Documentação de NetApp Data Classification

NetApp Data Classification

NetApp
February 06, 2026

Índice

Documentação de NetApp Data Classification

Notas de lançamento

Novidades na NetApp Data Classification

Saiba o que há de novo na NetApp Data Classification.

14 de janeiro de 2026

Versão 1.50

Esta versão do Data Classification inclui correções de erros e as seguintes atualizações:

Melhorias na classificação personalizada

A Classificação de Dados agora permite a criação de categorias personalizadas para seus dados. Você pode carregar arquivos para ajustar um modelo de IA que a Classificação de Dados usa para aplicar o marcador de categoria aos dados. A interface para todas as classificações personalizadas foi aprimorada.

Para mais informações, consulte "Crie uma classificação personalizada".

Definição personalizada de dados obsoletos

A Classificação de Dados agora permite personalizar a definição de dados obsoletos para que ela se adapte às necessidades da sua organização. Anteriormente, dados obsoletos eram definidos como quaisquer dados que tivessem sido modificados pela última vez há três anos. Agora, dados obsoletos podem ser identificados com base na data do último acesso *ou* da última modificação; o período pode variar de 6 meses a 10 anos atrás.

Para mais informações, consulte "Personalize a definição de dados obsoletos".

Desempenho aprimorado

Os tempos de carregamento de todas as páginas em Classificação de Dados, no relatório de mapeamento de dados e nos filtros da página de Investigação foram reduzidos.

Tempo estimado para relatórios de investigação

Ao fazer o download de um relatório de investigação, a Classificação de Dados agora exibe o tempo estimado para a conclusão do download.

08 de dezembro de 2025

Versão 1.49

Esta versão do Data Classification inclui correções de erros e as seguintes atualizações:

Monitore as métricas e o desempenho no painel de monitoramento de integridade.

O Data Classification agora oferece um painel de monitoramento de integridade, fornecendo monitoramento em tempo real de seus recursos e insights sobre uso de memória, uso de disco, utilização de disco e muito mais. Com as informações do painel de monitoramento de integridade, você pode analisar a infraestrutura da sua implementação e obter insights para otimizar o armazenamento e o desempenho.

Para mais informações, consulte "Monitore a integridade da Classificação de Dados.".

Desempenho de carregamento aprimorado

O desempenho de carregamento de todas as páginas em Classificação de Dados foi aprimorado para criar uma experiência de usuário mais eficiente.

10 de novembro de 2025

Versão 1.48

Esta versão do Data Classification inclui correções de erros, melhorias de segurança e otimizações de desempenho.

Clareza aprimorada no progresso da digitalização

As configurações de digitalização agora incluem informações aprimoradas sobre a conclusão da digitalização. Anteriormente, a barra de progresso era exibida apenas enquanto a digitalização estava em andamento. Agora, a barra de progresso permanece visível após a conclusão para confirmar que as verificações foram concluídas com sucesso. Você também poderá visualizar o número de arquivos mapeados e digitalizados.

Para obter mais informações sobre as configurações de digitalização, consulte "Alterar as configurações de verificação de NetApp Data Classification para seus repositórios".

06 de outubro de 2025

Versão 1.47

A BlueXP classification agora é NetApp Data Classification

A BlueXP classification foi renomeada para NetApp Data Classification. Além da renomeação, a interface do usuário foi aprimorada.

BlueXP agora é NetApp Console

O BlueXP foi renomeado e redesenhado para refletir melhor seu papel no gerenciamento de sua infraestrutura de dados.

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada.

Para obter detalhes sobre o que mudou, consulte o "Notas de versão do NetApp Console" .

Experiência de investigação aprimorada

Encontre e entenda seus dados mais rapidamente com novos filtros pesquisáveis, contagens de resultados por valor, insights em tempo real resumindo as principais descobertas e uma tabela de resultados atualizada com colunas personalizáveis e um painel de detalhes deslizante.

Para obter mais informações, consulte "Investigar dados" .

Novos painéis de governança e conformidade

Obtenha insights críticos mais rapidamente com widgets intuitivos, visuais mais claros e desempenho de carregamento aprimorado. Para mais informações, consulte"Revise as informações de governança sobre seus dados" e"Visualize informações de conformidade sobre seus dados" .

Políticas para consultas salvas (visualização)

A classificação de dados agora permite automatizar a governança com ações condicionais. Você pode criar regras de retenção com exclusão automática e configurar notificações periódicas por e-mail, tudo gerenciado a partir de uma página de consultas salvas atualizada.

Para obter mais informações, consulte "Criar políticas" .

Ações (visualização)

Assuma o controle direto da página Investigação: exclua, mova, copie ou marque arquivos individualmente ou em massa para gerenciamento e correção de dados eficientes.

Para obter mais informações, consulte "Investigar dados" .

Suporte para Google Cloud NetApp Volumes

A classificação de dados agora oferece suporte à digitalização no Google Cloud NetApp Volumes. Adicione facilmente o Google Cloud NetApp Volumes do NetApp Console para uma varredura e classificação de dados perfeitas. Para mais informações, consulte "Verificar Google Cloud NetApp Volumes".

11 de agosto de 2025

Versão 1.46

Esta versão de Classificação de Dados inclui correções de bugs e as seguintes atualizações:

Insights aprimorados sobre eventos de verificação na página de auditoria

A página Auditoria agora oferece suporte a insights aprimorados sobre eventos de verificação para BlueXP classification. A página Auditoria agora exibe quando a verificação de um sistema começa, os status dos sistemas e quaisquer problemas. Os status de compartilhamentos e sistemas estão disponíveis somente para verificações de mapeamento.

Para mais informações sobre a página Auditoria, consulte"Monitorar as operações do NetApp Console" .

Suporte para RHEL 9.6

Esta versão adiciona suporte ao Red Hat Enterprise Linux v9.6 para instalação manual local da BlueXP classification, incluindo implantações de site escuro.

Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão de BlueXP classification 1.30 ou superior: Red Hat Enterprise Linux versão 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 e 9.5.

14 de julho de 2025

Versão 1.45

Esta versão de BlueXP classification inclui alterações de código que otimizam a utilização de recursos e:

Fluxo de trabalho aprimorado para adicionar compartilhamentos de arquivos para digitalização

O fluxo de trabalho para adicionar compartilhamentos de arquivos a um grupo de compartilhamento de arquivos foi simplificado. O processo agora também diferencia o suporte ao protocolo CIFS com base no tipo de autenticação (Kerberos ou NTLM).

Para obter mais informações, consulte "Verificar compartilhamentos de arquivos" .

Informações aprimoradas sobre o proprietário do arquivo

Agora você pode visualizar mais informações sobre os proprietários dos arquivos capturados na guia Investigação. Ao visualizar os metadados de um arquivo na guia Investigação, localize o proprietário do arquivo e selecione **Exibir detalhes** para ver o nome de usuário, o e-mail e o nome da conta SAM. Você também pode ver outros itens de propriedade deste usuário. Este recurso está disponível somente para ambientes de trabalho com o Active Directory.

Para obter mais informações, consulte "Investigue os dados armazenados em sua organização" .

10 de junho de 2025

Versão 1.44

Esta versão de BlueXP classification inclui:

Tempos de atualização aprimorados para o painel de governança

Os tempos de atualização para componentes individuais do painel de governança foram melhorados. A tabela a seguir exibe a frequência de atualizações para cada componente.

Componente	Horários de atualização
Era dos Dados	24 horas
Categorias	24 horas
Visão geral dos dados	5 minutos
Arquivos duplicados	2 horas
Tipos de arquivo	24 horas
Dados não comerciais	2 horas
Permissões abertas	24 horas
Pesquisas salvas	2 horas
Dados sensíveis e permissões amplas	24 horas
Tamanho dos dados	24 horas
Dados obsoletos	2 horas
Principais repositórios de dados por nível de sensibilidade	2 horas

Você pode visualizar o horário da última atualização e atualizar manualmente os componentes Arquivos duplicados, Dados não comerciais, Pesquisas salvas, Dados obsoletos e Principais repositórios de dados por nível de sensibilidade. Para obter mais informações sobre o painel de governança, consulte"Visualize detalhes de governança sobre os dados armazenados em sua organização" .

Melhorias de desempenho e segurança

Foram feitas melhorias para melhorar o desempenho, o consumo de memória e a segurança da classificação BlueXP .

Correções de bugs

O Redis foi atualizado para melhorar a confiabilidade da BlueXP classification. A BlueXP classification agora usa o Elasticsearch para melhorar a precisão dos relatórios de contagem de arquivos durante as verificações.

12 de maio de 2025

Versão 1.43

Esta versão de classificação BlueXP inclui:

Priorizar varreduras de classificação

A Classificação de Dados oferece suporte à capacidade de priorizar verificações de Mapeamento e Classificação, além de verificações somente de Mapeamento, permitindo que você selecione quais verificações serão concluídas primeiro. A priorização de verificações de Map & Classify é suportada durante e antes do início das verificações. Se você optar por priorizar uma verificação enquanto ela estiver em andamento, tanto as verificações de mapeamento quanto as de classificação serão priorizadas.

Para obter mais informações, consulte "Priorizar varreduras" .

Suporte para categorias de dados de informações de identificação pessoal (PII) canadenses

As varreduras de classificação de dados identificam categorias de dados PII canadenses. Essas categorias incluem informações bancárias, números de passaporte, números de seguro social, números de carteira de motorista e números de cartão de saúde para todas as províncias e territórios canadenses.

Para obter mais informações, consulte "Categorias de dados pessoais" .

Classificação personalizada (visualização)

A Classificação de Dados oferece suporte a classificações personalizadas para verificações do Map & Classify. Com classificações personalizadas, você pode adaptar as verificações de Classificação de Dados para capturar dados específicos da sua organização usando expressões regulares. Este recurso está atualmente em versão prévia.

Para obter mais informações, consulte "Adicionar classificações personalizadas" .

Aba de pesquisas salvas

A aba **Políticas** foi renomeada**"Pesquisas salvas"** . A funcionalidade não foi alterada.

Enviar eventos de verificação para a página de auditoria

A classificação de dados oferece suporte ao envio de eventos de classificação (quando uma varredura é iniciada e quando ela termina) para o"Página de auditoria do NetApp Consle" .

Atualizações de segurança

- O pacote Keras foi atualizado, mitigando vulnerabilidades (BDSA-2025-0107 e BDSA-2025-1984).
- A configuração dos contêineres do Docker foi atualizada. O contêiner não tem mais acesso às interfaces de rede do host para criar pacotes de rede brutos. Ao reduzir o acesso desnecessário, a atualização atenua potenciais riscos de segurança.

Melhorias de desempenho

Melhorias no código foram implementadas para reduzir o uso de RAM e melhorar o desempenho geral da Classificação de Dados.

Correções de bugs

Foram corrigidos bugs que causavam falhas nas verificações do StorageGRID , o não carregamento das opções de filtro da página de investigação e o não download da Avaliação de Descoberta de Dados para avaliações de alto volume.

14 de abril de 2025

Versão 1.42

Esta versão de BlueXP classification inclui:

Digitalização em massa para ambientes de trabalho

A BlueXP classification oferece suporte a operações em massa para ambientes de trabalho. Você pode escolher habilitar verificações de mapeamento, habilitar verificações de mapeamento e classificação, desabilitar verificações ou criar uma configuração personalizada em todos os volumes no ambiente de trabalho. Se você fizer uma seleção para um volume individual, ela substituirá a seleção em massa. Para executar uma operação em massa, navegue até a página **Configuração** e faça sua seleção.

Baixe o relatório de investigação localmente

A BlueXP classification permite baixar relatórios de investigação de dados localmente para visualizar no navegador. Se você escolher a opção local, a investigação de dados estará disponível apenas no formato CSV e exibirá apenas as primeiras 10.000 linhas de dados.

Para obter mais informações, consulte "Investigue os dados armazenados em sua organização com a BlueXP classification" .

10 de março de 2025

Versão 1.41

Esta versão da BlueXP classification inclui melhorias gerais e correções de bugs. Inclui também:

Status da digitalização

A BlueXP classification rastreia o progresso em tempo real das varreduras de mapeamento e classificação *iniciais* em um volume. Barras progressivas separadas rastreiam as varreduras de mapeamento e classificação, apresentando uma porcentagem do total de arquivos varridos. Você também pode passar o mouse sobre uma barra de progresso para ver o número de arquivos verificados e o total de arquivos. Acompanhar o status das suas verificações cria insights mais profundos sobre o progresso da verificação, permitindo que você planeje melhor suas verificações e entenda a alocação de recursos.

Para visualizar o status das suas verificações, navegue até **Configuração** na BlueXP classification e selecione a **Configuração do ambiente de trabalho**. O progresso é exibido em linha para cada volume.

19 de fevereiro de 2025

Versão 1.40

Esta versão da BlueXP classification inclui as seguintes atualizações.

Suporte para RHEL 9.5

Esta versão oferece suporte ao Red Hat Enterprise Linux v9.5, além das versões suportadas anteriormente. Isso se aplica a qualquer instalação manual local da BlueXP classification, incluindo implantações em sites obscuros.

Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão de BlueXP classification 1.30 ou superior: Red Hat Enterprise Linux versão 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 e 9.5.

Priorizar varreduras somente de mapeamento

Ao realizar verificações somente de mapeamento, você pode priorizar as verificações mais importantes. Esse recurso ajuda quando você tem muitos ambientes de trabalho e quer garantir que as verificações de alta prioridade sejam concluídas primeiro.

Por padrão, as verificações são enfileiradas com base na ordem em que são iniciadas. Com a capacidade de priorizar verificações, você pode movê-las para a frente da fila. Várias varreduras podem ser priorizadas. A

prioridade é designada na ordem "primeiro a entrar, primeiro a sair", o que significa que a primeira varredura que você prioriza passa para a frente da fila; a segunda varredura que você prioriza se torna a segunda na fila, e assim por diante.

A prioridade é concedida apenas uma vez. As novas varreduras automáticas de dados de mapeamento ocorrem na ordem padrão.

A priorização é limitada a"varreduras somente de mapeamento" ; não está disponível para mapeamento e classificação de varreduras.

Para obter mais informações, consulte "Priorizar varreduras" .

Repetir todas as verificações

A BlueXP classification permite repetir em lote todas as verificações com falha.

Você pode tentar novamente as verificações em uma operação em lote com a função **Repetir tudo**. Se as verificações de classificação estiverem falhando devido a um problema temporário, como uma queda de rede, você pode tentar todas as verificações ao mesmo tempo com um botão, em vez de tentar novamente individualmente. As digitalizações podem ser repetidas quantas vezes forem necessárias.

Para repetir todas as verificações:

1. No menu de BlueXP classification , selecione **Configuração**.
2. Para repetir todas as verificações com falha, selecione **Repetir todas as verificações**.

Precisão aprimorada do modelo de categorização

A precisão do modelo de aprendizagem de máquina para"categorias predefinidas" melhorou em 11%.

22 de janeiro de 2025

Versão 1.39

Esta versão de BlueXP classification atualiza o processo de exportação do relatório de investigação de dados. Esta atualização de exportação é útil para executar análises adicionais em seus dados, criar visualizações adicionais nos dados ou compartilhar os resultados de sua investigação de dados com outras pessoas.

Anteriormente, a exportação do relatório de investigação de dados era limitada a 10.000 linhas. Com esta versão, o limite foi removido para que você possa exportar todos os seus dados. Essa alteração permite que você exporte mais dados dos seus relatórios de investigação de dados, proporcionando mais flexibilidade na sua análise de dados.

Você pode escolher o ambiente de trabalho, os volumes, a pasta de destino e o formato JSON ou CSV. O nome do arquivo exportado inclui um registro de data e hora para ajudar você a identificar quando os dados foram exportados.

Os ambientes de trabalho suportados incluem:

- Cloud Volumes ONTAP
- FSx para ONTAP
- ONTAP
- Grupo de compartilhamento

A exportação de dados do relatório de investigação de dados tem as seguintes limitações:

- O número máximo de registros para download é 500 milhões por tipo (arquivos, diretórios e tabelas)
- Espera-se que um milhão de registros levem cerca de 35 minutos para serem exportados.

Para obter detalhes sobre a investigação de dados e o relatório, consulte "Investigue os dados armazenados na sua organização" .

16 de dezembro de 2024

Versão 1.38

Esta versão da BlueXP classification inclui melhorias gerais e correções de bugs.

4 de novembro de 2024

Versão 1.37

Esta versão da BlueXP classification inclui as seguintes atualizações.

Suporte para RHEL 8.10

Esta versão oferece suporte ao Red Hat Enterprise Linux v8.10, além das versões suportadas anteriormente. Isso se aplica a qualquer instalação manual local da BlueXP classification, incluindo implantações em sites obscuros.

Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão de BlueXP classification 1.30 ou superior: Red Hat Enterprise Linux versão 8.8, 8.10, 9.0, 9.1, 9.2, 9.3 e 9.4.

Saiba mais sobre "BlueXP classification" .

Suporte para NFS v4.1

Esta versão oferece suporte ao NFS v4.1, além das versões suportadas anteriormente.

Saiba mais sobre "BlueXP classification" .

10 de outubro de 2024

Versão 1.36

Suporte para RHEL 9.4

Esta versão oferece suporte ao Red Hat Enterprise Linux v9.4, além das versões suportadas anteriormente. Isso se aplica a qualquer instalação manual local da BlueXP classification, incluindo implantações em sites obscuros.

Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão de BlueXP classification 1.30 ou superior: Red Hat Enterprise Linux versão 8.8, 9.0, 9.1, 9.2, 9.3 e 9.4.

Saiba mais sobre "Visão geral das implantações de BlueXP classification" .

Desempenho de digitalização aprimorado

Esta versão oferece desempenho de digitalização aprimorado.

2 de setembro de 2024

Versão 1.35

Verificar dados do StorageGRID

A BlueXP classification oferece suporte à digitalização de dados no StorageGRID.

Para mais detalhes, consulte"Verificar dados do StorageGRID" .

05 de agosto de 2024

Versão 1.34

Esta versão de BlueXP classification inclui a seguinte atualização.

Mudança do CentOS para o Ubuntu

A BlueXP classification atualizou seu sistema operacional Linux para Microsoft Azure e Google Cloud Platform (GCP) do CentOS 7.9 para o Ubuntu 22.04.

Para obter detalhes de implantação, consulte "Instalar em um host Linux com acesso à Internet e preparar o sistema host Linux" .

01 de julho de 2024

Versão 1.33

Suporte ao Ubuntu

Esta versão suporta a plataforma Linux Ubuntu 24.04.

As varreduras de mapeamento coletam metadados

Os seguintes metadados são extraídos dos arquivos durante as varreduras de mapeamento e são exibidos nos painéis de Governança, Conformidade e Investigação:

- Ambiente de trabalho
- Tipo de ambiente de trabalho
- 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

Dados adicionais em painéis

Esta versão atualiza quais dados aparecem nos painéis de Governança, Conformidade e Investigação durante

as verificações de mapeamento.

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

05 de junho de 2024

Versão 1.32

Nova coluna de status de mapeamento na página de configuração

Esta versão agora mostra uma nova coluna de status de mapeamento na página Configuração. A nova coluna ajuda você a identificar se o mapeamento está em execução, na fila, pausado, entre outros.

Para explicações sobre os status, consulte "Alterar configurações de digitalização" .

15 de maio de 2024

Versão 1.31

A classificação está disponível como um serviço principal no BlueXP

A BlueXP classification agora está disponível como um recurso principal dentro do BlueXP , sem custo adicional para até 500 TiB de dados digitalizados por conector. Não é necessária nenhuma licença de classificação ou assinatura paga. Como focamos a funcionalidade de BlueXP classification na varredura de sistemas de armazenamento NetApp com esta nova versão, algumas funcionalidades legadas estarão disponíveis apenas para clientes que pagaram anteriormente por uma licença. O uso desses recursos legados expirará quando o contrato pago atingir sua data final.

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" .

01 de abril de 2024

Versão 1.30

Suporte adicionado para BlueXP classification

Esta versão oferece suporte ao Red Hat Enterprise Linux v8.8 e v9.3, além do 9.x anteriormente suportado, que requer o Podman, em vez do mecanismo Docker. Isso se aplica a qualquer instalação manual local da BlueXP classification.

Os seguintes sistemas operacionais exigem o uso do mecanismo de contêiner Podman e exigem a versão de BlueXP classification 1.30 ou superior: Red Hat Enterprise Linux versão 8.8, 9.0, 9.1, 9.2 e 9.3.

Saiba mais sobre "Visão geral das implantações de BlueXP classification" .

A BlueXP classification será suportada se você instalar o Connector em um host RHEL 8 ou 9 que resida no local. Não há suporte se o host RHEL 8 ou 9 residir na AWS, Azure ou Google Cloud.

Opção para ativar a coleta de logs de auditoria removida

A opção para ativar a coleta de logs de auditoria foi desabilitada.

Velocidade de digitalização melhorada

O desempenho da varredura em nós secundários do scanner foi melhorado. Você pode adicionar mais nós de scanner se precisar de poder de processamento adicional para suas digitalizações. Para mais detalhes, consulte "Instalar a BlueXP classification em um host que tenha acesso à Internet" .

Atualizações automáticas

Se você implantou a BlueXP classification em um sistema com acesso à Internet, o sistema será atualizado automaticamente. Anteriormente, a atualização ocorria após um tempo específico decorrido desde a última atividade do usuário. Com esta versão, a BlueXP classification é atualizada automaticamente se o horário local estiver entre 1h e 5h. Se o horário local estiver fora desse horário, a atualização ocorrerá após um tempo específico desde a última atividade do usuário. Para mais detalhes, consulte "Instalar em um host Linux com acesso à Internet" .

Se você implantou a BlueXP classification sem acesso à Internet, será necessário atualizar manualmente. Para mais detalhes, consulte "Instalar a BlueXP classification em um host Linux sem acesso à Internet" .

04 de março de 2024

Versão 1.29

Agora você pode excluir dados de digitalização que residem em determinados diretórios de fonte de dados

Se quiser que a BlueXP classification exclua dados de digitalização que residem em determinados diretórios de fonte de dados, você pode adicionar esses nomes de diretório a um arquivo de configuração processado pela BlueXP classification . Esse recurso permite que você evite escanear diretórios desnecessários ou que resultariam em resultados falsos positivos de dados pessoais.

"Saber mais" .

O suporte a instâncias extragrandes agora é qualificado

Se precisar que a BlueXP classification verifique mais de 250 milhões de arquivos, você pode usar uma instância extragrande em sua implantação na nuvem ou instalação local. Este tipo de sistema pode escanear até 500 milhões de arquivos.

"Saber mais" .

10 de janeiro de 2024

Versão 1.27

Os resultados da página de investigação exibem o tamanho total, além do número total de itens

Os resultados filtrados na página Investigação exibem o tamanho total dos itens, além do número total de arquivos. Isso pode ajudar ao mover arquivos, excluir arquivos e muito mais.

Configurar IDs de grupo adicionais como "Aberto à organização"

Agora você pode configurar IDs de grupo no NFS para serem consideradas como "Abertas à organização" diretamente da BlueXP classification, caso o grupo não tenha sido definido inicialmente com essa permissão. Todos os arquivos e pastas que tiverem esses IDs de grupo anexados serão exibidos como "Abertos à organização" na página Detalhes da investigação. Veja como"adicionar IDs de grupo adicionais como "abertos à organização"" .

14 de dezembro de 2023

Versão 1.26.6

Esta versão incluiu algumas pequenas melhorias.

O lançamento também removeu as seguintes opções:

- A opção para ativar a coleta de logs de auditoria foi desabilitada.
- Durante a investigação dos Diretórios, a opção para calcular o número de dados de informações pessoais identificáveis (PII) pelos Diretórios não está disponível. Consulte "Investigue os dados armazenados em sua organização" .
- A opção de integrar dados usando rótulos do Azure Information Protection (AIP) foi desabilitada.

06 de novembro de 2023

Versão 1.26.3

Os seguintes problemas foram corrigidos nesta versão

- Corrigida uma inconsistência ao apresentar o número de arquivos verificados pelo sistema nos painéis.
- Melhorou o comportamento de verificação ao manipular e relatar arquivos e diretórios com caracteres especiais no nome e nos metadados.

04 de outubro de 2023

Versão 1.26

Suporte para instalações locais da BlueXP classification no RHEL versão 9

As versões 8 e 9 do Red Hat Enterprise Linux não oferecem suporte ao mecanismo Docker, que era necessário para a instalação da BlueXP classification . Agora oferecemos suporte à instalação da BlueXP classification no RHEL 9.0, 9.1 e 9.2 usando o Podman versão 4 ou superior como infraestrutura de contêiner. Se o seu ambiente exigir o uso das versões mais recentes do RHEL, agora você pode instalar a BlueXP classification (versão 1.26 ou superior) ao usar o Podman.

No momento, não oferecemos suporte a instalações de sites obscuros ou ambientes de digitalização distribuídos (usando nós de scanner mestre e remoto) ao usar o RHEL 9.x.

05 de setembro de 2023

Versão 1.25

Implantações pequenas e médias temporariamente indisponíveis

Ao implantar uma instância da BlueXP classification na AWS, a opção de selecionar **Implantar > Configuração** e escolher uma instância pequena ou média não estará disponível no momento. Você ainda pode implantar a instância usando o tamanho de instância grande selecionando **Implantar > Implantar**.

Aplique tags em até 100.000 itens da página Resultados da investigação

No passado, você só podia aplicar tags a uma única página por vez na página Resultados da investigação (20 itens). Agora você pode selecionar **todos** os itens nas páginas Resultados da investigação e aplicar tags a todos os itens — até 100.000 itens por vez.

Identifique arquivos duplicados com um tamanho mínimo de 1 MB

A BlueXP classification era usada para identificar arquivos duplicados somente quando os arquivos tinham 50 MB ou mais. Agora é possível identificar arquivos duplicados começando com 1 MB. Você pode usar os filtros da página Investigação "Tamanho do arquivo" junto com "Duplicatas" para ver quais arquivos de um determinado tamanho estão duplicados em seu ambiente.

17 de julho de 2023

Versão 1.24

Dois novos tipos de dados pessoais alemães são identificados pela BlueXP classification

A BlueXP classification pode identificar e categorizar arquivos que contêm os seguintes tipos de dados:

- ID alemão (Personalausweisnummer)
- Número de Segurança Social Alemão (Sozialversicherungsnummer)

"Veja todos os tipos de dados pessoais que a BlueXP classification pode identificar em seus dados" .

A BlueXP classification é totalmente suportada no modo Restrito e no modo Privado

A BlueXP classification agora é totalmente compatível com sites sem acesso à Internet (modo privado) e com acesso limitado à Internet de saída (modo restrito). "Saiba mais sobre os modos de implantação do BlueXP para o Conector" .

Capacidade de pular versões ao atualizar uma instalação em modo privado da BlueXP classification

Agora você pode atualizar para uma versão mais recente da BlueXP classification, mesmo que ela não seja sequencial. Isso significa que a limitação atual de atualização da BlueXP classification em uma versão por vez não é mais necessária. Este recurso é relevante a partir da versão 1.24.

A API de BlueXP classification já está disponível

A API de BlueXP classification permite que você execute ações, crie consultas e exporte informações sobre os dados que está verificando. A documentação interativa está disponível usando o Swagger. A documentação é separada em várias categorias, incluindo Investigação, Conformidade, Governança e Configuração. Cada categoria é uma referência às guias na interface de BlueXP classification .

"Saiba mais sobre as APIs de BlueXP classification" .

06 de junho de 2023

Versão 1.23

O japonês agora é suportado na busca por nomes de titulares de dados

Agora é possível inserir nomes japoneses ao pesquisar o nome de um sujeito em resposta a uma Solicitação de Acesso ao Titular de Dados (DSAR). Você pode gerar um"Relatório de solicitação de acesso do titular dos dados" com as informações resultantes. Você também pode inserir nomes japoneses no"Filtro "Assunto dos Dados" na página Investigação de Dados" para identificar arquivos que contêm o nome do sujeito.

O Ubuntu agora é uma distribuição Linux suportada na qual você pode instalar a BlueXP classification

O Ubuntu 22.04 foi qualificado como um sistema operacional suportado pela BlueXP classification. Você pode instalar a BlueXP classification em um host Ubuntu Linux na sua rede ou em um host Linux na nuvem ao usar a versão 1.23 do instalador. "Veja como instalar a BlueXP classification em um host com Ubuntu instalado" .

O Red Hat Enterprise Linux 8.6 e 8.7 não são mais suportados com novas instalações de BlueXP

classification

Essas versões não são compatíveis com novas implantações porque o Red Hat não oferece mais suporte ao Docker, o que é um pré-requisito. Se você tiver uma máquina de BlueXP classification existente em execução no RHEL 8.6 ou 8.7, a NetApp continuará a dar suporte à sua configuração.

A BlueXP classification pode ser configurada como um coletor FPolicy para receber eventos FPolicy de sistemas ONTAP

Você pode habilitar que logs de auditoria de acesso a arquivos sejam coletados no seu sistema de BlueXP classification para eventos de acesso a arquivos detectados em volumes em seus ambientes de trabalho. A BlueXP classification pode capturar os seguintes tipos de eventos FPolicy e os usuários que executaram as ações em seus arquivos: Criar, Ler, Gravar, Excluir, Renomear, Alterar proprietário/permissões e Alterar SACL/DACL.

As licenças BYOL do Data Sense agora são suportadas em sites obscuros

Agora você pode carregar sua licença BYOL do Data Sense na BlueXP digital wallet em um site escuro para ser notificado quando sua licença estiver acabando.

03 de abril de 2023

Versão 1.22

Novo Relatório de Avaliação de Descoberta de Dados

O Relatório de Avaliação de Descoberta de Dados fornece uma análise de alto nível do seu ambiente escaneado para destacar as descobertas do sistema e mostrar áreas de preocupação e possíveis etapas de correção. O objetivo deste relatório é aumentar a conscientização sobre preocupações com governança de dados, exposições de segurança de dados e lacunas de conformidade de dados do seu conjunto de dados. "Veja como gerar e usar o Relatório de Avaliação de Descoberta de Dados" .

Capacidade de implantar a BlueXP classification em instâncias menores na nuvem

Ao implantar a BlueXP classification de um BlueXP Connector em um ambiente AWS, agora você pode selecionar entre dois tipos de instância menores do que o disponível com a instância padrão. Se você estiver escaneando um ambiente pequeno, isso pode ajudar a economizar em custos de nuvem. No entanto, há algumas restrições ao usar a instância menor. "Veja os tipos de instâncias disponíveis e limitações" .

O script autônomo agora está disponível para qualificar seu sistema Linux antes da instalação da BlueXP classification

Se você quiser verificar se seu sistema Linux atende a todos os pré-requisitos, independentemente de executar a instalação da BlueXP classification , há um script separado que você pode baixar e que testa apenas os pré-requisitos. "Veja como verificar se o seu host Linux está pronto para instalar a BlueXP classification" .

07 de março de 2023

Versão 1.21

Nova funcionalidade para adicionar suas próprias categorias personalizadas na interface de BlueXP classification

A BlueXP classification agora permite que você adicione suas próprias categorias personalizadas para que a BlueXP classification identifique os arquivos que se enquadram nessas categorias. A BlueXP classification tem muitos "categorias predefinidas" , então esse recurso permite que você adicione categorias personalizadas para identificar onde as informações exclusivas da sua organização são encontradas nos seus dados.

Agora você pode adicionar palavras-chave personalizadas da interface de BlueXP classification

A BlueXP classification tem a capacidade de adicionar palavras-chave personalizadas que a BlueXP classification identificará em verificações futuras há algum tempo. No entanto, você precisava fazer login no host Linux de BlueXP classification e usar uma interface de linha de comando para adicionar as palavras-chave. Nesta versão, a capacidade de adicionar palavras-chave personalizadas está na interface de BlueXP classification , tornando muito fácil adicionar e editar essas palavras-chave.

Capacidade de fazer com que a BlueXP classification não escaneie arquivos quando o "último horário de acesso" for alterado

Por padrão, se a BlueXP classification não tiver permissões de "gravação" adequadas, o sistema não verificará os arquivos em seus volumes porque a BlueXP classification não pode reverter o "último horário de acesso" para o registro de data e hora original. No entanto, se você não se importa se o último horário de acesso será redefinido para o horário original em seus arquivos, você pode substituir esse comportamento na página Configuração para que a BlueXP classification verifique os volumes independentemente das permissões.

Junto com esse recurso, um novo filtro chamado "Evento de análise de verificação" foi adicionado para que você possa visualizar os arquivos que não foram classificados porque a BlueXP classification não conseguiu reverter o último horário de acesso, ou os arquivos que foram classificados mesmo que a BlueXP classification não tenha conseguido reverter o último horário de acesso.

"Saiba mais sobre o "Carimbo de data/hora do último acesso" e as permissões que a BlueXP classification requer" .

Três novos tipos de dados pessoais são identificados pela BlueXP classification

A BlueXP classification pode identificar e categorizar arquivos que contêm os seguintes tipos de dados:

- Número do Bilhete de Identidade do Botsuana (Omang)
- Número do passaporte de Botsuana
- Cartão de Identidade de Registro Nacional de Cingapura (NRIC)

"Veja todos os tipos de dados pessoais que a BlueXP classification pode identificar em seus dados" .

Funcionalidade atualizada para diretórios

- A opção "Relatório CSV leve" para relatórios de investigação de dados agora inclui informações de diretórios.
- O filtro de tempo "Último acesso" agora mostra o último horário de acesso para arquivos e diretórios.

Melhorias na instalação

- O instalador de BlueXP classification para sites sem acesso à Internet (dark sites) agora executa uma pré-verificação para garantir que seus requisitos de sistema e rede estejam prontos para uma instalação bem-sucedida.
- Os arquivos de log de auditoria de instalação são salvos agora; eles são gravados em `/ops/netapp/install_logs` .

05 de fevereiro de 2023

Versão 1.20

Capacidade de enviar e-mails de notificação baseados em políticas para qualquer endereço de e-mail

Em versões anteriores da BlueXP classification, você podia enviar alertas por e-mail aos usuários do BlueXP

em sua conta quando determinadas políticas críticas retornassem resultados. Este recurso permite que você receba notificações para proteger seus dados quando não estiver online. Agora você também pode enviar alertas por e-mail das Políticas para quaisquer outros usuários (até 20 endereços de e-mail) que não estejam na sua conta BlueXP .

"Saiba mais sobre o envio de alertas por e-mail com base nos resultados da política" .

Agora você pode adicionar padrões pessoais da interface de BlueXP classification

A BlueXP classification tem a capacidade de adicionar "dados pessoais" personalizados que a BlueXP classification identificará em verificações futuras por um tempo. No entanto, você precisava fazer login no host Linux de BlueXP classification e usar uma linha de comando para adicionar os padrões personalizados. Nesta versão, a capacidade de adicionar padrões pessoais usando uma regex está na interface de BlueXP classification , tornando muito fácil adicionar e editar esses padrões personalizados.

Capacidade de mover 15 milhões de arquivos usando a BlueXP classification

No passado, você podia fazer com que a BlueXP classification movesse no máximo 100.000 arquivos de origem para qualquer compartilhamento NFS. Agora você pode mover até 15 milhões de arquivos de uma vez.

Capacidade de ver o número de usuários que têm acesso aos arquivos do SharePoint Online

O filtro "Número de usuários com acesso" agora oferece suporte a arquivos armazenados em repositórios do SharePoint Online. No passado, apenas arquivos em compartilhamentos CIFS eram suportados. Observe que os grupos do SharePoint que não são baseados no Active Directory não serão contados neste filtro neste momento.

O novo status "Sucesso Parcial" foi adicionado ao painel Status da Ação

O novo status "Sucesso Parcial" indica que uma ação de BlueXP classification foi concluída e alguns itens falharam e outros foram bem-sucedidos, por exemplo, quando você move ou exclui 100 arquivos. Além disso, o status "Concluído" foi renomeado para "Sucesso". No passado, o status "Concluído" podia listar ações que foram bem-sucedidas e que falharam. Agora, o status "Sucesso" significa que todas as ações foram bem-sucedidas em todos os itens. "Veja como visualizar o painel Status das Ações" .

09 de janeiro de 2023

Versão 1.19

Capacidade de visualizar um gráfico de arquivos que contêm dados confidenciais e que são excessivamente permissivos

O painel de governança adicionou uma nova área *Dados confidenciais e permissões amplas* que fornece um mapa de calor de arquivos que contêm dados confidenciais (incluindo dados pessoais sensíveis e sigilosos) e que são excessivamente permissivos. Isso pode ajudar você a ver onde pode haver algum risco com dados confidenciais. "Saber mais" .

Três novos filtros estão disponíveis na página Investigação de Dados

Novos filtros estão disponíveis para refinar os resultados exibidos na página Investigação de Dados:

- O filtro "Número de usuários com acesso" mostra quais arquivos e pastas estão abertos a um determinado número de usuários. Você pode escolher um intervalo numérico para refinar os resultados - por exemplo, para ver quais arquivos são acessíveis por 51 a 100 usuários.
- Os filtros "Hora de criação", "Hora de descoberta", "Última modificação" e "Último acesso" agora permitem que você crie um intervalo de datas personalizado em vez de apenas selecionar um intervalo predefinido de dias. Por exemplo, você pode procurar por arquivos com "Hora de criação" "anterior a 6 meses" ou com uma data de "Última modificação" dentro dos "últimos 10 dias".

- O filtro "Caminho do arquivo" agora permite que você especifique caminhos que deseja excluir dos resultados da consulta filtrada. Se você inserir caminhos para incluir e excluir determinados dados, a BlueXP classification encontrará todos os arquivos nos caminhos incluídos primeiro, depois removerá os arquivos dos caminhos excluídos e exibirá os resultados.

"Veja a lista de todos os filtros que você pode usar para investigar seus dados" .

A BlueXP classification pode identificar o Número Individual Japonês

A BlueXP classification pode identificar e categorizar arquivos que contêm o Número Individual Japonês (também conhecido como Meu Número). Isso inclui o Meu Número Pessoal e Corporativo. "Veja todos os tipos de dados pessoais que a BlueXP classification pode identificar em seus dados" .

Limitações conhecidas na NetApp Data Classification

Limitações conhecidas identificam funções que não são suportadas ou não interoperam corretamente nesta versão. Revise essas limitações cuidadosamente.

Opções desabilitadas de NetApp Data Classification

A versão de dezembro de 2023 (versão 1.26.6) removeu as seguintes opções:

- A opção para ativar a coleta de logs de auditoria foi desabilitada.
- Durante a investigação dos Diretórios, a opção para calcular o número de dados de informações de identificação pessoal (PII) pelos Diretórios não está disponível.
- A opção de integrar dados usando rótulos do Azure Information Protection (AIP) foi desabilitada.

Escaneamento de classificação de dados

As seguintes limitações ocorrem com varreduras de Classificação de Dados.

A classificação de dados verifica apenas um compartilhamento em um volume

Se você tiver vários compartilhamentos de arquivos em um único volume, a Classificação de Dados verificará o compartilhamento com a hierarquia mais alta. Por exemplo, se você tiver ações como as seguintes:

- /UM
- /A/B
- /C
- /D/E

Nesta configuração, somente os dados em /A são verificados. Os dados em /C e /D não são escaneados.

Solução alternativa

Há uma solução alternativa para garantir que você esteja digitalizando dados de todos os compartilhamentos no seu volume. Siga estes passos:

1. No sistema, adicione o volume a ser escaneado.
2. Após a Classificação de Dados concluir a varredura do volume, vá para a página *Investigação de Dados* e crie um filtro para ver qual compartilhamento está sendo varrido:

Filtre os dados por "Nome do sistema" e "Tipo de diretório = Compartilhamento" para ver qual compartilhamento está sendo verificado.

3. Obtenha a lista completa de compartilhamentos que existem no volume para que você possa ver quais compartilhamentos não estão sendo verificados.
4. "Adicione as ações restantes a um grupo de ações" .

   Adicione todas as ações individualmente, por exemplo:

   ```
   /C
   /D
   ```

5. Execute estas etapas para cada volume no sistema que tenha vários compartilhamentos.

Último registro de data e hora acessado

Quando a Classificação de Dados realiza uma varredura de um diretório, a varredura afeta o campo **Último acesso** do diretório. Quando você visualiza o campo **Último acesso**, esses metadados refletem a data e a hora da verificação ou a última vez que um usuário acessou o diretório.

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.

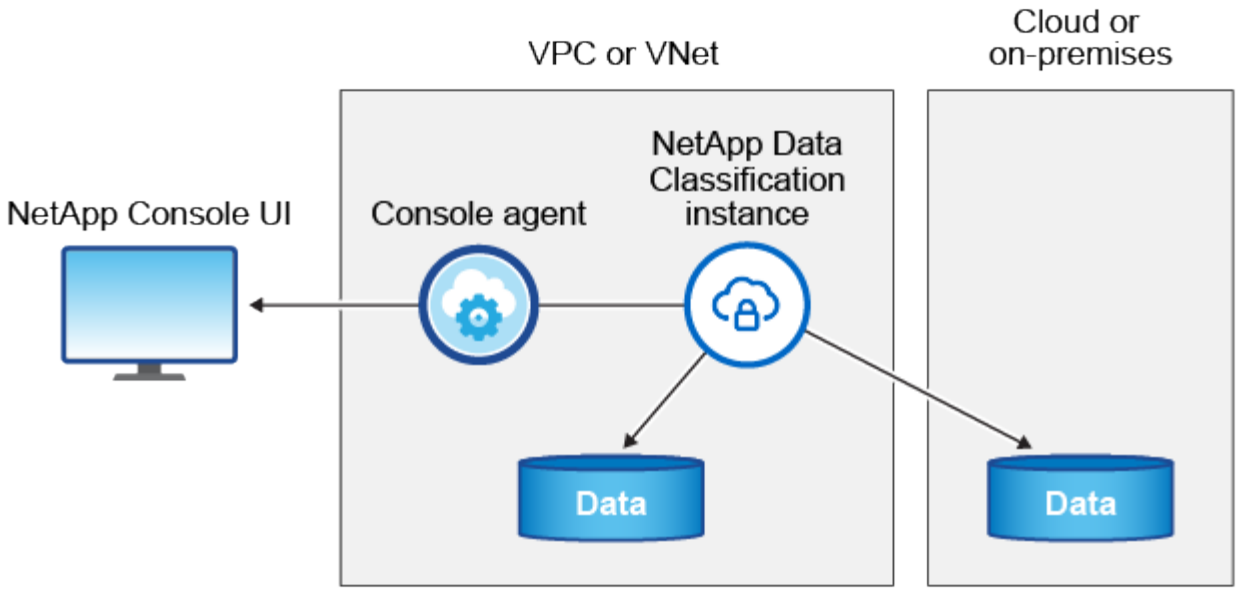
Custos de transferência de dados

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.

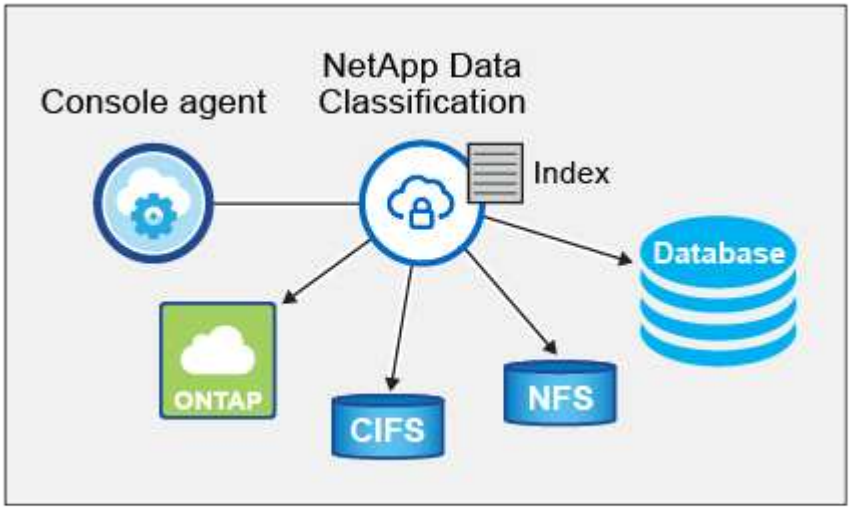
Como funciona a varredura de classificação de dados

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" .

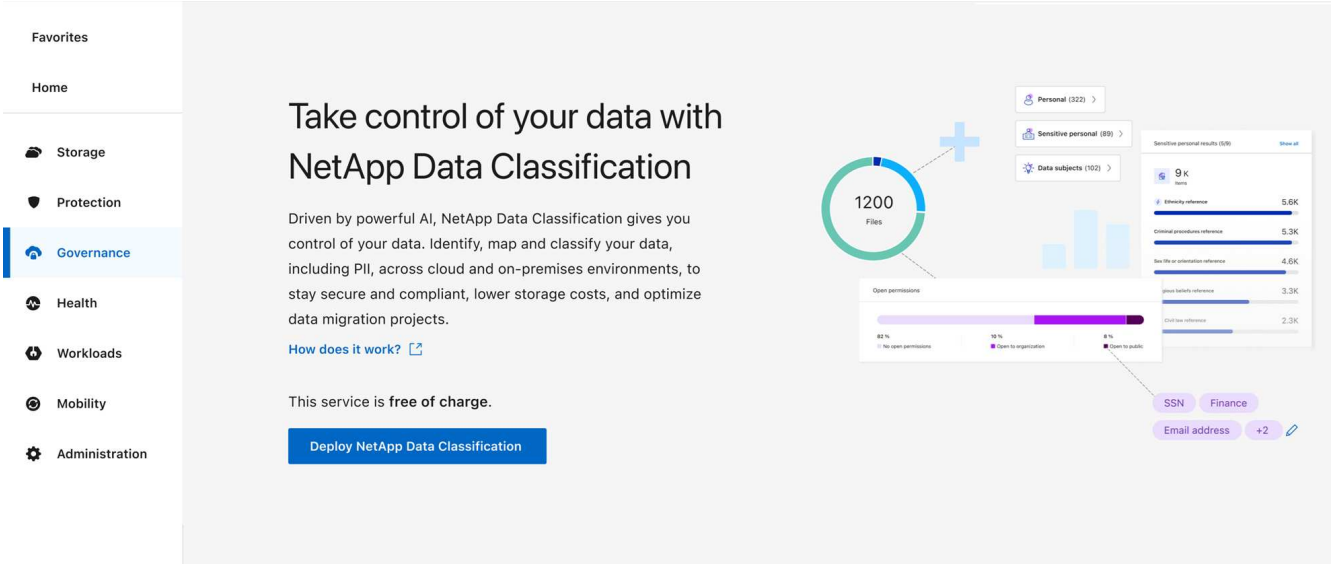
Antes de começar

- "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

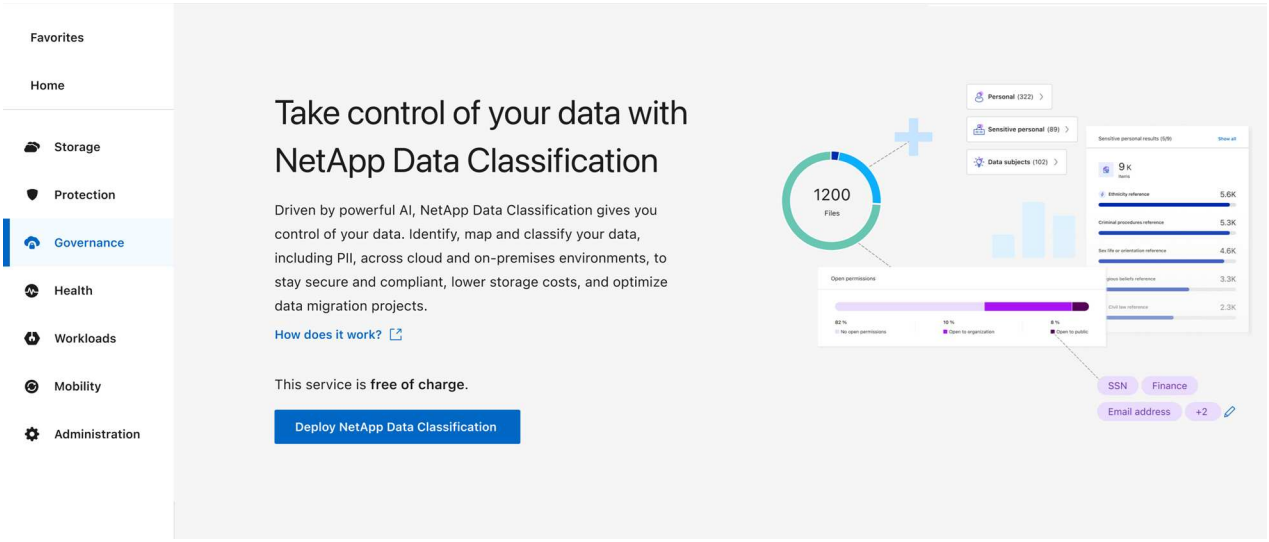
Siga estas etapas para implantar uma instância de Classificação de Dados na nuvem. O agente do Console implantará a instância na nuvem e, em seguida, instalará o software de classificação de dados nessa instância.

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**.

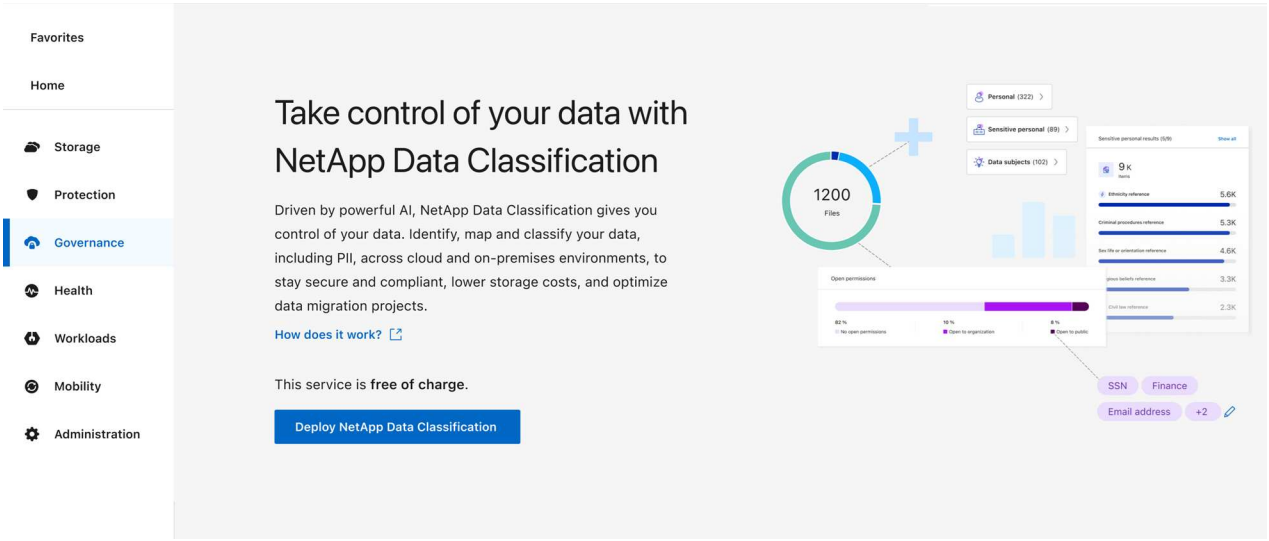


2. Na página *Instalação*, selecione **Implantar > Implantar** para usar o tamanho de instância "Grande" e iniciar o assistente de implantação na nuvem.
3. O assistente exibe o progresso à medida que avança nas etapas de implantação. Quando forem necessárias entradas ou se houver problemas, você será 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**.



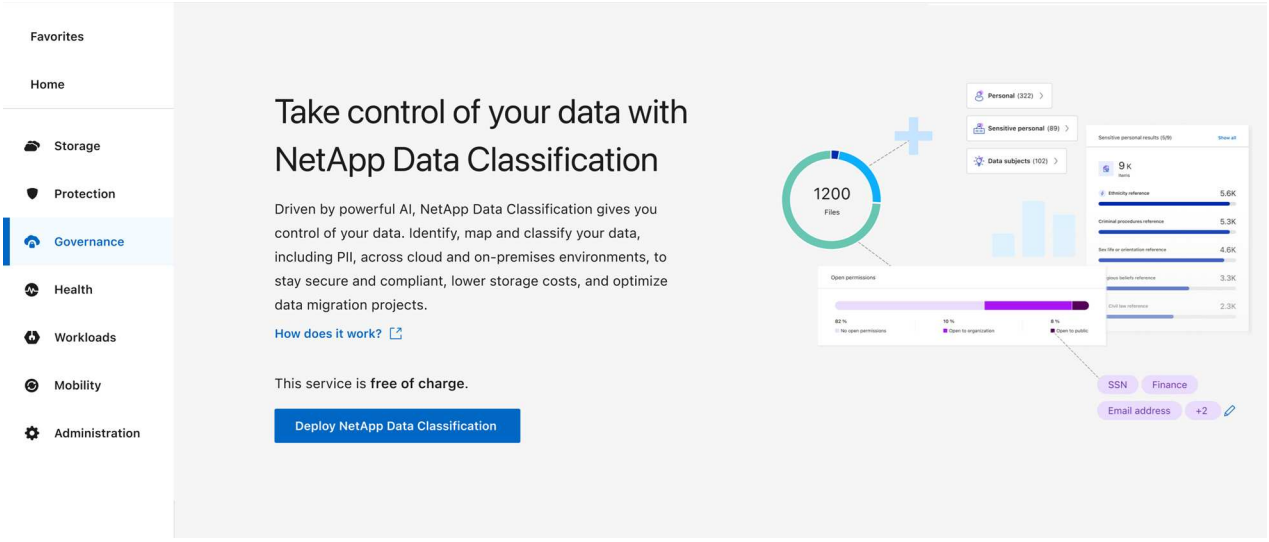
2. Selecione **Implantar** para iniciar o assistente de implantação na nuvem.

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

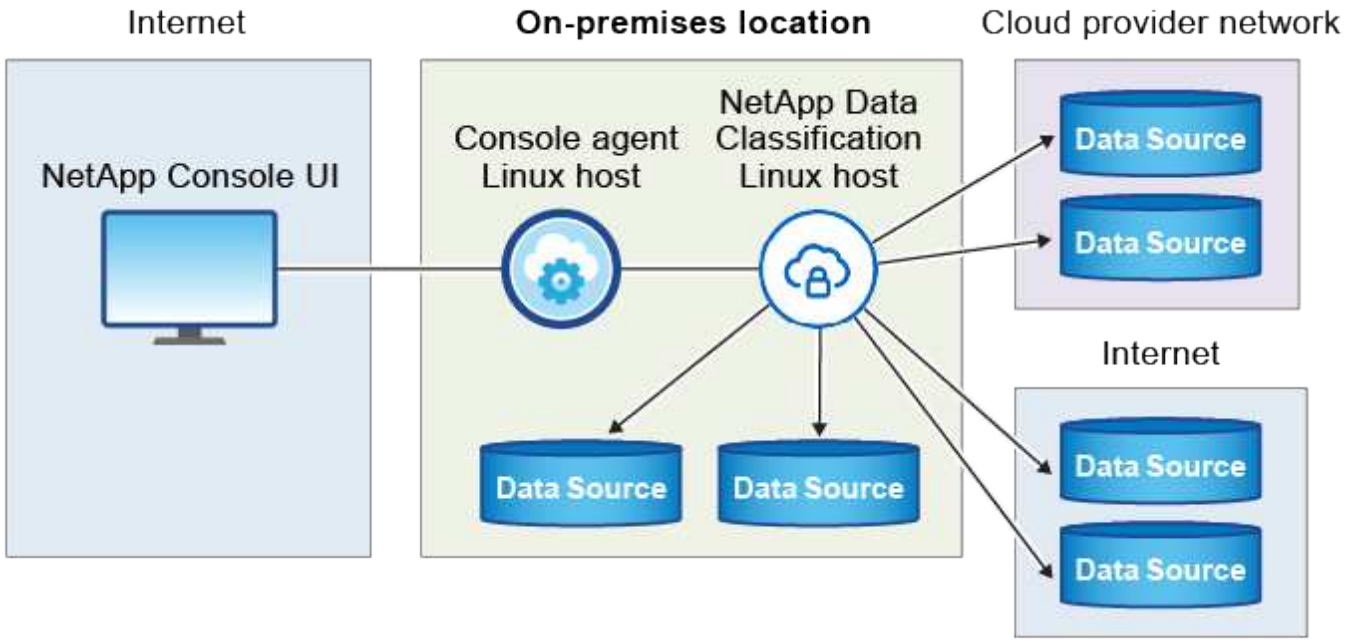
Para implantar a NetApp Data Classification em um host Linux na sua rede ou em um host Linux na nuvem que tenha acesso à Internet, você precisa implantar o host Linux manualmente na sua rede ou na nuvem.

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

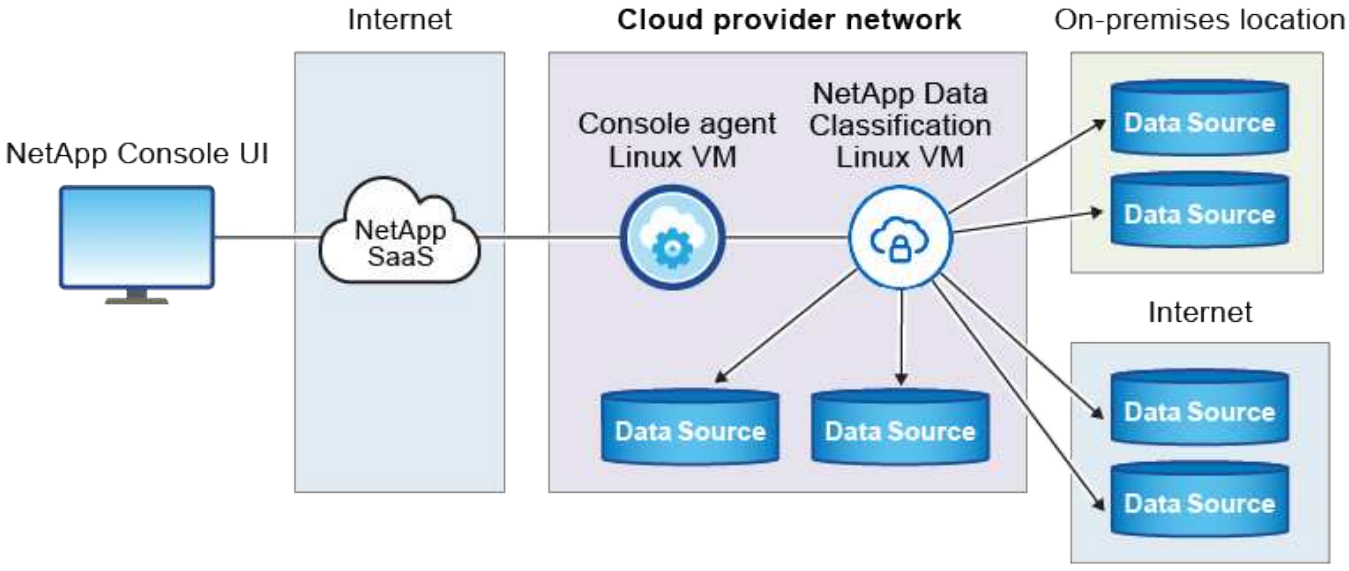
funciona da mesma forma, independentemente do método de instalação escolhido.

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 aosseguintes 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 • 895 GiB disponíveis em /var/lib/docker • 5 GiB em /tmp • **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 • 400 GiB disponíveis em /var/lib/docker ou para Podman /var/lib/containers • 5 GiB em /tmp • **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

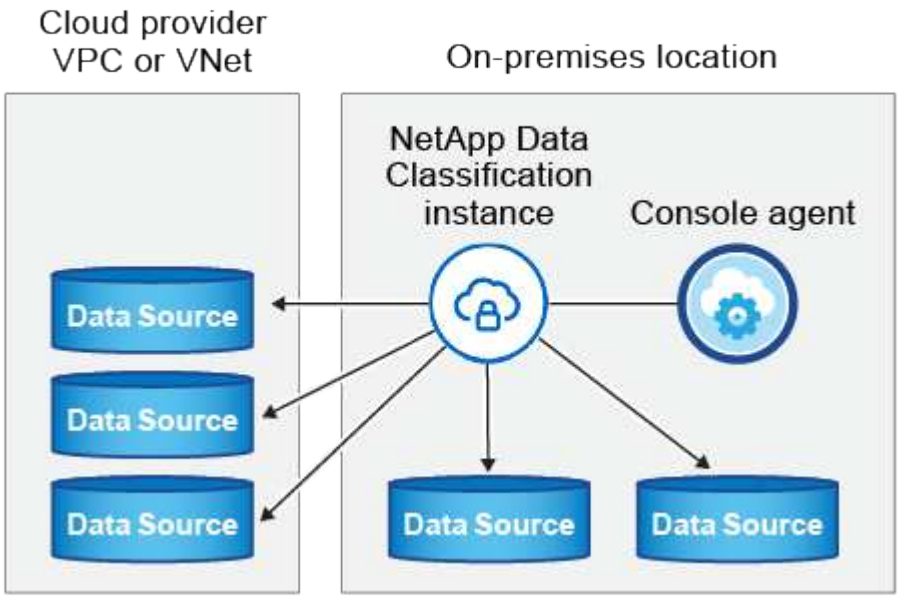
Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o agente do Console, a Classificação de Dados, o Active Directory e suas fontes de dados.

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: • 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. • 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) • 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. Certifique-se de que estas portas estejam abertas para a instância de Classificação de Dados: • Para NFS - 111 e 2049 • Para CIFS - 139 e 445 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. Você deve ter as informações do Active Directory: • Endereço IP do servidor DNS ou vários endereços IP • Nome de usuário e senha para 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)

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

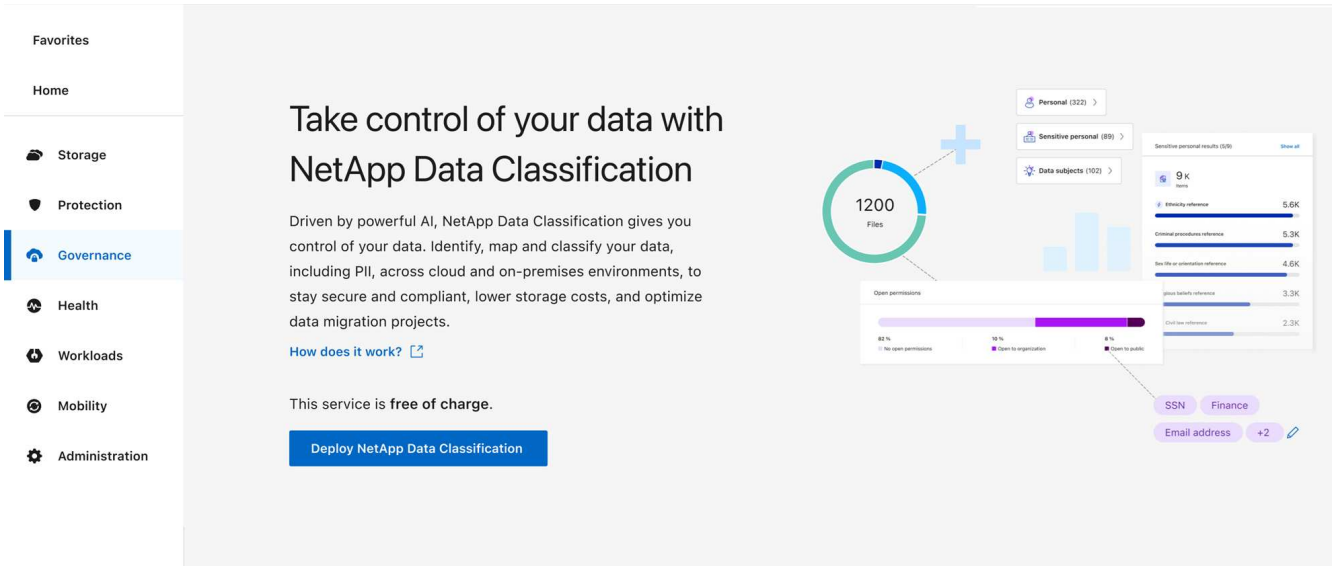
- Verifique se o seu sistema Linux atende aos requisitosrequisitos do host .
- Verifique se o sistema tem os dois pacotes de software pré-requisitos instalados (Docker Engine ou Podman e Python 3).
- Certifique-se de ter privilégios de root no sistema Linux.
- Se você estiver usando um proxy para acessar 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>` Se você estiver instalando em uma instância de nuvem (não em suas instalações), adicione `--manual-cloud-install <cloud_provider>`. 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. 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. 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: `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 • 895 GiB disponíveis em /var/lib/docker • 5 GiB em /tmp • **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 • 400 GiB disponíveis em /var/lib/docker ou para Podman /var/lib/containers • 5 GiB em /tmp • **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.

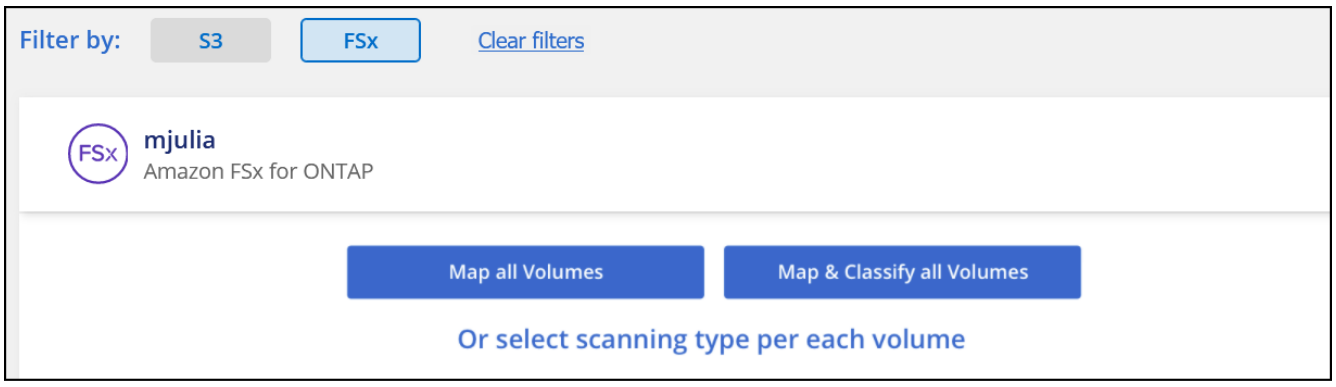
Observação: A implantação da Classificação de Dados em um local local não é suportada atualmente ao escanear volumes FSx.

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

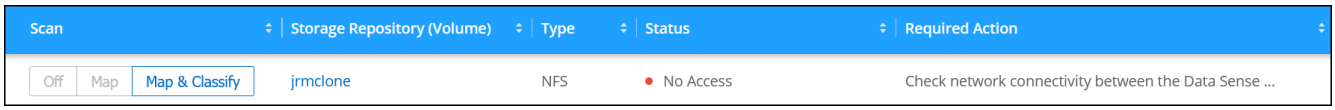
Certifique-se de que a Classificação de Dados possa acessar volumes verificando sua rede, grupos de segurança e políticas de exportação.

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.

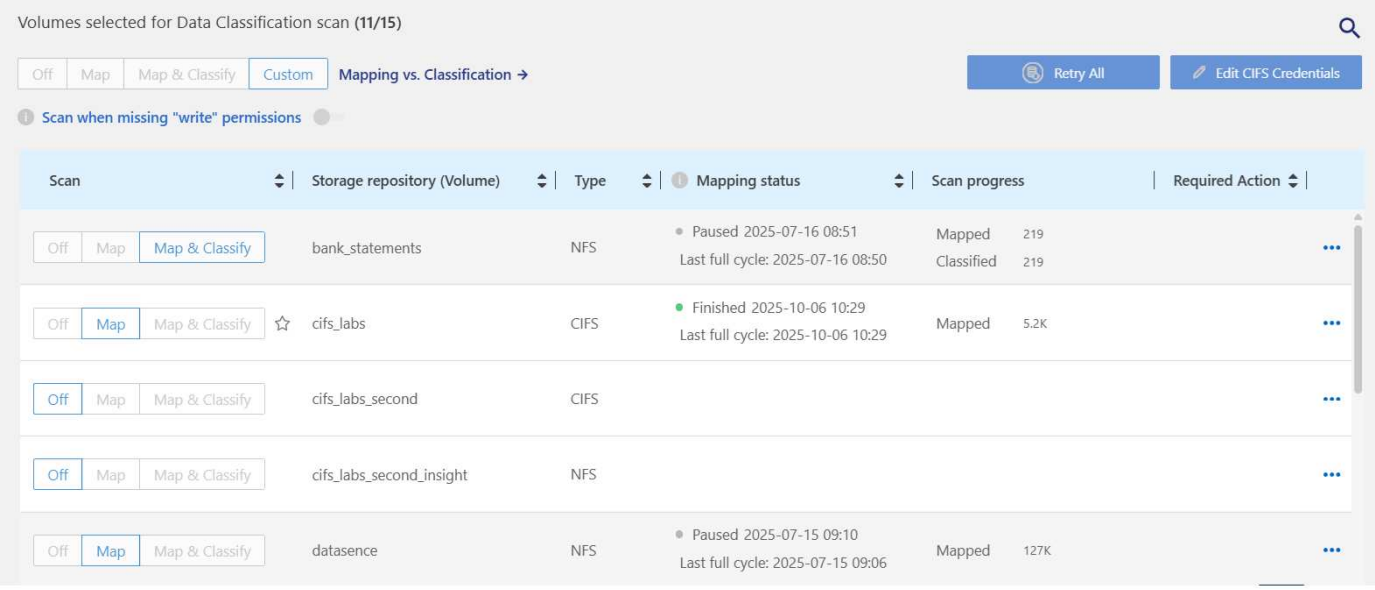
Habilitar e desabilitar verificações em volumes

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.

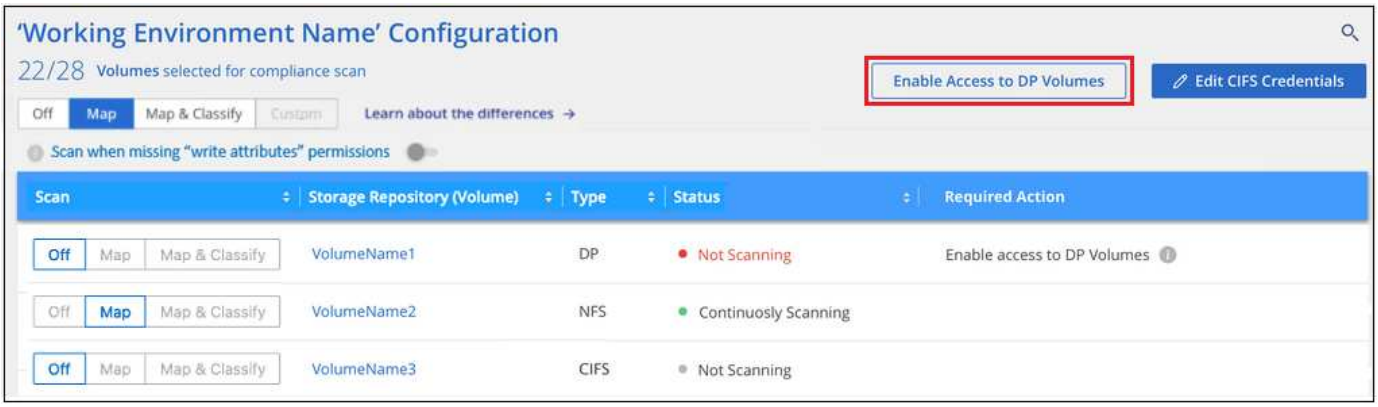
Resultado

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 .

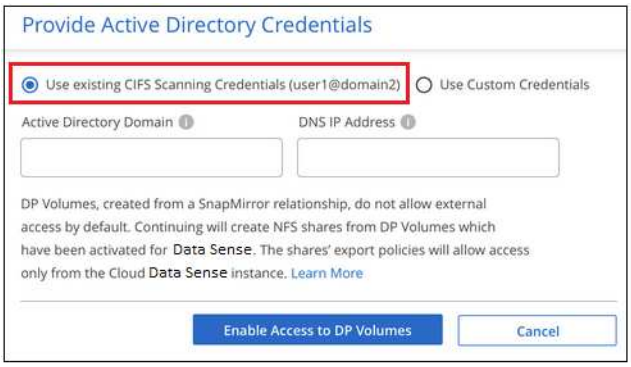
Inicialmente, a lista de volumes identifica esses volumes como *Tipo* **DP** com o *Status* **Não digitalizando** e a *Ação necessária* **Habilitar acesso a volumes DP**.

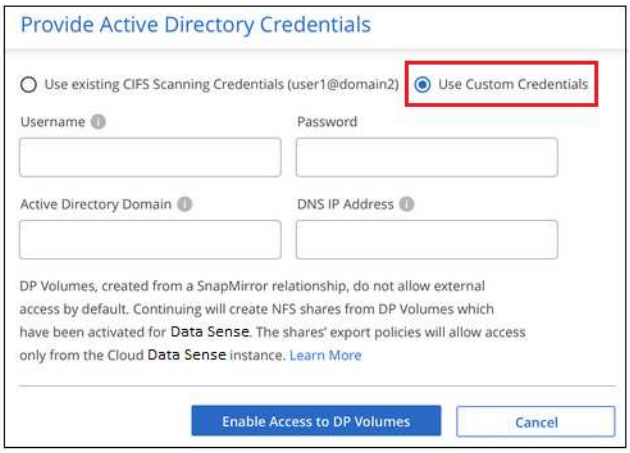


Passos

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**.

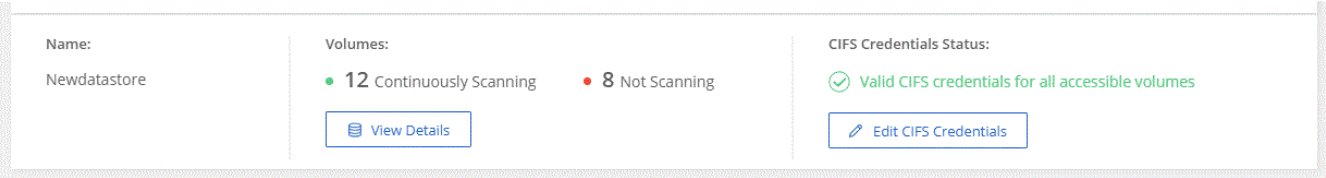
   a. Se você estiver usando CIFS (SMB), verifique se as credenciais do Active Directory estão corretas. Para cada sistema, selecione **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Data Classification precisa para acessar os volumes CIFS no sistema.

      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.

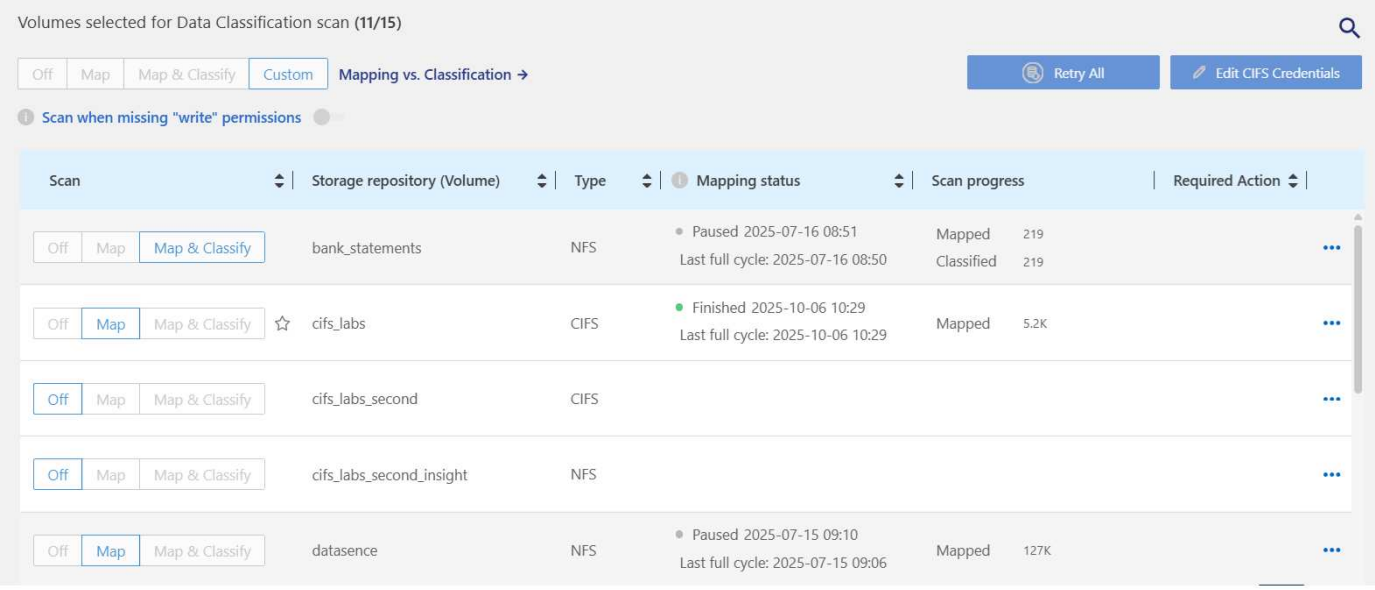
Habilitar ou desabilitar verificações em volumes

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

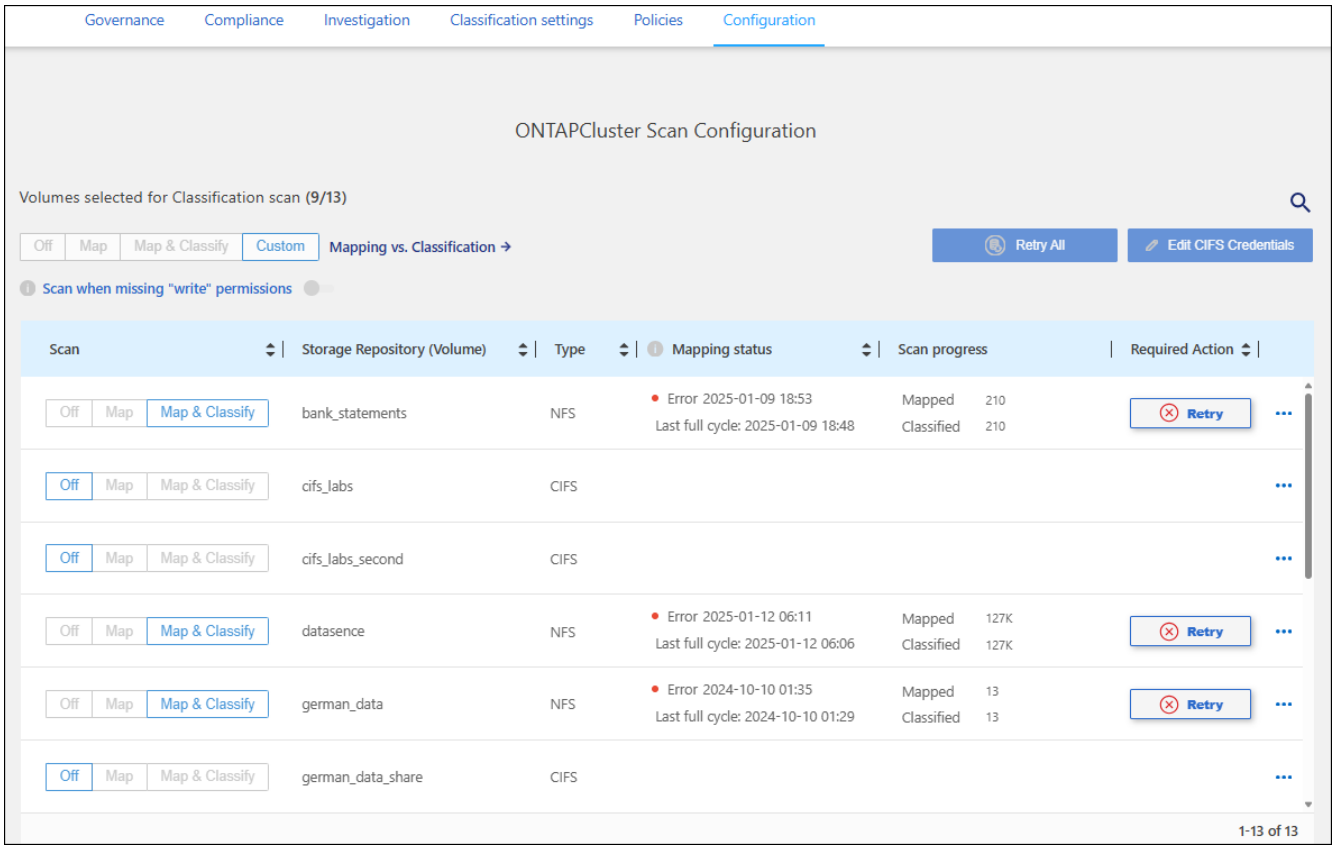
- Certifique-se de que haja uma conexão de rede entre a instância de Classificação de Dados e cada rede que inclua volumes para clusters Cloud Volumes ONTAP ou ONTAP locais.
- Certifique-se de que o grupo de segurança do Cloud Volumes ONTAP permita tráfego de entrada da instância de Classificação de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

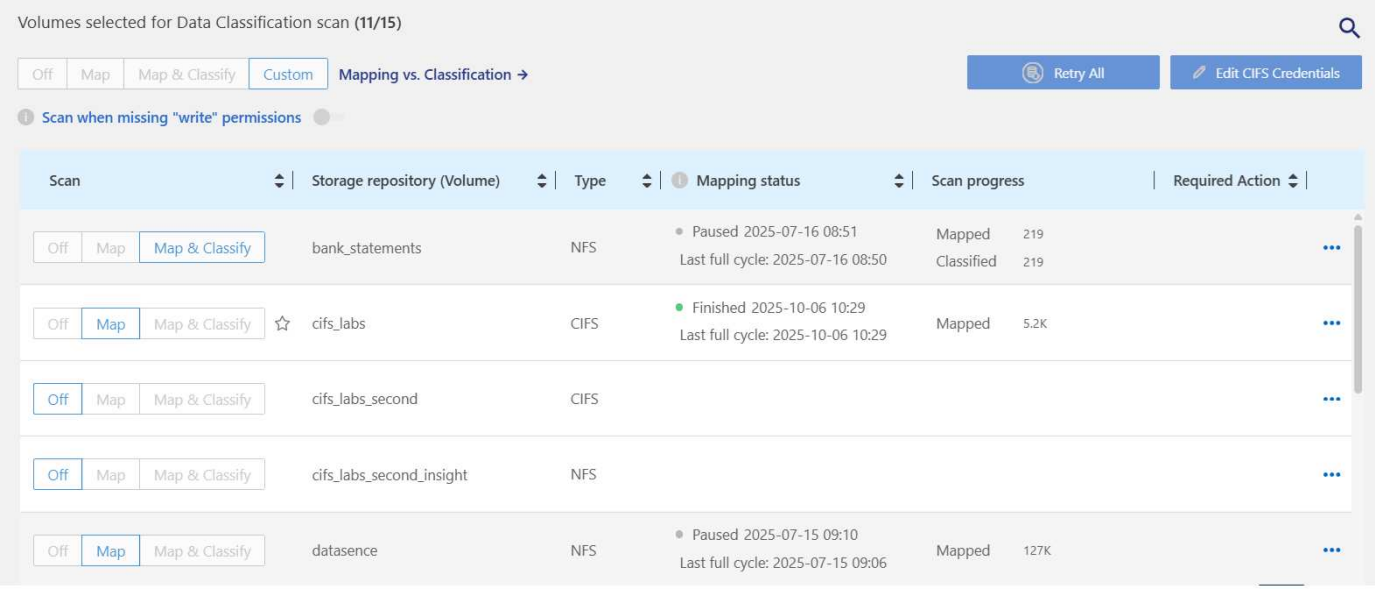
Habilitar ou desabilitar verificações em volumes

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.

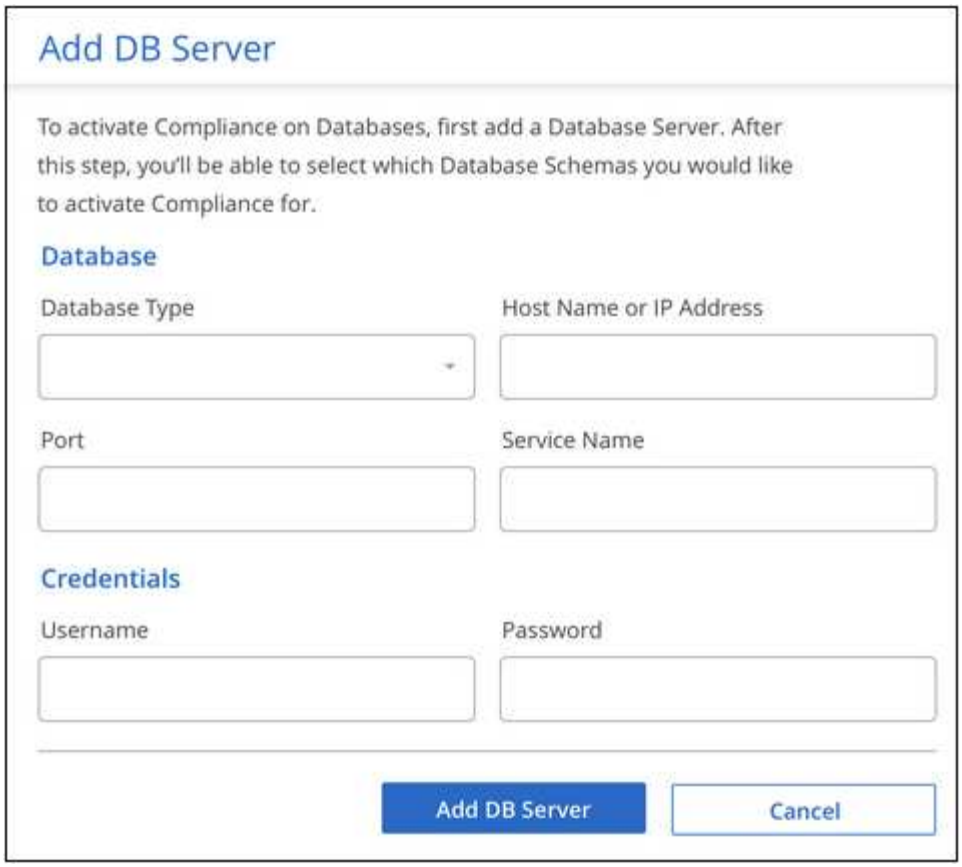
Se você estiver escaneando esquemas de banco de dados que podem ser acessados pela Internet, você pode"implementar a Classificação de Dados na nuvem" ou"implementar a Classificação de Dados em um local local com acesso à Internet" .

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.

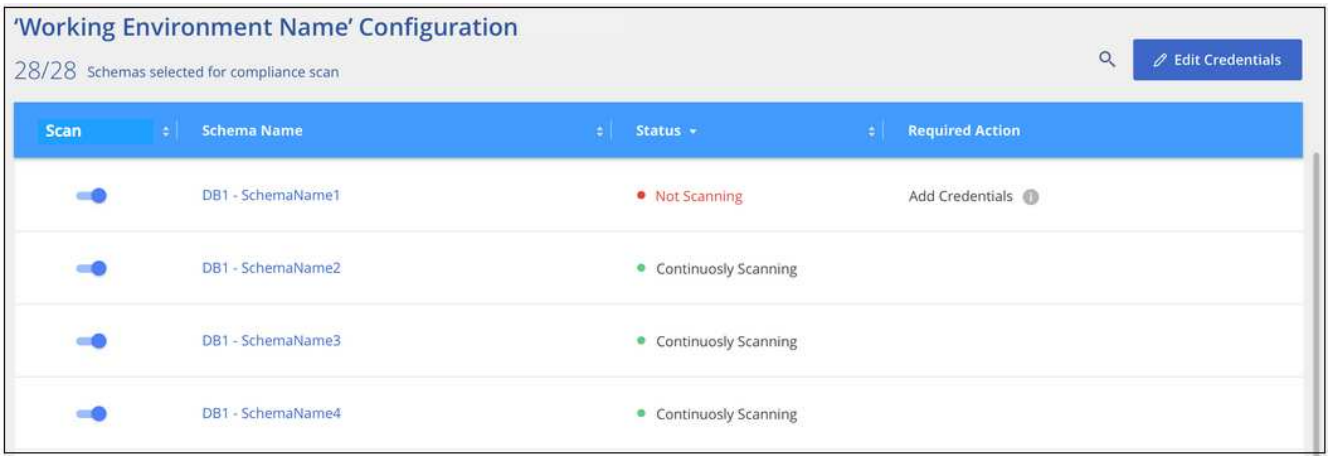
Habilitar e desabilitar varreduras em esquemas de banco de dados

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

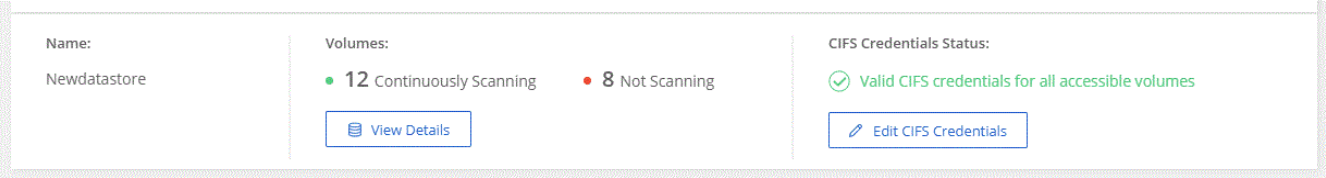
1. No menu Classificação de Dados, selecione **Configuração**.

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.

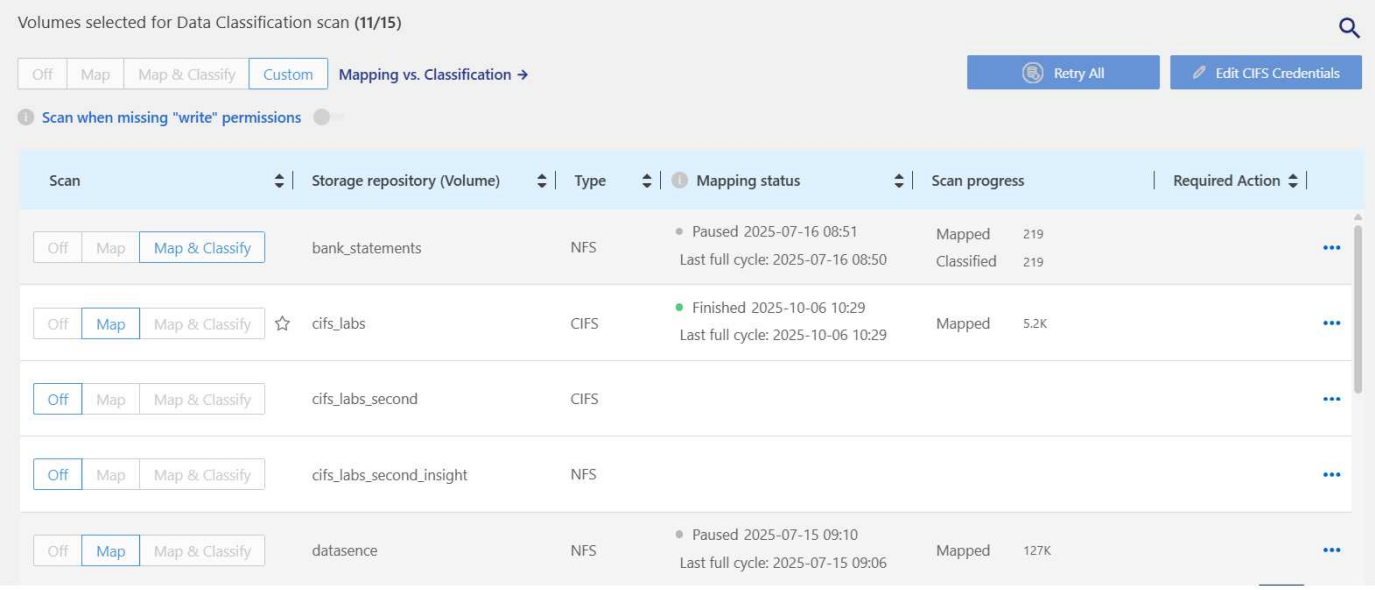
Habilitar e desabilitar verificações em volumes

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.

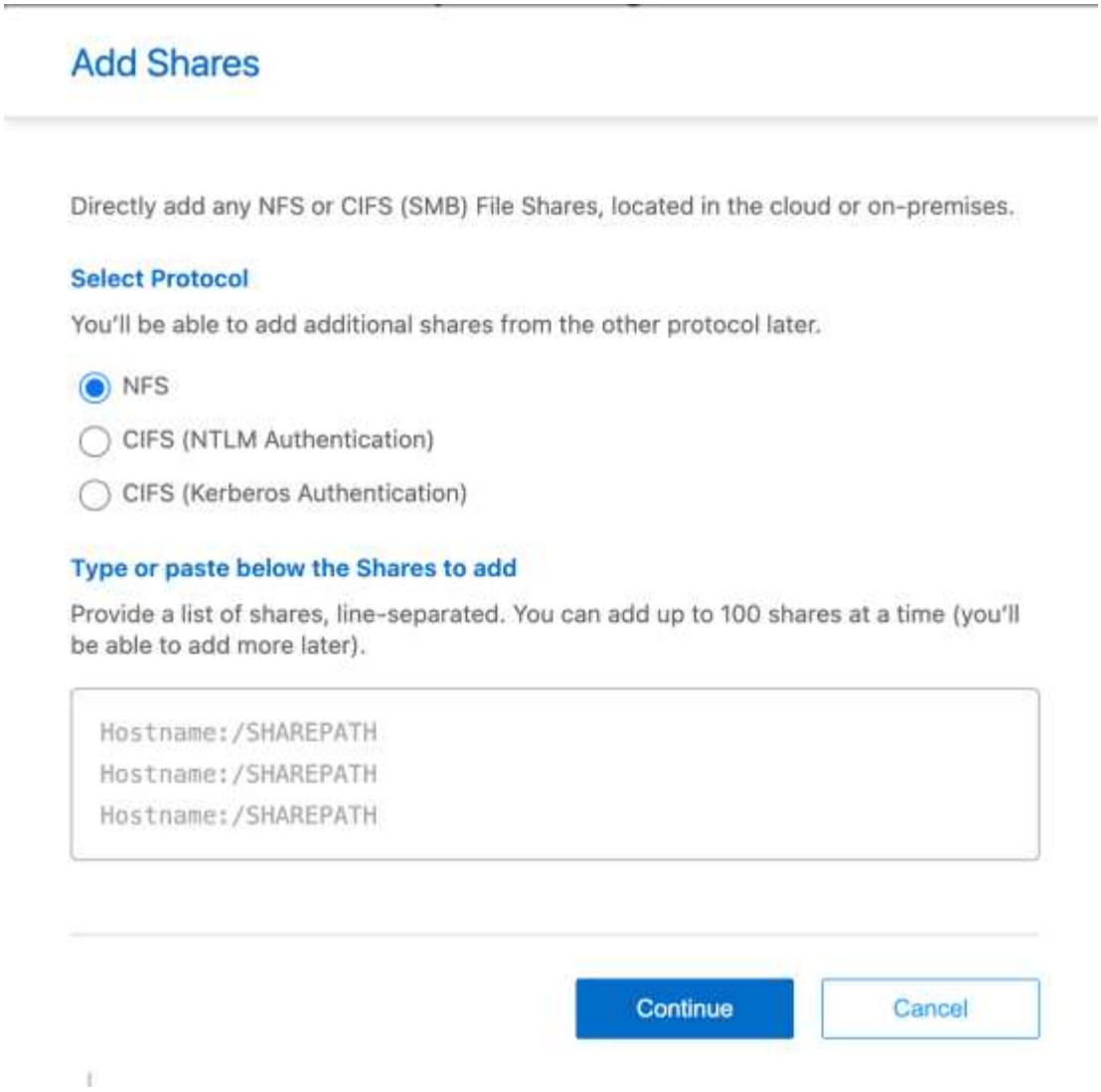
Criar um grupo de compartilhamentos de arquivos

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.

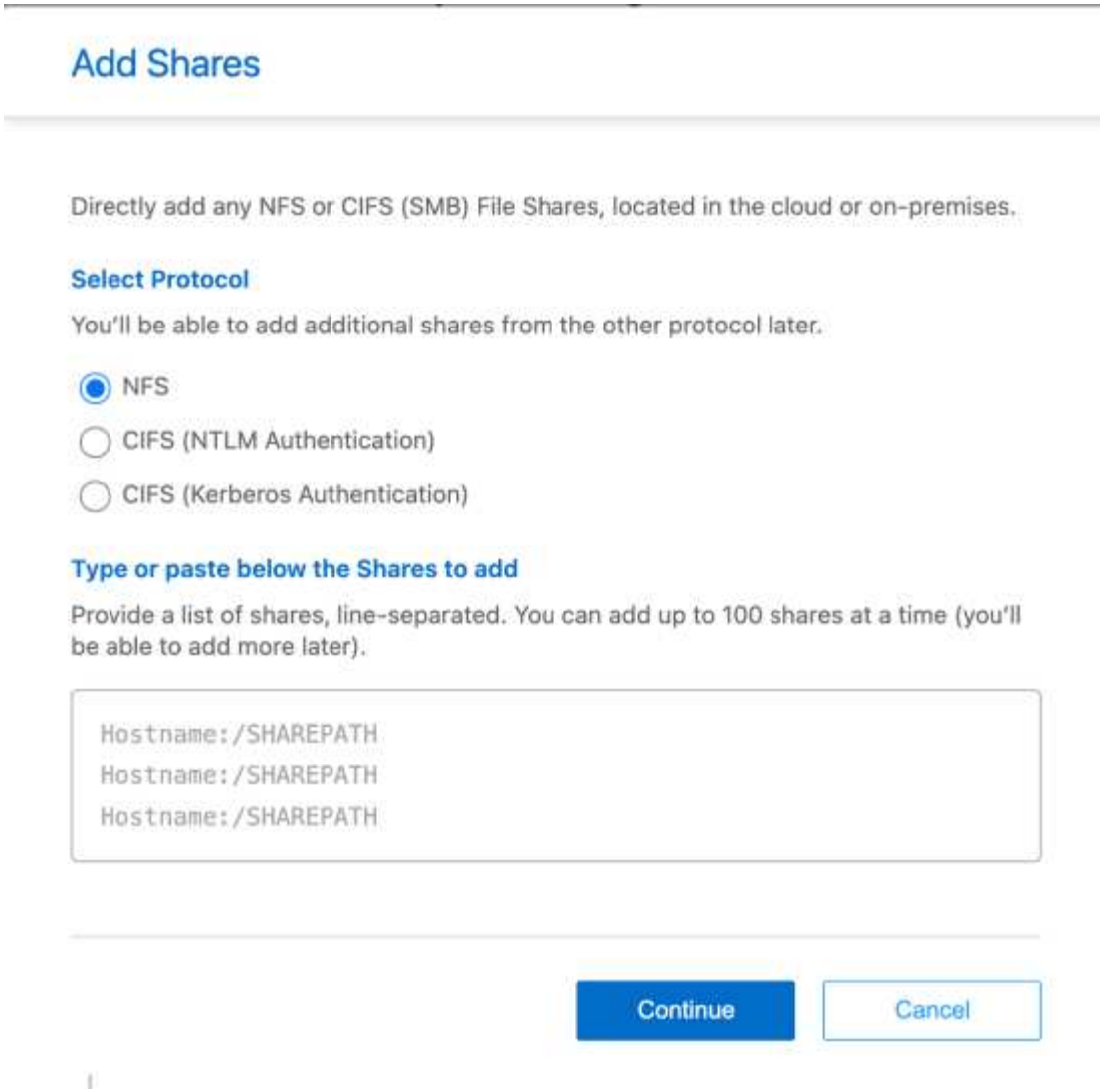
Editar a configuração do protocolo CIFS

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" .

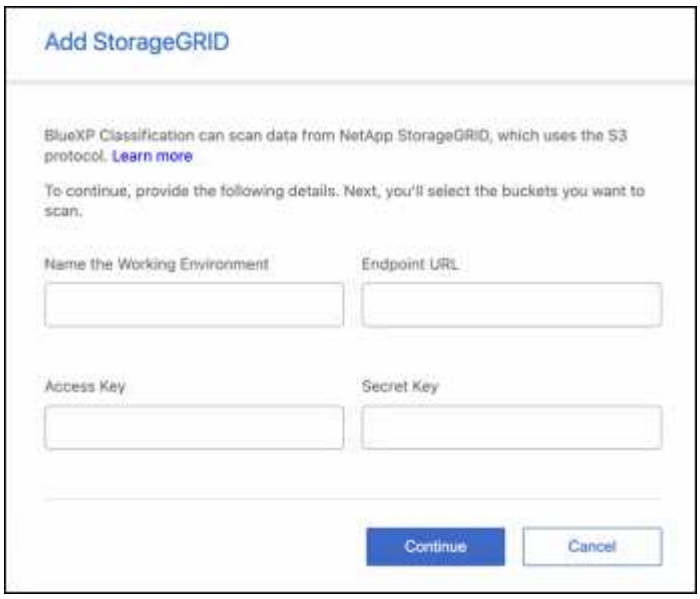
Se você estiver digitalizando dados do StorageGRID que foi instalado em um site escuro sem acesso à Internet, será necessário"implementar a Classificação de Dados no mesmo local que não tem acesso à Internet" . Isso também requer que o agente do Console seja implantado no mesmo local.

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:

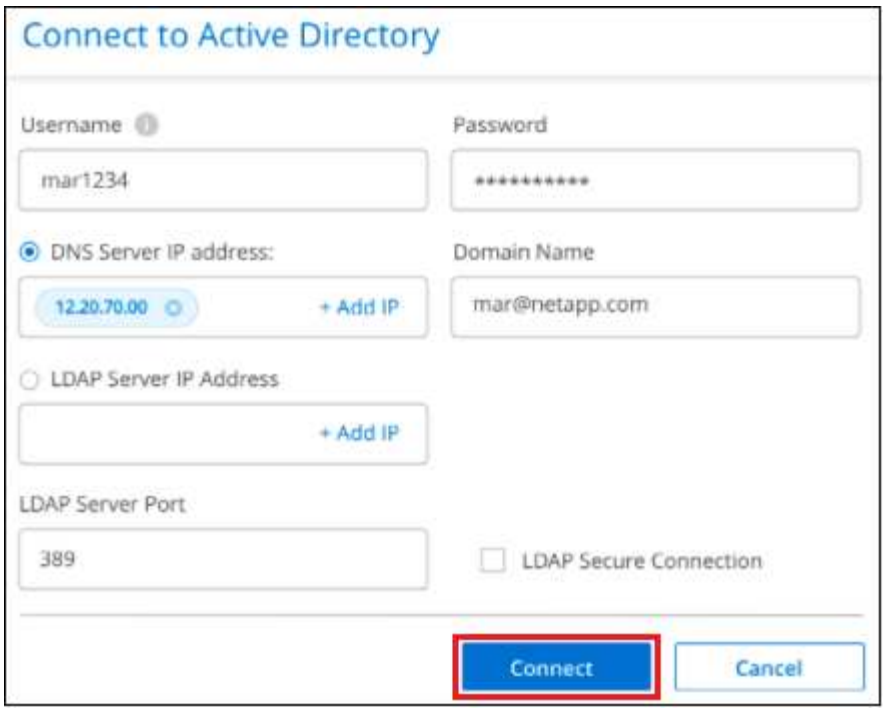
Protocolo	Porta	Destino	Propósito
TCP e UDP	389	Diretório ativo	LDAP
TCP	636	Diretório ativo	LDAP sobre SSL
TCP	3268	Diretório ativo	Catálogo Global
TCP	3269	Diretório ativo	Catálogo global sobre SSL

Passos

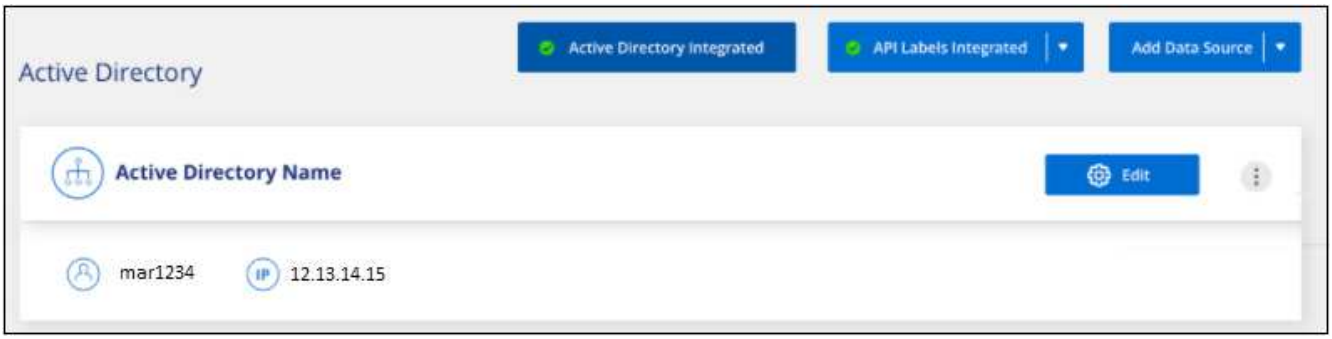
1. Na página Configuração de Classificação de Dados, clique em **Adicionar Active Directory**.

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**.

Classificação de dados de uso

Visualize detalhes de governança sobre os dados armazenados em sua organização com a NetApp Data Classification

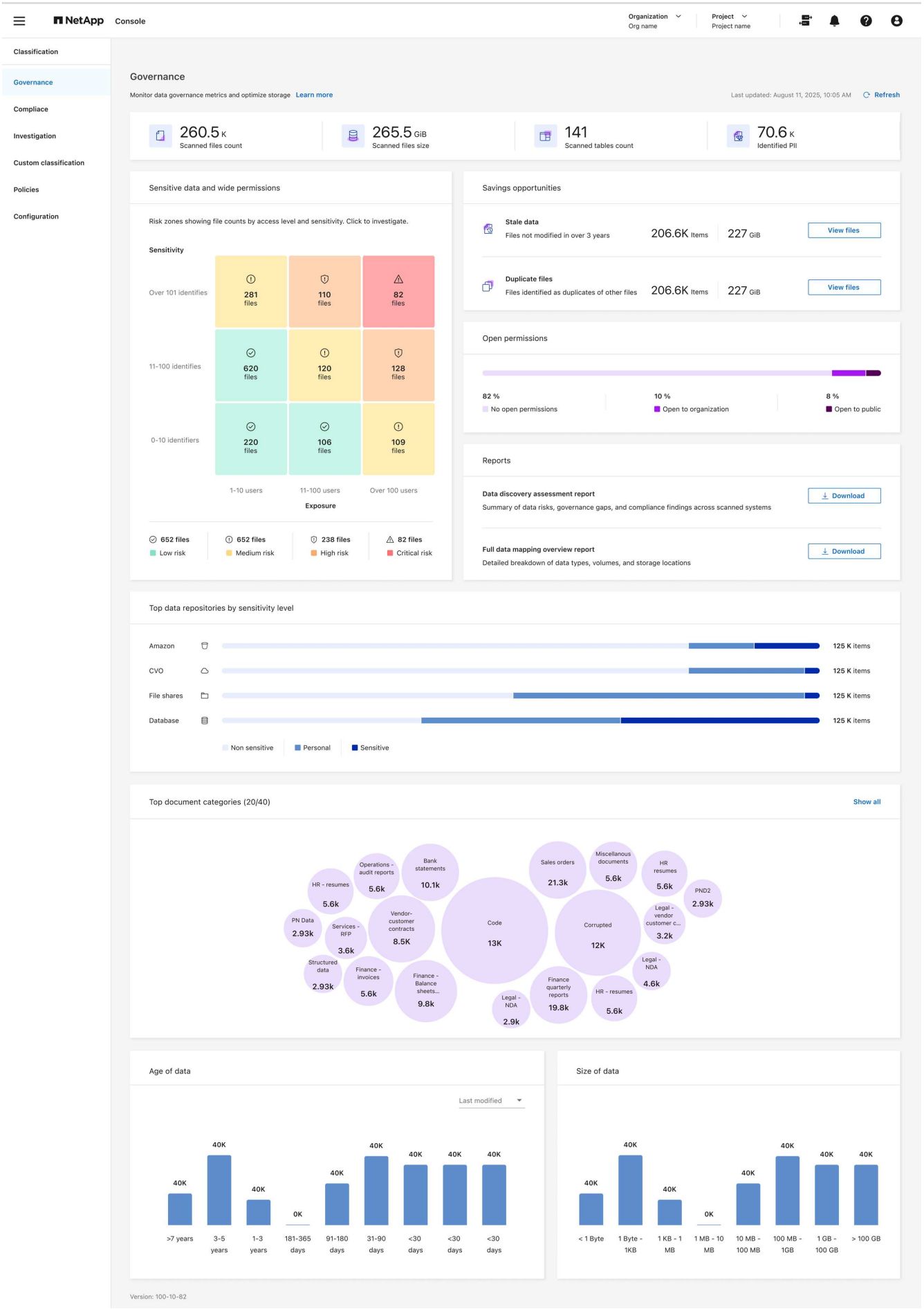
Obtenha controle dos custos relacionados aos dados nos recursos de armazenamento da sua organização. A NetApp Data Classification identifica a quantidade de dados obsoletos, arquivos duplicados e arquivos muito grandes em seus sistemas para que você possa decidir se deseja remover ou colocar alguns arquivos em um armazenamento de objetos mais barato.

É aqui que você deve começar sua pesquisa. No painel de Governança, você pode selecionar uma área para investigação mais aprofundada.

Além disso, se você estiver planejando migrar dados de locais locais para a nuvem, poderá visualizar o tamanho dos dados e se algum deles contém informações confidenciais antes de movê-los.

Revise o painel de governança

O painel de governança fornece informações para que você possa aumentar a eficiência e controlar os custos relacionados aos dados armazenados em seus recursos de armazenamento.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

Passos

1. No menu do NetApp Console , selecione **Governança > Classificação**.
2. Selecione **Governança**.

   O painel de governança é exibido.

Revisar oportunidades de economia

O componente *Oportunidades de economia* mostra dados que você pode excluir ou colocar em um armazenamento de objetos mais barato. Os dados em *Oportunidades de Economia* são atualizados a cada 2 horas. Você também pode atualizar os dados manualmente.

Passos

1. No menu Classificação de Dados, selecione **Governança**.
2. Em cada bloco Oportunidades de economia do painel Governança, selecione **Otimizar armazenamento** para visualizar os resultados filtrados na página Investigação. Para descobrir quaisquer dados que você deve excluir ou transferir para um armazenamento mais barato, investigue as *Oportunidades de economia*.
   - **Dados obsoletos** - Por padrão, os dados são considerados obsoletos se a última modificação ocorreu há mais de 3 anos. Você pode [personalizar a definição de dados obsoletos](task-stale-data.html).
   - **Arquivos duplicados** - Arquivos que são duplicados em outros locais nas fontes de dados que você está digitalizando. "Veja quais tipos de arquivos duplicados são exibidos" .

Se alguma de suas fontes de dados implementar a hierarquização de dados, os dados antigos que já residem no armazenamento de objetos poderão ser identificados na categoria *Dados Obsoletos*.

Crie o relatório de avaliação de descoberta de dados

O relatório de avaliação de descoberta de dados fornece uma análise de alto nível do ambiente escaneado para mostrar áreas de preocupação e possíveis etapas de correção. Os resultados são baseados no mapeamento e na classificação dos seus dados. O objetivo deste relatório é conscientizar sobre três aspectos significativos do seu conjunto de dados:

Recurso	Descrição
Preocupações com a governança de dados	Uma imagem detalhada de todos os dados que você possui e áreas onde você pode reduzir a quantidade de dados para economizar custos.
Exposições de segurança de dados	Áreas onde seus dados podem ser acessados por ataques internos ou externos devido a amplas permissões de acesso.
Lacunas de conformidade de dados	Onde suas informações pessoais ou pessoais confidenciais estão localizadas, tanto para segurança quanto para DSARs (solicitações de acesso do titular dos dados).

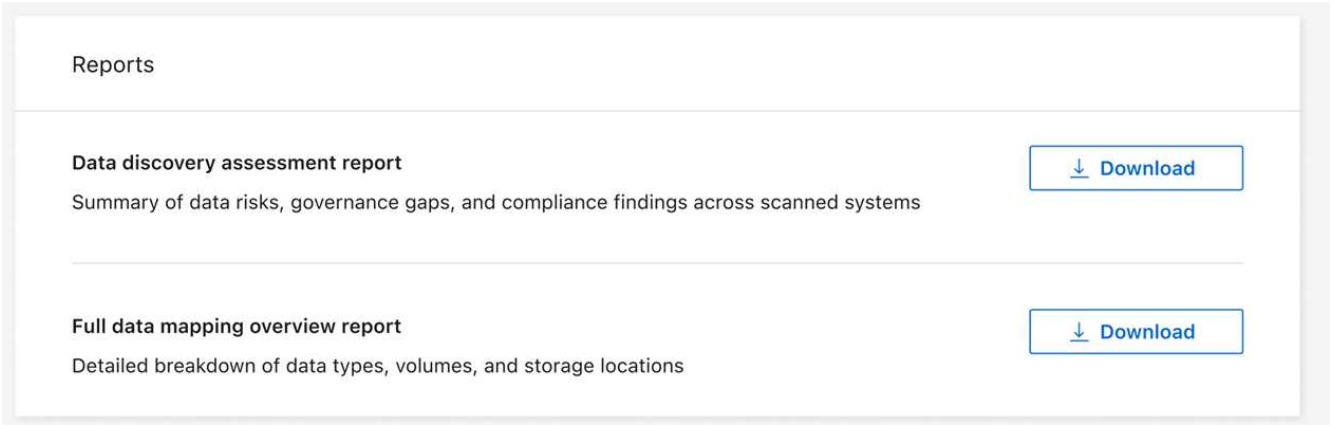
Com o relatório, você pode realizar as seguintes ações:

- Reduza os custos de armazenamento alterando sua política de retenção ou movendo ou excluindo determinados dados (dados obsoletos ou duplicados).
- Proteja seus dados com permissões amplas revisando as políticas globais de gerenciamento de grupos.

- Proteja seus dados que contêm informações pessoais ou confidenciais movendo PII para armazenamentos de dados mais seguros.

Passos

1. Em Classificação de Dados, selecione **Governança**.
2. No bloco de relatórios, selecione **Relatório de avaliação de descoberta de dados**.



Resultado

A Classificação de Dados gera um relatório em PDF que você pode revisar e compartilhar.

Crie o relatório de visão geral do mapeamento de dados

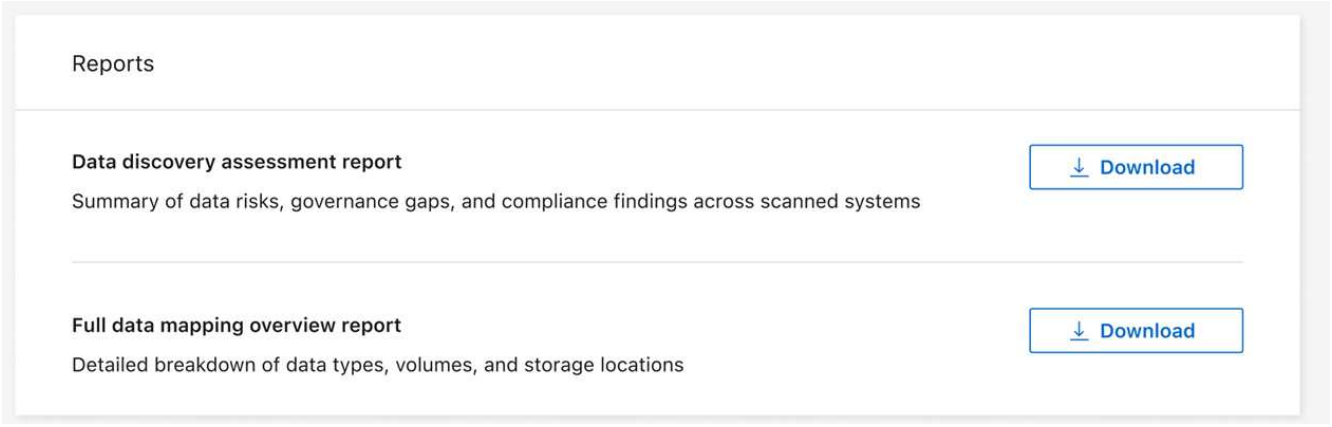
O relatório de visão geral do mapeamento de dados fornece uma visão geral dos dados armazenados em suas fontes de dados corporativos para ajudar você com decisões de migração, backup, segurança e processos de conformidade. O relatório resume todos os sistemas e fontes de dados. Ele também fornece uma análise para cada sistema.

O relatório inclui as seguintes informações:

Categoria	Descrição
Capacidade de uso	Para todos os sistemas: Lista o número de arquivos e a capacidade usada para cada sistema. Para sistemas únicos: lista os arquivos que estão usando mais capacidade.
Era dos Dados	Fornece três tabelas e gráficos para quando os arquivos foram criados, modificados pela última vez ou acessados pela última vez. Lista o número de arquivos e sua capacidade utilizada, com base em determinados intervalos de datas.
Tamanho dos dados	Lista o número de arquivos que existem dentro de determinados intervalos de tamanho em seus sistemas.

Passos

1. Em Classificação de Dados, selecione **Governança**.
2. No bloco de relatórios, selecione **Relatório de visão geral do mapeamento de dados completo**.



Resultado

A Classificação de Dados gera um relatório em PDF que você pode revisar e enviar a outros grupos, conforme necessário.

Se o relatório for maior que 1 MB, o arquivo PDF será retido na instância de Classificação de Dados e você verá uma mensagem pop-up sobre o local exato. Quando o Data Classification estiver instalado em uma máquina Linux em suas instalações ou em uma máquina Linux implantada na nuvem, você poderá navegar diretamente para o arquivo PDF. Quando a Classificação de Dados é implantada na nuvem, você precisa autorizar com SSH a instância da Classificação de Dados para baixar o arquivo PDF.

Revise os principais repositórios de dados listados por sensibilidade de dados

A área *Principais repositórios de dados por nível de sensibilidade* do relatório Visão geral do mapeamento de dados lista os quatro principais repositórios de dados (sistemas e fontes de dados) que contêm os itens mais sensíveis. O gráfico de barras para cada sistema é dividido em:

- Dados não sensíveis
- Dados pessoais
- Dados pessoais sensíveis

Esses dados são atualizados a cada duas horas e podem ser atualizados manualmente.

Passos

1. Para ver o número total de itens em cada categoria, posicione o cursor sobre cada seção da barra.
2. Para filtrar os resultados que aparecerão na página Investigação, selecione cada área na barra e investigue mais.

Revise dados confidenciais e permissões amplas

A área *Dados confidenciais e permissões amplas* do painel Governança mostra as contagens de arquivos que contêm dados confidenciais e têm permissões amplas. A tabela mostra os seguintes tipos de permissões:

- Das permissões mais restritivas às restrições mais permissivas no eixo horizontal.
- Dos dados menos sensíveis aos dados mais sensíveis no eixo vertical.

Passos

1. Para ver o número total de arquivos em cada categoria, posicione o cursor sobre cada caixa.
2. Para filtrar os resultados que aparecerão na página Investigação, selecione uma caixa e investigue mais.

Revisar dados listados por tipos de permissões abertas

A área *Permissões abertas* do relatório Visão geral do mapeamento de dados mostra a porcentagem para cada tipo de permissão que existe para todos os arquivos que estão sendo verificados. O gráfico mostra os seguintes tipos de permissões:

- Sem permissões abertas
- Aberto à organização
- Aberto ao público
- Acesso desconhecido

Passos

1. Para ver o número total de arquivos em cada categoria, posicione o cursor sobre cada caixa.
2. Para filtrar os resultados que aparecerão na página Investigação, selecione uma caixa e investigue mais.

Revise a idade e o tamanho dos dados

Você pode investigar os itens nos gráficos *Idade* e *Tamanho* do relatório Visão geral do mapeamento de dados para ver se há algum dado que você deve excluir ou colocar em um armazenamento de objetos mais barato.

Passos

1. No gráfico Idade dos Dados, para ver detalhes sobre a idade dos dados, posicione o cursor sobre um ponto no gráfico.
2. Para filtrar por faixa etária ou tamanho, selecione essa idade ou tamanho.
    - **Gráfico de idade dos dados** - categoriza os dados com base na hora em que foram criados, na última vez em que foram acessados ou na última vez em que foram modificados.
    - **Gráfico de tamanho de dados** - categoriza os dados com base no tamanho.

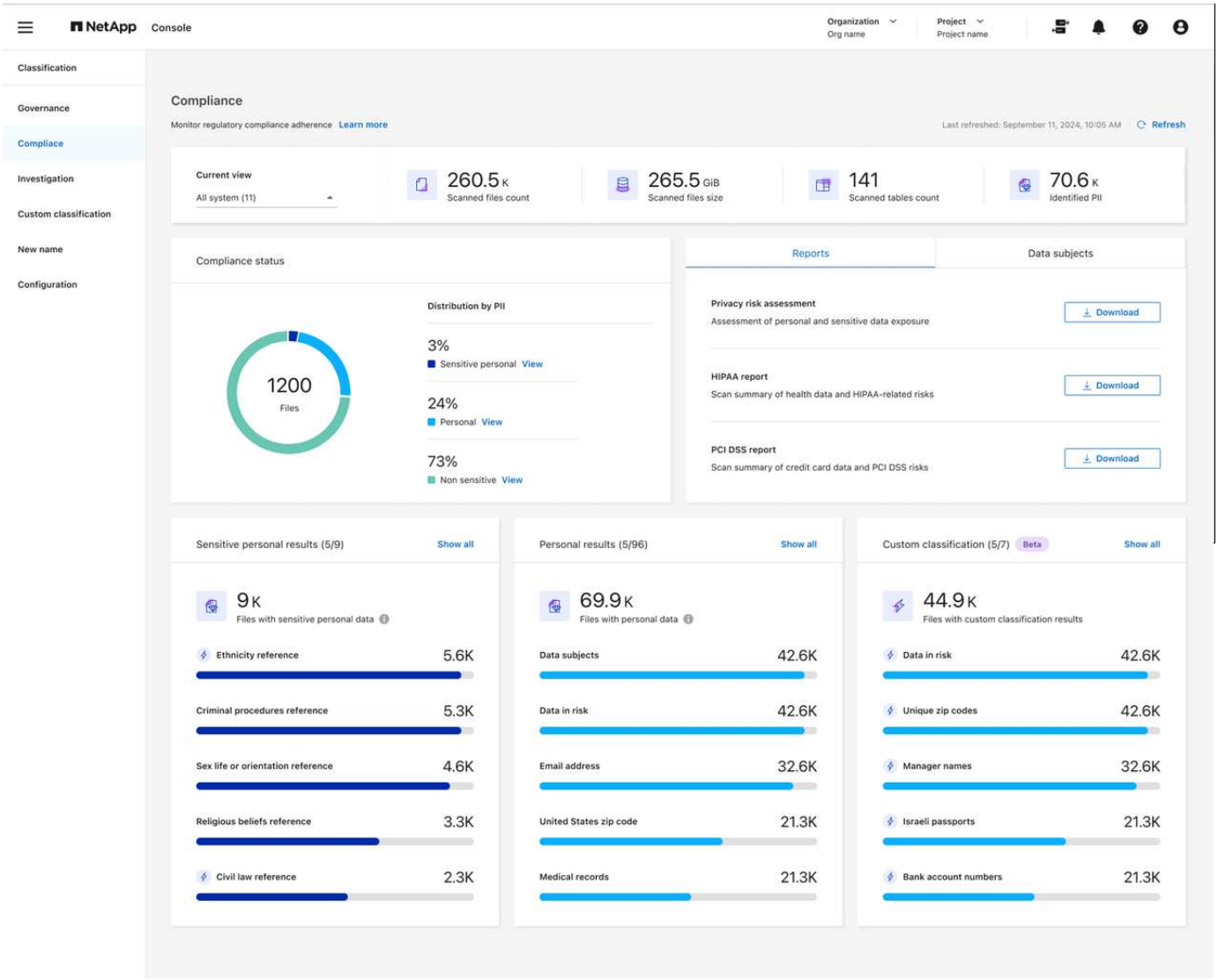
Se alguma de suas fontes de dados implementar a hierarquização de dados, dados antigos que já residem no armazenamento de objetos poderão ser identificados no gráfico *Idade dos Dados*.

Veja detalhes de conformidade sobre os dados privados armazenados em sua organização com a NetApp Data Classification

Obtenha controle dos seus dados privados visualizando detalhes sobre os dados pessoais (PII) e dados pessoais sensíveis (SPII) na sua organização. Você também pode obter visibilidade revisando as categorias e os tipos de arquivo que o NetApp Data Classification encontrou em seus dados.

Os detalhes de conformidade no nível do arquivo só estarão disponíveis se você executar uma verificação de classificação completa. As varreduras somente de mapeamento não produzem detalhes no nível do arquivo.

Por padrão, o painel Classificação de Dados exibe dados de conformidade para todos os sistemas e bancos de dados. Para ver dados de apenas alguns sistemas, selecione-os.



Você pode filtrar os resultados na página Investigação de Dados e baixar um relatório dos resultados como um arquivo CSV. Ver"Filtrando dados na página Investigação de Dados" para mais detalhes.

Ver arquivos que contêm dados pessoais

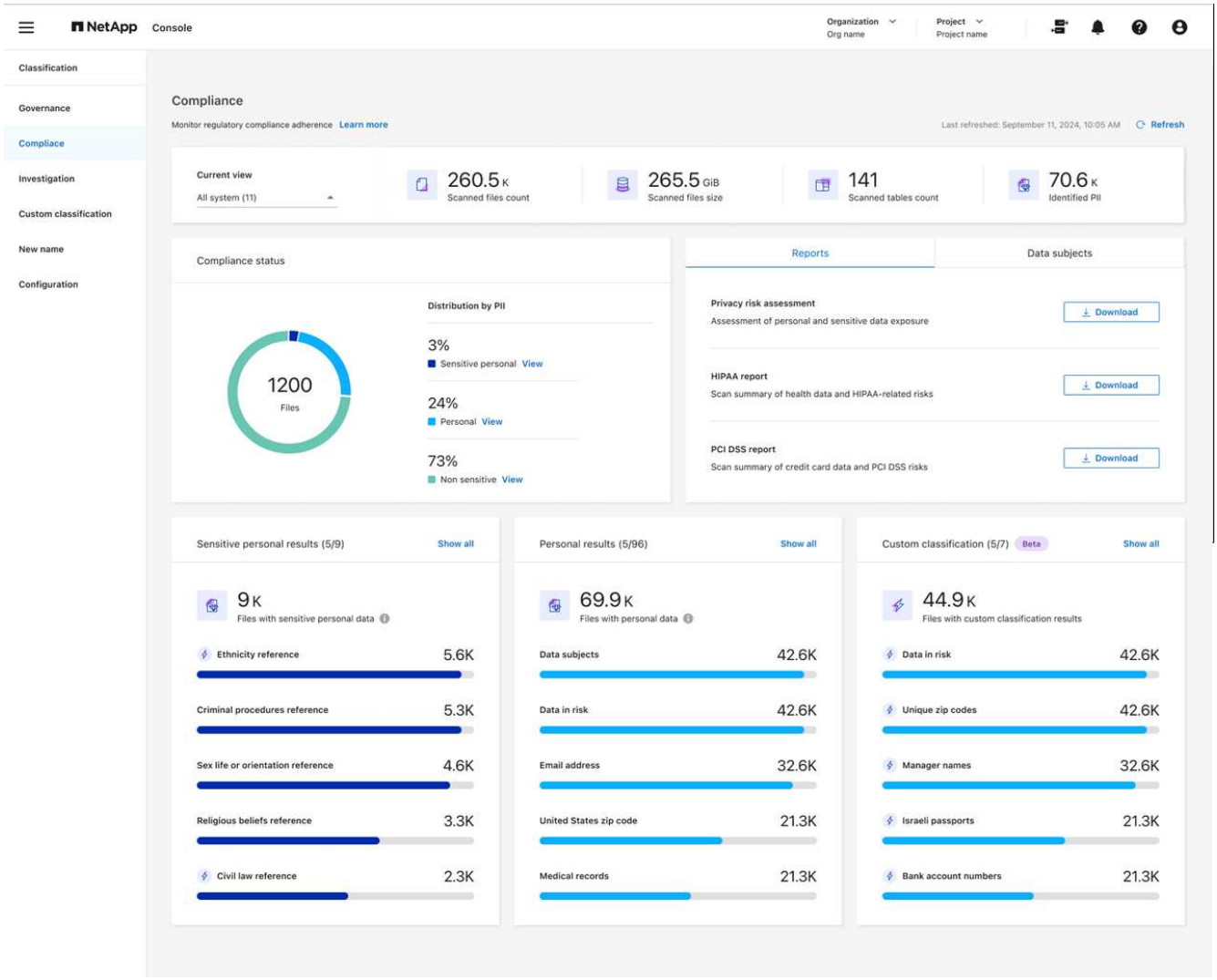
A Classificação de Dados identifica automaticamente palavras, strings e padrões específicos (Regex) dentro dos dados. "Por exemplo, números de cartão de crédito, números de previdência social, números de contas bancárias, senhas e muito mais."A Classificação de Dados identifica esse tipo de informação em arquivos individuais, em arquivos dentro de diretórios (compartilhamentos e pastas) e em tabelas de banco de dados.

Você também pode criar termos de pesquisa personalizados para identificar dados pessoais específicos da sua organização. Para obter mais informações, consulte "Crie uma classificação personalizada" .

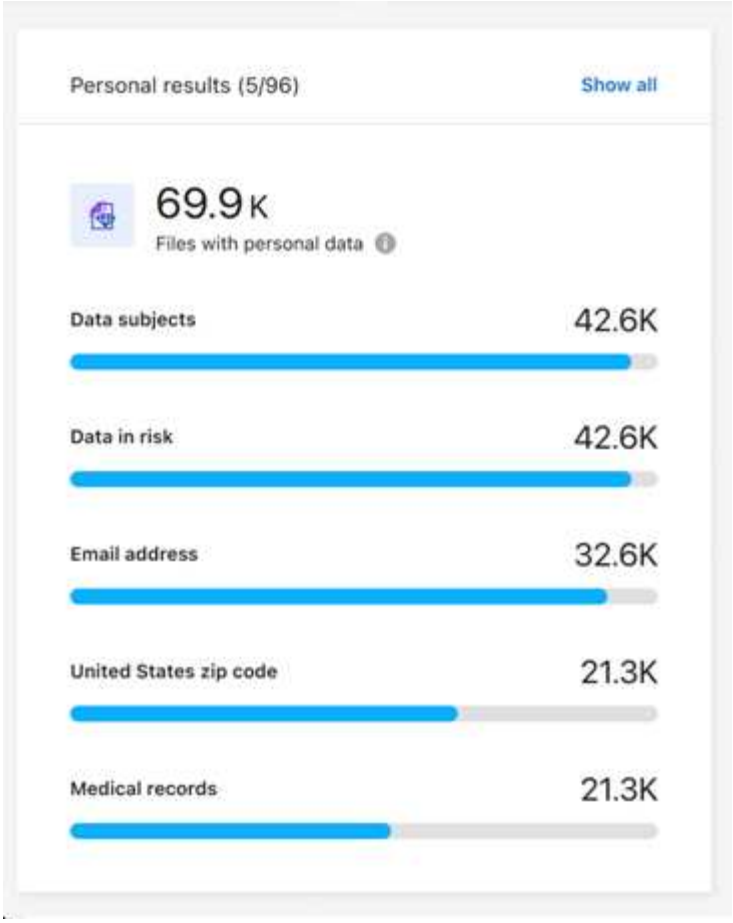
Para alguns tipos de dados pessoais, a Classificação de Dados usa *validação de proximidade* para validar suas descobertas. A validação ocorre pela busca de uma ou mais palavras-chave predefinidas próximas aos dados pessoais encontrados. Por exemplo, a Classificação de Dados identifica um número de previdência social (SSN) dos EUA como um SSN se vir uma palavra de proximidade ao lado dele — por exemplo, *SSN* ou *social security*. "A tabela de dados pessoais" mostra quando a Classificação de Dados usa validação de proximidade.

Passos

1. No menu Classificação de Dados, selecione a aba **Conformidade**.
2. Para investigar os detalhes de todos os dados pessoais, selecione o ícone ao lado da porcentagem de dados pessoais.

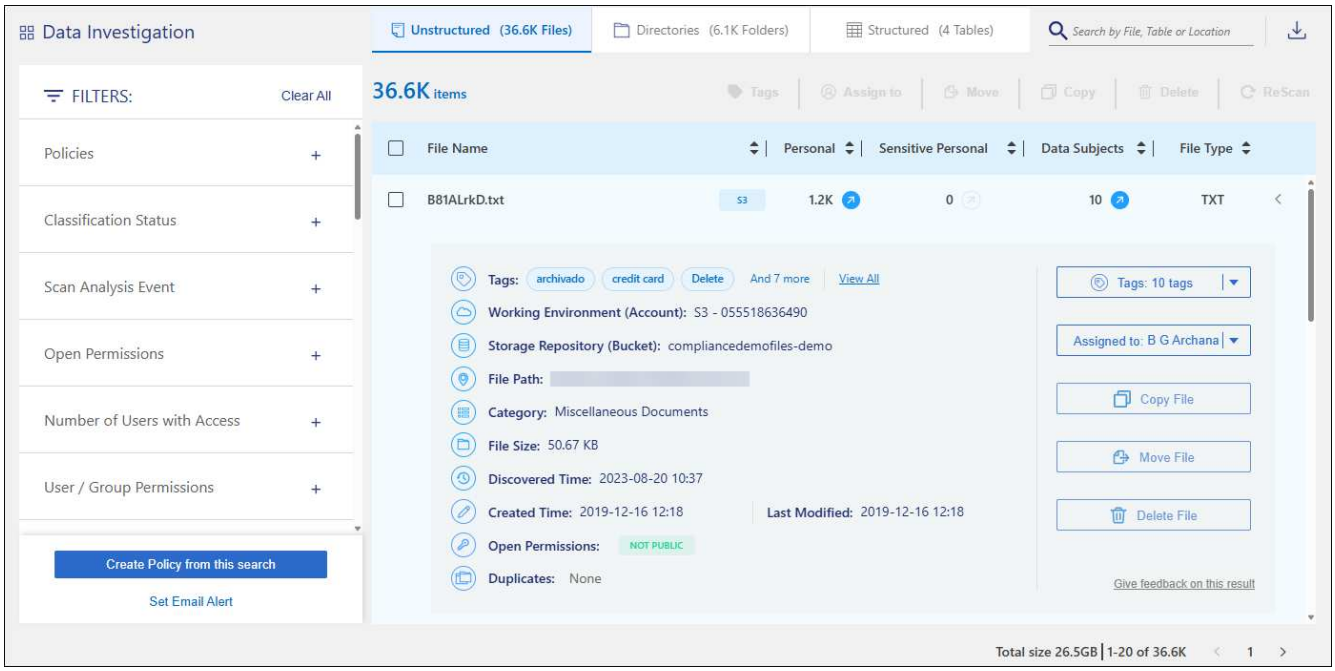


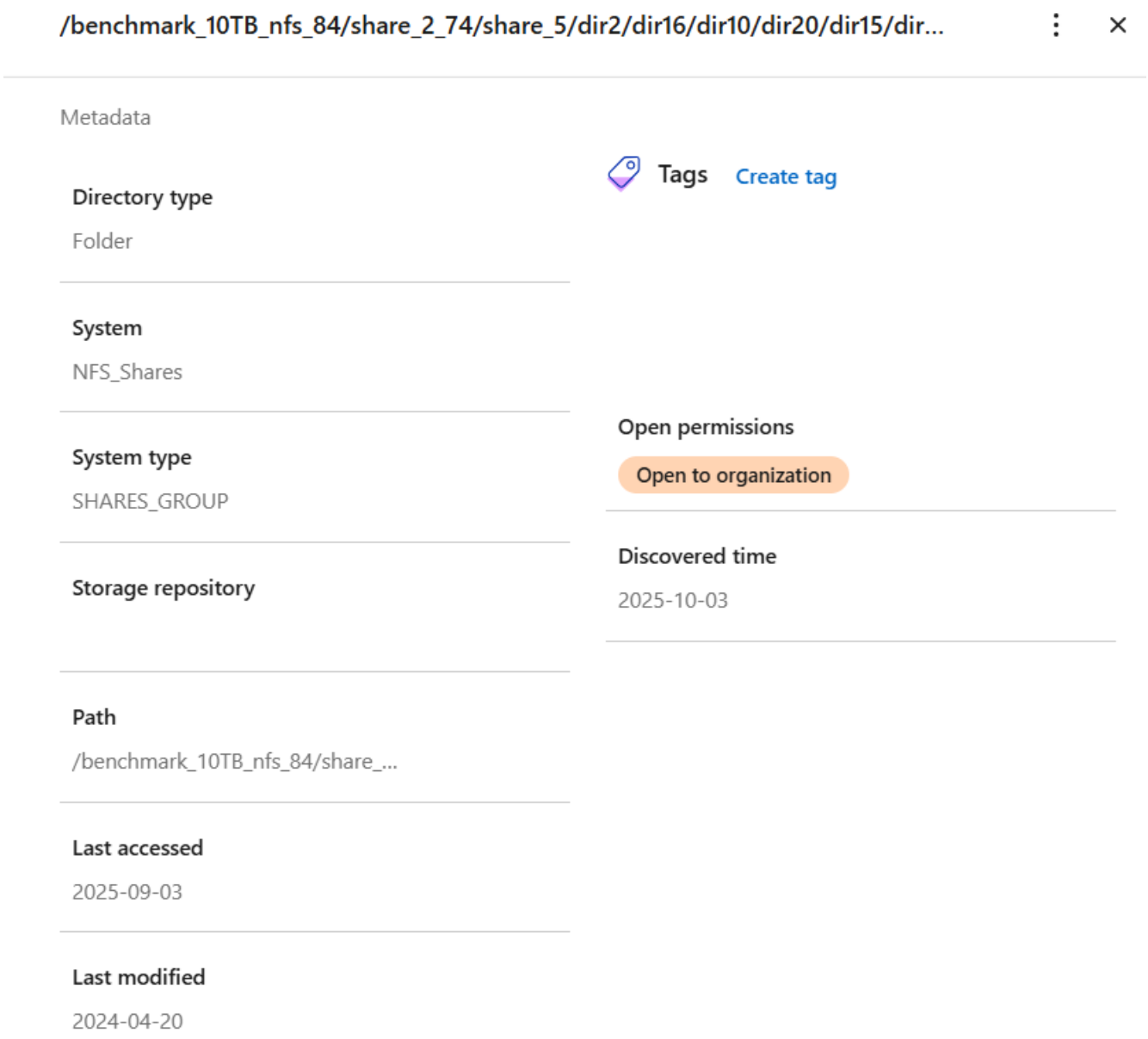
3. Para investigar os detalhes de um tipo específico de dados pessoais, selecione **Exibir tudo** e, em seguida, selecione o ícone de seta **Investigar resultados** para um tipo específico de dados pessoais, por exemplo, endereços de e-mail.



4. Investigue os dados pesquisando, classificando e expandindo detalhes de um arquivo específico, selecionando a seta **Investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

   As imagens a seguir mostram dados pessoais encontrados em um diretório (compartilhamentos e pastas). Na aba **Estruturado**, você visualiza dados pessoais encontrados em bancos de dados. Na aba **Não estruturado**, você pode visualizar dados em nível de arquivo.


Data Investigation
Unstructured (36.6K Files)
Directories (6.1K Folders)
Structured (4 Tables)
Search by File, Table or Location
FILTERS:
Clear All
Policies
Classification Status
Scan Analysis Event
Open Permissions
Number of Users with Access
User / Group Permissions
Create Policy from this search
Set Email Alert
36.6K items
Tags
Assign to
Move
Copy
Delete
ReScan
File Name
Personal
Sensitive Personal
Data Subjects
File Type
B81ALrkD.txt
S3
1.2K
0
10
TXT
Tags: archivado credit card Delete And 7 more View All
Working Environment (Account): S3 - 055518636490
Storage Repository (Bucket): compliancedemofiles-demo
File Path:
Category: Miscellaneous Documents
File Size: 50.67 KB
Discovered Time: 2023-08-20 10:37
Created Time: 2019-12-16 12:18
Last Modified: 2019-12-16 12:18
Open Permissions: NOT PUBLIC
Duplicates: None
Tags: 10 tags
Assigned to: B G Archana
Copy File
Move File
Delete File
Give feedback on this result
Total size 26.5GB | 1-20 of 36.6K
1



Exibir arquivos que contêm dados pessoais confidenciais

A Classificação de Dados identifica automaticamente tipos especiais de informações pessoais sensíveis, conforme definido por regulamentações de privacidade, como "artigos 9 e 10 do RGPD" . Por exemplo, informações sobre a saúde, origem étnica ou orientação sexual de uma pessoa. "Veja a lista completa" . A Classificação de Dados identifica esse tipo de informação em arquivos individuais, em arquivos dentro de diretórios (compartilhamentos e pastas) e em tabelas de banco de dados.

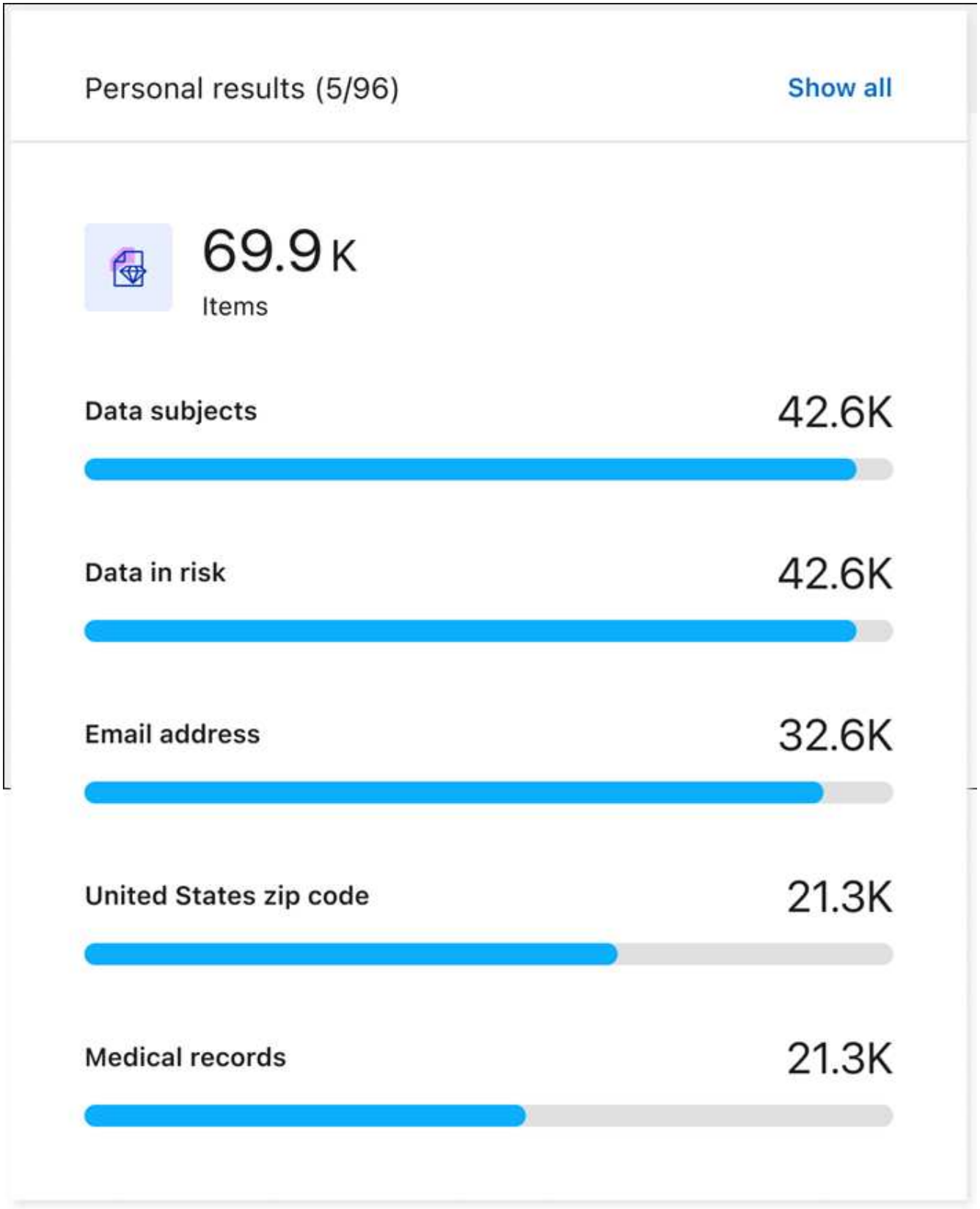
A classificação de dados usa IA, processamento de linguagem natural (PLN), aprendizado de máquina (ML) e computação cognitiva (CC) para entender o significado do conteúdo que ela examina, a fim de extrair entidades e categorizá-lo adequadamente.

Por exemplo, uma categoria de dados sensíveis do GDPR é a origem étnica. Devido às suas capacidades de PNL, a Classificação de Dados pode distinguir a diferença entre uma frase que diz "George é mexicano" (indicando dados sensíveis, conforme especificado no artigo 9 do GDPR) e "George está comendo comida mexicana".

Somente o inglês é suportado na verificação de dados pessoais confidenciais. Suporte para mais idiomas será adicionado posteriormente.

Passos

1. No menu Classificação de Dados, selecione **Conformidade**.
2. Para investigar os detalhes de todos os dados pessoais confidenciais, localize o cartão **Resultados pessoais confidenciais** e selecione **Mostrar tudo**.



.

3. Para investigar os detalhes de um tipo específico de dados pessoais sensíveis, selecione **Exibir tudo** e, em seguida, selecione o ícone de seta **Investigar resultados** para um tipo específico de dados pessoais sensíveis.
4. Investigue os dados pesquisando, classificando, expandindo detalhes de um arquivo específico, clicando

em **Investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

Categorias de dados privados na NetApp Data Classification

Há muitos tipos de dados privados que o NetApp Data Classification pode identificar em seus volumes e bancos de dados.

A Classificação de Dados identifica dois tipos de dados pessoais:

- **Informações de identificação pessoal (PII)**
- **Informações pessoais sensíveis (SPII)**

Se você precisar de Classificação de Dados para identificar outros tipos de dados privados, como números de identificação nacionais adicionais ou identificadores de assistência médica, entre em contato com seu gerente de conta.

Tipos de dados pessoais

Os dados pessoais, ou *informações de identificação pessoal* (PII), encontrados em arquivos podem ser dados pessoais gerais ou identificadores nacionais. A terceira coluna na tabela abaixo identifica se a Classificação de Dados usa"validação de proximidade" para validar suas descobertas para o identificador.

Os idiomas nos quais esses itens podem ser reconhecidos estão identificados na tabela.

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	japonês
Em geral	Número do cartão de crédito	Sim	✓	✓	✓		✓
	Titulares dos dados	Não	✓	✓	✓		
	Endereço de email	Não	✓	✓	✓		✓
	Número IBAN (Número Internacional de Conta Bancária)	Não	✓	✓	✓		✓
	Endereço IP	Não	✓	✓	✓		✓
	Senha	Sim	✓	✓	✓		✓

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	japonês
Identificadores Nacionais							

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	japonês

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	japonês

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	japonês

	Documento de identidade do Reino Unido (NINO)	Sim	✓	✓	✓		
Tipo	**Identificador**	**Validação de Proximidade?**	**Inglês**	**Alemão**	**Espanhol**	**Francês**	**japonês**
	Carteira de Habilitação EUA Califórnia	Sim	✓	✓	✓		
	Carteira de motorista de Indiana nos EUA	Sim	✓	✓	✓		
	Carteira de Habilitação EUA Nova York	Sim	✓	✓	✓		
	Carteira de motorista do Texas nos EUA	Sim	✓	✓	✓		
	Número de Seguro Social dos EUA (SSN)	Sim	✓	✓	✓		

Tipos de dados pessoais sensíveis

A Classificação de Dados pode encontrar as seguintes informações pessoais sensíveis (SPII) em arquivos.

O seguinte SPII atualmente só pode ser reconhecido em inglês:

- **Referência de Procedimentos Criminais**: Dados referentes a condenações e infrações criminais de uma pessoa física.
- **Referência de etnia**: Dados referentes à origem racial ou étnica de uma pessoa física.
- **Referência de saúde**: Dados relativos à saúde de uma pessoa física.
- **Códigos médicos CID-9-CM**: Códigos usados no setor médico e de saúde.
- **Códigos Médicos CID-10-CM**: Códigos usados no setor médico e de saúde.
- **Referência de Crenças Filosóficas**: Dados referentes às crenças filosóficas de uma pessoa natural.
- **Referência de Opiniões Políticas**: Dados relativos às opiniões políticas de uma pessoa física.
- **Referência de Crenças Religiosas**: Dados referentes às crenças religiosas de uma pessoa física.
- **Referência de vida sexual ou orientação**: Dados referentes à vida sexual ou orientação sexual de uma pessoa física.

Tipos de categorias

A Classificação de Dados categoriza seus dados da seguinte maneira.

A maioria dessas categorias pode ser reconhecida em inglês, alemão e espanhol.

Categoria	Tipo	Inglês	Alemão	Espanhol
Financiar	Balanços Patrimoniais	✓	✓	✓
	Ordens de Compra	✓	✓	✓
	Faturas	✓	✓	✓
	Relatórios Trimestrais	✓	✓	✓

Categoria	Tipo	Inglês	Alemão	Espanhol
RH	Verificações de antecedentes	✓		✓
	Planos de Compensação	✓	✓	✓
	Contratos de Funcionários	✓		✓
	Avaliações de funcionários	✓		✓
	Saúde	✓		✓
	Currículos	✓	✓	✓
Jurídico	Acordos de confidencialidade	✓	✓	✓
	Contratos entre fornecedores e clientes	✓	✓	✓
Marketing	Campanhas	✓	✓	✓
	Conferências	✓	✓	✓
Operações	Relatórios de Auditoria	✓	✓	✓
Vendas	Pedidos de Venda	✓	✓	
Serviços	RFI	✓		✓
	RFP	✓		✓
	SEMEAR	✓	✓	✓
	Treinamento	✓	✓	✓
Apoiar	Reclamações e multas	✓	✓	✓

Os seguintes metadados também são categorizados e identificados nos mesmos idiomas suportados:

- Dados do aplicativo
- Arquivos de arquivo
- Áudio
- Breadcrumbs de dados de aplicativos de negócios de classificação de dados
- Arquivos CAD
- Código
- Corrompido
- Arquivos de banco de dados e índice
- Arquivos de design
- Dados do aplicativo de e-mail
- Criptografado (arquivos com alta pontuação de entropia)
- Executáveis
- Dados de aplicação financeira
- Dados de aplicação de saúde

- Imagens
- Registros
- Documentos diversos
- Apresentações diversas
- Planilhas diversas
- Diversos "Desconhecido"
- Arquivos protegidos por senha
- Dados Estruturados
- Vídeos
- Arquivos de zero bytes

Tipos de arquivos

A Classificação de Dados verifica todos os arquivos em busca de insights de categoria e metadados e exibe todos os tipos de arquivo na seção de tipos de arquivo do painel. Quando a Classificação de Dados detecta Informações Pessoais Identificáveis (PII) ou quando realiza uma pesquisa DSAR, somente os seguintes formatos de arquivo são suportados:

`.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides`

Precisão das informações encontradas

A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que a Classificação de Dados identifica. Você deve sempre validar as informações revisando os dados.

Com base em nossos testes, a tabela abaixo mostra a precisão das informações encontradas pela Classificação de Dados. Nós dividimos por *precisão* e *recordação*:

Precisão
: A probabilidade de que o que a Classificação de Dados encontra tenha sido identificado corretamente. Por exemplo, uma taxa de precisão de 90% para dados pessoais significa que 9 em cada 10 arquivos identificados como contendo informações pessoais, na verdade contêm informações pessoais. 1 em cada 10 arquivos seria um falso positivo.

Lembrar
: A probabilidade de a Classificação de Dados encontrar o que deveria. Por exemplo, uma taxa de recall de 70% para dados pessoais significa que a Classificação de Dados pode identificar 7 de 10 arquivos que realmente contêm informações pessoais em sua organização. A classificação de dados perderia 30% dos dados e eles não apareceriam no painel.

Estamos constantemente melhorando a precisão dos nossos resultados. Essas melhorias estarão disponíveis automaticamente em versões futuras do Data Classification.

Tipo	Precisão	Lembrar
Dados pessoais - Geral	90%-95%	60%-80%
Dados pessoais - Identificadores de países	30%-60%	40%-60%

Tipo	Precisão	Lembrar
Dados pessoais sensíveis	80%-95%	20%-30%
Categorias	90%-97%	60%-80%

Crie uma classificação personalizada no NetApp Data Classification

O NetApp Data Classification permite criar categorias personalizadas ou identificadores pessoais para identificar dados específicos de acordo com os requisitos regulamentares e de conformidade da sua organização.

A Classificação de Dados suporta dois tipos de classificadores personalizados: categorias e identificadores pessoais. Categorias personalizadas são criadas com base em um conjunto de arquivos que você carrega, a partir dos quais a Classificação de Dados cria um modelo de IA para identificar dados semelhantes em sua organização (por exemplo, uma empresa de pesquisa na área da saúde pode criar uma categoria de análise clínica). Identificadores pessoais personalizados são criados usando listas de palavras-chave ou uma expressão regular (regex) para identificar informações específicas da sua organização que possam representar um risco de conformidade.

Todas as classificações personalizadas estão disponíveis no painel de controle de classificação personalizada.

Crie um identificador pessoal personalizado.

A Classificação de Dados permite criar um identificador pessoal personalizado usando palavras-chave contextuais ou uma expressão regular para identificar dados exclusivos da sua organização.

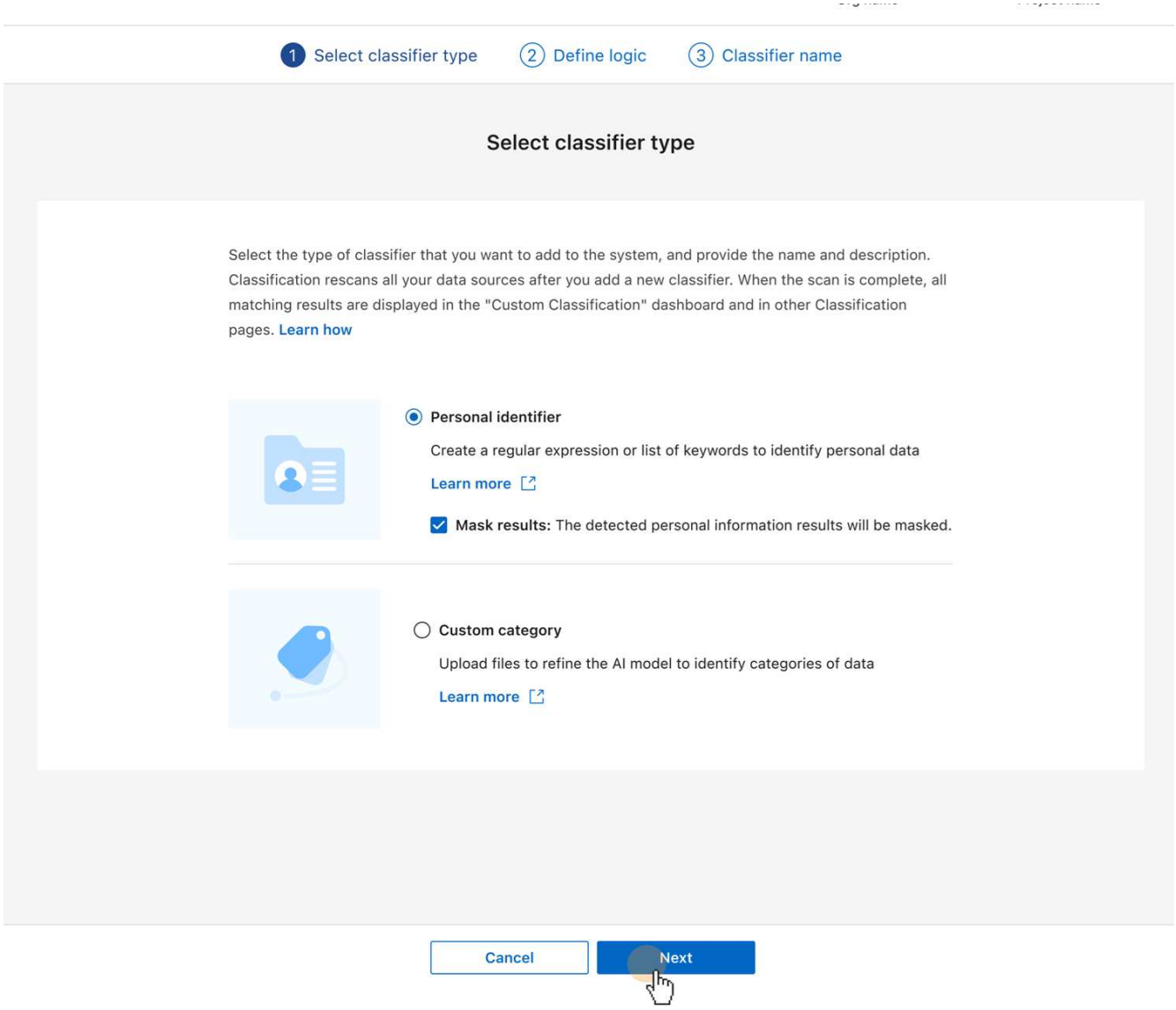
Requisitos para palavras-chave

Se você estiver criando seu identificador pessoal com uma lista de palavras-chave, a lista deve atender aos seguintes requisitos:

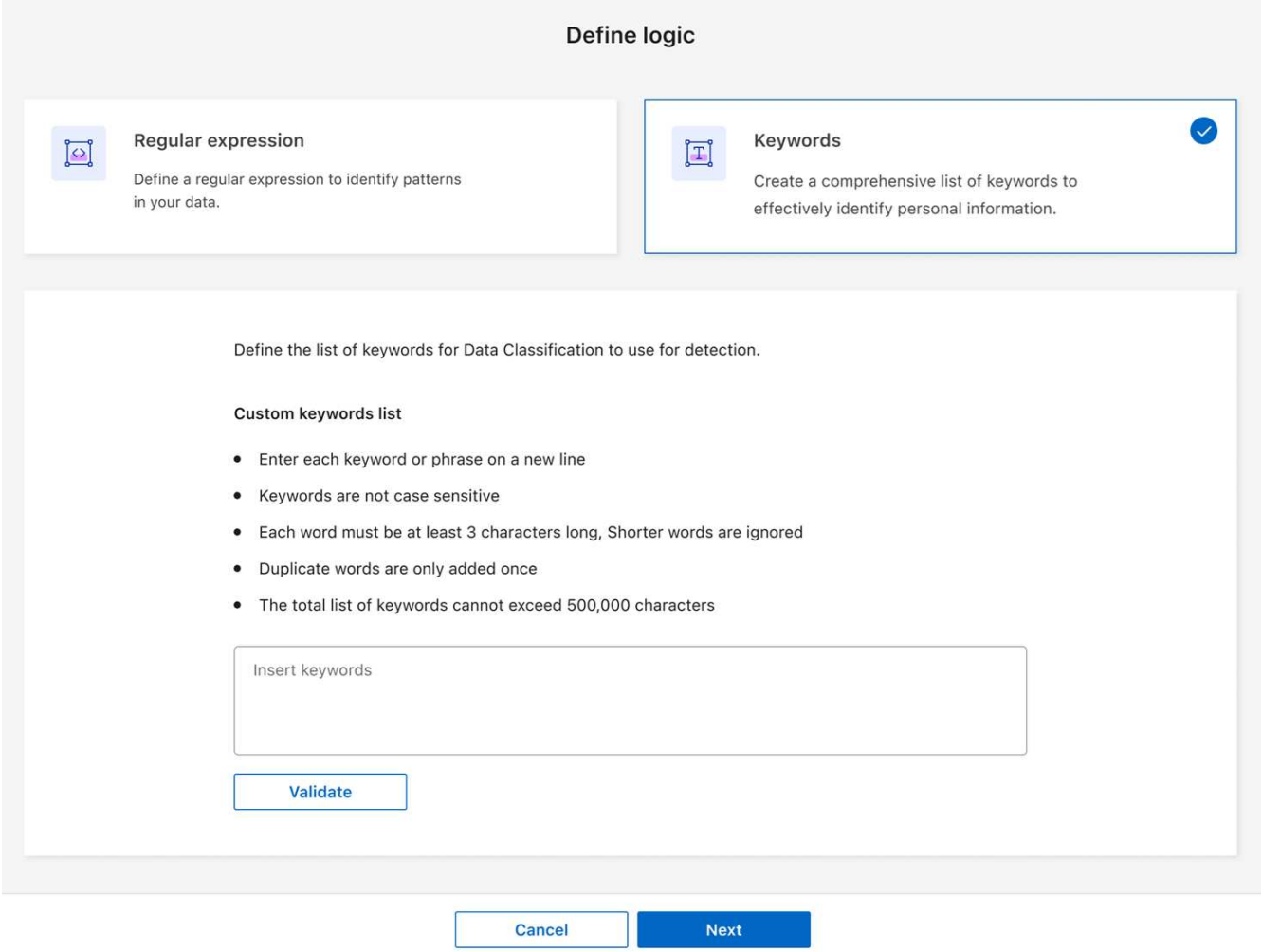
- As entradas de palavras-chave não diferenciam maiúsculas de minúsculas.
- As palavras-chave devem ter pelo menos três caracteres. Palavras com menos de três caracteres serão ignoradas.
- Palavras duplicadas são adicionadas apenas uma vez.
- A lista total de palavras-chave não pode exceder 500.000 caracteres. A lista deve incluir pelo menos uma palavra-chave.

Passos

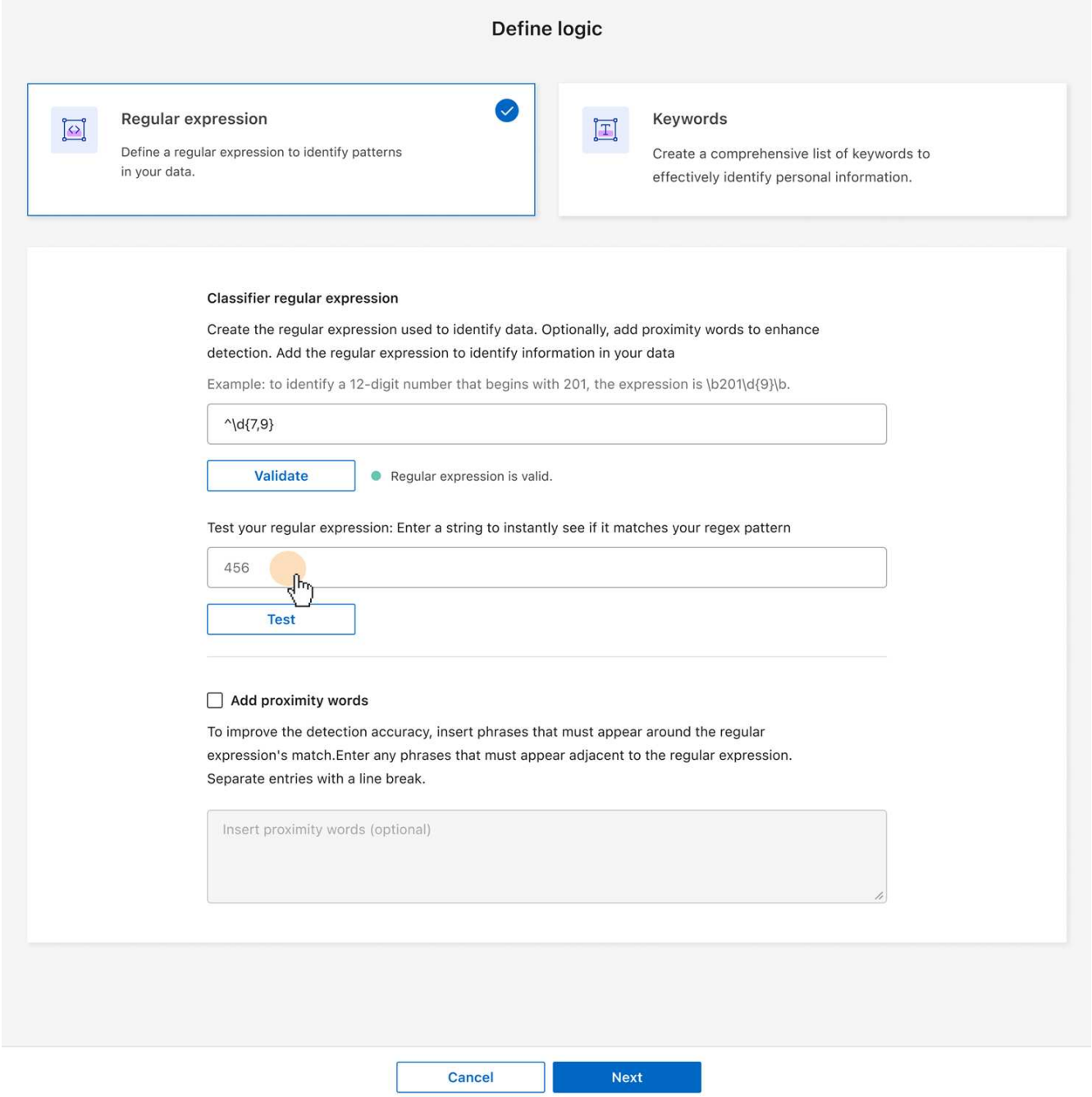
1. Selecione a aba **Classificação personalizada**.
2. Selecione **+ Novo Classificador** para criar o classificador personalizado.
3. Selecione **Identificador pessoal**. Opcionalmente, selecione **Ocultar resultados** para ocultar os dados pessoais detectados.
4. Selecione **Próximo**.



5. Para adicionar o classificador com palavras-chave, selecione **Palavras-chave**. Insira uma lista de palavras-chave, com cada entrada em uma linha separada. Certifique-se de que as palavras-chave estejam de acordo com os requisitos.



Para adicionar o classificador como uma expressão regular, selecione **Expressão regular** e, em seguida, adicione um padrão para detectar as informações específicas dos seus dados. Selecione **Validar** para confirmar a sintaxe da sua entrada.



a. Opcionalmente, insira uma string de exemplo que corresponda ao seu padrão de expressão regular e selecione **Testar** para verificá-la.

b. Opcionalmente, adicione palavras de proximidade. Se você adicionar palavras de proximidade, a Classificação de Dados só sinalizará o padrão regex se as palavras de proximidade forem adjacentes à string correspondente.

6. Selecione **Próximo**.
7. Insira um **Nome do Classificador** e uma **Descrição** para identificar a categoria personalizada no seu painel.
8. Selecione **Salvar** para criar o identificador pessoal personalizado.

Após a criação de um identificador pessoal personalizado, os resultados serão capturados na próxima verificação agendada. Para obter resultados mais rapidamente, realize uma digitalização sob demanda. Para

visualizar os resultados, consulte Gerar relatórios de conformidade.

Criar uma categoria personalizada

Com categorias personalizadas, você pode categorizar dados específicos da sua organização. Categorias personalizadas são criadas com base em arquivos de texto que você carrega, a partir dos quais a Classificação de Dados cria um modelo de IA para identificar informações semelhantes em outros arquivos.

Requisitos de dados de treinamento

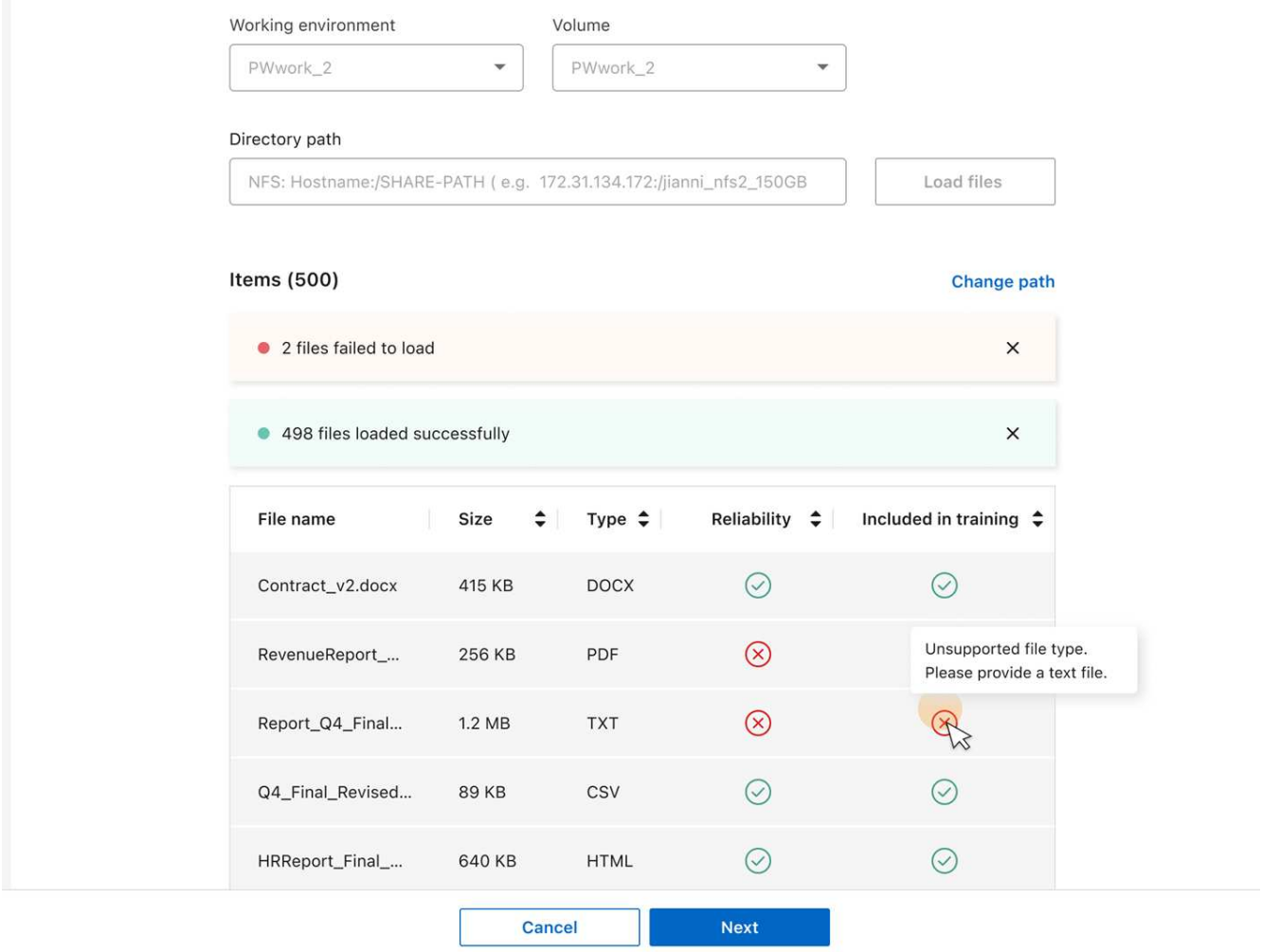
- O conjunto de dados de treinamento deve conter no mínimo 25 arquivos. O número máximo de arquivos é 1.000.
- Todos os arquivos devem estar localizados exatamente no caminho de arquivo que você fornecer.
- Todos os arquivos devem ter mais de 100 bytes.
- Os dados de treinamento para classificação de dados devem estar em um dos seguintes formatos de arquivo: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS ou XLSX. Você pode enviar uma combinação de todos os tipos de arquivo suportados.

Passos

1. Em NetApp Data Classification, selecione **Classificação personalizada**.
2. Selecione **+ Novo classificador**.
3. Selecione **Categoria personalizada** como seu tipo de classificador e clique em **Avançar**.
4. Defina a lógica para sua categoria personalizada com uma coleção de arquivos de texto. Forneça o endereço IP do **Endereço de trabalho** e, em seguida, selecione o **Volume** no menu suspenso.

   Insira o **caminho do diretório** que contém os dados de treinamento.

5. Selecione **Carregar arquivos** para Classificação de Dados para realizar uma verificação dos arquivos. Você pode consultar o resumo dos arquivos, que lista o nome do arquivo, o tamanho, o tipo e indica se o arquivo foi considerado adequado para treinamento.



a. Para alterar o caminho do arquivo ou reenviar arquivos, selecione **Alterar caminho**, insira os dados e carregue os arquivos novamente.

6. Quando estiver satisfeito com os arquivos enviados, selecione **Avançar**.
7. Insira um **Nome do Classificador** e uma **Descrição** para identificar a categoria personalizada no seu painel.
8. Selecione **Salvar** para criar a categoria personalizada.

Resultado

Após criar uma categoria personalizada, os resultados dela serão capturados na próxima verificação agendada. Para obter resultados mais rapidamente, inicie a digitalização manualmente.

Editar um classificador personalizado

Você pode modificar a lógica de um identificador pessoal depois de criá-lo. Não é possível alterar o tipo do identificador pessoal ou o tipo de lógica; por exemplo, não é possível alterar uma categoria personalizada para um identificador pessoal personalizado. Você também não pode alterar um identificador personalizado baseado em palavras-chave para um identificador personalizado baseado em expressões regulares.

Passos

1. Em NetApp Data Classification, selecione **Classificação personalizada**.
2. Identifique o classificador que deseja excluir e selecione o menu de ações. … no final da sua fila.

3. Selecione **Editar lógica**.
4. Se você estiver modificando palavras-chave, adicione, exclua ou edite as palavras-chave apropriadas. Se você estiver modificando uma expressão regular, insira a nova expressão regular e valide-a. Opcionalmente, adicione palavras-chave de proximidade.
5. Selecione **Salvar** para aplicar as alterações.

Excluir um classificador personalizado

1. Em NetApp Data Classification, selecione **Classificação personalizada**.
2. Identifique o classificador que deseja excluir e selecione o menu de ações. … no final da sua fila.
3. Selecione **Excluir classificador**.

Próximos passos

- Gerar relatórios de conformidade

Investigue os dados armazenados em sua organização com a NetApp Data Classification

O painel de investigação de dados exibe insights em nível de arquivo e diretório sobre seus dados, permitindo que você classifique e filtre os resultados. A página Investigação de Dados apresenta insights sobre metadados e permissões de arquivos e diretórios, além de identificar arquivos duplicados. Com insights em nível de arquivo, diretório e banco de dados, você pode tomar medidas para melhorar a conformidade da sua organização e economizar espaço de armazenamento. A página Investigação de Dados também oferece suporte para mover, copiar e excluir arquivos.

Para obter insights da página Investigação, você deve executar uma verificação de classificação completa em suas fontes de dados. Fontes de dados que passaram por uma varredura somente de mapeamento não mostram detalhes em nível de arquivo.

Estrutura de investigação de dados

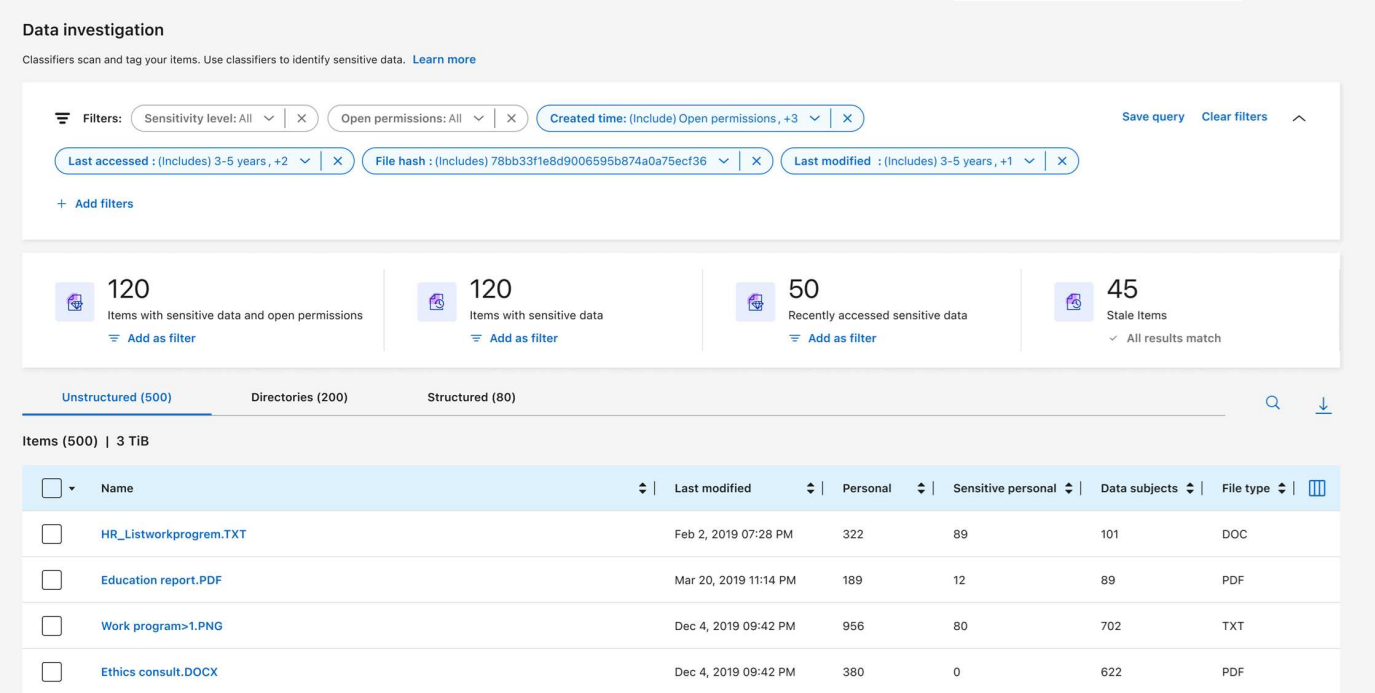
A página Investigação de Dados classifica os dados em três guias:

- **Dados não estruturados**: dados de arquivo
- **Diretórios**: pastas e compartilhamentos de arquivos
- **Estruturado**: banco de dados

Filtros de dados

A página Investigação de Dados fornece vários filtros para classificar seus dados e encontrar o que você precisa. Você pode usar vários filtros em conjunto.

Para adicionar um filtro, selecione o botão **Adicionar filtro**.



Sensibilidade e conteúdo do filtro

Use os seguintes filtros para visualizar quanta informação confidencial está contida em seus dados.

Filtro	Detalhes
Categoria	Selecione o"tipos de categorias" .
Nível de sensibilidade	Selecione o nível de sensibilidade: Pessoal, Pessoal sensível ou Não sensível.
Número de identificadores	Selecione o intervalo de identificadores sensíveis detectados por arquivo. Inclui dados pessoais e dados pessoais sensíveis. Ao filtrar em Diretórios, a Classificação de Dados totaliza as correspondências de todos os arquivos em cada pasta (e subpastas). OBSERVAÇÃO: a versão de dezembro de 2023 (versão 1.26.6) removeu a opção de calcular o número de dados de informações pessoais identificáveis (PII) por Diretórios.
Dados Pessoais	Selecione o"tipos de dados pessoais" .
Dados Pessoais Sensíveis	Selecione o"tipos de dados pessoais sensíveis" .
Titular dos dados	Insira o nome completo ou identificador conhecido do titular dos dados. "Saiba mais sobre os titulares dos dados aqui" .

Filtrar proprietário do usuário e permissões do usuário

Use os seguintes filtros para visualizar os proprietários dos arquivos e as permissões para acessar seus dados.

Filtro	Detalhes
Permissões abertas	Selecione o tipo de permissões dentro dos dados e dentro das pastas/compartilhamentos.

Filtro	Detalhes
Permissões de usuário/grupo	Selecione um ou vários nomes de usuário e/ou nomes de grupo, ou insira um nome parcial.
Proprietário do arquivo	Digite o nome do proprietário do arquivo.
Número de usuários com acesso	Selecione um ou vários intervalos de categorias para mostrar quais arquivos e pastas estão abertos a um determinado número de usuários.

Filtrar cronologicamente

Use os seguintes filtros para visualizar dados com base em critérios de tempo.

Filtro	Detalhes
Tempo de criação	Selecione um intervalo de tempo em que o arquivo foi criado. Você também pode especificar um intervalo de tempo personalizado para refinar ainda mais os resultados da pesquisa.
Tempo descoberto	Selecione um intervalo de tempo em que a Classificação de Dados descobriu o arquivo. Você também pode especificar um intervalo de tempo personalizado para refinar ainda mais os resultados da pesquisa.
Última modificação	Selecione um intervalo de tempo em que o arquivo foi modificado pela última vez. Você também pode especificar um intervalo de tempo personalizado para refinar ainda mais os resultados da pesquisa.
Último acesso	Selecione um intervalo de tempo em que o arquivo ou diretório* foi acessado pela última vez. Você também pode especificar um intervalo de tempo personalizado para refinar ainda mais os resultados da pesquisa. Para os tipos de arquivos que a Classificação de Dados verifica, esta é a última vez que a Classificação de Dados verificou o arquivo.

* O último horário de acesso de um diretório só está disponível para compartilhamentos NFS ou CIFS.

Filtrar metadados

Use os seguintes filtros para visualizar dados com base em localização, tamanho e diretório ou tipo de arquivo.

Filtro	Detalhes
Caminho do arquivo	Insira até 20 caminhos parciais ou completos que você deseja incluir ou excluir da consulta. Se você inserir caminhos de inclusão e exclusão, a Classificação de Dados encontrará todos os arquivos nos caminhos incluídos primeiro, depois removerá os arquivos dos caminhos excluídos e exibirá os resultados. Observe que usar "*" neste filtro não tem efeito e que você não pode excluir pastas específicas da verificação. Todos os diretórios e arquivos em um compartilhamento configurado serão verificados.
Tipo de diretório	Selecione o tipo de diretório: "Compartilhar" ou "Pasta".
Tipo de arquivo	Selecione o"tipos de arquivos" .

Filtro	Detalhes
Tamanho do arquivo	Selecione o intervalo de tamanho do arquivo.
Hash de arquivo	Digite o hash do arquivo para encontrar um arquivo específico, mesmo que o nome seja diferente.

Tipo de armazenamento de filtro

Use os seguintes filtros para visualizar dados por tipo de armazenamento.

Filtro	Detalhes
Tipo de sistema	Selecione o tipo de sistema.
Nome do ambiente do sistema	Selecione sistemas específicos.
Repositório de Armazenamento	Selecione o repositório de armazenamento, por exemplo, um volume ou um esquema.

Consulta de filtro

Use o filtro a seguir para visualizar dados por consultas salvas.

Filtro	Detalhes
Consulta salva	Selecione uma consulta salva ou várias. Vá para o"aba de consultas salvas" para visualizar a lista de consultas salvas existentes e criar novas.
Etiquetas	Selecione"a tag ou tags" que são atribuídos aos seus arquivos.

Status da análise do filtro

Use o filtro a seguir para visualizar dados pelo status de verificação de Classificação de Dados.

Filtro	Detalhes
Status da análise	Selecione uma opção para mostrar a lista de arquivos que estão com a primeira verificação pendente, com verificação concluída, com nova verificação pendente ou que falharam na verificação.
Evento de análise de varredura	Selecione se deseja visualizar arquivos que não foram classificados porque a Classificação de Dados não conseguiu reverter o horário do último acesso ou arquivos que foram classificados mesmo que a Classificação de Dados não tenha conseguido reverter o horário do último acesso.

"Veja detalhes sobre o carimbo de data/hora do "último acesso""para obter mais informações sobre os itens que aparecem na página Investigação ao filtrar usando o Evento de Análise de Verificação.

Filtrar dados por duplicatas

Use o filtro a seguir para visualizar arquivos duplicados no seu armazenamento.

Filtro	Detalhes
Duplicatas	Selecione se o arquivo será duplicado nos repositórios.

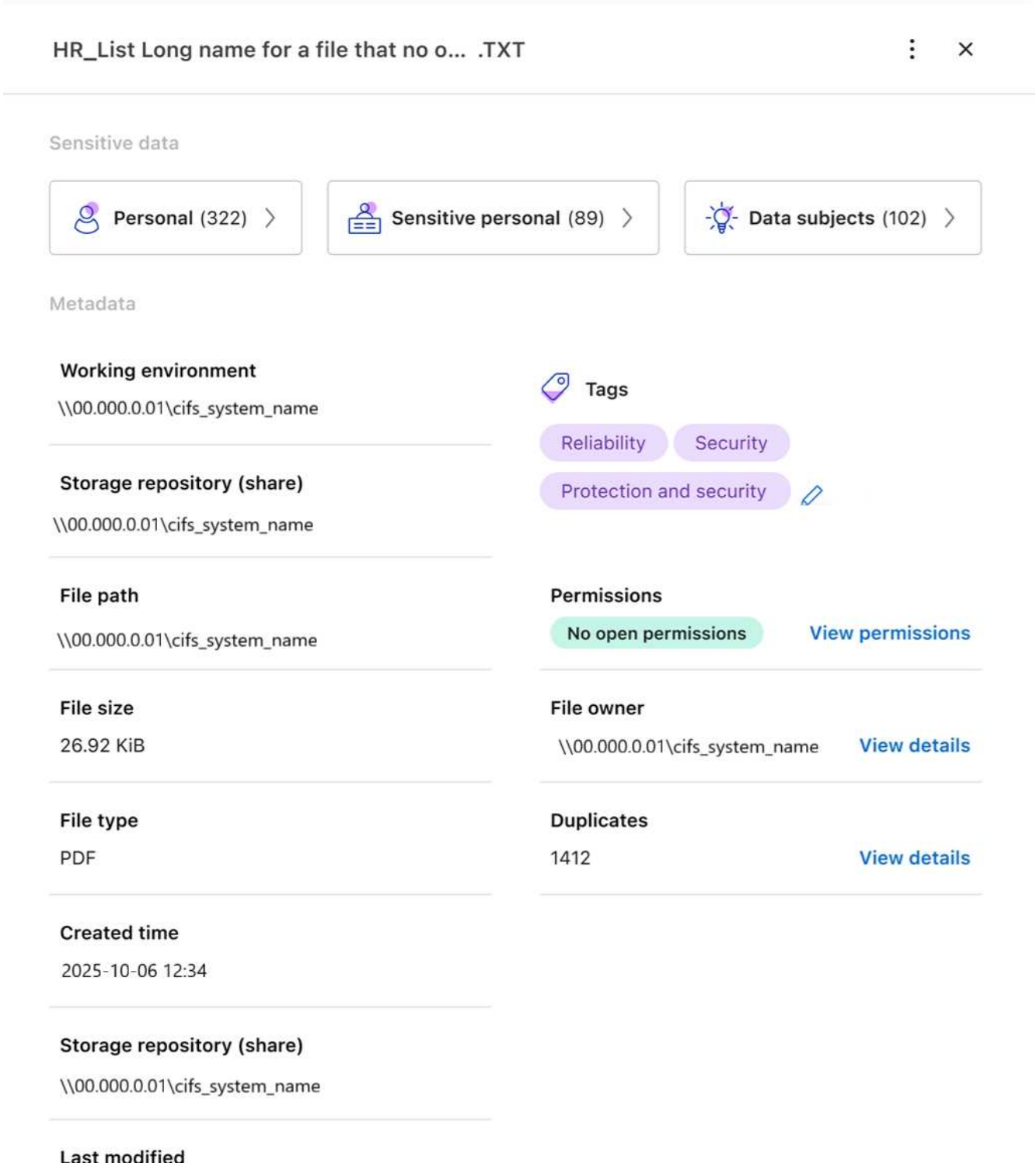
Exibir metadados do arquivo

Além de mostrar o sistema e o volume onde o arquivo reside, os metadados mostram muito mais informações, incluindo as permissões do arquivo, o proprietário do arquivo e se há duplicatas desse arquivo. Esta informação é útil se você estiver planejando"criar consultas salvas" porque você pode ver todas as informações que pode usar para filtrar seus dados.

A disponibilidade das informações depende da fonte de dados. Por exemplo, o nome do volume e as permissões não são compartilhados para arquivos de banco de dados.

Passos

1. No menu Classificação de Dados, selecione **Investigação**.
2. Na lista de Investigação de Dados à direita, selecione o cursor para baixo à direita para qualquer arquivo individual para visualizar os metadados do arquivo.



3. Opcionalmente, você pode criar ou adicionar uma tag ao arquivo com o botão **Criar tag**. Selecione uma tag existente no menu suspenso ou adicione uma nova tag com o botão **+ Adicionar**. Tags podem ser usadas para filtrar dados.

Ver permissões de usuário para arquivos e diretórios

Para visualizar uma lista de todos os usuários ou grupos que têm acesso a um arquivo ou diretório e os tipos de permissões que eles têm, selecione **Exibir todas as permissões**. Esta opção está disponível somente para dados em compartilhamentos CIFS.

Se você usar identificadores de segurança (SIDs) em vez de nomes de usuários e grupos, deverá integrar seu Active Directory à Classificação de Dados. Para obter mais informações, consulte "adicionar Active Directory à Classificação de Dados" .

Passos

1. No menu Classificação de Dados, selecione **Investigação**.
2. Na lista de Investigação de Dados à direita, selecione o cursor para baixo à direita para qualquer arquivo individual para visualizar os metadados do arquivo.
3. Para visualizar uma lista de todos os usuários ou grupos que têm acesso a um arquivo ou diretório e os tipos de permissões que eles têm, no campo Permissões abertas, selecione **Exibir todas as permissões**.

   A classificação de dados mostra até 100 usuários na lista.

4. Selecione o cursor para baixo botão para qualquer grupo para ver a lista de usuários que fazem parte do grupo.

   Você pode expandir um nível do grupo para ver os usuários que fazem parte do grupo.

5. Selecione o nome de um usuário ou grupo para atualizar a página Investigação para que você possa ver todos os arquivos e diretórios aos quais o usuário ou grupo tem acesso.

Verifique se há arquivos duplicados em seus sistemas de armazenamento

Você pode verificar se arquivos duplicados estão sendo armazenados em seus sistemas de armazenamento. Isso é útil se você quiser identificar áreas onde pode economizar espaço de armazenamento. Também é bom garantir que determinados arquivos que tenham permissões específicas ou informações confidenciais não sejam duplicados desnecessariamente em seus sistemas de armazenamento.

A Classificação de Dados compara todos os arquivos (exceto bancos de dados) em busca de duplicatas, caso existam:

- 1 MB ou lager
- Ou que contenham informações pessoais ou informações pessoais sensíveis.

A classificação de dados usa tecnologia de hash para determinar arquivos duplicados. Se um arquivo tiver o mesmo código hash que outro, os arquivos são duplicados exatos, mesmo que os nomes dos arquivos sejam diferentes.

Passos

1. No menu Classificação de Dados, selecione **Investigação**.
2. No painel Filtro, selecione "Tamanho do arquivo" junto com "Duplicatas" ("Tem duplicatas") para ver quais arquivos de um determinado intervalo de tamanho estão duplicados em seu ambiente.
3. Opcionalmente, baixe a lista de arquivos duplicados e envie-a ao administrador de armazenamento para que ele possa decidir quais arquivos, se houver, podem ser excluídos.
4. Opcionalmente, você pode excluir, marcar ou mover os arquivos duplicados. Selecione os arquivos nos quais deseja executar uma ação e, em seguida, selecione a ação apropriada.

Ver se um arquivo específico está duplicado

Você pode ver se um único arquivo tem duplicatas.

Passos

1. No menu Classificação de Dados, selecione **Investigação**.
2. Na lista Investigação de Dados, selecione à direita para qualquer arquivo individual para visualizar os metadados do arquivo.

   Se houver duplicatas para um arquivo, essa informação aparecerá ao lado do campo *Duplicatas*.

3. Para visualizar a lista de arquivos duplicados e onde eles estão localizados, selecione **Exibir detalhes**.
4. Na próxima página, selecione **Exibir duplicatas** para visualizar os arquivos na página Investigação.
5. Opcionalmente, você pode excluir, marcar ou mover os arquivos duplicados. Selecione os arquivos nos quais deseja executar uma ação e, em seguida, selecione a ação apropriada.

> Você pode usar o valor "hash do arquivo" fornecido nesta página e inseri-lo diretamente na página Investigação para procurar um arquivo duplicado específico a qualquer momento - ou pode usá-lo em uma consulta salva.

Baixe seu relatório

Você pode baixar seus resultados filtrados em formato CSV ou JSON.

Podem ser baixados até três arquivos de relatório se a Classificação de Dados estiver verificando arquivos (dados não estruturados), diretórios (pastas e compartilhamentos de arquivos) e bancos de dados (dados estruturados).

Os arquivos são divididos em arquivos com um número fixo de linhas ou registros:

- JSON: 100.000 registros por relatório que leva cerca de 5 minutos para ser gerado
- CSV: 200.000 registros por relatório que leva cerca de 4 minutos para ser gerado

> Você pode baixar uma versão do arquivo CSV para visualizar neste navegador. Esta versão é limitada a 10.000 registros.

O que está incluído no relatório para download

O **Relatório de Dados de Arquivos Não Estruturados** inclui as seguintes informações sobre seus arquivos:

- Nome do arquivo
- Tipo de localização
- Nome do sistema
- Repositório de armazenamento (por exemplo, um volume, bucket, compartilhamentos)
- Tipo de repositório
- Caminho do arquivo
- Tipo de arquivo
- Tamanho do arquivo (em MB)
- Tempo criado
- Última modificação

- Último acesso
- Proprietário do arquivo
  - Os dados do proprietário do arquivo abrangem o nome da conta, o nome da conta SAM e o endereço de e-mail quando o Active Directory está configurado.
- Categoria
- Informações pessoais
- Informações pessoais sensíveis
- Permissões abertas
- Erro de análise de varredura
- Data de detecção de exclusão

  A data de detecção de exclusão identifica a data em que o arquivo foi excluído ou movido. Isso permite que você identifique quando arquivos confidenciais foram movidos. Arquivos excluídos não contribuem para a contagem de números de arquivos que aparece no painel ou na página Investigação. Os arquivos só aparecem nos relatórios CSV.

O **Relatório de Dados de Diretórios Não Estruturados** inclui as seguintes informações sobre suas pastas e compartilhamentos de arquivos:

- Tipo de sistema
- Nome do sistema
- Nome do diretório
- Repositório de armazenamento (por exemplo, uma pasta ou compartilhamentos de arquivos)
- Proprietário do diretório
- Tempo criado
- Tempo descoberto
- Última modificação
- Último acesso
- Permissões abertas
- Tipo de diretório

O **Relatório de Dados Estruturados** inclui as seguintes informações sobre suas tabelas de banco de dados:

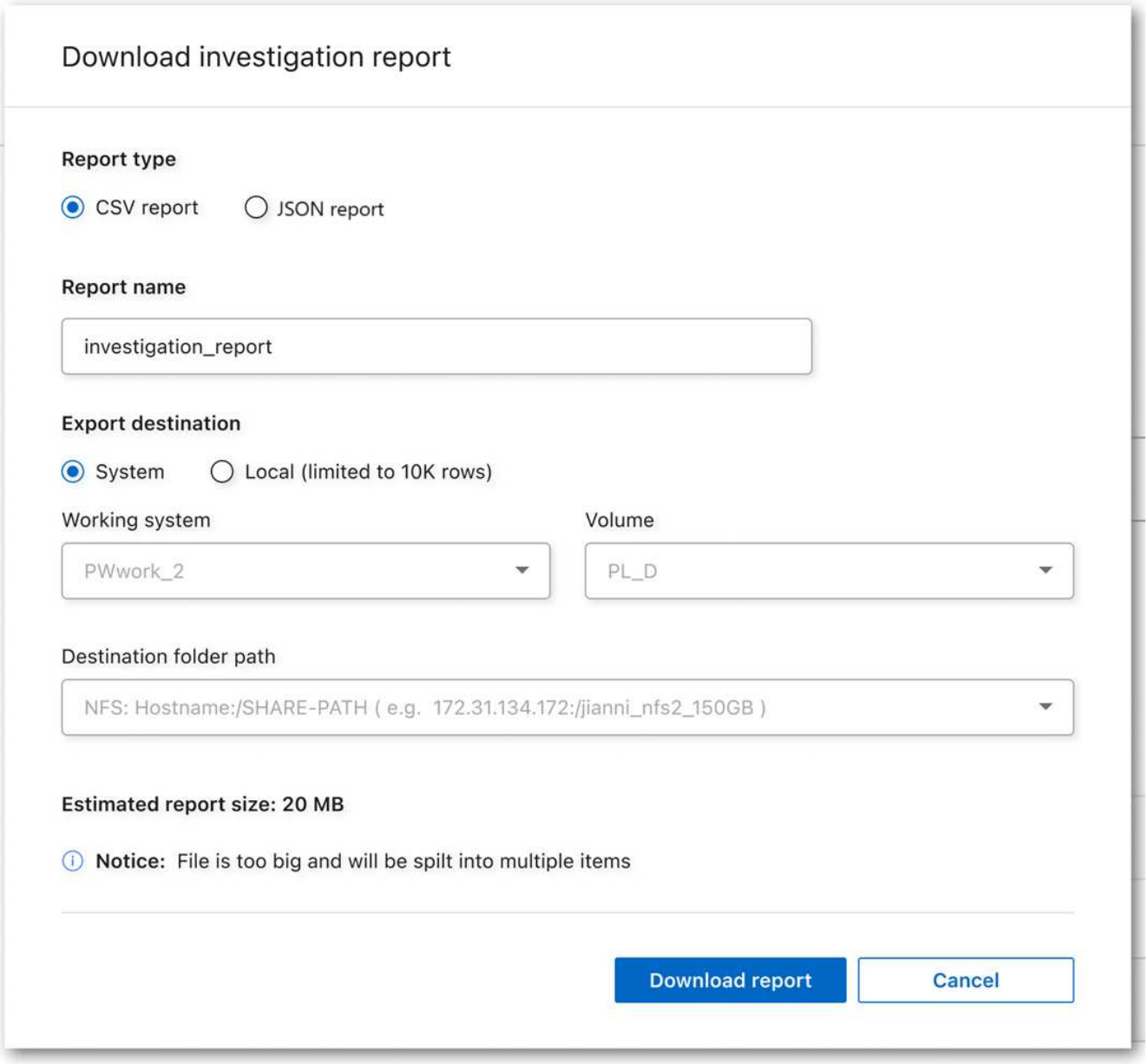
- Nome da tabela do BD
- Tipo de localização
- Nome do sistema
- Repositório de armazenamento (por exemplo, um esquema)
- Contagem de colunas
- Contagem de linhas
- Informações pessoais
- Informações pessoais sensíveis

Etapas para gerar o relatório

1. Na página Investigação de Dados, selecione o botão no canto superior direito da página.
2. Escolha o tipo de relatório: CSV ou JSON.
3. Digite um **Nome do relatório**.
4. Para baixar o relatório completo, selecione **Sistema** e escolha **Sistema** e **Volume** nos respectivos menus suspensos. Forneça um **Caminho para a pasta de destino**.

   Para baixar o relatório no navegador, selecione **Local** . Observe que esta opção limita o relatório às primeiras 10.000 linhas e está limitada ao formato **CSV**. Você não precisa preencher nenhum outro campo se selecionar **Local**.

5. Selecione **Baixar relatório**.



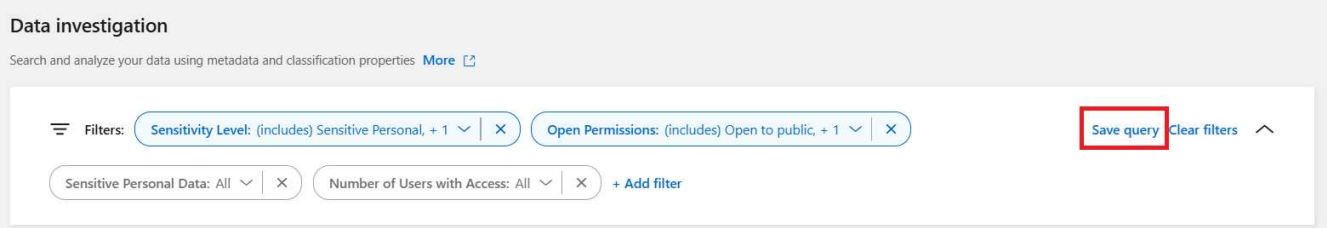
Resultado

Uma caixa de diálogo exibe uma mensagem informando que os relatórios estão sendo baixados.

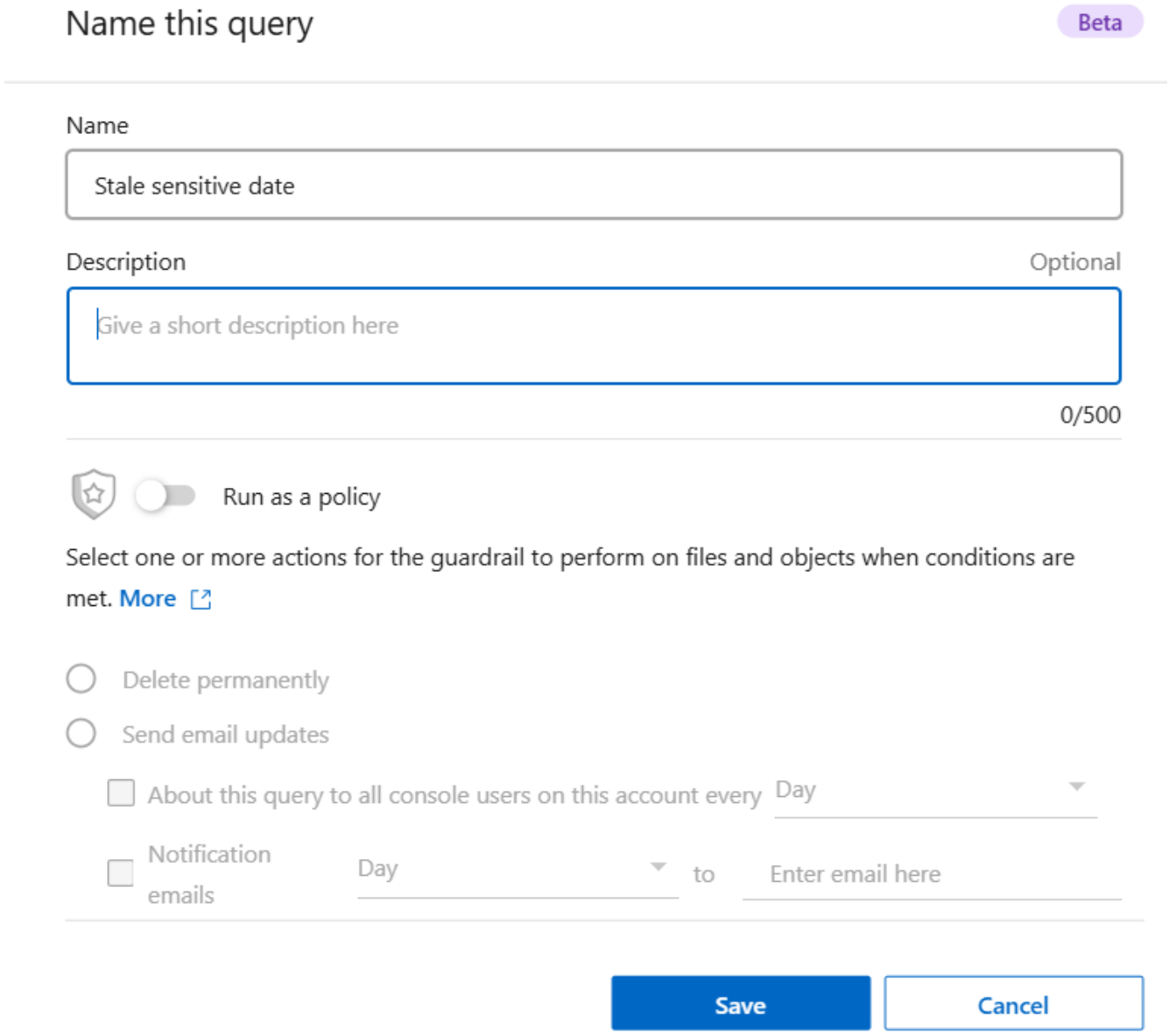
Crie uma consulta salva com base nos filtros selecionados

Passos

1. Na aba Investigação, defina uma pesquisa selecionando os filtros que deseja usar. Ver"Filtrando dados na página Investigação" para mais detalhes.
2. Depois de definir todas as características do filtro conforme sua preferência, selecione **Salvar consulta**.



3. Nomeie a consulta salva e adicione uma descrição. O nome deve ser único.
4. Opcionalmente, você pode salvar a consulta como política:
   a. Para salvar a consulta como uma política, alterne a opção **Executar como uma política**.
   b. Escolha **Excluir permanentemente** ou **Enviar atualizações por e-mail**. Se você escolher atualizações por e-mail, poderá enviar os resultados da consulta para *todos* os usuários do Console diariamente, semanalmente ou mensalmente. Como alternativa, você pode enviar a notificação para um endereço de e-mail específico com a mesma frequência.
5. Selecione **Salvar**.



Depois de criar a pesquisa ou política, você pode visualizá-la na aba **Consultas salvas**.

Pode levar até 15 minutos para que os resultados apareçam na página Consultas salvas.

Gerenciar consultas salvas com a NetApp Data Classification

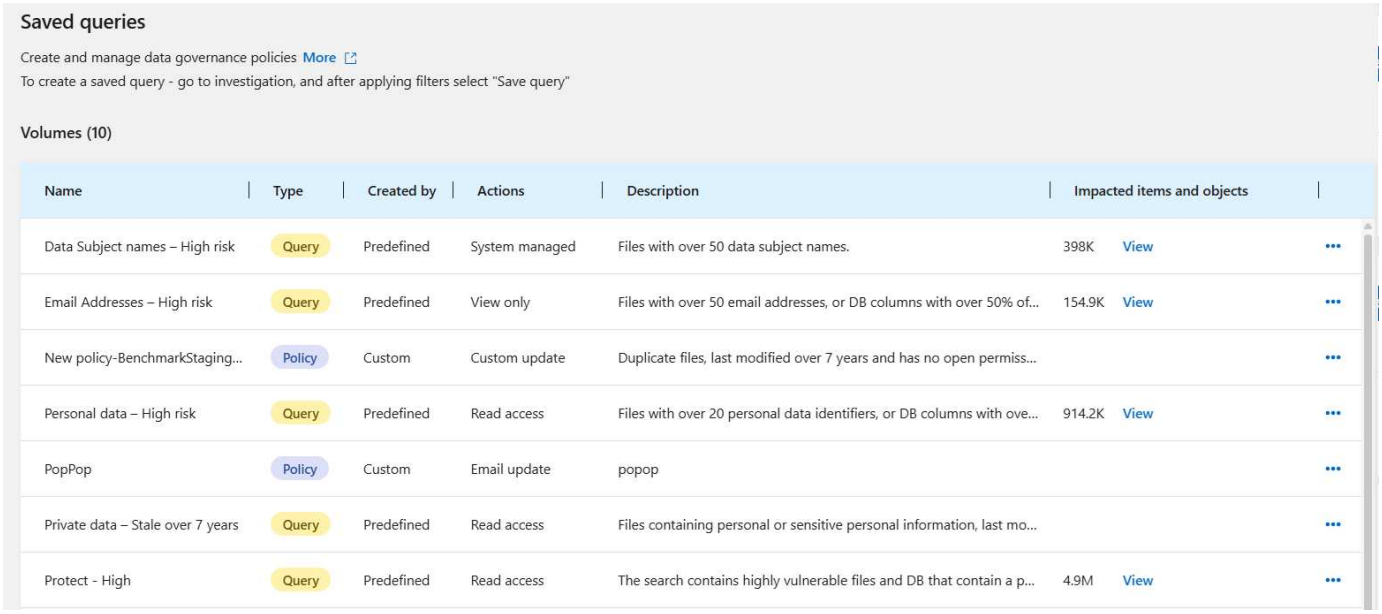
A classificação de dados do NetaApp permite salvar suas consultas de pesquisa. Com uma consulta salva, você pode criar filtros personalizados para classificar consultas frequentes da sua página de investigação de dados. A Classificação de Dados também inclui consultas salvas predefinidas com base em solicitações comuns.

A guia **Consultas salvas** no painel de Conformidade lista todas as consultas salvas predefinidas e

personalizadas disponíveis nesta instância de Classificação de Dados.

Consultas salvas também podem ser salvas como **políticas**. Enquanto as consultas filtram dados, as políticas permitem que você atue nos dados. Com uma política: você pode excluir dados descobertos ou enviar atualizações por e-mail sobre os dados descobertos.

As consultas salvas também aparecem na lista de filtros na página Investigação.



Ver resultados de consultas salvas na página Investigação

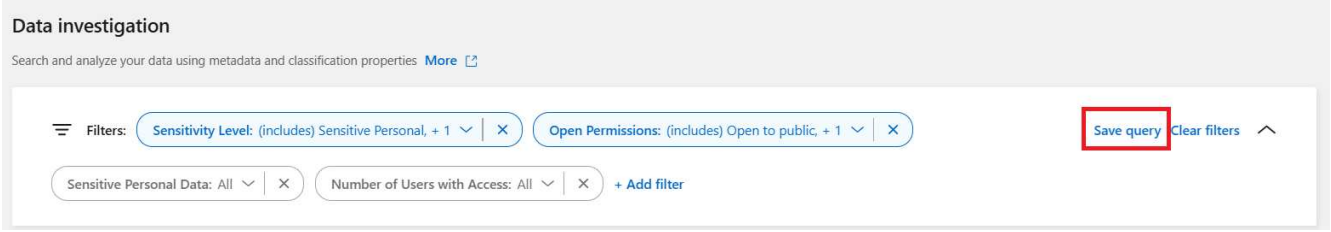
Para exibir os resultados de uma consulta salva na página Investigação, selecione botão para uma pesquisa específica e selecione **Investigar resultados**.

Crie consultas e políticas salvas

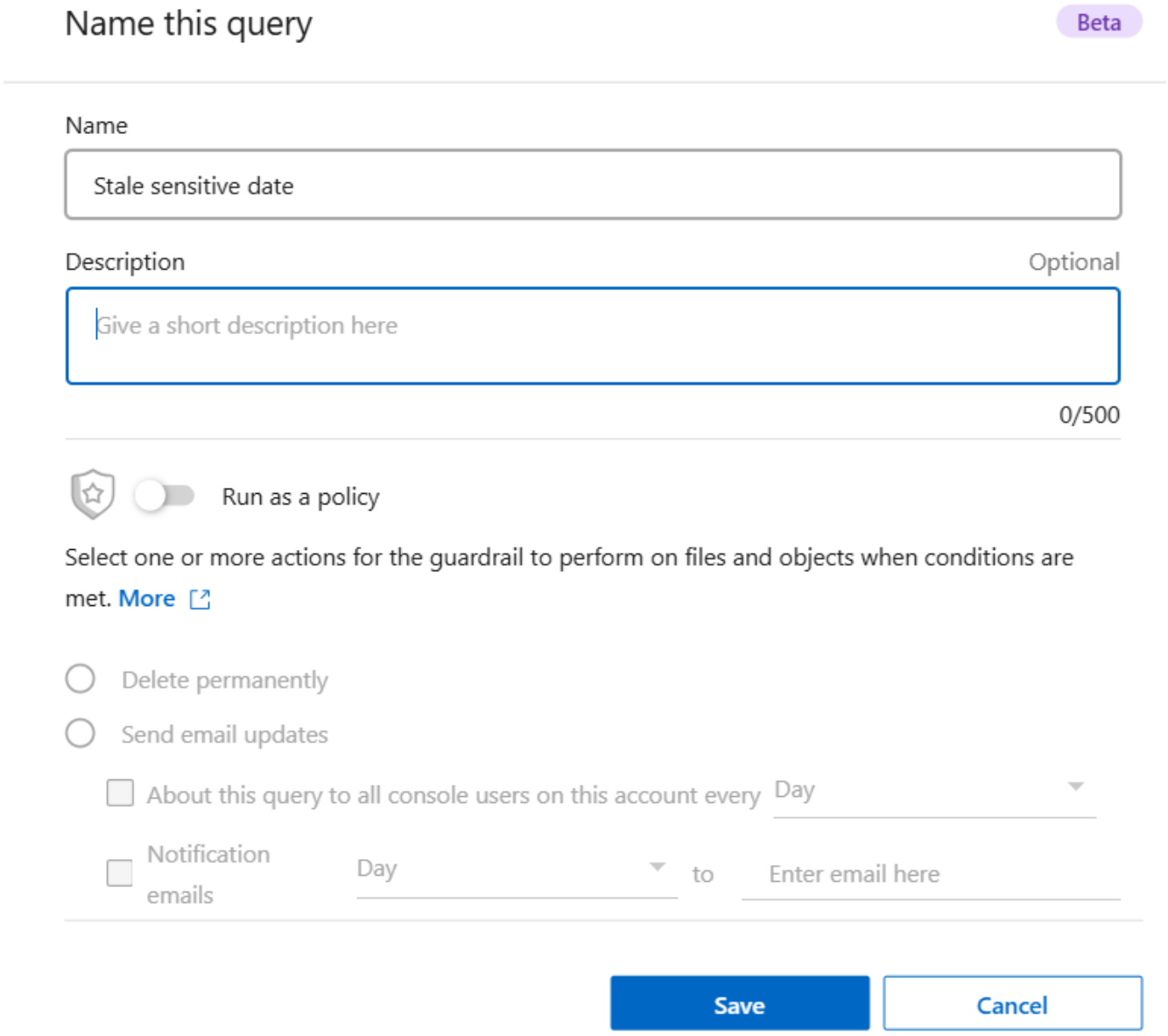
Você pode criar suas próprias consultas salvas personalizadas que fornecem resultados para consultas específicas da sua organização. Os resultados são retornados para todos os arquivos e diretórios (compartilhamentos e pastas) que correspondem aos critérios de pesquisa.

Passos

1. Na aba Investigação, defina uma pesquisa selecionando os filtros que deseja usar. Ver"Filtrando dados na página Investigação" para mais detalhes.
2. Depois de definir todas as características do filtro conforme sua preferência, selecione **Salvar consulta**.



3. Nomeie a consulta salva e adicione uma descrição. O nome deve ser único.
4. Opcionalmente, você pode salvar a consulta como política:
   a. Para salvar a consulta como uma política, alterne a opção **Executar como uma política**.
   b. Escolha **Excluir permanentemente** ou **Enviar atualizações por e-mail**. Se você escolher atualizações por e-mail, poderá enviar os resultados da consulta para *todos* os usuários do Console diariamente, semanalmente ou mensalmente. Como alternativa, você pode enviar a notificação para um endereço de e-mail específico com a mesma frequência.
5. Selecione **Salvar**.



Depois de criar a pesquisa ou política, você pode visualizá-la na aba **Consultas salvas**.

Editar consultas ou políticas salvas

Você pode modificar o nome e a descrição de uma consulta salva. Você também pode converter uma consulta em uma política e vice-versa.

Você não pode modificar consultas salvas padrão. Você não pode modificar os filtros de uma consulta salva. Você pode visualizar os resultados da investigação de uma consulta salva, alterar ou modificar os filtros e salvá-la como uma nova consulta ou política.

Passos

1. Na página Consultas salvas, selecione **Editar pesquisa** para a pesquisa que você deseja alterar.

2. Faça as alterações nos campos de nome e descrição. Para alterar apenas os campos de nome e descrição.

   Opcionalmente, você pode converter a consulta em uma política ou converter a política em uma consulta salva. Alterne a opção **Executar como uma política** conforme necessário. .. Se você estiver convertendo a consulta em uma política, escolha **Excluir permanentemente** ou **Enviar atualizações por e-mail**. Se você escolher atualizações por e-mail, poderá enviar os resultados da consulta para *todos* os usuários do Console diariamente, semanalmente ou mensalmente. Como alternativa, você pode enviar a notificação para um endereço de e-mail específico com a mesma frequência.

3. Selecione **Salvar** para concluir as alterações.

Excluir consultas salvas

Você pode excluir qualquer consulta ou política personalizada salva se não precisar mais dela. Você não pode excluir consultas salvas padrão.

Para excluir uma consulta salva, selecione o botão para uma pesquisa específica, selecione **Excluir consulta** e, em seguida, selecione **Excluir consulta** novamente na caixa de diálogo de confirmação.

Consultas padrão

A Classificação de Dados fornece as seguintes consultas de pesquisa definidas pelo sistema:

- **Nomes dos titulares dos dados - Alto risco**

  Arquivos com mais de 50 nomes de titulares de dados

- **Endereços de e-mail - Alto risco**

  Arquivos com mais de 50 endereços de e-mail ou colunas de banco de dados com mais de 50% de suas linhas contendo endereços de e-mail

- **Dados pessoais - Alto risco**

  Arquivos com mais de 20 identificadores de dados pessoais ou colunas de banco de dados com mais de 50% de suas linhas contendo identificadores de dados pessoais

- **Dados privados - desatualizados há mais de 7 anos**

  Arquivos contendo informações pessoais ou pessoais sensíveis, modificados pela última vez há mais de 7 anos

- **Proteger - Alto**

  Arquivos ou colunas de banco de dados que contêm uma senha, informações de cartão de crédito, número IBAN ou número de previdência social

- **Proteger - Baixo**

  Arquivos que não foram acessados por mais de 3 anos

- **Proteger - Médio**

  Arquivos que contêm arquivos ou colunas de banco de dados com identificadores de dados pessoais, incluindo números de identificação, números de identificação fiscal, números de carteira de motorista, IDs médicos ou números de passaporte

- **Dados pessoais sensíveis - Alto risco**

  Arquivos com mais de 20 identificadores de dados pessoais sensíveis ou colunas de banco de dados com mais de 50% de suas linhas contendo dados pessoais sensíveis

Alterar as configurações de verificação de NetApp Data Classification para seus repositórios

Você pode gerenciar como seus dados estão sendo verificados em cada um dos seus sistemas e fontes de dados. Você pode fazer as alterações com base no "repositório", ou seja, você pode fazer alterações para cada volume, esquema, usuário, etc., dependendo do tipo de fonte de dados que você está verificando.

Algumas das coisas que você pode alterar são se um repositório é verificado ou não e se a NetApp Data Classification está executando uma"varredura de mapeamento ou varredura de mapeamento e classificação" . Você também pode pausar e retomar a verificação, por exemplo, se precisar interromper a verificação de um volume por um período de tempo.

Visualize o status da verificação dos seus repositórios

Você pode visualizar os repositórios individuais que o NetApp Data Classification está verificando (volumes, buckets, etc.) para cada sistema e fonte de dados. Você também pode ver quantos foram "Mapeados" e quantos foram "Classificados". A classificação demora mais porque a identificação completa da IA está sendo realizada em todos os dados.

Você pode visualizar o status de verificação de cada ambiente de trabalho na página Configuração:

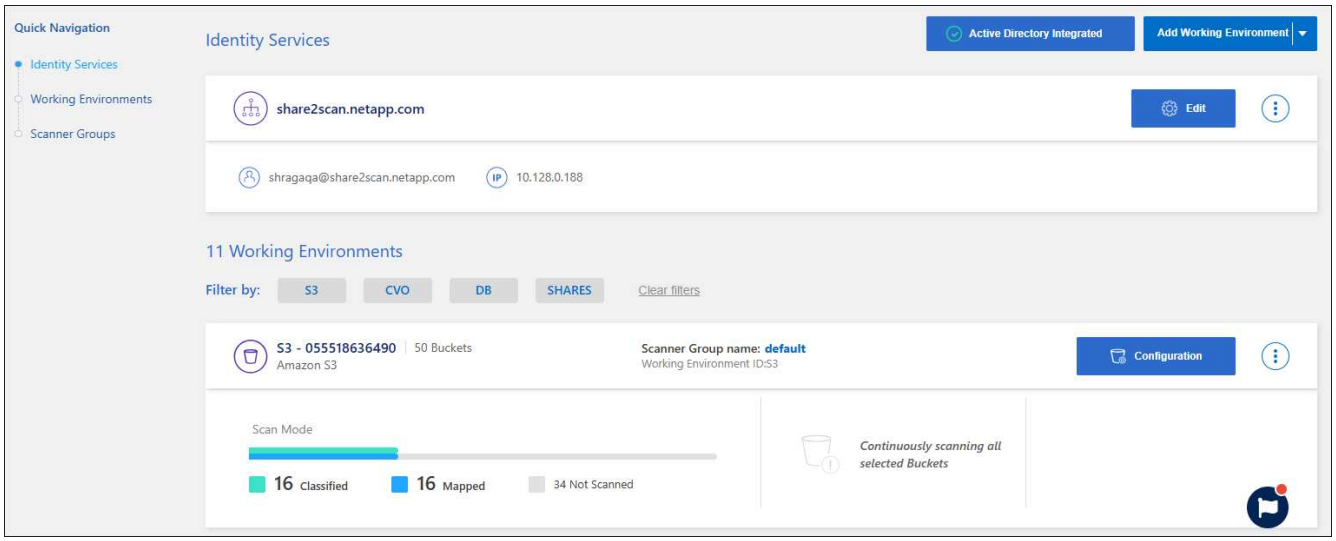
- **Inicializando** (ponto azul claro): A configuração do mapa ou classificação está ativada. Isso aparece brevemente antes de passar para o status de "fila pendente".
- **Fila pendente** (ponto laranja): A tarefa de verificação está aguardando para ser listada na fila de verificação.
- **Na fila** (ponto laranja): A tarefa foi adicionada com sucesso à fila de digitalização. O sistema começará a mapear ou classificar o volume quando chegar a sua vez na fila.
- **Em execução** (ponto verde): A tarefa de verificação, que estava na fila, está ativamente em andamento no repositório de armazenamento selecionado.
- **Concluído** (ponto verde): A verificação do repositório de armazenamento foi concluída.
- **Pausado** (ponto cinza): Você pausou a digitalização. Embora as alterações de volume não sejam exibidas no sistema, as informações obtidas por meio da digitalização permanecem disponíveis.
- **Erro** (ponto vermelho): A verificação não pode ser concluída porque encontrou problemas. Se você

precisar concluir uma ação, o erro aparecerá na dica de ferramenta na coluna “Ação necessária”. Caso contrário, o sistema mostra um status de “erro” e tenta recuperar. Quando termina, o status muda.

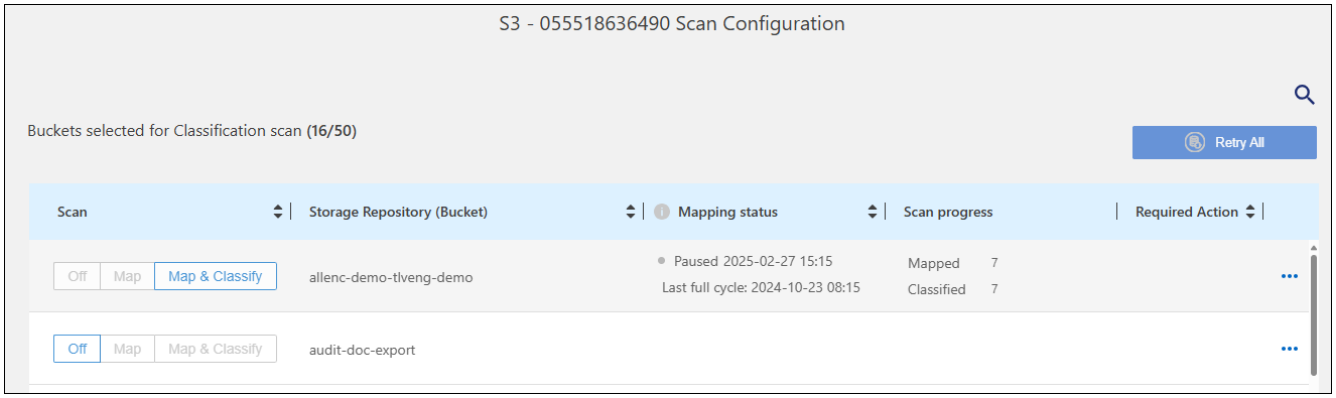
- **Não escaneando**: A configuração de volume "Desligado" foi selecionada e o sistema não está escaneando o volume.

Passos

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



2. Na guia Configuração, selecione o botão **Configuração** do sistema.
3. Na página Configuração de verificação, visualize as configurações de verificação para todos os repositórios.



4. Durante uma verificação, passe o cursor sobre a barra de progresso na coluna *Status do mapeamento* para visualizar o número de arquivos na fila a serem mapeados ou classificados para esse repositório.

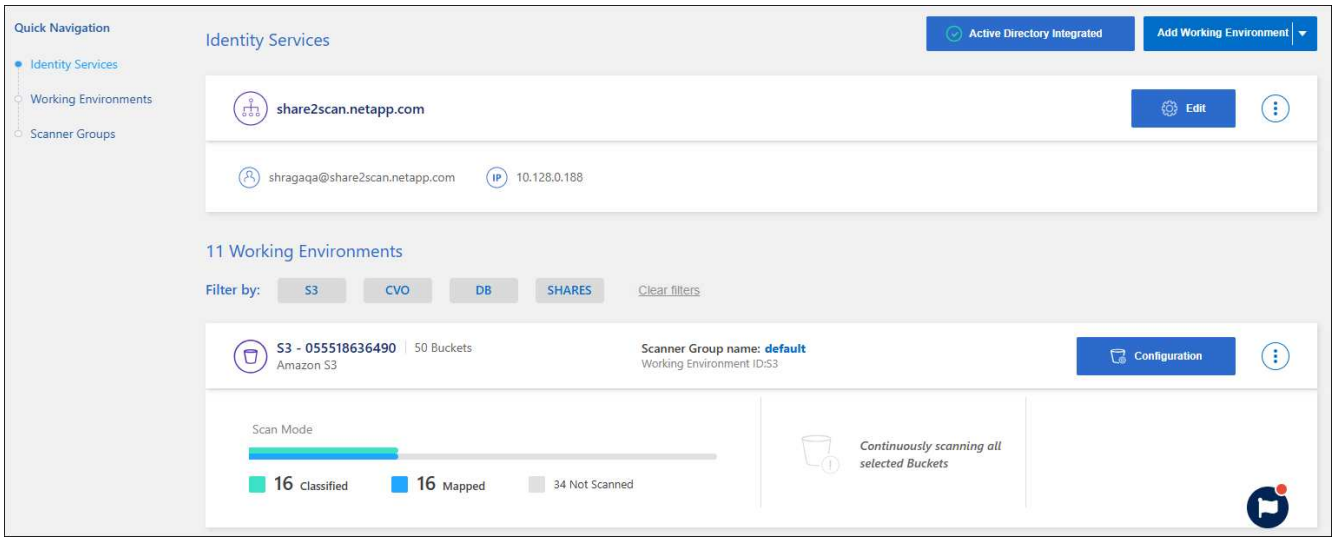
Alterar o tipo de digitalização de um repositório

Você pode iniciar ou parar verificações somente de mapeamento ou verificações de mapeamento e classificação em um sistema a qualquer momento na página Configuração. Você também pode mudar de varreduras somente de mapeamento para varreduras de mapeamento e classificação, e vice-versa.

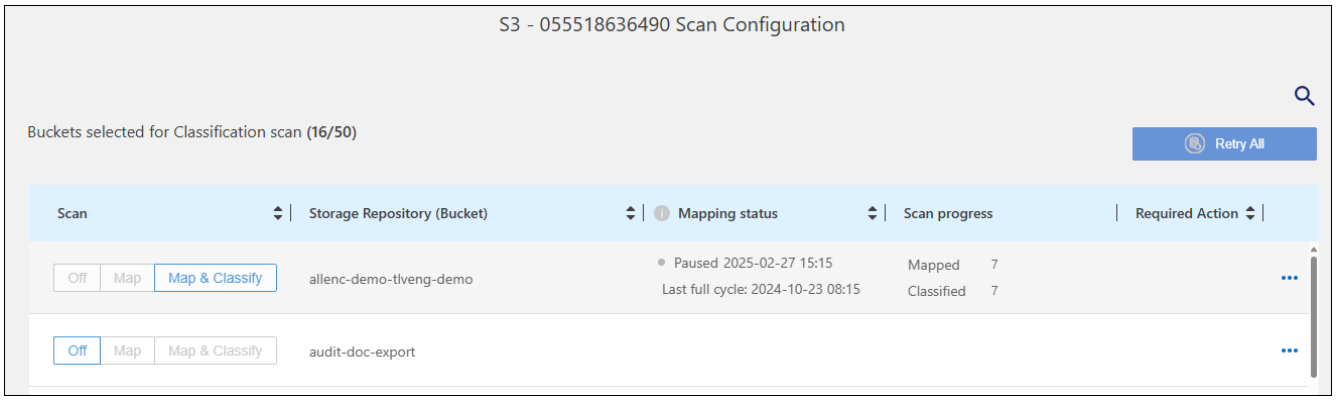
Os bancos de dados não podem ser configurados para varreduras somente de mapeamento. A varredura do banco de dados pode estar Desligada ou Ligada; onde Ligada é equivalente a Mapear e Classificar.

Passos

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na guia Configuração, selecione o botão **Configuração** do sistema.

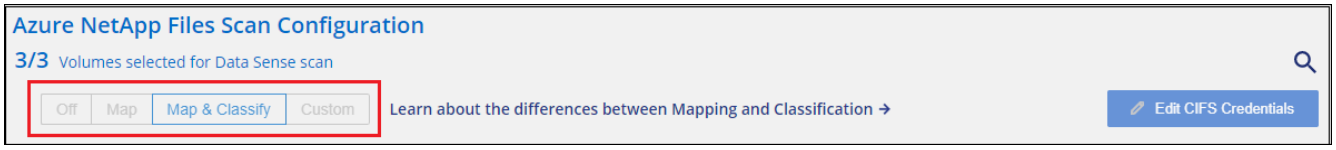


3. Na página Configuração de verificação, altere qualquer um dos repositórios (buckets neste exemplo) para executar verificações **Mapear** ou **Mapear e classificar**.



Certos tipos de sistemas permitem que você altere o tipo de verificação globalmente para todos os repositórios usando uma barra de botões na parte superior da página. Isso é válido para sistemas Cloud Volumes ONTAP, ONTAP local, Azure NetApp Files e Amazon FSx para ONTAP .

O exemplo abaixo mostra esta barra de botões para um sistema Azure NetApp Files .



Priorizar varreduras

Você pode priorizar as verificações de mapeamento mais importantes ou mapear e classificar verificações para garantir que as verificações de alta prioridade sejam concluídas primeiro.

Por padrão, as verificações são enfileiradas com base na ordem em que são iniciadas. Com a capacidade de

priorizar verificações, você pode movê-las para a frente da fila. Várias varreduras podem ser priorizadas. A prioridade é designada na ordem "primeiro a entrar, primeiro a sair", o que significa que a primeira varredura que você prioriza passa para a frente da fila; a segunda varredura que você prioriza se torna a segunda na fila, e assim por diante.

A prioridade é concedida apenas uma vez. As novas varreduras automáticas de dados de mapeamento ocorrem na ordem padrão.

Passos

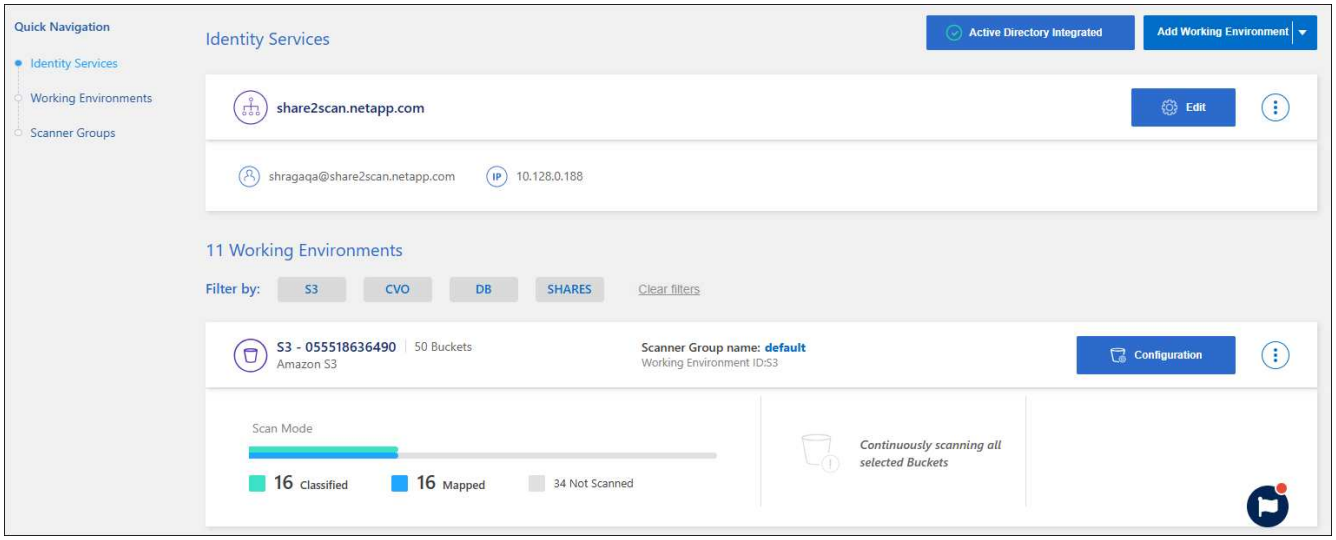
1. No menu Classificação de Dados, selecione **Configuração**.
2. Selecione os recursos que você deseja priorizar.
3. Das Ações ... opção, selecione **Priorizar verificação**.

Parar de procurar um repositório

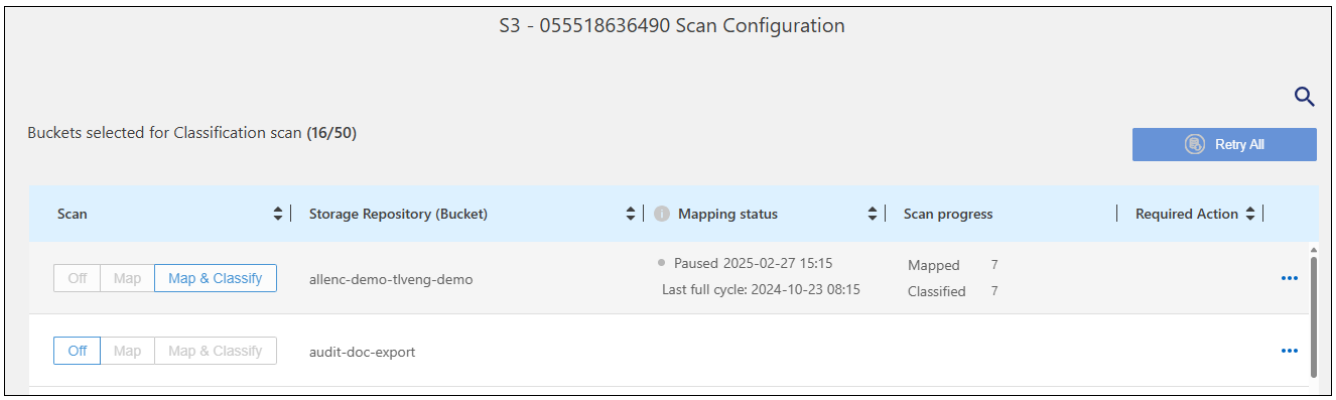
Você pode parar de escanear um repositório (por exemplo, um volume) se não precisar mais monitorá-lo para verificar a conformidade. Você faz isso desligando a digitalização. Quando a digitalização é desativada, toda a indexação e informações sobre esse volume são removidas do sistema, e a cobrança pela digitalização dos dados é interrompida.

Passos

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na guia Configuração, selecione o botão **Configuração** do sistema.



3. Na página Configuração de verificação, selecione **Desativado** para interromper a verificação de um bucket específico.



Pausar e retomar a varredura de um repositório

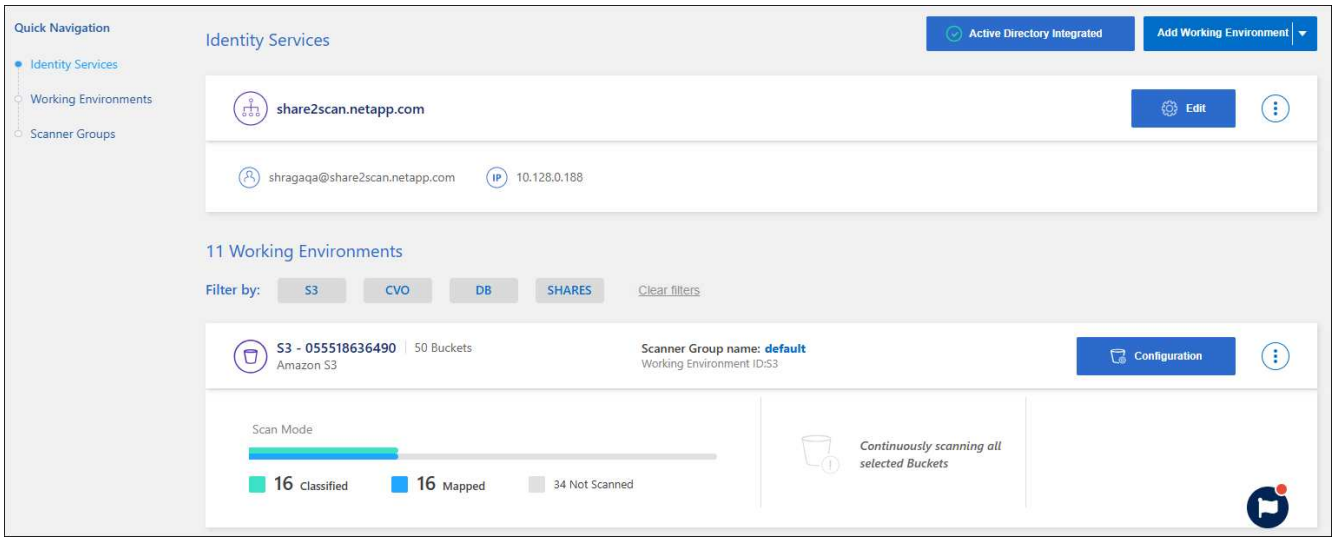
Você pode "pausar" a verificação em um repositório se quiser interromper temporariamente a verificação de determinado conteúdo. Pausar a verificação significa que a Classificação de Dados não realizará mais verificações em busca de alterações ou adições ao repositório. Todos os resultados de varredura atuais permanecem acessíveis na Classificação de Dados.

Se você pausar as digitalizações, isso não elimina as cobranças, pois os dados ainda permanecem no sistema.

Você pode retomar a digitalização a qualquer momento.

Passos

1. No menu Classificação de Dados, selecione **Configuração**.
2. Na guia Configuração, selecione o botão **Configuração** do sistema.



3. Na página Configuração de digitalização, selecione as Ações ••• ícone.
4. Selecione **Pausar** para pausar a varredura de um volume ou selecione **Retomar** para retomar a varredura de um volume que foi pausado anteriormente.

Exibir relatórios de conformidade da NetApp Data Classification

A NetApp Data Classification fornece relatórios que você pode usar para entender melhor o status do programa de privacidade de dados da sua organização.

Por padrão, os painéis de Classificação de Dados exibem dados de conformidade e governança para todos os sistemas, bancos de dados e fontes de dados. Se quiser visualizar relatórios que contenham dados apenas de alguns sistemas, você pode filtrar para ver apenas eles.

- Os relatórios de conformidade só estarão disponíveis se você realizar uma verificação de classificação completa em suas fontes de dados. Fontes de dados que passaram por uma varredura somente de mapeamento podem gerar apenas o Relatório de Mapeamento de Dados.
- A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que a Classificação de Dados identifica. Você deve sempre validar as informações revisando os dados.

Os seguintes relatórios estão disponíveis para Classificação de Dados:

- **Relatório de avaliação de descoberta de dados**: Fornece uma análise de alto nível do ambiente escaneado para destacar as descobertas do sistema e mostrar áreas de preocupação e possíveis etapas de correção. Este relatório está disponível no painel de Governança.
- **Relatório de visão geral do mapeamento de dados completo**: Fornece informações sobre o tamanho e o número de arquivos em seus sistemas. Isso inclui capacidade de uso, idade dos dados, tamanho dos dados e tipos de arquivo. Este relatório está disponível no painel de Governança.
- **Relatório de solicitação de acesso do titular dos dados**: permite que você extraia um relatório de todos os arquivos que contêm informações sobre o nome específico ou identificador pessoal de um titular dos dados. Este relatório está disponível no painel de conformidade.
- **Relatório HIPAA**: Ajuda você a identificar a distribuição de informações de saúde em seus arquivos. Este relatório está disponível no painel de conformidade.
- **Relatório PCI DSS**: Ajuda a identificar a distribuição de informações de cartão de crédito em seus arquivos. Este relatório está disponível no painel de conformidade.
- **Relatório de avaliação de risco de privacidade**: fornece insights de privacidade dos seus dados e uma pontuação de risco de privacidade. Este relatório está disponível no painel de conformidade.
- **Relatórios sobre um tipo específico de informação**: Há relatórios disponíveis que incluem detalhes sobre os arquivos identificados que contêm dados pessoais e dados pessoais confidenciais. Você também pode ver os arquivos divididos por categoria e tipo de arquivo.

Selecione os sistemas para relatórios

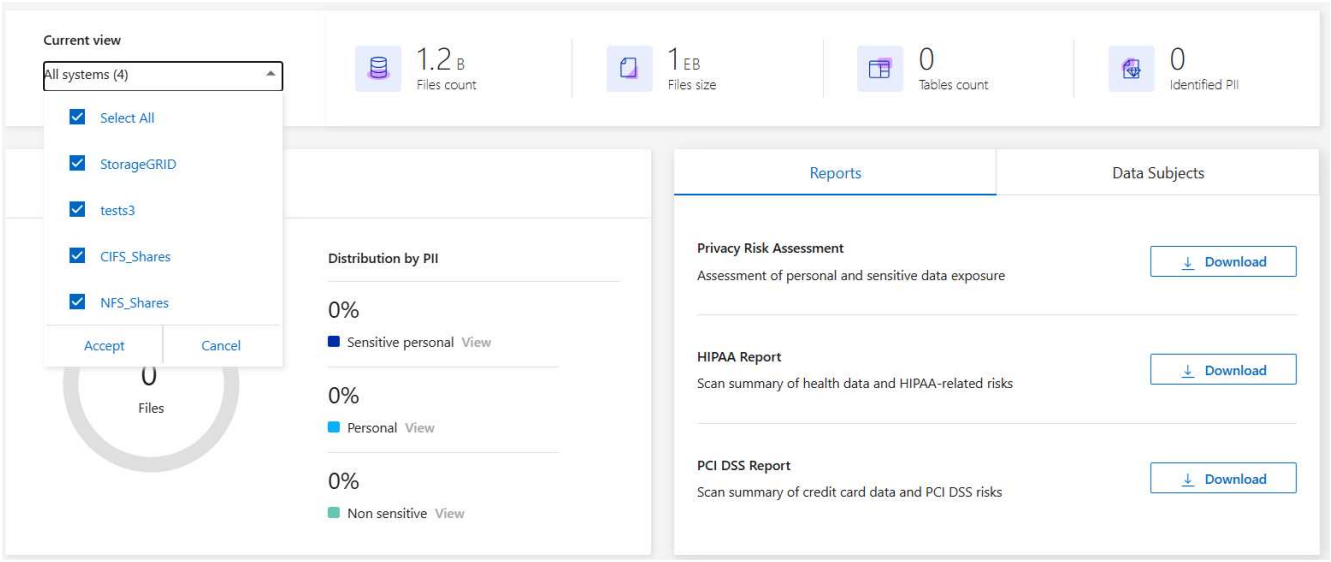
Você pode filtrar o conteúdo do painel Conformidade de Classificação de Dados para ver dados de conformidade de todos os sistemas e bancos de dados, ou apenas de sistemas específicos.

Ao filtrar o painel, a Classificação de Dados abrange os dados de conformidade e os relatórios apenas para os sistemas selecionados.

Passos

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

2. Selecione o filtro suspenso de sistemas e depois selecione os sistemas.
3. Selecione **Aceitar** para confirmar sua seleção.



Relatório de solicitação de acesso ao titular dos dados

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

Você pode responder a um DSAR pesquisando o nome completo do sujeito ou um identificador conhecido (como um endereço de e-mail) e depois baixando um relatório. O relatório foi criado para auxiliar a sua organização a cumprir com o GDPR ou leis semelhantes de privacidade de dados.

Como a Classificação de Dados pode ajudar você a responder a um DSAR?

Quando você realiza uma pesquisa de titular de dados, a Classificação de Dados encontra todos os arquivos que contêm o nome ou identificador dessa pessoa. A Classificação de Dados verifica os dados pré-indexados mais recentes para o nome ou identificador. Não inicia uma nova verificação.

Após a conclusão da pesquisa, você poderá baixar a lista de arquivos para um relatório de Solicitação de Acesso do Titular dos Dados. O relatório agrega insights dos dados e os coloca em termos legais que você pode enviar de volta à pessoa.

A pesquisa de titulares de dados não é suportada atualmente em bancos de dados.

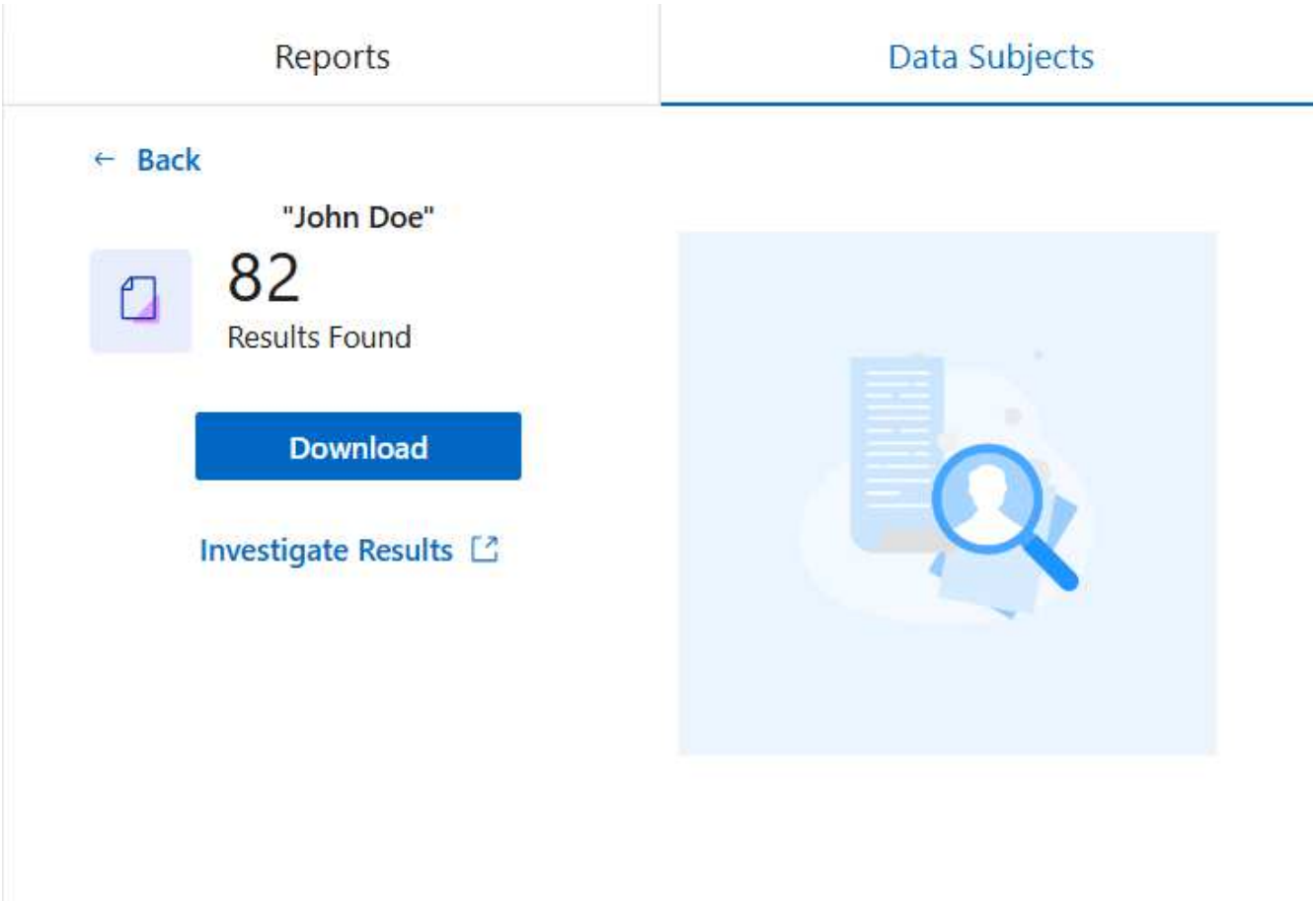
Pesquisar titulares de dados e baixar relatórios

Pesquise o nome completo do titular dos dados ou o identificador conhecido e baixe um relatório de lista de arquivos ou um relatório DSAR. Você pode pesquisar por"qualquer tipo de informação pessoal" .

Inglês, alemão, japonês e espanhol são suportados na busca por nomes de titulares de dados. Suporte para mais idiomas será adicionado posteriormente.

Passos

1. No menu Classificação de Dados, selecione **Conformidade**.
2. Na página Conformidade, localize a aba **Assuntos de Dados**.
3. Na seção **Assuntos de dados**, insira um nome ou identificador conhecido e selecione **Pesquisar**.
4. Quando a pesquisa for concluída, selecione **Baixar** para acessar a resposta da solicitação de acesso do titular dos dados. Selecione **Investigar resultados** para ver mais informações na página Investigação de dados.



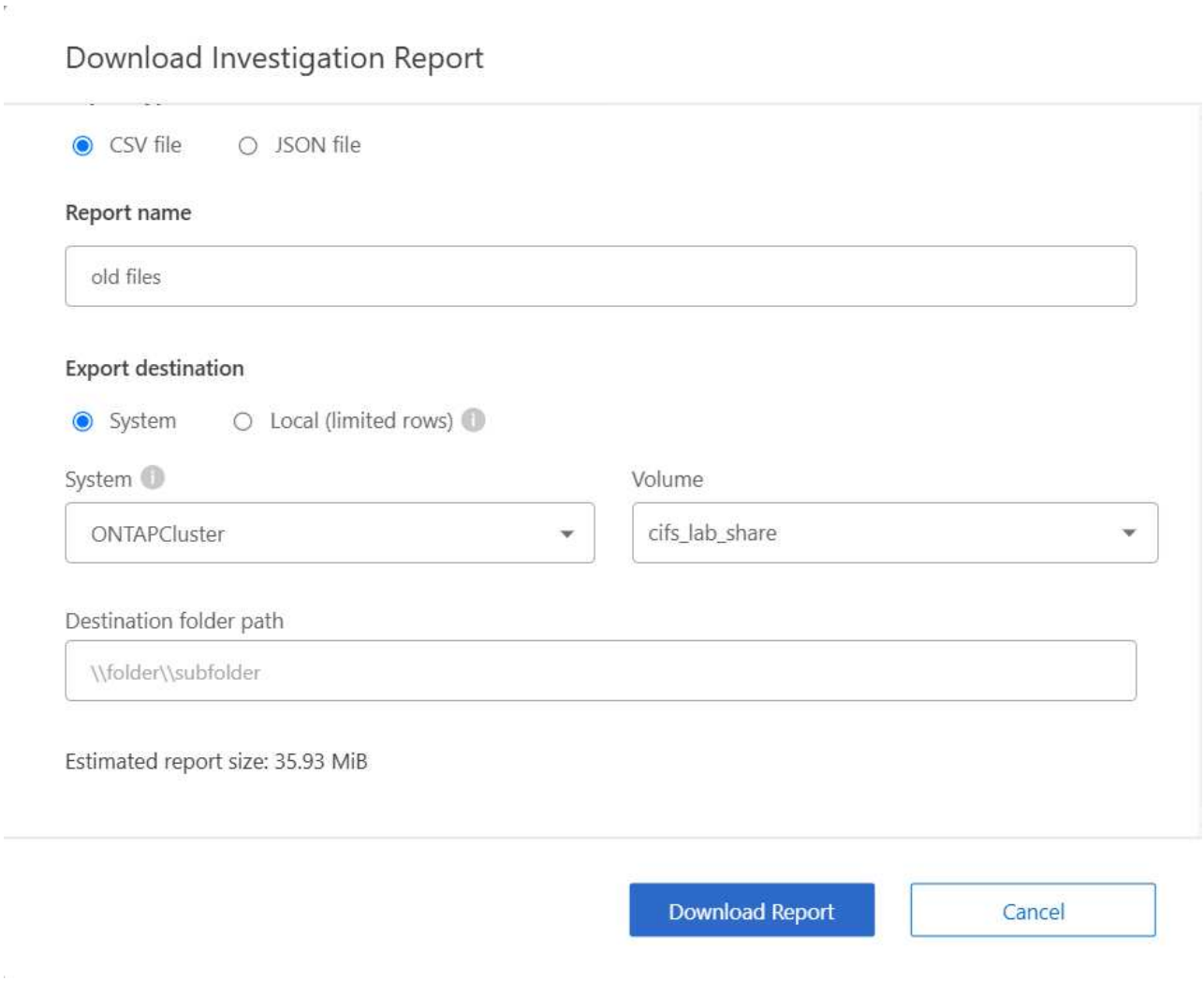
5. Revise os resultados na Classificação de Dados ou baixe-os como um relatório selecionando o ícone de download.

   a. Ao selecionar o ícone de download, configure suas configurações de download:
      - Escolha o formato do filme: CSV ou JSON
      - Digite um **Nome do relatório**
      - Escolha o destino da exportação: **Sistema** ou sua máquina **Local**.

        Se você escolher sistema, todos os dados serão baixados. Você também deve selecionar o **Sistema**, **Volume** e **Caminho da pasta de destino**.

   Se você escolher **Local**, o relatório será limitado às primeiras 10.000 linhas de dados não estruturados; 5.000 linhas de dados não estruturados e 1.000 linhas de dados estruturados.

   a. Selecione **Baixar relatório** para iniciar o download.



Relatório da Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)

O Relatório da Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) pode ajudar você a identificar arquivos que contêm informações de saúde. Ele foi desenvolvido para auxiliar a sua organização a cumprir as leis de privacidade de dados da HIPAA. As informações que a Classificação de Dados procura incluem:

- Padrão de referência de saúde
- Código médico CID-10-CM
- Código médico CID-9-CM
- RH - Categoria Saúde
- Categoria de dados de aplicação de saúde

O relatório inclui as seguintes informações:

- Visão geral: Quantos arquivos contêm informações de saúde e em quais sistemas.
- Criptografia: A porcentagem de arquivos contendo informações de saúde que estão em sistemas criptografados ou não criptografados. Estas informações são específicas do Cloud Volumes ONTAP.
- Proteção contra ransomware: a porcentagem de arquivos contendo informações de saúde que estão em sistemas que têm ou não proteção contra ransomware ativada. Estas informações são específicas do

Cloud Volumes ONTAP.

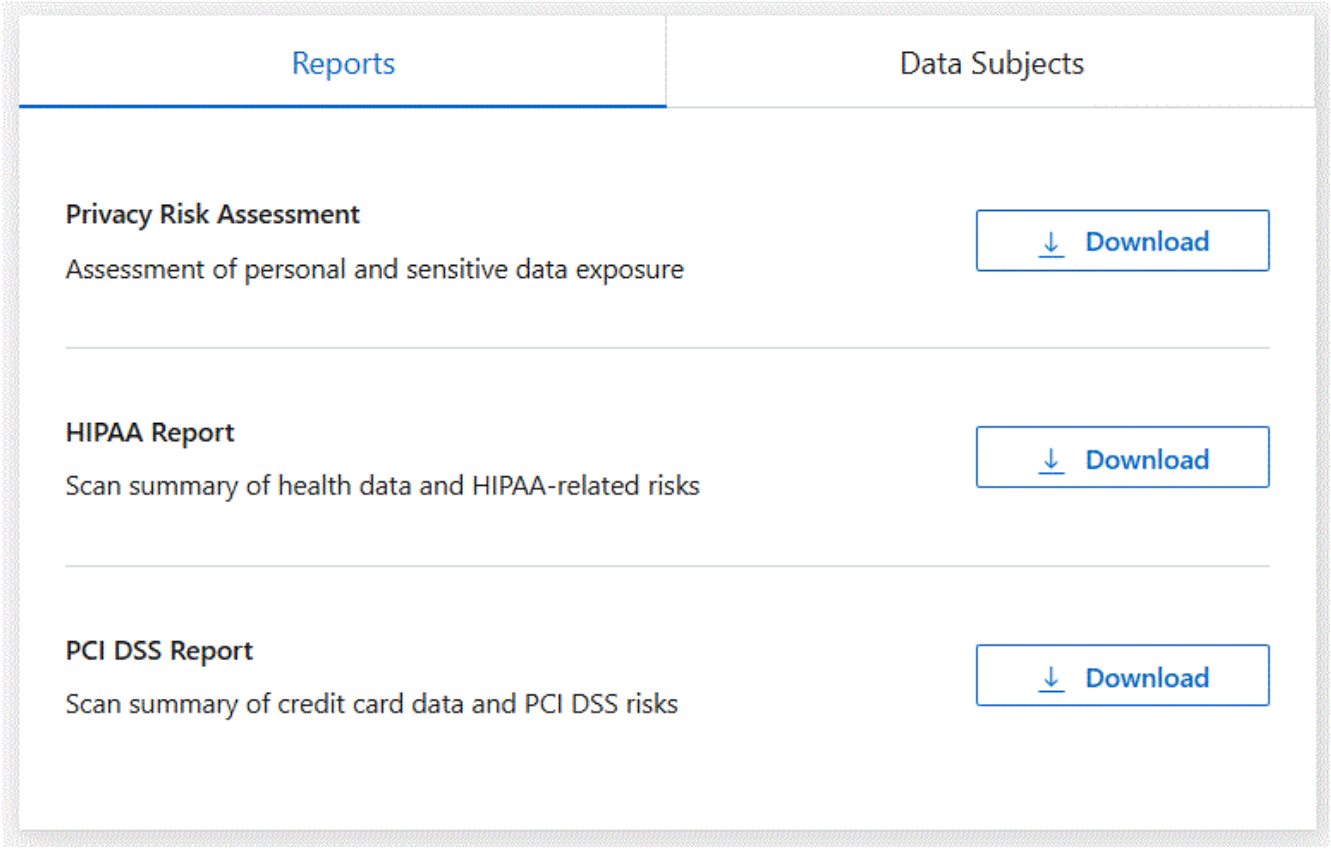
- Retenção: O período em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter informações de saúde por mais tempo do que o necessário para processá-las.
- Distribuição de informações de saúde: os sistemas onde as informações de saúde foram encontradas e se a criptografia e a proteção contra ransomware estão habilitadas.

Gerar o Relatório HIPAA

Acesse a aba Conformidade para gerar o relatório.

Passos

1. No menu Classificação de Dados, selecione **Conformidade**.
2. Localize o **Painel Relatórios**. Selecione o ícone de download ao lado de **Relatório HIPAA**.



Resultado

A classificação de dados gera um relatório em PDF.

Relatório do Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS)

O relatório do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) pode ajudar você a identificar a distribuição de informações de cartão de crédito em seus arquivos.

O relatório inclui as seguintes informações:

- Visão geral: Quantos arquivos contêm informações de cartão de crédito e em quais sistemas.

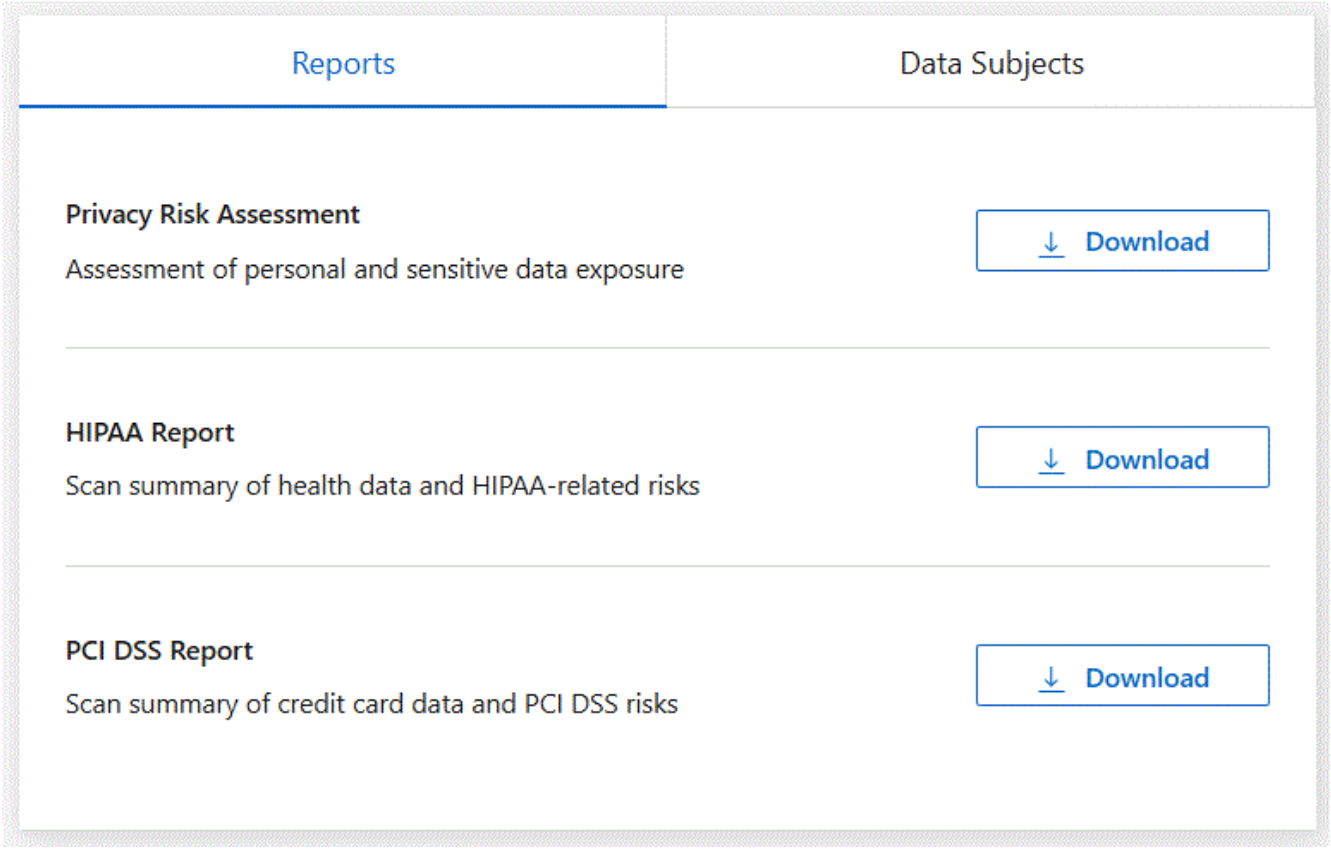
- Criptografia: A porcentagem de arquivos contendo informações de cartão de crédito que estão em sistemas criptografados ou não criptografados. Estas informações são específicas do Cloud Volumes ONTAP.
- Proteção contra ransomware: a porcentagem de arquivos contendo informações de cartão de crédito que estão em sistemas que têm ou não proteção contra ransomware ativada. Estas informações são específicas do Cloud Volumes ONTAP.
- Retenção: O período em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter informações de cartão de crédito por mais tempo do que o necessário para processá-las.
- Distribuição de informações de cartão de crédito: os sistemas onde as informações do cartão de crédito foram encontradas e se a criptografia e a proteção contra ransomware estão habilitadas.

Gerar o Relatório PCI DSS

Acesse a aba Conformidade para gerar o relatório.

Passos

1. No menu Classificação de Dados, selecione **Conformidade**.
2. Localize o **Painel Relatórios**. Selecione o ícone de download ao lado de **Relatório PCI DSS**.



Resultado

A Classificação de Dados gera um relatório em PDF que você pode revisar e enviar a outros grupos, conforme necessário.

Relatório de Avaliação de Risco de Privacidade

O Relatório de Avaliação de Risco de Privacidade fornece uma visão geral do status de risco de privacidade da sua organização, conforme exigido por regulamentações de privacidade como GDPR e CCPA.

O relatório inclui as seguintes informações:

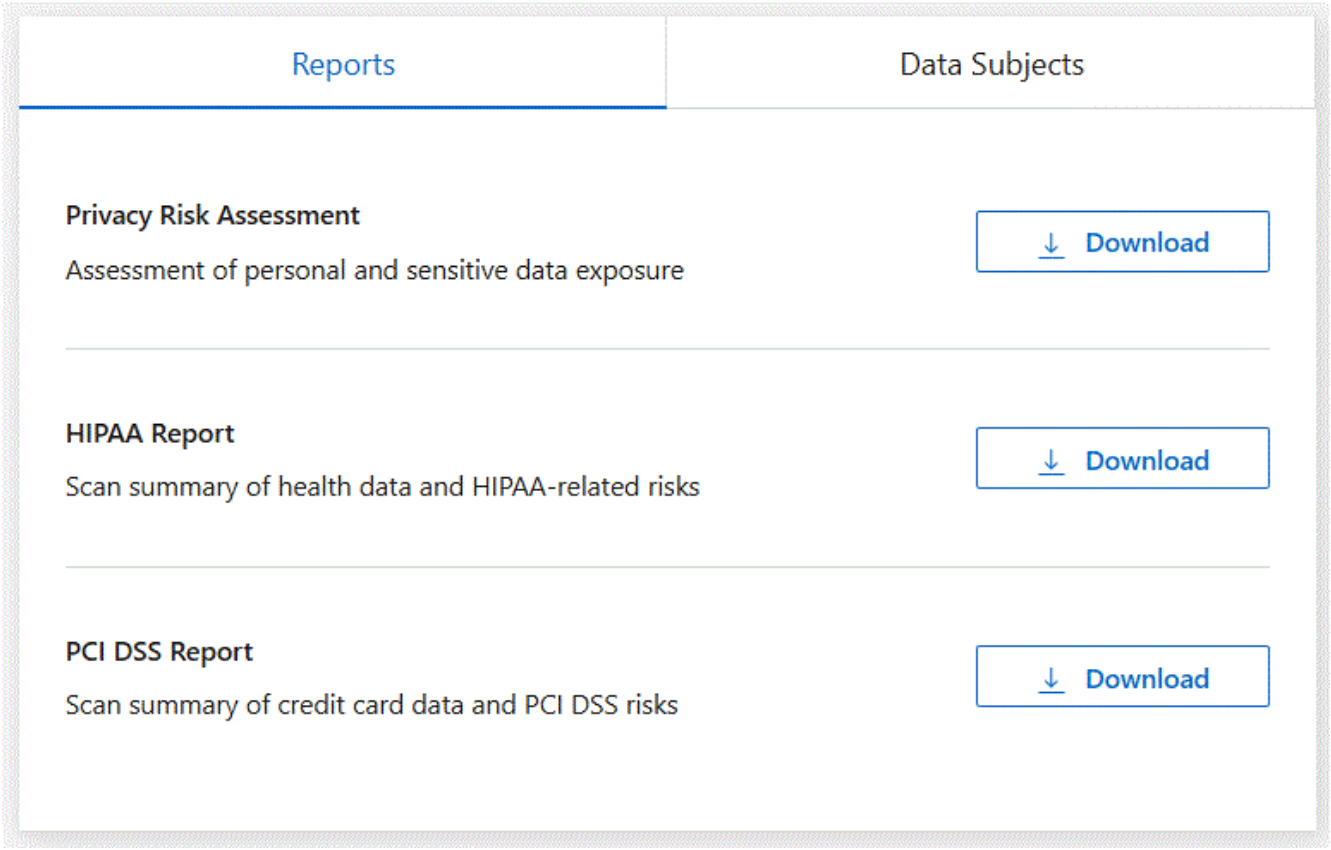
- Status de conformidade: uma pontuação de gravidade e a distribuição de dados, sejam eles não confidenciais, pessoais ou pessoais confidenciais.
- Visão geral da avaliação: Uma análise dos tipos de dados pessoais encontrados, bem como das categorias de dados.
- Assuntos dos dados nesta avaliação: O número de pessoas, por local, para as quais foram encontrados identificadores nacionais.

Gerar o Relatório de Avaliação de Risco de Privacidade

Acesse a aba Conformidade para gerar o relatório.

Passos

1. No menu Classificação de Dados, selecione **Conformidade**.
2. Localize o **Painel Relatórios**. Selecione o ícone de download ao lado de **Relatório de Avaliação de Risco de Privacidade**.



Resultado

A Classificação de Dados gera um relatório em PDF que você pode revisar e enviar a outros grupos, conforme necessário.

Pontuação de gravidade

A Classificação de Dados calcula a pontuação de gravidade do Relatório de Avaliação de Risco de Privacidade com base em três variáveis:

- A porcentagem de dados pessoais em relação a todos os dados.
- A porcentagem de dados pessoais sensíveis em relação a todos os dados.
- A porcentagem de arquivos que incluem titulares de dados, determinada por identificadores nacionais, como documentos de identidade nacionais, números de previdência social e números de identificação fiscal.

A lógica usada para determinar a pontuação é a seguinte:

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

Monitore a integridade da NetApp Data Classification.

O painel de controle do NetApp Data Classification Health Monitor fornece monitoramento em tempo real e insights sobre o desempenho. O Monitor de Saúde coleta informações sobre sua infraestrutura de Classificação de Dados, integridade do sistema, métricas de uso e dados de utilização, permitindo que você identifique e corrija problemas.

Informações do Monitor de Saúde

O painel de controle do Monitor de Saúde apresenta informações em quatro categorias.

- **Estado da infraestrutura**

  Visualize informações como o status da versão, a estabilidade do sistema, o tipo de implantação e a escala da máquina.

- **Recipientes problemáticos**

Analise o campo de contêineres problemáticos para obter informações sobre contêineres que são interrompidos ou reiniciados com frequência. Utilize essas informações para investigar os contêineres específicos.

- **Informações do sistema**

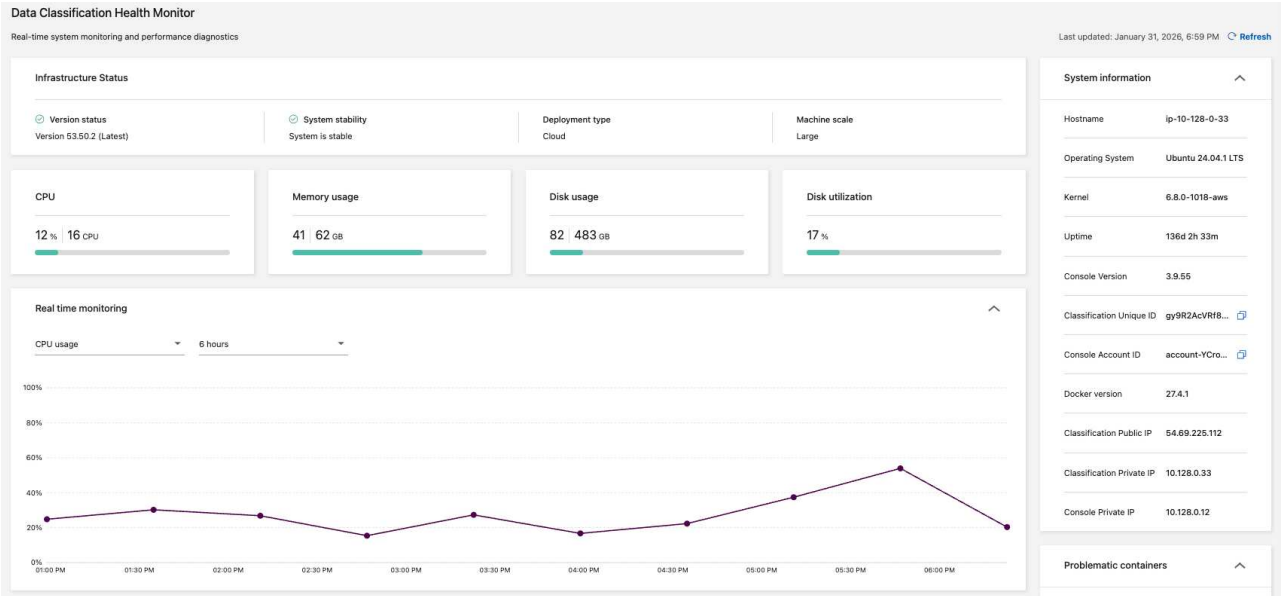
  O painel de informações do sistema captura informações críticas sobre o NetApp Console e a Classificação de Dados, como endereços IP públicos e privados, nome do host, sistema operacional, versão do Console e ID do Console.

- **Uso e utilização**

  Analise o uso da CPU, a utilização do disco e o uso da memória. Esses valores são exibidos em unidades de armazenamento (GB) ou em porcentagem do uso total. Se algum campo exibir um aviso, selecione-o para obter informações e recomendações de correção.

Acesse o painel de controle do Monitor de Saúde.

1. Em Classificação de Dados, selecione **Configuração**.
2. Na seção **Configuração**, selecione **Monitor de integridade da classificação de dados**.
3. No painel do Monitor de Saúde, você pode:
   - Analise o uso e a utilização. Se alguma métrica de uso ou utilização exibir avisos, selecione o aviso para obter recomendações sobre como resolver o problema.
   - Alterne o gráfico para exibir o uso da CPU, a utilização do disco e o uso da memória. Você pode alterar o eixo x para exibir o conteúdo ao longo de horas (6, 12 ou 24) ou dias (2, 7 ou 14).
   - Atualize o painel para visualizar as métricas de dados mais recentes.



Gerenciar classificação de dados

Excluir diretórios específicos das verificações de NetApp Data Classification

Se quiser que a NetApp Data Classification exclua diretórios específicos das verificações, você pode adicionar esses nomes de diretório a um arquivo de configuração. Depois de aplicar essa alteração, o mecanismo de Classificação de Dados exclui esses diretórios das verificações.

Por padrão, as verificações de Classificação de Dados excluem dados de instantâneos de volume, que são idênticos à sua origem no volume.

Fontes de dados suportadas

A exclusão de diretórios específicos de varreduras de Classificação de Dados é suportada para compartilhamentos NFS e CIFS nas seguintes fontes de dados:

- ONTAP local
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Compartilhamentos gerais de arquivos

Defina os diretórios a serem excluídos da verificação

Antes de poder excluir diretórios da verificação de classificação, você precisa fazer login no sistema de Classificação de Dados para poder editar um arquivo de configuração e executar um script. Veja como"faça login no sistema de classificação de dados" dependendo se você instalou manualmente o software em uma máquina Linux ou se implantou a instância na nuvem.

Considerações

- Você pode excluir no máximo 50 caminhos de diretório por sistema de classificação de dados.
- Excluir caminhos de diretório pode afetar o tempo de verificação.

Passos

1. No sistema de classificação de dados, vá para "/opt/netapp/config/custom_configuration" e abra o arquivo `data_provider.yaml` .
2. Na seção "data_providers", na linha "exclude:", insira os caminhos de diretório a serem excluídos. Por exemplo:

```
exclude:
- "folder1"
- "folder2"
```

Não modifique mais nada neste arquivo.

3. Salve as alterações no arquivo.
4. Acesse "/opt/netapp/Datasense/tools/customer_configuration/data_providers" e execute o seguinte script:

```
update_data_providers_from_config_file.sh
```

+ Este comando confirma os diretórios a serem excluídos da verificação no mecanismo de classificação.

Resultado

Todas as verificações subsequentes dos seus dados excluirão a verificação dos diretórios especificados.

Você pode adicionar, editar ou excluir itens da lista de exclusão usando estas mesmas etapas. A lista de exclusões revisada será atualizada depois que você executar o script para confirmar suas alterações.

Exemplos

Configuração 1:

Todas as pastas que contiverem "folder1" em qualquer lugar do nome serão excluídas de todas as fontes de dados.

```
data_providers:
   exclude:
   - "folder1"
```

Resultados esperados para caminhos que serão excluídos:

- /CVO1/pasta1
- /CVO1/nomedapasta1
- /CVO1/pasta10
- /CVO1/*pasta1
- /CVO1/+nomedapasta1
- /CVO1/nãopasta10
- /CVO22/pasta1
- /CVO22/nomedapasta1
- /CVO22/pasta10

Exemplos de caminhos que não serão excluídos:

- /CVO1/*pasta
- /CVO1/nomedapasta
- /CVO22/*pasta20

Configuração 2:

Todas as pastas que contiverem apenas "*pasta1" no início do nome serão excluídas.

```
data_providers:
   exclude:
   - "\\*folder1"
```

Resultados esperados para caminhos que serão excluídos:

- /CVO/*pasta1
- /CVO/*nomedapasta1
- /CVO/*pasta10

Exemplos de caminhos que não serão excluídos:

- /CVO/pasta1
- /CVO/nomedapasta1
- /CVO/não*pasta10

Configuração 3:

Todas as pastas na fonte de dados "CVO22" que contiverem "folder1" em qualquer lugar do nome serão excluídas.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

Resultados esperados para caminhos que serão excluídos:

- /CVO22/pasta1
- /CVO22/nomedapasta1
- /CVO22/pasta10

Exemplos de caminhos que não serão excluídos:

- /CVO1/pasta1
- /CVO1/nomedapasta1
- /CVO1/pasta10

Escapando caracteres especiais em nomes de pastas

Se você tiver um nome de pasta que contenha um dos seguintes caracteres especiais e quiser excluir dados dessa pasta da verificação, será necessário usar a sequência de escape \\ antes do nome da pasta.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
Por exemplo:
```

Caminho na fonte: `/project/*not_to_scan`

Sintaxe no arquivo de exclusão: `"\\*not_to_scan"`

Ver a lista de exclusões atual

É possível que o conteúdo do `data_provider.yaml` arquivo de configuração seja diferente do que realmente foi confirmado após a execução do `update_data_providers_from_config_file.sh` roteiro. Para visualizar a lista atual de diretórios que você excluiu da verificação de Classificação de Dados, execute o seguinte comando em "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Defina IDs de grupo adicionais como abertos à organização na NetApp Data Classification

Quando IDs de grupo (GIDs) são anexados a arquivos ou pastas em compartilhamentos de arquivos NFS, eles definem as permissões para o arquivo ou pasta; como se eles são "abertos à organização". Se alguns GIDs não estiverem configurados inicialmente com o nível de permissão "Aberto à organização", você poderá adicionar essa permissão ao GID para que todos os arquivos e pastas que tenham esse GID anexado sejam considerados "abertos à organização".

Depois que você fizer essa alteração e o NetApp Data Classification verificar novamente seus arquivos e pastas, todos os arquivos e pastas que tiverem essas IDs de grupo anexadas mostrarão essa permissão na página Detalhes da investigação e também aparecerão nos relatórios em que você estiver exibindo permissões de arquivo.

Para ativar essa funcionalidade, você precisa fazer login no sistema de Classificação de Dados para poder editar um arquivo de configuração e executar um script. Veja como"faça login no sistema de classificação de dados" dependendo se você instalou manualmente o software em uma máquina Linux ou se implantou a instância na nuvem.

Adicione a permissão "aberto à organização" aos IDs de grupo

Você precisa ter os números de ID do grupo (GIDs) antes de iniciar esta tarefa.

Passos

1. No sistema de classificação de dados, vá para "/opt/netapp/config/custom_configuration" e abra o arquivo `data_provider.yaml` .
2. Na linha "organization_group_ids: []" adicione os IDs do grupo. Por exemplo:

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   Não altere mais nada neste arquivo.
3. Salve as alterações no arquivo.
4. Acesse "/opt/netapp/Datasense/tools/customer_configuration/data_providers" e execute o seguinte script:

```
update_data_providers_from_config_file.sh
```

Este comando confirma as permissões revisadas do ID do grupo para o mecanismo de classificação.

Resultado

Todas as verificações subsequentes dos seus dados identificarão arquivos ou pastas que tenham esses IDs de grupo anexados como "abertos à organização".

Você pode editar a lista de IDs de grupo e excluir quaisquer IDs de grupo que você adicionou anteriormente usando estas mesmas etapas. A lista revisada de IDs de grupo será atualizada depois que você executar o script para confirmar suas alterações.

Ver a lista atual de IDs de grupo

É possível que o conteúdo do `data_provider.yaml` arquivo de configuração para diferir do que realmente foi confirmado após a execução do `update_data_providers_from_config_file.sh` roteiro. Para visualizar a lista atual de IDs de grupo que você adicionou à Classificação de Dados, execute o seguinte comando em "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Personalize a definição de dados obsoletos na NetApp Data Classification.

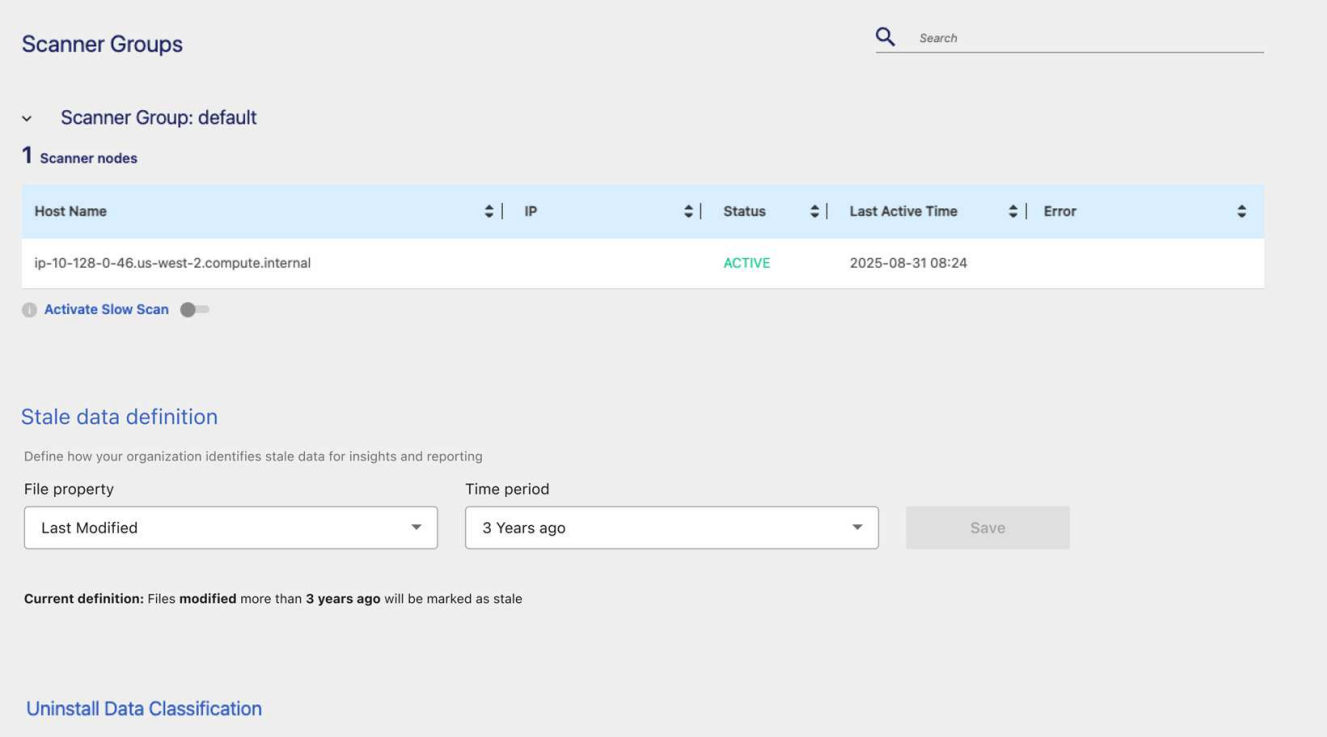
A NetApp Data Classification identifica dados obsoletos para ajudar você a identificar oportunidades de economia e riscos de governança. Como a definição de dados obsoletos pode variar em diferentes contextos organizacionais, você pode personalizar a forma como a Classificação de Dados define dados obsoletos.

Dados obsoletos podem ser definidos com base em quando foram *acessados pela última vez* ou *modificados pela última vez*. Os períodos de tempo selecionados variam de 6 meses atrás a 10 anos atrás.

Por padrão, os dados são considerados obsoletos se a última modificação ocorreu há três anos.

Defina dados obsoletos.

1. Em Resiliência a Ransomware, selecione **Configuração**.
2. Na página de Configuração, role até o cabeçalho **Definição de dados obsoletos**.
3. No menu suspenso **Propriedades do arquivo**, escolha se deseja definir dados obsoletos com base na data do **Último acesso** ou da **Última modificação**.
4. Selecione o período de tempo para a definição de dados obsoletos.



5. Selecione **Salvar**.

Remover fontes de dados da NetApp Data Classification

Se necessário, você pode impedir que o NetApp Data Classification verifique um ou mais sistemas, bancos de dados ou grupos de compartilhamento de arquivos.

Desativar varreduras para um sistema

Quando você desativa as verificações, a Classificação de Dados não verifica mais os dados no sistema e remove os insights indexados da instância da Classificação de Dados. Os dados do próprio sistema não são excluídos.

1. Na página *Configuração*, selecione o botão na linha do sistema e então **Desativar Classificação de Dados**.

Você também pode desabilitar as verificações de um sistema no painel Serviços ao selecionar o sistema.

Remover um banco de dados da Classificação de Dados

Se você não precisar mais verificar um determinado banco de dados, poderá excluí-lo da interface de Classificação de Dados e interromper todas as verificações.

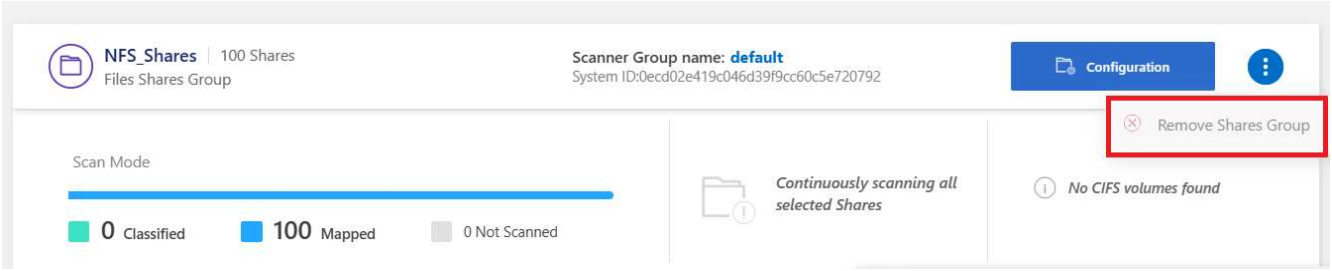
1. Na página *Configuração*, selecione o botão na linha do banco de dados e então **Remover Servidor de BD**.

Remover um grupo de compartilhamentos de arquivos da Classificação de Dados

Se não quiser mais verificar arquivos de usuário de um grupo de compartilhamento de arquivos, você pode excluir o Grupo de Compartilhamentos de Arquivos da interface de Classificação de Dados e interromper todas as verificações.

Passos

1. Na página *Configuração*, selecione o botão na linha do Grupo de Compartilhamentos de Arquivos e depois **Remover Grupo de Compartilhamentos de Arquivos**.



2. Selecione **Excluir Grupo de Compartilhamentos** na caixa de diálogo de confirmação.

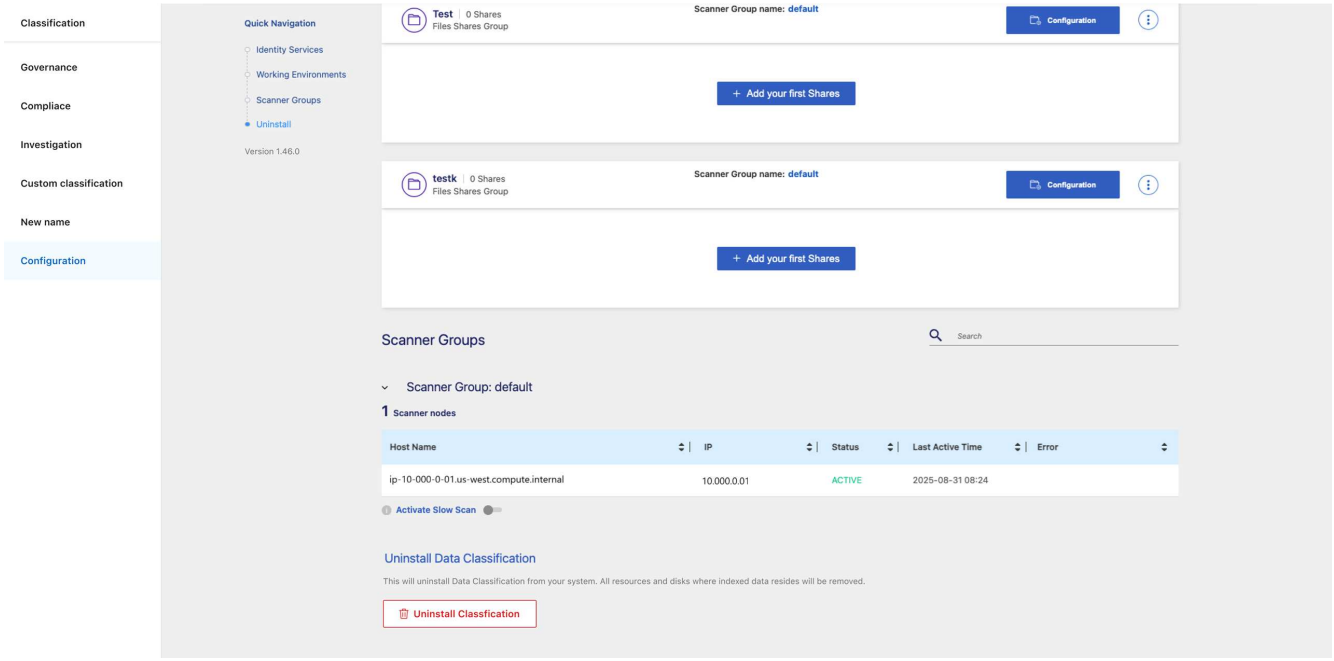
Desinstalar a NetApp Data Classification

Você pode desinstalar o NetApp Data Classification para solucionar problemas ou remover permanentemente o software do host. A exclusão da instância também exclui os discos associados onde os dados indexados residem, o que significa que todas as informações que a Classificação de Dados digitalizou serão excluídas permanentemente.

As etapas que você precisa seguir dependem se você implantou a Classificação de Dados na nuvem ou em um host local.

Desinstalar a Classificação de Dados de um provedor de nuvem

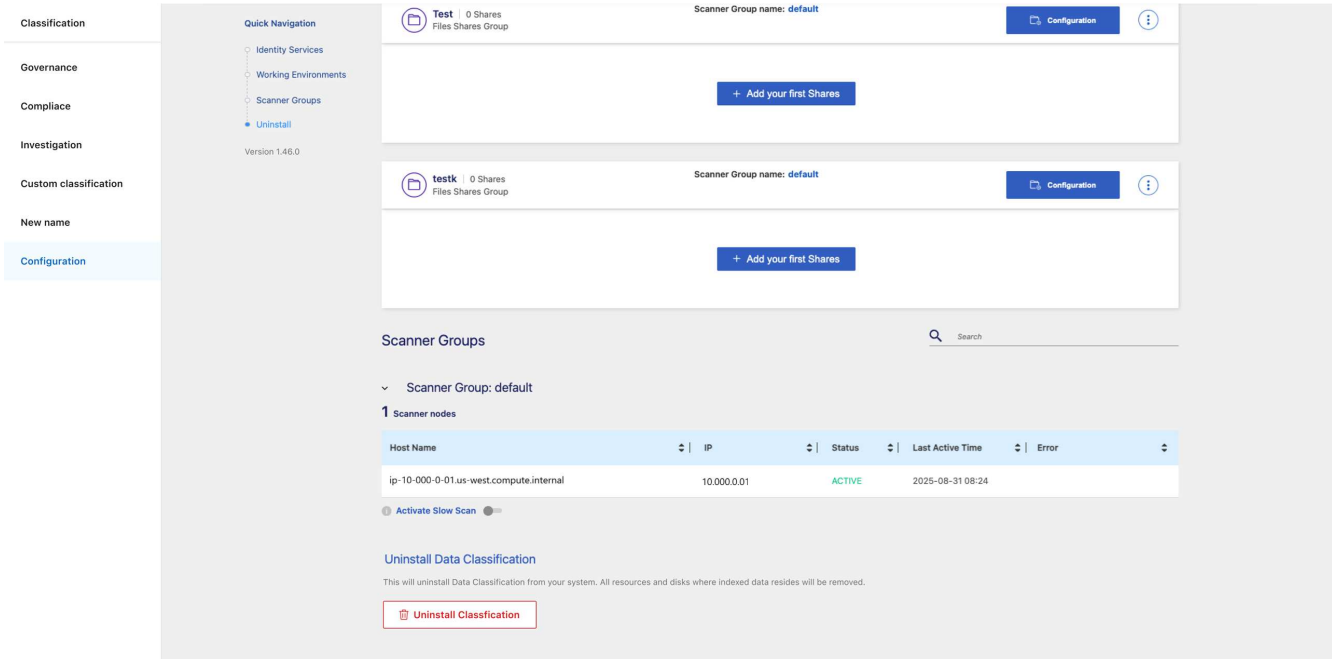
1. Em Classificação de dados, selecione **Configuração**.
2. Na parte inferior da página de configuração, selecione **Desinstalar classificação**.



3. Na caixa de diálogo, digite "desinstalar" para prosseguir com a desconexão da instância de Classificação de Dados do agente do Console. Selecione **Desinstalar** para confirmar.
4. Na caixa de diálogo *Desinstalar Classificação*, digite **uninstall** para confirmar que deseja desconectar a instância de Classificação de Dados do agente do Console e selecione **Desinstalar**.
5. Para finalizar o processo de desinstalação, acesse o console do seu provedor de nuvem e exclua a instância de Classificação de Dados. A instância é denominada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Desinstalar a Classificação de Dados de uma implantação local

1. Em Classificação de dados, selecione **Configuração**.
2. Na parte inferior da página de configuração, selecione **Desinstalar classificação**.



3. Na caixa de diálogo, digite "desinstalar" para prosseguir com a desconexão da instância de Classificação de Dados do agente do Console. Selecione **Desinstalar** para confirmar.
4. Para desinstalar o software do host, execute o `cleanup.sh` script na máquina host de Classificação de Dados, por exemplo:

```
cleanup.sh
```

O script está localizado no `/install/light_probe/onprem_installer/cleanup.sh` diretório. Veja como"faça login na máquina host de classificação de dados" .

Referência

Tipos de instância de NetApp Data Classification com suporte

O software NetApp Data Classification deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de software e assim por diante. Ao implantar a Classificação de Dados na nuvem, recomendamos que você use um sistema com características "grandes" para obter funcionalidade completa.

Você pode implantar a Classificação de Dados em um sistema com menos CPUs e menos RAM, mas há algumas limitações ao usar esses sistemas menos potentes. "Saiba mais sobre essas limitações" .

Nas tabelas a seguir, se o sistema marcado como "padrão" não estiver disponível na região onde você está instalando o Data Classification, o próximo sistema na tabela será implantado.

Tipos de instância da AWS

Tamanho do sistema	Especificações	Tipo de instância
Extra grande	32 CPUs, 128 GB de RAM, 1 TiB gp3 SSD	"m6i.8xlarge"(padrão)
Grande	16 CPUs, 64 GB de RAM, SSD de 500 GiB	"m6i.4xlarge"(padrão) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Médio	8 CPUs, 32 GB de RAM, SSD de 200 GiB	"m6i.2xlarge"(padrão) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Pequeno	8 CPUs, 16 GB de RAM, SSD de 100 GiB	"c6a.2xlarge"(padrão) c5a.2xlarge c5.2xlarge c4.2xlarge

Tipos de instância do Azure

Tamanho do sistema	Especificações	Tipo de instância
Extra grande	32 CPUs, 128 GB de RAM, disco do sistema operacional (2.048 GiB, taxa de transferência mínima de 250 MB/s) e disco de dados (SSD de 1 TiB, taxa de transferência mínima de 750 MB/s)	"Standard_D32_v3"(padrão)
Grande	16 CPUs, 64 GB de RAM, SSD de 500 GiB	"Standard_D16s_v3"(padrão)

Tipos de instância do GCP

Tamanho do sistema	Especificações	Tipo de instância
Grande	16 CPUs, 64 GB de RAM, SSD de 500 GiB	"n2-padrão-16"(padrão) n2d-standard-16 n1-standard-16

Metadados coletados de fontes de dados na NetApp Data Classification

A NetApp Data Classification coleta determinados metadados ao executar verificações de classificação nos dados de suas fontes de dados e sistemas. A Classificação de Dados pode acessar a maioria dos metadados necessários para classificar seus dados, mas há algumas fontes nas quais não conseguimos acessar os dados necessários.

	Metadados	CIFS	NFS
Carimbos de tempo	*Tempo de criação*	Disponível	Não disponível (sem suporte no Linux)
	Último horário de acesso	Disponível	Disponível
	Hora da última modificação	Disponível	Disponível
Permissões	*Permissões abertas*	Se o grupo "TODOS" tiver acesso ao arquivo, ele será considerado "Aberto à organização".	Se "Outros" tiver acesso ao arquivo, ele será considerado "Aberto à organização".
	Acesso de usuários/grupos	As informações de usuários e grupos são obtidas do LDAP	Não disponível (os usuários do NFS geralmente são gerenciados localmente no servidor, portanto, o mesmo indivíduo pode ter um UID diferente em cada servidor)

- A Classificação de Dados não extrai o "último horário de acesso" das fontes de dados do banco de dados.
- Versões mais antigas do sistema operacional Windows (por exemplo, Windows 7 e Windows 8) desabilitam a coleta do atributo "hora do último acesso" por padrão, pois isso pode afetar o desempenho do sistema. Quando esse atributo não for coletado, as análises de Classificação de Dados baseadas no "último horário de acesso" serão afetadas. Você pode habilitar a coleta do último horário de acesso nesses sistemas Windows mais antigos, se necessário.

Carimbo de data e hora do último acesso

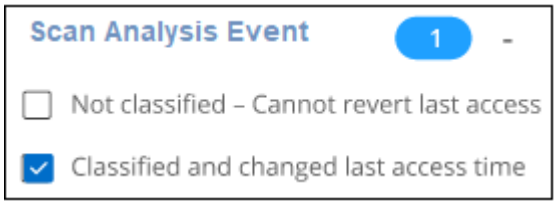
Quando a Classificação de Dados extrai dados de compartilhamentos de arquivos, o sistema operacional considera que está acessando os dados e altera o "último horário de acesso" de acordo. Após a digitalização, a Classificação de Dados tenta reverter o último horário de acesso para o registro de data e hora original. Se a Classificação de Dados não tiver permissões de gravação de atributos no CIFS ou permissões de gravação no NFS, o sistema não poderá reverter o último horário de acesso para o registro de data e hora original. Os volumes ONTAP configurados com SnapLock têm permissões somente leitura e também não podem reverter o último horário de acesso para o registro de data e hora original.

Por padrão, se a Classificação de Dados não tiver essas permissões, o sistema não verificará esses 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. No entanto, se você não se importa se o último horário de acesso será redefinido para o horário original em seus arquivos, você pode selecionar a opção **Verificar quando faltarem permissões de "atributos de gravação"** na parte inferior da página Configuração para que a Classificação

de Dados verifique os volumes independentemente das permissões.

Essa funcionalidade é aplicável a sistemas ONTAP locais, Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for NetApp ONTAP e compartilhamentos de arquivos de terceiros.

Há um filtro na página Investigação chamado *Evento de Análise de Verificação* que permite exibir os arquivos que não foram classificados porque a Classificação de Dados não conseguiu reverter o último horário de acesso ou os arquivos que foram classificados mesmo que a Classificação de Dados não tenha conseguido reverter o último horário de acesso.



As seleções de filtros são:

- "Não classificado — Não é possível reverter o último horário de acesso" - Isso mostra os arquivos que não foram classificados devido à falta de permissões de gravação.
- "Último horário de acesso classificado e atualizado" - Mostra os arquivos que foram classificados e a Classificação de Dados não conseguiu redefinir o último horário de acesso para a data original. Este filtro é relevante somente para ambientes em que você ativou a opção **Verificar quando faltarem permissões de "gravação de atributos"**.

Se necessário, você pode exportar esses resultados para um relatório para ver quais arquivos estão ou não sendo verificados devido às permissões. "Saiba mais sobre relatórios de investigação de dados".

Efetue login no sistema de NetApp Data Classification

Você precisa fazer login no sistema de NetApp Data Classification para poder acessar arquivos de log ou editar arquivos de configuração.

Quando o Data Classification é instalado em uma máquina Linux em suas instalações ou em uma máquina Linux implantada na nuvem, você pode acessar o arquivo de configuração e o script diretamente.

Quando a Classificação de Dados é implantada na nuvem, você precisa fazer SSH para a instância da Classificação de Dados. Faça login no sistema via SSH inserindo o usuário e a senha ou usando a chave SSH fornecida durante a instalação do agente do Console. O comando SSH é:

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
```

- `<path_to_the_ssh_key>`= localização das chaves de autenticação ssh
- `<machine_user>`:
  - Para AWS: use o <ec2-user>
  - Para o Azure: use o usuário criado para a instância do Console
  - Para GCP: use o usuário criado para a instância do Console
- `<datasense_ip>`= Endereço IP da instância da máquina virtual

Você precisa modificar as regras de entrada do grupo de segurança para acessar o sistema na nuvem. Para mais detalhes, consulte:

- "Regras de grupo de segurança na AWS"
- "Regras de grupo de segurança no Azure"
- "Regras de firewall no Google Cloud"

APIs de NetApp Data Classification

Os recursos de NetApp Data Classification disponíveis por meio da interface do usuário da Web também estão disponíveis por meio da API REST.

Há quatro categorias definidas na Classificação de Dados que correspondem às guias na IU:

- Investigação
- Conformidade
- Governança
- Configuração

As APIs na documentação do Swagger permitem que você pesquise, agregue dados, rastreie suas verificações e execute ações como copiar, mover e excluir.

Visão geral

A API permite que você execute as seguintes funções:

- Informações de exportação
  - Tudo o que está disponível na IU pode ser exportado por meio da API (com exceção de relatórios)
  - Os dados são exportados em formato JSON (fácil de analisar e enviar para aplicativos de terceiros, como o Splunk)
- Crie consultas usando instruções "AND" e "OR", inclua e exclua informações e muito mais.

  Por exemplo, você pode localizar arquivos *sem* Informações Pessoais Identificáveis (PII) específicas (funcionalidade não disponível na interface do usuário). Você também pode excluir campos específicos para a operação de exportação.

- Executar ações
  - Atualizar credenciais CIFS
  - Visualizar e cancelar ações

- Verifique novamente os diretórios
- Exportar dados

A API é segura e usa o mesmo método de autenticação da interface do usuário. Você pode encontrar informações sobre a autenticação no"Documentação do REST API" .

Acessando a referência da API do Swagger

Para acessar o Swagger, você precisará do endereço IP da sua instância de Classificação de Dados. No caso de uma implantação na nuvem, você usará o endereço IP público. Então você precisará acessar este endpoint:

https://<ip_de_classificação>/documentação

Exemplo usando as APIs

O exemplo a seguir mostra uma chamada de API para copiar arquivos.

Solicitação de API

Inicialmente, você precisará obter todos os campos e opções relevantes para que um sistema visualize todos os filtros na guia de investigação.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Resposta

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
```

```
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
```

```
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "system-type",
      "operators": [
        "IN",
        "NOT_IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "system",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
```

```
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
```

```
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
```

```
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Usaremos essa resposta em nossos parâmetros de solicitação para filtrar os arquivos desejados que queremos copiar.

Você pode aplicar uma ação em vários itens. Os tipos de ação suportados incluem: mover, excluir e copiar.

Criaremos a ação de cópia:

Solicitação de API

A próxima API é a API de ação e permite que você crie múltiplas ações.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Resposta

A resposta retornará o objeto de ação, então você pode usar as APIs get e delete para obter o status da ação ou cancelá-la.

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

Conhecimento e suporte

Registre-se para obter suporte do NetApp Console

O registro de suporte é necessário para receber suporte técnico específico para o NetApp Console e suas soluções de armazenamento e serviços de dados. O registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP .

O registro para suporte não habilita o suporte da NetApp para um serviço de arquivo do provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta do NetApp Console (seu número de série 960xxxxxxxx de 20 dígitos localizado na página Recursos de suporte no Console).

  Isso serve como seu único ID de assinatura de suporte para qualquer serviço no Console. Cada conta do Console deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (são números de série 909201xxxxxxxxx de 20 dígitos).

  Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo NetApp Console no momento da implantação do Cloud Volumes ONTAP .

Registrar ambos os tipos de números de série habilita recursos como abertura de tickets de suporte e geração automática de casos. O registro é concluído adicionando contas do NetApp Support Site (NSS) ao Console, conforme descrito abaixo.

Registre o NetApp Console para suporte ao NetApp

Para se registrar para obter suporte e ativar o direito ao suporte, um usuário na sua conta do NetApp Console deve associar uma conta do NetApp Support Site ao seu login no Console. A maneira como você se registra para o suporte da NetApp depende se você já tem uma conta no NetApp Support Site (NSS).

Cliente existente com uma conta NSS

Se você for um cliente NetApp com uma conta NSS, basta se registrar para receber suporte pelo Console.

Passos

1. Selecione **Administração** > **Credenciais**.
2. Selecione **Credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do NetApp Support Site (NSS).
4. Para confirmar que o processo de registro foi bem-sucedido, selecione o ícone Ajuda e selecione **Suporte**.

   A página **Recursos** deve mostrar que sua conta do Console está registrada para suporte.

   Observe que outros usuários do Console não verão o mesmo status de registro de suporte se não tiverem associado uma conta do Site de Suporte da NetApp ao seu login. No entanto, isso não significa que sua conta não esteja registrada para suporte. Desde que um usuário na organização tenha seguido essas etapas, sua conta foi registrada.

Cliente existente, mas sem conta NSS

Se você já for um cliente da NetApp com licenças e números de série existentes, mas *nenhuma* conta NSS, será necessário criar uma conta NSS e associá-la ao seu login do Console.

Passos

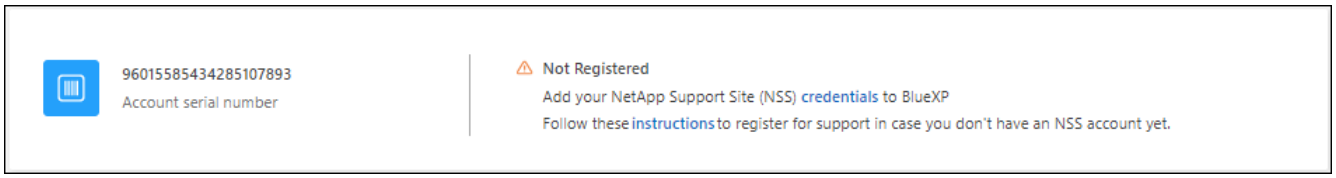
1. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta do Console (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento da conta.
2. Associe sua nova conta NSS ao seu login do Console concluindo as etapas emCliente existente com uma conta NSS .

Novidade na NetApp

Se você é novo na NetApp e não tem uma conta NSS, siga cada etapa abaixo.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.
2. Localize o número de série do seu ID de conta na página de Registro de Suporte.



3. Navegar para "Site de registro de suporte da NetApp" e selecione *Não sou um cliente registrado da NetApp *.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **Linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta da etapa 2 acima, conclua a verificação de segurança e confirme que você leu a Política Global de Privacidade de Dados da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Não deixe de verificar sua caixa de spam caso o e-mail de validação não chegue em alguns minutos.

7. Confirme a ação no e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta no site de suporte da NetApp .

8. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento.

Depois que você terminar

A NetApp entrará em contato com você durante esse processo. Este é um exercício de integração único para novos usuários.

Depois de ter sua conta do Site de Suporte NetApp , associe a conta ao seu login do Console concluindo as etapas emCliente existente com uma conta NSS .

Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP

É necessário associar as credenciais do NetApp Support Site à sua conta do Console para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

  É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer sua conta NSS para que o Console possa carregar sua chave de licença e habilitar a assinatura para o período que você comprou. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

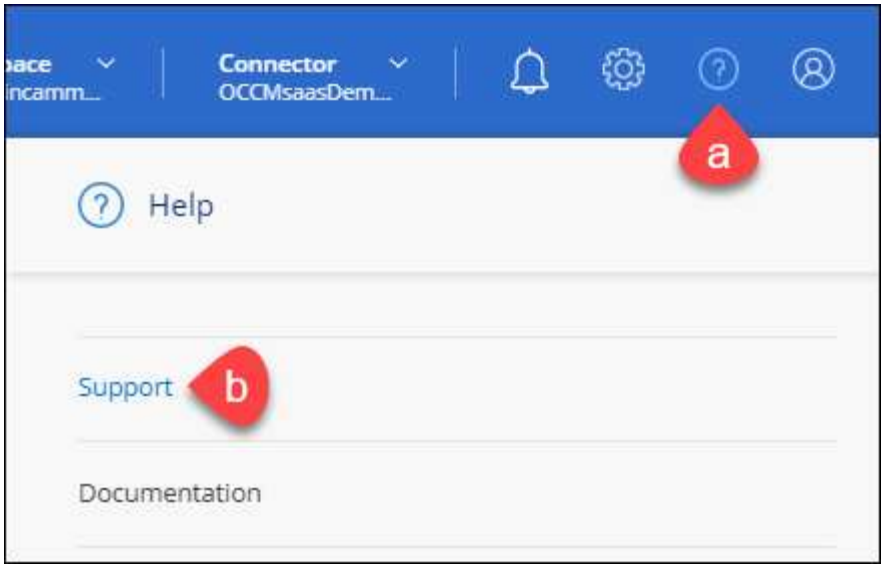
A associação de credenciais do NSS à sua conta do NetApp Console é diferente da associação da conta do NSS a um login de usuário do Console.

Essas credenciais NSS estão associadas ao ID específico da sua conta do Console. Usuários que pertencem à organização Console podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

- Se você tiver uma conta de nível de cliente, poderá adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, poderá adicionar uma ou mais contas NSS, mas elas não poderão ser adicionadas junto com contas de nível de cliente.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.



2. Selecione **Gerenciamento NSS > Adicionar conta NSS**.
3. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

   A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp para realizar o processo de autenticação.

   Essas ações permitem que o Console use sua conta NSS para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

   Observe o seguinte:

   - A conta NSS deve ser uma conta de nível de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS em nível de cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS em nível de cliente e existir uma conta em nível de parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipos diferentes."

   O mesmo é verdadeiro se você tiver contas NSS pré-existentes em nível de cliente e tentar adicionar uma conta em nível de parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no ••• menu.

     Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

Obtenha ajuda para a NetApp Data Classification

A NetApp fornece suporte para o NetApp Console e seus serviços de nuvem de diversas maneiras. Há diversas opções gratuitas de autoatendimento disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu cadastro no suporte inclui suporte técnico remoto por meio de tickets online.

Obtenha suporte para um serviço de arquivo de provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte a documentação desse produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para receber suporte técnico específico para a NetApp e suas soluções de armazenamento e serviços de dados, use as opções de suporte descritas abaixo.

Use opções de autoapoio

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do NetApp Console que você está visualizando no momento.

- "Base de conhecimento"

  Pesquise na base de conhecimento da NetApp para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Participe da comunidade do NetApp Console para acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autossuporte acima, você pode trabalhar com um especialista em suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar o recurso **Criar um caso**, você deve primeiro associar suas credenciais do site de suporte da NetApp ao seu login do console. "Aprenda a gerenciar credenciais associadas ao seu login do Console" .
- Se você estiver abrindo um caso para um sistema ONTAP que tenha um número de série, sua conta NSS deverá estar associada ao número de série desse sistema.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Na página **Recursos**, escolha uma das opções disponíveis em Suporte Técnico:

a. Selecione **Ligue para nós** se quiser falar com alguém por telefone. Você será direcionado para uma página no netapp.com que lista os números de telefone para os quais você pode ligar.

b. Selecione **Criar um caso** para abrir um tíquete com um especialista de suporte da NetApp :

   - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, * NetApp Console* quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do Console.
   - **Sistema**: Se aplicável ao armazenamento, selecione * Cloud Volumes ONTAP* ou **On-Prem** e, em seguida, o ambiente de trabalho associado.

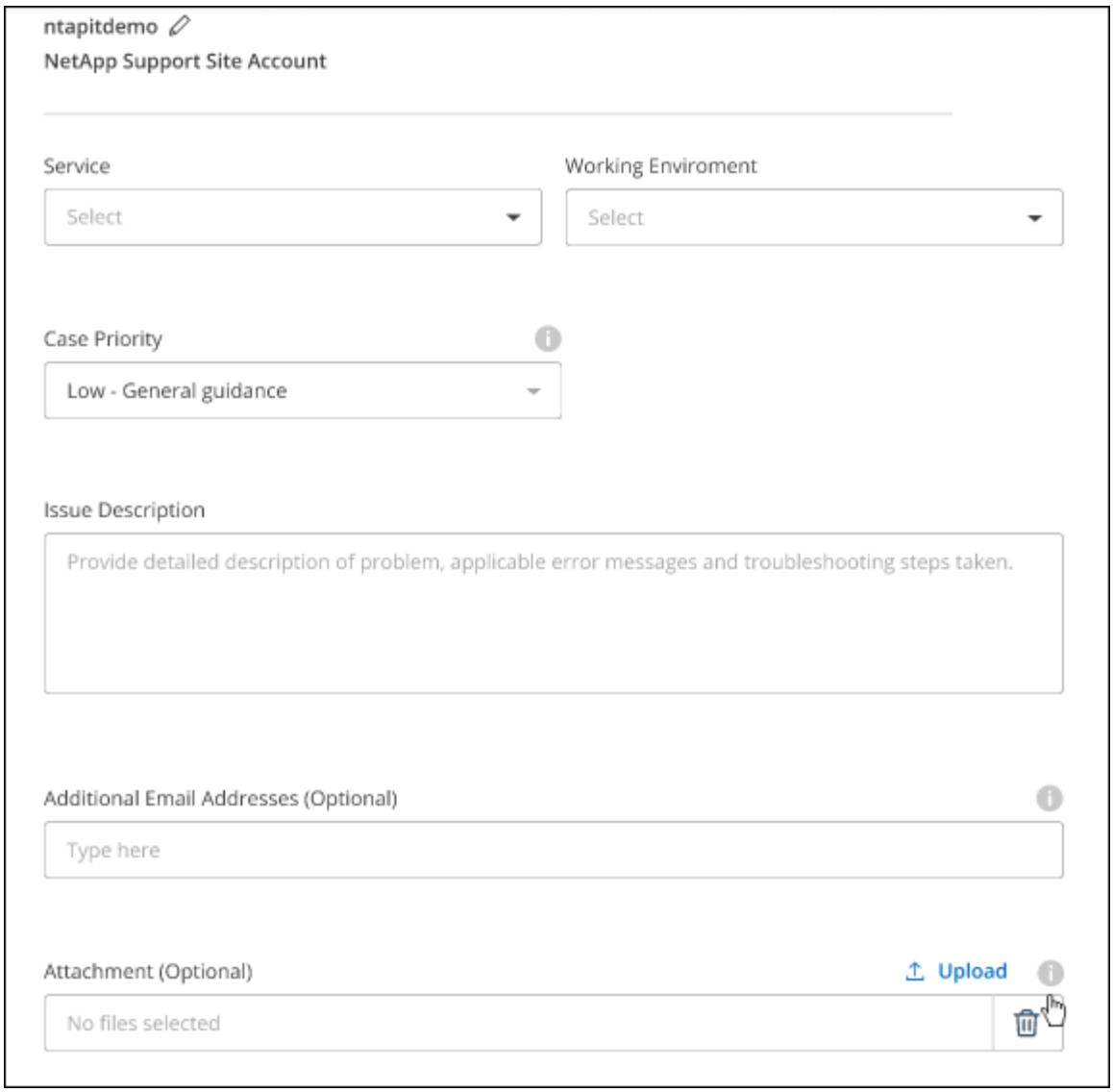
     A lista de sistemas está dentro do escopo da organização do Console e do agente do Console que você selecionou no banner superior.

   - **Prioridade do caso**: escolha a prioridade do caso, que pode ser Baixa, Média, Alta ou Crítica.

     Para saber mais detalhes sobre essas prioridades, passe o mouse sobre o ícone de informações ao lado do nome do campo.

   - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
   - **Endereços de e-mail adicionais**: insira endereços de e-mail adicionais se quiser informar outra pessoa sobre esse problema.
   - **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

     Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois que você terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para obter um histórico dos seus casos de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações chamadas "criar caso de suporte". Um botão na extrema direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa registrada à qual ela está associada não são a mesma empresa registrada para o número de série da conta do NetApp Console (por exemplo, 960xxxx) ou o número de série do ambiente de trabalho. Você pode buscar assistência usando uma das seguintes opções:

- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerencie seus casos de suporte

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do Console. Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta NSS do usuário que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

  Os resultados na tabela refletem os casos relacionados à exibição que você selecionou.
- Você pode adicionar ou remover colunas de interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas fornecem apenas recursos de classificação.

  Veja as etapas abaixo para mais detalhes.
- Em cada caso, oferecemos a possibilidade de atualizar notas do caso ou fechar um caso que ainda não esteja no status Fechado ou Pendente Fechado.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Selecione **Gerenciamento de casos** e, se solicitado, adicione sua conta NSS ao Console.

   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à sua conta de usuário do Console. Esta é a mesma conta NSS que aparece no topo da página **Gerenciamento NSS**.
3. Modifique opcionalmente as informações exibidas na tabela:
   - Em **Casos da organização**, selecione **Exibir** para visualizar todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um período de tempo diferente.
   - Filtrar o conteúdo das colunas.
   - Altere as colunas que aparecem na tabela selecionando e então escolher as colunas que você gostaria de exibir.
4. Gerencie um caso existente selecionando e selecionando uma das opções disponíveis:
   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - **Atualizar notas do caso**: Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

     Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Fechar caso**: Forneça detalhes sobre o motivo pelo qual você está fechando o caso e selecione **Fechar caso**.

Perguntas frequentes sobre a NetApp Data Classification

Estas perguntas frequentes podem ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

NetApp Data Classification

As perguntas a seguir fornecem uma compreensão geral da Classificação de Dados.

Como funciona a Classificação de Dados?

A Classificação de Dados implanta outra camada de IA junto com seu sistema NetApp Console e sistemas de armazenamento. Em seguida, ele verifica os dados em volumes, buckets, bancos de dados e outras contas de armazenamento e indexa os insights de dados encontrados. A classificação de dados utiliza inteligência artificial e processamento de linguagem natural, ao contrário de soluções alternativas que são comumente criadas em torno de expressões regulares e correspondência de padrões.

A classificação de dados usa IA para fornecer compreensão contextual dos dados para detecção e classificação precisas. Ele é impulsionado pela IA porque foi projetado para tipos de dados e escala modernos. Ele também entende o contexto dos dados para fornecer descoberta e classificação fortes e precisas.

"Saiba mais sobre como funciona a Classificação de Dados" .

O Data Classification tem uma API REST e funciona com ferramentas de terceiros?

Sim, o Data Classification tem uma API REST para os recursos suportados na versão do Data Classification que faz parte da plataforma principal do Console. Ver "Documentação do API" .

A classificação de dados está disponível nos mercados de nuvem?

A Classificação de Dados faz parte dos principais recursos do NetApp Console , portanto você não precisa usar os marketplaces para este serviço.

Classificação de dados, digitalização e análise

As perguntas a seguir estão relacionadas ao desempenho da varredura de classificação de dados e à análise.

Com que frequência a Classificação de Dados verifica meus dados?

Embora a verificação inicial dos seus dados possa demorar um pouco, as verificações subsequentes apenas inspecionam as alterações incrementais, o que reduz o tempo de verificação do sistema. A Classificação de Dados verifica seus dados continuamente em rodízio, seis repositórios por vez, para que todos os dados alterados sejam classificados muito rapidamente.

"Aprenda como funcionam as varreduras" .

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

As varreduras de dados têm um impacto insignificante em seus sistemas de armazenamento e em seus dados.

O desempenho da digitalização varia?

O desempenho da verificação pode variar com base na largura de banda da rede e no tamanho médio dos arquivos no seu ambiente. Também pode depender das características de tamanho do sistema host (na nuvem ou no local). Consulte "A instância de classificação de dados" e "Implementando a Classificação de Dados" para maiores informações.

Ao adicionar inicialmente novas fontes de dados, você também pode optar por executar apenas uma verificação de "mapeamento" (Mapping only) em vez de uma verificação de "classificação" completa (Map & Classify). O mapeamento pode ser feito em suas fontes de dados muito rapidamente porque ele não acessa arquivos para ver os dados dentro deles. "Veja a diferença entre um mapeamento e uma varredura de classificação" .

Posso pesquisar meus dados usando a Classificação de Dados?

A Classificação de Dados oferece amplos recursos de pesquisa que facilitam a busca por um arquivo ou dado específico em todas as fontes conectadas. A classificação de dados permite que os usuários pesquisem mais profundamente do que apenas o que os metadados refletem. É um serviço independente de idioma que também pode ler os arquivos e analisar uma infinidade de tipos de dados confidenciais, como nomes e IDs. Por exemplo, os usuários podem pesquisar em armazenamentos de dados estruturados e não estruturados para encontrar dados que podem ter vazado de bancos de dados para arquivos de usuários, violando a política corporativa. As pesquisas podem ser salvas para mais tarde, e políticas podem ser criadas para pesquisar e agir sobre os resultados em uma frequência definida.

Depois que os arquivos de interesse forem encontrados, as características podem ser listadas, incluindo tags, conta do sistema, bucket, caminho do arquivo, categoria (da classificação), tamanho do arquivo, última modificação, status de permissão, duplicatas, nível de sensibilidade, dados pessoais, tipos de dados sensíveis dentro do arquivo, proprietário, tipo de arquivo, tamanho do arquivo, hora de criação, hash do arquivo, se os dados foram atribuídos a alguém que busca sua atenção e muito mais. Filtros podem ser aplicados para filtrar características que não são pertinentes.

A Classificação de Dados também tem controle de acesso baseado em função (RBAC) para permitir que arquivos sejam movidos ou excluídos, se as permissões corretas estiverem presentes. Se as permissões corretas não estiverem presentes, as tarefas podem ser atribuídas a alguém na organização que tenha as permissões corretas.

Gestão e privacidade de classificação de dados

As perguntas a seguir fornecem informações sobre como gerenciar a Classificação de Dados e as configurações de privacidade.

Como habilitar ou desabilitar a Classificação de Dados?

Primeiro, você precisa implantar uma instância do Data Classification no Console ou em um sistema local. Depois que a instância estiver em execução, você poderá habilitar o serviço em sistemas, bancos de dados e outras fontes de dados existentes na guia **Configuração** ou selecionando um sistema específico. "Aprenda como começar" .

A ativação da Classificação de Dados em uma fonte de dados resulta em uma verificação inicial imediata. Os resultados da verificação serão exibidos logo em seguida.

Você pode desabilitar a Classificação de Dados para verificar um sistema individual, banco de dados ou grupo de compartilhamento de arquivos na página Configuração de Classificação de Dados. Ver "Remover fontes de dados da Classificação de Dados" .

Para remover completamente a instância de Classificação de Dados, remova-a manualmente do portal do seu provedor de nuvem ou do local local.

O serviço pode excluir dados de digitalização em determinados diretórios?

Sim. Se você quiser que a Classificação de Dados exclua dados de digitalização que residem em determinados diretórios de fonte de dados, você pode fornecer essa lista ao mecanismo de classificação. Depois de aplicar essa alteração, a Classificação de Dados excluirá os dados de digitalização nos diretórios especificados. "Saber mais" .

Os snapshots que residem em volumes ONTAP são verificados?

Não. A Classificação de Dados não verifica instantâneos porque o conteúdo é idêntico ao conteúdo do volume.

O que acontece se a hierarquização de dados estiver habilitada nos seus volumes ONTAP ?

Quando a Classificação de Dados verifica volumes que têm dados frios em camadas para armazenamento de objetos usando as verificações Somente mapeamento, ela verifica todos os dados — dados que estão em discos locais e dados frios em camadas para armazenamento de objetos. Isso também é válido para produtos que não são da NetApp e que implementam camadas.

A varredura somente de mapeamento não aquece os dados frios; eles permanecem frios e armazenados no armazenamento de objetos. Por outro lado, se você executar a verificação Map & Classify, algumas configurações podem aquecer os dados frios.

Tipos de sistemas de origem e tipos de dados

As perguntas a seguir estão relacionadas aos tipos de armazenamento que podem ser digitalizados e aos tipos de dados que são digitalizados.

Há alguma restrição quando implantado em uma região governamental?

A classificação de dados é suportada quando o agente do Console é implantado em uma região governamental (AWS GovCloud, Azure Gov ou Azure DoD), também conhecido como "modo restrito".

Quais fontes de dados posso escanear se instalar o Data Classification em um site sem acesso à Internet?

> 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" .

A Classificação de Dados só pode escanear dados de fontes de dados locais no site local. Neste momento, a Classificação de Dados pode escanear as seguintes fontes de dados locais no "modo privado" — também

conhecido como site "escuro":

- Sistemas ONTAP locais
- Esquemas de banco de dados
- Armazenamento de objetos que usa o protocolo Simple Storage Service (S3)

Quais tipos de arquivo são suportados?

A Classificação de Dados verifica todos os arquivos em busca de insights de categoria e metadados e exibe todos os tipos de arquivo na seção de tipos de arquivo do painel.

Quando a Classificação de Dados detecta Informações Pessoais Identificáveis (PII) ou quando realiza uma pesquisa DSAR, somente os seguintes formatos de arquivo são suportados:

`.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides`

Que tipos de dados e metadados a Classificação de Dados captura?

A Classificação de Dados permite que você execute uma verificação geral de "mapeamento" ou uma verificação completa de "classificação" em suas fontes de dados. O mapeamento fornece apenas uma visão geral de alto nível dos seus dados, enquanto a classificação fornece uma varredura profunda dos seus dados. O mapeamento pode ser feito em suas fontes de dados muito rapidamente porque ele não acessa arquivos para ver os dados dentro deles.

- **Verificação de mapeamento de dados (Verificação somente de mapeamento)**: A classificação de dados verifica apenas os metadados. Isso é útil para gerenciamento e governança geral de dados, definição rápida de escopo de projetos, grandes propriedades e priorização. O mapeamento de dados é baseado em metadados e é considerado uma varredura **rápida**.

  Após uma verificação rápida, você pode gerar um Relatório de Mapeamento de Dados. Este relatório é uma visão geral dos dados armazenados em suas fontes de dados corporativos para ajudar você a tomar decisões sobre utilização de recursos, migração, backup, segurança e processos de conformidade.

- **Verificação profunda de classificação de dados (verificação de mapa e classificação)**: a classificação de dados verifica os dados usando protocolos padrão e permissão somente leitura em todos os seus ambientes. Arquivos selecionados são abertos e verificados em busca de dados comerciais confidenciais, informações privadas e problemas relacionados a ransomware.

  Após uma verificação completa, há muitos recursos adicionais de Classificação de Dados que você pode aplicar aos seus dados, como visualizar e refinar dados na página Investigação de Dados, pesquisar nomes em arquivos, copiar, mover e excluir arquivos de origem e muito mais.

A Classificação de Dados captura metadados como: nome do arquivo, permissões, hora de criação, último acesso e última modificação. Isso inclui todos os metadados que aparecem na página Detalhes da Investigação de Dados e nos Relatórios de Investigação de Dados.

A classificação de dados pode identificar muitos tipos de dados privados, como informações pessoais (PII) e informações pessoais sensíveis (SPII). Para obter detalhes sobre dados privados, consulteCategorias de dados privados que a Classificação de Dados verifica .

Posso limitar as informações de Classificação de Dados a usuários específicos?

Sim, a Classificação de Dados é totalmente integrada ao NetApp Console. Os usuários do NetApp Console só podem ver informações dos sistemas que eles têm permissão para visualizar, de acordo com suas permissões.

Além disso, se você quiser permitir que determinados usuários apenas visualizem os resultados da verificação de Classificação de Dados sem ter a capacidade de gerenciar as configurações de Classificação de Dados, você pode atribuir a esses usuários a função **Visualizador de classificação** (ao usar o NetApp Console no modo padrão) ou a função **Visualizador de conformidade** (ao usar o NetApp Console no modo restrito). "Saber mais" .

Alguém pode acessar os dados privados enviados entre meu navegador e a Classificação de Dados?

Não. 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 partes da NetApp e não da NetApp não podem lê-los. A Classificação de Dados não compartilhará nenhum dado ou resultado com a NetApp , a menos que você solicite e aprove o acesso.

Os dados digitalizados permanecem no seu ambiente.

Como os dados confidenciais são tratados?

O NetApp não tem acesso a dados confidenciais e não os exibe na interface do usuário. Dados confidenciais são mascarados, por exemplo, os últimos quatro números são exibidos para informações de cartão de crédito.

Onde os dados são armazenados?

Os resultados da verificação são armazenados no Elasticsearch dentro da sua instância de Classificação de Dados.

Como os dados são acessados?

A Classificação de Dados acessa dados armazenados no Elasticsearch por meio de chamadas de API, que exigem autenticação e são criptografadas usando AES-128. Acessar o Elasticsearch diretamente requer acesso root.

Licenças e custos

A pergunta a seguir está relacionada ao licenciamento e aos custos para usar a Classificação de Dados.

Quanto custa a Classificação de Dados?

A classificação de dados é um recurso essencial do NetApp Console . Não é cobrado.

Implantação do agente de console

As perguntas a seguir estão relacionadas ao agente do Console.

O que é o agente do Console?

O agente do Console é um software executado em uma instância de computação na sua conta de nuvem ou no local, que permite que o NetApp Console gerencie com segurança os recursos da nuvem. Você deve implantar um agente do Console para usar a Classificação de Dados.

Onde o agente do Console precisa ser instalado?

Ao verificar dados, o agente do NetApp Console Console precisa ser instalado nos seguintes locais:

- Para Cloud Volumes ONTAP na AWS ou Amazon FSx para ONTAP: o agente do console está na AWS.
- Para Cloud Volumes ONTAP no Azure ou no Azure NetApp Files: o agente do console está no Azure.
- Para Cloud Volumes ONTAP no GCP: o agente do console está no GCP.
- Para sistemas ONTAP locais: o agente do console está local.

Se você tiver dados nesses locais, pode ser necessário usar "vários agentes de console" .

A Classificação de Dados requer acesso a credenciais?

A classificação de dados em si não recupera credenciais de armazenamento. Em vez disso, eles são armazenados no agente do Console.

A Classificação de Dados usa credenciais do plano de dados, por exemplo, credenciais CIFS para montar compartilhamentos antes da digitalização.

A comunicação entre o serviço e o agente do Console usa HTTP?

Sim, a Classificação de Dados se comunica com o agente do Console usando HTTP.

Implantação de classificação de dados

As perguntas a seguir estão relacionadas à instância separada de Classificação de Dados.

Quais modelos de implantação a Classificação de Dados suporta?

O NetApp Console permite que o usuário escaneie e gere relatórios sobre sistemas praticamente em qualquer lugar, incluindo ambientes locais, na nuvem e híbridos. A Classificação de Dados normalmente é implantada usando um modelo SaaS, no qual o serviço é habilitado por meio da interface do Console e não requer instalação de hardware ou software. Mesmo neste modo de implantação de clicar e executar, o gerenciamento de dados pode ser feito independentemente de os armazenamentos de dados estarem no local ou na nuvem pública.

Que tipo de instância ou VM é necessária para a Classificação de Dados?

Quando"implantado na nuvem" :

- Na AWS, a Classificação de Dados é executada em uma instância m6i.4xlarge com um disco GP2 de 500 GiB. Você pode selecionar um tipo de instância menor durante a implantação.
- No Azure, a Classificação de Dados é executada em uma VM Standard_D16s_v3 com um disco de 500 GiB.

- No GCP, a Classificação de Dados é executada em uma VM n2-standard-16 com um disco persistente Standard de 500 GiB.

"Saiba mais sobre como funciona a Classificação de Dados" .

Posso implantar a Classificação de Dados no meu próprio host?

Sim. Você pode instalar o software de classificação de dados em um host Linux que tenha acesso à Internet na sua rede ou na nuvem. Tudo funciona da mesma forma e você continua gerenciando a configuração e os resultados da verificação por meio do Console. Ver"Implementando a Classificação de Dados no local" para requisitos do sistema e detalhes de instalação.

E quanto aos sites seguros sem acesso à internet?

Sim, isso também é suportado. Você pode"implantar a Classificação de Dados em um site local que não tenha acesso à Internet" para sites completamente seguros.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de Privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

- "Aviso para o NetApp Console"
- "Aviso para NetApp Data Classification"

Informações sobre direitos autorais

Informações sobre marcas comerciais