



Getting started with Cloud Compliance for Amazon S3

Cloud Manager

Ben Cammett, Tom Onacki
June 15, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_scanning_s3.html on June 15, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Getting started with Cloud Compliance for Amazon S3 1
 - Pricing 1
 - Quick start 1
 - Reviewing prerequisites 2
 - Subscribing from the AWS Marketplace 6
 - Enabling Cloud Compliance 7
 - Configuring buckets 8
 - Scanning buckets from additional AWS accounts 10

Getting started with Cloud Compliance for Amazon S3

Cloud Compliance can scan your Amazon S3 buckets to identify the personal and sensitive data that resides in S3 object storage. Cloud Compliance can scan any bucket in the account, regardless if it was created for a NetApp solution.

Pricing

You need to pay to scan your Amazon S3 buckets. [Learn about pricing.](#)

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends. [Learn how to subscribe.](#)

Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.



Deploy Cloud Manager in AWS

If you haven't already done so, log in to [Cloud Central](#) and deploy Cloud Manager in AWS.

Cloud Manager automatically discovers the S3 buckets in this AWS account and displays them in an Amazon S3 working environment.



Set up your cloud environment

Ensure that your cloud environment can meet the requirements for Cloud Compliance, which includes preparing an IAM role, setting up connectivity from Cloud Compliance to S3, and more. [See the complete list.](#)



Subscribe from the AWS Marketplace

A subscription to the AWS Marketplace is required to scan Amazon S3 after the 30-day free trial ends.

Click **Settings > Credentials** and click **Add Subscription** for the Instance Profile.



Enable Cloud Compliance

Select the Amazon S3 working environment, click **Enable Compliance**, and select an IAM role that includes the required permissions.



Configure buckets

Select the buckets that you'd like to scan and Cloud Compliance will start scanning them.

Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

Requirements specific to S3

The first two requirements are specific to scanning S3 buckets.

Set up an IAM role for the Cloud Compliance instance

Cloud Compliance needs permissions to connect to the S3 buckets in your account and to scan them. Set up an IAM role that includes the permissions listed below. Cloud Manager prompts you to select an IAM role when you enable Cloud Compliance on the Amazon S3 working environment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Provide connectivity from Cloud Compliance to Amazon S3

Cloud Compliance needs a connection to Amazon S3. The best way to provide that connection is through a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Compliance instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Compliance can't connect to the S3 service.

If you experience any issues, see [AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?](#)

An alternative is to provide the connection by using a NAT Gateway.



You can't use a proxy to get to S3 over the internet.

General requirements

The requirements in this section apply to Cloud Compliance in general, whether you're scanning Amazon S3, Cloud Volumes ONTAP, or Azure NetApp Files. If you've already enabled Cloud Compliance (for Cloud Volumes ONTAP or Azure NetApp Files), then you can skip these requirements and [Subscribe from the AWS Marketplace](#).

Enable outbound internet access

Cloud Compliance requires outbound internet access. If your virtual network uses a proxy server for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints. Note that Cloud Manager deploys the Cloud Compliance instance in the same subnet as Cloud Manager.

Endpoints	Purpose
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Provides access to software images, manifests, and templates.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Compliance instance. You can find the latest Cloud Manager permissions in [the policies provided by NetApp](#).

Check your vCPU limits

Ensure that your cloud provider's vCPU limit allows for the deployment of an instance with 16 cores. You'll need to verify the vCPU limit for the relevant instance family in the region where Cloud Manager is running.

In AWS, the instance family is *On-Demand Standard instances*. In Azure, the instance family is

Standard DSv3 Family.

For more details on vCPU limits, see the following:

- [AWS documentation: Amazon EC2 Service Limits](#)
- [Azure documentation: Virtual machine vCPU quotas](#)

Ensure that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and the Cloud Compliance instance:

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

This connection enables deployment of the Cloud Compliance instance and enables you to view information in the Compliance tab.

- If your AWS network doesn't use a NAT or proxy for internet access, modify the security group for Cloud Manager to allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

This is required because the Cloud Compliance instance uses Cloud Manager as a proxy to access the internet.



This port is open by default on all new Cloud Manager instances, starting with version 3.7.5. It's not open on Cloud Manager instances created prior to that.

Ensure that you can keep Cloud Compliance running

The Cloud Compliance instance needs to stay on to continuously scan your data.

Ensure web browser connectivity to Cloud Compliance

After Cloud Compliance is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Cloud Compliance instance.

The Cloud Compliance instance uses a private IP address to ensure that the indexed data isn't accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to AWS or Azure (for example, a VPN), or from a host that's inside the same network as the Cloud Compliance instance.



If you're accessing Cloud Manager from a public IP address, then your web browser probably isn't running on a host inside the network.

Subscribing from the AWS Marketplace

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends.

These steps must be completed by a user who has the *Account Admin* role.

Steps

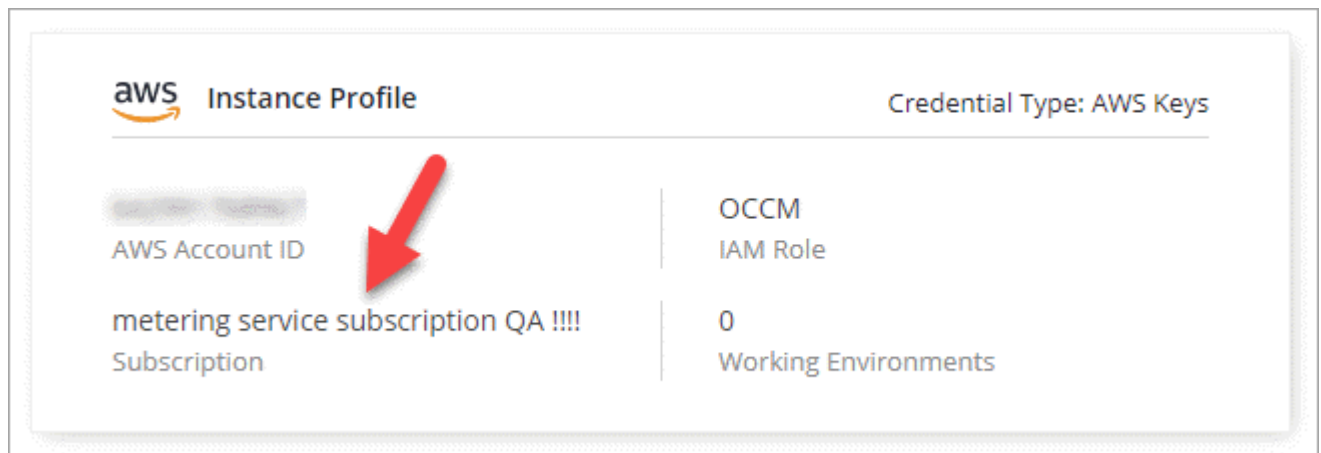
1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



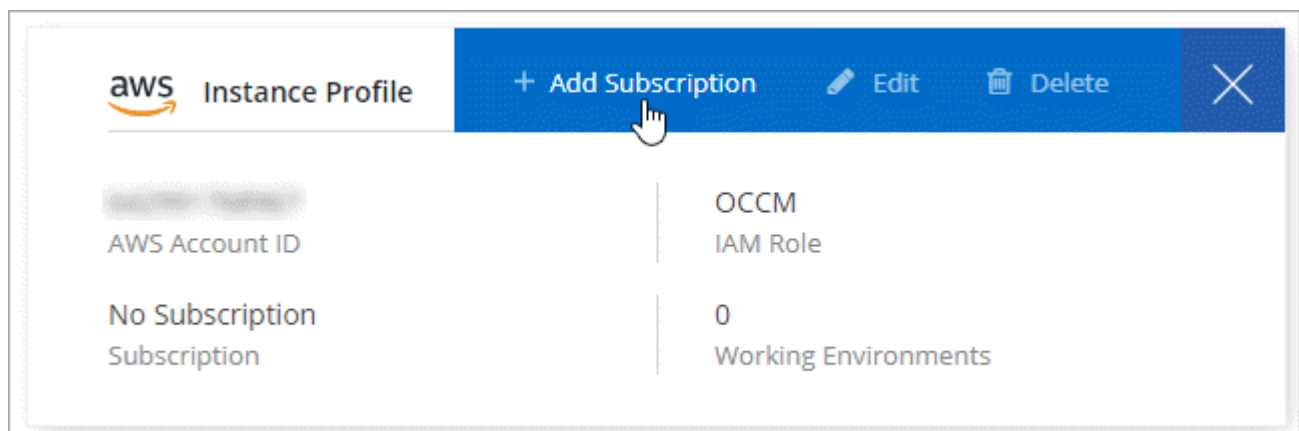
2. Find the credentials for the AWS Instance Profile.

The subscription must be added to the Instance Profile. Charging won't work otherwise.

If you already have a subscription, then you're all set—there's nothing else that you need to do.



3. If you don't have a subscription yet, hover over the credentials and click the action menu.
4. Click **Add Subscription**.



5. Click **Add Subscription**, click **Continue**, and follow the steps.

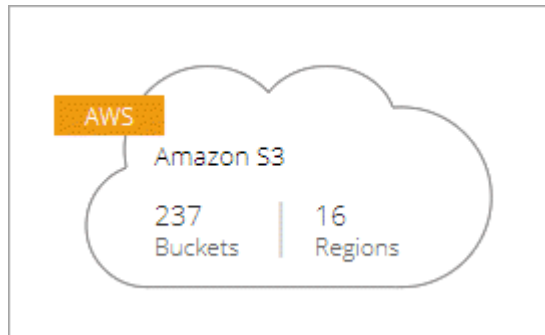
► https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4 (video)

Enabling Cloud Compliance

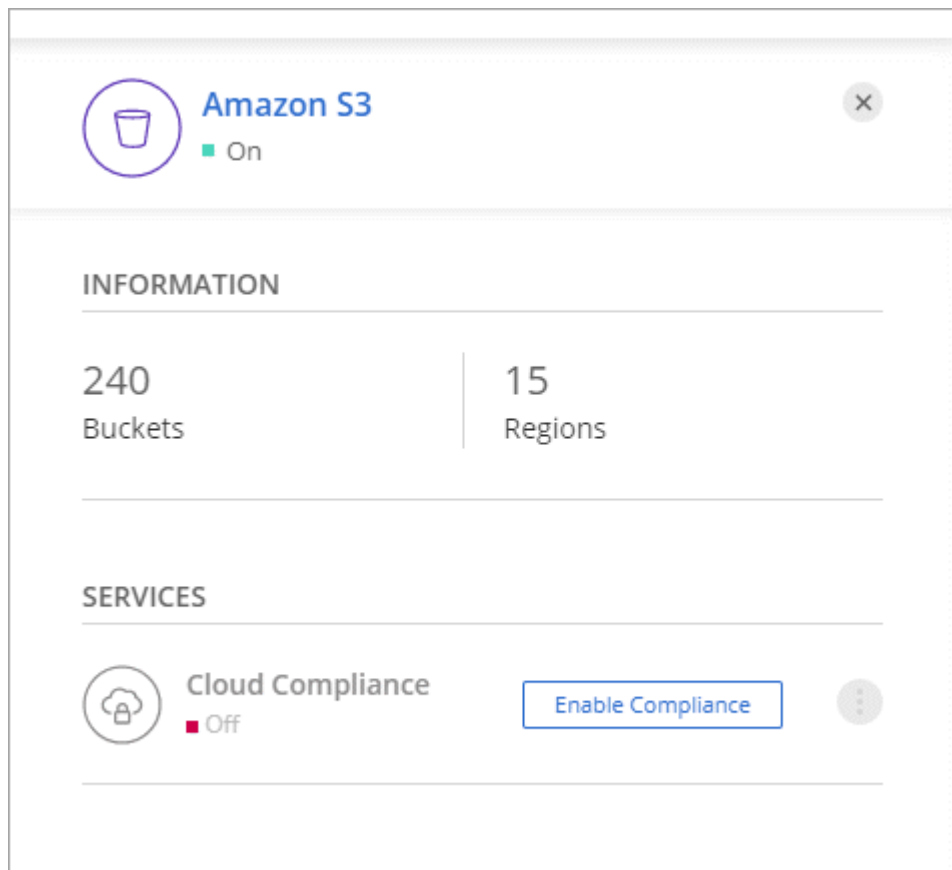
Enable Cloud Compliance on Amazon S3 after you verify the prerequisites.

Steps

1. At the top of Cloud Manager, click **Working Environments**.
2. Select the Amazon S3 working environment.



3. In the pane on the right, click **Enable Compliance**.



- When prompted, assign an IAM role to the Cloud Compliance instance that has [the required permissions](#).

Assign an AWS IAM Role for Cloud Compliance

To enable Cloud Compliance on Amazon S3 buckets, select an existing IAM role. Make sure that your AWS IAM role has the permission defined in the [Policy Requirements](#).

Select IAM Role

NetAppCloudCompliance ▼


VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Cloud Compliance can securely scan the data. Alternatively, ensure that the Cloud Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Enable ComplianceCancel

- Click **Enable Compliance**.



You can also enable compliance scans for a working environment from the Scan Configuration page by clicking the  icon and selecting **Activate Compliance**.

Result

If the Cloud Compliance instance hasn't been deployed yet, Cloud Manager deploys it. If it has been deployed, Cloud Manager assigns the IAM role to the instance.

Configuring buckets


After Cloud Manager enables Cloud Compliance on Amazon S3, the next step is to configure the buckets that you want to scan.

When Cloud Manager is running in the AWS account that has the S3 buckets you want to scan, it discovers those buckets and displays them in an Amazon S3 working environment.

Cloud Compliance can also [scan S3 buckets that are in different AWS accounts](#).

Steps

1. Select the Amazon S3 working environment.
2. In the pane on the right, click **Configure Buckets**.


 **Amazon S3** ■ On ×

INFORMATION

246
Buckets

16
Regions

SERVICES


 **Cloud Compliance** ■ On

[Configure Buckets](#) ⋮

Free Trial for Cloud Compliance

You are using a Free Trial version of Cloud Compliance for the Controlled Availability period. We will notify you when the Free Trial is about to expire.




3. Enable compliance on the buckets that you want to scan.

 **Cloud Compliance**

[< Back](#)

Amazon S3 Scan Configuration

15/28 Buckets in Scan Scope. Toggle ON/OFF to enable Compliance per Bucket

Compliance ▾	Bucket Name ↓↑	Status ▾	Required Action
	BucketName1	● Not Scanning	Add Credentials
	BucketName2	● Continuously Scanning	
	BucketName3	● Not Scanning	

Result

Cloud Compliance starts scanning the S3 buckets that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

Scanning buckets from additional AWS accounts

You can scan S3 buckets that are under a different AWS account by assigning a role from that account to access the existing Cloud Compliance instance.





Steps

1. Go to the target AWS account where you want to scan S3 buckets and create an IAM role by selecting **Another AWS account**.

Create role



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--


Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*



Options

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA 

Be sure to do the following:

- Enter the ID of the account where the Cloud Compliance instance resides.
- Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
- Attach the Cloud Compliance IAM policy. Make sure it has the required permissions.

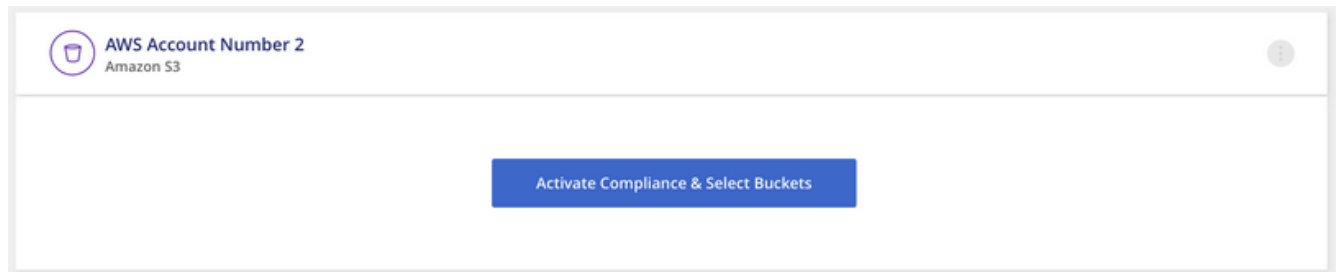
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Go to the source AWS account where the Cloud Compliance instance resides and select the IAM role that is attached to the instance.
 - a. Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
 - b. Click **Attach policies** and then click **Create policy**.
 - c. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

The Cloud Compliance instance profile account now has access to the additional AWS account.

3. Go to the **Amazon S3 Scan Configuration** page and the new AWS account is displayed. Note that it can take a few minutes for Cloud Compliance to sync the new account's working environment and show this information.



4. Click **Activate Compliance & Select Buckets** and select the buckets you want to scan.

Result

Cloud Compliance starts scanning the new S3 buckets that you enabled.

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.