AWS S3 and CloudWatch Integration with Catalyst 9000 Series Switches

Amazon Simple Storage Service (S3) is a service that provides a scalable storage infrastructure through a web service interface.

Amazon Web Services (AWS) CloudWatch, is a monitoring and logging service that provides data that enables you to understand, optimize, and enhance the performance of your applications, systems, and services.

This module describes how to integrate AWS S3 and CloudWatch with Cisco Catalyst 9000 Series Switches.

- Prerequisites for the AWS S3 and CloudWatch Integration, on page 1
- Guidelines for the AWS S3 and CloudWatch Integration, on page 2
- AWS S3 Integration, on page 2
- CloudWatch Integration, on page 2
- Integrating AWS S3 with Cisco Devices, on page 3
- Integrating AWS CloudWatch Profile with Cisco Devices, on page 5
- Verifying the AWS S3 and Cloudwatch Integration, on page 7
- Feature History for AWS S3 and CloudWatch Integration, on page 8

Prerequisites for the AWS S3 and CloudWatch Integration

Ensure that the prerequisites are complete before integrating AWS S3 and CloudWatch with Catalyst 9000 Series Switches.

- Create a CloudWatch group and streams in AWS.
- Create access credentials in AWS.
- Ensure that you have the AWS Identity and Access Management (IAM) access key ID and the secret key.
- Ensure that cloud filesystems have network interfaces and cloud reachability.
- Set a private configuration key for password encryption

For information about how to create CloudWatch group and streams, see the AWS documentation at: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Guidelines for the AWS S3 and CloudWatch Integration

Refer to the guidelines before integrating AWS S3 and CloudWatch with Catalyst 9000 Series Switches.

- The cloud storage is accessible only to the active device.
- Cloud reachability can be established through any service port, including device management ports, or forwarding interfaces on the device.
- Multiple cloud storage configuration profiles can be created for the same S3 bucket with different configuration parameters.
- Virtual device instances hosted on the AWS cloud can use the IAM role infrastructure to access the S3 storage.

AWS S3 Integration

The AWS S3 provides a scalable storage infrastructure through a web service interface. Using AWS S3, you can seamlessly supplement the built-in persistent storage on Cisco devices with the cloud-based storage.

With AWS S3, network administrators can mount an S3 bucket to the device memory. The S3 bucket enables easy distribution of software images, software maintenance upgrades (SMUs), and scripts to multiple devices without any disruptions. Network administrators can also create, edit, and delete the cloud storage instance using Amazon S3 buckets, and make them accessible as part of the bootflash.

The AWS S3 integration addresses the need for increased storage capacity by providing a reliable cloud-storage solution. It also enhances the existing onboard storage by seamlessly incorporating cloud-based storage solutions.

CloudWatch Integration

AWS CloudWatch is a monitoring and logging service that provides data, which enables you to understand, optimize, and enhance the performance of your applications, systems, and services.

Syslog monitoring and management is essential to maintain the optimal network performance, enhance security, and minimize network downtime. Traditional syslog management approaches, may not be capable of governing the volume of logs generated by a growing organization. The integration of CloudWatch with Cisco Catalyst 9000 Series Switches allows you to gain insights into applications, resources, and services that run on the AWS infrastructure. It provides a centralized monitoring of the network performance, and collects, analyzes, and derives value from this data across network devices; devices distributed across multiple branch and campus locations.

CloudWatch collects

- internal system-level metrics from the Amazon Elastic Cloud Compute (Amazon EC2) instances across operating systems and
- system-level metrics from on-premise devices.

Benefits of AWS CloudWatch Integration

The AWS CloudWatch integration with Cisco Catalyst 9000 Series Switches provides various benefits.

- Unified management experience: Allows you to collect and store logs from AWS services, on-prem services, and from other clouds. All device logs are consolidated into a single location that facilitates easy event monitoring and seamless action using the cloud services tools.

  This unified approach simplifies the monitoring of your hybrid infrastructure.

- Enhanced operational efficiency and resource optimization: Provides the option to automate the processes and set alarms for events or logs.

- Analyze data and gather insights from syslogs: Facilitates the analysis and visualization of logs, which helps you to take appropriate actions. It also enables you to create graphs and correlate the log patterns in single dashboard. This dashboard provides a comprehensive view for informed decision-making and quicker troubleshooting.

  The logs or data is stored in a persistent storage in the AWS platform, and helps in the in-depth analysis of network trends over a period of time. This data can also help identify long-term performance issues, plan capacity upgrades, and optimize network configurations. The analysis of historical data helps to forecast future needs, and ensure that the network can scale with the growth of the organization.

- Automated responses: CloudWatch can be configured to automatically respond to certain conditions. For example, if a specific performance threshold is breached, CloudWatch can initiate predefined actions, such as, executing scripts or sending notifications. This level of automation reduces manual intervention and accelerates response time.

- Compliance and security: Syslog messages sent from the Cisco Catalyst devices to CloudWatch are encrypted with Transport Layer Security (TLS) 1.2 that ensures data confidentiality. AWS Identity and Access Management (IAM) controls grant granular access management, and the data protection policies safeguard sensitive information.

Integrating AWS S3 with Cisco Devices

Perform this task to integrate AWS S3 with Catalyst 9000 Series Switches.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**cloud-services aws s3** *profile-name*	Configures an AWS S3 cloud services profile, and enters S3 profile configuration mode. • Only use alphanumeric characters for the profile name. Underscore (_) is the only special character that is supported.

	Command or Action	Purpose
Step 4	**bucket** *bucket-name* **mount-point** *mount-point*	Configures the AWS S3 storage bucket and the mountpoint. • A bucket is a container for objects stored in AWS S3. The mountpoint refers to the directory on your local file system where you mount the AWS S3 bucket. • The bucket is mounted in a directory with the given *profile-name* configured in Step 3, in the cloudfs directory.
Step 5	**description** *profile-description*	(Optional) Adds a description to the AWS S3 cloud services profile. • The *profile-description* argument supports up to 255 alphanumeric characters.
Step 6	**vrf** *mgmt-intf*	Configures the virtual routing and forwarding (VRF) management interface. • Configure this command for the AWS S3 bucket to be accessible over the service port (or the device management port).
Step 7	**access-key key-id** *key-id* **secret-key** {**0** | **8**} *secret-access-key*	Configures the IAM access key-id and secret to access the S3 bucket. • Use the same access key ID and the secret key created for the IAM role on the AWS console. • If any of these parameters are changed, it will result in the restart of the s3fs instance.
Step 8	**permissions** {**read-only** | **read-write**}	(Optional) Sets the AWS S3 bucket permission as read and write. By default, read-only permission is enabled.
Step 9	**region** *region*	Specifies the AWS S3 region where the cloud-based storage resides. • Changing the region will result in access disruption.
Step 10	**proxy** {**http-server** | **https-server**} *url-IP port-number*	(Optional) Configures an HTTP or HTTPS server URL, or IP address, and port details.
Step 11	**no shutdown**	Enables the AWS S3 profile.

	Command or Action	Purpose
		• When the profile is shutdown, the S3 bucket instance will not be available.
Step 12	**end**	Exits S3 profile configuration mode and returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# cloud-services aws s3 profile c9k_XT_HD
Device(config-s3fs-profile)# bucket c9k-B1 mount-point s3-mount
Device(config-s3fs-profile)# description c9k-External-Storage
Device(config-s3fs-profile)# vrf mgmt-Intf
Device(config-s3fs-profile)# access-key key-id iam-key-id secret-key 0 ******
Device(config-s3fs-profile)# permissions read-write
Device(config-s3fs-profile)# region us-west-1
Device(config-s3fs-profile)# proxy https-server 192.0.2.1 port 12
Device(config-s3fs-profile)# no shutdown
Device(config-s3fs-profile)# exit
Device#
```

Integrating AWS CloudWatch Profile with Cisco Devices

Perform this task to integrate an AWS CloudWatch profile with Cisco devices.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**cloud-services aws cloudwatch profile** *profile-name*	Configures an AWS CloudWatch profile, and enters CloudWatch profile configuration mode.
Step 4	**log group-name** *group-name* **stream-name** *stream-name* [**file-path** *file-path*]	Specifies the AWS CloudWatch log group name, log stream name, and an optional log file path. • If the log-file path is not provided, the default syslog path (/bootflash/syslog/*) is used. • The log-file path, if specified, need not be the same as the buffered logging

	Command or Action	Purpose
		persistent storage path directory or file name. • The log group and log stream used here must be the same as those created on the AWS CloudWatch server.
Step 5	**description** *profile-description*	(Optional) Adds a description to the AWS CloudWatch profile.
Step 6	**proxy** {**http-server** | **https-server**} *url-IP* **port** *port-number*	(Optional) Configures an HTTP or HTTPS server URL or IP address, and port details.
Step 7	**vrf mgmt-intf**	(Optional) Configures the management interface as the VRF interface. • Configure this command, if the agent traffic has to be sent through the management interface. By default, data-port interface is used. • Do not use this command when the management interface is not available.
Step 8	**access-key key-id** *iam-id* **secret-key** {**0** | **8**} *secret-key*	Configures the AWS CloudWatch access credentials. • Use the same access key ID and secret key created for the IAM user on the AWS console.
Step 9	**region** *region*	Specifies the AWS region where CloudWatch server is running on the cloud provider.
Step 10	**no shutdown**	Saves the configuration and enables it for AWS CloudWatch services.
Step 11	**end**	Exits CloudWatch profile configuration mode and returns to privileged EXEC mode.

Example

This example shows how to integrate an AWS CloudWatch profile with Cisco devices.

```
Device> enable
Device# configure terminal
Device(config)# cloud-services aws cloudwatch profile test-profile
Device(config-cloudwatch-profile)# log group-name
techgroup stream-name techstream file-path /home/test/statusReport
Device(config-cloudwatch-profile)# description test-c9k
Device(config-cloudwatch-profile)# proxy https-server 192.0.2.1 port 12
Device(config-cloudwatch-profile)# vrf mgmt-Intf
```

```
Device(config-cloudwatch-profile)# access-key key-id iam-key-id secret-key 0 ******
Device(config-cloudwatch-profile)# region us-west-1
Device(config-cloudwatch-profile)# no shutdown
Device(config-cloudwatch-profile)# end
Device#
```

Verifying the AWS S3 and Cloudwatch Integration

You can use **show** commands to verify your configuration.

The output of the **show cloud-services aws s3 summary** displays a summary of all the AWS S3 profiles.

```
Device# show cloud-services aws s3 summary

Profile Name                      Profile Status  Service Status
-------------------------------------------------------------------
test                              Started         Active

test2                             Started         Active
```

The output of the **show cloud-services aws s3 profile s1** displays the operational information of the configured AWS S3 profile.

```
Device# show cloud-services aws s3 profile s1

Profile Details

Profile Name          : s1
Bucket Name           : pb-s3-test1
Mount Point           : test
Bucket Permission     : Read-Only
Region                : us-west-1
VRF                   : Global

S3 Service Details

Service Status        : Active
Service PID           : 31934
Mount Time            : 09/28/23 17:06:25
Service Log Level     : Notice
```

The output of the **show cloud-services aws cloudwatch summary** displays a summary of all the CloudWatch profiles.

```
Device# show cloud-services aws cloudwatch summary

Profile Name                      Profile Status  Service Status
-------------------------------------------------------------------
demo3                             Started         Active

demo4                             Started         Active
```

The output of the **show cloud-services aws cloudwatch profile demo3** displays the operational information of the configured CloudWatch profile.

```
Device# show cloud-services aws cloudwatch profile demo3

Profile Details

Profile Name          : demo3
```

```
VRF                  : Global
Region               : ap-northeast-1

CloudWatch Service Details

Service Status       : Active
Service PID          : 31785
Service Log Level    : Notice

Log Details

Log Group Name                          Log Stream Name               Log File

-------------------------------------------------------------------------------
test                                    katar2
```

Feature History for AWS S3 and CloudWatch Integration

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE 17.15.1	AWS S3 and CloudWatch Integration with Catalyst 9000 Series Switches	AWS S3 and CloudWatch are integrated with Cisco Catalyst devices to provide a scalable storage infrastructure and a monitoring and logging service, respectively. In Cisco IOS XE 17.15.1, this feature was introduced on the following platforms: • Cisco Catalyst 9300 Series Switches