appviewX

AWS Process Discovery Solution Guide

Version: 2020.2.0

Copyright AppViewX, Inc.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Solution Guide AppViewX v20.2.0	May 2020

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Introduction

This documentation includes the problem statement, solution, and implementation of the AWS Process Discovery for windows instances.

Chapter 2: Problem Statement

User wants to automate the AppViewX to identify the instences and manage the certificate within the server. AppViewX must identify the windows instances that is deployed in the Amazon AWS cloud environment and manage the certificates within Amazon server.

Chapter 3: Solution

The Amazon AWS service, EC2 instances are integrated with AppViewX (under cloud inventory). Users can configure the S3 bucket and AWS account details in the AppViewX along with the regions to be scanned to establish communication. On successful configuration of the EC2 service accounts in AppViewX, windows instances running within the accounts are discovered by AppViewX. The regions are scanned and the total count of windows instances discovered is displayed in the cloud inventory.

The windows instance details and certificate discovery status will be auto-updated in the server instances. By default, AppViewX discovers and manages certificates at EC2 instances in the certificate inventory. The user can restrict the automatic certificate discovery, by configuring the Cert sync as Ignore.

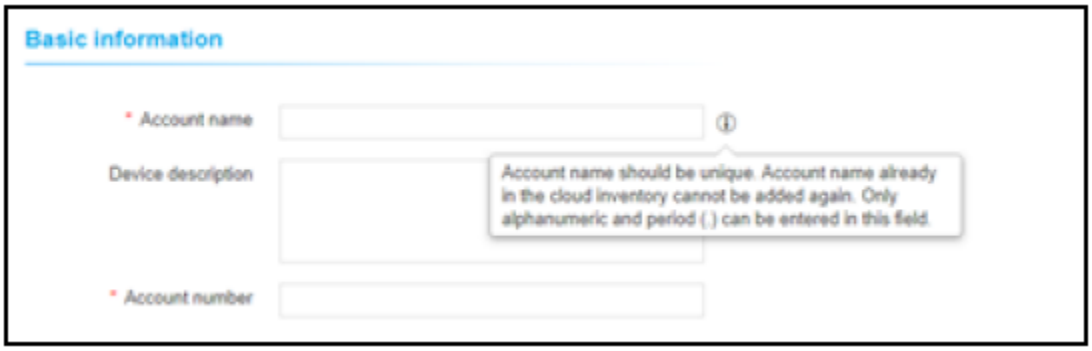
Chapter 4: Supported Server and Versions

A list of supported server and versions are mentioned in the table:

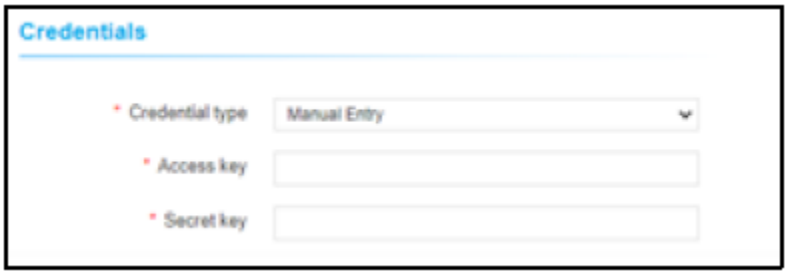
Server	Versions
Microsoft Windows	2012 R2 Standard
Microsoft Windows	2016
Microsoft Windows	2008 R2

Chapter 5: Implementation

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Inventory > Device > Cloud > Click "+" > AWS**.
4. On the AWS page, enter the details in the **Basic information, Credentials, Key information**, and **Additional attributes** sections.
5. Under the **Basic information** section, enter the **Account name** <*AppViewX ID*> that identifies the cloud account configured in AppViewX. The account name has to be unique, alphanumeric, and period (**.**) can be entered in this field. Enter the **Device description** and the AWS cloud **Account number** in which the EC2 service is active.

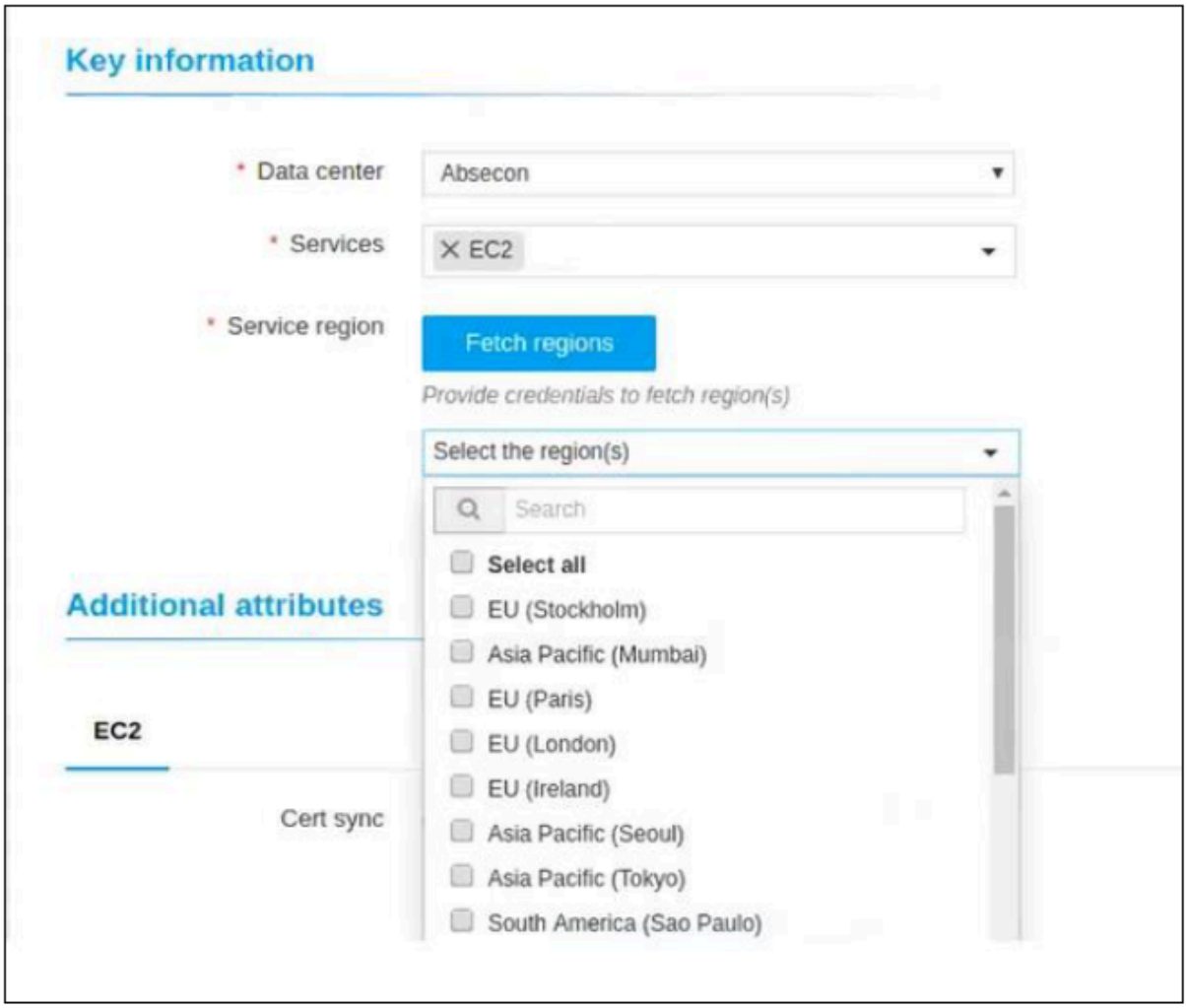


6. Under the **Credentials** section, enter the **Credential type, Access key,** and **Secret key**. You can store the credentials in CyperArk and share the CyperArk ID in AppViewX.



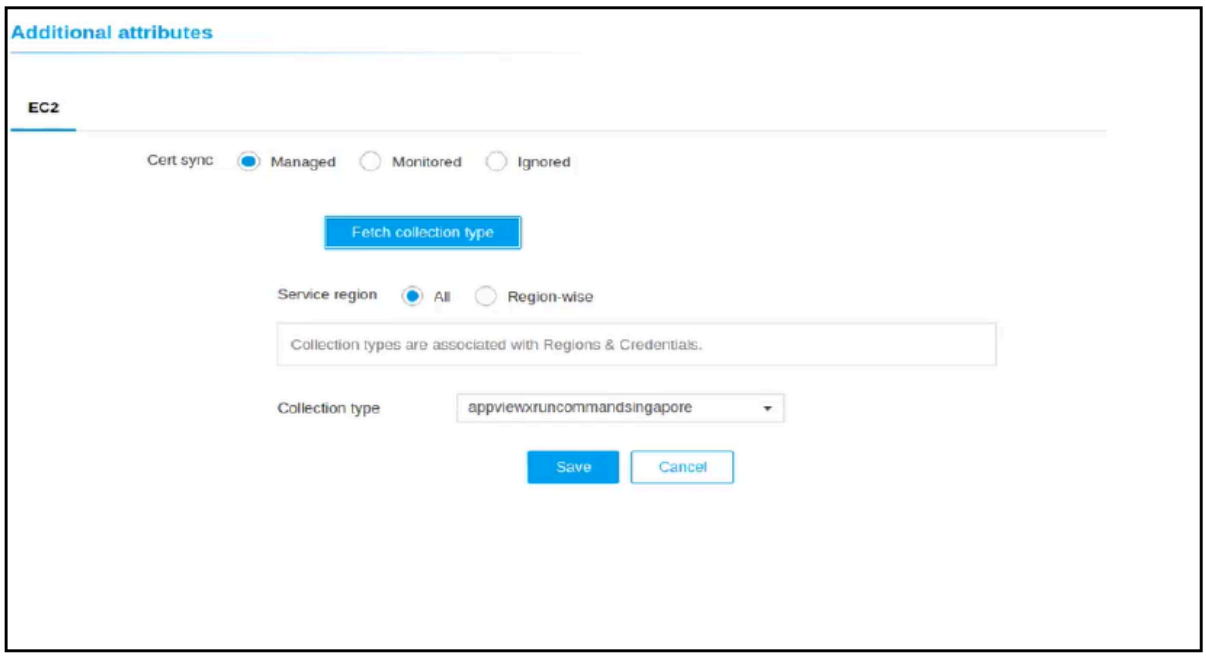
7. Under the **Key information** section, select the **Data center** and **Services** as **EC2**. In the **Service region**, the **Fetch regions** is triggered to retrieve all the region(s) associated with

the given account for instances. You can either select all regions (or) select specific regions.



8. Under the **Additional attributes** section, select **EC2**.
   - If the Cert sync is specified as **Managed,** CLM actions such as create, renew, revoke, and regenerate can be performed on the certificates.
   - If the Cert sync is specified as **Monitored,** no actions can be performed on the certificates. It helps to view and monitor the certificates.
   - If the Cert sync is specified as **Ignored,** the instances within the accounts are discovered.

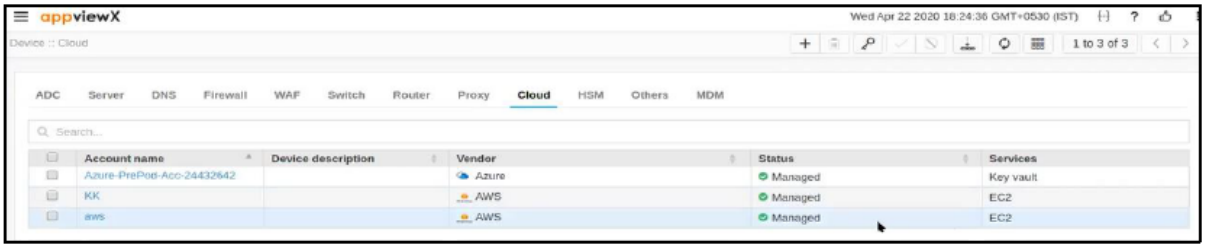
9. You should trigger the **Fetch collection type** to retrieve the S3 bucket.
   The **Service region** can be selected for all-region (or) specific region.

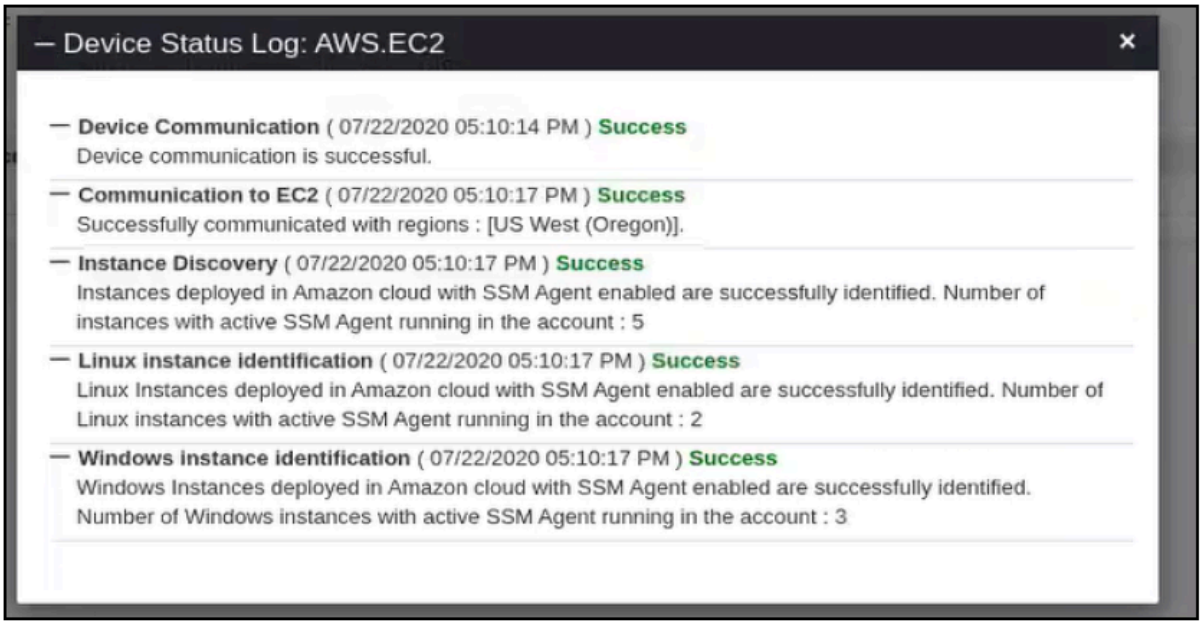


10. Click **Save**.
11. On submission, based on the credentials provided, AppViewX will scan for instances within the given regions.

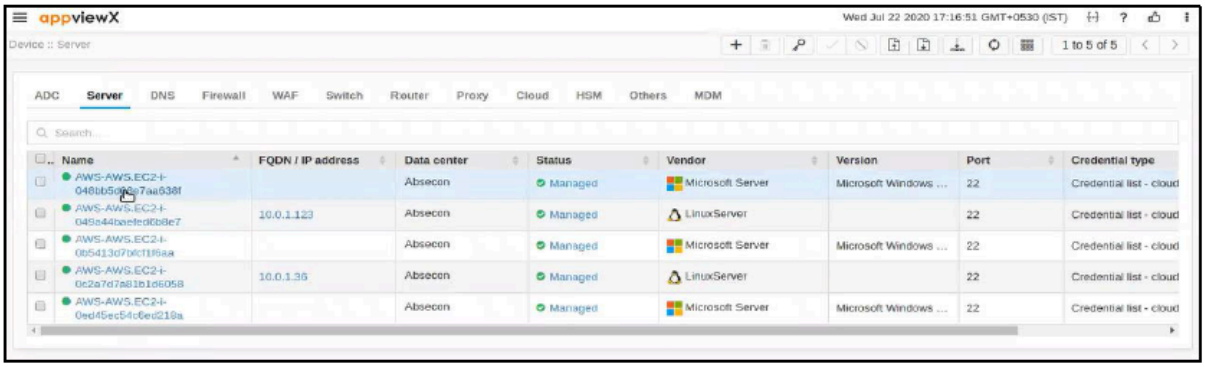
> **Note:** SSM agents should be actively running within the instances. And only the above mentioned version of the MS server will be discovered by AppViewX.

12. Once the scanning is completed successfully, you can view the summary log in the cloud inventory where the status is selected.





13. Go to **Menu > Inventory > Device > Server** and view the instances that are discovered from the AWS account.



14. Once the instances are automatically added to the server inventory, you can view the instance summary in the server inventory.
15. Click the server name to view the instances ID, regions, and so on within the server form. The credentials provided for the cloud account can be used for the instances.

> **Note:** Instance credentials and cloud acco unt credentials should be the same, if they are different, then the discovered instances will be added in the server inventory as unresolved.

16. If the credentials for the instances are changed after Process discovery, you can edit the credentials in the server form.
17. By default, the auto-discovery process enables the proxy for communication.
18. If the default proxy is set in the general setting, and then AppViewX proxy takes precedence for establishing communication.
19. By default, AppViewX is set up to scan for certificates only in *<c:/ drive>*. This setup is recommended to avoid performance issues that helps to add additional locations by editing the server form and clicking **config fetch**.
20. Enter the details, and click **Save**.