



# Tenha insights sobre a privacidade de dados

Cloud Manager 3.8

NetApp  
October 22, 2024

# Índice

- Tenha insights sobre a privacidade de dados ..... 1
- Saiba mais sobre o Cloud Compliance ..... 1
- Comece agora ..... 5
- Ter visibilidade e controle de dados privados ..... 28
- Visualização de relatórios de conformidade ..... 42
- Resposta a uma solicitação de acesso do titular dos dados ..... 47
- Desativação do Cloud Compliance ..... 49
- Perguntas frequentes sobre o Cloud Compliance ..... 50

# Tenha insights sobre a privacidade de dados

## Saiba mais sobre o Cloud Compliance

O Cloud Compliance é um serviço de conformidade e privacidade de dados do Cloud Manager que analisa volumes, buckets do Amazon S3 e bancos de dados para identificar os dados pessoais e confidenciais que residem nesses arquivos. Usando tecnologia orientada por inteligência artificial (AI), o Cloud Compliance ajuda as organizações a entender o contexto dos dados e identificar dados confidenciais.

["Saiba mais sobre os casos de uso do Cloud Compliance"](#).

### Caraterísticas

O Cloud Compliance fornece várias ferramentas para ajudar você a manter a conformidade. Você pode usar o Cloud Compliance para:

- Identificar informações pessoais identificáveis (PII)
- Identifique um amplo escopo de informações confidenciais conforme exigido pelas regulamentações de privacidade do GDPR, CCPA, PCI e HIPAA
- Responder às solicitações de acesso do titular dos dados (DSAR)

### Ambientes de trabalho e fontes de dados compatíveis

O Cloud Compliance pode analisar dados dos seguintes tipos de fontes de dados:

- Cloud Volumes ONTAP na AWS
- Cloud Volumes ONTAP no Azure
- Azure NetApp Files
- Amazon S3
- Bancos de dados que residem em qualquer lugar (não há requisito de que o banco de dados resida em um ambiente de trabalho)

**Observação:** para o Azure NetApp Files, o Cloud Compliance pode verificar todos os volumes que estão na mesma região que o Cloud Manager.

### Custo

- O custo para usar o Cloud Compliance depende da quantidade de dados que você está digitalizando. Em 7th de outubro de 2020, os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Isso inclui dados do Cloud Volumes ONTAP volumes, do Azure NetApp Files volumes, buckets do Amazon S3 e esquemas de banco de dados. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto. ["preços"](#) Consulte para obter detalhes.

["Saiba como se inscrever"](#).

- A instalação do Cloud Compliance requer a implantação de uma instância de nuvem, o que resulta em cobranças do provedor de nuvem onde ela é implantada. Consulte [o tipo de instância que é implantada](#)

[para cada provedor de nuvem](#)

- O Cloud Compliance exige que você implante um conector. Em muitos casos, você já tem um conector devido a outros serviços e storage que você está usando no Cloud Manager. A instância do conector resulta em cobranças do provedor de nuvem onde ela é implantada. Consulte "[tipo de instância implantada para cada provedor de nuvem](#)".

## Custos de transferência de dados

Os custos de transferência de dados dependem da configuração. Se a instância e a fonte de dados do Cloud Compliance estiverem na mesma zona de disponibilidade e região, não haverá custos de transferência de dados. Mas se a fonte de dados, como um cluster Cloud Volumes ONTAP ou um bucket do S3, estiver em uma zona de disponibilidade ou região *diferente*, você será cobrado pelo seu provedor de nuvem pelos custos de transferência de dados. Veja estes links para mais detalhes:

- "[AWS: Definição de preço do Amazon EC2](#)"
- "[Microsoft Azure: Detalhes de preços de largura de banda](#)"

## Como o Cloud Compliance funciona

Em um alto nível, o Cloud Compliance funciona assim:

1. Você implanta uma instância de Cloud Compliance no Cloud Manager.
2. Você o habilita em um ou mais ambientes de trabalho ou em seus bancos de dados.
3. O Cloud Compliance verifica os dados usando um processo de aprendizado de AI.
4. No Cloud Manager, você clica em **Compliance** e usa o painel e as ferramentas de relatórios fornecidos para ajudar em seus esforços de conformidade.

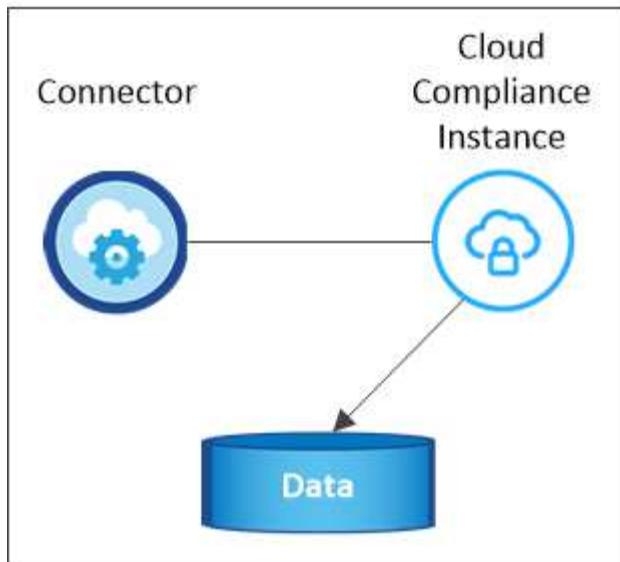
## A instância do Cloud Compliance

Quando você ativa o Cloud Compliance, o Cloud Manager implanta uma instância de Cloud Compliance na mesma sub-rede que o conector. "[Saiba mais sobre conectores.](#)"



Se o conector for instalado no local, ele implanta a instância de conformidade em nuvem na mesma VPC ou VNet como o primeiro sistema Cloud Volumes ONTAP na solicitação.

## VPC or VNet



Observe o seguinte sobre a instância:

- No Azure, o Cloud Compliance é executado em uma VM Standard\_D16s\_v3 com um disco de 512 GB.
- Na AWS, o Cloud Compliance é executado em uma instância do m5,4xlarge com um disco GP2 de 500 GB.

Em regiões onde o m5,4xlarge não está disponível, o Cloud Compliance é executado em uma instância do m4,4xlarge.



Alterar ou redimensionar o tipo de instância/VM não é suportado. Você precisa usar o tamanho fornecido.

- A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Somente uma instância do Cloud Compliance é implantada por conetor.
- As atualizações do software de conformidade na nuvem são automatizadas - você não precisa se preocupar com isso.



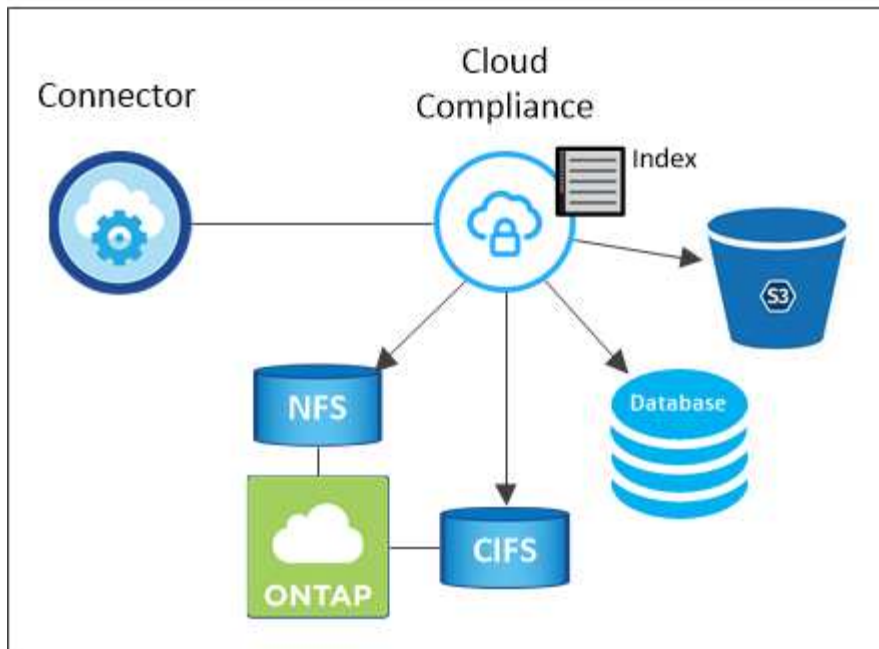
A instância deve permanecer em execução o tempo todo, porque o Cloud Compliance verifica continuamente os dados.

## Como as digitalizações funcionam

Depois de ativar o Cloud Compliance e selecionar os volumes, buckets ou esquemas de banco de dados que você deseja verificar, ele começará imediatamente a verificar os dados para identificar dados pessoais e confidenciais. Ele mapeia seus dados organizacionais, categoriza cada arquivo e identifica e extrai entidades e padrões predefinidos nos dados. O resultado da digitalização é um índice de informações pessoais, informações pessoais confidenciais e categorias de dados.

O Cloud Compliance conecta-se aos dados como qualquer outro cliente, com a montagem de volumes NFS e CIFS. Os volumes NFS são acessados automaticamente como somente leitura, enquanto você precisa fornecer credenciais do active Directory para verificar volumes CIFS.

## VPC or VNet



Após a verificação inicial, o Cloud Compliance verifica continuamente cada volume para detetar alterações incrementais (é por isso que é importante manter a instância em execução).

Pode ativar e desativar as digitalizações nas "nível de volume", em , "nível do balde" e "nível de esquema do banco de dados" em .

## Informações indexadas pelo Cloud Compliance

O Cloud Compliance coleta, indexa e atribui categorias a dados não estruturados (arquivos). Os dados indexados pelo Cloud Compliance incluem os seguintes:

### Metadados padrão

O Cloud Compliance coleta metadados padrão sobre arquivos: O tipo de arquivo, seu tamanho, datas de criação e modificação, etc.

### Dados pessoais

Informações de identificação pessoal, como endereços de e-mail, números de identificação ou números de cartão de crédito. ["Saiba mais sobre dados pessoais"](#).

### Dados pessoais confidenciais

Tipos especiais de informações sensíveis, como dados de saúde, origem étnica ou opiniões políticas, conforme definido pelo GDPR e outros regulamentos de privacidade. ["Saiba mais sobre dados pessoais confidenciais"](#).

### Categorias

O Cloud Compliance pega os dados que digitalizou e os divide em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. ["Saiba mais sobre categorias"](#).

### Reconhecimento de entidade de nome

O Cloud Compliance usa IA para extrair nomes de pessoas naturais de documentos. ["Saiba mais sobre como responder às solicitações de acesso do titular dos dados"](#).

## Visão geral da rede

O Cloud Manager implanta a instância do Cloud Compliance com um grupo de segurança que permite conexões HTTP de entrada da instância do conetor.

Ao usar o Cloud Manager no modo SaaS, a conexão com o Cloud Manager é feita por HTTPS, e os dados privados enviados entre o navegador e a instância de conformidade da nuvem são protegidos com criptografia de ponta a ponta, o que significa que o NetApp e terceiros não podem lê-lo.

Se você precisar usar a interface de usuário local em vez da interface de usuário SaaS por qualquer motivo, ainda poderá ["Acesse a IU local"](#).

As regras de saída estão completamente abertas. O acesso à Internet é necessário para instalar e atualizar o software Cloud Compliance e enviar métricas de uso.

Se você tem exigências estritas da rede, ["Saiba mais sobre os endpoints que o Cloud Compliance contacta"](#).

## Acesso do usuário às informações de conformidade

A função atribuída a cada usuário fornece diferentes recursos no Cloud Manager e no Cloud Compliance:

- **Administradores de conta** podem gerenciar configurações de conformidade e visualizar informações de conformidade para todos os ambientes de trabalho.
- **Os administradores do Workspace** podem gerenciar as configurações de conformidade e exibir informações de conformidade somente para sistemas aos quais eles têm permissões de acesso. Se um administrador do Workspace não puder acessar um ambiente de trabalho no Cloud Manager, ele não poderá ver nenhuma informação de conformidade para o ambiente de trabalho na guia Compliance.
- Os usuários com a função **Visualizador de conformidade na nuvem** só podem visualizar informações de conformidade e gerar relatórios para sistemas que eles têm permissão para acessar. Esses usuários não podem ativar/desativar a digitalização de volumes, buckets ou esquemas de banco de dados.

["Saiba mais sobre as funções do Cloud Manager"](#) e como ["adicione usuários com funções específicas"](#).

## Comece agora

### Implante o Cloud Compliance

Execute algumas etapas para implantar a instância de Cloud Compliance no workspace do Cloud Manager.

#### Início rápido

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



#### Crie um conetor

Se você ainda não tiver um conetor, crie um conetor no Azure ou na AWS. ["Criando um conetor na AWS"](#) Consulte ou ["Criando um conetor no Azure"](#).



## Reveja os pré-requisitos

Certifique-se de que seu ambiente de nuvem atenda aos pré-requisitos, que incluem 16 vCPUs para a instância Cloud Compliance, acesso de saída à Internet para a instância, conectividade entre o conector e o Cloud Compliance pela porta 80 e muito mais. [Veja a lista completa.](#)



## Implante o Cloud Compliance

Inicie o assistente de instalação para implantar a instância de Cloud Compliance no Cloud Manager.



## Inscreva-se no serviço Cloud Compliance

Os primeiros 1 TB de dados verificados pelo Cloud Compliance no Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto.

### Criando um conector

Se você ainda não tiver um conector, crie um conector no Azure ou na AWS. ["Criando um conector na AWS"](#) Consulte ou ["Criando um conector no Azure"](#). Na maioria dos casos, você provavelmente terá um conector configurado antes de tentar ativar o Cloud Compliance porque a maioria ["Os recursos do Cloud Manager precisam de um conector"](#), mas há casos em que você precisa configurar um agora.

Há alguns cenários em que você precisa usar um conector na AWS ou no Azure para conformidade com a nuvem.

- Ao digitalizar dados no Cloud Volumes ONTAP na AWS ou nos buckets do AWS S3, você usa um conector na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um conector no Azure.
- Os bancos de dados podem ser digitalizados usando qualquer um dos conectores.

Como você pode ver, pode haver algumas situações em que você precisa usar ["Vários conectores"](#).



Se você está planejando digitalizar o Azure NetApp Files, você precisa garantir que está implantando na mesma região que os volumes que deseja digitalizar.

### Rever pré-requisitos

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

### Ative o acesso de saída à Internet

A conformidade com a nuvem requer acesso de saída à Internet. Se a sua rede virtual usar um servidor proxy para acesso à Internet, certifique-se de que a instância do Cloud Compliance tenha acesso de saída à Internet para contactar os seguintes endpoints. Observe que o Cloud Manager implanta a instância de Cloud Compliance na mesma sub-rede que o conector.



Endpoints	Finalidade
<a href="https://cloudmanager.cloud.NetApp.com">https://cloudmanager.cloud.NetApp.com</a>	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
<a href="https://NetApp-cloud-account.auth0.com">https://NetApp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
<a href="https://cloud-compliance-support-NetApp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-NetApp.s3.us-west-2.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srnrn.cloudfront.net/">https://dseasb33srnrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Fornecer acesso a imagens de software, manifestos e modelos.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Permite que o NetApp transmita dados de Registros de auditoria.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	Permite que o Cloud Compliance acesse e baixe manifestos e modelos e envie logs e métricas.

### **Certifique-se de que o Cloud Manager tenha as permissões necessárias**

Certifique-se de que o Cloud Manager tenha permissões para implantar recursos e criar grupos de segurança para a instância do Cloud Compliance. Você pode encontrar as permissões mais recentes do Cloud Manager no ["As políticas fornecidas pela NetApp"](#).

### **Verifique os limites do seu vCPU**

Certifique-se de que o limite de vCPU do seu provedor de nuvem permita a implantação de uma instância com 16 núcleos. Você precisará verificar o limite do vCPU para a família de instâncias relevante na região em que o Cloud Manager está sendo executado.

Na AWS, a família de instâncias é *instâncias padrão sob demanda*. No Azure, a família de instâncias é *Standard D5v3 Family*.

Para obter mais detalhes sobre os limites do vCPU, consulte o seguinte:

- ["Documentação da AWS: Limites de serviço do Amazon EC2"](#)
- ["Documentação do Azure: Cotas de vCPU de máquina virtual"](#)

### **Garantir que o Cloud Manager possa acessar o Cloud Compliance**

Garanta a conectividade entre o conector e a instância de conformidade com a nuvem. O grupo de segurança do conector deve permitir o tráfego de entrada e saída pela porta 80 de e para a instância do Cloud Compliance.

Essa conexão permite a implantação da instância de conformidade na nuvem e permite exibir informações na guia conformidade.

### **Configure a descoberta do Azure NetApp Files**

Antes de poder digitalizar volumes para Azure NetApp Files, ["O Cloud Manager deve estar configurado para descobrir a configuração"](#).

## Garanta que você mantenha o Cloud Compliance em execução

A instância do Cloud Compliance precisa continuar a analisar seus dados continuamente.

## Garanta a conectividade do navegador da Web com o Cloud Compliance

Depois que o Cloud Compliance estiver ativado, certifique-se de que os usuários acessem a interface do Cloud Manager a partir de um host que tenha uma conexão com a instância do Cloud Compliance.

A instância Cloud Compliance usa um endereço IP privado para garantir que os dados indexados não sejam acessíveis à Internet. Como resultado, o navegador da Web que você usa para acessar o Cloud Manager deve ter uma conexão com esse endereço IP privado. Essa conexão pode vir de uma conexão direta com a AWS ou o Azure (por exemplo, uma VPN) ou de um host que esteja dentro da mesma rede que a instância de conformidade com a nuvem.

## Implantando a instância de Cloud Compliance

Você implanta uma instância do Cloud Compliance para cada instância do Cloud Manager.

### Passos

1. No Cloud Manager, clique em **Cloud Compliance**.
2. Clique em **Ativar Cloud Compliance** para iniciar o assistente de implantação.

Working Environment Compliance Replication Kubernetes Backup & Restore Monitoring Timeline

Cloud Compliance

How does it work?

### Always-on Privacy & Compliance Controls

Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.

[Activate Cloud Compliance](#)

Compliance Status

Data Distribution

- 75% Non-Sensitive
- 20% Personal
- 5% Sensitive Personal

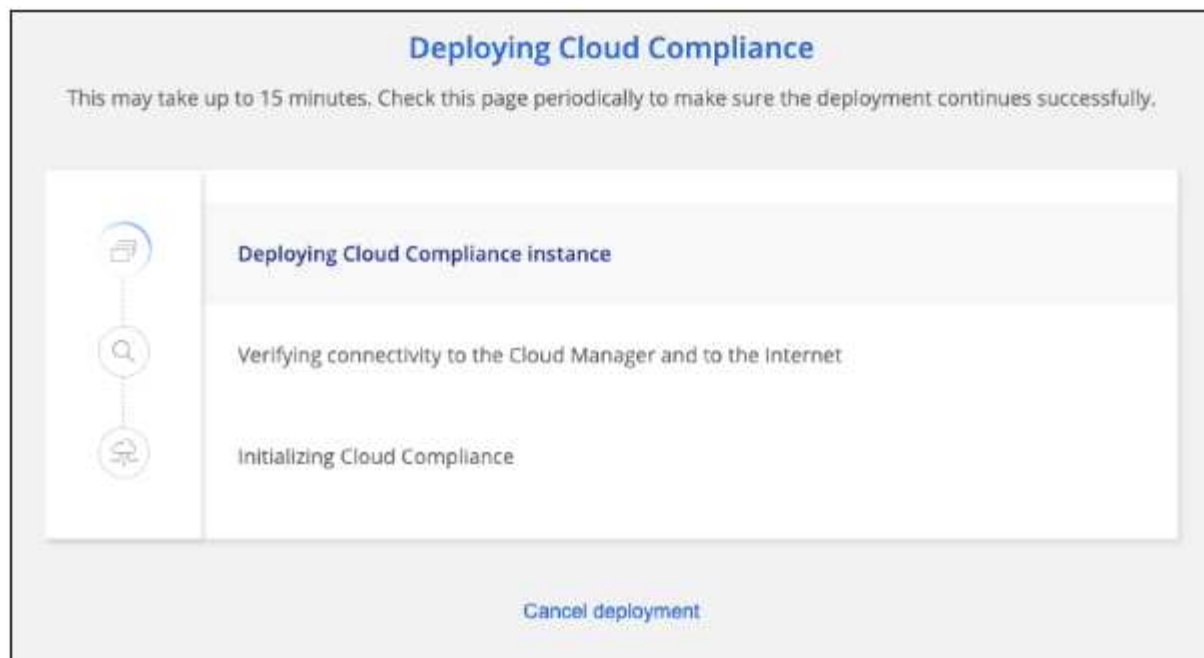
28,000 Personal Files

- Email Address: 2,700 Files
- Credit Card: 2,700 Files

7,000 Sensitive Personal Files

- Health: 2,700 Files
- Identity: 2,700 Files

3. O assistente exibe o progresso à medida que passa pelas etapas de implantação. Ele vai parar e pedir a entrada se ele se deparar com quaisquer problemas.



4. Quando a instância for implantada, clique em **Continue to Configuration** para ir para a página *Scan Configuration*.

### Resultado

O Cloud Manager implanta a instância de Cloud Compliance no seu provedor de nuvem.

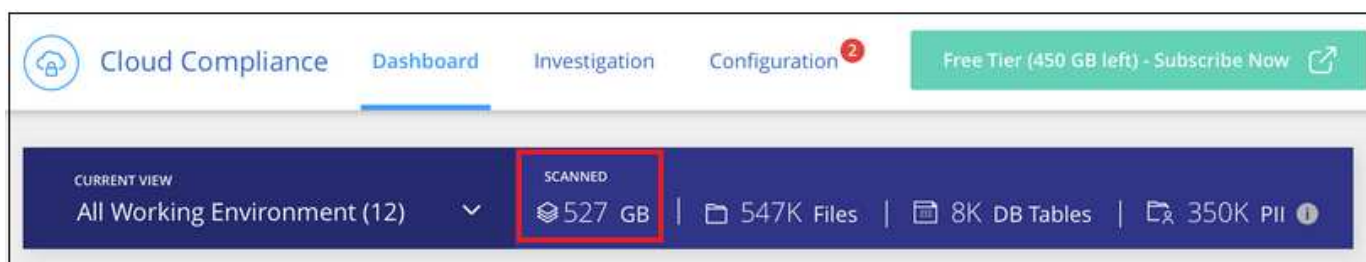
### O que vem a seguir

Na página Configuração de digitalização, você pode selecionar os ambientes de trabalho, volumes e buckets que você deseja verificar para conformidade. Você também pode se conectar a um servidor de banco de dados para verificar esquemas de banco de dados específicos. Ative o Cloud Compliance em qualquer uma dessas fontes de dados.

### Subscrever o serviço Cloud Compliance

Os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto.

Você pode se inscrever a qualquer momento e não será cobrado até que a quantidade de dados exceda 1 TB. Você sempre pode ver a quantidade total de dados que está sendo digitalizada no Painel de conformidade da nuvem. E o botão *Inscrever-se agora* facilita a assinatura quando estiver pronto.



**Observação:** se você for solicitado pelo Cloud Compliance para se inscrever, mas já tiver uma assinatura do Azure, provavelmente estará usando a antiga assinatura do **Gerenciador de nuvem** e precisará mudar para a nova assinatura do **Gerenciador de nuvem** do NetApp. [Mudando para o novo plano do NetApp Cloud](#)

[Manager no Azure](#) Consulte para obter detalhes.

## Passos

Essas etapas devem ser concluídas por um usuário que tenha a função *Account Admin*.

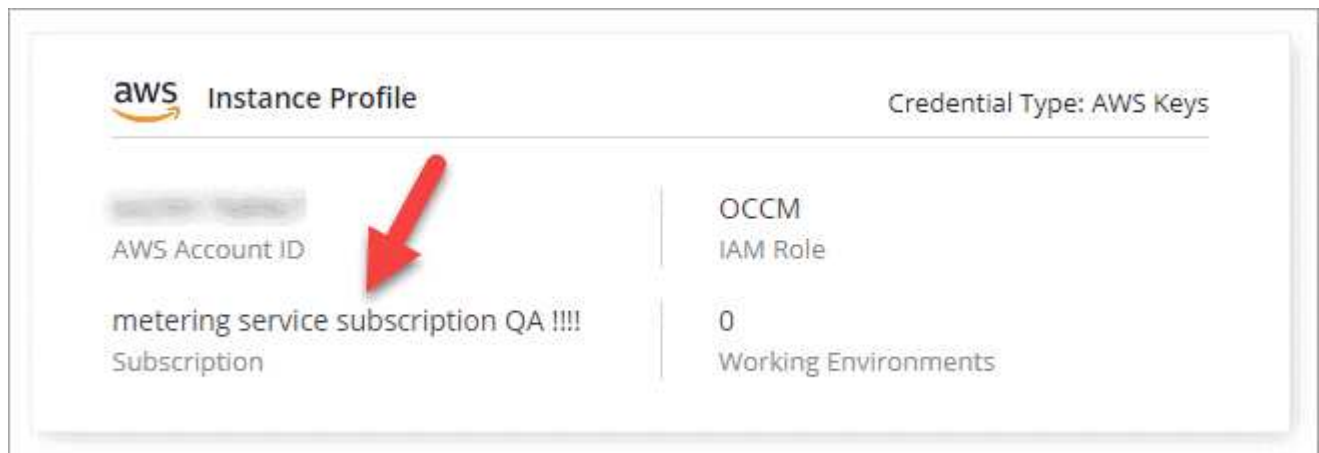
1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



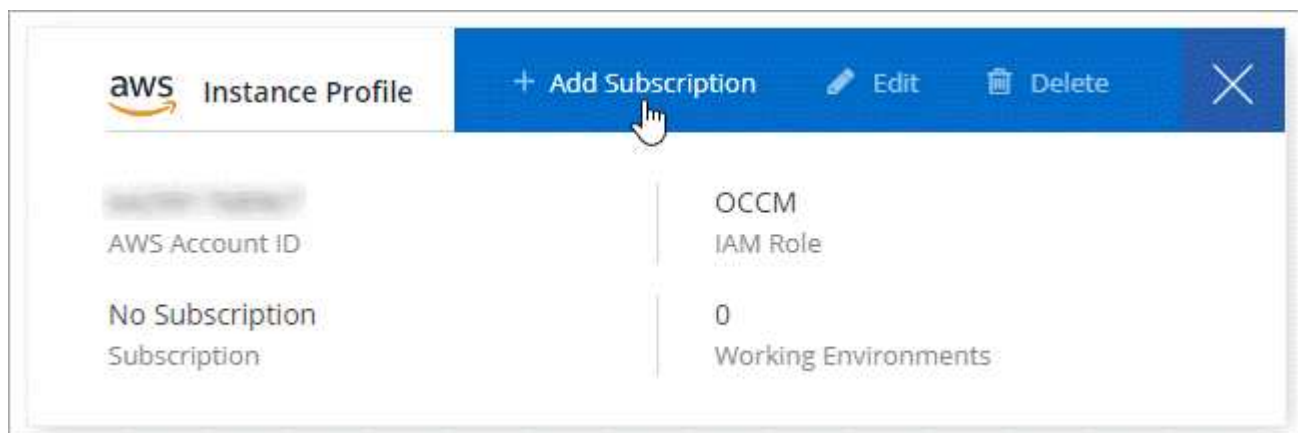
2. Encontre as credenciais para o perfil de instância da AWS ou identidade do serviço gerenciado do Azure.

A assinatura deve ser adicionada ao Perfil de instância ou identidade de serviço gerenciado. O carregamento não funciona de outra forma.

Se você já tem uma assinatura, então você está tudo pronto - não há mais nada que você precisa fazer.



3. Se você ainda não tiver uma assinatura, passe o Mouse sobre as credenciais e clique no menu de ação.
4. Clique em **Adicionar assinatura**.



5. Clique em **Adicionar assinatura**, clique em **continuar** e siga as etapas.

O vídeo a seguir mostra como associar uma assinatura do Marketplace a uma assinatura da AWS:

► [https://docs.netapp.com/pt-br/occm38//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/pt-br/occm38//media/video_subscribing_aws.mp4) (video)

O vídeo a seguir mostra como associar uma assinatura do Marketplace a uma assinatura do Azure:

► [https://docs.netapp.com/pt-br/occm38//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/pt-br/occm38//media/video_subscribing_azure.mp4) (video)

## Mudando para o novo plano do Cloud Manager no Azure

O Cloud Compliance foi adicionado à assinatura do Azure Marketplace chamada **Gerenciador de nuvem da NetApp** em 7 de outubro de 2020. Se você já tiver a assinatura original do Azure **Cloud Manager**, ela não permitirá que você use o Cloud Compliance.

Você precisa seguir estas etapas e selecionar a nova assinatura **Gerenciador de nuvem do NetApp** e remover a antiga assinatura **Gerenciador de nuvem**.



Se sua assinatura já tiver sido emitida com uma oferta particular especial, você precisa entrar em Contato com a NetApp para que possamos emitir uma nova oferta privada especial com conformidade incluída.

### Passos

Essas etapas são semelhantes à adição de uma nova assinatura conforme descrito acima, mas variam em alguns lugares.

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Encontre as credenciais para a identidade do Serviço gerenciado do Azure para a qual você deseja alterar a assinatura e passe o Mouse sobre as credenciais e clique em **assinatura associada**.

Os detalhes da sua assinatura atual do Marketplace são exibidos.

3. Clique em **Adicionar assinatura**, clique em **continuar** e siga as etapas. Você é redirecionado para o portal do Azure para criar a nova assinatura.
4. Certifique-se de selecionar o plano **Gerenciador de nuvem da NetApp** que fornece acesso ao Cloud Compliance e não ao **Gerenciador de nuvem**.
5. Siga as etapas no vídeo para associar uma assinatura do Marketplace a uma assinatura do Azure:

► [https://docs.netapp.com/pt-br/occm38//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/pt-br/occm38//media/video_subscribing_azure.mp4) (video)

6. Retorne ao Cloud Manager, selecione a nova assinatura e clique em **Associate**.
7. Para verificar se sua assinatura foi alterada, passe o Mouse sobre a assinatura "i" acima no cartão de credenciais.

Agora você pode cancelar sua assinatura antiga no portal do Azure.

8. No portal do Azure, acesse Software as a Service (SaaS), selecione a assinatura e clique em **Cancelar inscrição**.

## 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**.

View Dashboard >

Scan Configuration How to add AWS accounts to scan S3

**AWS Account Number 1**  
Amazon S3

To enable Compliance for Amazon S3 on this AWS account or other, go to Working Environment tab, select the Amazon S3 cloud and activate Compliance from the right hand panel.

**Azure Netapp Files**  
Azure NetApp Files

Activate Compliance for All Volumes  
or select Volumes

**Working Environment Name 1**  
Cloud Volumes ONTAP

Activate Compliance for All Volumes  
or select Volumes

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.

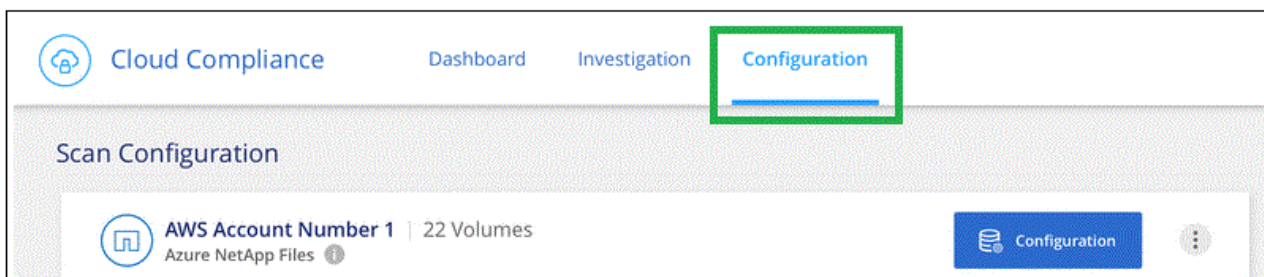


Para o Azure NetApp Files, o Cloud Compliance só pode verificar volumes que estejam na mesma região que o Cloud Manager.

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.

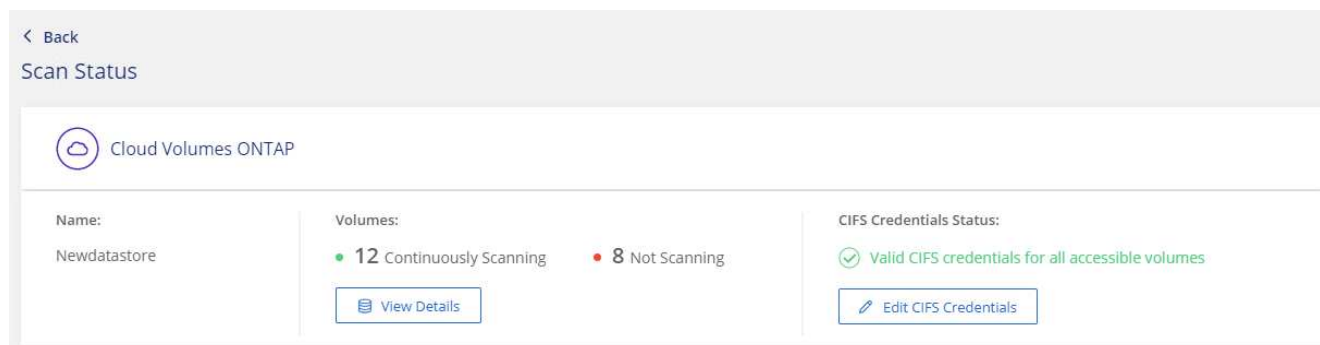
3. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Cloud Compliance para que ela possa acessar os dados em cada volume.
4. Se você usar CIFS, forneça as credenciais do Cloud Compliance para que ele possa verificar os volumes CIFS.
  - a. Na parte superior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



Back

Newdatastore Scan Configuration

Activate Compliance for all Volumes | 28/28 Volumes selected for compliance scan

Compliance	Name ↑↑	Protocol ↑↑	Status ↑↑	Required Action ↑↑
<input checked="" type="checkbox"/>	10.160.7.6:/yuval22	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	10.160.7.6:/yuvalnewtarget	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	\\10.160.7.6\Danny_share	CIFS	No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

### 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.

Back

Newdatastore Scan Configuration

Activate Compliance for all Volumes | 27/28 Volumes selected for compliance scan

Compliance	Volume Name ↑↑	Status	Required Action
<input checked="" type="checkbox"/>	VolumeName1	Not Scanning	Add CIFS Credentials
<input checked="" type="checkbox"/>	VolumeName2	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	Not Scanning	
<input checked="" type="checkbox"/>	VolumeName4	Continuously Scanning	
<input checked="" type="checkbox"/>	VolumeName5	Continuously Scanning	

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 <b>Ativar conformidade para todos os volumes</b> 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 <b>Ativar conformidade para todos os volumes</b> 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

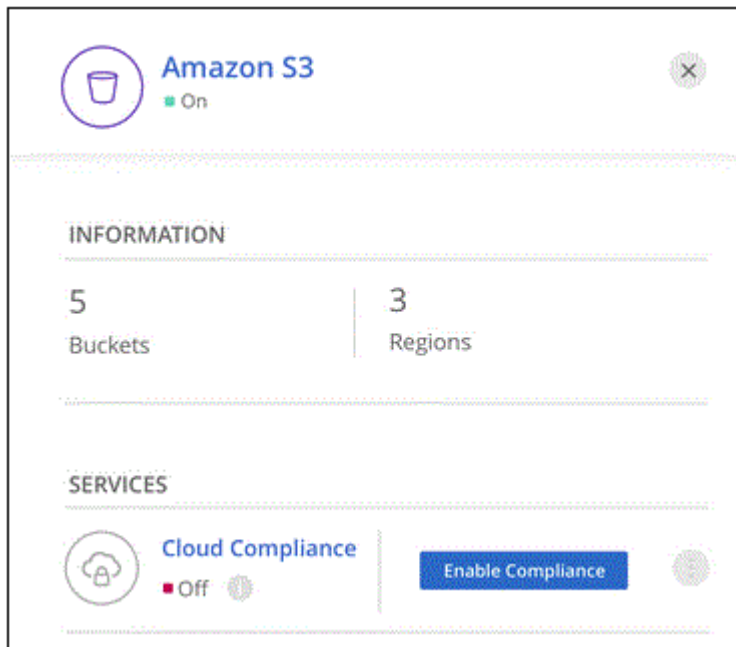
Ative o Cloud Compliance no Amazon S3 depois de verificar os pré-requisitos.

#### Passos

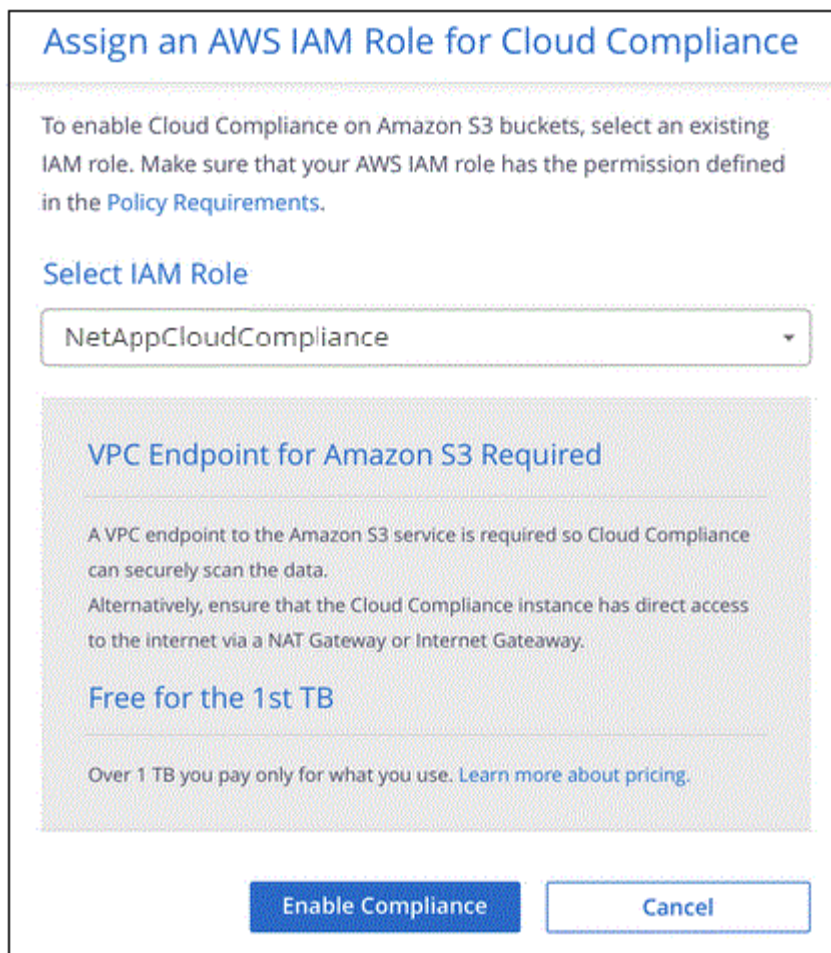
1. Na parte superior do Cloud Manager, clique em **ambientes de trabalho**.
2. Selecione o ambiente de trabalho do Amazon S3.



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

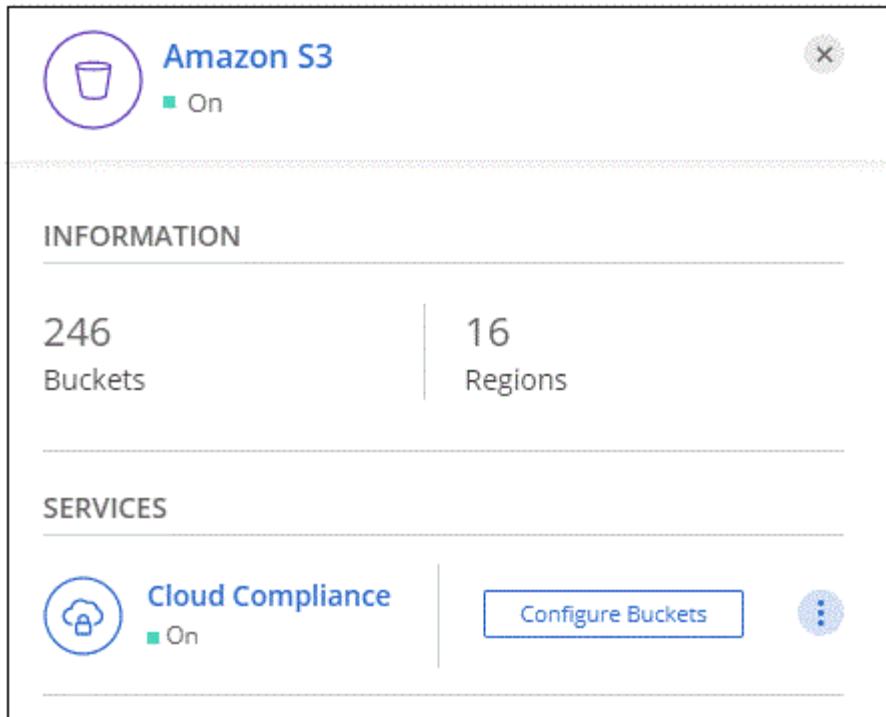
Depois que o Cloud Manager ativar o Cloud Compliance no Amazon S3, a próxima etapa é configurar os buckets que você deseja analisar.

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.

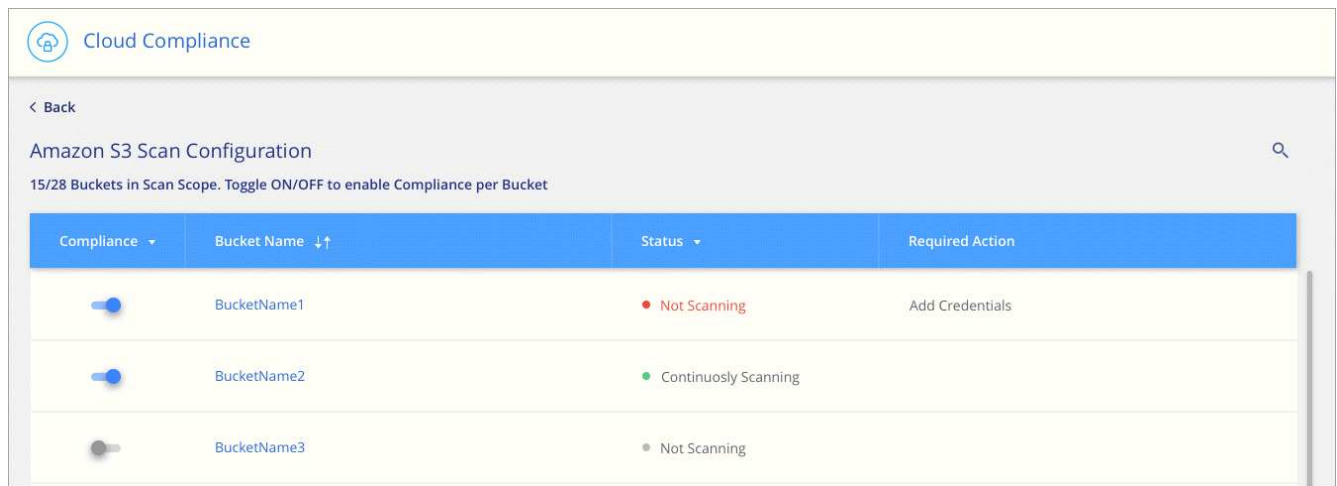
O Cloud Compliance também [Examine os buckets do S3 que estão em diferentes contas da AWS](#) pode .

### 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

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> 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": "*"
    }
  ]
}
```

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



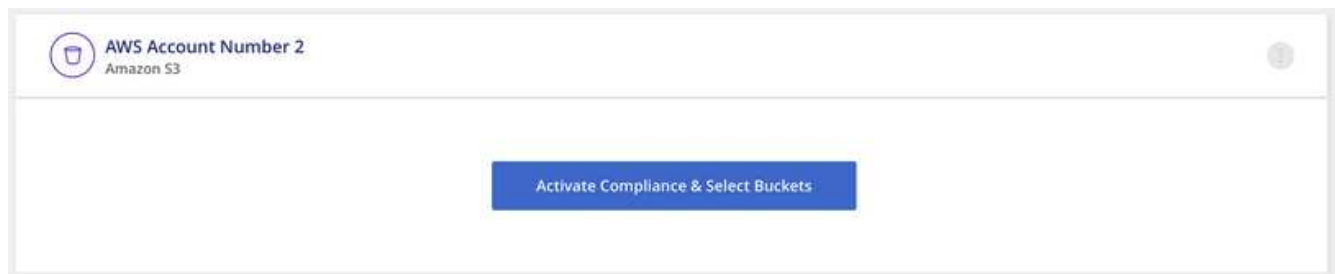
```

{
  "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.

- 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.



- 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.

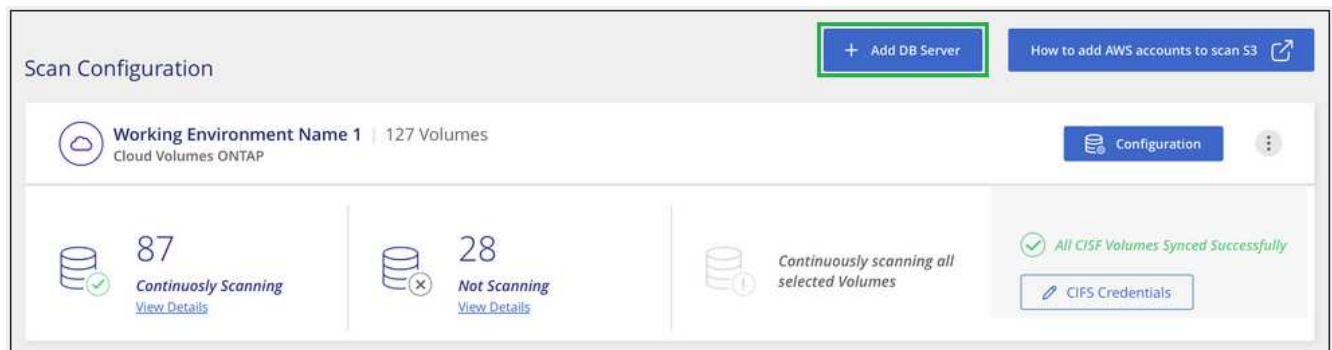
**Observação:** para MongoDB, é necessária uma função de administração somente leitura.

#### 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

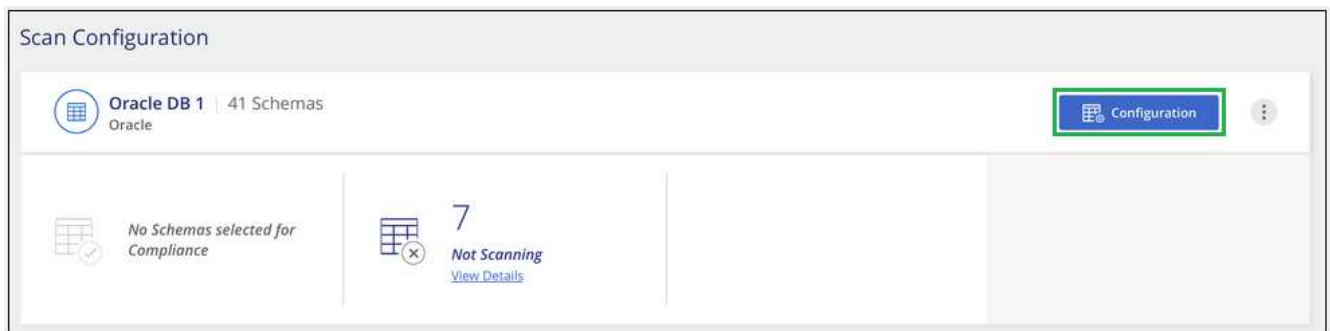
Password

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			
Compliance	Schema Name	Status	Required Action
<input 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](#)".

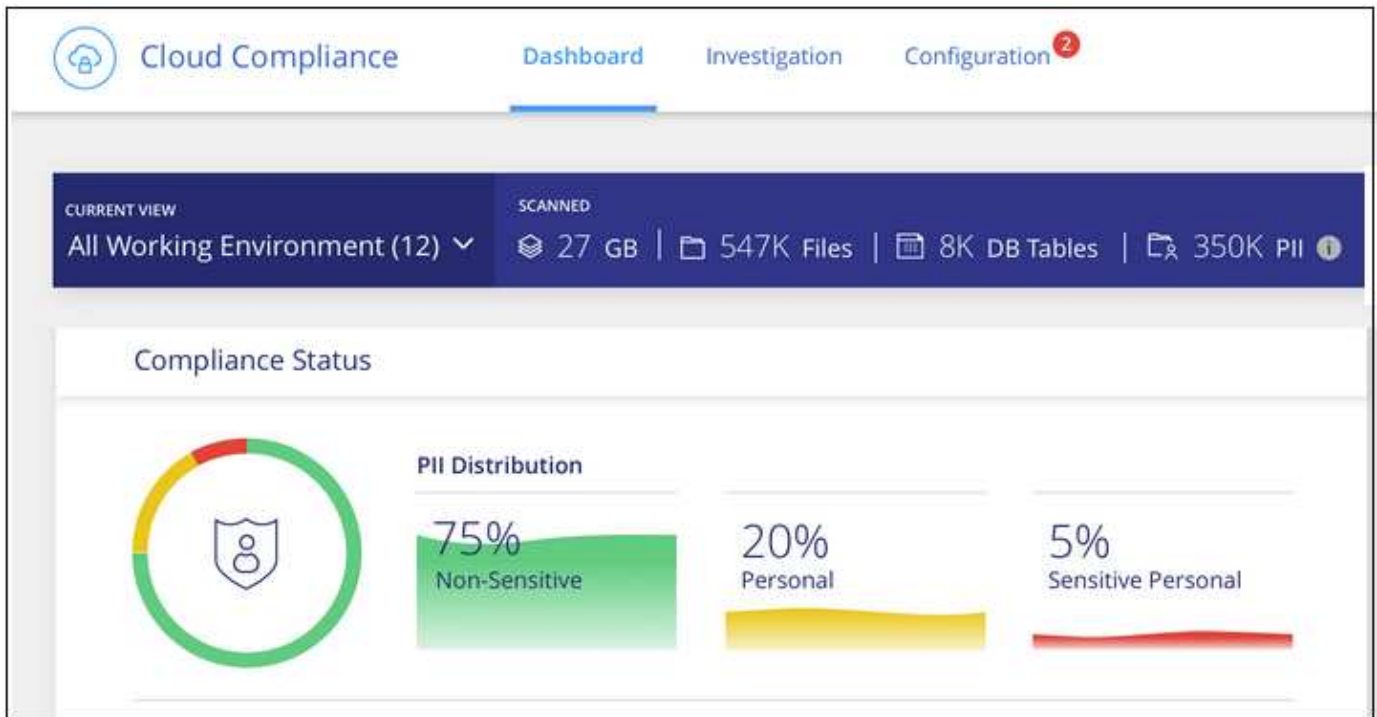
2. Para volumes DP criados a partir de volumes de origem SMB, a partir da CLI do ONTAP, configure os volumes de destino SMB para acesso aos dados. (Isso não é necessário para volumes NFS porque o acesso aos dados é habilitado automaticamente pelo Cloud Compliance.)
  - a. ["Crie um compartilhamento SMB 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.

## Ter visibilidade e controle de dados privados

Obtenha controle de seus dados privados visualizando detalhes sobre os dados pessoais e dados pessoais confidenciais em sua organização. Você também pode ter visibilidade revisando as categorias e tipos de arquivo que o Cloud Compliance encontrou nos seus dados.

Por padrão, o dashboard do Cloud Compliance exibe dados de conformidade para todos os ambientes de trabalho e bancos de dados.



Se desejar ver os dados apenas para alguns dos ambientes de trabalho [selecione esses ambientes de trabalho](#), .

## Dados pessoais

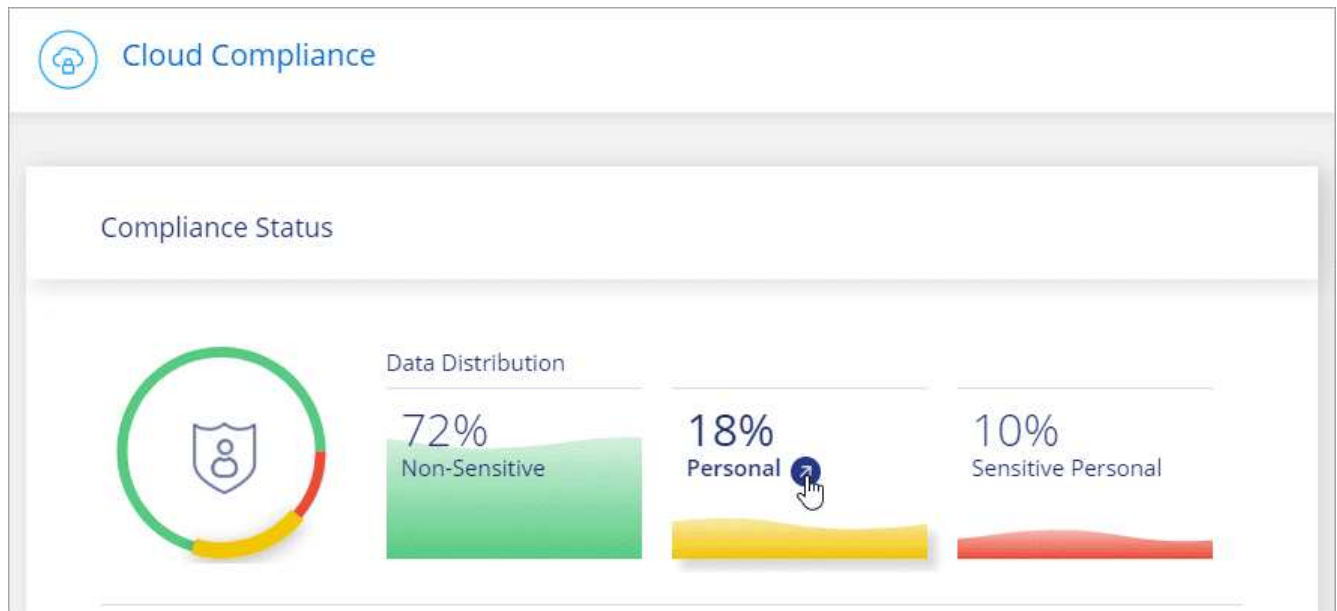
O Cloud Compliance identifica automaticamente palavras, strings e padrões específicos (Regex) dentro dos dados. Por exemplo, informações de identificação pessoal (PII), números de cartão de crédito, números de segurança social, números de conta bancária e muito mais. [Veja a lista completa](#).

Para alguns tipos de dados pessoais, o Cloud Compliance usa *validação de proximidade* para validar suas descobertas. A validação ocorre procurando uma ou mais palavras-chave predefinidas próximas aos dados pessoais encontrados. Por exemplo, o Cloud Compliance identifica um SSN (número de segurança social) dos EUA como um SSN se ele vir uma palavra de proximidade ao lado dele - por exemplo, *SSN* ou *segurança social*. [A lista abaixo](#) Mostra quando o Cloud Compliance usa validação de proximidade.

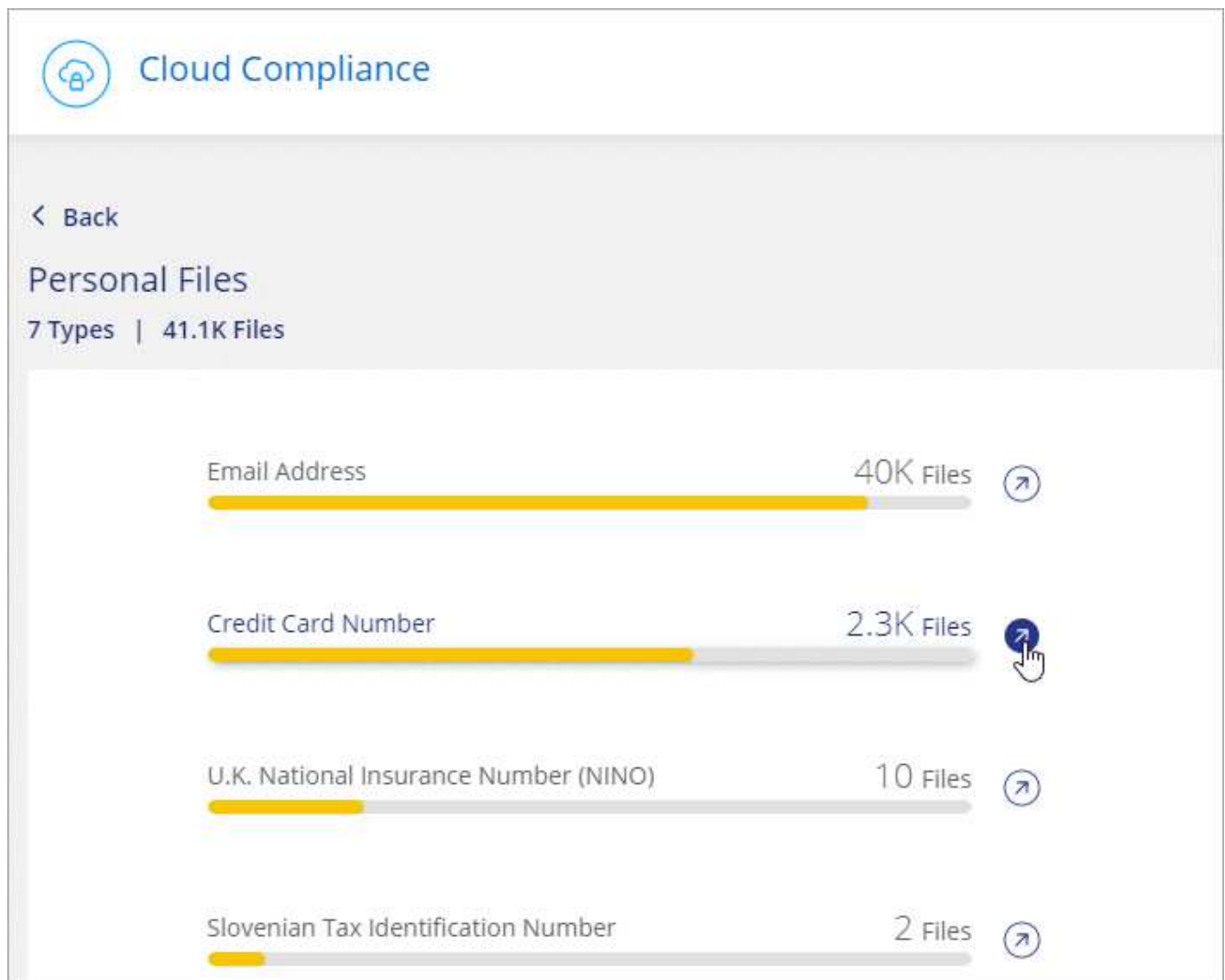
## Visualização de arquivos que contêm dados pessoais

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance** e clique na guia **Dashboard**.
2. Para investigar os detalhes de todos os dados pessoais, clique no ícone ao lado da porcentagem de dados pessoais.

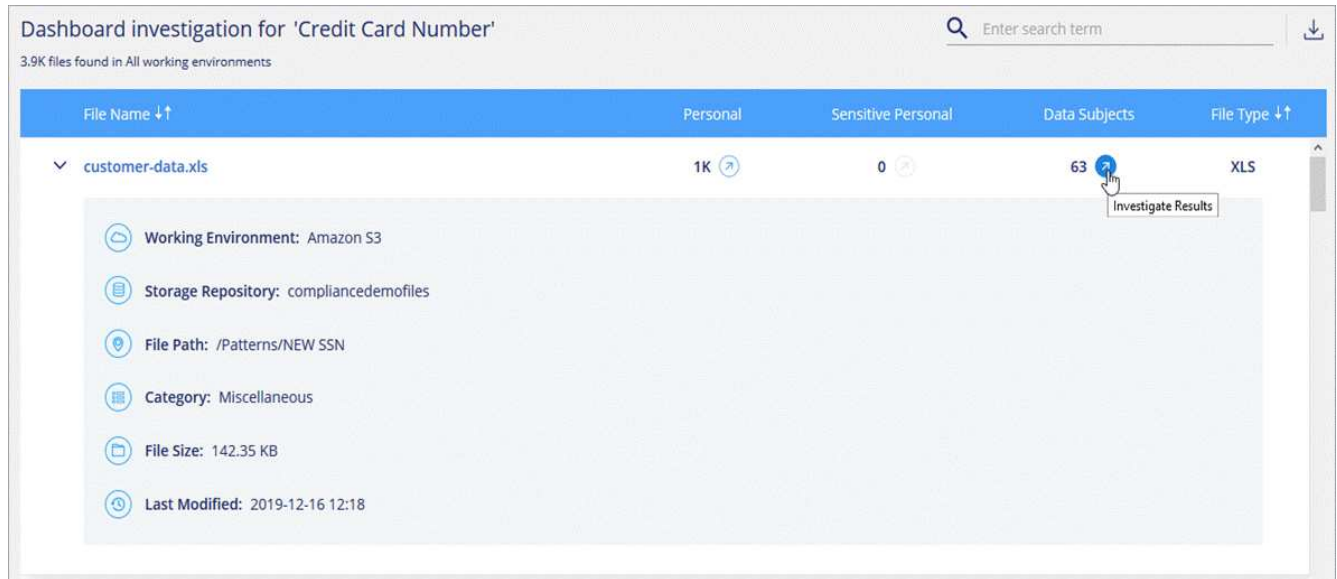


- Para investigar os detalhes de um tipo específico de dados pessoais, clique em **Exibir todos** e, em seguida, clique no ícone **investigar resultados** para um tipo específico de dados pessoais.



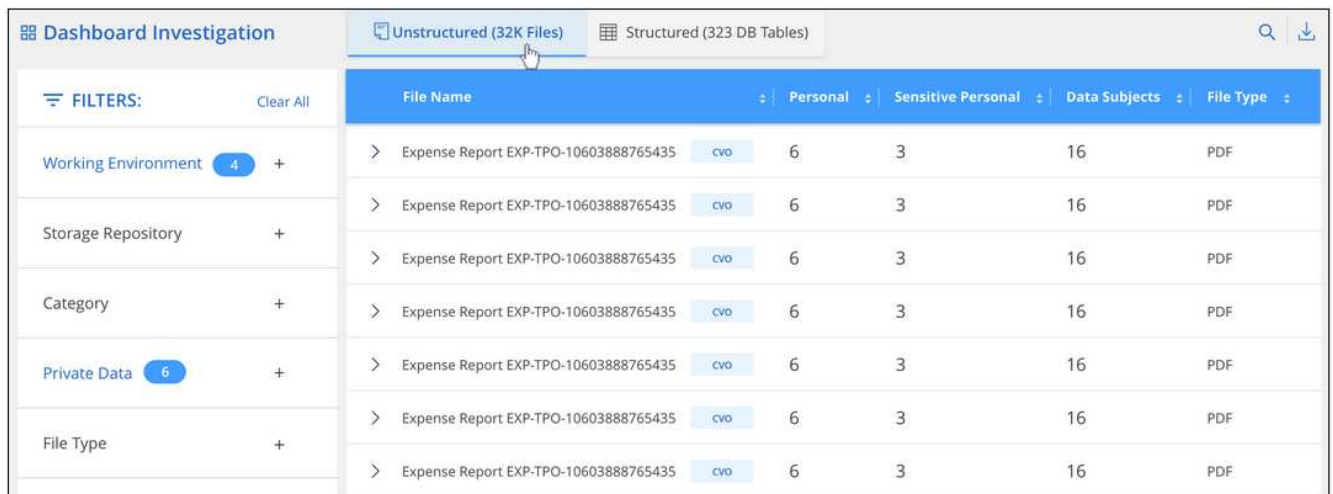


- Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.



- Você também pode filtrar o conteúdo da página de investigação para exibir apenas os resultados que deseja ver. As guias de nível superior permitem exibir dados de arquivos (dados não estruturados) ou de bancos de dados (dados estruturados).

Em seguida, você tem filtros para ambiente de trabalho, repositório de armazenamento, categoria, dados privados, tipo de arquivo, data da última modificação e se as permissões do objeto S3 estão abertas ao acesso público.



## Tipos de dados pessoais

Os dados pessoais encontrados nos arquivos podem ser dados pessoais gerais ou identificadores nacionais. A terceira coluna identifica se o Cloud Compliance usa [validação de proximidade](#) para validar suas descobertas para o identificador.

<b>Tipo</b>	<b>Identificador</b>	<b>Validação de proximidade?</b>
Geral	Endereço de e-mail	Não
	Número do cartão de crédito	Não
	Número IBAN (número de conta bancária internacional)	Não

<b>Tipo</b>	<b>Identificador</b>	<b>Validação de proximidade?</b>
Identificadores nacionais	ID belga (Numero National)	Sim
	Identidade Brasileira (CPF)	Sim
	ID búlgaro (UCN)	Sim
	Licença de motorista da Califórnia	Sim
	ID croata (OIB)	Sim
	Número de identificação fiscal do Chipre (TIC)	Sim
	Código checo/eslovaco	Sim
	ID dinamarquesa (CPR)	Sim
	ID holandesa (BSN)	Sim
	ID da Estónia	Sim
	ID finlandês (HETU)	Sim
	Número de identificação fiscal Francês (SPI)	Sim
	Número de identificação fiscal Alemão (Steuerliche Identifikationsrommer)	Sim
	ID grega	Sim
	Número de identificação fiscal húngaro	Sim
	ID irlandesa (PPS)	Sim
	ID israelense	Sim
	Número de identificação fiscal italiano	Sim
	ID letão	Sim
	ID lituano	Sim
	ID Luxemburgo	Sim
	ID maltês	Sim
	ID polaco (PESEL)	Sim
	Número de identificação fiscal Português (NIF)	Sim
	Identificação romena (CNP)	Sim
	Slovenian ID (EMSO)	Sim
	ID sul-africana	Sim
	Número de identificação fiscal espanhol	Sim
ID sueco	Sim	
ID DO REINO UNIDO (NINO)	Sim	
Número da Segurança Social dos EUA (SSN)	Sim	

## Dados pessoais confidenciais

O Cloud Compliance identifica automaticamente tipos especiais de informações pessoais confidenciais, conforme definido por regulamentos de privacidade, "artigos 9.º e 10.º do RGPD" como . Por exemplo, informações sobre a saúde de uma pessoa, origem étnica ou orientação sexual. [Veja a lista completa.](#)

O Cloud Compliance usa inteligência artificial (AI), processamento de linguagem natural (NLP), aprendizado de máquina (ML) e computação cognitiva (CC) para entender o significado do conteúdo verificado para extrair entidades e categorizá-lo de acordo.

Por exemplo, uma categoria de dados confidenciais do GDPR é a origem étnica. Por causa de suas habilidades de PNL, o Cloud Compliance pode distinguir a diferença entre uma frase que diz "George é mexicano" (indicando dados confidenciais conforme especificado no artigo 9 do GDPR), em comparação com "George está comendo comida mexicana".

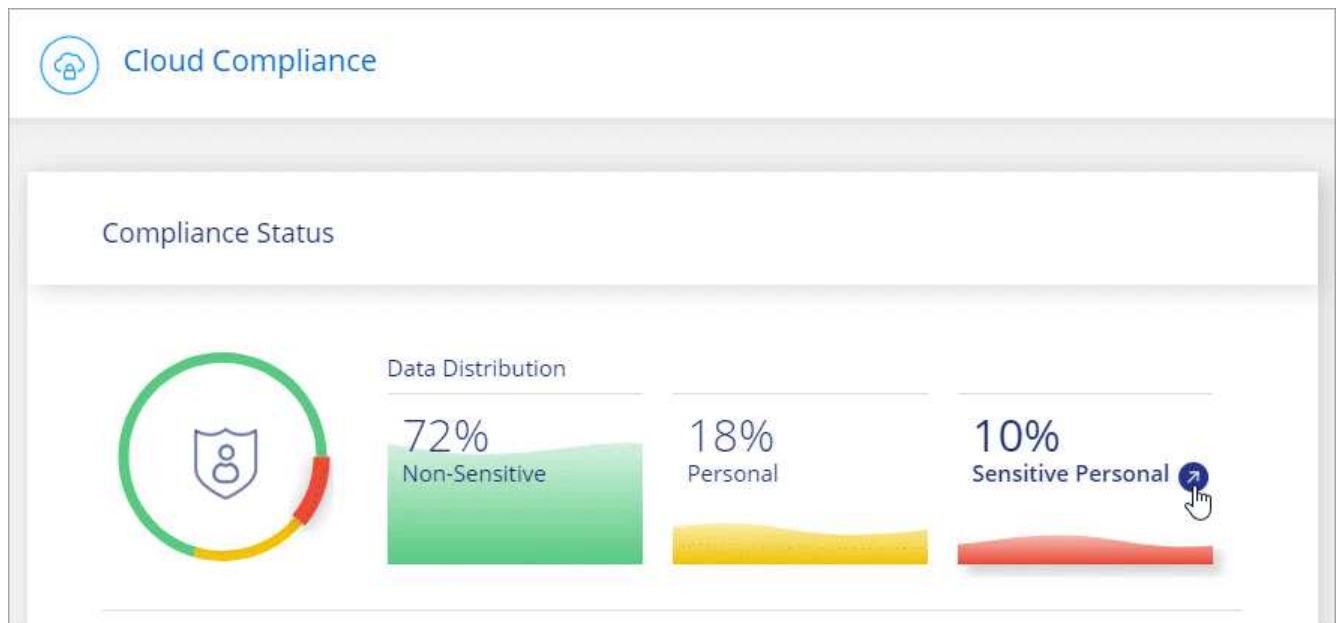


Apenas o inglês é suportado durante a digitalização de dados pessoais confidenciais. O suporte para mais idiomas será adicionado mais tarde.

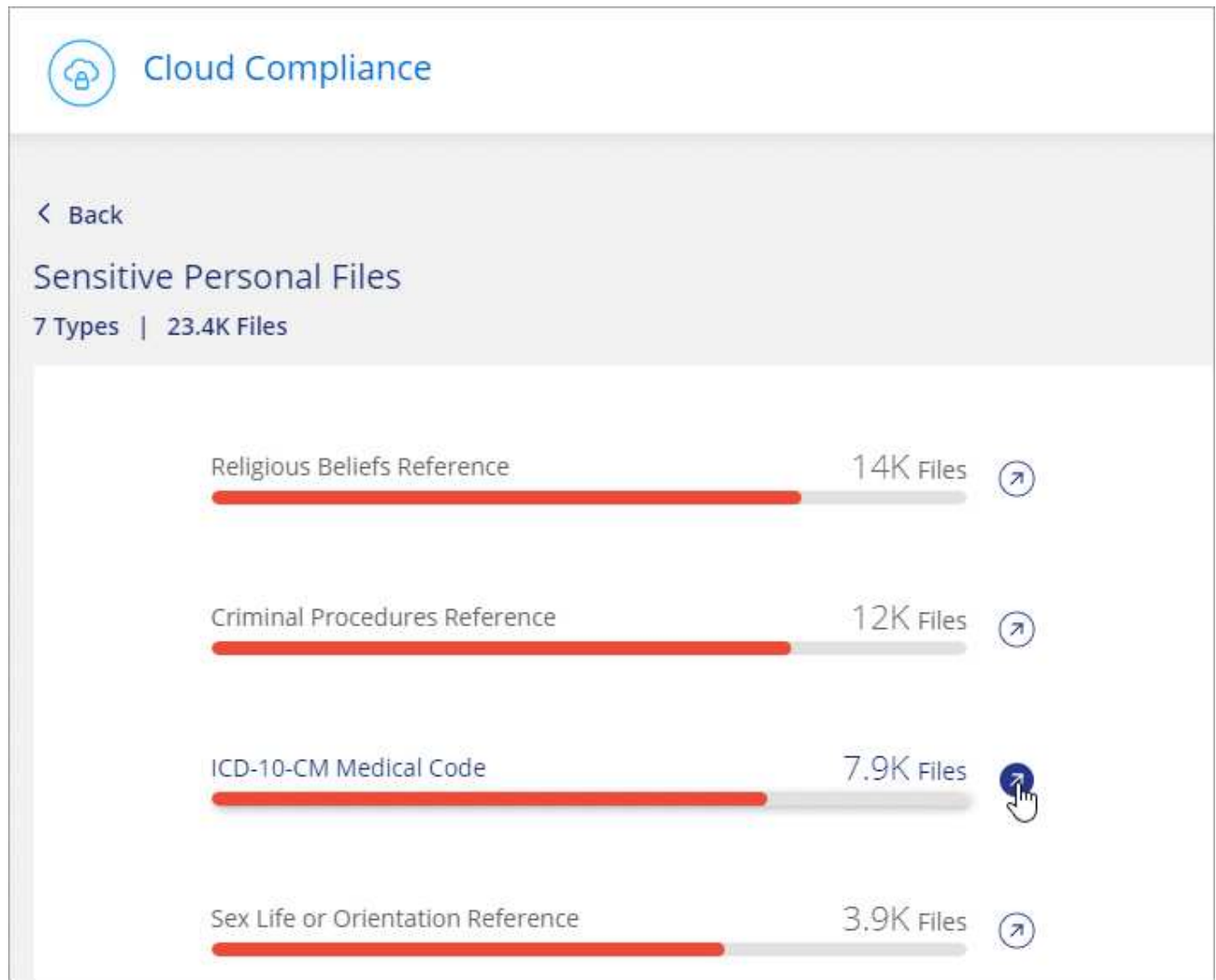
## Visualização de arquivos que contêm dados pessoais confidenciais

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Para investigar os detalhes de todos os dados pessoais confidenciais, clique no ícone ao lado da porcentagem de dados pessoais confidenciais.



3. Para investigar os detalhes de um tipo específico de dados pessoais confidenciais, clique em **Exibir todos** e, em seguida, clique no ícone **investigar resultados** para um tipo específico de dados pessoais confidenciais.



4. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

### **Tipos de dados pessoais sensíveis**

Os dados pessoais confidenciais que o Cloud Compliance pode encontrar nos arquivos incluem o seguinte:

#### **Referência de procedimentos criminais**

Dados relativos às condenações e infrações penais de uma pessoa singular.

#### **Etnia de referência**

Dados relativos à origem racial ou étnica de uma pessoa singular.

#### **Referência de Saúde**

Dados relativos à saúde de uma pessoa singular.

#### **Códigos médicos CID-9-CM**

Códigos utilizados na indústria médica e de saúde.

#### **Códigos médicos CID-10-CM**

Códigos utilizados na indústria médica e de saúde.

### Referência de crenças filosóficas

Dados relativos às crenças filosóficas de uma pessoa natural.

### Referência de crenças religiosas

Dados relativos às crenças religiosas de uma pessoa natural.

### Vida sexual ou Orientação Referência

Dados relativos à vida sexual ou orientação sexual de uma pessoa natural.

## Categorias

O Cloud Compliance pega os dados que digitalizou e os divide em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. [Veja a lista de categorias.](#)

As categorias podem ajudá-lo a entender o que está acontecendo com seus dados, mostrando os tipos de informações que você tem. Por exemplo, uma categoria como currículos ou contratos de funcionários pode incluir dados confidenciais. Ao investigar os resultados, você pode descobrir que os contratos de funcionários são armazenados em um local inseguro. Você pode então corrigir esse problema.

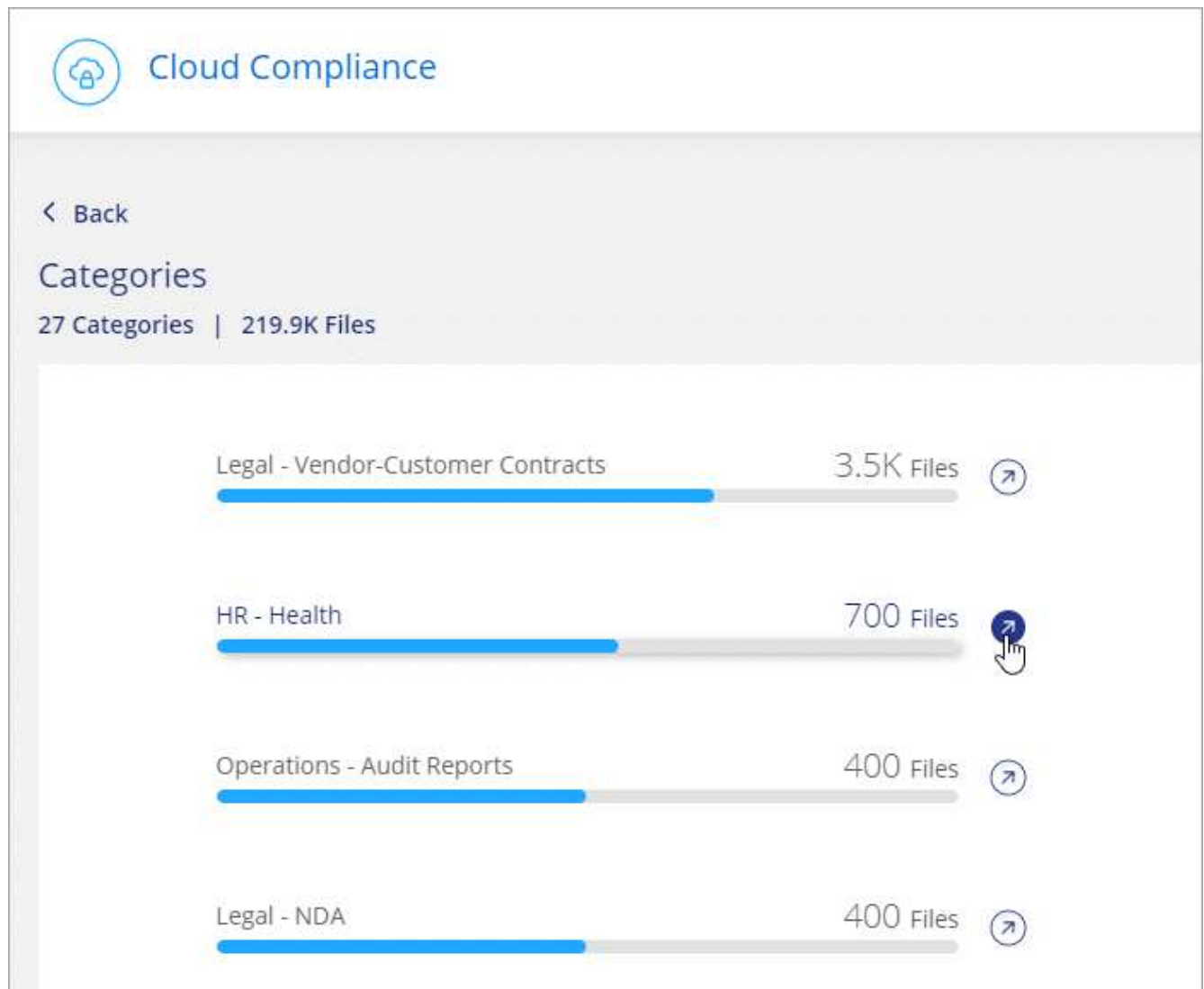


Apenas o inglês é suportado para categorias. O suporte para mais idiomas será adicionado mais tarde.

### Visualizar ficheiros por categorias

#### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique no ícone **investigar resultados** para uma das 4 categorias principais diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone de qualquer uma das categorias.



3. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

### Tipos de categorias

O Cloud Compliance categoriza seus dados da seguinte forma:

#### Finanças

- Balanços
- Ordens compra
- Faturas
- Relatórios trimestrais

#### HR

- Verificações de fundo
- Planos de compensação
- Contratos de funcionários
- Avaliações de funcionários

- Saúde
- Retoma

### **Legal**

- NDAs
- Contratos fornecedor-cliente

### **Marketing**

- Campanhas
- Conferências

### **Operações**

- Relatórios de auditoria

### **Vendas**

- Ordens vendas

### **Serviços**

- RFI
- RFP
- SOW
- Formação

### **Suporte**

- Reclamações e bilhetes

### **Categorias de metadados**

- Dados da aplicação
- Arquivar ficheiros
- Áudio
- Dados de aplicações empresariais
- Ficheiros CAD
- Código
- Banco de dados e arquivos de índice
- Arquivos de design
- Dados do aplicativo de e-mail
- Executáveis
- Dados de aplicações financeiras
- Dados da aplicação de integridade
- Imagens
- Registos
- Documentos diversos
- Apresentações diversas



- Folhas de cálculo diversas
- Vídeos

## Tipos de ficheiros

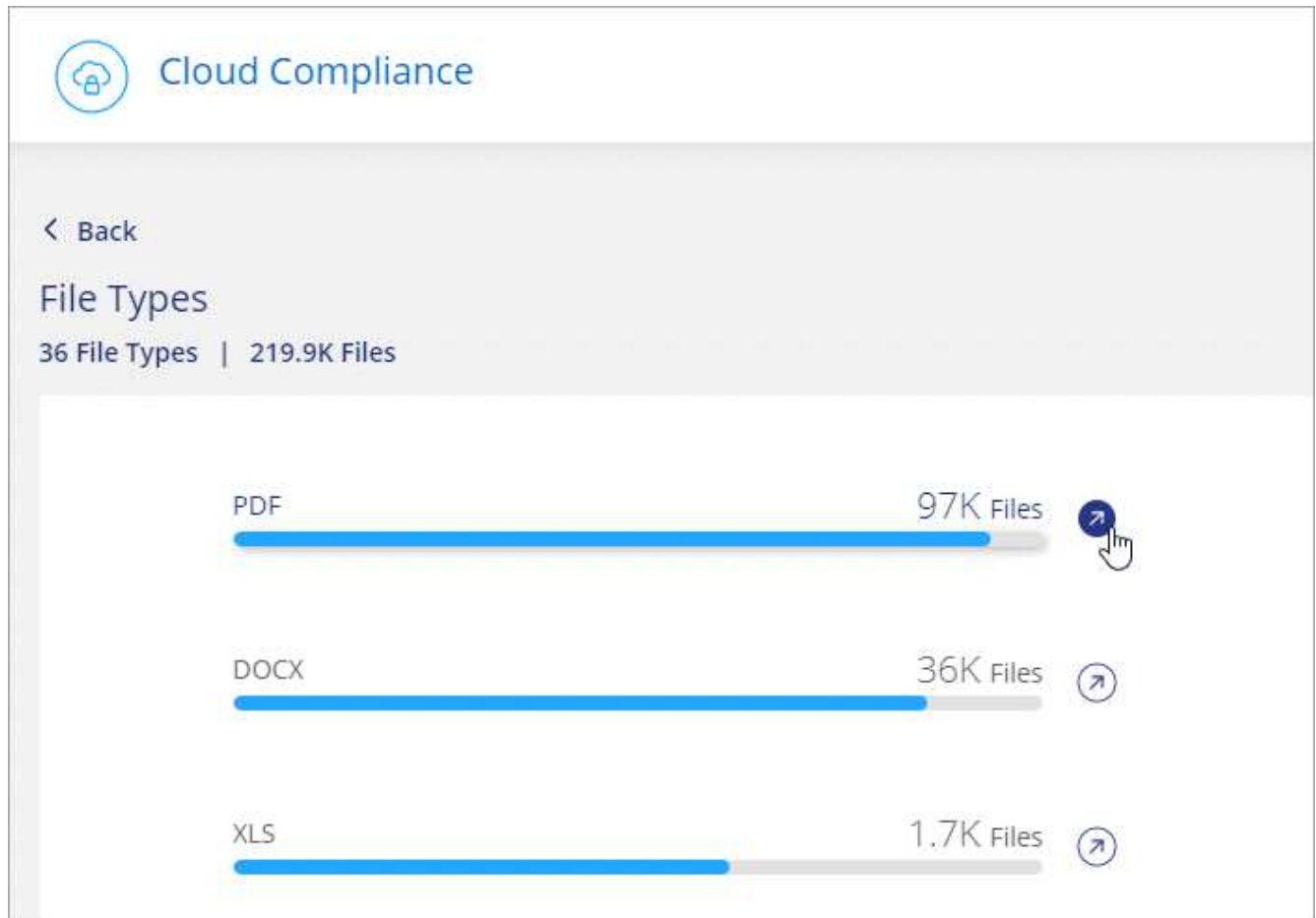
O Cloud Compliance coleta os dados que digitalizou e os divide por tipo de arquivo. A revisão dos tipos de arquivo pode ajudá-lo a controlar seus dados confidenciais, porque você pode descobrir que certos tipos de arquivo não estão armazenados corretamente. [Veja a lista de tipos de arquivo.](#)

Por exemplo, você pode estar armazenando arquivos CAD que incluem informações muito confidenciais sobre sua organização. Se eles não estiverem protegidos, você poderá assumir o controle dos dados confidenciais restringindo permissões ou movendo os arquivos para outro local.

### Exibindo tipos de arquivo

#### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique no ícone **investigar resultados** para um dos 4 principais tipos de arquivo diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone para qualquer um dos tipos de arquivo.



3. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

## Tipos de arquivos

O Cloud Compliance verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivo na seção tipos de arquivo do painel.

Mas quando o Cloud Compliance detecta informações pessoais identificáveis (PII), ou quando realiza uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF e .JSON.

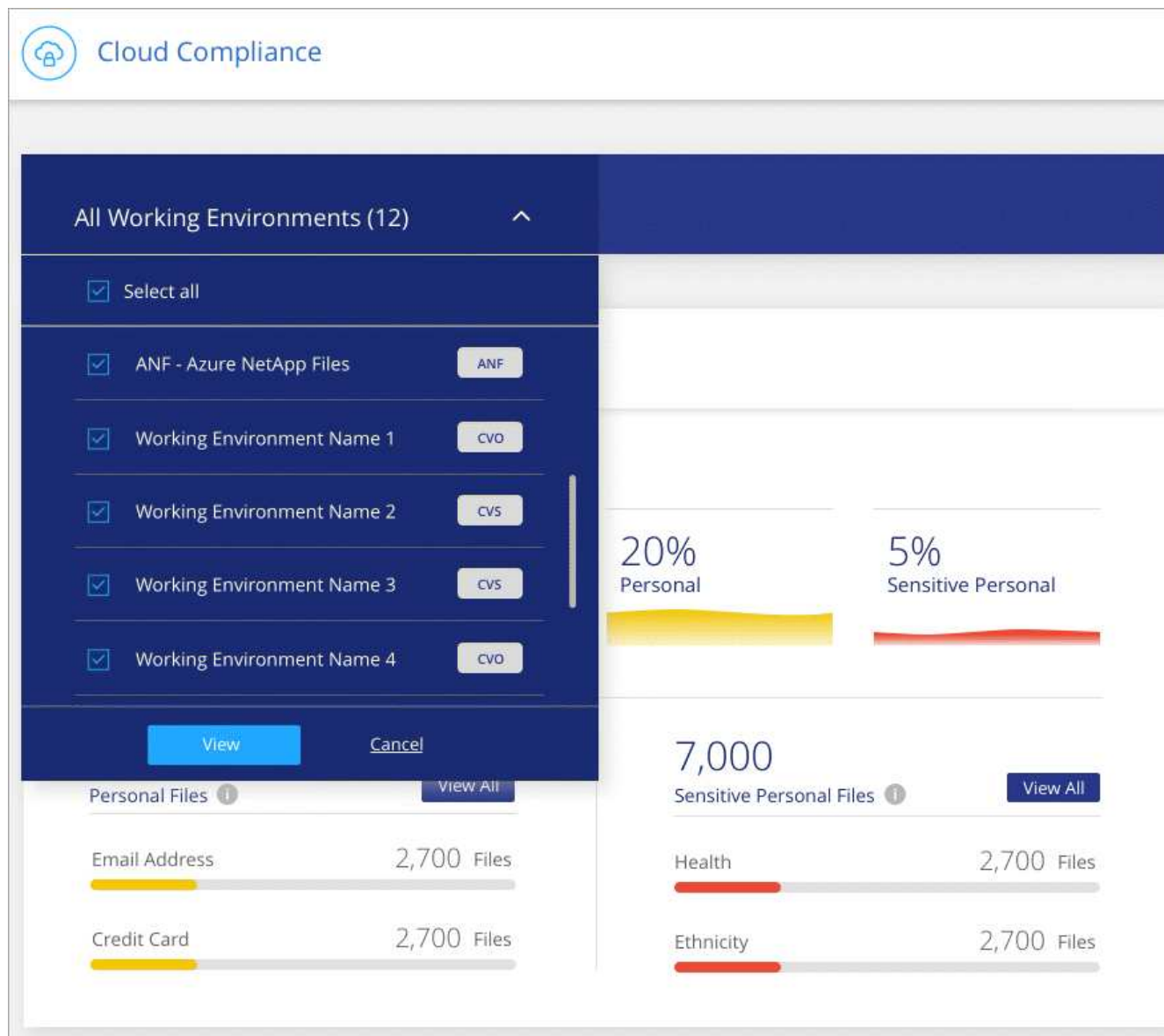
## Visualização de dados de ambientes de trabalho específicos

Você pode filtrar o conteúdo do dashboard do Cloud Compliance para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, o Cloud Compliance escolhe os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

### Passos

1. Clique no menu suspenso filtro, selecione os ambientes de trabalho para os quais deseja exibir dados e clique em **Exibir**.



## Precisão das informações encontradas

A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

Com base em nossos testes, a tabela abaixo mostra a precisão das informações encontradas pelo Cloud Compliance. Nós quebramos isso por *precisão* e *recall*:

### Precisão

A probabilidade de que o Cloud Compliance encontre tenha sido identificado corretamente. Por exemplo, uma taxa de precisão de 90% para dados pessoais significa que 9 em cada 10 arquivos identificados como contendo informações pessoais, contêm informações pessoais. 1 de 10 arquivos seria um falso positivo.

### Recolha

A probabilidade de o Cloud Compliance encontrar o que deveria. Por exemplo, uma taxa de recall de 70% para dados pessoais significa que o Cloud Compliance pode identificar 7 em cada 10 arquivos que realmente contêm informações pessoais em sua organização. O Cloud Compliance perderia 30% dos dados, e isso não aparecerá no painel.

O Cloud Compliance está em uma versão de disponibilidade controlada e estamos constantemente melhorando a precisão de nossos resultados. Essas melhorias estarão disponíveis automaticamente em futuras versões do Cloud Compliance.

Tipo	Precisão	Recolha
Dados pessoais - Geral	90%-95%	60%-80%
Dados pessoais - identificadores de país	30%-60%	40%-60%
Dados pessoais confidenciais	80%-95%	20%-30%
Categorias	90%-97%	60%-80%

## O que está incluído em cada relatório de lista de arquivos (arquivo CSV)

A partir de cada página de investigação, você pode baixar listas de arquivos (em formato CSV) que incluem detalhes sobre os arquivos identificados. Se houver mais de 10.000 resultados, apenas os 10.000 primeiros aparecem na lista.

Cada lista de arquivos inclui as seguintes informações:

- Nome do ficheiro
- Tipo de localização
- Ambiente de trabalho
- Repositório de storage
- Protocolo
- Caminho do ficheiro
- Tipo de ficheiro
- Categoria
- Informações pessoais
- Informações pessoais sensíveis
- Data de deteção de eliminação

Uma data de deteção de exclusão identifica a data em que o arquivo foi excluído ou movido. Isso permite que você identifique quando os arquivos confidenciais foram movidos. Os arquivos excluídos não fazem parte da contagem de números de arquivo que aparece no painel ou na página de investigação. Os arquivos só aparecem nos relatórios CSV.

## Visualização de relatórios de conformidade

O Cloud Compliance fornece relatórios que você pode usar para entender melhor o status do programa de privacidade de dados da sua organização.

Por padrão, o dashboard do Cloud Compliance exibe dados de conformidade para todos os ambientes de trabalho e bancos de dados. Se desejar exibir relatórios que contenham dados apenas para alguns dos ambientes de trabalho [selecione esses ambientes de trabalho](#), .



A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

## Relatório de avaliação de risco de privacidade

O Relatório de avaliação de risco de privacidade fornece uma visão geral do status de risco à privacidade da sua organização, conforme exigido pelas regulamentações de privacidade, como GDPR e CCPA. O relatório inclui as seguintes informações:

### Status de conformidade

A [pontuação de gravidade](#) e a distribuição de dados, sejam eles não sensíveis, pessoais ou sensíveis.

### Visão geral da avaliação

Uma discriminação dos tipos de dados pessoais encontrados, bem como das categorias de dados.

### Sujeitos de dados nesta avaliação

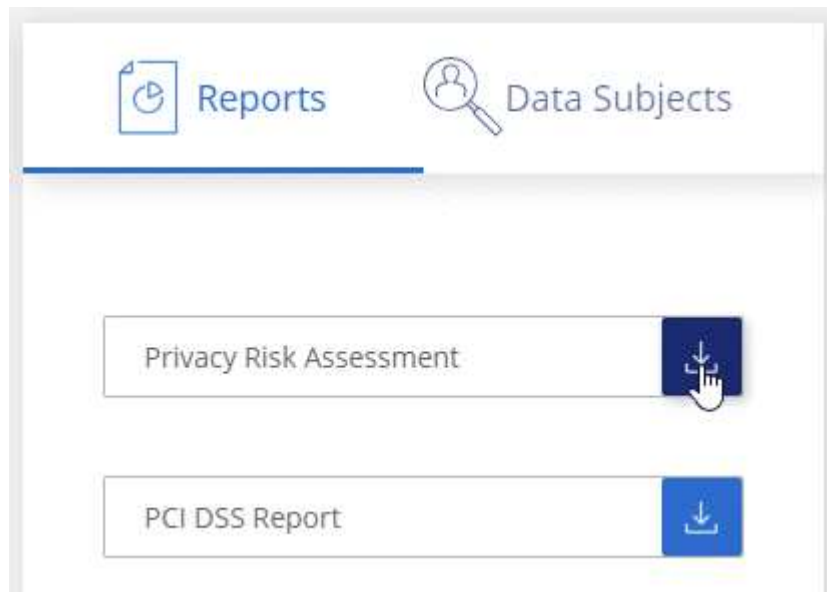
O número de pessoas, por localização, para as quais foram encontrados identificadores nacionais.

## Gerando o Relatório de avaliação de risco de Privacidade

Vá para a guia conformidade para gerar o relatório.

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **avaliação de risco de privacidade**.



### Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.

## Pontuação de gravidade

O Cloud Compliance calcula a pontuação de gravidade para o Relatório de avaliação de risco de privacidade com base em três variáveis:

- A porcentagem de dados pessoais de todos os dados.
- A porcentagem de dados pessoais sensíveis de todos os dados.
- O percentual de arquivos que incluem titulares de dados, determinado por identificadores nacionais, como IDs nacionais, números de Segurança Social e números de identificação fiscal.

A lógica utilizada para determinar a pontuação é a seguinte:

Pontuação de gravidade	Lógica
0	Todas as três variáveis são exatamente 0%
1	Uma das variáveis é maior que 0%
2	Uma das variáveis é maior que 3%
3	Duas das variáveis são maiores que 3%
4	Três das variáveis são maiores que 3%
5	Uma das variáveis é maior que 6%
6	Duas das variáveis são maiores que 6%
7	Três das variáveis são maiores que 6%
8	Uma das variáveis é maior que 15%
9	Duas das variáveis são maiores que 15%
10	Três das variáveis são maiores que 15%

## Relatório PCI DSS

O Relatório padrão de Segurança de dados da indústria de cartões de pagamento (PCI DSS) pode ajudá-lo a identificar a distribuição de informações de cartão de crédito entre seus arquivos. O relatório inclui as seguintes informações:

### Visão geral

Quantos arquivos contêm informações de cartão de crédito e em que ambientes de trabalho.

### Criptografia

A porcentagem de arquivos que contêm informações de cartão de crédito que estão em ambientes de trabalho criptografados ou não criptografados. Esta informação é específica do Cloud Volumes ONTAP.

### Proteção contra ransomware

A porcentagem de arquivos que contêm informações de cartão de crédito que estão em ambientes de trabalho que possuem ou não proteção contra ransomware ativada. Esta informação é específica do Cloud Volumes ONTAP.

### Retenção

O período de tempo em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter as informações do cartão de crédito por mais tempo do que precisa processá-las.

## Distribuição de informações de cartão de crédito

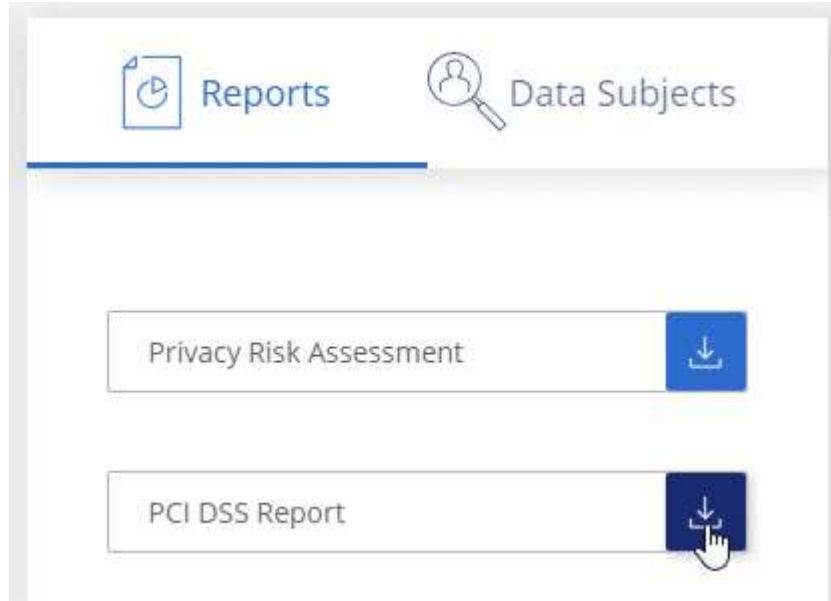
Os ambientes de trabalho onde as informações do cartão de crédito foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

## Gerando o Relatório PCI DSS

Vá para a guia conformidade para gerar o relatório.

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **Relatório PCI DSS**.



### Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.

## Relatório HIPAA

O Relatório HIPAA (Health Insurance Portability and Accountability Act) pode ajudá-lo a identificar arquivos contendo informações de saúde. Criado para auxiliar a organização a obedecer às leis de privacidade de dados HIPAA. As informações que o Cloud Compliance procura incluem:

- Padrão de referência de saúde
- Código médico ICD-10-CM
- Código médico ICD-9-CM
- RH – categoria Saúde
- Categoria de dados da aplicação de integridade

O relatório inclui as seguintes informações:

## Visão geral

Quantos arquivos contêm informações de saúde e em quais ambientes de trabalho.

## Criptografia

A porcentagem de arquivos que contêm informações de integridade que estão em ambientes de trabalho criptografados ou não criptografados. Esta informação é específica do Cloud Volumes ONTAP.

## Proteção contra ransomware

A porcentagem de arquivos que contêm informações de integridade que estão em ambientes de trabalho que possuem ou não proteção contra ransomware habilitada. Esta informação é específica do Cloud Volumes ONTAP.

## Retenção

O período de tempo em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter as informações de saúde por mais tempo do que precisa processá-las.

## Distribuição de informações em Saúde

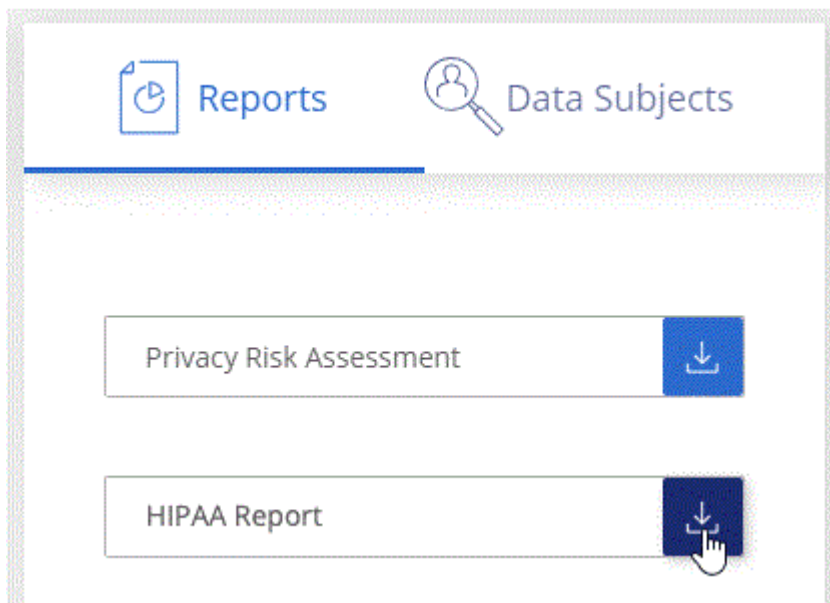
Os ambientes de trabalho onde as informações de integridade foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

## Gerando o Relatório HIPAA

Vá para a guia conformidade para gerar o relatório.

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **Relatório HIPAA**.



### Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.



## Selecionar os ambientes de trabalho para relatórios

Você pode filtrar o conteúdo do dashboard do Cloud Compliance para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, o Cloud Compliance escolhe os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

### Passos

1. Clique no menu suspenso filtro, selecione os ambientes de trabalho para os quais deseja exibir dados e clique em **Exibir**.

The screenshot displays the Cloud Compliance interface. On the left, a filter menu is open, showing 'All Working Environments (12)' with a list of six items, each with a checked checkbox and a 'View' button: 'ANF - Azure NetApp Files', 'Working Environment Name 1', 'Working Environment Name 2', 'Working Environment Name 3', and 'Working Environment Name 4'. Below the list are 'View' and 'Cancel' buttons. The main dashboard area shows summary statistics: '20% Personal' and '5% Sensitive Personal' with corresponding progress bars. Below this, it shows '7,000 Personal Files' and '7,000 Sensitive Personal Files', each with a 'View All' button. At the bottom, there are two rows of data: 'Email Address' and 'Credit Card' (both with 2,700 files and yellow progress bars), and 'Health' and 'Ethnicity' (both with 2,700 files and red progress bars).

## Resposta a uma solicitação de acesso do titular dos dados

Responder a uma solicitação de acesso ao titular dos dados (DSAR), pesquisando o nome completo ou identificador conhecido de um indivíduo (como um endereço de e-mail) e, em seguida, baixando um relatório. O relatório foi projetado para auxiliar na

exigência de sua organização em cumprir com o GDPR ou leis de privacidade de dados semelhantes.



A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

## O que é uma solicitação de acesso ao titular dos dados?

As regulamentações de privacidade, como o GDPR europeu, concedem aos titulares dos dados (como clientes ou funcionários) o direito de acessar seus dados pessoais. Quando um titular de dados solicita essas informações, isso é conhecido como DSAR (solicitação de acesso do titular dos dados). As organizações devem responder a essas solicitações "sem demora indevida" e, o mais tardar, no prazo de um mês após o recebimento.

## Como o Cloud Compliance pode ajudá-lo a responder a um DSAR?

Quando você realiza uma pesquisa de titular de dados, o Cloud Compliance localiza todos os arquivos que possuem o nome ou identificador dessa pessoa. O Cloud Compliance verifica os dados pré-indexados mais recentes para o nome ou identificador. Não inicia uma nova digitalização.

Depois que a pesquisa estiver concluída, você poderá baixar a lista de arquivos para um relatório de solicitação de acesso do titular dos dados. O relatório agrega insights dos dados e os coloca em termos legais que você pode enviar de volta para a pessoa.

## Procurar por titulares de dados e transferir relatórios

Procure o nome completo ou identificador conhecido do titular dos dados e, em seguida, transfira um relatório de lista de ficheiros ou relatório DSAR. Pode pesquisar por "[qualquer tipo de informação pessoal](#)".

Apenas o inglês é suportado ao procurar os nomes dos titulares dos dados. O suporte para mais idiomas será adicionado mais tarde.

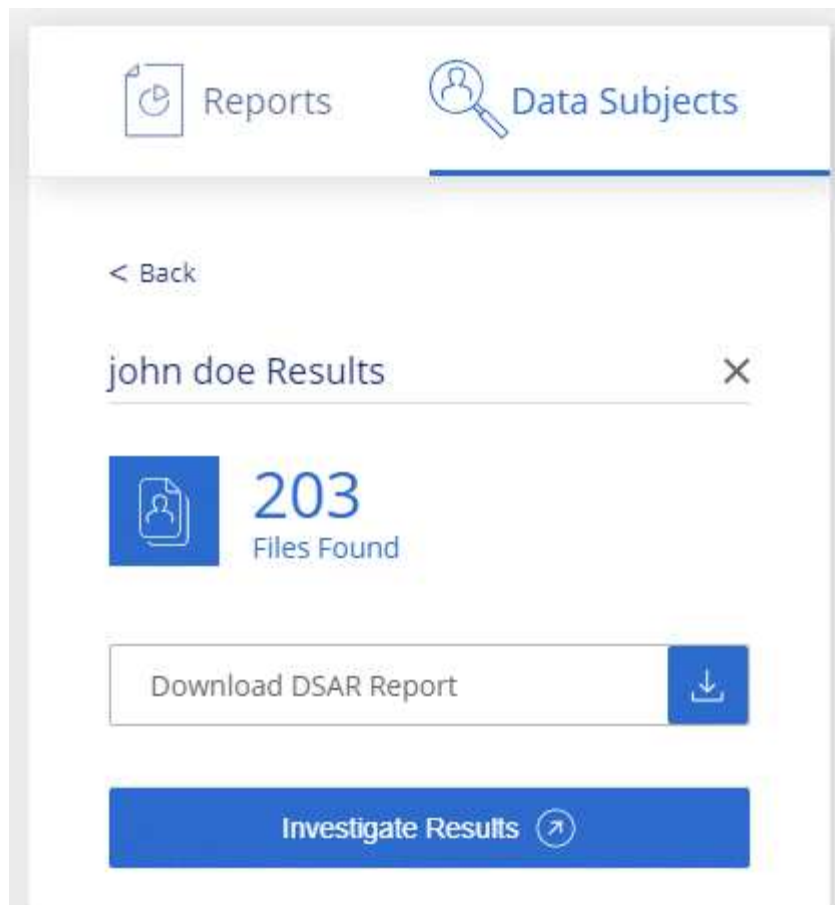


A pesquisa de titulares de dados não é suportada em bases de dados neste momento.

### Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique em **Assunto de dados**.
3. Procure o nome completo ou identificador conhecido do titular dos dados.

Aqui está um exemplo que mostra uma pesquisa para o nome *john doe*:



4. Escolha uma das opções disponíveis:

- **Download de Relatório DSAR:** Uma resposta formal à solicitação de acesso que você pode enviar ao titular dos dados. Este relatório contém informações geradas automaticamente com base nos dados que o Cloud Compliance foi encontrado no titular dos dados e foi projetado para ser usado como modelo. Você deve preencher o formulário e revisá-lo internamente antes de enviá-lo para o titular dos dados.
- **Investigar resultados:** Uma página que permite investigar os dados pesquisando, classificando, expandindo detalhes para um arquivo específico e baixando a lista de arquivos.



Se houver mais de 10.000 resultados, apenas os 10.000 primeiros aparecem na lista de arquivos.

## Desativação do Cloud Compliance


Se necessário, você pode impedir que o Cloud Compliance escaneie um ou mais ambientes de trabalho ou bancos de dados. Você também pode excluir a instância do Cloud Compliance se não quiser mais usar o Cloud Compliance com seus ambientes de trabalho.

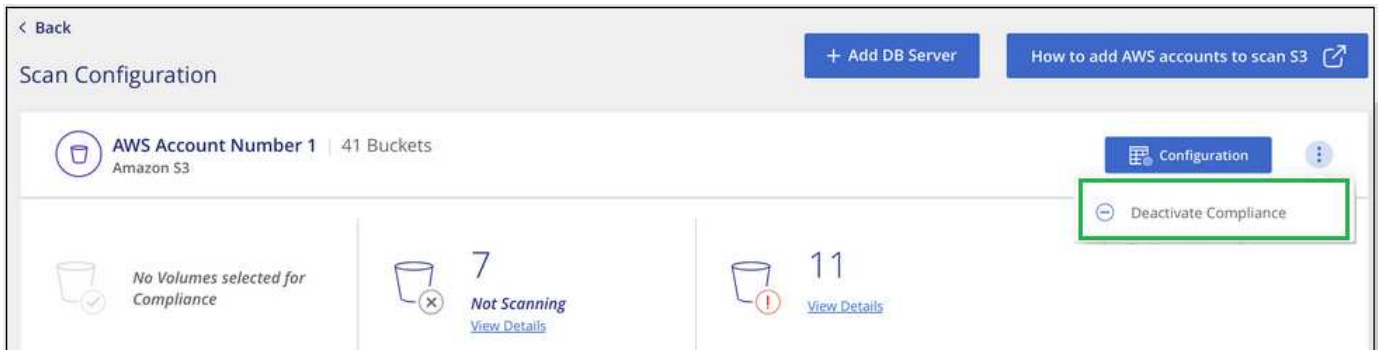
### A desativação da conformidade verifica se há um ambiente de trabalho

Quando você desativa as verificações, o Cloud Compliance não verifica mais os dados no sistema e remove os insights de conformidade indexados da instância do Cloud Compliance (os dados do ambiente de trabalho

ou do próprio banco de dados não são excluídos).

## Passos

Na página *Scan Configuration*, clique no  botão na linha do ambiente de trabalho e, em seguida, clique em **Deactivate Compliance**.



Você também pode desativar as verificações de conformidade para um ambiente de trabalho no painel Serviços quando você selecionar o ambiente de trabalho.

## Excluindo a instância do Cloud Compliance

Você pode excluir a instância do Cloud Compliance se não quiser mais usar o Cloud Compliance. A exclusão da instância também exclui os discos associados onde os dados indexados residem.

### Passo

1. Vá para o console do seu provedor de nuvem e exclua a instância do Cloud Compliance.

A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo:  
*CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

## Perguntas frequentes sobre o Cloud Compliance

Esta FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

### O que é o Cloud Compliance?

O Cloud Compliance é uma oferta de nuvem que usa a tecnologia orientada por Inteligência artificial (AI) para ajudar as organizações a entender o contexto dos dados e identificar dados confidenciais em suas configurações do Azure NetApp Files, sistemas Cloud Volumes ONTAP hospedados na AWS ou Azure, buckets do Amazon S3 e bancos de dados.

O Cloud Compliance fornece parâmetros predefinidos (como categorias e tipos de informações confidenciais) para lidar com as novas regulamentações de conformidade de dados para a privacidade e a sensibilidade dos dados, como GDPR, CCPA, HIPAA e muito mais.

### Por que devo usar o Cloud Compliance?

O Cloud Compliance ajuda você a:

- Cumprir as regulamentações de privacidade e conformidade de dados.
- Obedecer às políticas de retenção de dados.
- Localize e reporte facilmente dados específicos em resposta aos titulares do dados, conforme exigido pelo GDPR, CCPA, HIPAA e outras regulamentações sobre a privacidade de dados.

## Quais são os casos de uso comuns para o Cloud Compliance?

- Identificar informações pessoais identificáveis (PII).
- Identifique um amplo escopo de informações confidenciais conforme exigido pelas regulamentações de privacidade do GDPR e CCPA.
- Cumprir as novas e futuras regulamentações de privacidade de dados.

["Saiba mais sobre os casos de uso do Cloud Compliance"](#).

## Que tipos de dados podem ser verificados com o Cloud Compliance?

O Cloud Compliance dá suporte à verificação de dados não estruturados em protocolos NFS e CIFS gerenciados pela Cloud Volumes ONTAP e Azure NetApp Files. O Cloud Compliance também pode verificar os dados armazenados nos buckets do Amazon S3.

Além disso, o Cloud Compliance pode verificar bancos de dados localizados em qualquer lugar - eles não precisam ser gerenciados pelo Cloud Manager.

["Saiba como as digitalizações funcionam"](#).

## Quais fornecedores de nuvem são compatíveis?

O Cloud Compliance opera como parte do Cloud Manager e, atualmente, é compatível com AWS e Azure. Isso proporciona à sua organização uma visibilidade unificada da privacidade entre diferentes fornecedores de nuvem. O suporte ao Google Cloud Platform (GCP) será adicionado em breve.

## Como faço para acessar o Cloud Compliance?

O Cloud Compliance é operado e gerenciado por meio do Cloud Manager. Você pode acessar os recursos de conformidade na nuvem a partir da guia **Compliance** no Cloud Manager.

## Como funciona o Cloud Compliance?

O Cloud Compliance implanta outra camada de inteligência artificial ao lado do sistema e dos sistemas de storage do Cloud Manager. Em seguida, ele verifica os dados em volumes, buckets e bancos de dados e indexa os insights de dados encontrados.

["Saiba mais sobre como o Cloud Compliance funciona"](#).

## Quanto custa o Cloud Compliance?

O custo para usar o Cloud Compliance depende da quantidade de dados que você está digitalizando. Os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto. ["preços"](#) Consulte para obter detalhes.

## Com que frequência o Cloud Compliance verifica meus dados?

Os dados são alterados com frequência. Assim, o Cloud Compliance verifica seus dados continuamente sem impacto nos dados. Embora a digitalização inicial dos seus dados possa demorar mais tempo, as digitalizações subsequentes apenas analisam as alterações incrementais, o que reduz os tempos de digitalização do sistema.

["Saiba como as digitalizações funcionam"](#).

## O Cloud Compliance oferece relatórios?

Sim. As informações oferecidas pelo Cloud Compliance podem ser relevantes para outras partes interessadas em suas organizações, por isso, permitimos que você gere relatórios para compartilhar os insights.

Os seguintes relatórios estão disponíveis para conformidade com a nuvem:

### Relatório de avaliação de risco de privacidade

Fornecer insights de privacidade de seus dados e uma pontuação de risco de privacidade. ["Saiba mais"](#).

### Relatório de solicitação de acesso do titular dos dados

Permite que você extraia um relatório de todos os arquivos que contêm informações sobre o nome específico ou identificador pessoal de um titular de dados. ["Saiba mais"](#).

### Relatório PCI DSS

Ajuda você a identificar a distribuição de informações de cartão de crédito entre seus arquivos. ["Saiba mais"](#).

### Relatório HIPAA

Ajuda você a identificar a distribuição de informações de saúde entre seus arquivos. ["Saiba mais"](#).

### Relatórios sobre um tipo de informação específico

Estão disponíveis relatórios que incluem detalhes sobre os arquivos identificados que contêm dados pessoais e dados pessoais confidenciais. Você também pode ver os arquivos divididos por categoria e tipo de arquivo. ["Saiba mais"](#).

## Que tipo de instância ou VM é necessário para o Cloud Compliance?

- No Azure, o Cloud Compliance é executado em uma VM Standard\_D16s\_v3 com um disco de 512 GB.
- Na AWS, o Cloud Compliance é executado em uma instância do m5,4xlarge com um disco GP2 de 500 GB.

Em regiões onde o m5,4xlarge não está disponível, o Cloud Compliance é executado em uma instância do m4,4xlarge.



Alterar ou redimensionar o tipo de instância/VM não é suportado. Você precisa usar o tamanho padrão fornecido.

["Saiba mais sobre como o Cloud Compliance funciona"](#).

## O desempenho da digitalização varia?

O desempenho da digitalização pode variar com base na largura de banda da rede e no tamanho médio do ficheiro no seu ambiente de nuvem.

## Quais tipos de arquivo são suportados?

O Cloud Compliance verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivo na seção tipos de arquivo do painel.

Quando o Cloud Compliance deteta informações pessoais identificáveis (PII) ou quando realiza uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF e .json.

## Como habilito o Cloud Compliance?

Primeiro, você precisa implantar uma instância de Cloud Compliance no Cloud Manager. Quando a instância estiver em execução, você poderá ativá-la em ambientes de trabalho e bancos de dados existentes na guia **Compliance** ou selecionando um ambiente de trabalho específico.

["Saiba como começar"](#).



A ativação do Cloud Compliance resulta em uma verificação inicial imediata. Os resultados de conformidade são exibidos pouco depois.

## Como posso desativar o Cloud Compliance?

Você pode desativar o Cloud Compliance na página ambientes de trabalho depois de selecionar um ambiente de trabalho individual.

["Saiba mais"](#).



Para remover completamente a instância do Cloud Compliance, você pode remover manualmente a instância do Cloud Compliance do portal do seu provedor de nuvem.

## O que acontece se a disposição de dados em categorias estiver ativada no Cloud Volumes ONTAP?

Você pode querer habilitar o Cloud Compliance em um sistema Cloud Volumes ONTAP que categoriza dados inativos no storage de objetos. Se a disposição de dados em categorias estiver ativada, o Cloud Compliance verifica todos os dados que estão em discos e dados inativos dispostos no storage de objetos.

A verificação de conformidade não aquece os dados frios - permanece fria e dividida em armazenamento de objetos.

## Posso usar o Cloud Compliance para analisar o storage ONTAP no local?

A digitalização dos dados diretamente de um ambiente de trabalho do ONTAP no local não é compatível. Mas você pode digitalizar seus dados ONTAP locais replicando os dados NFS ou CIFS locais em um ambiente de trabalho Cloud Volumes ONTAP e ativando a conformidade nesses volumes. Estamos planejando dar suporte ao Cloud Compliance com ofertas de nuvem adicionais, como o Cloud Volumes Service.

["Saiba mais"](#).

## **O Cloud Compliance pode enviar notificações para minha organização?**

Não, mas você pode baixar relatórios de status que você pode compartilhar internamente em sua organização.

## **Posso personalizar o serviço de acordo com as necessidades da minha organização?**

O Cloud Compliance fornece insights prontos para uso para seus dados. Esses insights podem ser extraídos e usados para atender às necessidades da sua organização.

## **Posso limitar as informações de conformidade na nuvem a usuários específicos?**

Sim, o Cloud Compliance é totalmente integrado ao Cloud Manager. Os usuários do Cloud Manager só podem ver informações sobre os ambientes de trabalho que estão qualificados para visualizar de acordo com a Privileges do workspace.

Além disso, se você quiser permitir que certos usuários visualizem apenas os resultados da verificação do Cloud Compliance sem ter a capacidade de gerenciar as configurações de Cloud Compliance, você pode atribuir a esses usuários a função *Cloud Compliance Viewer*.

["Saiba mais"](#).



## 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.