



AWS Process Discovery Solution Guide

Version: 2020.2.0

Copyright AppViewX, Inc.

Copyright © 2020 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

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).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Copyright AppViewX, Inc.....	ii
Copyright © 2020 AppViewX, Inc. All Rights Reserved.....	ii
Trademarks.....	ii
External Reference Links.....	ii
Contact Information.....	ii
Preface.....	iv
Revision History.....	iv
Text Conventions.....	iv
Chapter 1. Introduction.....	5
Chapter 2. Problem Statement.....	6
Chapter 3. Solution.....	7
Chapter 4. Supported Server and Versions.....	8
Chapter 5. Implementation.....	9

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	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 instances 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.

Basic information

* Account name ⓘ

Device description

* Account number

Account name should be unique. Account name already in the cloud inventory cannot be added again. Only alphanumeric and period (.) can be entered in this field.

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.

Credentials

* Credential type

* Access key

* Secret key

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.

The screenshot displays a configuration interface with two main sections: **Key information** and **Additional attributes**.

Key information section:

- Data center:** A dropdown menu with 'Absecon' selected.
- Services:** A dropdown menu with 'X EC2' selected.
- Service region:** A dropdown menu with 'Fetch regions' selected. Below it is a blue button labeled 'Fetch regions' and the text 'Provide credentials to fetch region(s)'.

Additional attributes section:

- EC2:** A dropdown menu with 'EC2' selected.
- Cert sync:** A dropdown menu.

A modal window titled 'Select the region(s)' is open, showing a search bar and a list of regions with checkboxes:

- Select all
- EU (Stockholm)
- Asia Pacific (Mumbai)
- EU (Paris)
- EU (London)
- EU (Ireland)
- Asia Pacific (Seoul)
- Asia Pacific (Tokyo)
- South America (Sao Paulo)

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.

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

Additional attributes

EC2

Cert sync: Managed Monitored Ignored

Fetch collection type

Service region: All Region-wise

Collection types are associated with Regions & Credentials.

Collection type: appviewxruncommandsingapore

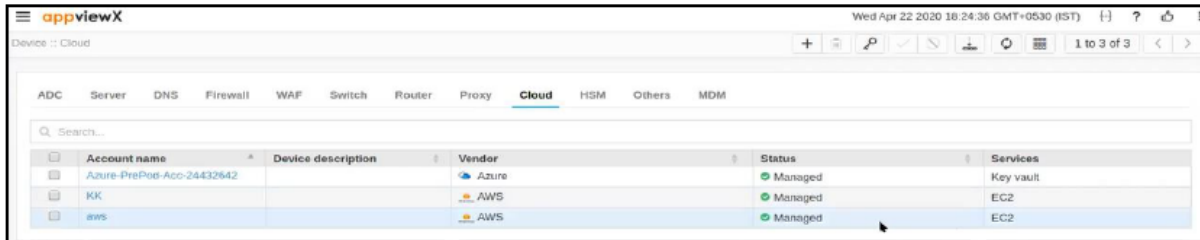
Save **Cancel**

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

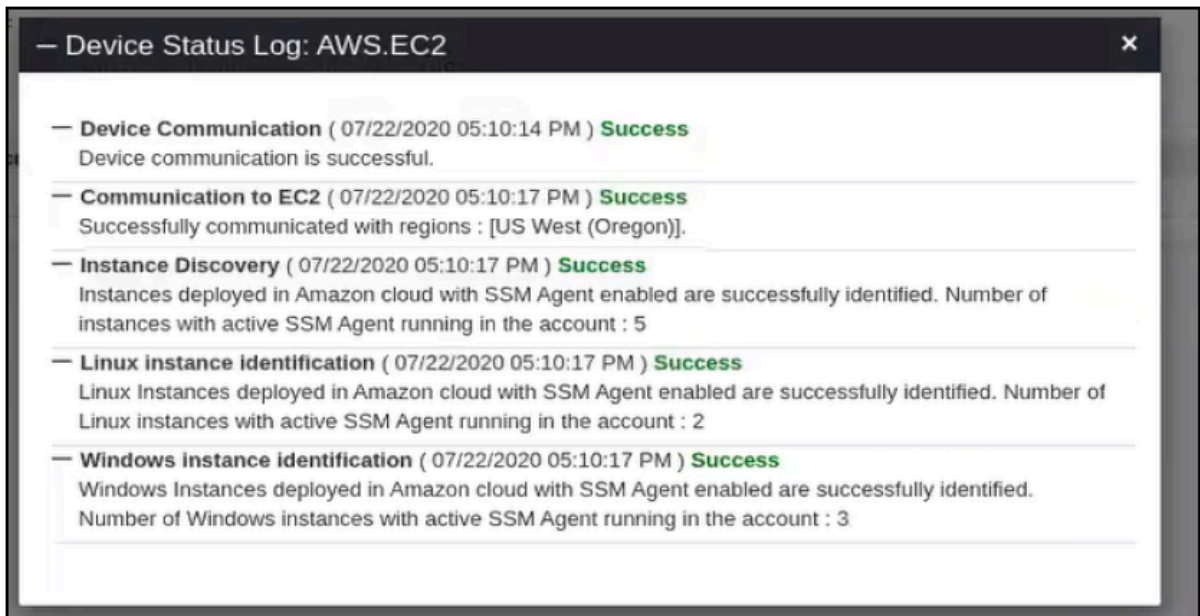


Note: SSM agents should be actively running within the instances. And only the above mentioned version of the MS server will be discovered by AppViewX.

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



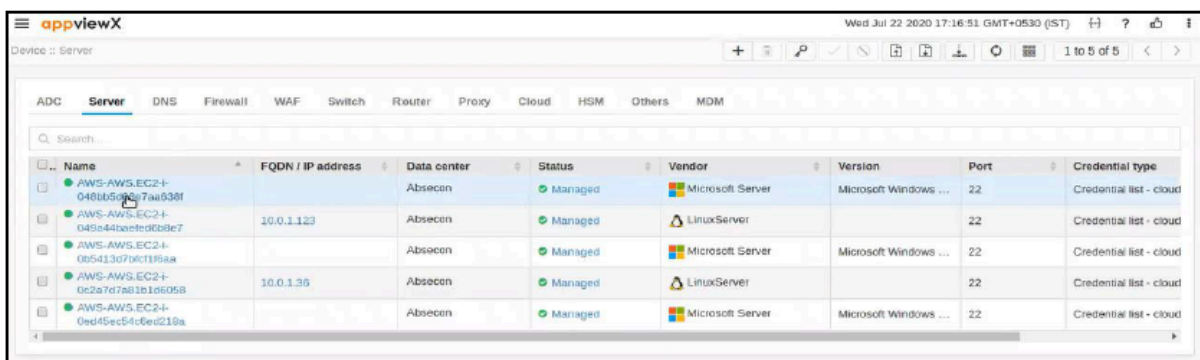
Account name	Device description	Vendor	Status	Services
Azure-PreProd-Acc-24432642		Azure	Managed	Key vault
KK		AWS	Managed	EC2
aws		AWS	Managed	EC2



— Device Status Log: AWS.EC2

- Device Communication (07/22/2020 05:10:14 PM) Success**
Device communication is successful.
- Communication to EC2 (07/22/2020 05:10:17 PM) Success**
Successfully communicated with regions : [US West (Oregon)].
- Instance Discovery (07/22/2020 05:10:17 PM) Success**
Instances deployed in Amazon cloud with SSM Agent enabled are successfully identified. Number of instances with active SSM Agent running in the account : 5
- Linux instance identification (07/22/2020 05:10:17 PM) Success**
Linux Instances deployed in Amazon cloud with SSM Agent enabled are successfully identified. Number of Linux instances with active SSM Agent running in the account : 2
- Windows instance identification (07/22/2020 05:10:17 PM) Success**
Windows Instances deployed in Amazon cloud with SSM Agent enabled are successfully identified. Number of Windows instances with active SSM Agent running in the account : 3

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



Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
AWS-AWS.EC2-I-048b6509c77aa638f		Absecon	Managed	Microsoft Server	Microsoft Windows ...	22	Credential list - cloud
AWS-AWS.EC2-I-045c442aeed0bde7	10.0.1.123	Absecon	Managed	LinuxServer		22	Credential list - cloud
AWS-AWS.EC2-I-0e5413d77xct119aa		Absecon	Managed	Microsoft Server	Microsoft Windows ...	22	Credential list - cloud
AWS-AWS.EC2-I-0c2a7d7a83b1a605a	10.0.1.35	Absecon	Managed	LinuxServer		22	Credential list - cloud
AWS-AWS.EC2-I-0ed45ec54c6ec218a		Absecon	Managed	Microsoft Server	Microsoft Windows ...	22	Credential list - cloud

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 account 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**.

appviewX Wed Jul 22 2020 17:23:28 GMT+0530 (IST)

Device: Server > Modify

Microsoft Server

Server name: AWS-AWS-EC2-i-048b5d9e7aa638f

Data center: Abacoan

Communication mode: Gateway SSM

Hostname: 100.1.238

Cert sync: Managed Monitored Ignored

Credentials

Credential type: Credential List - CloudAccount

Account name: AWS-EC2

Vendor Specific Details

Region: us-west-2

Instance id: i-048b5d9e7aa638f

SSM document name: AWS-RunPowerShellScript

SSM document version: 1

S3 bucket name: appviewxuncommandingsingapore

Proxy required:

Certificate details

Certificate location: C:

Password: *****

Add

Certificate location	Delete
C:	

Save Cancel