# Começar

## NetApp Data Classification

NetApp
February 06, 2026

# Índice

# Começar

## Saiba mais sobre a NetApp Data Classification

O NetApp Data Classification é um serviço de governança de dados para o NetApp Console que verifica suas fontes de dados corporativas locais e na nuvem para mapear e classificar dados e identificar informações privadas. Isso pode ajudar a reduzir seus riscos de segurança e conformidade, diminuir custos de armazenamento e auxiliar em seus projetos de migração de dados.

A partir da versão 1.31, a Classificação de Dados está disponível como um recurso principal no NetApp Console. Não há custo adicional. Não é necessária nenhuma licença de classificação ou assinatura. + Se você estiver usando a versão legada 1.30 ou anterior, essa versão estará disponível até sua assinatura expirar.

### NetApp Console

A classificação de dados pode ser acessada por meio do NetApp Console.

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados da NetApp em ambientes locais e na nuvem em nível empresarial. O Console é necessário para acessar e usar os serviços de dados do NetApp . Como uma interface de gerenciamento, ele permite que você gerencie muitos recursos de armazenamento a partir de uma única interface. Os administradores do console podem controlar o acesso ao armazenamento e aos serviços de todos os sistemas da empresa.

Você não precisa de uma licença ou assinatura para começar a usar o NetApp Console e só incorrerá em cobranças quando precisar implantar agentes do Console na sua nuvem para garantir a conectividade com seus sistemas de armazenamento ou serviços de dados do NetApp . No entanto, alguns serviços de dados da NetApp acessíveis pelo Console são licenciados ou baseados em assinatura.

Saiba mais sobre o"NetApp Console" .

### Características

A classificação de dados usa inteligência artificial (IA), processamento de linguagem natural (PLN) e aprendizado de máquina (ML) para entender o conteúdo que ela verifica, a fim de extrair entidades e categorizar o conteúdo adequadamente. Isso permite que a Classificação de Dados forneça as seguintes áreas de funcionalidade.

"Aprenda sobre casos de uso para Classificação de Dados" .

#### Manter a conformidade

A Classificação de Dados fornece diversas ferramentas que podem ajudar em seus esforços de conformidade. Você pode usar a Classificação de Dados para:

- Identifique Informações Pessoais Identificáveis (PII).
- Identifique uma ampla gama de informações pessoais confidenciais, conforme exigido pelos regulamentos de privacidade GDPR, CCPA, PCI e HIPAA.
- Responda às solicitações de acesso do titular dos dados (DSAR) com base no nome ou endereço de e-mail.

**Fortalecer a segurança**

A Classificação de Dados pode identificar dados que correm risco potencial de serem acessados para fins criminosos. Você pode usar a Classificação de Dados para:

- Identifique todos os arquivos e diretórios (compartilhamentos e pastas) com permissões abertas que estão expostos a toda a sua organização ou ao público.
- Identifique dados confidenciais que residem fora do local inicial dedicado.
- Cumpra as políticas de retenção de dados.
- Use *Políticas* para detectar automaticamente novos problemas de segurança para que a equipe de segurança possa agir imediatamente.

**Otimize o uso do armazenamento**

A Classificação de Dados fornece ferramentas que podem ajudar com o custo total de propriedade (TCO) do seu armazenamento. Você pode usar a Classificação de Dados para:

- Aumente a eficiência do armazenamento identificando dados duplicados ou não relacionados aos negócios.
- Economize custos de armazenamento identificando dados inativos que você pode colocar em camadas para armazenamento de objetos mais barato. "Saiba mais sobre camadas dos sistemas Cloud Volumes ONTAP" . "Saiba mais sobre camadas de sistemas ONTAP locais" .

## Sistemas e fontes de dados suportados

A Classificação de Dados pode escanear e analisar dados estruturados e não estruturados dos seguintes tipos de sistemas e fontes de dados:

**Sistemas**

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP (implantado na AWS, Azure ou GCP)
- Clusters ONTAP locais
- StorageGRID
- Google Cloud NetApp Volumes

**Fontes de dados**

- Compartilhamentos de arquivos NetApp
- Bancos de dados:
  - Serviço de banco de dados relacional da Amazon (Amazon RDS)
  - MongoDB
  - MySQL
  - Oráculo
  - PostgreSQL
  - SAP HANA
  - Servidor SQL (MSSQL)

A Classificação de Dados oferece suporte às versões 3.x, 4.0 e 4.1 do NFS e às versões 1.x, 2.0, 2.1 e 3.0 do CIFS.

## Custo

A Classificação de Dados é de uso gratuito. Não é necessária nenhuma licença de classificação ou assinatura paga.

### Custos de infraestrutura

- A instalação do Data Classification na nuvem requer a implantação de uma instância de nuvem, o que resulta em cobranças do provedor de nuvem onde ela é implantada. Ver o tipo de instância que é implantada para cada provedor de nuvem . Não há custo se você instalar o Data Classification em um sistema local.
- A Classificação de Dados exige que você tenha implantado um agente do Console. Em muitos casos, você já tem um agente do Console por causa de outros armazenamentos e serviços que está usando no Console. A instância do agente do Console resulta em cobranças do provedor de nuvem onde é implantada. Veja o "tipo de instância que é implantada para cada provedor de nuvem" . Não há custo se você instalar o agente do Console em um sistema local.

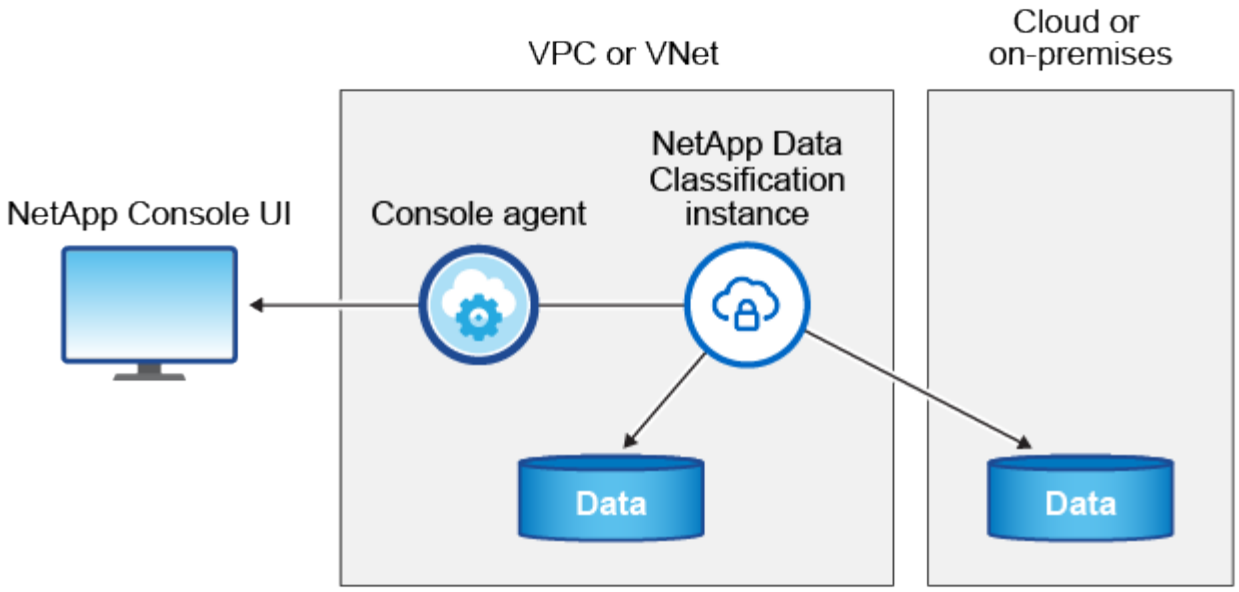
### Custos de transferência de dados

Os custos de transferência de dados dependem da sua configuração. Se a instância de Classificação de Dados e a fonte de dados estiverem na mesma Zona de Disponibilidade e região, não haverá custos de transferência de dados. Mas se a fonte de dados, como um sistema Cloud Volumes ONTAP , 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: Preços do Amazon Elastic Compute Cloud (Amazon EC2)"
- "Microsoft Azure: Detalhes de preços de largura de banda"
- "Google Cloud: preços do serviço de transferência de armazenamento"

## A instância de classificação de dados

Quando você implanta a Classificação de Dados na nuvem, o Console implanta a instância na mesma sub-rede que o agente do Console. "Saiba mais sobre o agente do Console."




Observe o seguinte sobre a instância padrão:

- Na AWS, a Classificação de Dados é executada em um "instância m6i.4xlarge" com um disco GP2 de 500 GiB. A imagem do sistema operacional é o Amazon Linux 2. Quando implantado na AWS, você pode escolher um tamanho de instância menor se estiver digitalizando uma pequena quantidade de dados.
- No Azure, a Classificação de Dados é executada em um"Standard_D16s_v3 VM" com um disco de 500 GiB. A imagem do sistema operacional é o Ubuntu 22.04.
- No GCP, a Classificação de Dados é executada em um"VM n2-padrão-16" com um disco persistente padrão de 500 GiB. A imagem do sistema operacional é o Ubuntu 22.04.
- Em regiões onde a instância padrão não está disponível, a Classificação de Dados é executada em uma instância alternativa. "Veja os tipos de instância alternativos" .
- A instância é denominada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Apenas uma instância de Classificação de Dados é implantada por Agente de Console.

Você também pode implantar a Classificação de Dados em um host Linux em suas instalações ou em um host em seu provedor de nuvem preferido. O software funciona exatamente da mesma maneira, independentemente do método de instalação escolhido. As atualizações do software de classificação de dados são automatizadas desde que a instância tenha acesso à Internet.

A instância deve permanecer em execução o tempo todo porque a Classificação de Dados verifica os dados continuamente.

**Implantar em diferentes tipos de instância**

Revise as seguintes especificações para tipos de instância:

| Tamanho do sistema | Especificações | Limitações |
|---|---|---|
| Extra grande | 32 CPUs, 128 GB de RAM, 1 TiB SSD | Pode escanear até 500 milhões de arquivos. |

| Tamanho do sistema | Especificações | Limitações |
| --- | --- | --- |
| Grande (padrão) | 16 CPUs, 64 GB de RAM, SSD de 500 GiB | Pode escanear até 250 milhões de arquivos. |

Ao implantar a Classificação de Dados no Azure ou no GCP, envie um e-mail para ng-contact-data-sense@netapp.com para obter assistência se desejar usar um tipo de instância menor.

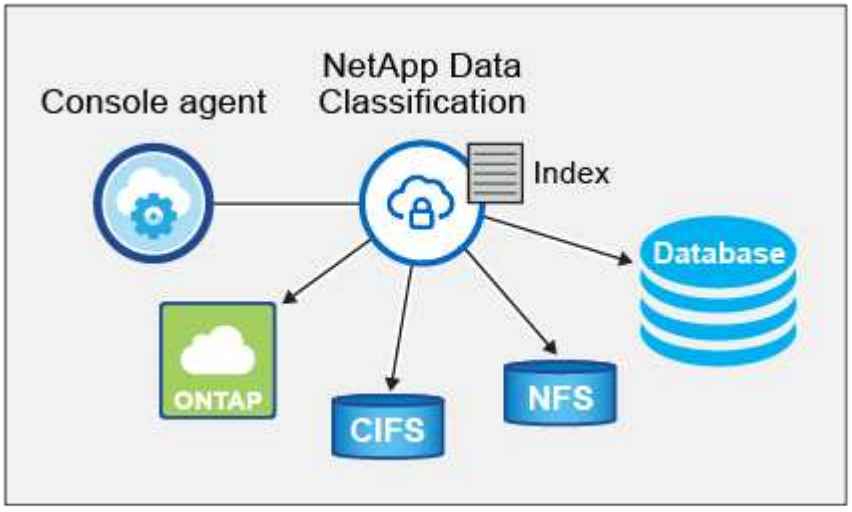
## Como funciona a varredura de classificação de dados

Em um nível mais alto, a varredura de classificação de dados funciona assim:

1. Você implanta uma instância de Classificação de Dados no Console.
2. Você habilita o mapeamento de alto nível (chamado de varreduras *Somente mapeamento*) ou varreduras de nível profundo (chamadas de varreduras *Mapear e classificar*) em uma ou mais fontes de dados.
3. A Classificação de Dados analisa dados usando um processo de aprendizado de IA.
4. Use os painéis e ferramentas de relatórios fornecidos para ajudar em seus esforços de conformidade e governança.

Depois de habilitar a Classificação de Dados e selecionar os repositórios que você deseja verificar (volumes, esquemas de banco de dados ou outros dados do usuário), ele imediatamente inicia a verificação dos dados para identificar dados pessoais e confidenciais. Na maioria dos casos, você deve se concentrar na digitalização de dados de produção ao vivo, em vez de backups, espelhos ou sites de DR. Em seguida, a Classificação de Dados mapeia seus dados organizacionais, categoriza cada arquivo e identifica e extrai entidades e padrões predefinidos nos dados. O resultado da verificação é um índice de informações pessoais, informações pessoais confidenciais, categorias de dados e tipos de arquivo.

A Classificação de Dados se conecta aos dados como qualquer outro cliente montando 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.




Após a verificação inicial, a Classificação de Dados verifica continuamente seus dados em um sistema round-robin para detectar alterações incrementais. É por isso que é importante manter a instância em execução.

Você pode habilitar e desabilitar verificações no nível do volume ou no nível do esquema do banco de dados.

A Classificação de Dados não impõe um limite à quantidade de dados que pode escanear. Cada agente do Console suporta a digitalização e a exibição de 500 TiB de dados. Para escanear mais de 500 TiB de dados,"instalar outro agente do Console" então"implantar outra instância de Classificação de Dados" . + A interface do usuário do console exibe dados de um único conector. Para obter dicas sobre como visualizar dados de vários agentes do Console, consulte"Trabalhar com vários agentes do Console" .

## Qual é a diferença entre varreduras de mapeamento e classificação?

Você pode realizar dois tipos de varreduras na Classificação de Dados:

- **As verificações somente de mapeamento** fornecem apenas uma visão geral de alto nível dos seus dados e são realizadas em fontes de dados selecionadas. As varreduras somente de mapeamento levam menos tempo do que as varreduras de mapeamento e classificação porque não acessam arquivos para ver os dados contidos neles. Talvez você queira fazer isso inicialmente para identificar áreas de pesquisa e depois executar uma varredura de Mapear e Classificar nessas áreas.
- **As varreduras de Mapa e Classificação** fornecem uma varredura profunda dos seus dados.

Para obter detalhes sobre as diferenças entre as varreduras de mapeamento e classificação, consulte"Qual é a diferença entre varreduras de mapeamento e classificação?" .

## Informações que a Classificação de Dados categoriza

A Classificação de Dados coleta, indexa e atribui categorias aos seguintes dados:

- **Metadados padrão** sobre arquivos: o tipo de arquivo, seu tamanho, datas de criação e modificação e assim por diante.
- **Dados pessoais**: Informações de identificação pessoal (PII), como endereços de e-mail, números de identificação ou números de cartão de crédito, que a Classificação de Dados identifica usando palavras, sequências de caracteres e padrões específicos nos arquivos. "Saiba mais sobre dados pessoais" .
- **Dados pessoais sensíveis**: Tipos especiais de informações pessoais sensíveis (SPII), como dados de saúde, origem étnica ou opiniões políticas, conforme definido pelo Regulamento Geral de Proteção de Dados (GDPR) e outros regulamentos de privacidade. "Saiba mais sobre dados pessoais sensíveis" .
- **Categorias**: A classificação de dados pega os dados escaneados 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**: A classificação de dados usa IA para extrair nomes naturais de pessoas de documentos. "Saiba mais sobre como responder às solicitações de acesso do titular dos dados" .

## Visão geral da rede

A Classificação de Dados implanta um único servidor, ou cluster, onde você escolher: na nuvem ou no local. Os servidores se conectam por meio de protocolos padrão às fontes de dados e indexam as descobertas em um cluster do Elasticsearch, que também é implantado nos mesmos servidores. Isso permite suporte para ambientes multi-cloud, cross-cloud, nuvem privada e locais.

O Console implanta a instância de Classificação de Dados com um grupo de segurança que permite conexões HTTP de entrada do agente do Console.

Quando você usa o Console no modo SaaS, a conexão com o Console é feita por HTTPS, e os dados

privados enviados entre seu navegador e a instância de Classificação de Dados são protegidos com criptografia de ponta a ponta usando TLS 1.2, o que significa que a NetApp e terceiros não podem lê-los.

As regras de saída são completamente abertas. O acesso à Internet é necessário para instalar e atualizar o software de classificação de dados e para enviar métricas de uso.

Se você tiver requisitos de rede rigorosos,"aprenda sobre os endpoints que a Classificação de Dados contata" .

# NetApp Data Classification

## Você pode acessar a NetApp Data Classification por meio do NetApp Console.

Para fazer login no Console, você pode usar suas credenciais do Site de Suporte da NetApp ou pode se inscrever para um login no NetApp Console usando seu e-mail e uma senha. "Saiba mais sobre como fazer login no Console" .

Tarefas específicas exigem funções específicas do usuário do Console. "Saiba mais sobre as funções de acesso do Console para todos os serviços" .

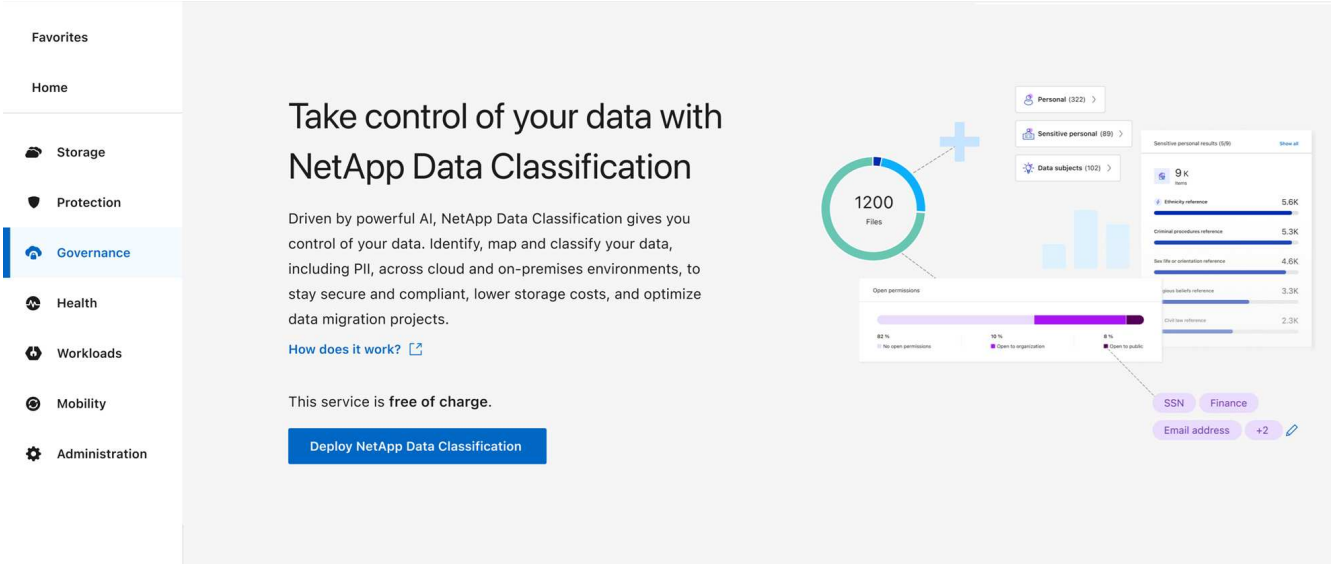
**Antes de começar**

- "Você deve adicionar um agente do Console."
- "Entenda qual estilo de implantação de Classificação de Dados é mais adequado à sua carga de trabalho."

**Passos**

1. Em um navegador da web, navegue até o"Console" .
2. Efetue login no Console.
3. Na página principal do NetApp Console, selecione **Governança** > **Classificação de dados**.
4. Se esta for a primeira vez que você acessa a Classificação de Dados, a página de destino será exibida.

   Selecione **Implantar classificação no local ou na nuvem** para começar a implantar sua instância de classificação. Para mais informações, consulte"Qual implantação de classificação de dados você deve usar?"



Caso contrário, o Painel de Classificação de Dados será exibido.

# Implantar classificação de dados

## Qual implantação de NetApp Data Classification você deve usar?

Você pode implantar a NetApp Data Classification de diferentes maneiras. Aprenda qual método atende às suas necessidades.

A classificação de dados pode ser implantada das seguintes maneiras:

- "Implante na nuvem usando o Console" . O Console implanta a instância de Classificação de Dados na mesma rede do provedor de nuvem que o agente do Console.
- "Instalar em um host Linux com acesso à Internet" . Instale o Data Classification em um host Linux na sua rede ou em um host Linux na nuvem que tenha acesso à Internet. Esse tipo de instalação pode ser uma boa opção se você preferir escanear sistemas ONTAP locais usando uma instância de Classificação de Dados que também esteja localizada no local, embora isso não seja um requisito.
- "Instalar em um host Linux em um site local sem acesso à Internet", também conhecido como *modo privado*. Esse tipo de instalação, que usa um script de instalação, não tem conectividade com a camada SaaS do Console.

> O modo privado BlueXP (interface BlueXP legada) normalmente é usado com ambientes locais que não têm conexão com a Internet e com regiões de nuvem seguras, o que inclui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. A NetApp continua a oferecer suporte a esses ambientes com a interface legada BlueXP . Para documentação do modo privado na interface BlueXP legada, consulte"Documentação em PDF para o modo privado do BlueXP" .

Tanto a instalação em um host Linux com acesso à Internet quanto a instalação local em um host Linux sem acesso à Internet usam um script de instalação. O script começa verificando se o sistema e o ambiente atendem aos pré-requisitos. Se os pré-requisitos forem atendidos, a instalação será iniciada. Se você quiser verificar os pré-requisitos independentemente de executar a instalação da Classificação de Dados, há um pacote de software separado que você pode baixar e que testa apenas os pré-requisitos.

Consulte "Verifique se o seu host Linux está pronto para instalar a Classificação de Dados" .

## Implante a NetApp Data Classification na nuvem usando o NetApp Console

Você pode implantar o NetApp Data Classification na nuvem com o NetApp Console. O Console implanta a instância de Classificação de Dados na mesma rede do provedor de nuvem que o agente do Console.

Observe que você também pode"instalar a Classificação de Dados em um host Linux que tenha acesso à Internet" . Esse tipo de instalação pode ser uma boa opção se você preferir escanear sistemas ONTAP locais usando uma instância de Classificação de Dados que também esteja localizada no local, mas isso não é um requisito. O software funciona exatamente da mesma maneira, independentemente do método de instalação escolhido.

### Início rápido

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

### 1 Criar um agente de console

Se você ainda não tiver um agente do Console, crie um. Ver"criando um agente de console na AWS" ,"criando um agente de console no Azure" , ou"criando um agente de console no GCP" .

Você também pode"instalar o agente do Console no local" em um host Linux em sua rede ou em um host Linux na nuvem.

### 2 Pré-requisitos

Certifique-se de que seu ambiente atenda aos pré-requisitos. Isso inclui acesso à internet de saída para a instância, conectividade entre o agente do Console e a Data Classification pela porta 443, entre outros. Veja a lista completa.

### 3 Implantar classificação de dados

Inicie o assistente de instalação para implantar a instância de Classificação de Dados na nuvem.

#### Criar um agente de console

Se você ainda não tiver um agente do Console, crie um agente do Console no seu provedor de nuvem. Ver "criando um agente de console na AWS" ou "criando um agente de console no Azure" , ou "criando um agente de console no GCP" . Na maioria dos casos, você provavelmente já terá um agente de console configurado antes de tentar ativar a Classificação de Dados, pois a maioria "Os recursos do console exigem um agente do console" Mas há casos em que você precisará configurar um agora.

Existem alguns cenários em que você precisa usar um agente do Console implantado em um provedor de nuvem específico:

- Ao escanear dados no Cloud Volumes ONTAP na AWS ou no Amazon FSx para buckets ONTAP , você usa um agente de console na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um agente de console no Azure.
  - Para o Azure NetApp Files, ele deve ser implantado na mesma região que os volumes que você deseja verificar.
- Ao escanear dados no Cloud Volumes ONTAP no GCP, você usa um agente do Console no GCP.

Sistemas ONTAP locais, compartilhamentos de arquivos NetApp e bancos de dados podem ser verificados ao usar qualquer um desses agentes do Console na nuvem.

Observe que você também pode "instalar o agente do Console no local" em um host Linux em sua rede ou na nuvem. Alguns usuários que planejam instalar o Data Classification no local também podem optar por instalar o agente do Console no local.

Pode haver situações em que você precise usar "vários agentes de console" .

A Classificação de Dados não impõe um limite à quantidade de dados que pode escanear. Cada agente do Console suporta a digitalização e a exibição de 500 TiB de dados. Para escanear mais de 500 TiB de dados,"instalar outro agente do Console" então"implantar outra instância de Classificação de Dados" . + A interface do usuário do console exibe dados de um único conector. Para obter dicas sobre como visualizar dados de vários agentes do Console, consulte"Trabalhar com vários agentes do Console" .

#### Apoio regional do governo

A classificação de dados é suportada quando o agente do Console é implantado em uma região governamental (AWS GovCloud, Azure Gov ou Azure DoD). Quando implantada dessa maneira, a Classificação de Dados tem as seguintes restrições:

"Saiba mais sobre como implantar o agente do Console em uma região governamental.".

### Pré-requisitos

Revise os seguintes pré-requisitos para garantir que você tenha uma configuração compatível antes de implantar a Classificação de Dados na nuvem. Quando você implanta a Classificação de Dados na nuvem, ela fica localizada na mesma sub-rede que o agente do Console.

#### Habilitar acesso de saída à Internet a partir da Classificação de Dados

A classificação de dados requer acesso de saída à Internet. Se sua rede virtual ou física usar um servidor proxy para acesso à Internet, certifique-se de que a instância de Classificação de Dados tenha acesso de saída à Internet para contatar os seguintes endpoints. O proxy deve ser opaco. Proxies transparentes não são suportados atualmente.

Revise a tabela apropriada abaixo, dependendo se você está implantando a Classificação de Dados na AWS, Azure ou GCP.

**Pontos de extremidade necessários para AWS**

| Pontos finais | Propósito |
|---|---|
| \ https://api.console.netapp.com | Comunicação com o serviço Console, que inclui contas NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicação com o site do Console para autenticação centralizada do usuário. |
| \ https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornece acesso a imagens de software, manifestos e modelos. |
| \ https://kinesis.us-east-1.amazonaws.com | Permite que o NetApp transmita dados de registros de auditoria. |
| \ https://cognito-idp.us-east-1.amazonaws.com \ https://cognito-identity.us-east-1.amazonaws.com \ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com \ https://customer-data-production.s3.us-west-2.amazonaws.com | Permite que a Classificação de Dados acesse e baixe manifestos e modelos, além de enviar logs e métricas. |

**Pontos de extremidade necessários para o Azure**

| Pontos finais | Propósito |
|---|---|
| \ https://api.console.netapp.com | Comunicação com o serviço Console, que inclui contas NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicação com o site do Console para autenticação centralizada do usuário. |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornece acesso a imagens de software, manifestos, modelos e para enviar logs e métricas. |
| \ https://support.compliance.api.console.netapp.com/ | Permite que o NetApp transmita dados de registros de auditoria. |

**Pontos de extremidade necessários para o GCP**

| Pontos finais | Propósito |
|---|---|
| \ https://api.console.netapp.com | Comunicação com o serviço Console, que inclui contas NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicação com o site do Console para autenticação centralizada do usuário. |

| Pontos finais | Propósito |
| --- | --- |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornece acesso a imagens de software, manifestos, modelos e para enviar logs e métricas. |
| \ https://support.compliance.api.console.netapp.com/ | Permite que o NetApp transmita dados de registros de auditoria. |

**Certifique-se de que a Classificação de Dados tenha as permissões necessárias**

Certifique-se de que a Classificação de Dados tenha permissões para implantar recursos e criar grupos de segurança para a instância da Classificação de Dados.

- "Permissões do Google Cloud"
- "Permissões da AWS"
- "Permissões do Azure"

**Garantir que o agente do Console possa acessar a Classificação de Dados**

Garanta a conectividade entre o agente do Console e a instância de Classificação de Dados. O grupo de segurança do agente do Console deve permitir tráfego de entrada e saída pela porta 443 de e para a instância de Classificação de Dados. Essa conexão permite a implantação da instância de Classificação de Dados e permite que você visualize informações nas guias Conformidade e Governança. A classificação de dados é suportada em regiões governamentais na AWS e no Azure.

Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações da AWS e AWS GovCloud. Ver "Regras para o agente do Console na AWS" para mais detalhes.

Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações do Azure e do Azure Government. Ver "Regras para o agente do Console no Azure" para mais detalhes.

**Garanta que você pode manter a Classificação de Dados em execução**

A instância de Classificação de Dados precisa permanecer ativa para escanear continuamente seus dados.

**Garantir a conectividade do navegador da web com a Classificação de Dados**

Depois que a Classificação de Dados estiver habilitada, certifique-se de que os usuários acessem a interface do Console de um host que tenha uma conexão com a instância da Classificação de Dados.

A instância de Classificação de Dados 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 Console deve ter uma conexão com esse endereço IP privado. Essa conexão pode vir de uma conexão direta com seu provedor de nuvem (por exemplo, uma VPN) ou de um host que esteja dentro da mesma rede que a instância de Classificação de Dados.

**Verifique seus limites de vCPU**

Certifique-se de que o limite de vCPU do seu provedor de nuvem permite a implantação de uma instância com o número necessário de núcleos. Você precisará verificar o limite de vCPU para a família de instâncias relevante na região onde o Console está sendo executado. "Veja os tipos de instância

necessários" .

Veja os links a seguir para mais detalhes sobre os limites de vCPU:

- "Documentação da AWS: cotas de serviço do Amazon EC2"
- "Documentação do Azure: Cotas de vCPU de máquina virtual"
- "Documentação do Google Cloud: Cotas de recursos"

**Implantar classificação de dados na nuvem**

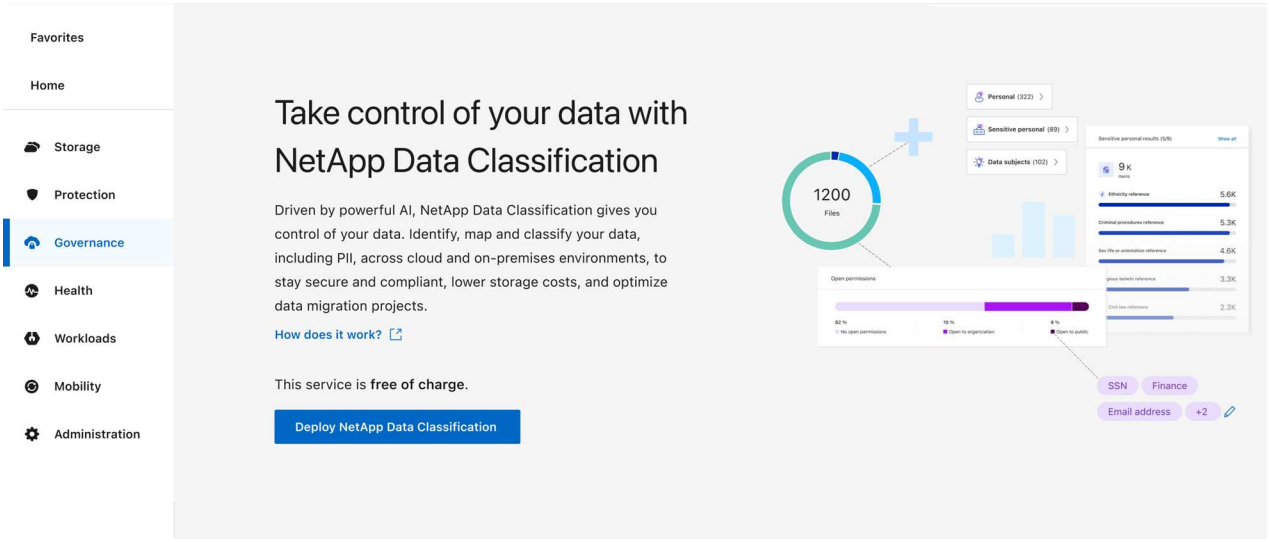
Siga estas etapas para implantar uma instância de Classificação de Dados na nuvem. O agente do Console implantará a instância na nuvem e, em seguida, instalará o software de classificação de dados nessa instância.

Em regiões onde o tipo de instância padrão não está disponível, a Classificação de Dados é executada em um"tipo de instância alternativo" .

### Implantar na AWS

#### Passos

1. Na página principal de Classificação de Dados, selecione **Implantar classificação no local ou na nuvem**.

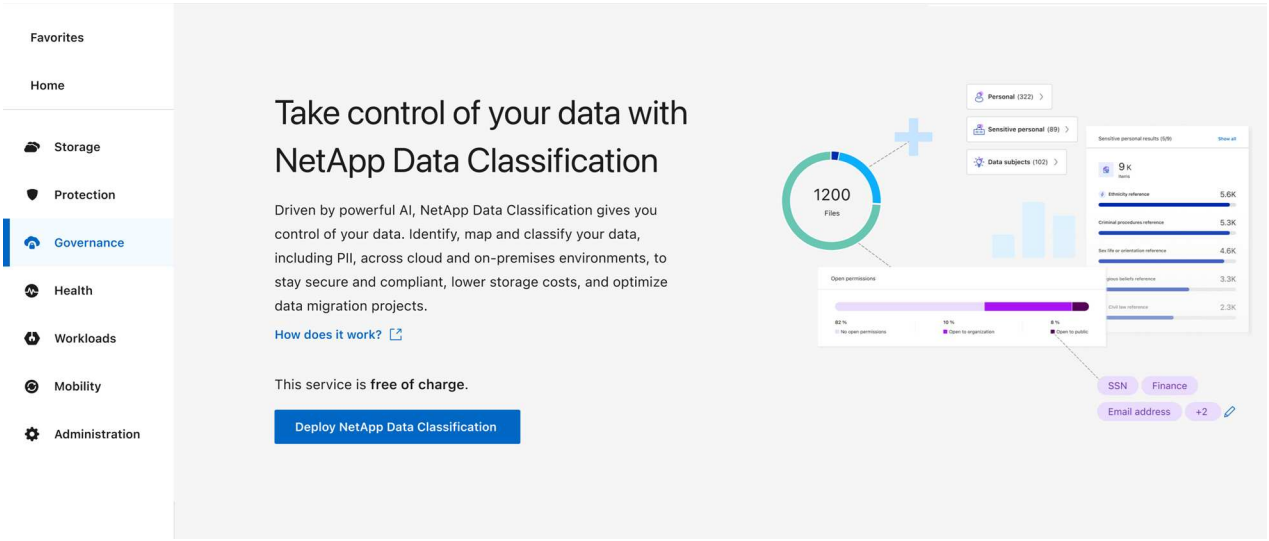



2. Na página *Instalação*, selecione **Implantar > Implantar** para usar o tamanho de instância "Grande" e iniciar o assistente de implantação na nuvem.
3. O assistente exibe o progresso à medida que avança nas etapas de implantação. Quando forem necessárias entradas ou se houver problemas, você será solicitado.
4. Quando a instância for implantada e a Classificação de Dados estiver instalada, selecione **Continuar para a configuração** para ir para a página *Configuração*.

### Implantar no Azure

#### Passos

1. Na página principal de Classificação de Dados, selecione **Implantar classificação no local ou na nuvem**.



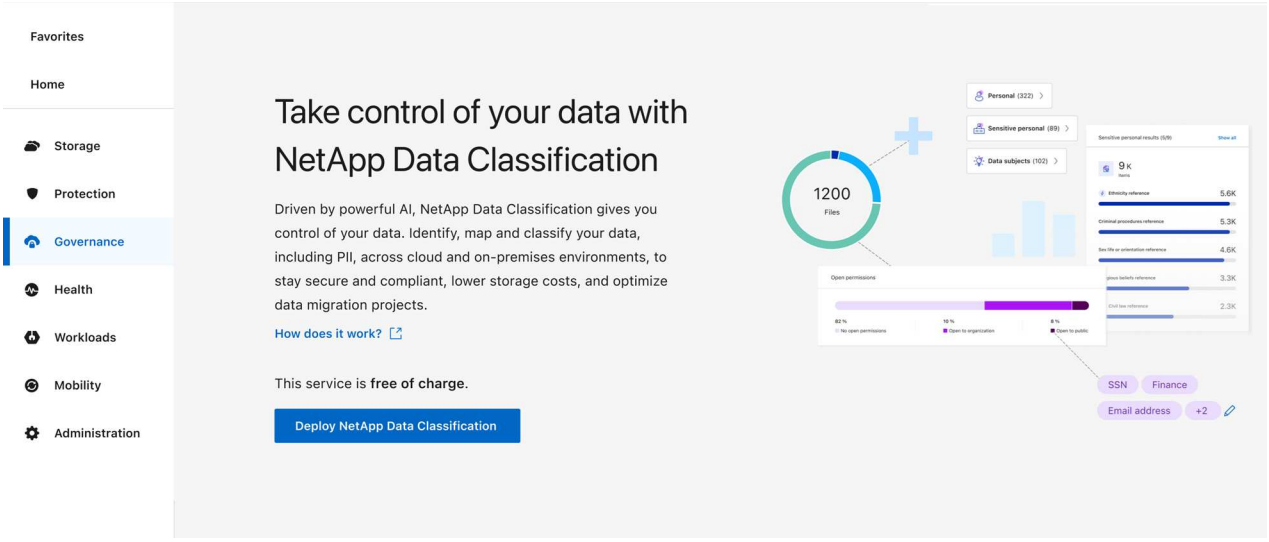

2. Selecione **Implantar** para iniciar o assistente de implantação na nuvem.

3. O assistente exibe o progresso à medida que avança nas etapas de implantação. Ele irá parar e solicitar uma entrada caso encontre algum problema.
4. Quando a instância for implantada e a Classificação de Dados estiver instalada, selecione **Continuar para a configuração** para ir para a página *Configuração*.

**Implantar no Google Cloud**

**Passos**

1. Na página principal de Classificação de Dados, selecione **Governança > Classificação**.
2. Selecione **Implantar classificação no local ou na nuvem**.




3. Selecione **Implantar** para iniciar o assistente de implantação na nuvem.
4. O assistente exibe o progresso à medida que avança nas etapas de implantação. Ele irá parar e solicitar uma entrada caso encontre algum problema.
5. Quando a instância for implantada e a Classificação de Dados estiver instalada, selecione **Continuar para a configuração** para ir para a página *Configuração*.

**Resultado**

O Console implanta a instância de Classificação de Dados no seu provedor de nuvem.

As atualizações do agente do Console e do software de classificação de dados são automatizadas, desde que as instâncias tenham conectividade com a Internet.

**O que vem a seguir**

Na página Configuração, você pode selecionar as fontes de dados que deseja verificar.

## Instalar a NetApp Data Classification em um host que tenha acesso à Internet

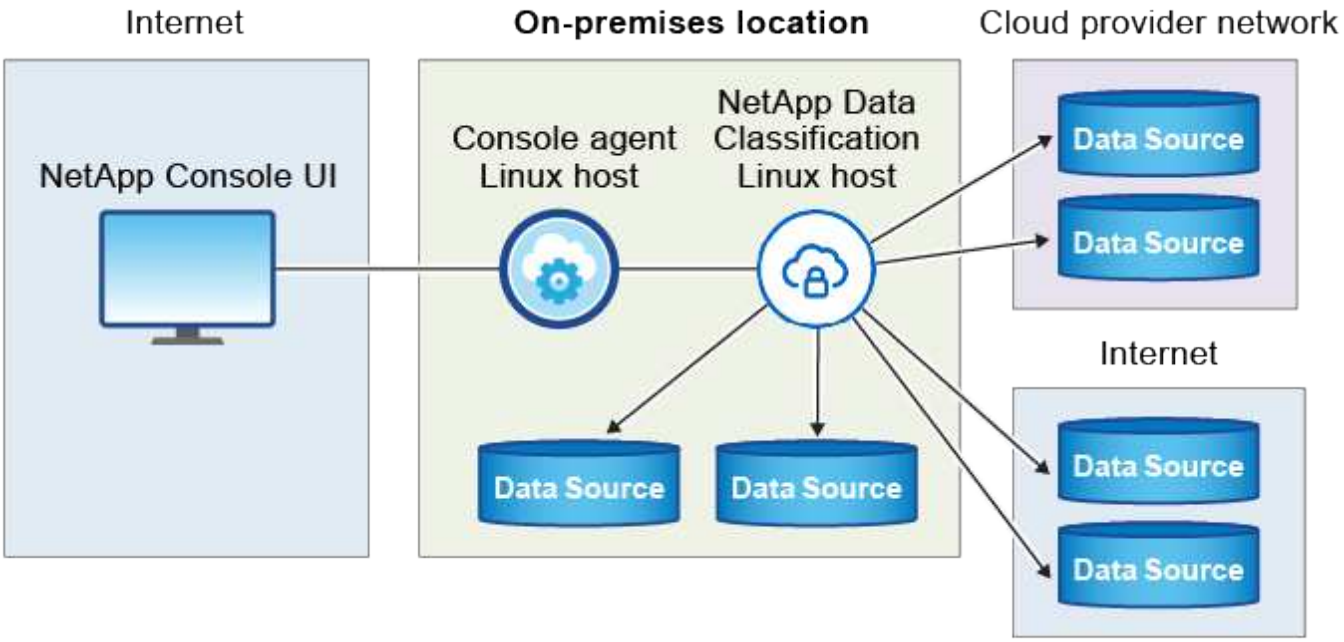
Para implantar a NetApp Data Classification em um host Linux na sua rede ou em um host Linux na nuvem que tenha acesso à Internet, você precisa implantar o host Linux manualmente na sua rede ou na nuvem.

A instalação local é uma boa opção se você preferir escanear sistemas ONTAP locais usando uma instância de Classificação de Dados que também esteja localizada no local. Isto não é um requisito. O software

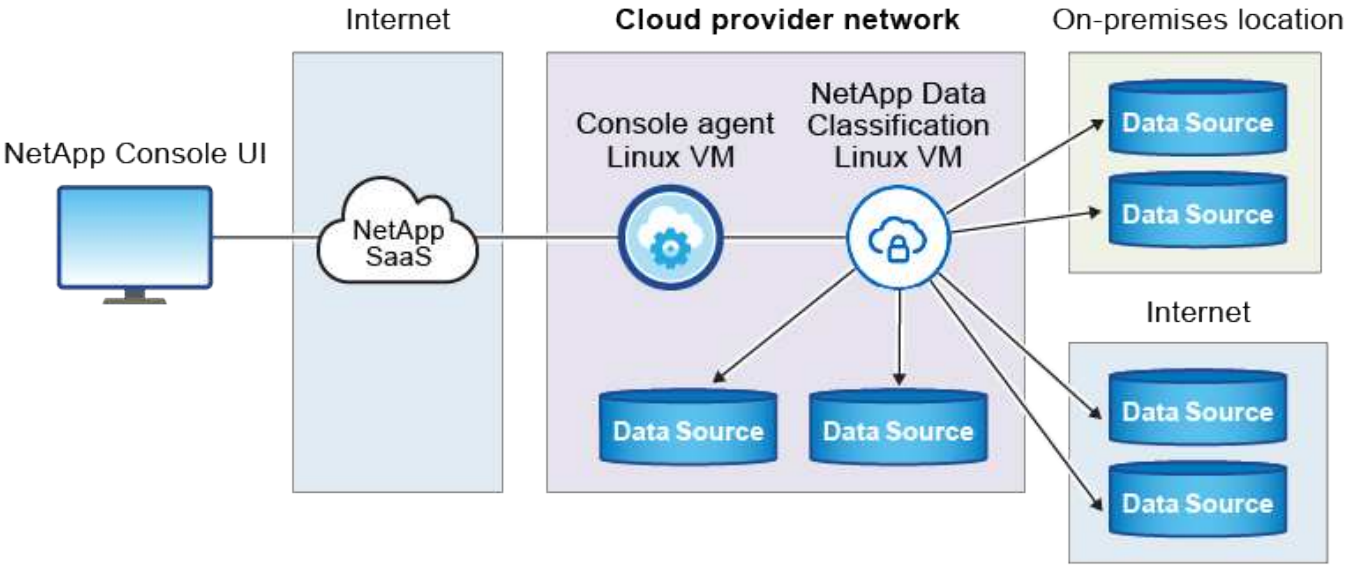
funciona da mesma forma, independentemente do método de instalação escolhido.

O script de instalação do Data Classification começa verificando se o sistema e o ambiente atendem aos pré-requisitos necessários. Se todos os pré-requisitos forem atendidos, a instalação será iniciada. Se você quiser verificar os pré-requisitos independentemente de executar a instalação da Classificação de Dados, há um pacote de software separado que você pode baixar e que testa apenas os pré-requisitos. "Veja como verificar se o seu host Linux está pronto para instalar o Data Classification" .

A instalação típica em um host Linux *em suas instalações* tem os seguintes componentes e conexões.




A instalação típica em um host Linux *na nuvem* tem os seguintes componentes e conexões.




**Início rápido**

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

### 1 Criar um agente de console

Se você ainda não tem um agente de console, "implantar o agente do Console no local" em um host Linux na sua rede ou em um host Linux na nuvem.

Você também pode criar um agente de console com seu provedor de nuvem. Ver "criando um agente de console na AWS" , "criando um agente de console no Azure" , ou "criando um agente de console no GCP" .

### 2 Revise os pré-requisitos

Certifique-se de que seu ambiente possa atender aos pré-requisitos. Isso inclui acesso de saída à Internet para a instância, conectividade entre o agente do Console e a Classificação de Dados pela porta 443 e muito mais. Veja a lista completa .

Você também precisa de um sistema Linux que atenda osseguintes requisitos .

### 3 Baixar e implantar a Classificação de Dados

Baixe o software Cloud Data Classification no site de suporte da NetApp e copie o arquivo do instalador para o host Linux que você planeja usar. Em seguida, inicie o assistente de instalação e siga as instruções para implantar a instância de Classificação de Dados.

#### Criar um agente de console

Um agente de console é necessário antes que você possa instalar e usar a Classificação de Dados. Na maioria dos casos, você provavelmente terá um agente de console configurado antes de tentar ativar a Classificação de Dados porque a maioria "Os recursos do console exigem um agente do console" , mas há casos em que você precisará configurar um agora.

Para criar um no ambiente do seu provedor de nuvem, consulte "criando um agente de console na AWS" , "criando um agente de console no Azure" , ou "criando um agente de console no GCP" .

Existem alguns cenários em que você precisa usar um agente do Console implantado em um provedor de nuvem específico:

- Ao digitalizar dados no Cloud Volumes ONTAP na AWS ou no Amazon FSx para ONTAP, você usa um agente de console na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um agente de console no Azure.

  Para o Azure NetApp Files, ele deve ser implantado na mesma região que os volumes que você deseja verificar.

- Ao escanear dados no Cloud Volumes ONTAP no GCP, você usa um agente do Console no GCP.

Sistemas ONTAP locais, compartilhamentos de arquivos NetApp e contas de banco de dados podem ser verificados usando qualquer um desses agentes do Cloud Console.

Observe que você também pode "implantar o agente do Console no local" em um host Linux na sua rede ou em um host Linux na nuvem. Alguns usuários que planejam instalar o Data Classification no local também podem optar por instalar o agente do Console no local.

Você precisará do endereço IP ou nome do host do sistema do agente do Console ao instalar o Data Classification. Você terá essas informações se tiver instalado o agente do Console em suas instalações. Se o agente do Console estiver implantado na nuvem, você poderá encontrar essas informações no Console: selecione o ícone Ajuda, depois **Suporte** e depois **Agente do Console**.

### Preparar o sistema host Linux

O software de classificação de dados deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de software e assim por diante. O host Linux pode estar na sua rede ou na nuvem.

Certifique-se de que você pode manter a Classificação de Dados em execução. A máquina de classificação de dados precisa permanecer ligada para escanear continuamente seus dados.

- A classificação de dados deve estar em um host dedicado. O host não pode ser compartilhado com outros aplicativos ou softwares de terceiros, como antivírus.
- Escolha o tamanho que esteja de acordo com o conjunto de dados que você planeja analisar com a Classificação de Dados.

| Tamanho do sistema | CPU | RAM (a memória swap deve ser desabilitada) | Disco |
|---|---|---|---|
| **Extra Grande** | 32 CPUs | 128 GB de RAM | • 1 TiB SSD em /, ou 100 GiB disponíveis em /opt<br>• 895 GiB disponíveis em /var/lib/docker<br>• 5 GiB em /tmp<br>• **Para Podman, 30 GB em /var/tmp** |
| **Grande** | 16 CPUs | 64 GB de RAM | • SSD de 500 GiB em /, ou 100 GiB disponíveis em /opt<br>• 400 GiB disponíveis em /var/lib/docker ou para Podman /var/lib/containers<br>• 5 GiB em /tmp<br>• **Para Podman, 30 GB em /var/tmp** |

- Ao implantar uma instância de computação na nuvem para sua instalação de Classificação de Dados, é recomendável usar um sistema que atenda aos requisitos de sistema "Grande" acima:
  - **Tipo de instância do Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Veja tipos adicionais de instâncias da AWS" .
  - **Tamanho da VM do Azure**: "Standard_D16s_v3". "Veja tipos adicionais de instância do Azure" .
  - **Tipo de máquina GCP**: "n2-standard-16". "Veja tipos de instância adicionais do GCP" .
- **Permissões de pasta UNIX**: As seguintes permissões mínimas do UNIX são necessárias:

| Pasta | Permissões mínimas |
| --- | --- |
| /tmp | `rwxrwxrwt` |
| /optar | `rwxr-xr-x` |
| /var/lib/docker | `rwx------` |
| /usr/lib/systemd/sistema | `rwxr-xr-x` |

- **Sistema operacional**:
  - Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Docker:
    - Red Hat Enterprise Linux versão 7.8 e 7.9
    - Ubuntu 22.04 (requer classificação de dados versão 1.23 ou superior)
    - Ubuntu 24.04 (requer classificação de dados versão 1.23 ou superior)
  - Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão 1.30 ou superior do Data Classification:
    - Red Hat Enterprise Linux versão 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
  - As extensões de vetor avançadas (AVX2) devem estar habilitadas no sistema host.
- **Red Hat Subscription Management**: O host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o sistema não poderá acessar repositórios para atualizar o software de terceiros necessário durante a instalação.
- **Software adicional**: Você deve instalar o seguinte software no host antes de instalar o Data Classification:
  - Dependendo do sistema operacional que você estiver usando, será necessário instalar um dos mecanismos de contêiner:
    - Docker Engine versão 19.3.1 ou superior. "Ver instruções de instalação" .
    - Podman versão 4 ou superior. Para instalar o Podman, digite(`sudo yum install podman netavark -y` ).
- Python versão 3.6 ou superior. "Ver instruções de instalação" .
  - **Considerações sobre NTP**: A NetApp recomenda configurar o sistema de classificação de dados para usar um serviço de protocolo de tempo de rede (NTP). O tempo deve ser sincronizado entre o sistema de Classificação de Dados e o sistema do agente do Console.
- **Considerações sobre firewall**: Se você está planejando usar `firewalld` , recomendamos que você o habilite antes de instalar a Classificação de Dados. Execute os seguintes comandos para configurar `firewalld` para que seja compatível com a Classificação de Dados:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se você estiver planejando usar hosts de Classificação de Dados adicionais como nós do scanner, adicione estas regras ao seu sistema primário neste momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Observe que você deve reiniciar o Docker ou o Podman sempre que habilitar ou atualizar `firewalld` configurações.

O endereço IP do sistema host de Classificação de Dados não pode ser alterado após a instalação.

### Habilitar acesso de saída à Internet a partir da Classificação de Dados

A classificação de dados requer acesso de saída à Internet. Se sua rede virtual ou física usar um servidor proxy para acesso à Internet, certifique-se de que a instância de Classificação de Dados tenha acesso de saída à Internet para contatar os seguintes endpoints.

| Pontos finais | Propósito |
|---|---|
| \ https://api.console.netapp.com | Comunicação com o Console, que inclui contas NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicação com o site do Console para autenticação centralizada do usuário. |
| \ https://support.compliance.api.bluexp.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornece acesso a imagens de software, manifestos, modelos e para enviar logs e métricas. |
| https://support.compliance.api.bluexp.netapp.com/ | Permite que o NetApp transmita dados de registros de auditoria. |
| \ https://github.com/docker \ https://download.docker.com | Fornece pacotes de pré-requisitos para instalação do docker. |
| \ http://packages.ubuntu.com/ \ http://archive.ubuntu.com | Fornece pacotes de pré-requisitos para instalação do Ubuntu. |

### Verifique se todas as portas necessárias estão habilitadas

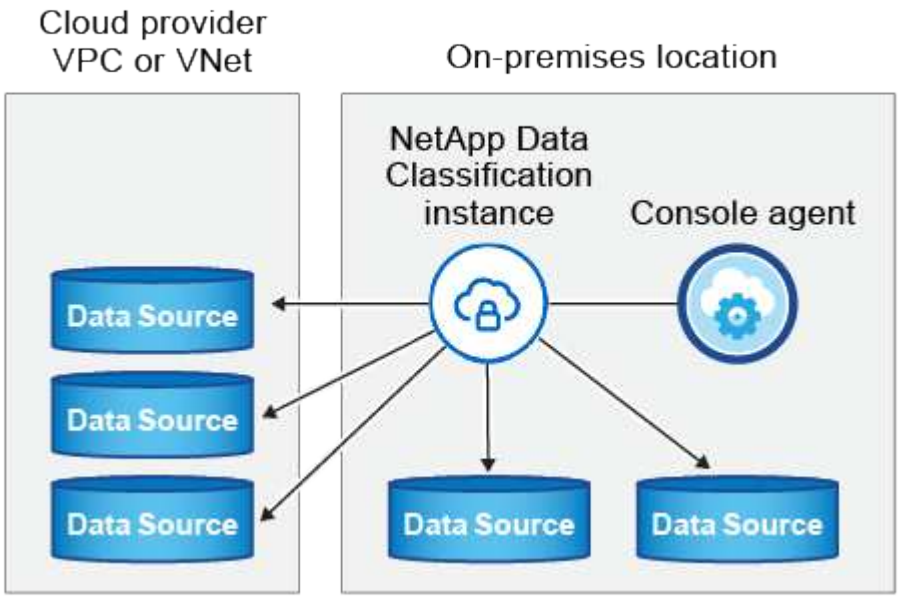
Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o agente do Console, a Classificação de Dados, o Active Directory e suas fontes de dados.

| Tipo de conexão | Portos | Descrição |
| --- | --- | --- |
| Agente de console <> Classificação de dados | 8080 (TCP), 443 (TCP) e 80. 9000 | As regras de firewall ou roteamento para o agente do Console devem permitir tráfego de entrada e saída pela porta 443 de e para a instância de Classificação de Dados. Certifique-se de que a porta 8080 esteja aberta para que você possa ver o progresso da instalação no Console. Se um firewall for usado no host Linux, a porta 9000 será necessária para processos internos em um servidor Ubuntu. |
| Agente de console <> cluster ONTAP (NAS) | 443 (TCP) | O Console descobre clusters ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, elas deverão atender aos seguintes requisitos:<br>• O host do agente do Console deve permitir acesso HTTPS de saída pela porta 443. Se o agente do Console estiver na nuvem, toda a comunicação de saída será permitida pelas regras predefinidas de firewall ou roteamento.<br>• O cluster ONTAP deve permitir acesso HTTPS de entrada pela porta 443. A política de firewall padrão "mgmt" permite acesso HTTPS de entrada de todos os endereços IP. Se você modificou esta política padrão ou criou sua própria política de firewall, deverá associar o protocolo HTTPS a essa política e habilitar o acesso do host do agente do Console. |
| Classificação de Dados <> cluster ONTAP | • Para NFS - 111 (TCP\UDP) e 2049 (TCP\UDP)<br>• Para CIFS - 139 (TCP\UDP) e 445 (TCP\UDP) | A Classificação de Dados precisa de uma conexão de rede com cada sub-rede Cloud Volumes ONTAP ou sistema ONTAP local. Firewalls ou regras de roteamento para o Cloud Volumes ONTAP devem permitir conexões de entrada da instância de Classificação de Dados.<br>Certifique-se de que estas portas estejam abertas para a instância de Classificação de Dados:<br>• Para NFS - 111 e 2049<br>• Para CIFS - 139 e 445<br>As políticas de exportação de volume NFS devem permitir acesso da instância de Classificação de Dados. |

| Tipo de conexão | Portos | Descrição |
| --- | --- | --- |
| Classificação de Dados <> Active Directory | 389 (TCP e UDP), 636 (TCP), 3268 (TCP) e 3269 (TCP) | Você deve ter um Active Directory já configurado para os usuários da sua empresa. Além disso, a Classificação de Dados precisa de credenciais do Active Directory para verificar volumes CIFS.<br><br>Você deve ter as informações do Active Directory:<br><br>• Endereço IP do servidor DNS ou vários endereços IP<br>• Nome de usuário e senha para o servidor<br>• Nome de domínio (nome do Active Directory)<br>• Se você está usando LDAP seguro (LDAPS) ou não<br>• Porta do servidor LDAP (normalmente 389 para LDAP e 636 para LDAP seguro) |

**Instalar a Classificação de Dados no host Linux**

Para configurações típicas, você instalará o software em um único sistema host. Veja esses passos aqui .




VerPreparando o sistema host Linux eRevisando pré-requisitos para obter a lista completa de requisitos antes de implantar a Classificação de Dados.

As atualizações do software de classificação de dados são automatizadas, desde que a instância tenha conectividade com a Internet.

Atualmente, a Classificação de Dados não consegue verificar buckets S3, Azure NetApp Files ou FSx para ONTAP quando o software está instalado no local. Nesses casos, você precisará implantar um agente de console separado e uma instância de classificação de dados na nuvem e "alternar entre conectores" para suas diferentes fontes de dados.

#### Instalação de host único para configurações típicas

Revise os requisitos e siga estas etapas ao instalar o software de classificação de dados em um único host local.

"Assista a este vídeo"para ver como instalar o Data Classification.

Observe que todas as atividades de instalação são registradas durante a instalação do Data Classification. Caso encontre algum problema durante a instalação, você pode visualizar o conteúdo do log de auditoria da instalação. Está escrito para `/opt/netapp/install_logs/` .

**Antes de começar**

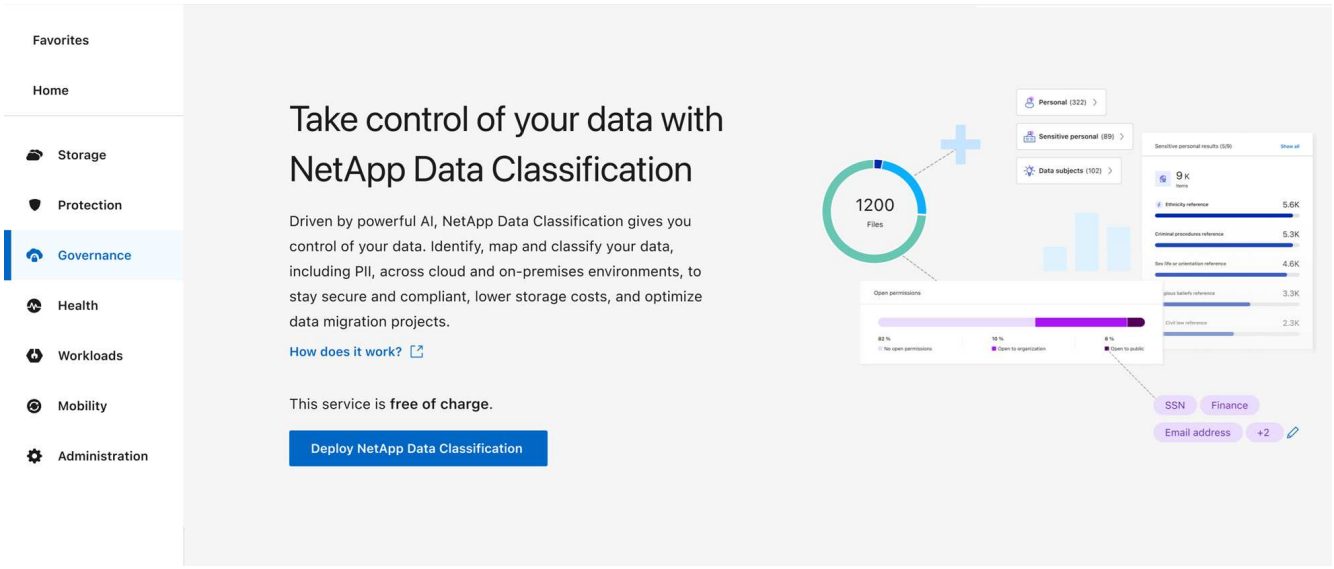
- Verifique se o seu sistema Linux atende aos requisitosrequisitos do host .
- Verifique se o sistema tem os dois pacotes de software pré-requisitos instalados (Docker Engine ou Podman e Python 3).
- Certifique-se de ter privilégios de root no sistema Linux.
- Se você estiver usando um proxy para acessar a Internet:
  - Você precisará das informações do servidor proxy (endereço IP ou nome do host, porta de conexão, esquema de conexão: https ou http, nome de usuário e senha).
  - Se o proxy estiver executando a interceptação TLS, você precisará saber o caminho no sistema Linux de classificação de dados onde os certificados TLS CA estão armazenados.
  - O proxy deve ser opaco. Atualmente, a Classificação de Dados não oferece suporte a proxies transparentes.
  - O usuário deve ser um usuário local. Usuários de domínio não são suportados.
- Verifique se o seu ambiente offline atende aos requisitospermissões e conectividade .

**Passos**

1. Baixe o software de classificação de dados do "Site de suporte da NetApp" . O arquivo que você deve selecionar é chamado **DATASENSE-INSTALLER-<versão>.tar.gz**.
2. Copie o arquivo do instalador para o host Linux que você planeja usar (usando `scp` ou algum outro método).
3. Descompacte o arquivo do instalador na máquina host, por exemplo:

   ```
   tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
   ```

4. No Console, selecione **Governança > Classificação**.
5. Selecione **Implantar classificação no local ou na nuvem**.




6. Dependendo se você estiver instalando a Classificação de Dados em uma instância preparada na nuvem ou em uma instância preparada em suas instalações, selecione a opção **Implantar** apropriada para iniciar a instalação da Classificação de Dados.
7. A caixa de diálogo *Implantar classificação de dados no local* é exibida. Copie o comando fornecido (por exemplo: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq` ) e cole-o em um arquivo de texto para que você possa usá-lo mais tarde. Em seguida, selecione **Fechar** para fechar a caixa de diálogo.
8. Na máquina host, insira o comando que você copiou e siga uma série de prompts, ou você pode fornecer o comando completo, incluindo todos os parâmetros necessários, como argumentos de linha de comando.

   Observe que o instalador realiza uma pré-verificação para garantir que os requisitos do sistema e da rede estejam corretos para uma instalação bem-sucedida. "Assista a este vídeo" para entender as mensagens e implicações da pré-verificação.

| Insira os parâmetros conforme solicitado: | Digite o comando completo: |
| --- | --- |
| a. Cole o comando que você copiou da etapa 7: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>`<br><br>Se você estiver instalando em uma instância de nuvem (não em suas instalações), adicione `--manual-cloud-install <cloud_provider>`.<br><br>b. Insira o endereço IP ou o nome do host da máquina host de Classificação de Dados para que ela possa ser acessada pelo sistema do agente do Console.<br><br>c. Insira o endereço IP ou o nome do host da máquina host do agente do Console para que ele possa ser acessado pelo sistema de Classificação de Dados.<br><br>d. Insira os detalhes do proxy conforme solicitado. Se o seu agente do Console já usa um proxy, não há necessidade de inserir essas informações novamente aqui, pois a Classificação de Dados usará automaticamente o proxy usado pelo agente do Console. | Como alternativa, você pode criar o comando completo com antecedência, fornecendo os parâmetros de host e proxy necessários:<br>`sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>` |

Valores variáveis:

- *account_id* = ID da conta NetApp
- *client_id* = ID do cliente do agente do console (adicione o sufixo "clients" ao ID do cliente, caso ainda não esteja lá)
- *user_token* = token de acesso do usuário JWT
- *ds_host* = endereço IP ou nome do host do sistema Data Classification Linux.
- *cm_host* = endereço IP ou nome do host do sistema do agente do Console.
- *cloud_provider* = Ao instalar em uma instância de nuvem, digite "AWS", "Azure" ou "Gcp", dependendo do provedor de nuvem.
- *proxy_host* = IP ou nome do host do servidor proxy se o host estiver atrás de um servidor proxy.
- *proxy_port* = Porta para conectar ao servidor proxy (padrão 80).
- *proxy_scheme* = Esquema de conexão: https ou http (padrão http).
- *proxy_user* = Usuário autenticado para se conectar ao servidor proxy, se autenticação básica for necessária. O usuário deve ser um usuário local - usuários de domínio não são suportados.
- *proxy_password* = Senha para o nome de usuário que você especificou.
- *ca_cert_dir* = Caminho no sistema Linux de classificação de dados contendo pacotes adicionais de certificados CA TLS. Necessário somente se o proxy estiver executando interceptação TLS.

**Resultado**

O instalador do Data Classification instala pacotes, registra a instalação e instala o Data Classification. A

instalação pode levar de 10 a 20 minutos.

Se houver conectividade pela porta 8080 entre a máquina host e a instância do agente do Console, você verá o progresso da instalação na guia Classificação de Dados no Console.

**O que vem a seguir**

Na página Configuração, você pode selecionar as fontes de dados que deseja verificar.

## Instalar o NetApp Data Classification em um host Linux sem acesso à Internet

A instalação do NetApp Data Classification em um host Linux em um site local que não tem acesso à Internet é conhecida como *modo privado*. Este tipo de instalação, que usa um script de instalação, não tem conectividade com a camada SaaS do NetApp Console .

> O modo privado BlueXP (interface BlueXP legada) normalmente é usado com ambientes locais que não têm conexão com a Internet e com regiões de nuvem seguras, o que inclui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. A NetApp continua a oferecer suporte a esses ambientes com a interface legada BlueXP . Para documentação do modo privado na interface BlueXP legada, consulte"Documentação em PDF para o modo privado do BlueXP" .

## Verifique se o seu host Linux está pronto para instalar o NetApp Data Classification

Antes de instalar o NetApp Data Classification manualmente em um host Linux, opcionalmente, execute um script no host para verificar se todos os pré-requisitos estão em vigor para instalar o Data Classification. Você pode executar este script em um host Linux na sua rede ou em um host Linux na nuvem. O host pode estar conectado à Internet ou pode residir em um site que não tem acesso à Internet (um *dark site*).

O script de instalação do Data Classification inclui um script de teste para garantir que seu ambiente atenda aos requisitos. Você pode executar este script separadamente para verificar se o host Linux está pronto antes de executar o script de instalação.

**Começando**

Você executará as seguintes tarefas.

- Opcionalmente, instale um agente do Console caso você ainda não tenha um instalado. Você pode executar o script de teste sem ter um agente do Console instalado, mas o script verifica a conectividade entre o agente do Console e a máquina host de Classificação de Dados. Portanto, é recomendável que você tenha um agente do Console.
- Prepare a máquina host e verifique se ela atende a todos os requisitos.
- Habilite o acesso de saída à Internet a partir da máquina host de Classificação de Dados.
- Verifique se todas as portas necessárias estão habilitadas em todos os sistemas.
- Baixe e execute o script de teste de pré-requisito.

### Criar um agente de console

Um agente de console é necessário antes que você possa instalar e usar a Classificação de Dados. No entanto, você pode executar o script de pré-requisitos sem um agente do Console.

Você pode "instalar o agente do Console no local" em um host Linux em sua rede ou em um host Linux na nuvem. Você também pode instalar o Data Classification localmente se o agente do Console estiver instalado localmente.

Para criar um agente de console no ambiente do seu provedor de nuvem, consulte:

- "criando um agente de console na AWS"
- "criando um agente de console no Azure"
- "criando um agente de console no GCP"

Você precisa do endereço IP ou do nome do host do sistema do agente do Console ao executar o script de pré-requisitos. Você possui essas informações se instalou o agente do Console em suas instalações. Se o agente do Console estiver implantado na nuvem, você poderá encontrar essas informações no Console: selecione o ícone Ajuda e, em seguida, **Suporte**; na seção Agente e Auditoria, selecione **Acessar o agente**.

### Verificar os requisitos do host

O software de classificação de dados deve ser executado em um host que atenda a requisitos específicos de sistema operacional, requisitos de RAM e requisitos de software.

- A classificação de dados deve estar em um host dedicado. O host não pode ser compartilhado com outros aplicativos ou softwares de terceiros, como antivírus.
- Escolha o tamanho que esteja de acordo com o conjunto de dados que você planeja analisar com a Classificação de Dados.

| Tamanho do sistema | CPU | RAM (a memória swap deve ser desabilitada) | Disco |
|---|---|---|---|
| **Extra Grande** | 32 CPUs | 128 GB de RAM | • 1 TiB SSD em /, ou 100 GiB disponíveis em /opt<br>• 895 GiB disponíveis em /var/lib/docker<br>• 5 GiB em /tmp<br>• **Para Podman, 30 GB em /var/tmp** |
| **Grande** | 16 CPUs | 64 GB de RAM | • SSD de 500 GiB em /, ou 100 GiB disponíveis em /opt<br>• 400 GiB disponíveis em /var/lib/docker ou para Podman /var/lib/containers<br>• 5 GiB em /tmp<br>• **Para Podman, 30 GB em /var/tmp** |

- Ao implantar uma instância de computação na nuvem para sua instalação de Classificação de Dados, é recomendável usar um sistema que atenda aos requisitos de sistema "Grande" acima:
  - **Tipo de instância do Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Veja tipos adicionais de instâncias da AWS" .
  - **Tamanho da VM do Azure**: "Standard_D16s_v3". "Veja tipos adicionais de instância do Azure" .
  - **Tipo de máquina GCP**: "n2-standard-16". "Veja tipos de instância adicionais do GCP" .
- **Permissões de pasta UNIX**: As seguintes permissões mínimas do UNIX são necessárias:

| Pasta | Permissões mínimas |
|---|---|
| /tmp | `rwxrwxrwt` |
| /optar | `rwxr-xr-x` |
| /var/lib/docker | `rwx------` |
| /usr/lib/systemd/sistema | `rwxr-xr-x` |

- **Sistema operacional**:
  - Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Docker:
    - Red Hat Enterprise Linux versão 7.8 e 7.9
    - Ubuntu 22.04 (requer classificação de dados versão 1.23 ou superior)
    - Ubuntu 24.04 (requer classificação de dados versão 1.23 ou superior)
  - Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão 1.30 ou superior do Data Classification:
    - Red Hat Enterprise Linux versão 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
  - As extensões de vetor avançadas (AVX2) devem estar habilitadas no sistema host.
- **Red Hat Subscription Management**: O host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o sistema não poderá acessar repositórios para atualizar o software de terceiros necessário durante a instalação.
- **Software adicional**: Você deve instalar o seguinte software no host antes de instalar o Data Classification:
  - Dependendo do sistema operacional que você estiver usando, será necessário instalar um dos mecanismos de contêiner:
    - Docker Engine versão 19.3.1 ou superior. "Ver instruções de instalação" .
    - Podman versão 4 ou superior. Para instalar o Podman, digite(`sudo yum install podman netavark -y` ).
- Python versão 3.6 ou superior. "Ver instruções de instalação" .
  - **Considerações sobre NTP**: A NetApp recomenda configurar o sistema de classificação de dados para usar um serviço de protocolo de tempo de rede (NTP). O tempo deve ser sincronizado entre o sistema de Classificação de Dados e o sistema do agente do Console.
- **Considerações sobre firewall**: Se você está planejando usar `firewalld` , recomendamos que você o habilite antes de instalar a Classificação de Dados. Execute os seguintes comandos para configurar `firewalld` para que seja compatível com a Classificação de Dados:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se você estiver planejando usar hosts de Classificação de Dados adicionais como nós de scanner (em um modelo distribuído), adicione estas regras ao seu sistema primário neste momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Observe que você deve reiniciar o Docker ou o Podman sempre que habilitar ou atualizar `firewalld` configurações.

### Habilitar acesso de saída à Internet a partir da Classificação de Dados

A classificação de dados requer acesso de saída à Internet. Se sua rede virtual ou física usar um servidor proxy para acesso à Internet, certifique-se de que a instância de Classificação de Dados tenha acesso de saída à Internet para contatar os seguintes endpoints.

Esta seção não é necessária para sistemas host instalados em sites sem conectividade com a Internet.

| Pontos finais | Propósito |
|---|---|
| \ https://api.console.netapp.com | Comunicação com o serviço Console, que inclui contas NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicação com o site do Console para autenticação centralizada do usuário. |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornece acesso a imagens de software, manifestos, modelos e para enviar logs e métricas. |
| \ https://support.compliance.api.console.netapp.com/ | Permite que o NetApp transmita dados de registros de auditoria. |
| \ https://github.com/docker \ https://download.docker.com | Fornece pacotes de pré-requisitos para instalação do docker. |

| Pontos finais | Propósito |
| --- | --- |
| \ http://packages.ubuntu.com/ \ http://archive.ubuntu.com | Fornece pacotes de pré-requisitos para instalação do Ubuntu. |

### Verifique se todas as portas necessárias estão habilitadas

Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o agente do Console, a Classificação de Dados, o Active Directory e suas fontes de dados.

| Tipo de conexão | Portos | Descrição |
| --- | --- | --- |
| Agente de console <> Classificação de dados | 8080 (TCP), 443 (TCP) e 80. 9000 | As regras de firewall ou roteamento para o agente do Console devem permitir tráfego de entrada e saída pela porta 443 de e para a instância de Classificação de Dados. Certifique-se de que a porta 8080 esteja aberta para que você possa ver o progresso da instalação no Console. Se um firewall for usado no host Linux, a porta 9000 será necessária para processos internos em um servidor Ubuntu. |
| Agente de console <> cluster ONTAP (NAS) | 443 (TCP) | O Console descobre clusters ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, o host do agente do Console deverá permitir acesso HTTPS de saída pela porta 443. Se o agente do Console estiver na nuvem, toda a comunicação de saída será permitida pelas regras predefinidas de firewall ou roteamento. |

### Execute o script de pré-requisitos de classificação de dados

Siga estas etapas para executar o script de pré-requisitos de Classificação de Dados.

"Assista a este vídeo"para ver como executar o script de pré-requisitos e interpretar os resultados.

#### Antes de começar

- Verifique se o seu sistema Linux atende aos requisitosrequisitos do host .
- Verifique se o sistema tem os dois pacotes de software pré-requisitos instalados (Docker Engine ou Podman e Python 3).
- Certifique-se de ter privilégios de root no sistema Linux.

#### Passos

1. Baixe o script de pré-requisitos de classificação de dados do "Site de suporte da NetApp" . O arquivo que você deve selecionar é chamado **standalone-pre-requisite-tester-<version>**.
2. Copie o arquivo para o host Linux que você planeja usar (usando `scp` ou algum outro método).
3. Atribua permissões para executar o script.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. Execute o script usando o seguinte comando.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

   Adicione a opção "--darksite" somente se estiver executando o script em um host que não tenha acesso à Internet. Certos testes de pré-requisito são ignorados quando o host não está conectado à Internet.

5. O script solicita o endereço IP da máquina host de classificação de dados.
   - Digite o endereço IP ou nome do host.
6. O script pergunta se você tem um agente do Console instalado.
   - Digite **N** se você não tiver um agente de console instalado.
   - Digite **Y** se você tiver um agente de console instalado. Em seguida, insira o endereço IP ou o nome do host do agente do Console para que o script de teste possa testar essa conectividade.
7. O script executa uma variedade de testes no sistema e exibe os resultados à medida que avança. Quando termina, ele grava um log da sessão em um arquivo chamado `prerequisites-test-<timestamp>.log` no diretório `/opt/netapp/install_logs` .

**Resultado**

Se todos os testes de pré-requisitos forem executados com sucesso, você poderá instalar o Data Classification no host quando estiver pronto.

Se algum problema for descoberto, ele será categorizado como "Recomendado" ou "Obrigatório" para ser corrigido. Problemas recomendados geralmente são itens que tornariam as tarefas de digitalização e categorização de Classificação de Dados mais lentas. Esses itens não precisam ser corrigidos, mas você pode querer resolvê-los.

Se você tiver algum problema "Obrigatório", corrija-o e execute o script de teste de Pré-requisitos novamente.

# Ative a digitalização em suas fontes de dados

## Digitalizar fontes de dados com a NetApp Data Classification

A NetApp Data Classification verifica os dados nos repositórios (volumes, esquemas de banco de dados ou outros dados do usuário) que você seleciona para identificar dados pessoais e confidenciais. A Classificação de Dados mapeia seus dados organizacionais, categoriza cada arquivo e identifica padrões predefinidos nos dados. O resultado da verificação é um índice de informações pessoais, informações pessoais confidenciais, categorias de dados e tipos de arquivo.

Após a verificação inicial, a Classificação de Dados verifica continuamente seus dados em um sistema round-robin para detectar alterações incrementais. É por isso que é importante manter a instância em execução.

Você pode habilitar e desabilitar verificações no nível do volume ou no nível do esquema do banco de dados.

**Qual é a diferença entre varreduras de mapeamento e classificação?**

Você pode realizar dois tipos de varreduras na Classificação de Dados:

- **As verificações somente de mapeamento** fornecem apenas uma visão geral de alto nível dos seus dados e são realizadas em fontes de dados selecionadas. As varreduras somente de mapeamento levam menos tempo do que as varreduras de mapeamento e classificação porque não acessam os arquivos para ver os dados contidos neles. Talvez você queira fazer isso inicialmente para identificar áreas de pesquisa e depois executar uma varredura de Mapear e Classificar nessas áreas.
- **As varreduras de Mapa e Classificação** fornecem uma varredura profunda dos seus dados.

A tabela abaixo mostra algumas das diferenças:

| Recurso | Mapear e classificar varreduras | Varreduras somente de mapeamento |
|---|---|---|
| Velocidade de digitalização | Lento | Rápido |
| Preços | Livre | Livre |
| Capacidade | Limitado a 500 TiB* | Limitado a 500 TiB* |
| Lista de tipos de arquivo e capacidade utilizada | Sim | Sim |
| Número de arquivos e capacidade utilizada | Sim | Sim |
| Idade e tamanho dos arquivos | Sim | Sim |
| Capacidade de executar um"Relatório de Mapeamento de Dados" | Sim | Sim |
| Página de investigação de dados para visualizar detalhes do arquivo | Sim | Não |
| Pesquisar nomes dentro de arquivos | Sim | Não |
| Criar"consultas salvas" que fornecem resultados de pesquisa personalizados | Sim | Não |
| Capacidade de executar outros relatórios | Sim | Não |
| Capacidade de ver metadados de arquivos** | Não | Sim |

{asterisco} A Classificação de Dados não impõe um limite na quantidade de dados que pode escanear. Cada agente do Console suporta a digitalização e a exibição de 500 TiB de dados. Para escanear mais de 500 TiB de dados,"instalar outro agente do Console" então"implantar outra instância de Classificação de Dados" . + A interface do usuário do console exibe dados de um único conector. Para obter dicas sobre como visualizar dados de vários agentes do Console, consulte"Trabalhar com vários agentes do Console" .

{asterisco}{asterisco} Os seguintes metadados são extraídos dos arquivos durante as varreduras de mapeamento:

- Sistema
- Tipo de sistema
- Repositório de armazenamento
- Tipo de arquivo
- Capacidade utilizada
- Número de arquivos
- Tamanho do arquivo

- Criação de arquivo
- Último acesso ao arquivo
- Última modificação do arquivo
- Hora da descoberta do arquivo
- Extração de permissões

**Diferenças do painel de governança:**

| Recurso | Mapear e classificar | Mapa |
|---|---|---|
| Dados obsoletos | Sim | Sim |
| Dados não comerciais | Sim | Sim |
| Arquivos duplicados | Sim | Sim |
| Consultas salvas predefinidas | Sim | Não |
| Consultas salvas padrão | Sim | Sim |
| Relatório DDA | Sim | Sim |
| Relatório de mapeamento | Sim | Sim |
| Detecção do nível de sensibilidade | Sim | Não |
| Dados sensíveis com permissões amplas | Sim | Não |
| Permissões abertas | Sim | Sim |
| Era dos dados | Sim | Sim |
| Tamanho dos dados | Sim | Sim |
| Categorias | Sim | Não |
| Tipos de arquivo | Sim | Sim |

**Diferenças do painel de conformidade:**

| Recurso | Mapear e classificar | Mapa |
|---|---|---|
| Informações pessoais | Sim | Não |
| Informações pessoais sensíveis | Sim | Não |
| Relatório de avaliação de risco de privacidade | Sim | Não |
| Relatório HIPAA | Sim | Não |
| Relatório PCI DSS | Sim | Não |

**Diferenças nos filtros de investigação:**

| Recurso | Mapear e classificar | Mapa |
|---|---|---|
| Consultas salvas | Sim | Sim |
| Tipo de sistema | Sim | Sim |
| Sistema | Sim | Sim |
| Repositório de armazenamento | Sim | Sim |
| Tipo de arquivo | Sim | Sim |
| Tamanho do arquivo | Sim | Sim |
| Tempo criado | Sim | Sim |
| Tempo descoberto | Sim | Sim |
| Última modificação | Sim | Sim |
| Último acesso | Sim | Sim |
| Permissões abertas | Sim | Sim |
| Caminho do diretório de arquivos | Sim | Sim |
| Categoria | Sim | Não |
| Nível de sensibilidade | Sim | Não |
| Número de identificadores | Sim | Não |
| Dados pessoais | Sim | Não |
| Dados pessoais sensíveis | Sim | Não |
| Titular dos dados | Sim | Não |
| Duplicatas | Sim | Sim |
| Status de classificação | Sim | O status é sempre "Insights limitados" |
| Evento de análise de varredura | Sim | Sim |
| Hash de arquivo | Sim | Sim |
| Número de usuários com acesso | Sim | Sim |
| Permissões de usuário/grupo | Sim | Sim |
| Proprietário do arquivo | Sim | Sim |
| Tipo de diretório | Sim | Sim |

## Escaneie o Amazon FSx em busca de volumes ONTAP com a NetApp Data Classification

Conclua algumas etapas para escanear o Amazon FSx em busca de volumes ONTAP com a NetApp Data Classification.

### Antes de começar

- Você precisa de um agente de console ativo na AWS para implantar e gerenciar a Classificação de Dados.
- O grupo de segurança selecionado ao criar o sistema deve permitir tráfego da instância de Classificação de Dados. Você pode encontrar o grupo de segurança associado usando o ENI conectado ao sistema de arquivos FSx para ONTAP e editá-lo usando o AWS Management Console.

  "Grupos de segurança da AWS para instâncias Linux"

  "Grupos de segurança da AWS para instâncias do Windows"

  "Interfaces de rede elásticas (ENI) da AWS"

- Certifique-se de que as seguintes portas estejam abertas para a instância de Classificação de Dados:
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.

### Implantar a instância de classificação de dados

"Implantar classificação de dados"se ainda não houver uma instância implantada.

Você deve implantar a Classificação de Dados na mesma rede AWS que o agente do Console para AWS e os volumes FSx que deseja verificar.

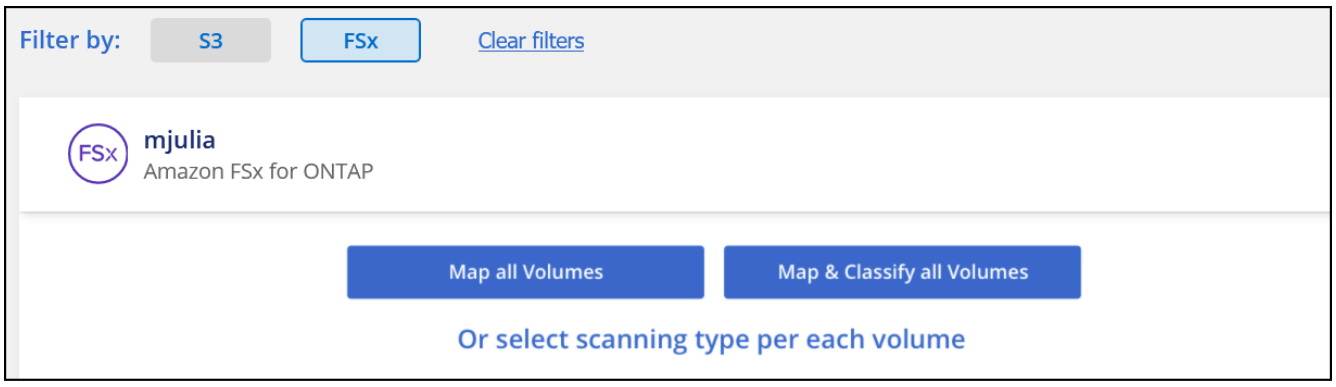
**Observação:** A implantação da Classificação de Dados em um local local não é suportada atualmente ao escanear volumes FSx.

As atualizações do software de classificação de dados são automatizadas, desde que a instância tenha conectividade com a Internet.

### Habilite a classificação de dados em seus sistemas

Você pode habilitar a Classificação de Dados para FSx para volumes ONTAP .

1. No NetApp Console, **Governança > Classificação**.
2. No menu Classificação de Dados, selecione **Configuração**.




3. Selecione como você deseja verificar os volumes em cada sistema. "Aprenda sobre mapeamento e varreduras de classificação":
   - Para mapear todos os volumes, selecione **Mapear todos os volumes**.

- Para mapear e classificar todos os volumes, selecione **Mapear e classificar todos os volumes**.
- Para personalizar a verificação para cada volume, selecione **Ou selecione o tipo de verificação para cada volume** e, em seguida, escolha os volumes que deseja mapear e/ou classificar.

4. Na caixa de diálogo de confirmação, selecione **Aprovar** para que a Classificação de Dados comece a verificar seus volumes.

**Resultado**

A Classificação de Dados inicia a varredura dos volumes selecionados no sistema. Os resultados estarão disponíveis no painel de conformidade assim que a Classificação de Dados concluir as verificações iniciais. O tempo que isso leva depende da quantidade de dados: pode levar alguns minutos ou horas. Você pode acompanhar o progresso da verificação inicial navegando até o menu **Configuração** e selecionando **Configuração do sistema**. Acompanhe o progresso de cada verificação na barra de progresso; você pode passar o mouse sobre a barra de progresso para ver o número de arquivos verificados em relação ao total de arquivos no volume.

- Por padrão, se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos em seus volumes porque a Classificação de Dados não pode reverter o "último horário de acesso" para o registro de data e hora original. Se não se importar se o último horário de acesso for redefinido, selecione **Ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode ativar para que a Classificação de Dados verifique os volumes independentemente das permissões.
- A Classificação de Dados verifica apenas um compartilhamento de arquivo em um volume. Se você tiver vários compartilhamentos em seus volumes, será necessário verificar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Veja mais detalhes sobre esta limitação de Classificação de Dados" .

### Verifique se a Classificação de Dados tem acesso aos volumes

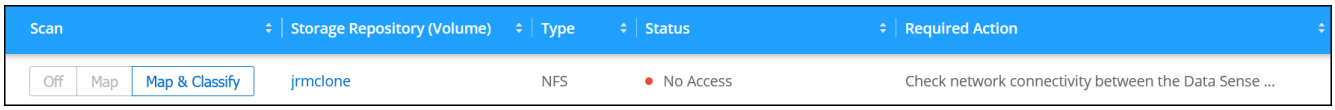
Certifique-se de que a Classificação de Dados possa acessar volumes verificando sua rede, grupos de segurança e políticas de exportação.

Você precisará fornecer à Classificação de Dados credenciais CIFS para que ela possa acessar volumes CIFS.

**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na página Configuração, selecione **Exibir detalhes** para revisar o status e corrigir quaisquer erros.

   Por exemplo, a imagem a seguir mostra um volume que a Classificação de Dados não consegue escanear devido a problemas de conectividade de rede entre a instância da Classificação de Dados e o volume.




3. Certifique-se de que haja uma conexão de rede entre a instância de Classificação de Dados e cada rede que inclui volumes para FSx para ONTAP.

   Para o FSx para ONTAP, a Classificação de Dados pode escanear volumes somente na mesma região que o Console.

4. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Classificação de Dados para que ela possa acessar os dados em cada volume.
5. Se você usar CIFS, forneça a Classificação de Dados com credenciais do Active Directory para que ele possa verificar volumes CIFS.

    a. No menu Classificação de Dados, selecione **Configuração**.

    b. Para cada sistema, selecione **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Data Classification precisa para acessar volumes CIFS no sistema.

    As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a Classificação de Dados possa ler quaisquer dados que exijam permissões elevadas. As credenciais são armazenadas na instância de Classificação de Dados.

    Se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de Classificação de Dados, é recomendável que o usuário tenha permissões de Gravação de Atributos no CIFS ou permissões de gravação no NFS. Se possível, configure o usuário do Active Directory como parte de um grupo pai na organização que tenha permissões para todos os arquivos.

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

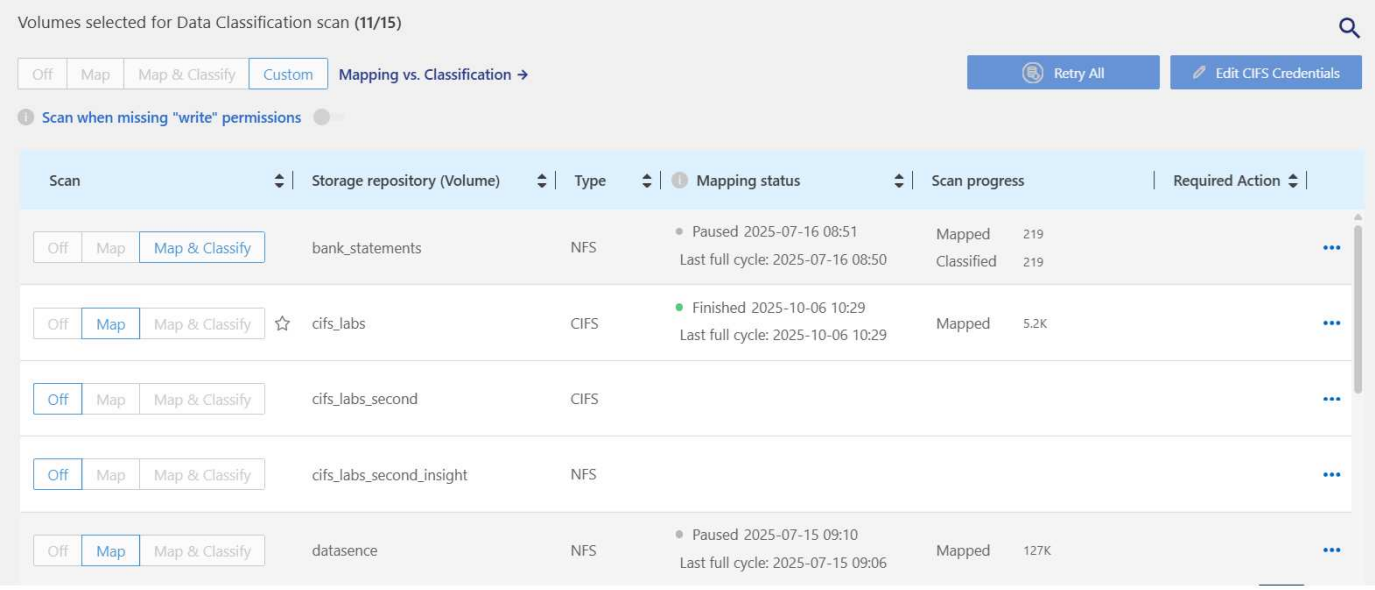
### Habilitar e desabilitar verificações em volumes

Você pode iniciar ou interromper verificações em qualquer sistema a qualquer momento na página Configuração. Você também pode alternar as verificações de somente mapeamento para verificações de mapeamento e classificação, e vice-versa. É recomendável que você escaneie todos os volumes em um sistema.

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você seleciona a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando definido como **Personalizado** ou **Desativado** na área de título, você precisará ativar o mapeamento e/ou a varredura completa em cada novo volume adicionado ao sistema.

O botão no topo da página para **Verificar quando faltarem permissões de "gravação"** está desabilitado por padrão. Isso significa que se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a Classificação de Dados não poderá reverter o "último horário de acesso" para o registro de data e hora original. Se você não se importa se o último horário de acesso for redefinido, ligue o interruptor e todos os arquivos serão verificados, independentemente das permissões. "Saber mais".

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você define a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando a configuração para todos os volumes for **Personalizada** ou **Desativada**, você precisará ativar a verificação manualmente para cada novo volume adicionado.




**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Escolha um sistema e selecione **Configuração**.
3. Para habilitar ou desabilitar verificações para todos os volumes, selecione **Mapear**, **Mapear e classificar** ou **Desativar** no título acima de todos os volumes.

   Para habilitar ou desabilitar verificações para volumes individuais, encontre os volumes na lista e selecione **Mapear**, **Mapear e classificar** ou **Desativar** ao lado do nome do volume.

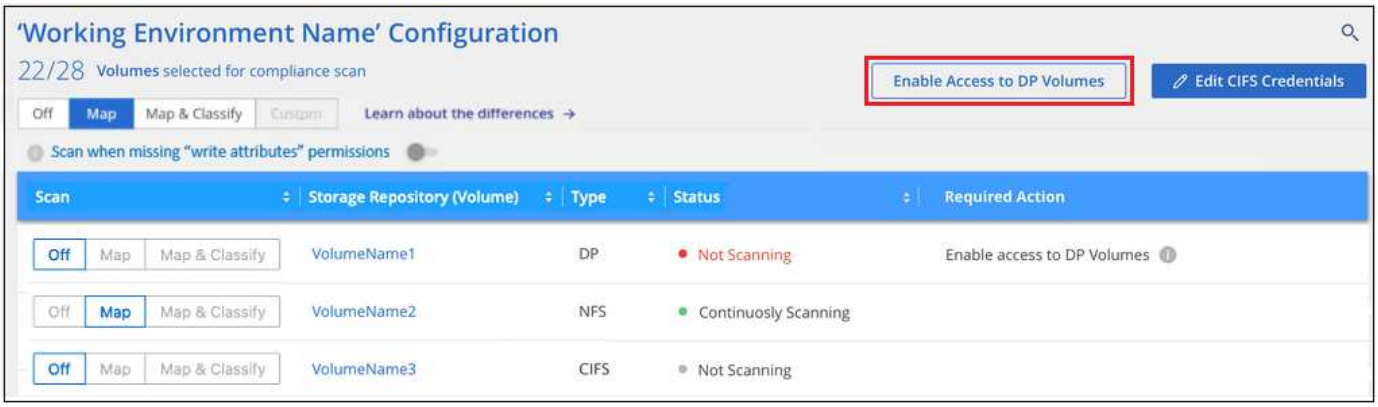
**Resultado**

Quando você ativa a digitalização, a Classificação de Dados inicia a digitalização dos volumes selecionados no sistema. Os resultados começam a aparecer no painel de conformidade assim que a Classificação de Dados inicia a verificação. O tempo de conclusão da verificação depende da quantidade de dados, variando de minutos a horas.

### Digitalizar volumes de proteção de dados

Por padrão, os volumes de proteção de dados (DP) não são verificados porque não são expostos externamente e a Classificação de Dados não pode acessá-los. Esses são os volumes de destino para operações do SnapMirror de um sistema de arquivos FSx para ONTAP .

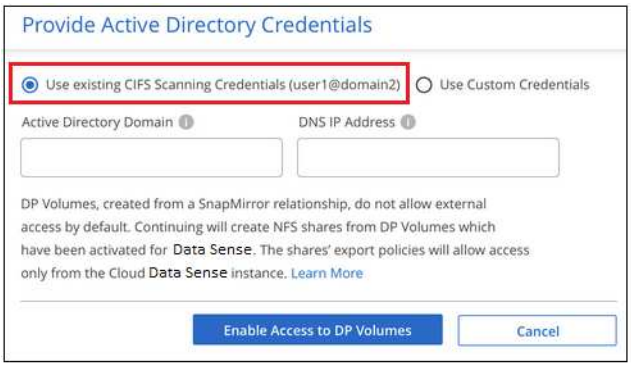
Inicialmente, a lista de volumes identifica esses volumes como *Tipo* **DP** com o *Status* **Não digitalizando** e a *Ação necessária* **Habilitar acesso a volumes DP**.

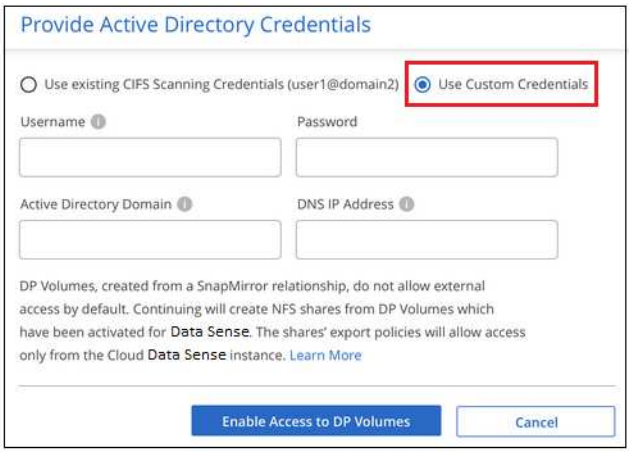



**Passos**

Se você quiser escanear esses volumes de proteção de dados:

1. No menu Classificação de Dados, selecione **Configuração**.
2. Selecione **Habilitar acesso a volumes DP** na parte superior da página.
3. Revise a mensagem de confirmação e selecione **Habilitar acesso aos volumes DP** novamente.
   - Os volumes que foram criados inicialmente como volumes NFS no sistema de arquivos FSx de origem para ONTAP são habilitados.
   - Os volumes que foram criados inicialmente como volumes CIFS no sistema de arquivos FSx de origem para ONTAP exigem que você insira credenciais CIFS para verificar esses volumes DP. Se você já inseriu credenciais do Active Directory para que a Classificação de Dados possa escanear volumes CIFS, você pode usar essas credenciais ou especificar um conjunto diferente de credenciais de administrador.




4. Ative cada volume DP que você deseja escanear.

**Resultado**

Uma vez ativada, a Classificação de Dados cria um compartilhamento NFS de cada volume DP que foi ativado para verificação. As políticas de exportação de compartilhamento só permitem acesso a partir da instância de Classificação de Dados.

Se você não tinha volumes de proteção de dados CIFS quando habilitou inicialmente o acesso aos volumes DP e depois adicionou alguns, o botão **Habilitar acesso ao CIFS DP** aparece na parte superior da página Configuração. Selecione este botão e adicione credenciais CIFS para habilitar o acesso a esses volumes CIFS DP.

As credenciais do Active Directory são registradas somente na VM de armazenamento do primeiro volume CIFS DP, portanto, todos os volumes DP nessa SVM serão verificados. Quaisquer volumes que residam em outras SVMs não terão as credenciais do Active Directory registradas, portanto, esses volumes DP não serão verificados.

## Verificar volumes do Azure NetApp Files com a NetApp Data Classification

Conclua algumas etapas para começar a usar a NetApp Data Classification para Azure NetApp Files.

### Descubra o sistema Azure NetApp Files que você deseja verificar

Se o sistema Azure NetApp Files que você deseja verificar ainda não estiver no NetApp Console como um sistema,"adicione-o na página Sistemas" .

### Implantar a instância de classificação de dados

"Implantar classificação de dados"se ainda não houver uma instância implantada.

A Classificação de Dados deve ser implantada na nuvem ao verificar volumes do Azure NetApp Files e deve ser implantada na mesma região dos volumes que você deseja verificar.

**Observação:** A implantação da Classificação de Dados em um local não é suportada atualmente ao verificar volumes do Azure NetApp Files .

### Habilite a classificação de dados em seus sistemas

Você pode habilitar a Classificação de Dados nos seus volumes do Azure NetApp Files .

1. No menu Classificação de Dados, selecione **Configuração**.


2. Selecione como você deseja verificar os volumes em cada sistema. "Aprenda sobre mapeamento e varreduras de classificação":
   - Para mapear todos os volumes, selecione **Mapear todos os volumes**.
   - Para mapear e classificar todos os volumes, selecione **Mapear e classificar todos os volumes**.
   - Para personalizar a digitalização para cada volume, selecione **Ou selecione o tipo de digitalização para cada volume** e escolha os volumes que deseja mapear ou mapear e classificar.

     VerHabilitar ou desabilitar verificações em volumes para mais detalhes.

3. Na caixa de diálogo de confirmação, selecione **Aprovar**.

**Resultado**

A Classificação de Dados inicia a varredura dos volumes selecionados no sistema. Os resultados estarão disponíveis no painel de conformidade assim que a Classificação de Dados concluir as verificações iniciais. O tempo que isso leva depende da quantidade de dados: pode levar alguns minutos ou horas. Você pode acompanhar o progresso da verificação inicial navegando até o menu **Configuração** e selecionando **Configuração do sistema**. A Classificação de Dados exibe uma barra de progresso para cada verificação. Você pode passar o mouse sobre a barra de progresso para ver o número de arquivos verificados em relação ao número total de arquivos no volume.

- Por padrão, se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos em seus volumes porque a Classificação de Dados não pode reverter o "último horário de acesso" para o registro de data e hora original. Se não se importar se o último horário de acesso for redefinido, selecione **Ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode ativar para que a Classificação de Dados verifique os volumes independentemente das permissões.
- A Classificação de Dados verifica apenas um compartilhamento de arquivo em um volume. Se você tiver vários compartilhamentos em seus volumes, será necessário verificar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Saiba mais sobre esta limitação de classificação de dados" .

### Verifique se a Classificação de Dados tem acesso aos volumes

Certifique-se de que a Classificação de Dados possa acessar volumes verificando sua rede, grupos de segurança e políticas de exportação. Você precisa fornecer à Classificação de Dados credenciais CIFS para que ela possa acessar volumes CIFS.

Para o Azure NetApp Files, a Classificação de Dados só pode verificar volumes na mesma região que o Console.

**Lista de verificação**

- Certifique-se de que haja uma conexão de rede entre a instância de Classificação de Dados e cada rede que inclui volumes para o Azure NetApp Files.
- Certifique-se de que as seguintes portas estejam abertas para a instância de Classificação de Dados:
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.
- Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Classificação de Dados para que ela possa acessar os dados em cada volume.

**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.

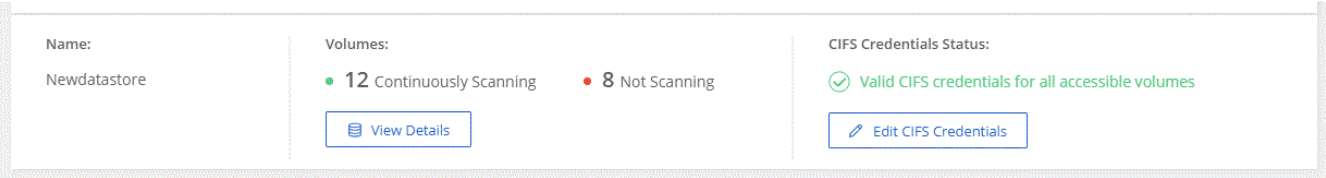
   a. Se você estiver usando CIFS (SMB), verifique se as credenciais do Active Directory estão corretas. Para cada sistema, selecione **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Data Classification precisa para acessar os volumes CIFS no sistema.

      As credenciais podem ser somente leitura; fornecer credenciais de administrador garante que a Classificação de Dados possa ler quaisquer dados que exijam permissões elevadas. As credenciais são armazenadas na instância de Classificação de Dados.

      Se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de Classificação de Dados, é recomendável que o usuário tenha

permissões de Gravação de Atributos no CIFS ou permissões de gravação no NFS. Se possível, configure o usuário do Active Directory como parte de um grupo pai na organização que tenha permissões para todos os arquivos.

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




2. Na página Configuração, selecione **Exibir detalhes** para revisar o status de cada volume CIFS e NFS. Se necessário, corrija quaisquer erros, como problemas de conectividade de rede.

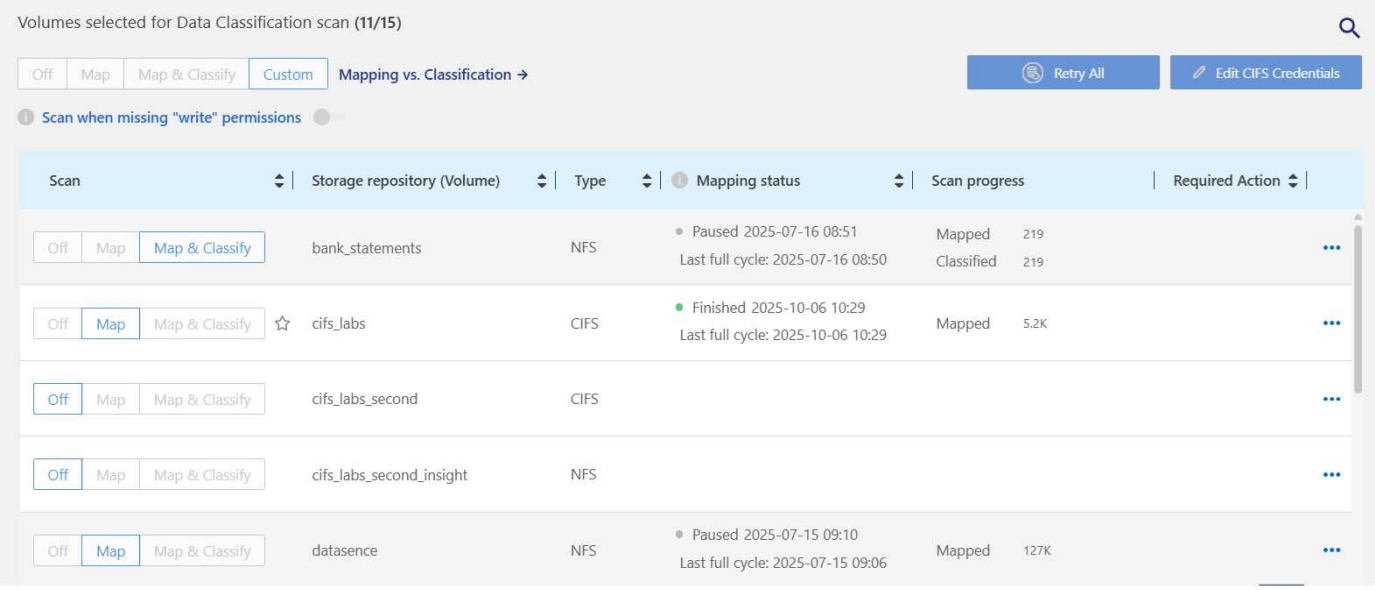
### Habilitar ou desabilitar verificações em volumes

Você pode iniciar ou interromper verificações em qualquer sistema a qualquer momento na página Configuração. Você também pode alternar as verificações de somente mapeamento para verificações de mapeamento e classificação, e vice-versa. É recomendável que você escaneie todos os volumes em um sistema.

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você seleciona a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando definido como **Personalizado** ou **Desativado** na área de título, você precisará ativar o mapeamento e/ou a varredura completa em cada novo volume adicionado ao sistema.

O botão no topo da página para **Verificar quando faltarem permissões de "gravação"** está desabilitado por padrão. Isso significa que se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a Classificação de Dados não poderá reverter o "último horário de acesso" para o registro de data e hora original. Se você não se importa se o último horário de acesso for redefinido, ligue o interruptor e todos os arquivos serão verificados, independentemente das permissões. "Saber mais".

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você define a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando a configuração para todos os volumes for **Personalizada** ou **Desativada**, você precisará ativar a verificação manualmente para cada novo volume adicionado.




**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Escolha um sistema e selecione **Configuração**.
3. Para habilitar ou desabilitar verificações para todos os volumes, selecione **Mapear**, **Mapear e classificar** ou **Desativar** no título acima de todos os volumes.

   Para habilitar ou desabilitar verificações para volumes individuais, encontre os volumes na lista e selecione **Mapear**, **Mapear e classificar** ou **Desativar** ao lado do nome do volume.

**Resultado**

Quando você ativa a digitalização, a Classificação de Dados inicia a digitalização dos volumes selecionados no sistema. Os resultados começam a aparecer no painel de conformidade assim que a Classificação de Dados inicia a verificação. O tempo de conclusão da verificação depende da quantidade de dados, variando de minutos a horas.

## Escaneie Cloud Volumes ONTAP e volumes ONTAP locais com a NetApp Data Classification

Conclua algumas etapas para começar a escanear seus volumes Cloud Volumes ONTAP e ONTAP locais usando o NetApp Data Classification.

**Pré-requisitos**

Antes de habilitar a Classificação de Dados, certifique-se de ter uma configuração compatível.

- Se você estiver escaneando o Cloud Volumes ONTAP e os sistemas ONTAP locais que podem ser acessados pela Internet, você pode"implementar a Classificação de Dados na nuvem" ou"em um local com acesso à Internet" .
- Se você estiver escaneando sistemas ONTAP locais que foram instalados em um site escuro sem acesso à Internet, você precisa"implementar a Classificação de Dados no mesmo local que não tem acesso à Internet" . Isso requer que o agente do Console seja implantado no mesmo local.

### Verifique se a Classificação de Dados tem acesso aos volumes

Certifique-se de que a Classificação de Dados possa acessar volumes verificando sua rede, grupos de segurança e políticas de exportação. Você precisará fornecer à Classificação de Dados credenciais CIFS para que ela possa acessar volumes CIFS.

#### Lista de verificação

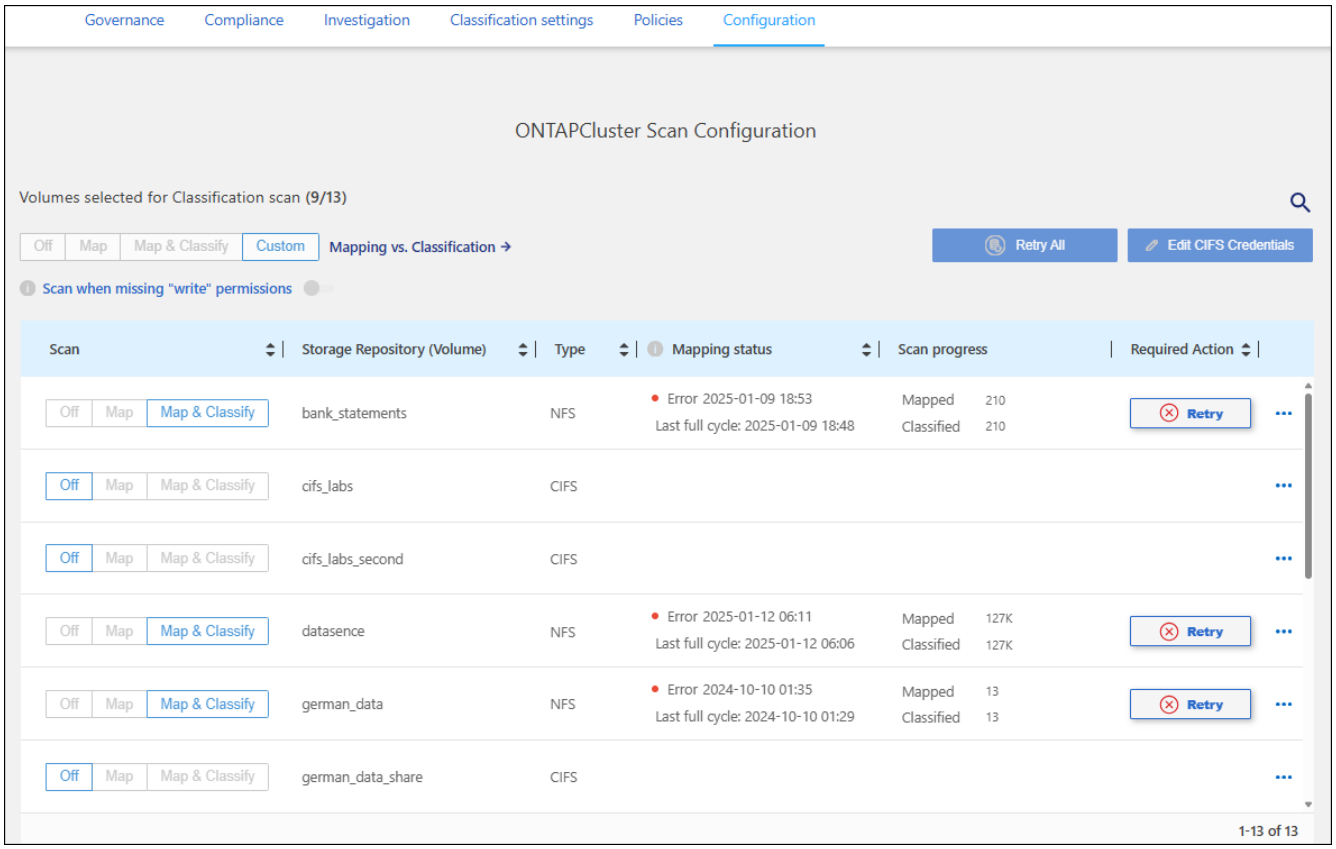
- Certifique-se de que haja uma conexão de rede entre a instância de Classificação de Dados e cada rede que inclua volumes para clusters Cloud Volumes ONTAP ou ONTAP locais.
- Certifique-se de que o grupo de segurança do Cloud Volumes ONTAP permita tráfego de entrada da instância de Classificação de Dados.

  Você pode abrir o grupo de segurança para o tráfego do endereço IP da instância de Classificação de Dados ou pode abrir o grupo de segurança para todo o tráfego de dentro da rede virtual.

- Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Classificação de Dados para que ela possa acessar os dados em cada volume.

#### Passos

1. No menu Classificação de Dados, selecione **Configuração**.




2. Se você usar CIFS, forneça a Classificação de Dados com credenciais do Active Directory para que ele possa verificar volumes CIFS. Para cada sistema, selecione **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Data Classification precisa para acessar volumes CIFS no sistema.

   As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a Classificação de Dados possa ler quaisquer dados que exijam permissões elevadas. As credenciais são armazenadas na instância de Classificação de Dados.

Se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de Classificação de Dados, é recomendável que o usuário tenha permissões de Gravação de Atributos no CIFS ou permissões de gravação no NFS. Se possível, configure o usuário do Active Directory como parte de um grupo pai na organização que tenha permissões para todos os arquivos.

Se você inseriu as credenciais corretamente, uma mensagem confirmará que todos os volumes CIFS foram autenticados com sucesso.

3. Na página Configuração, selecione **Configuração** para revisar o status de cada volume CIFS e NFS e corrigir quaisquer erros.

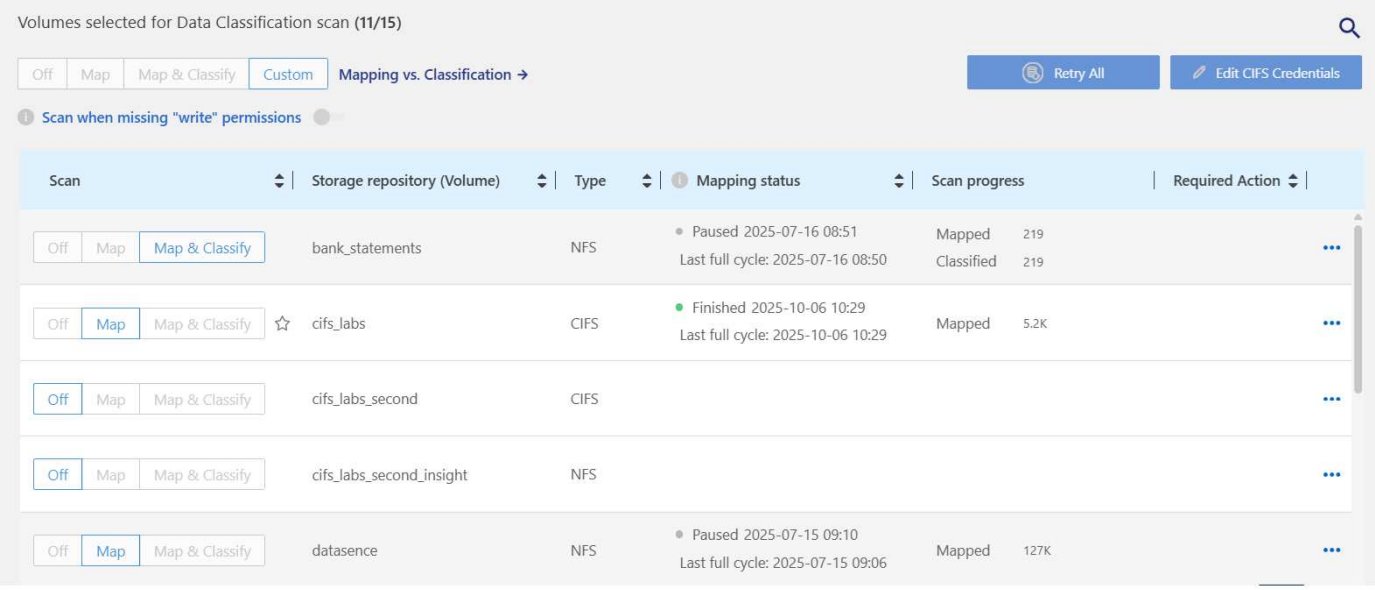
### Habilitar ou desabilitar verificações em volumes

Você pode iniciar ou interromper verificações em qualquer sistema a qualquer momento na página Configuração. Você também pode alternar as verificações de somente mapeamento para verificações de mapeamento e classificação, e vice-versa. É recomendável que você escaneie todos os volumes em um sistema.

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você seleciona a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando definido como **Personalizado** ou **Desativado** na área de título, você precisará ativar o mapeamento e/ou a varredura completa em cada novo volume adicionado ao sistema.

O botão no topo da página para **Verificar quando faltarem permissões de "gravação"** está desabilitado por padrão. Isso significa que se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a Classificação de Dados não poderá reverter o "último horário de acesso" para o registro de data e hora original. Se você não se importa se o último horário de acesso for redefinido, ligue o interruptor e todos os arquivos serão verificados, independentemente das permissões. "Saber mais".

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você define a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando a configuração para todos os volumes for **Personalizada** ou **Desativada**, você precisará ativar a verificação manualmente para cada novo volume adicionado.



**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Escolha um sistema e selecione **Configuração**.
3. Para habilitar ou desabilitar verificações para todos os volumes, selecione **Mapear**, **Mapear e classificar** ou **Desativar** no título acima de todos os volumes.

   Para habilitar ou desabilitar verificações para volumes individuais, encontre os volumes na lista e selecione **Mapear**, **Mapear e classificar** ou **Desativar** ao lado do nome do volume.

**Resultado**

Quando você ativa a digitalização, a Classificação de Dados inicia a digitalização dos volumes selecionados no sistema. Os resultados começam a aparecer no painel de conformidade assim que a Classificação de Dados inicia a verificação. O tempo de conclusão da verificação depende da quantidade de dados, variando de minutos a horas.

A Classificação de Dados verifica apenas um compartilhamento de arquivo em um volume. Se você tiver vários compartilhamentos em seus volumes, será necessário verificar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Veja mais detalhes sobre esta limitação de Classificação de Dados" .

## Escaneie esquemas de banco de dados com a NetApp Data Classification

Conclua algumas etapas para começar a escanear seus esquemas de banco de dados com o NetApp Data Classification.

### Revise os pré-requisitos

Revise os seguintes pré-requisitos para garantir que você tenha uma configuração compatível antes de habilitar a Classificação de Dados.

#### Bancos de dados suportados

A Classificação de Dados pode escanear esquemas dos seguintes bancos de dados:

- Serviço de banco de dados relacional da Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oráculo
- PostgreSQL
- SAP HANA
- Servidor SQL (MSSQL)

O recurso de coleta de estatísticas **deve ser habilitado** no banco de dados.

#### Requisitos do banco de dados

Qualquer banco de dados com conectividade com a instância de Classificação de Dados 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 uma senha, é importante escolher um que tenha permissões totais de leitura para todos os esquemas e tabelas que você deseja verificar. Recomendamos que você crie um usuário dedicado para o sistema de Classificação de Dados com todas as permissões necessárias.

Para o MongoDB, é necessária uma função de administrador somente leitura.

**Implantar a instância de classificação de dados**

Implante a Classificação de Dados se ainda não houver uma instância implantada.

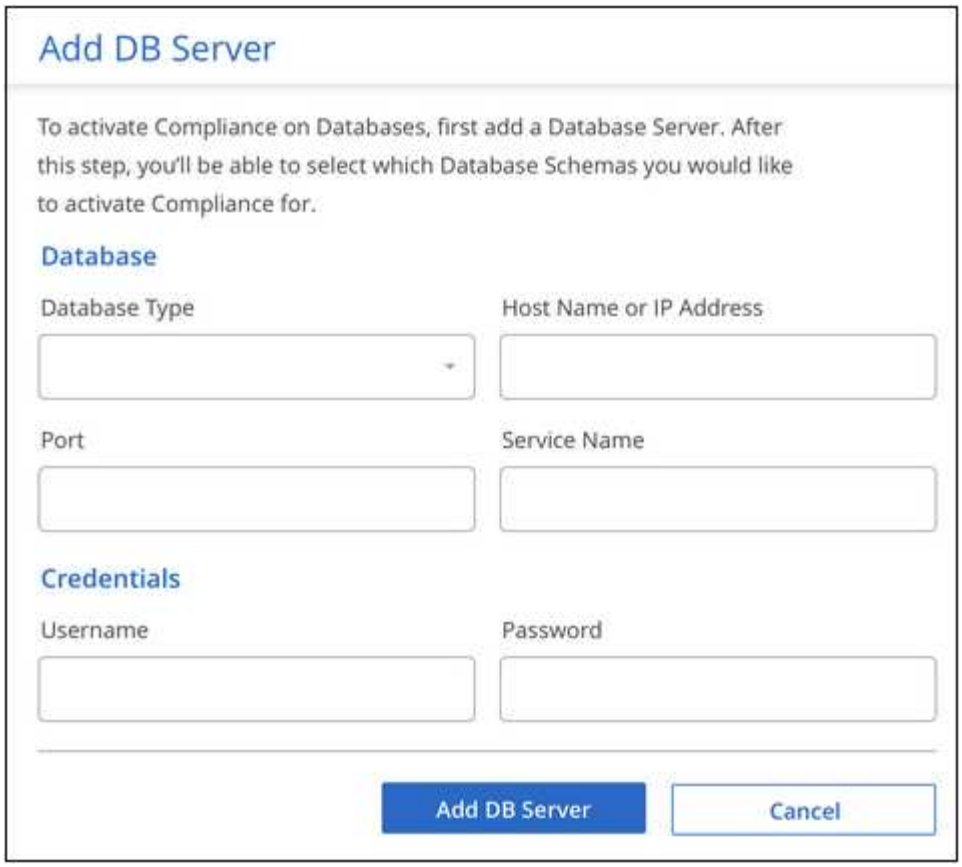
Se você estiver escaneando esquemas de banco de dados que podem ser acessados pela Internet, você pode"implementar a Classificação de Dados na nuvem" ou"implementar a Classificação de Dados em um local local com acesso à Internet" .

Se você estiver escaneando esquemas de banco de dados que foram instalados em um site escuro que não tem acesso à Internet, você precisa"implementar a Classificação de Dados no mesmo local que não tem acesso à Internet" . Isso também requer que o agente do Console seja implantado no mesmo local.

**Adicionar o servidor de banco de dados**

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

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na página Configuração, selecione **Adicionar Sistema** > **Adicionar Servidor de Banco de Dados**.
3. Insira as informações necessárias para identificar o servidor de banco de dados.
   a. Selecione o tipo de banco de dados.
   b. Digite a porta e o nome do host ou endereço IP para conectar ao banco de dados.
   c. Para bancos de dados Oracle, insira o nome do serviço.
   d. Insira as credenciais para que o Data Classification possa acessar o servidor.
   e. Selecione **Adicionar servidor de banco de dados**.




O banco de dados é adicionado à lista de sistemas.

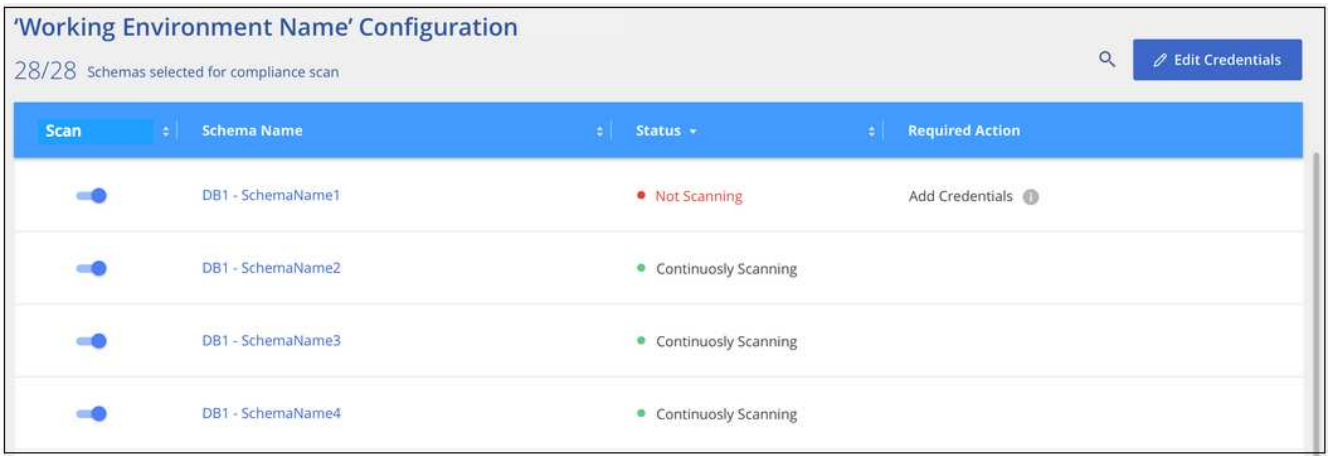
**Habilitar e desabilitar varreduras em esquemas de banco de dados**

Você pode parar ou iniciar a varredura completa dos seus esquemas a qualquer momento.

Não há opção para selecionar varreduras somente de mapeamento para esquemas de banco de dados.

1. Na página Configuração, selecione o botão **Configuração** para o banco de dados que você deseja configurar.


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




**Resultado**

A Classificação de Dados inicia a varredura dos esquemas de banco de dados que você habilitou. Você pode acompanhar o progresso da verificação inicial navegando até o menu **Configuração** e selecionando **Configuração do sistema**. O progresso de cada verificação é mostrado como uma barra de progresso. Você também pode passar o mouse sobre a barra de progresso para ver o número de arquivos verificados em relação ao número total de arquivos no volume. Se houver algum erro, ele aparecerá na coluna Status, junto com as ações necessárias para corrigi-lo.

A Classificação de Dados verifica seus bancos de dados uma vez por dia; os bancos de dados não são verificados continuamente como outras fontes de dados.

## Escaneie Google Cloud NetApp Volumes com a NetApp Data Classification

A NetApp Data Classification oferece suporte ao Google Cloud NetApp Volumes como um sistema. Saiba como escanear seu sistema Google Cloud NetApp Volumes .

### Descubra o sistema Google Cloud NetApp Volumes que você deseja escanear

Se o sistema Google Cloud NetApp Volumes que você deseja verificar ainda não estiver no NetApp Console como um sistema,"adicione-o à página Sistemas" .

### Implantar a instância de classificação de dados

"Implantar classificação de dados"se ainda não houver uma instância implantada.

A Classificação de Dados deve ser implantada na nuvem ao verificar os Google Cloud NetApp Volumes e deve ser implantada na mesma região dos volumes que você deseja verificar.

**Observação:** a implantação da Classificação de Dados em um local não é compatível no momento ao verificar o Google Cloud NetApp Volumes.

### Habilite a classificação de dados em seus sistemas

Você pode habilitar a Classificação de Dados no seu sistema Google Cloud NetApp Volumes .

1. No menu Classificação de Dados, selecione **Configuração**.
2. Selecione como você deseja verificar os volumes em cada sistema. "Aprenda sobre mapeamento e varreduras de classificação":

- Para mapear todos os volumes, selecione **Mapear todos os volumes**.
- Para mapear e classificar todos os volumes, selecione **Mapear e classificar todos os volumes**.
- Para personalizar a verificação para cada volume, selecione **Ou selecione o tipo de verificação para cada volume** e, em seguida, escolha os volumes que deseja mapear e/ou classificar.

  VerHabilitar e desabilitar verificações em volumes para mais detalhes.

3. Na caixa de diálogo de confirmação, selecione **Aprovar**.

**Resultado**

A Classificação de Dados inicia a varredura dos volumes selecionados no sistema. Os resultados estarão disponíveis no painel de conformidade assim que a Classificação de Dados concluir as verificações iniciais. O tempo que isso leva depende da quantidade de dados: de alguns minutos a algumas horas. Você pode acompanhar o progresso da verificação inicial na seção **Configuração do sistema** do menu **Configuração**. A Classificação de Dados exibe uma barra de progresso para cada verificação. Você também pode passar o mouse sobre a barra de progresso para ver o número de arquivos verificados em relação ao total de arquivos no volume.

- Por padrão, se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos em seus volumes porque a Classificação de Dados não pode reverter o "último horário de acesso" para o registro de data e hora original. Se não se importar se o último horário de acesso for redefinido, selecione **Ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode ativar para que a Classificação de Dados verifique os volumes independentemente das permissões.
- A Classificação de Dados verifica apenas um compartilhamento de arquivo em um volume. Se você tiver vários compartilhamentos em seus volumes, precisará verificar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Saiba mais sobre esta limitação de classificação de dados".

### Verifique se a Classificação de Dados tem acesso aos volumes

Garanta que a Classificação de Dados possa acessar volumes verificando sua rede, grupos de segurança e políticas de exportação. Para volumes CIFS, você precisa fornecer Classificação de Dados com credenciais CIFS.

Para o Google Cloud NetApp Volumes, a Classificação de Dados só pode verificar volumes na mesma região que o Console.

**Lista de verificação**

- Certifique-se de que haja uma conexão de rede entre a instância de Classificação de Dados e cada rede que inclui volumes para o Google Cloud NetApp Volumes.
- Certifique-se de que as seguintes portas estejam abertas para a instância de Classificação de Dados:
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.
- Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Classificação de Dados para que ela possa acessar os dados em cada volume.

**Passos**

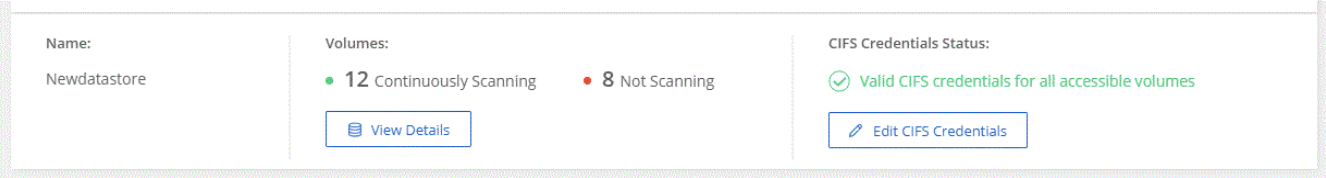
1. No menu Classificação de Dados, selecione **Configuração**.

a. Se você estiver usando CIFS (SMB), verifique se as credenciais do Active Directory estão corretas. Para cada sistema, selecione **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Data Classification precisa para acessar os volumes CIFS no sistema.

   As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a Classificação de Dados possa ler quaisquer dados que exijam permissões elevadas. As credenciais são armazenadas na instância de Classificação de Dados.

   Se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de Classificação de Dados, é recomendável que o usuário tenha permissões de Gravação de Atributos no CIFS ou permissões de gravação no NFS. Se possível, configure o usuário do Active Directory como parte de um grupo pai na organização que tenha permissões para todos os arquivos.

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




2. Na página Configuração, selecione **Exibir detalhes** para revisar o status de cada volume CIFS e NFS e corrigir quaisquer erros.

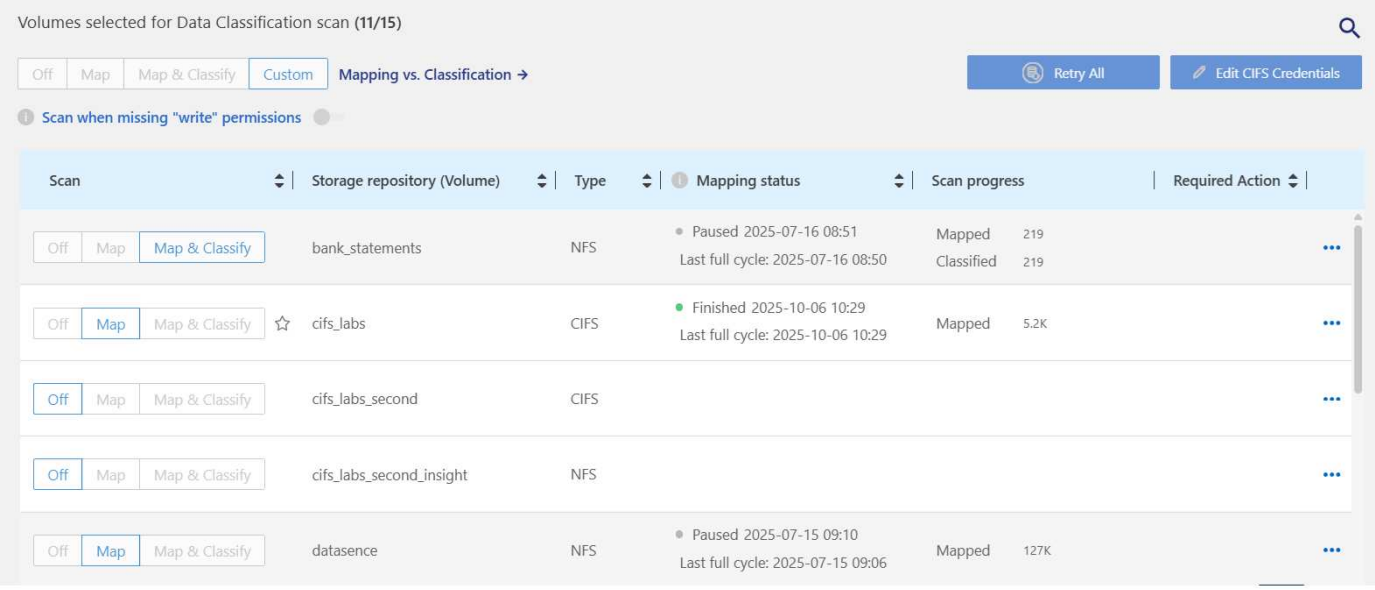
### Habilitar e desabilitar verificações em volumes

Você pode iniciar ou interromper verificações em qualquer sistema a qualquer momento na página Configuração. Você também pode alternar as verificações de somente mapeamento para verificações de mapeamento e classificação, e vice-versa. É recomendável que você escaneie todos os volumes em um sistema.

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você seleciona a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando definido como **Personalizado** ou **Desativado** na área de título, você precisará ativar o mapeamento e/ou a varredura completa em cada novo volume adicionado ao sistema.

O botão no topo da página para **Verificar quando faltarem permissões de "gravação"** está desabilitado por padrão. Isso significa que se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a Classificação de Dados não poderá reverter o "último horário de acesso" para o registro de data e hora original. Se você não se importa se o último horário de acesso for redefinido, ligue o interruptor e todos os arquivos serão verificados, independentemente das permissões. "Saber mais".

Novos volumes adicionados ao sistema são escaneados automaticamente somente quando você define a configuração **Mapa** ou **Mapa e Classificação** na área de título. Quando a configuração para todos os volumes for **Personalizada** ou **Desativada**, você precisará ativar a verificação manualmente para cada novo volume adicionado.




**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Escolha um sistema e selecione **Configuração**.
3. Para habilitar ou desabilitar verificações para todos os volumes, selecione **Mapear**, **Mapear e classificar** ou **Desativar** no título acima de todos os volumes.

   Para habilitar ou desabilitar verificações para volumes individuais, encontre os volumes na lista e selecione **Mapear**, **Mapear e classificar** ou **Desativar** ao lado do nome do volume.

**Resultado**

Quando você ativa a digitalização, a Classificação de Dados inicia a digitalização dos volumes selecionados no sistema. Os resultados começam a aparecer no painel de conformidade assim que a Classificação de Dados inicia a verificação. O tempo de conclusão da verificação depende da quantidade de dados, variando de minutos a horas.

## Verificar compartilhamentos de arquivos com a NetApp Data Classification

Para verificar compartilhamentos de arquivos, você deve primeiro criar um grupo de compartilhamentos de arquivos no NetApp Data Classification. Os grupos de compartilhamentos de arquivos são para compartilhamentos NFS ou CIFS (SMB) hospedados no local ou na nuvem.

A verificação de dados de compartilhamentos de arquivos que não sejam da NetApp não é suportada na versão principal do Data Classification.

**Pré-requisitos**

Revise os seguintes pré-requisitos para garantir que você tenha uma configuração compatível antes de habilitar a Classificação de Dados.

- Os compartilhamentos podem ser hospedados em qualquer lugar, inclusive na nuvem ou no local. Compartilhamentos CIFS de sistemas de armazenamento NetApp 7-Mode mais antigos podem ser verificados como compartilhamentos de arquivos.

    - A Classificação de Dados não pode extrair permissões ou o "último horário de acesso" dos sistemas do Modo 7.
    - Devido a um problema conhecido entre algumas versões do Linux e compartilhamentos CIFS em sistemas 7-Mode, você deve configurar o compartilhamento para usar somente SMBv1 com autenticação NTLM habilitada.
- É necessário haver conectividade de rede entre a instância de Classificação de Dados e os compartilhamentos.
- Você pode adicionar um compartilhamento DFS (Distributed File System) como um compartilhamento CIFS regular. Como a Classificação de Dados não sabe que o compartilhamento é criado em vários servidores/volumes combinados como um único compartilhamento CIFS, você pode receber erros de permissão ou conectividade sobre o compartilhamento quando a mensagem realmente se aplica apenas a uma das pastas/compartilhamentos que está localizada em um servidor/volume diferente.
- Para compartilhamentos CIFS (SMB), certifique-se de ter credenciais do Active Directory que forneçam acesso de leitura aos compartilhamentos. Credenciais de administrador são preferenciais caso a Classificação de Dados precise verificar quaisquer dados que exijam permissões elevadas.

  Se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de Classificação de Dados, é recomendável que o usuário tenha permissões de Gravação de Atributos no CIFS ou permissões de gravação no NFS. Se possível, configure o usuário do Active Directory como parte de um grupo pai na organização que tenha permissões para todos os arquivos.

- Todos os compartilhamentos de arquivos CIFS em um grupo devem usar as mesmas credenciais do Active Directory.
- Você pode misturar compartilhamentos NFS e CIFS (usando Kerberos ou NTLM). Você deve adicionar as ações ao grupo separadamente. Ou seja, você deve concluir o processo duas vezes — uma vez por protocolo.
    - Não é possível criar um grupo de compartilhamentos de arquivos que misture tipos de autenticação CIFS (Kerberos e NTLM).
- Se você estiver usando CIFS com autenticação Kerberos, certifique-se de que o endereço IP fornecido seja acessível à Classificação de Dados. Os compartilhamentos de arquivos não podem ser adicionados se o endereço IP estiver inacessível.

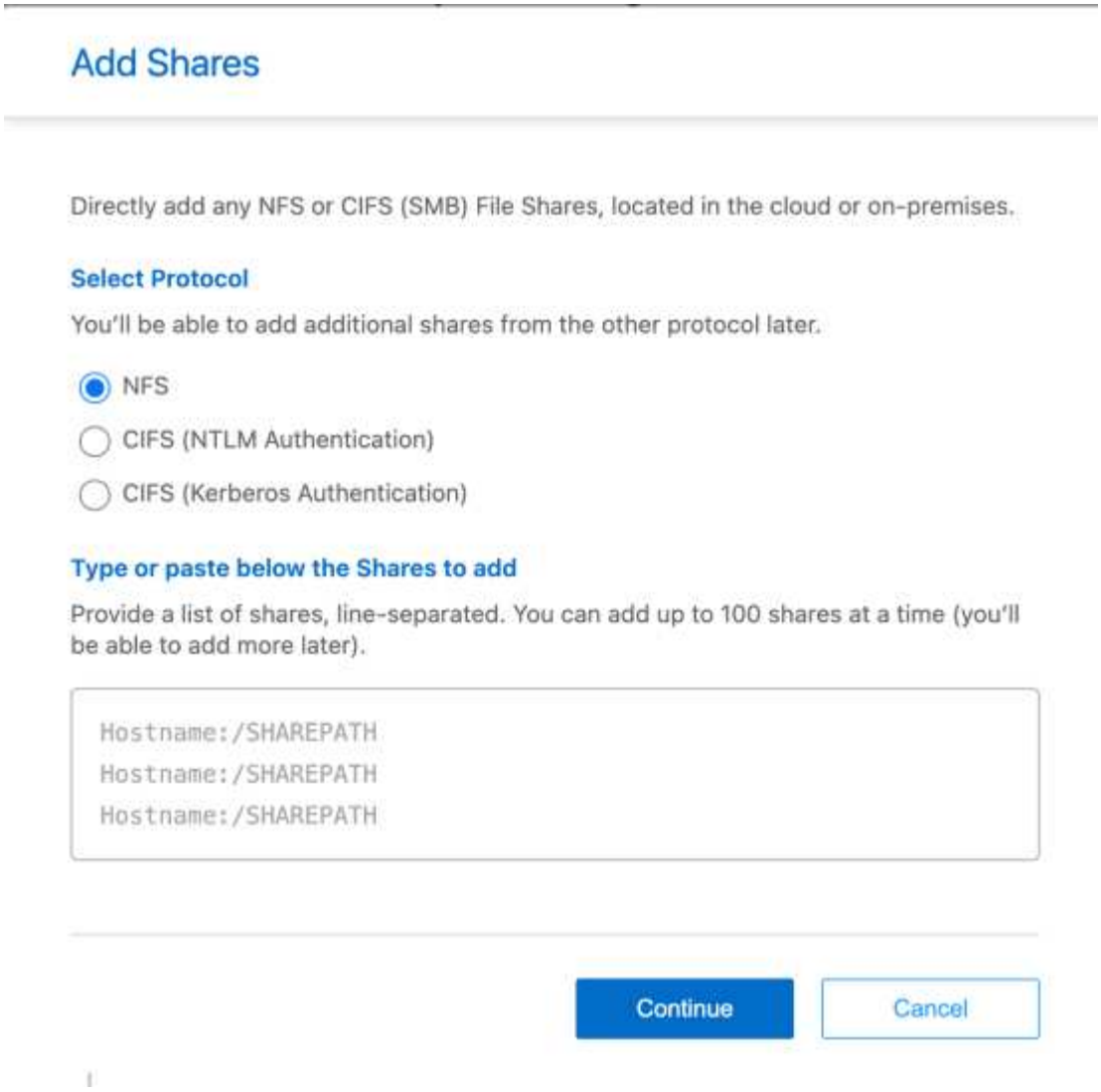
**Criar um grupo de compartilhamentos de arquivos**

Ao adicionar compartilhamentos de arquivos ao grupo, você deve usar o formato `<host_name>:/<share_path>`.

Você pode adicionar compartilhamentos de arquivos individualmente ou inserir uma lista separada por linhas dos compartilhamentos de arquivos que deseja verificar. Você pode adicionar até 100 ações por vez.

**Passos**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na página Configuração, selecione **Adicionar Sistema** > **Adicionar Grupo de Compartilhamentos de Arquivos**.
3. Na caixa de diálogo Adicionar grupo de compartilhamentos de arquivos, insira o nome do grupo de compartilhamentos e selecione **Continuar**.
4. Selecione o protocolo para os compartilhamentos de arquivos que você está adicionando.




a. Se você estiver adicionando compartilhamentos CIFS com autenticação NTLM, insira as credenciais do Active Directory para acessar os volumes CIFS. Embora credenciais somente leitura sejam suportadas, é recomendável que você forneça acesso total com credenciais de administrador. Selecione **Salvar**.

5. Adicione os compartilhamentos de arquivos que você deseja verificar (um compartilhamento de arquivo por linha). Em seguida, selecione **Continuar**.
6. Uma caixa de diálogo de confirmação exibe o número de compartilhamentos que foram adicionados.

   Se a caixa de diálogo listar quaisquer compartilhamentos que não puderam ser adicionados, capture essas informações para que você possa resolver o problema. Se o problema estiver relacionado a uma convenção de nomenclatura, você poderá adicionar novamente o compartilhamento com um nome corrigido.

7. Configurar a varredura no volume:
   - Para habilitar verificações somente de mapeamento em compartilhamentos de arquivos, selecione **Mapear**.
   - Para habilitar verificações completas em compartilhamentos de arquivos, selecione **Mapear e classificar**.
   - Para desabilitar a verificação em compartilhamentos de arquivos, selecione **Desativado**.

O botão no topo da página para **Verificar quando faltarem permissões de "gravação de atributos"** está desabilitado por padrão. Isso significa que se a Classificação de Dados não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a Classificação de Dados não poderá reverter o "último horário de acesso" para o registro de data e hora original. + Se você alternar **Verificar quando faltarem permissões de "gravação de atributos"** para **Ativado**, a verificação redefinirá o último horário de acesso e verificará todos os arquivos, independentemente das permissões. + Para saber mais sobre o último registro de data e hora acessado, consulte"Metadados coletados de fontes de dados na Classificação de Dados" .

**Resultado**

A Classificação de Dados inicia a verificação dos arquivos nos compartilhamentos de arquivos que você adicionou. Você podeAcompanhe o progresso da digitalização e visualize os resultados da verificação no **Painel**.

Se a verificação não for concluída com sucesso para uma configuração CIFS com autenticação Kerberos, verifique se há erros na guia **Configuração**.

### Editar um grupo de compartilhamentos de arquivos

Depois de criar um grupo de compartilhamentos de arquivos, você pode editar o protocolo CIFS ou adicionar e remover compartilhamentos de arquivos.

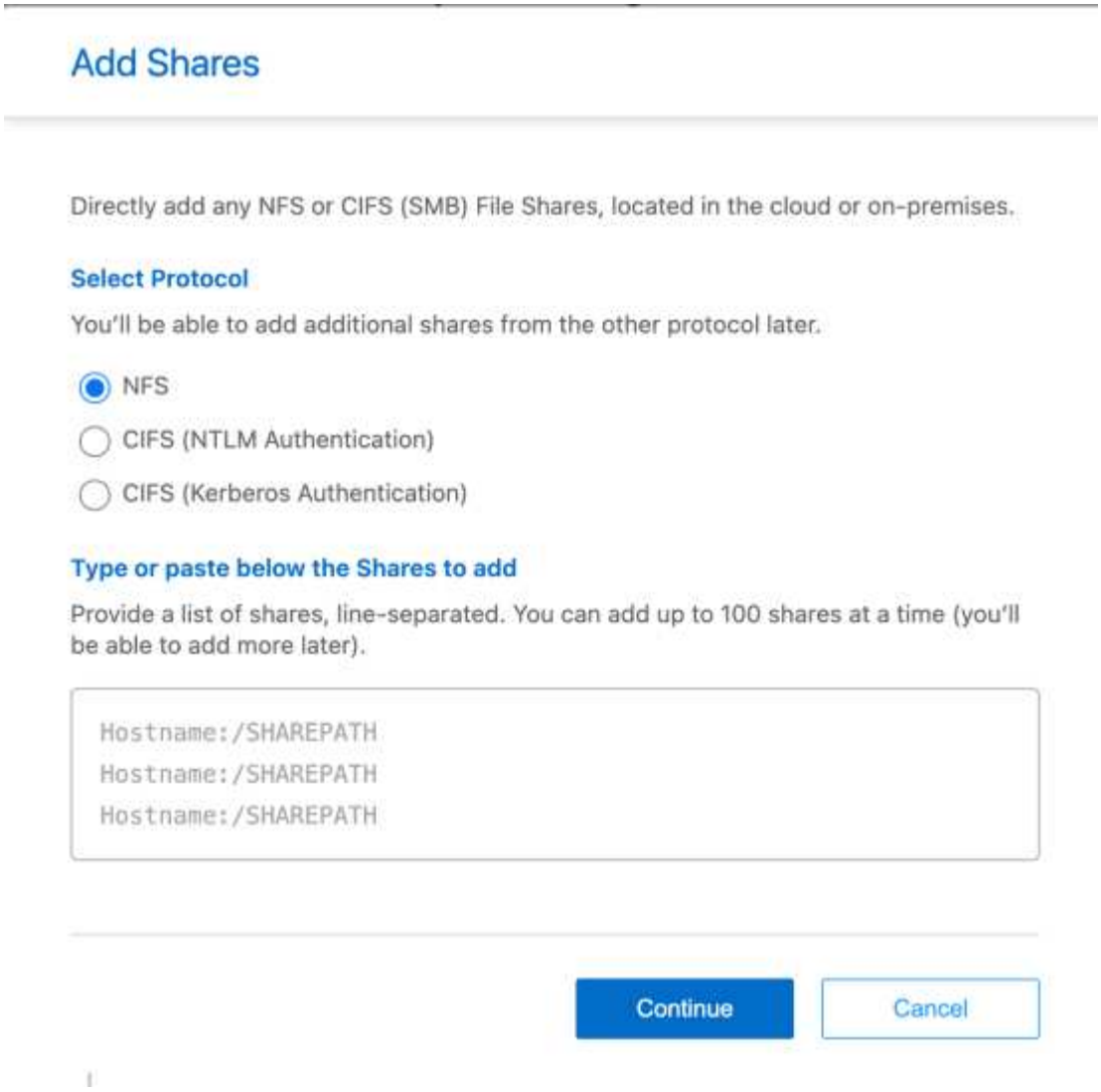
#### Editar a configuração do protocolo CIFS

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na página Configuração, selecione o grupo de compartilhamentos de arquivos que você deseja modificar.
3. Selecione **Editar credenciais CIFS**.


4. Escolha o método de autenticação: **NTLM** ou **Kerberos**.
5. Digite o **Nome de usuário** e a **Senha** do Active Directory.
6. Selecione **Salvar** para concluir o processo.

**Adicionar compartilhamentos de arquivos às verificações**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na página Configuração, selecione o grupo de compartilhamentos de arquivos que você deseja modificar.
3. Selecione **+ Adicionar compartilhamentos**.
4. Selecione o protocolo para os compartilhamentos de arquivos que você está adicionando.




Se você estiver adicionando compartilhamentos de arquivos a um protocolo já configurado, nenhuma alteração será necessária.

Se você estiver adicionando compartilhamentos de arquivos com um segundo protocolo, certifique-se de ter configurado corretamente a autenticação conforme detalhado no"pré-requisitos" .

5. Adicione os compartilhamentos de arquivos que você deseja escanear (um compartilhamento de arquivo por linha) usando o formato `<host_name>:/<share_path>` .
6. Selecione **Continuar** para concluir a adição dos compartilhamentos de arquivos.

**Remover um compartilhamento de arquivo das verificações**

1. No menu Classificação de Dados, selecione **Configuração**.
2. Selecione o sistema do qual você deseja remover os compartilhamentos de arquivos.
3. Selecione **Configuração**.
4. Na página Configuração, selecione as Ações ••• para o compartilhamento de arquivo que você deseja remover.
5. No menu Ações, selecione **Remover compartilhamento**.

### Acompanhe o progresso da digitalização

Você pode acompanhar o progresso da verificação inicial.

1. Selecione o menu **Configuração**.
2. Selecione a **Configuração do sistema**.
3. Para o repositório de armazenamento, verifique a coluna Progresso da verificação para visualizar seu status.

## Escaneie dados do StorageGRID com a NetApp Data Classification

Conclua algumas etapas para começar a escanear dados no StorageGRID diretamente com o NetApp Data Classification.

### Revisar os requisitos do StorageGRID

Revise os seguintes pré-requisitos para garantir que você tenha uma configuração compatível antes de habilitar a Classificação de Dados.

- Você precisa ter o URL do endpoint para se conectar ao serviço de armazenamento de objetos.
- Você precisa ter a chave de acesso e a chave secreta do StorageGRID para que o Data Classification possa acessar os buckets.

### Implantar a instância de classificação de dados

Implante a Classificação de Dados se ainda não houver uma instância implantada.

Se você estiver digitalizando dados do StorageGRID que podem ser acessados pela Internet, você pode"implementar a Classificação de Dados na nuvem" ou"implementar a Classificação de Dados em um local local com acesso à Internet" .

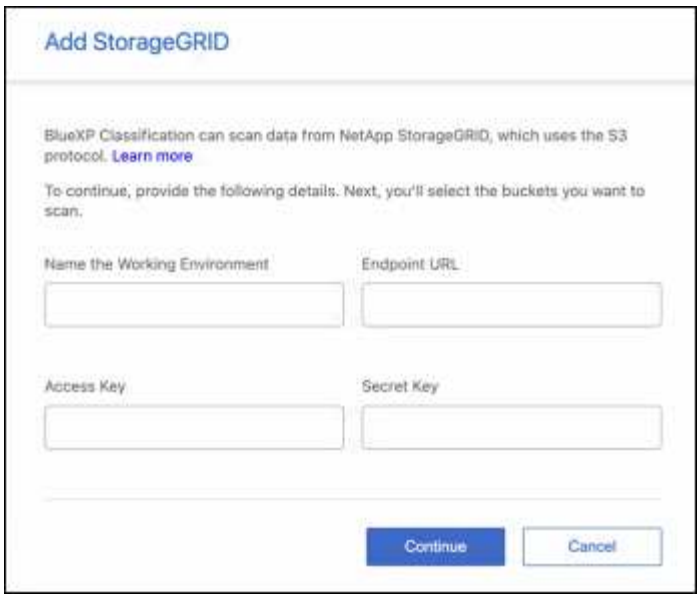
Se você estiver digitalizando dados do StorageGRID que foi instalado em um site escuro sem acesso à Internet, será necessário"implementar a Classificação de Dados no mesmo local que não tem acesso à Internet" . Isso também requer que o agente do Console seja implantado no mesmo local.

### Adicione o serviço StorageGRID à Classificação de Dados

Adicione o serviço StorageGRID .

**Passos**

1. No menu Classificação de Dados, selecione a opção **Configuração**.
2. Na página Configuração, selecione **Adicionar Sistema** > **Adicionar StorageGRID**.
3. Na caixa de diálogo Adicionar serviço StorageGRID , insira os detalhes do serviço StorageGRID e selecione **Continuar**.
   a. Digite o nome que você deseja usar para o Sistema. Este nome deve refletir o nome do serviço StorageGRID ao qual você está se conectando.
   b. Insira a URL do Endpoint para acessar o serviço de armazenamento de objetos.
   c. Insira a chave de acesso e a chave secreta para que a Classificação de Dados possa acessar os buckets no StorageGRID.




**Resultado**

StorageGRID é adicionado à lista de sistemas.

### Habilitar e desabilitar varreduras em buckets do StorageGRID

Depois de habilitar a Classificação de Dados no StorageGRID, a próxima etapa é configurar os buckets que você deseja verificar. A Classificação de Dados descobre esses buckets e os exibe no sistema que você criou.

**Passos**

1. Na página Configuração, localize o sistema StorageGRID .
2. No bloco do sistema StorageGRID , selecione **Configuração**.
3. Conclua uma das seguintes etapas para habilitar ou desabilitar a verificação:
    - Para habilitar varreduras somente de mapeamento em um bucket, selecione **Mapear**.
    - Para habilitar verificações completas em um bucket, selecione **Mapear e classificar**.
    - Para desabilitar a varredura em um bucket, selecione **Desativado**.

**Resultado**

A Classificação de Dados inicia a varredura dos buckets que você habilitou. Você pode acompanhar o progresso da verificação inicial navegando até o menu **Configuração** e selecionando **Configuração do sistema**. O progresso de cada verificação é mostrado como uma barra de progresso. Você também pode passar o mouse sobre a barra de progresso para ver o número de arquivos verificados em relação ao total de arquivos no volume. Se houver algum erro, ele aparecerá na coluna Status, junto com a ação necessária para corrigi-lo.

# Integre seu Active Directory com a NetApp Data Classification

Você pode integrar um Active Directory global com a NetApp Data Classification para aprimorar os resultados que a Classificação de Dados relata sobre proprietários de arquivos e quais usuários e grupos têm acesso aos seus arquivos.

Ao configurar determinadas fontes de dados (listadas abaixo), você precisa inserir credenciais do Active Directory para que a Classificação de Dados verifique os volumes CIFS. Essa integração fornece à Classificação de Dados detalhes sobre o proprietário do arquivo e as permissões dos dados que residem nessas fontes de dados. O Active Directory inserido para essas fontes de dados pode ser diferente das credenciais globais do Active Directory inseridas aqui. A Classificação de Dados procurará em todos os Diretórios Ativos integrados detalhes de usuários e permissões.

Esta integração fornece informações adicionais nos seguintes locais na Classificação de Dados:

- Você pode usar o "Proprietário do Arquivo""filtro" e veja os resultados nos metadados do arquivo no painel Investigação. Em vez do proprietário do arquivo conter o SID (Identificador de Segurança), ele é preenchido com o nome do usuário real.

  Você também pode visualizar mais detalhes sobre o proprietário do arquivo: nome da conta, endereço de e-mail e nome da conta SAM, ou visualizar itens de propriedade desse usuário.

- Você pode ver"permissões completas de arquivo" para cada arquivo e diretório quando você clica no botão "Exibir todas as permissões".
- No"Painel de governança" , o painel Permissões abertas mostrará um nível maior de detalhes sobre seus dados.

SIDs de usuários locais e SIDs de domínios desconhecidos não são traduzidos para o nome de usuário real.

## Fontes de dados suportadas

Uma integração do Active Directory com a Classificação de Dados pode identificar dados das seguintes fontes de dados:

- Sistemas ONTAP locais
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSx para ONTAP

## Conecte-se ao seu servidor Active Directory

Depois de implantar a Classificação de Dados e ativar a verificação em suas fontes de dados, você pode integrar a Classificação de Dados ao seu Active Directory. O Active Directory pode ser acessado usando um endereço IP de servidor DNS ou um endereço IP de servidor LDAP.

As credenciais do Active Directory podem ser somente leitura, mas fornecer credenciais de administrador garante que a Classificação de Dados possa ler quaisquer dados que exijam permissões elevadas. As credenciais são armazenadas na instância de Classificação de Dados.

Para volumes/compartilhamentos de arquivos CIFS, se você quiser ter certeza de que os "últimos horários de acesso" dos seus arquivos não serão alterados pelas verificações de classificação de Classificação de Dados, o usuário deverá ter permissão para Gravar Atributos. Se possível, recomendamos tornar o usuário configurado do Active Directory parte de um grupo pai na organização que tenha permissões para todos os arquivos.

**Requisitos**

- Você deve ter um Active Directory já configurado para os usuários da sua empresa.

- Você deve ter as informações do Active Directory:
  - Endereço IP do servidor DNS ou vários endereços IP

    ou

    Endereço IP do servidor LDAP ou vários endereços IP
  - Nome de usuário e senha para acessar o servidor
  - Nome de domínio (nome do Active Directory)
  - Se você está usando LDAP seguro (LDAPS) ou não
  - Porta do servidor LDAP (normalmente 389 para LDAP e 636 para LDAP seguro)
- As seguintes portas devem estar abertas para comunicação de saída pela instância de Classificação de Dados:

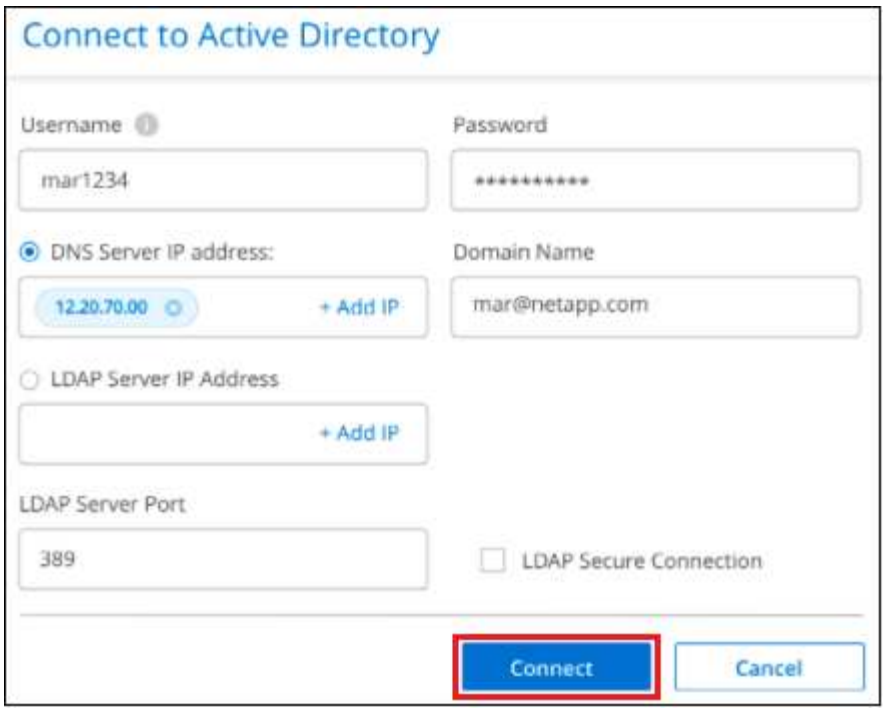
| Protocolo | Porta | Destino | Propósito |
|---|---|---|---|
| TCP e UDP | 389 | Diretório ativo | LDAP |
| TCP | 636 | Diretório ativo | LDAP sobre SSL |
| TCP | 3268 | Diretório ativo | Catálogo Global |
| TCP | 3269 | Diretório ativo | Catálogo global sobre SSL |

**Passos**

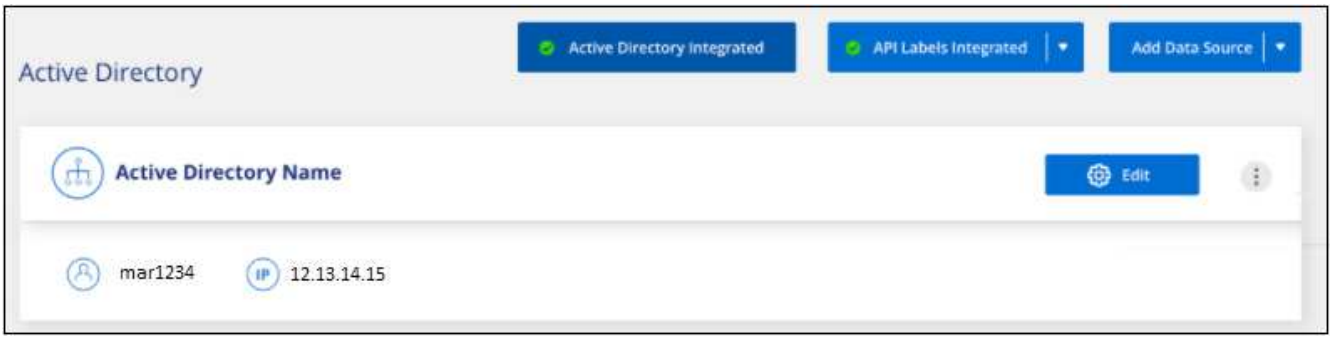
1. Na página Configuração de Classificação de Dados, clique em **Adicionar Active Directory**.


2. Na caixa de diálogo Conectar ao Active Directory, insira os detalhes do Active Directory e clique em **Conectar**.

   Você pode adicionar vários endereços IP, se necessário, selecionando **Adicionar IP**.




A Classificação de Dados é integrada ao Active Directory e uma nova seção é adicionada à página Configuração.




## Gerencie sua integração com o Active Directory

Se precisar modificar algum valor na sua integração com o Active Directory, clique no botão **Editar** e faça as alterações.

Você também pode excluir a integração selecionando o botão e depois **Remover Active Directory**.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais