BOCADA.

N2WS Backup & Recovery
(CPM Cloud Protection Manager)
Plugin Configuration Guide

Contents

N2WS (CPM) Configuration Checklist

Detailed preparation and installation steps are included below, this is an overview of the steps to configure N2WS (CPM) collections on your Bocada Data Collection Server:

- ☐ N2WS (CPM) API authentication key
- ☐ AWS Access key ID
- ☐ AWS Secret access key
- ☐ Ensure your Data Collection Server can reach the N2WS (CPM) Server
- ☐ Open Firewall Ports

Supported Collection Types

The plugin currently supports the following collection types from N2WS (CPM) servers, known as *nodes* in N2WS (CPM):

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 N2WS (CPM) data sources:
- N2WS (CPM) REST API
- AWS Rest API

Requirements

The following are required to collect data with the Bocada plugin for N2WS (CPM):

Access Keys
- N2WS (CPM) API authentication key (N2WS Delegate User)
- AWS Access key ID (AWS User with IAM N2WS Policies permission)
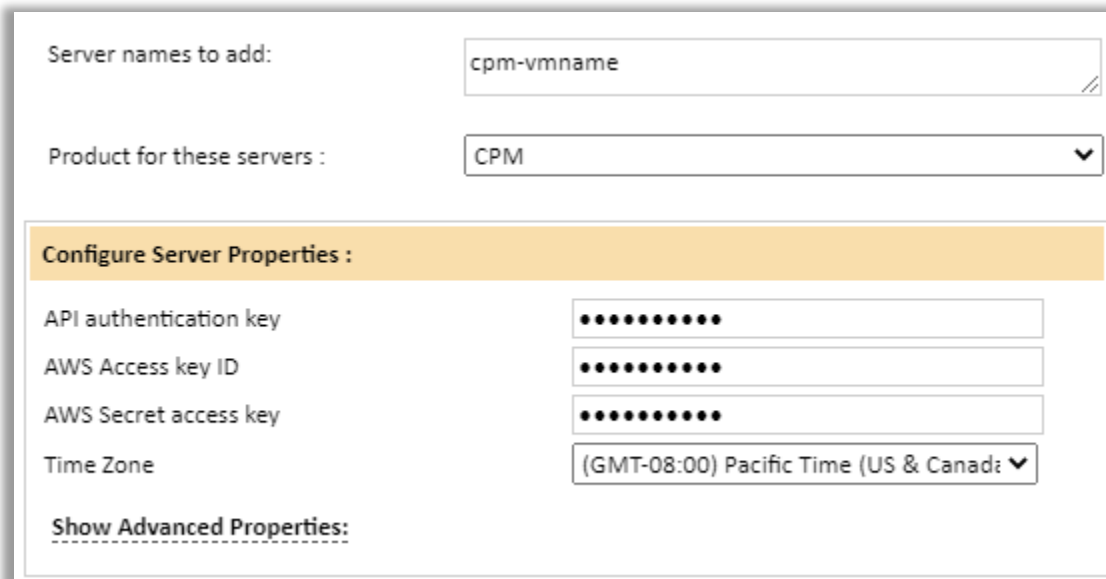- AWS Secret Access key (for above AWS Access Key ID)

Firewall Ports

The Bocada Data Collection Server must be able to connect to the N2WS (CPM) Server on these ports:

Service	Default Port	Note
HTTPS	443 TCP	-

Setup

Server Properties

Backup Server Properties determine how the plugin will interface with N2WS (CPM) and AWS and are managed through the Backup Servers view.

Field Definitions

Server names to add

Name or IP address of your N2WS (CPM) server
FQDN is recommended because the IP address could change during a N2WS (CPM) upgrade

API authentication key

Paste the N2WS (CPM) API Authentication Key captured from the N2WS (CPM) interface

AWS Access Key ID

Enter an Access Key ID with authorization to manage the N2WS (CPM) EC2 instance. For steps on confirming which AWS Access Key ID to use, Click here.

AWS Secret access key

Enter the Secret Access Key for the Access Key ID above. Please note, the secret access key can only be retrieved when the key is created.

Time Zone

Select the time zone where the N2WS (CPM) resides. This setting ensures times are displayed

consistently in environments that span multiple time zones.

Create N2WS (CPM) API Authentication Key

An API Authentication key is required from delegate user. This user should be a delegate of the user that which backup data will be collected. To create a new delegate user, following the steps below. If a delegate user is already created, skip to Create an API Authentication key.

Create a delegate user
1. Log into N2WS (CPM) server as root
2. Click users:

3. For the user's account that will be added to Bocada, click 'delegates':

4. Click "Add New Delegate" and update with the permission settings below:
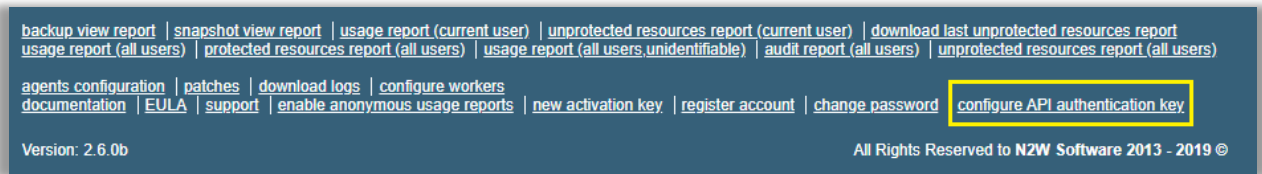
Create an API Authentication key:
1. Log into the N2WS (CPM) server as the delegate user, scroll to the bottom of the page
2. Click 'configure API authentication key'

3. If API Access is already Enabled and a Authentication Key is present, copy and paste this key into Bocada. If API Access is set to Disable, change this field to Enable and click "new authentication key". A pop-up will be displayed stating the old key will no longer be valid.   Click Ok. The Authentication Key will now be displayed on the screen. Copy and paste this key into Bocada.


Confirming AWS Access Key ID

The AWS Access Key ID and AWS Secret access key should be from a user within AWS that has the same Policy Permissions as the IAM role configured for the N2WS (CPM) Instance. To confirm, follow the steps below:

1. Log into AWS and navigate to EC2
2. Locate and select the N2WS (CPM) Instance
3. Under the Description Tab, click on the IAM role
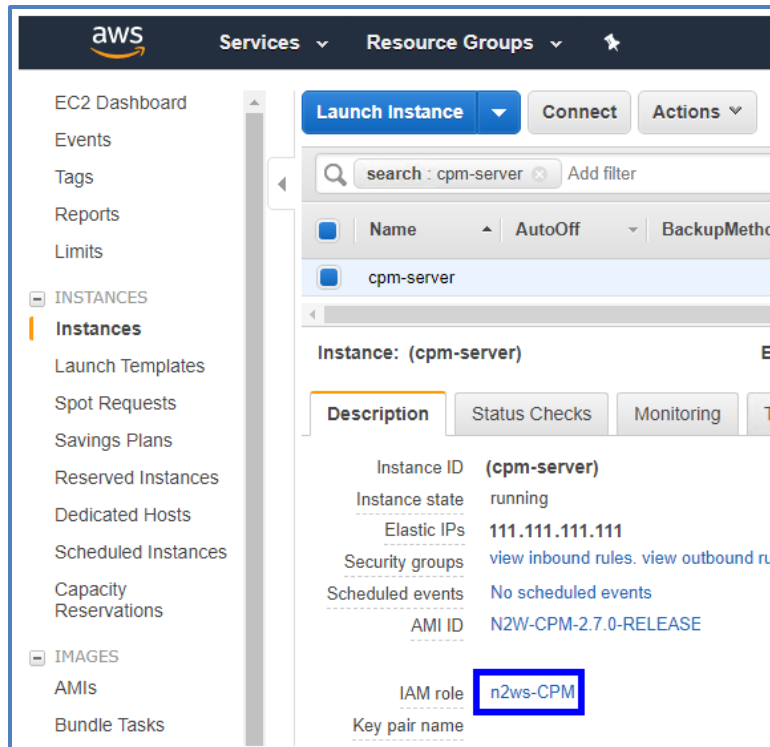
4. On the Roles Summary page, record the Policy Name/s used
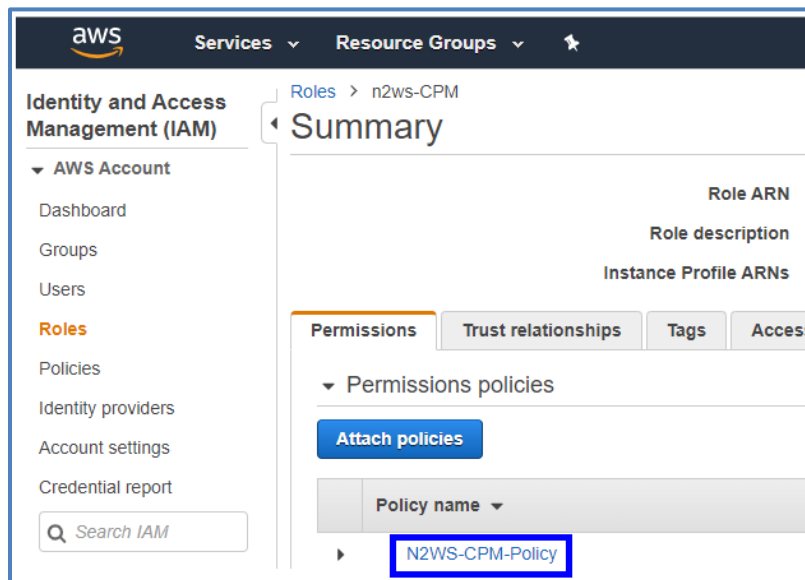
5. The AWS Access Key ID and AWS Secret access key should be from a user with the Policy names defined in step 4.

Reporting Notes

Some backup jobs will not have bytes associated with them.

CPM Plugin Configuration Guide

Technical Support

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

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