



Ative a digitalização nas suas fontes de dados

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Ative a digitalização nas suas fontes de dados 1
 - Primeiros passos com o Cloud Compliance para Cloud Volumes ONTAP e Azure NetApp Files 1
 - Introdução ao Cloud Compliance para Amazon S3 5
 - Digitalização de esquemas de banco de dados 13
 - Verificação de dados do ONTAP no local com o Cloud Compliance usando o SnapMirror 16

Ative a digitalização nas suas fontes de dados

Primeiros passos com o Cloud Compliance para Cloud Volumes ONTAP e Azure NetApp Files

Conclua algumas etapas para dar os primeiros passos com o Cloud Compliance for Cloud Volumes ONTAP ou Azure NetApp Files.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.



Implante a instância do Cloud Compliance

"[Implante o Cloud Compliance no Cloud Manager](#)" se ainda não houver uma instância implantada.



Habilite o Cloud Compliance em seus ambientes de trabalho

Clique em **Cloud Compliance**, selecione a guia **Configuration** e ative as verificações de conformidade para ambientes de trabalho específicos.



Garanta o acesso aos volumes

Agora que o Cloud Compliance está ativado, garanta que ele possa acessar volumes.

- A instância de conformidade em nuvem precisa de uma conexão de rede para cada sub-rede Cloud Volumes ONTAP ou sub-rede Azure NetApp Files.
- Os grupos de segurança do Cloud Volumes ONTAP devem permitir conexões de entrada da instância de conformidade com a nuvem.
- As políticas de exportação de volume NFS devem permitir o acesso a partir da instância do Cloud Compliance.
- O Cloud Compliance precisa de credenciais do active Directory para verificar volumes CIFS.

Clique em **Cloud Compliance > Scan Configuration > Edit CIFS Credentials** e forneça as credenciais. As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que o Cloud Compliance possa ler dados que exigem permissões elevadas.



Configure volumes para digitalizar

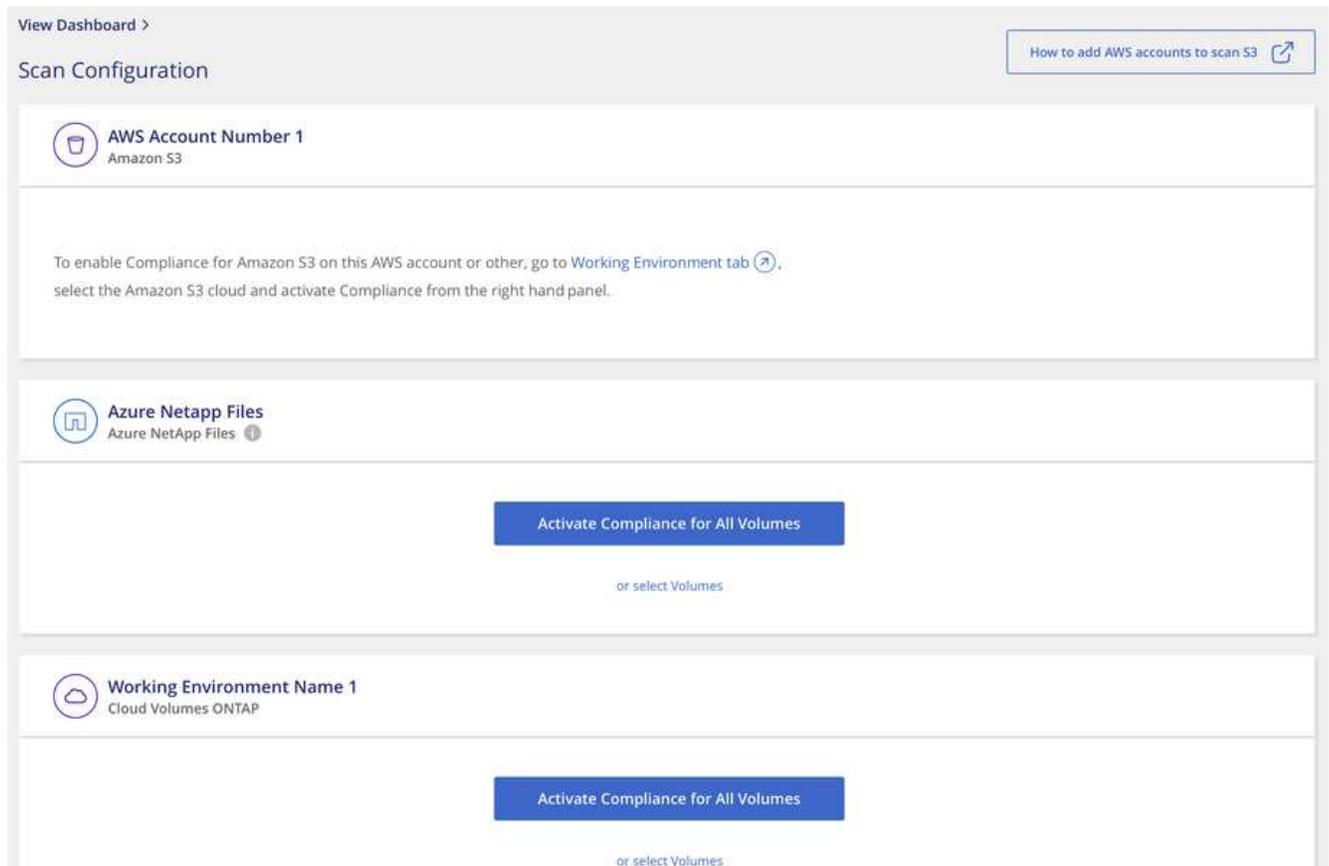
Selecione os volumes que você deseja verificar e o Cloud Compliance começará a digitalizá-los.

Implantando a instância de Cloud Compliance

"[Implante o Cloud Compliance no Cloud Manager](#)" se ainda não houver uma instância implantada.

Habilitando o Cloud Compliance em seus ambientes de trabalho

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance** e selecione a guia **Configuration**.



2. Para digitalizar todos os volumes em um ambiente de trabalho, clique em **Ativar conformidade para todos os volumes**.

Para digitalizar apenas determinados volumes num ambiente de trabalho, clique em **ou selecione volumes** e, em seguida, escolha os volumes que pretende digitalizar.

[Ativar e desativar verificações de conformidade em volumes](#) Consulte para obter detalhes.

Resultado

O Cloud Compliance começa a analisar os dados em cada ambiente de trabalho. Os resultados estarão disponíveis no painel de conformidade assim que o Cloud Compliance concluir as verificações iniciais. O tempo que leva depende da quantidade de dados - pode ser de alguns minutos ou horas.

Verificar se o Cloud Compliance tem acesso a volumes

Verifique se o Cloud Compliance pode acessar volumes verificando suas políticas de rede, grupos de segurança e exportação. Você precisará fornecer as credenciais CIFS do Cloud Compliance para acessar os volumes CIFS.

Passos

1. Verifique se há uma conexão de rede entre a instância do Cloud Compliance e cada rede que inclua volumes para Cloud Volumes ONTAP ou Azure NetApp Files.

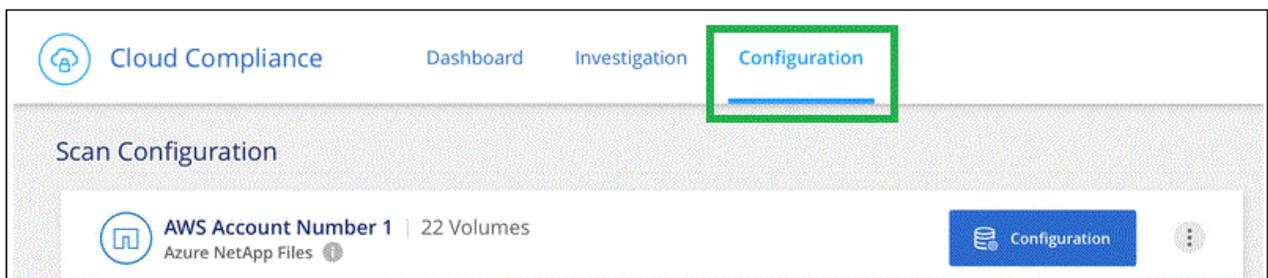


Para o Azure NetApp Files, o Cloud Compliance só pode verificar volumes que estejam na mesma região que o Cloud Manager.

2. Certifique-se de que o grupo de segurança do Cloud Volumes ONTAP permita o tráfego de entrada da instância de conformidade com a nuvem.

Você pode abrir o grupo de segurança para o tráfego a partir do endereço IP da instância de conformidade na nuvem ou abrir o grupo de segurança para todo o tráfego dentro da rede virtual.

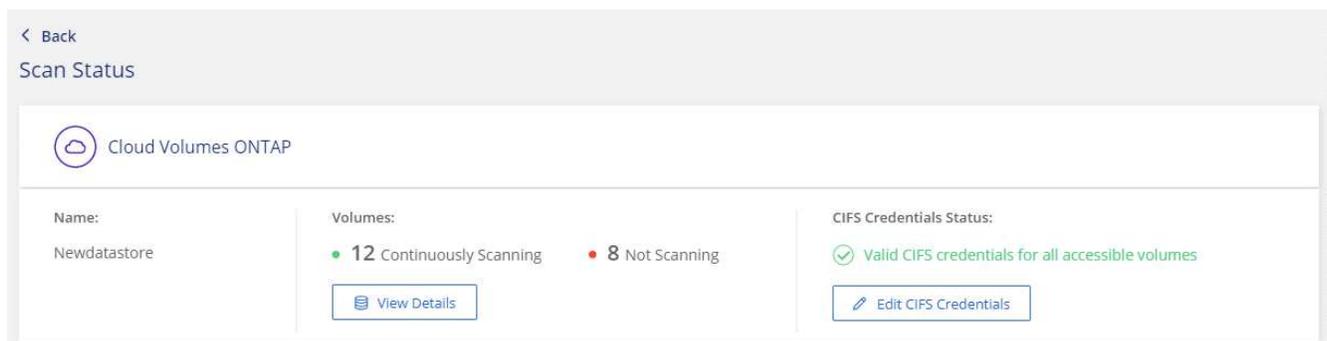
3. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Cloud Compliance para que ela possa acessar os dados em cada volume.
4. Se você usar CIFS, forneça as credenciais do Cloud Compliance para que ele possa verificar os volumes CIFS.
 - a. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
 - b. Clique na guia **Configuração**.



- c. Para cada ambiente de trabalho, clique em **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Cloud Compliance precisa para acessar volumes CIFS no sistema.

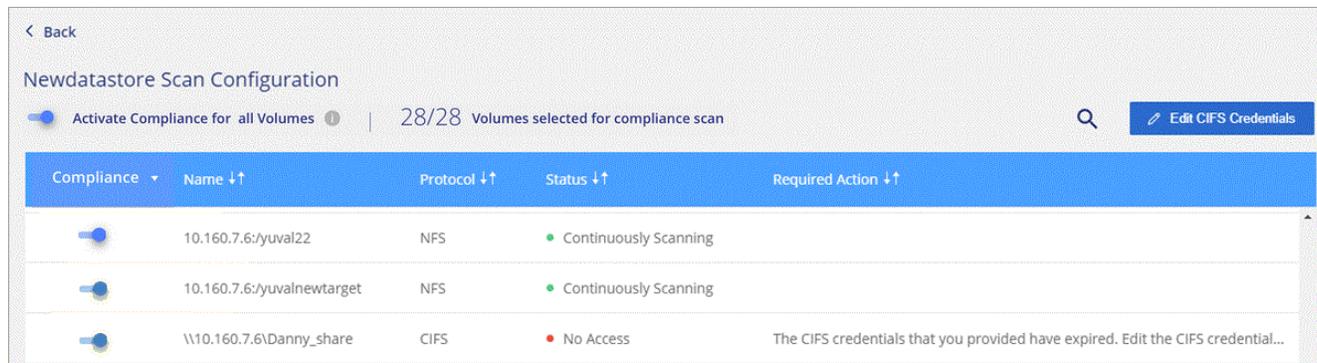
As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que o Cloud Compliance possa ler todos os dados que exigem permissões elevadas. As credenciais são armazenadas na instância do Cloud Compliance.

Depois de inserir as credenciais, você verá uma mensagem informando que todos os volumes CIFS foram autenticados com êxito.



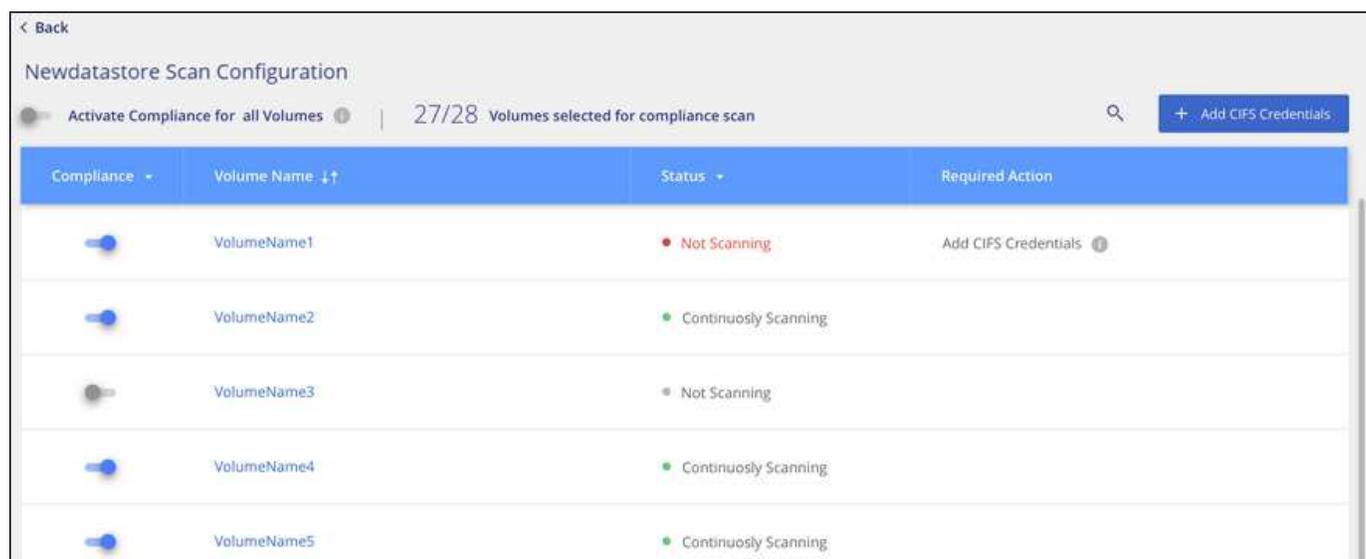
5. Na página *Scan Configuration*, clique em **View Details** (Ver detalhes) para rever o estado de cada volume CIFS e NFS e corrigir quaisquer erros.

Por exemplo, a imagem a seguir mostra três volumes; um dos quais o Cloud Compliance não pode ser verificado devido a problemas de conectividade de rede entre a instância do Cloud Compliance e o volume.



Ativar e desativar verificações de conformidade em volumes

Pode parar ou iniciar a digitalização de volumes num ambiente de trabalho a qualquer momento a partir da página Configuração de digitalização. Recomendamos que você digitalize todos os volumes.



Para:	Faça isso:
Desativar a procura de um volume	Mova o controle deslizante de volume para a esquerda
Desative a digitalização de todos os volumes	Mova o controle deslizante Ativar conformidade para todos os volumes para a esquerda
Ativar a digitalização de um volume	Mova o controle deslizante de volume para a direita
Ative a digitalização de todos os volumes	Mova o controle deslizante Ativar conformidade para todos os volumes para a direita

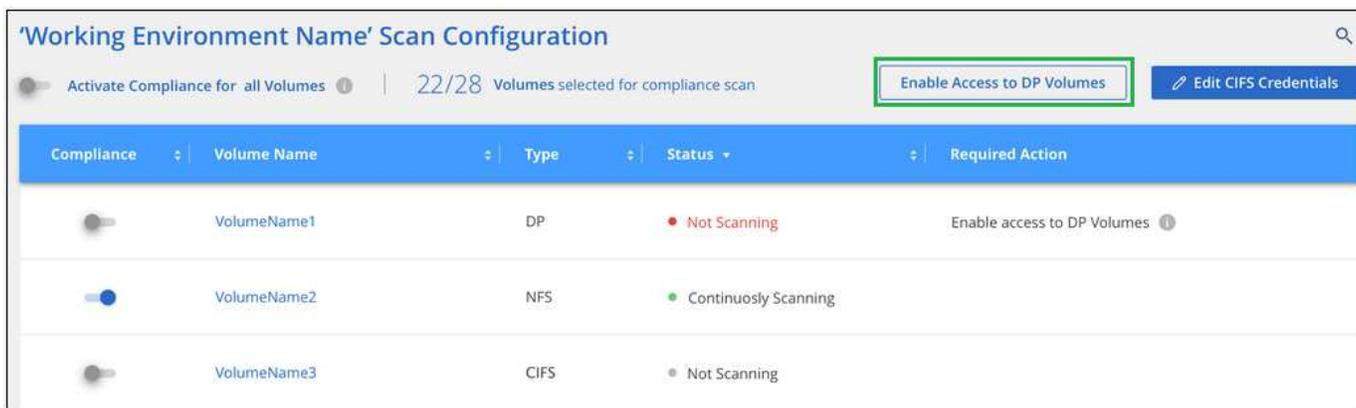


Os novos volumes adicionados ao ambiente de trabalho são automaticamente verificados somente quando a configuração **Ativar conformidade para todos os volumes** estiver ativada. Quando esta definição estiver desativada, terá de ativar a digitalização em cada novo volume criado no ambiente de trabalho.

Digitalização de volumes de proteção de dados

Por padrão, os volumes de proteção de dados (DP) não são verificados porque não são expostos externamente e o Cloud Compliance não pode acessá-los. Esses volumes geralmente são os volumes de destino para operações do SnapMirror a partir de um cluster do ONTAP no local.

Inicialmente, a lista de volumes do Cloud Compliance identifica esses volumes como *Type DP* com o *Status Not Scanning* e a *Required Action Enable Access to DP volumes*.



Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

Passos

Se você quiser analisar esses volumes de proteção de dados:

1. Clique no botão **Ativar acesso aos volumes DP** na parte superior da página.
2. Ative cada volume DP que você deseja digitalizar ou use o controle **Ativar conformidade para todos os volumes** para habilitar todos os volumes, incluindo todos os volumes DP.

Uma vez ativado, o Cloud Compliance cria um compartilhamento NFS a partir de cada volume DP ativado para conformidade, para que possa ser verificado. As políticas de exportação de compartilhamento só permitem acesso a partir da instância de conformidade com a nuvem.



Apenas os volumes criados inicialmente como volumes NFS no sistema ONTAP de origem são mostrados na lista de volumes. Os volumes de origem criados inicialmente como CIFS não aparecem no Cloud Compliance.

Introdução ao Cloud Compliance para Amazon S3

O Cloud Compliance pode verificar seus buckets do Amazon S3 para identificar os dados pessoais e confidenciais que residem no storage de objetos do S3. O Cloud Compliance pode verificar qualquer bucket da conta, independentemente de ter sido criado para uma solução da NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.



Configure os requisitos do S3 em seu ambiente de nuvem

Garanta que seu ambiente de nuvem atenda aos requisitos de conformidade com a nuvem, incluindo a preparação de uma função do IAM e a configuração da conectividade do Cloud Compliance para o S3. [Veja a lista completa.](#)



Implante a instância do Cloud Compliance

"[Implante o Cloud Compliance no Cloud Manager](#)" se ainda não houver uma instância implantada.



Ative a conformidade no seu ambiente de trabalho S3

Selecione o ambiente de trabalho do Amazon S3, clique em **Ativar conformidade** e selecione uma função do IAM que inclua as permissões necessárias.



Selecione os intervalos para digitalizar

Selecione os buckets que você gostaria de verificar e o Cloud Compliance começará a digitalizá-los.

Rever os pré-requisitos do S3

Os requisitos a seguir são específicos para a digitalização de buckets S3.

Configure uma função do IAM para a instância do Cloud Compliance

O Cloud Compliance precisa de permissões para se conectar aos buckets do S3 na sua conta e verificá-los. Configure uma função do IAM que inclua as permissões listadas abaixo. O Cloud Manager solicita que você selecione uma função do IAM ao ativar o Cloud Compliance no ambiente de trabalho do Amazon S3.

```

{
  "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/*"
      ]
    }
  ]
}

```

Fornecer conectividade do Cloud Compliance para o Amazon S3

O Cloud Compliance precisa de uma conexão com o Amazon S3. A melhor maneira de fornecer essa conexão é por meio de um VPC Endpoint ao serviço S3. Para obter instruções, ["Documentação da AWS: Criando um endpoint do Gateway"](#) consulte .

Quando você criar o VPC Endpoint, certifique-se de selecionar a região, VPC e tabela de rotas que corresponde à instância do Cloud Compliance. Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que permita o tráfego para o endpoint S3. Caso contrário, o Cloud Compliance não pode se conectar ao serviço S3.

Se tiver algum problema, consulte ["AWS Support Knowledge Center: Por que não consigo me conectar a um bucket do S3 usando um endpoint VPC de gateway?"](#)

Uma alternativa é fornecer a conexão usando um NAT Gateway.



Você não pode usar um proxy para chegar ao S3 pela internet.

Implantando a instância de Cloud Compliance

["Implante o Cloud Compliance no Cloud Manager"](#) se ainda não houver uma instância implantada.

Você precisa implantar a instância em um AWS Connector para que o Cloud Manager descubra automaticamente os buckets do S3 nessa conta da AWS e os exiba em um ambiente de trabalho do Amazon S3.

Ativar a conformidade no seu ambiente de trabalho S3

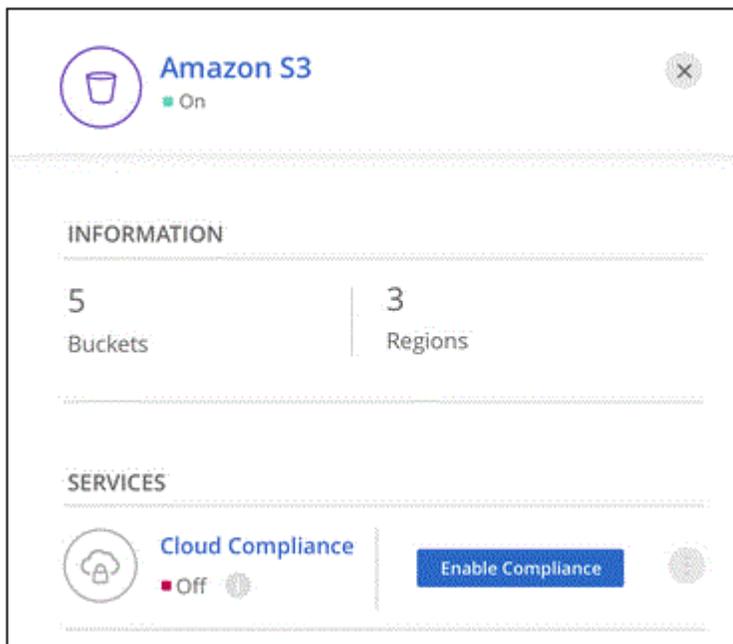
Ative o Cloud Compliance no Amazon S3 depois de verificar os pré-requisitos.

Passos

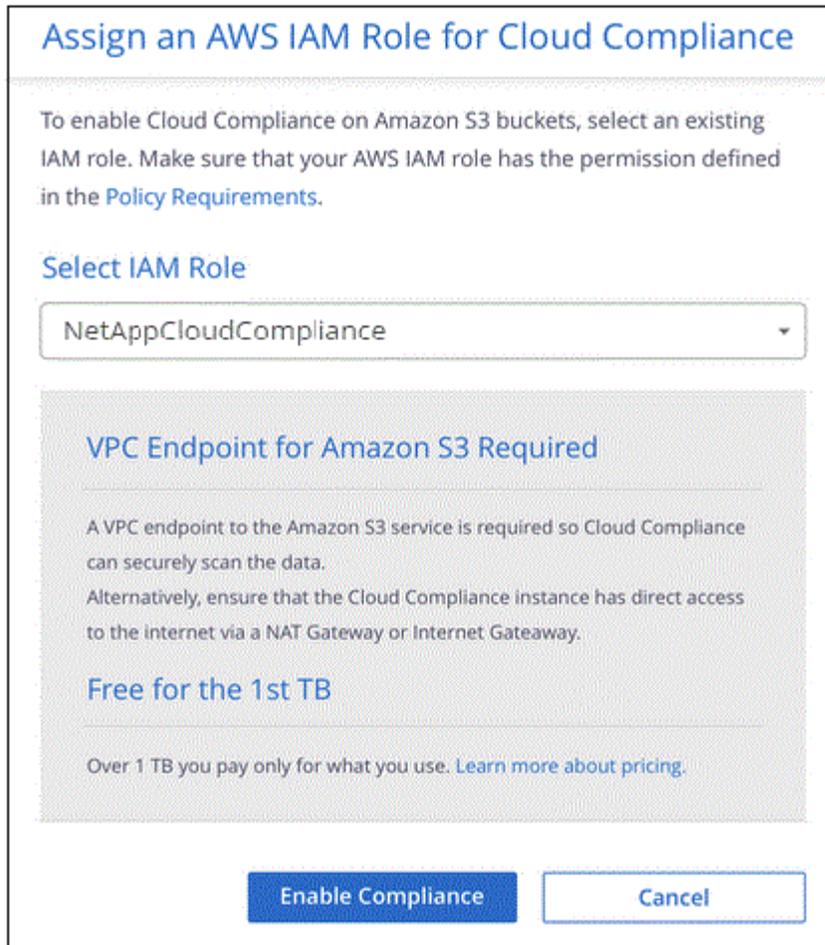
1. Na parte superior do Cloud Manager, clique em **ambientes de trabalho**.
2. Selecione o ambiente de trabalho do Amazon S3.



3. No painel à direita, clique em **Ativar conformidade**.



4. Quando solicitado, atribua uma função do IAM à instância do Cloud Compliance que tem [as permissões necessárias](#).



5. Clique em **Ativar conformidade**.



Você também pode habilitar verificações de conformidade para um ambiente de trabalho na página Configuração de digitalização clicando no  botão e selecionando **Ativar conformidade**.

Resultado

O Cloud Manager atribui a função IAM à instância.

Ativar e desativar verificações de conformidade em buckets do S3

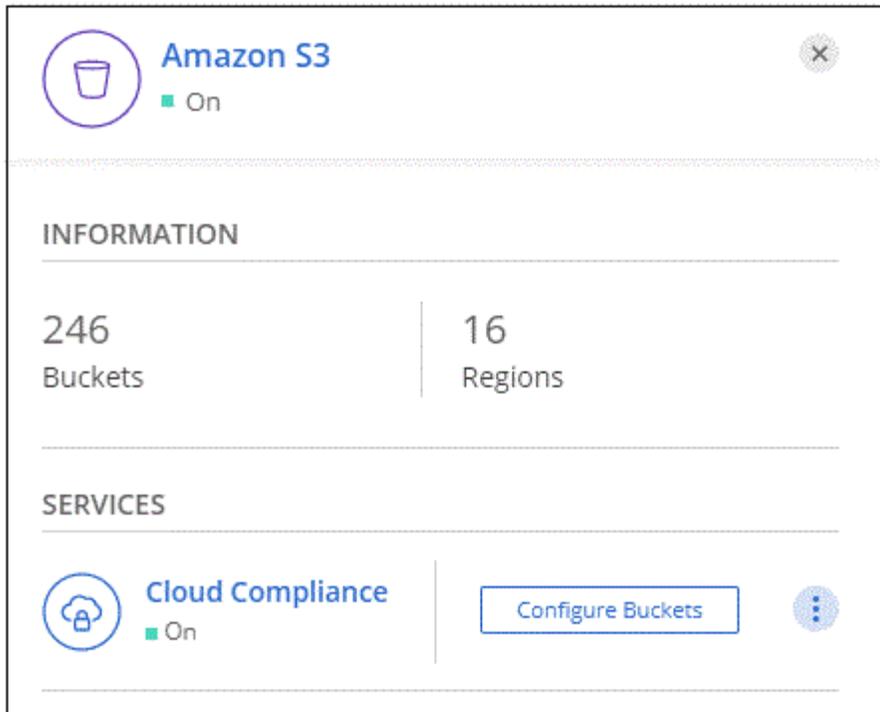
Depois que o Cloud Manager ativar o Cloud Compliance no Amazon S3, a próxima etapa é configurar os buckets que você deseja analisar.

Quando o Cloud Manager está em execução na conta da AWS que tem os buckets do S3 que você deseja verificar, ele descobre esses buckets e os exibe em um ambiente de trabalho do Amazon S3.

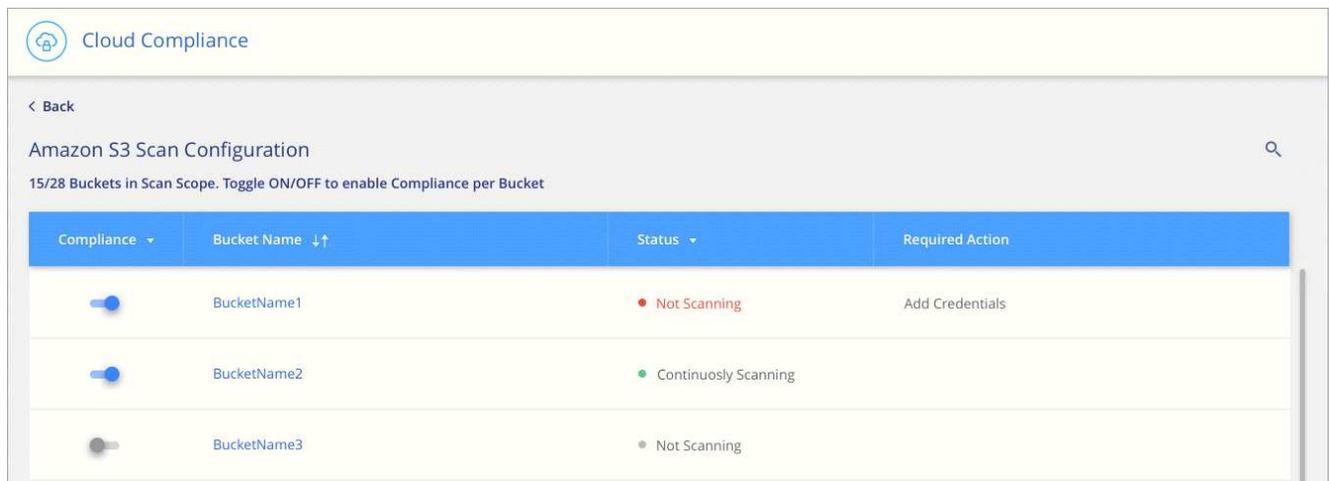
O Cloud Compliance também [Examine os buckets do S3 que estão em diferentes contas da AWS](#) pode .

Passos

1. Selecione o ambiente de trabalho do Amazon S3.
2. No painel à direita, clique em **Configurar baldes**.



3. Ative a conformidade nos buckets que você deseja analisar.



Resultado

O Cloud Compliance começa a verificar os buckets do S3 ativados. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Digitalização de buckets a partir de contas adicionais da AWS

Você pode verificar buckets do S3 em uma conta diferente da AWS atribuindo uma função dessa conta para acessar a instância existente do Cloud Compliance.

Passos

1. Vá para a conta AWS de destino onde você deseja analisar buckets do S3 e criar uma função do IAM selecionando **outra conta da AWS**.

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 ⓘ

Certifique-se de fazer o seguinte:

- Insira o ID da conta onde reside a instância do Cloud Compliance.
- Altere a duração máxima da sessão CLI/API* de 1 hora para 12 horas e salve essa alteração.
- Anexe a política do Cloud Compliance IAM. Certifique-se de que tem as permissões necessárias.

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

2. Vá para a conta da AWS de origem onde reside a instância do Cloud Compliance e selecione a função do IAM anexada à instância.
 - a. Altere a duração máxima da sessão CLI/API* de 1 hora para 12 horas e salve essa alteração.
 - b. Clique em **Anexar políticas** e, em seguida, clique em **criar política**.
 - c. Crie uma política que inclua a ação "sts:AssumeRole" e o ARN da função que você criou na conta de destino.

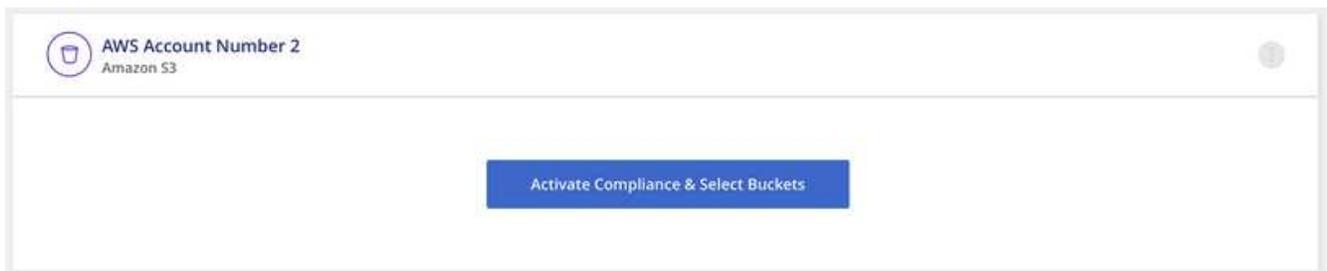
```

{
  "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/*"
      ]
    }
  ]
}

```

A conta de perfil de instância do Cloud Compliance agora tem acesso à conta AWS adicional.

3. Vá para a página **Configuração de digitalização do Amazon S3** e a nova conta da AWS será exibida. Observe que pode levar alguns minutos para que o Cloud Compliance sincronize o ambiente de trabalho da nova conta e mostre essas informações.



4. Clique em **Activate Compliance & Select Buckets** (Ativar conformidade e Selecionar baldes*) e selecione os baldes que pretende digitalizar.

Resultado

O Cloud Compliance começa a verificar os novos buckets do S3 ativados.

Digitalização de esquemas de banco de dados

Conclua algumas etapas para começar a verificar seus esquemas de banco de dados com o Cloud Compliance.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.



Rever pré-requisitos da base de dados

Certifique-se de que a sua base de dados é suportada e de que tem as informações necessárias para se ligar à base de dados.



Implante a instância do Cloud Compliance

"[Implante o Cloud Compliance no Cloud Manager](#)" se ainda não houver uma instância implantada.



Adicione o servidor de banco de dados

Adicione o servidor de banco de dados que você deseja acessar.



Selecione os esquemas

Selecione os esquemas que pretende digitalizar.

Rever pré-requisitos

Revise os pré-requisitos a seguir para garantir que você tenha uma configuração compatível antes de ativar o Cloud Compliance.

Bancos de dados compatíveis

O Cloud Compliance pode verificar esquemas dos seguintes bancos de dados:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)



O recurso de coleta de estatísticas **deve estar ativado** no banco de dados.

Requisitos de banco de dados

Qualquer banco de dados com conectividade com a instância de conformidade com a nuvem pode ser verificado, independentemente de onde esteja hospedado. Você só precisa das seguintes informações para se conectar ao banco de dados:

- Endereço IP ou nome do host
- Porta
- Nome do serviço (somente para acessar bancos de dados Oracle)
- Credenciais que permitem acesso de leitura aos esquemas

Ao escolher um nome de usuário e senha, é importante escolher um que tenha permissões de leitura completas para todos os esquemas e tabelas que você deseja digitalizar. Recomendamos que você crie um usuário dedicado para o sistema de conformidade com a nuvem com todas as permissões necessárias.

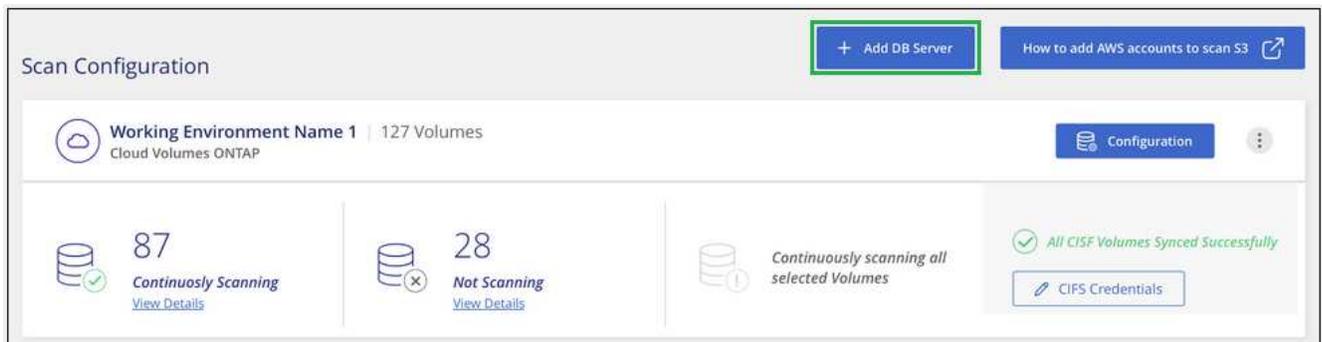
Observação: para MongoDB, é necessária uma função de administração somente leitura.

Adicionando o servidor de banco de dados

Você deve ter "[Já implantou uma instância do Cloud Compliance no Cloud Manager](#)".

Adicione o servidor de banco de dados onde os esquemas residem.

1. Na página *Scan Configuration*, clique no botão **Add DB Server**.



2. Introduza as informações necessárias para identificar o servidor da base de dados.
 - a. Selecione o tipo de banco de dados.
 - b. Insira a porta e o nome do host ou endereço IP para se conectar ao banco de dados.
 - c. Para bancos de dados Oracle, insira o nome do serviço.
 - d. Insira as credenciais para que o Cloud Compliance possa acessar o servidor.
 - e. Clique em **Add DB Server**.

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type Host Name or IP Address

Port Service Name

Credentials

Username Password

O banco de dados é adicionado à lista de diretórios de trabalho.

Ativar e desativar verificações de conformidade em esquemas de banco de dados

Você pode parar ou começar a digitalizar esquemas a qualquer momento.

1. Na página *Scan Configuration*, clique no botão **Configuration** do banco de dados que deseja configurar.



2. Selecione os esquemas que deseja digitalizar movendo o controle deslizante para a direita.

'Working Environment Name' Scan Configuration			
28/28 Schemas selected for compliance scan		<input type="button" value="Edit Credentials"/>	
Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

Resultado

O Cloud Compliance começa a verificar os esquemas de banco de dados que você ativou. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Removendo um banco de dados do Cloud Manager

Se você não quiser mais digitalizar um determinado banco de dados, você pode excluí-lo da interface do Cloud Manager e parar todas as verificações.

Na página *Scan Configuration*, clique no  botão na linha do banco de dados e clique em **Remove DB Server**.



Verificação de dados do ONTAP no local com o Cloud Compliance usando o SnapMirror

Você pode digitalizar seus dados ONTAP locais com o Cloud Compliance replicando os dados NFS ou CIFS on-premises em um ambiente operacional da Cloud Volumes ONTAP e habilitando a conformidade. A digitalização dos dados diretamente de um ambiente de trabalho ONTAP local não é suportada.

Você deve ter "[Já implantou uma instância do Cloud Compliance no Cloud Manager](#)".

Passos

1. No Cloud Manager, crie uma relação de SnapMirror entre o cluster ONTAP no local e o Cloud Volumes ONTAP.

- a. ["Descubra o cluster no local no Cloud Manager"](#).
 - b. ["Crie uma replicação do SnapMirror entre o cluster do ONTAP no local e o Cloud Volumes ONTAP a partir do Cloud Manager"](#).
2. Para volumes DP criados a partir de volumes de origem SMB, a partir da CLI do ONTAP, configure os volumes de destino SMB para acesso aos dados. (Isso não é necessário para volumes NFS porque o acesso aos dados é habilitado automaticamente pelo Cloud Compliance.)
- a. ["Crie um compartilhamento SMB no volume de destino"](#).
 - b. ["Aplique as ACLs apropriadas ao compartilhamento SMB no volume de destino"](#).
3. No Cloud Manager, ative o Cloud Compliance no ambiente de trabalho do Cloud Volumes ONTAP que contém os dados do SnapMirror:
- a. Clique em **ambientes de trabalho**.
 - b. Selecione o ambiente de trabalho que contém os dados do SnapMirror e clique em **Ativar conformidade**.
- ["Clique aqui se precisar de ajuda para ativar o Cloud Compliance em um sistema Cloud Volumes ONTAP"](#).
- c. Clique no botão **Ativar acesso aos volumes DP** na parte superior da página *Configuração de digitalização*.
 - d. Ative cada volume DP que você deseja digitalizar ou use o controle **Ativar conformidade para todos os volumes** para habilitar todos os volumes, incluindo todos os volumes DP.

Consulte ["Digitalização de volumes de proteção de dados"](#) para obter mais informações sobre a digitalização de volumes DP.

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.