Microsoft Azure Backup Server (MABS) Plugin Configuration Guide

Contents

Azure Backup Server

This is a guide to the Bocada plug-in for Microsoft Azure Backup Server (MABS). Azure Backup Server is an on-premises backup solution from Microsoft.

Bocada also has a plug-in for Azure Cloud backups with Microsoft Azure Recovery Services (MARS) and a plugin for Microsoft System Center DPM.

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 Backup Server Configuration Checklist

While detailed steps are included below, this is an overview of the steps to configure Azure Backup Server collections on your Bocada Data Collection Server:

- ☐ Verify location of the Azure Backup Server database
- ☐ Create a SQL login with Read (and preferably also Write) access on that database
- ☐ Verify the required TCP port has been opened

Supported Collection Types

The plug-in currently supports the following collection types from Azure Backup Server:

Collection Type	Supported	Description
Backup	✓	Collects transactional details about backup, duplication and restore jobs. Example metrics include, start times, durations, bytes, files, errors etc.
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.

Data Sources

The plugin relies on the following Azure Backup Server data sources:

- MABS database

Requirements

This section lists requirements that must be met prior to collecting data with the Bocada plugin for Microsoft Azure on Premises.

MABS Database

Location

The plugin requires access to the Azure database to collect data. By default, the data to be mined, resides in the following locations:

- SQL Server: Co-located with the Microsoft Azure backup server
- Instance: MSDPMINSTANCE
- Database: DPMDB

Permissions

To query data from the MABS database, the plugin requires a SQL login with read access permissions. By default, the Azure SQL instance allows only Windows Authentication. If SQL Authentication is desired, the Azure SQL instance must be configured to allow SQL Server Authentication.

Note: Providing user credentials with write access to the MABS database is not required to perform data collection. However, write access can improve collection responses from our queries by allowing the Bocada data collection to create an index. Again, this is not required but can lead to improved update performance.

Note: If the *Bocada Data Collection Service* is run using the Local System account on the Data Collection Server, then the Azure Backup Server plug-in will require a SQL user with SQL Server Authentication. See the Troubleshooting section on SQL Server User creation, below.

Communications

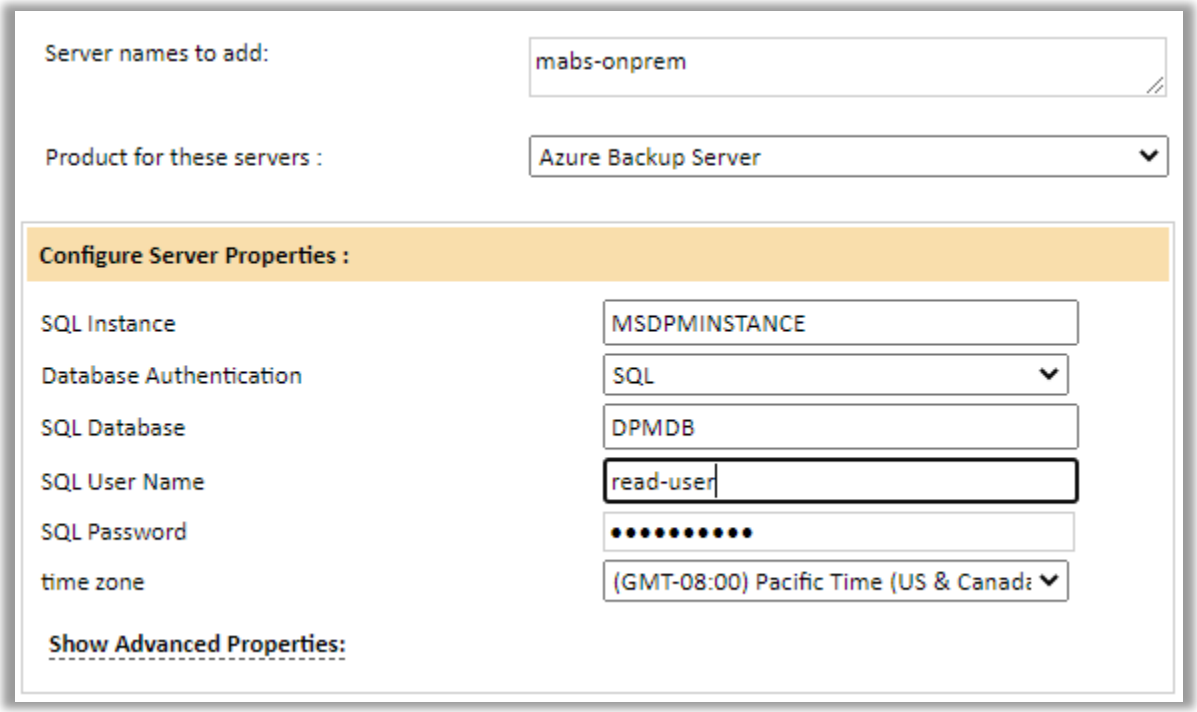
Ports

Service	Default Port	Direction	Notes
TCP/IP	1433	inbound	MS SQL Server default port for the TCP/IP protocol. This is configured in the SQL Server Configuration Manager.

Setup

Server Properties

Backup Server Properties determine how the plugin will interface with the MABS server and are managed through the Backup Servers view.



Field Definitions

SQL Instance

Provide the SQL instance where the Azure database resides (default is 'MSDPMINSTANCE').

Database Authentication

Specify the authentication method used to access the Azure database

SQL Database

Provide the name of the Azure database (default database name is 'DPMDB').

SQL User Name and Password

Enter the username and password the plugin will use to access the Azure Database. The account specified must have read access (and preferably write access).

Time Zone

Select the time zone where Azure Backup server resides. This setting ensures times are displayed consistently in environments that span multiple time zones.

Terminology

The following table defines terms used by Bocada and the equivalent corresponding MS Azure Backup Server term:

Bocada Term	Definition	Equivalent Azure Term
Job Group	An aggregate of one or more backup jobs that are scheduled to start at the same date/time.	Protection Group
Backup Server	A computer that transmits data from one or more backup clients to a storage device. Backup servers also keep metadata describing backup activities.	Azure Backup Server
Backup Client	A computer that is eligible to be backed up by a backup server.	Server
Target	The smallest target resource that the backup software can account for individually with respect to key metrics like backup date/time, byte count, errors, etc.	Selected Members for a Protection Group
Media Library	A hardware device that automatically manipulates two or more media volumes. Media Libraries contain one or more media devices and a robotic arm to manipulate media volumes.	Library
Media Device	A hardware unit that reads and writes backed up data to and from media volumes.	Drive
Media Volume	A hardware unit used for long term storage of backed up data. Media volumes typically take the form of magnetic tapes or hard disks.	Tape

Reporting Notes

A few notes about Azure specific reporting in Bocada.

- *Azure / DPM Recovery Point Summary* is a dedicated report in Bocada under Backup Activity in Bocada.
- *Azure / DPM Recovery Point Status* is a dedicated report in Bocada under Backup Activity in Bocada.

Troubleshooting

Allowing SQL authentication access to the Azure SQL instance:

These steps may be necessary if the default SQL user 'sa' is locked down:

1. In SQL Server Management Studio (SSMS), connect to the Azure SQL instance (default location: <SERVER_NAME>\ MSDPMINSTANCE)
2. Enable SQL authentication (mixed mode):
    a. Right-click on the instance and select *Properties*
    b. In the Server Properties window that appears, select *Security*
    c. Under *Server authentication*, select *SQL Server and Windows Authentication mode*
    d. Click *OK*.
3. Add a new user with SQL authentication:
    a. In the SSMS Object Explorer, click on the plus icon next to *Security* to expand
    b. Right-click on *Logins* and select *New Login*
    c. In the new Login window that appears, on the General tab:
        i. Select the *SQL Server authentication* button.
        ii. Enter the login name and a password which meets your password policy.
    d. On the Server Roles tab: Select the appropriate role.
    e. On the User Mapping tab:
        i. Select your Azure database (default is DPMDB)
        ii. Select the appropriate membership roles (db_datareader is required; db_datawriter is advised to allow the plug-in to add an index to table tbl_TE_TaskTrail)
    f. On the Status tab:
        i. Verify Permission to connect is *Granted*
        ii. Verify Login is *Enabled*

Technical Support

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

E-mail: support@bocada.com
Support Portal: https://bocada-support.force.com/s/
Phone: +1-425-898-2400