgreSQL Servers and Subnets
- PostgreSQL Servers and PostgreSQL Server Replicas
- PostgreSQL Servers and Virtual Networks
- Recovery Service Vaults and Resource Groups
- Redis Cache Servers and Redis Cache Servers
- Redis Caches and Resource Groups
- Redis Caches and Subnets
- Redis Caches and System Topics
- Redis Caches and Virtual Networks
- Resource Groups and System Topics
- Service Bus Namespaces and Resource Groups
- Service Bus Namespaces and Service Bus Namespaces
- Service Bus Namespaces and Subnets
- Service Bus Namespaces and System Topics
- Service Bus Namespaces and Virtual Networks

- SignalR and System Topics
- SQL Databases and Resource Groups
- SQL Servers and Resource Groups
- SQL Servers and Server Replicas
- SQL Servers and Subnets
- SQL Servers and Virtual Networks
- SQL Servers and Virtual Network Subnets
- Storage Accounts and Resource Groups
- Traffic Manager Profiles and Resource Groups
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups
- Virtual Machines and Storage Accounts
- Virtual Machines and Virtual Networks
- Virtual Machines and Virtual Network Subnets
- Virtual Machine Scale Sets and Load Balancers
- Virtual Machine Scale Sets and Resource Groups
- Virtual Machine Scale Sets and Virtual Network Subnets
- Virtual Machine Scale Set Virtual Machines and Resource Groups
- Virtual Networks and Resource Groups
- VPN Gateways and Resource Groups
- VPN Gateways and Virtual Network Subnets
- WAF CDN Policies and Endpoints
- WAF CDN Policies and Resource Groups
- WAF Gateway Policies and Application Gateways
- WAF Gateway Policies and Resource Groups

Additionally, the platform can automatically build relationships between Azure component devices and other associated devices:

- If you discover Cisco Cloud Center devices using the Dynamic Applications in the "Cisco: CloudCenter" PowerPack version 103 or later, Skylar One automatically creates relationships between Azure Virtual Machines and Cisco Cloud Center applications.
- If you discover Dynatrace environments using the Dynamic Applications in the "Dynatrace" PowerPack, Skylar One automatically creates relationships between the following device types:
    - Azure Virtual Machines and Dynatrace Hosts
    - Azure Virtual Machine Scale Sets and Dynatrace Hosts

- If you discover Office 365 services using the Dynamic Applications in the "Microsoft: Office 365" PowerPack version 101 or later, Skylar One automatically creates relationships between Azure Active Directory tenants and Office 365 Active Directory tenants.

Chapter 4

Monitoring Azure Unified Alerts

Overview

This section describes the Azure unified alert Event Policies that are included in the "Microsoft: Azure" PowerPack and information about configuring Azure and Skylar One to generate events based on Azure unified alerts.

This chapter covers the following topics:

Prerequisites for Configuring Azure Unified Alerts *46*

Azure Unified Alert Event Policies *47*

Enabling the "Microsoft: Azure Unified Alerts Performance" Dynamic Application *48*

Viewing Azure Unified Alert Counts *48*

Prerequisites for Configuring Azure Unified Alerts

In addition to Skylar One collecting metrics for Azure resources, you can configure Azure to send alert information to Skylar One via API. Skylar One can then generate an event for each alert.

To monitor Azure unified alerts, you must first configure Azure to proactively send alerts when important conditions are found in your Azure monitoring data. Azure bases these alerts on metrics and activity logs, and raises them when the alert's monitor condition is set to "fired".

You must also create alert rules in Azure that determine the following:

- The resource that the alert is targeting
- The signal from the target resource that could trigger the alert

- The logic that determines whether the signal from the target resource actually triggers the alert

For details about how to create and manage alert rules, see https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview.

Azure Unified Alert Event Policies

The "Microsoft: Azure" PowerPack includes several pre-defined event policies for unified alerts, based on their severity:

Event Policy Name	Event Source	Severity
Microsoft: Azure Alert Severity 0	API	Critical
Microsoft: Azure Alert Severity 1	API	Major
Microsoft: Azure Alert Severity 2	API	Minor
Microsoft: Azure Alert Severity 3	API	Notice
Microsoft: Azure Alert Severity 4	API	Notice
Microsoft: Azure Alert Severity 0 Resolved Microsoft: Azure Alert Severity 1 Resolved Microsoft: Azure Alert Severity 2 Resolved Microsoft: Azure Alert Severity 3 Resolved Microsoft: Azure Alert Severity 4 Resolved	API	Healthy

NOTE: The Healthy events trigger when the alert's monitor condition is "resolved" or the alert state is "acknowledged" or "closed".

These events are aligned to Azure component devices in the following way:

- If Skylar One can determine the specific Azure resource that generated the alert, it checks whether that resource is discovered as a component device. If so, Skylar One aligns the event with that resource's component device.
- If Skylar One cannot determine the specific resource, it checks whether it can determine the Azure service that generated the alert instead. If that service is discovered as a component device, Skylar One aligns the event with that service's component device.
- In version 122 and later of the "Microsoft: Azure" PowerPack, if Skylar One cannot determine an appropriate resource or service component device, it aligns the event with the Azure subscription component device. If you do not want alerts aligned with the Azure subscription component device, then you can *disable that feature*.

Enabling the "Microsoft: Azure Unified Alerts Performance" Dynamic Application

The "Microsoft: Azure" PowerPack also includes a "Microsoft: Azure Unified Alerts Performance" Dynamic Application. This Dynamic Application collects alerts from the Azure API for all available resources and associates the alerts with the appropriate Azure component devices in Skylar One, if applicable. If an appropriate component device does not exist in Skylar One or cannot be determined, Skylar One instead associates the alert with the component device for the Azure subscription.

You must enable this Dynamic Application if you want Skylar One to generate unified alert events.

To enable the "Microsoft: Azure Unified Alerts Performance" Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. Locate the "Microsoft: Azure Unified Alerts Performance" Dynamic Application and then click its wrench icon (🔧). The **Dynamic Applications Properties Editor** page appears.
3. In the ***Operational State*** field, select *Enabled*.
4. Click **[Save]**.

Starting in version 122 of the "Microsoft: Azure" PowerPack, you can opt to disable unified alert collection for an entire Azure subscription using the "Enable Unified Alert Collection" threshold object in the "Microsoft: Azure Unified Alerts Performance" Dynamic Application.

To configure this threshold:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. Locate the "Microsoft: Azure Unified Alerts Performance" Dynamic Application and then click its wrench icon (🔧). The **Dynamic Applications Properties Editor** page appears.
3. Click the ***Thresholds*** tab.
4. Locate the "Enable Unified Alert Collection" threshold object and click its wrench icon (🔧).
5. In the ***Threshold Value*** field, type "0".
6. Click **[Save]**.

Viewing Azure Unified Alert Counts

After you have enabled the "Microsoft: Azure Unified Alerts Performance" Dynamic Application and it has begun collecting alerts from the Azure API, you can view a count of the total number of alerts generated for each severity level for a given component device.

NOTE: By default, the "Microsoft: Azure Unified Alerts Performance" Dynamic Application collects alerts over a one-day period.

To view Azure unified alert counts:

1. Go to the **Device Components** page (Devices > Device Components).
2. Click the plus-sign icon (+) for your Azure service until you locate the Azure component device for which you want to see an alert count. Click its graph icon (). The **Device Summary** page appears.
3. Click the **[Performance]** tab. The **Device Performance** page appears.
4. Click the **Microsoft: Azure Unified Alerts Performance** link to expand the options listed, and then select the alert severity for which you want to see metrics. The performance graph displays a graph detailing the count for your selected alert severity over the selected timespan.

Chapter 5

Azure Run Book Actions and Automations

Overview

This section describes how to use the run book action and automation policies that are included in the "Microsoft: Azure" PowerPack.

This chapter covers the following topics:

Azure Run Book Automation Permissions *50*

About the Azure Run Book Actions and Automations *51*

Disabling VMs or Storage Disks by VM Tag *52*

Disabling Databricks by Tag *56*

Discovering VMs and Merging Physical Devices with Components *60*

Vanishing Terminated or Terminating VM Instances *67*

Azure Run Book Automation Permissions

If you use a custom database user, or you use RDS instead of the central database credential that connects as root, you must set the following permissions in your database. These permissions are required to use the run book automations in the "Microsoft: Azure" PowerPack:

```
GRANT EXECUTE ON PROCEDURE 'master'.'process_unmerge_devices' TO 'azure_
pp_rba'@'%';
```

```
GRANT EXECUTE ON FUNCTION 'master'.'primary_db_id' TO 'azure_pp_rba'@'%';
```

```
GRANT EXECUTE ON PROCEDURE 'master'.'process_merge_devices' TO 'azure_pp_
rba'@'%';
```

About the Azure Run Book Actions and Automations

The "Microsoft: Azure" PowerPack includes Run Book Actions and Run Book Automation policies that can be used to:

- Automatically disable data collection for Virtual Machines, Virtual Machine Scale Sets (VMSS), and Storage Disks based on their VM tag
- Automatically disable data collection for Databricks based on tags
- Automatically create and start a discovery session using the public or private IP address of a Virtual Machine, and after the device is discovered, merge the physical device with the corresponding component
- Automatically move a Virtual Machine to a vanished state if the component is in a terminated state

The following table describes the Run Book Automation policies and what they do:

Run Book Automation Policy Name	Result
Microsoft Azure: Disable and Discover from IP	If a component device belongs to the Virtual Machines device group and has a relevant Azure tag, Skylar One disables the device.
Microsoft Azure: Disable Storage Disks	If a component device belongs to the Storage Disks device group and has a relevant Azure tag, Skylar One disables the device.
Microsoft Azure: Discover from IP	Skylar One automatically discovers VM instances by public or private IP address.
Microsoft Azure: Merge with VM	If Skylar One finds the "Device Record Created" event on the newly discovered physical device, Skylar One merges the newly discovered physical device with the corresponding component device.
Microsoft Azure: Vanish Terminated VMs	If a device is in a terminated or terminating state, Skylar One un-merges the VM instance and physical device (if applicable), clears the device's associated events, and then moves the device to a vanished state.
Microsoft: Azure Data Lake Devices Classification Required	Assigns the correct device class to Storage Account devices.
Microsoft: Azure Resource Reclassification	Aligns the correct device class to fully-supported Azure services, and then tries to unalign the Resource List Configuration Dynamic Application.
Microsoft Azure: Disable Databricks	If a component device belongs to the Databricks device group and has a relevant Azure tag, Skylar One disables the device.

> **NOTE:** The Run Book Automation policies in the "Microsoft: Azure" PowerPack are disabled by default. To use these Run Book Automations, you must enable the Run Book Automation policies and modify the parameters in the Run Book Actions as needed. See the following procedures for more information.

As a prerequisite for discovering physical devices, make sure that traffic to the following ports is allowed in the inbound security rules on the Azure Portal for a Virtual Machine:

- **Port 161**. Allows the discovery session to use SNMP credentials.
- **Ports 5985, 5986**. Allows the discovery session to use PowerShell credentials.

If the above ports are not open or cannot be opened, you can include extra credentials for the discovery session by modifying the following parameter in the "Microsoft Azure: Discover from IP" Run Book Action, using a comma-separated list of credential IDs:

```
EXTRA_CREDS = "<ID1>,<ID2>,<ID3>"
```

> **NOTE:** When a discovery session is given a list of credentials, the system uses the first credential that successfully authenticates to discover a physical device.

For more information about Microsoft Azure inbound security rules, see the following Microsoft article: How to open ports to a virtual machine with the Azure portal.

Disabling VMs or Storage Disks by VM Tag

> **NOTE:** The following Run Book Automation policies do not enable data collection for Azure VMs or Storage Disks. You must manually enable data collection for these VMs or Storage Disks.

Run Book Automation Policy: Disable and Discover from IP

The "Disable and Discover from IP" Run Book Automation policy runs only on newly discovered VMs. The policy takes no action for existing VMs.

The automation for disabling Azure VMs or Azure VMSSs includes the following Run Book Actions, which are executed in the following order:

- ***Microsoft Azure: Get Unique ID***. This action retrieves the unique ID of the component. This action runs on the Database Server.
- ***Microsoft Azure: Collect VM Configuration***. This action retrieves the VM configuration, including the tags used to disable the VM. This action runs on the Collector.
- ***Microsoft Azure: Disable By VM Tag***. If a newly discovered VM contains the tags specified in the snippet, this action disables collection for this component.
- ***Microsoft Azure: Discover from IP***. If the VM is running and is newly discovered, this action creates the discovery session and runs automatically to discover the physical device. This action will *not* create a discovery session for a discovered VM that was disabled right after being discovered. By default the snippet uses the public IP address and PowerShell (unless you specify SNMP) to create the discovery session. You can update these parameters as needed.

The following Run Book Automation policy triggers the above Run Book Actions:

- ***Microsoft Azure: Disable and Discover from IP***. This Run Book Automation policy executes when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this Run Book Automation policy if you want to disable VM instances by Azure tag *and* want to enable automated discovery of VM instances by public or private IP address. This policy is configured to run both processes in the correct order for VM instances.

Run Book Automation Policy: Disable Storage Disks

The "Disable Storage Disks" Run Book Automation policy runs only on newly discovered Storage Disks. The policy takes no action for existing Storage Disks.

The automation for disabling Azure Storage Disks includes the following Run Book Actions, which are executed in the following order:

- ***Microsoft Azure: Get Unique ID***. This action retrieves the unique ID of the component. This action runs on the Database Server.
- ***Microsoft Azure: Collect Storage Disk Configuration***. This action retrieves disk and VM configurations, including the tags that belong to the VM used by the Storage Disk. This action runs on the Collector.
- ***Microsoft Azure: Disable By VM Tag***. If a newly discovered Storage Disk belongs to a VM that contains the tags specified in the snippet, this action disables collection for the component.

The following Run Book Automation policy triggers the above actions:

- ***Microsoft Azure: Disable Storage Disks***. This Run Book Automation policy executes when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this policy if you want to disable Storage Disk instances by Azure tag, but do not want to enable automated discovery of Storage Disk instances by public or private IP address.

Configuration Steps

To use these automations, you must:

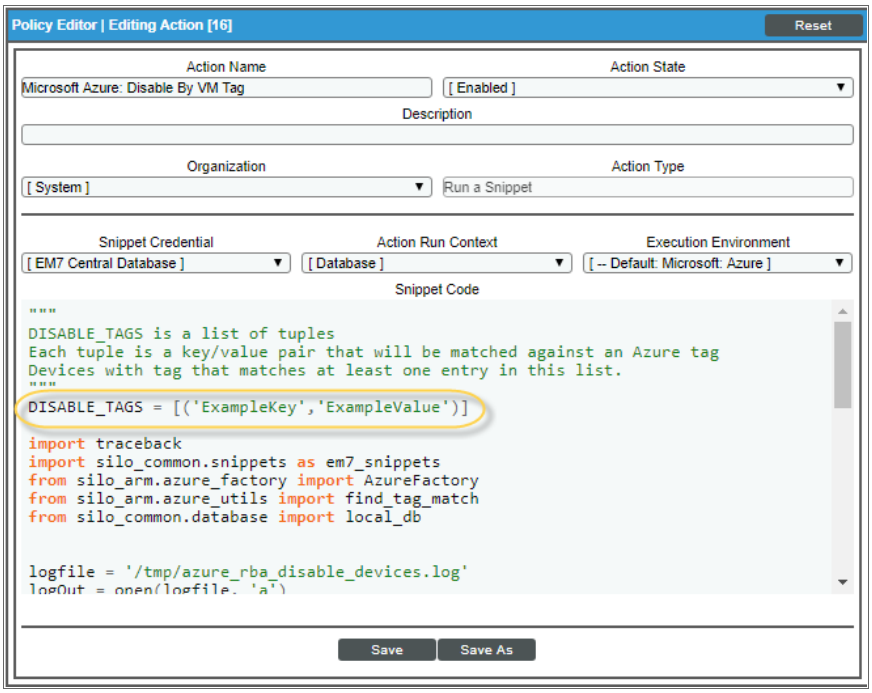
- *Modify the parameters of the "Disable By VM Tag" Run Book Action*
- *Enable the "Component Device Record Created" event policy*
- *Enable the Run Book Automation policies*
- *Configure your system to preserve these changes*

Modifying the Parameters of the "Disable By VM Tag" Run Book Action

The snippet for the "Microsoft Azure: Disable by VM Tag" Run Book Action includes the pre-defined list of key/value pairs that Skylar One compares to the tags collected from Azure. You must modify this list to include the key/value pairs that you want to use to disable VM instances.

To modify the parameters for the "Microsoft Azure: Disable by VM Tag" Run Book Action:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Click the wrench icon (🔧) for the "Microsoft Azure: Disable by VM Tag" Run Book Action.



3. In the ***Snippet Code*** field, locate and edit the following line:

```
DISABLE_TAGS = [('ExampleKey','ExampleValue')]
```

The line must be in the following format: each key and value inside single-quotes, each key/value pair inside parentheses, and each pair separated by a comma.

```
DISABLE_TAGS = [('Key','Value'),('Key','Value'),...,('Key','Value')]
```

For example, suppose you want to disable a VM instance where the "Environment" key is either "dev" or "test" or the "Owner" key is "Sales." You would update the line so it looks like this:

```
DISABLE_TAGS = [('Environment','dev'),('Environment','test'),
('Owner','Sales')]
```

4. When you are done editing, click the **[Save]** button.

Enabling the "Component Device Record Created" Event Policy

To enable the "Component Device Record Created" event policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon (🔧) for the "Component Device Record Created" event policy.
3. In the ***Operational State*** field, select *Enabled*.
4. Click **[Save]**.

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the ***Selective PowerPack Field Protection*** option. To enable this option:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Check the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click **[Save]**.

Enabling the Run Book Automation Policies

To enable one or more Run Book Automation policies in the "Microsoft: Azure" PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the wrench icon (🔧) for the Run Book Automation policy you want to enable.
3. In the ***Policy State*** field, select *Enabled*.
4. Click **[Save]**.

Preserving Automation Changes

If you have modified Run Book Actions and Run Book Automation policies that are included in the "Microsoft: Azure" PowerPack, updating the PowerPack on your system overwrites those changes. If you have modified Run Book Actions and Run Book Automation policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the "Microsoft: Azure"PowerPack.
- Remove the content from the PowerPack on your system. When the "Microsoft: Azure" PowerPack is updated in your system, the system does not install updated versions of this content, and preserves your local changes.

To remove Run Book Action or Run Book Automation policy content from the "Microsoft: Azure" PowerPack on your system:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the wrench icon ( ) for the "Microsoft: Azure" PowerPack. The **Editing PowerPack** page appears.
3. In the left navigation bar of the **Editing PowerPack** page, select the type of content you want to remove:
   - To remove a Run Book Action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
   - To remove a Run Book Automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
4. In the upper pane, click the delete icon ( ) for each Run Book Action or Run Book Automation policy that you want to remove from the "Microsoft: Azure" PowerPack on your system.

Disabling Databricks by Tag

> **NOTE**: The following Run Book Automation policy does not enable data collection for Azure Databricks. You must manually enable data collection for these Databricks.

Run Book Automation Policy: Disable Databricks

The "Disable Databricks" Run Book Automation policy runs only on newly discovered Databricks. The policy takes no action for existing Databricks.

The automation for disabling Azure Databricks includes the following Run Book Actions, which are executed in the following order:

- ***Microsoft: Azure Get Unique ID***. This action retrieves the unique ID of the component. This action runs on the Database Server.
- ***Microsoft: Azure Collect Databricks Configuration***. This action retrieves Databricks configurations, including the tags. This action runs on the Data Collector.

- ***Microsoft: Azure Disable By Databrick Tag***. If a newly discovered Databricks contains the tags specified in the snippet, this action disables collection for the component. This action runs on the Database Server.

The following Run Book Automation policy triggers the above actions:

- ***Microsoft Azure: Disable Databricks***. This Run Book Automation policy executes when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this policy if you want to disable Databricks instances by Azure tag.

Configuration Steps

To use these automations, you must:

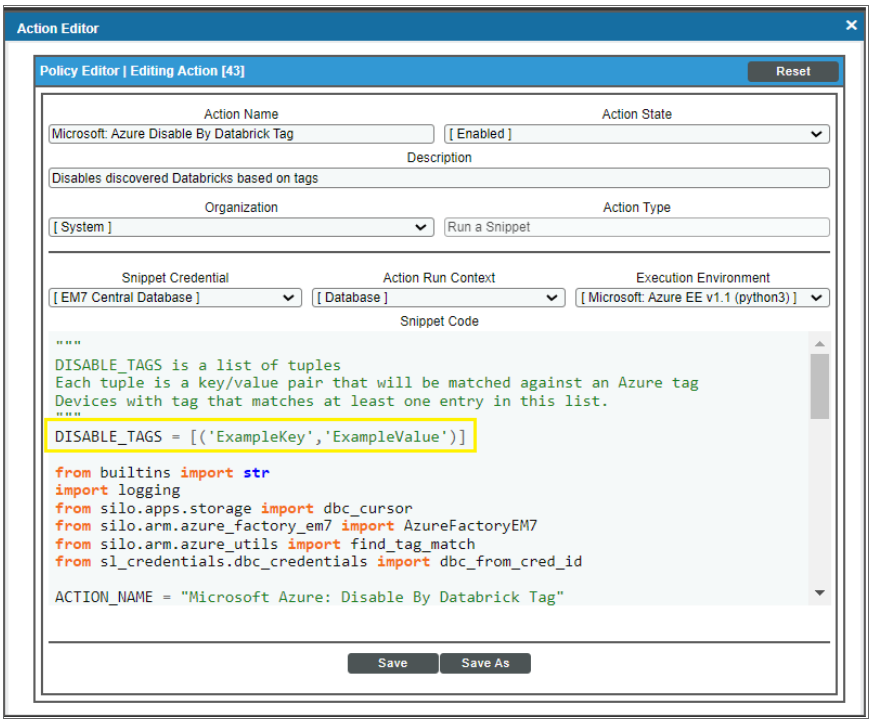
- *Modify the parameters of the "Disable by Databrick Tag" Run Book Action*
- *Enable the "Component Device Record Created" event policy*
- *Enable the Run Book Automation policies*
- *Configure your system to preserve these changes*

Modifying the Parameters of the "Disable By Databrick Tag" Run Book Action

The snippet for the "Microsoft: Azure Disable By Databrick Tag" Run Book Action includes the pre-defined list of key/value pairs that Skylar One compares to the tags collected from Azure. You must modify this list to include the key/value pairs that you want to use to disable Databricks instances.

To modify the parameters for the "Microsoft: Azure Disable By Databrick Tag" Run Book Action:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Click the wrench icon (🔧) for the "Microsoft: Azure Disable By Databrick Tag" Run Book Action.



3. In the ***Snippet Code*** field, locate and edit the following line:

```
DISABLE_TAGS = [('ExampleKey','ExampleValue')]
```

The line must be in the following format, with each key and each value inside single-quotes and each key/value pair comma-separated inside parentheses, with commas separating each key/value pair.

```
DISABLE_TAGS = [('Key','Value'),('Key','Value'),...,
('Key','Value')]
```

For example, suppose you want to disable a VM instance where the "Environment" key is "dev" or "test," or the "Owner" key is "Sales." Update the line so it looks like this:

```
DISABLE_TAGS = [('Environment','dev'),('Environment','test'),
('Owner','Sales')]
```

4. Click **[Save]**.

Enabling the "Component Device Record Created" Event Policy (Discover from IP Only)

To enable the "Component Device Record Created" event policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon (🔧) for the "Component Device Record Created" event policy.
3. In the ***Operational State*** field, select *Enabled*.
4. Click **[Save]**.

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the ***Selective PowerPack Field Protection*** option. To enable this option:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Check the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click **[Save]**.

Enabling the Run Book Automation Policies

To enable one or more Run Book Automation policies in the "Microsoft: Azure" PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the wrench icon (🔧) for the Run Book Automation policy you want to enable.
3. In the ***Policy State*** field, select *Enabled*.
4. Click **[Save]**.

Preserving Automation Changes

If you have modified Run Book Actions and Run Book Automation policies that are included in the "Microsoft: Azure" PowerPack, updating the PowerPack on your system overwrites those changes. If you have modified Run Book Actions and Run Book Automation policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the "Microsoft: Azure"PowerPack.
- Remove the content from the PowerPack on your system. When the "Microsoft: Azure" PowerPack is updated in your system, the system does not install updated versions of this content, and preserves your local changes.

To remove Run Book Action or Run Book Automation policy content from the "Microsoft: Azure" PowerPack on your system:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the wrench icon ( ) for the "Microsoft: Azure" PowerPack. The **Editing PowerPack** page appears.
3. In the left navigation bar of the **Editing PowerPack** page, select the type of content you want to remove:
    - To remove a Run Book Action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
    - To remove a Run Book Automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
4. In the upper pane, click the delete icon ( ) for each Run Book Action or Run Book Automation policy that you want to remove from the "Microsoft: Azure" PowerPack on your system.

Discovering VMs and Merging Physical Devices with Components

Run Book Automation Policy: Discover from IP

The "Discover from IP" Run Book Automation policy runs only on newly discovered VMs. The policy takes no action for existing VMs.

The automation for discovering Azure VMs or VMSSs by public or private IP addresses and then discovering the physical device includes three Run Book Actions that are executed in the following order:

- ***Microsoft Azure: Get Unique ID***. This action retrieves the unique ID of the component. This action runs on the Database Server.
- ***Microsoft Azure: Collect VM Configuration***. This action retrieves the VM configuration, including public or private IP address and open ports. This action runs on the Collector.
- ***Microsoft Azure: Discover from IP***. If the VM is running and is newly discovered, this action creates the discovery session and runs automatically to discover the physical device. The discovery session name uses the following format: **Azure_VM-*IP_address***.

The following Run Book Automation policy triggers the above Run Book Actions:

- ***Microsoft Azure: Discover From IP***. This Run Book Automation policy executes when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Use this action to enable automated discovery of VM instances by public or private IP address. By default the snippet uses the public IP address and PowerShell (unless you specify SNMP) to create the discovery session. You can update these parameters as needed.

> **NOTE:** If a VM was created as "Stopped" by default, and that VM was discovered by the PowerPack, the Run Book Action does not create a discovery session. The action cannot collect an IP address for a stopped VM.

Run Book Automation Policy: Merge with VM

When the "Merge with VM" Run Book Automation policy finds the "Device Record Created" event on the newly discovered physical device, the policy triggers the following Run Book Action:

- ***Microsoft Azure: Merge Physical with Component***. This action merges the newly discovered physical device with the corresponding component device.

The "Merge with VM" Run Book Automation policy runs only on newly discovered devices. The policy takes no action for existing VMs. The discovery session created with the "Discover from IP" Run Book Action, above, discovers the physical device.

Configuration Steps

To use these automations, you must:

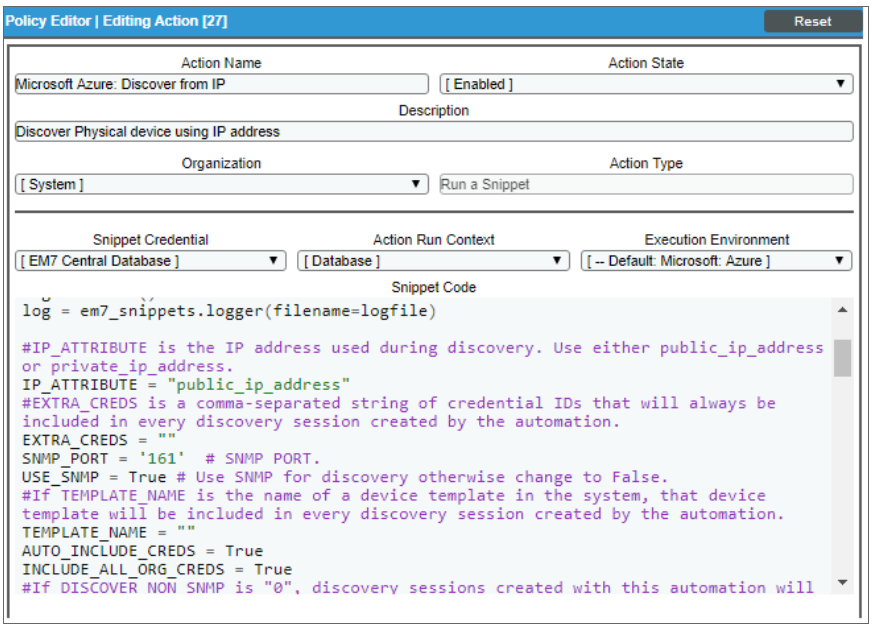
- *Modify the parameters of the Run Book Actions*
- *Enable the "Component Device Record Created" event policy* (Discover from IP policy only)
- *Enable the "Device Record Created" event policy*
- *Enable the Run Book Automation policies*
- *Configure your system to preserve these changes*

Modifying the Parameters of the Run Book Actions

The snippet for the "Microsoft Azure: Discover from IP" Run Book Action includes parameters that define how the Run Book Action creates discovery sessions. By default the snippet uses the public IP address and PowerShell (unless you specify SNMP) to create the discovery session. You can update these parameters as needed.

To modify the parameters for the "Microsoft Azure: Discover from IP" Run Book Action:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Click the wrench icon (🔧) for the "Microsoft Azure: Discover from IP" Run Book Action.
3. In the ***Snippet Code*** field, locate and edit the lines for the parameters you want to change:



4. As needed, update the following lines:
   - Discovery uses the PowerShell credential by default.

> **NOTE:** For Linux servers, add the user-defined credentials in the `EXTRA_CREDS` parameter.

   - To change from the default public IP address to *private* IP address:

     ```
     IP_ATTRIBUTE = 'private_ip_address'
     ```

     If you change the IP address value to private for this Run Book Action, then you must also update the following line in the "Microsoft Azure: Merge with VM" Run Book Action:

     ```
     IP_ATTRIBUTE = 'c-VM-public_ipaddress"'
     ```

- To include additional user-defined credentials in the discovery session, use a comma-separated list of credential IDs:

  ```
  EXTRA_CREDS = "<ID1>,<ID2>,<ID3>"
  ```

- If you want to use `EXTRA_CREDS` only, set `AUTO_INCLUDE_CREDS` to `False`:

  ```
  AUTO_INCLUDE_CREDS = False
  ```

- To apply a device template to all newly discovered physical devices, specify the name of the template:

  ```
  TEMPLATE_NAME = "<Name>"
  ```

- To disable the automatic alignment of credentials to the discovery session, change this line to:

  ```
  AUTO_INCLUDE_CREDS = False
  ```

- If `INCLUDE_ALL_ORG_CREDS` is "True" and the `AUTO_INCLUDE_CREDS` parameter is "True",," credentials that are aligned with all organizations (credentials that do not have an explicit organization alignment) are automatically included in the discovery session when that credential meets the other requirements for being automatically included in the discovery session.

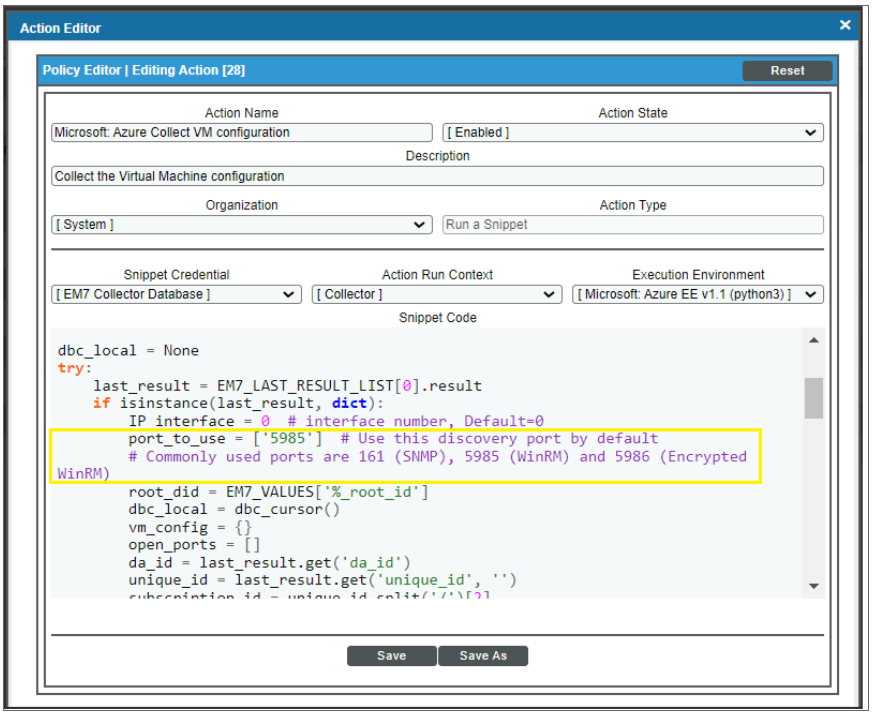
  ```
  INCLUDE_ALL_ORG_CREDS = True
  ```

- To enable discovery using SNMP credentials, update the following lines:

  ```
  USE_SNMP = True
  ```

  ```
  DISCOVER_NON_SNMP = '0'
  ```

5. Click the wrench icon (🔧) for the "Microsoft Azure: Collect VM configuration" Run Book Action.
6. In the ***Snippet Code*** field, locate and edit the `port_to_use` variable with the desired discovery port.



5. When you are done editing, click the **[Save]** button.

Enabling the "Component Device Record Created" Event Policy (Discover from IP Only)

To enable the "Component Device Record Created" event policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon (🔧) for the "Component Device Record Created" event policy.
3. In the ***Operational State*** field, select *Enabled*.
4. Click **[Save]**.

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the ***Selective PowerPack Field Protection*** option. To enable this option:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Check the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click **[Save]**.

Enabling the "Device Record Created" Event Policy

To enable the "Device Record Created" event policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon (🔧) for the "Device Record Created" event policy.
3. In the ***Operational State*** field, select *Enabled*.
4. Click **[Save]**.

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the ***Selective PowerPack Field Protection*** option. To enable this option:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Check the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click **[Save]**.

Enabling the Run Book Policies

To enable one or more Run Book Automation policies in the "Microsoft: Azure" PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the wrench icon (🔧) for the Run Book Automation policy you want to enable.
3. In the ***Policy State*** field, select *Enabled*.
4. Click **[Save]**.

Preserving Automation Changes

If you have modified Run Book Actions and Run Book Automation policies that are included in the "Microsoft: Azure" PowerPack, updating the PowerPack on your system overwrites those changes. If you have modified Run Book Actions and Run Book Automation policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the "Microsoft: Azure"PowerPack.
- Remove the content from the PowerPack on your system. When the "Microsoft: Azure" PowerPack is updated in your system, the system does not install updated versions of this content, and preserves your local changes.

To remove Run Book Action or Run Book Automation policy content from the "Microsoft: Azure" PowerPack on your system:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the wrench icon ( ) for the "Microsoft: Azure" PowerPack. The **Editing PowerPack** page appears.
3. In the left navigation bar of the **Editing PowerPack** page, select the type of content you want to remove:
    - To remove a Run Book Action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
    - To remove a Run Book Automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
4. In the upper pane, click the delete icon ( ) for each Run Book Action or Run Book Automation policy that you want to remove from the "Microsoft: Azure" PowerPack on your system.

Vanishing Terminated or Terminating VM Instances

If a device is in a terminated or terminating state, the "Vanish Terminated VMs" Run Book Action un-merges the VM instance and physical device (if applicable), clears the device's associated events, and then moves the device to a vanished state.

The "Vanish Terminated VMs" Run Book Automation policy runs only on newly discovered VMs. The policy takes no action for existing VMs.

The automation for vanishing terminated VM instances includes the following Run Book Actions:

- ***Microsoft Azure: Get Unique ID***. This action retrieves the unique ID of the component. This action runs on the Database Server.
- ***Microsoft Azure: Check VM Availability***. This action uses the unique ID of the component to get the device availability status. If the device availability status is "Terminated",," this action moves to the following Run Book Action, "Vanish Terminated VMs".." This action runs on the Collector.
- ***Microsoft Azure: Vanish Terminated VMs***. This action moves the device to the Vanish state when the VM has been terminated in the Azure Portal. This action runs on the Database Server. This action determines if the component was merged with a physical device:
  - If the component was not merged, the action deletes the device's events and moves the device to a Vanish state.
  - If the component was merged, the action unmerges the component with the physical device, clears the device's events, and moves the device to a Vanish state.
  - If the component was merged but the VM was powered off, the action does not do anything until the VM is powered on, at which point the action updates the IP address of the physical device.

    When a merged device is un-merged, the component device vanishes, and the physical device moves to an automatically created Collector group named "Virtual Group".

The following Run Book Automation policy triggers the above actions:

- ***Microsoft Azure: Vanish Terminated Instances***. This Run Book Automation policy executes when the "Availability Check Failed" event is raised on the virtual machine when it terminated.

To use this automation, you must:

- *Enable the Run Book Automation policies*
- *Configure your system to preserve this change*

Enabling the Run Book Automation Policies

To enable one or more Run Book Automation policies in the "Microsoft: Azure" PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the wrench icon (🔧) for the Run Book Automation policy you want to enable.
3. In the ***Policy State*** field, select *Enabled*.
4. Click **[Save]**.

Preserving Automation Changes

If you have modified Run Book Actions and Run Book Automation policies that are included in the "Microsoft: Azure" PowerPack, updating the PowerPack on your system overwrites those changes. If you have modified Run Book Actions and Run Book Automation policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the "Microsoft: Azure"PowerPack.
- Remove the content from the PowerPack on your system. When the "Microsoft: Azure" PowerPack is updated in your system, the system does not install updated versions of this content, and preserves your local changes.

To remove Run Book Action or Run Book Automation policy content from the "Microsoft: Azure" PowerPack on your system:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the wrench icon (🔧) for the "Microsoft: Azure" PowerPack. The **Editing PowerPack** page appears.
3. In the left navigation bar of the **Editing PowerPack** page, select the type of content you want to remove:
    - To remove a Run Book Action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
    - To remove a Run Book Automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
4. In the upper pane, click the delete icon (🗑) for each Run Book Action or Run Book Automation policy that you want to remove from the "Microsoft: Azure" PowerPack on your system.

Chapter 6

Azure Dashboards

Overview

This section describes the device dashboards that are included in the "Microsoft: Azure" PowerPack.

This chapter covers the following topics:

Device Dashboards *69*

Device Dashboards

The "Microsoft: Azure" PowerPack includes device dashboards in the Skylar One classic user interface that provide summary information for Azure component devices. The following device dashboards in the "Microsoft: Azure" PowerPack are aligned as the default device dashboards for their equivalent device classes.

Microsoft: Azure Batch Account

The "Microsoft: Azure Batch Account" device dashboard displays the following information:

- The basic information about the device
- Task Fail Events
- Topology Map
- Node Counts
- Device Logs

Microsoft: Azure Cache for Redis

The "Microsoft: Azure Cache for Redis" device dashboard displays the following information:

- The basic information about the device
- Top CPU Usage
- Top Memory Usage
- Top Server Load
- Top Errors
- Cache Latency
- Top Evicted Keys
- Top Operations per Second
- Device Logs

Microsoft: Azure Key Vault

The "Microsoft: Azure Key Vault" device dashboard displays the following information:

- The basic information about the device
- Bottom Vault Availability
- Top Vault Saturation
- Topology Map
- Top Service API Hits
- Overall Service API Latency
- Device Logs

Microsoft: Azure Kubernetes Cluster

The "Microsoft: Azure Kubernetes Cluster" device dashboard displays the following information:

- The basic information about the device
- Total Available CPU & Memory
- Topology Map
- Top Pods by Phase
- Top Pods in Ready State
- Top Node Conditions
- Device Logs

Microsoft: Azure MySQL Server

The "Microsoft: Azure MySQL Server" device dashboard displays the following information:

- The basic information about the device
- CPU & Memory Usage
- IO, Storage, Storage Log Usage
- Topology Map
- Device Logs

Microsoft: Azure PostgreSQL Server

The "Microsoft: Azure PostgreSQL Server" device dashboard displays the following information:

- The basic information about the device
- CPU, Memory, Log Storage, Storage Percent
- Topology Map
- Device Logs

Microsoft: Azure Service Bus Namespace

The "Microsoft: Azure Service Bus Namespace" device dashboard displays the following information:

- The basic information about the device
- CPU & Memory Usage
- Active Connections
- Topology Map
- Top Server Errors
- Top User Errors
- Top Throttled Requests
- Top Deadlettered Messages
- Device Logs

Microsoft: Azure WAF on CDN Policy

The "Microsoft: Azure WAF on CDN Policy" device dashboard displays the following information:

- The basic information about the device
- Top Requests By Action
- Topology Map
- Top Requests By Rule Name

- Requests Total
- Device Logs

Appendix

A

Key Metrics Collected by the Microsoft: Azure PowerPack

Overview

This section lists the key metrics for Microsoft Azure services that the "Microsoft: Azure" PowerPack collects by Dynamic Application. Coverage of these services uses service-specific APIs that collect performance and configuration metrics that generate alerts and events. Coverage also includes DCM+R to Resource Groups, Networks, Network Security Groups, Subnets, and Storage Accounts. It also collects any alerts that Azure generates and aligns them to component devices.

For some services, *partial coverage* exists that is not service-specific. This partial coverage includes some configuration information, such as health status from the Resource Health API, CMDB sync, status events, and Azure Unified Alerts.

This chapter covers the following topics:

Azure Active Directory Tenant Service *75*

Azure API Management *76*

Azure App Service *81*

Azure Application Gateway Service *83*

Azure Automation Service *85*

Azure Backup Policies Service *86*

Azure Batch Service *87*

Azure Cache for Redis *91*

Azure Container Instances 94
Azure Container Registry 96
Azure Content Delivery Network 98
Azure CosmosDB Service 101
Azure Data Factory 104
Azure Database for MySQL 106
Azure Database for PostgreSQL 109
Azure Databricks Service 112
Azure DNS Service 113
Azure Event Grid 113
Azure ExpressRoute Service 119
Azure Fabric Capacity Service 123
Azure Firewall Service 123
Azure Front Door Service 126
Azure Function App Service Plan 127
Azure Functions 128
Azure HDInsight Service 128
Azure Key Vault 132
Azure Kubernetes Service (AKS) 134
Azure Load Balancer Service 136
Azure Logic App Service 138
Azure Managed Disks Service 140
Azure Network Security Group Service 140
Azure OpenAI Service 145
Azure Recovery Service Vault 147
Azure Resource Group Service 148
Azure Resource List Services 148
Azure Service Bus (Relay) 149
Azure Site Recovery 152
Azure SQL Managed Instance Service 154
Azure SQL Servers Service 156

Azure Storage Service 158
Azure Traffic Manager Service 164
Azure Virtual Desktop Host Pool Service 166
Azure Virtual Machines Service 168
Azure Virtual Network Service 172
Azure VM Scale Sets Service 177
Azure Web Application Firewall (WAF) 183
Other Supported Services 186

Azure Active Directory Tenant Service

Microsoft: Azure Active Directory Tenant Configuration	
Object Name	Object Description
Organization ID	Organization Identifier.
Assigned Plans	The group label for the assigned plans group.
Country Letter Code	The ISO 2-alpha code for the country; for example, "US" or "UK".
Default Domain	True if this is the default domain associated with the tenant; otherwise, false.
Directory Sync Enabled	True if this object is synced from an on-premises directory; false if this object was originally synced from an on-premises directory but is no longer synced; null if this object has never been synced from an on-premises directory (default).
Domain Capabilities	The Capabilities of an Azure Active Directory. For example, "Email", "OfficeCommunicationsOnline".
Domain Name	The domain name of the Active Directory tenant.
Domain Type	The type of an Azure Active Directory domain. For example, "Managed".
ID	The ID of an Azure Active Directory tenant.
Last On-Premise Sync Time	The time and date at which the tenant was last synced with the on-premise directory.
Office 365 AD Tenant/Azure AD Tenant	Office 365 namespace.
Service	The name of the service; for example, "SharePoint", "MicrosoftOffice", or "Exchange".
Service Plan ID	A GUID that identifies the service plan.
Status	The status of an assigned plan. For example, "Enabled".

Microsoft: Azure Active Directory Tenant Configuration	
Object Name	Object Description
Tenant Name	The display name of an Azure Active Directory tenant.
Timestamp	The date and time at which the plan was assigned; for example: 2013-01-02T19:32:30Z.
Verified Domains	The group label for the verified domains group.

Azure API Management

Microsoft: Azure API Management Configuration	
Object Name	Object Description
Azure API Management / Resource Group	Resource id of the Resource Group.
Azure API Management / Subnet	The full resource ID of a subnet in a virtual network to deploy the API Management service in.
Capacity	Capacity of the SKU (number of deployed units of the SKU)
Certificate Source	Certificate Source.
Ciphers TripleDes168	Custom properties of the API Management service.
Client ID	System or User Assigned Managed identity clientId as generated by Azure AD.
Created At	The timestamp of resource creation (UTC).
Created By	The identity that created the resource.
Created By Type	The type of identity that created the resource.
Default SSL Binding	Used to setup the certificate associated with this Hostname as the Default SSL Certificate.
Developer Portal Url	Developer Portal endpoint URL of the API Management service.
Disable Gateway	Property only valid for an Api Management service deployed in multiple locations. This can be used to disable the gateway in master region.
Etag	ETag of the resource.
Gateway Regional Url	Gateway URL of the API Management service in the Default Region.
Gateway Regional Url	Gateway URL of the API Management service in the Region.
Gateway Url	Gateway URL of the API Management service.
Host Name	Hostname to configure on the Api Management service.

Microsoft: Azure API Management Configuration	
Object Name	Object Description
Http2	Custom properties of the API Management service.
Id	Resource ID.
ID	Private Endpoint connection resource id.
IP Addresses	Public Static Load Balanced IP addresses of the API Management service in Primary region.
Last Modified At	The timestamp of resource last modification (UTC).
Last Modified By	The identity that last modified the resource.
Last Modified By Type	The type of identity that last modified the resource.
Location	Resource location.
Location	The location name of the additional region among Azure Data center regions.
Management Api Url	Management API endpoint URL of the API Management service.
Name	Resource name.
Name	Name of the Sku.
Name	Private Endpoint Connection Name.
Name	Resource Group name.
Name	The user identity ARM resource ID.
Negotiate Client Certificate	Used to always negotiate client certificate on the hostname.
Notification Sender Email	Email address from which the notification will be sent.
Platform Version	Compute Platform Version running the service in this location.
Portal Url	Publisher portal endpoint URL of the API Management service.
Principal ID	The principal id of the identity.
Principal ID	The principal id of user assigned identity.
Private Endpoint	Resource ID of the private endpoint.
Private IP Addresses	Private Static Load Balanced IP addresses of the API Management service.
Private IP Addresses	Private Static Load Balanced IP addresses of the API Management service which is deployed in an Internal Virtual Network in a particular additional location.
Provisioning State	The current provisioning state of the API Management service.
Provisioning State	The provisioning state of the private endpoint

Microsoft: Azure API Management Configuration	
Object Name	Object Description
	connection resource.
Public Ip Address Id	Public Standard SKU IP V4 based IP address to be associated with Virtual Network deployed service in the region.
Public IP Addresses	Public Static Load Balanced IP addresses of the API Management service in Primary region.
Public IP Addresses	Public Static Load Balanced IP addresses of the API Management service in Primary region.
Public Network Access	Whether or not public endpoint access is allowed for this API Management service.
Publisher Email	Publisher email.
Publisher Name	Publisher name.
Scm Url	SCM endpoint URL of the API Management service.
Ssl30	Custom properties of the API Management service.
Ssl30	Custom properties of the API Management service.
Subnet Name	Virtual subnet name.
Tag Key	Tags key.
Tag Value	Tags value.
Target Provisioning State	The provisioning state of the API Management service, which is targeted by the long running operation started on the service.
Tenant ID	The client tenant id of the identity.
Tls10	Custom properties of the API Management service.
Tls10	Custom properties of the API Management service.
Tls11	Custom properties of the API Management service.
Tls11	Custom properties of the API Management service.
Type	Resource type for API Management resource is set to Microsoft.ApiManagement.
Type	Hostname type.
Type	The type of identity used for the resource.
Zone	A list of availability zones denoting where the resource needs to come from.

Microsoft: Azure API Management Performance	
Object Name	Object Description
Capacity per Location	Utilization metric for ApiManagement service. Note: For skus other than Premium, Max aggregation will show the value as 0.

Microsoft: Azure API Management Performance	
Object Name	Object Description
Dropped EventHub Events	Number of events skipped because of queue size limit reached.
Duration of Backend Requests Per Hostname	Duration of Backend Requests in milliseconds.
Duration of Backend Requests Per Location	Duration of Backend Requests in milliseconds.
Duration of Gateway Requests by Hostname	Overall Duration of Gateway Requests in milliseconds.
Duration of Gateway Requests by Location	Overall Duration of Gateway Requests in milliseconds.
Failed EventHub Events	Number of failed EventHub events.
Rejected EventHub Events	Number of rejected EventHub events (wrong configuration or unauthorized).
Requests by Backend Response Code	Gateway request metrics with multiple dimensions.
Requests by Backend Response Code Category	Gateway request metrics with multiple dimensions.
Requests by Gateway Response Code	Gateway request metrics with multiple dimensions.
Requests by Gateway Response Code Category	Gateway request metrics with multiple dimensions.
Requests by Hostname	Gateway request metrics with multiple dimensions.
Requests by Last Error Reason	Gateway request metrics with multiple dimensions.
Requests by Location	Gateway request metrics with multiple dimensions.
Size of EventHub Events	Total size of EventHub events in bytes.
Successful EventHub Events	Number of successful EventHub events.
Throttled EventHub Events	Number of throttled EventHub events.
Timed Out EventHub Events	Number of timed out EventHub events.
Total EventHub Events	Number of events sent to EventHub.

Microsoft: Azure API Management APIS Configuration	
Object Name	Object Description
API Revision	Describes the revision of the API.
Description	Description of the API. May include HTML formatting tags.
Display Name	API name.
ID	Fully qualified resource ID for the resource.
Is Current	Indicates if API revision is current api revision.
Name	The name of the resource.
Path	Relative URL uniquely identifying this API and all of its resource paths within the API Management service instance.
Protocols	Describes on which protocols the operations in this

Microsoft: Azure API Management APIS Configuration	
Object Name	Object Description
	API can be invoked.
Service URL	Absolute URL of the backend service implementing this API.
Type	Type of API.

Microsoft: Azure API Management APIS Operations Configuration	
Object Name	Object Description
Name	The name of the resource
Display Name	Operation Name.
Method	A Valid HTTP Operation Method. Typical Http Methods like GET, PUT, POST but not limited by only them.
URL Template	Relative URL template identifying the target resource for this operation. May include parameters. Example: /customers/{cid}/orders/{oid}/?date={date}
Template Parameters	Collection of URL template parameters.
Description	Description of the operation. May include HTML formatting tags.

Microsoft: Azure API Management APIS Products Configuration	
Object Name	Object Description
ID	API product identifier.
Name	API product name.
Display Name	API product display name.
Approval Required	Whether subscription approval is required. If false, new subscriptions will be approved automatically enabling developers to call the product's APIs immediately after subscribing. If true, administrators must manually approve the subscription before the developer can call any of the product's APIs. Can be present only if subscriptionRequired property is present and has a value of false.
Subscription Limit	The number of subscriptions a user can have to this product at the same time. Set to null or omit to allow unlimited subscriptions per user. This value can be present only if the subscriptionRequired property is present and set to false.
Subscription Required	Whether a product subscription is required for accessing APIs included in this product. If true, the

Microsoft: Azure API Management APIS Products Configuration	
Object Name	Object Description
	product is referred to as "protected" and a valid subscription key is required for a request to an API included in the product to succeed. If false, the product is referred to as "open" and requests to an API included in the product can be made without a subscription key. If property is omitted when creating a new product its value is assumed to be true.
State	Whether the product is published or not. Published products are discoverable by users of the developer portal. Unpublished products are visible only to administrators. Default state of Product is notPublished.

Azure App Service

Microsoft: Azure App Configuration	
Object Name	Object Description
Name	Resource Group Name.
Admin Enabled	Admin enabled state.
Availability State	Management information availability state for the app.
Azure App/Resource Group	Resource Group identifier.
Container Size	Size of the function container.
Daily Memory Time Quota	Maximum allowed daily memory-time quota (applicable on dynamic apps only).
Default Host Name	Default hostname of the app. Read-only.
Enabled	true if the app is enabled; otherwise, false. Setting this value to false disables the app (takes the app offline).
Kind	Kind of resource.
Max Number Of Workers	Maximum number of workers. This only applies to Functions container.
Name	Name of the app.
Name	Key of the tag.
Repository Site Name	Name of the repository site.
Sku	Sku type.

Microsoft: Azure App Configuration	
Object Name	Object Description
State	Current state of the app.
Usage State	State indicating whether the app has exceeded its quota usage. Read-only.
Value	Value of the tag.
Web Space	Web Space of the app.

Microsoft: Azure App Performance	
Object Name	Object Description
App Connections	The average of App Connections.
Average Memory Working Set	Average of memory working set.
Average Response Time	Average of Response Time.
Bytes Received	Total bytes received.
Bytes Sent	Total bytes sent.
Cpu Time	Total of CPU Time.
Current Assemblies	Average of current Assemblies.
File System Usage	File System Usage.
Gen 0 Collections	Total number of Gen 0 Garbage Collections.
Gen 1 Collections	Total number of Gen 1 Garbage Collections.
Gen 2 Collections	Total number of Gen 2 Garbage Collections.
Handles	Average of Handle Count.
Health Check Status	Health check status.
Http Response Time	Response Time.
Http101	Total of Http 101 responses.
Http2xx	Total of Http 2xx responses.
Http3xx	Total of Http 3xx responses.
Http401	Total of Http 401 responses.
Http403	Total of Http 403 responses.
Http404	Total of Http 404 responses.
Http406	Total of Http 406 responses.
Http4xx	Total of Http 4xx responses.
Http5xx	Total of Http 5xx errors.
Io Other Bytes Per Second	Total of IO Other Bytes Per Second.
Io Other Operations Per Second	Total of IO Other Operations Per Second.
Io Read Bytes Per Second	Total of IO Read Bytes Per Second.
Io Read Operations Per Second	Total of IO Read Operations Per Second.

Microsoft: Azure App Performance	
Object Name	Object Description
Io Write Bytes Per Second	Total of IO Write Bytes Per Second.
Io Write Operations Per Second	Total of IO Write Operations Per Second.
Memory Working Set	Average of Memory working set.
Private Bytes	Total of Private bytes.
Requests	Total number of Requests.
Requests In Application Queue	Average of Requests In Application Queue.
Threads	Average of Thread Count.
Total App Domains	Total of App Domains.
Total App Domains Unloaded	Total of App Domains Unloaded.

Azure Application Gateway Service

Microsoft: Azure Application Gateway Configuration	
Object Name	Object Description
Name	Name of Frontend IP configuration.
Name	Name of the listener.
Port	Associated port.
Protocol	Listener protocol.
Resource Group Name	Azure Resource Group Name associated with Azure Application Gateway.
Subnet Name	Subnet name of the Application Gateway configuration for relationship.
Type	Frontend IP configuration type.
Virtual Network	Virtual Network
Azure Application Gateway/Resource Group	Azure Resource Group ID associated with Azure Application Gateway.
Azure Application Gateway/Subnets	Azure Subnet ID associated with Azure Application Gateway.
Frontend IP Configuration Name	Associated Frontend IP configuration.
Instance Count	The instance count of the Application Gateway.
IP Address	IP address for Frontend configuration.
IP Allocation Method	Private IP allocation method.
Key	Tag key.
Location	Application Gateway location.

Microsoft: Azure Application Gateway Configuration	
Object Name	**Object Description**
Name	Application Gateway name.
Operational State	Operational state of the Application Gateway. Possible values Stopping | Starting | Running
Provisioning State	Provision state of the Application Gateway. Possible values: Updating | Succeeded | Failed
SKU Name	Gateway identifier. Possible values Standard_Small | Standard_Medium | Standard_Large | WAF_ Medium | WAF_Large
Tier	Application Gateway tier. Possible values Standard | WAF.
Value	Tag value.

Microsoft: Azure Application Gateway Performance	
Object Name	**Object Description**
Application Gateway Total Time	Time that it takes for a request to be processed and its response to be sent.
Avg Request Count Per Healthy Host	Average request count per minute per healthy backend host in a pool.
Backend Connect Time	Time spent establishing a connection with a backend server.
Backend First Byte Response Time	Time interval between start of establishing a connection to backend server and receiving the first byte of the response header.
Backend Response Status	The number of HTTP response codes generated by the backend members.
Bytes Received	The total number of bytes received by the Application Gateway from the clients.
Bytes Sent	The total number of bytes sent by the Application Gateway to the clients.
Capacity Units	Capacity Units consumed.
Client Rtt	Round trip time between clients and Application Gateway.
Compute Units	Compute Units consumed.
Cpu Utilization	Current CPU utilization of the Application Gateway.
Current Connections	The most recent total Current Conections metric for an Azure Application Gateway.
Failed Requests	The most recent total Failed Request metric for an Azure Application Gateway.
Healthy Host Count	The most recent average Healthy Host Count metric

Microsoft: Azure Application Gateway Performance	
Object Name	Object Description
	for an Azure Application Gateway.
HTTP 5xx Response Count	The total count of HTTP responses with 5xx (server error) status codes returned by the Application Gateway or its backend pool members.
New Connections Per Second	New connections per second established with Application Gateway.
Response Status	The most recent total Response Status metric for an Azure Application Gateway.
Throughput	The most recent total Throughput metric for an Azure Application Gateway.
Total Requests	The most recent Total Request metric for an Azure Application Gateway.
Unhealthy Host Count	The most recent Average Unhealthy Host Count metric for an Azure Application Gateway.

Azure Automation Service

Microsoft: Azure Automation Configuration	
Object Name	Object Description
Name	Automation account certificate name
Name	Automation account Runbook Name
Associated Runbook	Automation account associated runbook to the job
State	Automation account Runbook State
Status	Automation account job status
Type	Automation account Runbook Type
Expiry Time	Automation account certificate expiration date
Id	Automation account certificate identifier
Last Modified Time	Gets the last modified time.
Last Modified Time	Gets the last modified time.
Azure Automation/Resource Group	Automation account Resource Group Identifier
Certificates	Azure Automation stores certificates securely for access by runbooks and DSC configurations
Id	Automation account Runbook Identifier
Id	Automation account job identifier
Jobs	Azure Automation supports an environment to run jobs from the same Automation account. A single

Microsoft: Azure Automation Configuration	
Object Name	Object Description
	runbook can have many jobs running at one time. The more jobs you run at the same time, the more often they can be dispatched to the same sandbox.
Key	Automation account Tag Key
Name	Automation account Resource Group Name
Remaining Days	Expiration remaining days for automation account certificate.
Resource Group Relationship	Automation account Resource Group relationship
Runbooks	The Azure Automation Process Automation feature supports several types of runbooks
Tags	Automation account Tags
Value	Automation account Tag Value

Microsoft: Azure Automation Performance	
Object Name	Object Description
Total Jobs	The total number of jobs.
Total Update Deployment Machine Runs	Total software update deployment machine runs in a software update deployment run.
Total Update Deployment Runs	Total software update deployment runs.

Azure Backup Policies Service

Microsoft: Azure Backup Job Performance	
Object Name	Object Description
Completed Jobs	The number of Backup Jobs completed or completed with warnings in the last 24 hours.
Failed Jobs	The number of Backup Jobs failed, canceled or in the canceling state in the last 24 hours.

Microsoft: Azure Backup Policy Configuration	
Object Name	Object Description
Name	The name of the backup policy.
Backup Frequency	The schedule frequency. We have 2 possible values: daily and weekly.
Backup Management Type	The backup management type.

Microsoft: Azure Backup Policy Configuration	
Object Name	Object Description
Backup Time	The scheduled time to execute the backup.
Days of Week	The schedule days to execute the backup.

Microsoft: Azure Backup Protected Items Configuration	
Object Name	Object Description
Item Name	The item name associated with the resource.
Backup Policy Name	Backup Policy Name.
Last Backup Status	Status could be: In progress, Completed, Completed with Information, Completed with Errors, Failed, Canceled, Canceling, Waiting for action.
Backup Management Type	Backup Management Type.
Backup Protected Items	All the backup protected items.
Number of Backup Protected Items	Number of protected items.
Protected Item ID	Protected Item ID
Protected Item Type	Protected Item Type.
Protection State	Protection State.
Protection Status	Protection Status.
Workload Type	WorkLoad Type.

Azure Batch Service

Microsoft: Azure Batch Account Configuration	
Object Name	Object Description
Id	The ID of the resource.
Account Endpoint	The account endpoint used to interact with the Batch service.
Active Job And Job Schedule Quota	The active job and job schedule quota for the Batch account.
Azure Batch Account/Key Vault	Azure Key Vault ID associated with Azure Batch Account.
Azure Batch Account/Resource Group	Azure Resource Group ID associated with the Azure Batch Account.
Azure Batch Account/Storage Account	Azure Storage Account Id associated with Azure Batch Account.
Azure Key Vault Name	The name of the Azure Key Vault.

Microsoft: Azure Batch Account Configuration	
Object Name	Object Description
Azure Key Vault URL	The URL of the Azure Key Vault.
Azure Resource Group Name	The Resource Group Name.
Azure Storage Account Name	The name of the Azure Storage Account.
Dedicated Core Quota	The dedicated core quota for the Batch account. For accounts with PoolAllocationMode set to UserSubscription, quota is managed on the subscription so this value is not returned.
Dedicated Core Quota Per VM Family Enforced	A value indicating whether the core quota for the Batch Account is enforced per Virtual Machine family or not. Batch is transitioning its core quota system for dedicated cores to be enforced per Virtual Machine family. During this transitional phase, the dedicated core quota per Virtual Machine family may not yet be enforced. If this flag is false, dedicated core quota is enforced via the old dedicatedCoreQuota property on the account and does not consider Virtual Machine family. If this flag is true, dedicated core quota is enforced via the dedicatedCoreQuotaPerVMFamily property on the account, and the old dedicatedCoreQuota does not apply.
Location	The location of the resource.
Low Priority Core Quota	The low-priority core quota for the Batch account. For accounts with PoolAllocationMode set to UserSubscription, quota is managed on the subscription so this value is not returned.
Name	The name of the resource.
Pool Allocation Mode	The allocation mode to use for creating pools in the Batch account. The allocation mode for creating pools in the Batch account.
Pool Quota	The pool quota for the Batch account.
Provisioning State	The provisioned state of the resource.
Public Network Access	The network interface type for accessing Azure Batch service and Batch account operations. If not specified, the default value is 'enabled'.
Tag Key	Tags key.
Tag Value	Tags values.

Microsoft: Azure Batch Account Job Configuration	
Object Name	Object Description
Name	A string that uniquely identifies the Job within the

Microsoft: Azure Batch Account Job Configuration	
Object Name	Object Description
	Account.
State	The current state of the Job.
Pool	The ID of an existing Pool. All the Tasks of the Job will run on the specified Pool.
Priority	The priority of the Job. Priority values can range from -1000 to 1000, with -1000 being the lowest priority and 1000 being the highest priority.
Failed Tasks	The total number of Tasks in the Job that failed during the given time range.
Succeeded Tasks	The total number of Tasks successfully completed in the Job during the given time range.
All Tasks Complete Policy	The action the Batch service should take when all Tasks in the Job are in the completed state.
Max Task Retry Count	The maximum number of times each Task may be retried. The Batch service retries a Task if its exit code is nonzero.
Task Failure Policy	The action the Batch service should take when any Task in the Job fails.
Use Task Dependencies	Whether Tasks in the Job can define dependencies on each other.
Creation Date	The creation time of the Job.

Microsoft: Azure Batch Account Job Pool Task Performance	
Object Name	Object Description
Job Delete Complete Events	Total number of jobs that have been successfully deleted.
Job Delete Start Events	Total number of jobs that have been requested to be deleted.
Job Disable Complete Events	Total number of jobs that have been successfully disabled.
Job Disable Start Events	Total number of jobs that have been requested to be disabled.
Job Start Events	Total number of jobs that have been successfully started.
Job Terminate Complete Events	Total number of jobs that have been successfully terminated.
Job Terminate Start Events	Total number of jobs that have been requested to be terminated.
Pool Create Events	Total number of pools that have been created.

Microsoft: Azure Batch Account Job Pool Task Performance	
Object Name	Object Description
Pool Delete Complete Events	Total number of pool deletes that have completed.
Pool Delete Start Events	Total number of pool deletes that have started.
Pool Resize Complete Events	Total number of pool resizes that have completed.
Pool Resize Start Events	Total number of pool resizes that have started.
Task Complete Events	Total number of tasks that have completed.
Task Fail Events	Total number of tasks that have completed in a failed state.
Task Start Events	Total number of tasks that have started.

Microsoft: Azure Batch Account Node Performance	
Object Name	Object Description
Creating Node Count	Number of nodes being created.
Dedicated Core Count	Total number of dedicated cores in the batch account.
Dedicated Node Count	Total number of dedicated nodes in the batch account.
Idle Node Count	Number of idle nodes.
Leaving Pool Node Count	Number of nodes leaving the Pool.
Low-Priority Node Count	Total number of low-priority nodes in the batch account.
LowPriority Core Count	Total number of low-priority cores in the batch account.
Offline Node Count	Number of offline nodes.
Preempted Node Count	Number of preempted nodes.
Rebooting Node Count	Number of rebooting nodes.
Reimaging Node Count	Number of reimaging nodes.
Running Node Count	Number of running nodes.
Start Task Failed Node Count	Number of nodes where the Start Task has failed.
Starting Node Count	Number of nodes starting.
Unusable Node Count	Number of unusable nodes.
Waiting For Start Task Node Count	Number of nodes waiting for the Start Task to complete.

Microsoft: Azure Batch Account Pool Configuration	
Object Name	Object Description
Name	The name of the resource.

Microsoft: Azure Batch Account Pool Configuration	
Object Name	Object Description
Allocation State	Whether the pool is resizing.
Provisioning State	The current state of the pool.
Tasks Per Node	The number of task slots that can be used to run concurrent tasks on a single compute node in the pool.
Dedicated Nodes	The number of compute nodes currently in the pool.
Low Priority Nodes	The number of low priority compute nodes currently in the pool.
Os Type	The publisher of the Azure Virtual Machines Marketplace image.
Os Version	The version of the Azure Virtual Machines Marketplace image.
Vm Size	The size of virtual machines in the pool. All VMs in a pool are the same size.
Inter Node Communication	Whether the pool permits direct communication between nodes.
Node Deallocation	Determines what to do with a node and its running task(s) if the pool size is decreasing.
Node Fill Type	How tasks should be distributed across compute nodes.
Scale Type	Defines the desired size of the pool. This can either be fixedScale where the requested targetDedicatedNodes is specified, or autoScale which defines a formula which is periodically reevaluated. If this property is not specified, the pool will have a fixed scale with 0 targetDedicatedNodes.
Creation Date	The creation time of the pool.

Azure Cache for Redis

Microsoft: Azure Cache for Redis Configuration	
Object Name	Object Description
Name	Resource name for the Redis cache.
Name	The type of Redis cache to deploy. Valid values: (Basic, Standard, Premium)
Name	Name of the Redis config property.
Name	Resource name for the Redis cache firewall rule.
Name	The name of the redis cache associated with the

Microsoft: Azure Cache for Redis Configuration	
Object Name	Object Description
	linked server.
Name	The name of the resource associated with the resource group.
Name	Virtual Network resource name.
Name	Subnet resource name.
Redis Configuration	All Redis Settings
SSL Port	Redis SSL port.
Start IP	lowest IP address included in the range
Azure Redis Cache Server/Redis Cache Server	Fully qualified resourceId of the linked redis cache server.
Azure Redis Cache/Resource Group	The resource Id associated with the resource group.
Azure Redis Cache/Subnet	The full resource ID of a subnet in a virtual network to deploy the Redis cache in.
Azure Redis Cache/Virtual Network	The Virtual Network resource id.
Capacity	The size of the Redis cache to deploy. Valid values: for C (Basic/Standard) family (0, 1, 2, 3, 4, 5, 6), for P (Premium) family (1, 2, 3, 4).
End IP	highest IP address included in the range
Family	The SKU family to use. Valid values: (C, P). (C = Basic/Standard, P = Premium).
Host Name	Redis host name.
Linked Servers Relationships	Gets the list of linked servers associated with this redis cache (requires Premium SKU).
Location	The geo-location where the resource lives.
Minimal TLS Version	Minimal version requires clients to use a specified TLS version.
Non-SSL Port	Specifies whether the non-ssl Redis server port is enabled.
Port	Redis non-SSL port.
Provisioning State	Redis instance provisioning status.
Provisioning State	Terminal state of the link between primary and secondary redis cache.
Redis Version	Redis version.
Shard Count	The number of shards to be created on a Premium Cluster Cache.
Static IP	Static IP address. Required when deploying a Redis cache inside an existing Azure Virtual Network.
Tag Key	An Azure redis cache tag key.

Microsoft: Azure Cache for Redis Configuration	
Object Name	Object Description
Tag Value	An Azure redis cache tag value.
Tags	Resource tags.
Value	Value of the Redis Config Property.
Virtual Network Subnet Relationships	Gets the list of virtual network subnets associated with the redis cache.

Microsoft: Azure Cache for Redis Keys Performance	
Object Name	Object Description
Evicted Keys	The number of items evicted from the cache during the specified reporting interval due to the maxmemory limit. This number maps to evicted_ keys from the Redis INFO command.
Evicted Keys Labels	Evicted Keys Labels
Expired Keys	The number of items expired from the cache during the specified reporting interval. This value maps to expired_keys from the Redis INFO command.
Expired Keys Labels	Expired Keys Labels
Total Keys	The maximum number of keys in the cache during the past reporting time period. This number maps to keyspace from the Redis INFO command. Due to a limitation of the underlying metrics system, for caches with clustering enabled, Total Keys returns the maximum number of keys of the shard that had the maximum number of keys during the reporting interval.
Total Keys Labels	Total Keys Labels

Microsoft: Azure Cache for Redis Operations Performance	
Object Name	Object Description
Gets	The Redis Cache Gets Total Count.
Gets Labels	The Redis Cache Gets Total Count labels.
Operations per Second	The Redis Cache Operations per Second Count.
Operations per Second Labels	The Redis Cache Operations per Second Count labels.
Sets	The Redis Cache Sets Total Count.
Sets Labels	The Redis Cache Sets Total Count labels.
Total Operations	The Redis Cache Total Operations Count.
Total Operations Labels	The Redis Cache Total Operations Count labels

Microsoft: Azure Cache for Redis Performance	
Object Name	Object Description
Cache Hits	Cache hits.
Cache Hits Labels	Cache Hits Labels
Cache Latency	Cache latency.
Cache Misses	Cache misses.
Cache Misses Labels	Cache Misses Labels.
Cache Read	Cache read.
Cache Read Labels	Cache Read Labels.
Cache Write	Cache write.
Cache Write Labels	Cache Write Labels.

Microsoft: Azure Cache for Redis System Performance	
Object Name	Object Description
Clients Connected	The number of client connections to the cache during the specified reporting interval.
Clients Connected Labels	Clients Connected Labels.
CPU Usage	The CPU utilization of the Azure Cache for Redis server as a percentage during the specified reporting interval.
CPU Usage Labels	CPU Usage Labels.
Errors	Specific failures and performance issues that the cache could be experiencing during a specified reporting interval.
Errors Labels	Errors Labels.
Memory Usage	The percentage of total memory that is being used during the specified reporting interval.
Memory Usage Labels	Memory Usage Labels.
Server Load	Percentage of cycles in which the Redis server is busy processing and not waiting idle for messages.
Server Load Labels	Server Load Labels.

Azure Container Instances

Microsoft: Azure Container Instances Configuration	
Object Name	Object Description
Name	The user-provided name of the container instance.

Microsoft: Azure Container Instances Configuration	
Object Name	Object Description
Image	The name of the image used to create the container instance.
State	The state of the container group.
Containers	Containers Group.
CPU	The CPU limit of this container instance.
DNS Name Label	The Dns name label for the IP.
Environment Variables	The environment variable to set within the container instance.
Finish Time	The date-time when the container instance state finished.
FQDN	The FQDN for the IP.
IP	The IP exposed to the public internet.
IP Address	IP Address Group.
Location	The resource location.
Memory In GB	The memory limit in GB of this container instance.
Name	The resource name.
Name	Resource Group name.
OS Type	The operating system type required by the containers in the container group.
Ports	The exposed ports on the container instance.
Ports	The list of ports exposed on the container group.
Previous Exit Code	The container instance exit codes correspond to those from the docker run command.
Previous State	Previous container instance state.
Provisioning State	The provisioning state of the container group.
Resource Group Relationships	Resource Group Relationships Group.
Restart Count	The number of times that the init container has been restarted.
Restart Policy	Restart policy for all containers within the container group.
SKU	The SKU for a container group.
Tag Key	Tags Key.
Tag Value	Tags Value.
Tags	Tags Group.
Type	The type of identity used for the container group.
Type	Specifies if the IP is exposed to the public internet or private VNET.

Microsoft: Azure Container Instances Configuration	
Object Name	Object Description
Volume Mounts	The volume mounts available to the container instance.

Microsoft: Azure Container Instances Performance	
Object Name	Object Description
CPU Total Available	Number of vCPUs
CPU Usage	CPU usage on all cores in millicores.
CPU Usage (Labels)	CPU usage Container name.
Memory Total Available	The memory limit in GB of this container instance.
Memory Usage	Total memory usage in byte.
Memory Usage (Labels)	Total memory container name.
Network Bytes Received	The network bytes received per second.
Network Bytes Transmitted	The network bytes transmitted per second.

Azure Container Registry

Microsoft: Azure Container Registry Configuration	
Object Name	Object Description
Name	The name of the container registry.
Admin User Enabled	The value that indicates whether the admin user is enabled.
Login Server	The URL that can be used to log into the container registry.
Name	The name of the usage.
Value	Specifies the IP or IP range in CIDR format. Only IPV4 address is allowed.
Action	The action of IP ACL rule.
Azure Container Registry / Resource Group	Resource group Id.
Creation Date	The creation date of the container registry in ISO8601 format.
Current Value	The current value of the usage.
Data Endpoint Enabled	Data Endpoint Enabled
Encryption Status	Encryption Status
Endpoint Host Names	Endpoint Host Names Group
Export Policy Status	The value that indicates whether the policy is

Microsoft: Azure Container Registry Configuration	
Object Name	Object Description
	enabled or not.
Host Names	List of host names that will serve data when Data Endpoint Enabled is true.
Limit	The limit of the usage.
Name	Resource group Name.
Network Rule Bypass Options	Network Rule Bypass Options
Network Rule Set Default Action	The default action of allow or deny when no other rules match.
Network Rule Set IP Rules	Network Rule Set IP Rules
Policies	Policies
Provisioning State	The provisioning state of the container registry at the time the operation was called.
Public Network Access	Public Network Access
Quarantine Status	The value that indicates whether the policy is enabled or not.
Registry Usage	Registry Usage
Resource Group Relationship	Resource Group Relationship
Retention Policy Days	The number of days to retain an untagged manifest after which it gets purged.
Retention Policy Status	The value that indicates whether the policy is enabled or not.
SKU	The SKU tier based on the SKU name.
Tag Key	Tags Key.
Tag Value	Tags Value.
Tags	Tags group.
Trust Policy Status	The value that indicates whether the policy is enabled or not.
Trust Policy Type	The type of trust policy.
Unit	The unit of measurement.
Zone Redundancy	Zone Redundancy state.

Microsoft: Azure Container Registry Performance	
Object Name	Object Description
AgentPool CPU Time	AgentPool CPU Time in seconds.
Run Duration	Run Duration in milliseconds.
Storage used	The amount of storage used by the container registry. For a registry account, it is the sum of

Microsoft: Azure Container Registry Performance	
Object Name	Object Description
	capacity used by all the repositories within a registry. It is sum of capacity used by shared layers, manifest files, and replica copies in each of its repositories.
Successful Pull Count	Number of successful image pulls.
Successful Push Count	Number of successful image pushes.
Total Pull Count	Number of image pulls in total.
Total Push Count	Number of image pushes in total.

Azure Content Delivery Network

Microsoft: Azure CDN Endpoint Configuration	
Object Name	Object Description
Name	Name of the endpoint.
Name	Custom domain resource name.
Origin Name	Origin name which must be unique within the endpoint.
Host Name	The host name of the custom domain. Must be a domain name.
Origin Enable	Origin is enabled for load balancing or not. By default, origin is always enabled.
Origin Group Name	Origin group name which must be unique within the endpoint.
Origin Host Header	The host header value sent to the origin with each request. If you leave this blank, the request hostname determines this value. Azure CDN origins, such as Web Apps, Blob Storage, and Cloud Services require this host header value to match the origin hostname by default. If endpoint uses multiple origins for load balancing, then the host header at endpoint is ignored and this one is considered.
Origin Host Name	The address of the origin. It can be a domain name, IPv4 address, or IPv6 address. This should be unique across all origins in an endpoint.
Priority	Priority of origin in given origin group for load balancing. Higher priorities will not be used for load balancing if any lower priority origin is healthy. Must be between 1 and 5.

Microsoft: Azure CDN Endpoint Configuration	
Object Name	Object Description
Relative Path	Relative path applicable to geo filter. (e.g. /mypictures, /mypicture/kitty.jpg, and etc.)
Resource State	Resource status of the custom domain.
Weight	Weight of the origin in given origin group for load balancing. Must be between 1 and 1000
Action	Action of the geo filter, i.e. allow or block access.
Content Type	Content type on which compression apply.
Country Codes	Two letter country codes defining user country access in a geo filter, e.g. AU, MX, US.
Custom Https Provisioning State	Provisioning status of Custom Https of the custom domain.
Custom Https Provisioning Substate	Provisioning substate shows the progress of custom HTTPS enabling/disabling process step by step.
Host Name	The host name of the endpoint structured as {endpointName}.{DNSZone}, e.g. contoso.azureedge.net
HTTP Port	The value of the HTTP port. Must be between 1 and 65535.
HTTPS Port	The value of the HTTPS port. Must be between 1 and 65535.
Is Compression Enabled	Indicates whether content compression is enabled on CDN. Default value is false. If compression is enabled, content will be served as compressed if user requests for a compressed version. Content won't be compressed on CDN when requested content is smaller than 1 byte or larger than 1 MB.
Is Http Allowed	Indicates whether HTTP traffic is allowed on the endpoint. Default value is true. At least one protocol (HTTP or HTTPS) must be allowed.
Is Https Allowed	Indicates whether HTTPS traffic is allowed on the endpoint. Default value is true. At least one protocol (HTTP or HTTPS) must be allowed.
Optimization Type	Specifies what scenario the customer wants this CDN endpoint to optimize for, e.g. Download, Media services. With this information, CDN can apply scenario driven optimization.
Origin Host Header	The host header value sent to the origin with each request. This property can only be set when the endpoint uses a single origin. If you leave this blank, the request hostname determines this value. Azure CDN origins, such as Web Apps, Blob Storage, and Cloud Services require this host header value to

Microsoft: Azure CDN Endpoint Configuration	
Object Name	Object Description
	match the origin hostname by default.
Origin Path	A directory path on the origin that CDN can use to retrieve content from, e.g. contoso.cloudapp.net/originpath.
Probe Interval	The number of seconds between health probes. Default is 240sec.
Probe Path	Path to a file hosted on the origin which helps accelerate delivery of the dynamic content and calculate the most optimal routes for the CDN. This is relative to the origin path. This property is only relevant when using a single origin.
Probe Path	The path relative to the origin that is used to determine the health of the origin.
Probe Protocol	Protocol to use for health probe.
Probe Request Type	The type of health probe request that is made.
Provisioning State	Provisioning status of the endpoint.
Provisioning State	Provisioning status of the custom domain.
Query String Caching Behavior	Defines how CDN caches requests that include query strings. You can ignore any query strings when caching, bypass caching to prevent requests that contain query strings from being cached, or cache every request with a unique URL.
Resource State	Resource status of the endpoint.
Tag Key	Tags key.
Tag Value	Tags values.
Traffic Restoration Time (Min)	Time in minutes to shift the traffic to the endpoint gradually when an unhealthy endpoint comes healthy or a new endpoint is added. Default is 10 mins. This property is currently not supported.

Microsoft: Azure CDN Profile Configuration	
Object Name	Object Description
Name	Resource name.
Name	The Resource Group Name.
Azure CDN Profile/Resource Group	Azure Resource Group ID associated with the Azure CDN Profile.
Location	Resource location.
Provisioning State	Provisioning status of the profile.
Resource State	Resource status of the profile.

Microsoft: Azure CDN Profile Configuration	
Object Name	Object Description
Sku Name	Name of the pricing tier.
Tag Key	Tags key.
Tag Value	Tags values.
Type	Resource type.

Azure CosmosDB Service

Microsoft: Azure CosmosDB Configuration	
Object Name	Object Description
Name	Cosmos DB database account name.
Kind	Indicates the type of database account. This can only be set at database account creation.
Location	The location of the resource group to which the resource belongs.
Database Account Offer Type	The offer type for the database - Standard.
Enable Automatic Failover	Enables automatic failover of the write region in the rare event that the region is unavailable due to an outage. Automatic failover will result in a new write region for the account and is chosen based on the failover priorities configured for the account.
Enable Multiple Write Locations	Enables the account to write in multiple locations.
EnabledApiTypes	The API types enabled to cosmos db account.
IP Range Filter	Cosmos DB Firewall Support: This value specifies the set of IP addresses or IP address ranges in CIDR form to be included as the allowed list of client IPs for a given database account. IP addresses/ranges must be comma separated and must not contain any spaces.
Is Virtual Network Filter Enabled	Flag to indicate whether to enable/disable Virtual Network ACL rules.
Azure CosmosDB/Virtual Network Subnets	Resource ID of a subnet.
ID	The Fail over policy unique identifier.
Location Name	The name of the region.
Provisioning State	The provisioning state to cosmos db account.
Subnet Name	The Virtual Network subnet Name.
Azure CosmosDB/Resource Group	The resource group id.

Microsoft: Azure CosmosDB Configuration	
Object Name	Object Description
Azure CosmosDB/Virtual Network	The Virtual network id.
Default Consistency Level	The default consistency level and configuration settings of the Cosmos DB account. - Eventual, Session, BoundedStaleness, Strong, ConsistentPrefix.
Document Endpoint	Write location document endpoint.
Document Endpoint	Read location document endpoint.
Failover Priority	The failover priority of the region. A failover priority of 0 indicates a write region. The maximum value for a failover priority = (total number of regions - 1). Failover priority values must be unique for each of the regions in which the database account exists.
Failover Priority	Write location failover priority.
Failover Priority	Read location failover priority.
Ignore Missing VNet Service Endpoint	Create firewall rule before the virtual network has vnet service endpoint enabled.
Key	The tag key of the resource.
Location Name	Write location name.
Location Name	Read location name.
Max Interval In Seconds	When used with the Bounded Staleness consistency level, this value represents the time amount of staleness (in seconds) tolerated. Accepted range for this value is 5 - 86400. Required when defaultConsistencyPolicy is set to BoundedStaleness.
Max Staleness Prefix	When used with the Bounded Staleness consistency level, this value represents the number of stale requests tolerated.
Name	The resource group name.
Name	The Virtual network name.
Provisioning State	Write location provisioning state.
Provisioning State	Read location provisioning state.
Value	The tag value of the resource.

Microsoft: Azure CosmosDB Location Performance	
Object Name	Object Description
Available Storage	Total available storage reported at 5 minutes granularity.
Data Usage	Total data usage reported at 5 minutes granularity.

Microsoft: Azure CosmosDB Location Performance	
Object Name	Object Description
Document Count	Total document count reported at 5 minutes granularity.
Document Quota	Total storage quota reported at 5 minutes granularity.
Index Usage	Total index usage reported at 5 minutes granularity.
Metadata Requests	Count of metadata requests. Cosmos DB maintains system metadata collection for each account, that allows you to enumerate collections, databases, etc, and their configurations, free of charge.
Mongo Request Charge	Mongo Request Units Consumed.
Mongo Requests	Number of Mongo Requests Made.
Total Request Units	Request Units consumed.
Total Requests	Number of requests made.

Microsoft: Azure CosmosDB Performance	
Object Name	Object Description
Available Storage	Used to monitor available storage capacity (applicable only for fixed storage collections) Minimum granularity should be 5 minutes.
Cassandra Connection Closures	Number of Cassandra Connections closed.
Cassandra Request Charges	Units consumed by Cassandra API requests.
Cassandra Requests	Number of Cassandra API requests made.
Data Usage	Total data usage reported at 5-minutes granularity per region.
Document Count	Total document count reported at 5-minutes granularity per region.
Document Quota	Used to monitor total quota at container and region, minimum granularity should be 5 minutes.
Index Usage	Used to monitor total data usage at container and region, minimum granularity should be 5 minutes.
Metadata Requests	Count of metadata requests. Azure Cosmos DB maintains system metadata container for each account, that allows you to enumerate collections, databases, etc., and their configurations, free of charge.
Mongo Request Charge	Mongo Request Units Consumed.
Mongo Requests	Number of Mongo Requests Made.
Provisioned Throughput	Provisioned throughput at container granularity.
Service Availability	Account requests availability at one hour

Microsoft: Azure CosmosDB Performance	
Object Name	Object Description
	granularity.
Total Request Units	Request Units consumed.
Total Requests	Number of requests made.

Azure Data Factory

Microsoft: Azure Data Factory Configuration	
Object Name	Object Description
Azure Data Factory / Resource Group	Resource id of the Resource Group.
Create Time	Time the factory was created in ISO8601 format.
Factory Size	The size of the data factory in GB.
Location	The resource location.
Max Allowed Factory Size	The max allowed size of the data factory in GB.
Max Allowed Resource Count	The max allowed resource count of the data factory.
Name	The resource name.
Name	Resource Group name.
Provisioning State	Factory provisioning state.
Tag Key	Tags key.
Tag Value	Tags value.
Total Resource Count	The resource count of the data factory.
Type	The resource type.
Version	Version of the factory.

Microsoft: Azure Data Factory Performance	
Object Name	Object Description
Activity Cancelled Runs	The total number of activity runs that were canceled within a minute window.
Activity Failed Runs	The total number of activity runs that failed within a minute window.
Activity Succeeded Runs	The total number of activity runs that succeeded within a minute window.
Factory Size In Gb Units	Total factory size (GB unit).
Integration Runtime Available Memory	Integration runtime available memory.
Integration Runtime Available Node Number	Integration runtime available node count.

Microsoft: Azure Data Factory Performance	
Object Name	Object Description
Integration Runtime Average Task Pickup Delay	Integration runtime queue duration.
Integration Runtime Cpu Percentage	Integration runtime CPU utilization.
Integration Runtime Queue Length	Integration runtime queue length.
Max Allowed Factory Size In Gb Units	Maximum allowed factory size (GB unit).
Max Allowed Resource Count	Maximum allowed entities count.
Pipeline Cancelled Runs	The total number of pipeline runs that were canceled within a minute window.
Pipeline Elapsed Time Runs	Number of times, within a minute window, a pipeline runs longer than user-defined expected duration.
Pipeline Failed Runs	The total number of pipeline runs that failed within a minute window.
Pipeline Succeeded Runs	The total number of pipeline runs that succeeded within a minute window.
Resource Count	Total entities count.
Ssisintegration Runtime Start Cancel	The total number of SSIS integration runtime starts that were canceled within a minute window.
Ssisintegration Runtime Start Failed	The total number of SSIS integration runtime starts that failed within a minute window.
Ssisintegration Runtime Start Succeeded	The total number of SSIS integration runtime starts that succeeded within a minute window.
Ssisintegration Runtime Stop Stuck	The total number of SSIS integration runtime stops that were stuck within a minute window.
Ssisintegration Runtime Stop Succeeded	The total number of SSIS integration runtime stops that succeeded within a minute window.
Ssispackage Execution Cancel	The total number of SSIS package executions that were canceled within a minute window.
Ssispackage Execution Failed	The total number of SSIS package executions that failed within a minute window.
Ssispackage Execution Succeeded	The total number of SSIS package executions that succeeded within a minute window.
Trigger Cancelled Runs	The total number of trigger runs that were canceled within a minute window.
Trigger Failed Runs	The total number of trigger runs that failed within a minute window.
Trigger Succeeded Runs	The total number of trigger runs that succeeded within a minute window.

Azure Database for MySQL

Microsoft: Azure Database for MySQL DB Configuration	
Object Name	Object Description
Name	The name of the resource.
Charset	The charset of the database.
Collation	The collation of the database.

Microsoft: Azure Database for MySQL Parameters Configuration	
Object Name	Object Description
Parameter Name	The name of the resource
Parameter Name	The name of the resource
Parameter Name	The name of the resource
Default Value	Default value of the configuration.
Default Value	Default value of the configuration.
Default Value	Default value of the configuration.
Current Value	Value of the configuration.
Current Value	Value of the configuration.
Current Value	Value of the configuration.
Allowed Values	Allowed values of the configuration.
Allowed Values	Allowed values of the configuration.
Allowed Values	Allowed values of the configuration.
Pending Restart	Represents if the server needs to be restart, cause one or more static properties were changed.
Pending Restart	Represents if the server needs to be restart, cause one or more static properties were changed.
Pending Restart	Represents if the server needs to be restart, cause one or more static properties were changed.
Source	Source of the configuration.
Source	Source of the configuration.
Source	Source of the configuration.
Description	Description of the configuration.
Description	Description of the configuration.
Description	Description of the configuration.
Server Innodb Parameters Configuration	Label for the group
Server Log Parameters Configuration	Label for the group

Microsoft: Azure Database for MySQL Parameters Configuration	
Object Name	Object Description
Server Parameters Overall Configuration	Label for the group

Microsoft: Azure Database for MySQL Performance	
Object Name	Object Description
Active Connections	The number of active connections to the server.
Backup Storage Used	The amount of backup storage used.
CPU Percent	The percentage of CPU in use.
Failed Connections	The number of failed connections to the server.
IO Percent	The percentage of IO in use.(Not applicable for Basic tier servers)
Memory Percent	The percentage of memory in use.
Network In	Network In across active connections.
Network Out	Network Out across active connections.
Replication Lag in Seconds	The number of seconds the replica server is lagging against the master server. (Not applicable for Basic tier servers)
Server Log Storage Limit	The maximum server log storage for this server.
Server Log Storage Percent	The percentage of server log storage used out of the server's maximum server log storage.
Server Log Storage Used	The amount of server log storage in use.
Storage Limit	The maximum storage for this server.
Storage Percent	The percentage of storage used out of the server's maximum.
Storage Used	The amount of storage in use. The storage used by the service may include the database files, transaction logs, and the server logs.

Microsoft: Azure Database for MySQL Server Configuration	
Object Name	Object Description
Firewall Rule Name	Name for firewall rule.
Name	Name of the Replica.
Name	Resource Group Name.
Name	The virtual network resource name.
Rule Name	Virtual Network Rule Name.
Start IP	Start IP address for the MySQL firewall rule.
Administrator Login	The MySQL Server Administrator Login.

Microsoft: Azure Database for MySQL Server Configuration	
Object Name	Object Description
Azure MySQL Server/MySQL Server Replica	Resource id of the MySQL Server Replica.
Azure MySQL Server/Resource Group	Resource id of the Resource Group.
Azure MySQL Server/Subnet	Resource id of the virtual network subnet.
Azure MySQL Server/Virtual Network	Resource id of the Virtual Network.
Backup Retention Days	Backup retention days for the server.
By OK Enforcement	Status showing whether the server data encryption is enabled with customer-managed keys.
Earliest Restore Date	Earliest restore point creation time (ISO8601 format).
End IP	End IP address for the MySQL firewall rule.
Fully Qualified Domain Name	The fully qualified domain name of a server.
Geo Redundant Backup	Enable Geo-redundant or not for server backup.
Infrastructure Encryption	Status showing whether the server enabled infrastructure encryption.
Key	The MySQL Server tag keys.
Location	The geo-location where the resource lives.
Master Server Id	The master server id of a replica server.
Minimal TLS Version	Enforce a minimal Tls version for the server.
Name	The administrators login name of a server.
Public Network Access	Whether or not public network access is allowed for this server. Value is optional but if passed in, must be 'Enabled' or 'Disabled'
Replication Role	The replication role of the server.
SSL Enforcement	Enable ssl enforcement or not when connect to server.
State	A state of a server that is visible to user.
Storage Autogrow	Enable Storage Auto Grow.
Storage(MB)	Max storage allowed for a server.
Value	The MySQL Server tag values.
Version	The MySQL Server version.

Azure Database for PostgreSQL

Microsoft: Azure Database for PostgreSQL DB Configuration	
Object Name	Object Description
Name	The name of the resource.
Collation	The collation of the database.
Charset	The charset of the database.

Microsoft: Azure Database for PostgreSQL Params Configuration	
Object Name	Object Description
Parameter Name	The name of the resource Parameter config.
Parameter Name	The name of the resource Parameter config.
Parameter Name	The name of the resource Parameter config.
Value	Value of the configuration.
Value	Value of the configuration.
Value	Value of the configuration.
Data Type	Data type of the configuration.
Data Type	Data type of the configuration.
Data Type	Data type of the configuration.
Default Value	Default value of the configuration.
Default Value	Default value of the configuration.
Default Value	Default value of the configuration.
Pending Restart	if the parameter requires a server restart.
Pending Restart	if the parameter requires a server restart.
Pending Restart	if the parameter requires a server restart.
Description	Description of the configuration.
Description	Description of the configuration.
Description	Description of the configuration.

Microsoft: Azure Database for PostgreSQL Server Configuration	
Object Name	Object Description
Firewall Rule Name	The Firewall Rule name of the resource.
Name	The name of the sku, typically, tier + family + cores, e.g. B_Gen4_1, GP_Gen5_8.
Rule Name	A virtual network rule name.

Microsoft: Azure Database for PostgreSQL Server Configuration	
Object Name	Object Description
Name	The name of the postgreSQL resource.
Name	Resource Group Name.
Name	The replica name of the resource
Name	The virtual network resource name.
Start Ip	The start IP address of the server firewall rule. Must be IPv4 format.
State	Virtual Network Rule State
Tier	The tier of the particular SKU, e.g. Basic.
Administrator Login	The administrator's login name of a server. Can only be specified when the server is being created (and is required for creation).
Azure PostgreSQL Server/PostgreSQL Server Replica	PostgreSQL resource ID.
Azure PostgreSQL Server/Resource Group	Resource id of the Resource Group.
Azure PostgreSQL Server/Subnet	The ARM resource id of the virtual network subnet.
Azure PostgreSQL Server/Virtual Network	Resource id of the Virtual Network.
Backup Retention Days	Backup retention days for the server.
By Ok Enforcement	Status showing whether the server data encryption is enabled with customer-managed keys.
Capacity	The scale up/out capacity, representing server's compute units.
Earliest Restore Date	Earliest restore point creation time (ISO8601 format)
End Ip	The end IP address of the server firewall rule. Must be IPv4 format.
Family	The family of hardware.
Fully Qualified Domain Name	The fully qualified domain name of a server.
Geo Redundant Backup	Enable Geo-redundant or not for server backup.
Ignore Missing Vnet Service Endpoint	Create firewall rule before the virtual network has vnet service endpoint enabled.
Infrastructure Encryption	Status showing whether the server enabled infrastructure encryption.
Key	The PostgreSQL Server tag keys.
Master Server Id	The master server id of a replica server.
Minimal Tls Version	Enforce a minimal Tls version for the server.
Principal Id	The Azure Active Directory principal id.
Public Network Access	Whether or not public network access is allowed for this server. Value is optional but if passed in, must be Enabled or Disabled.

Microsoft: Azure Database for PostgreSQL Server Configuration	
Object Name	Object Description
Replica Capacity	The maximum number of replicas that a master server can have.
Replication Role	The replication role of the server.
Replication Role	The replication role of the server.
Size	The size code, to be interpreted by resource as appropriate.
Ssl Enforcement	Enable ssl enforcement or not when connect to server.
Storage (MB)	Max storage allowed for a server.
Storage Autogrow	Enable Storage Auto Grow.
Tenant Id	The Azure Active Directory tenant id.
Type	The identity type. Set this to 'SystemAssigned' in order to automatically create and assign an Azure Active Directory principal for the resource.
User Visible State	A state of a server that is visible to user.
Value	The PostgreSQL Server tag values.
Version	Server version.

Microsoft: Azure Database for PostgreSQL Server Performance	
Object Name	Object Description
Active Connections	Active Connections.
Backup Storage Used	Backup Storage Used.
CPU Percent	CPU percent.
Failed Connections	Failed Connections.
IO Percent	IO percent.(Not applicable for Basic tier servers.)
Max Lag Across Replicas	Lag in bytes of the most lagging replica.
Memory Percent	Memory percent.
Network In	Network In across active connections.
Network Out	Network Out across active connections.
Replica Lag	Replica lag in seconds.
Server Log Storage Limit	Server Log storage limit.
Server Log Storage Percent	Server Log storage percent.
Server Log Storage Used	Server Log storage used.
Storage Limit	Storage limit.
Storage Percent	Storage percent.
Storage Used	Storage used.

Azure Databricks Service

Microsoft: Azure Databricks Configuration	
Object Name	Object Description
Id	Fully qualified resource Id for the resource. Ex - /subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/{resourceProviderNamespace}/{resourceType}/{resourceName}
Id	The unique identifier of the databricks workspace in databricks control plane.
Name	The name of the resource.
Storage Account Name	Default DBFS storage account name.
SKU Name	The SKU name.
Storage Account Sku Name	Storage account SKU name, ex: Standard_GRS, Standard_LRS. Refer https://aka.ms/storageskus for valid inputs.
Url	The workspace URL which is of the format: adb-{workspaceId}.{random}.azuredatabricks.net
Azure Databrick/Resource Group	Databricks Resource Group Identifier.
Azure Databrick/Storage Account	Databricks Storage Account Identifier.
Created Date	Specifies the date and time when the workspace is created.
Enable No Public IP	Should the Public IP be Disabled?
Key	Databricks Tag Key.
Managed Resource Group	The managed resource group Id.
Name	Databricks Resource Group Name.
Name	Databricks Storage Account Name.
Nat Gateway Name	Name of the NAT gateway for Secure Cluster Connectivity (No Public IP) workspace subnets.
Provisioning State	The workspace provisioning state.
Public IP Name	Name of the Public IP for No Public IP workspace with managed vNet.
Relay Namespace Name	Relay Namespace Name of the device.
Value	Databricks Tag Value.
Vnet Address Prefix	Address prefix for Managed virtual network. Default value for this input is 10.139.

Azure DNS Service

Microsoft: Azure DNS Zone Configuration	
Object Name	Object Description
Resource Group Name	Azure resource group Name assosiated with Azure DNS Zone.
Azure DNS/Resource Group	Azure resource group ID assosiated with Azure DNS Zone.
ID	The ID of an Azure DNS zone.
Key	Key of the tag pair.
Location	The location of an Azure DNS zone.
Max Number of Record Sets	The maximum number of record sets of an Azure DNS zone.
Name	The name of an Azure DNS zone.
Name Servers	The name servers of an Azure DNS zone.
Number of Record Sets	The number of record sets of an Azure DNS zone.
Value	Value of the tag pair.

Microsoft: Azure DNS Zone Performance	
Object Name	Object Description
Query Volume	Number of queries served for a DNS zone.
Record Set Capacity Utilization	Percent of Record Set capacity utilized by a DNS zone.
Record Set Count	Number of Record Sets in a DNS zone.

Azure Event Grid

Microsoft: Azure Event Grid Domain Configuration	
Object Name	Object Description
Azure Event Grid Domain / Resource Group	Resource id of the Resource Group.
Endpoint	Endpoint for the Event Grid Domain Resource which is used for publishing the events.
ID	Fully qualified identifier of the resource.
Name	Name of the resource.
Name	Resource Group name.

Microsoft: Azure Event Grid Domain Configuration	
Object Name	Object Description
Provisioning State	Provisioning state of the Event Grid Domain Resource.
Tag Key	Tags Key.
Tag Value	Tags Value.

Microsoft: Azure Event Grid Domain Performance	
Object Name	Object Description
Advanced Filter Evaluations	Total advanced filters evaluated across event subscriptions for this topic.
Dead Lettered Events	Total dead lettered events matching to this event subscription.
Delivered Events	Total events delivered to this event subscription.
Delivery Failed Events	Total events failed to deliver to this event subscription.
Destination Processing Duration	Destination processing duration in milliseconds.
Dropped Events	Total dropped events matching to this event subscription.
Error Delivery Failed Events	Error events failed to deliver to this event subscription.
Error Delivery Failed Events(Labels)	The Error name.
Error Publish Failed Events	Error events failed to publish to this topic.
Error Publish Failed Events (Labels)	The Error name.
Matched Events	Total events matched to this event subscription.
Publish Failed Events	Total events failed to publish to this topic.
Publish Success Latency	Publish success latency in milliseconds.
Published Events	Total events published to this topic.

Microsoft: Azure Event Grid Domain Subscription Configuration	
Object Name	Object Description
Advanced Filtering On Arrays	Allows advanced filters to be evaluated against an array of values instead of expecting a singular value.
Azure Event Grid Domain Event Subscription / Resource Group	Resource id of the Resource Group.
Destination	The Id that represents the endpoint of the destination of an event subscription.
Destination Endpoint Type	Type of the endpoint for the event subscription destination.

Microsoft: Azure Event Grid Domain Subscription Configuration	
Object Name	Object Description
Destination Name	Name of the destination.
Event Delivery Schema	The event delivery schema for the event subscription.
ID	Fully qualified identifier of the resource.
Included Event Types	A list of applicable event types that need to be part of the event subscription. If it is desired to subscribe to all default event types, set the IncludedEventTypes to null.
Is Subject Case Sensitvie	Specifies if the SubjectBeginsWith and SubjectEndsWith properties of the filter should be compared in a case sensitive manner.
Key	The field/property in the event based on which you want to filter.
Name	Name of the resource.
Name	Resource Group name.
Operator Type	The operator type used for filtering, e.g., NumberIn, StringContains, BoolEquals and others
Provisioning State	Provisioning state of the event subscription.
Resource Group Relationships	Resource Group name.
Retry Policy	Maximum number of delivery retry attempts for events.
Subject Begins With	An optional string to filter events for an event subscription based on a resource path prefix.
Subject Ends With	An optional string to filter events for an event subscription based on a resource path suffix.
Value	The filter value.

Microsoft: Azure Event Grid Domain Topic Subscription Config	
Object Name	Object Description
Advanced Filtering On Arrays	Allows advanced filters to be evaluated against an array of values instead of expecting a singular value.
Azure Event Grid Domain Event Subscription / Resource Group	Resource id of the Resource Group.
Destination	The Id that represents the endpoint of the destination of an event subscription.
Destination Endpoint Type	Type of the endpoint for the event subscription destination.
Destination Name	Name of the destination.

Microsoft: Azure Event Grid Domain Topic Subscription Config	
Object Name	Object Description
Event Delivery Schema	The event delivery schema for the event subscription.
ID	Fully qualified identifier of the resource.
Included Event Types	A list of applicable event types that need to be part of the event subscription. If it is desired to subscribe to all default event types, set the IncludedEventTypes to null.
Is Subject Case Sensitvie	Specifies if the SubjectBeginsWith and SubjectEndsWith properties of the filter should be compared in a case sensitive manner.
Key	The field/property in the event based on which you want to filter.
Name	Resource Group name.
Name	Name of the resource.
Operator Type	The operator type used for filtering, e.g., NumberIn, StringContains, BoolEquals and others
Provisioning State	Provisioning state of the event subscription.
Resource Group Relationships	Resource Group name.
Retry Policy	Maximum number of delivery retry attempts for events.
Subject Begins With	An optional string to filter events for an event subscription based on a resource path prefix.
Subject Ends With	An optional string to filter events for an event subscription based on a resource path suffix.
Value	The filter value.

Microsoft: Azure Event Grid Domain Topics Configuration	
Object Name	Object Description
Azure Event Grid Topic / Resource Group	Resource id of the Resource Group.
ID	Fully qualified identifier of the resource.
Name	Name of the resource.
Name	Resource Group name.
Provisioning State	Provisioning state of the domain topic.

Microsoft: Azure Event Grid Event Subscription Performance	
Object Name	Object Description
Dead Lettered Events	Total dead lettered events matching to this event subscription.

Microsoft: Azure Event Grid Event Subscription Performance	
Object Name	Object Description
Delivered Events	Total events delivered to this event subscription.
Delivery Failed Events	Total events failed to deliver to this event subscription.
Destination Processing Duration	Destination processing duration in milliseconds.
Dropped Events	Total dropped events matching to this event subscription.
Matched Events	Total events matched to this event subscription

Microsoft: Azure Event Grid System Topics Configuration	
Object Name	Object Description
Azure Event Grid System Topic / Resource Group	Resource id of the Resource Group.
Azure Event Grid System Topic / Source	Source id of the Source.
Id	Fully qualified identifier of the resource.
Name	Name of the resource.
Name	Resource Group name.
Name	Source name.
Provisioning State	Provisioning state of the system topic.
Tag Key	Tags key.
Tag Value	Tags value.
Topic Type	TopicType for the system topic.

Microsoft: Azure Event Grid System Topics Performance	
Object Name	Object Description
Advanced Filter Evaluations	Total advanced filters evaluated across event subscriptions for this topic.
Dead Lettered Events	Total dead lettered events matching to this event subscription.
Delivered Events	Total events delivered to this event subscription.
Delivery Failed Events	Total events failed to deliver to this event subscription.
Destination Processing Duration	Destination processing duration in milliseconds.
Dropped Events	Total dropped events matching to this event subscription.
Matched Events	Total events matched to this event subscription.
Publish Failed Events	Total events failed to publish to this topic.
Publish Success Latency	Publish success latency in milliseconds.

Microsoft: Azure Event Grid System Topics Performance	
Object Name	Object Description
Published Events	Total events published to this topic.
Unmatched Events	Total events not matching any of the event subscriptions for this topic.

Microsoft: Azure Event Grid Topic Configuration	
Object Name	Object Description
Azure Event Grid Topic / Resource Group	Resource id of the Resource Group.
Endpoint	Endpoint for the topic.
ID	Fully qualified identifier of the resource.
Name	Name of the resource.
Name	Resource Group name.
Provisioning State	Provisioning state of the Event Grid Domain Resource.
Tag Key	Tags Key.
Tag Value	Tags value.

Microsoft: Azure Event Grid Topic Performance	
Object Name	Object Description
Advanced Filter Evaluations	Total advanced filters evaluated across event subscriptions for this topic.
Dead Lettered Events	Total dead lettered events matching to the event subscriptions for this topic
Delivered Events	Total events failed to deliver to the event subscriptions for this topic
Delivery Failed Events	Total events delivered to the event subscriptions for this topic
Destination Processing Duration	Destination processing duration in millisecond
Dropped Events	Total dropped events matching to the event subscriptions for this topic
Matched Events	Total events matched to the event subscriptions for this topic
Publish Failed Events	Total events failed to publish to this topic
Publish Success Latency	Total events published to this topic
Published Events	Publish success latency in milliseconds
Unmatched Events	Total events not matching any of the event subscriptions for this topic

Azure ExpressRoute Service

Microsoft: Azure ExpressRoute Circuit Configuration	
Object Name	Object Description
Bandwidth	Bandwith in Mbps
Circuit Provisioning State	The State of provisioning
ID	the id of circuit
Location	the location of circuit
Name	the name of circuit
Peering Location	the location of peering
Provisioning State	the state of circuit
Service Key	the service key of circuit
Service Provider Name	the service provider name
Service Provider Provisioning State	The state of service provider

Microsoft: Azure ExpressRoute Circuit Connection Configuration	
Object Name	Object Description
Address Prefix	The ExpressRoute Circuit Connection address prefix.
Circuit Connection State	The ExpressRoute Circuit Connection Status.
ID	The ID of the ExpressRoute Circuit Connection.
Name	The ExpressRoute Circuit Connection name.
Peer Circuit Peering ID	The ExpressRoute Peer Circuit; Peering ID.
Provisioning State	The Provisioning State of the ExpressRoute Circuit Connection.

Microsoft: Azure ExpressRoute Circuit Performance	
Object Name	Object Description
ARP Availability Overall	Overall ARP availability across peers
ARP Availability Primary	ARP availability for the Primary peer
ARP Availability Secondary	ARP availability for the Secondary peer
BGP Availability Overall	Aggregate BGP availability across peers
BGP Availability Primary	BGP availability for the Primary peer
BGP Availability Secondary	BGP availability for the Secondary peer
Bits In Per Second	Bits ingressing Azure per second

Microsoft: Azure ExpressRoute Circuit Performance	
Object Name	Object Description
Bits Out Per Second	Bits egressing Azure per second
Egress Bandwidth Utilization	Egress Link Bandwidth percentage utilization.
FastPath Routes Count	Count of FastPath routes configured on the circuit.
Global Reach Bits In Per Second	Bits ingressing Azure per second via Global Reach.
Global Reach Bits Out Per Second	Bits egressing Azure per second via Global Reach.
Ingress Bandwidth Utilization	Ingress Link Bandwidth percentage utilization.
Qos Drop Bits In Per Second	Bits per second dropped on ingress due to QoS policy.
Qos Drop Bits Out Per Second	Bits per second dropped on egress due to QoS policy.

NOTE: A Major alert triggers when BGP or ARP availability drops below 100% for a single peer. A Critical alert triggers when both peers are down, which automatically suppresses the Major alert.

Microsoft: Azure ExpressRoute Direct Configuration	
Object Name	Object Description
Name	Name of child port resource that is unique among child port resources of the parent.
Name	Resource name.
Admin State	Administrative state of the physical port.
Azure ExpressRoute Direct / Resource Group	Resource id of the Resource Group.
Bandwidth	Bandwidth of procured ports in Gbps.
Billing Type	The billing type of the ExpressRoutePort resource.
ColoLocation	ColoLocation for ExpressRoute Hybrid Direct.
Connector Type	Physical fiber port type.
Encapsulation	Encapsulation method on physical ports.
Ether Type	Ether type of the physical port.
Interface Name	Name of Azure router interface.
Links	Links
Location	Resource location.
MTU	Maximum transmission unit of the physical port pair (s).
Name	Resource Group Name.

Microsoft: Azure ExpressRoute Direct Configuration	
Object Name	Object Description
Patch Panel Id	Mapping between physical port to patch panel port.
Peering Location	The name of the peering location that the ExpressRoutePort is mapped to physically.
Provisioned Bandwidth	Aggregate Gbps of associated circuit bandwidths.
Provisioning State	The provisioning state of the express route port resource.
Rack Id	Mapping of physical patch panel to rack.
Router Name	Name of Azure router associated with physical port.
Tag Key	Tags Key.
Tag Value	Tags Value.
Tags	Tags

Microsoft: Azure ExpressRoute Direct Performance	
Object Name	Object Description
Admin State	Admin state of the port
Admin State Labels	Admin State Labels
Bits In Per Second	Bits ingressing Azure per second.
Bits In Per Second Labels	Bits In Per Second Labels
Bits Out Per Second	Bits egressing Azure per second
Bits Out Per Second Labels	Bits Out Per Second Labels
Fast Path Routes Count	Count of fastpath routes configured on port
Line Protocol	Line protocol status of the port
Line Protocol Labels	Line Protocol Labels
Rx Light Level	Rx Light level in dBm
Rx Light Level Labels	Rx Light Level Labels
Tx Light Level	Tx Light level in dBm
Tx Light Level Labels	Tx Light Level Labels

NOTE: When configuring the threshold values for the "Microsoft: Azure ExpressRoute Direct Performance" Dynamic Application, enter the threshold values as positive numbers. The alert formula multiplies the value entered by negative one (-1) to reach the correct threshold value.

Microsoft: Azure ExpressRoute Peering Configuration	
Object Name	Object Description
Advertised Public Prefixes	The reference of AdvertisedPublicPrefixes.
Advertised Public Prefixes	The reference of AdvertisedPublicPrefixes.
Advertised Public Prefixes State	AdvertisedPublicPrefixState of the Peering resource. Possible values are NotConfigured, Configuring, Configured, and ValidationNeeded.
Azure ASN	The Azure ASN.
Customer ASN	The CustomerASN of the peering.
ID	Resource ID.
Last Modified By	Gets whether the provider or the customer last modified the peering.
Name	The name of the Peering resource.
Peer ASN	The peer ASN.
Peering Type	The Peering type. Possible values are: AzurePublicPeering, AzurePrivatePeering, and MicrosoftPeering.
Primary Azure Port	The primary port.
Primary Peer Address Prefix	The primary address prefix.
Primary Peer Address Prefix	The primary address prefix.
Provisioning State	The provisioning state of the public IP resource. Possible values are: Succeeded, Updating, Deleting and Failed.
Secondary Azure Port	The secondary port.
Secondary Peer Address Prefix	The secondary address prefix.
Secondary Peer Address Prefix	The secondary address prefix.
State	The state of peering. Possible values are: Disabled and Enabled.
State	The state of peering. Possible values are: Disabled and Enabled.
VLAN ID	The VLAN ID.

Microsoft: Azure ExpressRoute Peering Performance	
Object Name	Object Description
Bits In Per Second	Bits ingressing Azure per second
Bits Out Per Second	Bits egressing Azure per second

Azure Fabric Capacity Service

Microsoft: Azure Fabric Capacity Configuration	
Object Name	Object Description
Admin Member	An administrator user identity for the Fabric capacity resource.
Administration	The administration properties of the Fabric capacity resource.
Azure Fabric Capacity / Resource Group	The fully qualified resource ID for the Fabric capacity resource within the resource group.
Location	The geo-location where the resource lives.
Name	The name of the resource.
Provisioning State	The current deployment state of Microsoft Fabric resource. The provisioningState is to indicate states for resource provisioning.
Resource Group Name	The name of the resource group containing this Fabric capacity resource.
Resource Groups	The resource group containing this Fabric capacity resource.
SKU Name	The name of the SKU level.
SKU Tier	The name of the Azure pricing tier to which the SKU applies.
State	The current state of Microsoft Fabric resource. The state is to indicate more states outside of resource provisioning.
Tag Key	The key of the tag applied to the Fabric capacity resource.
Tag Value	The value of the tag applied to the Fabric capacity resource.
Tags	Resource tags.

Azure Firewall Service

Microsoft: Azure Firewall Configuration	
Object Name	Object Description
Name	Name of the resource that is unique within a resource group. This name can be used to access the resource.

Microsoft: Azure Firewall Configuration	
Object Name	Object Description
Name	The name of the resource that is unique within the Azure firewall. This name can be used to access the resource.
Name	The name of the resource that is unique within the Azure firewall. This name can be used to access the resource.
Name	The name of the resource that is unique within the Azure firewall. This name can be used to access the resource.
Private IP Address	The Firewall Internal Load Balancer IP to be used as the next hop in User Defined Routes.
Provisioning State	The provisioning state of the Azure firewall IP configuration resource.
Resource Group name.	Resource Group name.
Action	The action type of a rule collection.
Action	The action type of a rule collection.
Action	The action type of a NAT rule collection.
Azure Firewall / Resource Group	Resource id of the Resource Group.
Azure Firewall / Subnet	Reference to the subnet resource. This resource must be named AzureFirewallSubnet or AzureFirewallManagementSubnet.
Etag	A unique read-only string that changes whenever the resource is updated.
Firewall Policy Id	The Firewall Policy associated with this azure firewall.
Hub IPs Count	The number of Public IP addresses associated with azure firewall.
Hub Private IP	Private IP Address associated with azure firewall.
Hub Public IPs	The list of Public IP addresses associated with azure firewall or IP addresses to be retained.
IP Configurations	IP Configurations
Location	Resource location
Name	Resource name
Name	Name of an Azure Firewall SKU.
Priority	Priority of the network rule collection resource.
Priority	Priority of the application rule collection resource.
Priority	Priority of the NAT rule collection resource.
Provisioning State	The current provisioning state.
Provisioning State	The provisioning state of the NAT rule collection

Microsoft: Azure Firewall Configuration	
Object Name	Object Description
	resource.
Provisioning State	The provisioning state of the application rule collection resource.
Provisioning State	The provisioning state of the network rule collection resource.
Public IP Address	Reference to the PublicIP resource. This field is a mandatory input if subnet is not null.
Resource Group Relationships	Resource Group Relationships
Tag Key	Tags key.
Tag Value	Tags value.
Tags	Tags
Threat Intelligence Mode	The operation mode for Threat Intelligence.
Tier	Tier of an Azure Firewall.
Virtual Hub	The virtualHub to which the firewall belongs.
Zones	A list of availability zones denoting where the resource needs to come from.

Microsoft: Azure Firewall Performance	
Object Name	Object Description
Application Rules Hit	Number of times Application rules were hit
Application Rules Hit	Number of times Application rules were hit
Data Processed	Total amount of data processed by this firewall
Firewall Health	Indicates the overall health of this firewall
Firewall Health By Reason	Firewall health percentage broken down by contributing reason code.
Firewall Latency Probe	Average latency, in milliseconds, measured by a health probe sent from the firewall. A value of 0 indicates probe failure.
Network Rules Hit	Number of times Network rules were hit.
Network Rules Hit	Number of times Network rules were hit.
Network Rules Hit	Number of times Network rules were hit.
Observed Capacity	The percentage of the firewall's provisioned capacity currently in use, based on throughput, connections per second, rule processing time, and SNAT port utilization.
SNAP Port Utilization	Percentage of outbound SNAT ports currently in use.
Throughput	Throughput processed by this firewall.

Azure Front Door Service

Microsoft: Azure Front Door Configuration	
Object Name	Object Description
Name	The Front Door profile name.
Name	The Resource Group Name.
ARM Resource ID	Full ARM path of the Front Door profile resource.
Azure Front Door Profile/Resource Group	Azure Resource Group ID associated with the Azure Front Door Profile.
Front Door ID	Unique ID of the Front Door profile resource.
Health Probe Interval	Interval between health probes in seconds for the first origin group.
Health Probe Path	Path relative to the origin used to determine origin health for the first origin group.
Location	Resource location.
Origin Group Count	The number of Origin Groups configured for the Front Door profile.
Provisioning State	Current provisioning status: Succeeded|Failed|Updating|Deleting|Creating
Resource State	Operational state: Creating | Active | Deleting | Disabled | Migrating | Migrated | PendingMigrationCommit | CommittingMigration | AbortingMigration
SKU Name	Name of the pricing tier.
Tag Key	Tags key.
Tag Value	Tags values.
Type	Resource type.
WAF Policy Enabled	Set to True if the WAF Policy name is found, otherwise False.
WAF Policy Name	Name of the Web application firewall policy associated with the Front Door profile.

Microsoft: Azure Front Door Performance	
Object Name	Object Description
Origin Health Percentage	The percentage of successful health probes from AFDX to backends.
Origin Latency	The time calculated from when the request was sent by AFDX edge to the backend until AFDX received

Microsoft: Azure Front Door Performance	
Object Name	Object Description
	the last response byte from the backend.
Origin Request Count	The number of requests sent from AFDX to origin.
Percentage of 4XX	The percentage of all the client requests for which the response status code is 4XX.
Percentage of 5XX	The percentage of all the client requests for which the response status code is 5XX.
Request Count	The number of client requests served by the HTTP/S proxy.
Request Size	The number of bytes sent as requests from clients to AFDX.
Response Size	The number of bytes sent as responses from HTTP/S proxy to clients.
Total Latency	The time calculated from when the client request was received by the HTTP/S proxy until the client acknowledged the last response byte from the HTTP/S proxy.
Web Application Firewall Request Count	The number of client requests processed by the Web Application Firewall.

Azure Function App Service Plan

Microsoft: Azure Function App Performance	
Object Name	Object Description
App Connections	The average of App Connections.
Average Memory Working Set	Average of memory working set.
Bytes Received	Total bytes received.
Bytes Sent	Total bytes sent.
Current Assemblies	Average of current Assemblies.
File System Usage	File System Usage.
Function Execution Count	Function Execution Count for the Function App.
Function Execution Units	Function Execution Units for the Function App.
Gen 0 Collections	Total number of Gen 0 Garbage Collections.
Gen 1 Collections	Total number of Gen 1 Garbage Collections.
Gen 2 Collections	Total number of Gen 2 Garbage Collections.
Handles	Average of Handle Count.
Health Check Status	Health check status.

Microsoft: Azure Function App Performance	
Object Name	Object Description
Http5xx	Total of Http 5xx errors.
Io Other Bytes Per Second	Total of IO Other Bytes Per Second.
Io Other Operations Per Second	Total of IO Other Operations Per Second.
Io Read Bytes Per Second	Total of IO Read Bytes Per Second.
Io Read Operations Per Second	Total of IO Read Operations Per Second.
Io Write Bytes Per Second	Total of IO Write Bytes Per Second.
Io Write Operations Per Second	Total of IO Write Operations Per Second.
Memory Working Set	Average of Memory working set.
Private Bytes	Total of Private bytes.
Requests In Application Queue	Average of Requests In Application Queue.
Threads	Average of Thread Count.
Total App Domains	Total of App Domains.
Total App Domains Unloaded	Total of App Domains Unloaded.

Azure Functions

Microsoft: Azure Function List Configuration	
Object Name	Object Description
Function URL	The Function URL.
Language	The Function language.
Name	The Function name.
Status	The value indicating whether the function is disabled.

Azure HDInsight Service

Microsoft: Azure HDInsight Cluster Applications Configuration	
Object Name	Object Description
Application State	The application state.
Application Type	The application type.
Created Date	The application create date time.
ID	Fully qualified resource ID for the resource.

Microsoft: Azure HDInsight Cluster Applications Configuration	
Object Name	Object Description
Marketplace Identifier	The marketplace identifier.
Name	The name of the resource.
Provisioning State	The provisioning state of the application.
Tag Application Name	Tags application.
Tag Key	Tags key.
Tag Value	Tags value.

Microsoft: Azure HDInsight Cluster Configuration	
Object Name	Object Description
Role	The name of the role.
Target Instance Count	The instance count of the cluster.
Autoscale	The autoscale request parameters
Azure HDInsight Cluster/Storage Account	The resource ID of storage account, only to be specified for Azure Data Lake Storage Gen 2.
Encrypt Data Disks	Indicates whether encrypt the data disks.
Encryption At Host	Indicates whether or not resource disk encryption is enabled.
Hardware Profile VM Size	The hardware profile. The size of the VM.
Kafka Security Group Name	The AAD security group name.
Kind	The type of cluster.
Name	The name of the endpoint.
Name	The name of the storage account.
OS Profile	The operating system profile.
Port	The port to connect to.
Protocol	The protocol of the endpoint.
Vault Uri	Base key vault URI where the customers key is located eg.
Version	The versions of different services in the cluster.
Azure HDInsight Cluster/Datalake	The datalake account of the HDInsight.
Azure HDInsight Cluster/Resource Group	Resource id of the Resource Group.
Azure HDInsight Cluster/Virtual Network Profile	The virtual network profile.
Blueprint	The link to the blueprint.
Cluster Hdp Version	The hdp version of the cluster.
Cluster Id	The cluster id.
Cluster Identity Type	The type of identity used for the cluster. The type SystemAssigned, UserAssigned includes both an

Microsoft: Azure HDInsight Cluster Configuration	
Object Name	Object Description
	implicitly created identity and a set of user assigned identities.
Cluster Status	The state of the cluster.
Cluster Version	The version of the cluster.
Container / Directory	The container in the storage account, only to be specified for WASB storage accounts.
Cores Used	The cores used by the cluster.
Created Date	The date on which the cluster was created.
Disk Encryption Properties	Disk Encryption Properties
Enable Compute Isolation	The flag indicates whether enable compute isolation or not.
Encryption Algorithm	Algorithm identifier for encryption, default RSA-OAEP.
Etag	The ETag for the resource.
Excluded Services Config	Excluded Services Config
Excluded Services Config Id	The config id of excluded services.
Excluded Services List	The list of excluded services.
File System	The filesystem, only to be specified for Azure Data Lake Storage Gen 2.
id	Connectivity endpoint identifier.
Id	Microsoft resource identifier. Specifies the identifying URL of the resource.
Is Default	Whether or not the storage account is the default storage account.
Is Encryption In Transit Enabled	Indicates whether or not inter cluster node communication is encrypted in transit.
kafka Configuration Override	The configurations that need to be overriden.
Kafka Security Group Id	The AAD security group id.
key Name	Key name that is used for enabling disk encryption.
key Version	Specific key version that is used for enabling disk encryption.
Location	The location of the endpoint.
Min Supported Tls Version	The minimal supported tls version.
MSI Resource Id	Resource ID of Managed Identity that is used to access the key vault.
Name	HDInsight cluster name.
Name	Resource Group name.

Microsoft: Azure HDInsight Cluster Configuration	
Object Name	Object Description
Name	Name of the Datalake
Os Type	The type of operating system.
Private IP Address	The private ip address of the endpoint.
Provisioning State	The provisioning state, which only appears in the response. Canceled, Deleting, Failed, InProgress, Succeeded
Storage Account Relationships	Storage Account Relationships.
Tag Key	Tags Key.
Tag Value	Tags value.
Tier	The cluster tier.

Microsoft: Azure HDInsight Cluster Counter Performance	
Object Name	Object Description
Cluster Counter	The count of clusters per location.

Microsoft: Azure HDInsight Cluster Performance	
Object Name	Object Description
Categorized Gateway Requests	Number of gateway requests by categories (1xx/2xx/3xx/4xx/5xx).
Categorized Gateway Requests	Number of gateway requests by categories (1xx/2xx/3xx/4xx/5xx).
Gateway Requests	Number of gateway requests.
Gateway Requests	Number of gateway requests.
Number of Active Workers	Number of Active Workers.
Number of Active Workers	Number of Active Workers.
Pending CPU	Pending CPU Requests in YARN.
Pending Memory	Pending Memory Requests in YARN.

Microsoft: Azure HDInsight Cluster Script Actions Configuration	
Object Name	Object Description
Script Execution ID	The execution id of the script action.
Name	The name of the script action.
Status	The current execution status of the script action.
Application Name	The application name of the script action, if any.
Roles	The list of roles where script will be executed.

Microsoft: Azure HDInsight Cluster Script Actions Configuration	
Object Name	Object Description
URL	The URI to the script.
Parameters	The parameters for the script

Azure Key Vault

Microsoft: Azure Key Vault Configuration	
Object Name	Object Description
Name	Resource key vault name.
Azure Active Directory Tenant ID	The Azure Active Directory tenant ID that should be used for authenticating requests to the key vault.
Azure Key Vault/Private Endpoint	Full identifier of the private endpoint resource.
Name	The subnet resource name.
Name	Virtual Network resource name.
Name	SKU name to specify whether the key vault is a standard vault or a premium vault.
Name	The name of the resource associated with the resource group.
Object Id	The object ID of a user, service principal or security group in the Azure Active Directory tenant for the vault. The object ID must be unique for the list of access policies.
Status	Indicates whether the connection has been approved, rejected or removed by the key vault owner.
URI	The URI of the vault for performing operations on keys and secrets.
Application Id	Application ID of the client making request on behalf of a principal.
Azure Active Directory Tenant ID	The Azure Active Directory tenant ID that should be used for authenticating requests to the key vault.
Azure Key Vault Rule/Subnet	A rule governing the accessibility of a vault from a specific virtual network.
Azure Key Vault/Resource Group	The resource Id associated with the resource group.
Azure Key Vault/Virtual Network	Virtual Network Resource Id.
Deployment	Property to specify whether Azure Virtual Machines are permitted to retrieve certificates stored as secrets from the key vault.

Microsoft: Azure Key Vault Configuration	
Object Name	Object Description
Description	The reason for approval or rejection of the linked private network.
Disk Encryptation	Property to specify whether Azure Disk Encryption is permitted to retrieve secrets from the vault and unwrap keys.
Family	SKU family name.
IP Rule	A rule governing the accessibility of a vault from a specific ip address or ip range. An IPv4 address range in CIDR notation, such as 124.56.78.91 (simple IP address) or 124.56.78.0/24 (all addresses that start with 124.56.78).
Network bypass	Tells what traffic can bypass network rules. This can be 'AzureServices' or 'None'. If not specified the default is 'AzureServices'.
Network Default Action	The default action when no rule from ipRules and from virtualNetworkRules match. This is only used after the bypass property has been evaluated.
Permissions to Certificates	Permissions to certificates.
Permissions to Keys	Permissions to keys.
Permissions to Secrets	Permissions to secrets.
Permissions to Storage Accounts	Permissions to storage accounts
Provisioning State	The current provisioning state.
Rbac Authorization	Property that controls how data actions are authorized. When true, the key vault will use Role Based Access Control (RBAC) for authorization of data actions, and the access policies specified in vault properties will be ignored (warning: this is a preview feature). When false, the key vault will use the access policies specified in vault properties, and any policy stored on Azure Resource Manager will be ignored. If null or not specified, the vault is created with the default value of false. Note that management actions are always authorized with RBAC.
Sof Delete Retention (Days)	Soft Delete data retention days. It accepts >=7 and <=90.
Soft Delete	Property to specify whether the 'soft delete' functionality is enabled for this key vault. If it's not set to any value (true or false) when creating new key vault, it will be set to true by default. Once set to true, it cannot be reverted to false.

Microsoft: Azure Key Vault Configuration	
Object Name	Object Description
Tag Key	Tags key.
Tag Value	Tags values.
Template Deployment	Property to specify whether Azure Resource Manager is permitted to retrieve secrets from the key vault.

Microsoft: Azure Key Vault Performance	
Object Name	Object Description
Overall Service Api Latency	Overall latency of service api requests
Overall Service Api Latency Labels	Service Api Latency Labels based on Activity Type.
Overall Vault Availability	Vault requests availability.
Overall Vault Availability Labels	Availability Labels based on Activity Type.
Overall Vault Saturation	Vault capacity used.
Overall Vault Saturation Labels	Saturation Shoebox Labels based on Activity Type.
Total Service Api Hits	Number of total service api hits.
Total Service Api Hits Labels	Service Api Hit Labels based on Activity Type.
Total Service Api Results	Number of total service api results.
Total Service Api Results Labels	Service Api Result Labels based on Activity Type.

Azure Kubernetes Service (AKS)

Microsoft: Azure Kubernetes Cluster Configuration	
Object Name	Object Description
Name	Unique name of the agent pool profile in the context of the subscription and resource group.
Subnet Name	Azure virtual network subnet Name associated with Azure kubernetes agent pool.
API server address	FQDN for the master pool.
Azure Kubernetes Agent Pool/Subnet	Azure virtual network subnet ID associated with Azure kubernetes agent pool.
DNS Prefix	DNS prefix specified when creating the managed cluster.
DNS Service IP	An IP address assigned to the Kubernetes DNS service. It must be within the Kubernetes service address range specified in serviceCidr.
Docker Bridge CIDR	A CIDR notation IP range assigned to the Docker

Microsoft: Azure Kubernetes Cluster Configuration	
Object Name	Object Description
	bridge network. It must not overlap with any Subnet IP ranges or the Kubernetes service address range.
Kubernetes Version	Version of Kubernetes specified when creating the managed cluster.
Kubernetes Version	Version of orchestrator specified when creating the managed cluster.
Load Balancer SKU	The load balancer sku for the managed cluster.
Location	Location of the resource.
Max Agent Pools	The max number of agent pools for the managed cluster.
Max Pods	Maximum number of pods that can run on a node.
Mode	Represents mode of an agent pool.
Name	Resource name.
Network Plugin	Network plugin used for building Kubernetes network.
Node Count	Number of agents (VMs) to host docker containers. Allowed values must be in the range of 0 to 100 (inclusive) for user pools and in the range of 1 to 100 (inclusive) for system pools. The default value is 1.
Node Image Version	Version of node image.
Node Resource Group	Name of the resource group containing agent pool nodes.
Node Sizes	Size of agent VMs.
OS Disk Size(GB)	OS Disk Size in GB to be used to specify the disk size for every machine in this master/agent pool. If you specify 0, it will apply the default osDisk size according to the vmSize specified.
OS Disk Type	OS disk type to be used for machines in a given agent pool. Allowed values are "Ephemeral" and "Managed". Defaults to "Managed". May not be changed after creation.
OS Type	OsType to be used to specify os type. Choose from Linux and Windows. Default to Linux.
Pod CIDR	A CIDR notation IP range from which to assign pod IPs when kubenet is used.
Power State	Describes whether the Agent Pool is Running or Stopped.
Power State	Represents the Power State of the cluster.
Provisioning State	The current deployment or provisioning state, which only appears in the response.

Microsoft: Azure Kubernetes Cluster Configuration	
Object Name	Object Description
Provisioning State	The current deployment or provisioning state, which only appears in the response.
Role-Based Access Control (RBAC)	Whether to enable Kubernetes Role-Based Access Control.
Service CIDR	A CIDR notation IP range from which to assign service cluster IPs. It must not overlap with any Subnet IP ranges.
SKU Name	Name of a managed cluster SKU.
SKU Tier	Tier of a managed cluster SKU.
Tag Key	Tags key.
Tag Value	Tags values.
Type	Represents types of an agent pool.
Type	Resource type.

Microsoft: Azure Kubernetes Cluster Performance	
Object Name	Object Description
Number of Pods by Phase	Number of pods by phase.
Number of Pods by Phase Labels	Phase of the Pod.
Number of Pods in Ready State	Number of pods in Ready state.
Number of Pods in Ready State Labels	Namespace of the Pod.
Statuses for Various Node Conditions	Statuses for various node conditions.
Statuses for Various Node Conditions Labels	Condition Type Represented on this metric.
Total Amount of Available Memory	Total amount of available memory in a managed cluster.
Total Number of Available CPU Cores	Total number of available cpu cores in a managed cluster.

Azure Load Balancer Service

Microsoft: Azure Load Balancer Configuration	
Object Name	Object Description
Azure Resource Group Name	The name of the Resource Group.
Azure Load Balancer/Resource Group	Azure Resource Group ID associated with Azure Load Balancer.
IP Address	Private IP Address to assign to the Load Balancer.

Microsoft: Azure Load Balancer Configuration	
Object Name	Object Description
IP Address Type	The type of IP Address configuration. Possible values are: 'Public' or 'Private'.
IP Allowed Method	The public or private IP allocation method. Possible values are: 'Static' or 'Dynamic'.
Location	Specifies the supported Azure location of the Load Balancer.
Name	User-defined name of the Backend Address Pool.
Name	The name of the Load Balancer.
Name	User-defined name of the Frontend IP configuration.
Provisioning State	Provisioning state of the Backend Address Pool.
Provisioning State	Provisioning state of the Load Balancer.
Tag Key	The key of tag pair, these keys are used by the Load Balancer.
Tag Value	The value of tag pair, these values are used by the Load Balancer.

Microsoft: Azure Standard Load Balancer Performance	
Object Name	Object Description
Allocated Snat Ports	Total number of SNAT ports allocated within time period.
Byte Count	Total number of Bytes transmitted within time period.
Data Path Availability	Average Load Balancer data path availability per time duration.
Health Probe Status	Average Load Balancer health probe status per time duration.
Packet Count	Total number of Packets transmitted within time period.
SNAT Connection Count	Total number of new SNAT connections created within time period.
SYN Count	Total number of SYN Packets transmitted within time period.
Used Snat Ports	Total number of SNAT ports used within time period.

Azure Logic App Service

Microsoft: Azure Logic App Configuration	
Object Name	Object Description
$Schema	The location for the JSON schema file that describes the Workflow Definition Language version.
Access Endpoint	The Access Endpoint.
Action Name	The Action Name.
Azure Logic App / Resource Group	Resource id of the Resource Group.
Changed Time	The changed time.
Content Version	The content version.
Created Time	The created time.
Id	Microsoft resource identifier. Specifies the identifying URL of the resource.
Location	The resource location.
Name	The resource name.
Name	Resource Group name.
Output Name	The output name.
Parameter Name	Parameter name.
Provisioning State	The Provisioning State of the Logic App.
State	The state.
Tag Key	Tags Key.
Tag Value	Tags value.
Trigger Name	Trigger name.
Type	The type.
Version	The version.

Microsoft: Azure Logic App Performance	
Object Name	Object Description
Action Latency	Latency of completed workflow actions.
Action Success Latency	Latency of succeeded workflow actions.
Action Throttled Events	Number of workflow action throttled events.
Actions Completed	Number of workflow actions completed.
Actions Failed	Number of workflow actions failed.
Actions Skipped	Number of workflow actions skipped.

Microsoft: Azure Logic App Performance	
Object Name	Object Description
Actions Started	Number of workflow actions started.
Actions Succeeded	Number of workflow actions succeeded.
Billable Action Executions	Number of workflow action executions getting billed.
Billable Trigger Executions	Number of workflow trigger executions getting billed.
Billing Usage Native Operation Executions	Number of native operation executions getting billed.
Billing Usage Standard Connector Executions	Number of standard connector executions getting billed.
Billing Usage Storage Consumption Executions	Number of storage consumption executions getting billed.
Run Failure Percentage	Percentage of workflow runs failed.
Run Latency	Latency of completed workflow runs.
Run Start Throttled Events	Number of workflow run start throttled events.
Run Success Latency	Latency of succeeded workflow runs.
Run Throttled Events	Number of workflow action or trigger throttled events.
Runs Cancelled	Number of workflow runs canceled.
Runs Completed	Number of workflow runs completed.
Runs Failed	Number of workflow runs failed.
Runs Started	Number of workflow runs started.
Runs Succeeded	Number of workflow runs succeeded.
Total Billable Executions	Number of workflow executions getting billed.
Trigger Fire Latency	Latency of fired workflow triggers.
Trigger Latency	Latency of completed workflow triggers.
Trigger Success Latency	Latency of succeeded workflow triggers.
Trigger Throttled Events	Number of workflow trigger throttled events.
Triggers Completed	Number of workflow triggers completed.
Triggers Failed	Number of workflow triggers failed.
Triggers Fired	Number of workflow triggers fired.
Triggers Skipped	Number of workflow triggers skipped.
Triggers Started	Number of workflow triggers started.
Triggers Succeeded	Number of workflow triggers succeeded.

Azure Managed Disks Service

Microsoft: Azure Managed Disks Configuration	
Object Name	Object Description
Azure Virtual Machine Name	Virtual Machine name.
Resource Group Name	Resource Group Name.
Azure Managed Disk/Resource Group	Resource Group identifier.
Azure Managed Disk/Virtual Machine	Virtual Machine identifier.
Create Option	This enumerates the possible sources of a disk's creation.
Disk Size GB	The disk size.
Disk State	The disk state.
Image Reference	Image reference name.
Name	Name of the managed disk.
Name	The sku name.
Name	Key of the tag.
OS Type	OS Type.
Repository Site Name	Name of the repository site.
Tier	The sku tier.
Time Created	The time when the disk was created.
Value	Value of the tag.

Azure Network Security Group Service

Microsoft: Azure Network Security Group Configuration	
Object Name	Object Description
Azure Resource Group Name	The Resource Group Name.
Access	The access policy of the default inbound security rule associated with the Azure network security group.
Access	The access policy of the outbound default security rule associated with the Azure network security group.
Access	The access policy of the inbound security rule associated with the Azure network security group.
Access	The access policy of the outbound security rule

Microsoft: Azure Network Security Group Configuration	
Object Name	Object Description
	associated with the Azure network security group.
Azure Network Security Group/Resource Group	Relationship between Azure Network Security Group and Resource Group.
Description	The description of the outbound default security rule associated with the Azure network security group.
Description	The description of the inbound default security rule associated with the Azure network security group.
Description	The description of the inbound security rule associated with the Azure network security group.
Description	The description of the outbound security rule associated with the Azure network security group.
Destination Address Prefix	The destination address prefix of the inbound default security rule associated with the Azure network security group. The destination filter can be Any, an IP address range, or a default tag. It specifies the outgoing traffic from a specified destination IP address range that will be allowed or denied by this rule.
Destination Address Prefix	The destination address prefix of the outbound default security rule associated with the Azure network security group. The destination filter can be Any, an IP address range, or a default tag. It specifies the outgoing traffic from a specified destination IP address range that will be allowed or denied by this rule.
Destination Address Prefix	The destination address prefix of the inbound security rule associated with the Azure network security group. The destination filter can be Any, an IP address range, or a default tag. It specifies the outgoing traffic from a specified destination IP address range that will be allowed or denied by this rule.
Destination Address Prefix	The destination address prefix of the outbound security rule associated with the Azure network security group. The destination filter can be Any, an IP address range, or a default tag. It specifies the outgoing traffic from a specified destination IP address range that will be allowed or denied by this rule.
Destination Port Range	The destination port range of the inbound default security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or

Microsoft: Azure Network Security Group Configuration	
Object Name	Object Description
	denied.
Destination Port Range	The destination port range of the outbound default security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Destination Port Range	The destination port range of the inbound security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Destination Port Range	The destination port range of the outbound security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Direction	The direction of the inbound default security rule associated with the Azure network security group.
Direction	The direction of the outbound default security rule associated with the Azure network security group.
Direction	The direction of the inbound security rule associated with the Azure network security group.
Direction	The direction of the outbound security rule associated with the Azure network security group.
Name	The name of the inbound default security rule associated with the Azure network security group.
Name	The name of the outbound default security rule associated with the Azure network security group.
Name	The name of the Azure network security group.
Name	The name of the inbound security rule associated with the Azure network security group.
Name	The name of the outbound security rule associated with the Azure network security group.
Priority	The priority of the inbound default security rule associated with the Azure network security group. Rules are processed in priority order; the lower the number, the higher the priority. It is recommended to add gaps between rules - 100, 200, 300 etc.
Priority	The priority of the inbound security rule associated

Microsoft: Azure Network Security Group Configuration	
Object Name	Object Description
	with the Azure network security group. Rules are processed in priority order; the lower the number, the higher the priority. It is recommended to add gaps between rules - 100, 200, 300 etc.
Priority	The priority of the outbound security rule associated with the Azure network security group. Rules are processed in priority order; the lower the number, the higher the priority. It is recommended to add gaps between rules - 100, 200, 300 etc.
Priority	The priority of the outbound default security rule associated with the Azure network security group. Rules are processed in priority order; the lower the number, the higher the priority. It is recommended to add gaps between rules - 100, 200, 300 etc.
Protocol	The protocol of the inbound security rule associated with the Azure network security group.
Protocol	The protocol of the outbound default security rule associated with the Azure network security group.
Protocol	The protocol of the outbound security rule associated with the Azure network security group.
Protocol	The protocol of the inbound default security rule associated with the Azure network security group.
Provisioning State	The state of the inbound security rule associated with the Azure network security group.
Provisioning State	The state of the outbound default security rule associated with the Azure network security group.
Provisioning State	The state of the Azure network security group.
Provisioning State	The state of the outbound security rule associated with the Azure network security group.
Provisioning State	The state of the inbound default security rule associated with the Azure network security group.
Source Address Prefix	The source address prefix of the inbound security rule associated with the Azure network security group. The source filter can be Any, an IP address range, or a default tag. It specifies the incoming traffic from a specified source IP address range that will be allowed or denied by this rule.
Source Address Prefix	The source address prefix of the inbound default security rule associated with the Azure network security group. The source filter can be Any, an IP address range, or a default tag. It specifies the incoming traffic from a specified source IP address range that will be allowed or denied by this rule.

Microsoft: Azure Network Security Group Configuration	
Object Name	Object Description
Source Address Prefix	The source address prefix of the outbound default security rule associated with the Azure network security group. The source filter can be Any, an IP address range, or a default tag. It specifies the incoming traffic from a specified source IP address range that will be allowed or denied by this rule.
Source Address Prefix	The source address prefix of the outbound security rule associated with the Azure network security group. The source filter can be Any, an IP address range, or a default tag. It specifies the incoming traffic from a specified source IP address range that will be allowed or denied by this rule.
Source Port Range	The source port range of the outbound security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Source Port Range	The source port range of the inbound default security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Source Port Range	The source port range of the outbound default security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Source Port Range	The source port range of the inbound security rule associated with the Azure network security group. A single port, such as 80, or a port range, such as 1024-65535, can be specified. This specifies the ports at which traffic will be allowed or denied.
Tag Key	An Azure network security group tag key.
Tag Value	An Azure network security group tag value.

Azure OpenAI Service

Microsoft: Azure OpenAI Configuration	
Object Name	Object Description
Created At	The timestamp when the resource was created.
Created By	The identity that created the resource.
Created By Type	The type of creator.
Custom Sub Domain Name	The custom subdomain name used in the endpoint URL. Must be globally unique across Azure.
Date Created	When the account was provisioned.
Default Action	Default behavior when no rule matches.
Endpoint	The REST API endpoint URL for the OpenAI instance.
Etag	Entity tag used for optimistic concurrency control. Changes when the resource is modified.
Id	The fully qualified Azure resource ID for the account.
Internal Id	An internal Azure-generated GUID identifier for the account, separate from the ARM resource ID.
Is Migrated	Whether this account was migrated from an older Cognitive Services resource format.
Kind	The type of Cognitive Service.
Last Modified At	The timestamp of the last modification.
Last Modified By	The identity that last modified the resource.
Last Modified By Type	The type of last modifier.
Location	The Azure region where the account is deployed.
Name	The name of the Cognitive Services account resource.
Name	The SKU name.
Name	The capability identifier.
Provisioning State	The current provisioning state of the resource.
Public Network Access	Controls whether the resource can be accessed from the public internet.
Type	The resource type.
Value	The capability value.

Microsoft: Azure OpenAI Performance	
Object Name	Object Description
Active Tokens	Total tokens minus cached tokens over a period of time. Applies to PTU and PTU-managed deployments. Use this metric to understand your TPS or TPM based utilization for PTUs and compare to your benchmarks for target TPS or TPM for your scenarios.
Availability Rate	Availability percentage with the following calculation: (Total Calls - Server Errors)/Total Calls. Server Errors include any HTTP responses >=500.
Blocked Volume	Calls being rejected by content filters. Unexpected spikes could indicate misuse or overly aggressive filter configuration.
Generated Completion Tokens	Number of tokens generated (output) from an OpenAI model. Applies to PTU, PTU-managed and Pay-as-you-go deployments. To break down this metric, you can add a filter or apply splitting by the following dimensions: ModelDeploymentName and ModelName.
Harmful Volume	Calls flagged as harmful. Important for compliance and abuse monitoring.
Managed Utilization	Utilization % for a provisioned-managed deployment, calculated as (PTUs consumed / PTUs deployed) x 100. When utilization is greater than or equal to 100%, calls are throttled and error code 429 returned.
Processed Inference Tokens	Number of inference tokens processed on an OpenAI model. Calculated as prompt tokens (input) plus generated tokens (output). Applies to PTU, PTU-managed and Pay-as-you-go deployments. To break down this metric, you can add a filter or apply splitting by the following dimensions: ModelDeploymentName and ModelName.
Processed Prompt Tokens	Tokens consumed as input.
Requests	Number of calls made to the Azure OpenAI API over a period of time. Applies to PTU, PTU-Managed and Pay-as-you-go deployments. To break down API requests, you can add a filter or apply splitting by the following dimensions: ModelDeploymentName, ModelName, ModelVersion, StatusCode (successful, client errors, server errors), StreamType (Streaming vs non-streaming requests) and operation.
Time Between Token	For streaming requests; model token generation rate, measured in milliseconds. Applies to PTU and

Microsoft: Azure OpenAI Performance	
Object Name	Object Description
	PTU-managed deployments.
Time to 1st Byte	For streaming and non-streaming requests; time it takes for first byte of response data to be received after request is made by model, normalized by token.
Time to Last Byte	For streaming and non-streaming requests; time it takes for last byte of response data to be received after request is made by model. Applies to PTU, PTU-managed, and Pay-as-you-go deployments.
Time To Response	Recommended latency (responsiveness) measure for streaming requests. Applies to PTU and PTU-managed deployments. Calculated as time taken for the first response to appear after a user sends a prompt, as measured by the API gateway. This number increases as the prompt size increases and/or cache hit size reduces. To break down time to response metric, you can add a filter or apply splitting by the following dimensions: ModelDeploymentName, ModelName, and ModelVersion. This metric is an approximation, as measured latency is heavily dependent on multiple factors, including concurrent calls and overall workload pattern. In addition, it does not account for any client-side latency that may exist between your client and the API endpoint. Refer to your own logging for optimal latency tracking.
Token Cache Match Rate	Percentage of prompt tokens that hit the cache. Applies to PTU and PTU-managed deployments
Tokens Per Second	Enumerates the generation speed for a given Azure OpenAI model response. The total tokens generated is divided by the time to generate the tokens, in seconds. Applies to PTU and PTU-managed deployments.

Azure Recovery Service Vault

Microsoft: Azure Recovery Services Vault Configuration	
Object Name	Object Description
Resource Group Name	The name of the resource group.
Azure Recovery Vault/Resource Group	The relationship identifier with resource group.

Microsoft: Azure Recovery Services Vault Configuration	
Object Name	Object Description
Location	The recovery vault location.
Sku Name	The sku is a unique identifier of the resource. Possible values RS0
Sku Type	The sku is a unique identifier of the resource. Possible values Standard.
Tag Key	The key of the tag.
Tag Value	The value of the tag.
Vault Name	The name of the recovery vault.
Vault Provisioning State	The provision state of the vault.

Azure Resource Group Service

Microsoft: Azure Resource Group Configuration	
Object Name	Object Description
Resource Name	The name of the resource.
Resource Type	The type of the resource.
Id	Id of the resource group.
Resource Location	The location of the resource.
Tag Key	The key of tag pair.
Tag Value	The value of tag pair.
Type	The Type of the resource group.

Azure Resource List Services

Microsoft: Azure Resource List Configuration	
Object Name	Object Description
Availability State	Availability status of the resource. When it is null, this object represents an availability impacting event.
Azure Resource/Resource Group	Resource group unique identifier that this resource belongs to.
Capacity	The SKU capacity.
Detailed Status	Details of the availability status.

Microsoft: Azure Resource List Configuration	
Object Name	Object Description
Family	The SKU family.
ID	Resource unique identifier.
Last Update	Timestamp for when last change in health status occurred.
Model	The SKU model.
Name	Resource tag key.
Name	Resource group name that this resource belongs to.
Name	The name of SKU.
Reason Chronicity	Chronicity of the availability transition.
Reason Type	When the resource's availabilityState is Unavailable, it describes where the health impacting event was originated. Examples are planned, unplanned, user initiated or an outage etc.
Resource Name	Resource name.
Size	The SKU size.
Summary	Summary description of the availability status.
Tier	The tier of SKU.
Type	Resource service type.
Value	Resource tag value.

Azure Service Bus (Relay)

Microsoft: Azure Service Bus Configuration	
Object Name	Object Description
IP Mask	IP Mask.
Name	Name of this SKU.
Name	The name of the resource associated with the resource group.
Name	Network Resource Name.
Name	Virtual Network resource name.
Namespace Alias Name	The namespace alias name.
Role	role of namespace in GEO DR - possible values Primary or PrimaryNotReplicating or Secondary
Tier	The billing tier of this particular SKU.
Virtual Network Subnets Relationship	Virtual Network Subnets Relationship Group

Microsoft: Azure Service Bus Configuration	
Object Name	Object Description
Action	The IP Filter Action
Azure Service Bus Namespace/ Service Bus Namespace	ARM Id of the Primary/Secondary eventhub namespace name, which is part of GEO DR pairing.
Azure Service Bus Namespace/Resource Group	The resource Id associated with the resource group.
Azure Service Bus Namespace/Subnet	Resource ID of Virtual Network Subnet.
Azure Service Bus Namespace/Virtual Network	Resource ID of Virtual Network.
Capacity	The specified messaging units for the tier. For Premium tier, capacity are 1,2 and 4.
Created At	The time the namespace was created.
Endpoint	Endpoint you can use to perform Service Bus operations.
Ignore Missing	Value that indicates whether to ignore missing VNet Service Endpoint
Location	The Geo-location where the resource lives.
Metric Id	Identifier for Azure Insights metrics.
Name	Azure Service Bus Resource name
Network Default Action	Default Action for Network Rule Set
Provisioning State	Provisioning state of the namespace.
Resource Group Relationships	Resource Group Relationship
Service Bus Namespace Relationship	Service Bus Namespace Relationship
SKU	SKU
Status	Status of the Namespace.
Tag Key	Tags key.
Tag Value	Tags values.
Tags	Tags
Virtual Network Relationships	Virtual Network Relationships

Microsoft: Azure Service Bus Performance	
Object Name	Object Description
Active Connections	Total Active Connections for Microsoft.ServiceBus.
Active Messages	Count of active messages in a Queue/Topic.
Active Messages	Count of active messages in a Queue/Topic.
Connections Closed	Connections Closed for Microsoft.ServiceBus.
Connections Closed	Connections Closed for Microsoft.ServiceBus.
Connections Opened	Connections Opened for Microsoft.ServiceBus.
Connections Opened	Connections Opened for Microsoft.ServiceBus.

Microsoft: Azure Service Bus Performance	
Object Name	Object Description
Deadlettered Messages	Count of dead-lettered messages in a Queue/Topic.
Deadlettered Messages	Count of dead-lettered messages in a Queue/Topic.
Incoming Messages	Incoming Messages for Microsoft.ServiceBus.
Incoming Messages	Incoming Messages for Microsoft.ServiceBus.
Incoming Requests	Incoming Requests for Microsoft.ServiceBus.
Incoming Requests	Incoming Requests for Microsoft.ServiceBus.
Messages	Count of messages in a Queue/Topic.
Messages	Count of messages in a Queue/Topic.
Namespace CPU Usage	Service bus premium namespace CPU usage metric.
Namespace Memory Usage	Service bus premium namespace memory usage metric.
Outgoing Messages	Outgoing Messages for Microsoft.ServiceBus.
Outgoing Messages	Outgoing Messages for Microsoft.ServiceBus.
Scheduled Messages	Count of scheduled messages in a Queue/Topic.
Scheduled Messages	Count of scheduled messages in a Queue/Topic.
Server Errors	Server Errors for Microsoft.ServiceBus.
Server Errors	Server Errors for Microsoft.ServiceBus.
Size	Size of an Queue/Topic in Bytes.
Size	Size of an Queue/Topic in Bytes.
Successful Requests	Total successful requests for a namespace
Successful Requests	Total successful requests for a namespace
Throttled Requests	Throttled Requests for Microsoft.ServiceBus.
Throttled Requests	Throttled Requests for Microsoft.ServiceBus.
User Errors	User Errors for Microsoft.ServiceBus.
User Errors	User Errors for Microsoft.ServiceBus.

Microsoft: Azure Service Bus Queues Configuration	
Object Name	Object Description
Name	Resource name
Status	Enumerates the possible values for the status of a messaging entity.
Current Size (MB)	The size of the queue, in megabytes.
Max Size (MB)	The maximum size of the queue in megabytes, which is the size of memory allocated for the queue.
Dead Letter	A value that indicates whether this queue has dead

Microsoft: Azure Service Bus Queues Configuration	
Object Name	Object Description
	letter support when a message expires.
Enable Express	A value that indicates whether Express Entities are enabled. An express queue holds a message in memory temporarily before writing it to persistent storage.
Enable Partitioning	A value that indicates whether the queue is to be partitioned across multiple message brokers.
Max Delivery	The maximum delivery count.
Requires Session	A value that indicates whether the queue supports the concept of sessions.
Created Time	The exact time the message was created.

Microsoft: Azure Service Bus Topics Configuration	
Object Name	Object Description
Name	Resource Topic name.
Status	Enumerates the possible values for the status of a messaging entity.
Subscription Count	Number of subscriptions.
Current Size (B)	Size of the topic, in bytes.
Max Size (MB)	Maximum size of the topic in megabytes, which is the size of the memory allocated for the topic. Default is 1024.
Enable Express	Value that indicates whether Express Entities are enabled. An express topic holds a message in memory temporarily before writing it to persistent storage.
Enable Partitioning	Value that indicates whether the topic to be partitioned across multiple message brokers is enabled.
Created Time	Exact time the message was created.

Azure Site Recovery

Microsoft: Azure Site Recovery Plans Configuration	
Object Name	Object Description
Name	The name of the Site Recovery plan.
Primary Fabric Name	The primary fabric name.

Microsoft: Azure Site Recovery Plans Configuration	
Object Name	Object Description
Recovery Fabric Name	The recovery fabric name.
Allowed Operations	The list of allowed operations.
Failover Deployment Model	The failover deployment model.
Number of Site Recovery Plans	The number of Site Recovery plans.
Replication Providers	The list of replication providers.
Type	The type of the Site Recovery plan.

Microsoft: Azure Site Recovery Policy Configuration	
Object Name	Object Description
Name	The name of the Site Recovery policy.
Instance Type	Gets the class type. Overridden in derived classes.
App Consistent Frequency	The app consistent snapshot frequency in minutes.
Crash Consistent Frequency	The crash consistent snapshot frequency in minutes.
Multi VM Sync Status	A value indicating whether multi-VM sync has to be enabled.
Number of Site Recovery Policies	Number of policies.
Recovery Point	The duration in minutes until which the recovery points need to be stored.
Recovery Point Threshold	The recovery point threshold in minutes.
Type	The type of the Site Recovery policy.

Microsoft: Azure Site Recovery Protected Items Configuration	
Object Name	Object Description
Item Name	The name associated with the resource.
Site Recovery Policy Name	Site Recovery Policy Name.
Primary Fabric Name	The friendly name of the primary fabric.
Recovery Fabric Name	The friendly name of recovery fabric.
Active Location	The Current active location of the PE.
Failover Health	The consolidated failover health for the VM.
Number of Site Recovery Protected Items	Number of protected items.
Protected Item ID	Protected Item ID.
Protected Item Type	Protected Item Type.
Protection State	Protection State.
Replication Health	The consolidated protection health for the VM taking any issues with SRS as well as all the replication

Microsoft: Azure Site Recovery Protected Items Configuration	
Object Name	Object Description
	units associated with the VM's replication group into account.
Site Recovery Protected Items	All the site recovery protected items.
Test Failover State	The Test failover state.

Azure SQL Managed Instance Service

Microsoft: Azure SQL Managed Instance Configuration	
Object Name	Object Description
Administrator Login	Administrator Login
Azure SQL Managed Instance / Resource Group	Resource id of the Resource Group.
Azure SQL Managed Instance / Virtual Network	The Virtual Network resource id.
Azure SQL Managed Instance / Virtual Network Subnet	The full resource ID of a subnet in a virtual network that this resource belongs to.
Capacity	An ARM Resource Capacity of the particular SKU.
Collation	Collation of the managed instance.
Current Backup Storage Redundancy	The storage account type used to store backups for this instance. The options are Local (LocallyRedundantStorage), Zone (ZoneRedundantStorage), Geo (GeoRedundantStorage) and GeoZone (GeoZoneRedundantStorage).
Dns Zone	The Dns Zone that the managed instance is in.
Family	If the service has different generations of hardware, for the same SKU, then that can be captured here.
Fully Qualified Domain Name	The fully qualified domain name of the managed instance.
License Type	The license type. Possible values are 'LicenseIncluded' (regular price inclusive of a new SQL license) and 'BasePrice' (discounted AHB price for bringing your own SQL licenses).
Location	Resource location.
Minimal Tls Version	Minimal TLS version. Allowed values: 'None', '1.0', '1.1', '1.2'.
Name	The name of the SKU, typically, a letter + Number code, e.g. P3.
Name	Resource name.

Microsoft: Azure SQL Managed Instance Configuration	
Object Name	Object Description
Name	Resource Group Name.
Name	Subnet resource name.
Name	The Virtual Network resource name.
Provisioning State	The resource provisioning state.
Proxy Override	Connection type used for connecting to the instance.
Public Data Endpoint Enabled	Whether or not the public data endpoint is enabled.
Requested Backup Storage Redundancy	The storage account type to be used to store backups for this instance. The options are Local (LocallyRedundantStorage), Zone (ZoneRedundantStorage), Geo (GeoRedundantStorage) and GeoZone (GeoZoneRedundantStorage).
State	The state of the managed instance.
Storage Size In Gb	Storage size in GB. Minimum value: 32. Maximum value: 8192. Increments of 32 GB allowed only.
Subnet Id	Subnet resource ID for the managed instance.
Tag Key	Tags Key.
Tag Value	Tags Value.
Tags	Tags
Tier	The tier or edition of the particular SKU, e.g. Basic, Premium.
Timezone Id	Id of the timezone. Allowed values are timezones supported by Windows.
Type	The identity type. Set this to 'SystemAssigned' in order to automatically create and assign an Azure Active Directory principal for the resource.
V Cores	The number of vCores. Allowed values: 8, 16, 24, 32, 40, 64, 80.
Virtual Network Relationships	Virtual Network Relationships
Virtual Network Subnet Relationships	Virtual Network Subnet Relationships
Zone Redundant	Whether or not the multi-az is enabled.

Microsoft: Azure SQL Managed Instance Database Configuration	
Object Name	Object Description
Collation	Collation of the managed database.
Creation Date	Creation date of the database.
Default Secondary Location	Geo paired region.

Microsoft: Azure SQL Managed Instance Database Configuration	
Object Name	Object Description
Earliest Restore Point	Earliest restore point in time for point in time restore.
Location	Resource location.
Name	Resource name.
Status	Status of the database.

Microsoft: Azure SQL Managed Instance Failover Configuration	
Object Name	Object Description
Group Name	Resource name.
Instance Replication Role	Local replication role of the failover group instance: Primary, Secondary
Replication State	Replication state of the failover group instance.
Id	Resource ID.

Microsoft: Azure SQL Managed Instance Performance	
Object Name	Object Description
Average CPU Percentage	Average CPU percentage.
IO Bytes Read	IO bytes read.
IO Bytes Written	IO bytes written.
IO Requests Count	IO requests count.
Storage Space Reserved	Storage space reserved.
Storage Space Used	Storage space used.
Virtual Core Count	Virtual core count.

Azure SQL Servers Service

Microsoft: Azure SQL Database Configuration	
Object Name	Object Description
Name	The name of the SKU, typically, a letter + Number code, e.g. P3.
Azure Resource Group Name	The Resource Group Name.
Azure SQL Database/Resource Group	Azure Resource Group ID associated with Azure SQL Database.
Collation	Specifies the name of the SQL database collation.
Creation Date	Specifies the date and time that the database was created.

Microsoft: Azure SQL Database Configuration	
Object Name	Object Description
Database ID	Specifies the identifier of the database.
Database Name	The name of the SQL database.
Default Secondary Location	Specifies the default location of the secondary Azure server.
Earliest Restore Date	Specifies the date and time that the database was restored.
Edition	Specifies the edition of the database.
Family	If the service has different generations of hardware, for the same SKU, then that can be captured here.
Kind	Specifies the SQL Server version and the database type.
Location	The location of the SQL database component.
Maximum Size (GB)	Specifies the maximum size to which the database may grow.
Server Version	Displays the version of SQL Server.
Service Level Objective	Specifies the performance level of the database.
Status	The status of the SQL database component.
Subscription ID	The subscription identifier value.
Tag	Tags are key/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.
Tag Key	Key of the tag pair.
Tag Value	Value of the tag pair.
Tier	The tier or edition of the particular SKU, e.g. Basic, Premium.

Microsoft: Azure SQL Database Performance	
Object Name	Object Description
Blocked by Firewall	Specifies the count of connection attempts blocked by the firewall.
CPU Percentage	Specifies the average CPU utilization.
Data IO Percentage	Specifies the average IO utilization.
Database Size Percentage	Specifies the percent of the maximum size for the database.
Deadlock	Specifies the count of deadlocks.
DTU Limit	Specifies the current DTU limit for the database.

Microsoft: Azure SQL Database Performance	
Object Name	Object Description
DTU Percentage	Specifies the average DTU utilization.
DTU Used	Specifies the average DTU utilization.
Failed Connections	Specifies the count of failed connections.
In-Memory OLTP Storage Percent	Specifies the percent of In-Memory OLTP storage.
Log IO Percentage	Specifies the average log utilization.
Sessions Percentage	Specifies the percent of maximum concurrent active sessions.
Successful Connections	Specifies the count of successful connections.
Total Database Size	Specifies the total size of the database.
Workers Percentage	Specifies the percent of maximum concurrent active workers (requests).

Microsoft: Azure SQL Server Configuration	
Object Name	Object Description
Azure Resource Group Name	The Resource Group Name.
Azure SQL Server/Resource Group	Resource Group Id.
FQDN	Azure SQL Server Fully Qualified Domain Name.
ID	Azure SQL Server ID.
Location	Azure SQL Server location.
Name	Azure SQL Server Name.
State	Azure SQL Server state.
Tag Key	Tag Key.
Tag Value	Tag Value.
Type	Azure SQL Server type.
Version	Azure SQL Server version.

Azure Storage Service

Microsoft: Azure Storage Account Blob Performance	
Object Name	Object Description
Average Availability	The percentage of availability for the storage service or the specified API operation. Availability is calculated by taking the TotalBillableRequests value and dividing it by the number of applicable requests, including those that produced unexpected errors. All

Microsoft: Azure Storage Account Blob Performance	
Object Name	Object Description
	unexpected errors result in reduced availability for the storage service or the specified API operation.
Average E2E Latency	The average end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.
Average Server Latency	The average latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in AverageE2ELatency.
Index Capacity	The amount of storage used by ADLS Gen2 (Hierarchical) Index in bytes.
Total Blob Capacity	The amount of storage used by the storage account's Blob service, in bytes.
Total Blob Container	The number of blob containers in the storage account's Blob service.
Total Blob Count	The number of committed and uncommitted blobs in the storage account's Blob service.
Total Egress	The amount of egress data, in bytes. This number includes egress from an external client into Azure Storage as well as egress within Azure. As a result, this number does not reflect billable egress.
Total Ingress	The amount of ingress data, in bytes. This number includes ingress from an external client into Azure Storage as well as ingress within Azure.
Total Transactions	The number of requests made to a storage service or the specified API operation. This number includes successful and failed requests, as well as requests which produced errors.

Microsoft: Azure Storage Account Configuration	
Object Name	Object Description
Azure Virtual Network Name	The Virtual Network Name.
Name	Virtual Network name.
Value	An Azure storage account tag value.
Action	IP rule action.
Action	Virtual network rule action.
Azure Resource Group Name	The Resource Group Name.

Microsoft: Azure Storage Account Configuration	
Object Name	Object Description
Azure Storage Account/Resource Group	Azure Resource Group ID associated with Azure storage account.
Azure Storage Account/Virtual Network	Azure Virtual Network ID associated with Azure Storage Account.
Creation Time	Gets the creation date and time of the storage account in UTC.
Key	An Azure storage account tag key.
Kind	Indicates the type of storage account.
Location	Resource location
Name	Resource name.
Name	Gets the sku name.
Name	The primary endpoint name
Name	The secondary endpoint name
Primary Location	Gets the location of the primary data center for the storage account.
Primary Status	Gets the status indicating whether the primary location of the storage account is available or unavailable.
Provisioning State	Gets the status of the storage account at the time the operation was called.
Secondary Location	Gets the location of the geo-replicated secondary for the storage account. Only available if the accountType is Standard_GRS or Standard_ RAGRS.
Secondary Status	Gets the status indicating whether the secondary location of the storage account is available or unavailable. Only available if the SKU name is Standard_GRS or Standard_RAGRS.
State	Gets the state of virtual network rule.
Tier	Gets the sku tier. This is based on the SKU name.
Value	The primary endpoint value
Value	The secondary endpoint value
Value	IP rule value.

Microsoft: Azure Storage Account File Performance	
Object Name	Object Description
Average Availability	The percentage of availability for the storage service or the specified API operation. Availability is calculated by taking the TotalBillableRequests value

Microsoft: Azure Storage Account File Performance	
Object Name	Object Description
	and dividing it by the number of applicable requests, including those that produced unexpected errors. All unexpected errors result in reduced availability for the storage service or the specified API operation.
Average E2E Latency	The average end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.
Average File Capacity	The amount of storage used by the storage account's File service in bytes.
Average File Count	The number of file in the storage account's File service.
Average File Share Count	The number of file shares in the storage account's File service.
Average Server Latency	The average latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in AverageE2ELatency.
File Share Capacity Quota	The upper limit on the amount of storage that can be used by Azure Files Service in bytes.
File Share Snapshot Count	The number of snapshots present on the share in storage account's Files Service.
File Share Snapshot Size	The amount of storage used by the snapshots in storage account's File service in bytes.
Total Egress	The amount of egress data, in bytes. This number includes egress from an external client into Azure Storage as well as egress within Azure. As a result, this number does not reflect billable egress.
Total Ingress	The amount of ingress data, in bytes. This number includes ingress from an external client into Azure Storage as well as ingress within Azure.
Total Transactions	The number of requests made to a storage service or the specified API operation. This number includes successful and failed requests, as well as requests which produced errors. Use ResponseType dimension for the number of different type of response.

Microsoft: Azure Storage Account Performance	
Object Name	Object Description
Average Availability	The percentage of availability for the storage service or the specified API operation. Availability is calculated by taking the total billable requests value and dividing it by the number of applicable requests, including those requests that produced unexpected errors. All unexpected errors result in reduced availability for the storage service or the specified API operation.
Average E2E Latency	The average end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.
Average Server Latency	The average latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in AverageE2ELatency.
Total Egress	The amount of egress data, in bytes. This number includes egress from an external client into Azure Storage as well as egress within Azure. As a result, this number does not reflect billable egress.
Total Ingress	The amount of ingress data, in bytes. This number includes ingress from an external client into Azure Storage as well as ingress within Azure.
Total Transactions	The number of requests made to a storage service or the specified API operation. This number includes successful and failed requests, as well as requests which produced errors.
Total Used Capacity	The amount of storage used by the storage account. For standard storage accounts, it's the sum of capacity used by blob, table, file, and queue. For premium storage accounts and Blob storage accounts, it is the same as BlobCapacity.

Microsoft: Azure Storage Account Queue Performance	
Object Name	Object Description
Average Availability	The percentage of availability for the storage service or the specified API operation. Availability is calculated by taking the TotalBillableRequests value and dividing it by the number of applicable requests, including those that produced unexpected errors. All unexpected errors result in reduced availability for the storage service or the specified API operation.

Microsoft: Azure Storage Account Queue Performance	
Object Name	Object Description
Average E2E Latency	The average end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.
Average Server Latency	The average latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in AverageE2ELatency.
Total Egress	The amount of egress data, in bytes. This number includes egress from an external client into Azure Storage as well as egress within Azure. As a result, this number does not reflect billable egress.
Total Ingress	The amount of ingress data, in bytes. This number includes ingress from an external client into Azure Storage as well as ingress within Azure.
Total Queue Capacity	The amount of storage used by the storage account's Queue service, in bytes.
Total Queue Count	The number of queues in the storage account's Queue service.
Total Queue Message Count	The number of message queues in the storage account's Queue service.
Total Transactions	The number of requests made to a storage service or the specified API operation. This number includes successful and failed requests, as well as requests which produced errors.

Microsoft: Azure Storage Account Table Performance	
Object Name	Object Description
Average Availability	The percentage of availability for the storage service or the specified API operation. Availability is calculated by taking the TotalBillableRequests value and dividing it by the number of applicable requests, including those that produced unexpected errors. All unexpected errors result in reduced availability for the storage service or the specified API operation.
Average E2E Latency	The average end-to-end latency of successful requests made to a storage service or the specified API operation, in milliseconds. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.

Microsoft: Azure Storage Account Table Performance	
Object Name	Object Description
Average Server Latency	The average latency used by Azure Storage to process a successful request, in milliseconds. This value does not include the network latency specified in AverageE2ELatency.
Total Egress	The amount of egress data, in bytes. This number includes egress from an external client into Azure Storage as well as egress within Azure. As a result, this number does not reflect billable egress.
Total Ingress	The amount of ingress data, in bytes. This number includes ingress from an external client into Azure Storage as well as ingress within Azure.
Total Table Capacity	The amount of storage used by the storage account's Table service, in bytes.
Total Table Count	The number of tables in the storage account's Table service.
Total Table Entity Count	The number of entity tables in the storage account's Table service.
Total Transactions	The number of requests made to a storage service or the specified API operation. This number includes successful and failed requests, as well as requests which produced errors.

Azure Traffic Manager Service

Microsoft: Azure Traffic Manager Profile Configuration	
Object Name	Object Description
Azure Resource Group Name	The Resource Group Name.
Azure Traffic Manager Name	The name of the Traffic Manager Profile.
Azure Traffic Manager Profile/Resource Group	Azure Resource Group ID associated with Azure traffic manager profile.
Azure Traffic Manager/Traffic Manager	Specifies the em7 resource ID of the child profile that this endpoint will direct traffic to.
DNS TTL	Specifies the DNS Time-to-Live (TTL), in seconds.
FQDN	The fully-qualified domain name of the Traffic Manager profile. This is a read-only property, formed from the concatenation of the relativeName with the DNS domain used by Azure Traffic Manager.

Microsoft: Azure Traffic Manager Profile Configuration	
Object Name	Object Description
ID	The ID of an Azure traffic manager profile.
ID	Specifies the ARM resource ID of the endpoint. Each endpoint is a child resource of the parent profile resource, hence each endpoint has a unique ARM resource ID.
Key	A tag key for an Azure traffic manager profile.
Location	Specifies the location of the endpoint. This value is used in the 'Performance' traffic-routing method when determining which endpoint is closest to the end user.
Monitor Status	Indicates the overall health status for the Traffic Manager profile.
Monitor Status	Indicates the health status for the endpoint.
Name	The name of an Azure traffic manager profile.
Name	Specifies the name (ARM resource name) of the endpoint.
Priority	Specifies the priority of this endpoint when using the 'Priority' traffic routing method.
Relative Name	Specifies the relative DNS name provided by this Traffic Manager profile.
Routing Method	The traffic routing method of an Azure traffic manager profile.
Status	Specifies whether the profile should be enabled or disabled.
Status	Specifies the status of the endpoint. . If the endpoint is Enabled, it is probed for endpoint health and is included in the traffic routing method.
Target Resource	The fully-qualified DNS name of the endpoint. Traffic Manager returns this value in DNS responses when it directs traffic to this endpoint. Applicable to endpoints of type 'AzureEndpoints' and 'ExternalEndpoints' only.
Type	Specifies the type of the endpoint.
Value	A tag value for an Azure traffic manager profile.
Weight	Specifies the weight assigned by Traffic Manager to the endpoint.

Microsoft: Azure Traffic Manager Profile Performance	
Object Name	Object Description
Endpoint Status by Endpoint	1 if an endpoint probe status is "Enabled", 0

Microsoft: Azure Traffic Manager Profile Performance	
Object Name	Object Description
	otherwise.
Queries by Endpoint Returned	Number of times a Traffic Manager endpoint was returned in the given time frame.

Azure Virtual Desktop Host Pool Service

Microsoft: Azure Host Pool Configuration	
Object Name	Object Description
Agent Version	Version of the Azure Virtual Desktop agent on the session host.
Allow New Session	Whether the session host is accepting new user sessions.
Azure Host Pool/Resource Group	Resource id of the Resource Group.
Azure Host Pool/Virtual Machine	Defines relationship between Azure Host Pool and Azure Virtual Machine using the resource ID of the virtual machine.
Health Check Name	Represents the name of the health check operation performed.
Health Check Result	Represents the Health state of the health check we performed.
Host Pool Type	Host pool type (Personal or Pooled).
ID	Fully qualified resource ID for the resource.
Load Balancer Type	Load balancer type for the host pool (e.g., BreadthFirst, DepthFirst, Persistent).
Max Session Limit	Maximum number of sessions allowed per session host in the host pool. Cached for Host Pool Performance.
Name	Resource Group name.
Session Host Name	The name of the resource.
Status	Status for a SessionHost.
Update State	Update state of the session host agent.
Validation Environment	Whether the host pool is flagged as a validation environment.
VM ID	Virtual Machine Id of SessionHost virtual machine.
VM Name	Virtual Machine Name of SessionHost virtual machine.

Microsoft: Azure Host Pool Performance	
Object Name	Object Description
Drained Host Count	Number of session hosts not accepting new sessions (allowNewSession is false).
Host Count	Number of session hosts in the host pool.
Host Pool Name	Azure Virtual Desktop host pool name.
Host Sessions	Number of sessions on SessionHost.
Max Session Limit	Maximum sessions allowed per host, read from the Host Pool Configuration cache.
Session Host Name	SessionHost name.
Total Sessions	Total number of sessions across all session hosts in the host pool.

Microsoft: Azure Host Pool Scaling Configuration	
Object Name	Object Description
Attachment State	Whether a scaling plan is attached to this host pool and enabled: Attached, Disabled, or NotAttached.
Days of Week	Days of the week the schedule is active.
Exclusion Tag	Exclusion tag configured on the scaling plan.
Friendly Name	Friendly name of the scaling plan.
Host Pool Type	Scaling plan host pool type (Pooled or Personal).
Off Peak Load Balancing	Load balancing algorithm during off-peak.
Off Peak Start Time	Off-peak period start time (HH:MM).
Peak Load Balancing	Load balancing algorithm during peak.
Peak Start Time	Peak period start time (HH:MM).
Ramp Down Capacity Threshold Pct	Capacity threshold percentage during ramp-down.
Ramp Down Force Logoff	Whether users are forcibly logged off during ramp-down.
Ramp Down Load Balancing	Load balancing algorithm during ramp-down.
Ramp Down Minimum Hosts Pct	Minimum percentage of hosts running during ramp-down.
Ramp Down Start Time	Ramp-down period start time (HH:MM).
Ramp Down Stop Hosts When	When to stop hosts during ramp-down (ZeroSessions or ZeroActiveSessions).
Ramp Down Wait Minutes	Minutes to wait before stopping hosts during ramp-down.
Ramp Up Capacity Threshold Pct	Capacity threshold percentage during ramp-up.
Ramp Up Load Balancing	Load balancing algorithm during ramp-up.
Ramp Up Minimum Hosts Pct	Minimum percentage of hosts running during ramp-

Microsoft: Azure Host Pool Scaling Configuration	
Object Name	Object Description
	up.
Ramp Up Start Time	Ramp-up period start time (HH:MM).
Scaling Plan Enabled	scalingPlanEnabled flag on the hostPoolReference for this pool.
Scaling Plan Name	Azure resource name of the governing scaling plan.
Schedule Name	Name of the scaling schedule (row index).
Time Zone	Time zone the scaling plan schedules run in.

Azure Virtual Machines Service

Microsoft: Azure Virtual Machine Configuration	
Object Name	Object Description
Name	The name of a data disk that is aligned with an Azure virtual machine.
Name	The name of SKU.
Family	The Family of this particular SKU.
Name	The virtual machine OS Disk.
Size	The Size of the SKU.
Size (GB)	The size of a data disk that is aligned with an Azure virtual machine.
Tier	Specifies the tier of virtual machines in a scale set.
Enabled	Whether boot diagnostics is enabled on the Virtual Machine.
Type	The type of a data disk that is aligned with an Azure virtual machine.
Type	The operating system disk type of an Azure virtual machine.
Azure Virtual Network Name	The name of the virtual network.
CPU Core Count	Number of vCPUs for this specific machine.
Host	Host name.
Installed Memory (GB)	Installed memory in Gigabytes for this machine.
Max Disk Count	Max quantity of disks for this machine
OS Disk Size (GB)	OS Disk Size in Gigabytes for this machine.
Resource Disk Size (MB)	Max Resource Disk Size in Megabytes.
Storage Account Name	The Storage Account Name associated with the Azure Virtual machine.

Microsoft: Azure Virtual Machine Configuration	
Object Name	Object Description
Storage Account Type	Specifies the storage account type for the managed disk. Possible values are: Standard_LRS | Premium_LRS.
Storage Account Type	Specifies the storage account type for the managed disk. Possible values are: Standard_LRS | Premium_LRS.
Automatic Updates	Indicates whether or not automatic updates are enabled.
Azure Network Security Group Name	The Network Security Group Name.
Azure Resource Group Name	The Resource Group Name.
Azure Subnet Name	The Subnet Name associated with the Azure Virtual machine.
Azure Virtual Machine Identifier Namespace	The namespace used to link the CCC application.
Azure Virtual Machine Name	The name of the Virtual machine.
Azure Virtual Machine/Network Security Group	Azure Network Security Group ID associated with network interface.
Azure Virtual Machine/Resource Group	Azure Resource Group ID associated with Azure virtual machine.
Azure Virtual Machine/Storage Account	Azure Storage Account ID that contains the OS disk of Virtual Machine, and it is associated with Azure virtual machine.
Azure Virtual Machine/Subnet	Azure Subnet ID associated with Azure virtual machine.
Azure Virtual Machine/Virtual Network	Azure Virtual Network ID associated with Azure virtual machine.
Caching	Specifies the caching requirements. Possible values are: None | ReadOnly | ReadWrite.
Caching	Specifies the caching requirements. Possible values are: None | ReadOnly | ReadWrite.
Certificate Url	Specifies the URL of the certificate with which new virtual machines are provisioned.
Code	Specifies the code of disk statuses from virtual machines.
Computer Name	The computer name of an Azure virtual machine.
Config Name	An Azure IP configuration name, utilized by an Azure virtual machine.
Created From	Method in which Azure virtual machine was created.
Deployment Status	The deployment status of an Azure virtual machine
Display Status	Specifies the display status of disks from virtual machines.

Microsoft: Azure Virtual Machine Configuration	
Object Name	Object Description
Dynatrace Host/Azure Virtual Machine	Dynatrace namespace.
Hardware Type	The Azure virtual machine hardware type. This will let Azure know the configuration that is needed by a virtual machine.
ID	Specifies the identifying URL of the virtual machine
Interface MAC Address	Azure network interface MAC Address
Interface Name	Azure network interface name utilized by an Azure virtual machine.
Interface Resource GUID	Azure network interface global unique identifier.
IP Allocation Method	The Private IP Address Allocation Method for an Azure network interface. Expected to be either Dynamic or Static.
IP Version	The Private IP Address version for an Azure network interface. Expected to be either IPv6 or IPv4.
Level	Specifies the level of disk statuses from virtual machines.
Location	The location where an Azure virtual machine resides.
Location	Specifies the supported Azure location where the availability set exists.
Name	The name of an Azure virtual machine.
Name	Specifies the name of the availability set.
Name	Specifies the name of disk from virtual machines.
Network Interface Name	Network interface that belongs to a network security group.
OS SKU	The operating system release SKU of an Azure virtual machine.
OS Type	The operating system type of an Azure virtual machine.
OS Version	The operating system version of an Azure virtual machine.
Platform Fault Domain Count	Specifies the fault domain of the virtual machine.
Platform Update Domain Count	Specifies the update domain of the virtual machine.
Private IP Address	The Private IP Address for an Azure network interface.
Protocol	Specifies the protocol of listener.
Sku	Specifies the sku of the image used to create the virtual machine.

Microsoft: Azure Virtual Machine Configuration	
Object Name	Object Description
SKU	Virtual Machine Subscription Information
Status	The name of an Azure virtual machine status.
Status Level	The priority level of an Azure virtual machine status entry.
Status Message	The message for an Azure virtual machine status entry.
Status Time	The time of occurrence for an Azure virtual machine status entry.
Storage Uri	Uri of the storage account to use for placing the console output and screenshot.
Tag Key	An Azure virtual machine tag key.
Tag Value	An Azure virtual machine tag value.
Time	Specifies the timestamp of last disk statuses from virtual machines.
Type	Specifies the type of compute resource.
URI	The uri of a data disk that is aligned with an Azure virtual machine.
URI	The virtual machine OS disk URI.
VM ID	Specifies the VM unique ID, which is a 128-bits identifier that is encoded and stored in all Azure IaaS VMs SMBIOS and can be read using platform BIOS commands.

Microsoft: Azure Virtual Machine Performance	
Object Name	Object Description
CPU Average	The most recent average CPU counter for an Azure virtual machine.
CPU Credits Consumed	Total number of credits consumed by the Virtual Machine.
CPU Credits Remaining	Total number of credits available to burst.
Disk Read Bytes	Total bytes read from disk during monitoring period.
Disk Read Operations/Second	Total number of read I/O operations per second.
Disk Write Bytes	Total bytes written to disk during monitoring period.
Disk Write Operations/Second	Total number of write I/O operations per second.
Inbound Flows	Inbound Flows are number of current flows in the inbound direction (traffic going into the VM).
Inbound Flows Maximum Creation Rate	The maximum creation rate of inbound flows (traffic going into the VM).

Microsoft: Azure Virtual Machine Performance	
Object Name	Object Description
Network In	The number of bytes received on all network interfaces by the Virtual Machine(s) (Incoming Traffic)
Network Out	The number of bytes out on all network interfaces by the Virtual Machine(s) (Outgoing Traffic)
Outbound Flows	Outbound Flows are number of current flows in the outbound direction (traffic going out of the VM).
Outbound Flows Maximum Creation Rate	The maximum creation rate of outbound flows (traffic going out of the VM).

Azure Virtual Network Service

Microsoft: Azure Virtual Network Configuration	
Object Name	Object Description
Name	The name of the Virtual Network Peering.
Address Prefix	The address prefix associated with the Virtual Network. This is a comma-separated list.
Allow Forwarded Traffic	Possible values are: True: Forwarded traffic (traffic not originating from the VMs in the peer Virtual Network) will be allowed. False: Forwarded traffic (traffic not originating from the VMs in the peer Virtual Network) will not be allowed.
Allow Gateway Transit	Indicates if peer Virtual Networks can access the Virtual Network's Gateway. It does not indicate if the Gateway is already being used. Possible values are: True: The peer Virtual Network can use the Virtual network Gateway of this Virtual network for connecting to on-premises networks. False: The peer Virtual Network can not use the Virtual network Gateway of this Virtual network for connecting to on-premises networks.
Allow VNet Access	Indicates if communication between the two virtual networks is possible by automatic opening of ACLs. Possible values are: True: (default) The peer Virtual Network's address is included as part of the VIRTUAL_NETWORK tag False: The peer Virtual Network's address is not included as part of the VIRTUAL_NETWORK tag. The VMs in the peer Virtual Network space would not be able to access the VMs in the local Virtual Network space. You would have to set explicit NSG rules to allow

Microsoft: Azure Virtual Network Configuration	
Object Name	Object Description
	communication between the Virtual Networks.
Peering State	State of the Virtual Network peering. Possible values are: Initiated, Connected, or Disconnected.
Provisioning State	Provisioning state of the Virtual Network Peering.
Use Remote Gateways	Possible values are: True: If the flag is set to true, and allowGatewayTransit on peer Virtual Network is also true, the Virtual Network will use the Gateway of the peer Virtual Network for transit. Only 1 peering can have this flag set to true. False: If this flag is set to false, the Virtual Network is not able to use the remote Gateway for transit.
Address Space	AddressSpace contains an array of IP address ranges that can be used by subnets of the virtual network.
Azure Resource Group Name	The Resource Group Name.
Azure Virtual Network/Resource Group	Azure Resource Group ID associated with Azure virtual network.
Azure Virtual Network/Virtual Network Relationship	The identifying URI of the peer Virtual Network.
DDOS Protection	Indicates if DDoS protection is enabled for all the protected resources in the virtual network. It requires a DDoS protection plan associated with the resource.
Delegation Action key	The actions permitted to the service upon delegation.
Delegation Action val	The actions permitted to the service upon delegation.
Delegation etag	A unique read-only string that changes whenever the resource is updated.
Delegation ID	Subnet delegation identifier.
Delegation Name	Subnet delegation name.
Delegation Provisioning State	The provisioning state of the service delegation resource.
Delegation Service Name	The name of the service to which the subnet should be delegated (e.g. Microsoft.Sql/servers).
Delegation Type	Resource type.
DNS Servers	An array of DNS servers available to VMs deployed in the virtual network.
Peering Sync Level	The peering sync status of the virtual network peering. Possible values: FullyInSync LocalAndRemoteNotInSync LocalNotInSync RemoteNotInSync

Microsoft: Azure Virtual Network Configuration	
Object Name	Object Description
Private Endpoint Network Policies	Is the Private Endpoint Network Policy enabled or disabled
Private Link Service Network Policies	Is the Private Link Service Network Policy enabled or disabled
Provisioning State	Provisioning state of the Virtual Network.
Remote Address Prefixes	Address prefix for the remote virtual network address space
Subnet Address Prefix	Virtual network prefixes of subnet.
Subnet Name	A virtual network corresponding subnet name.
Subnet Provisioning State	Provisioning state of the subnet.
Tag Key	Key of the tag pair.
Tag Value	Value of the tag pair.
Virtual Network Location	Specifies the supported Azure location of the virtual network.
Virtual Network Name	The name of a virtual network.
Virtual Network Peering Provisioning State	Provisioning state of the Virtual Network Peering.

Microsoft: Azure Virtual Network Gateway Configuration	
Object Name	Object Description
Name	The Name of the SKU
Name	Name of the Virtual Network Gateway connection.
Address Prefixes	A list of address blocks reserved for this virtual network in CIDR notation.
Azure Virtual Network Gateway/Resource Group	The Resource Group ID of the Virtual Network Gateway.
Azure Virtual Network Gateway/Subnet	The Subnet ID of the Virtual Network Gateway.
Gateway Type	The type of this Virtual Network Gateway. Possible values are: Vpn and ExpressRoute.
ID	The ID of the Virtual Network Gateway.
IP address	Public IP of the virtual Network Gateway.
Is BGP enabled	Whether BGP is enabled for this Virtual Network Gateway or not.
Key	The Key of a tag.
Name	The name of the Virtual Network Gateway.
Provisioning State	The provisioning state of the Virtual Network Gateway resource. Possible values are: Updating, Deleting, and Failed.

Microsoft: Azure Virtual Network Gateway Configuration	
Object Name	Object Description
Provisioning State	The provisioning state of the public IP resource. Possible values are: Updating, Deleting, and Failed.
Resource Group Name	The Resource Group Name which contains the Virtual Network Gateway.
Resource ID	The Resource ID of the public IP address.
SKU tier	The Gateway SKU tier.
Status	The status of the connection.
Subnet Name	The Subnet name of the Virtual Network Gateway.
Tier	The Tier of the SKU
Type	The connection type.
Value	The value of the tag.
Virtual Network Gateway Type	The type of this Virtual Network Gateway. Possible values are: PolicyBased and RouteBased.

Microsoft: Azure Virtual Network Gateway Performance	
Object Name	Object Description
Bgp Peer Status	Status of the BGP peer. 1 indicates connected, 0 indicates disconnected.
Bgp Routes Advertised	Count of BGP routes advertised through the tunnel.
Bgp Routes Learned	Count of BGP routes learned through the tunnel.
ER Gateway Bits Per Second (Classic)	Total bits received on the ExpressRoute Gateway per second (Classic SKU metric name).
ER Gateway Bits Per Second (Scalable)	Total bits received on the ExpressRoute Gateway per second (Scalable/Az SKU metric name).
ER Gateway CPU Utilization (Classic)	CPU utilization of the ExpressRoute Gateway (Classic SKU metric name).
ER Gateway CPU Utilization (Scalable)	CPU utilization of the ExpressRoute Gateway (Scalable/Az SKU metric name).
ER Gateway Packets Per Second (Classic)	Total packets received on the ExpressRoute Gateway per second (Classic SKU metric name).
ER Gateway Packets Per Second (Scalable)	Total packets received on the ExpressRoute Gateway per second (Scalable/Az SKU metric name).
Gateway P2S Bandwidth	Average point-to-site bandwidth in bytes per second for Virtual Network Gateway.
Gateway S2S Bandwidth	Average site-to-site bandwidth in bytes per second for Virtual Network Gateway.
Inbound Flows Count	Number of 5-tuple flows entering the VPN gateway.

Microsoft: Azure Virtual Network Gateway Performance	
Object Name	Object Description
Outbound Flows Count	Number of 5-tuple flows exiting the VPN gateway.
P2S Connection Count	Point-to-site connection count for Virtual Network Gateway.
Tunnel Bandwidth	Average bandwidth of tunnel in bytes per second for Virtual Network Gateway.
Tunnel Egress Bytes	Outgoing bytes of tunnel for Virtual Network Gateway.
Tunnel Egress Packet Drop Count	Count of outgoing tunnel packets dropped.
Tunnel Egress Packet Drop TS Mismatch	Outgoing packet drop count from traffic selector mismatch of tunnel for Virtual Network Gateway.
Tunnel Egress Packets	Outgoing packet count of tunnel for Virtual Network Gateway.
Tunnel Ingress Bytes	Incoming bytes of tunnel for Virtual Network Gateway.
Tunnel Ingress Packet Drop Count	Count of incoming tunnel packets dropped.
Tunnel Ingress Packet Drop TS Mismatch	Incoming packet drop count from traffic selector mismatch of tunnel for Virtual Network Gateway.
Tunnel Ingress Packets	Incoming packet count of tunnel for Virtual Network Gateway.

Microsoft: Azure Virtual Network Subnet Configuration	
Object Name	Object Description
Name	The name of the resource that is unique within a subnet. This name can be used to access the resource.
Service Name	The name of the service to which the subnet should be delegated (e.g. Microsoft.Sql/servers).
Subnet Name	A virtual network corresponding subnet name.
Type	Resource type.
Address Prefix	Virtual network prefixes of subnet.
Azure Network Security Group Name	The Network Security Group Name.
Azure Virtual Network Subnet/Network Security Group	Reference to the network security group that will be applied to all corresponding subnets.
Network Security Group	Network security group (NSG) contains a list of access control list (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network.
Private Endpoint Network Policies	Enable or Disable apply network policies on private end point in the subnet.

Microsoft: Azure Virtual Network Subnet Configuration	
Object Name	Object Description
Private Link Service Network Policies	Enable or Disable apply network policies on private link service in the subnet.
Provisioning State	Provisioning state of the Virtual Network subnet.
Provisioning State	The provisioning state of the service delegation resource.
Route Table	Azure Route Tables, or User Defined Routing, allow you to create network routes so that your F-Series Firewall VM can handle the traffic both between your subnets and to the Internet.

Azure VM Scale Sets Service

Microsoft: Azure VMSS Configuration	
Object Name	Object Description
Size (GB)	The size of a data disk that is aligned with an Azure virtual machine scale set.
Type	The type of a data disk that is aligned with an Azure virtual machine scale set.
Type	The type of an OS disk that is aligned with an Azure virtual machine scale set.
Name	Name of the resource group.
Name	Name of the sub-net.
Name	Name of the load balancer.
Storage Account Type	The Storage Account Type associated with the Azure virtual machine scale set.
Storage Account Type	Specifies the storage account type for the managed disk. Possible values are: Standard_LRS | Premium_LRS.
Automatic OS Upgrade	Whether OS upgrades should automatically be applied to scale set instances in a rolling fashion when a newer version of the image becomes available.
Autoscaling	Whether or not auto-scaling feature is enabled in the scale set. Possible values are: "On" and "Off"
Availability Zone	Availability zones for the virtual machine scale set.
Azure VMSS/Load Balancer	Load balancer identifier.
Azure VMSS/Resource Group	Resource Group identifier.

Microsoft: Azure VMSS Configuration	
Object Name	Object Description
Azure VMSS/Subnet	Subnet identifier.
Caching	The caching requirements of an Azure virtual machine scale set.
Caching	Specifies the caching requirements. Possible values are: None | ReadOnly | ReadWrite.
Computer Name Prefix	The computer name prefix of an Azure virtual machine scale set.
Creation Option	The operating system creation option of an Azure virtual machine scale set.
Dynatrace Host/Azure Virtual Machine Scale Set	VMSS namespace.
Enabled Accelerated Network	Specifies whether the network interface is accelerated networking-enabled.
IP Configurations	The IP configuration name.
Key	Key of the tag pair.
Location	The location where an Azure virtual machine scale set resides.
Mode	Specifies the mode of an upgrade to virtual machines in the scale set. Possible values are: Manual | Automatic
Name	The IP Address Name
Name	The network configuration name.
Name	The name of an Azure virtual machine scale set.
Offer	Specifies the offer of the platform image or marketplace image used to create the virtual machine.
Primary	Specifies the primary network interface in case the virtual machine has more than 1 network interface.
Private IP Address Version	It represents whether the specific ipconfiguration is IPv4 or IPv6. Possible values are: IPv4 | IPv6
Provisioning State	Provisioning state of the Azure virtual machine scale set. Possible values: Updating | Succeeded | Failed
Public IP	Public IP Address.
Publisher	The image publisher.
Single Placement Group	The single placement group of an Azure virtual machine scale set of max size 100 virtual machines.
SKU	The image SKU.
Sku Capacity	Specifies the number of virtual machines in the scale set.

Microsoft: Azure VMSS Configuration	
Object Name	Object Description
Sku Name	The sku name.
Sku Tier	Specifies the tier of virtual machines in a scale set. Possible values are: Standard | Basic
Type	Specifies the type of an Azure virtual machine scale set.
Value	Value of the tag pair.
Version	Specifies the version of the platform image or marketplace image used to create the virtual machine.
VMSS Name|Dynatrace Host Name	VMSS name

Microsoft: Azure VMSS Performance	
Object Name	Object Description
CPU Average	The percentage of allocated compute units that are currently in use by the Virtual Machine(s)
CPU Credits Consumed	Total number of credits consumed by the Virtual Machine.
CPU Credits Remaining	Total number of credits available to burst.
Disk Read Bytes	Total bytes read from disk during monitoring period.
Disk Read Operations/Second	Disk Read IOPS.
Disk Write Bytes	Total bytes written to disk during monitoring period.
Disk Write Operations/Second	Disk Write IOPS.
Network In	The number of bytes received on all network interfaces by the Virtual Machine Scale Set (Incoming Traffic)
Network Out	The number of bytes out on all network interfaces by the Virtual Machine scale set(Outgoing Traffic)

Microsoft: Azure VMSS Profiles Configuration	
Object Name	Object Description
Name	The name of the profile.
Mode	The mode of the profile.
Profile Name	The profile name.
Default Limit	The number of instances that will be set if metrics are not available for evaluation. The default is only used if the current instance count is lower than the default.
Max Limit	The maximum number of instances for the resource.

Microsoft: Azure VMSS Profiles Configuration	
Object Name	Object Description
	The actual maximum number of instances is limited by the cores that are available in the subscription.
Metric Name	The name of the metric that defines what the rule monitors.
Min Limit	The minimum number of instances for the resource.
Number of Rules	The number of rules in the profile.
Time Zone	The timezone for the hours of the profile.
Direction	The scale direction. Whether the scaling action increases or decreases the number of instances.
Start Date	The start time for the profile in ISO 8601 format.
Cooldown	The amount of time to wait since the last scaling action before this action occurs. It must be between 1 week and 1 minute in ISO 8601 format.
Enabled	The enabled flag. Specifies whether automatic scaling is enabled for the resource. The default value is 'true'.
End Date	The end time for the profile in ISO 8601 format.
Name	Azure resource name.
Operator	The operator that is used to compare the metric data and the threshold.
Recurrence	The collection of days that the profile takes effect on. Possible values are Sunday through Saturday.
Statistic	The metric statistic type. How the metrics from multiple instances are combined.
Threshold	The threshold of the metric that triggers the scale action.
Time Aggregation	Time aggregation type. How the data that is collected should be combined over time. The default value is Average.
Time Grain	The granularity of metrics the rule monitors. Must be one of the predefined values returned from metric definitions for the metric. Must be between 12 hours and 1 minute.
Time Window	The range of time in which instance data is collected. This value must be greater than the delay in metric collection, which can vary from resource-to-resource. Must be between 12 hours and 5 minutes.
Value	The number of instances that are involved in the scaling action. This value must be 1 or greater. The default value is 1.

Microsoft: Azure VMSS Virtual Machine Configuration	
Object Name	Object Description
Azure VMSS Virtual Machine/Resource Group	The resource group device identifier.
Caching Requirements	Specifies the caching requirements. Possible values are: None, ReadOnly and ReadWrite.
Code	Disk statuses code.
Code	VM statuses code.
Code	VM Agent statuses code.
Computer Name	The computer name assigned to the virtual machine.
Config Name	The IP configuration name.
Created From	Specifies how the virtual machine should be created. Possible values are: Attach and FromImage.
Deployment Status	The instance provisioning state.
Hardware Type	The stock keeping unit name.
Instance ID	The virtual machine instance ID.
Interface MAC Address	The MAC address of the network interface.
Interface Name	The network interface name.
Interface Resource GUID	The resource GUID property of the network interface resource.
IP Allocation Method	Defines how a private IP address is assigned. Possible values are: "Static" and "Dynamic".
IP Version	It represents whether the specific ipconfiguration is IPv4 or IPv6.
Key	The instance tag name.
Latest Model Applied	Specifies whether the latest model has been applied to the virtual machine.
Level	Disk statuses level.
Level	VM statuses level.
Level	VM Agent statuses level.
Location	The resource location.
Message	VM Agent statuses message.
Name	The device name.
Name	The disk name.
Name	Disk statuses.
OS Disk Size GB	Specifies the size of an empty data disk in gigabytes. This value cannot be larger than 1023 GB.

Microsoft: Azure VMSS Virtual Machine Configuration	
Object Name	Object Description
OS Offer	Specifies the offer of the platform image or marketplace image used to create the virtual machine.
OS Publisher	The image publisher.
OS SKU	The image SKU(Stock Keeping Unit).
OS Type	This property allows you to specify the type of the OS that is included in the disk. Possible values are Windows and Linux.
OS Version	Specifies the version of the platform image or marketplace image used to create the virtual machine.
Placement Group Id	VM Placement Group Id.
Platform Fault Domain Count	VM Platform Fault Domain Count.
Platform Update Domain Count	VM Platform Update Domain Count.
Private IP Address	Private IP address of the IP configuration.
Resource Group Name	The resource group device name.
Status	Disk statuses displayStatus.
Status	VM statuses displayStatus.
Status	VM Agent statuses displayStatus.
Storage Account Type	Specifies the storage account type for the managed disk. Possible values are Standard_LRS or Premium_LRS.
Time	Disk statuses time.
Time	VM statuses time.
Time	VM Agent statuses time.
Uri	Specifies the virtual hard disk's uri.
Value	The instance tag value.
VM Agent Version	Specifies the version of the agent in the virtual machine.
VM ID	Azure Virtual Machine unique ID.

Microsoft: Azure VMSS Virtual Machine Performance	
Object Name	Object Description
CPU Credits Consumed	Total number of credits consumed by the Virtual Machine.
CPU Credits Remaining	Total number of credits available to burst.
CPU Utilization	The percentage of allocated compute units that are currently in use by the Virtual Machine(s)

Microsoft: Azure VMSS Virtual Machine Performance	
Object Name	Object Description
Disk Read Bytes	Total bytes read from disk during monitoring period.
Disk Read Operations/Second	Disk Read IOPS.
Disk Write Bytes	Total bytes written to disk during monitoring period.
Disk Write Operations/Second	Disk Write IOPS.
Network In	The number of bytes received on all network interfaces by the Virtual Machine Scale Set Virtual Machine (Incoming Traffic)
Network Out	The number of bytes out on all network interfaces by the Virtual Machine Scale Set Virtual Machine (Outgoing Traffic)

Azure Web Application Firewall (WAF)

Microsoft: Azure WAF on Application Gateway Policy Configuration	
Object Name	Object Description
Match Variable	The variable to be excluded. - RequestHeaderNames, RequestCookieNames, RequestArgNames
Name	The application Gateway Resource Name.
Name	The application HTTP Listener Resource Name.
Name	The name of the resource that is unique within a policy. This name can be used to access the resource.
Action	Type of Actions. - Allow, Block, Log
Azure Resource Group Name	The Resource Group Name.
Azure WAF Gateway Policy/Application Gateway	The application Gateway Resource Id.
Azure WAF Gateway Policy/HTTP Listener	The application HTTP Listener Resource Id.
Azure WAF Gateway Policy/Resource Group	Azure Resource Group ID associated.
File Upload Limit (Mb)	Maximum file upload size in Mb for WAF.
Match Operator	When matchVariable is a collection, operate on the selector to specify which elements in the collection this exclusion applies to. - Equals, Contains, StartsWith, EndsWith, EqualsAny.
Max Request Body Size (Kb)	Maximum request body size in Kb for WAF.
Mode	he mode of the policy. - Prevention or Detection.
Name	The name of the policy.
Priority	Priority of the rule. Rules with a lower value will be

Microsoft: Azure WAF on Application Gateway Policy Configuration	
Object Name	Object Description
	evaluated before rules with a higher value.
Provisioning State	The Provisioning state of the Policy.
Request Body Check	Whether to allow WAF to check request Body.
Rule Set Type	Defines the rule set type to use.
Rule Set Version	Defines the version of the rule set to use.
Rule Type	The rule type. - MatchRule or Invalid.
Selector	When matchVariable is a collection, operator used to specify which elements in the collection this exclusion applies to.
State	The state of the policy. - Disabled or Enabled.
Tag Key	Tags key.
Tag Value	Tags values.

Microsoft: Azure WAF on CDN Policy Configuration	
Object Name	Object Description
Enabled State	Describes if the policy is in enabled state or disabled state. Disabled or Enabled.
Mode	Describes if it is in detection mode or prevention mode at policy level. Prevention or Detection.
Azure Resource Group Name	The Resource Group Name.
Default Redirect Url	Default Redirect Url.
Endpoint Name	CDN profile endpoint name.
Name	Defines the name of the custom rule.
Name	The name of the Cdn Web Application Firewall Policy.
Name	Defines the name of the custom rule.
Rule Set Type	Defines the rule set type to use.
Rule Set Version	Defines the version of the rule set to use.
Action	Describes what action to be applied when rule matches. Allow, Block, Log, Redirect.
Action	Describes what action to be applied when rule matches. - Allow, Block, Log, Redirect.
Anomaly Score	Verizon only : If the rule set supports anomaly detection mode, this describes the threshold for blocking requests.
Azure WAF CDN Policy/Endpoint	endpoint Link.
Azure WAF CDN Policy/Resource Group	Azure Resource Group ID associated.

Microsoft: Azure WAF on CDN Policy Configuration	
Object Name	Object Description
Custom Rules	Custom Rules
Default Custom Block Response Body	If the action type is block, customer can override the response body. The body must be specified in base64 encoding.
Default Custom Block Response Status Code	If the action type is block, this field defines the default customer overridable http response status code.
Enabled State	Describes if the custom rule is in enabled or disabled state.
Enabled State	Describes if the custom rule is in enabled or disabled state.
Endpoint Relationships	Endpoint Relationships
Location	Resource location.
Managed Rules	Managed Rules
Policy Settings	Policy Settings
Priority	Defines in what order this rule be evaluated in the overall list of custom rules.
Priority	Defines in what order this rule be evaluated in the overall list of rules.
Provisioning State	The provision state on WAF CDN Policy.
Rate Limit Duration (Min)	Defines rate limit duration. Default is 1 minute.
Rate Limit Rules	Rate Limit Rules
Rate Limit Threshold	Defines rate limit threshold.
Resource Group Relationships	Resource Group Relationships
Resource State	Resource State of the azure WAF cdn resource.
SKU Name	Pricing Tier
Tag Key	Tags key.
Tag Value	Tags values.
Tags	Tags

Microsoft: Azure WAF on CDN Policy Performance	
Object Name	Object Description
Requests By Action	The number of client requests processed by the Web Application Firewall by Action Name.
Requests By Action Label	WAF requests by action label.
Requests By Rule Name	The number of client requests processed by the Web Application Firewall by Rule Name.
Requests By Rule Name Label	WAF requests by rule name label.

Microsoft: Azure WAF on CDN Policy Performance	
Object Name	Object Description
Requests Total	The total number of client requests processed by the Web Application Firewall.

Other Supported Services

The following services are fully supported using performance metrics within already supported services:

Azure Service	Service in Which it is Fully Supported
Azure Disk Storage	*Azure Managed Disks Service*
Archive Storage	*Azure Storage Service*
Azure Blob Storage	
Queue Storage	
Table Storage	
Azure Spot Virtual Machines	*All Azure VM Services*
Data Science Virtual Machines	
VPN Gateway	*Azure Virtual Network Service*

The following services have partial coverage with configuration information, health status, and Azure alerts:

Azure Service	Service in Which it is Partially Supported
API Management	*Resource List*
Azure Analysis Services	
Azure Arc	
Azure Bastion	
Azure Cognitive Services	
Azure Database for MariaDB	
Azure Database for MySQL Flexible Server	
Azure Database for PostgreSQL Flexible Server	
Azure Database for Migration Service	
Azure Dedicated Host	
Azure Digital Twins	
Azure IoT Hub	
Azure Purview	
Azure Service Fabric	
Azure Spring Cloud	
Azure Stream Analytics	
Azure Synapse Analytics	
Data Lake Analytics	
Event Hubs	
HDInsight	
Log Analytics	
Media Services	
Microsoft Purview	
Mobile Apps	
Notification Hubs	
PowerBI Embedded	

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information herein, the information provided in this document may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described herein at any time without notice.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010