Microsoft Data Protection Manager (DPM) Plugin Configuration Guide

Contents

Microsoft System Center Data Protection Manager (DPM)

This is a guide to the Bocada plug-in for Microsoft System Center Data Protection Manager (DPM).

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

DPM Configuration Checklist

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

- ☐ Verify location of the DPM database.
- ☐ Create a SQL login with Read (and preferably Write) access on that database OR add services account as an authorized Windows user in SQL DPM Server.
- ☐ Verify required TCP port has been opened.
- ☐ Add the DPM server to Bocada under Operations > Backup Servers, and set Server Properties.

Supported Collection Types

The plugin currently supports the following collection types from Microsoft DPM 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.
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 DPM data sources:

- DPM database

Requirements

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

Microsoft DPM Database

Location

The plugin requires access to the DPM database in order to collect data. By default, this resides in the following locations:

- Server: Co-located with the Microsoft DPM backup server
- DPM 2007 Instance: MS$DPM2007$
- DPM 2010 Instance: MSDPM2010
- DPM 2012 Instance: MSDPM2012
- DPM Database: DPMDB

Permissions

In order to query data from the DPM database, the plugin requires a login with read access permissions. By default, the DPM SQL instance allows only Windows Authentication, and you need only insure that the Windows user running the Bocada services is an authorized user. If SQL Authentication with a SQL login is desired, the DPM SQL instance must be configured to allow SQL Server Authentication as well as have the user added.

Note: Providing a user with write access to the DPM database is not required to perform data collection; however, it can improve collection responses from our queries by allowing 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 DPM plug-in will require a SQL user with SQL Server Authentication. See the Troubleshooting section on SQL Server User creation, below.

Communications

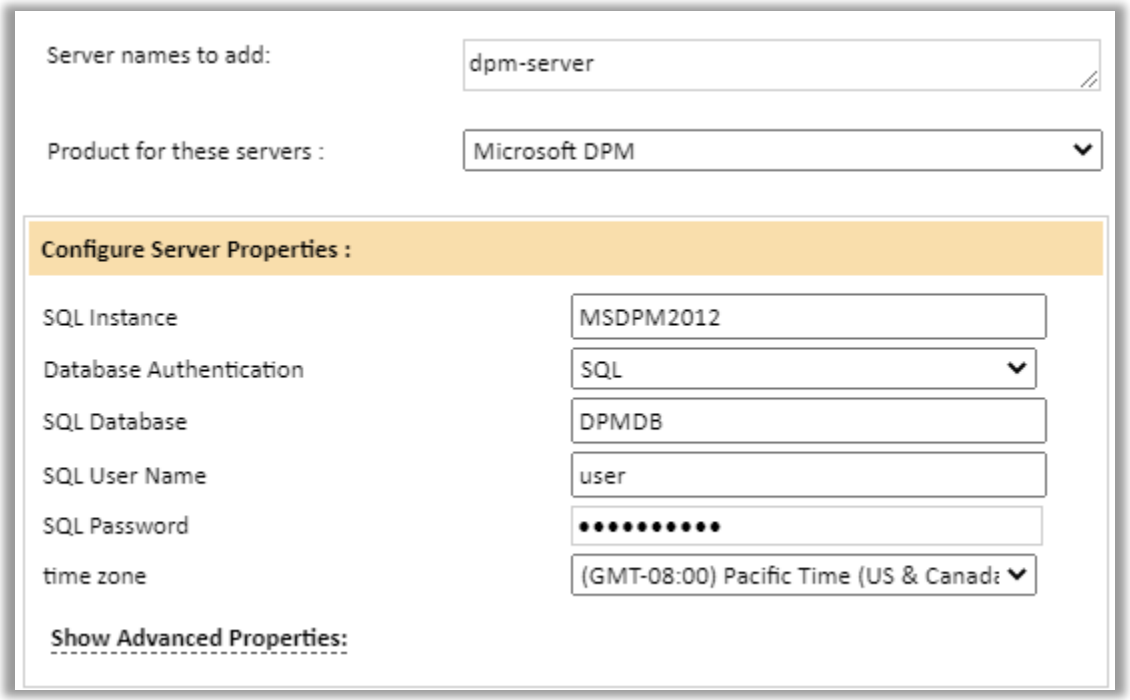
Ports

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 DPM Server and are managed through the Backup Servers view.



Field Definitions

SQL Instance

Provide the SQL instance where the DPM database resides. See above for DPM default locations.

Database Authentication

Specify the authentication method used to access the DPM database.

SQL Database

Provide the name of the DPM database. The default database name is DPMDB.

SQL User Name and Password

If you are using SQL Authentication, then enter the username and password the plugin will use to access the DPM Database. If you use Windows Authentication, then the account that runs your Bocada services will be used and these fields will be ignored. The SQL account must have read access and may have better performance if it also was write access.

Time Zone

Select the time zone where DPM 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 Microsoft DPM term.

vpConnect Term	Definition	Equivalent Microsoft DPM 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.	Microsoft DPM Protection 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 device 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

Troubleshooting

Allowing SQL authentication access to the DPM SQL instance:

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

1. In SQL Server Management Studio, connect to the DPM SQL instance (see above for default locations)
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 DPM 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