

**Azure Cloud Storage & Legacy**

**Plugin Configuration Guide**

Contents

[Azure Storage & Legacy Server 2](#_Toc49326287)

[Azure Storage & Legacy Configuration Checklist 2](#_Toc49326288)

[Supported Collection Types 2](#_Toc49326289)

[Data Sources 4](#_Toc49326290)

[Backup Data (Legacy) 4](#_Toc49326291)

[Inventory Data 4](#_Toc49326292)

[Requirements 4](#_Toc49326293)

[Backup data: Storage Accounts 4](#_Toc49326294)

[Backup data: Access keys 6](#_Toc49326295)

[Inventory: Azure API 7](#_Toc49326296)

[Setup 12](#_Toc49326297)

[Server Properties 12](#_Toc49326298)

[Field Definitions 12](#_Toc49326299)

[Reporting Notes 13](#_Toc49326300)

[Reporting Notes 13](#_Toc49326301)

[Troubleshooting 16](#_Toc49326302)

[No Data Collected with Warning 16](#_Toc49326303)

[Technical Support 17](#_Toc49326304)

# Azure Storage & Legacy Server

This is a guide to the legacy Bocada plug-in for Microsoft Azure Recovery Services (MARS) which is an Azure cloud backup solution. The backup jobs reporting for Azure has been implemented with the new Azure REST API tools and can be found in Bocada as *Azure Cloud Recovery*. Storage reporting has not yet been migrated to the REST API method, so you will still need this *Azure Storage & Legacy* plugin.

Bocada also has a plugin for MS System Center DPM, and a plug-in for MS Azure Backup Server (MABS).

This Microsoft documentation will help explain the different types of MS Azure backup offerings:

<https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup>

# Azure Storage & Legacy Configuration Checklist

This checklist is an overview of the steps required to configure Azure Cloud Collections on your Bocada Data Collection Server. Detailed instructions are below.

* Backup data: Please use the new Plugin for your backup job reporting. A Storage Account must be linked to each Recovery Services Vault you wish to collect from for this legacy plugin, and you can deploy both plugins initially if desired.
* Inventory Data: You will need Tenant Id, Subscription Id, Client Id, Client Secret

# Supported Collection Types

The plugin, supports the following collection types from Azure Cloud servers:

|  |  |  |
| --- | --- | --- |
| **Collection Type** | **Supported** | **Description** |
| Backup | ✓\* | Collects transactional details about backup, duplication and restore jobs. Example metrics include, start times, durations, bytes, files, errors etc. This includes In Progress jobs. |
| Storage | ✓ | Collects point-in-time inventory information. Example metrics include, total recoverable gigabytes (storage), media volume count, media volume status, etc. |
| Policy |  | Collects and stores information on policy attributes, schedules, storage units, storage groups, storage lifecycle policies, and clients. |
| In Progress |  | Collects basic information on backups that are running or have completed since the previous full Backup jobs data collection. These updates are included in the Backup updates, but are lightweight and can be scheduled more often than backup updates if needed. |

\* Depreciated in favor of new REST API based Bocada *Azure Cloud Recovery* plugin which provides improved data, but does not yet have Storage data collection.

# Data Sources

The plugin relies on two different Azure Cloud data sources.

### Backup Data (Legacy)

A [Storage Account](https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction) associated with a [Azure Cloud Recovery Services Vault](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm) for backup is required to collect snapshot information.

### Inventory Data

Inventory data enables Bocada to determine the inventory within Azure to identify unprotected resources and requires access through the Azure REST API, using App Registration credentials.

# Requirements

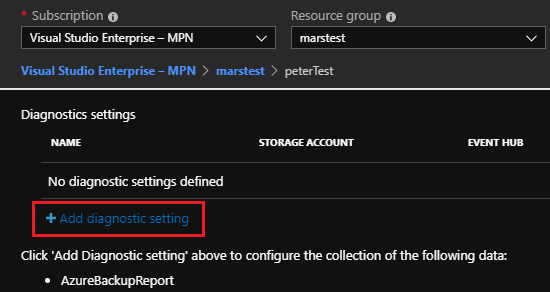
This section lists requirements that must be met before collecting data with the Bocada plugin for Azure Cloud.

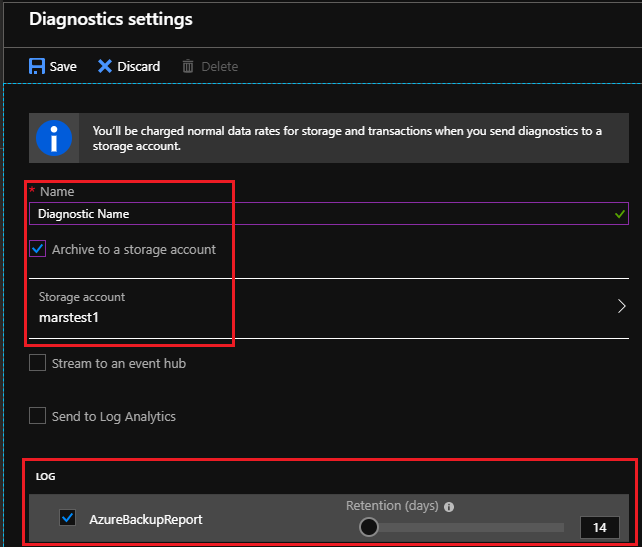
### Backup data: Storage Accounts

Each Recovery Services Vault you wish to collect from has an associated/attached Storage Account. To determine the Storage Account for the Recovery Services Vault open the Azure Portal.

#### Configure Diagnostic Settings

1. choose *+ Add diagnostic setting*:

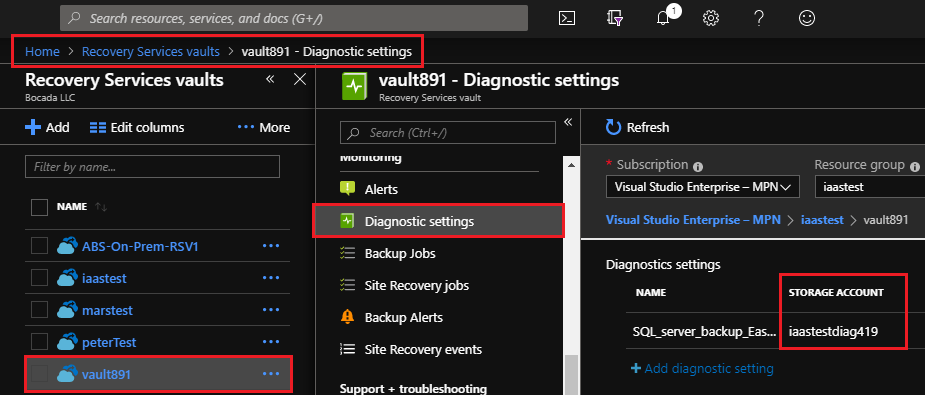


1. Name the diagnostic, choose a storage account for archive. Check the box to LOG AzureBackupReport.  
   

When you configure the Azure Diagnostic Settings it will not populate with backup records from the past.

#### After Diagnostic Settings are configured

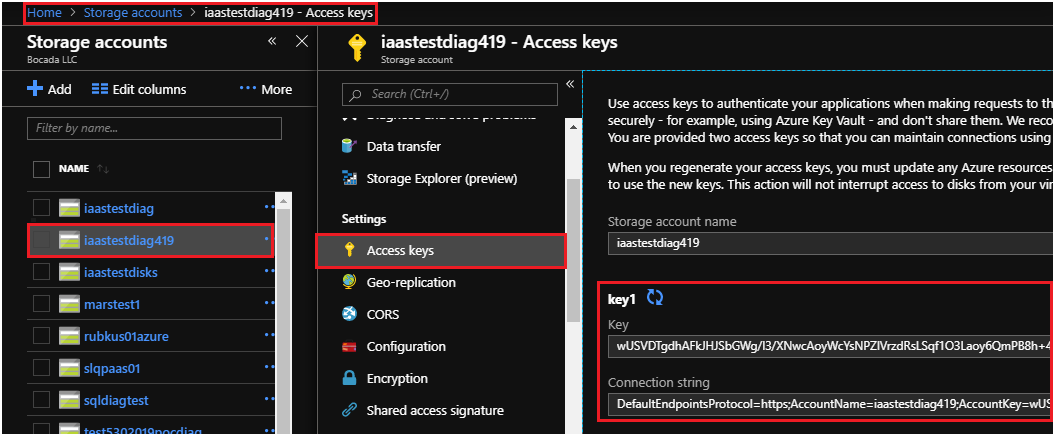
Navigate to *Recovery Services Vaults*, choose the vault of interest, choose *Diagnostic settings*:



### Backup data: Access keys

On the Azure Portal, navigate to the selected the Storage Account and copy Access keys (under Settings).

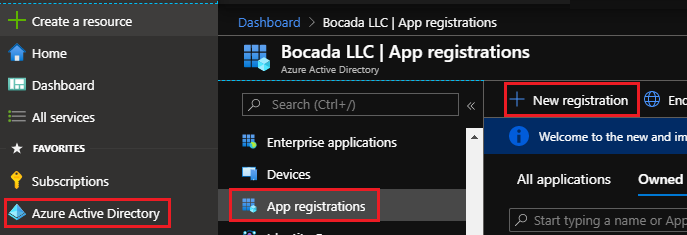
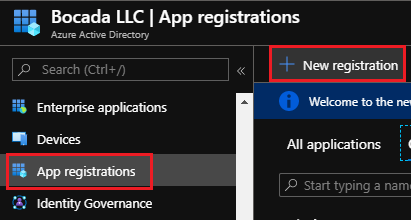
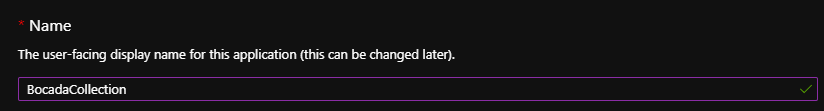
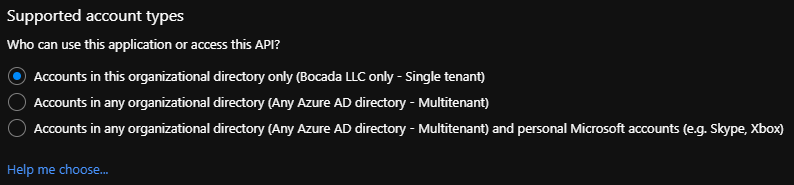
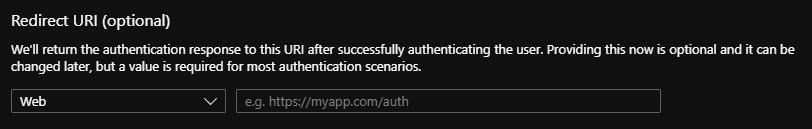
Navigate to Storage accounts, choose the storage account of interest, choose Access Keys:

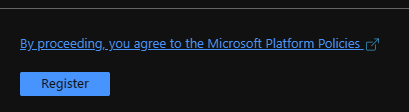


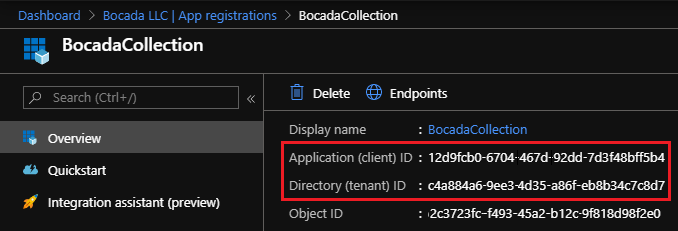
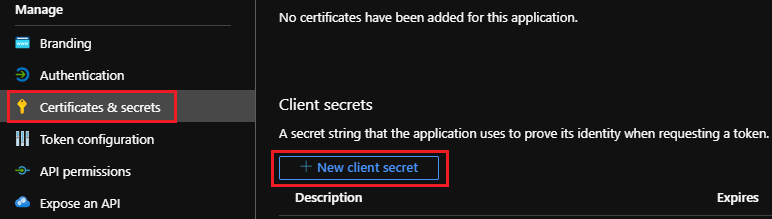
### Inventory: Azure API

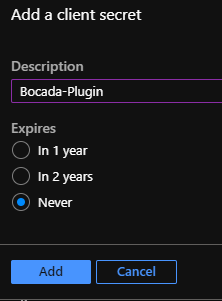
#### Tenant ID, Client Id, & Client Secret

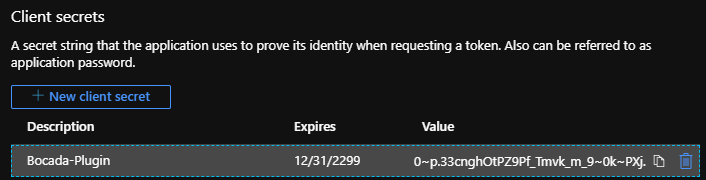
To obtain the needed properties, create a New App Registration:

1. Navigate to Azure Active Directory, then App Registration to add a new registration.  
     
   
2. Name the new App:  
   
3. Choose the Supported Account Type:  
   
4. Do not set the Redirect URI:  
   
5. Register:



1. Note the ***Client ID*** and ***Tenant ID***:  
   
2. Navigate to Certificates and Secrets, create a New client secret:
3. Enter a description, set expiration to “Never” and Add:

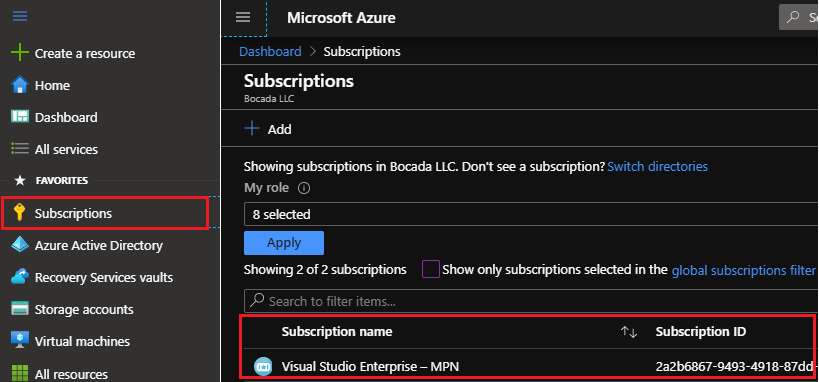
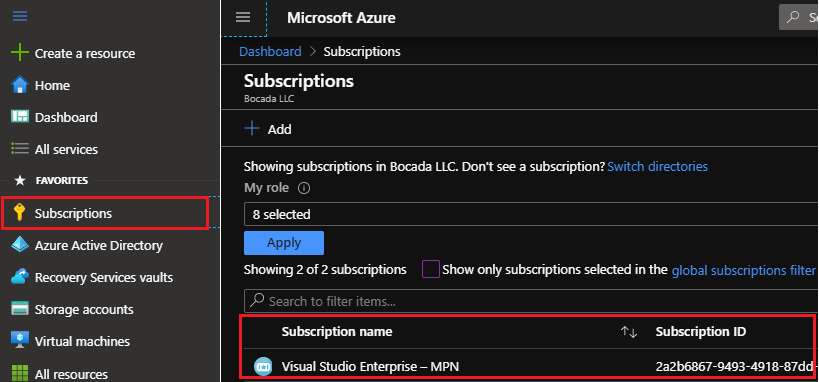


1. Copy the Value of the ***Client Secret***:

#### Subscription ID

To obtain the ***Subscription ID***:

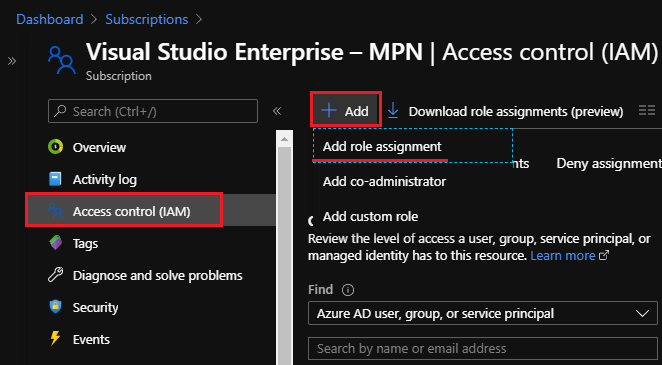
1. Open the Azure Portal, <https://portal.azure.com>

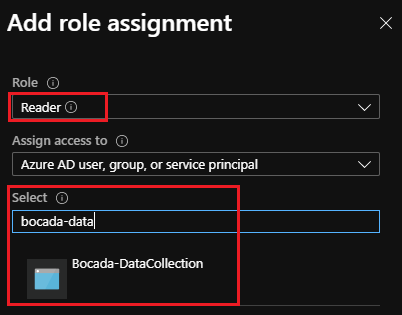
Navigate to Subscriptions, note the ***Subscription ID***  


#### Assign Role to the Application

To access resources in your subscription, you must assign a role to the application.

1. Click into the relevant subscription, navigate to *Access control (IAM)*, Add role assignment

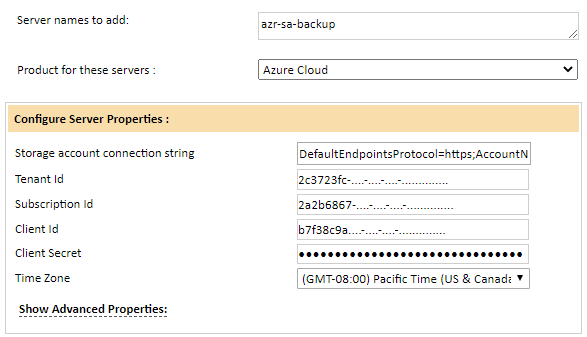


1. Choose *Reader*, the appropriate user, and Save:

# Setup

### Server Properties

Backup Server Properties determine how the plugin will interface with the Azure Cloud.



### Field Definitions

#### Server name

Enter your preferred name for the server. The name of the Recovery Services Vault is suggested.

#### Storage Account Connection String

Enter the connection string for the Storage Account (obtained from the Storage Account on the Azure Portal).

#### Tenant Id

The *Tenant ID* is the Directory ID of the Azure Active Directory that governs access to the resources of the account being inventoried. The Bocada plugin relies on an App registration tied to an Azure AD.

#### Subscription Id

The [***Subscription ID***](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory?) is the Azure subscription associated with the Active Directory tenant:

#### Client Id

The *Client Id* is the ID of an Azure Directory App that will be created for Bocada data collection.

#### Client Secret

The *Client Secret* is the key that you assign to the App used for Bocada data collection.

#### Time Zone

Select the time zone where Azure Cloud server resides. This setting ensures times are displayed consistently in environments that span multiple time zones (Azure groups by regions, e.g. USWest).

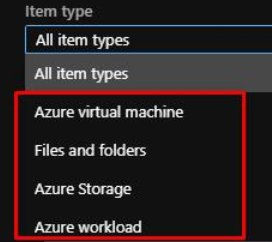
# Reporting Notes

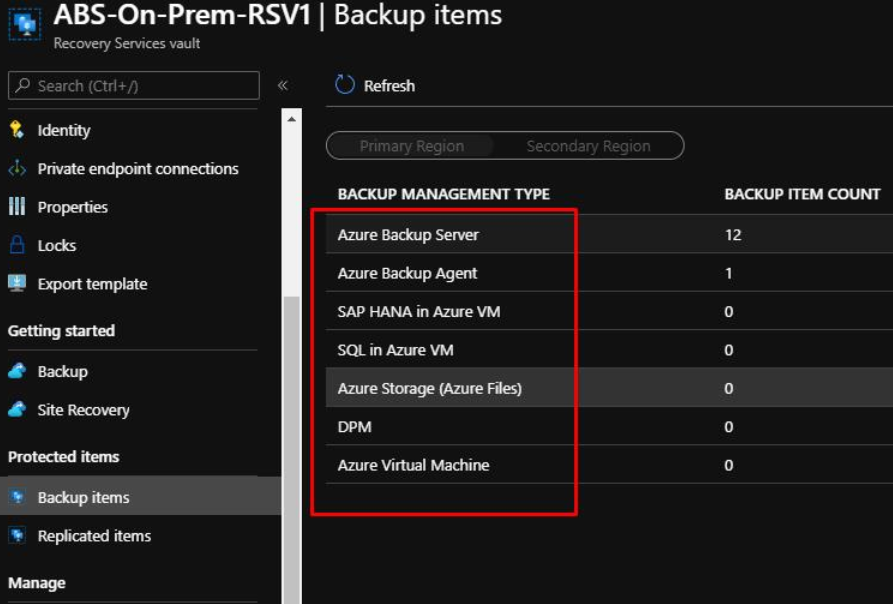
This section offers a few notes about Azure Cloud specific reporting in Bocada.

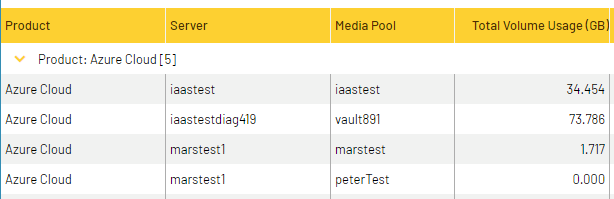
# Reporting Notes

In Bocada you will see your Azure "Protected Server" reported as the Bocada backup client and the Azure "Backup Item" as the Bocada backup target.

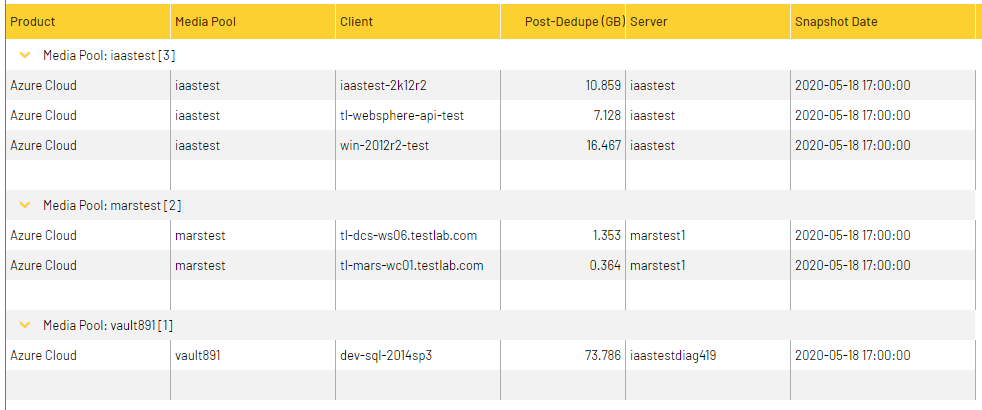
Bocada will report on the same assets that you see in Backup Jobs report in Azure Recovery Services Vault. The Azure Protection Analysis Reports in Bocada will show you which of your Azure assets have backup records and which do not. This will include VM, Workload, Storage, Files & Folder , and DPM Backup assets and Azure backups for these can also be seen in the Bocada Job Trends report. The screen snips below show examples:





To report on Azure Vault storage usage see the Bocada Storage Servers report. The “Media Pool” is the Recovery Services Vault. For example

The Storage Clients report will break out by client/VM how much is storage consumed:



# Troubleshooting

This section will be expanded as useful troubleshooting scenarios are discovered.

### No Data Collected with Warning

Error Message: *No data found on Azure with connection string*

When you first configure the Azure Diagnostic Settings it will not receive backup records from the past. When you do data collection immediately after the configuration, before backups have be run, you may mine no data in Bocada with the following Warning:

No data found on Azure with connection string:...

If you think this might be the cause, then please and try data collection again. Keep in mind that there can be a long delay from when a backup runs to when Microsoft posts the data to the storage group diagnostic, so it is best to wait a day.

# 

# Technical Support

For technical support or a copy of our standard support agreement, please contact us.

**E-mail:** [support@bocada.com](mailto:support@bocada.com)

**Support Portal:** [https://bocada-support.force.com](https://bocada-support.force.com/)

**Phone:** +1-425-898-2400