Classificação de dados de uso

NetApp Data Classification

NetApp
February 11, 2026

Índice

Classificação de dados de uso

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

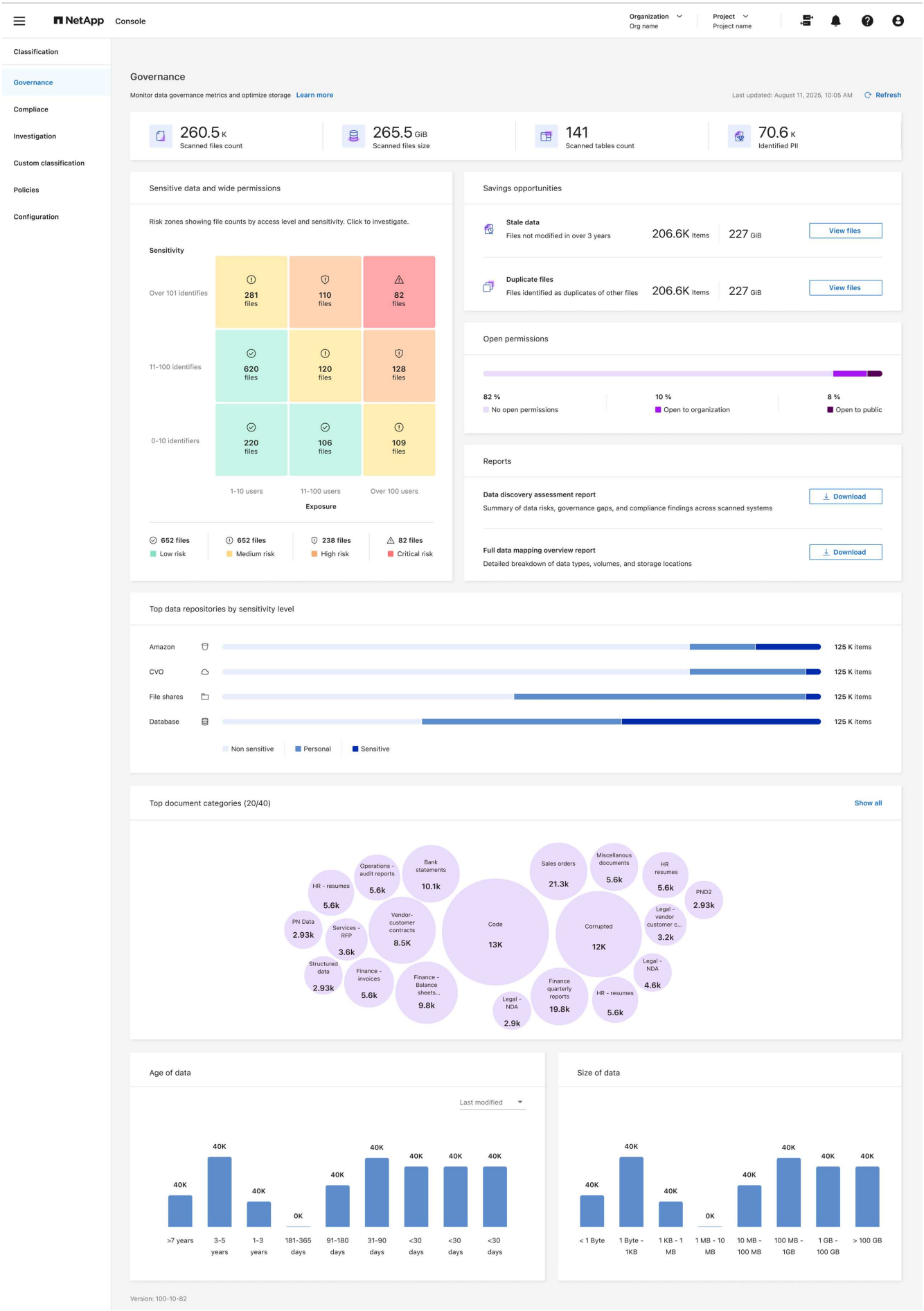
Obtenha controle dos custos relacionados aos dados nos recursos de armazenamento da sua organização. A NetApp Data Classification identifica a quantidade de dados obsoletos, arquivos duplicados e arquivos muito grandes em seus sistemas para que você possa decidir se deseja remover ou colocar alguns arquivos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

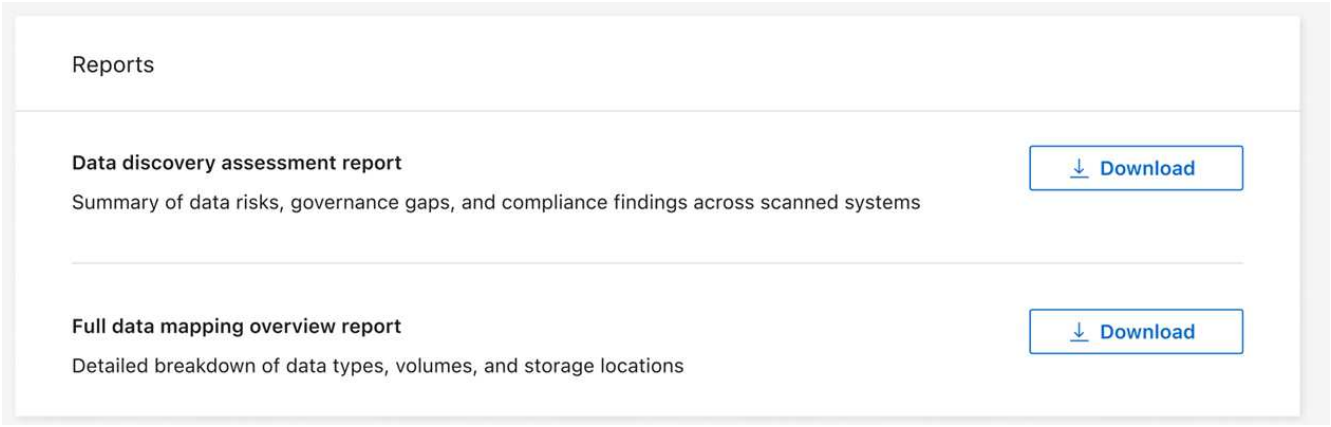
Com o relatório, você pode realizar as seguintes ações:

- 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

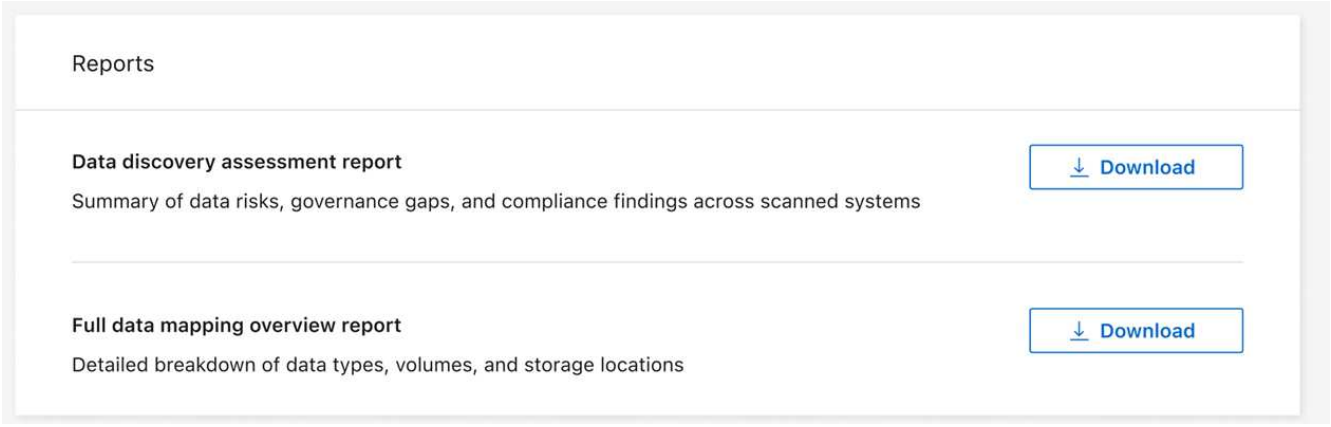
O relatório de visão geral do mapeamento de dados fornece uma visão geral dos dados armazenados em suas fontes de dados corporativos para ajudar você com decisões de migração, backup, segurança e processos de conformidade. O relatório resume todos os sistemas e fontes de dados. Ele também fornece uma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

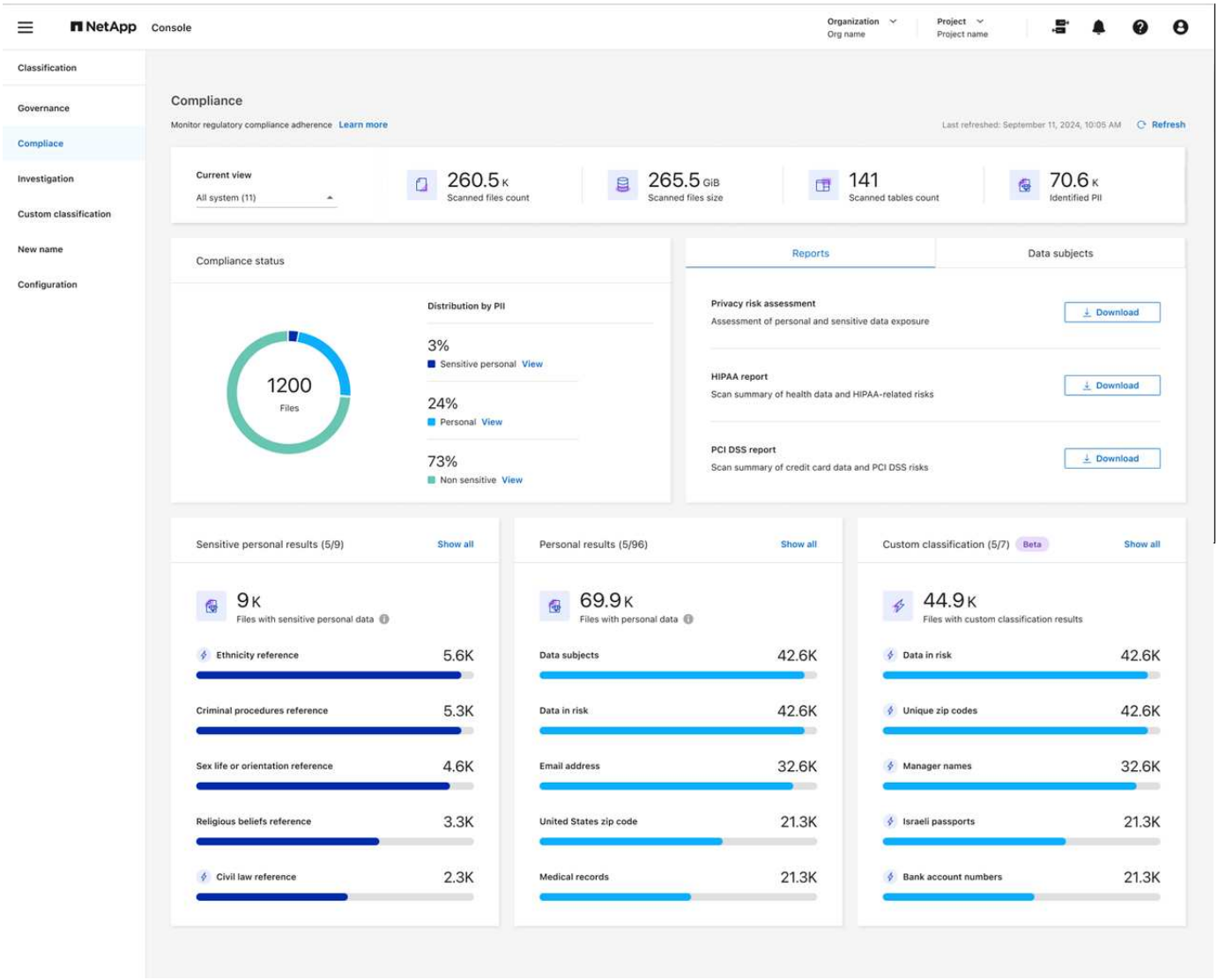
Se alguma de suas fontes de dados implementar a hierarquização de dados, dados antigos que já residem no armazenamento de objetos poderão ser identificados no gráfico *Idade dos Dados*.

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

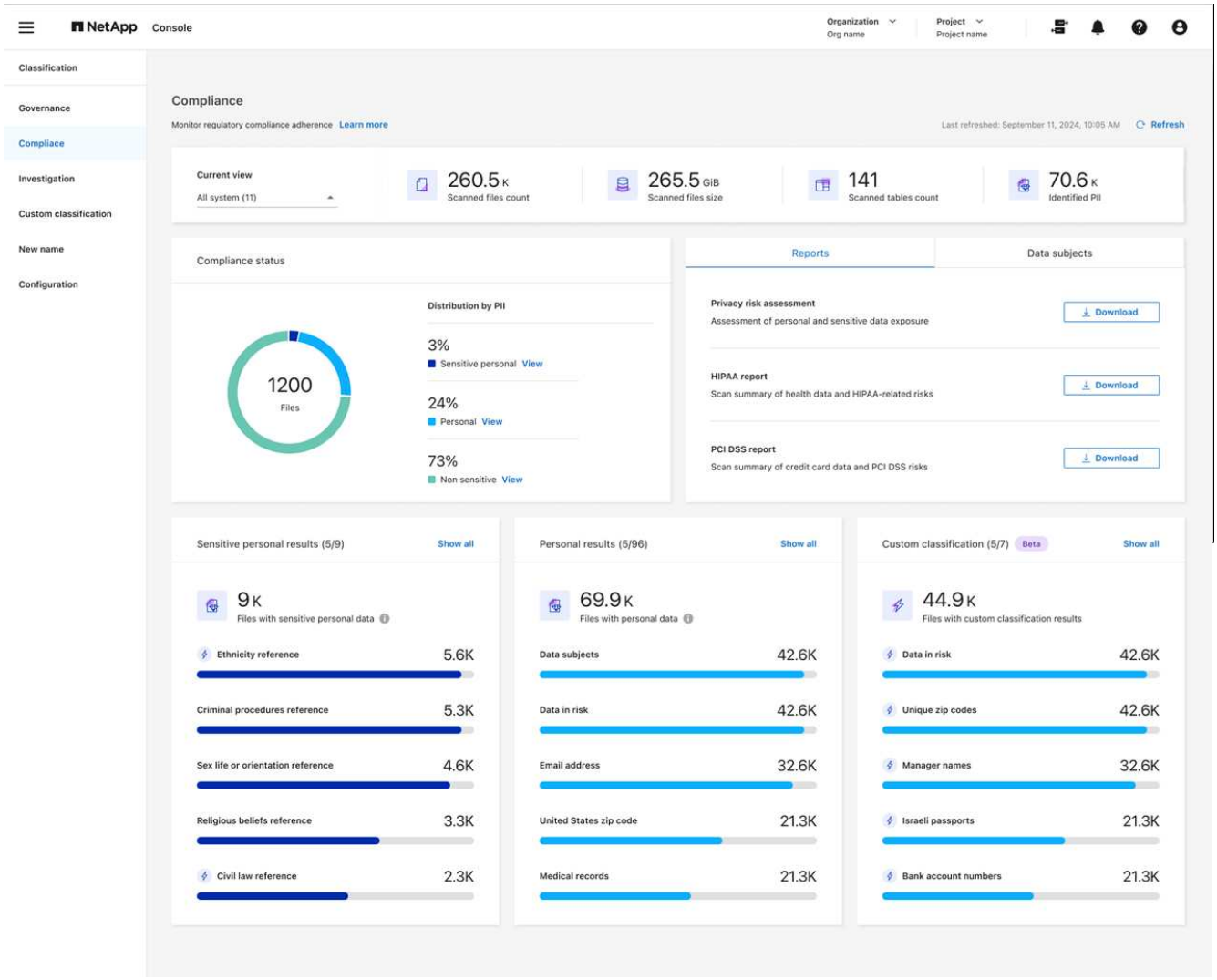
A Classificação de Dados identifica automaticamente palavras, strings e padrões específicos (Regex) dentro dos dados. "Por exemplo, números de cartão de crédito, números de previdência social, números de contas bancárias, senhas e muito mais."A Classificação de Dados identifica esse tipo de informação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

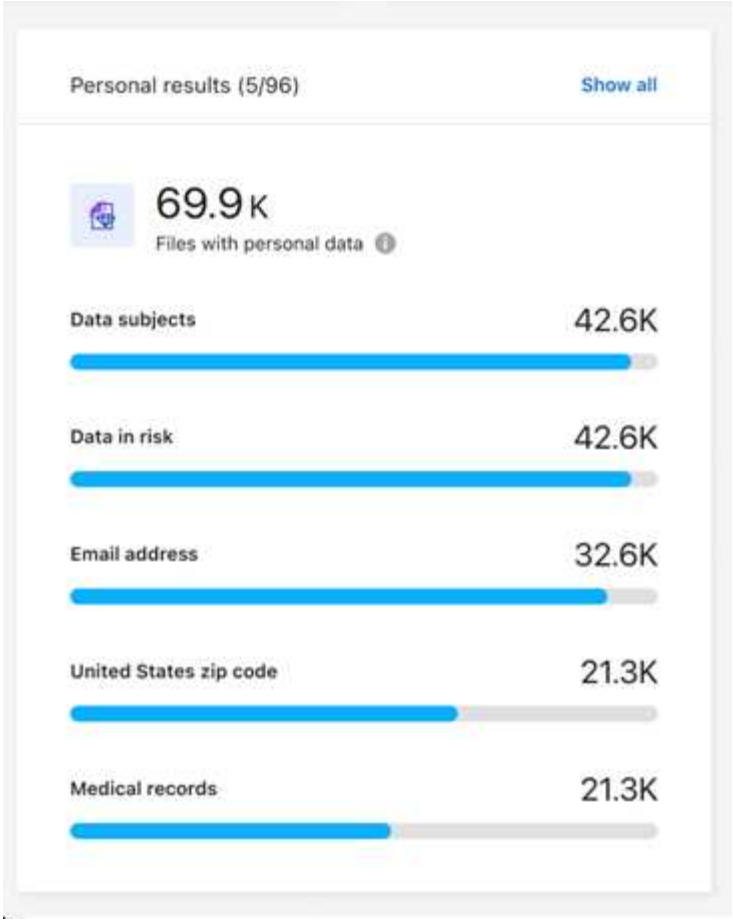
Para alguns tipos de dados pessoais, a Classificação de Dados usa *validação de proximidade* para validar suas descobertas. A validação ocorre pela busca de uma ou mais palavras-chave predefinidas próximas aos dados pessoais encontrados. Por exemplo, a Classificação de Dados identifica um número de previdência 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.

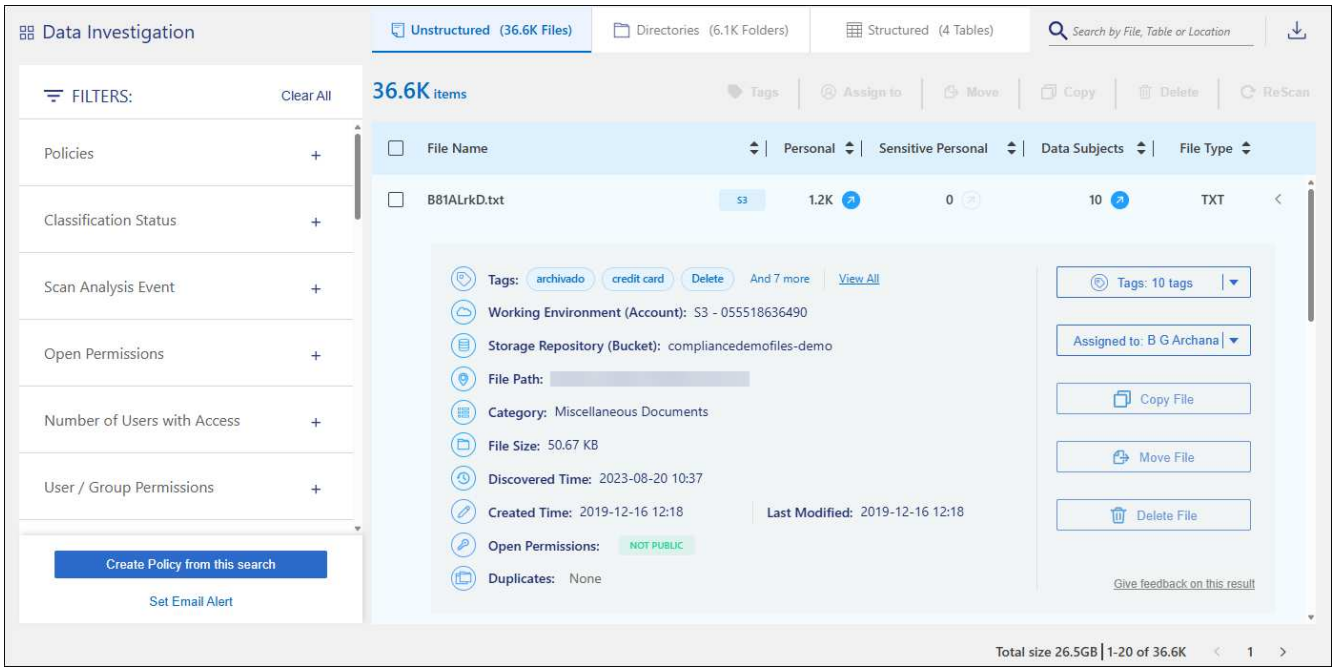


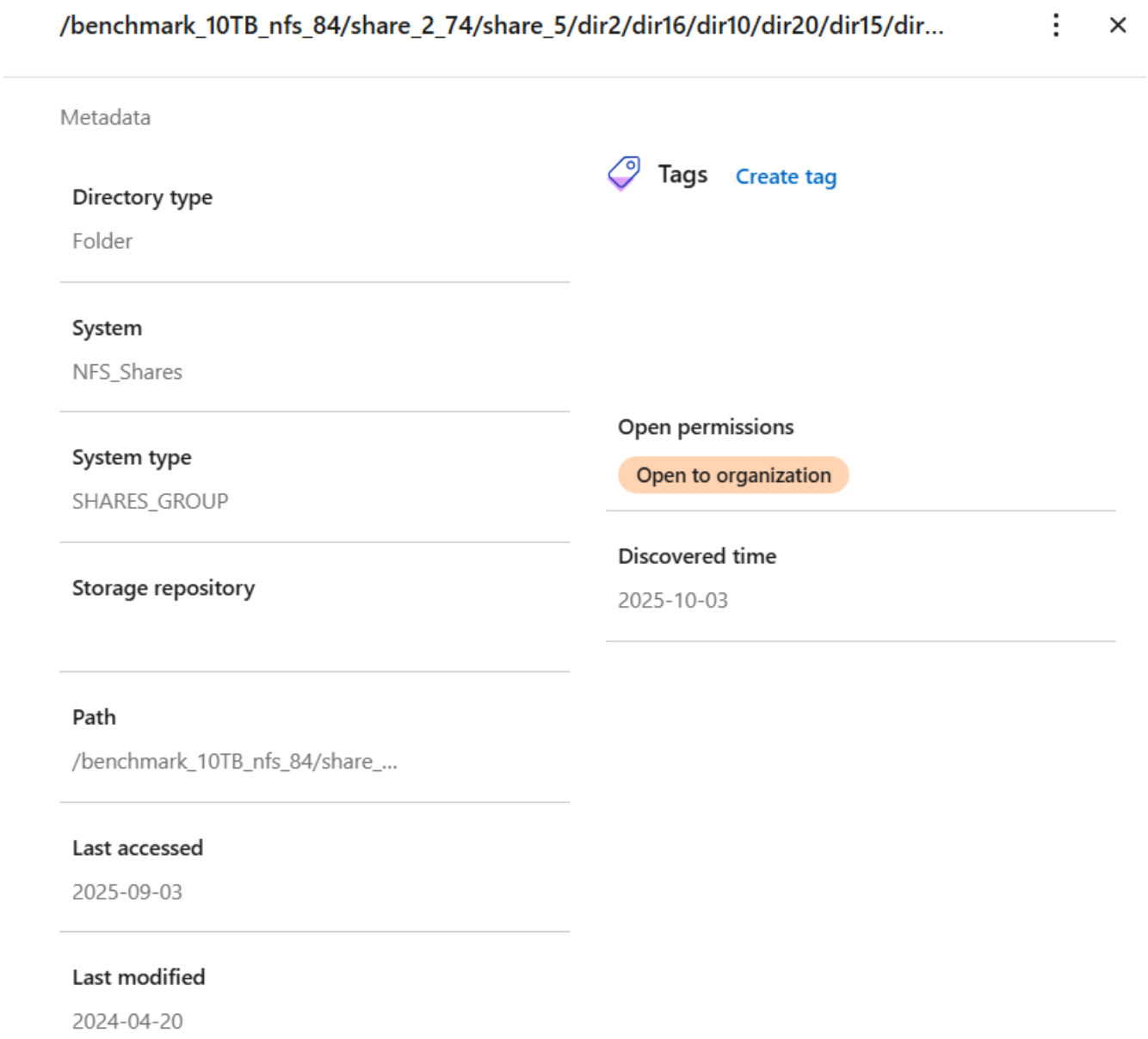
3. Para investigar os detalhes de um tipo específico de dados pessoais, selecione **Exibir tudo** e, em seguida, selecione o ícone de seta **Investigar resultados** para um tipo específico de dados pessoais, por exemplo, endereços de e-mail.



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.

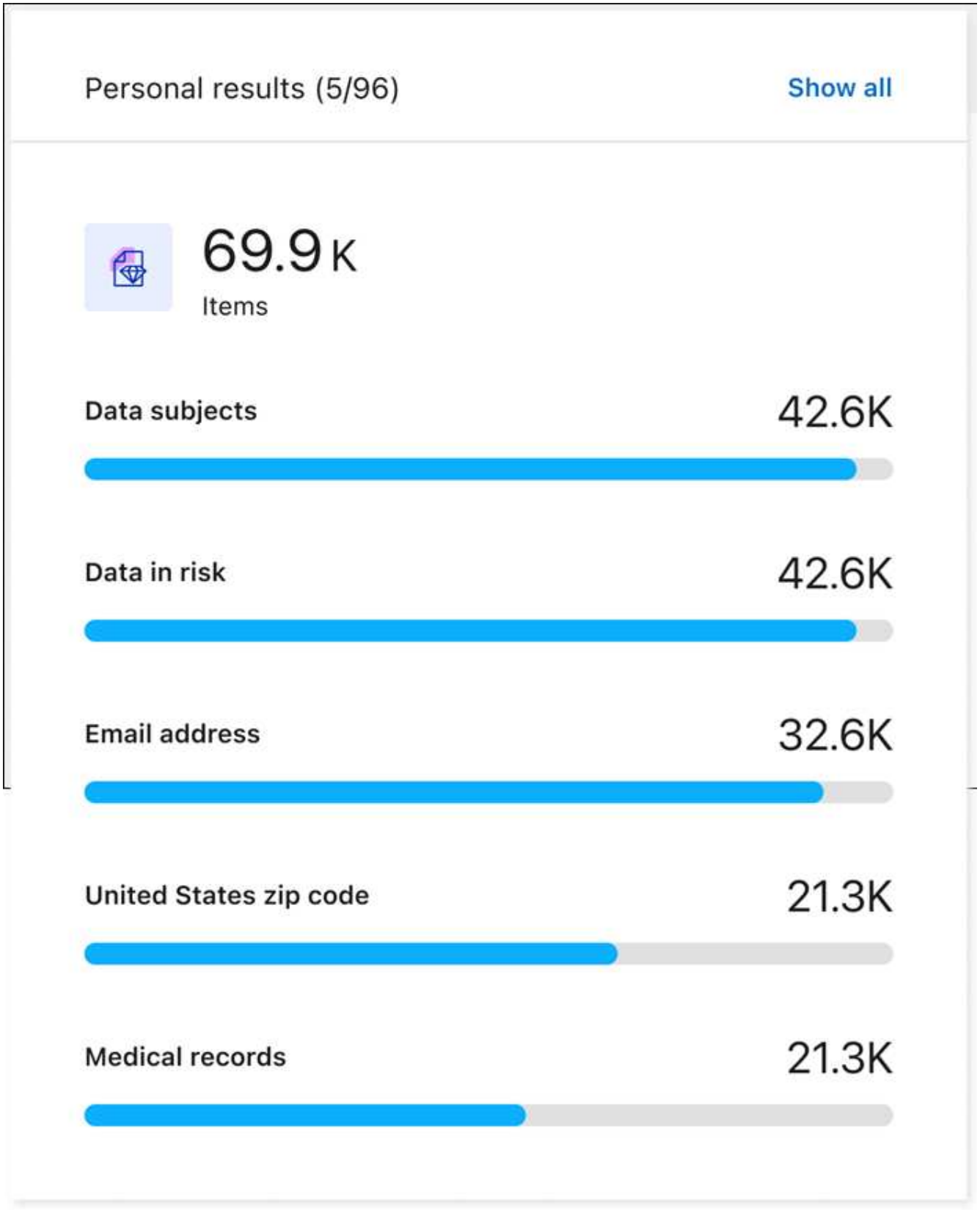
A classificação de dados usa IA, processamento de linguagem natural (PLN), aprendizado de máquina (ML) e computação cognitiva (CC) para entender o significado do conteúdo que ela examina, a fim de extrair entidades e categorizá-lo adequadamente.

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.

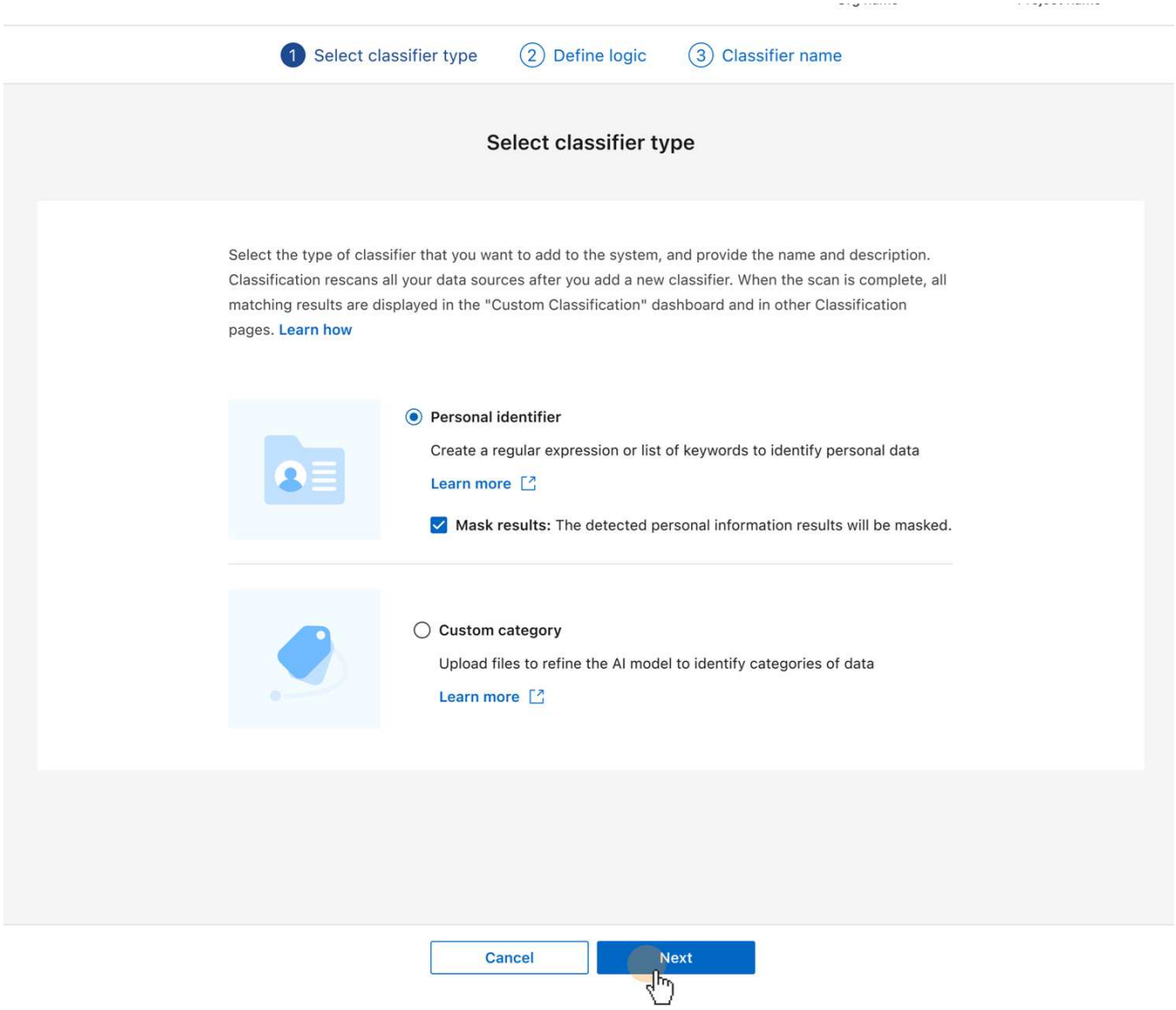
Requisitos para palavras-chave

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

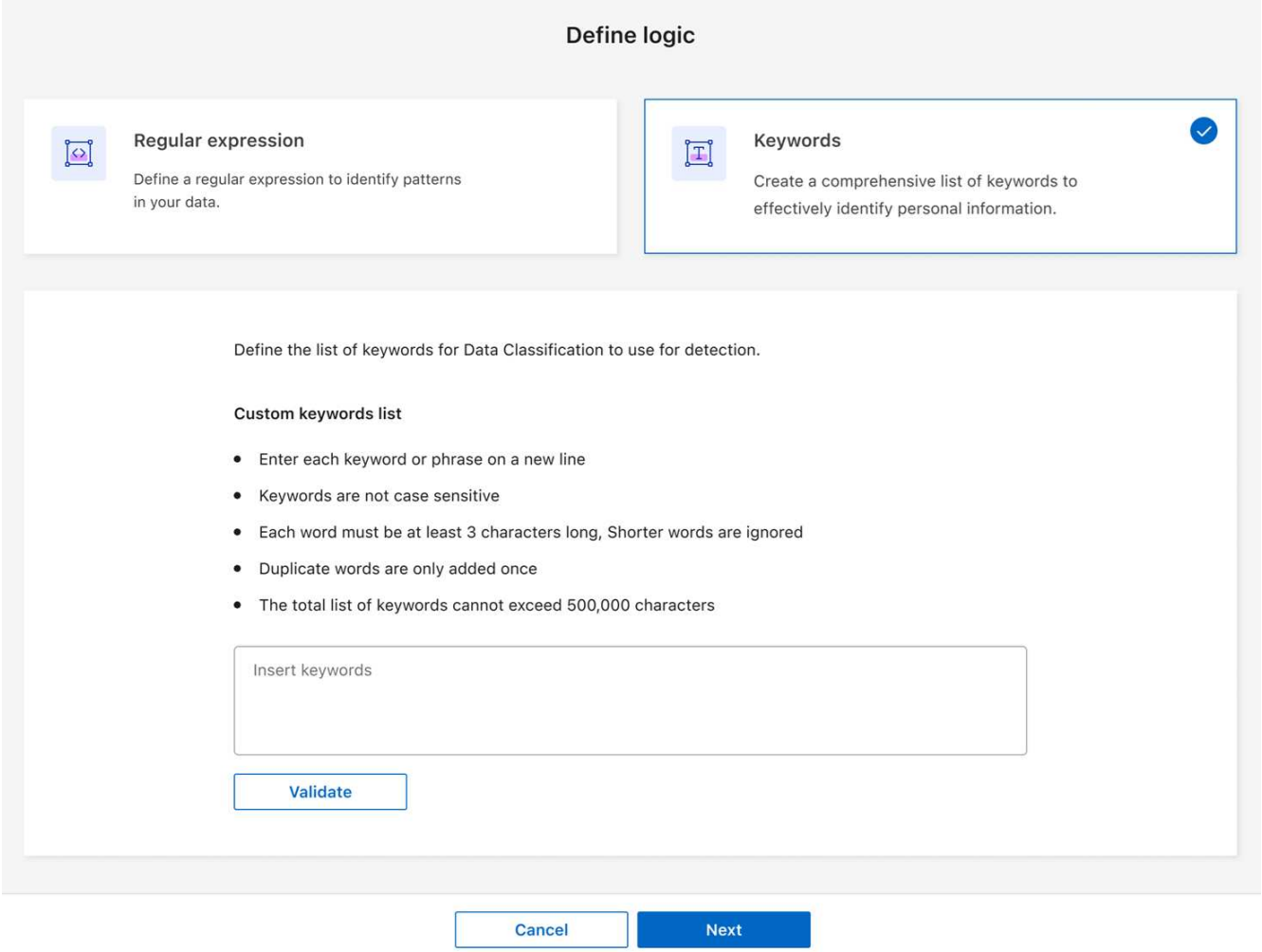
- As entradas de palavras-chave não diferenciam maiúsculas de minúsculas.
- As palavras-chave devem ter pelo menos três caracteres. Palavras com menos de três caracteres serão ignoradas.
- Palavras duplicadas são adicionadas apenas uma vez.
- A lista total de palavras-chave não pode exceder 500.000 caracteres.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

Passos

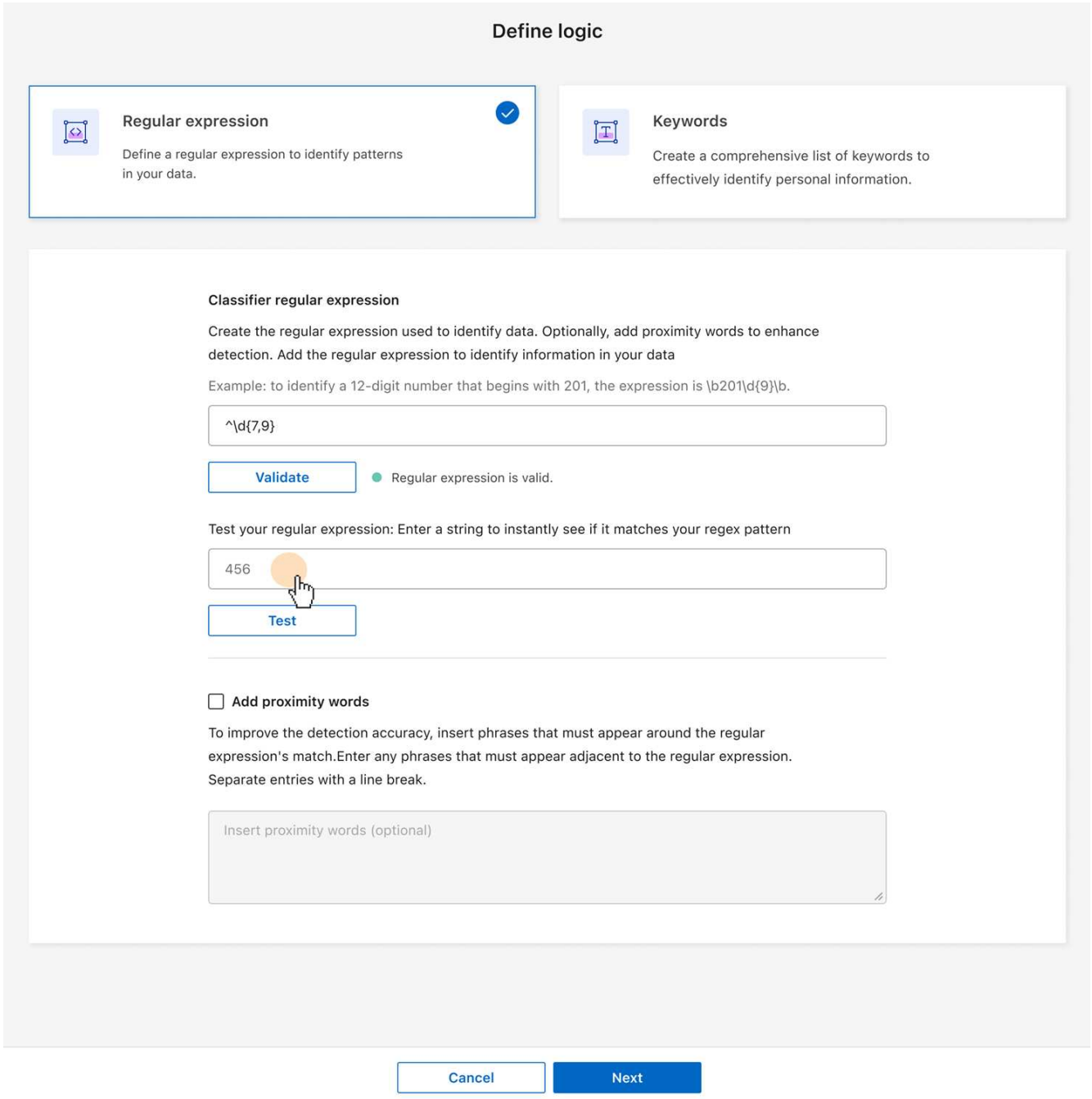
1. Selecione a aba **Classificação personalizada**.
2. Selecione **+ Novo Classificador** para criar o classificador personalizado.
3. Selecione **Identificador pessoal**. Opcionalmente, selecione **Ocultar resultados** para ocultar os dados pessoais detectados.
4. Selecione **Próximo**.



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

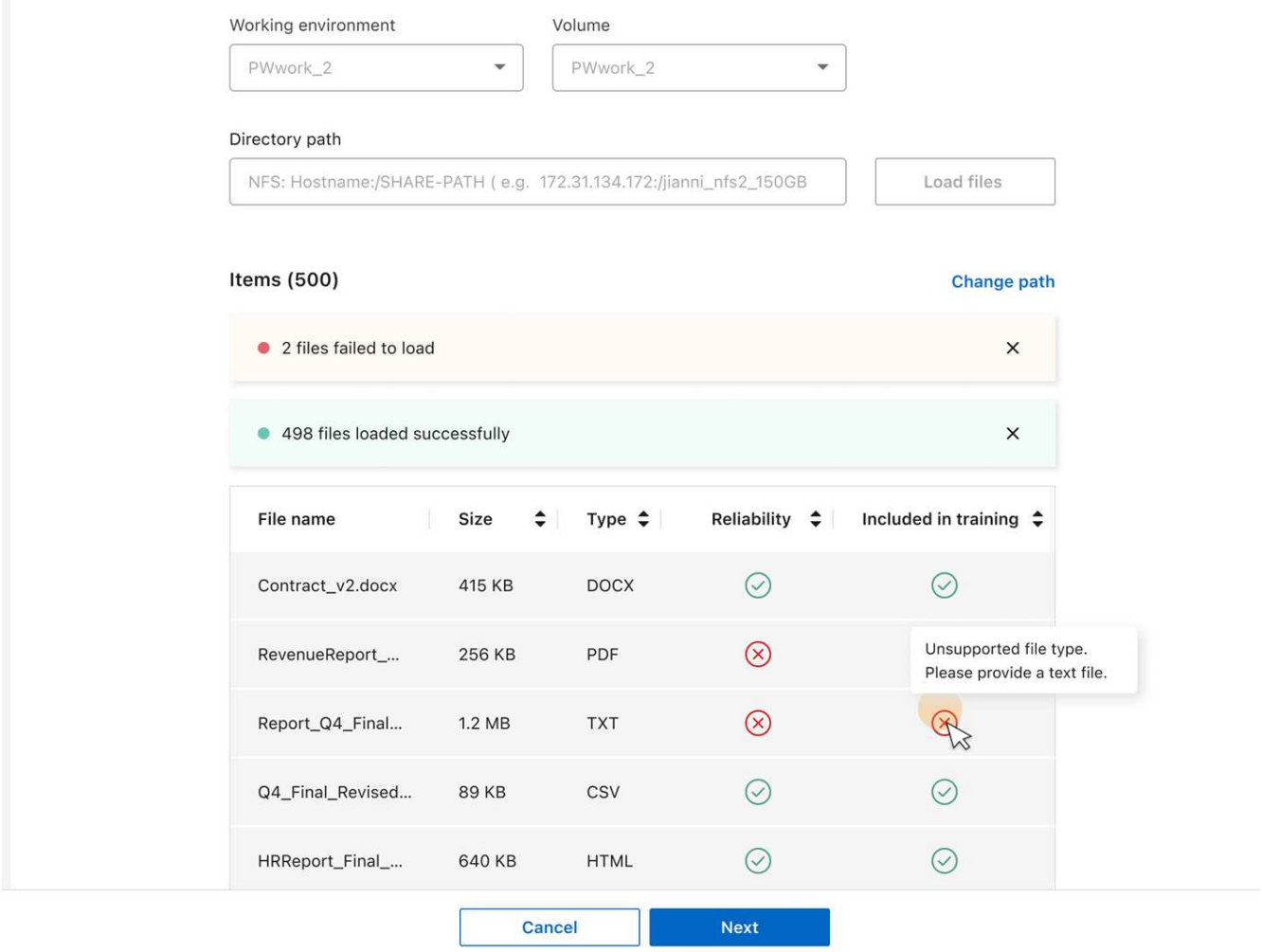
- O conjunto de dados de treinamento deve conter no mínimo 25 arquivos. O número máximo de arquivos é 1.000.
- Todos os arquivos devem estar localizados exatamente no caminho de arquivo que você fornecer.
- Todos os arquivos devem ter mais de 100 bytes.
- Os dados de treinamento para classificação de 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 Classificação de Dados exibe o tempo estimado de conclusão para o treinamento dos dados. .. Para alterar o caminho do arquivo ou reenviar os arquivos, selecione **Alterar caminho** e 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

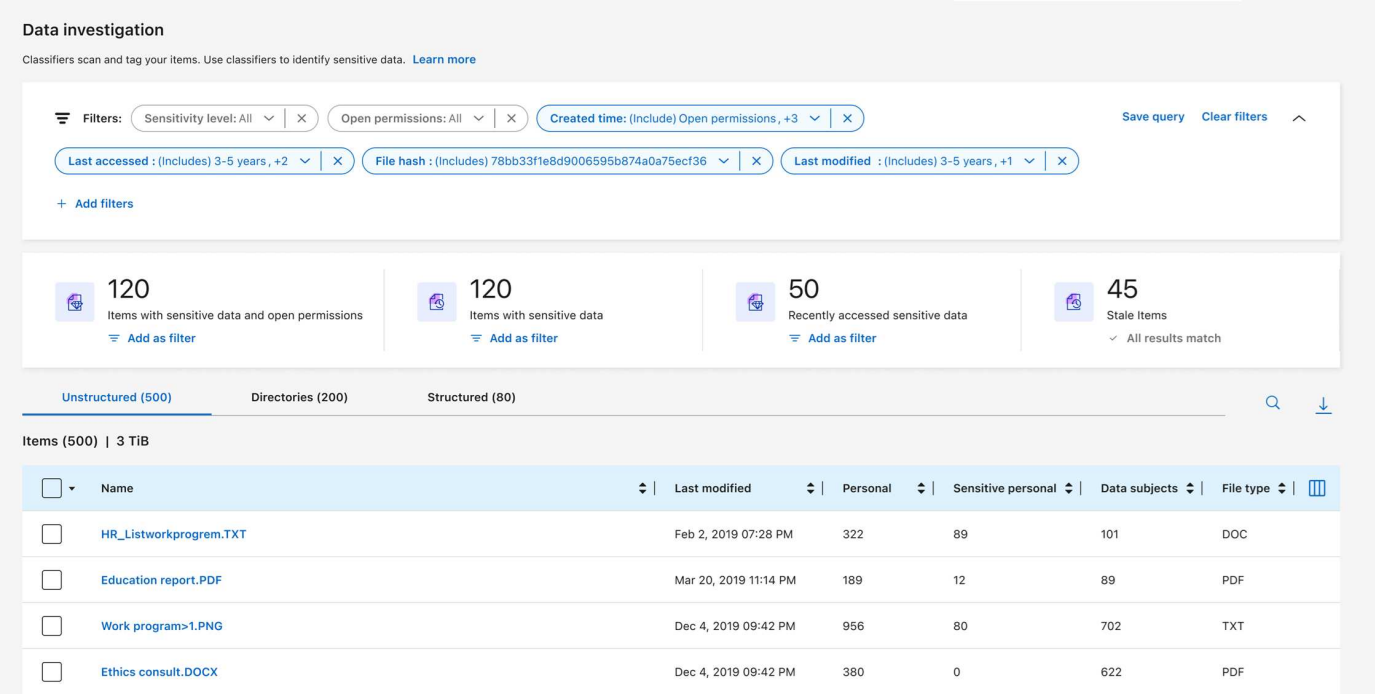
A página Investigação de Dados classifica os dados em três guias:

- **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.

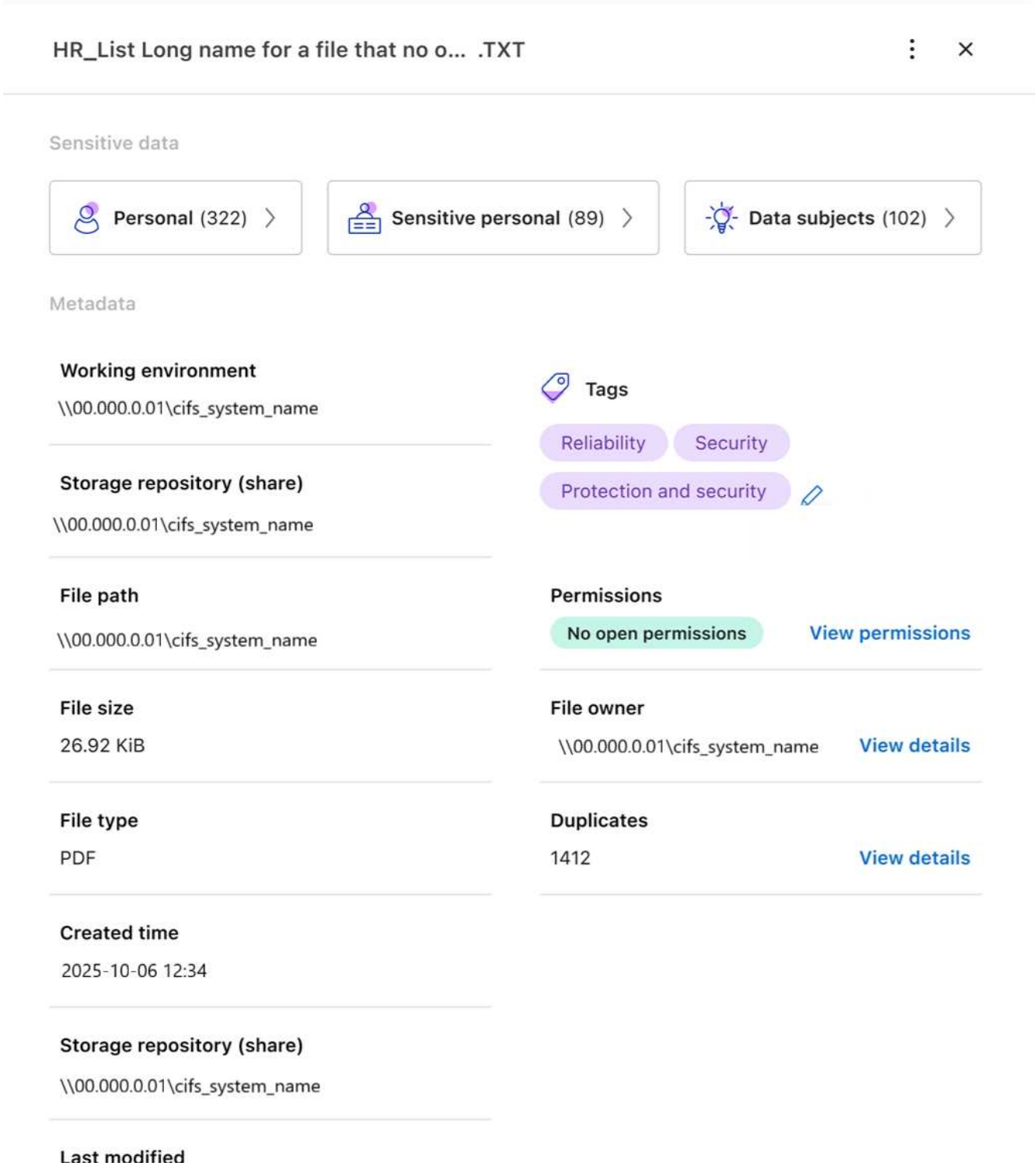
Exibir metadados do arquivo

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:

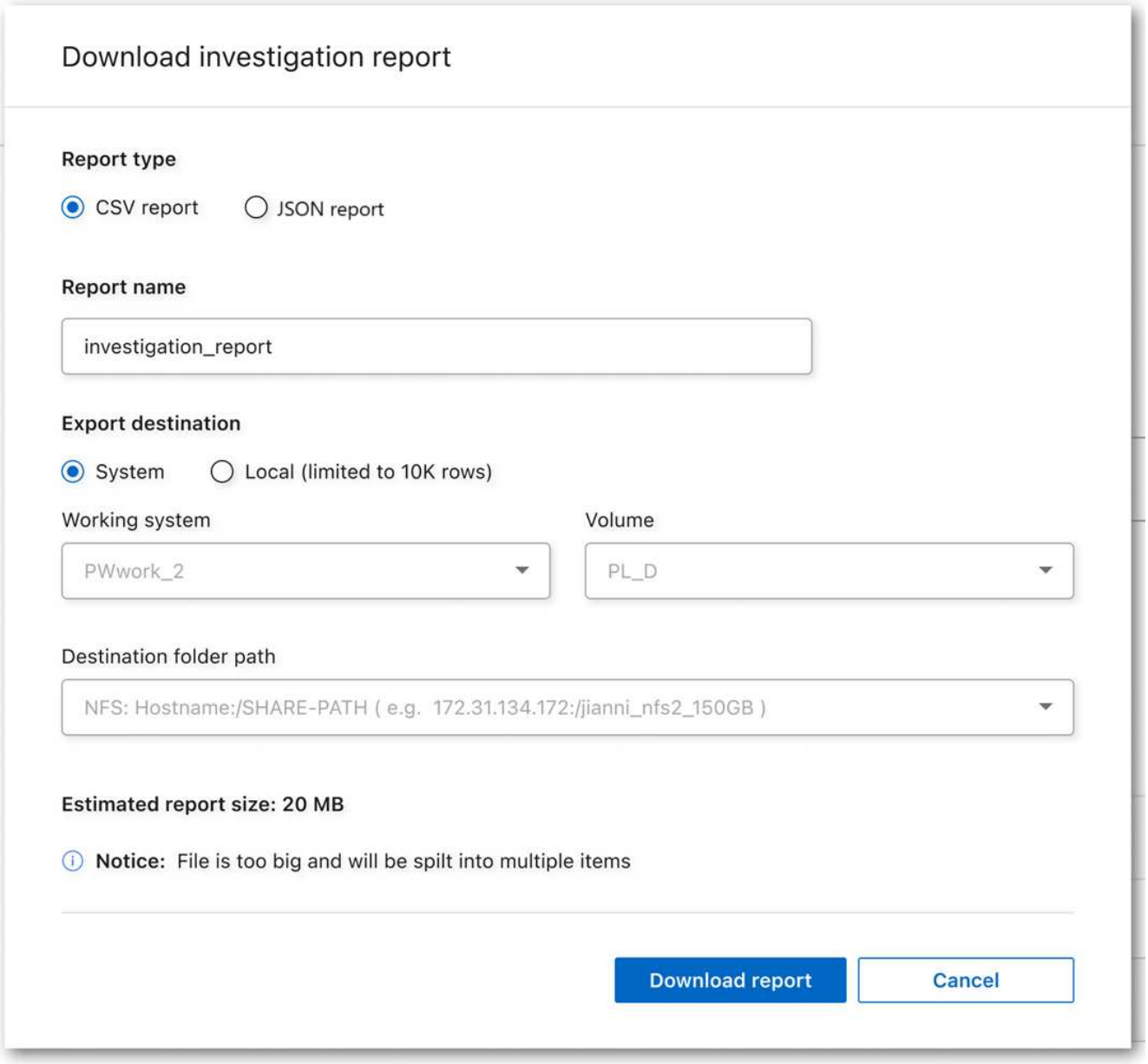
- Nome da tabela do BD
- Tipo de localização
- Nome do sistema
- Repositório de armazenamento (por exemplo, um esquema)
- Contagem de colunas
- Contagem de linhas
- Informações pessoais
- Informações pessoais sensíveis

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**.



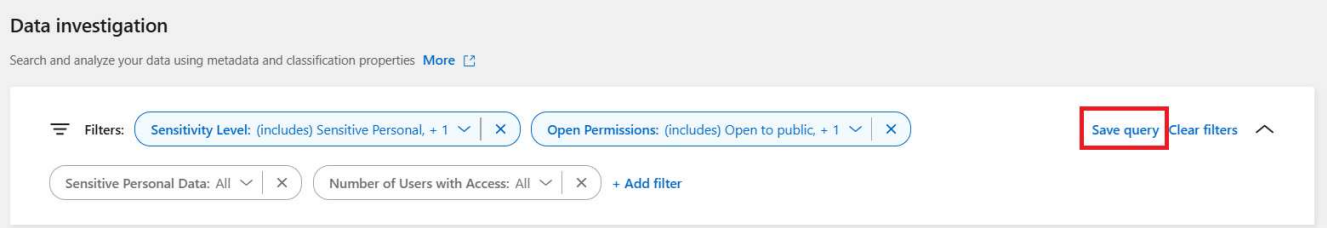
Resultado

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

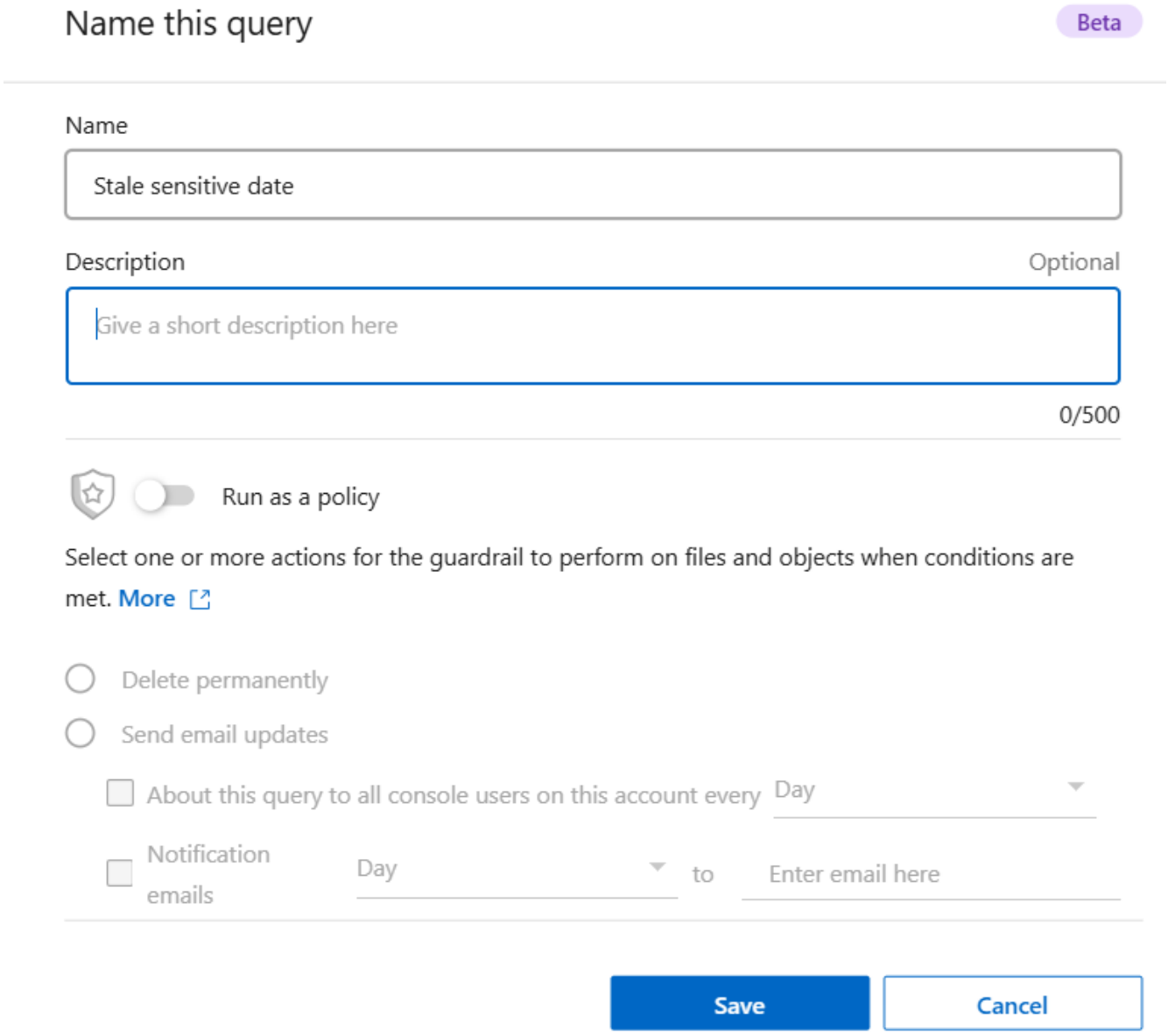
Crie uma consulta salva com base nos filtros selecionados

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

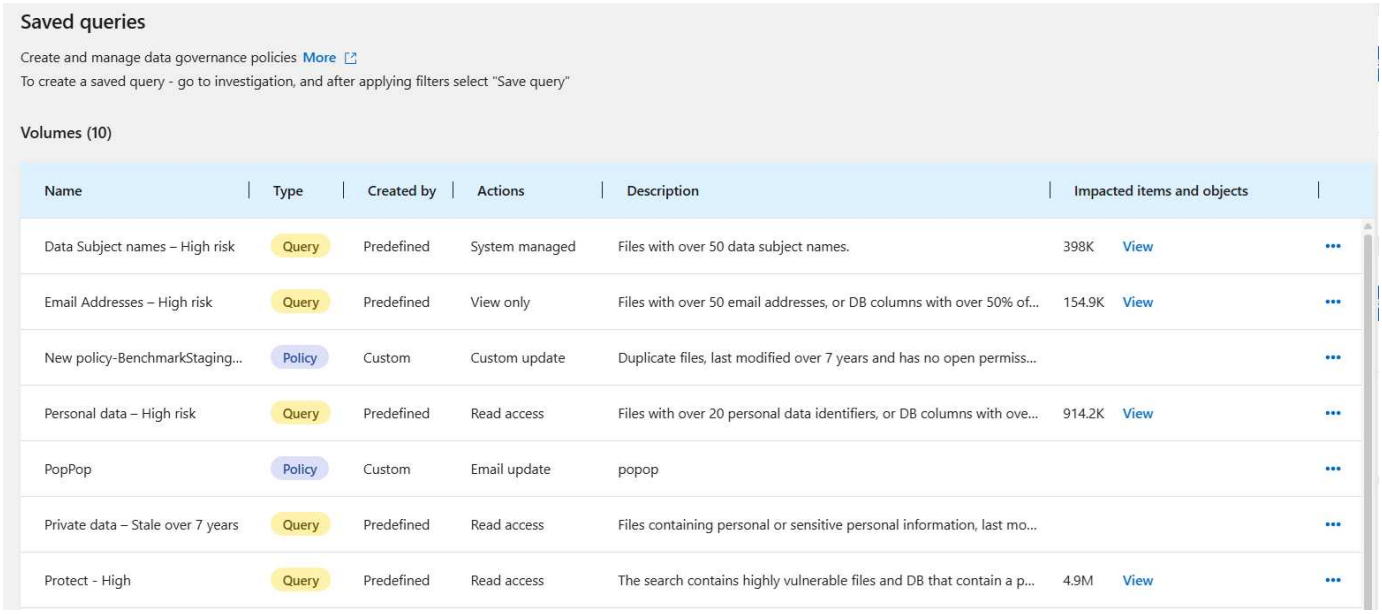
A classificação de dados do NetaApp permite salvar suas consultas de pesquisa. Com uma consulta salva, você pode criar filtros personalizados para classificar consultas frequentes da sua página de investigação de dados. A Classificação de Dados também inclui consultas salvas predefinidas com base em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

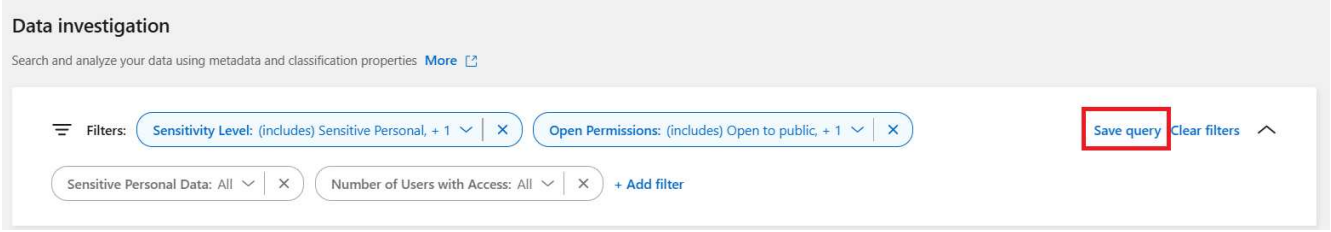
Para exibir os resultados de uma consulta salva na página Investigação, selecione botão para uma pesquisa específica e selecione **Investigar resultados**.

Crie consultas e políticas salvas

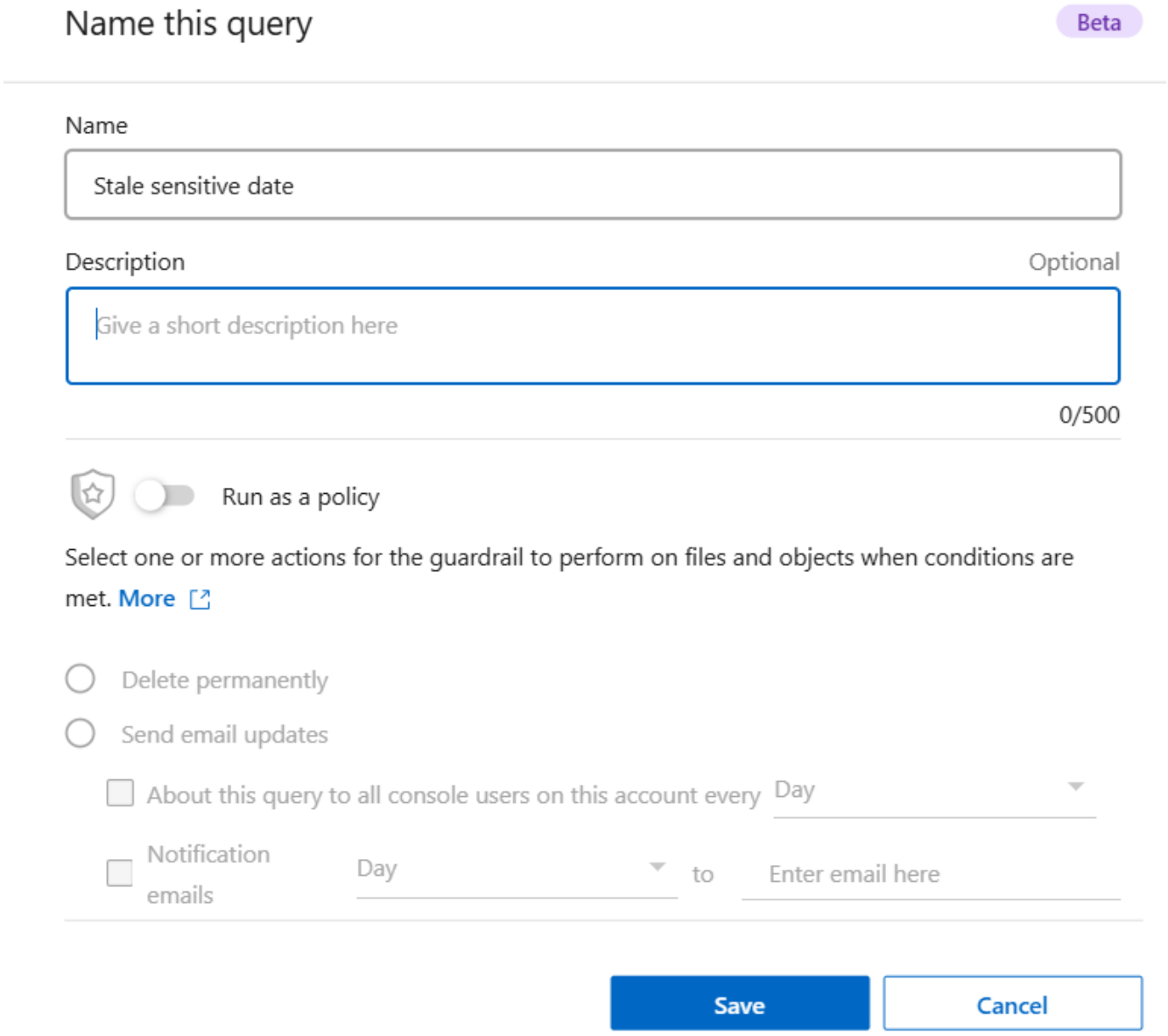
Você pode criar suas próprias consultas salvas personalizadas que fornecem resultados para consultas específicas da sua organização. Os resultados são retornados para todos os arquivos e diretórios (compartilhamentos e pastas) que correspondem aos critérios de pesquisa.

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:

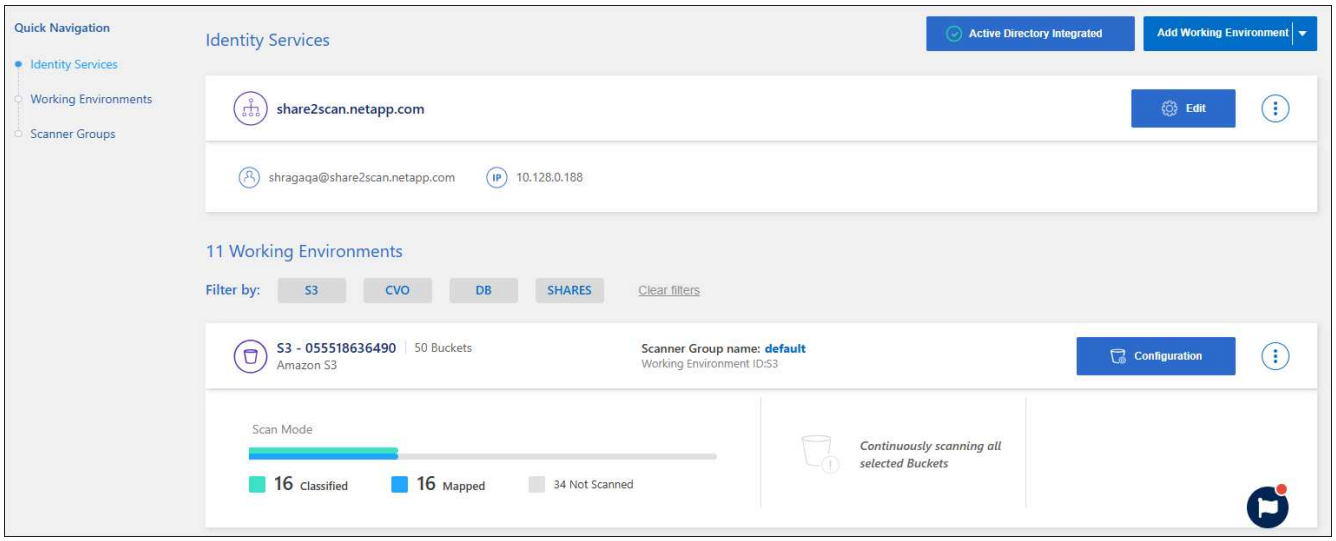
- **Inicializando** (ponto azul claro): A configuração do mapa ou classificação está ativada. Isso aparece brevemente antes de passar para o status de "fila pendente".
- **Fila pendente** (ponto laranja): A tarefa de verificação está aguardando para ser listada na fila de verificação.
- **Na fila** (ponto 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.

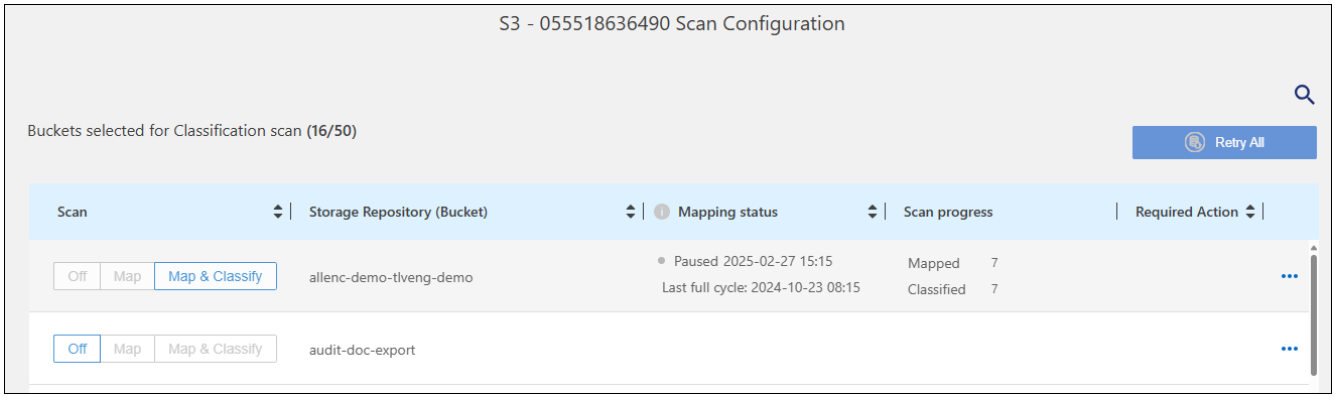
- **Não escaneando**: A configuração de volume "Desligado" foi selecionada e o sistema não está escaneando o volume.

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.

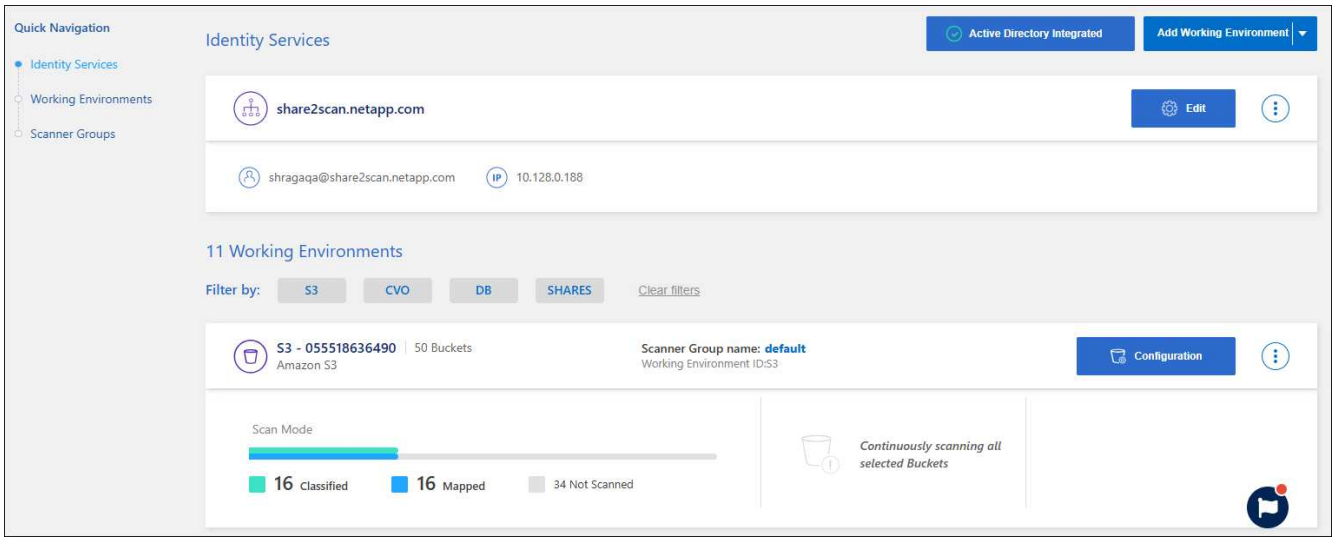
Alterar o tipo de digitalização de um repositório

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.

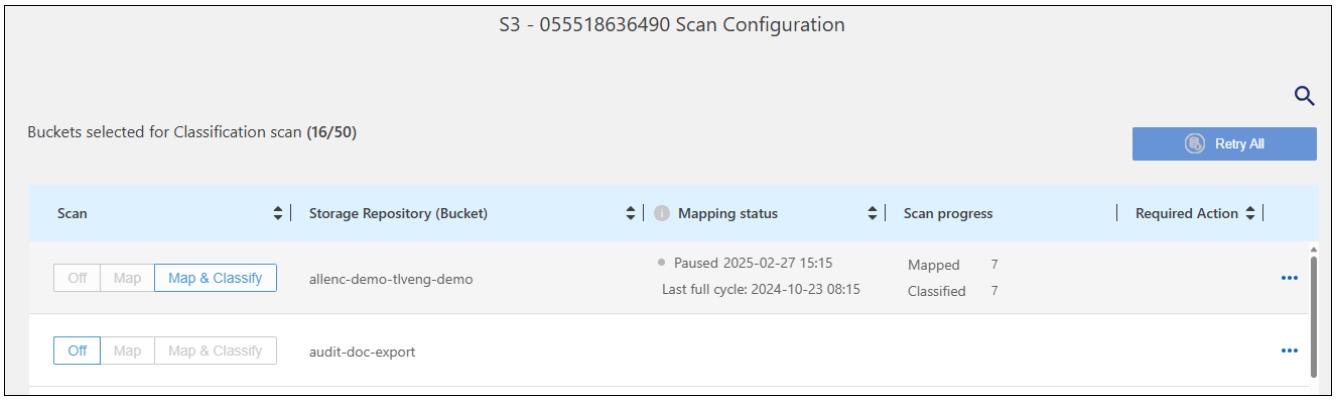
Os bancos de dados não podem ser configurados para varreduras somente de mapeamento. A varredura do banco de dados pode estar Desligada ou Ligada; onde Ligada é equivalente a Mapear e Classificar.

Passos

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

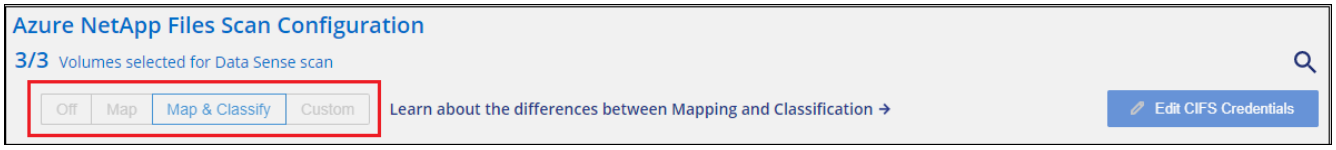


3. Na página Configuração de verificação, altere qualquer um dos repositórios (buckets neste exemplo) para executar verificações **Mapear** ou **Mapear e classificar**.



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

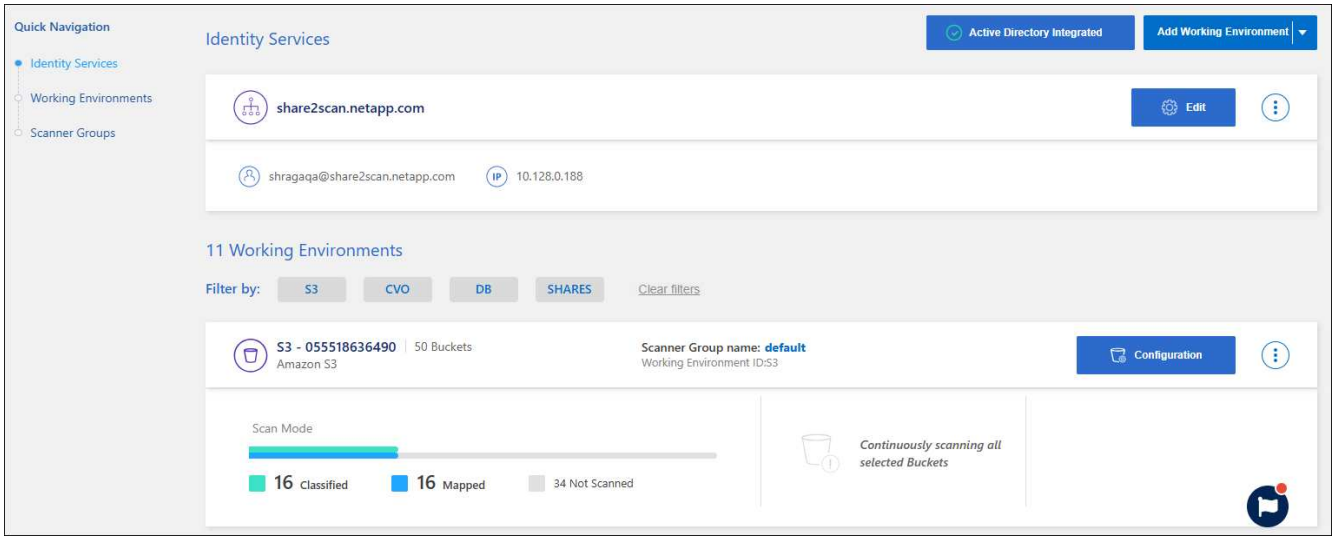
1. No menu Classificação de Dados, selecione **Configuração**.
2. Selecione os recursos que você deseja priorizar.
3. Das Ações … opção, selecione **Priorizar verificação**.

Parar de procurar um repositório

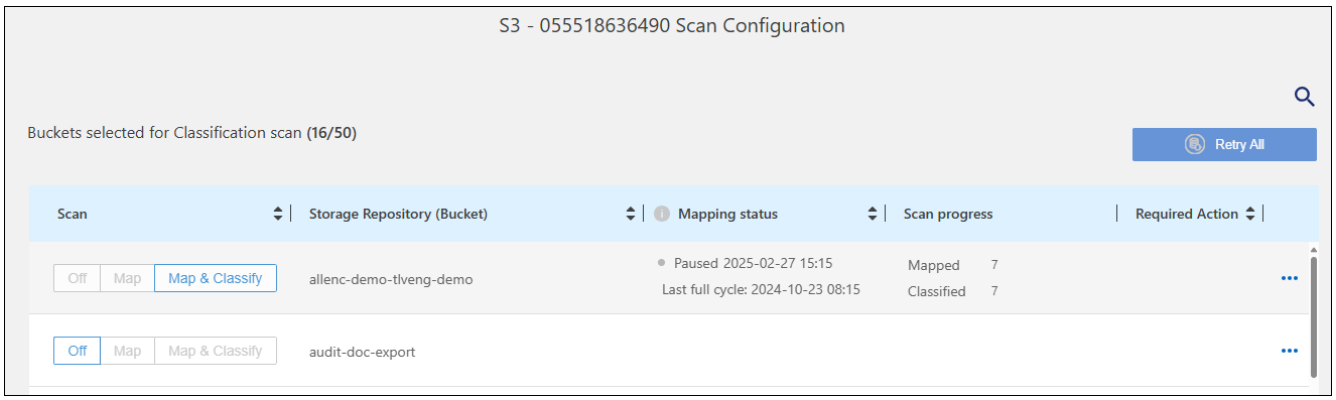
Você pode parar de escanear um repositório (por exemplo, um volume) se não precisar mais monitorá-lo para verificar a conformidade. Você faz isso desligando a digitalização. Quando a digitalização é desativada, toda a indexação e informações sobre esse volume são removidas do sistema, e a cobrança pela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

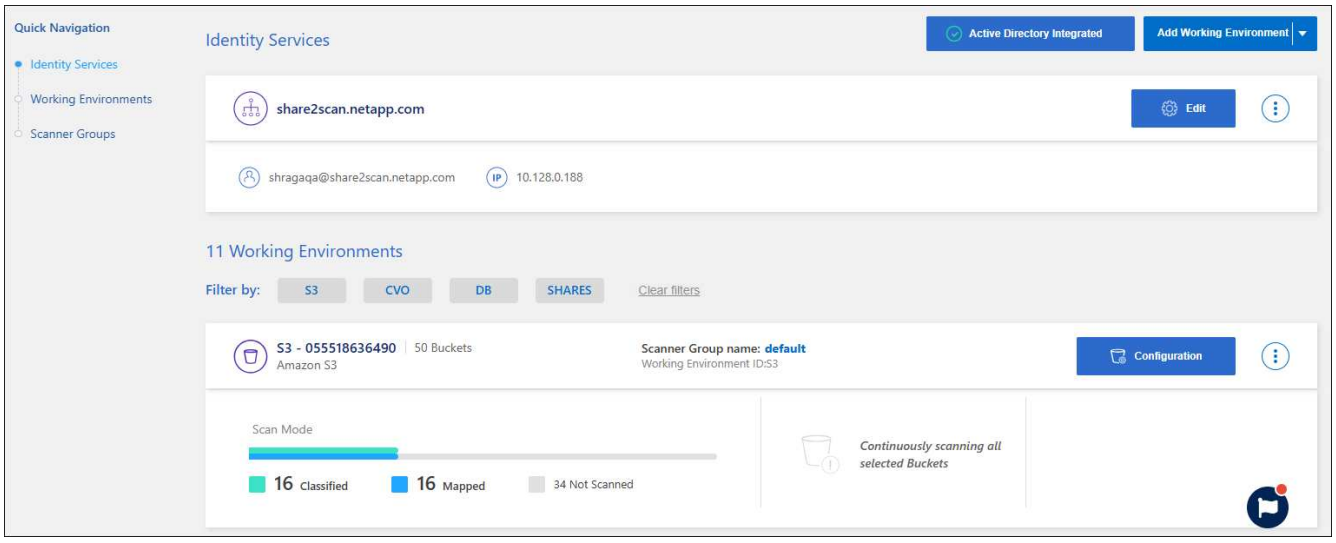
Você pode "pausar" a verificação em um repositório se quiser interromper temporariamente a verificação de determinado conteúdo. Pausar a verificação significa que a Classificação de Dados não realizará mais verificações em busca de alterações ou adições ao repositório. Todos os resultados de varredura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

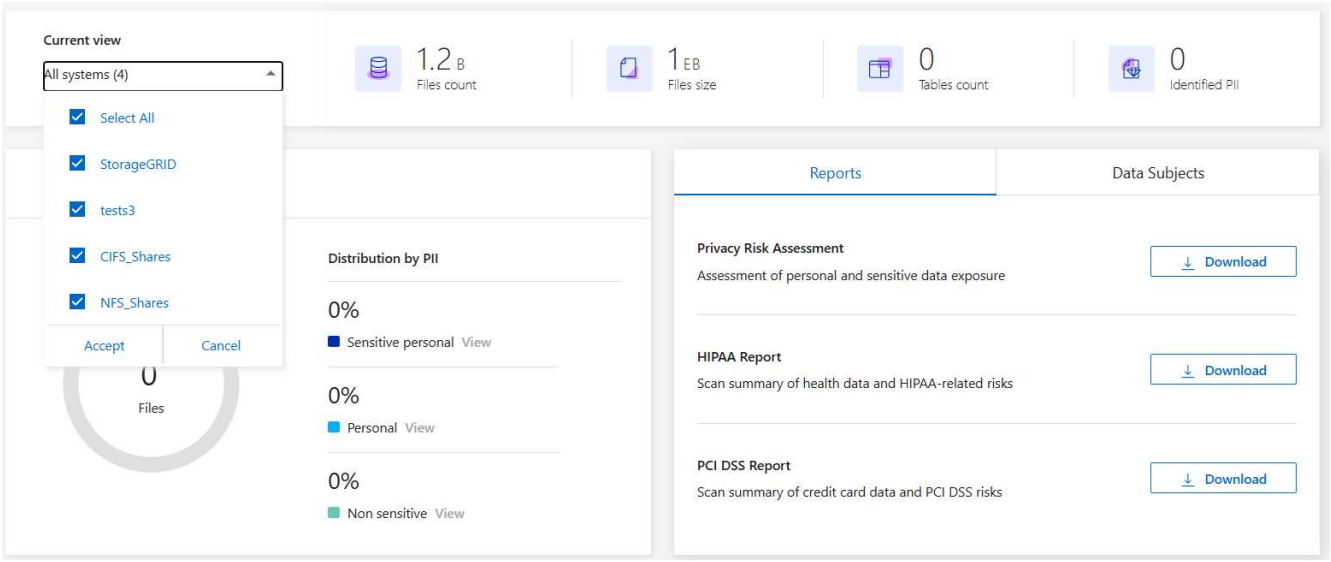
Você pode filtrar o conteúdo do painel Conformidade de Classificação de Dados para ver dados de conformidade de todos os sistemas e bancos de dados, ou apenas de sistemas específicos.

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.

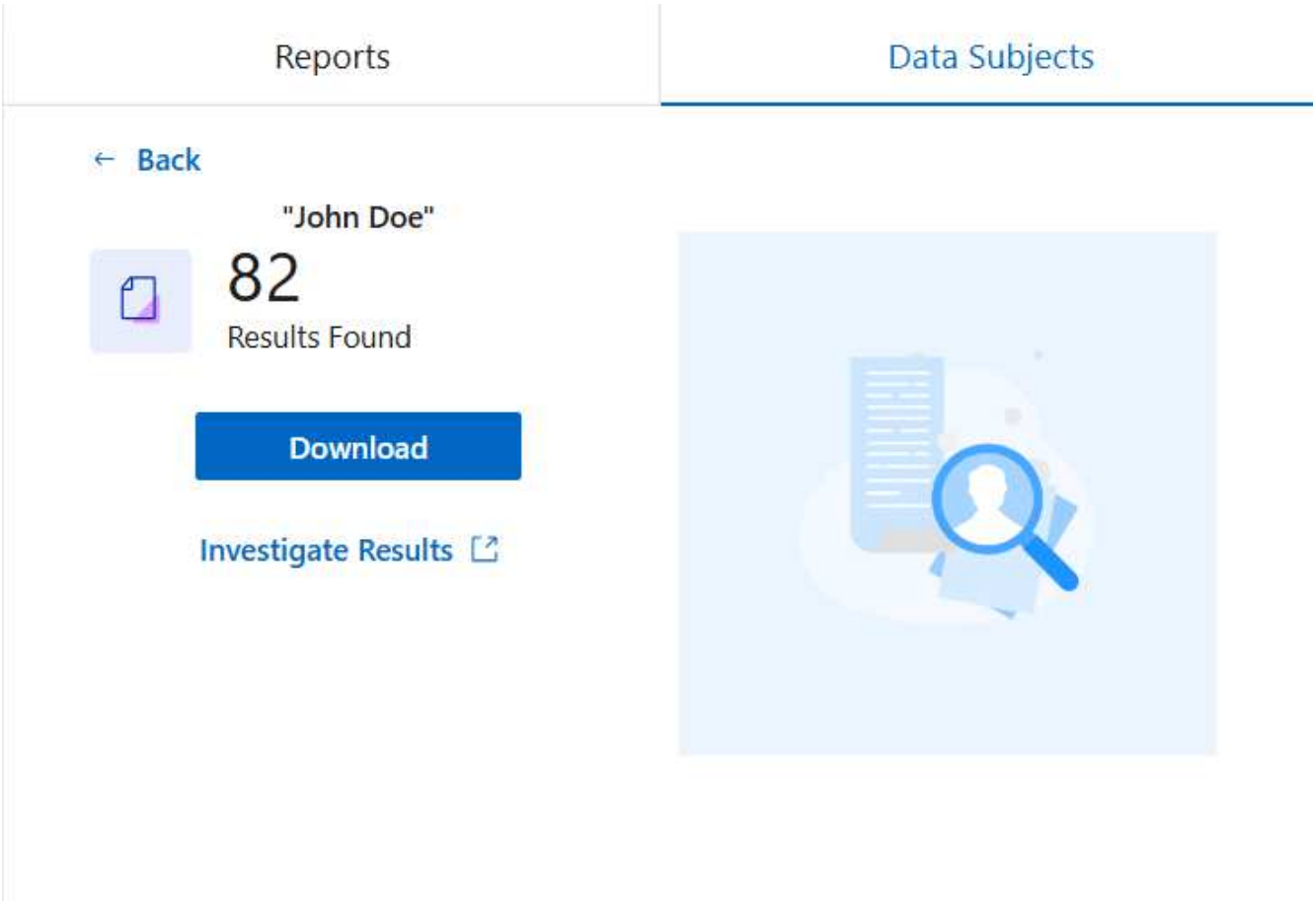
Pesquisar titulares de dados e baixar relatórios

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.



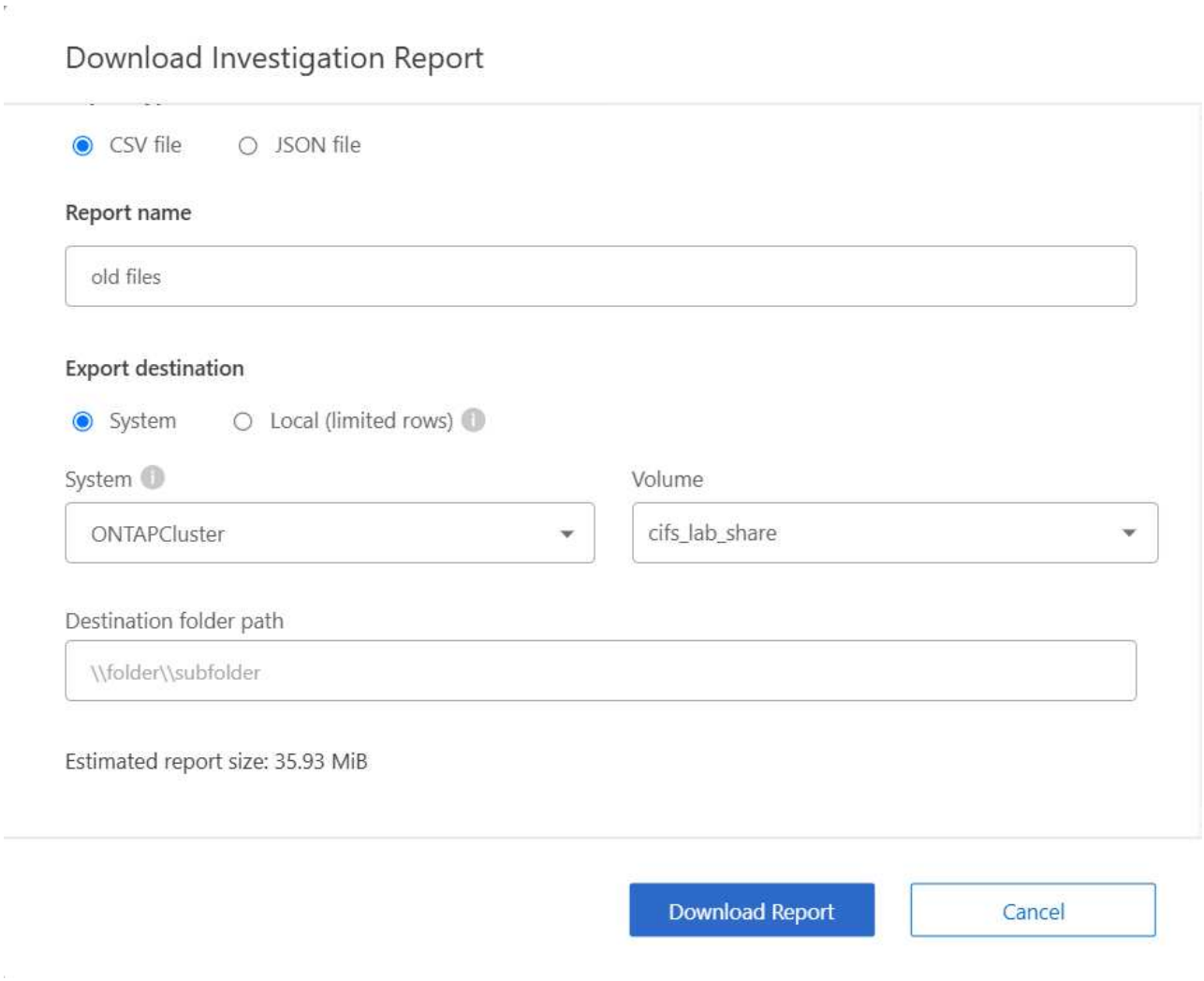
5. Revise os resultados na Classificação de Dados ou baixe-os como um relatório selecionando o ícone de download.

   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.

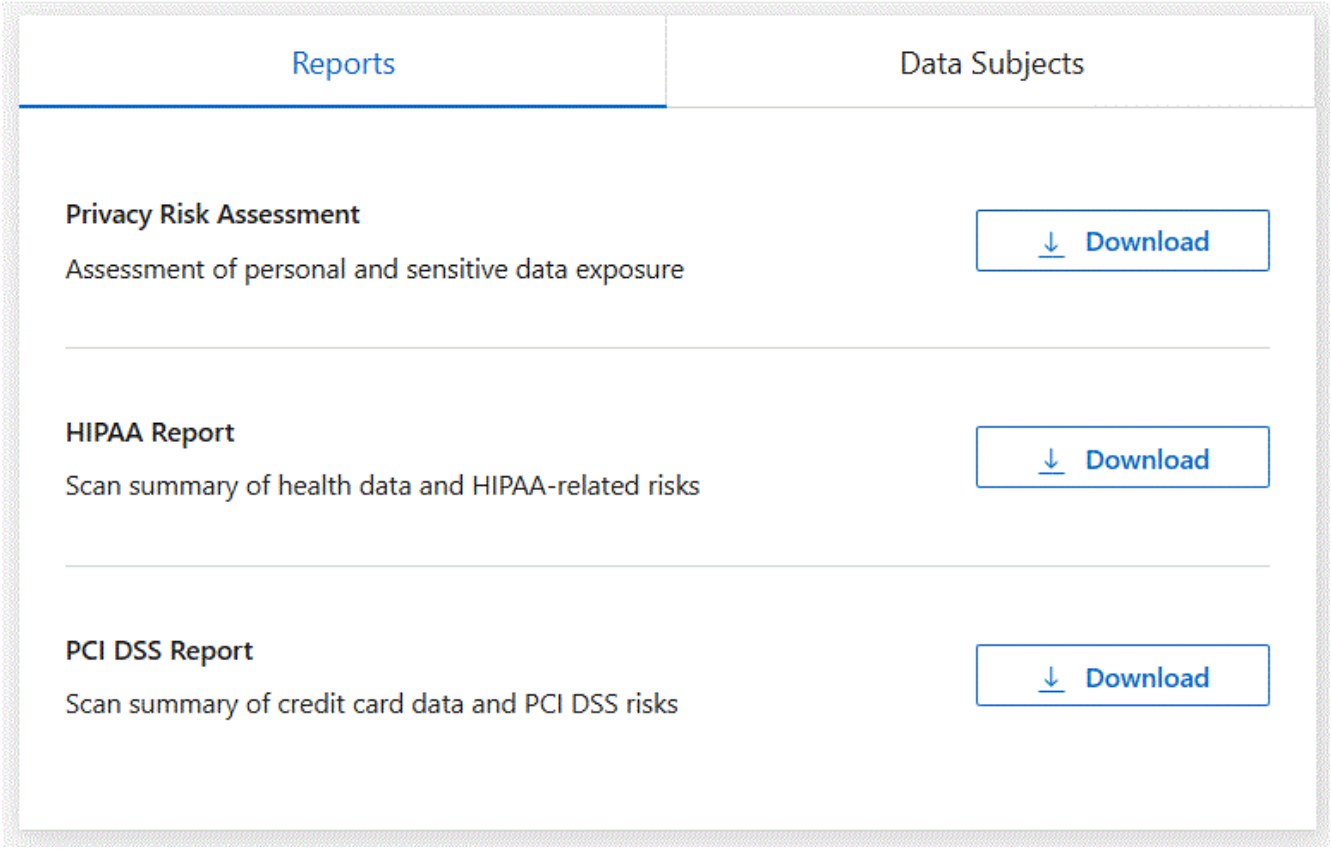
- Retenção: O período em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter informações de saúde por mais tempo do que o necessário para processá-las.
- Distribuição de informações de saúde: os sistemas onde as informações de saúde foram encontradas e se a criptografia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

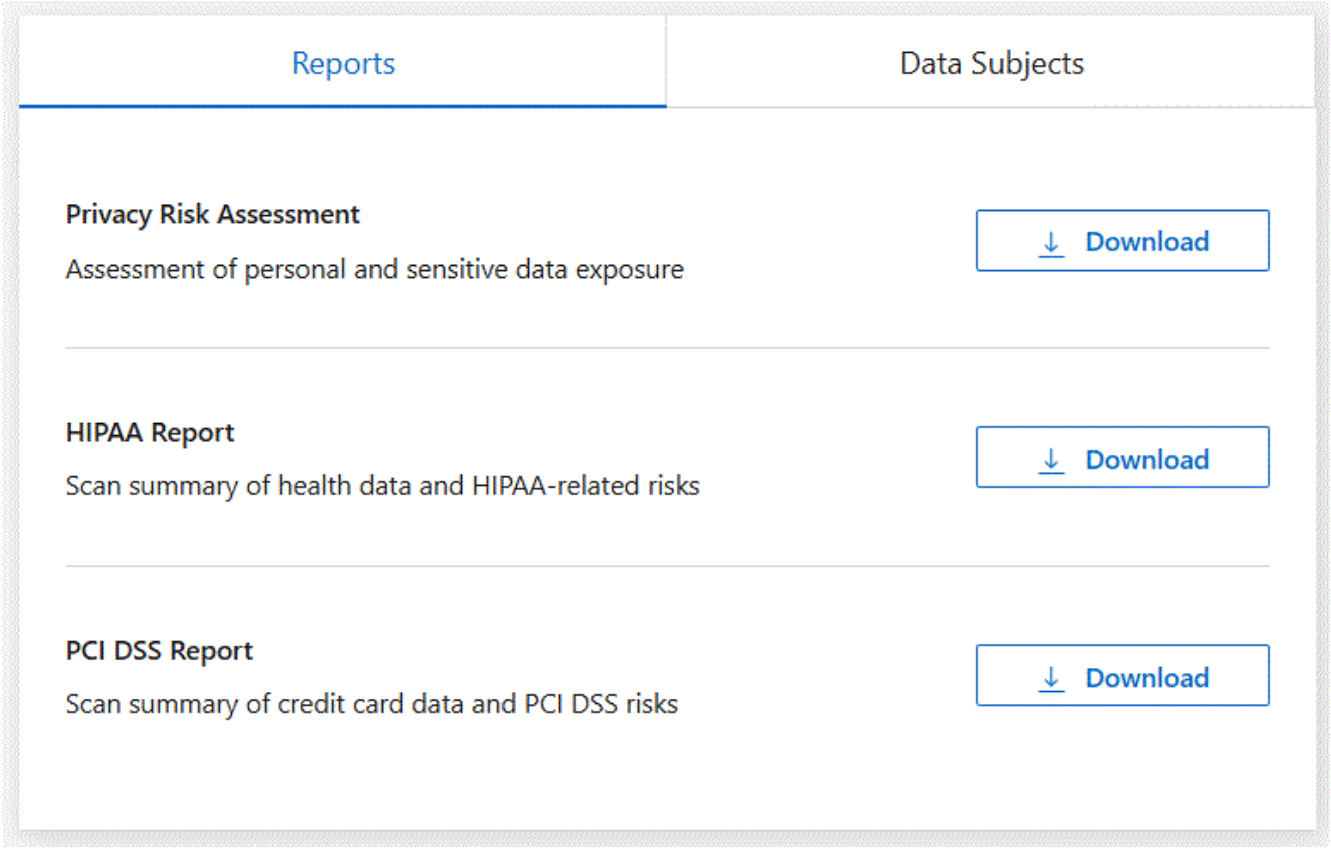
- Criptografia: A porcentagem de arquivos contendo informações de cartão de crédito que estão em sistemas criptografados ou não criptografados. Estas informações são específicas do Cloud Volumes ONTAP.
- Proteção contra ransomware: a porcentagem de arquivos contendo informações de cartão de crédito que 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:

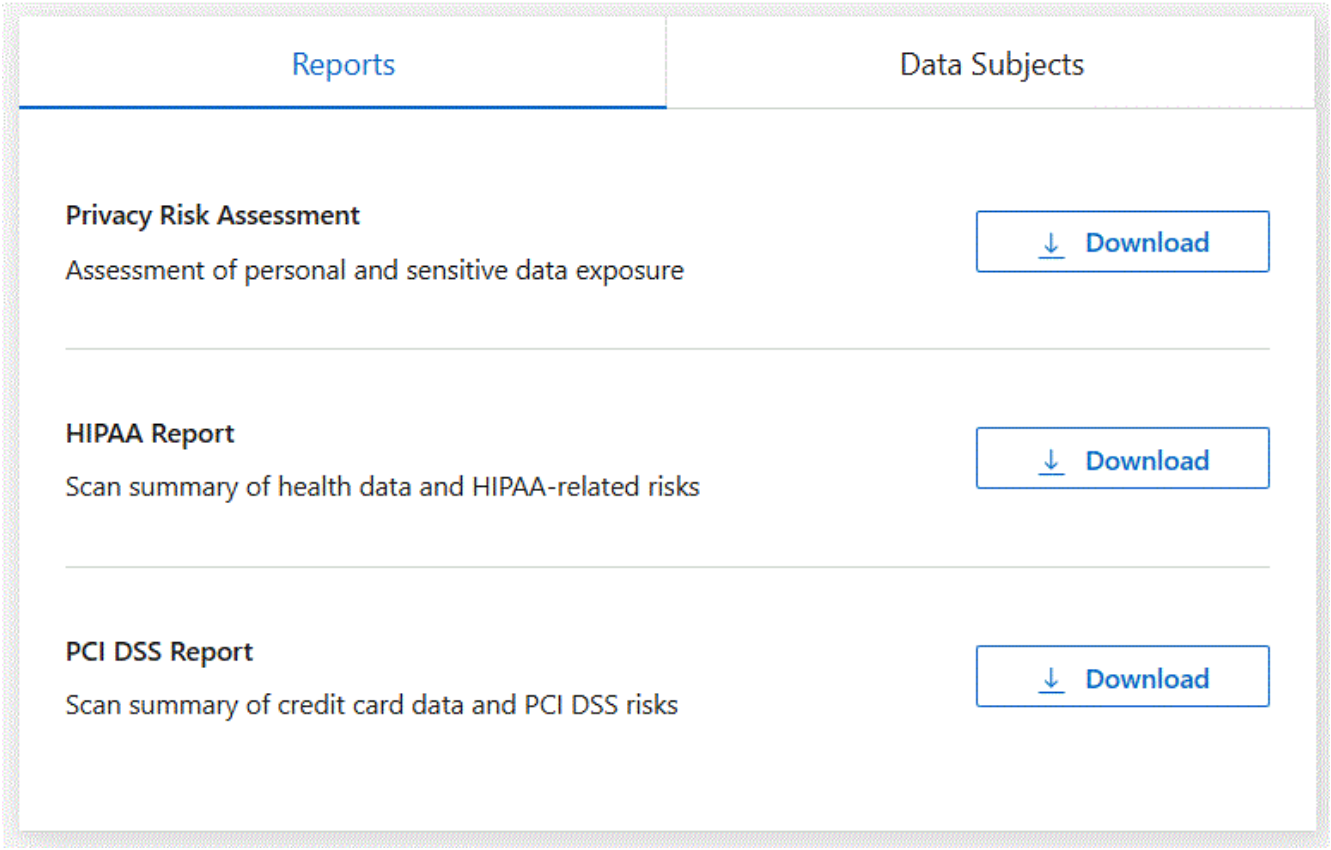
- Status de conformidade: uma pontuação de gravidade e a distribuição de dados, sejam eles não confidenciais, pessoais ou pessoais confidenciais.
- Visão geral da avaliação: Uma análise dos tipos de dados pessoais encontrados, bem como das categorias de dados.
- Assuntos dos dados nesta avaliação: O 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**

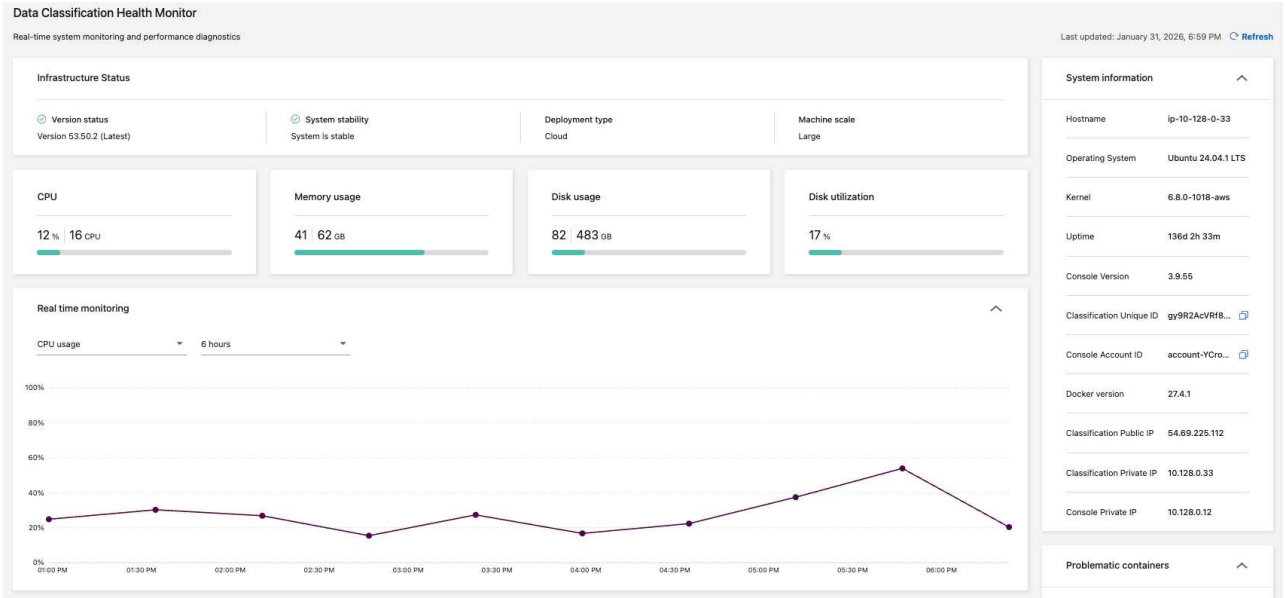
  O painel de informações do sistema captura informações críticas sobre o NetApp Console e a Classificação de Dados, como endereços IP públicos e privados, nome do host, sistema operacional, versão do Console e ID do Console.

- **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.



Informações sobre direitos autorais

Informações sobre marcas comerciais