

**Azure Cloud Recovery**

**Plugin Configuration Guide**

Contents

[Azure Recovery Services vault 2](#_Toc109722435)

[Azure Cloud Recovery Configuration Checklist 2](#_Toc109722436)

[Requirements 2](#_Toc109722437)

[Ports 2](#_Toc109722438)

[Supported Collection Types 3](#_Toc109722439)

[Data Sources 3](#_Toc109722440)

[Base URLs we use to collect data 3](#_Toc109722441)

[Requirements 4](#_Toc109722442)

[Tenant ID, Client Id, & Client Secret 4](#_Toc109722443)

[Subscription ID 7](#_Toc109722444)

[Assign Role to the Application 8](#_Toc109722445)

[SQL Log Backups Configuration (optional) 11](#_Toc109722446)

[Setup 13](#_Toc109722447)

[Server Properties 13](#_Toc109722448)

[Field Definitions 13](#_Toc109722449)

[Reporting Notes 14](#_Toc109722450)

[Azure to Bocada Data and Item Mapping 14](#_Toc109722451)

[Backup Type Coverage 15](#_Toc109722452)

[Troubleshooting 16](#_Toc109722453)

[Technical Support 17](#_Toc109722454)

# Azure Recovery Services vault

This is a guide to the Bocada plug-in for Microsoft Azure Recovery Services (MARS) which is an Azure cloud backup solution.

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>

Recovery Services vaults overview:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>

As of Bocada 21.3.12 :

* ***Backup Services*** from Azure Recovery Services vaults is supported.
* ***Site Recovery Services*** from Azure Recovery services vaults is not yet supported. Please contact Bocada for current status if you require reporting on Site Recovery Services.

# Azure Cloud Recovery Configuration Checklist

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

* Verify access from Bocada DCS to the Azure REST API website.
* Obtain Tenant Id, Subscription Id, Client Id, Client Secret
* For Bocada 21.1.2 or older versions obtain Resource Group Name, Recovery Services vault name

# Requirements

This section lists requirements that must be met prior to collecting data with the Bocada plugin for Azure:

### Ports

|  |  |  |
| --- | --- | --- |
| **Service** | **Default Port** | **Note** |
| *HTTPS* | 443 | Outbound from DCS API connection via HTTPS |

# Supported Collection Types

The plugin, supports the following collection types from Azure Cloud Recovery 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. |

# Data Sources

The plugin relies on the [Azure REST API](https://docs.microsoft.com/en-us/rest/api/azure/) data source. Currently, the Bocada Azure plugin support all Azure Recovery Services vaults protected workloads (SQL in Azure VM, Azure Virtual Machine, Azure Backup Agent, Azure Backup Server, DPM, Azure Storage (Azure Files), SAP HANA in Azure VM), Azure SQL Managed Instance, Azure SQL Database.

### Base URLs we use to collect data

* https://login.microsoftonline.com/
* https://management.azure.com/
* https://api.loganalytics.io/

Please note that these URLs are base, so if you want to limit network access - expect that they will be extended by specific API endpoints and by your specific data (subscription GUID etc.).

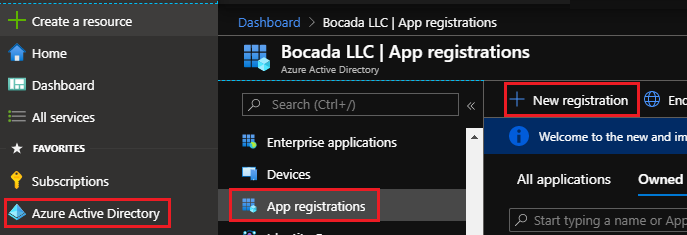
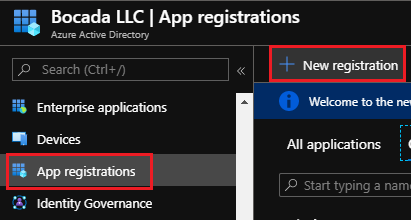
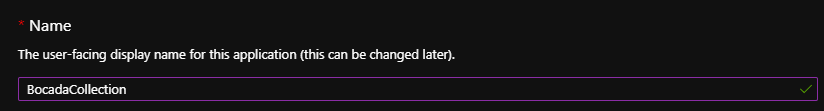
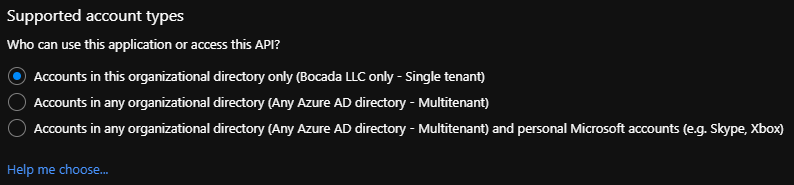
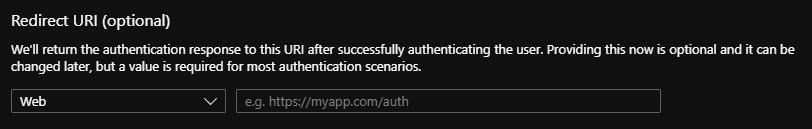
For example, on our data - one of the endpoints to get details for a specific job: <https://management.azure.com/subscriptions/2a2b6867-9493-4918-87dd-7532a22b5a79/resourceGroups/ABS-On-Prem-RSV1-RG/providers/Microsoft.RecoveryServices/vaults/ABS-On-Prem-RSV1/backupJobs/f4c37d3a-938c-4038-92d4-0149fae75325>

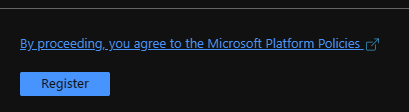
# Requirements

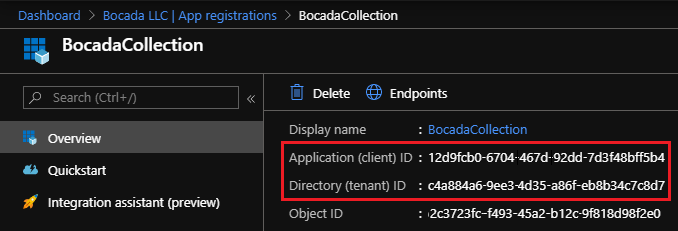
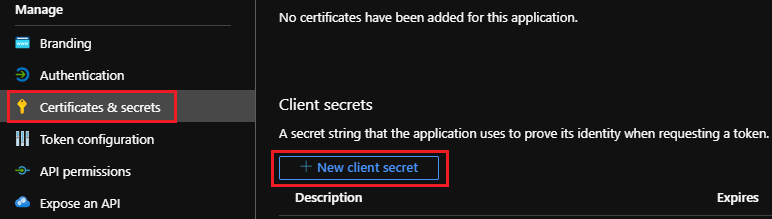
This section lists requirements that must be met before collecting data with the Bocada plugin for Azure Cloud Recovery.

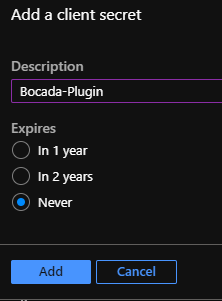
### Tenant ID, Client Id, & Client Secret

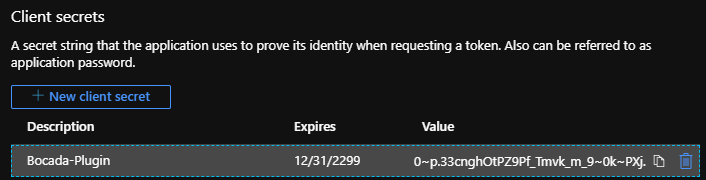
To obtain the needed properties, create a New App Registration:

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”, or the largest value available, and Add:

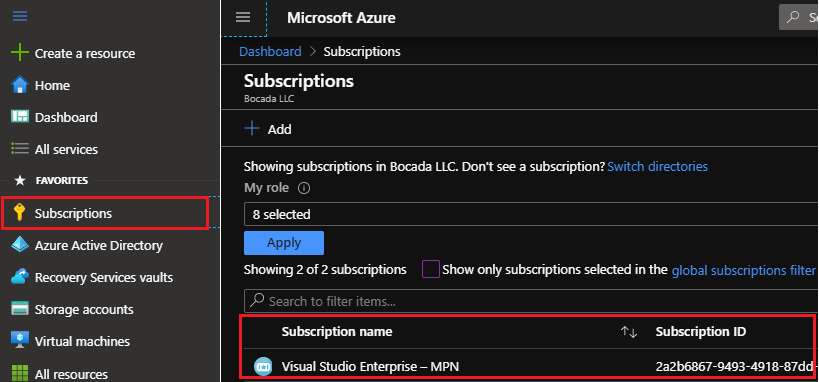


1. Copy the Value of the ***Client Secret***:

### Subscription ID

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

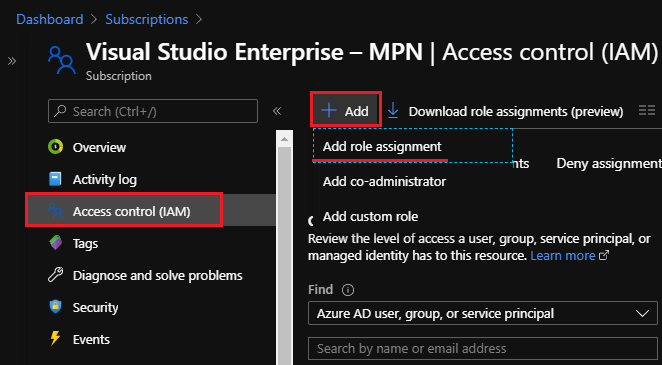
1. Open the Azure Portal, <https://portal.azure.com>

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 the *Reader* role and click Members:  
   A screenshot of a computer

   Description automatically generated with medium confidence
2. Click *Select members* and select the Bocada App Client created above:  
   Graphical user interface, text, application

   Description automatically generatedGraphical user interface, application

   Description automatically generatedGraphical user interface, text

   Description automatically generatedGraphical user interface, text, application, email

   Description automatically generated
3. Review and Assign  
   Graphical user interface, text

   Description automatically generated
4. Validate the following:

* Note the icon the Type added should be an App (not a user)
* App has Reader Role

A screenshot of a computer screen

Description automatically generated with medium confidence

# SQL Log Backups Configuration (optional)

For collecting data on SQL log backups set by “SQL Server in Azure VM” R VM” Recovery Service Vault (RSV) policy type – need to add diagnostic setting to your RSV with the “Send to Log Analytics workspace” value and log “AddonAzureBackupJobs”. Also, please set the “Resource specific” destination table. See screenshot below.

Graphical user interface, text

Description automatically generated

Please note that if you there is no Log Analytics workspace at you Azure deployment, need to create it first:

A screenshot of a computer

Description automatically generated with medium confidence

You may also check log backup jobs on Azure Log Analytics workspace side by running the request below:

*AddonAzureBackupJobs*

*| where OperationName == "Job"*

*| where JobOperationSubType == "Log"*

*| where JobStartDateTime >= datetime(2021-06-01 11:00:00Z) // Set needed date*

*| where JobStartDateTime <= datetime(2021-12-30 11:00:00Z) // Set needed date*

*| sort by JobStartDateTime desc*

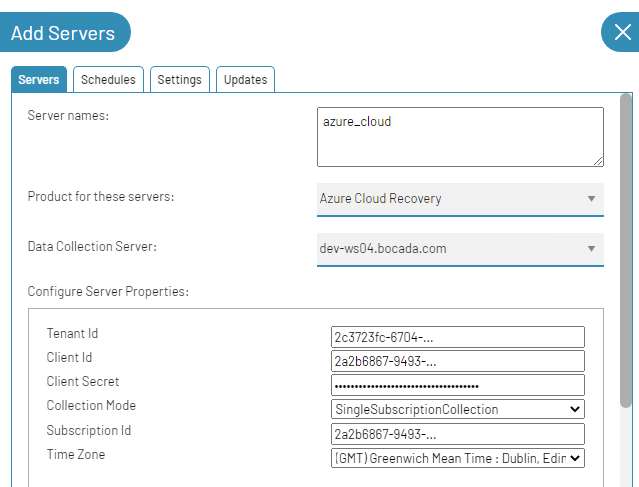
A screenshot of a computer

Description automatically generated with medium confidence

# Setup

### Server Properties

Backup Server Properties determine how the plugin will interact with the Azure.



### Field Definitions

#### Server name

Enter your preferred name for the server. It must be a single token with letters, numbers, dot (.), hyphen (-), and underscore only. On Bocada 21.1.3 and later versions it can be suitable name for representing the group of all Azure instances with the same subscription ID. On Bocada 21.1.2 and older the name of the Recovery Services Vault is suggested.

#### 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.

#### 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.

#### Collection Mode

Select "Multiple Subscription Collection" if you need this server to collect data from all accessible subscriptions under "Tenant Id".

Select "Single Subscription Collection" if you need this server to collect data only from one subscription, which you will set on the "Subscription Id" property.

A corresponding zone and rules will be created for each Azure subscription, from which you collect data.

#### 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. Appears only for the "Single Subscription Collection" Collection Mode.

#### Time Zone

Select the time zone where Azure Cloud Recovery 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

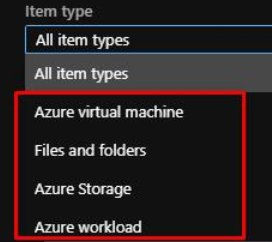
### Azure to Bocada Data and Item Mapping

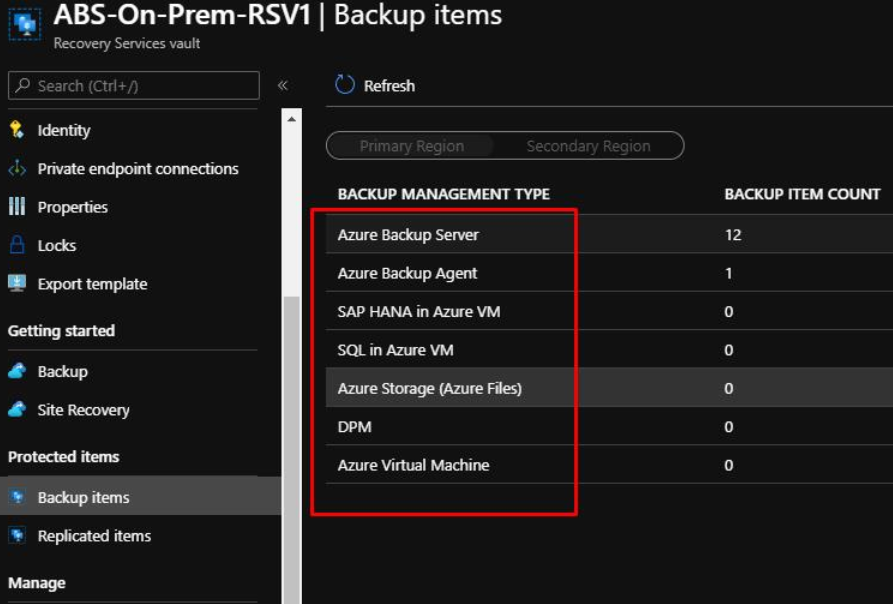
In Bocada you will see your Azure "Protected Server" which shows under the column “Name” reported as the backup client. Sometimes “Name” is different from “Computer name”.



And the Azure "Backup Item" as the 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 Azure 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:





### Backup Type Coverage

Both built-in PaaS backups and custom backups that are going to a Storage Account are reported on.

# Troubleshooting

This section describes issues found and how they have been resolved.

***Problem: Data Collection fails with the following message: Error: Azure REST API issue while getting client resources: The HTTP status code of the response was not expected (403).***

Data collection can fail because the needed Role has not been assigned. With this problem the connection can get an auth token for the subscription, but it will not have enough permissions to access the needed resources.

To correct, review the section *Assign Role to the Application* above. If you want to independently verify the credential problem, obtain the Azure Cloud Recovery Postman diagnostic package from Bocada Support.

**Here is an example Bocada data collection log file for this issue:**

Status: 403

Response:

{"error":{"code":"AuthorizationFailed","message":"The client '…-…-…-… with object id …-…-….-…-…' does not have authorization to perform action 'Microsoft.Resources/subscriptions/resources/read' over scope '/subscriptions/…-…-…-…-…' or the scope is invalid. If access was recently granted, please refresh your credentials."}}

Inner Exception:

at AzureREST.AzureRestPlugin.CollectBackupLog()

at CollectBackupLog(SByte\* repositoryPath, SByte\* server, SByte\* properties, Double startDate, Double endDate)

Error 545: CollectBackupException: Error found while collecting backup data. Please review log for detail.

Error: Azure REST API issue while getting client resources: The HTTP status code of the response was not expected (403).

***Problem: Data Collection succeeds, but there is incomplete data in the tenancy.***

This can be caused by the access credentials not having enough permission to access all Azure assets. Please check the following:

* Verify that you have added the App Client aka Service Principal, to all the Subscriptions within the tenant.
* To independently verify the credential problem, obtain the Azure Cloud Recovery Postman diagnostic package from Bocada Support.

***Problem: Data Collection fails with the following message: Error: Azure REST API issue while getting Backup Jobs: The HTTP status code of the response was not expected (404).***

Error code 404 on Azure Rest API describes a case where the specified API resource does not exist. It could be that one of the fields for server properties on Bocada needs to be corrected (for example – Resource Group Name) in order to fix this issue. Suggested solution would be to verify each of the fields on server properties is correct and then run another backup collection. If this issue is not resolved this way, run logging on Bocada to see more details on the root cause.

#### Note that the following server properties are retired and do not do anything

##### *Under* Show Advanced Properties: Resource Group Name

Decommissioned: The *Resource Group Name* from Azure to which the Recovery Services Vault belongs.

##### *Under* Show Advanced Properties: Recovery Services vault name

Decommissioned: The *Recovery Services vault name* is the name of Recovery Services Vault from Azure.

# 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