



Cloud Compliance for Amazon S3 の利用を開始してください

Cloud Manager

Tom Onacki, Ben Cammett
May 10, 2021

目次

Cloud Compliance for Amazon S3 の利用を開始してください.....	1
クイックスタート	1
S3 の前提条件の確認.....	1
Cloud Compliance インスタンスの導入	2
S3 作業環境でのコンプライアンスのアクティブ化	3
S3 バケットでの準拠スキャンの有効化と無効化	4
追加の AWS アカウントからバケットをスキャンする	5

Cloud Compliance for Amazon S3 の利用を開始してください

Cloud Compliance では、Amazon S3 バケットをスキャンして、S3 オブジェクトストレージに格納されている個人データや機密データを特定できます。Cloud Compliance は、ネットアップソリューション用に作成されたバケットであるかどうかに関係なく、アカウント内の任意のバケットをスキャンできます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

クラウド環境で **S3** の要件を設定します

クラウド環境が Cloud Compliance の要件を満たしていることを確認します。たとえば、IAM ロールの準備と Cloud Compliance から S3 への接続の設定を行います。 [すべてのリストを参照してください](#)。

Cloud Compliance インスタンスを導入します

"[Cloud Compliance の導入](#)" インスタンスが展開されていない場合。

S3 作業環境でコンプライアンスをアクティブ化します

Amazon S3 作業環境を選択し、* 準拠の有効化 * をクリックして、必要な権限を含む IAM ロールを選択します。

スキャンするバケットを選択します

スキャンするバケットを選択すると、Cloud Compliance でスキャンが開始されます。

S3 の前提条件の確認

S3 バケットのスキャンに固有の要件を次に示します。

Cloud Compliance インスタンス用の **IAM** ロールを設定します

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

Cloud Compliance から Amazon S3 への接続を提供

VPC エンドポイントを作成するときは、Cloud Compliance インスタンスに対応するリージョン、VPC、およびルーティングテーブルを選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、Cloud Compliance は S3 サービスに接続できません。

問題が発生した場合は、を参照してください ["AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"](#)

別の方法として、NAT ゲートウェイを使用して接続を提供する方法があります。



インターネット経由で S3 にアクセスするためにプロキシを使用することはできません。

Cloud Compliance インスタンスの導入

["Cloud Manager に Cloud Compliance を導入"](#) インスタンスが展開されていない場合。

この AWS アカウントで S3 バケットが Cloud Manager で自動的に検出されて Amazon S3 作業環境に表示されるように、AWS コネクタにインスタンスを導入する必要があります。

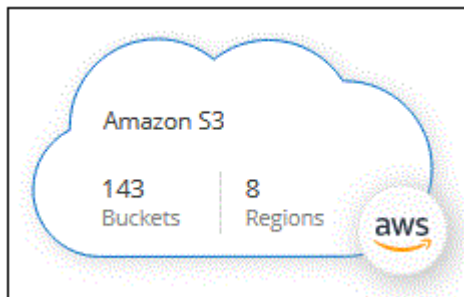
- 注： * オンプレミスの場所に Cloud Compliance を導入することは、現在 S3 バケットのスキャンではサポートされていません。

S3 作業環境でのコンプライアンスのアクティブ化

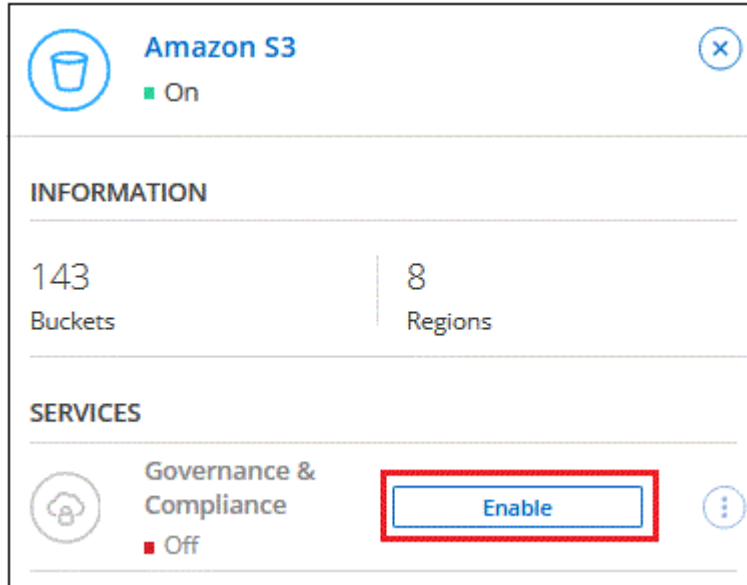
前提条件を確認したら、Amazon S3 で Cloud Compliance を有効にします。

手順

1. Cloud Manager の上部にある * Canvas * をクリックします。
2. Amazon S3 作業環境を選択します。



3. 右側のペインで、[Enable] をクリックします。



4. プロンプトが表示されたら、の Cloud Compliance インスタンスに IAM ロールを割り当てます [必要な権限](#)。

Assign an AWS IAM Role for Governance & Compliance

To enable Governance & 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

occm

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Governance & Compliance can securely scan the data.

Alternatively, ensure that the Governance & Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. [Enable] をクリックします。



また、作業環境のコンプライアンススキャンを有効にすることもできます Configuration ページでをクリックします  ボタンを押して、 * コンプライアンスを有効にする * を選択します。

Cloud Manager によって、インスタンスに IAM ロールが割り当てられます。

S3 バケットでの準拠スキャンの有効化と無効化

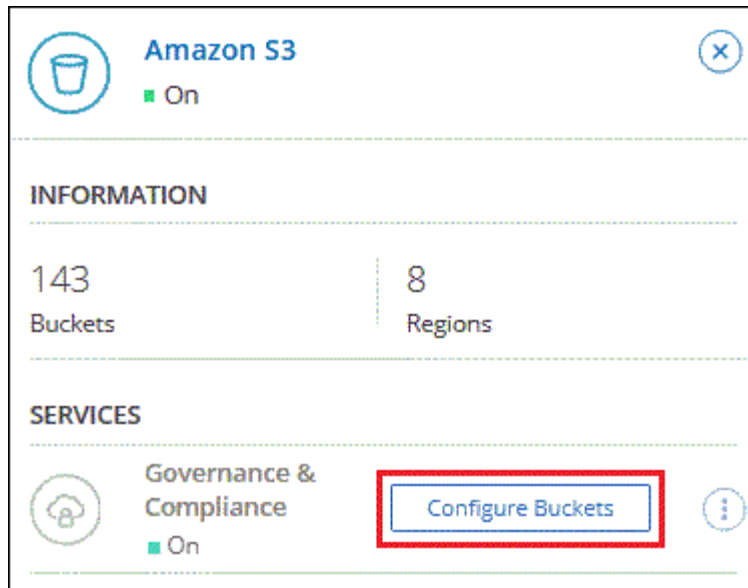
Cloud Manager で Amazon S3 の Cloud Compliance が有効になったら、次の手順でスキャンするバケットを設定します。

スキャンする S3 バケットを含む AWS アカウントで Cloud Manager を実行している場合は、そのバケットが検出され、Amazon S3 作業環境に表示されます。

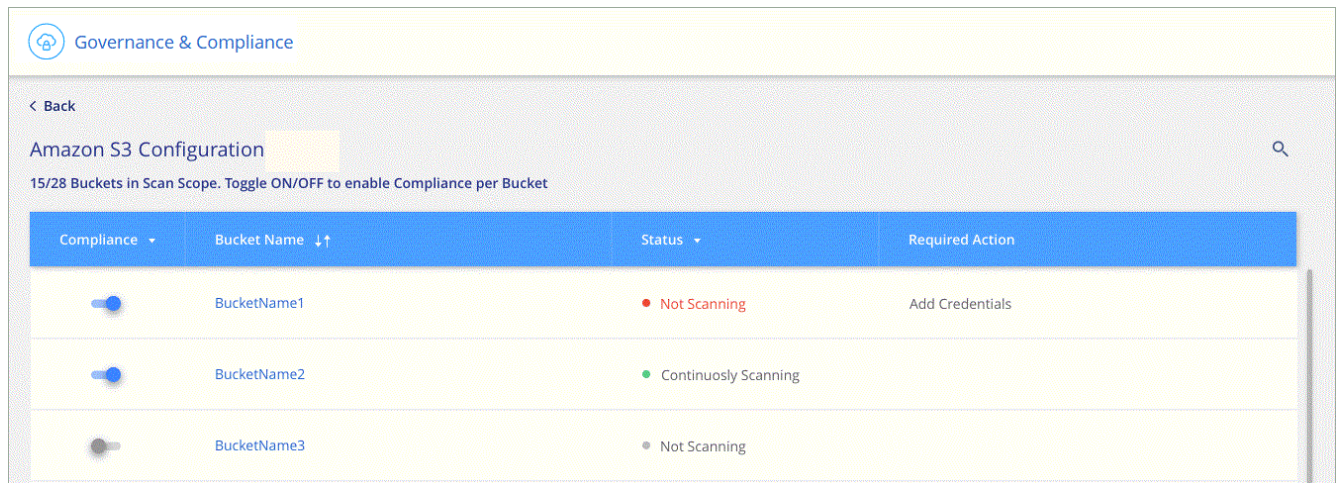
Cloud Compliance も同様です [別々の AWS アカウントにある S3 バケットをスキャンします](#)。

手順

1. Amazon S3 作業環境を選択します。
2. 右側のペインで、 * バケットの設定 * をクリックします。



3. スキャンするバケットで準拠を有効にします。



Cloud Compliance で、有効にした S3 バケットのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス]列に表示されます。

追加の **AWS** アカウントからバケットをスキャンする

別の AWS アカウントを使用している S3 バケットをスキャンするには、そのアカウントからロールを割り当てて、既存の Cloud Compliance インスタンスにアクセスします。

手順

1. S3 バケットをスキャンするターゲット AWS アカウントに移動し、* 別の AWS アカウント * を選択して IAM ロールを作成します。

Create role





1

2

3

4


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 

必ず次の手順を実行してください。

- Cloud Compliance インスタンスが存在するアカウントの ID を入力します。
- 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
- Cloud Compliance IAM ポリシーを関連付けます。必要な権限があることを確認します。

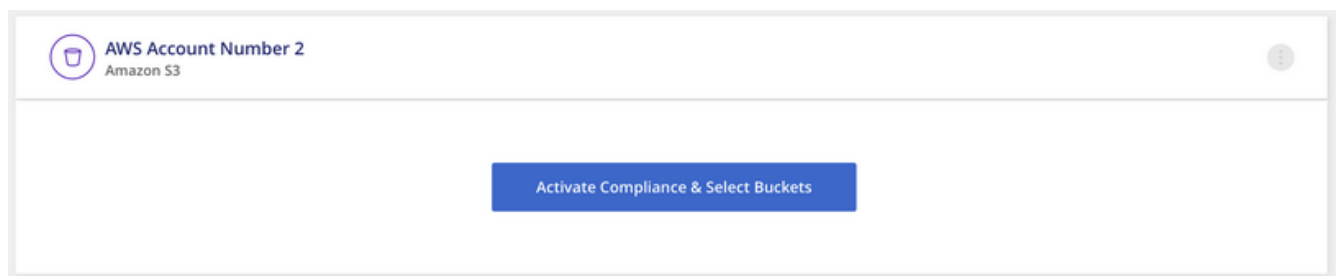
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Cloud Compliance インスタンスが存在するソース AWS アカウントに移動し、インスタンスに関連付けられている IAM ロールを選択します。
 - a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
 - b. [* ポリシーの適用 *] をクリックし、[ポリシーの作成 *] をクリックします。
 - c. 「 STS : AssumeRole 」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロールの ARN を指定します。


```
{
  "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/*"
      ]
    }
  ]
}
```

Cloud Compliance インスタンスのプロファイルアカウントで追加の AWS アカウントにアクセスできるようになりました。

3. Amazon S3 Configuration * ページに移動し、新しい AWS アカウントが表示されます。Cloud Compliance が新しいアカウントの作業環境を同期し、この情報を表示するまでに数分かかることがあります。



4. [Activate Compliance & Select Buckets] をクリックして、スキャンするバケットを選択します。

Cloud Compliance によって、有効にした新しい S3 バケットのスキャンが開始されます。

Copyright Information

Copyright © 2021 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.