Micro Focus Data Protector Plugin Configuration Guide

Contents

Introduction

This document tells you how to add a Data Protection backup Server to Bocada and configure Bocada to collect data for reporting the backup server. There are two ways to mine data from Data Protector. Both methods are described in the document below.

Data Protector Configuration Checklist

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

Backup Collection

- ☐ Backup Firewall ports have been opened
- ☐ Requirements have been met
  - (Linux/Unix) Install 64-bit PuTTY on the DCS
  - (Windows) Configure WinRM credentials
- ☐ Cell Manager has been added with the relevant server properties defined

Storage Collection

- ☐ Storage Firewall Ports have been opened
- ☐ Requirements have been met
  - Enable access to the PostgreSQL database 'hpdbidb' in the pg_hba.conf file
  - Configure a superuser on the database if default user 'hpdp' is unavailable
- ☐ Relevant server properties defined

Policy Collection

- ☐ Policy Firewall ports have been opened
- ☐ Requirements have been met:
  - Provide access to the file share where policy data specifications are defined
- ☐ Relevant server properties defined

Legacy Backup Collection (Data Protector 9.0x)

- ☐ Backup Legacy versions ports are open.
- ☐ Specify port ranges in omnirc file
- ☐ Cell Manager has been added with the relevant server properties defined

Supported Collection Types

The plugin currently supports the following collection types from Data Protector Cell Managers:

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

Backup data is mined using server commands typically found in the following locations:

- C:\Program Files\OmniBack\bin (Windows cell managers)
- /opt/omni/bin (Unix cell managers)

Policy (backup specification) data is mined by reading files located directly on the Cell Managers file structure.

Storage data is mined by executing read-only queries on the PostgreSQL Data Protector internal database (hpdpidb).

Backup Data Collection

Port Communication

The following ports are required to be open between any server running the Bocada Data Collection Service (DCS) and each Data Protector Cell Manager:

Data Protector Versions	Bocada Data Collection	Protocol or Daemon	Default Port	Direction	Notes
9.1+	Backup	SSH	22	Inbound to DP Server, bi-directional	Required for UNIX/Linux Cell Managers
9.1+	Backup	WinRM	5985	Inbound to DP Server, bi-directional	Required for Windows Cell Managers
9.0x, 8.1.x	Backup	TCP	5555/TCP (*inetd*)	Inbound to DP Server, bi-directional	See appendix for more about these legacy versions of Data Protector

All ports must be opened bi-directionally.

Requirements

Collection of backup data from Data Protector cell mangers using SSH protocol to authenticate and gather data from those cell managers. Requirements for this method include either PuTTy installation on the Bocada DCS for communication with UNIX/Linux Cell Managers, or WinRM configuration on Windows Cell Managers.

PuTTy:

Download and install the latest 64-bit version (the 32-bit version is not supported) of PuTTy on the Bocada DCS for communication with UNIX/Linux Cell Managers: https://www.putty.org/

WinRM:

For Data Protector Cell Managers running on Windows OS, Windows Remote Management (WinRM) must be configured to allow the Bocada DCS to collect data from the Cell Manager.

WinRM Information

Description: https://msdn.microsoft.com/en-us/library/aa384426%28v=vs.85%29.aspx?
Configuration: https://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx

Cell Manager Configuration

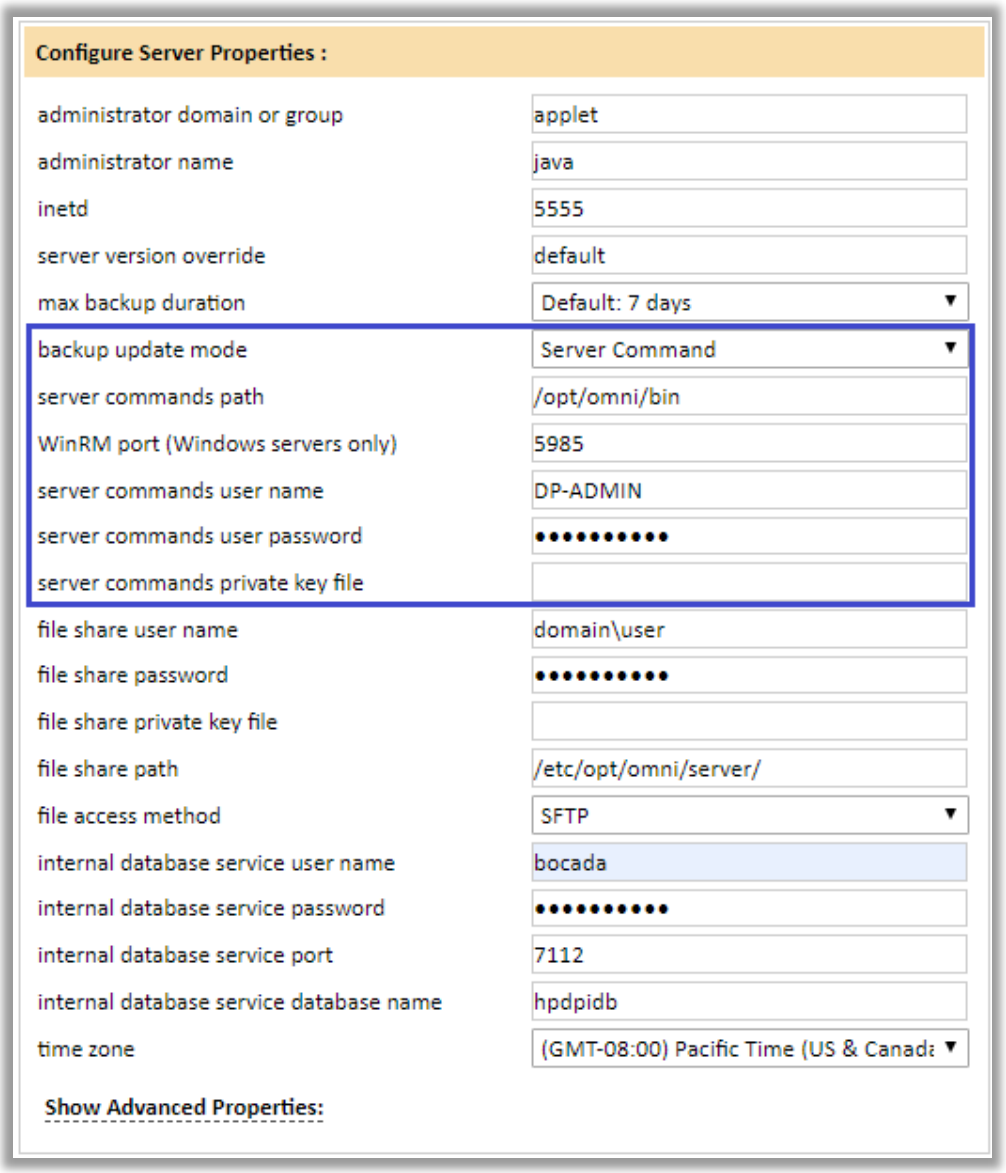
1. Run Windows Command prompt as Administrator
2. Enter the command: **winrm quickconfig**
3. Type **y** in response to: **Make these changes [y/n]?**

Successful configuration will display the following output:

```
WinRM has been updated for remote management.
WinRM service type changed to delayed auto start.
WinRM service started.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any
IP on this machine.
```

Bocada Server Properties (Backup)

These backup collection properties are valid for all supported versions of Data Protector and rely on native Data Protector commands. The connection methods utilize PuTTy or WinRM connections as described in the Requirements section above.



Backup update mode

This determines the method of backup data collection and should be set to "Server Command" for all supported Data Protector versions. For 9.0x and older versions of Data Protector, please reference the legacy collection method.

Server commands path

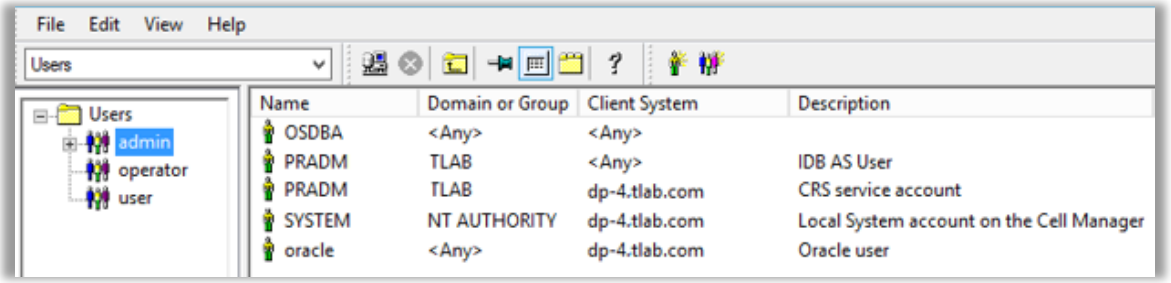
The commands in the path are used to gather data from the Data Protector Cell Manager. The default locations for the Server Commands are:

- Windows Cell Manager: C:\Program Files\OmniBack\bin
- Linux/Unix Cell Manager: /opt/omni/bin

WinRM port (Windows servers only)
The port the communications through WinRM used to communicate with Windows Cell Managers.

Server commands username/password
The server commands rely on a local user which is a member of the admin role in Data Protector:

- Windows Cell Managers require users to be Windows administrators and Data Protector Administrator on the machine.
  - Note the Password requirement/limitation for Data Protector Users from the DP documentation as special characters in the user password can cause updates to fail. The password must comply to the following conditions:
    - Must be 8-20 characters long
    - Includes at least one upper case letter
    - Includes at least one of these special character: an asterisk (*), a dot (.), an hyphen (-), or an underscore (_). NOTE: no other special characters should be used.
    - Includes at least one numeral
    - Does not include spaces
- Unix Cell Managers require the user to be added to the hpdp group on Unix Cell Managers. This can be done with the command: *usermod -aG <group> <user>.*



Server commands private key file (optional)
This field is used for Backup collection if a private key file (.ppk) is used to securely connect to the Cell Manager. Server commands username (see above) is still required.

Additional Server Properties

Max backup duration

Set this property to the longest duration backup job on the DP Cell Manager. The larger the value, the more impact it will have on the performance of the Bocada updates.

Time Zone
Select the time zone where Data Protector Cell Manager resides. This setting ensures times are displayed consistently in environments that span multiple time zones. Data extracted from the server is converted to Coordinated Universal Time (UTC) then to the time zone chosen in report criteria.

Storage Data Collection

The data accessed for collection is stored in the PostgreSQL database used by the Cell Manager, which is 'hpdbidb' by default.

Port Communication

The following ports are required to be open between any server running the Bocada Data Collection Service (DCS) and each Data Protector Cell Manager:

Protocol or Daemon	Default Port	Direction	Notes
PostgreSQL	7112	Inbound to DP Server, Bi-directional	Default service port to connect to the Data Protector PostgreSQL database (see Setup, below)

All ports must be opened bi-directionally.

Requirements

For the Bocada plug-in to access this data, two requirements must be met:

1. The pg_hba.conf file must be edited to allow access to the PostgreSQL databases from the server running the Bocada Data Collection Service.
2. A superuser role with a known password must be added to the Data Protector IDB (with password authentication).

Enable Host Database Access

The pg_hba.conf file governs client authentication with the PostgreSQL databases on the server. More information and instructions regarding allowing Bocada Data Collection servers (clients) access to the PostgreSQL databases on the Cell Manager (Host) can be found in the PostGreSQL documentation: http://www.postgresql.org/docs/9.2/static/auth-pg-hba-conf.html

In these steps, this document references the following default directories:

Data Protector Install Directory = C:\Program Files\OmniBack\idb\bin\
Data Protector DB Install Directory = C:\ProgramData\Omniback\server\db80\pg

Creating a PostgreSQL Database User

1. Navigate to <Data Protector DB Install Dir>
2. Create a copy of pg_hba.conf named pg_nba_original.conf
    - Add the following line as the **first**[1] entry in the Configuration Section of the pg_hba.conf and save the file:

[1] Since the `pg_hba.conf` records are examined sequentially for each connection attempt, the order of the records is significant, and this must be the first non-comment line in the file. Reference: https://www.postgresql.org/docs/9.3/static/auth-pg-hba-conf.html

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
host    all             all             all                     trust
host    postgres        hpdp            127.0.0.1/32            sspi map=hpdpidb
host    postgres        hpdp            ::1/128                 sspi map=hpdpidb
```

3. Reload the pg_hba.conf file by running the following command:

   `<Data Protector Install Dir>\pg_ctl.exe reload -D "<Data Protector DB Install Dir>"`

```
E:\Program Files\OmniBack\idb\bin>pg_ctl.exe reload -D "E:\ProgramData\OmniBack\server\db80\pg"
server signaled
```

4. Create the PostgreSQL Database User and password using the following command:

   `<Data Protector Install Dir>\createuser.exe -p <port> -h <dp host ip> -U hpdp -P -s <new_username>`

   Notes:

   - The username must be all lower case. No capital letters may be used.
   - Use the IP address of your Data Protector cell manager.
   - As above, you will be asked to "Enter password for new role", and then "Enter it again" (see screenshot below). If the system asks for a password after you enter it the second time, there is an error; Review Steps 1 through 4; Possible reasons for this are that the new entry in the pg_hba.conf is incorrect, or that the pg_hba.conf has not been reloaded. Here is an example call with a new username of "*bocada*", but you can use any lowercase username that you prefer.

```
E:\Program Files\OmniBack\idb\bin>createuser.exe -p 7112 -h 192.168.1.12 -U hpdp -P -s bocada
Enter password for new role:
Enter it again:
```

5. Update the first entry added to the *pg_hba.conf* in step 5, above to be the following and then save the file:

   `Host  all  <new_username>  samenet  md5`

   Note: 'samenet' may be used when the Bocada server and Data Protector server are in the same subnet. If they are on different subnets, this may be set to the IP of the Bocada server or 'all'.

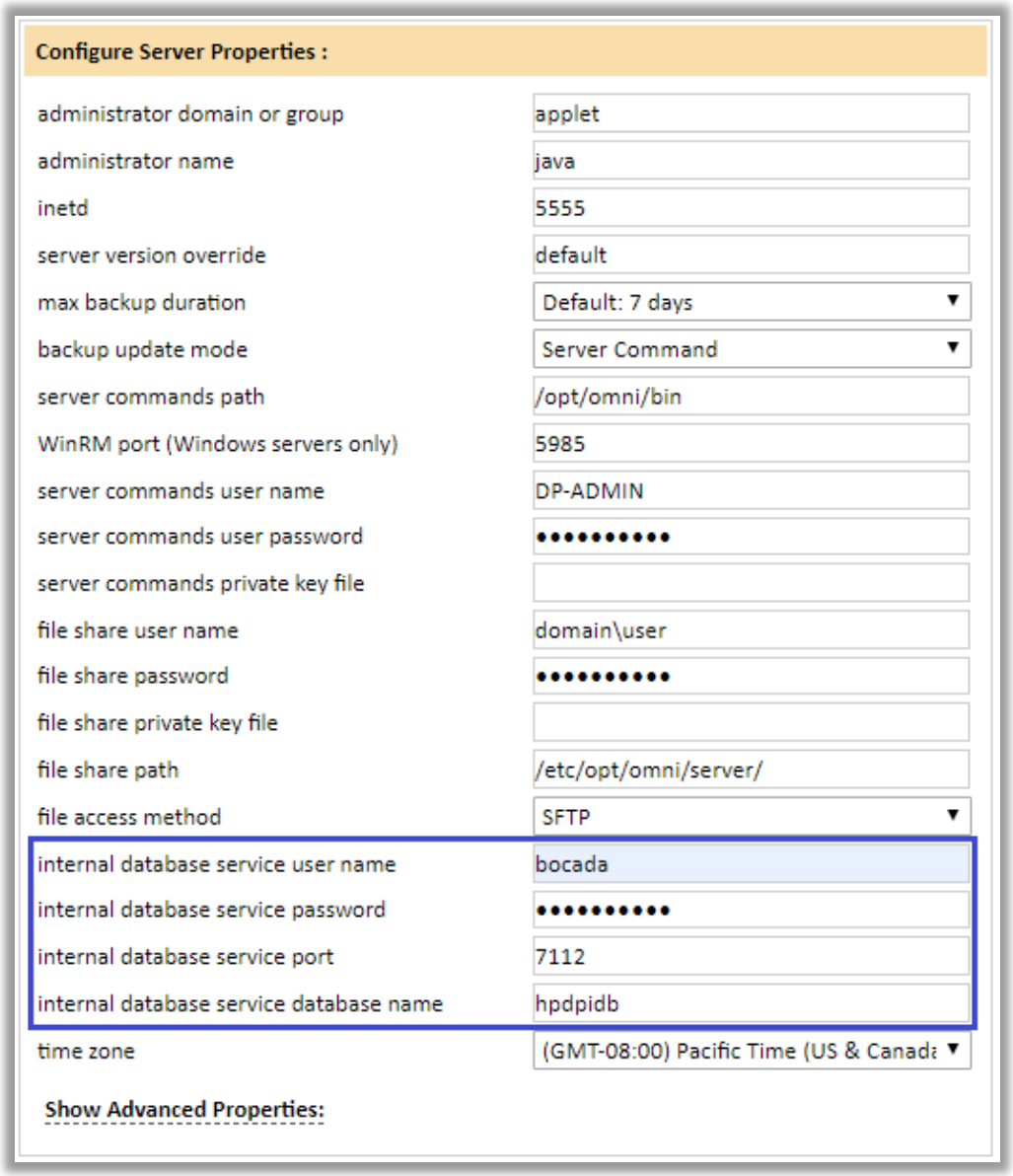
```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
host    all             bocada          samenet                 md5
host    postgres        hpdp            127.0.0.1/32            sspi map=hpdpidb
host    postgres        hpdp            ::1/128                 sspi map=hpdpidb
```

6. Reload the pg_hba.conf file again by running the following command:

   `<Data Protector Install Dir>\pg_ctl.exe reload -D "<Data Protector DB Install Dir>"`

```
E:\Program Files\OmniBack\idb\bin>pg_ctl.exe reload -D "E:\ProgramData\OmniBack\server\db80\pg"
server signaled
```

Bocada Server Properties (Storage)



Internal database service user name
Enter the username of the Superuser Login Role added to the Data Protector PostgreSQL database.

Internal database service password
Enter the password of the Superuser Login Role added to the Data Protector PostgreSQL database.

Internal database service port
Enter the port specified during the installation of the Cell Manager for the IDB port. The default port is 7112.

Internal database service database name
Enter the database name of the Data Protector internal database. The default name is hpdpidb.

Policy Data Collection

The data accessed for collection is stored in the file system on the Cell Manager and access will need to be granted directly or through an SFTP share.

Port Communication

The following ports are required to be open between any server running the Bocada Data Collection Service (DCS) and each Data Protector Cell Manager:

Protocol or Daemon	Default Port	Direction	Notes
SFTP	22	Inbound to DP Server, bi-directional	Required for Windows and Unix/Linux Cell Managers

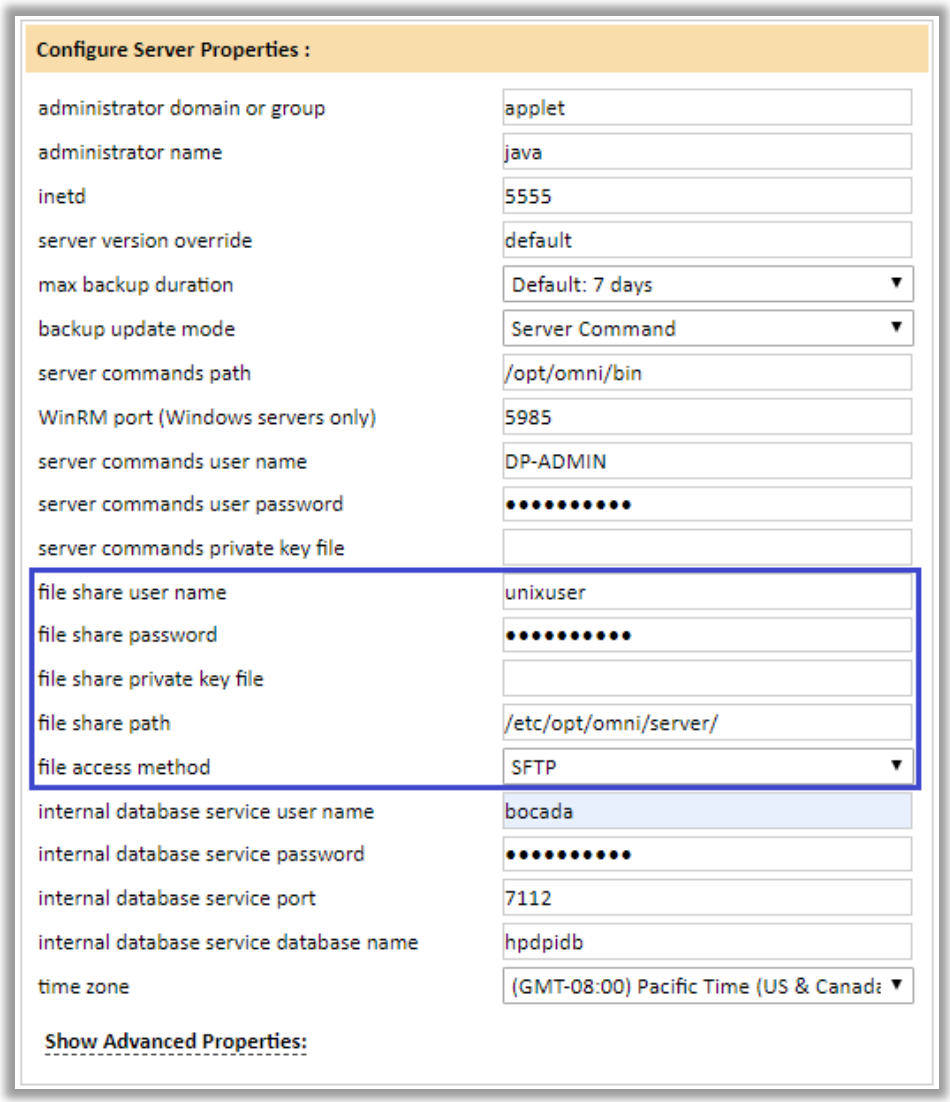
All ports must be opened bi-directionally.

Requirements

To collect Policy data (backup specification), the Bocada plug-in must be given access to the file share on the Cell Manager where these specifications are defined. For example, the default location on a Windows installation of Data Protector is C:\ProgramData\OmniBack\Config\Server.

The recommended method of making files accessible to the plugin from a Linux machine is to set up an SFTP share to the location where the policy specifications are defined. The default installation location is /etc/opt/omni/server.

Bocada Server Properties (Policy)



File share username / password

Enter a user credentials with access to the files system on the Cell Manager. On Windows the user must be a member the Administrator or Backup Operator group but does not need to be a Data Protector user.

File share private key file

This field is used for Policy collection if a private key file (.rsa) is used to securely connect to the Cell Manager. If you are using a .ppk file for Backup collections this file can be converted to a .rsa file using Putty (instruction is easily available via internet search). File share username (see above) is still required.

File share path

This is location on the Data Protector Cell Manager where the backup specification (policy) definitions are stored. The default locations are:

- Windows Cell Manager: C:\ProgramData\OmniBack\Config\Server
- Linux/Unix Cell Manager: /etc/opt/omni/server/

Reporting Notes

The *VM Protection Analysis* report displays VMware VM inventory and will indicate if those VMs are protected by backup applications or are exposed as unprotected. Bocada will correlate Data Protector client data with vCenter virtual machine data, in the following scenario:

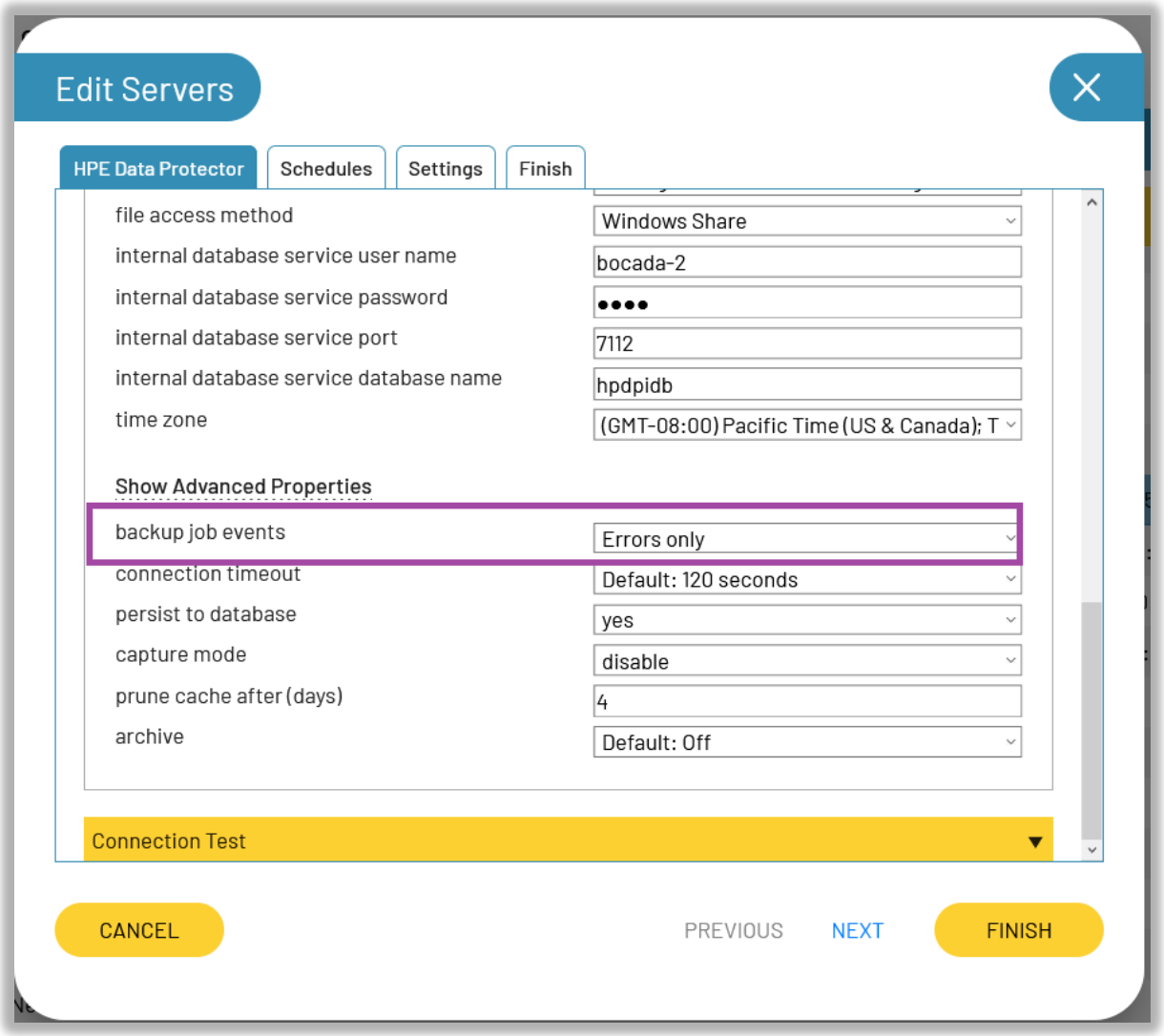
- The backup client is a virtual machine managed by vCenter.
- The vCenter virtual machines have been added to Bocada data collection and previously inventoried using the vCenter plugin in Bocada.

Troubleshooting

This section covers some limited trouble areas. We encourage you to contact Bocada support with any issues or questions, whether large or small, about you Bocada deployment.

Problem: Data Collection for a Data Protector Cell Manager is Slow

Sometimes collecting data from a large busy Data Protector Cell Manager can be slow. One setting that can help with this problem is to collect job message events only for backups that have encountered an error, instead of for all backup jobs. To access this, edit your backup server. In the Backup Server properties in Bocada, under *Show Advanced Properties*, you will see a property named *backup job events* which is set to *Default: All* when you add a Data Protector Cell Manager. Change this setting to *Errors only*.



Problem: Data Collection fails with: Session doesn't exist" or you have errors in Data Collection about duplicate session IDs

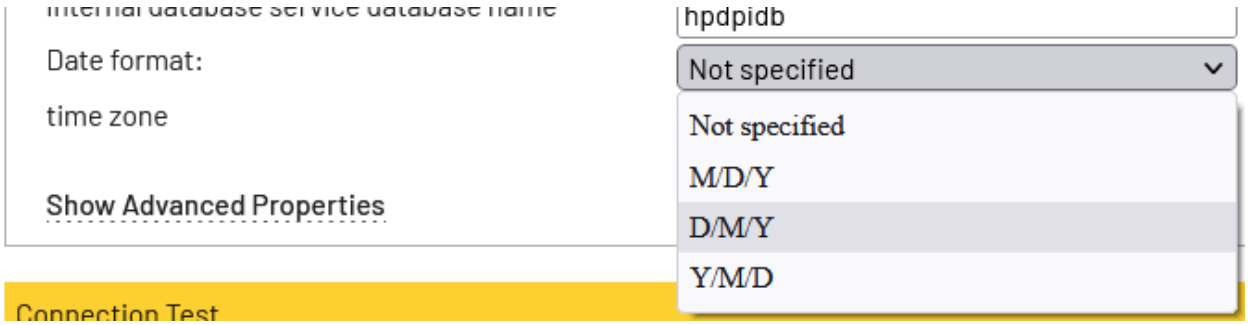
If your Data Protector server is receiving replications from another Data Protector server then there can be duplicate session IDs in the DP database. In Bocada 20.3.11 and earlier these duplicate session IDs will cause data collection to fail. There is a hotfix available for Bocada 20.3.11 that will continue collecting data after encountering a duplicate session ID, and later versions of Bocada will not need a hotfix. However, Bocada Data Collection will continue to log errors when it encounters a duplicate session ID. Please contact Micro Focus support to request a fix to eliminate duplicate session IDs in Data Protector.

Problem: Data Collection fails with: Cannot insert the value NULL into column 'createddate', table 'Bocada.dbo.medialog'; column does not allow nulls. INSERT fails.

If you Data Protector server is configured with non-US properties then then another setting may be needed. You can confirm this further by turning on logging, and doing a collection. You will see in the log file lines such as:

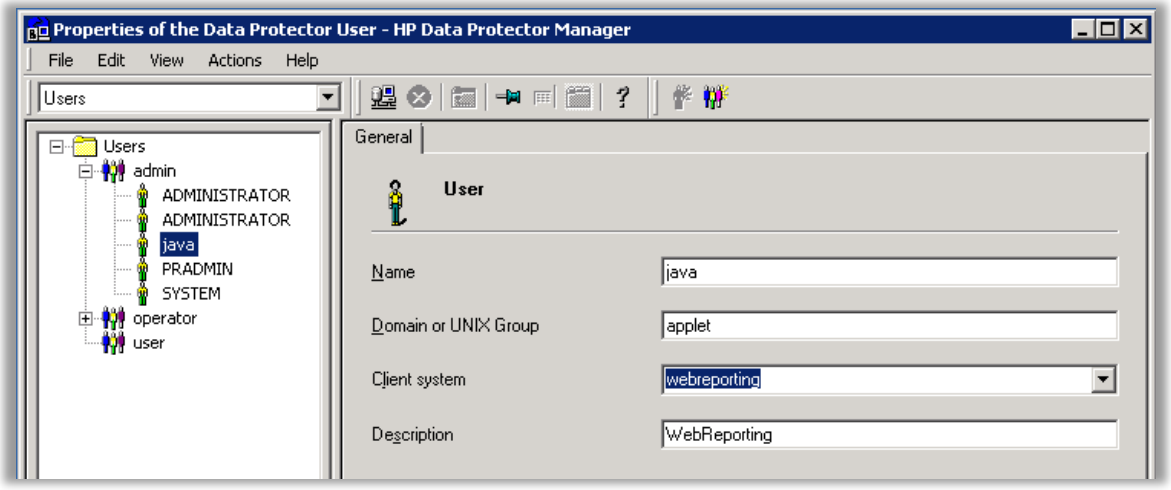
> *Could not parse Date and Time string 27/07/2021 08:04:54, System.FormatException: String was not recognized as a valid DateTime.*

Find the date format setting in the plugin properties and set it to the date format used in you system:



Appendix A: Data Protector Users

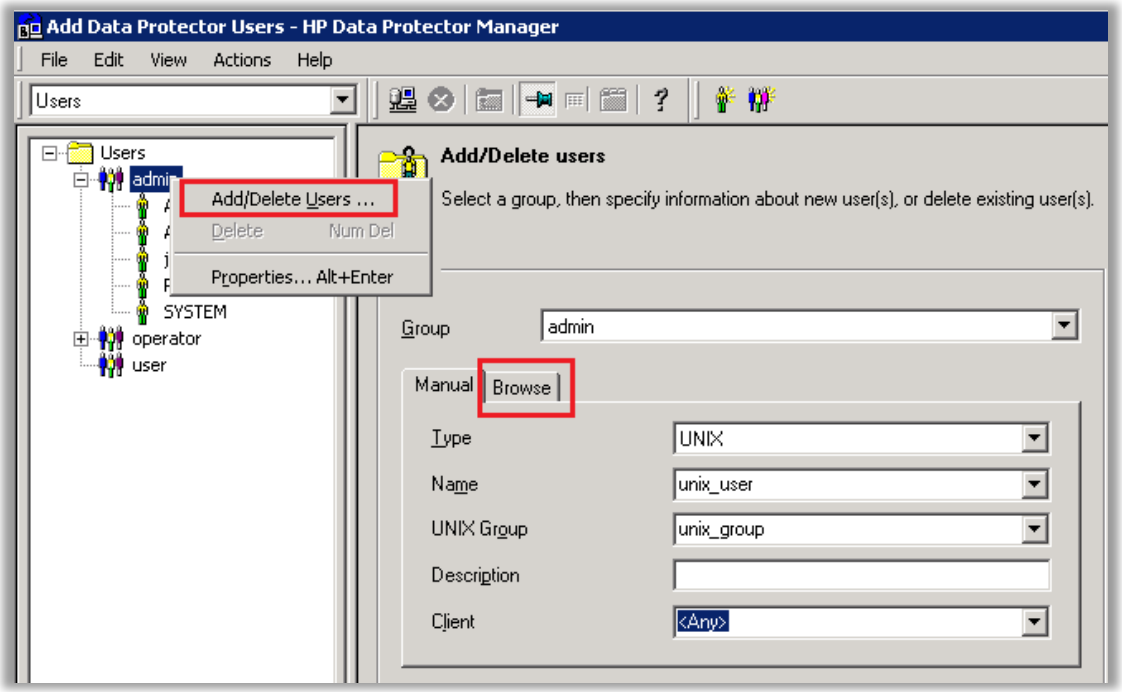
Data Protector users are created from the User section of the Data Protector Manager console:



Note: For security reasons the "applet\java" user account may have been deleted from the Cell Manager. Before using this account, determine that it is still valid. If this account is no longer present, the plug-in will need the Domain/Group and Name from another account with Admin permissions.

If a new account with Admin permissions needs to be created, this is done in Data Protector Manager as follows:

1. Select 'Users' from the top left pull-down menu.
2. Right-click on the 'admin' role to add an Admin user. This user may be Windows, UNIX, or LDAP:



It should not matter what *Type* of user is added, so long as that user has Admin permissions.

Appendix B: Legacy Backup Data Collection

Requirements

Valid only for Data Protector versions 9.0.x and older, this method uses low level protocol for backup metadata collection.

The Data Protector Plugin mines backup data by making requests to a Data Protector agent on the Data Protector Cell Manager using sockets. There are several high-level requests including:

1. Client information
2. Backup information
3. Version information
4. Licensing information
5. Status information (ping)

Port Configuration

The following illustrates the syntax for the variables OB2PORTRANGE and OB2PORTRANGESPEC found in the "omnirc.TMPL" file when the port range needs to be limited to a smaller, specific range through a firewall. Configuring the port range in these two variables forces OpenView Storage Data Protector to listen only to the specified port range (OB2PORTRANGE) and specifies the ports to which the agents or services use to listen (OB2PORTRANGESPEC). Set the variable OB2PORTRANGE as follows:

Data Protector Versions	Bocada Data Collection	Protocol or Daemon	Default Port	Direction	Notes
9.0x, 8.1.x	Backup	TCP	5555/TCP (*inetd*)		The listening port *inted* cannot share the same port with another application. If this port is in use, the Cell Manager will use a different port.
9.0x, 8.1x	Backup	TCP response port	Range of ports TCP and UDP	Inbound	Bocada initiates communication to Data Protector across the *inetd* port; however, response occurs from a range of ports. Data Protector will use ports dynamically from a range of 1025 – 65535 as specified in OB2PORTRANGE in the *omnirc* file.

All ports must be opened bi-directionally.

Syntax

OB2PORTRANGE=<start port>-<end port>

Example

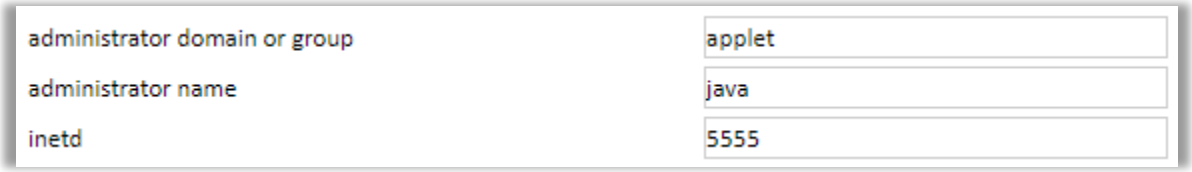
OB2PORTRANGE=40000-40030

Result

The following ports should be opened at the firewall:
40000 - 40030/TCP inbound

Bocada Legacy Updates

These properties are valid only for versions 9.0x and lower of Data Protector Cell Managers. These properties are being deprecated and we recommend utilizing the Server Command properties.



Administrator domain or group

This is required to communicate with the WebReporting feature of the Cell Manager. Enter the domain or group for a valid Cell Manager account. The default setting is domain "applet", which is for the WebReporting account automatically created during installation of Data Protector (see screenshot in Appendix A, below).

Administrator name

Enter the name of a valid Cell Manager User account with administrator rights. The default setting is "java", which is the WebReporting account automatically created during installation of Data Protector. For more information on user creation, please see Appendix A.

Inetd

Enter the port number used by the inetd daemon. Inetd is the daemon a Data Protector server uses to start processes within a backup cell. By default, inetd uses port number 5555. However, inetd cannot share the same port with another application. To avoid conflicts, the Data Protector server may use a port number other than the default.

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
Phone: +1-425-898-2400