

**AWS Backup**

**Plugin Configuration Guide**

Contents

[Introduction 1](#_Toc1911595324)

[Supported Collection Types 2](#_Toc1566081823)

[AWS Configuration Checklist 2](#_Toc2026819113)

[Data Sources 3](#_Toc1774754722)

[Requirements 3](#_Toc847619368)

[AWS Ports 3](#_Toc1977048087)

[Network Connectivity 3](#_Toc1331885308)

[Bocada Setup 3](#_Toc871438726)

[IAM User – Collection for a Single AWS Account 4](#_Toc917191413)

[Server Properties 4](#_Toc1559482839)

[Field Definitions 4](#_Toc746355713)

[IAM Roles – Collection for Multiple AWS Accounts 5](#_Toc743125736)

[Server Properties 5](#_Toc1557266280)

[Field Definitions 5](#_Toc1849869158)

[Reporting Notes 5](#_Toc966578010)

[Troubleshooting 6](#_Toc234155022)

[Data Collection Fail – Error 545 6](#_Toc1966615705)

[Appendix A: Configure AWS User 7](#_Toc2965950)

[￼Appendix B: Configure IAM Role & Policy 8](#_Toc331410440)

[Additional Configuration 11](#_Toc340852625)

[Add the AssumeRole action to the Bocada-Policy 12](#_Toc186159541)

[For Each AWS Account 12](#_Toc183141876)

[Technical Support 13](#_Toc1313231650)

# Introduction

The Bocada plugin for AWS provides backup reporting for:

* + AWS Native Snapshots
    - EBS Volumes
    - EC2 Instances
    - RDS
    - DynamoDB
    - Redshift
    - FSx
  + AWS Backups
    - EBS Volumes
    - EC2 Instances
    - RDS
    - DynamoDB
    - EFS
    - Storage Gateway volumes

There are two ways to collect data from AWS accounts:

1. IAM User
   1. Collection from a single AWS account
   2. Bocada server running on any platform (on-prem, cloud, etc.)
   3. Supported for all Bocada versions
2. IAM Role assigned to an AWS EC2 Instance running Bocada
   1. Collection from multiple AWS accounts
   2. AWS Policy to govern IAM Role to assume access within each account
   3. Supported starting in Bocada version 21.12.3

# Supported Collection Types

The plugin currently supports the following collection types from AWS for Snapshot reporting:

|  |  |  |
| --- | --- | --- |
| **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 (occupancy), 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. |

# AWS Configuration Checklist

Detailed steps are in sections below. This checklist is an overview of the steps to configure AWS collections on your Bocada Data Collection Server:

Single AWS Account: IAM User

Verify IAM User exists with proper read-access to AWS Services

Have ready: Access Key ID & Secret Access Key for the above IAM User

Verify that your Bocada Data Collection server can reach <https://aws.amazon.com/>

Multiple AWS Accounts: IAM Roles

Verify IAM Role is assigned to the EC2 Instance where Bocada Data Collection is installed

Subnet that allows internet access via an Internet Gateway or a NAT Gateway.

Verify AWS Policy exists which will govern the Roles to assume access within multiple AWS Accounts

# Data Sources

The plugin relies on the AWS API via Amazon SDK (Software Development Kit) that handles the REST API calls to collect data.

# Requirements

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

## AWS Ports

|  |  |  |
| --- | --- | --- |
| **Service** | **Default Port** | **Note** |
| *HTTPS* | 443 | API connection through HTTPS. Specific Amazon URL is determined by the Amazon SDK. |

## Network Connectivity

* Bocada must communicate with public AWS APIs, so outbound connectivity to the Internet is required. This communication can be achieved by placing the instance in a public subnet with a public IP address, by assigning an Elastic IP to the instance, using a NAT instance or by using an Internet Gateway.
* RDP is used for the initial installation of Bocada. Allowing port 3389 for inbound traffic in the VPC Security group is required.

Allowing HTTP and/or HTTPS ports for inbound traffic in the VPC security group is required for access to the Bocada GUI

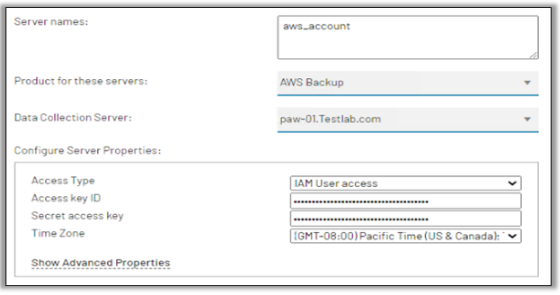
# Bocada Setup

## IAM User – Collection for a Single AWS Account

Supported for all Bocada versions, you will need an AWS Access Key ID & Secret Access Key for AWS API access to each AWS Account and Bocada will report only on what the Access Keys has permission to view. See [*Appendix A: How to set up AWS user for Bocada data mining*](#_Appendix_A:_How) for steps to create or modify an IAM User.

### Server Properties

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



### Field Definitions

#### Server name

This field can be any string token with letters, numbers, hyphen, underscore, and dot. No other special characters are allowed and capitalization will be ignored. Please use a name that can be easily identifiable for the AWS account that you are adding to Bocada.

#### Access Type

Select *IAM User access*

#### Access Key ID

For ‘IAM User access’, enter an Access Key ID with Read-only access to the services and resources you wish to report on. For steps on creating the Access Key ID, [click here](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey).

#### Secret access key

For ‘IAM User access’, enter the Secrete 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

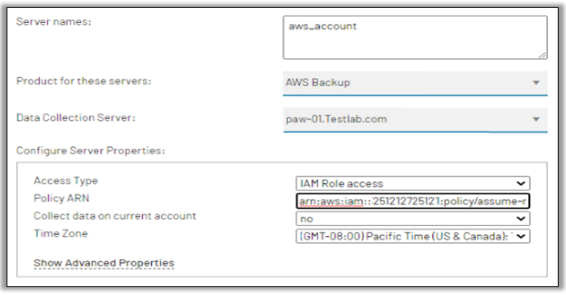
Select the time zone associated with the AWS account, if unsure leave as the default.

## IAM Roles – Collection for Multiple AWS Accounts

Supported starting in Bocada version 21.12.3, when running Bocada on an AWS Instance Bocada data collection leverages an IAM Role assigned to the instance to assume Roles across multiple AWS accounts provided by an AWS customer managed policy (using the Policy ARN). See [*Appendix B: Creating IAM Role & Policy*](#_Appendix_B:_Creating) for steps on how to configure the relevant IAM Role and Policy within AWS.

### Server Properties

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



### Field Definitions

#### Server name

This field can be any string token with letters, numbers, hyphen, underscore, and dot. No other special characters are allowed and capitalization will be ignored.

#### Access Type

Choose IAM Role access

#### Policy ARN

For ‘IAM Roles access’, enter Policy ARN where the policy defines all the accounts Bocada Data Collection can switch to and assume a new role. The IAM Role assigned to the Bocada instance in AWS requires read access to the policy to determine all the roles to assume within each account. This policy MUST be created as a customer managed policy.

#### Collect data on current account

Select ‘yes’ to enable collection on the AWS account in which the Bocada Data Collection server is running. Default is set to no.

# Reporting Notes

A few notes about AWS specific reporting in Bocada.

* *AWS Snapshots* is a dedicated report for AWS in Bocada under *Storage Monitoring* in Bocada.
* *AWS Unprotected, Protected, and All* are dedicated AWS reports for verifying AWS data is being backed up coverage under *Asset* *Protection*.
* AWS does not provide access to how much incremental data is being used by each backup snapshot. Only the capacity size for each snapshot is possible to mine, and that is what Bocada reports on.
* Bocada does not collect data for AWS Vault.
* Some Bocada fields to AWS field name mapping are in the below table.

|  |  |
| --- | --- |
| **Bocada Names** | **AWS Names** |
| Server or *Backup Server* | Name used when adding your AWS Account |
| Client or *Backup Client* | For EC2: NameTag (InstanceID) or InstanceID.  For RDS: DB Instance OR DB Cluster for Aurora.  For Dynamo DB: Table.  For Redshift: DB Cluster.  For FSx: File System.  For EBS: Volume. |
| Tag | VM Tag Name |
| Target or Asset | For EC2/EBS: NameTag (VolumeID) OR VolumeID.  For RDS: Engine EngineVersion.  For Dynamo DB: Table.  For Redshift: DB Name.  For FSx: File System. |
| Media Proprietary Type | AWS Service: e.g. DynamoDB, EBS, EC2, EFS, FSx, RDS, Storage Gateway |
| Job Group | Contains the AWS Account ID plus Region in which the resource resides. |

# Troubleshooting

## **Data Collection Fail – Error 545**

If you have the following conditions:

* Bocada release 22.1.2
* MSSQL Server 2012 or MSSQL Server 2014

Data collection fails with the error:

*Error 545: Cannot execute SQL statement [SQLSTATE=S0002] [Microsoft][SQL Server Native Client 11.0][SQL Server]Invalid object name 'STRING\_SPLIT'.*

*You need:*

* *get the hotfix* d381\_hotfix\_AWS\_Plugin\_Release\_22\_1\_2\_Sql2012\_2014.sql
* *Connect to your Bocada MS Sql Server Database with a username with dbo\_owner role in Bocada database.*
* *Run the script provided by the hotfix.*

# Appendix A: Configure AWS User

You will need an AWS user to be configured for Bocada to mine data from AWS.

Create a User and record Access Key ID and Secret Access Key

1. Log into the AWS account via your AWS Management Console:  
    <https://console.aws.amazon.com/>
2. In the page header, click on Services and search for IAM
3. From the left panel, click on Users
4. Click on Add User
5. Username = Bocada-Collector-User (or any user name)
6. Access type = Programmatic access
7. Click Next: Permissions
8. Set permissions = Attach existing policies directly
9. Assign policies for services which you want to report:

* AWS Backup
  + AWSBackupOperatorAccess
* AWS Native Snapshots
  + EC2 - AmazonEC2ReadOnlyAccess
  + RDS – AmazonRDSReadOnlyAccess
  + DynamoDB – AmazonDynamoDBReadOnlyAccess
  + Redshift – AmazonRedshiftReadOnlyAccess
  + FSx – AmazonFSxReadOnlyAccess
* Extra Logging for all backups
  + [AWSCloudTrailReadOnlyAccess](https://console.aws.amazon.com/iam/home?region=us-west-2#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSCloudTrailReadOnlyAccess)

1. Click Next: Tags
2. Add Tags (Optional) then click Next: Review
3. Click Create User
4. The next pages shows that the user was created successfully.
   1. Record the Access Key ID
   2. Record the Secret Access Key (Make sure you record this Secret Access key from this screen. **This is the ONLY time the Secret Access Key is visible**. If this key is lost, a new key will need to be generated)

To update an existing user

1. Log into your AWS account via the AWS Management Console

<https://console.aws.amazon.com/>

1. In the page header, click on Services and search for IAM
2. From the left panel, click on Users
3. In the main panel, click on the current user
4. Click Add Permissions
5. Click Attach existing policies directly
6. Assign policies for services which you want to report (see above for new user)
7. Click Next: Review
8. Click Add permission

# Appendix B: Configure IAM Role & Policy

The following steps are to create the required IAM Role, which is to be assigned to the Bocada Instance. The policy created in these steps must be created as a customer managed policy

1. In the AWS console, go to IAM
2. Under Access Management, click Policies, then click Create policy

Graphical user interface

Description automatically generated

1. Click on the JSON tab and replace everything in it with the [JSON code found here](https://bva.bocada.com/Docs/Bocada-IAM-Role.txt)

Text

Description automatically generated

1. Click Review Policy
2. Set Name to Bocada-Policy
3. Update Description as needed
4. Click Create policy
5. Copy the ARN of this policy as this will be needed during the Bocada Collection setup process
6. Back on the IAM main page, under Access management, click Roles. The click Create Role.

Graphical user interface, text, application

Description automatically generated

1. Under Select type of trust entity, select AWS service
2. Under Choose a use case, select EC2.

Graphical user interface, text, application, email

Description automatically generated

1. Click on Next: Permissions
2. In the filter policies, search for Bocada

Graphical user interface, text, application

Description automatically generated

1. Select Bocada-Policy and click Next: Tags
2. Add any needed Tags, then click Next: Review
3. Set Role name to Bocada-Role

Graphical user interface, text, application, email

Description automatically generated

1. Click Create role

## Additional Configuration

### Add the AssumeRole action to the Bocada-Policy

1. In the AWS console, go to IAM
2. Under Access Management, click Policies and search for Bocada
3. Click on the policy.
4. On the permissions tab, click edit policy
5. Click on the JSON tab and add the following lines of code between the 3rd and 4th line. Replace the 000000000000 and 000000000001 with the account numbers where collections are needed. There will be line entry for each required account:

{

"Effect": "Allow",

"Action": "sts:AssumeRole",

"Resource": [

"arn:aws:iam::000000000000:role/Bocada-Role",

"arn:aws:iam::000000000001:role/Bocada-Role"

]

},

1. Click Review Policy, then Save Changes

### For Each AWS Account

1. Log into each additional account
2. go to IAM
3. Under Access Management, click Policies, then click Create policy
4. Click on the JSON tab and replace everything in it with the [JSON code found here](https://bva.bocada.com/Docs/Bocada-IAM-Role.txt)
5. Click Next: Tags and add any required tags
6. Click Next: Review
7. Set Name to Bocada-Policy
8. Update Description as needed
9. Click Create policy
10. Back on the IAM main page, under Access management, click Roles. The click Create Role.
11. Under Select type of trust entity, select “Another AWS account”
12. Update the Account ID with the account where the Bocada instance is configured.
13. Both options should be left unchecked

Graphical user interface, text, application

Description automatically generated

1. Click on Next: Permissions
2. In the filter policies, search for Bocada

Graphical user interface, text, application

Description automatically generated

1. Select Bocada-Policy and click Next: Tags
2. Add any needed Tags, then click Next: Review
3. Set Role name to Bocada-Role
4. Click Create role

# 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:** <http://www.bocada.com/support/>

**Phone:** +1-425-898-2400