Documentação de classificação BlueXP

BlueXP classification

NetApp
December 18, 2024

This PDF was generated from https://docs.netapp.com/pt-br/bluexp-classification/index.html on December 18, 2024. Always check docs.netapp.com for the latest.

Índice

Documentação de classificação BlueXP

Notas de lançamento

O que há de novo na classificação BlueXP

Saiba o que há de novo na classificação BlueXP .

16 de dezembro de 2024

Versão 1,38

Esta versão de classificação do BlueXP inclui melhorias gerais e correções de bugs.

4 de novembro de 2024

Versão 1,37

Esta versão de classificação do BlueXP inclui as seguintes atualizações.

Suporte para RHEL 8,10

Esta versão fornece suporte para Red Hat Enterprise Linux v8,10, além de versões anteriormente suportadas. Isso é aplicável a qualquer instalação manual no local da classificação do BlueXP , incluindo implantações em locais escuros.

Os seguintes sistemas operacionais requerem o uso do motor de contentor Podman, e eles exigem a classificação BlueXP versão 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 "Classificação BlueXP" sobre o .

Suporte para NFS v4,1

Esta versão fornece suporte para NFS v4,1, além de versões com suporte anterior.

Saiba mais "Classificação BlueXP" sobre o .

10 de outubro de 2024

Versão 1,36

Suporte para RHEL 9,4

Esta versão fornece suporte para Red Hat Enterprise Linux v9,4, além de versões anteriormente suportadas. Isso é aplicável a qualquer instalação manual no local da classificação do BlueXP , incluindo implantações em locais escuros.

Os seguintes sistemas operacionais requerem o uso do motor de contentor Podman, e eles exigem a classificação BlueXP versão 1,30 ou superior: Red Hat Enterprise Linux versão 8,8, 9,0, 9,1, 9,2, 9,3 e 9,4.

Saiba mais "Visão geral das implantações de classificação BlueXP " sobre o .

Desempenho de digitalização melhorado

Esta versão proporciona um melhor desempenho de digitalização.

2 de setembro de 2024

Versão 1,35

Digitalizar dados StorageGRID

A classificação BlueXP pode agora digitalizar dados no StorageGRID.

Para obter detalhes, "Digitalizar dados StorageGRID"consulte .

5 de agosto de 2024

Versão 1,34

Esta versão de classificação do BlueXP inclui a seguinte atualização.

Mude de CentOS para Ubuntu

A classificação BlueXP atualizou seu sistema operacional Linux para Microsoft Azure e Google Cloud Platform (GCP) do CentOS 7,9 para o Ubuntu 22,04.04.

Para obter detalhes sobre a implantação, "Instale em um host Linux com acesso à Internet e prepare o sistema host Linux" consulte .

1 de julho de 2024

Versão 1,33

Ubuntu suportado

Esta versão suporta a plataforma Ubuntu 24,04 Linux.

As digitalizações de mapeamento recolhem metadados

Os metadados a seguir são extraídos de arquivos durante verificações de mapeamento e são exibidos nos painéis de governança, conformidade e investigação:

- Ambiente de trabalho
- Tipo de ambiente de trabalho
- Repositório de storage
- Tipo de ficheiro
- Capacidade utilizada
- Número de ficheiros
- Tamanho do ficheiro
- Criação de ficheiros
- Último acesso ao ficheiro
- Ficheiro modificado pela última vez
- Hora descoberta do ficheiro
- Extração de permissões

Dados adicionais em painéis

Esta versão atualiza os dados que aparecem nos painéis de governança, conformidade e investigação

durante verificações de mapeamento.

Para obter detalhes, consulte "Qual é a diferença entre mapeamento e classificação de exames"

5 de junho de 2024

Versão 1,32

Nova coluna de estado do mapeamento na página Configuração

Esta versão agora mostra uma nova coluna de status do Mapeamento na página Configuração. A nova coluna ajuda a identificar se o mapeamento está em execução, na fila, em pausa ou mais.

Para obter explicações sobre os Estados, "Alterar as definições de digitalização" consulte .

15 de maio de 2024

Versão 1,31

A classificação está disponível como um serviço principal dentro do BlueXP

A classificação BlueXP está agora disponível como um recurso principal no BlueXP sem custo adicional para até 500 TIB de dados digitalizados. Nenhuma licença de classificação ou assinatura paga é necessária. À medida que focamos a funcionalidade de classificação do BlueXP na digitalização de sistemas de armazenamento NetApp com esta nova versão, algumas funcionalidades antigas só estarão disponíveis para clientes que já haviam pago uma licença. O uso desses recursos herdados expirará quando o contrato pago atingir sua data final.

"Saiba mais sobre os recursos obsoletos".

1 de abril de 2024

Versão 1,30

Suporte adicionado para classificação RHEL v8,8 e v9,3 BlueXP

Esta versão fornece suporte para Red Hat Enterprise Linux v8,8 e v9,3, além do 9.x anteriormente suportado, que requer Podman, em vez do motor Docker. Isto é aplicável a qualquer instalação manual no local da classificação BlueXP .

Os seguintes sistemas operacionais requerem o uso do motor de contentor Podman, e eles exigem a classificação BlueXP versão 1,30 ou superior: Red Hat Enterprise Linux versão 8,8, 9,0, 9,1, 9,2 e 9,3.

Saiba mais "Visão geral das implantações de classificação BlueXP " sobre o .

A classificação BlueXP é suportada se você instalar o conetor em um host RHEL 8 ou 9 que reside no local. Não será compatível se o host RHEL 8 ou 9 residir na AWS, Azure ou Google Cloud.

Opção para ativar a coleção de logs de auditoria removida

A opção para ativar a coleção de registos de auditoria foi desativada.

Velocidade de digitalização melhorada

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

Atualizações automáticas

Se você implantou a classificação do BlueXP em um sistema com acesso à Internet, o sistema será atualizado automaticamente. Anteriormente, a atualização ocorreu após um tempo específico decorrido desde a última atividade do utilizador. Com esta versão, a classificação do BlueXP é atualizada automaticamente se a hora local estiver entre as 1:00 e as 5:00 horas. Se a hora local estiver fora dessas horas, a atualização ocorre após um tempo específico decorrido desde a última atividade do usuário. Para obter detalhes, "Instale em um host Linux com acesso à Internet" consulte .

Se você implantou a classificação do BlueXP sem acesso à Internet, precisará atualizar manualmente. Para obter detalhes, "Instale a classificação BlueXP em um host Linux sem acesso à Internet" consulte .

4 de março de 2024

Versão 1,29

Agora você pode excluir dados de digitalização que residem em certos diretórios de origem de dados

Se você quiser que a classificação do BlueXP exclua os dados de digitalização que residem em determinados diretórios de origem de dados, você pode adicionar esses nomes de diretório a um arquivo de configuração que a classificação do BlueXP processa. Este recurso permite evitar a verificação de diretórios desnecessários ou que resultariam na devolução de resultados falsos positivos de dados pessoais.

"Saiba mais".

O suporte a instâncias extra grandes agora está qualificado

Se você precisar da classificação do BlueXP para analisar mais de 250 milhões de arquivos, poderá usar uma instância extra Large na implantação na nuvem ou na instalação no local. Este tipo de sistema pode digitalizar até 500 milhões de arquivos.

"Saiba mais".

10 de janeiro de 2024

Versão 1,27

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

Os resultados filtrados na página de investigação agora mostram 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 "Open to Organization"

Agora você pode configurar IDs de grupo em NFS para serem considerados como "Open to Organization" diretamente da classificação BlueXP se o grupo não tivesse sido definido inicialmente com essa permissão. Todos os arquivos e pastas que tenham esses IDs de grupo anexados serão exibidos como "Open to Organization" na página Detalhes da investigação. Consulte como "Adicionar IDs de grupo adicionais como "aberto à organização"" .

14 de dezembro de 2023

Versão 1.26.6

Esta versão incluiu algumas pequenas melhorias.

A versão também removeu as seguintes opções:

- A opção para ativar a coleção de registos de auditoria foi desativada.
- Durante a investigação de diretórios, a opção de calcular o número de dados pessoais identificáveis (PII) por diretórios não está disponível. "Investigue os dados armazenados em sua organização"Consulte a .
- A opção de integrar dados usando rótulos AIP (proteção de informações do Azure) foi desativada. "Organize os seus dados privados"Consulte a .

6 de novembro de 2023

Versão 1.26.3

Os seguintes problemas foram corrigidos nesta versão

- Corrigido uma inconsistência ao apresentar o número de arquivos digitalizados pelo sistema em painéis.
- Melhorou o comportamento de digitalização, manipulando e relatando arquivos e diretórios com carateres especiais no nome e metadados.

4 de outubro de 2023

Versão 1,26

Suporte para instalações locais da classificação BlueXP no RHEL versão 9

As versões 8 e 9 do Red Hat Enterprise Linux não suportam o mecanismo Docker; o que era necessário para a instalação de classificação do BlueXP . Agora oferecemos suporte à instalação de classificação BlueXP no RHEL 9,0, 9,1 e 9,2 usando o Podman versão 4 ou superior como infraestrutura de contentor. Se o seu ambiente requer o uso das versões mais recentes do RHEL, agora você pode instalar a classificação BlueXP (versão 1,26 ou superior) ao usar o Podman.

Neste momento, não suportamos instalações de locais escuros ou ambientes de digitalização distribuídos (usando um nó de scanner mestre e remoto) ao usar o RHEL 9.x.

5 de setembro de 2023

Versão 1,25

Implantações pequenas e médias temporariamente indisponíveis

Ao implantar uma instância de classificação do BlueXP na AWS, a opção de selecionar **Deploy > Configuration** 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 **Deploy > Deploy**.

Aplique etiquetas em até 100.000 itens da página de resultados da investigação

No passado, você só poderia aplicar tags a uma única página de cada vez na página de resultados da investigação (20 itens). Agora você pode selecionar **todos** itens nas páginas de resultados da investigação e aplicar tags a todos os itens - até 100.000 itens de cada vez. "Veja como".

Identificar arquivos duplicados com um tamanho mínimo de arquivo de 1 MB

Classificação BlueXP usada para identificar arquivos duplicados somente quando os arquivos eram 50 MB ou maiores. Agora, arquivos duplicados começando com 1 MB podem ser identificados. Você pode usar os filtros de página de investigação "tamanho do arquivo" junto com "Duplicates" para ver quais arquivos de um determinado tamanho são duplicados em seu ambiente.

17 de julho de 2023

Versão 1,24

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

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

- ID Alemão (Personalausweisnummer)
- Número da Segurança Social Alemã (Sozialversicherungsnummer)

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

A classificação BlueXP é totalmente suportada no modo restrito e no modo Privado

A classificação BlueXP é agora totalmente suportada em 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 conetor".

Capacidade de ignorar versões ao atualizar uma instalação em modo privado da classificação BlueXP

Agora você pode atualizar para uma versão mais recente da classificação BlueXP , mesmo que não seja sequencial. Isso significa que a atual limitação de atualização da classificação BlueXP por uma versão de cada vez não é mais necessária. Esta função é relevante a partir da versão 1,24 em diante.

A API de classificação BlueXP já está disponível

A API de classificação do BlueXP permite executar ações, criar consultas e exportar informações sobre os dados que você está digitalizando. A documentação interativa está disponível usando Swagger. A documentação é separada em várias categorias, incluindo investigação, conformidade, Governança e Configuração. Cada categoria é uma referência às guias na IU de classificação do BlueXP .

"Saiba mais sobre as APIs de classificação do BlueXP ".

6 de junho de 2023

Versão 1,23

O japonês agora é suportado ao procurar nomes de titulares de dados

Os nomes japoneses agora podem ser inseridos ao procurar 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. Também pode introduzir nomes japoneses no "Filtro "titular dos dados" na página Investigação de dados" para identificar ficheiros que contenham o nome do assunto.

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

O Ubuntu 22,04 foi qualificado como um sistema operacional suportado para a classificação BlueXP . Você pode instalar a classificação BlueXP em um host Linux Ubuntu em sua rede, ou em um host Linux na nuvem ao usar a versão 1,23 do instalador. "Veja como instalar a classificação BlueXP em um host com Ubuntu instalado".

O Red Hat Enterprise Linux 8,6 e 8,7 não são mais compatíveis com novas instalações de classificação BlueXP

Essas versões não são suportadas com novas implantações porque a Red Hat não suporta mais Docker, o que é um pré-requisito. Se você tiver uma máquina de classificação BlueXP existente em execução no RHEL 8,6 ou 8,7, o NetApp continuará a suportar sua configuração.

A classificação BlueXP pode ser configurada como um Coletor FPolicy para receber eventos FPolicy de sistemas ONTAP

Você pode habilitar logs de auditoria de acesso a arquivos para serem coletados no sistema de classificação do BlueXP para eventos de acesso a arquivos detetados em volumes em seus ambientes de trabalho. A classificação BlueXP pode capturar os seguintes tipos de eventos FPolicy e os usuários que realizaram 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 compatíveis com dark sites

Agora você pode carregar sua licença BYOL do Data Sense para a carteira digital BlueXP em um site escuro para que você seja notificado quando sua licença estiver ficando baixa. "Veja como obter e carregar sua licença BYOL do Data Sense".

3 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 digitalizado 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 a governança de dados, exposições à 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 classificação do BlueXP em instâncias menores na nuvem

Ao implantar a classificação do BlueXP a partir de um BlueXP Connector em um ambiente AWS, agora você pode selecionar entre dois tipos de instância menores do que o que está disponível com a instância padrão. Se você estiver digitalizando um ambiente pequeno, isso pode ajudá-lo a economizar nos custos da nuvem. No entanto, há algumas restrições ao usar a instância menor. "Consulte os tipos e limitações de instâncias disponíveis".

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

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

7 de março de 2023

Versão 1,21

Nova funcionalidade para adicionar suas próprias categorias personalizadas a partir da IU de classificação do BlueXP

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

"Saiba mais".

Agora você pode adicionar palavras-chave personalizadas a partir da IU de classificação do BlueXP

A classificação BlueXP teve a capacidade de adicionar palavras-chave personalizadas que a classificação BlueXP identificará em futuras varreduras por um tempo. No entanto, você precisava fazer login no host Linux

de classificação BlueXP e usar uma interface de linha de comando para adicionar as palavras-chave. Nesta versão, a capacidade de adicionar palavras-chave personalizadas está na IU de classificação do BlueXP , tornando muito fácil adicionar e editar essas palavras-chave.

"Saiba mais sobre como adicionar palavras-chave personalizadas a partir da IU de classificação do BlueXP ".

Capacidade de ter arquivos de varredura de classificação BlueXP not quando o "último tempo de acesso" será alterado

Por padrão, se a classificação BlueXP não tiver permissões de "gravação" adequadas, o sistema não digitalizará arquivos em seus volumes porque a classificação BlueXP não pode reverter o "último tempo de acesso" para o carimbo de data/hora original. No entanto, se você não se importa se a última hora de acesso é redefinida para a hora original em seus arquivos, você pode substituir esse comportamento na página Configuração para que a classificação BlueXP digitalize os volumes independentemente das permissões.

Em conjunto com esta capacidade, e um novo filtro chamado "Scan Analysis Event" foi adicionado para que você possa visualizar os arquivos que não foram classificados porque a classificação BlueXP não pôde reverter a última hora acessada, ou os arquivos que foram classificados, mesmo que a classificação BlueXP não pudesse reverter a última hora acessada.

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

Três novos tipos de dados pessoais são identificados pela classificação BlueXP

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

- Número do cartão de identidade do Botswana (Omang)
- Número de passaporte do Botsuana
- Cartão de identidade de Registro Nacional de Cingapura (NRIC)

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

Funcionalidade atualizada para diretórios

- A opção "Light CSV Report" para relatórios de investigação de dados agora inclui informações de diretórios.
- O filtro de tempo "último acesso" agora mostra o último tempo acessado para arquivos e diretórios.

Melhorias na instalação

- O instalador de classificação BlueXP para sites sem acesso à Internet (dark sites) agora executa uma pré-verificação para garantir que seus requisitos de sistema e rede estejam em vigor para uma instalação bem-sucedida.
- Os arquivos de log de auditoria de instalação são salvos agora; eles são gravados no `/ops/netapp/install_logs`.

5 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 classificação do BlueXP , você pode enviar alertas por e-mail para os usuários do BlueXP em sua conta quando certas políticas críticas retornam resultados. Esse recurso permite que você receba notificações para proteger seus dados quando não estiver online. Agora você também pode enviar alertas de e-mail de políticas para quaisquer outros usuários - até 20 endereços de e-mail - que não estejam

em sua conta do BlueXP .

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

Agora você pode adicionar padrões pessoais a partir da IU de classificação do BlueXP

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

"Saiba mais sobre como adicionar padrões personalizados a partir da IU de classificação do BlueXP ".

Capacidade de mover 15 milhões de arquivos usando a classificação BlueXP

No passado, você poderia fazer com que a classificação BlueXP movesse um máximo de 100.000 arquivos de origem para qualquer compartilhamento NFS. Agora você pode mover até 15 milhões de arquivos de cada vez. "Saiba mais sobre como mover arquivos de origem usando a classificação BlueXP ".

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

O filtro "número de usuários com acesso" agora suporta arquivos armazenados em repositórios do SharePoint Online. No passado, apenas os arquivos em compartilhamentos CIFS eram suportados. Observe que os grupos do SharePoint que não são baseados em diretório ativo não serão contados neste filtro neste momento.

Foi adicionado novo estado "Partial success" (sucesso parcial) ao painel Action Status (Estado da ação)

O novo status "sucesso parcial" indica que uma ação de classificação BlueXP foi concluída e alguns itens falharam e alguns itens foram bem-sucedidos, por exemplo, quando você está movendo ou excluindo arquivos 100. Além disso, o status "terminado" foi renomeado para "sucesso". No passado, o status "terminado" pode listar ações que tiveram êxito e que falharam. Agora, o status "sucesso" significa que todas as ações foram bem-sucedidas em todos os itens. "Consulte como exibir o painel Status das ações".

9 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 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 confidenciais e confidenciais) e que são excessivamente permissivos. Isso pode ajudá-lo a ver onde você pode ter alguns riscos com dados confidenciais. "Saiba 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 para um determinado número de usuários. Você pode escolher um intervalo de números para refinar os resultados - por exemplo, para ver quais arquivos são acessíveis por usuários do 51-100.
- Os filtros "hora criada", "hora descoberta", "última modificação" e "último acesso" agora permitem que você crie um intervalo de datas personalizado em vez de apenas selecionar um intervalo de dias predefinido. Por exemplo, você pode procurar arquivos com "hora criada" "mais de 6 meses" ou com uma data "Last Modified" dentro dos "últimos 10 dias".

- O filtro "caminho do arquivo" agora permite que você especifique caminhos que você deseja excluir dos resultados da consulta filtrada. Se você inserir caminhos para incluir e excluir determinados dados, a classificação BlueXP localiza todos os arquivos nos caminhos incluídos primeiro, então remove arquivos de caminhos excluídos e, em seguida, exibe os resultados.

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

A classificação BlueXP pode identificar o número individual japonês

A classificação BlueXP 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 classificação BlueXP pode identificar em seus dados".

Limitações conhecidas

As limitações conhecidas identificam funções que não são suportadas por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações com cuidado.

Opções de liberação de classificação BlueXP removidas

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

- A opção para ativar a coleção de registos de auditoria foi desativada.
- Durante a investigação de diretórios, a opção de calcular o número de dados pessoais identificáveis (PII) por diretórios não está disponível.
- A opção de integrar dados usando rótulos AIP (proteção de informações do Azure) foi desativada.

Limitações de digitalização da classificação BlueXP

A classificação BlueXP verifica apenas uma partilha sob um volume

Se você tiver vários compartilhamentos de arquivo em um único volume, a classificação BlueXP verificará o compartilhamento com a hierarquia mais alta. Por exemplo, se você tiver compartilhamentos como o seguinte:

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

Em seguida, os dados em /A serão digitalizados. Os dados em /C e /D não serão digitalizados.

Solução alternativa

Existe uma solução alternativa para verificar se você está digitalizando dados de todos os compartilhamentos do seu volume. Siga estes passos:

1. No ambiente de trabalho, adicione o volume a ser lido.
2. Depois que a classificação do BlueXP concluir a digitalização do volume, vá para a página *Investigação de dados* e crie um filtro para ver qual compartilhamento está sendo digitalizado:

   Você filtrará os dados por "Nome do ambiente de trabalho" e "tipo de diretório" 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 digitalizados.
4. "Adicione os compartilhamentos restantes a um grupo de ações".

   Você precisará adicionar todos os compartilhamentos individualmente, por exemplo:

   ```
   /C
   /D
   ```

5. Execute estas etapas para cada volume no ambiente de trabalho que tenha vários compartilhamentos.

Comece agora

Saiba mais sobre a classificação BlueXP

A classificação do BlueXP (Cloud Data Sense) é um serviço de governança de dados do BlueXP que analisa suas fontes de dados corporativas no local e na nuvem para mapear e classificar dados e identificar informações privadas. Isso pode ajudar a reduzir os riscos de segurança e conformidade, diminuir os custos de storage e auxiliar nos projetos de migração de dados.

IMPORTANTE

A partir de maio de 2024 com a versão 1,31, a classificação BlueXP está agora disponível como uma capacidade principal dentro do BlueXP sem nenhum custo adicional. Nenhuma licença de classificação ou assinatura é necessária. Também concentramos a funcionalidade de classificação do BlueXP em sistemas de armazenamento NetApp, de modo que alguns recursos não utilizados ou subutilizados foram obsoletos.

"Veja uma lista de recursos obsoletos".

Os usuários que usam versões antigas 1,30 ou anteriores continuarão a poder usar essa versão até que sua assinatura expire.

Caraterísticas

A classificação do BlueXP usa inteligência artificial (AI), processamento de linguagem natural (PNL) e aprendizado de máquina (ML) para entender o conteúdo verificado, extrair entidades e categorizar o conteúdo de acordo. Isso permite que a classificação BlueXP forneça as seguintes áreas de funcionalidade.

"Saiba mais sobre os casos de uso da classificação BlueXP ".

Manter a conformidade

A classificação BlueXP fornece várias ferramentas que podem ajudar com seus esforços de conformidade. Você pode usar a classificação BlueXP para:

- Identificar informações pessoais identificáveis (PII).
- Identifique um amplo escopo de informações pessoais confidenciais conforme exigido pelas regulamentações de privacidade do GDPR, CCPA, PCI e HIPAA.
- Responder a solicitações de acesso do titular dos dados (DSAR) com base no nome ou endereço de e-mail.

Fortalecer a segurança

A classificação do BlueXP pode identificar dados que estão potencialmente em risco de serem acessados para fins criminais. Você pode usar a classificação BlueXP para:

- Identifique todos os arquivos e diretórios (compartilhamentos e pastas) com permissões abertas que são expostas a toda a sua organização ou ao público.
- Identificar dados confidenciais que residam fora do local inicial dedicado.

- Obedecer às políticas de retenção de dados.
- Use *policies* para detetar automaticamente novos problemas de segurança para que a equipe de segurança possa agir imediatamente.

Otimizar a utilização do storage

A classificação do BlueXP fornece ferramentas que podem ajudar no custo total de propriedade (TCO) de storage. Você pode usar a classificação BlueXP para:

- Aumente a eficiência do storage identificando dados duplicados ou não relacionados aos negócios.
- Economize em custos de storage identificando dados inativos que podem ser categorizados para storage de objetos mais barato. "Saiba mais sobre a disposição em camadas dos sistemas Cloud Volumes ONTAP". "Saiba mais sobre a disposição em camadas em sistemas ONTAP no local".

Ambientes de trabalho e fontes de dados compatíveis

A classificação BlueXP pode digitalizar e analisar dados estruturados e não estruturados a partir dos seguintes tipos de ambientes de trabalho e fontes de dados:

Ambientes de trabalho

- Cloud Volumes ONTAP (implantado na AWS, Azure ou GCP)
- Clusters ONTAP on-premises
- StorageGRID
- Azure NetApp Files
- Amazon FSX para ONTAP
- Google Cloud NetApp volumes
- Fontes de dados*
- Compartilhamentos de arquivo do NetApp
- Bancos de dados:
  - Amazon Relational Database Service (Amazon RDS)
  - MongoDB
  - MySQL
  - Oracle
  - PostgreSQL
  - SAP HANA
  - SQL Server (MSSQL)

A classificação do BlueXP é compatível com as versões NFS 3.x, 4,0 e 4,1, e as versões CIFS 1.x, 2,0, 2,1 e 3,0.

Custo

A classificação BlueXP é agora livre de usar. Nenhuma licença de classificação ou assinatura paga é necessária.

Custos de infraestrutura

- A instalação da classificação do BlueXP na nuvem requer a implantação de uma instância de nuvem, o que resulta em cobranças do provedor de nuvem onde ela é implantada. o tipo de instância que é implantada para cada provedor de nuvemConsulte . Não há custo se você instalar a classificação do BlueXP em um sistema local.
- A classificação BlueXP requer que você tenha implantado um conetor BlueXP . Em muitos casos, você já tem um conetor devido a outros serviços e storage que você está usando no BlueXP . A instância do conetor resulta em cobranças do provedor de nuvem onde ela é implantada. Consulte "tipo de instância implantada para cada provedor de nuvem" . Não há custo se você instalar o conetor em um sistema local.

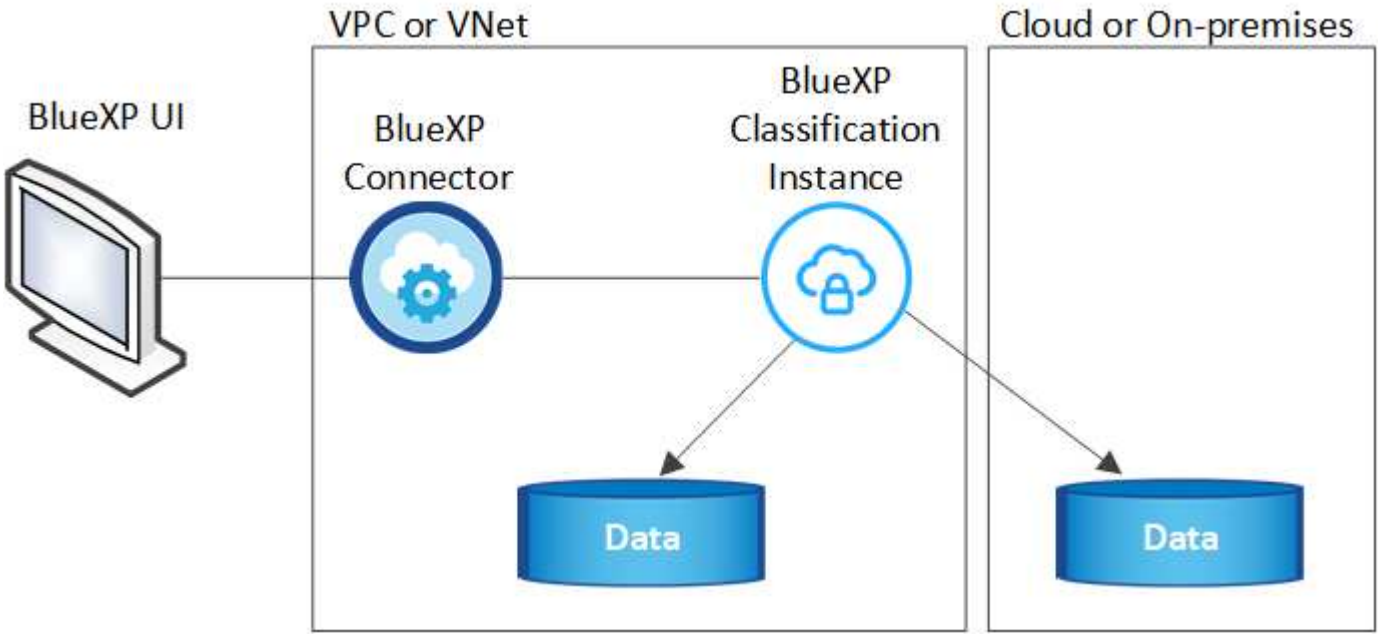
Custos de transferência de dados

Os custos de transferência de dados dependem da configuração. Se a instância de classificação BlueXP 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 ou região de disponibilidade *diferente*, você será cobrado pelo seu provedor de nuvem pelos custos de transferência de dados. Veja estes links para mais detalhes:

- "AWS: Definição de preço do Amazon Elastic Compute Cloud (Amazon EC2)"
- "Microsoft Azure: Detalhes de preços de largura de banda"
- "Google Cloud: Preços do Serviço de transferência de storage"

A instância de classificação BlueXP

Ao implantar a classificação do BlueXP na nuvem, o BlueXP implanta a instância na mesma sub-rede que o conetor. "Saiba mais sobre conetores."



Observe o seguinte sobre a instância padrão:

- Na AWS, a classificação BlueXP é executada em um "instância m6i.4xlarge" com um disco GP2 GiB de 500 GB. 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 BlueXP é executada em a "Standard_D16s_v3 VM" com um disco de 500 GiB. A imagem do sistema operacional é Ubuntu 22,04.04.
- No GCP, a classificação BlueXP é executada em um "VM N2-standard-16" com um disco persistente padrão de 500 GiB. A imagem do sistema operacional é Ubuntu 22,04.04.
- Em regiões onde a instância padrão não está disponível, a classificação BlueXP é executada em uma instância alternativa. "Consulte os tipos de instância alternativos".
- A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Apenas uma instância de classificação BlueXP é implantada por conetor.

Você também pode implantar a classificação do BlueXP em um host Linux no local ou em um host no seu provedor de nuvem preferido. O software funciona exatamente da mesma forma, independentemente do método de instalação que você escolher. As atualizações do software de classificação BlueXP são automatizadas, desde que a instância tenha acesso à Internet.

A instância deve permanecer em execução o tempo todo porque a classificação BlueXP verifica continuamente os dados.

Deploy em diferentes tipos de instância

Você pode implantar a classificação BlueXP em um sistema com menos CPUs e menos RAM.

Tamanho do sistema	Especificações	Limitações
Extra grande	32 CPUs, 128 GB de RAM, 1 TIB SSD	Pode digitalizar até 500 milhões de arquivos.
Grande (predefinição)	16 CPUs, 64 GB de RAM, 500 GiB SSD	Pode digitalizar até 250 milhões de arquivos.

Ao implantar a classificação do BlueXP no Azure ou no GCP, envie um e-mail para NetApp.com para obter assistência se você quiser usar um tipo de instância menor.

Como funciona a classificação BlueXP

Em um alto nível, a classificação BlueXP funciona assim:

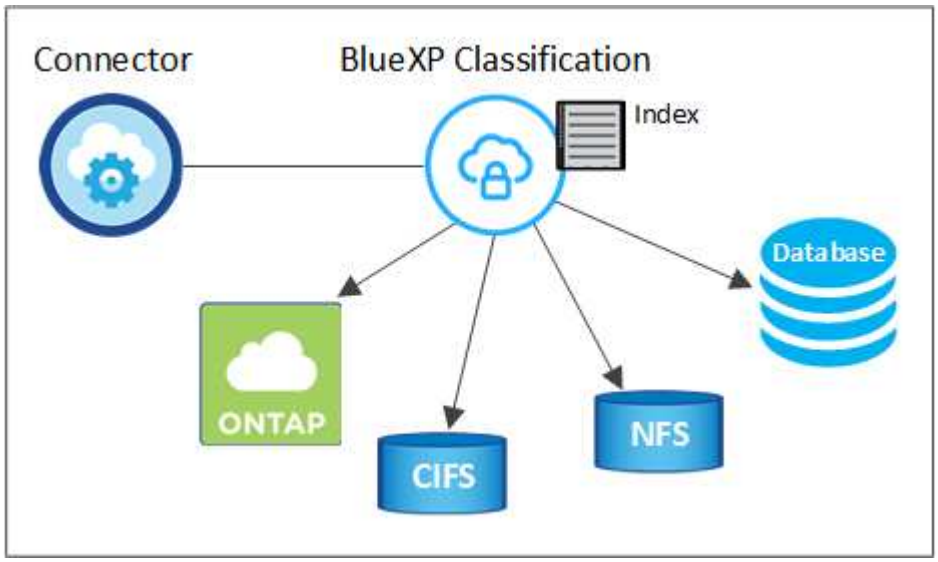
1. Você implanta uma instância de classificação BlueXP no BlueXP .
2. Você habilita o mapeamento de alto nível ou a varredura de nível profundo em uma ou mais fontes de dados.
3. A classificação BlueXP verifica os dados usando um processo de aprendizado de IA.
4. Você usa os painéis e as ferramentas de relatórios fornecidos para ajudar nos seus esforços de conformidade e governança.

Como as digitalizações funcionam

Depois de ativar a classificação do BlueXP e selecionar os repositórios que deseja analisar (estes são os volumes, esquemas de banco de dados ou outros dados do usuário), ele imediatamente começa a digitalizar os dados para identificar dados pessoais e confidenciais. Você deve se concentrar na digitalização de dados de produção ao vivo na maioria dos casos, em vez de backups, espelhos ou locais de DR. Em seguida, a

classificação BlueXP mapeia seus dados organizacionais, categoriza cada arquivo e identifica e extrai entidades e padrões predefinidos nos dados. O resultado da digitalização é um índice de informações pessoais, informações pessoais confidenciais, categorias de dados e tipos de arquivos.

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



Após a verificação inicial, a classificação do BlueXP verifica continuamente os seus dados de forma redonda para detetar alterações incrementais (é por isso que é importante manter a instância em execução).

Você pode ativar e desativar digitalizações no nível de volume ou no nível do esquema do banco de dados.

Qual é a diferença entre Mapeamento e classificação digitalizações

A classificação BlueXP permite-lhe executar uma digitalização geral de "mapeamento" em fontes de dados selecionadas. O mapeamento fornece apenas uma visão geral de alto nível dos seus dados, enquanto a classificação fornece uma varredura de nível profundo dos seus dados. O mapeamento pode ser feito em suas fontes de dados muito rapidamente, porque não acessa arquivos para ver os dados dentro.

Muitos usuários gostam dessa funcionalidade porque desejam Escanear rapidamente seus dados para identificar as fontes de dados que exigem mais pesquisas e, em seguida, podem habilitar varreduras de classificação apenas nas fontes de dados ou volumes necessários.

A tabela abaixo mostra algumas das diferenças:

Recurso	Classificação	Mapeamento
Velocidade de digitalização	Lento	Rápido
Preços	Livre	Livre
Capacidade	Limitado a 500 TB	Limitado a 500 TB
Lista de tipos de arquivo e capacidade usada	Sim	Sim
Número de arquivos e capacidade utilizada	Sim	Sim
Idade e tamanho dos arquivos	Sim	Sim

Recurso	Classificação	Mapeamento
Capacidade de executar a. "Relatório de mapeamento de dados"	Sim	Sim
Página de investigação de dados para ver os detalhes do ficheiro	Sim	Não
Procure nomes dentro de arquivos	Sim	Não
Crie "políticas" que forneça resultados de pesquisa personalizados	Sim	Não
Capacidade de executar outros relatórios	Sim	Não
Capacidade de ver metadados de arquivos*	Não	Sim

*Os seguintes metadados são extraídos de arquivos durante as varreduras de mapeamento:

- Ambiente de trabalho
- Tipo de ambiente de trabalho
- Repositório de storage
- Tipo de ficheiro
- Capacidade utilizada
- Número de ficheiros
- Tamanho do ficheiro
- Criação de ficheiros
- Último acesso ao ficheiro
- Ficheiro modificado pela última vez
- Hora descoberta do ficheiro
- Extração de permissões

Diferenças no painel de governança:

Recurso	Mapear e classificar	Mapa
Dados obsoletos	Sim	Sim
Dados não comerciais	Sim	Sim
Ficheiros duplicados	Sim	Sim
Políticas predefinidas	Sim	Não
Políticas personalizadas	Sim	Sim
Relatório DDA	Sim	Sim
Relatório de mapeamento	Sim	Sim
Detecção do nível de sensibilidade	Sim	Não
Dados confidenciais com permissões amplas	Sim	Não
Abrir permissões	Sim	Sim
Idade dos dados	Sim	Sim
Tamanho dos dados	Sim	Sim
Categorias	Sim	Não
Tipos de ficheiros	Sim	Sim

Diferenças no dashboard de conformidade:

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

Diferenças de filtros de investigação:

Recurso	Mapear e classificar	Mapa
Políticas	Sim	Sim
Tipo de ambiente de trabalho	Sim	Sim
Ambiente de trabalho	Sim	Sim
Repositório de storage	Sim	Sim
Tipo de ficheiro	Sim	Sim
Tamanho do ficheiro	Sim	Sim
Hora criada	Sim	Sim
Hora descoberta	Sim	Sim
Modificado pela última vez	Sim	Sim
Último acesso	Sim	Sim
Abrir permissões	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 confidenciais	Sim	Não
Titular dos dados	Sim	Não
Duplicatas	Sim	Sim
Estado da classificação	Sim	O status é sempre "informações limitadas"
Evento de análise de digitalização	Sim	Sim
Hash de ficheiro	Sim	Sim
Número de usuários com acesso	Sim	Sim
Permissões de usuário/grupo	Sim	Sim
Proprietário do ficheiro	Sim	Sim
Tipo de diretório	Sim	Sim

A rapidez com que a classificação BlueXP analisa os dados

A velocidade de digitalização é afetada pela latência da rede, latência do disco, largura de banda da rede, tamanho do ambiente e tamanhos de distribuição de arquivos.

- Ao realizar exames de mapeamento, a classificação BlueXP pode digitalizar entre 100-150 Tibs de dados

por dia.

- Ao executar exames de classificação, a classificação BlueXP pode digitalizar entre 15-40 Tibs de dados por dia.

Informação que a classificação BlueXP categoriza

A classificação BlueXP coleta, indexa e atribui categorias aos seus dados (arquivos). Os dados que a classificação BlueXP indexa incluem os seguintes:

- * 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. "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 GDPR e outros regulamentos de privacidade. "Saiba mais sobre dados pessoais confidenciais".
- **Categorias**: A classificação BlueXP leva os dados que digitalizou e divide-os em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. "Saiba mais sobre categorias".
- * Tipos*: A classificação BlueXP pega os dados que digitalizou e os divide por tipo de arquivo. "Saiba mais sobre tipos".
- * Reconhecimento de entidade de nome*: A classificação BlueXP usa IA para extrair os nomes naturais das pessoas de documentos. "Saiba mais sobre como responder às solicitações de acesso do titular dos dados".

Visão geral da rede

O BlueXP implanta a instância de classificação do BlueXP com um grupo de segurança que permite conexões HTTP de entrada da instância do conetor.

Ao usar o BlueXP no modo SaaS, a conexão com o BlueXP é servida por HTTPS, e os dados privados enviados entre o navegador e a instância de classificação do BlueXP são protegidos com criptografia de ponta a ponta usando TLS 1,2, o que significa que o NetApp e terceiros não podem lê-lo.

As regras de saída estão completamente abertas. O acesso à Internet é necessário para instalar e atualizar o software de classificação BlueXP e enviar métricas de utilização.

Se você tem exigências estritas da rede, "Saiba mais sobre os endpoints que a classificação BlueXP contacta".

Funções de utilizador na classificação BlueXP

A função atribuída a cada utilizador fornece diferentes capacidades dentro da classificação BlueXP e dentro da classificação BlueXP . Para obter detalhes, consulte o seguinte:

- "Funções do BlueXP IAM" (Ao utilizar o BlueXP no modo padrão)
- "Funções de conta do BlueXP " (Ao utilizar o BlueXP no modo restrito ou no modo privado)

Implantar a classificação BlueXP

Qual implantação de classificação BlueXP você deve usar?

Você pode implantar a classificação do BlueXP de maneiras diferentes. Saiba qual método atende às suas necessidades.

A classificação BlueXP pode ser implantada das seguintes maneiras:

- "Implante na nuvem usando o BlueXP ". O BlueXP implantará a instância de classificação BlueXP na mesma rede de provedores de nuvem que o BlueXP Connector.
- "Instale em um host Linux com acesso à Internet". Instale a classificação BlueXP em um host Linux em 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 digitalizar sistemas ONTAP locais usando uma instância de classificação BlueXP que também está localizada no local, mas isso não é um requisito.
- "Instale em um host Linux em um site no local sem acesso à Internet", Também conhecido como *private mode.* este tipo de instalação, que usa um script de instalação, não tem conetividade com a camada SaaS do BlueXP .

Tanto a instalação em um host Linux com acesso à Internet quanto a instalação no 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 de classificação do BlueXP , há um pacote de software separado que você pode baixar que apenas testa os pré-requisitos.

"Verifique se o seu host Linux está pronto para instalar a classificação BlueXP "Consulte a .

Implante a classificação do BlueXP na nuvem usando o BlueXP

Conclua algumas etapas para implantar a classificação do BlueXP na nuvem. O BlueXP implantará a instância de classificação BlueXP na mesma rede de provedores de nuvem que o BlueXP Connector.

Observe que você também "Instale a classificação BlueXP em um host Linux que tenha acesso à Internet"pode . Esse tipo de instalação pode ser uma boa opção se você preferir digitalizar sistemas ONTAP on-premises usando uma instância de classificação BlueXP que também está localizada no local, mas isso não é um requisito. O software funciona exatamente da mesma forma, independentemente do método de instalação que você escolher.

Início rápido

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

Crie um conetor

Se você ainda não tiver um conetor, crie um conetor agora. Consulte "Criando um conetor na AWS" "Criando um conetor no Azure" , , ou "Criando um conetor no GCP".

Você também pode "Instale o conetor no local" em um host Linux em sua rede ou em um host Linux na nuvem.

2 Reveja os pré-requisitos

Certifique-se de que seu ambiente atenda aos pré-requisitos. Isso inclui acesso de saída à Internet, por exemplo, conetividade entre o conetor e a classificação BlueXP na porta 443 e muito mais. Veja a lista completa.

3 Implantar a classificação BlueXP

Inicie o assistente de instalação para implantar a instância de classificação do BlueXP na nuvem.

Crie um conetor

Se você ainda não tiver um conetor, crie um conetor no seu provedor de nuvem. "Criando um conetor na AWS"Consulte ou "Criando um conetor no Azure", ou "Criando um conetor no GCP". Na maioria dos casos, você provavelmente terá um conetor configurado antes de tentar ativar a classificação BlueXP porque a maioria "Os recursos do BlueXP exigem um conetor", mas há casos em que você precisará configurar um agora.

Existem alguns cenários em que você precisa usar um conetor que é implantado em um provedor de nuvem específico:

- Ao digitalizar dados no Cloud Volumes ONTAP nos buckets do AWS ou do Amazon FSX for ONTAP, você usa um conetor na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um conetor no Azure.
  - Para o Azure NetApp Files, ele deve ser implantado na mesma região que os volumes que você deseja analisar.
- Ao digitalizar dados no Cloud Volumes ONTAP no GCP, você usa um conetor no GCP.

Os sistemas ONTAP locais, compartilhamentos de arquivos NetApp e bancos de dados podem ser verificados usando qualquer um desses conetores de nuvem.

Observe que você também pode "Instale o conetor no local" em um host Linux em sua rede ou na nuvem. Alguns usuários que planejam instalar a classificação do BlueXP no local também podem optar por instalar o conetor no local.

Como você pode ver, pode haver algumas situações em que você precisa usar "Vários conetores".

Apoio governamental na região

A classificação do BlueXP é suportada quando o conetor é implantado em uma região governamental (AWS GovCloud, Azure Gov ou Azure DoD). Quando implementada desta forma, a classificação BlueXP tem as seguintes restrições:

"Consulte mais informações sobre como implantar o conetor em uma região do governo".

Reveja os pré-requisitos

Revise os pré-requisitos a seguir para garantir que você tenha uma configuração compatível antes de implantar a classificação do BlueXP na nuvem. Quando você implementa a classificação BlueXP na nuvem, ela está localizada na mesma sub-rede que o conetor.

Ative o acesso de saída à Internet a partir da classificação BlueXP

A classificação BlueXP requer acesso de saída à Internet. Se a sua rede virtual ou física utilizar um servidor proxy para acesso à Internet, certifique-se de que a instância de classificação do BlueXP tem acesso de saída à Internet para contactar os seguintes endpoints. O proxy deve ser não transparente - atualmente não oferecemos suporte a proxies transparentes.

Consulte a tabela apropriada abaixo, dependendo se você está implantando a classificação do BlueXP na AWS, no Azure ou no GCP.

Endpoints necessários para a AWS

Endpoints	Finalidade
https://api.BlueXP .NetApp.com	Comunicação com o serviço BlueXP , que inclui contas NetApp.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o site BlueXP para autenticação centralizada de usuários.
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 a classificação do BlueXP para acessar e baixar manifestos e modelos, e para enviar logs e métricas.

Endpoints necessários para o Azure

Endpoints	Finalidade
https://api.BlueXP .NetApp.com	Comunicação com o serviço BlueXP , que inclui contas NetApp.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o site BlueXP para autenticação centralizada de usuários.
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.

Pontos de extremidade necessários para o GCP

Endpoints	Finalidade
https://api.BlueXP .NetApp.com	Comunicação com o serviço BlueXP , que inclui contas NetApp.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o site BlueXP para autenticação centralizada de usuários.

Endpoints	Finalidade
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.

Certifique-se de que o BlueXP tem as permissões necessárias

Certifique-se de que o BlueXP tenha permissões para implantar recursos e criar grupos de segurança para a instância de classificação do BlueXP . Você pode encontrar as permissões de BlueXP mais recentes no "As políticas fornecidas pela NetApp".

Certifique-se de que o conetor BlueXP pode aceder à classificação BlueXP

Garanta a conetividade entre o conetor e a instância de classificação BlueXP . O grupo de segurança do conetor deve permitir tráfego de entrada e saída pela porta 443 de e para a instância de classificação BlueXP . Essa conexão permite a implantação da instância de classificação do BlueXP e permite exibir informações nas guias conformidade e Governança. A classificação do BlueXP é compatível com regiões governamentais na AWS e no Azure.

Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações AWS e AWS GovCloud. "Regras para o conetor na AWS"Consulte para obter detalhes.

Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações do Azure e do Azure Government. "Regras para o conetor no Azure"Consulte para obter detalhes.

Certifique-se de que você pode manter a classificação BlueXP em execução

A instância de classificação do BlueXP precisa permanecer ligada para verificar continuamente seus dados.

Garanta a conetividade do navegador da Web com a classificação BlueXP

Depois que a classificação do BlueXP estiver ativada, certifique-se de que os usuários acessem a interface do BlueXP a partir de um host que tenha uma conexão com a instância de classificação do BlueXP .

A instância de classificação do BlueXP 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 BlueXP 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 BlueXP .

Verifique os limites do seu vCPU

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

Consulte os links a seguir para obter mais detalhes sobre os limites do 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"

Implante a classificação do BlueXP na nuvem

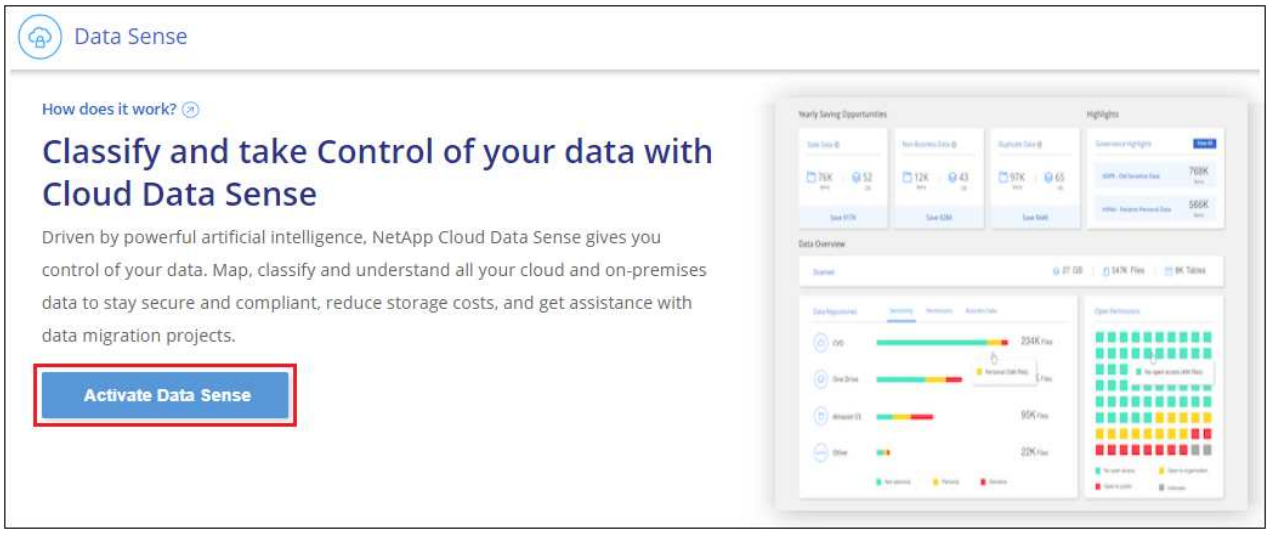
Siga estas etapas para implantar uma instância de classificação do BlueXP na nuvem. O conetor irá implantar a instância na nuvem e, em seguida, instalar o software de classificação BlueXP nessa instância.

Em regiões onde o tipo de instância padrão não está disponível, a classificação BlueXP é executada em um "tipo de instância alternativa".

Implante na AWS

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação**.



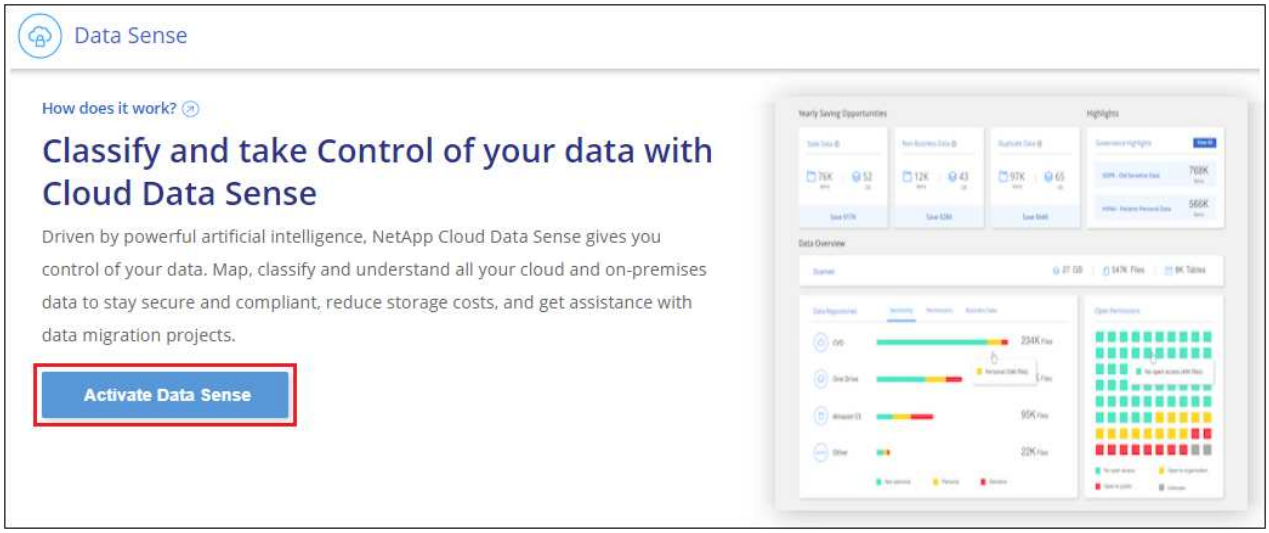
2. Clique em **Activate Data Sense**.
3. Na página *Installation*, clique em **Deploy > Deploy** para usar o tamanho da instância "grande" e iniciar o assistente de implantação na nuvem.
4. O assistente exibe o progresso à medida que passa pelas etapas de implantação. Ele irá parar e pedir a entrada se ele se deparar com quaisquer problemas.

5. Quando a instância for implantada e a classificação BlueXP estiver instalada, clique em **Continue to Configuration** para ir para a página *Configuration*.

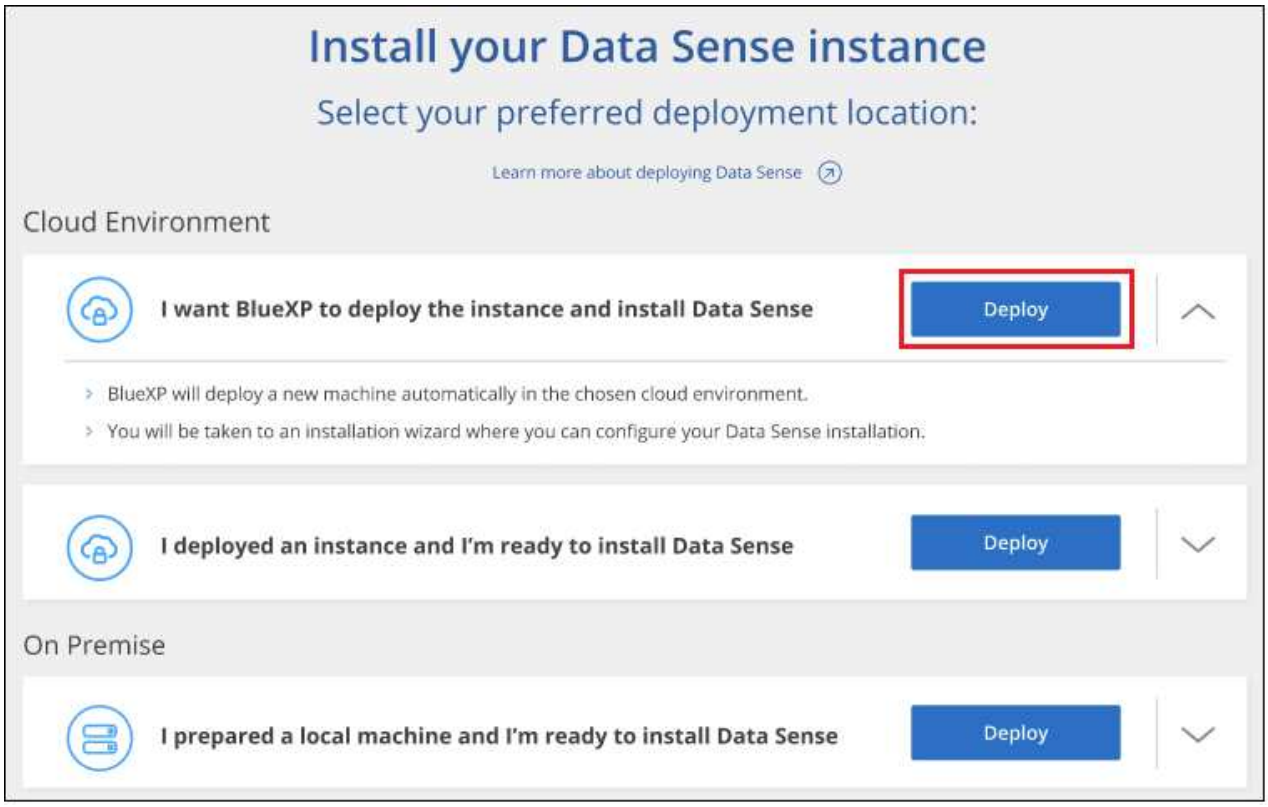
Implantar no Azure

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação**.
2. Clique em **Activate Data Sense**.



3. Clique em **Deploy** para iniciar o assistente de implantação na nuvem.



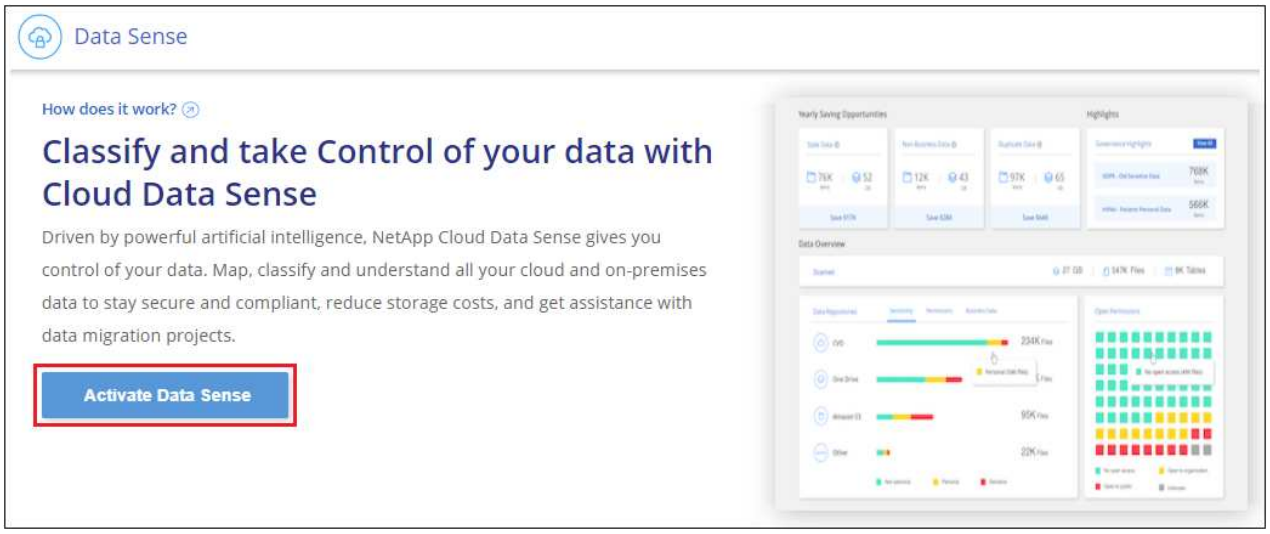
4. O assistente exibe o progresso à medida que passa pelas etapas de implantação. Ele irá parar e pedir a entrada se ele se deparar com quaisquer problemas.

5. Quando a instância for implantada e a classificação BlueXP estiver instalada, clique em **Continue to Configuration** para ir para a página *Configuration*.

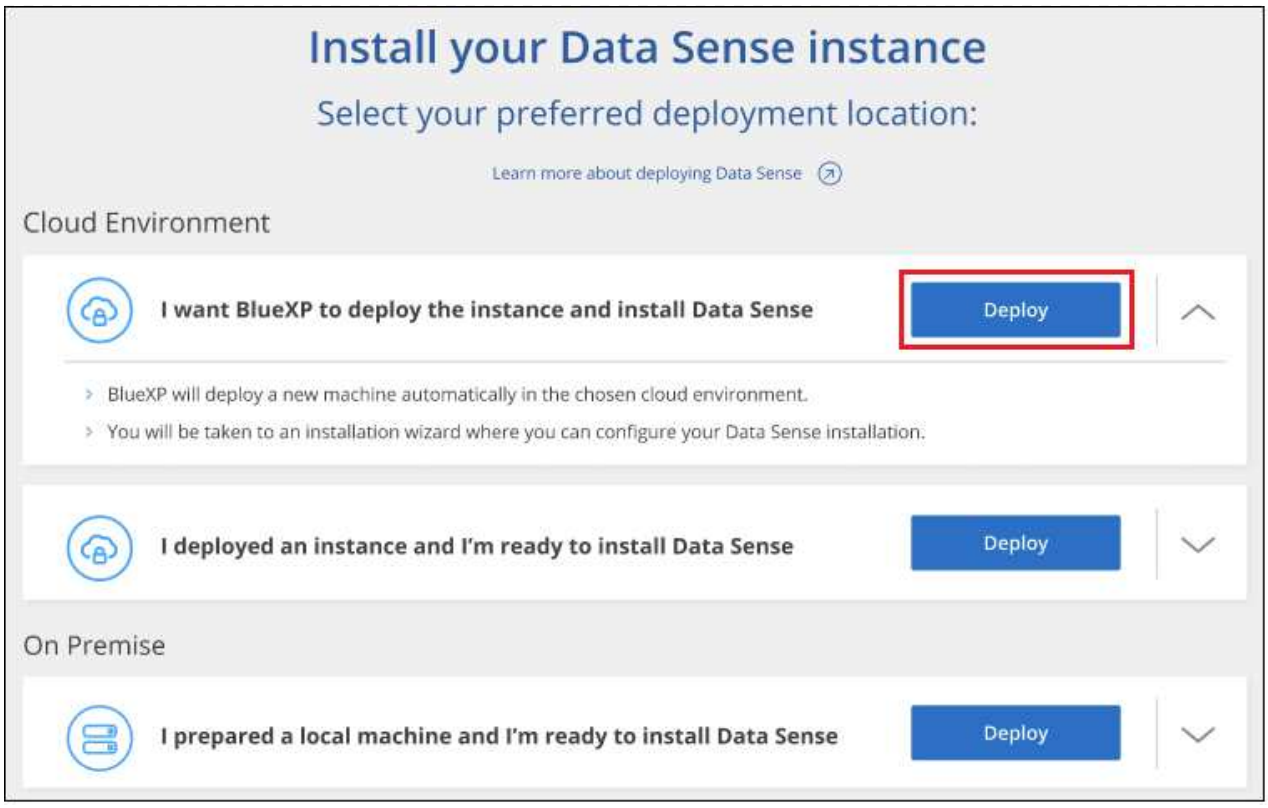
Implantar no Google Cloud

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação**.
2. Clique em **Activate Data Sense**.



3. Clique em **Deploy** para iniciar o assistente de implantação na nuvem.



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

5. Quando a instância for implantada e a classificação BlueXP estiver instalada, clique em **Continue to Configuration** para ir para a página *Configuration*.

Resultado

O BlueXP implanta a instância de classificação do BlueXP em seu provedor de nuvem.

As atualizações para o BlueXP Connector e o software de classificação BlueXP são automatizadas, desde que as instâncias tenham conetividade com a Internet.

O que vem a seguir

Na página Configuração, pode selecionar as fontes de dados que pretende digitalizar.

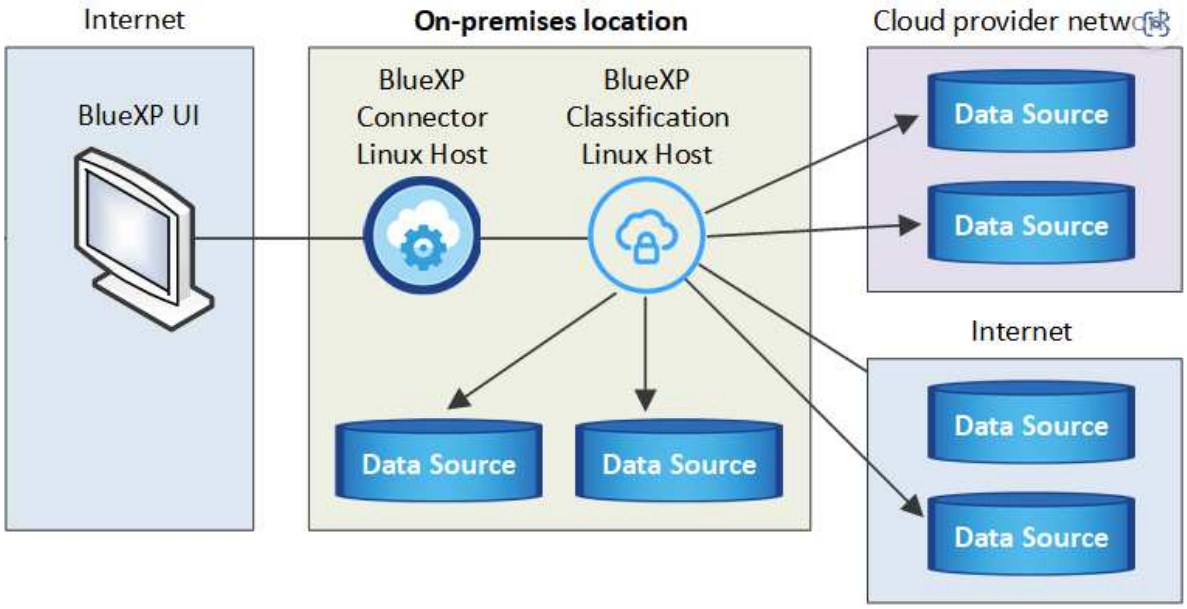
Instale a classificação BlueXP em um host que tenha acesso à Internet

Conclua algumas etapas para instalar a classificação BlueXP em um host Linux em sua rede, ou em um host Linux na nuvem, que tenha acesso à Internet. Você precisará implantar o host Linux manualmente em sua rede ou na nuvem como parte dessa instalação.

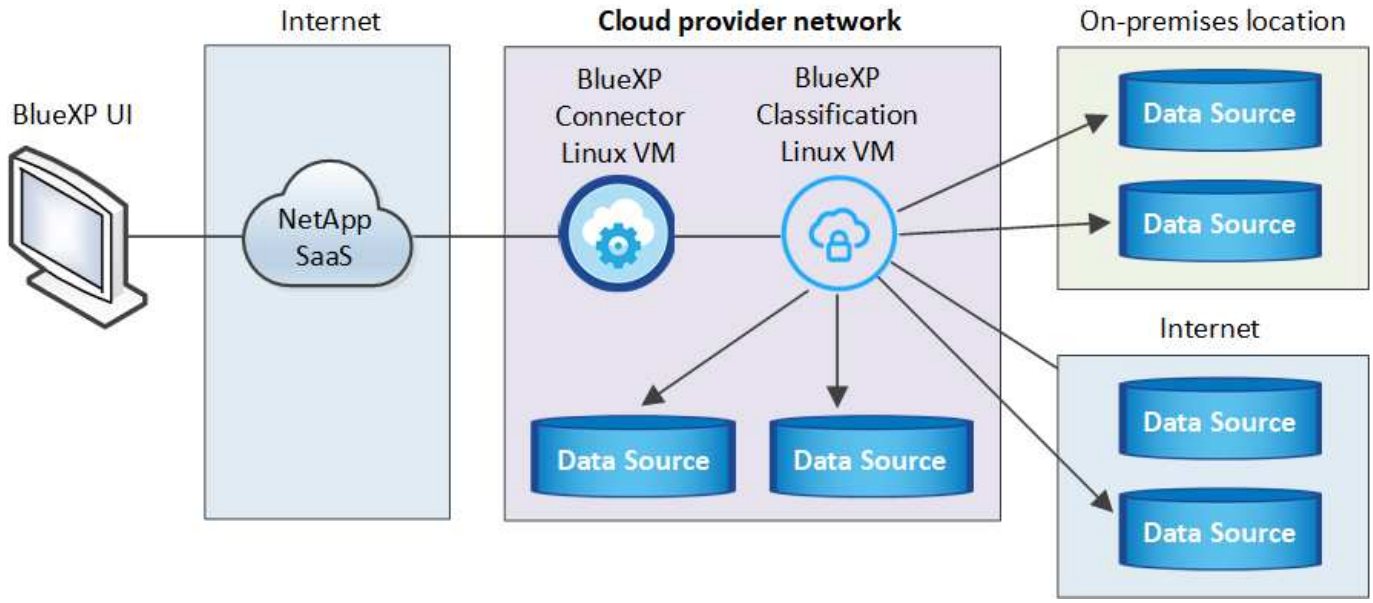
A instalação no local pode ser uma boa opção se você preferir digitalizar sistemas ONTAP locais usando uma instância de classificação do BlueXP que também esteja localizada no local, mas isso não é um requisito. O software funciona exatamente da mesma forma, independentemente do método de instalação que você escolher.

O script de instalação da classificação BlueXP 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 de classificação do BlueXP , há um pacote de software separado que você pode baixar que apenas testa os pré-requisitos. "Veja como verificar se o seu host Linux está pronto para instalar a classificação BlueXP ".

A instalação típica em um host Linux *in Your Premises* tem os seguintes componentes e conexões.



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



Para versões antigas 1,30 e anteriores, se for necessário instalar a classificação BlueXP em vários hosts, "Instale a classificação BlueXP em vários hosts sem acesso à Internet"consulte .

Você também "Instale a classificação BlueXP em um site local que não tenha acesso à Internet"pode .

Início rápido

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

1 Crie um conetor

Se você ainda não tiver um conetor, "Implante o conetor no local" em um host Linux em sua rede ou em um host Linux na nuvem.

Você também pode criar um conetor com seu provedor de nuvem. Consulte "Criando um conetor na AWS" "Criando um conetor no Azure" , , ou "Criando um conetor no GCP".

2 Reveja os pré-requisitos

Certifique-se de que seu ambiente atenda aos pré-requisitos. Isso inclui acesso de saída à Internet, por exemplo, conetividade entre o conetor e a classificação BlueXP na porta 443 e muito mais. Veja a lista completa.

Você também precisa de um sistema Linux que atenda ao seguindo os requisitos.

3 Baixe e implante a classificação BlueXP

Faça o download do software de classificação Cloud BlueXP 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 do BlueXP .

Crie um conetor

É necessário um conetor BlueXP antes de poder instalar e utilizar a classificação BlueXP . Na maioria dos casos, você provavelmente terá um conetor configurado antes de tentar ativar a classificação BlueXP porque a maioria "Os recursos do BlueXP exigem um conetor", mas há casos em que você precisará configurar um agora.

Para criar um no ambiente do provedor de nuvem, consulte "Criando um conetor na AWS" "Criando um conetor no Azure" , ou "Criando um conetor no GCP".

Existem alguns cenários em que você precisa usar um conetor que é implantado em um provedor de nuvem específico:

- Ao digitalizar dados no Cloud Volumes ONTAP na AWS ou no Amazon FSX for ONTAP, você usa um conetor na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um conetor no Azure.

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

- Ao digitalizar dados no Cloud Volumes ONTAP no GCP, você usa um conetor no GCP.

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

Observe que você também pode "Implante o conetor no local" em um host Linux em sua rede ou em um host Linux na nuvem. Alguns usuários que planejam instalar a classificação do BlueXP no local também podem optar por instalar o conetor no local.

Você precisará do endereço IP ou do nome do host do sistema de conetores ao instalar a classificação BlueXP . Você terá esta informação se você instalou o conetor em suas instalações. Se o conetor for implantado na nuvem, você poderá encontrar essas informações no console do BlueXP : Clique no ícone Ajuda, selecione **suporte** e clique em **conetor BlueXP** .

Prepare o sistema host Linux

O software de classificação BlueXP deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de software etc. O host Linux pode estar em sua rede ou na nuvem.

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

- A classificação BlueXP não é suportada em um host que é compartilhado com outros aplicativos - o host deve ser um host dedicado.
- Ao criar o sistema host em suas instalações, você pode escolher entre esses tamanhos de sistema, dependendo do tamanho do conjunto de dados que você planeja fazer a verificação de classificação do BlueXP .

Tamanho do sistema	CPU	RAM (a memória swap deve ser desativada)	Disco
* Extra grande *	32 CPUs	128 GB DE RAM	1 TIB SSD ON /, OR - 100 GiB disponível em /opt - 895 GiB disponível em /var/lib/docker - 5 GiB em /tmp
* Grande *	16 CPUs	64 GB DE RAM	500 GiB SSD ON /, OR - 100 GiB disponível em /opt - 395 GiB disponível em /var/lib/docker ou Podman /var/lib/containers ou Podman /var/lib/containers - 5 GiB em /tmp

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

Pasta	Permissões mínimas
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operacional**:
  - Os seguintes sistemas operacionais requerem o uso do mecanismo de contentor Docker:
    - Red Hat Enterprise Linux versão 7,8 e 7,9
    - Ubuntu 22,04 (requer classificação BlueXP versão 1,23 ou superior)
    - Ubuntu 24,04 (requer classificação BlueXP versão 1,23 ou superior)
  - Os seguintes sistemas operacionais requerem o uso do motor de contentores Podman, e eles exigem a classificação BlueXP versão 1,30 ou superior:
    - Red Hat Enterprise Linux versão 8,8, 9,0, 9,1, 9,2, 9,3, 9,4
- **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 necessário de 3rd partes durante a instalação.
- * Software adicional*: Você deve instalar o seguinte software no host antes de instalar a classificação BlueXP :
  - Dependendo do sistema operacional que você estiver usando, você precisará instalar um dos motores de contentor:

- Docker Engine versão 19.3.1 ou superior. "Veja as 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. "Veja as instruções de instalação".
  - **Considerações de NTP**: A NetApp recomenda configurar o sistema de classificação BlueXP para usar um serviço de protocolo de tempo de rede (NTP). O tempo deve ser sincronizado entre o sistema de classificação BlueXP e o sistema de conetores BlueXP .
  - **Considerações sobre o Firewalld**: Se você estiver planejando usar `firewalld`, recomendamos que você a ative antes de instalar a classificação do BlueXP . Execute os seguintes comandos para configurar `firewalld` de modo que seja compatível com a classificação BlueXP :

```
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 BlueXP adicionais como nós de scanner, adicione essas regras ao seu sistema principal 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 ativar ou atualizar `firewalld` as configurações.

O endereço IP do sistema anfitrião de classificação BlueXP não pode ser alterado após a instalação.

Ative o acesso de saída à Internet a partir da classificação BlueXP

A classificação BlueXP requer acesso de saída à Internet. Se a sua rede virtual ou física utilizar um servidor proxy para acesso à Internet, certifique-se de que a instância de classificação do BlueXP tem acesso de saída à Internet para contactar os seguintes endpoints.

Endpoints	Finalidade
https://api.BlueXP .NetApp.com	Comunicação com o serviço BlueXP , que inclui contas NetApp.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o site BlueXP para autenticação centralizada de usuários.

Endpoints	Finalidade
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 pré-requisitos para instalação do docker.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fornece pacotes pré-requisitos para instalação do Ubuntu.

Verifique se todas as portas necessárias estão ativadas

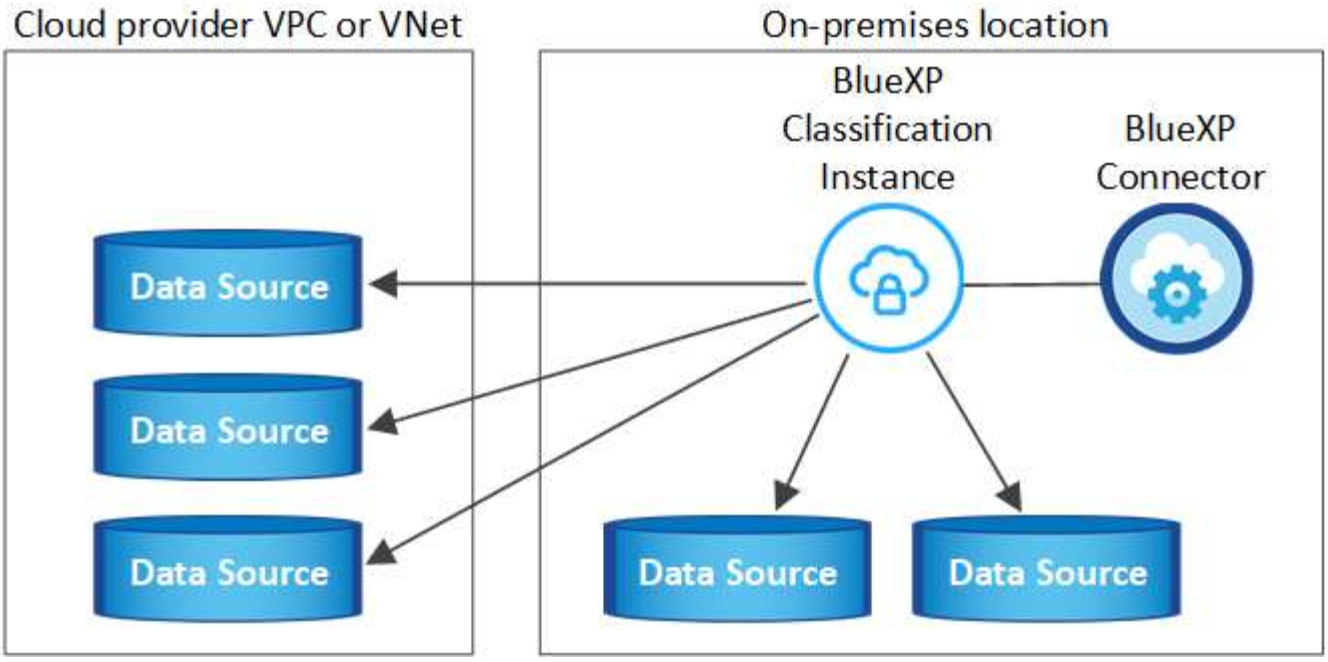
Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o conetor, a classificação do BlueXP , o ative Directory e suas fontes de dados.

Tipo de ligação	Portas	Descrição
Conetor >> classificação BlueXP	8080 (TCP), 443 (TCP) e 80. 9000	O firewall ou as regras de roteamento para o conetor devem permitir o tráfego de entrada e saída pela porta 443 de e para a instância de classificação BlueXP . Certifique-se de que a porta 8080 esteja aberta para que você possa ver o progresso da instalação no BlueXP . Se um firewall for usado no host Linux, a porta 9000 será necessária para processos internos dentro de um servidor Ubuntu.
Conetor do cluster do ONTAP (nas)	443 (TCP)	O BlueXP descobre clusters do ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, elas devem atender aos seguintes requisitos: • O host do conetor deve permitir o acesso HTTPS de saída através da porta 443. Se o conetor estiver na nuvem, toda a comunicação de saída é permitida pelo firewall predefinido ou pelas regras de roteamento. • O cluster ONTAP deve permitir acesso HTTPS de entrada através da porta 443. A política de firewall "mgmt" padrão permite o acesso HTTPS de entrada de todos os endereços IP. Se você modificou essa política padrão, ou se criou sua própria política de firewall, associe o protocolo HTTPS a essa política e habilite o acesso do host do conetor.

Tipo de ligação	Portas	Descrição
Classificação do BlueXP >> cluster ONTAP	• Para NFS - 111 (TCP/UDP) e 2049 (TCP/UDP) • Para CIFS - 139 (TCP/UDP) e 445 (TCP/UDP)	A classificação BlueXP precisa de uma conexão de rede para cada sub-rede Cloud Volumes ONTAP ou sistema ONTAP local. Firewalls ou regras de roteamento para Cloud Volumes ONTAP devem permitir conexões de entrada da instância de classificação BlueXP . Certifique-se de que essas portas estejam abertas para a instância de classificação BlueXP : • Para NFS - 111 e 2049 • Para CIFS - 139 e 445 As políticas de exportação de volume NFS devem permitir o acesso a partir da instância de classificação BlueXP .
Classificação do BlueXP >> ative Directory	389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)	Você deve ter um ative Directory já configurado para os usuários em sua empresa. Além disso, a classificação do BlueXP precisa de credenciais do ative Directory para verificar volumes CIFS. Você deve ter as informações do ative Directory: • Endereço IP do servidor DNS ou vários endereços IP • Nome de usuário e senha para o servidor • Nome de domínio (Nome do ative Directory) • Quer esteja a utilizar LDAP seguro (LDAPS) ou não • Porta de servidor LDAP (normalmente 389 para LDAP e 636 para LDAP seguro)

Instale a classificação BlueXP no host Linux

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



Preparando o sistema host LinuxConsulte e Rever pré-requisitos para obter a lista completa de requisitos antes de implantar a classificação do BlueXP .

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Atualmente, a classificação do BlueXP não consegue digitalizar buckets do S3, Azure NetApp Files ou FSX for ONTAP quando o software é instalado no local. Nesses casos, você precisará implantar um conetor separado e uma instância de classificação do BlueXP na nuvem e "Alternar entre os conetores" para suas diferentes fontes de dados.

Instalação de um único host para configurações típicas

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

"Assista a este vídeo" Para ver como instalar a classificação BlueXP .

Observe que todas as atividades de instalação são registradas ao instalar a classificação BlueXP . Se você encontrar algum problema durante a instalação, poderá visualizar o conteúdo do log de auditoria de instalação. Está escrito para `/opt/netapp/install_logs/`. "Veja mais detalhes aqui".

O que você vai precisar

- Verifique se o sistema Linux atende ao requisitos de host.
- Verifique se o sistema tem os dois pacotes de software pré-requisito instalados (Docker Engine ou Podman, e Python 3).
- Certifique-se de ter o root Privileges no sistema Linux.
- Se você estiver usando um proxy para acesso à 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 intercetação TLS, você precisará saber o caminho no sistema Linux de

classificação BlueXP onde os certificados de CA TLS são armazenados.

- O proxy deve ser não transparente - atualmente não oferecemos suporte a proxies transparentes.
- O utilizador tem de ser um utilizador local. Os usuários de domínio não são suportados.

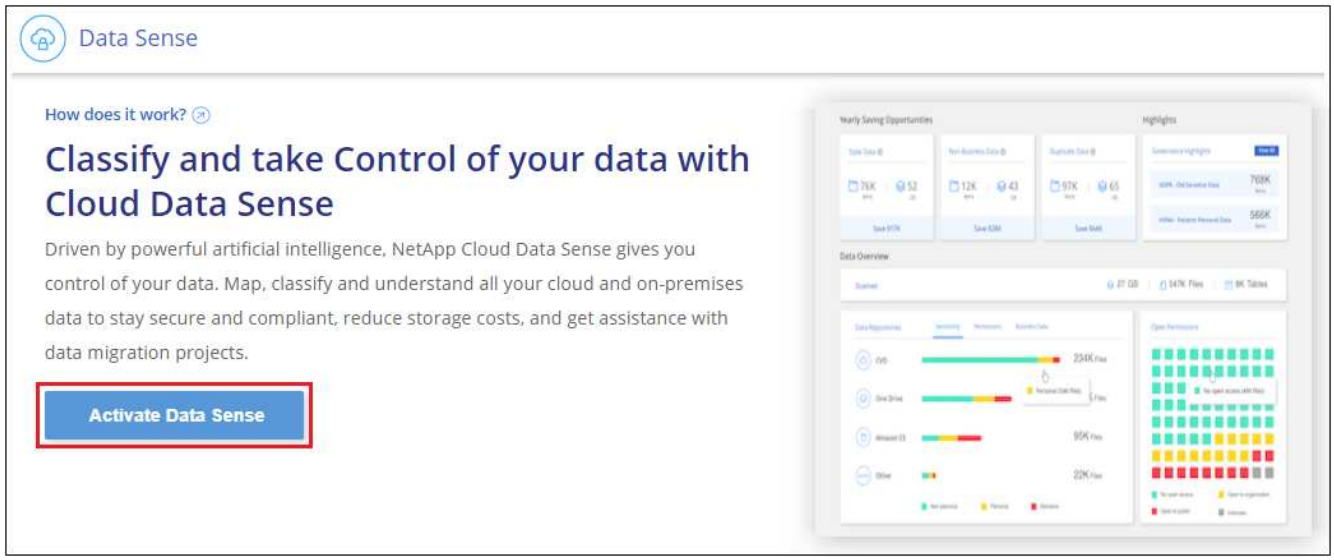
- Verifique se o ambiente off-line atende ao permissões e conetividadenecessário .

Passos

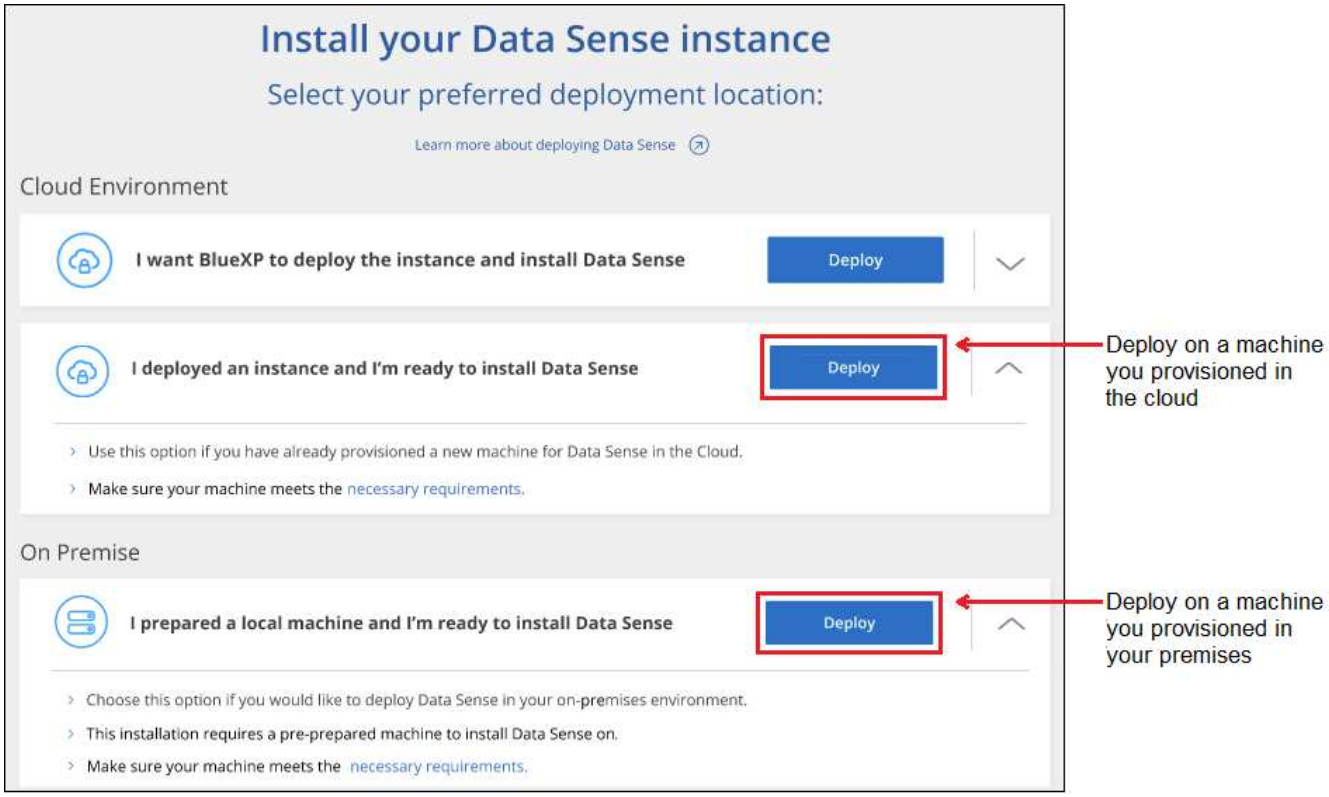
1. Transfira o software de classificação BlueXP a partir do "Site de suporte da NetApp". O arquivo que você deve selecionar é chamado **DATASENSE-installer-<version>.tar.gz**.
2. Copie o arquivo do instalador para o host Linux que você pretende usar (usando `scp` ou algum outro método).
3. Descompacte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

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

4. No BlueXP , selecione **Governança > classificação**.
5. Clique em **Activate Data Sense**.



6. Dependendo se você está instalando a classificação do BlueXP em uma instância preparada na nuvem ou em uma instância preparada em suas instalações, clique no botão **Deploy** apropriado para iniciar a instalação da classificação do BlueXP .



7. A caixa de diálogo *Deploy Data Sense on Premises* 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, clique em **Fechar** para ignorar a caixa de diálogo.
8. Na máquina host, digite 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 executa uma pré-verificação para garantir que seus requisitos de sistema e rede estejam em vigor para uma instalação bem-sucedida. "Assista a este vídeo" compreender as mensagens de pré-verificação e implicações.

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 no local), adicione `--manual-cloud-install <cloud_provider>`o . b. Insira o endereço IP ou o nome do host da máquina host de classificação BlueXP para que ele possa ser acessado pelo sistema de conetores. c. Insira o endereço IP ou o nome do host da máquina host do conetor BlueXP para que ele possa ser acessado pelo sistema de classificação BlueXP . d. Insira os detalhes do proxy conforme solicitado. Se o seu conetor BlueXP já usa um proxy, não há necessidade de inserir essas informações novamente aqui, já que a classificação BlueXP usará automaticamente o proxy usado pelo conetor.	Como alternativa, você pode criar todo o comando 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 do NetApp
- ID do cliente do conetor (adicione o sufixo "clients" ao ID do cliente se ele ainda não estiver lá)
- *User_token*: Token de acesso de usuário JWT
- *ds_host*: Endereço IP ou nome de host do sistema Linux de classificação BlueXP .
- *Cm_host*: Endereço IP ou nome de host do sistema do conetor BlueXP .
- *Cloud_provider*: Ao instalar em uma instância de nuvem, digite "AWS", "Azure" ou "GCP", dependendo do provedor de nuvem.
- *Proxy_host*: IP ou nome de host do servidor proxy se o host estiver atrás de um servidor proxy.
- *Proxy_port*: Porta para conetar ao servidor proxy (padrão 80).
- *Proxy_scheme*: Esquema de conexão: HTTPS ou http (http padrão).
- *Proxy_user*: Usuário autenticado para se conetar ao servidor proxy, se a autenticação básica for necessária. O usuário deve ser um usuário local - os usuários de domínio não são suportados.
- *Proxy_password*: Senha para o nome de usuário que você especificou.
- *CA_cert_dir*: Caminho na classificação do sistema Linux do BlueXP contendo pacotes adicionais de certificado de CA TLS. Somente necessário se o proxy estiver executando intercetação TLS.

Resultado

O instalador de classificação BlueXP instala pacotes, Registra a instalação e instala a classificação BlueXP . A instalação pode levar de 10 a 20 minutos.

Se houver conetividade pela porta 8080 entre a máquina host e a instância do conetor, você verá o progresso da instalação na guia classificação do BlueXP no BlueXP .

O que vem a seguir

Na página Configuração, pode selecionar as fontes de dados que pretende digitalizar.

Instale a classificação BlueXP em um host Linux sem acesso à Internet

Conclua algumas etapas para instalar a classificação BlueXP em um host Linux em um site local que não tenha acesso à Internet - também conhecido como *modo privado*. Esse tipo de instalação, que usa um script de instalação, não tem conetividade com a camada SaaS do BlueXP .

"Saiba mais sobre os diferentes modos de implantação para o conetor BlueXP e a classificação BlueXP ".

Observe que você também "Implante a classificação BlueXP em um site local que tenha acesso à Internet"pode .

O script de instalação da classificação BlueXP 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 de classificação do BlueXP , há um pacote de software separado que você pode baixar que apenas testa os pré-requisitos. "Veja como verificar se o seu host Linux está pronto para instalar a classificação BlueXP ".

Para versões antigas 1,30 e anteriores, se for necessário instalar a classificação BlueXP em vários hosts, "Instale a classificação BlueXP em vários hosts sem acesso à Internet"consulte .

Fontes de dados compatíveis

Quando instalado modo privado (às vezes chamado de site "off-line" ou "escuro"), a classificação BlueXP só pode digitalizar dados de fontes de dados que também são locais para o site local. Neste momento, a classificação BlueXP pode analisar as seguintes fontes de dados **locais**:

- Sistemas ONTAP no local
- Esquemas de banco de dados

Atualmente, não há suporte para a verificação de contas Cloud Volumes ONTAP, Azure NetApp Files ou FSX for ONTAP quando a classificação BlueXP é implantada no modo privado.

Limitações

A maioria dos recursos de classificação BlueXP funciona quando é implantado em um site sem acesso à Internet. No entanto, certos recursos que exigem acesso à Internet não são suportados, por exemplo:

- Definir funções do BlueXP para diferentes utilizadores (por exemplo, Administrador de contas ou Visualizador de conformidade)
- Copiar e sincronizar arquivos de origem usando cópia e sincronização do BlueXP
- Atualizações automatizadas de software da BlueXP

  Tanto o conetor BlueXP quanto a classificação BlueXP exigirão atualizações manuais periódicas para habilitar novos recursos. Você pode ver a versão de classificação do BlueXP na parte inferior das páginas da IU de classificação do BlueXP . Verifique o "Notas de lançamento da classificação BlueXP " para ver os

novos recursos em cada versão e se você deseja esses recursos. Em seguida, pode seguir os passos para "Atualize o conetor BlueXP " e Atualize seu software de classificação BlueXP .

Início rápido

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

Instale o conetor BlueXP

Se você ainda não tiver um conetor instalado no modo privado, "Implante o conetor" em um host Linux agora.

Rever pré-requisitos de classificação BlueXP

Verifique se o sistema Linux atende ao requisitos de host, se ele tem todo o software necessário instalado e se o ambiente off-line atende ao permissões e conetividadenecessário .

Baixe e implante a classificação BlueXP

Faça o download do software de classificação BlueXP do 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 do BlueXP .

Instale o conetor BlueXP

Se você ainda não tiver um conetor BlueXP instalado em modo privado, "Implante o conetor" em um host Linux em seu site offline.

Prepare o sistema host Linux

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

- A classificação BlueXP não é suportada em um host que é compartilhado com outros aplicativos - o host deve ser um host dedicado.
- Ao criar o sistema host em suas instalações, você pode escolher entre esses tamanhos de sistema, dependendo do tamanho do conjunto de dados que você planeja fazer a verificação de classificação do BlueXP .

Tamanho do sistema	CPU	RAM (a memória swap deve ser desativada)	Disco
* Extra grande *	32 CPUs	128 GB DE RAM	1 TIB SSD ON /, OR - 100 GiB disponível em /opt - 895 GiB disponível em /var/lib/docker - 5 GiB em /tmp

Tamanho do sistema	CPU	RAM (a memória swap deve ser desativada)	Disco
* Grande *	16 CPUs	64 GB DE RAM	500 GiB SSD ON /, OR - 100 GiB disponível em /opt - 395 GiB disponível em /var/lib/docker ou Podman /var/lib/containers ou Podman /var/lib/containers - 5 GiB em /tmp

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

Pasta	Permissões mínimas
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operacional**:
  - Os seguintes sistemas operacionais requerem o uso do mecanismo de contentor Docker:
    - Red Hat Enterprise Linux versão 7,8 e 7,9
    - Ubuntu 22,04 (requer classificação BlueXP versão 1,23 ou superior)
    - Ubuntu 24,04 (requer classificação BlueXP versão 1,23 ou superior)
  - Os seguintes sistemas operacionais requerem o uso do motor de contentores Podman, e eles exigem a classificação BlueXP versão 1,30 ou superior:
    - Red Hat Enterprise Linux versão 8,8, 9,0, 9,1, 9,2, 9,3, 9,4
- **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 necessário de 3rd partes durante a instalação.
- * Software adicional*: Você deve instalar o seguinte software no host antes de instalar a classificação BlueXP :
  - Dependendo do sistema operacional que você estiver usando, você precisará instalar um dos motores de contentor:
    - Docker Engine versão 19.3.1 ou superior. "Veja as 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. "Veja as instruções de instalação".
  - **Considerações de NTP**: A NetApp recomenda configurar o sistema de classificação BlueXP para usar um serviço de protocolo de tempo de rede (NTP). O tempo deve ser sincronizado entre o sistema de classificação BlueXP e o sistema de conetores BlueXP .
  - **Considerações sobre o Firewalld**: Se você estiver planejando usar `firewalld`, recomendamos que você a ative antes de instalar a classificação do BlueXP . Execute os seguintes comandos para configurar `firewalld` de modo que seja compatível com a classificação BlueXP :

    ```
    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
    ```

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

O endereço IP do sistema anfitrião de classificação BlueXP não pode ser alterado após a instalação.

Verifique os pré-requisitos de classificação BlueXP e BlueXP

Reveja os pré-requisitos a seguir para se certificar de que você tem uma configuração suportada antes de implantar a classificação do BlueXP .

- Verifique se o conetor tem permissões para implantar recursos e criar grupos de segurança para a instância de classificação do BlueXP . Você pode encontrar as permissões de BlueXP mais recentes no "As políticas fornecidas pela NetApp".
- Certifique-se de que você pode manter a classificação BlueXP em execução. A instância de classificação do BlueXP precisa permanecer ligada para verificar continuamente seus dados.
- Garanta a conetividade do navegador da Web com a classificação BlueXP . Depois que a classificação do BlueXP estiver ativada, certifique-se de que os usuários acessem a interface do BlueXP a partir de um host que tenha uma conexão com a instância de classificação do BlueXP .

  A instância de classificação do BlueXP usa um endereço IP privado para garantir que os dados indexados não sejam acessíveis a outros. Como resultado, o navegador da Web que você usa para acessar o BlueXP deve ter uma conexão com esse endereço IP privado. Essa conexão pode vir de um host que está dentro da mesma rede que a instância de classificação BlueXP .

Verifique se todas as portas necessárias estão ativadas

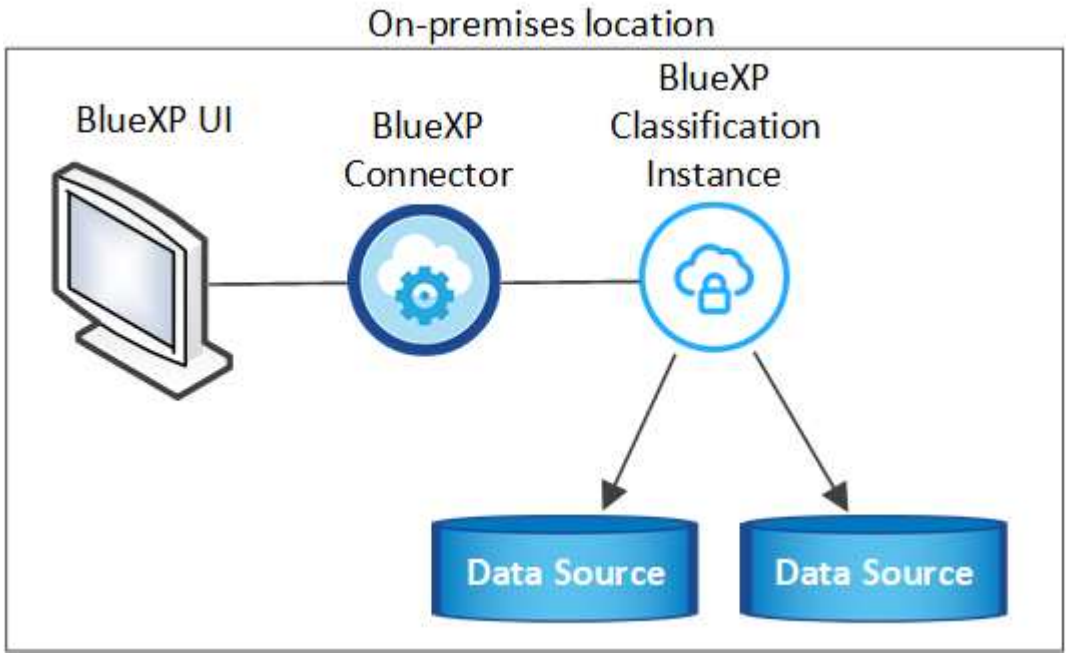
Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o conetor, a classificação do BlueXP , o ative Directory e suas fontes de dados.

Tipo de ligação	Portas	Descrição
Conetor >> classificação BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) E 80. 9000	O grupo de segurança do conetor deve permitir tráfego de entrada e saída através das portas 6000 e 443 de e para a instância de classificação BlueXP . • A porta 6000 é necessária para que a licença BYOL de classificação do BlueXP funcione em um local escuro. • A porta 8080 deve estar aberta para que você possa ver o progresso da instalação no BlueXP . • Se um firewall for usado no host Linux, a porta 9000 será necessária para processos internos dentro de um servidor Ubuntu.
Conetor do cluster do ONTAP (nas)	443 (TCP)	O BlueXP descobre clusters do ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, elas devem atender aos seguintes requisitos: • O host do conetor deve permitir o acesso HTTPS de saída através da porta 443. Se o conetor estiver na nuvem, toda a comunicação de saída é permitida pelo grupo de segurança predefinido. • O cluster ONTAP deve permitir acesso HTTPS de entrada através da porta 443. A política de firewall "mgmt" padrão permite o acesso HTTPS de entrada de todos os endereços IP. Se você modificou essa política padrão, ou se criou sua própria política de firewall, associe o protocolo HTTPS a essa política e habilite o acesso do host do conetor.
Classificação do BlueXP >> cluster ONTAP	• Para NFS - 111 (TCP/UDP) e 2049 (TCP/UDP) • Para CIFS - 139 (TCP/UDP) e 445 (TCP/UDP)	A classificação BlueXP precisa de uma conexão de rede para cada sub-rede Cloud Volumes ONTAP ou sistema ONTAP local. Os grupos de segurança para Cloud Volumes ONTAP devem permitir conexões de entrada da instância de classificação BlueXP . Certifique-se de que essas portas estejam abertas para a instância de classificação BlueXP : • Para NFS - 111 e 2049 • Para CIFS - 139 e 445 As políticas de exportação de volume NFS devem permitir o acesso a partir da instância de classificação BlueXP .

Tipo de ligação	Portas	Descrição
Classificação do BlueXP >> ative Directory	389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)	Você deve ter um ative Directory já configurado para os usuários em sua empresa. Além disso, a classificação do BlueXP precisa de credenciais do ative Directory para verificar volumes CIFS. Você deve ter as informações do ative Directory: • Endereço IP do servidor DNS ou vários endereços IP • Nome de usuário e senha para o servidor • Nome de domínio (Nome do ative Directory) • Quer esteja a utilizar LDAP seguro (LDAPS) ou não • Porta de servidor LDAP (normalmente 389 para LDAP e 636 para LDAP seguro)
Se um firewall for usado no host Linux	9000	Necessário para processos internos dentro de um servidor Ubuntu.

Instale a classificação BlueXP no host Linux local

Para configurações típicas, você instalará o software em um único sistema host.



Instalação de um único host para configurações típicas

Siga estas etapas ao instalar o software de classificação BlueXP em um único host local em um ambiente off-line.

Observe que todas as atividades de instalação são registradas ao instalar a classificação BlueXP . Se você encontrar algum problema durante a instalação, poderá visualizar o conteúdo do log de auditoria de

instalação. Está escrito para `/opt/netapp/install_logs/`. "Veja mais detalhes aqui".

O que você vai precisar

- Verifique se o sistema Linux atende ao requisitos de host.
- Verifique se você instalou os dois pacotes de software pré-requisito (Docker Engine ou Podman, e Python 3).
- Certifique-se de ter o root Privileges no sistema Linux.
- Verifique se o ambiente off-line atende ao permissões e conetividadenecessário .

Passos

1. Num sistema configurado pela Internet, transfira o software de classificação BlueXP a partir do "Site de suporte da NetApp". O arquivo que você deve selecionar é chamado **DataSense-offline-bundle-<version>.tar.gz**.
2. Copie o pacote de instalação para o host Linux que você pretende usar no modo privado.
3. Descompacte o pacote de instalação na máquina host, por exemplo:

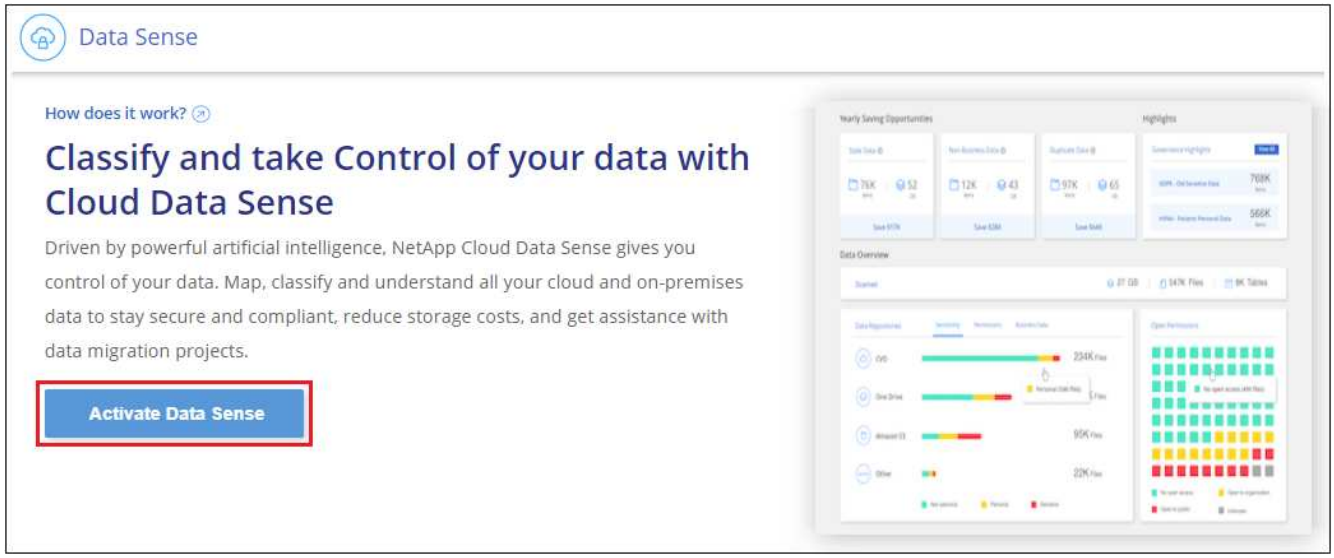
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   Isso extrai o software necessário e o arquivo de instalação real **cc_onprem_installer.tar.gz**.

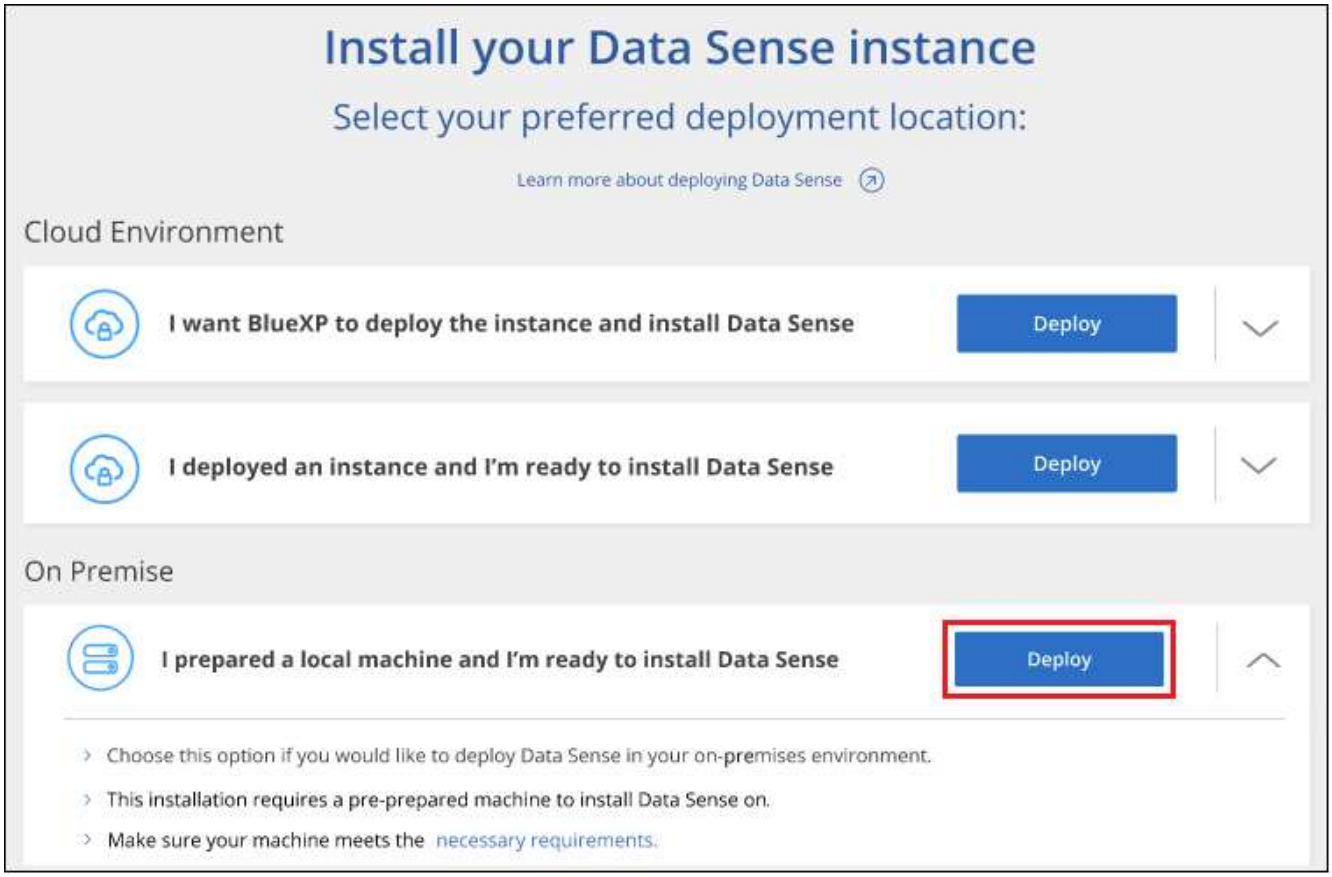
4. Descompacte o arquivo de instalação na máquina host, por exemplo:

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

5. Inicie o BlueXP e selecione **Governança > classificação**.
6. Clique em **Activate Data Sense**.



7. Clique em **Deploy** para iniciar a instalação no local.



8. A caixa de diálogo *Deploy Data Sense on Premises* é exibida. Copie o comando fornecido (por exemplo: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) E cole-o em um arquivo de texto para que você possa usá-lo mais tarde. Em seguida, clique em **Fechar** para ignorar a caixa de diálogo.
9. Na máquina host, digite 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 executa uma pré-verificação para garantir que seus requisitos de sistema e rede estejam em vigor para uma instalação bem-sucedida.

Insira os parâmetros conforme solicitado:	Digite o comando completo:
a. Cole as informações que você copiou da etapa 8: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. Insira o endereço IP ou o nome do host da máquina host de classificação BlueXP para que ele possa ser acessado pelo sistema de conetores. c. Insira o endereço IP ou o nome do host da máquina host do conetor BlueXP para que ele possa ser acessado pelo sistema de classificação BlueXP .	Alternativamente, você pode criar todo o comando com antecedência, fornecendo os parâmetros de host necessários: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

Valores variáveis:

- *Account_id* - ID da conta do NetApp
- ID do cliente do conetor (adicione o sufixo "clients" ao ID do cliente se ele ainda não estiver lá)
- *User_token*: Token de acesso de usuário JWT
- *ds_host*: Endereço IP ou nome de host do sistema de classificação BlueXP .
- *Cm_host*: Endereço IP ou nome de host do sistema do conetor BlueXP .

Resultado

O instalador de classificação BlueXP instala pacotes, Registra a instalação e instala a classificação BlueXP . A instalação pode levar de 10 a 20 minutos.

Se houver conetividade pela porta 8080 entre a máquina host e a instância do conetor, você verá o progresso da instalação na guia classificação do BlueXP no BlueXP .

O que vem a seguir

Na página Configuração, pode selecionar o local "Clusters ONTAP no local" e "bancos de dados" que pretende digitalizar.

Atualizar o software de classificação BlueXP

Uma vez que o software de classificação BlueXP é atualizado com novos recursos regularmente, você deve entrar em uma rotina para verificar se há novas versões periodicamente para se certificar de que você está usando o software e os recursos mais recentes. Você precisará atualizar o software de classificação BlueXP manualmente porque não há conetividade à Internet para realizar a atualização automaticamente.

Antes de começar

- Recomendamos que o software BlueXP Connector seja atualizado para a versão mais recente disponível. "Consulte os passos de atualização do conetor".
- A partir da classificação BlueXP versão 1,24, você pode realizar atualizações para qualquer versão futura do software.

  Se o seu software de classificação BlueXP estiver executando uma versão anterior a 1,24, você poderá atualizar apenas uma versão principal de cada vez. Por exemplo, se você tiver a versão 1,21.x instalada, você pode atualizar apenas para 1,22.x. Se você está algumas versões principais atrás, você precisará atualizar o software várias vezes.

Passos

1. Num sistema configurado pela Internet, transfira o software de classificação BlueXP a partir do "Site de suporte da NetApp". O arquivo que você deve selecionar é chamado **DataSense-offline-bundle-<version>.tar.gz**.
2. Copie o pacote de software para o host Linux onde a classificação BlueXP está instalada no site escuro.
3. Descompacte o pacote de software na máquina host, por exemplo:

   ```
   tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   Isso extrai o arquivo de instalação **cc_onprem_installer.tar.gz**.

4. Descompacte o arquivo de instalação na máquina host, por exemplo:

```
tar -xzf cc_onprem_installer.tar.gz
```

Isso extrai o script de atualização **start_darksite_upgrade.sh** e qualquer software de terceiros necessário.

5. Execute o script de atualização na máquina host, por exemplo:

```
start_darksite_upgrade.sh
```

Resultado

O software de classificação BlueXP é atualizado em seu host. A atualização pode levar de 5 a 10 minutos.

Você pode verificar se o software foi atualizado verificando a versão na parte inferior das páginas da IU de classificação do BlueXP .

Verifique se o seu host Linux está pronto para instalar a classificação BlueXP

Antes de instalar a classificação BlueXP manualmente em um host Linux, você pode executar um script no host para verificar se todos os pré-requisitos estão em vigor para instalar a classificação BlueXP . Você pode executar esse script em um host Linux em sua rede ou em um host Linux na nuvem. O host pode ser conetado à internet, ou o host pode residir em um site que não tem acesso à internet (um *site escuro*).

Há também um script de teste pré-requisito que faz parte do script de instalação de classificação BlueXP . O script descrito aqui é projetado especificamente para usuários que desejam verificar o host Linux independentemente de executar o script de instalação de classificação BlueXP .

Como começar

Você executará as seguintes tarefas.

1. Opcionalmente, instale um conetor BlueXP se você ainda não tiver um instalado. Você pode executar o script de teste sem ter um conetor instalado, mas o script verifica a conetividade entre o conetor e a máquina host de classificação BlueXP - por isso, é recomendável que você tenha um conetor.
2. Prepare a máquina host e verifique se ela atende a todos os requisitos.
3. Ative o acesso de saída à Internet a partir da máquina host de classificação BlueXP .
4. Verifique se todas as portas necessárias estão ativadas em todos os sistemas.
5. Baixe e execute o script de teste pré-requisito.

Crie um conetor

É necessário um conetor BlueXP antes de poder instalar e utilizar a classificação BlueXP . Você pode, no entanto, executar o script pré-requisitos sem um conetor.

Você pode "Instale o conetor no local" em um host Linux em sua rede ou em um host Linux na nuvem. Alguns

usuários que planejam instalar a classificação do BlueXP no local também podem optar por instalar o conetor no local.

Para criar um conetor no ambiente do provedor de nuvem, consulte "Criando um conetor na AWS" "Criando um conetor no Azure" , "Criando um conetor no GCP" ou .

Você precisará do endereço IP ou do nome do host do sistema do conetor ao executar o script de pré-requisitos. Você terá esta informação se você instalou o conetor em suas instalações. Se o conetor for implantado na nuvem, você poderá encontrar essas informações no console do BlueXP : Clique no ícone Ajuda, selecione **suporte** e clique em **conetor BlueXP** .

Verifique os requisitos do host

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

- A classificação BlueXP não é suportada em um host que é compartilhado com outros aplicativos - o host deve ser um host dedicado.
- Ao criar o sistema host em suas instalações, você pode escolher entre esses tamanhos de sistema, dependendo do tamanho do conjunto de dados que você planeja fazer a verificação de classificação do BlueXP .

Tamanho do sistema	CPU	RAM (a memória swap deve ser desativada)	Disco
* Extra grande *	32 CPUs	128 GB DE RAM	1 TIB SSD ON /, OR - 100 GiB disponível em /opt - 895 GiB disponível em /var/lib/docker - 5 GiB em /tmp
* Grande *	16 CPUs	64 GB DE RAM	500 GiB SSD ON /, OR - 100 GiB disponível em /opt - 395 GiB disponível em /var/lib/docker ou Podman /var/lib/containers ou Podman /var/lib/containers - 5 GiB em /tmp

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

Pasta	Permissões mínimas
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`

Pasta	Permissões mínimas
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operacional**:
  - Os seguintes sistemas operacionais requerem o uso do mecanismo de contentor Docker:
    - Red Hat Enterprise Linux versão 7,8 e 7,9
    - Ubuntu 22,04 (requer classificação BlueXP versão 1,23 ou superior)
    - Ubuntu 24,04 (requer classificação BlueXP versão 1,23 ou superior)
  - Os seguintes sistemas operacionais requerem o uso do motor de contentores Podman, e eles exigem a classificação BlueXP versão 1,30 ou superior:
    - Red Hat Enterprise Linux versão 8,8, 9,0, 9,1, 9,2, 9,3, 9,4
- **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 necessário de 3rd partes durante a instalação.
- * Software adicional*: Você deve instalar o seguinte software no host antes de instalar a classificação BlueXP :
  - Dependendo do sistema operacional que você estiver usando, você precisará instalar um dos motores de contentor:
    - Docker Engine versão 19.3.1 ou superior. "Veja as 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. "Veja as instruções de instalação".
  - **Considerações de NTP**: A NetApp recomenda configurar o sistema de classificação BlueXP para usar um serviço de protocolo de tempo de rede (NTP). O tempo deve ser sincronizado entre o sistema de classificação BlueXP e o sistema de conetores BlueXP .
  - **Considerações sobre o Firewalld**: Se você estiver planejando usar `firewalld`, recomendamos que você a ative antes de instalar a classificação do BlueXP . Execute os seguintes comandos para configurar `firewalld` de modo que seja compatível com a classificação BlueXP :

```
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 BlueXP adicionais como nós de scanner (em um modelo distribuído), adicione essas regras ao seu sistema principal 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 ativar ou atualizar `firewalld` as configurações.

Ative o acesso de saída à Internet a partir da classificação BlueXP

A classificação BlueXP requer acesso de saída à Internet. Se a sua rede virtual ou física utilizar um servidor proxy para acesso à Internet, certifique-se de que a instância de classificação do BlueXP tem acesso de saída à Internet para contactar os seguintes endpoints.

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

Endpoints	Finalidade
https://api.BlueXP .NetApp.com	Comunicação com o serviço BlueXP , que inclui contas NetApp.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o site BlueXP para autenticação centralizada de usuários.
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 pré-requisitos para instalação do docker.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fornece pacotes pré-requisitos para instalação do Ubuntu.

Verifique se todas as portas necessárias estão ativadas

Você deve garantir que todas as portas necessárias estejam abertas para comunicação entre o conetor, a classificação do BlueXP , o ative Directory e suas fontes de dados.

Tipo de ligação	Portas	Descrição
Conetor >> classificação BlueXP	8080 (TCP), 443 (TCP) e 80. 9000	O firewall ou as regras de roteamento para o conetor devem permitir o tráfego de entrada e saída pela porta 443 de e para a instância de classificação BlueXP . Certifique-se de que a porta 8080 esteja aberta para que você possa ver o progresso da instalação no BlueXP . Se um firewall for usado no host Linux, a porta 9000 será necessária para processos internos dentro de um servidor Ubuntu.
Conetor do cluster do ONTAP (nas)	443 (TCP)	O BlueXP descobre clusters do ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, o host do conetor deve permitir o acesso HTTPS de saída através da porta 443. Se o conetor estiver na nuvem, toda a comunicação de saída é permitida pelo firewall predefinido ou pelas regras de roteamento.

Execute o script de pré-requisitos de classificação do BlueXP

Siga estas etapas para executar o script de pré-requisitos de classificação do BlueXP .

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

O que você vai precisar

- Verifique se o sistema Linux atende ao requisitos de host.
- Verifique se o sistema tem os dois pacotes de software pré-requisito instalados (Docker Engine ou Podman, e Python 3).
- Certifique-se de ter o root Privileges no sistema Linux.

Passos

1. Faça download do script de pré-requisitos de classificação do BlueXP no "Site de suporte da NetApp". O arquivo que você deve selecionar é chamado **standalone-pre-required-tester-<version>**.
2. Copie o arquivo para o host Linux que você pretende 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 você estiver executando o script em um host que não tem acesso à Internet. Certos testes pré-requisitos são ignorados quando o host não está conetado à internet.

5. O script solicita o endereço IP da máquina host de classificação BlueXP .

- Introduza o endereço IP ou o nome do anfitrião.

6. O script solicita se você tem um conetor BlueXP instalado.
   - Introduza **N** se não tiver um conetor instalado.
   - Introduza **Y** se tiver um conetor instalado. E, em seguida, insira o endereço IP ou o nome do host do conetor BlueXP para que o script de teste possa testar essa conetividade.
7. O script executa uma variedade de testes no sistema e exibe resultados à medida que avança. Quando ele 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 pré-requisitos forem executados com sucesso, você poderá instalar a classificação BlueXP no host quando estiver pronto.

Se algum problema foi descoberto, eles são categorizados como "recomendado" ou "obrigatório" para ser corrigido. Os problemas recomendados são tipicamente itens que fariam as tarefas de digitalização e categorização de classificação do BlueXP serem executadas mais lentamente. Esses itens não precisam ser corrigidos - mas você pode querer abordá-los.

Se você tiver algum problema "necessário", você deve corrigir os problemas e executar o script de teste pré-requisitos novamente.

Ative a digitalização nas suas fontes de dados

Digitalize volumes Azure NetApp Files com a classificação BlueXP

Complete alguns passos para começar a usar a classificação BlueXP para Azure NetApp Files.

Início rápido

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

Descubra os sistemas Azure NetApp Files que pretende digitalizar

Antes de poder digitalizar volumes Azure NetApp Files, "O BlueXP deve ser configurado para descobrir a configuração".

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP no BlueXP " se ainda não houver uma instância implantada.

Ative a classificação BlueXP e selecione os volumes a digitalizar

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

4 Garanta o acesso aos volumes

Agora que a classificação BlueXP está ativada, certifique-se de que ela pode acessar todos os volumes.

- A instância de classificação BlueXP precisa de uma conexão de rede para cada sub-rede Azure NetApp Files.
- Certifique-se de que essas portas estejam abertas para a instância de classificação BlueXP :
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.
- As políticas de exportação de volume NFS devem permitir o acesso a partir da instância de classificação BlueXP .
- A classificação do BlueXP precisa de credenciais do ative Directory para analisar volumes CIFS.

  Clique em **Compliance** > **Configuration** > **Edit CIFS Credentials** e forneça as credenciais.

5 Gerencie os volumes que deseja digitalizar

Selecione ou anule a seleção dos volumes que pretende digitalizar e a classificação BlueXP iniciará ou deixará de os digitalizar.

Descubra o sistema Azure NetApp Files que pretende digitalizar

Se o sistema Azure NetApp Files que você deseja digitalizar ainda não estiver no BlueXP como um ambiente de trabalho, você pode adicioná-lo à tela neste momento.

"Veja como descobrir o sistema Azure NetApp Files no BlueXP ".

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

A classificação do BlueXP deve ser implantada na nuvem ao digitalizar volumes do Azure NetApp Files e deve ser implantada na mesma região que os volumes que deseja verificar.

Observação: a implantação da classificação do BlueXP em um local local local não é suportada atualmente ao digitalizar volumes do Azure NetApp Files.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Ative a classificação BlueXP nos seus ambientes de trabalho

Você pode ativar a classificação BlueXP no Azure NetApp Files volumes.

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.

2. Selecione como pretende digitalizar os volumes em cada ambiente de trabalho. "Saiba mais sobre o mapeamento e a classificação de exames":
   - Para mapear todos os volumes, clique em **Mapear todos os volumes**.
   - Para mapear e classificar todos os volumes, clique em **Map & Classify All volumes**.
   - Para personalizar a digitalização para cada volume, clique em **ou selecione o tipo de digitalização para cada volume** e, em seguida, escolha os volumes que pretende mapear e/ou classificar.

     Ative e desative verificações de conformidade em volumesConsulte para obter detalhes.

3. Na caixa de diálogo de confirmação, clique em **Approve** para que a classificação BlueXP comece a digitalizar seus volumes.

Resultado

A classificação BlueXP inicia a digitalização dos volumes selecionados no ambiente de trabalho. Os resultados estarão disponíveis no painel de conformidade assim que a classificação BlueXP terminar as verificações iniciais. O tempo que leva depende da quantidade de dados - pode ser de alguns minutos ou horas.

- Por padrão, se a classificação do BlueXP 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 do BlueXP não pode reverter o "último tempo de acesso" para o carimbo de data/hora original. Se não se importar se a última hora de acesso for redefinida, clique em **ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode habilitar para que a classificação BlueXP digitalize os volumes independentemente das permissões.
- A classificação BlueXP verifica apenas um compartilhamento de arquivo sob um volume. Se você tiver vários compartilhamentos em seus volumes, precisará analisar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Veja mais detalhes sobre esta limitação de classificação BlueXP ".

Verifique se a classificação BlueXP tem acesso a volumes

Certifique-se de que a classificação do BlueXP possa acessar volumes verificando suas políticas de rede, grupos de segurança e exportação. Você precisará fornecer a classificação BlueXP com credenciais CIFS para que possa acessar volumes CIFS.

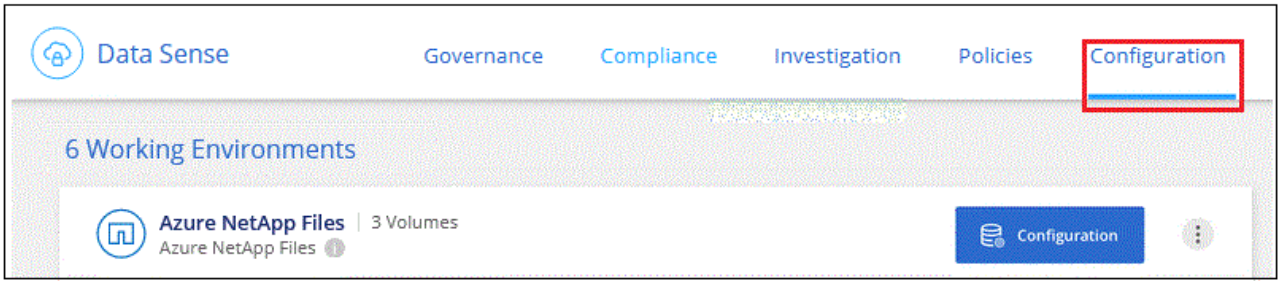
Passos

1. Verifique se há uma conexão de rede entre a instância de classificação BlueXP e cada rede que inclua volumes para Azure NetApp Files.

Para o Azure NetApp Files, a classificação BlueXP só pode digitalizar volumes que estejam na mesma região que o BlueXP .

2. Certifique-se de que as seguintes portas estejam abertas para a instância de classificação BlueXP :
   - Para NFS – portas 111 e 2049.
   - Para CIFS – portas 139 e 445.
3. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de classificação BlueXP para que ela possa acessar os dados em cada volume.
4. Se você usar o CIFS, forneça a classificação do BlueXP com credenciais do ative Directory para que ele possa analisar volumes CIFS.

   a. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.

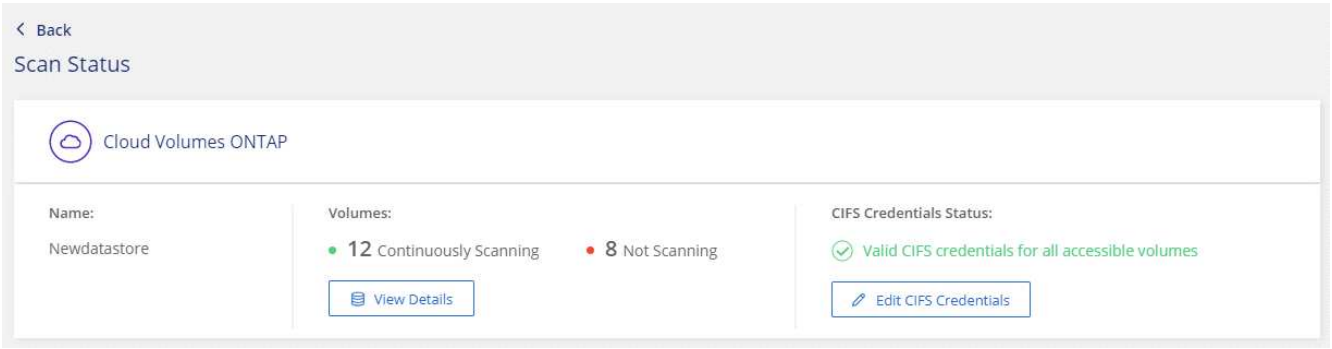


   b. Para cada ambiente de trabalho, clique em **Editar credenciais CIFS** e introduza o nome de utilizador e a palavra-passe de que a classificação BlueXP necessita para aceder aos volumes CIFS no sistema.

      As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a classificação do BlueXP possa ler qualquer dado que exija permissões elevadas. As credenciais são armazenadas na instância de classificação do BlueXP .

      Se você quiser garantir que seus arquivos "últimos tempos acessados" sejam inalterados pelas verificações de classificação do BlueXP , recomendamos que o usuário tenha permissões de atributos de gravação em CIFS ou permissões de gravação em NFS. Se possível, recomendamos tornar o usuário configurado do ative Directory parte de um grupo pai na organização que tem permissões para todos os arquivos.

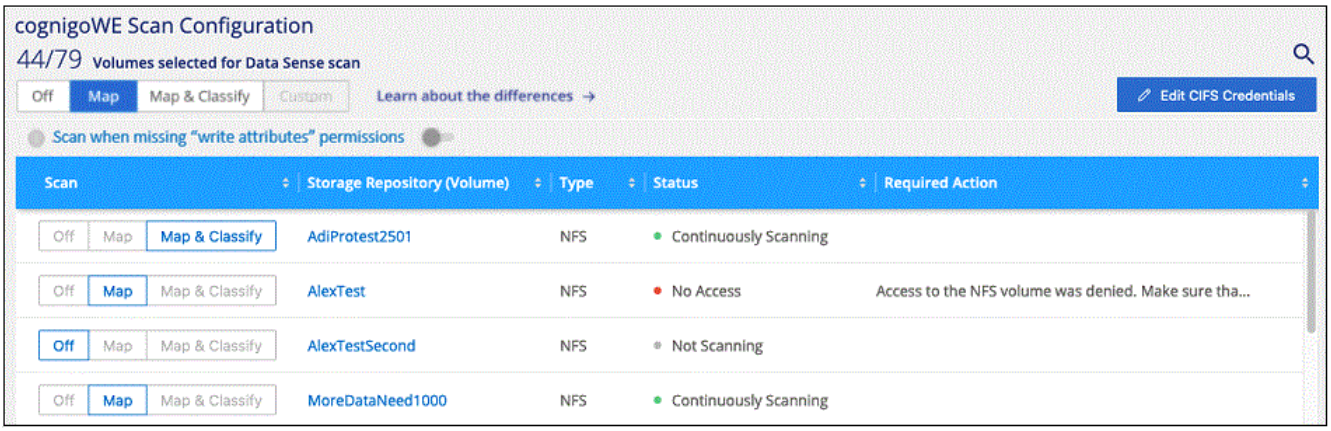
      Depois de inserir as credenciais, você verá uma mensagem informando que todos os volumes CIFS foram autenticados com êxito.



5. Na página *Configuration*, clique em **View Details** (Ver detalhes) para rever o status de cada volume CIFS

e NFS e corrigir quaisquer erros.

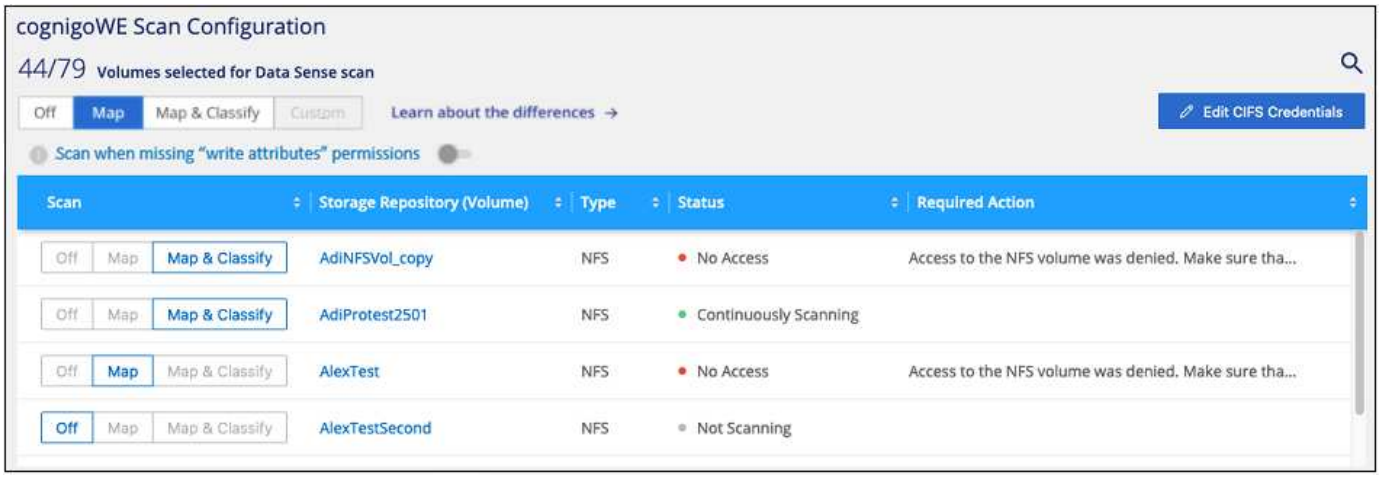
Por exemplo, a imagem a seguir mostra quatro volumes; um dos quais a classificação BlueXP não pode digitalizar devido a problemas de conetividade de rede entre a instância de classificação BlueXP e o volume.



Ative e desative verificações de conformidade em volumes

Pode iniciar ou parar exames apenas de mapeamento ou exames de mapeamento e classificação num ambiente de trabalho a qualquer momento a partir da página Configuração. Você também pode mudar de digitalizações somente de mapeamento para digitalizações de mapeamento e classificação, e vice-versa. Recomendamos que você digitalize todos os volumes.

A opção na parte superior da página para **Scan when missing "write attributes" permissions** está desativada por padrão. Isso significa que se a classificação BlueXP não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a classificação BlueXP não poderá reverter o "último tempo de acesso" para o carimbo de data/hora original. Se você não se importa se a última hora de acesso é redefinida, LIGUE o interrutor e todos os arquivos serão digitalizados independentemente das permissões. "Saiba mais".



Para:	Faça isso:
Ative digitalizações apenas de mapeamento num volume	Na área de volume, clique em **Map**
Ative a digitalização completa num volume	Na área de volume, clique em **Map & Classify**

Para:	Faça isso:
Desativar a digitalização num volume	Na área de volume, clique em **Off**
Ative digitalizações apenas de mapeamento em todos os volumes	Na área de cabeçalho, clique em **Map**
Ative a digitalização completa em todos os volumes	Na área de cabeçalho, clique em **Map & Classify**
Desative a digitalização em todos os volumes	Na área de cabeçalho, clique em **Off**

Os novos volumes adicionados ao ambiente de trabalho são automaticamente digitalizados apenas quando você definir a configuração **Map** ou **Map & Classify** na área de cabeçalho. Quando definido como **Custom** ou **Off** na área de cabeçalho, você precisará ativar o mapeamento e/ou a digitalização completa em cada novo volume adicionado no ambiente de trabalho.

Verifique o Amazon FSX para volumes ONTAP com a classificação BlueXP

Conclua algumas etapas para começar a digitalizar o volume do Amazon FSX for ONTAP com a classificação BlueXP .

Antes de começar

- Você precisa de um conetor ativo na AWS para implantar e gerenciar a classificação do BlueXP .
- O grupo de segurança selecionado ao criar o ambiente de trabalho deve permitir o tráfego da instância de classificação do BlueXP . Você pode encontrar o grupo de segurança associado usando o ENI conetado ao sistema de arquivos FSX for ONTAP e editá-lo usando o Console de Gerenciamento da AWS.

  "Grupos de segurança da AWS para instâncias Linux"

  "Grupos de segurança da AWS para instâncias do Windows"

  "Interfaces de rede AWS Elastic (ENI)"

Início rápido

Comece rapidamente seguindo estes passos ou role para baixo para obter detalhes completos.

1 Descubra os sistemas de arquivos FSX for ONTAP que você deseja digitalizar

Antes de poder digitalizar o FSX para ONTAP volumes "Você deve ter um ambiente de trabalho do FSX com volumes configurados", .

2 Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP no BlueXP " se ainda não houver uma instância implantada.

3 Ative a classificação BlueXP e selecione os volumes a digitalizar

Selecione a guia **Configuração** e ative as verificações de conformidade para volumes em ambientes de trabalho específicos.

4 Garanta o acesso aos volumes

Agora que a classificação BlueXP está ativada, certifique-se de que ela pode acessar todos os volumes.

- A instância de classificação do BlueXP precisa de uma conexão de rede para cada sub-rede do FSX for ONTAP.
- Certifique-se de que as seguintes portas estejam abertas para a instância de classificação BlueXP :
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.
- As políticas de exportação de volume NFS devem permitir o acesso a partir da instância de classificação BlueXP .
- A classificação do BlueXP precisa de credenciais do ative Directory para analisar volumes CIFS. Clique em **Compliance** > **Configuration** > **Edit CIFS Credentials** e forneça as credenciais.

5 Gerencie os volumes que deseja digitalizar

Selecione ou anule a seleção dos volumes que pretende digitalizar e a classificação BlueXP inicia ou pára de os digitalizar.

Descubra o sistema de arquivos FSX for ONTAP que você deseja digitalizar

Se o sistema de arquivos FSX for ONTAP que você deseja digitalizar ainda não está no BlueXP como um ambiente de trabalho, você pode adicioná-lo à tela neste momento.

"Veja como descobrir ou criar o sistema de arquivos FSX for ONTAP no BlueXP ".

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

Você deve implantar a classificação do BlueXP na mesma rede da AWS que o conetor para AWS e os volumes do FSX que deseja analisar.

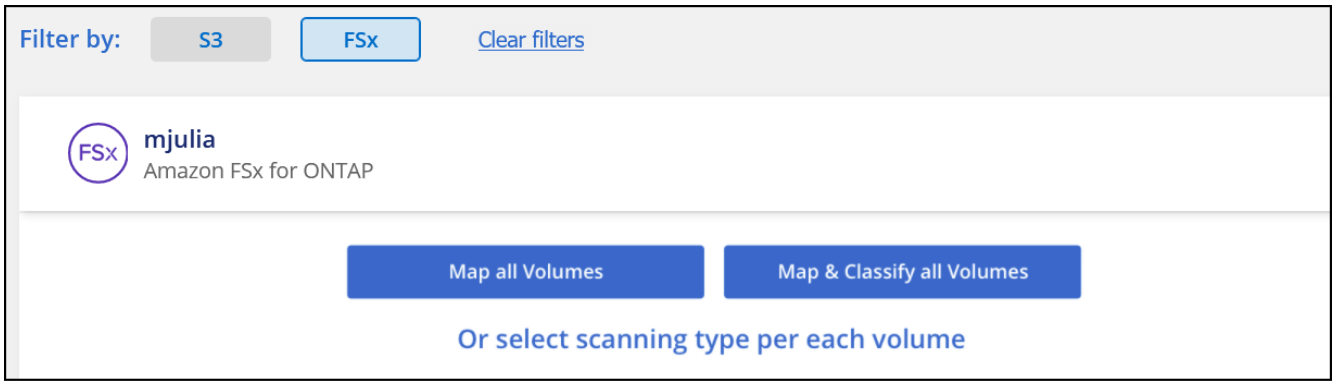
Observação: a implantação da classificação do BlueXP em um local local local não é suportada atualmente ao digitalizar volumes FSX.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Ative a classificação BlueXP nos seus ambientes de trabalho

Você pode ativar a classificação do BlueXP para o FSX for ONTAP volumes.

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.



2. Selecione como pretende digitalizar os volumes em cada ambiente de trabalho. "Saiba mais sobre o mapeamento e a classificação de exames":
   - Para mapear todos os volumes, clique em **Mapear todos os volumes**.
   - Para mapear e classificar todos os volumes, clique em **Map & Classify All volumes**.
   - Para personalizar a digitalização para cada volume, clique em **ou selecione o tipo de digitalização para cada volume** e, em seguida, escolha os volumes que pretende mapear e/ou classificar.

     Consulte Ativar e desativar verificações de conformidade em volumes para obter detalhes.
3. Na caixa de diálogo de confirmação, clique em **Approve** para que a classificação BlueXP comece a digitalizar seus volumes.

Resultado

A classificação BlueXP inicia a digitalização dos volumes selecionados no ambiente de trabalho. Os resultados estarão disponíveis no painel de conformidade assim que a classificação BlueXP terminar as verificações iniciais. O tempo que leva depende da quantidade de dados - pode ser de alguns minutos ou horas.

- Por padrão, se a classificação do BlueXP 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 do BlueXP não pode reverter o "último tempo de acesso" para o carimbo de data/hora original. Se não se importar se a última hora de acesso for redefinida, clique em **ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode habilitar para que a classificação BlueXP digitalize os volumes independentemente das permissões.
- A classificação BlueXP verifica apenas um compartilhamento de arquivo sob um volume. Se você tiver vários compartilhamentos em seus volumes, precisará analisar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Veja mais detalhes sobre esta limitação de classificação BlueXP ".

Verifique se a classificação BlueXP tem acesso a volumes

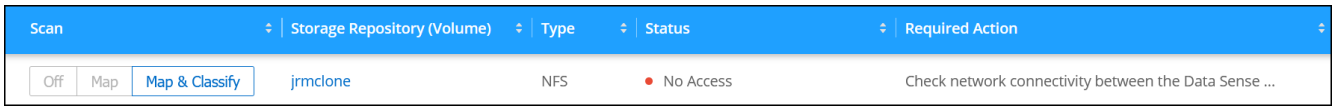
Verifique se a classificação do BlueXP pode acessar volumes verificando suas políticas de rede, grupos de segurança e exportação.

Você precisará fornecer a classificação BlueXP com credenciais CIFS para que possa acessar volumes CIFS.

Passos

1. Na página *Configuration*, clique em **View Details** (Ver detalhes) para rever o estado e corrigir quaisquer erros.

Por exemplo, a imagem a seguir mostra uma classificação de volume BlueXP não pode ser verificada devido a problemas de conetividade de rede entre a instância de classificação BlueXP e o volume.



2. Verifique se há uma conexão de rede entre a instância de classificação do BlueXP e cada rede que inclua volumes para o FSX for ONTAP.

   Para o FSX for ONTAP, a classificação BlueXP pode digitalizar volumes apenas na mesma região que o BlueXP .

3. Certifique-se de que as portas a seguir estejam abertas para a instância de classificação BlueXP .
   - Para NFS – portas 111 e 2049.
   - Para CIFS – portas 139 e 445.
4. Garanta que as políticas de exportação de volume NFS incluam o endereço IP da instância de classificação BlueXP para que ela possa acessar os dados em cada volume.
5. Se você usar o CIFS, forneça a classificação do BlueXP com credenciais do ative Directory para que ele possa analisar volumes CIFS.

   a. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.
   b. Para cada ambiente de trabalho, clique em **Editar credenciais CIFS** e introduza o nome de utilizador e a palavra-passe de que a classificação BlueXP necessita para aceder aos volumes CIFS no sistema.

      As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a classificação do BlueXP possa ler qualquer dado que exija permissões elevadas. As credenciais são armazenadas na instância de classificação do BlueXP .

      Se você quiser garantir que seus arquivos "últimos tempos acessados" sejam inalterados pelas verificações de classificação do BlueXP , recomendamos que o usuário tenha permissões de atributos de gravação em CIFS ou permissões de gravação em NFS. Se possível, recomendamos tornar o usuário configurado do ative Directory parte de um grupo pai na organização que tem permissões para todos os arquivos.

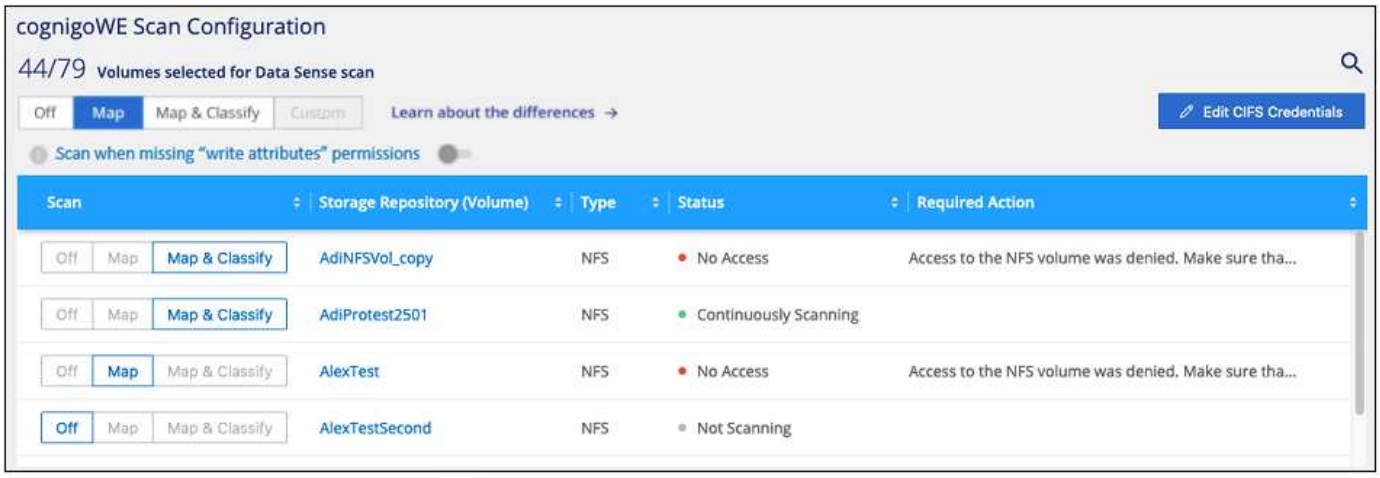
   Depois de inserir as credenciais, você verá uma mensagem informando que todos os volumes CIFS foram autenticados com êxito.

Ative e desative verificações de conformidade em volumes

Pode iniciar ou parar exames apenas de mapeamento ou exames de mapeamento e classificação num ambiente de trabalho a qualquer momento a partir da página Configuração. Você também pode mudar de digitalizações somente de mapeamento para digitalizações de mapeamento e classificação, e vice-versa. Recomendamos que você digitalize todos os volumes.

A opção na parte superior da página para **Scan when missing "write attributes" permissions** está desativada por padrão. Isso significa que se a classificação BlueXP não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a classificação BlueXP não poderá reverter o "último tempo de acesso" para o carimbo de data/hora original. Se

você não se importa se a última hora de acesso é redefinida, LIGUE o interrutor e todos os arquivos serão digitalizados independentemente das permissões. "Saiba mais".



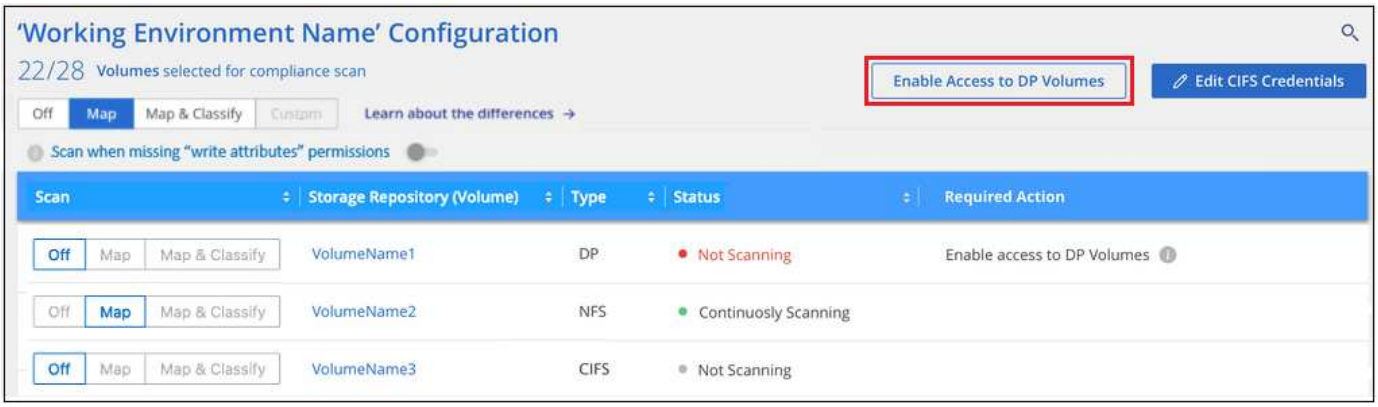
Para:	Faça isso:
Ative digitalizações apenas de mapeamento num volume	Na área de volume, clique em **Map**
Ative a digitalização completa num volume	Na área de volume, clique em **Map & Classify**
Desativar a digitalização num volume	Na área de volume, clique em **Off**
Ative digitalizações apenas de mapeamento em todos os volumes	Na área de cabeçalho, clique em **Map**
Ative a digitalização completa em todos os volumes	Na área de cabeçalho, clique em **Map & Classify**
Desative a digitalização em todos os volumes	Na área de cabeçalho, clique em **Off**

Os novos volumes adicionados ao ambiente de trabalho são automaticamente digitalizados apenas quando você definir a configuração **Map** ou **Map & Classify** na área de cabeçalho. Quando definido como **Custom** ou **Off** na área de cabeçalho, você precisará ativar o mapeamento e/ou a digitalização completa em cada novo volume adicionado no ambiente de trabalho.

Analisar 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 BlueXP não pode acessá-los. Estes são os volumes de destino para operações do SnapMirror a partir de um sistema de arquivos FSX for ONTAP.

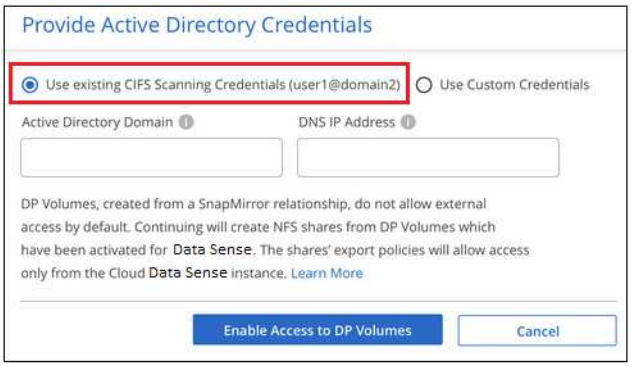
Inicialmente, a lista de volumes identifica esses volumes como *Type* **DP** com o *Status* **Not Scanning** e a *Required Action* **Enable Access to DP volumes**.

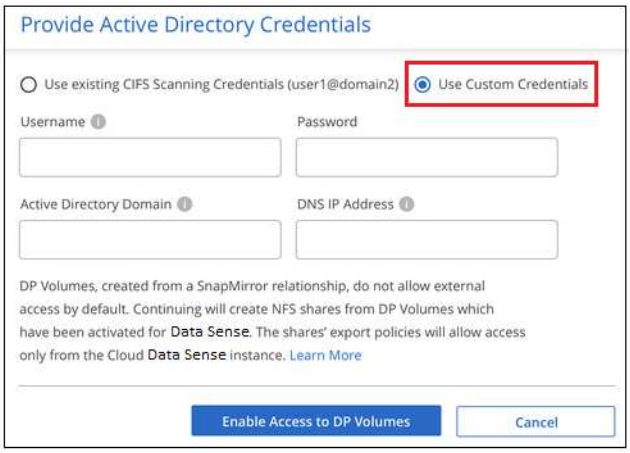


Passos

Se você quiser analisar esses volumes de proteção de dados:

1. Clique em **Ativar o acesso aos volumes DP** na parte superior da página.
2. Revise a mensagem de confirmação e clique em **Ativar o acesso aos volumes DP** novamente.
   - Os volumes criados inicialmente como volumes NFS no sistema de arquivos FSX for ONTAP de origem estão ativados.
   - Os volumes criados inicialmente como volumes CIFS no sistema de arquivos FSX for ONTAP de origem exigem que você insira credenciais CIFS para verificar esses volumes DP. Se você já inseriu credenciais do ative Directory para que a classificação do BlueXP possa analisar volumes CIFS, você pode usar essas credenciais ou especificar um conjunto diferente de credenciais de administrador.





3. Ative cada volume DP que pretende digitalizar.

Resultado

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

Observação: se você não tiver volumes de proteção de dados CIFS quando você ativou inicialmente o acesso a volumes DP e depois adicionar alguns, o botão **Ativar acesso ao CIFS DP** aparece na parte superior da página Configuração. Clique neste botão e adicione credenciais CIFS para permitir o acesso a esses volumes CIFS DP.

As credenciais do active Directory são registradas apenas na VM de storage do primeiro volume CIFS DP, de modo que todos os volumes de DP nesse SVM serão verificados. Quaisquer volumes que residam em outros SVMs não terão as credenciais do ative Directory registradas, portanto, esses volumes DP não serão verificados.

Analise volumes Cloud Volumes ONTAP e ONTAP no local com a classificação BlueXP

Conclua algumas etapas para iniciar a digitalização de volumes Cloud Volumes ONTAP e ONTAP locais usando a classificação BlueXP .

Início rápido

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

1 Descubra as fontes de dados que pretende digitalizar

Antes de poder digitalizar volumes, você deve adicionar os sistemas como ambientes de trabalho no BlueXP :

- Para sistemas Cloud Volumes ONTAP, esses ambientes de trabalho já devem estar disponíveis no BlueXP
- Para sistemas ONTAP on-premises, "O BlueXP precisa descobrir os clusters do ONTAP"

2 Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3 Ative a classificação BlueXP e selecione os volumes a digitalizar

Selecione a guia **Configuração** e ative as verificações de conformidade para volumes em ambientes de trabalho específicos.

4 Garanta o acesso aos volumes

Agora que a classificação BlueXP está ativada, certifique-se de que ela pode acessar todos os volumes.

- A instância de classificação BlueXP precisa de uma conexão de rede para cada sub-rede Cloud Volumes ONTAP ou sistema ONTAP local.
- Os grupos de segurança para Cloud Volumes ONTAP devem permitir conexões de entrada da instância de classificação BlueXP .
- Certifique-se de que essas portas estejam abertas para a instância de classificação BlueXP :
  - Para NFS - portas 111 e 2049.
  - Para CIFS - portas 139 e 445.
- As políticas de exportação de volume NFS devem permitir o acesso a partir da instância de classificação BlueXP .

- A classificação do BlueXP precisa de credenciais do ative Directory para analisar volumes CIFS.

  Clique em **Compliance** > **Configuration** > **Edit CIFS Credentials** e forneça as credenciais.

5 Gerencie os volumes que deseja digitalizar

Selecione ou anule a seleção dos volumes que pretende digitalizar e a classificação BlueXP iniciará ou deixará de os digitalizar.

Descubra as fontes de dados que pretende digitalizar

Se as fontes de dados que você deseja digitalizar ainda não estiverem em seu ambiente BlueXP , você poderá adicioná-las à tela neste momento.

Seus sistemas Cloud Volumes ONTAP já devem estar disponíveis no Canvas no BlueXP . Para sistemas ONTAP on-premises, você precisará ter "BlueXP Descubra esses clusters"o .

Implante a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

Se estiver a digitalizar sistemas Cloud Volumes ONTAP e ONTAP locais acessíveis através da Internet, pode "Implante a classificação do BlueXP na nuvem" ou "em um local no local que tem acesso à internet".

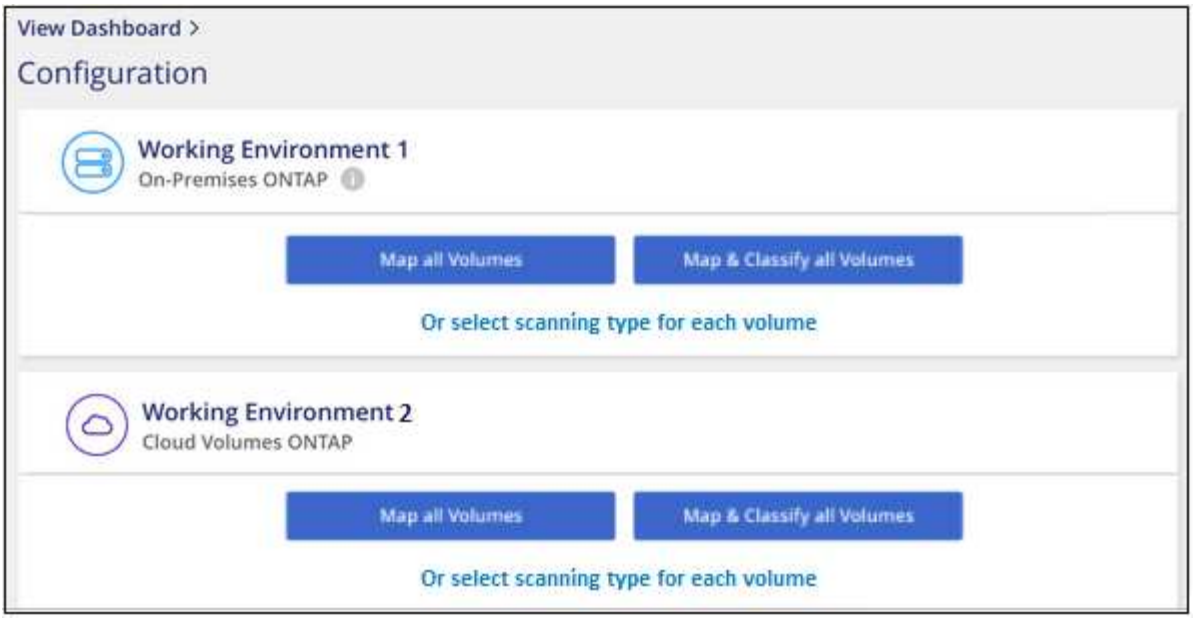
Se você estiver digitalizando sistemas ONTAP locais que foram instalados em um site escuro que não tem acesso à Internet, você precisa "Implante a classificação BlueXP no mesmo local que não tem acesso à Internet". Isso também requer que o BlueXP Connector seja implantado no mesmo local.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Ative a classificação BlueXP nos seus ambientes de trabalho

É possível habilitar a classificação do BlueXP em sistemas Cloud Volumes ONTAP em qualquer fornecedor de nuvem compatível e em clusters de ONTAP on-premises.

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.



2. Selecione como pretende digitalizar os volumes em cada ambiente de trabalho. "Saiba mais sobre o mapeamento e a classificação de exames":
   - Para mapear todos os volumes, clique em **Mapear todos os volumes**.
   - Para mapear e classificar todos os volumes, clique em **Map & Classify All volumes**.
   - Para personalizar a digitalização para cada volume, clique em **ou selecione o tipo de digitalização para cada volume** e, em seguida, escolha os volumes que pretende mapear e/ou classificar.

     Ative e desative verificações de conformidade em volumesConsulte para obter detalhes.

3. Na caixa de diálogo de confirmação, clique em **Approve** para que a classificação BlueXP comece a digitalizar seus volumes.

Resultado

A classificação BlueXP inicia a digitalização dos volumes selecionados no ambiente de trabalho. Os resultados estarão disponíveis no painel de conformidade assim que a classificação BlueXP terminar as verificações iniciais. O tempo que leva depende da quantidade de dados - pode ser de alguns minutos ou horas.

- Por padrão, se a classificação do BlueXP 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 do BlueXP não pode reverter o "último tempo de acesso" para o carimbo de data/hora original. Se não se importar se a última hora de acesso for redefinida, clique em **ou selecione o tipo de digitalização para cada volume**. A página resultante tem uma configuração que você pode habilitar para que a classificação BlueXP digitalize os volumes independentemente das permissões.
- A classificação BlueXP verifica apenas um compartilhamento de arquivo sob um volume. Se você tiver vários compartilhamentos em seus volumes, precisará analisar esses outros compartilhamentos separadamente como um grupo de compartilhamentos. "Veja mais detalhes sobre esta limitação de classificação BlueXP ".

Verifique se a classificação BlueXP tem acesso a volumes

Certifique-se de que a classificação do BlueXP possa acessar volumes verificando suas políticas de rede,

grupos de segurança e exportação. Você precisará fornecer a classificação BlueXP com credenciais CIFS para que possa acessar volumes CIFS.

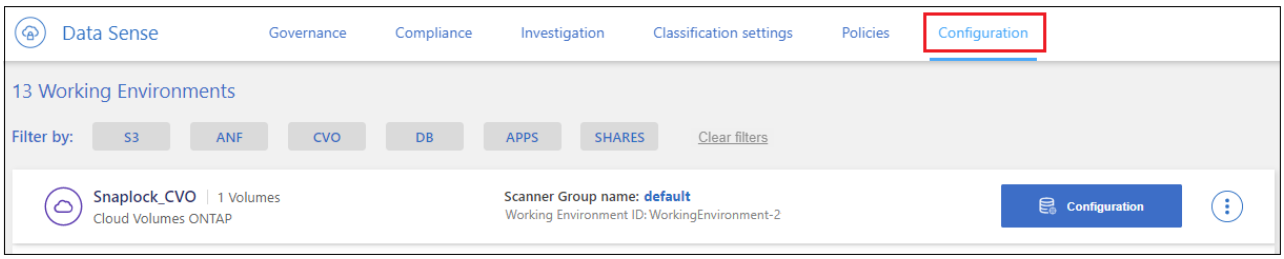
Passos

1. Verifique se há uma conexão de rede entre a instância de classificação do BlueXP e cada rede que inclua volumes para clusters Cloud Volumes ONTAP ou ONTAP no local.
2. Certifique-se de que o grupo de segurança do Cloud Volumes ONTAP permita o tráfego de entrada da instância de classificação do BlueXP .

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

3. Certifique-se de que as seguintes portas estejam abertas para a instância de classificação BlueXP :
   - Para NFS - portas 111 e 2049.
   - Para CIFS - portas 139 e 445.
4. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de classificação BlueXP para que ela possa acessar os dados em cada volume.
5. Se você usar o CIFS, forneça a classificação do BlueXP com credenciais do ative Directory para que ele possa analisar volumes CIFS.

   a. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e selecione a guia **Configuração**.

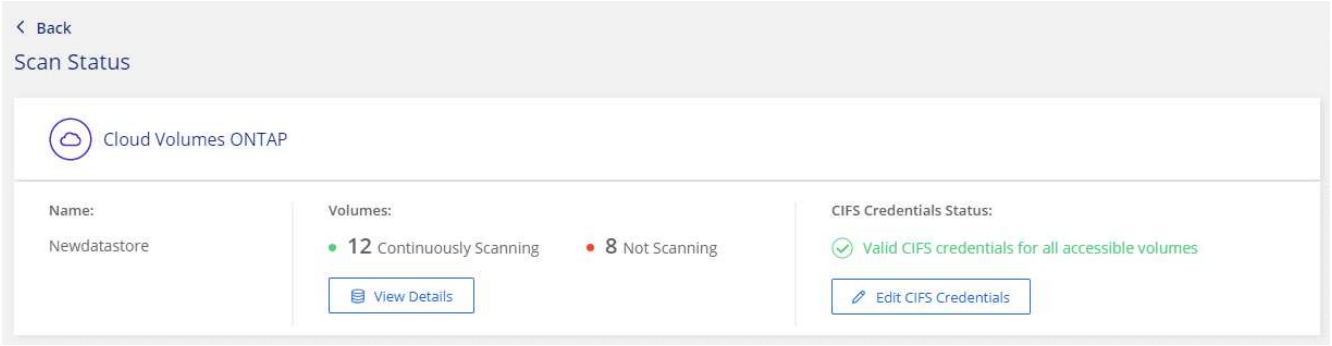
   

   b. Para cada ambiente de trabalho, clique em **Editar credenciais CIFS** e introduza o nome de utilizador e a palavra-passe de que a classificação BlueXP necessita para aceder aos volumes CIFS no sistema.

      As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que a classificação do BlueXP possa ler qualquer dado que exija permissões elevadas. As credenciais são armazenadas na instância de classificação do BlueXP .

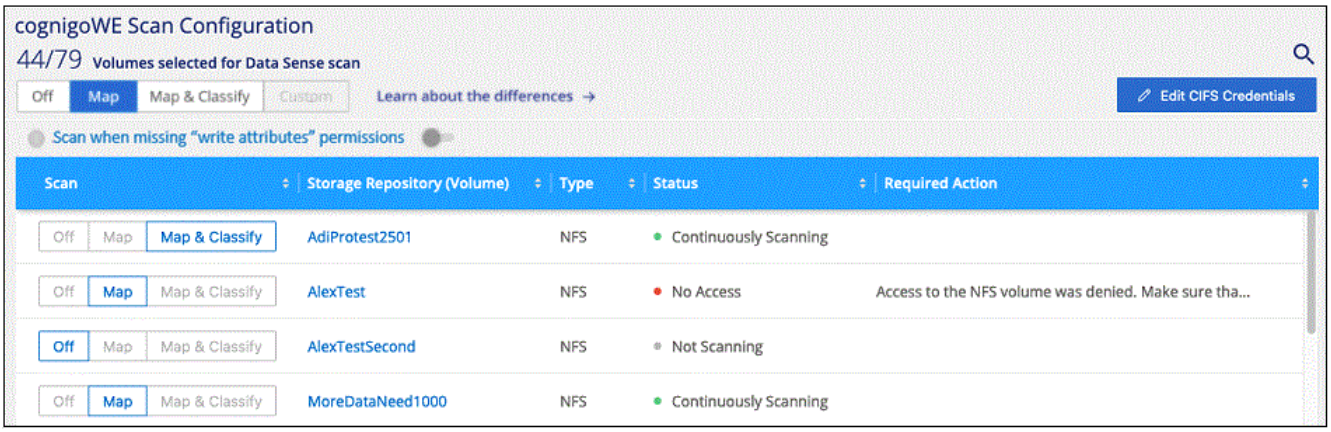
      Se você quiser garantir que seus arquivos "últimos tempos acessados" sejam inalterados pelas verificações de classificação do BlueXP , recomendamos que o usuário tenha permissões de atributos de gravação em CIFS ou permissões de gravação em NFS. Se possível, recomendamos tornar o usuário configurado do ative Directory parte de um grupo pai na organização que tem permissões para todos os arquivos.

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



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

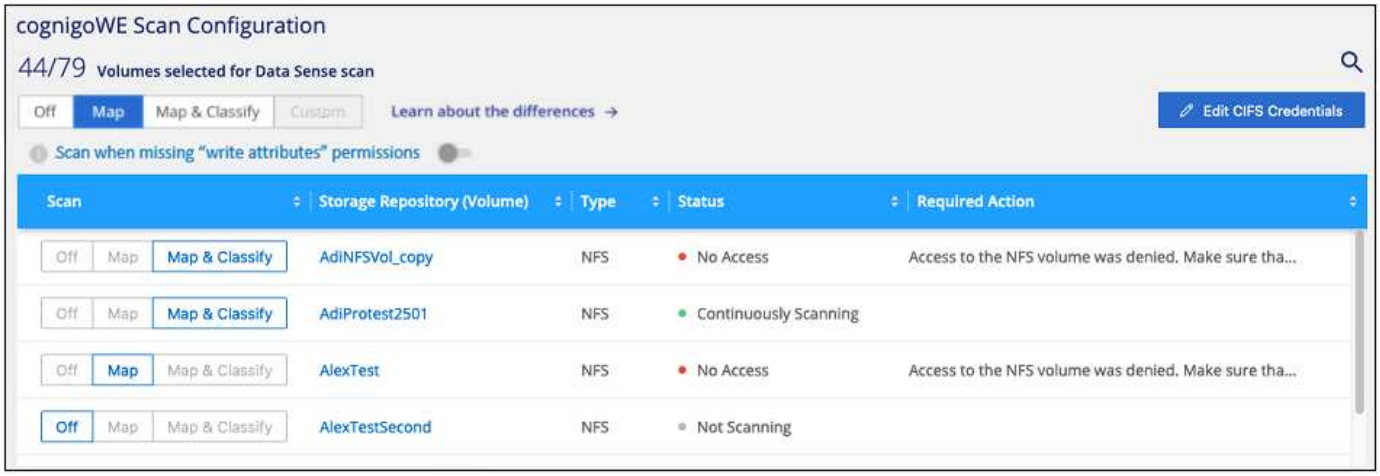
   Por exemplo, a imagem a seguir mostra quatro volumes; um dos quais a classificação BlueXP não pode digitalizar devido a problemas de conetividade de rede entre a instância de classificação BlueXP e o volume.



Ative e desative verificações de conformidade em volumes

Pode iniciar ou parar exames apenas de mapeamento ou exames de mapeamento e classificação num ambiente de trabalho a qualquer momento a partir da página Configuração. Você também pode mudar de digitalizações somente de mapeamento para digitalizações de mapeamento e classificação, e vice-versa. Recomendamos que você digitalize todos os volumes.

A opção na parte superior da página para **Scan when missing "write attributes" permissions** está desativada por padrão. Isso significa que se a classificação BlueXP não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a classificação BlueXP não poderá reverter o "último tempo de acesso" para o carimbo de data/hora original. Se você não se importa se a última hora de acesso é redefinida, LIGUE o interrutor e todos os arquivos serão digitalizados independentemente das permissões. "Saiba mais".



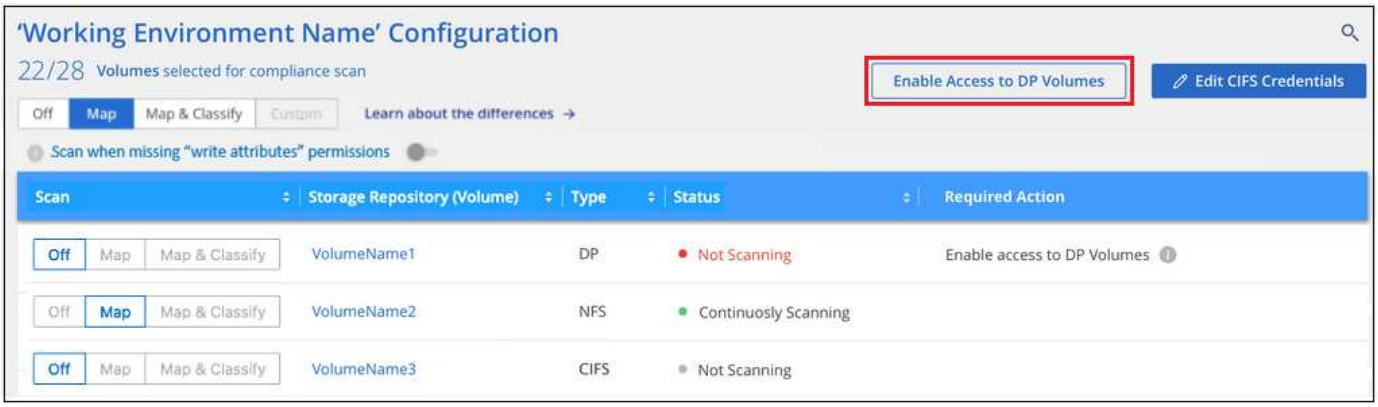
Para:	Faça isso:
Ative digitalizações apenas de mapeamento num volume	Na área de volume, clique em **Map**
Ative a digitalização completa num volume	Na área de volume, clique em **Map & Classify**
Desativar a digitalização num volume	Na área de volume, clique em **Off**
Ative digitalizações apenas de mapeamento em todos os volumes	Na área de cabeçalho, clique em **Map**
Ative a digitalização completa em todos os volumes	Na área de cabeçalho, clique em **Map & Classify**
Desative a digitalização em todos os volumes	Na área de cabeçalho, clique em **Off**

Os novos volumes adicionados ao ambiente de trabalho são automaticamente digitalizados apenas quando você definir a configuração **Map** ou **Map & Classify** na área de cabeçalho. Quando definido como **Custom** ou **Off** na área de cabeçalho, você precisará ativar o mapeamento e/ou a digitalização completa em cada novo volume adicionado no ambiente de trabalho.

Analisar 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 BlueXP não pode acessá-los. Esses são os volumes de destino para operações do SnapMirror a partir de um sistema ONTAP no local ou de um sistema Cloud Volumes ONTAP.

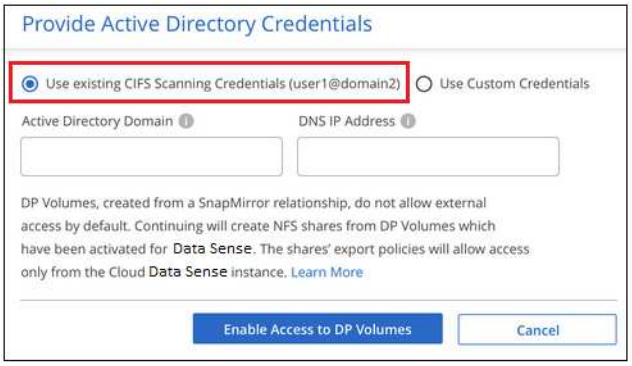
Inicialmente, a lista de volumes identifica esses volumes como *Type* **DP** com o *Status* **Not Scanning** e a *Required Action* **Enable Access to DP volumes**.

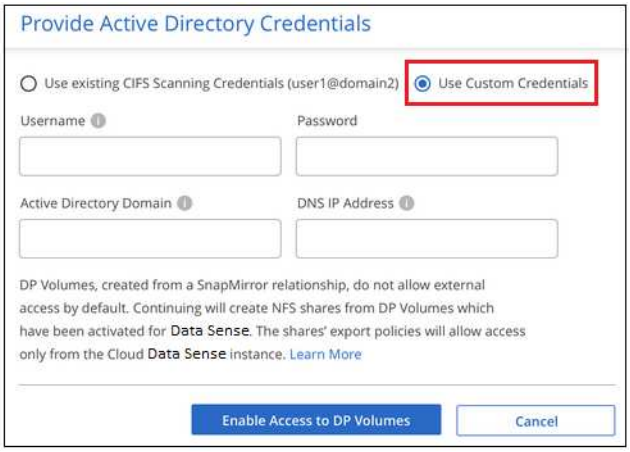


Passos

Se você quiser analisar esses volumes de proteção de dados:

1. Clique em **Ativar o acesso aos volumes DP** na parte superior da página.
2. Revise a mensagem de confirmação e clique em **Ativar o acesso aos volumes DP** novamente.
   - Os volumes inicialmente criados como volumes NFS no sistema ONTAP de origem são ativados.
   - Os volumes criados inicialmente como volumes CIFS no sistema ONTAP de origem exigem que você insira credenciais CIFS para verificar esses volumes DP. Se você já inseriu credenciais do ative Directory para que a classificação do BlueXP possa analisar volumes CIFS, você pode usar essas credenciais ou especificar um conjunto diferente de credenciais de administrador.





3. Ative cada volume DP que pretende digitalizar.

Resultado

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

Observação: se você não tiver volumes de proteção de dados CIFS quando você ativou inicialmente o acesso a volumes DP e depois adicionar alguns, o botão **Ativar acesso ao CIFS DP** aparece na parte superior da página Configuração. Clique neste botão e adicione credenciais CIFS para permitir o acesso a esses volumes CIFS DP.

As credenciais do active Directory são registradas apenas na VM de storage do primeiro volume CIFS DP, de modo que todos os volumes de DP nesse SVM serão verificados. Quaisquer volumes que residam em outros SVMs não terão as credenciais do ative Directory registradas, portanto, esses volumes DP não serão verificados.

Analise esquemas de banco de dados com classificação BlueXP

Conclua algumas etapas para começar a digitalizar seus esquemas de banco de dados com a classificação BlueXP .

Início rápido

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

1 Rever pré-requisitos da base de dados

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

2 Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3 Adicione o servidor de banco de dados

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

4 Selecione os esquemas

Selecione os esquemas que pretende digitalizar.

Reveja os pré-requisitos

Reveja os seguintes pré-requisitos para se certificar de que tem uma configuração suportada antes de ativar a classificação BlueXP .

Bancos de dados compatíveis

A classificação BlueXP pode digitalizar esquemas a partir dos seguintes bancos de dados:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA

- SQL Server (MSSQL)

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

Requisitos de banco de dados

Qualquer banco de dados com conetividade com a instância de classificação BlueXP pode ser digitalizado, independentemente de onde está hospedado. Você só precisa das seguintes informações para se conetar ao banco de dados:

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

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

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

Implante a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

Se você estiver digitalizando esquemas de banco de dados acessíveis pela Internet, você pode "Implante a classificação do BlueXP na nuvem" ou "Implante a classificação BlueXP em um local local que tenha acesso à Internet".

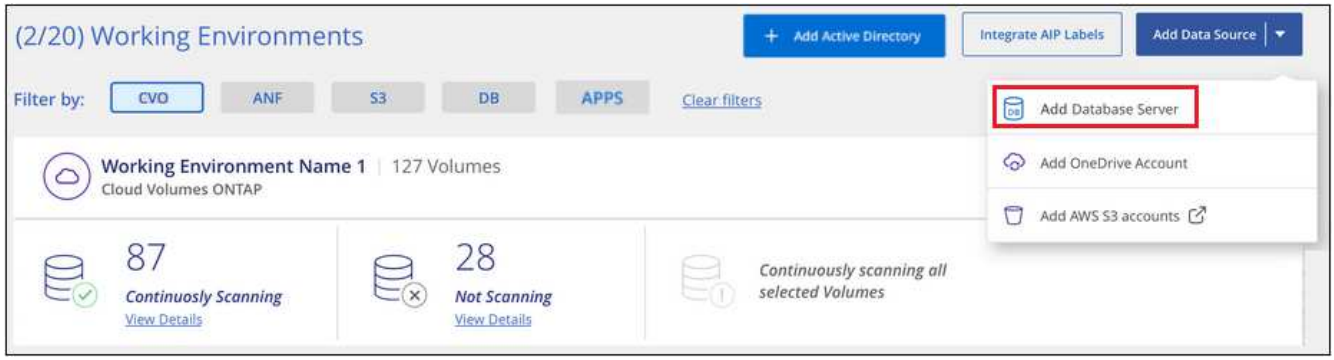
Se você estiver escaneando esquemas de banco de dados que foram instalados em um site escuro que não tem acesso à Internet, você precisará "Implante a classificação BlueXP no mesmo local que não tem acesso à Internet". Isso também requer que o BlueXP Connector seja implantado no mesmo local.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

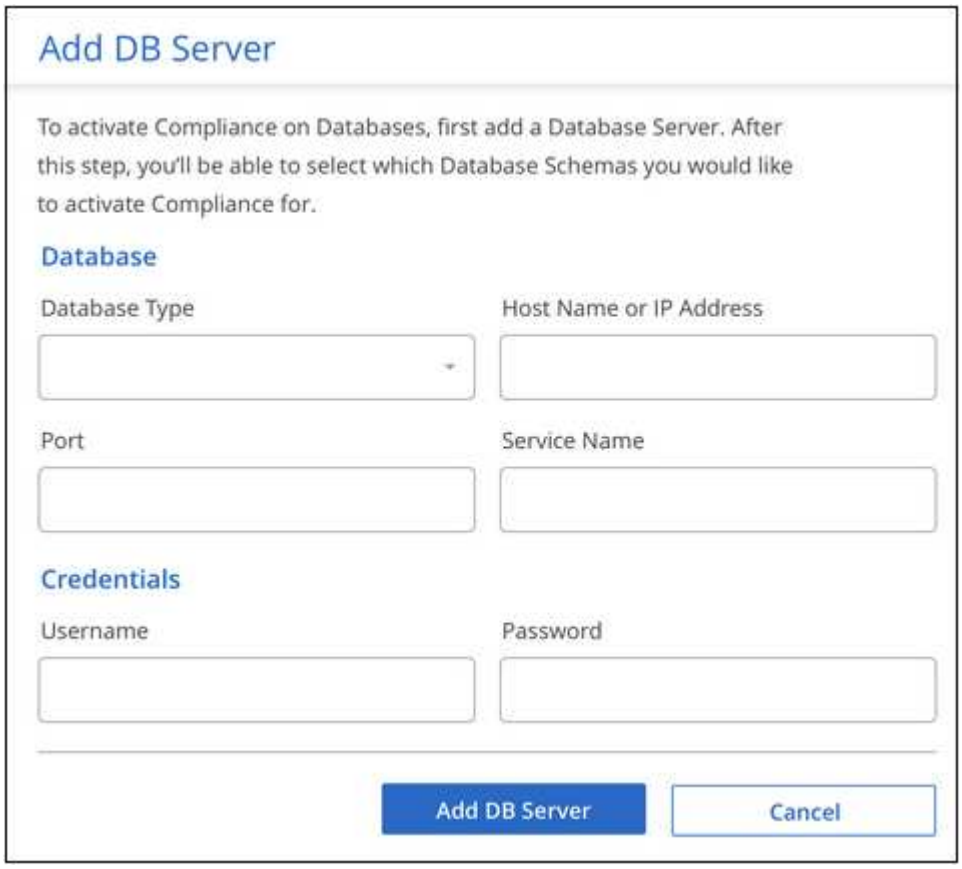
Adicione o servidor de banco de dados

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

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar servidor de banco de dados**.



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



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

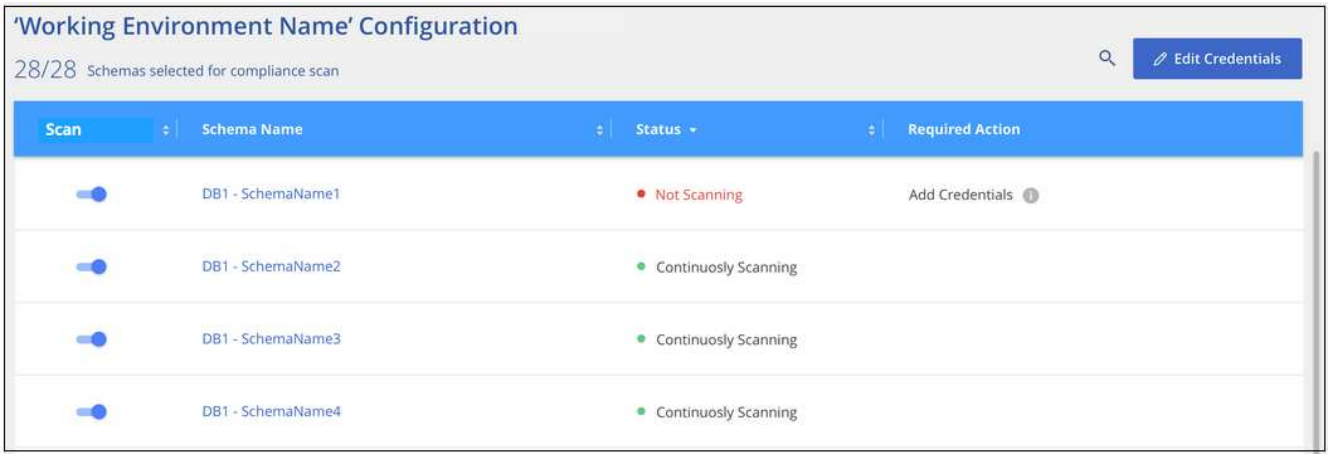
Ative e desative verificações de conformidade em esquemas de banco de dados

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

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

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

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



Resultado

A classificação BlueXP começa a digitalizar os esquemas de banco de dados que você ativou. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Observe que a classificação do BlueXP verifica seus bancos de dados uma vez por dia - os bancos de dados não são verificados continuamente como outras fontes de dados.

Partilha de ficheiros de leitura com a classificação BlueXP

Conclua algumas etapas para iniciar a verificação de compartilhamentos de arquivos NFS ou CIFS a partir de volumes do Google Cloud NetApp e de sistemas NetApp 7-modo mais antigos. Esses compartilhamentos de arquivos podem residir no local ou na nuvem.

A digitalização de dados de compartilhamentos de arquivos não NetApp não é suportada na versão principal da classificação BlueXP .

Início rápido

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

Rever pré-requisitos de partilha de ficheiros

Para compartilhamentos CIFS (SMB), verifique se você tem credenciais para acessar os compartilhamentos.

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

Crie um grupo para manter os compartilhamentos de arquivo

O grupo é um contentor para os compartilhamentos de arquivo que você deseja analisar e é usado como o nome do ambiente de trabalho para esses compartilhamentos de arquivo.

Adicione os compartilhamentos de arquivo ao grupo

Adicione a lista de compartilhamentos de arquivo que você deseja digitalizar e selecione o tipo de digitalização. Você pode adicionar até 100 compartilhamentos de arquivo de cada vez.

Reveja os requisitos de compartilhamento de arquivos

Reveja os seguintes pré-requisitos para se certificar de que tem uma configuração suportada antes de ativar a classificação BlueXP .

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

  Observe que a classificação BlueXP não pode extrair permissões ou o "último tempo de acesso" de sistemas do modo 7. Além disso, devido a um problema conhecido entre algumas versões do Linux e compartilhamentos CIFS em sistemas 7-Mode, você deve configurar o compartilhamento para usar apenas SMB v1 com autenticação NTLM ativada.

- É necessário haver conetividade de rede entre a instância de classificação BlueXP e os compartilhamentos.
- Certifique-se de que essas portas estejam abertas para a instância de classificação BlueXP :
  - Para NFS – portas 111 e 2049.
  - Para CIFS – portas 139 e 445.
- Você pode adicionar um compartilhamento DFS (Distributed File System) como um compartilhamento CIFS regular. No entanto, como a classificação do BlueXP não sabe que o compartilhamento é construído em vários servidores/volumes combinados como um único compartilhamento CIFS, você pode receber erros de permissão ou conetividade sobre o compartilhamento quando a mensagem realmente se aplica a uma das pastas/compartilhamentos localizados em um servidor/volume diferente.
- Para compartilhamentos CIFS (SMB), verifique se você tem credenciais do ative Directory que fornecem acesso de leitura aos compartilhamentos. As credenciais de administrador são preferidas no caso de a

classificação do BlueXP precisar analisar quaisquer dados que requeiram permissões elevadas.

Se você quiser garantir que seus arquivos "últimos tempos acessados" sejam inalterados pelas verificações de classificação do BlueXP , recomendamos que o usuário tenha permissões de atributos de gravação em CIFS ou permissões de gravação em NFS. Se possível, recomendamos tornar o usuário configurado do ative Directory parte de um grupo pai na organização que tem permissões para todos os arquivos.

- Você precisará da lista de compartilhamentos que deseja adicionar no formato `<host_name>:/<share_path>`. Você pode inserir os compartilhamentos individualmente ou fornecer uma lista separada por linha dos compartilhamentos de arquivo que deseja analisar.

Implante a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

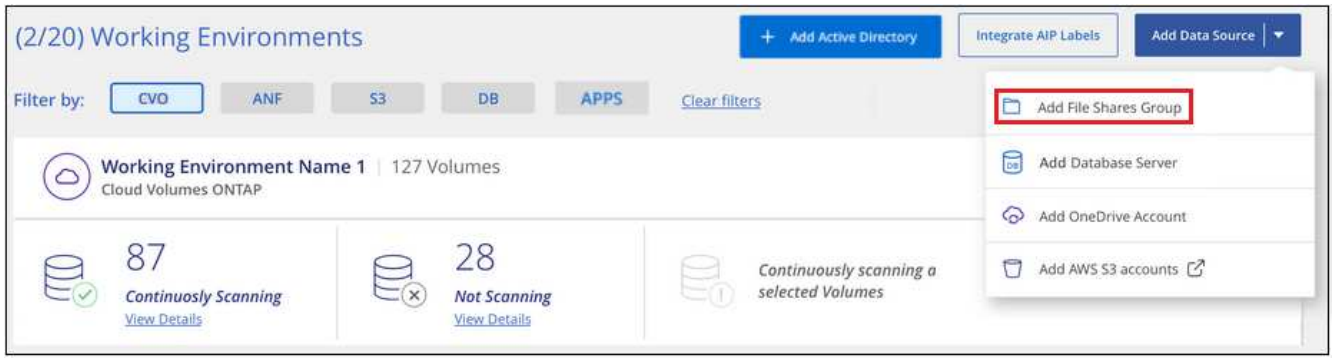
Crie o grupo para os compartilhamentos de arquivo

Você deve adicionar um "grupo" de compartilhamentos de arquivos antes de adicionar seus compartilhamentos de arquivo. O grupo é um recipiente para os compartilhamentos de arquivo que você deseja analisar e o nome do grupo é usado como o nome do ambiente de trabalho para esses compartilhamentos de arquivo.

Você pode misturar compartilhamentos NFS e CIFS no mesmo grupo. No entanto, todos os compartilhamentos de arquivos CIFS em um grupo precisam estar usando as mesmas credenciais do active Directory. Se você planeja adicionar compartilhamentos CIFS que usam credenciais diferentes, será necessário criar um grupo separado para cada conjunto exclusivo de credenciais.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar grupo de compartilhamentos de arquivos**.



2. Na caixa de diálogo Grupo Adicionar compartilhamentos de arquivos, digite o nome do grupo de compartilhamentos e clique em **continuar**.

O novo Grupo de compartilhamentos de arquivo é adicionado à lista de ambientes de trabalho.

Adicionar compartilhamentos de arquivo a um grupo

Você adiciona compartilhamentos de arquivo ao Grupo compartilhamentos de arquivo para que os arquivos

nesses compartilhamentos sejam verificados pela classificação BlueXP . Você adiciona os compartilhamentos no formato `<host_name>:/<share_path>`.

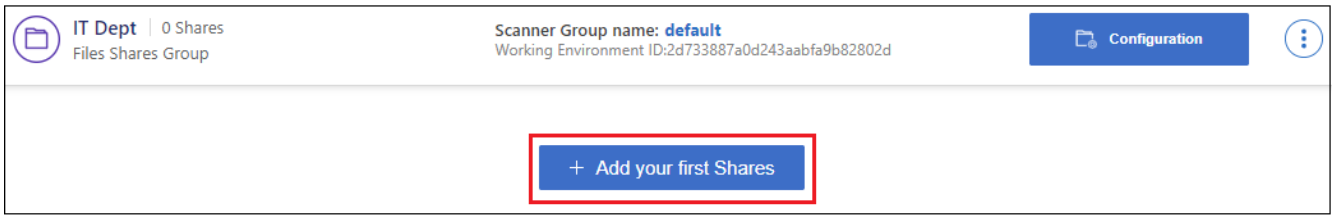
Você pode adicionar compartilhamentos de arquivo individuais ou fornecer uma lista separada por linha dos compartilhamentos de arquivo que deseja analisar. Você pode adicionar até 100 compartilhamentos de cada vez.

Ao adicionar compartilhamentos NFS e CIFS em um único grupo, você precisará executar o processo duas vezes, uma vez que adicionar compartilhamentos NFS e, em seguida, adicionar novamente os compartilhamentos CIFS.

Passos

1. Na página *ambientes de trabalho*, clique no botão **Configuração** do Grupo compartilhamentos de arquivos.

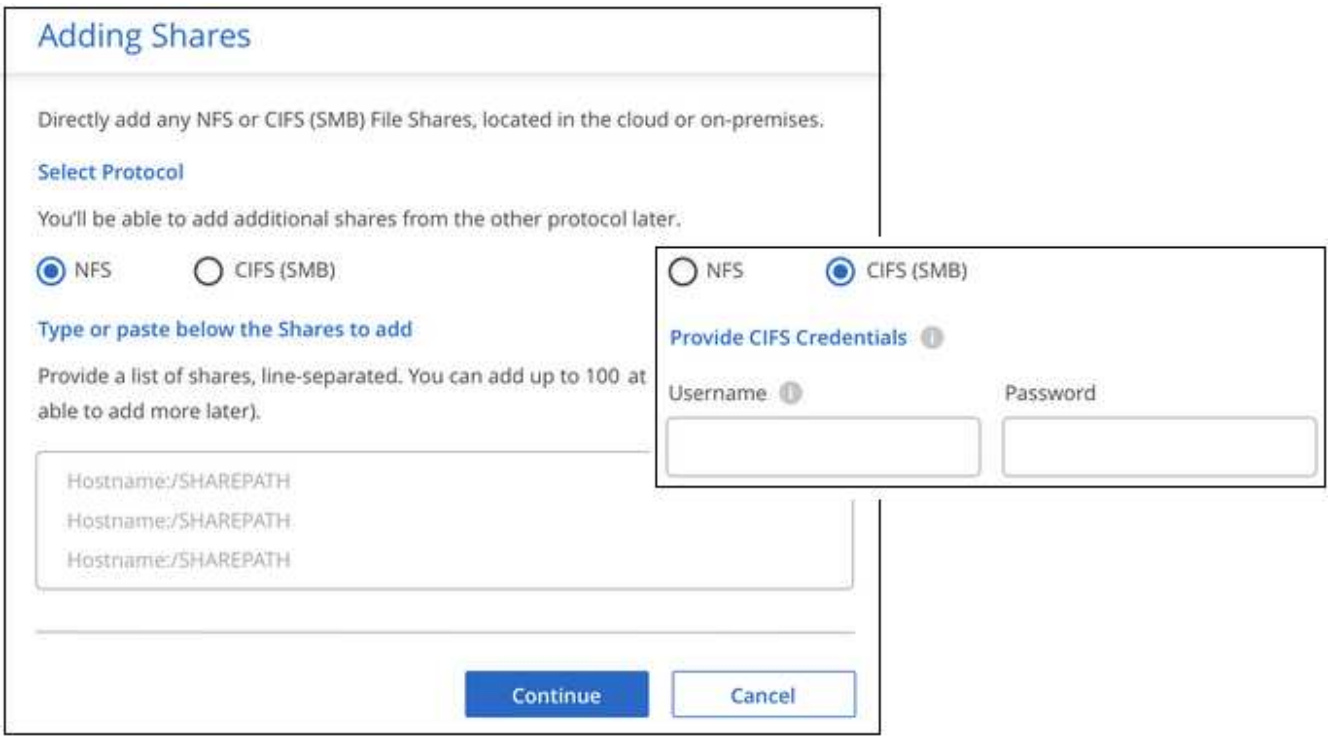
2. Se esta for a primeira vez que adicionar compartilhamentos de arquivo para este Grupo de compartilhamentos de arquivo, clique em **Adicionar seus primeiros compartilhamentos**.



Se você estiver adicionando compartilhamentos de arquivo a um grupo existente, clique em **Adicionar compartilhamentos**.

3. Selecione o protocolo para os compartilhamentos de arquivo que você está adicionando, adicione os compartilhamentos de arquivo que você deseja digitalizar - um compartilhamento de arquivo por linha - e clique em **continuar**.

Ao adicionar compartilhamentos CIFS (SMB), você precisa inserir as credenciais do ative Directory que fornecem acesso de leitura aos compartilhamentos. As credenciais de administrador são preferidas.



Uma caixa de diálogo de confirmação exibe o número de compartilhamentos que foram adicionados.

Se a caixa de diálogo listar quaisquer compartilhamentos que não possam ser adicionados, Capture essas informações para que você possa resolver o problema. Em alguns casos, você pode adicionar novamente o compartilhamento com um nome de host ou nome de compartilhamento corrigido.

4. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação em cada partilha de ficheiros.

Para:	Faça isso:
Ativar varreduras somente de mapeamento em compartilhamentos de arquivo	Clique em **mapa**
Ative digitalizações completas em compartilhamentos de arquivo	Clique em **Map & Classify**
Desative a digitalização em compartilhamentos de arquivo	Clique em **Off**

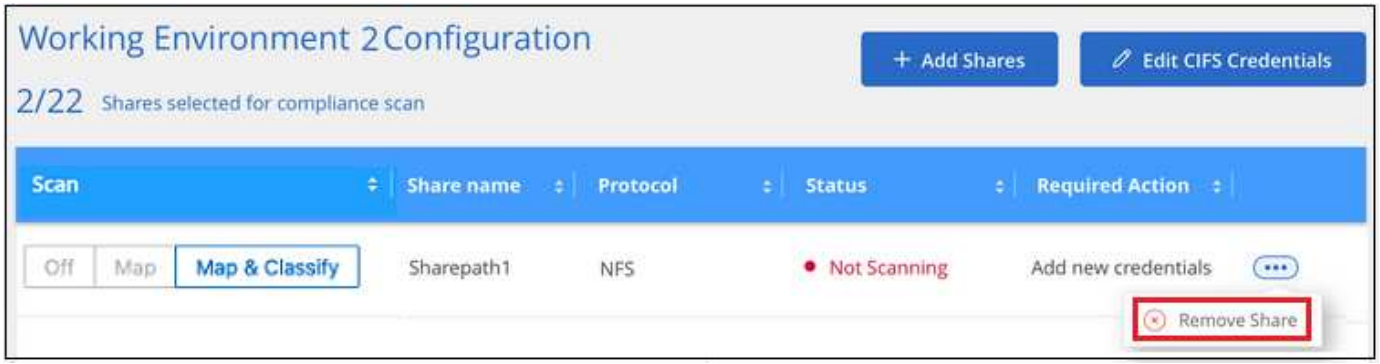
A opção na parte superior da página para **Scan when missing "write attributes" permissions** está desativada por padrão. Isso significa que se a classificação BlueXP não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não verificará os arquivos porque a classificação BlueXP não poderá reverter o "último tempo de acesso" para o carimbo de data/hora original. Se você não se importa se a última hora de acesso é redefinida, LIGUE o interrutor e todos os arquivos serão digitalizados independentemente das permissões. "Saiba mais".

Resultado

A classificação do BlueXP começa a digitalizar os arquivos nos compartilhamentos de arquivo adicionados e os resultados são exibidos no Painel e em outros locais.

Remover um compartilhamento de arquivos de verificações de conformidade

Se você não precisar mais digitalizar certos compartilhamentos de arquivo, você pode remover compartilhamentos de arquivo individuais de ter seus arquivos digitalizados a qualquer momento. Basta clicar em **Remover compartilhamento** na página Configuração.



Analisar dados StorageGRID com classificação BlueXP

Conclua algumas etapas para iniciar a digitalização de dados dentro do StorageGRID diretamente com a classificação BlueXP .

Início rápido

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

1. **Reveja os pré-requisitos do StorageGRID**

Você precisa ter o URL do endpoint para se conetar ao serviço StorageGRID.

Você precisa ter a chave de acesso e a chave secreta do StorageGRID para que a classificação BlueXP possa acessar os buckets.

2. **Implante a instância de classificação do BlueXP**

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3. **Adicione o Serviço StorageGRID**

Adicione o serviço StorageGRID à classificação BlueXP .

4. **Selecione os intervalos para digitalizar**

Selecione os intervalos que você gostaria de digitalizar e a classificação BlueXP começará a digitalizá-los.

Rever os requisitos do StorageGRID

Reveja os seguintes pré-requisitos para se certificar de que tem uma configuração suportada antes de ativar a classificação BlueXP .

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

Implante a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

Se estiver a digitalizar dados a partir do StorageGRID que está acessível através da Internet, pode "Implante a classificação do BlueXP na nuvem" ou "Implante a classificação BlueXP em um local local que tenha acesso à Internet".

Se você estiver digitalizando dados do StorageGRID que foram instalados em um site escuro que não tem acesso à Internet, será necessário "Implante a classificação BlueXP no mesmo local que não tem acesso à Internet". Isso também requer que o BlueXP Connector seja implantado no mesmo local.

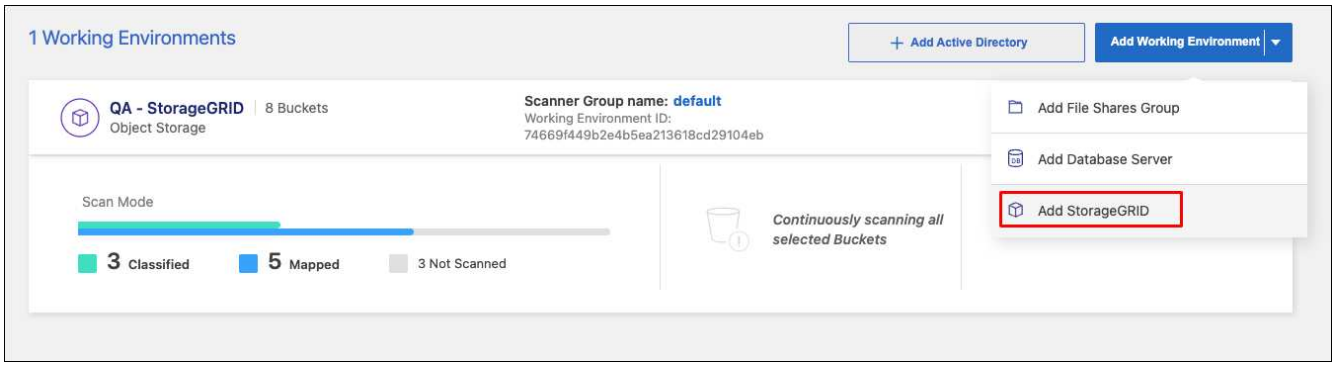
As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Adicione o serviço StorageGRID à classificação BlueXP

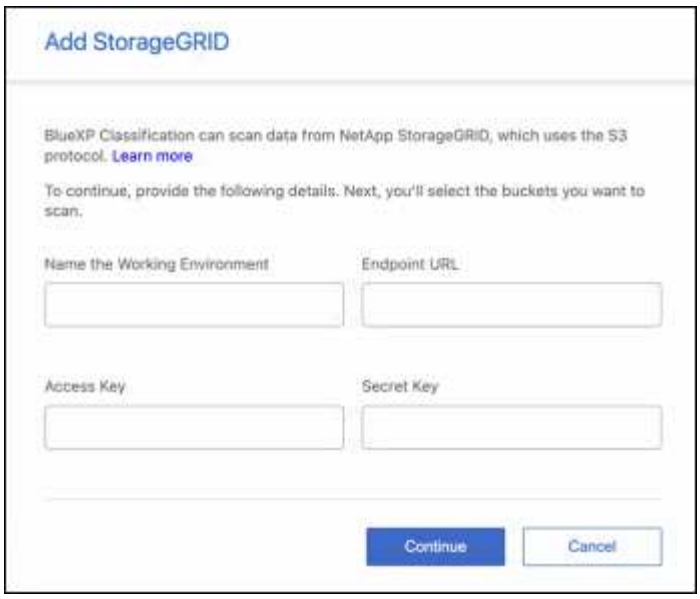
Adicione o serviço StorageGRID.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar StorageGRID**.



2. Na caixa de diálogo Adicionar serviço StorageGRID, insira os detalhes do serviço StorageGRID e clique em **continuar**.
   a. Introduza o nome que pretende utilizar para o ambiente de trabalho. Esse nome deve refletir o nome do serviço StorageGRID ao qual você está se conetando.
   b. Insira o 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 BlueXP possa acessar os buckets no StorageGRID.



Resultado

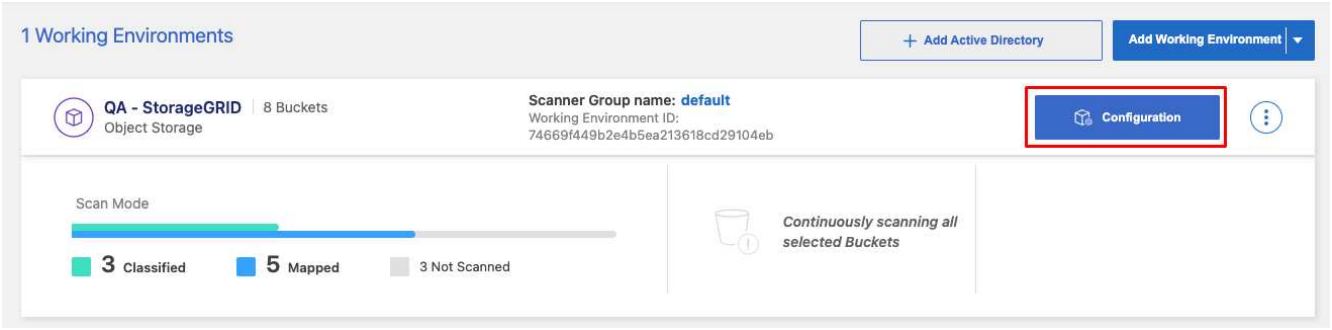
O StorageGRID é adicionado à lista de ambientes de trabalho.

Ative e desative verificações de conformidade em buckets do StorageGRID

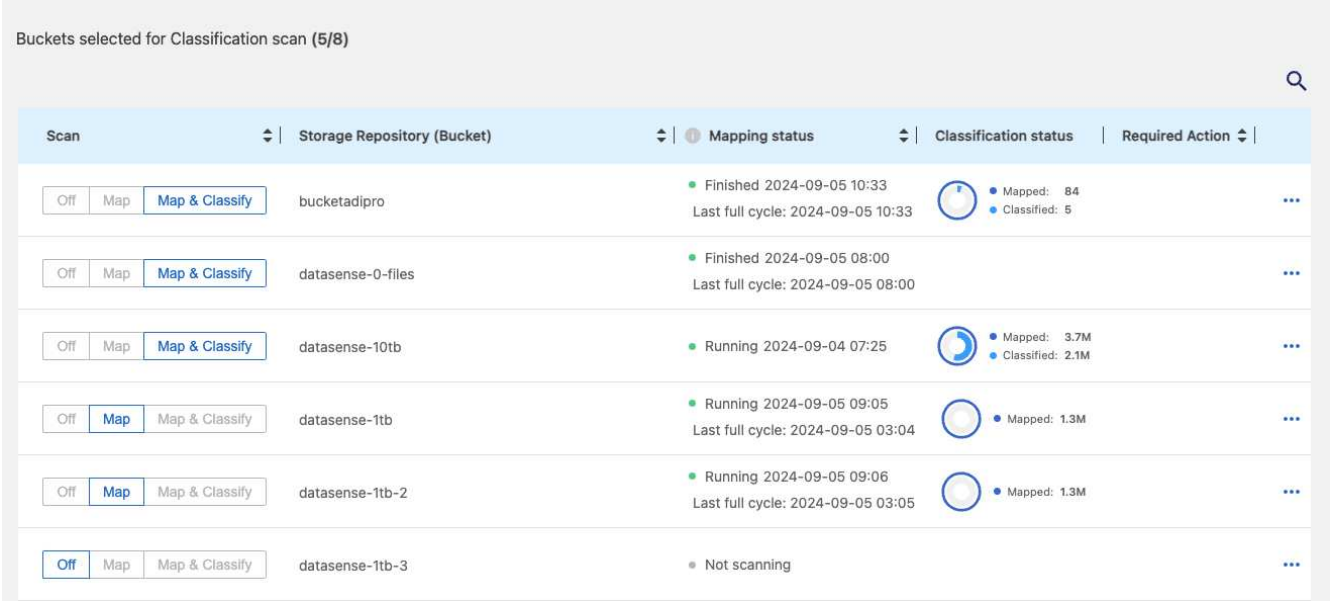
Depois de ativar a classificação BlueXP no StorageGRID, a próxima etapa é configurar os intervalos que você deseja digitalizar. A classificação BlueXP descobre esses buckets e os exibe no ambiente de trabalho que você criou.

Passos

1. Na página Configuração, clique em **Configuração** no ambiente de trabalho do StorageGRID.



2. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação nos seus buckets.



Para:	Faça isso:
Ative digitalizações apenas de mapeamento num balde	Clique em **mapa**
Ative digitalizações completas num balde	Clique em **Map & Classify**
Desative a digitalização em um balde	Clique em **Off**

Resultado

A classificação BlueXP começa a digitalizar os intervalos que você ativou. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Integre seu ative Directory com a classificação BlueXP

Você pode integrar uma classificação global do ative Directory com o BlueXP para melhorar os resultados que a classificação do BlueXP relata sobre proprietários de arquivos e quais usuários e grupos têm acesso aos seus arquivos.

Quando você configura determinadas fontes de dados (listadas abaixo), você precisa inserir credenciais do ative Directory para que a classificação do BlueXP analise volumes CIFS. Essa integração fornece classificação BlueXP com o proprietário do arquivo e detalhes de permissões para os dados que residem nessas fontes de dados. O ative Directory inserido para essas fontes de dados pode ser diferente das credenciais globais do ative Directory inseridas aqui. A classificação BlueXP irá procurar em todos os diretórios ativos integrados para obter detalhes de usuário e permissão.

Esta integração fornece informações adicionais nos seguintes locais na classificação BlueXP :

- Você pode usar o "proprietário do arquivo" "filtro" e ver os resultados nos metadados do arquivo no painel de investigação. Em vez do proprietário do arquivo que contém o SID (identificador de segurança), ele é preenchido com o nome de usuário real.
- Você pode ver "permissões de arquivo completas" para cada arquivo e diretório quando você clicar no botão "Exibir todas as permissões".
- No "Painel de governança", o painel Open Permissions (permissões abertas) mostrará um maior nível de

detalhes sobre os dados.

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

Fontes de dados compatíveis

Uma integração do ative Directory com a classificação BlueXP pode identificar dados de dentro das seguintes fontes de dados:

- Sistemas ONTAP no local
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX para ONTAP
- Contas OneDrive e contas SharePoint (para versões antigas 1,30 e anteriores)

Não há suporte para identificar informações de usuários e permissões de esquemas de banco de dados, contas do Google Drive, contas do Amazon S3 ou armazenamento de objetos que usam o protocolo Simple Storage Service (S3).

Conete-se ao servidor do ative Directory

Depois de implantar a classificação do BlueXP e ativar a verificação em suas fontes de dados, você pode integrar a classificação do BlueXP ao ative Directory. O ative Directory pode ser acessado usando um endereço IP do servidor DNS ou um endereço IP do servidor LDAP.

As credenciais do ative Directory podem ser somente leitura, mas fornecer credenciais de administrador garante que a classificação do BlueXP possa ler qualquer dado que exija permissões elevadas. As credenciais são armazenadas na instância de classificação do BlueXP .

Para volumes/compartilhamentos de arquivos CIFS, se você quiser garantir que seus arquivos "últimos tempos acessados" sejam inalterados pelas verificações de classificação de BlueXP , recomendamos que o usuário tenha permissão de gravação de atributos. Se possível, recomendamos tornar o usuário configurado do ative Directory parte de um grupo pai na organização que tem permissões para todos os arquivos.

Requisitos

- Você deve ter um ative Directory já configurado para os usuários em sua empresa.
- Você deve ter as informações do ative Directory:
  - Endereço IP do servidor DNS ou vários endereços IP

    ou

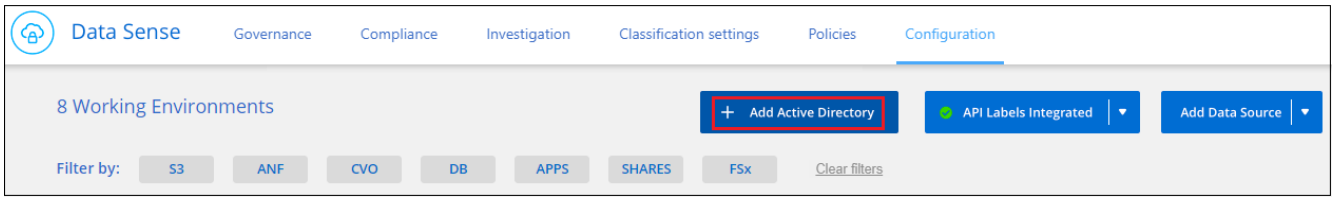
  Endereço IP do servidor LDAP ou vários endereços IP
  - Nome de utilizador e palavra-passe para aceder ao servidor
  - Nome de domínio (Nome do ative Directory)
  - Quer esteja a utilizar LDAP seguro (LDAPS) ou não
  - Porta de servidor LDAP (normalmente 389 para LDAP e 636 para LDAP seguro)

- As seguintes portas devem estar abertas para comunicação de saída pela instância de classificação BlueXP :

Protocolo	Porta	Destino	Finalidade
TCP E UDP	389	Ative Directory	LDAP
TCP	636	Ative Directory	LDAP em SSL
TCP	3268	Ative Directory	Catálogo Global
TCP	3269	Ative Directory	Catálogo Global sobre SSL

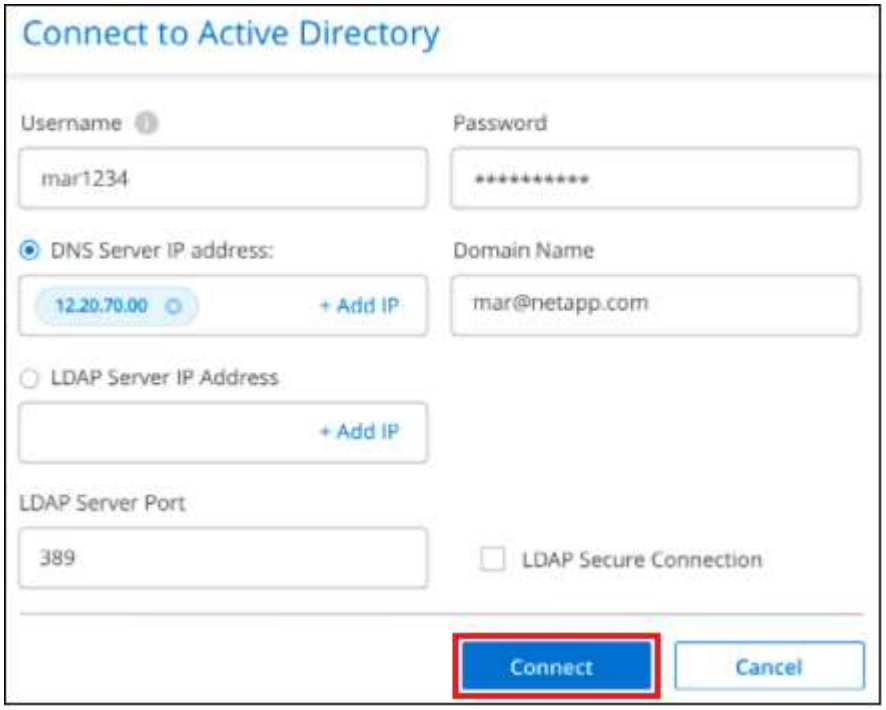
Passos

1. Na página Configuração de classificação do BlueXP , clique em **Adicionar ative Directory**.

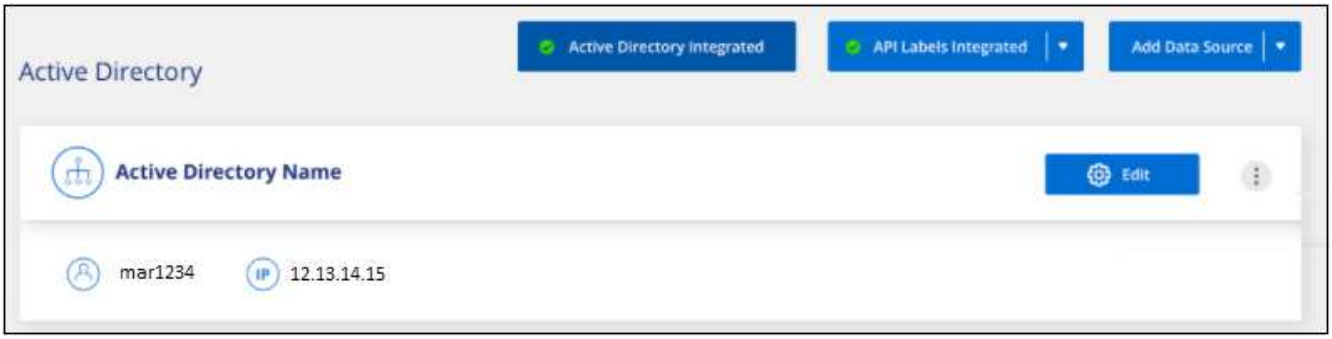


2. Na caixa de diálogo conetar ao ative Directory, insira os detalhes do ative Directory e clique em **conetar**.

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



   A classificação do BlueXP integra-se ao ative Directory e uma nova seção é adicionada à página Configuração.



Gerencie sua integração com o ative Directory

Se você precisar modificar quaisquer valores na integração do ative Directory, clique no botão **Editar** e faça as alterações.

Você também pode excluir a integração se não precisar mais clicando no botão e depois em **Remover ative Directory**.

Perguntas frequentes sobre a classificação BlueXP

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

Serviço de classificação BlueXP

As perguntas a seguir fornecem uma compreensão geral da classificação BlueXP .

O que é a classificação BlueXP ?

A classificação da BlueXP é uma oferta de nuvem que usa a tecnologia orientada por Inteligência artificial (AI) para ajudar você a entender o contexto dos dados e identificar dados confidenciais em seus sistemas de storage. Os sistemas podem ser ambientes de trabalho que você adicionou ao BlueXP Canvas e muitos tipos de fontes de dados que a classificação BlueXP pode acessar em suas redes. "Veja a lista completa abaixo".

A classificação do BlueXP fornece parâmetros predefinidos (como categorias e tipos de informações confidenciais) para lidar com as novas regulamentações de conformidade de dados relativas à privacidade e sensibilidade de dados, como GDPR, CCPA, HIPAA e muito mais.

Como funciona a classificação BlueXP ?

A classificação do BlueXP implanta outra camada de inteligência artificial ao lado do sistema e dos sistemas de storage da BlueXP . Em seguida, ele verifica os dados em volumes, buckets, bancos de dados e outras contas de storage e indexa os insights de dados encontrados. A classificação BlueXP aproveita a inteligência artificial e o processamento de linguagem natural, em vez de soluções alternativas que são comumente construídas em torno de expressões regulares e correspondência de padrões.

A classificação BlueXP usa a IA para fornecer compreensão contextual dos dados para deteção e classificação precisas. Ela é baseada em AI porque foi projetada para tipos e escala de dados modernos. Ele também entende o contexto dos dados, a fim de fornecer forte, preciso, descoberta e classificação.

"Saiba mais sobre como funciona a classificação BlueXP ".

"Saiba mais sobre os casos de uso da classificação BlueXP ".

E a arquitetura da classificação BlueXP ?

A classificação do BlueXP implanta um único servidor ou cluster, onde quer que você escolha, na nuvem ou no local. Os servidores se conetam através 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 a ambientes multicloud, entre nuvens, nuvem privada e on-premises.

Quais fornecedores de nuvem são compatíveis?

A classificação do BlueXP opera como parte do BlueXP e é compatível com AWS, Azure e GCP. Isso proporciona à sua organização uma visibilidade unificada da privacidade entre diferentes fornecedores de nuvem.

A classificação BlueXP tem uma API REST e funciona com ferramentas de terceiros?

Não, a classificação BlueXP não tem uma API REST.

A classificação BlueXP está disponível através dos marketplaces?

Sim, a classificação do BlueXP e do BlueXP está disponível nos marketplaces da AWS, do Azure e do GCP.

Análise e análise de classificação BlueXP

As perguntas a seguir referem-se ao desempenho de varredura de classificação do BlueXP e às análises disponíveis aos usuários.

Com que frequência a classificação BlueXP verifica os meus dados?

Embora a varredura inicial de seus dados possa levar um pouco de tempo, as verificações subsequentes apenas inspecionam as alterações incrementais, o que reduz os tempos de varredura do sistema. A classificação do BlueXP verifica seus dados continuamente de forma redonda, seis repositórios de cada vez, para que todos os dados alterados sejam classificados muito rapidamente.

"Saiba como as digitalizações funcionam".

Observe que a classificação BlueXP verifica bancos de dados apenas uma vez por dia - os bancos de dados não são continuamente verificados como outras fontes de dados.

As verificações de dados têm um impactos insignificante nos sistemas de storage e nos dados. No entanto, se você estiver preocupado com até mesmo um impactos muito pequeno, você pode configurar a classificação BlueXP para executar verificações "lentas". "Veja como reduzir a velocidade de digitalização".

Posso pesquisar meus dados usando a classificação BlueXP ?

A classificação BlueXP oferece recursos de pesquisa abrangentes que facilitam a pesquisa de um arquivo ou pedaço de dados específico em todas as fontes conetadas. A classificação do BlueXP permite que os usuários pesquisem mais do que apenas o que os metadados refletem. É um serviço independente de linguagem 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 possam ter vazado de bancos de dados para arquivos de usuários, violando a política corporativa. As pesquisas podem ser salvas para mais tarde, e as políticas podem ser criadas para pesquisar e agir sobre os resultados em uma frequência definida.

Uma vez que os arquivos de interesse são encontrados, as caraterísticas podem ser listadas, incluindo tags, conta de ambiente de trabalho, bucket, caminho do arquivo, categoria (da classificação), tamanho do arquivo, última modificação, status de permissão, duplicatas, nível de sensibilidade, dados pessoais, tipos de dados confidenciais dentro do arquivo, proprietário, tipo de arquivo, tamanho do arquivo, tempo criado, hash do arquivo, se os dados foram atribuídos a alguém buscando sua atenção e muito mais. Os filtros podem ser aplicados para filtrar as caraterísticas que não são pertinentes. A classificação BlueXP também tem controles RBAC para permitir que arquivos sejam movidos ou excluídos, se as permissões certas estiverem presentes. Se as permissões certas não estiverem presentes, as tarefas poderão ser atribuídas a alguém da organização que tenha as permissões certas.

A classificação BlueXP oferece relatórios?

Sim. As informações oferecidas pela classificação BlueXP podem ser relevantes para outras partes interessadas em suas organizações, portanto, permitimos que você gere relatórios para compartilhar os insights. Os seguintes relatórios estão disponíveis para a classificação BlueXP :

Relatório de avaliação de risco de privacidade

Fornece insights de privacidade de seus dados e uma pontuação de risco de privacidade. "Saiba mais".

Relatório de solicitação de acesso do titular dos dados

Permite extrair um relatório de todos os ficheiros que contêm informações relativas ao nome específico ou identificador pessoal de um titular de dados. "Saiba mais".

Relatório PCI DSS

Ajuda você a identificar a distribuição de informações de cartão de crédito entre seus arquivos. "Saiba mais".

Relatório HIPAA

Ajuda você a identificar a distribuição de informações de saúde entre seus arquivos. "Saiba mais".

Relatório de mapeamento de dados

Fornece informações sobre o tamanho e o número de arquivos em seus ambientes de trabalho. Isso inclui capacidade de uso, idade dos dados, tamanho dos dados e tipos de arquivo. "Saiba mais".

Relatório de avaliação de descoberta de dados

Fornece uma análise de alto nível do ambiente digitalizado para destacar as descobertas do sistema e mostrar áreas de preocupação e possíveis etapas de correção. "Modo de aprendizagem".

Relatórios sobre um tipo de informação específico

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

O desempenho da digitalização varia?

O desempenho da digitalização pode variar com base na largura de banda da rede e no tamanho médio do ficheiro no seu ambiente. Isso também pode depender das características de tamanho do sistema de host (na nuvem ou no local). "A instância de classificação BlueXP "Consulte e "Implantando a classificação BlueXP " para obter mais informações.

Ao adicionar inicialmente novas fontes de dados, você também pode optar por realizar apenas uma varredura de "mapeamento" em vez de uma varredura completa de "classificação". O mapeamento pode ser feito em suas fontes de dados muito rapidamente, porque não acessa arquivos para ver os dados dentro. "Veja a

diferença entre um exame de mapeamento e classificação".

Gestão e privacidade da classificação BlueXP

As perguntas a seguir fornecem informações sobre como gerenciar as configurações de classificação e privacidade do BlueXP .

Como posso ativar a classificação BlueXP ?

Primeiro, você precisa implantar uma instância de classificação do BlueXP no BlueXP ou em um sistema local. Quando a instância estiver em execução, você poderá ativar o serviço em ambientes de trabalho existentes, bancos de dados e outras fontes de dados a partir da guia **Configuração** ou selecionando um ambiente de trabalho específico.

"Saiba como começar".

A ativação da classificação BlueXP numa fonte de dados resulta numa digitalização inicial imediata. Os resultados da digitalização são apresentados pouco depois.

Como posso desativar a classificação BlueXP ?

Você pode desativar a classificação do BlueXP de digitalizar um ambiente de trabalho individual, banco de dados ou grupo de compartilhamento de arquivos na página Configuração de classificação do BlueXP .

"Saiba mais".

Para remover completamente a instância de classificação do BlueXP , você pode remover manualmente a instância de classificação do BlueXP do portal do seu fornecedor de nuvem ou do local no local.

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

A classificação BlueXP fornece insights para seus dados. Esses insights podem ser extraídos e usados para atender às necessidades da sua organização.

Além disso, a classificação BlueXP fornece muitas maneiras de adicionar uma lista personalizada de "dados pessoais" que a classificação BlueXP identificará nas varreduras, dando a você uma visão completa sobre onde os dados potencialmente confidenciais residem em *all* arquivos de suas organizações.

- Você pode adicionar identificadores exclusivos com base em colunas específicas em bancos de dados que você está digitalizando — chamamos isso de **Data Fusion**.
- Você pode adicionar palavras-chave personalizadas a partir de um arquivo de texto.
- Você pode adicionar padrões personalizados usando uma expressão regular (regex).

"Saiba mais".

Posso instruir o serviço a excluir dados de digitalização em determinados diretórios?

Sim. Se você quiser que a classificação do BlueXP exclua os dados de digitalização que residem em determinados diretórios de origem de dados, você pode fornecer essa lista ao mecanismo de classificação. Depois de aplicar essa alteração, a classificação BlueXP excluirá os dados de digitalização nos diretórios especificados.

"Saiba mais".

Os snapshots que residem no ONTAP volumes são digitalizados?

Não. A classificação BlueXP não faz a varredura de instantâneos porque o conteúdo é idêntico ao conteúdo no volume.

O que acontece se a disposição de dados em categorias estiver habilitada no ONTAP volumes?

Quando a classificação do BlueXP verifica volumes que têm dados inativos dispostos em camadas no storage de objetos, ela verifica todos os dados --dados que estão em discos locais e dados inativos dispostos em camadas no storage de objetos. Isso também é verdade para produtos que não são da NetApp que implementam a disposição em camadas.

A digitalização não aquece os dados frios - permanece fria e permanece no armazenamento de objetos.

Tipos de sistemas de origem e tipos de dados

As perguntas a seguir referem-se aos tipos de armazenamento que podem ser digitalizados e aos tipos de dados que são digitalizados.

Que fontes de dados podem ser digitalizadas com a classificação BlueXP ?

A classificação do BlueXP pode analisar dados de ambientes de trabalho que você adicionou ao BlueXP Canvas e de muitos tipos de fontes de dados estruturados e não estruturados que a classificação do BlueXP pode acessar em suas redes.

"Ambientes de trabalho e fontes de dados compatíveis"Consulte .

Há alguma restrição quando implantado em uma região do governo?

A classificação do BlueXP é suportada quando o conetor é implantado em uma região governamental (AWS GovCloud, Azure Gov ou Azure DoD) - também conhecido como "modo restrito". Quando implementada desta forma, a classificação BlueXP tem as seguintes restrições:

> **NOTA** esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

- As contas do OneDrive, contas do SharePoint e contas do Google Drive não podem ser verificadas.
- A funcionalidade de etiqueta AIP (proteção de informações do Microsoft Azure) não pode ser integrada.

Que fontes de dados posso verificar se instalar a classificação BlueXP num site sem acesso à Internet?

A classificação BlueXP só pode digitalizar dados de fontes de dados locais para o local. Neste momento, a classificação BlueXP pode analisar as seguintes fontes de dados locais no "modo privado" - também conhecido como um site "escuro":

- Sistemas ONTAP no local
- Esquemas de banco de dados
- Storage de objetos que usa o protocolo Simple Storage Service (S3)

"Ambientes de trabalho e fontes de dados compatíveis"Consulte .

Quais tipos de arquivo são suportados?

A classificação do BlueXP verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivos na seção tipos de arquivos do painel.

Quando a classificação BlueXP deteta informações pessoais identificáveis (PII) ou quando executa uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados:

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

Que tipos de dados e metadados captura a classificação do BlueXP ?

A classificação BlueXP permite-lhe executar uma análise geral de "mapeamento" ou uma verificação completa de "classificação" nas suas fontes de dados. O mapeamento fornece apenas uma visão geral de alto nível dos seus dados, enquanto a classificação fornece uma varredura de nível profundo dos seus dados. O mapeamento pode ser feito em suas fontes de dados muito rapidamente, porque não acessa arquivos para ver os dados dentro.

- * Digitalização de mapeamento de dados*: A classificação BlueXP verifica apenas os metadados. Isso é útil para gerenciamento e governança de dados gerais, escopo rápido de projetos, propriedades muito grandes 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 corporativas para ajudá-lo a tomar decisões sobre a utilização de recursos, migração, backup, segurança e processos de conformidade.

- * Análise de classificação de dados (profunda)*: A classificação BlueXP digitaliza usando protocolos padrão e permissão somente leitura em todos os seus ambientes. Os arquivos selecionados são abertos e digitalizados para dados confidenciais relacionados a negócios, informações privadas e problemas relacionados ao ransomware.

  Depois de uma verificação completa, há muitos recursos adicionais de classificação do BlueXP que você pode aplicar aos seus dados, como visualizar e refinar dados na página Investigação de dados, pesquisar nomes dentro de arquivos, copiar, mover e excluir arquivos de origem e muito mais.

A classificação BlueXP captura metadados como: Nome do arquivo, permissões, tempo 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 BlueXP pode identificar muitos tipos de dados privados, como informações pessoais (PII) e informações pessoais confidenciais (PII). Para obter detalhes sobre dados privados, "Categorias de dados privados que a classificação BlueXP verifica" consulte .

Posso limitar as informações de classificação do BlueXP a usuários específicos?

Sim, a classificação BlueXP está totalmente integrada com o BlueXP . Os usuários do BlueXP só podem ver informações sobre os ambientes de trabalho que estão qualificados para visualizar de acordo com suas permissões.

Além disso, se você quiser permitir que certos usuários visualizem apenas os resultados da varredura de

classificação do BlueXP sem ter a capacidade de gerenciar as configurações de classificação do BlueXP , você pode atribuir a esses usuários a função **Visualizador de classificação** (ao usar o BlueXP no modo padrão) ou a função **Visualizador de conformidade** (ao usar o BlueXP no modo restrito).

"Saiba mais".

Alguém pode acessar os dados privados enviados entre o meu navegador e a classificação BlueXP ?

Não. Os dados privados enviados entre o seu navegador e a instância de classificação do BlueXP são protegidos com criptografia de ponta a ponta usando TLS 1,2, o que significa que as partes NetApp e não-NetApp não podem lê-los. A classificação BlueXP não compartilhará nenhum dado ou resultado com o NetApp, a menos que você solicite e aprove o acesso.

Os dados digitalizados permanecem dentro do seu ambiente.

Como os dados confidenciais são tratados?

O NetApp não tem acesso a dados confidenciais e não os exibe na IU. Os 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 digitalização são armazenados no Elasticsearch dentro da sua instância de classificação do BlueXP .

Como os dados são acessados?

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

Licenças e custos

A seguinte pergunta diz respeito ao licenciamento e aos custos de utilização da classificação BlueXP .

Quanto custa a classificação BlueXP ?

A classificação BlueXP é uma capacidade de núcleo BlueXP e não é cobrada.

Implantação do conetor

As seguintes questões referem-se ao conetor BlueXP .

O que é o conetor?

O conector é um software executado em uma instância de computação na sua conta de nuvem ou no local que permite que o BlueXP gerencie com segurança os recursos de nuvem. Você deve implantar um conetor para usar a classificação BlueXP .

Onde o conetor precisa ser instalado?

- Ao digitalizar dados no Cloud Volumes ONTAP na AWS ou no Amazon FSX for ONTAP, você usa um conetor na AWS.

- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um conetor no Azure.
- Ao digitalizar dados no Cloud Volumes ONTAP no GCP, você usa um conetor no GCP.
- Ao digitalizar dados em sistemas ONTAP locais, compartilhamentos de arquivos NetApp ou bancos de dados, você pode usar um conetor em qualquer um desses locais de nuvem.

Portanto, se você tiver dados em muitos desses locais, talvez seja necessário usar "Vários conetores"o .

A classificação BlueXP requer acesso a credenciais?

A própria classificação do BlueXP não recupera credenciais de armazenamento. Em vez disso, eles são armazenados dentro do conetor BlueXP .

A classificação BlueXP usa credenciais de plano de dados, por exemplo, credenciais CIFS para montar compartilhamentos antes da digitalização.

Posso implantar o conetor no meu próprio host?

Sim. Você pode "Implante o conetor no local" em um host Linux em sua rede ou em um host na nuvem. Se você está planejando implantar a classificação do BlueXP no local, talvez queira instalar o conetor no local também; mas isso não é necessário.

A comunicação entre o serviço e o conetor usa HTTP?

Sim, a classificação BlueXP se comunica com o conetor BlueXP usando HTTP.

E quanto a sites seguros sem acesso à Internet?

Sim, isso também é suportado. Você pode "Implante o conetor em um host Linux local que não tenha acesso à Internet". "Isso também é conhecido como "modo privado"". Depois, você pode descobrir clusters ONTAP locais e outras fontes de dados locais e verificar os dados usando a classificação do BlueXP .

Implantação da classificação BlueXP

As perguntas a seguir referem-se à instância de classificação BlueXP separada.

Quais modelos de implantação são compatíveis com a classificação BlueXP ?

O BlueXP permite ao usuário digitalizar e gerar relatórios em sistemas praticamente em qualquer lugar, incluindo ambientes locais, na nuvem e híbridos. A classificação do BlueXP é normalmente implantada usando um modelo SaaS, no qual o serviço é habilitado através da interface BlueXP e não requer instalação de hardware ou software. Mesmo nesse modo de implantação com clique e execute, 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 necessário para a classificação BlueXP ?

Quando "implantado na nuvem":

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

- No GCP, a classificação BlueXP é executada em uma VM padrão n2-16 com um disco persistente padrão 500 GiB.

"Saiba mais sobre como funciona a classificação BlueXP ".

Posso implantar a classificação BlueXP no meu próprio host?

Sim. Você pode instalar o software de classificação BlueXP em um host Linux que tenha acesso à Internet em sua rede ou na nuvem. Tudo funciona da mesma forma e você continua a gerenciar a configuração e os resultados da digitalização por meio do BlueXP . "Implantação da classificação do BlueXP no local"Consulte para obter os requisitos do sistema e os detalhes de instalação.

E quanto a sites seguros sem acesso à Internet?

Sim, isso também é suportado. Você pode "Implante a classificação BlueXP em um site local que não tenha acesso à Internet" para sites completamente seguros.

Use a classificação BlueXP

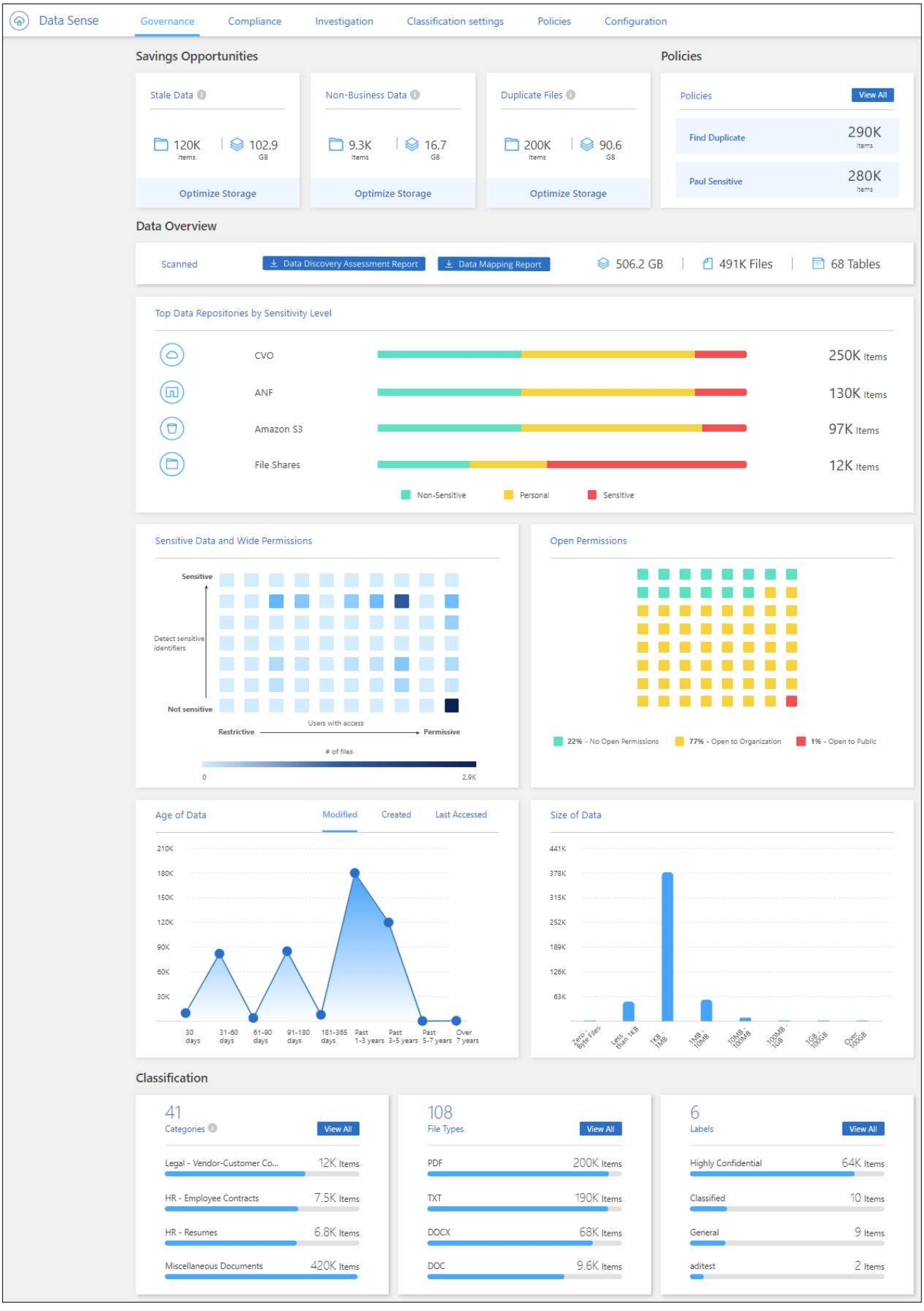
Veja detalhes de governança sobre os dados armazenados em sua organização

Controle os custos relacionados aos dados sobre os recursos de storage da sua organização. A classificação do BlueXP identifica a quantidade de dados obsoletos, dados não comerciais, arquivos duplicados e arquivos muito grandes em seus sistemas. Assim, você pode decidir se deseja remover ou categorizar alguns arquivos para um storage de objetos mais econômico.

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

O painel Governança

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


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate
290K Items
Paul Sensitive
280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO
250K Items
ANF
130K Items
Amazon S3
97K Items
File Shares
12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co...
12K Items
HR - Employee Contracts
7.5K Items
HR - Resumes
6.8K Items
Miscellaneous Documents
420K Items
108
File Types
View All
PDF
200K Items
TXT
190K Items
DOCX
68K Items
DOC
9.6K Items
6
Labels
View All
Highly Confidential
64K Items
Classified
10 Items
General
9 Items
aditest
2 Items

Salvar oportunidades

Você pode querer investigar os itens na área *Saving Opportunities* para ver se há dados que você deve excluir ou categorizar para armazenamento de objetos mais barato. Clique em cada item para ver os resultados filtrados na página de investigação.

- **Dados obsoletos** - dados que foram modificados pela última vez há mais de 3 anos.
- **Dados não comerciais** - dados considerados não relacionados ao negócio, com base na sua Categoria ou tipo de ficheiro. Isso inclui:
  - Dados da aplicação
  - Áudio
  - Executáveis
  - Imagens
  - Registos
  - Vídeos
  - Diversos (categoria geral "outros")
- **Duplicate Files** - arquivos que são duplicados em outros locais nas fontes de dados que você está digitalizando. "Veja que tipos de arquivos duplicados são exibidos".

> Se alguma das suas fontes de dados implementar a disposição em camadas de dados, os dados antigos que já residem no armazenamento de objetos podem ser identificados na categoria *dados obsoletos*.

Políticas com o maior número de resultados

Na área *policies*, as políticas com o maior número de resultados aparecem no topo da lista. Clique no nome de uma política para exibir os resultados na página de investigação. Clique em **Exibir tudo** para exibir a lista de todas as políticas disponíveis.

Clique "aqui" para saber mais sobre políticas.

Visão geral dos dados

A seção *Visão geral de dados* fornece uma visão geral rápida de todos os dados que estão sendo digitalizados. Clique no botão para baixar um relatório completo de mapeamento de dados que inclui capacidade de uso, idade dos dados, tamanho dos dados e tipos de arquivo para todos os seus ambientes de trabalho e fontes de dados. Consulte Relatório de mapeamento de dados para obter detalhes completos sobre este relatório.

Principais repositórios de dados listados por sensibilidade de dados

A área *Top Data Repositories by Sensitivity Level* lista os quatro principais repositórios de dados (ambientes de trabalho e fontes de dados) que contêm os itens mais sensíveis. O gráfico de barras para cada ambiente de trabalho é dividido em:

- Dados não confidenciais
- Dados pessoais
- Dados pessoais confidenciais

Você pode posicionar o cursor sobre cada seção para ver o número total de itens em cada categoria.

Clique em cada área para ver os resultados filtrados na página de investigação para que possa investigar mais.

Dados listados por tipos de permissões abertas

A área *open permissions* mostra a porcentagem para cada tipo de permissões que existem 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

Você pode posicionar o cursor sobre cada seção para ver o número total de arquivos em cada categoria. Clique em cada área para ver os resultados filtrados na página de investigação para que possa investigar mais.

Idade dos dados e tamanho dos gráficos de dados

Você pode querer investigar os itens nos gráficos *Age* e *size* para ver se há dados que você deve excluir ou classificar para armazenamento de objetos menos caro.

Você pode posicionar o cursor sobre um ponto nos gráficos para ver detalhes sobre a idade ou o tamanho dos dados nessa categoria. Clique para ver todos os ficheiros filtrados por essa faixa etária ou tamanho.

- **Age of Data graph** - categoriza os dados com base na hora em que foi criado, na última vez em que foi acessado ou na última vez em que foi modificado.
- * Tamanho do gráfico de dados * - categoriza os dados com base no tamanho.

> Se alguma das suas fontes de dados implementar a disposição em camadas de dados, os dados antigos que já residem no armazenamento de objetos podem ser identificados no gráfico *idade dos dados*.

A maioria das classificações de dados identificadas

A área *Classification* fornece uma lista dos dados mais identificados "Categorias" e "Tipos de ficheiros"verificados.

Categorias

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

Consulte "Visualizar ficheiros por categorias" para obter mais informações.

Tipos de ficheiros

A revisão dos tipos de arquivo pode ajudá-lo a controlar seus dados confidenciais, porque você pode descobrir que certos tipos de arquivo não estão armazenados corretamente.

Consulte "Exibindo tipos de arquivo" para obter mais informações.

Relatório de mapeamento de dados

O Relatório de Mapeamento de dados fornece uma visão geral dos dados que estão sendo armazenados em suas fontes de dados corporativas para ajudá-lo nas decisões de migração, backup, segurança e processos de conformidade. Primeiro, o relatório lista uma visão geral que resume todos os seus ambientes de trabalho e fontes de dados e, em seguida, fornece uma análise para cada ambiente de trabalho.

O relatório inclui as seguintes informações:

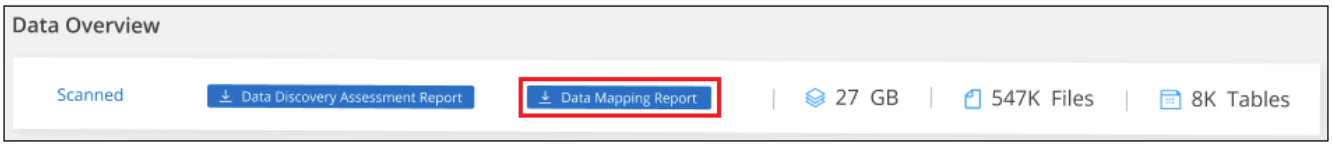
Categoria	Descrição
Capacidade de utilização	Para todos os ambientes de trabalho: Lista o número de arquivos e a capacidade usada para cada ambiente de trabalho. Para ambientes de trabalho individuais: Lista os arquivos que estão usando a maior capacidade.
Idade dos dados	Fornece três gráficos e gráficos para quando os arquivos foram criados, modificados pela última vez ou acessados pela última vez. Lista o número de arquivos e sua capacidade usada, 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 ambientes de trabalho.
Tipos de ficheiros	Lista o número total de arquivos e a capacidade usada para cada tipo de arquivo que está sendo armazenado em seus ambientes de trabalho.

Gerar o Relatório de Mapeamento de dados

Você gera esse relatório a partir da guia Governança na classificação BlueXP .

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Governança** e, em seguida, clique no botão **Relatório de Mapeamento de dados**.



Resultado

A classificação BlueXP gera um relatório .pdf que pode rever e enviar para outros grupos, conforme necessário.

Se o relatório for maior que 1 MB, o arquivo .pdf será retido na instância de classificação do BlueXP e você verá uma mensagem pop-up sobre a localização exata. Quando a classificação do BlueXP é instalada em uma máquina Linux em suas instalações ou em uma máquina Linux implantada na nuvem, você pode navegar diretamente para o arquivo .pdf. Quando a classificação do BlueXP é implantada na nuvem, você precisará fazer SSH para a instância de classificação do BlueXP para baixar o arquivo .pdf. "Veja como acessar dados na instância de classificação".

Observe que você pode personalizar o nome da empresa que aparece na primeira página do relatório a partir

da parte superior da página de classificação do BlueXP clicando e, em seguida, clicando em **alterar nome da empresa**. Na próxima vez que você gerar o relatório, ele incluirá o novo nome.

Relatório de avaliação da descoberta de dados

O Relatório de avaliação de descoberta de dados fornece uma análise de alto nível do ambiente digitalizado para destacar as descobertas do sistema e mostrar áreas de preocupação e possíveis etapas de correção. Os resultados são baseados em mapeamento e classificação de seus dados. O objetivo deste relatório é aumentar a conscientização 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 ser capaz de reduzir a quantidade de dados para economizar custos.
Exposições de segurança de dados	Áreas onde seus dados estão acessíveis a ataques internos ou externos devido a permissões de acesso amplas.
Lacunas de conformidade de dados	Onde suas informações pessoais ou confidenciais estão localizadas para segurança e para DSARs (solicitações de acesso do titular dos dados).

Após a avaliação, este relatório identifica áreas onde você pode:

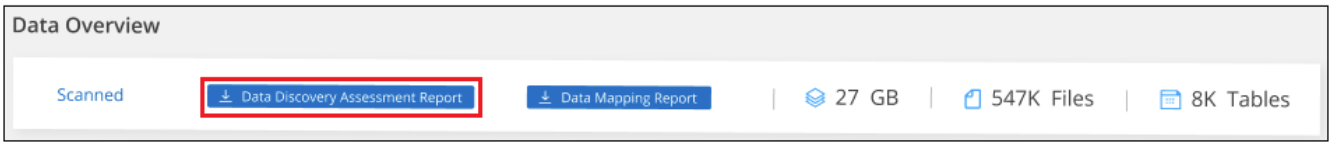
- Reduza os custos de armazenamento alterando sua política de retenção ou movendo ou excluindo determinados dados (dados obsoletos, duplicados ou não comerciais)
- Proteja seus dados com permissões amplas revisando as políticas globais de gerenciamento de grupos
- Proteja seus dados que tenham informações pessoais ou confidenciais, movendo PII para armazenamentos de dados mais seguros

Gerar o Relatório de avaliação de descoberta de dados

Você gera esse relatório a partir da guia Governança na classificação BlueXP .

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Governança** e, em seguida, clique no botão **Relatório de avaliação de descoberta de dados**.



Resultado

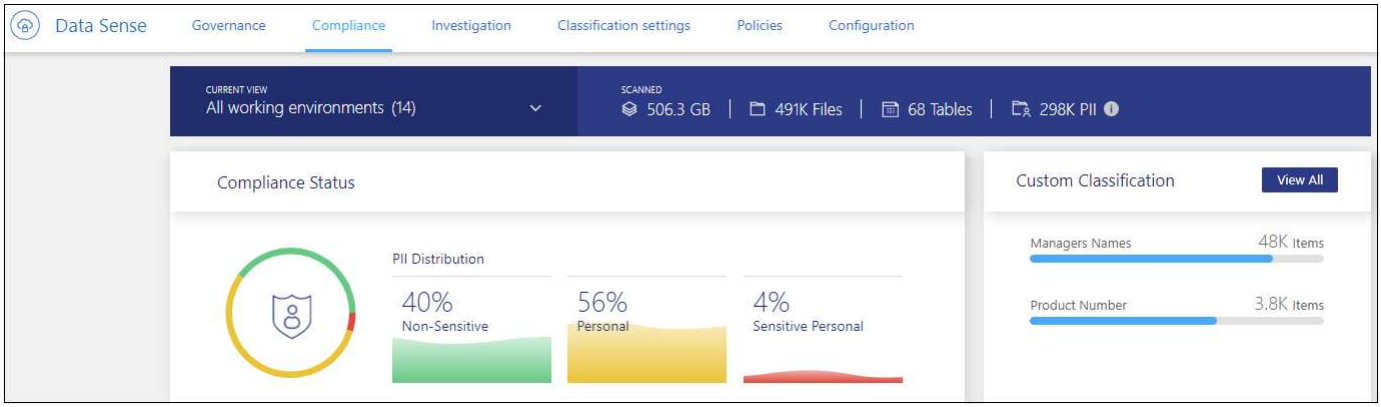
A classificação BlueXP gera um relatório .pdf que pode rever e enviar para outros grupos, conforme necessário.

Veja os detalhes de conformidade sobre os dados privados armazenados na sua organização

Obtenha controle de seus dados privados visualizando detalhes sobre os dados pessoais (PII) e dados pessoais confidenciais (SPii) em sua organização. Você também pode ganhar visibilidade revisando as categorias e tipos de arquivo que a classificação do BlueXP encontrou em seus dados.

> As capacidades descritas nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma varredura somente de mapeamento não mostram detalhes no nível do arquivo.

Por padrão, o painel de classificação do BlueXP exibe dados de conformidade para todos os ambientes de trabalho e bancos de dados.



Se desejar ver os dados apenas para alguns dos ambientes de trabalhoselecione esses ambientes de trabalho, .

Você também pode filtrar os resultados da página Investigação de dados e fazer o download de um relatório dos resultados como um arquivo CSV. "Filtrando dados na página Investigação de dados"Consulte para obter detalhes.

Exibir arquivos que contêm dados pessoais

A classificação BlueXP identifica automaticamente palavras, strings e padrões específicos (Regex) dentro dos dados. Por exemplo, informações de identificação pessoal (PII), números de cartão de crédito, números de segurança social, números de conta bancária, senhas e muito mais. "Veja a lista completa". A classificação BlueXP identifica esse tipo de informação em arquivos individuais, em arquivos dentro de diretórios (compartilhamentos e pastas) e em tabelas de banco de dados.

Além disso, se você adicionou um servidor de banco de dados para ser verificado, o recurso *Data Fusion* permite que você verifique seus arquivos para identificar se identificadores exclusivos de seus bancos de dados são encontrados nesses arquivos ou em outros bancos de dados. "Adicionando identificadores de dados pessoais usando o Data Fusion"Consulte para obter detalhes.

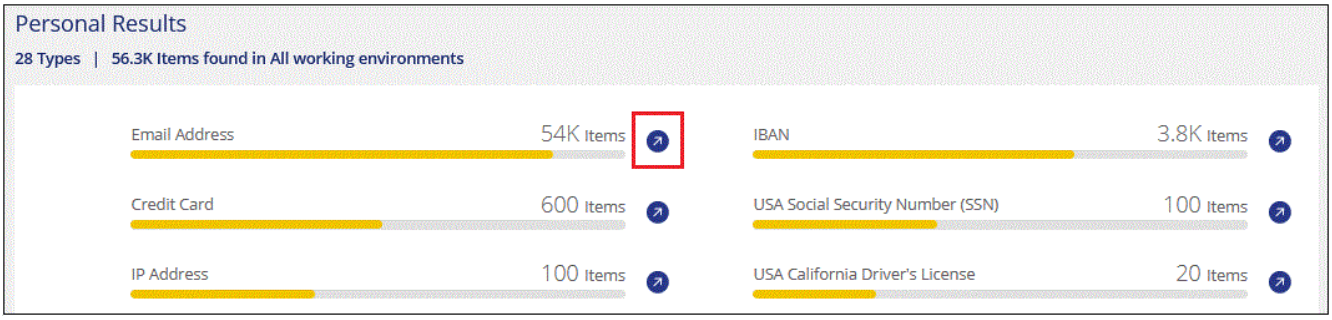
Para alguns tipos de dados pessoais, a classificação BlueXP usa *validação de proximidade* para validar suas descobertas. A validação ocorre procurando uma ou mais palavras-chave predefinidas próximas aos dados pessoais encontrados. Por exemplo, a classificação BlueXP identifica um número de segurança social dos EUA (SSN) como um SSN se ele vir uma palavra de proximidade ao lado dele - por exemplo, *SSN* ou

segurança social. "A tabela de dados pessoais" Mostra quando a classificação BlueXP utiliza a validação de proximidade.

Passos

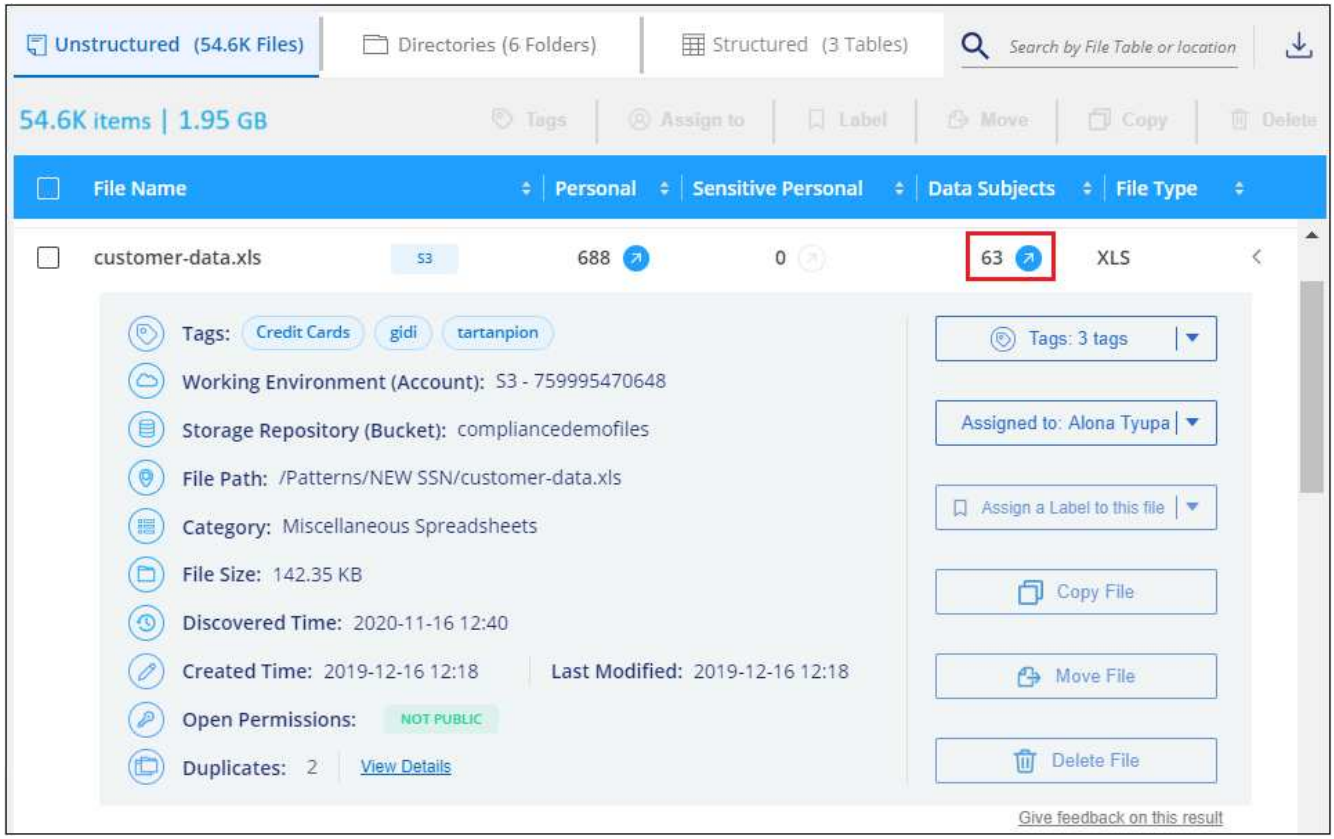
1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e, em seguida, clique na guia **conformidade**.
2. Para investigar os detalhes de todos os dados pessoais, clique no ícone ao lado da porcentagem de dados pessoais.

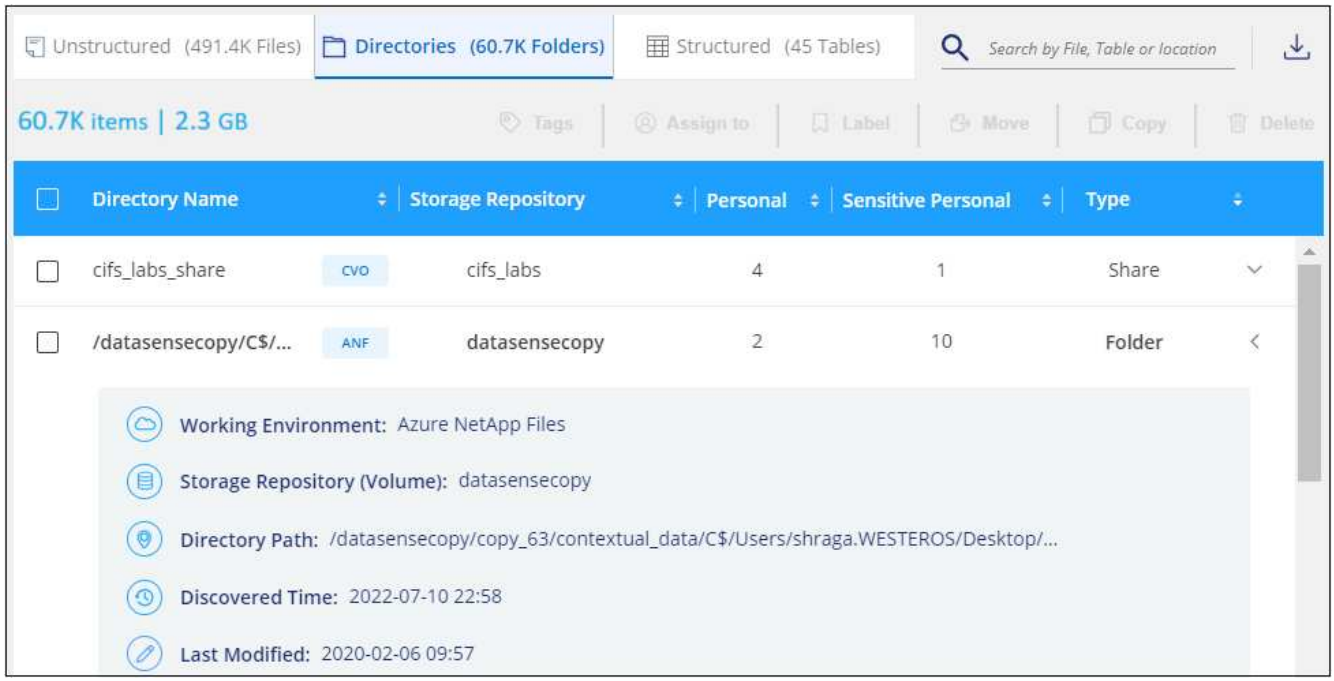
3. Para investigar os detalhes de um tipo específico de dados pessoais, clique em **Exibir todos** e, em seguida, clique no ícone **investigar resultados** para um tipo específico de dados pessoais; por exemplo, endereços de e-mail.



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

   As 2 capturas de tela abaixo mostram dados pessoais encontrados em arquivos individuais e encontrados em arquivos dentro de diretórios (compartilhamentos e pastas). Você também pode selecionar a guia **Structured** para exibir dados pessoais encontrados em bancos de dados.





Exibir arquivos que contêm dados pessoais confidenciais

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

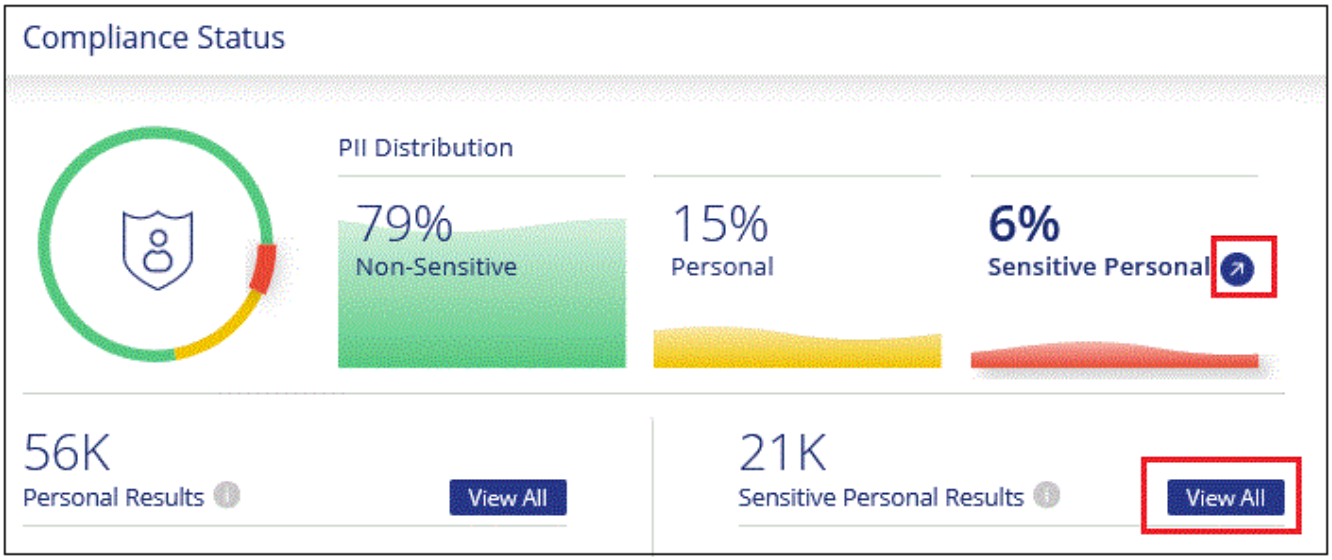
A classificação do BlueXP usa inteligência artificial (AI), processamento de linguagem natural (PNL), aprendizado de máquina (ML) e computação cognitiva (CC) para entender o significado do conteúdo verificado para extrair entidades e categorizá-lo de acordo.

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

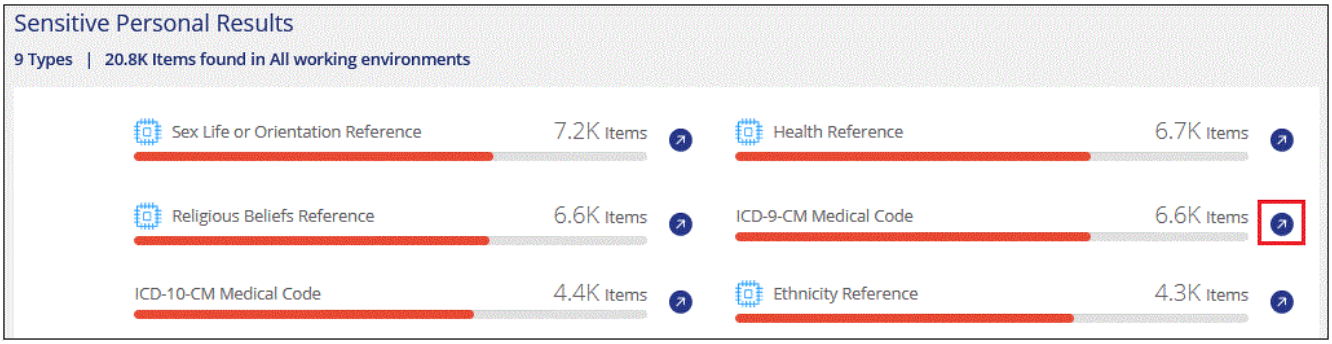
Apenas o inglês é suportado durante a digitalização de dados pessoais confidenciais. O suporte para mais idiomas será adicionado mais tarde.

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e, em seguida, clique na guia **conformidade**.
2. Para investigar os detalhes de todos os dados pessoais confidenciais, clique no ícone ao lado da porcentagem de dados pessoais confidenciais.



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



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

Exibir arquivos por categorias

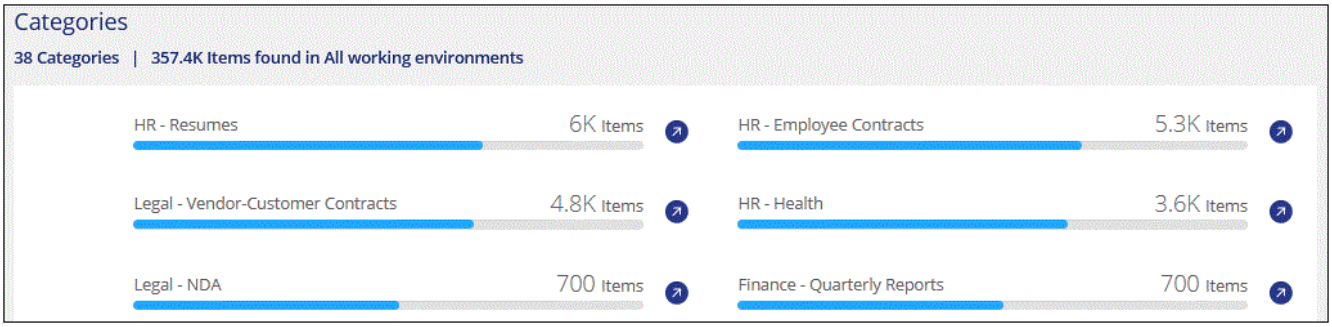
A classificação BlueXP leva os dados que digitalizou e divide-os em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. "Veja a lista de categorias".

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

Inglês, alemão e espanhol são suportados para categorias. O suporte para mais idiomas será adicionado mais tarde.

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e, em seguida, clique na guia **conformidade**.
2. Clique no ícone **investigar resultados** para uma das 4 categorias principais diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone de qualquer uma das categorias.



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

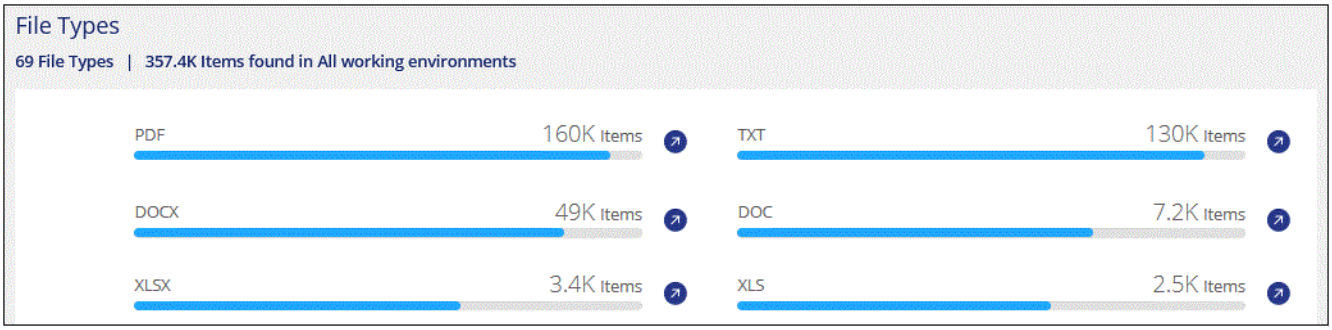
Exibir arquivos por tipos de arquivo

A classificação BlueXP pega os dados que digitalizou e os divide por tipo de arquivo. A revisão dos tipos de arquivo pode ajudá-lo a controlar seus dados confidenciais, porque você pode descobrir que certos tipos de arquivo não estão armazenados corretamente. "Veja a lista de tipos de arquivo".

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

Passos

1. No menu de navegação esquerdo do BlueXP , clique em **Governança > classificação** e, em seguida, clique na guia **conformidade**.
2. Clique no ícone **investigar resultados** para um dos 4 principais tipos de arquivo diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone para qualquer um dos tipos de arquivo.



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

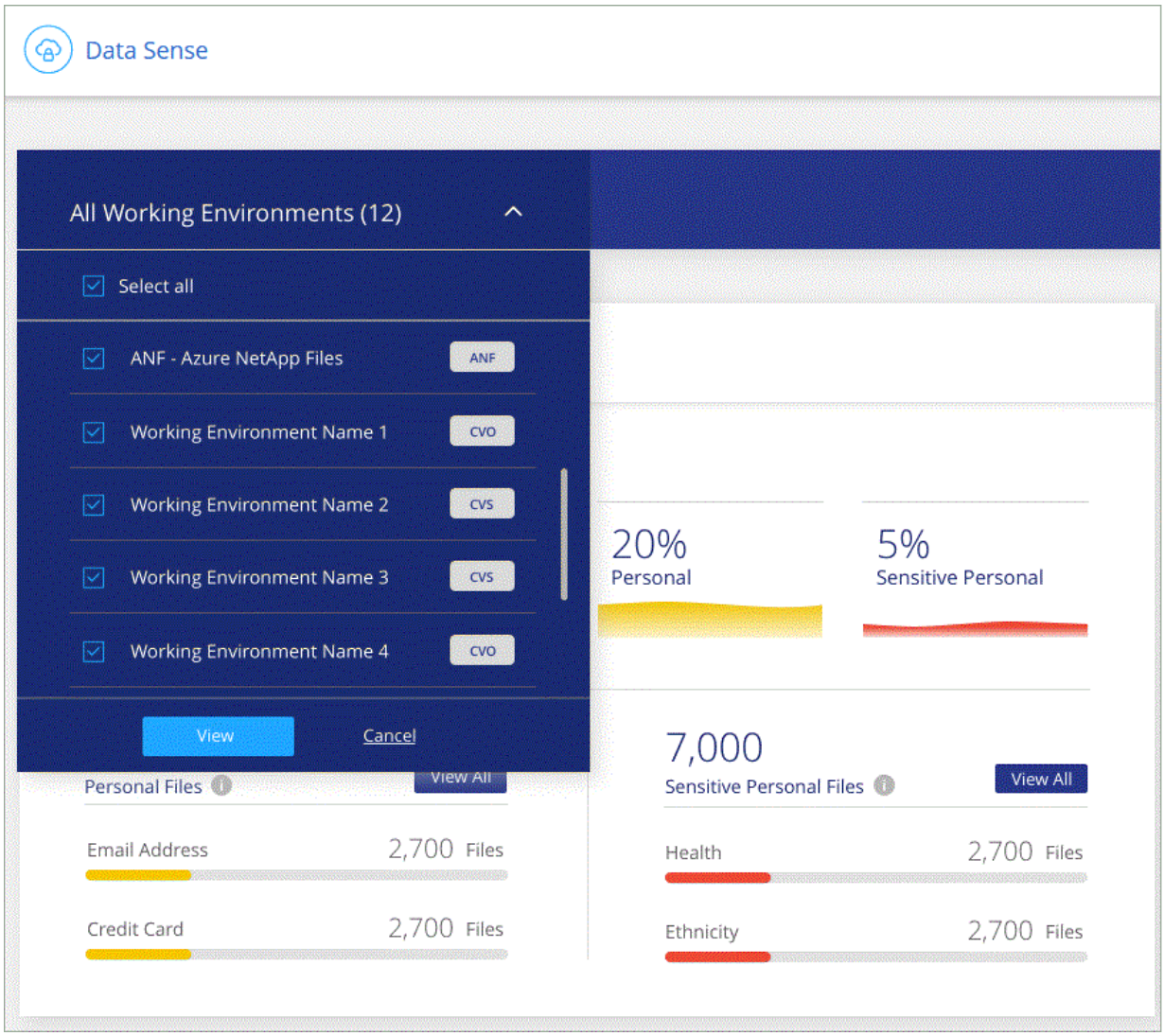
Exibir dados do Dashboard para ambientes de trabalho específicos

Você pode filtrar o conteúdo do painel de classificação do BlueXP para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, a classificação do BlueXP escoa os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

Passos

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



Categorias de dados privados

Há muitos tipos de dados privados que a classificação do BlueXP pode identificar em seus volumes e bancos de dados.

A classificação BlueXP identifica dois tipos de dados pessoais:

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

Se você precisar da classificação BlueXP para identificar outros tipos de dados privados, como números de identificação nacionais adicionais ou identificadores de saúde, envie um e-mail para NetApp.com com com sua solicitação.

Tipos de dados pessoais

Os dados pessoais, ou *informações pessoais identificáveis* (PII), encontrados em arquivos podem ser dados pessoais gerais ou identificadores nacionais. A terceira coluna da tabela abaixo identifica se a classificação BlueXP usa "validação de proximidade" para validar seus resultados para o identificador.

Os idiomas em que esses itens podem ser reconhecidos são identificados na tabela.

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	Japonês
Geral	Número do cartão de crédito	Não	✓	✓	✓		✓
	Titulares dos dados	Não	✓	✓	✓		
	Endereço de e-mail	Não	✓	✓	✓		✓
	Número IBAN (número de conta bancária internacional)	Não	✓	✓	✓		✓
	Endereço IP	Não	✓	✓	✓		✓
	Palavra-passe	Sim	✓	✓	✓		✓

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	Japonês
Identificadores nacionais							

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	Japonês

	Número de identificação fiscal espanhol	Sim	✓	✓	✓		
	ID sueco	Sim	✓	✓	✓		
	Texas Driver's License	Sim	✓	✓	✓		
	ID DO REINO UNIDO (NINO)	Sim	✓	✓	✓		
	EUA California Driver's License	Sim	✓	✓	✓		
	EUA Indiana carteira de motorista	Sim	✓	✓	✓		
	EUA Nova York carteira de motorista	Sim	✓	✓	✓		
	Número da Segurança Social dos EUA (SSN)	Sim	✓	✓	✓		

Tipo	Identificador	Validação de proximidade?	Inglês	Alemão	Espanhol	Francês	Japonês

Tipos de dados pessoais sensíveis

A classificação BlueXP pode encontrar as seguintes informações pessoais confidenciais (SPii) em arquivos.

Os itens nesta categoria só podem ser reconhecidos em inglês neste momento.

- * Referência de procedimentos penais*: Dados relativos às condenações e infrações penais de uma pessoa singular.
- * Referência étnica*: Dados relativos à origem racial ou étnica de uma pessoa natural.
- **Referência de Saúde**: Dados relativos à saúde de uma pessoa singular.
- **CID-9-CM Medical Codes**: Códigos utilizados na indústria médica e de saúde.
- **CID-10-CM Medical Codes**: Códigos utilizados na indústria médica e de saúde.
- * Referência de crenças filosóficas *: Dados relativos às crenças filosóficas de uma pessoa natural.
- **Pareceres políticos Referência**: Dados relativos às opiniões políticas de uma pessoa singular.
- * Referência de crenças religiosas *: Dados relativos às crenças religiosas de uma pessoa natural.
- * Referência de vida sexual ou Orientação *: Dados relativos à vida sexual ou orientação sexual de uma pessoa natural.

Tipos de categorias

A classificação BlueXP categoriza seus dados da seguinte forma.

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

Categoria	Tipo	Inglês	Alemão	Espanhol
Finanças	Balanços	✓	✓	✓
	Ordens compra	✓	✓	✓
	Faturas	✓	✓	✓
	Relatórios trimestrais	✓	✓	✓

Categoria	Tipo	Inglês	Alemão	Espanhol
HR	Verificações de fundo	✓		✓
	Planos de compensação	✓	✓	✓
	Contratos de funcionários	✓		✓
	Avaliações de funcionários	✓		✓
	Saúde	✓		✓
	Retoma	✓	✓	✓
Legal	NDAs	✓	✓	✓
	Contratos fornecedor-cliente	✓	✓	✓
Marketing	Campanhas	✓	✓	✓
	Conferências	✓	✓	✓
Operações	Relatórios de auditoria	✓	✓	✓
Vendas	Ordens vendas	✓	✓	
Serviços	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	Formação	✓	✓	✓
Suporte	Reclamações e bilhetes	✓	✓	✓

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

- Dados da aplicação
- Arquivar ficheiros
- Áudio
- Breadcrumbs da classificação BlueXP dados de aplicativo de negócios
- Ficheiros CAD
- Código
- Corrompido
- Banco de dados e arquivos de índice
- Arquivos de design
- Dados do aplicativo de e-mail
- Encriptado (ficheiros com uma pontuação de entropia elevada)
- Executáveis
- Dados de aplicações financeiras
- Dados da aplicação de integridade
- Imagens

- Registos
- Documentos diversos
- Apresentações diversas
- Folhas de cálculo diversas
- Diversos "desconhecido"
- Ficheiros protegidos por palavra-passe
- Dados estruturados
- Vídeos
- Ficheiros Zero-Byte

Tipos de arquivos

A classificação BlueXP verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivo na seção tipos de arquivo do painel.

Mas quando a classificação BlueXP deteta informações pessoais identificáveis (PII) ou quando realiza uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados:

`.CSV, .DCM, .DICOM, .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 sensíveis que a classificação BlueXP identifica. Deve sempre validar as informações através da revisão dos dados.

Com base em nossos testes, a tabela abaixo mostra a precisão das informações que a classificação BlueXP encontra. Nós quebramos isso por *precisão* e *recall*:

Precisão
: A probabilidade de que o que a classificação BlueXP encontra foi identificada corretamente. Por exemplo, uma taxa de precisão de 90% para dados pessoais significa que 9 em cada 10 arquivos identificados como contendo informações pessoais, contêm informações pessoais. 1 de 10 arquivos seria um falso positivo.

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

Estamos constantemente melhorando a precisão de nossos resultados. Essas melhorias estarão automaticamente disponíveis em futuras versões de classificação do BlueXP .

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

Tipo	Precisão	Recolha
Categorias	90%-97%	60%-80%

Investigue os dados armazenados em sua organização

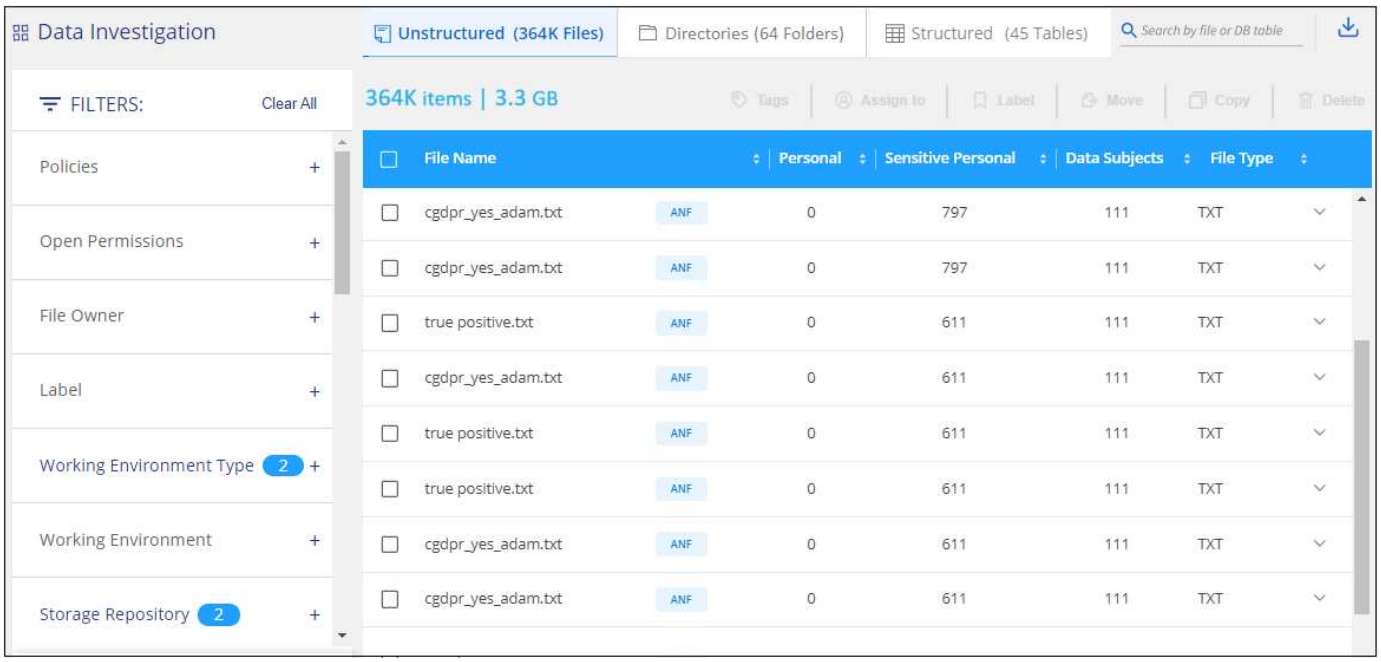
Você pode investigar os dados da sua organização exibindo detalhes na página Investigação de dados. É possível navegar para essa página em várias áreas da IU de classificação do BlueXP , incluindo os painéis de governança e conformidade.

As capacidades descritas nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma varredura somente de mapeamento não mostram detalhes no nível do arquivo.

Filtre os dados na página Investigação de dados

Você pode filtrar o conteúdo da página de investigação para exibir apenas os resultados que deseja ver. Este é um recurso muito poderoso porque depois de ter refinado os dados, você pode usar a barra de botões na parte superior da página para executar uma variedade de ações, incluindo copiar arquivos, mover arquivos, adicionar uma tag ou rótulo AIP aos arquivos e muito mais.

Se você quiser baixar o conteúdo da página como um relatório depois de refiná-lo, clique no botão . Acesse aqui para obter detalhes sobre o relatório de investigação de dados.



- As guias de nível superior permitem exibir dados de arquivos (dados não estruturados), diretórios (pastas e compartilhamentos de arquivos) ou de bancos de dados (dados estruturados).
- Os controles na parte superior de cada coluna permitem classificar os resultados em ordem numérica ou alfabética.
- Os filtros do painel esquerdo permitem refinar os resultados selecionando os atributos descritos nas próximas seções.

Filtrar dados por sensibilidade e conteúdo

Use os filtros a seguir para ver quanta informação sensível 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 detetados por ficheiro. Inclui dados pessoais e dados pessoais sensíveis. Ao filtrar em diretórios, a classificação BlueXP totaliza as correspondências de todos os arquivos em cada pasta (e subpastas). NOTA: A versão de dezembro de 2023 (versão 1.26.6) removeu a opção de calcular o número de dados pessoais identificáveis (PII) pelos diretórios.
Dados pessoais	Selecione o "tipos de dados pessoais".
Dados pessoais confidenciais	Selecione o "tipos de dados pessoais sensíveis".
Titular dos dados	Introduza o nome completo ou identificador conhecido do titular dos dados. "Saiba mais sobre assuntos de dados aqui".

Filtrar dados por proprietário do usuário e permissões do usuário

Use os filtros a seguir para exibir proprietários de arquivos e permissões para acessar seus dados.

Filtro	Detalhes
Abrir permissões	Selecione o tipo de permissões dentro dos dados e dentro de pastas/compartilhamentos.
Permissões de utilizador/grupo	Selecione um ou vários nomes de utilizador e/ou nomes de grupo ou introduza um nome parcial.
Proprietário do ficheiro	Introduza o nome do proprietário do ficheiro.
Número de usuários com acesso	Selecione um ou vários intervalos de categorias para mostrar quais arquivos e pastas estão abertos para um determinado número de usuários.

Filtrar dados por tempo

Use os filtros a seguir para exibir dados com base em critérios de tempo.

Filtro	Detalhes
Hora criada	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.
Hora descoberta	Selecione um intervalo de tempo quando a classificação BlueXP descobriu o arquivo. Você também pode especificar um intervalo de tempo personalizado para refinar ainda mais os resultados da pesquisa.

Filtro	Detalhes
Último modificado	Selecione um intervalo de tempo quando o ficheiro 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 quando o arquivo, ou diretório (somente CIFS ou NFS), 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 ficheiros que a classificação BlueXP verifica, esta é a última vez que a classificação BlueXP digitalizou o ficheiro. Observe que a classificação do BlueXP não extrai o "último tempo acessado" das seguintes fontes de dados: SharePoint Online, SharePoint on-premises (SharePoint Server), OneDrive, Google Drive e Amazon S3.

Filtrar dados por metadados

Use os filtros a seguir para exibir dados com base na localização, tamanho e diretório ou tipo de arquivo.

Filtro	Detalhes
Caminho do ficheiro	Insira até 20 caminhos parciais ou completos que você deseja incluir ou excluir da consulta. Se você inserir ambos os caminhos incluir e excluir, a classificação BlueXP localiza todos os arquivos nos caminhos incluídos primeiro, então remove arquivos de caminhos excluídos e, em seguida, exibe os resultados. Observe que o uso de "*" 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 ficheiro	Selecione o "tipos de arquivos".
Tamanho do ficheiro	Selecione o intervalo de tamanho do ficheiro.
Ficheiro Hash	Insira o hash do arquivo para encontrar um arquivo específico, mesmo que o nome seja diferente.

Filtrar dados por tipo de armazenamento

Use os filtros a seguir para exibir dados por tipo de armazenamento.

Filtro	Detalhes
Tipo de ambiente de trabalho	Selecione o tipo de ambiente de trabalho. OneDrive, SharePoint e Google Drive são categorizados em "Apps".
Nome do ambiente de trabalho	Selecione ambientes de trabalho específicos.
Repositório de armazenamento	Selecione o repositório de armazenamento, por exemplo, um volume ou um esquema.

Filtrar dados por políticas

Use o filtro a seguir para exibir dados por políticas.

Filtro	Detalhes
Políticas	Selecione uma política ou políticas. Vá "aqui" para ver a lista de políticas existentes e para criar suas próprias políticas personalizadas.

Filtrar dados por status da análise

Utilize o seguinte filtro para visualizar os dados pelo estado do exame de classificação BlueXP .

Filtro	Detalhes
Estado análise	Selecione uma opção para mostrar a lista de ficheiros que são Pending First Scan, Completed being Scanned, Pending Rescan ou that has Failed to be Scanned.
Evento análise exame	Selecione se você deseja exibir arquivos que não foram classificados porque a classificação do BlueXP não pôde reverter a última hora acessada, ou arquivos que foram classificados, mesmo que a classificação do BlueXP não pôde reverter a última hora acessada.

"Consulte detalhes sobre o carimbo de data/hora "último acesso"" Para obter mais informações sobre os itens que aparecem na página de investigação ao filtrar usando o evento análise de digitalização.

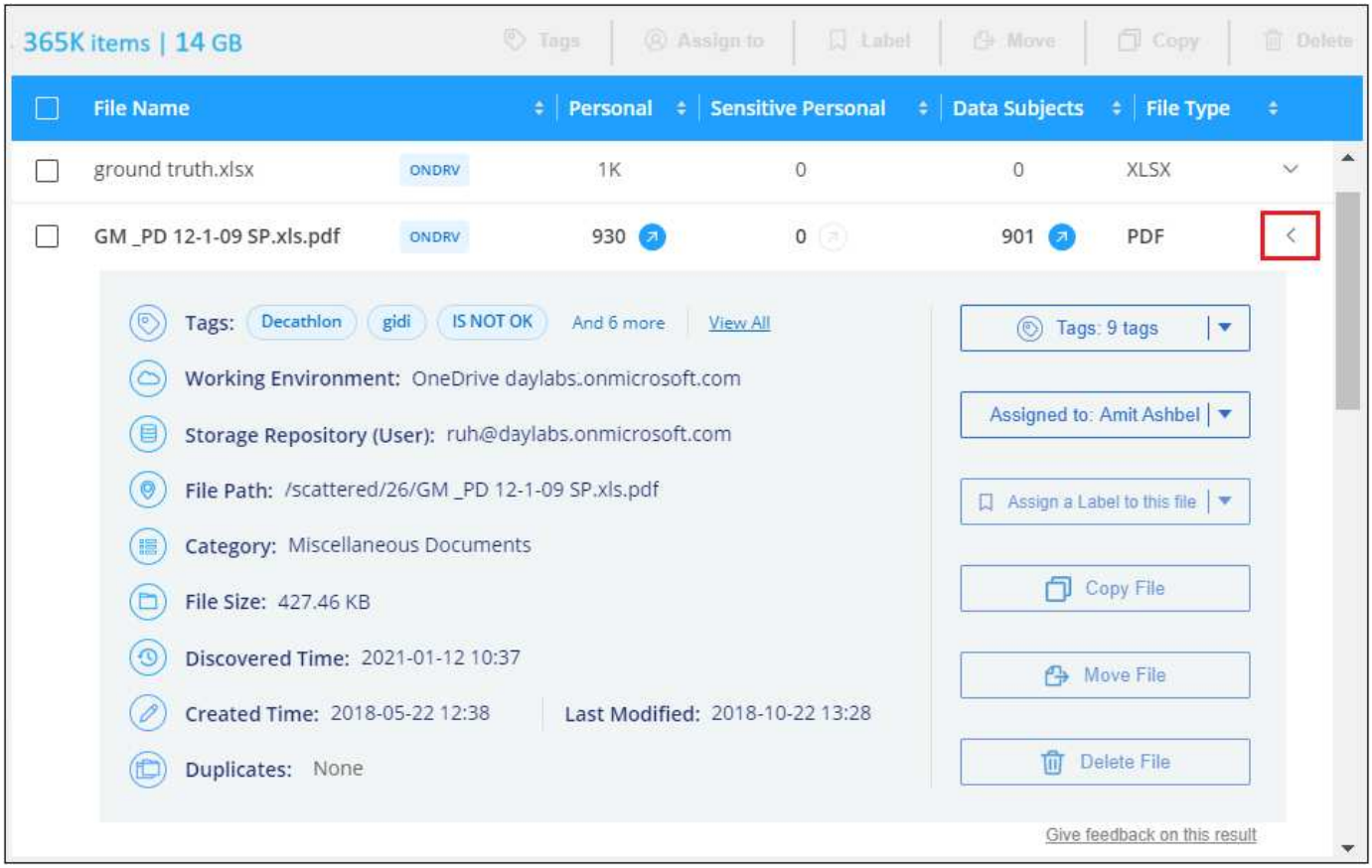
Filtrar dados por duplicatas

Use o filtro a seguir para exibir arquivos duplicados em seu armazenamento.

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

Ver metadados do ficheiro

No painel resultados da investigação de dados, você pode clicar em qualquer arquivo para exibir os metadados do arquivo.



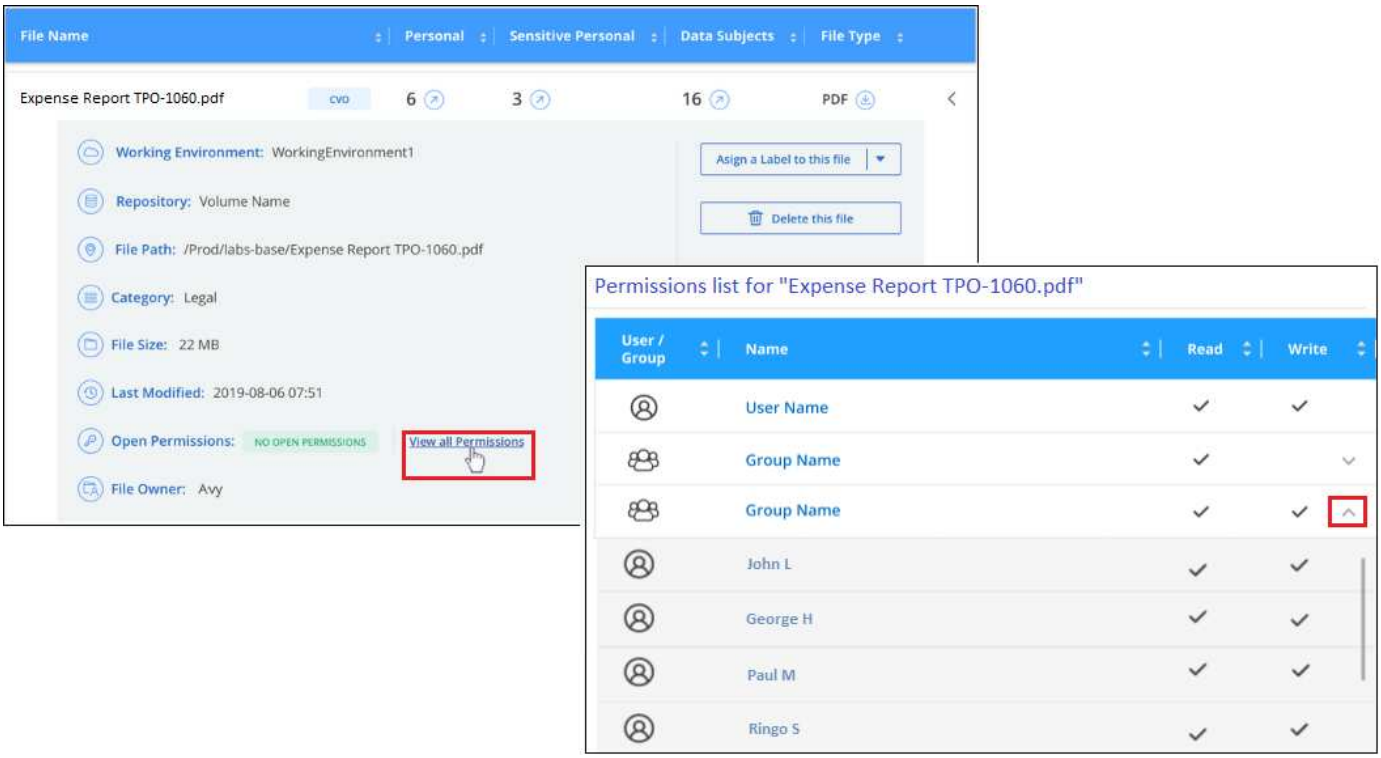
Além de mostrar o ambiente de trabalho e o volume em que o arquivo reside, os metadados mostram muito mais informações, incluindo as permissões de arquivo, o proprietário do arquivo e se há duplicatas desse arquivo. Esta informação é útil se você está planejando "Criar políticas"porque você pode ver todas as informações que você pode usar para filtrar seus dados.

Note que nem todas as informações estão disponíveis para todas as fontes de dados - apenas o que é apropriado para essa fonte de dados. Por exemplo, o nome do volume e as permissões não são relevantes para arquivos de banco de dados.

Exibir permissões para arquivos e diretórios

Para exibir uma lista de todos os usuários ou grupos que têm acesso a um arquivo ou a um diretório e os tipos de permissões que eles têm, clique em **Exibir todas as permissões**. Este botão está disponível apenas para dados em compartilhamentos CIFS.

Observe que se você vir SIDs (identificadores de segurança) em vez de nomes de usuários e grupos, você deve integrar seu ative Directory à classificação do BlueXP . "Veja como fazer isso".



Você pode clicar em para qualquer grupo para ver a lista de usuários que fazem parte do grupo.

Além disso, você pode clicar no nome de um usuário ou grupo e a página de investigação é exibida com o nome desse usuário ou grupo preenchido no filtro "permissões de usuário / grupo" 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 ver se arquivos duplicados estão sendo armazenados em seus sistemas de armazenamento. Isso é útil se você quiser identificar áreas onde você pode economizar espaço de armazenamento. Também pode ser útil garantir que certos arquivos com permissões específicas ou informações confidenciais não sejam duplicados desnecessariamente em seus sistemas de armazenamento.

Todos os seus arquivos (não incluindo bancos de dados) com 1 MB ou mais e que contenham informações pessoais ou confidenciais, são comparados para ver se há duplicatas. Você pode usar os filtros de página de investigação "tamanho do arquivo" junto com "Duplicates" para ver quais arquivos de um determinado intervalo de tamanho são duplicados em seu ambiente.

A classificação BlueXP usa a tecnologia de hash para determinar arquivos duplicados. Se qualquer arquivo tiver o mesmo código hash que outro arquivo, podemos ter 100% de certeza de que os arquivos são duplicados exatos - mesmo que os nomes dos arquivos sejam diferentes.

Você pode baixar a lista de arquivos duplicados e enviá-la para o administrador de armazenamento para que eles possam decidir quais arquivos, se houver, podem ser excluídos. Ou você pode "elimine o ficheiro" se você estiver confiante de que uma versão específica do arquivo não é necessária.

Ver todos os ficheiros duplicados

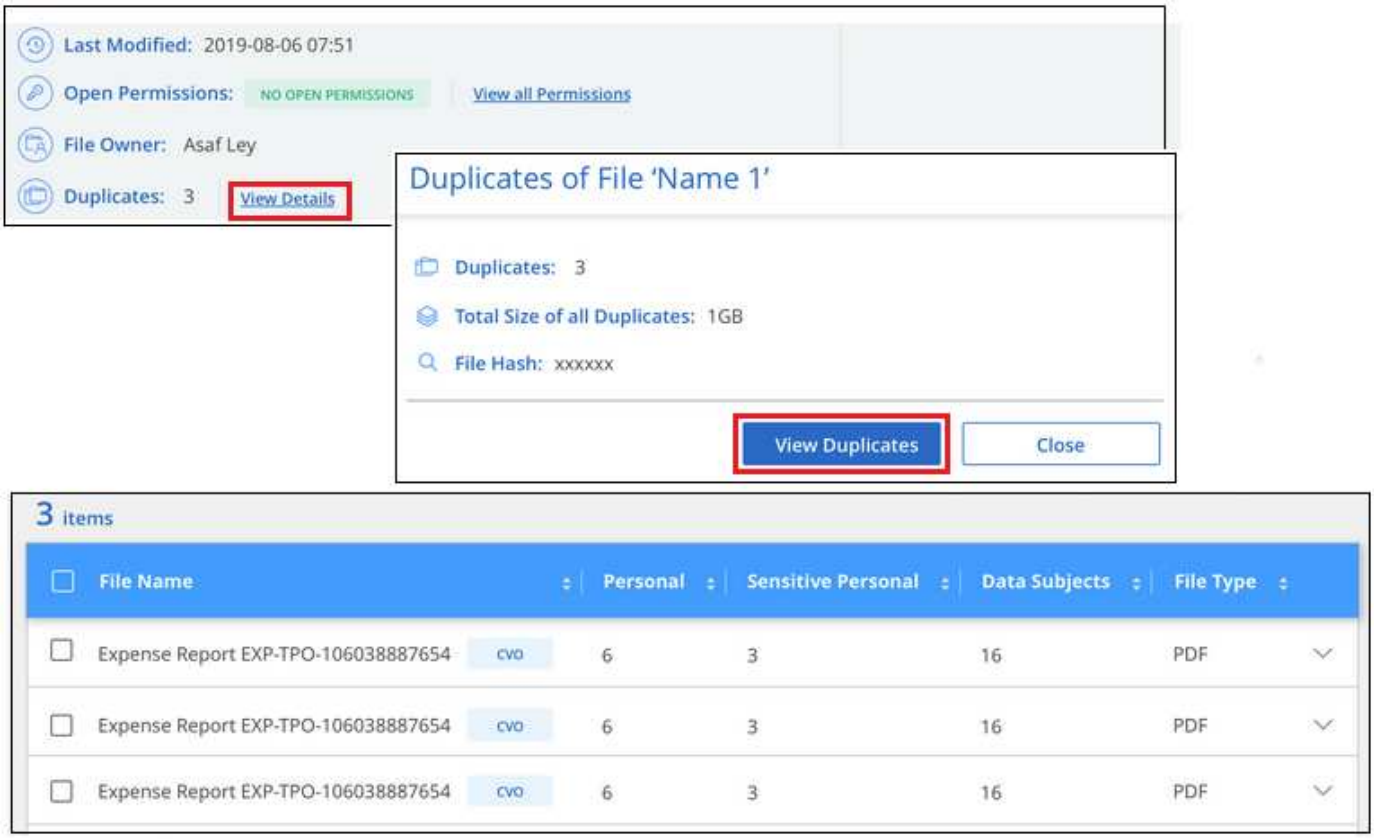
Se você quiser uma lista de todos os arquivos duplicados nos ambientes de trabalho e fontes de dados que você está digitalizando, você pode usar o filtro chamado **Duplicates > has duplicatas** na página Investigação de dados.

Todos os arquivos duplicados são exibidos na página de resultados.

Exibir se um arquivo específico é duplicado

Se você quiser ver se um único arquivo tem duplicatas, no painel resultados da investigação de dados, você pode clicar em para qualquer arquivo para exibir os metadados do arquivo. Se houver duplicatas de um determinado arquivo, essas informações serão exibidas ao lado do campo *Duplicates*.

Para exibir a lista de arquivos duplicados e onde eles estão localizados, clique em **Exibir detalhes**. Na próxima página, clique em **Exibir duplicados** para exibir os arquivos na página de investigação.



Você pode usar o valor "hash de arquivo" fornecido nesta página e inseri-lo diretamente na página de investigação para procurar um arquivo duplicado específico a qualquer momento - ou você pode usá-lo em uma Política.

Relatório de investigação de dados

O Relatório de Investigação de dados é um download do conteúdo filtrado da página Investigação de dados.

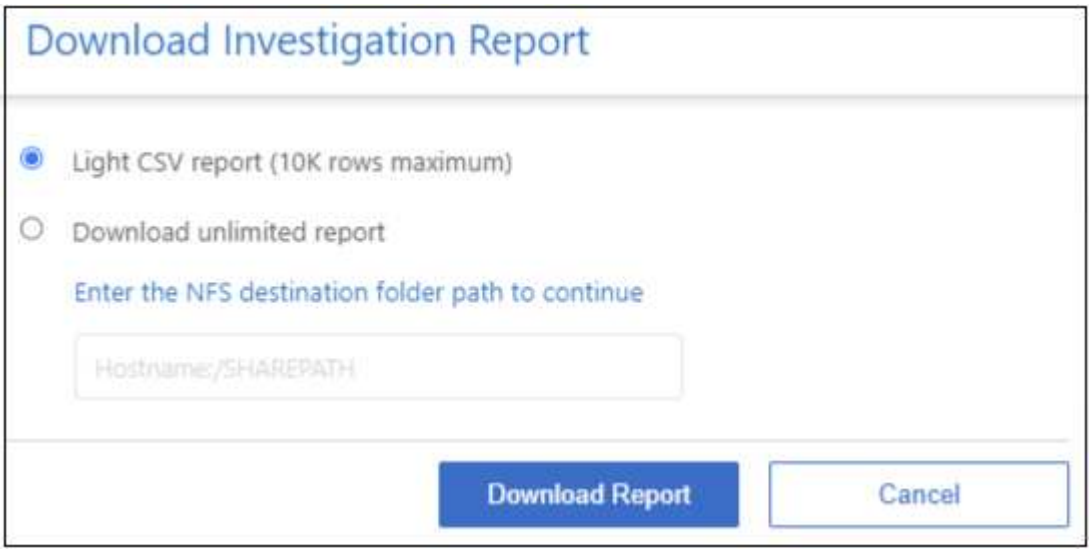
O relatório está disponível como um arquivo .CSV que você pode salvar na máquina local.

Pode haver até três arquivos de relatório baixados se a classificação do BlueXP estiver escaneando arquivos (dados não estruturados), diretórios (pastas e compartilhamentos de arquivos) e bancos de dados (dados estruturados).

Gerar o Relatório de Investigação de dados

Passos

1. Na página Investigação de dados, clique no botão na parte superior direita da página.
2. Selecione para fazer o download de um relatório .CSV dos dados e clique em **Download Report**.



Resultado

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

O que está incluído no Relatório de Investigação de dados

O **Relatório de dados de arquivos não estruturados** inclui as seguintes informações sobre seus arquivos:

- Nome do ficheiro
- Tipo de localização
- Nome do ambiente de trabalho
- Repositório de storage (por exemplo, um volume, bucket, compartilhamentos)
- Tipo de repositório
- Caminho do ficheiro
- Tipo de ficheiro
- Tamanho do ficheiro (em MB)
- Hora criada
- Modificado pela última vez
- Último acesso
- Proprietário do ficheiro
- Categoria
- Informações pessoais
- Informações pessoais sensíveis
- Abrir permissões
- Erro de análise de digitalização
- Data de deteção de eliminação

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

O **Relatório de dados de diretórios não estruturados** inclui as seguintes informações sobre suas pastas e compartilhamentos de arquivos:

- Tipo de ambiente de trabalho
- Nome do ambiente de trabalho
- Nome do diretório
- Repositório de armazenamento (por exemplo, uma pasta ou compartilhamentos de arquivo)
- Proprietário do diretório
- Hora criada
- Hora descoberta
- Modificado pela última vez
- Último acesso
- Abrir permissões
- Tipo de diretório

O **Relatório de dados estruturados** inclui as seguintes informações sobre as tabelas da sua base de dados:

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

Atribua políticas aos seus dados

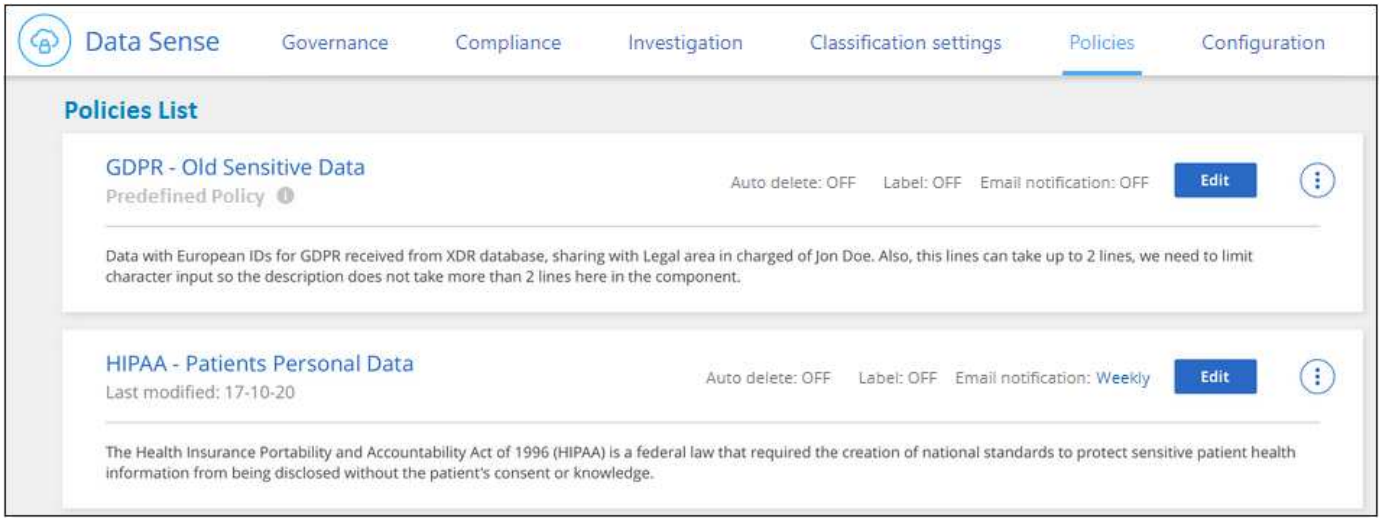
As políticas são como uma lista de favoritos de filtros personalizados que fornecem resultados de pesquisa na página de investigação para consultas de conformidade comumente solicitadas. A classificação BlueXP fornece um conjunto de políticas predefinidas com base em solicitações comuns do cliente. Você pode criar políticas personalizadas que fornecem resultados para pesquisas específicas para sua organização.

As políticas oferecem a seguinte funcionalidade:

- Políticas predefinidas Do NetApp com base nas solicitações do usuário
- Capacidade de criar suas próprias políticas personalizadas

- Inicie a página de investigação com os resultados das suas políticas com um clique

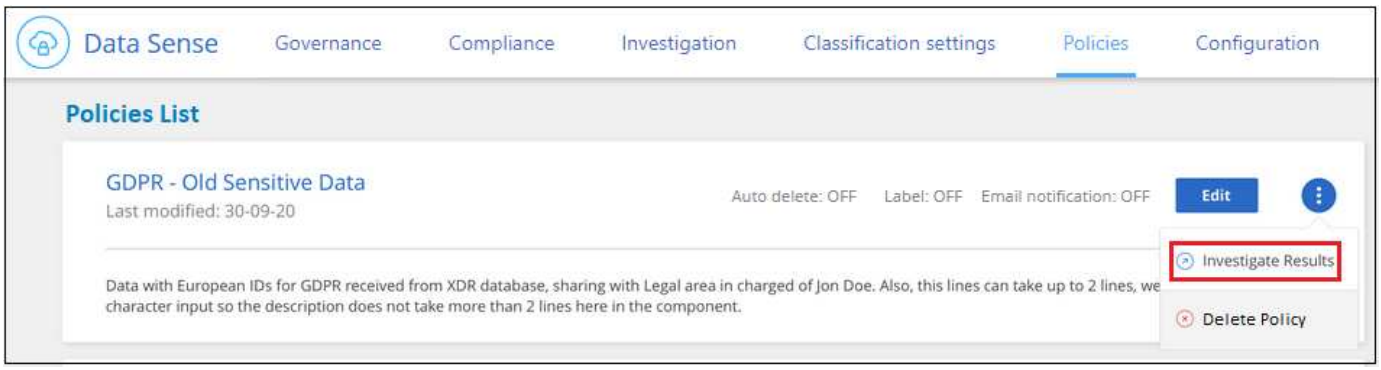
A guia **políticas** no Painel de conformidade lista todas as políticas predefinidas e personalizadas disponíveis nesta instância da classificação do BlueXP .



Além disso, as políticas aparecem na lista de filtros na página de investigação.

Exibir os resultados da política na página de investigação

Para exibir os resultados de uma política na página de investigação, clique no botão de uma política específica e selecione **investigar resultados**.

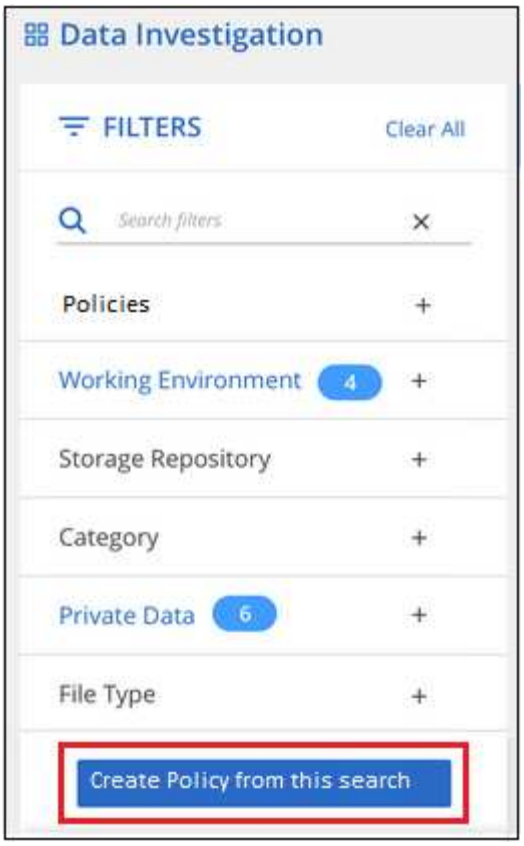


Crie políticas personalizadas

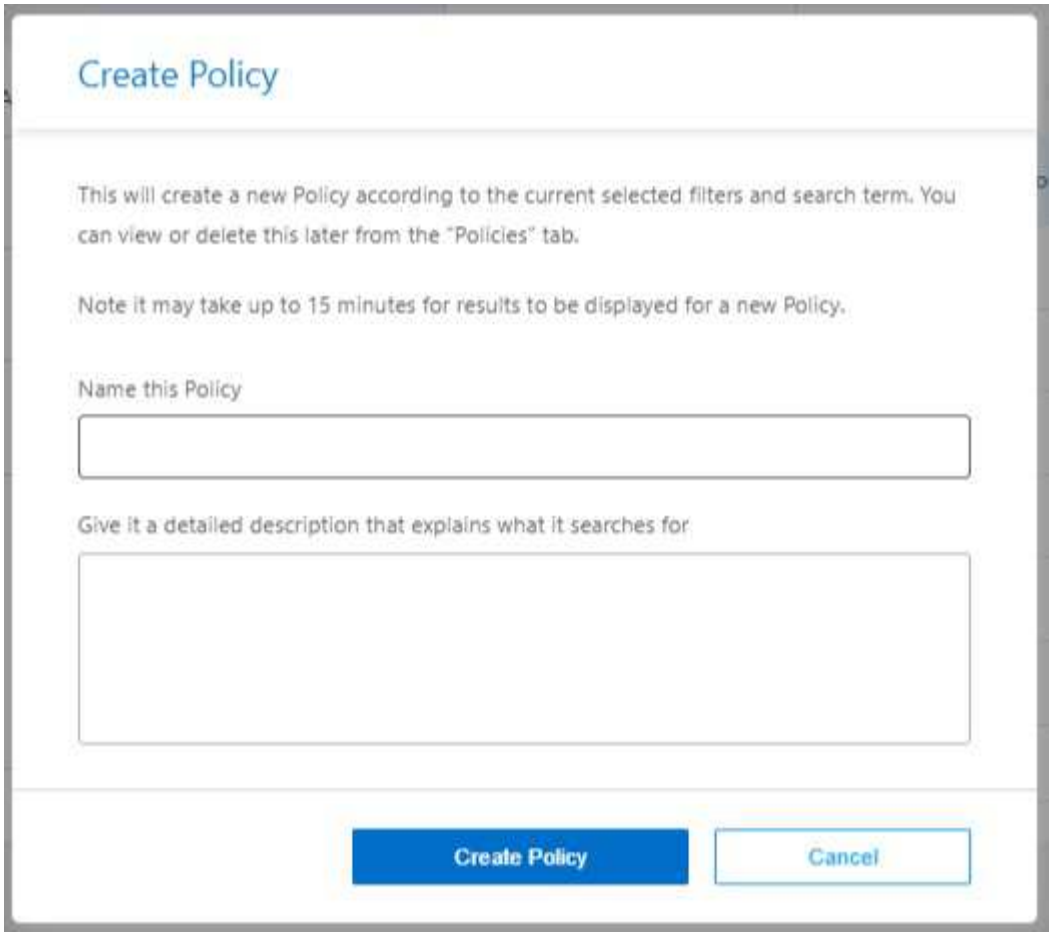
Você pode criar suas próprias políticas personalizadas que fornecem resultados para pesquisas específicas para sua organização. Os resultados são retornados para todos os arquivos e diretórios (compartilhamentos e pastas) que correspondem aos critérios de pesquisa.

Passos

1. Na página Investigação de dados, defina sua pesquisa selecionando todos os filtros que deseja usar. "Filtrando dados na página Investigação de dados"Consulte para obter detalhes.
2. Depois de ter todas as caraterísticas do filtro exatamente como você deseja, clique em **criar política a partir desta pesquisa**.



3. Nomeie a política e selecione outras ações que podem ser executadas pela política:
   a. Introduza um nome e uma descrição únicos.
   b. Opcionalmente, marque a caixa para excluir automaticamente arquivos que correspondam aos parâmetros da política.
   c. Clique em **criar política**.



Resultado

A nova política é exibida na guia políticas.

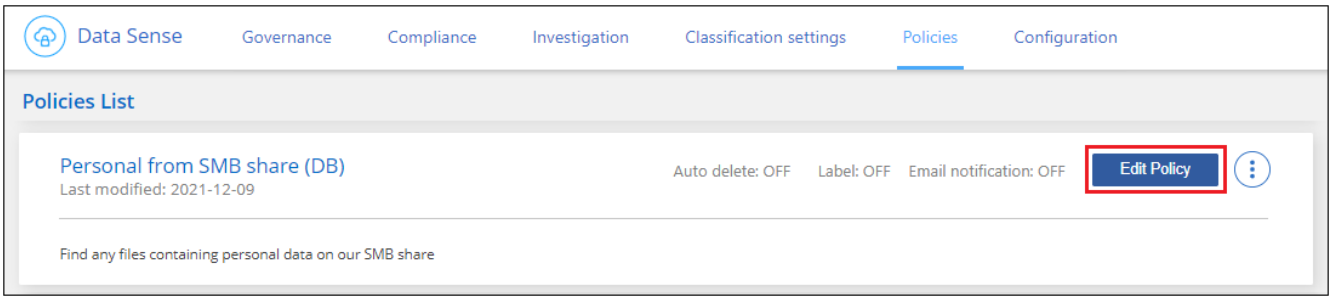
Editar políticas

Você pode modificar qualquer critério para uma política existente que você criou anteriormente. Isso pode ser especialmente útil se você quiser alterar a consulta (os itens que você definiu usando filtros) para adicionar ou remover certos parâmetros.

Para políticas predefinidas, você só pode modificar se as notificações de e-mail são enviadas e se os rótulos AIP são adicionados. Nenhum outro valor pode ser alterado.

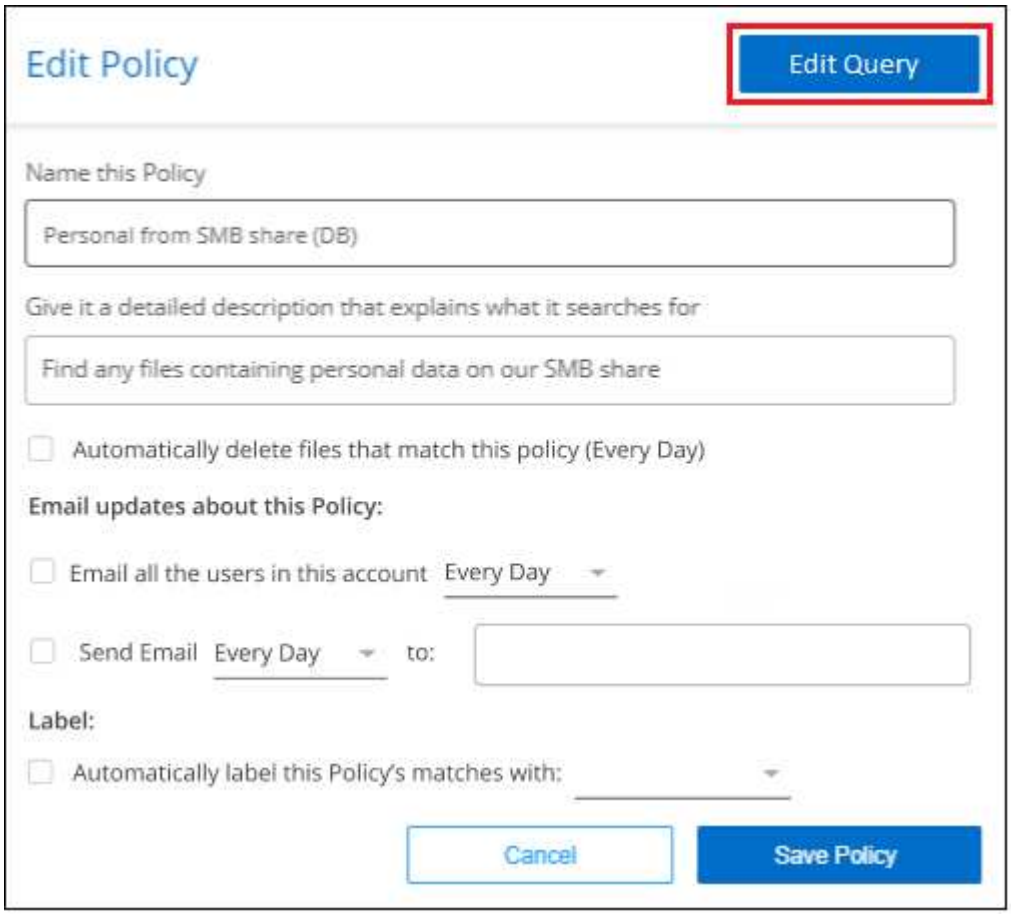
Passos

1. Na página Lista de políticas, clique em **Editar** para a Política que você deseja alterar.

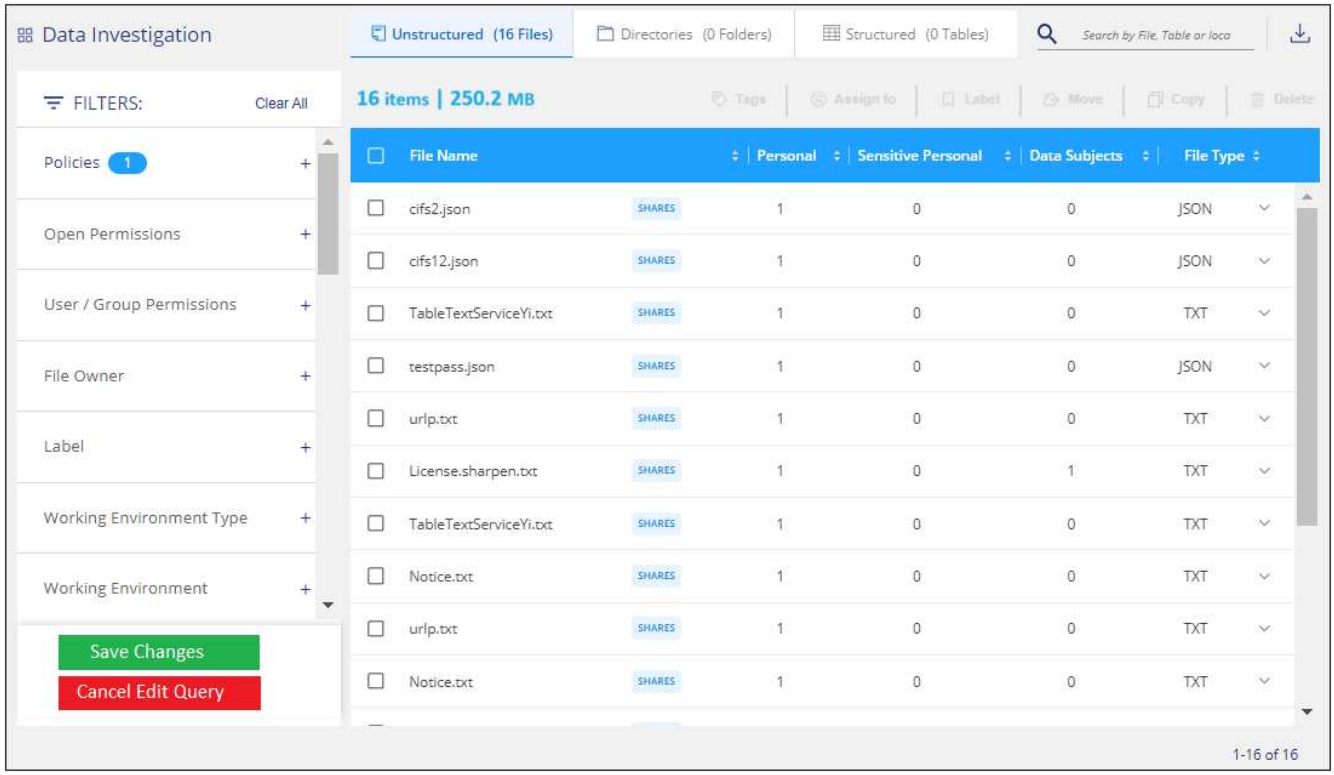


2. Se você quiser apenas alterar os itens nesta página (Nome, Descrição, se as notificações por e-mail são enviadas e se os rótulos AIP são adicionados), faça a alteração e clique em **Salvar política**.

   Se você quiser alterar os filtros para a consulta salva, clique em **Editar consulta**.



3. Na página de investigação que define essa consulta, edite a consulta adicionando, removendo ou personalizando os filtros e clique em **Salvar alterações** .



Resultado

A política é alterada imediatamente. Quaisquer ações definidas para que essa política envie um e-mail, adicione rótulos AIP ou exclua arquivos ocorrerão no próximo interno.

Eliminar políticas

Você pode excluir qualquer política personalizada que você criou se não precisar mais dela. Não é possível excluir nenhuma das políticas predefinidas.

Para excluir uma política, clique no botão de uma política específica, clique em **Excluir política** e, em seguida, clique em **Excluir política** novamente na caixa de diálogo de confirmação.

Lista de políticas predefinidas

A classificação BlueXP fornece as seguintes políticas definidas pelo sistema:

Nome	Descrição	Lógica
Dados privados - obsoletos ao longo de 7 anos	Arquivos contendo informações pessoais ou confidenciais, modificados pela última vez há mais de 7 anos.	Arquivos contendo informações pessoais ou confidenciais, modificados pela última vez há mais de 7 anos
Nomes dos titulares dos dados - Alto risco	Arquivos com mais de 50 nomes de titulares de dados.	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	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

Nome	Descrição	Lógica
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.	Arquivos com mais de 20 colunas pessoais ou DB com mais de 50% de suas linhas contendo pessoal
Dados pessoais sensíveis - Alto risco	Arquivos com mais de 20 identificadores de dados pessoais confidenciais, ou colunas de banco de dados com mais de 50% de suas linhas contendo dados pessoais confidenciais.	Arquivos com mais de 20 colunas pessoais sensíveis ou DB com mais de 50% de suas linhas contendo pessoal sensível

Exibir relatórios de conformidade

A classificação BlueXP 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 do BlueXP exibem dados de conformidade e governança para todos os ambientes de trabalho, bancos de dados e fontes de dados. Se desejar exibir relatórios que contenham dados apenas para alguns dos ambientes de trabalhoselecione esses ambientes de trabalho, .

- Os relatórios descritos nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma digitalização somente de mapeamento só podem gerar o Relatório de Mapeamento de dados.
- A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais sensíveis que a classificação BlueXP identifica. Deve sempre validar as informações através da revisão dos dados.

Relatório de avaliação de risco de privacidade

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

Status de conformidade

A pontuação de gravidade e a distribuição de dados, sejam eles não sensíveis, pessoais ou sensíveis.

Visão geral da avaliação

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

Sujeitos de dados nesta avaliação

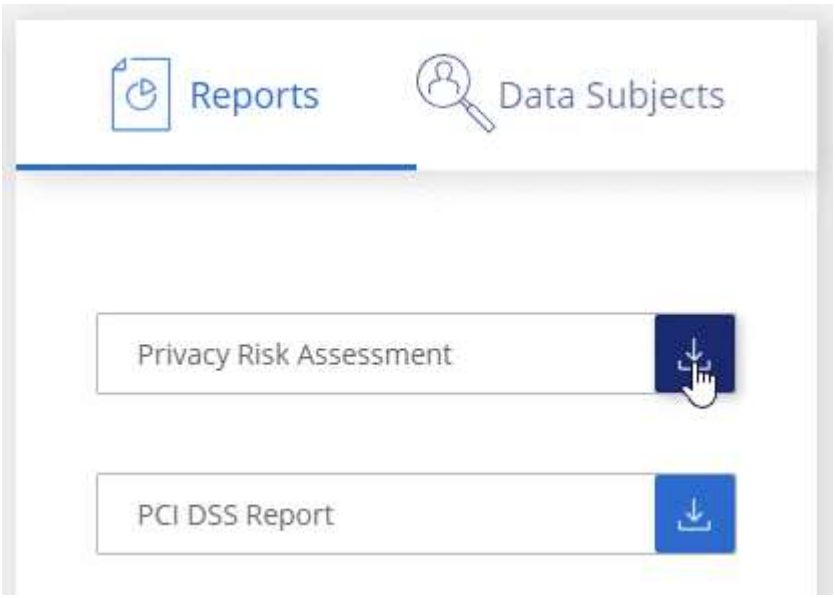
O número de pessoas, por localização, para as quais foram encontrados identificadores nacionais.

Gere o Relatório de avaliação de risco de privacidade

Vá para a guia conformidade para gerar o relatório.

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Compliance** e, em seguida, clique no ícone de download ao lado de **Privacy Risk Assessment** em **Reports**.



Resultado

A classificação BlueXP gera um relatório PDF que pode ser revisado e enviado para outros grupos conforme necessário.

Pontuação de gravidade

A classificação BlueXP calcula a pontuação de gravidade para o Relatório de avaliação de risco de Privacidade com base em três variáveis:

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

A lógica utilizada para determinar a pontuação é a seguinte:

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

Pontuação de gravidade	Lógica
8	Uma das variáveis é maior que 15%
9	Duas das variáveis são maiores que 15%
10	Três das variáveis são maiores que 15%

Relatório PCI DSS

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

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

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

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

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

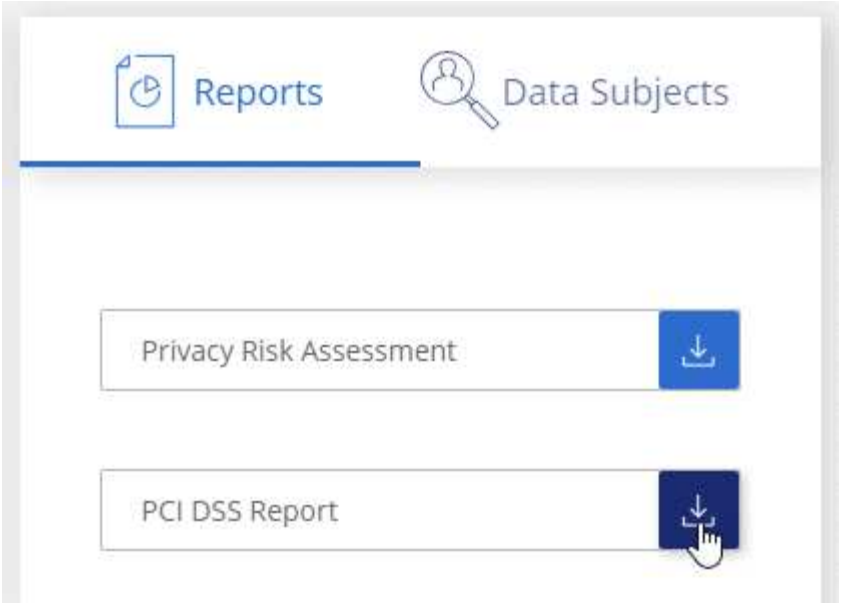
Distribuição de informações de cartão de crédito
: Os ambientes de trabalho onde as informações do cartão de crédito foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

Gere o Relatório PCI DSS

Vá para a guia conformidade para gerar o relatório.

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Compliance** e, em seguida, clique no ícone de download ao lado de **Relatório PCI DSS** em **relatórios**.



Resultado

A classificação BlueXP gera um relatório PDF que pode ser revisado e enviado para outros grupos conforme necessário.

Relatório HIPAA

O Relatório HIPAA (Health Insurance Portability and Accountability Act) pode ajudá-lo a identificar arquivos contendo informações de saúde. Criado para auxiliar a organização a obedecer às leis de privacidade de dados HIPAA. A informação que a classificação BlueXP procura inclui:

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

O relatório inclui as seguintes informações:

Visão geral

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

Criptografia

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

Proteção contra ransomware

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

Retenção

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

Distribuição de informações em Saúde

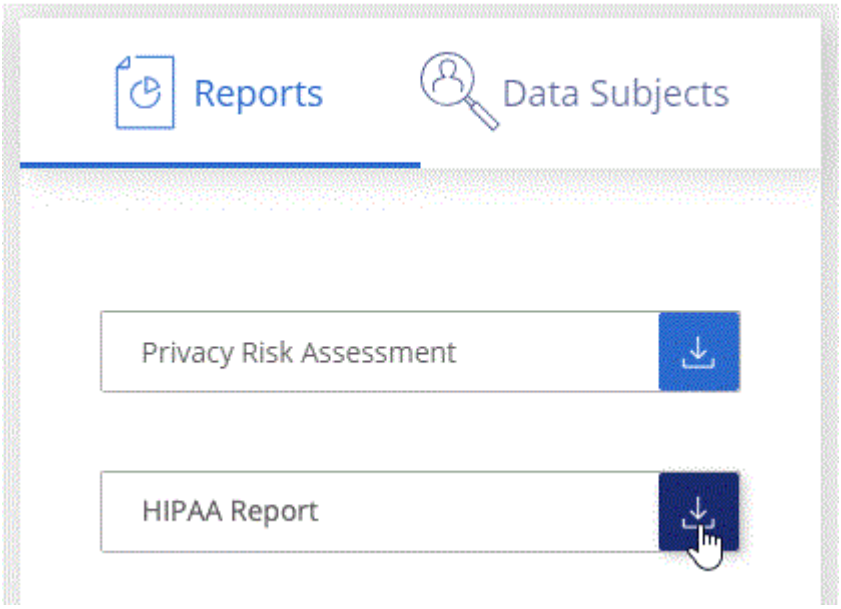
Os ambientes de trabalho onde as informações de integridade foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

Gerar o Relatório HIPAA

Vá para a guia conformidade para gerar o relatório.

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Compliance** e, em seguida, clique no ícone de download ao lado de **Relatório HIPAA** em **relatórios**.



Resultado

A classificação BlueXP gera um relatório PDF que pode ser revisado e enviado para outros grupos conforme necessário.

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

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

Você pode responder a um DSAR pesquisando o nome completo de um assunto ou identificador conhecido (como um endereço de e-mail) e, em seguida, baixando um relatório. O relatório foi projetado para auxiliar na exigência de sua organização em cumprir com o GDPR ou leis de privacidade de dados semelhantes.

Como a classificação BlueXP pode ajudá-lo a responder a um DSAR?

Quando você executa uma pesquisa de titular de dados, a classificação do BlueXP localiza todos os arquivos, buckets, OneDrive e contas do SharePoint que têm o nome ou identificador dessa pessoa nela. A classificação BlueXP verifica os dados pré-indexados mais recentes para o nome ou identificador. Não inicia

uma nova digitalização.

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

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

PESQUISE por titulares de dados e transfira relatórios

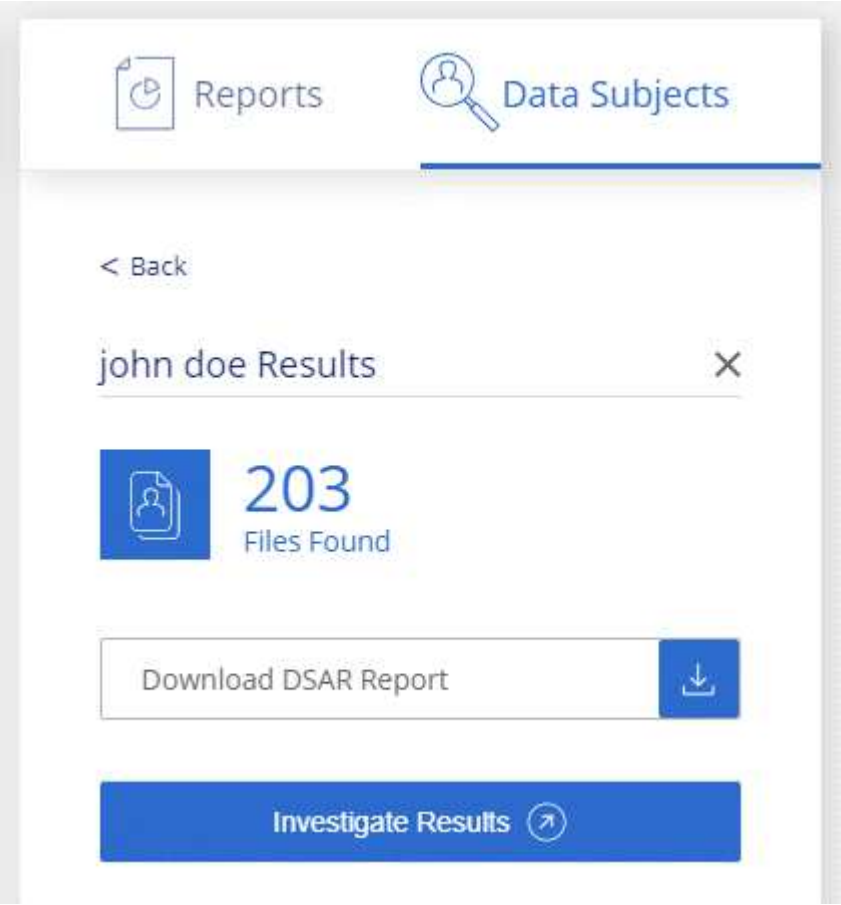
Procure o nome completo ou identificador conhecido do titular dos dados e, em seguida, transfira um relatório de lista de ficheiros ou relatório DSAR. Pode pesquisar por "qualquer tipo de informação pessoal".

O inglês, o alemão, o japonês e o espanhol são suportados ao procurar os nomes dos titulares dos dados. O suporte para mais idiomas será adicionado mais tarde.

Passos

1. No menu BlueXP , clique em **Governança > classificação**.
2. Clique em **Assunto de dados**.
3. Procure o nome completo ou identificador conhecido do titular dos dados.

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



4. Escolha uma das opções disponíveis:

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

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

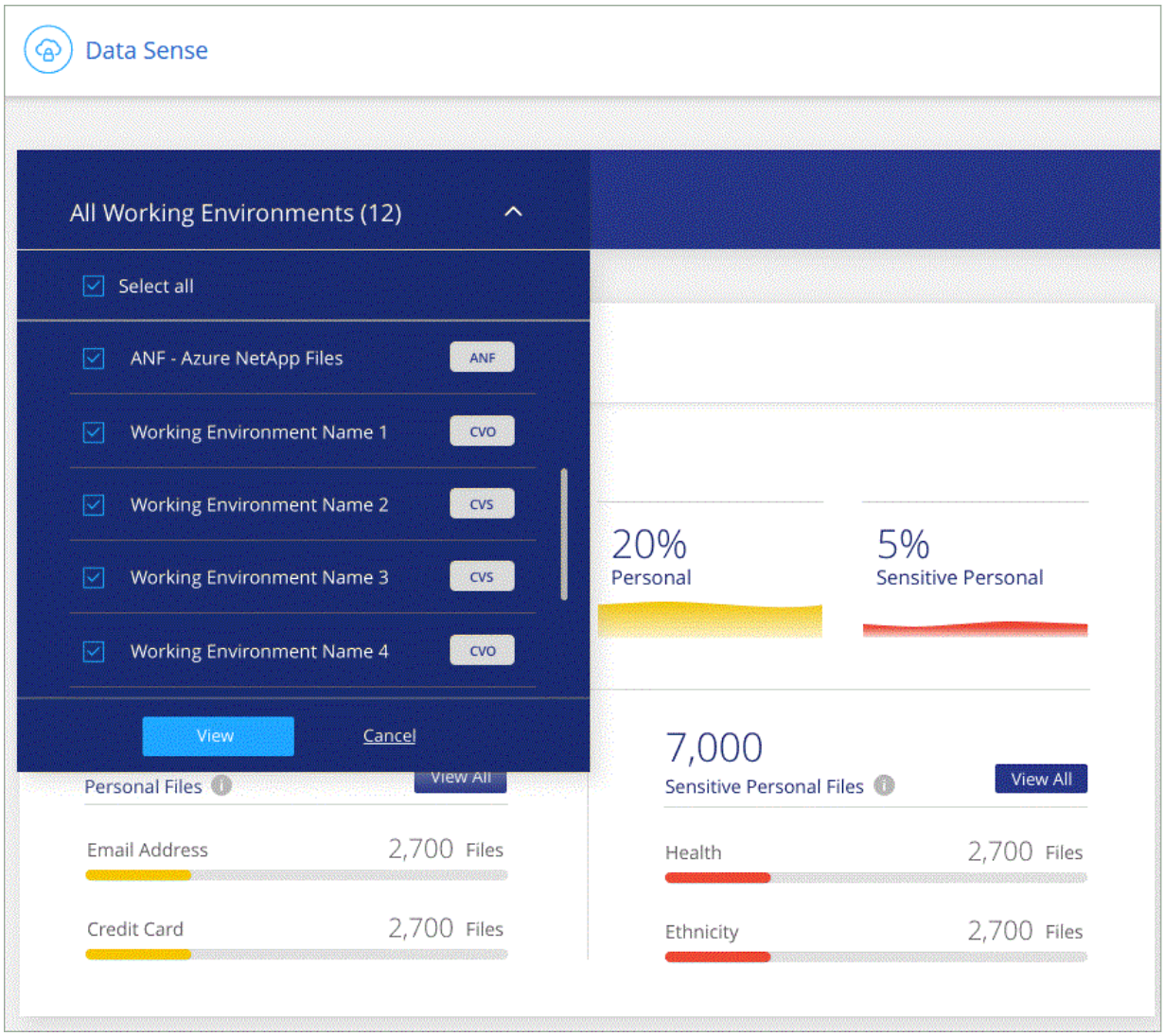
Selecione os ambientes de trabalho para relatórios

Você pode filtrar o conteúdo do painel de conformidade de classificação do BlueXP para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, a classificação do BlueXP escoa os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

Passos

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


Data Sense
All Working Environments (12)
Select all
ANF - Azure NetApp Files
ANF
Working Environment Name 1
CVO
Working Environment Name 2
CVS
Working Environment Name 3
CVS
Working Environment Name 4
CVO
View
Cancel
20%
Personal
5%
Sensitive Personal
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
7,000
Sensitive Personal Files
View All
Health
2,700 Files
Ethnicity
2,700 Files

Gerir a classificação BlueXP

Excluir diretórios específicos de exames de classificação do BlueXP

Se você quiser que a classificação do BlueXP exclua os dados de digitalização que residem em determinados diretórios de origem de dados, você pode adicionar esses nomes de diretório a um arquivo de configuração. Depois de aplicar esta alteração, o motor de classificação BlueXP excluirá os dados de digitalização nesses diretórios.

Observe que a classificação BlueXP é configurada por padrão para excluir dados instantâneos de volume de digitalização, pois esse conteúdo é idêntico ao conteúdo do volume.

Esta funcionalidade está disponível na classificação BlueXP versão 1,29 e superior (a partir de março de 2024).

Fontes de dados compatíveis

A exclusão de diretórios específicos de varreduras de classificação do BlueXP é compatível com compartilhamentos NFS e CIFS nas seguintes fontes de dados:

- ONTAP no local
- Cloud Volumes ONTAP
- Amazon FSX para NetApp ONTAP
- Azure NetApp Files
- Compartilhamentos de arquivo geral

Defina os diretórios a excluir da digitalização

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

- Você pode excluir um máximo de 50 caminhos de diretório por sistema de classificação BlueXP .
- A exclusão de caminhos de diretório pode afetar os tempos de digitalização.

Passos

1. No sistema de classificação BlueXP , vá para "/opt/NetApp/config/custom_Configuration" e abra o `data_provider.yaml` arquivo .
2. Na seção "data_Providers", na linha "Excluir:", digite os caminhos do diretório a serem excluídos. Por exemplo:

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

Não altere mais nada neste arquivo.

3. Salve as alterações no arquivo.
4. Vá para "/opt/NetApp/Datasense/Tools/customer_Configuration/data_Providers" e execute o seguinte script:

```
update_data_providers_from_config_file.sh
```

Este comando compromete os diretórios a serem excluídos da digitalização para o mecanismo de classificação.

Resultado

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

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

Exemplos

Configuração 1:

Todas as pastas que contêm "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/folder1
- /CVO1/folder1name
- /CVO1/folder10
- /CVO1/*folder1
- /CVO1/-folder1name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Exemplos de caminhos que não serão excluídos:

- /CVO1/*pasta
- /CVO1/foldername
- /CVO22/*folder20

Configuração 2:

Todas as pastas que contenham "*folder1" apenas no início do nome serão excluídas.

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

Resultados esperados para caminhos que serão excluídos:

- /CVO/*folder1
- /CVO/*folder1name
- /CVO/*folder10

Exemplos de caminhos que não serão excluídos:

- /CVO/folder1
- /CVO/folder1name
- /CVO/not*folder10

Configuração 3:

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

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

Resultados esperados para caminhos que serão excluídos:

- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Exemplos de caminhos que não serão excluídos:

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

Escapando carateres especiais em nomes de pastas

Se você tiver um nome de pasta que contém um dos seguintes carateres especiais e quiser excluir dados nessa pasta de serem digitalizados, você precisará usar a sequência de escape antes do nome da pasta.

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

Caminho na fonte: `/project/*not_to_scan`

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

Veja a lista de exclusão atual

É possível que o conteúdo do `data_provider.yaml` arquivo de configuração seja diferente do que realmente foi confirmado após a execução `update_data_providers_from_config_file.sh` do script. Para exibir a lista atual de diretórios excluídos da verificação de classificação do BlueXP , execute o seguinte comando de "/opt/NetApp/Datasense/Tools/customer_Configuration/data_Providers":

```
get_data_providers_configuration.sh
```

Defina IDs de grupo adicionais como abertos à organização

Quando os 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 estão "abertos à organização". Se alguns IDs de grupo (GIDs) não estiverem configurados inicialmente com o nível de permissão "Open to Organization", você pode adicionar essa permissão ao GID para que quaisquer arquivos e pastas que tenham esse GID anexado sejam considerados "abertos à organização".

Depois que você fizer essa alteração e a classificação do BlueXP refizer seus arquivos e pastas, todos os arquivos e pastas que tenham esses IDs de grupo anexados mostrarão essa permissão na página Detalhes da investigação, e eles também aparecerão nos relatórios onde você estiver exibindo permissões de arquivo.

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

Adicione a permissão "Open to Organization" às IDs de grupo

É necessário ter os números de ID do grupo (GIDs) antes de iniciar esta tarefa.

Passos

1. No sistema de classificação BlueXP , vá para "/opt/NetApp/config/custom_Configuration" e abra o `data_provider.yaml` arquivo .
2. Na linha "Organization_group_IDs: []" adicione as 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. Vá para "/opt/NetApp/Datasense/Tools/customer_Configuration/data_Providers" e execute o seguinte script:

```
update_data_providers_from_config_file.sh
```

Este comando compromete as permissões de ID de grupo revisadas ao mecanismo de classificação.

Resultado

Todas as verificações subsequentes dos seus dados identificarão ficheiros ou pastas que tenham estes 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 no passado usando essas mesmas etapas. A lista revisada de IDs de grupo será atualizada depois que você executar o script para confirmar suas alterações.

Exibir a lista atual de IDs de grupo

É possível que o conteúdo do `data_provider.yaml` arquivo de configuração seja diferente do que realmente foi confirmado depois de executar o `update_data_providers_from_config_file.sh` script. Para exibir a lista atual de IDs de grupo que você adicionou à classificação BlueXP , execute o seguinte comando de "/opt/NetApp/Datasense/Tools/customer_Configuration/data_Providers":

```
get_data_providers_configuration.sh
```

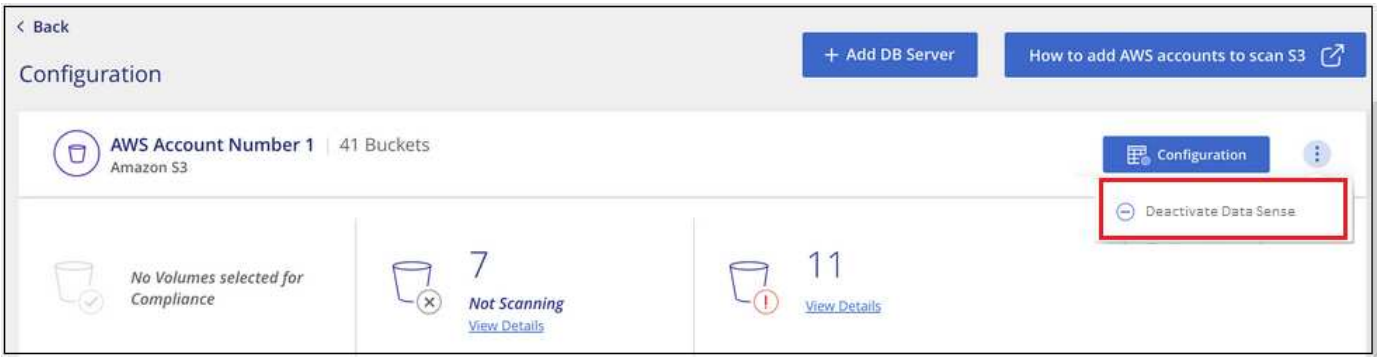
Remover fontes de dados da classificação BlueXP

Se necessário, você pode impedir que a classificação do BlueXP digitalize um ou mais ambientes de trabalho, bancos de dados ou grupos de compartilhamento de arquivos.

Desativar verificações de conformidade para um ambiente de trabalho

Quando você desativa as varreduras, a classificação BlueXP não verifica mais os dados no ambiente de trabalho e remove os insights de conformidade indexados da instância de classificação BlueXP (os dados do próprio ambiente de trabalho não são excluídos).

1. Na página *Configuration*, clique no botão na linha do ambiente de trabalho e, em seguida, clique em **Deactivate Data Sense**.



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

Remova um banco de dados da classificação BlueXP

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

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

Remova um grupo de compartilhamentos de arquivo da classificação BlueXP

Se você não quiser mais analisar arquivos de usuário de um grupo de compartilhamentos de arquivos, você pode excluir o Grupo de compartilhamentos de arquivos da interface de classificação do BlueXP e parar todas as verificações.

Passos

1. Na página *Configuration*, clique no botão na linha do Grupo de compartilhamentos de arquivos e clique em **Remover grupo de compartilhamentos de arquivos**.

2. Clique em **Excluir Grupo de compartilhamentos** na caixa de diálogo de confirmação.

Desinstalar a classificação BlueXP

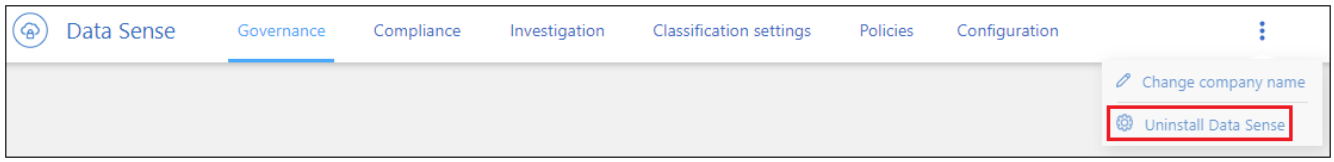
Você pode desinstalar o software de classificação BlueXP para solucionar problemas ou remover permanentemente o software do host. A exclusão da instância também exclui os discos associados onde residem os dados indexados - todas as informações que a classificação BlueXP digitalizada serão excluídas permanentemente.

As etapas que você precisa usar dependem da implantação da classificação do BlueXP na nuvem ou em um host local.

Desinstalar a classificação do BlueXP de uma implantação na nuvem

Você pode desinstalar e excluir a instância de classificação do BlueXP do ambiente do provedor de nuvem se não quiser mais usar a classificação do BlueXP .

1. Na parte superior da página de classificação do BlueXP , clique em **Desinstalar o Sensor de dados**.



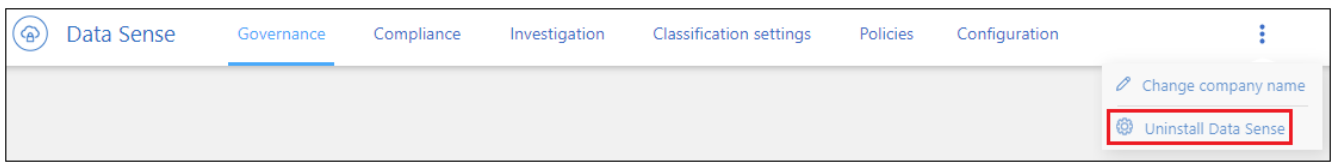
2. Na caixa de diálogo *Uninstall Data Sense*, digite **uninstall** para confirmar que deseja desconetar a instância de classificação BlueXP do conetor BlueXP e clique em **Uninstall**.
3. Vá para o console do seu provedor de nuvem e exclua a instância de classificação do BlueXP . A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

   Isso exclui a instância e todos os dados associados que foram coletados pela classificação BlueXP .

Desinstalar a classificação do BlueXP de uma implantação local

Você pode desinstalar a classificação do BlueXP de um host se não quiser mais usar a classificação do BlueXP ou se tiver um problema que exija a reinstalação.

1. Na parte superior da página de classificação do BlueXP , clique em **Desinstalar o Sensor de dados**.



2. Na caixa de diálogo *Uninstall Data Sense*, digite **uninstall** para confirmar que deseja desconetar a instância de classificação BlueXP do conetor BlueXP e clique em **Uninstall**.
3. Para desinstalar o software do host, execute o `cleanup.sh` script na máquina host, por exemplo:

```
cleanup.sh
```

Consulte como "Faça login na máquina host de classificação BlueXP ".

Funcionalidades obsoletas

Classificação BlueXP funcionalidades obsoletas

A classificação BlueXP está disponível como uma capacidade principal dentro do BlueXP sem nenhum custo adicional. Ao incluir a classificação do BlueXP como uma funcionalidade principal do BlueXP disponível para todos os clientes, o NetApp permite que você acesse o gerenciamento de dados personalizado com recursos principais.

Existem alguns recursos e funcionalidades que são obsoletos na versão do núcleo do BlueXP a partir da versão 1,31 e posterior e ainda são suportados nas versões anteriores 1,30 e anteriores.

Fontes de dados compatíveis

Fonte de dados	Versões antigas 1,30 e anteriores	BlueXP core versões 1,31 e posteriores
Cloud Volumes ONTAP (implantado na AWS, Azure ou GCP)	Sim	Sim
Clusters ONTAP on-premises	Sim	Sim
StorageGRID	Sim	Sim
Azure NetApp Files	Sim	Sim
Amazon FSX para ONTAP	Sim	Sim
Google Cloud NetApp volumes	Sim	Sim
Cloud Volumes Service para Google Cloud	Sim	Sim
Bancos de dados	Sim	Sim
Amazon S3	Sim	Não
Google Cloud Storage	Sim	Não
OneDrive	Sim	Não
SharePoint Online	Sim	Não
SharePoint no local (SharePoint Server)	Sim	Não
Google Drive	Sim	Não

Recursos de conformidade

Recurso	Versões antigas 1,30 e anteriores	BlueXP core versões 1,31 e posteriores
Identificar informações pessoais identificáveis (PII)	Sim	Sim
Identificar informações pessoais confidenciais	Sim	Sim

Recurso	Versões antigas 1,30 e anteriores	BlueXP core versões 1,31 e posteriores
Responder às solicitações de acesso do titular dos dados (DSAR)	Sim	Sim
Crie uma lista personalizada de "dados pessoais" identificados	Sim	Não
Notifique os usuários por e-mail quando os arquivos contêm certas PII. (Você define esses critérios "Políticas"usando .)	Sim	Não
Use filtros de nível de diretório	Sim	Sim
Use a análise PII no nível do diretório	Sim	Não

Recursos para gerenciar seus dados

Recurso	Versões antigas 1,30 e anteriores	BlueXP core versões 1,31 e posteriores
Mover, copiar e excluir arquivos de origem	Sim	Não
Categorize os dados usando as etiquetas de status	Sim	Não
Categorize os dados usando rótulos AIP	Sim	Não
Atribua arquivos aos usuários	Sim	Não
Volte a digitalizar os dados sob demanda	Sim	Não
Crie classificadores personalizados	Sim	Não
Excluir diretórios da digitalização	Sim	Sim
Procure nomes dentro de arquivos	Sim	Sim
Exportar dados para NFS da investigação	Sim	Não
Exportar dados para CSV da investigação	Sim	Sim
Suporte vários scanners	Sim	Não
Integrar o ative Directory	Sim	Sim
Use a análise de permissões e filtros	Sim	Sim
Use o cartão de arquivo	Sim	Sim
Utilize o mapa de calor	Sim	Sim
Use ações no Dashboard e no cartão de arquivo	Sim	Não
Use o log de auditoria de acesso a arquivos	Sim	Não
Ative o acesso a ficheiros a partir da página Configuração	Sim	Não
Use certas políticas predefinidas	Sim	Não

Implantar depreciações de classificação do BlueXP

Instale a classificação BlueXP em vários hosts para grandes configurações sem acesso à Internet

Conclua algumas etapas para instalar a classificação BlueXP em vários hosts em um site local que não tenha acesso à Internet - também conhecido como *modo privado*. Este tipo de instalação é perfeito para seus sites seguros.

Para configurações muito grandes em que você estará verificando petabytes de dados em sites sem acesso à Internet, você pode incluir vários hosts para fornecer poder de processamento adicional. Ao usar vários sistemas host, o sistema primário é chamado de nó *Manager* e os sistemas adicionais que fornecem poder de processamento extra são chamados de *nó do scanner*.

Siga estas etapas ao instalar o software de classificação BlueXP em vários hosts locais em um ambiente off-line.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

O que você vai precisar

- Verifique se todos os seus sistemas Linux para os nós de Gerenciador e scanner atendem aos requisitos do host.
- Verifique se você instalou os dois pacotes de software pré-requisito (Docker Engine ou Podman, e Python 3).
- Certifique-se de que você tem Privileges root nos sistemas Linux.
- Verifique se seu ambiente off-line atende às permissões e conetividade necessárias.
- Você deve ter os endereços IP dos hosts do nó do scanner que você pretende usar.
- As seguintes portas e protocolos devem estar ativados em todos os hosts:

Porta	Protocolos	Descrição
2377	TCP	Comunicações de gerenciamento de cluster
7946	TCP, UDP	Comunicação entre nós
4789	UDP	Sobreponha o tráfego de rede
50	ESP	Tráfego de rede de sobreposição IPsec criptografada (ESP)
111	TCP, UDP	Servidor NFS para compartilhamento de arquivos entre os hosts (necessário de cada nó do scanner para nó do gerente)
2049	TCP, UDP	Servidor NFS para compartilhamento de arquivos entre os hosts (necessário de cada nó do scanner para nó do gerente)

Passos

1. Siga as etapas de 1 a 8 do "Instalação de host único"no nó do gerente.
2. Como mostrado na etapa 9, quando solicitado pelo instalador, você pode inserir os valores necessários em uma série de prompts, ou você pode fornecer os parâmetros necessários como argumentos de linha

de comando para o instalador.

Além das variáveis disponíveis para uma instalação de um único host, uma nova opção **-n <node_ip>** é usada para especificar os endereços IP dos nós do scanner. Vários IPs de nó são separados por uma vírgula.

Por exemplo, este comando adiciona 3 nós de scanner:
`sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy --darksite`

3. Antes da conclusão da instalação do nó do gerente, uma caixa de diálogo exibe o comando de instalação necessário para os nós do scanner. Copie o comando (por exemplo: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) E salve-o em um arquivo de texto.
4. No host **Each** do nó do scanner:
   a. Copie o arquivo do instalador do Data Sense (**cc_onprem_installer.tar.gz**) para a máquina host.
   b. Descompacte o arquivo do instalador.
   c. Cole e execute o comando que você copiou na etapa 3.

      Quando a instalação termina em todos os nós do scanner e eles foram Unidos ao nó do gerente, a instalação do nó do gerente também termina.

Resultado

O instalador de classificação BlueXP termina a instalação de pacotes e Registra a instalação. A instalação pode levar de 15 a 25 minutos.

O que vem a seguir

Na página Configuração, pode selecionar o local "Clusters ONTAP no local" e o local "bancos de dados" que pretende digitalizar.

Analisar descontinuações de dados

Verifique os buckets do Amazon S3

A classificação do BlueXP pode analisar seus buckets do Amazon S3 para identificar os dados pessoais e confidenciais que residem no armazenamento de objetos do S3. A classificação BlueXP pode verificar qualquer intervalo na conta, independentemente de ter sido criado para uma solução NetApp.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Início rápido

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

1 Configure os requisitos do S3 em seu ambiente de nuvem

Garanta que seu ambiente de nuvem atenda aos requisitos de classificação do BlueXP , incluindo a preparação de uma função do IAM e a configuração da conectividade da classificação do BlueXP para o S3. Veja a lista completa.

2 Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3 Ative a classificação BlueXP no seu ambiente de trabalho S3

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

4 Selecione os intervalos para digitalizar

Selecione os intervalos que você gostaria de digitalizar e a classificação BlueXP começará a digitalizá-los.

Rever os pré-requisitos do S3

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

Configure uma função do IAM para a instância de classificação do BlueXP

A classificação do BlueXP precisa de permissões para se conetar aos buckets do S3 em sua conta e digitalizá-los. Configure uma função do IAM que inclua as permissões listadas abaixo. O BlueXP solicita que você selecione uma função do IAM ao ativar a classificação do BlueXP no ambiente de trabalho do Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Fornecer conetividade da classificação BlueXP ao Amazon S3

A classificação BlueXP precisa de uma conexão com o Amazon S3. A melhor maneira de fornecer essa conexão é por meio de um VPC Endpoint ao serviço S3. Para obter instruções, "Documentação da AWS: Criando um endpoint do Gateway" consulte .

Ao criar o endpoint VPC, certifique-se de selecionar a tabela de região, VPC e rota que corresponde à instância de classificação do BlueXP . Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que permita o tráfego para o endpoint S3. Caso contrário, a classificação BlueXP não pode se conetar ao serviço S3.

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

Uma alternativa é fornecer a conexão usando um NAT Gateway.

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

Implantando a instância de classificação do BlueXP

"Implantar a classificação BlueXP no BlueXP " se ainda não houver uma instância implantada.

Você precisa implantar a instância usando um conetor implantado na AWS para que o BlueXP descubra automaticamente os buckets do S3 nessa conta da AWS e os exiba em um ambiente de trabalho do Amazon S3.

Observação: a implantação da classificação BlueXP em um local local local não é suportada atualmente ao digitalizar buckets do S3.

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

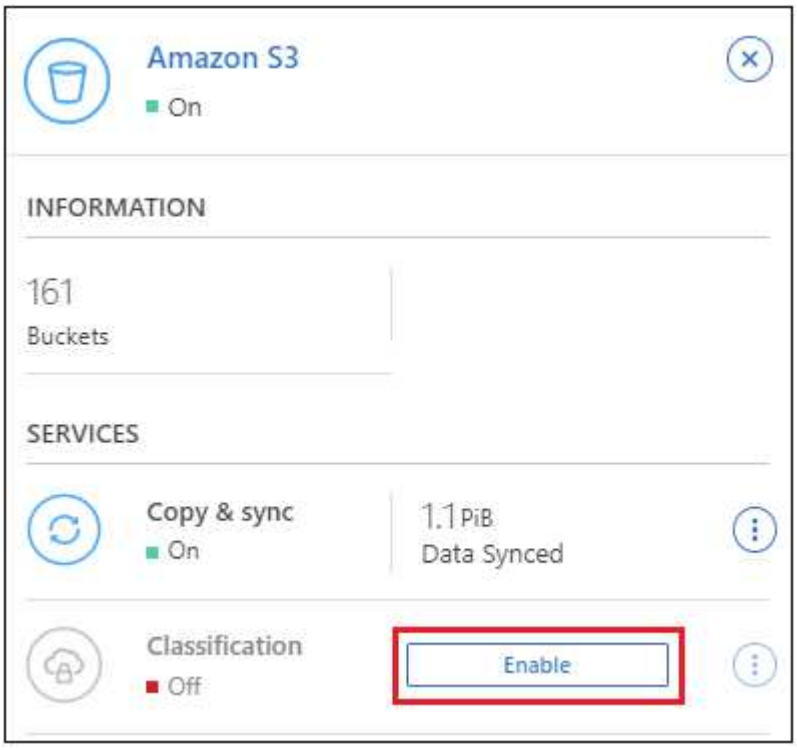
Ativar a classificação BlueXP no seu ambiente de trabalho S3

Ative a classificação BlueXP no Amazon S3 depois de verificar os pré-requisitos.

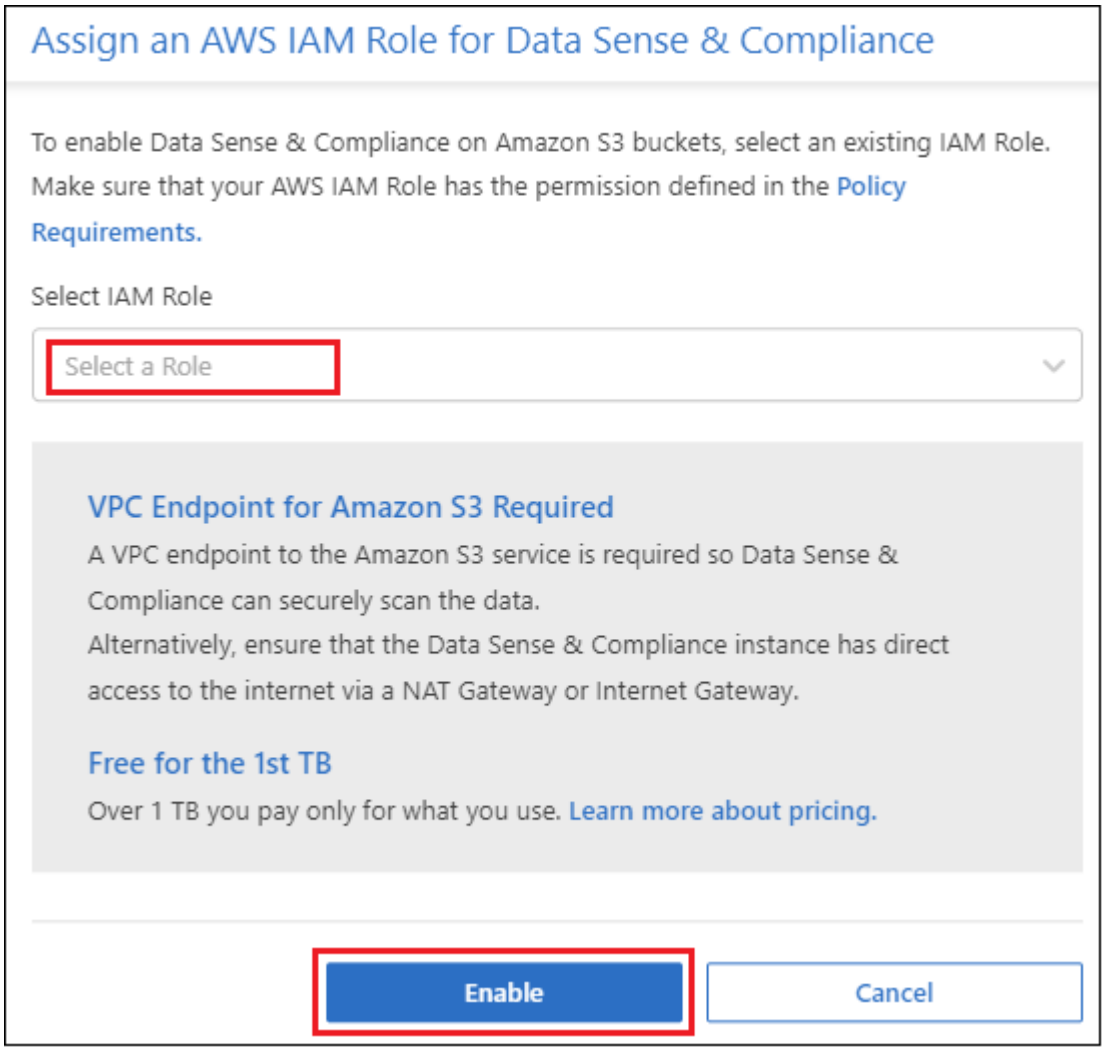
Passos

1. No menu de navegação esquerdo do BlueXP , clique em **armazenamento > tela**.
2. Selecione o ambiente de trabalho do Amazon S3.

3. No painel Serviços à direita, clique em **Ativar** ao lado de **classificação**.



4. Quando solicitado, atribua uma função do IAM à instância de classificação do BlueXP que tem as permissões necessárias.



5. Clique em **Ativar**.

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

Resultado

O BlueXP atribui a função do IAM à instância.

Ativar e desativar verificações de conformidade em buckets do S3

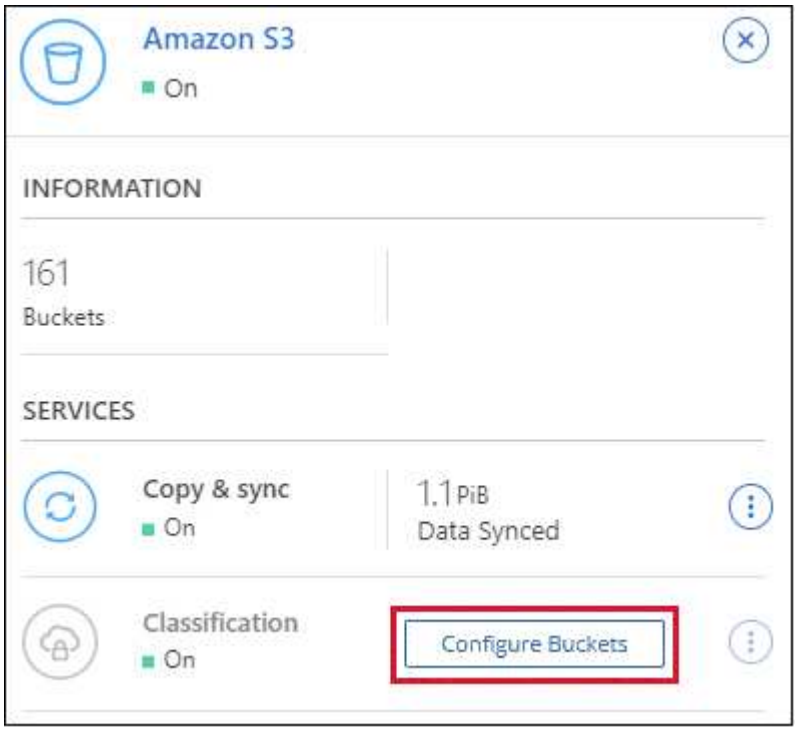
Depois que o BlueXP ativar a classificação do BlueXP no Amazon S3, a próxima etapa é configurar os buckets que você deseja verificar.

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

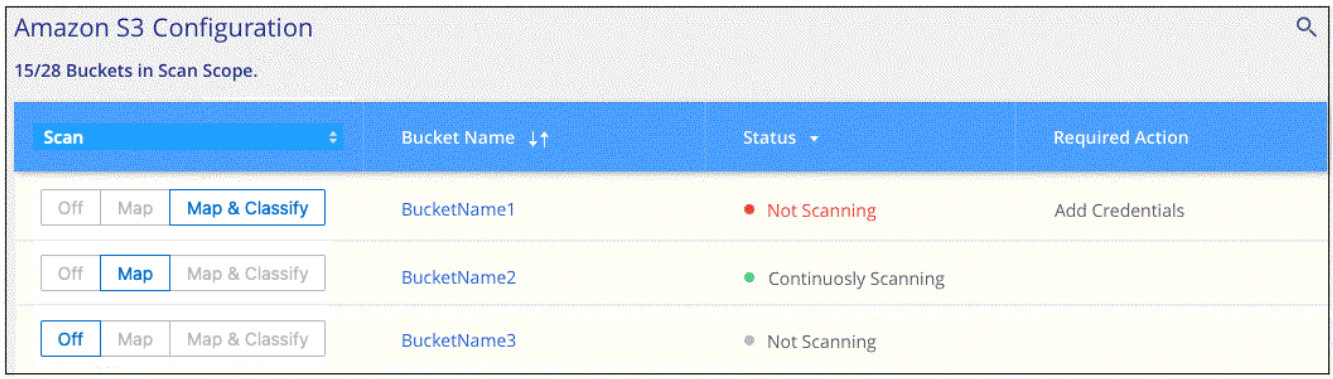
A classificação BlueXP também Examine os buckets do S3 que estão em diferentes contas da AWSpode .

Passos

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



3. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação nos seus buckets.



Para:	Faça isso:
Ative digitalizações apenas de mapeamento num balde	Clique em **mapa**
Ative digitalizações completas num balde	Clique em **Map & Classify**
Desative a digitalização em um balde	Clique em **Off**

Resultado

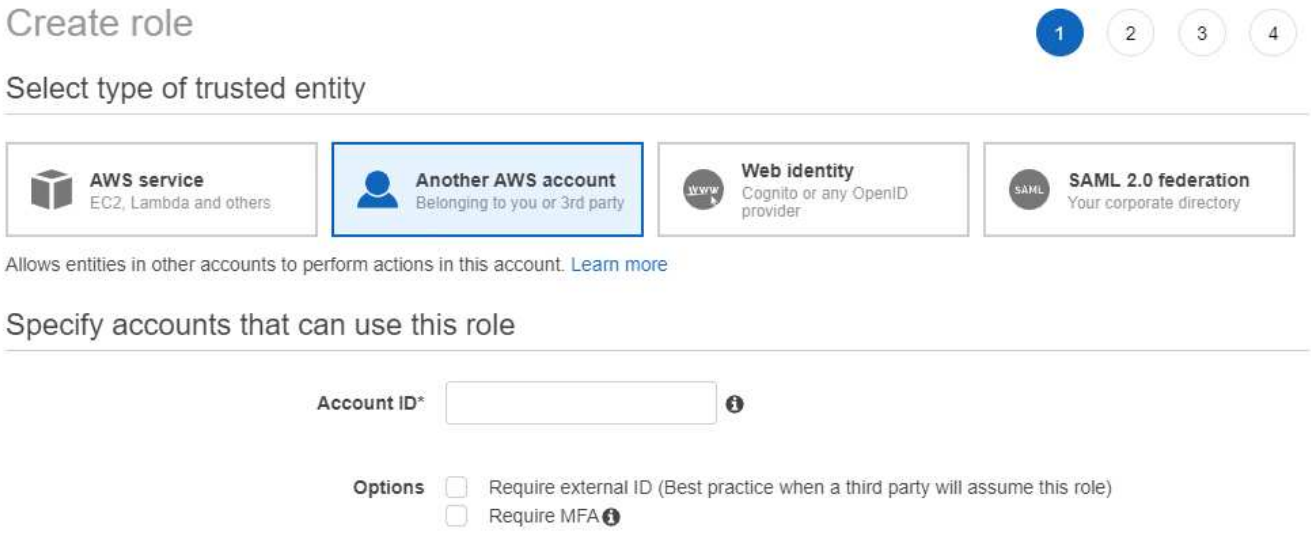
A classificação BlueXP começa a digitalizar os buckets S3 ativados. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Digitalização de buckets a partir de contas adicionais da AWS

Você pode verificar buckets do S3 que estão em uma conta diferente da AWS atribuindo uma função dessa conta para acessar a instância de classificação existente do BlueXP .

Passos

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



Certifique-se de fazer o seguinte:

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

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

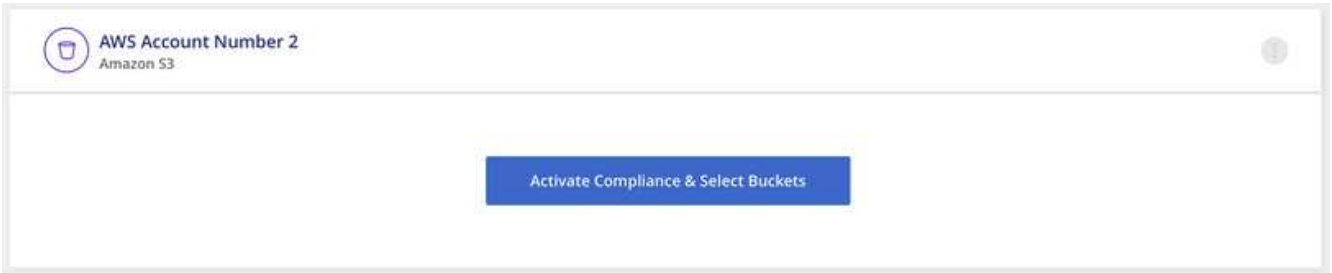
2. Vá para a conta AWS de origem onde reside a instância de classificação do BlueXP e selecione a função do IAM anexada à instância.
   a. Altere a duração máxima da sessão CLI/API* de 1 hora para 12 horas e salve essa alteração.
   b. Clique em **Anexar políticas** e, em seguida, clique em **criar política**.

c. Crie uma política que inclua a ação "sts:AssumeRole" e especifique o ARN da função que você criou na conta de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

A conta de perfil de instância de classificação do BlueXP agora tem acesso à conta AWS adicional.

3. Vá para a página **Configuração do Amazon S3** e a nova conta da AWS será exibida. Observe que pode levar alguns minutos para a classificação do BlueXP sincronizar o ambiente de trabalho da nova conta e mostrar essas informações.



4. Clique em **Activate Classification & Select Buckets** (Ativar classificação do BlueXP) e selecione os baldes que pretende digitalizar.

Resultado

A classificação BlueXP começa a digitalizar os novos buckets S3 ativados.

Digitalizar contas OneDrive

Conclua algumas etapas para iniciar a digitalização de arquivos nas pastas do OneDrive do usuário com a classificação BlueXP .

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Início rápido

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

Reveja os pré-requisitos do OneDrive

Certifique-se de que tem as credenciais de administrador para iniciar sessão na conta do OneDrive.

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

Adicione a conta do OneDrive

Usando credenciais de usuário Admin, faça login na conta do OneDrive que você deseja acessar para que ela seja adicionada como um novo ambiente de trabalho.

Adicione os usuários e selecione o tipo de digitalização

Adicione a lista de usuários da conta do OneDrive que você deseja digitalizar e selecione o tipo de digitalização. Você pode adicionar até 100 usuários ao mesmo tempo.

Rever os requisitos do OneDrive

Reveja os seguintes pré-requisitos para se certificar de que tem uma configuração suportada antes de ativar a classificação BlueXP .

- Tem de ter as credenciais de início de sessão Admin para a conta OneDrive for Business que forneça acesso de leitura aos ficheiros do utilizador.
- Você precisará de uma lista separada por linha dos endereços de e-mail para todos os usuários cujas pastas do OneDrive você deseja digitalizar.

Implantando a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

A classificação BlueXP pode ser "implantado na nuvem" ou "em um local no local que tem acesso à internet".

As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha

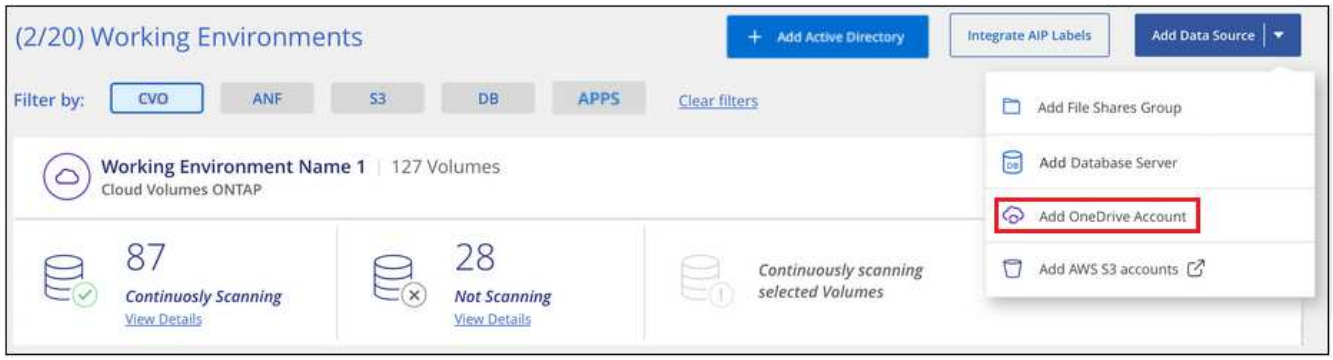
conetividade com a Internet.

Adicionar a conta OneDrive

Adicione a conta do OneDrive onde os arquivos de usuário residem.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar conta OneDrive**.



2. Na caixa de diálogo Adicionar uma conta do OneDrive, clique em **entrar no OneDrive**.
3. Na página da Microsoft exibida, selecione a conta do OneDrive e insira o usuário e a senha de administrador necessários e clique em **aceitar** para permitir que a classificação do BlueXP leia os dados dessa conta.

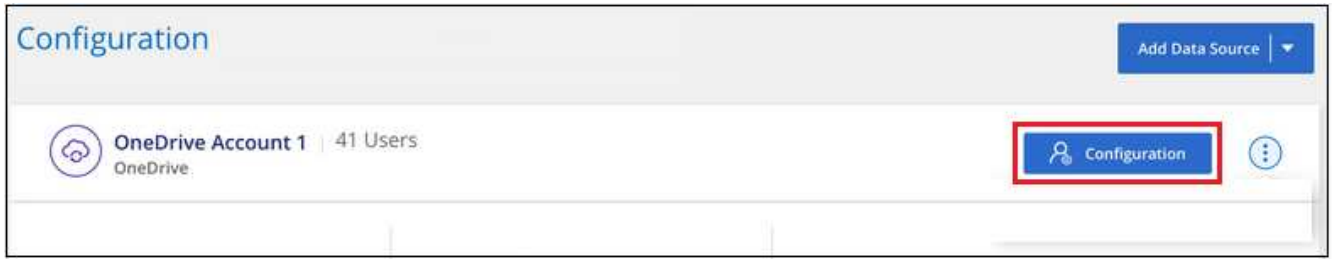
A conta do OneDrive é adicionada à lista de ambientes de trabalho.

Adicionando usuários do OneDrive às verificações de conformidade

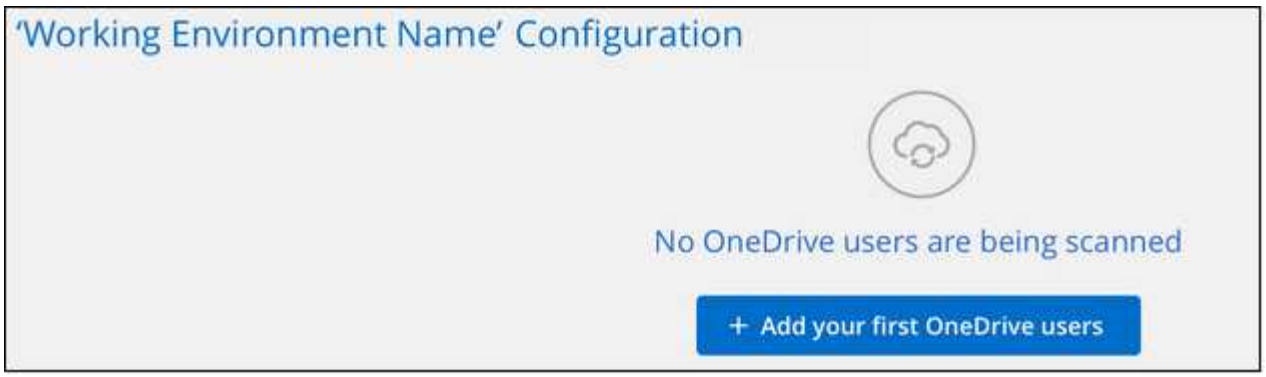
Você pode adicionar usuários individuais do OneDrive, ou todos os usuários do OneDrive, para que seus arquivos sejam verificados pela classificação do BlueXP .

Passos

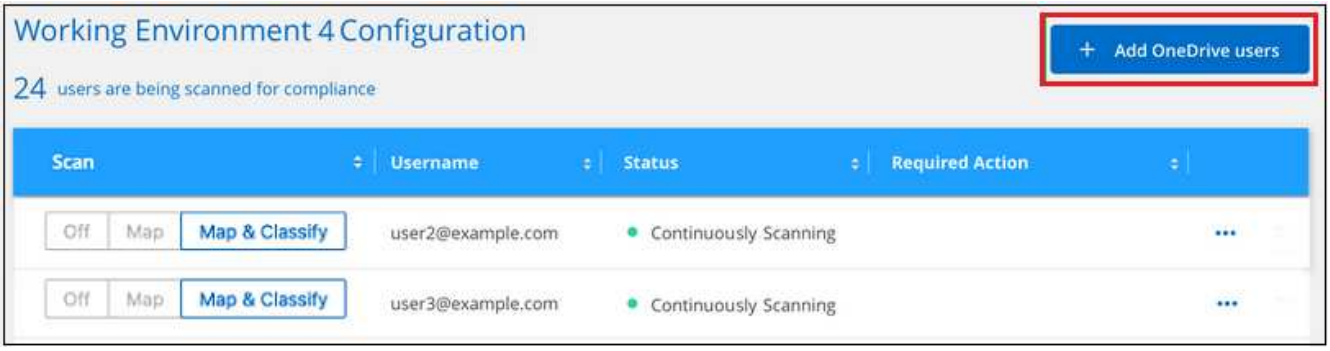
1. Na página *Configuration*, clique no botão **Configuration** da conta OneDrive.



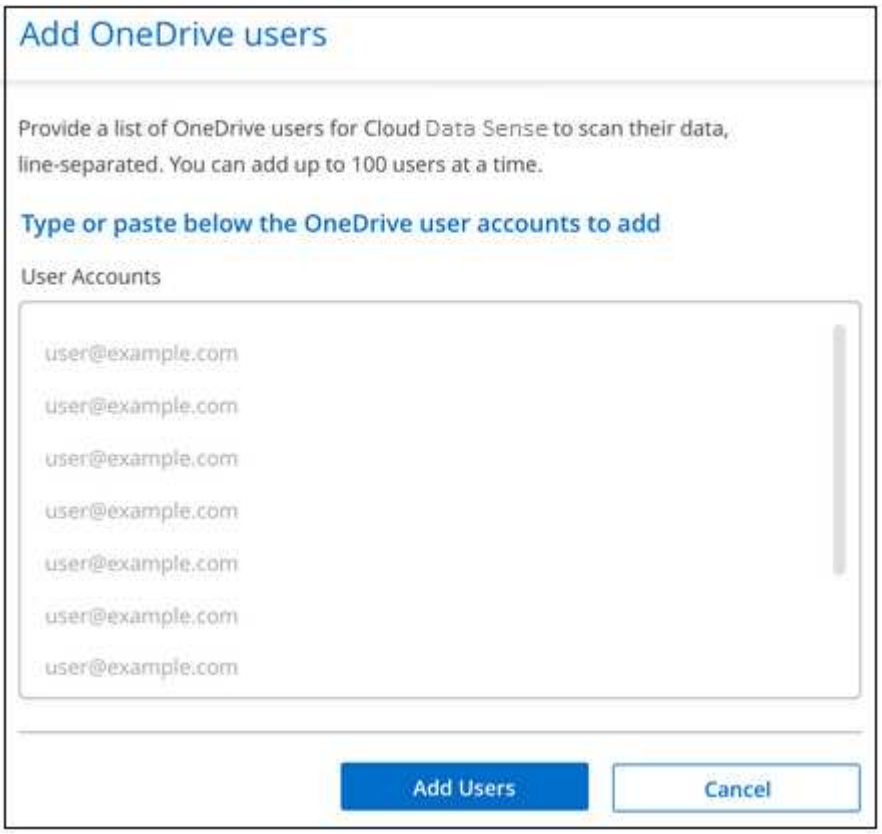
2. Se esta for a primeira vez que adicionar usuários para esta conta do OneDrive, clique em **Adicionar seus primeiros usuários do OneDrive**.



Se você estiver adicionando usuários adicionais de uma conta do OneDrive, clique em **Adicionar usuários do OneDrive**.



3. Adicione os endereços de e-mail para os usuários cujos arquivos você deseja digitalizar - um endereço de e-mail por linha (máximo de 100 por sessão) - e clique em **Adicionar usuários**.



Uma caixa de diálogo de confirmação exibe o número de usuários que foram adicionados.

Se a caixa de diálogo listar os usuários que não puderam ser adicionados, Capture essas informações para que você possa resolver o problema. Em alguns casos, você pode adicionar novamente o usuário com um endereço de e-mail corrigido.

4. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação em ficheiros do utilizador.

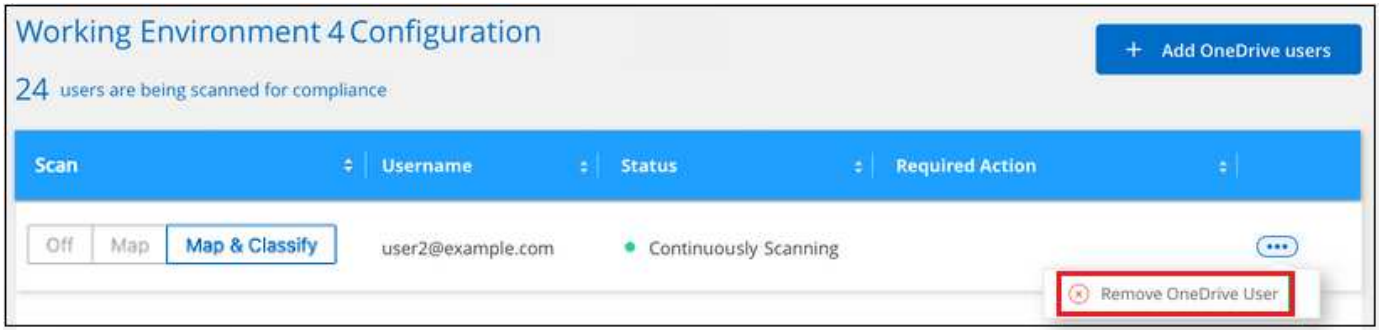
Para:	Faça isso:
Ativar digitalizações apenas de mapeamento em ficheiros de utilizador	Clique em **mapa**
Ative digitalizações completas em ficheiros de utilizador	Clique em **Map & Classify**
Desativar a digitalização em ficheiros de utilizador	Clique em **Off**

Resultado

A classificação do BlueXP começa a digitalizar os arquivos para os usuários adicionados e os resultados são exibidos no Painel e em outros locais.

Remover um usuário do OneDrive das verificações de conformidade

Se os usuários saírem da empresa ou se o endereço de e-mail mudar, você poderá remover usuários individuais do OneDrive de ter seus arquivos digitalizados a qualquer momento. Basta clicar em **Remover usuário do OneDrive** da página Configuração.



Analisar contas do SharePoint

Conclua algumas etapas para iniciar a digitalização de arquivos em suas contas on-premise do SharePoint Online e SharePoint com a classificação BlueXP .

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Início rápido

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

1 Revise os pré-requisitos do SharePoint

Certifique-se de que tem credenciais qualificadas para iniciar sessão na conta do SharePoint e de que tem as URLs dos sites do SharePoint que pretende analisar.

2 Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3 Faça login na conta do SharePoint

Usando credenciais de usuário qualificadas, faça login na conta do SharePoint que você deseja acessar para que ela seja adicionada como uma nova fonte de dados/ambiente de trabalho.

4 Adicione os URLs do site do SharePoint à verificação

Adicione a lista de URLs de sites do SharePoint que você deseja analisar na conta do SharePoint e selecione o tipo de digitalização. Você pode adicionar até 100 URLs ao mesmo tempo - e até 1.000 sites no total para cada conta.

Revise os requisitos do SharePoint

Reveja os seguintes pré-requisitos para se certificar de que está pronto para ativar a classificação do BlueXP numa conta do SharePoint.

- Você deve ter as credenciais de login do usuário Admin para a conta do SharePoint que fornece acesso de leitura a todos os sites do SharePoint.
  - Para o SharePoint Online, você pode usar uma conta que não seja de administrador, mas esse usuário deve ter permissão para acessar todos os sites do SharePoint que você deseja analisar.
- Para o SharePoint no local, você também precisará da URL do SharePoint Server.
- Você precisará de uma lista separada por linha dos URLs do site do SharePoint para todos os dados que deseja analisar.

Implante a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

- Para o SharePoint Online, a classificação do BlueXP pode ser "implantado na nuvem".
- Para SharePoint on-premises, a classificação BlueXP pode ser instalada "em um local no local que tem acesso à internet" ou "em um local no local que não tem acesso à internet".

Quando a classificação BlueXP é instalada em um site sem acesso à Internet, o conetor BlueXP também deve ser instalado nesse mesmo site sem acesso à Internet. "Saiba mais".

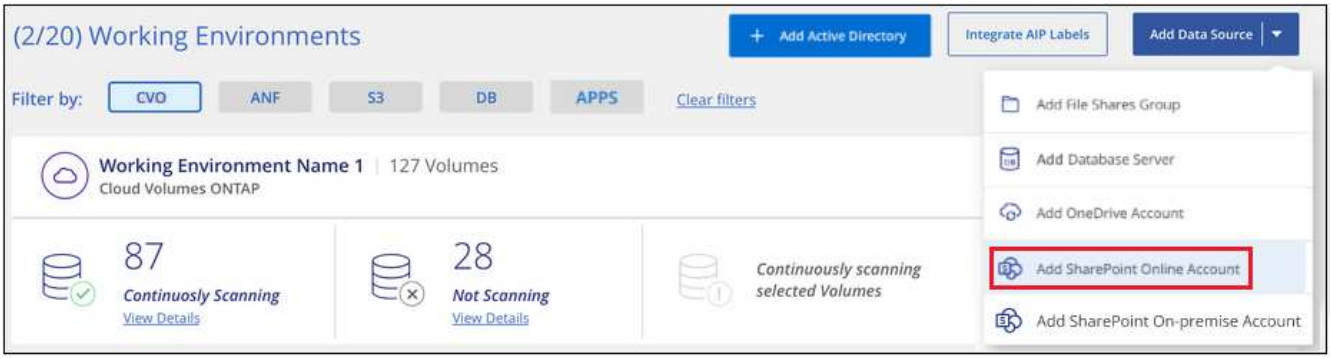
As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Adicione uma conta do SharePoint Online

Adicione a conta do SharePoint Online onde os arquivos de usuário residem.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar conta do SharePoint Online**.



2. Na caixa de diálogo Adicionar uma conta do SharePoint Online, clique em **entrar no SharePoint**.
3. Na página da Microsoft exibida, selecione a conta do SharePoint e insira o usuário e a senha (usuário administrador ou outro usuário com acesso aos sites do SharePoint) e clique em **Accept** para permitir que a classificação do BlueXP leia os dados dessa conta.

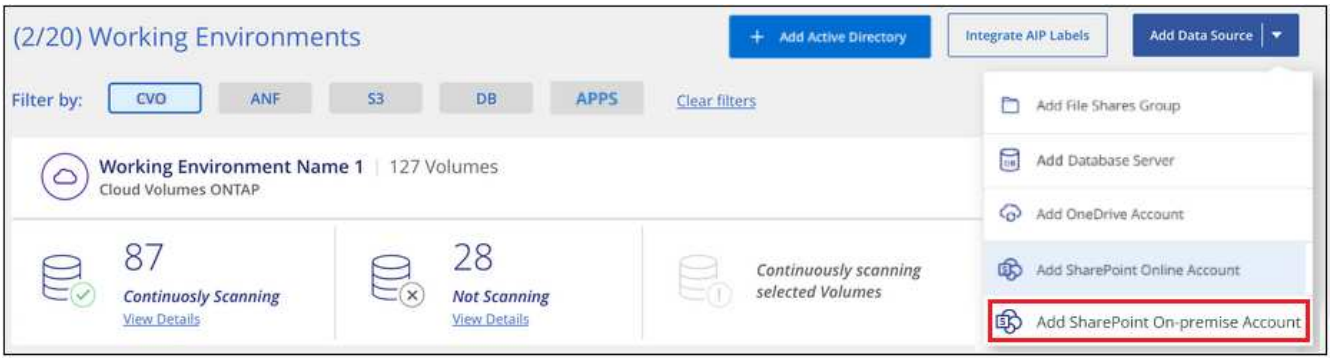
A conta do SharePoint Online é adicionada à lista de ambientes de trabalho.

Adicione uma conta no local do SharePoint

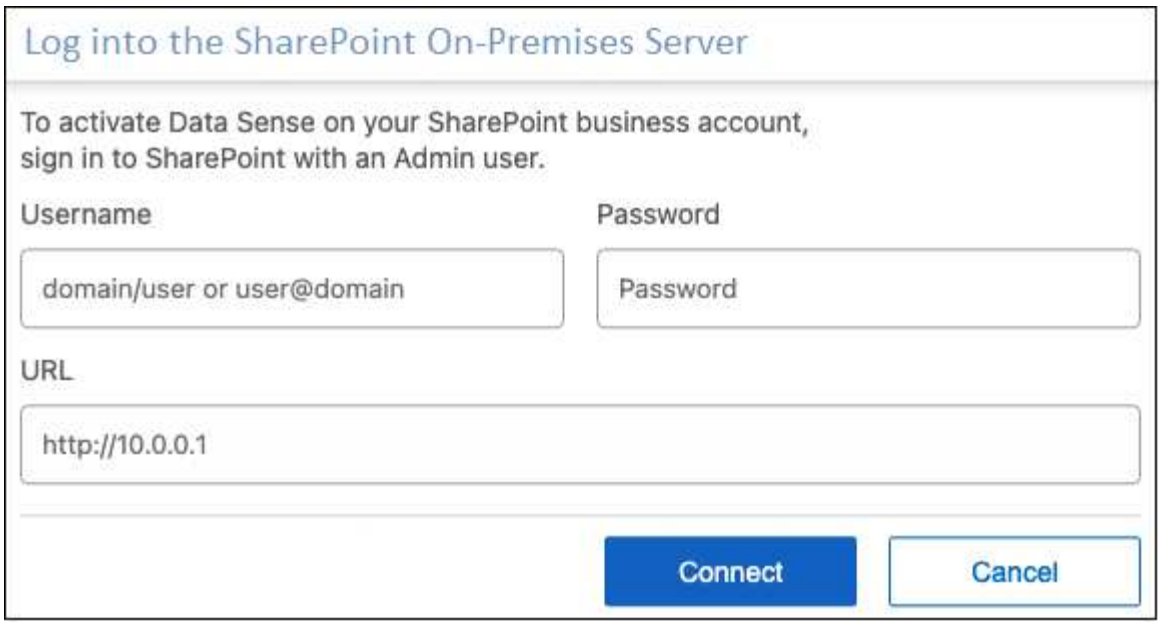
Adicione a conta no local do SharePoint onde os arquivos de usuário residem.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar conta no local do SharePoint**.



2. Na caixa de diálogo Log in the SharePoint On-Premise Server (Iniciar sessão no servidor no local do SharePoint), introduza as seguintes informações:
   - Admin usuário no formato "domínio/usuário" ou "usuário no domínio", e senha de administrador
   - URL do SharePoint Server



3. Clique em **Connect**.

A conta no local do SharePoint é adicionada à lista de ambientes de trabalho.

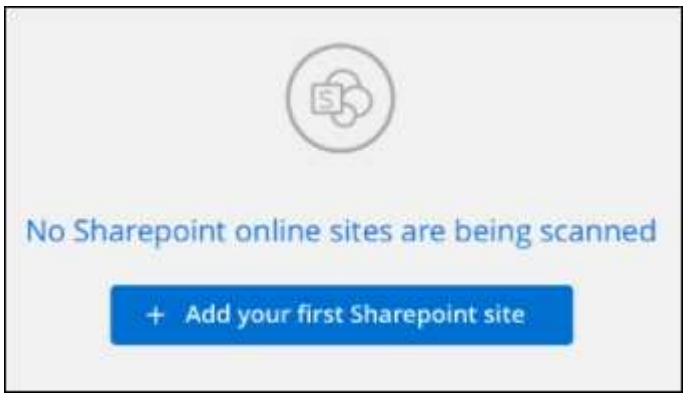
Adicione sites do SharePoint às verificações de conformidade

Você pode adicionar sites individuais do SharePoint ou até 1.000 sites do SharePoint na conta, para que os arquivos associados sejam verificados pela classificação do BlueXP . As etapas são as mesmas se você estiver adicionando sites no local do SharePoint Online ou SharePoint.

Passos

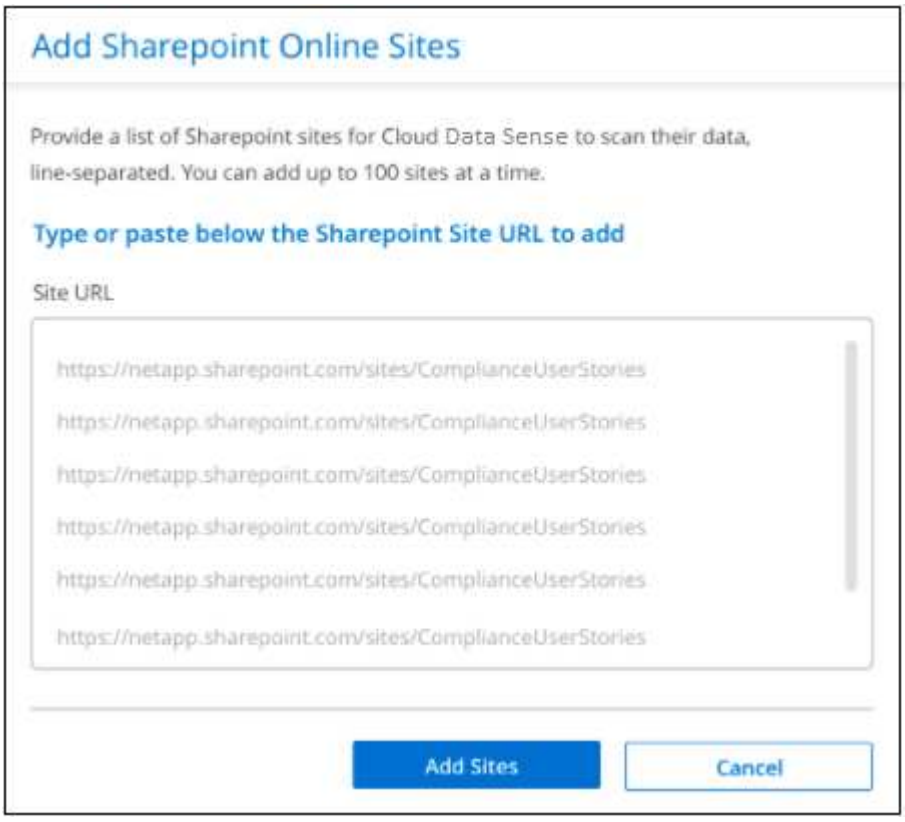
1. Na página *Configuration*, clique no botão **Configuration** da conta do SharePoint.

2. Se esta for a primeira vez que adicionar sites para esta conta do SharePoint, clique em **Adicionar seu primeiro site do SharePoint**.



Se você estiver adicionando usuários adicionais de uma conta do SharePoint, clique em **Adicionar sites do SharePoint**.

3. Adicione os URLs para os sites cujos arquivos você deseja digitalizar - um URL por linha (até 100 no máximo por sessão) - e clique em **Adicionar sites**.



Uma caixa de diálogo de confirmação exibe o número de sites que foram adicionados.

Se a caixa de diálogo listar quaisquer sites que não possam ser adicionados, Capture essas informações para que você possa resolver o problema. Em alguns casos, você pode adicionar novamente o site com um URL corrigido.

4. Se você precisar adicionar mais de 100 sites para essa conta, basta clicar em **Adicionar sites do SharePoint** novamente até que você tenha adicionado todos os sites para essa conta (até 1.000 sites no total para cada conta).
5. Ative varreduras somente de mapeamento ou varreduras de mapeamento e classificação nos arquivos nos sites do SharePoint.

Para:	Faça isso:
Ativar digitalizações apenas de mapeamento em ficheiros	Clique em **mapa**

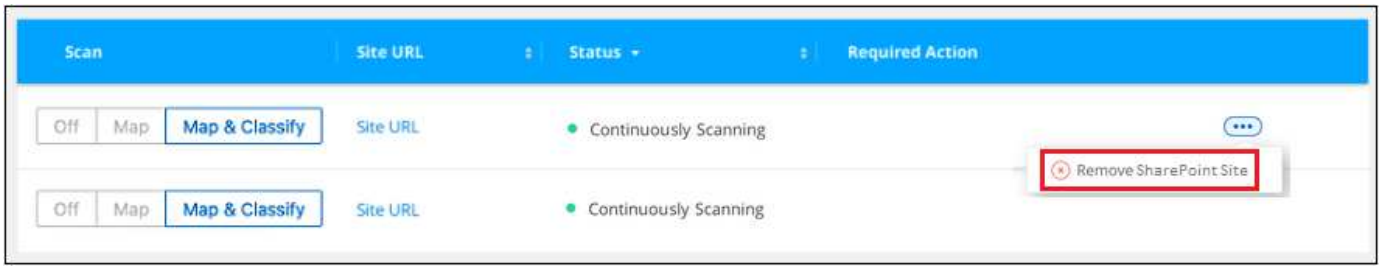
Para:	Faça isso:
Ative digitalizações completas em ficheiros	Clique em **Map & Classify**
Desativar a digitalização em ficheiros	Clique em **Off**

Resultado

A classificação do BlueXP começa a digitalizar os arquivos nos sites do SharePoint que você adicionou, e os resultados são exibidos no Painel e em outros locais.

Remover um site do SharePoint de verificações de conformidade

Se você remover um site do SharePoint no futuro ou decidir não digitalizar arquivos em um site do SharePoint, você poderá remover sites individuais do SharePoint de ter seus arquivos digitalizados a qualquer momento. Basta clicar em **Remove SharePoint Site** da página Configuração.



Observe que você pode "Exclua toda a conta do SharePoint da classificação do BlueXP " se você não quiser mais verificar os dados de usuário da conta do SharePoint.

Analisar contas do Google Drive

Conclua algumas etapas para começar a digitalizar arquivos de usuário em suas contas do Google Drive com a classificação BlueXP .

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Início rápido

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

1 **Reveja os pré-requisitos do Google Drive**

Certifique-se de que tem as credenciais de administrador para iniciar sessão na conta do Google Drive.

2 **Implantar a classificação BlueXP**

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

3 Faça login na conta do Google Drive

Usando credenciais de usuário Admin, faça login na conta do Google Drive que você deseja acessar para que ela seja adicionada como uma nova fonte de dados.

4 Selecione o tipo de digitalização para os ficheiros de utilizador

Selecione o tipo de digitalização que pretende executar nos ficheiros de utilizador; mapeamento ou mapeamento e classificação.

Reveja os requisitos do Google Drive

Reveja os seguintes pré-requisitos para se certificar de que está pronto para ativar a classificação do BlueXP numa conta Google Drive.

- Você deve ter as credenciais de login de administrador para a conta do Google Drive que fornece acesso de leitura aos arquivos do usuário

Restrições atuais

Os seguintes recursos de classificação do BlueXP não são atualmente suportados com arquivos do Google Drive:

- Ao visualizar arquivos na página Investigação de dados, as ações na barra de botões não estão ativas. Você não pode copiar, mover, excluir, etc. quaisquer arquivos.
- As permissões não podem ser identificadas em arquivos no Google Drive, portanto, nenhuma informação de permissão é exibida na página de investigação.

Implantar a classificação BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

A classificação BlueXP pode ser "implantado na nuvem" ou "em um local no local que tem acesso à internet".

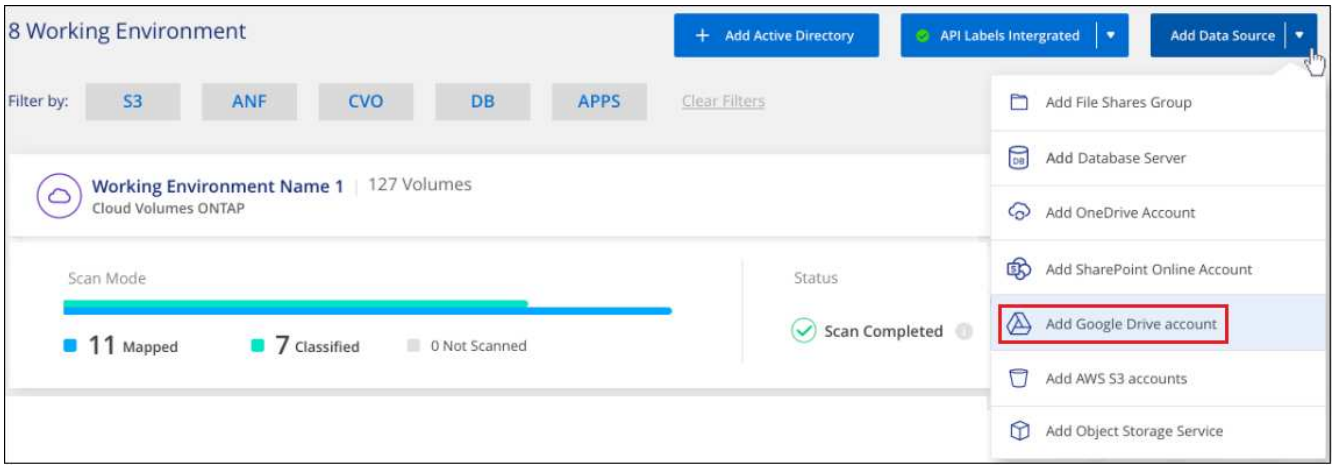
As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Adicione a conta do Google Drive

Adicione a conta do Google Drive onde os arquivos de usuário residem. Se você quiser digitalizar arquivos de vários usuários, precisará executar esta etapa para cada usuário.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar conta do Google Drive**.



2. Na caixa de diálogo Adicionar uma conta do Google Drive, clique em **entrar no Google Drive**.
3. Na página do Google exibida, selecione a conta do Google Drive e insira o usuário e a senha de administrador necessários e clique em **aceitar** para permitir que a classificação do BlueXP leia os dados dessa conta.

A conta do Google Drive é adicionada à lista de ambientes de trabalho.

Selecione o tipo de digitalização para dados do utilizador

Selecione o tipo de digitalização que a classificação BlueXP executará nos dados do utilizador.

Passos

1. Na página *Configuration*, clique no botão **Configuration** da conta do Google Drive.
2. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação nos ficheiros da conta do Google Drive.

Para:	Faça isso:
Ativar digitalizações apenas de mapeamento em ficheiros	Clique em **mapa**
Ative digitalizações completas em ficheiros	Clique em **Map & Classify**
Desativar a digitalização em ficheiros	Clique em **Off**

Resultado

A classificação do BlueXP começa a digitalizar os arquivos na conta do Google Drive que você adicionou, e os resultados são exibidos no Painel e em outros locais.

Remova uma conta do Google Drive das verificações de conformidade

Como apenas os arquivos do Google Drive de um único usuário fazem parte de uma única conta do Google Drive, se você quiser parar de digitalizar arquivos da conta do Google Drive de um usuário, você deve "Exclua a conta do Google Drive da classificação do BlueXP ".

Digitalizar dados StorageGRID

Conclua algumas etapas para iniciar a digitalização de dados dentro do armazenamento de objetos diretamente com a classificação BlueXP . A classificação do BlueXP pode analisar dados de qualquer serviço de armazenamento de objetos que use o protocolo Simple Storage Service (S3). Isso inclui NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3 e muito mais.

NOTA usando a classificação BlueXP que faz parte do BlueXP principal, agora você pode digitalizar dados do StorageGRID. Consulte "Digitalizar dados StorageGRID". As informações restantes aqui são relevantes apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Início rápido

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

Reveja os pré-requisitos de armazenamento de objetos

Você precisa ter o URL do endpoint para se conetar ao serviço de armazenamento de objetos.

Você precisa ter a chave de acesso e a chave secreta do provedor de armazenamento de objetos para que a classificação BlueXP possa acessar os buckets.

Implante a instância de classificação do BlueXP

"Implantar a classificação BlueXP " se ainda não houver uma instância implantada.

Adicione o Object Storage Service

Adicione o serviço de storage de objetos à classificação do BlueXP .

Selecione os intervalos para digitalizar

Selecione os intervalos que você gostaria de digitalizar e a classificação BlueXP começará a digitalizá-los.

Revisão dos requisitos de armazenamento de objetos

Reveja os seguintes pré-requisitos para se certificar de que tem uma configuração suportada antes de ativar a classificação BlueXP .

- Você precisa ter o URL do endpoint para se conetar ao serviço de armazenamento de objetos.

- Você precisa ter a chave de acesso e a chave secreta do provedor de armazenamento de objetos para que a classificação BlueXP possa acessar os buckets.

Implantando a instância de classificação do BlueXP

Implante a classificação do BlueXP se ainda não houver uma instância implantada.

Se você estiver digitalizando dados do armazenamento de objetos S3 que é acessível pela Internet, você pode "Implante a classificação do BlueXP na nuvem" ou "Implante a classificação BlueXP em um local local que tenha acesso à Internet".

Se você estiver digitalizando dados do armazenamento de objetos S3 que foi instalado em um site escuro que não tem acesso à Internet, é necessário "Implante a classificação BlueXP no mesmo local que não tem acesso à Internet". Isso também requer que o BlueXP Connector seja implantado no mesmo local.

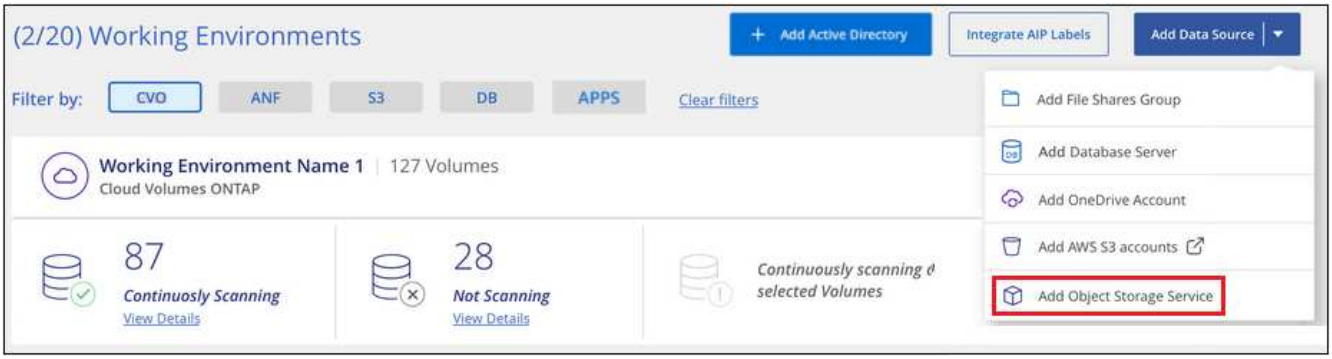
As atualizações para o software de classificação BlueXP são automatizadas, desde que a instância tenha conetividade com a Internet.

Adicionando o serviço de storage de objetos à classificação do BlueXP

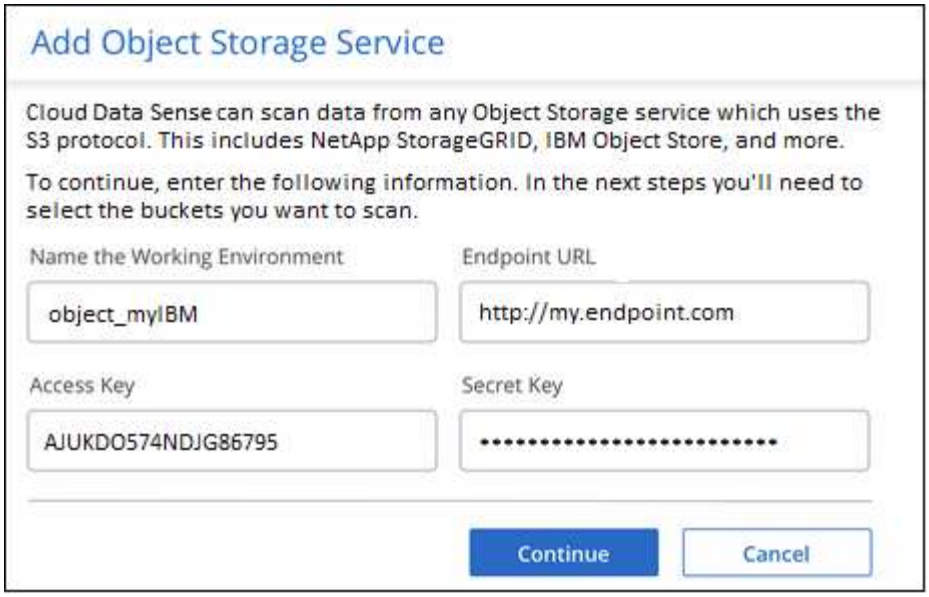
Adicione o serviço de storage de objetos.

Passos

1. Na página Configuração de ambientes de trabalho, clique em **Adicionar fonte de dados** > **Adicionar serviço de armazenamento de objetos**.



2. Na caixa de diálogo Adicionar serviço de armazenamento de objetos, insira os detalhes do serviço de armazenamento de objetos e clique em **continuar**.
   a. Introduza o nome que pretende utilizar para o ambiente de trabalho. Esse nome deve refletir o nome do serviço de storage de objetos ao qual você está se conetando.
   b. Insira o 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 BlueXP possa acessar os buckets no armazenamento de objetos.



Resultado

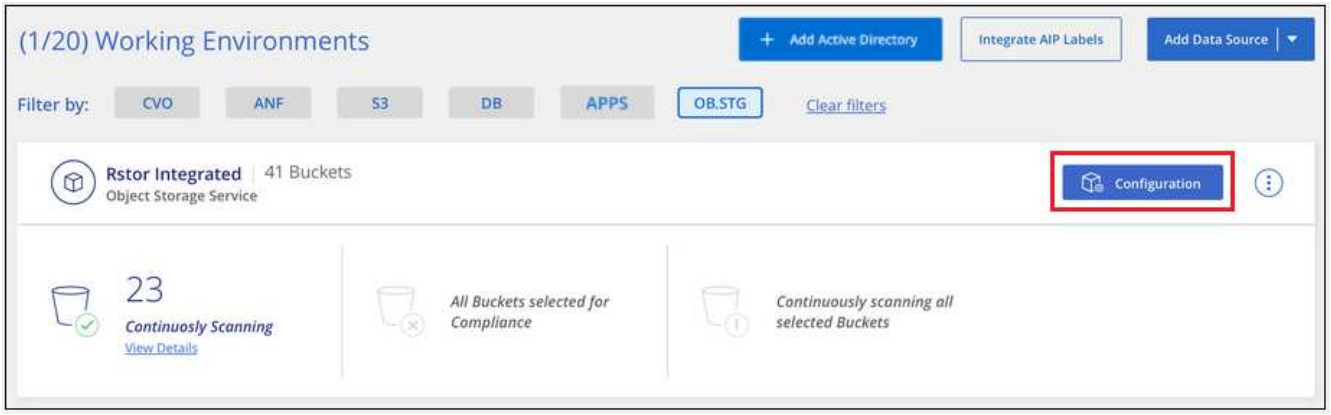
O novo Object Storage Service é adicionado à lista de ambientes de trabalho.

Habilitando e desabilitando varreduras de conformidade em buckets de armazenamento de objetos

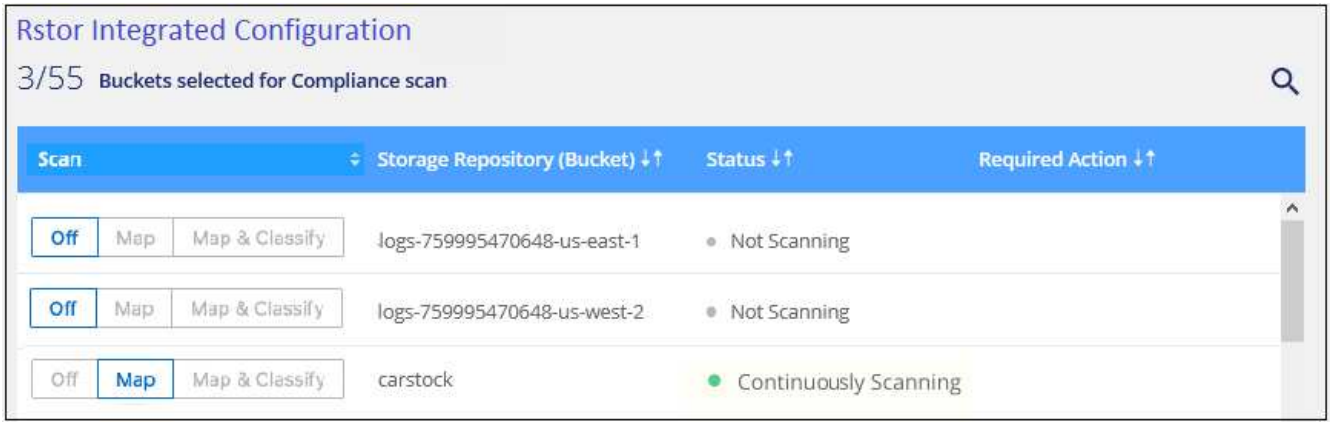
Depois de ativar a classificação do BlueXP no seu Serviço de armazenamento de objetos, a próxima etapa é configurar os intervalos que você deseja analisar. A classificação BlueXP descobre esses buckets e os exibe no ambiente de trabalho que você criou.

Passos

1. Na página Configuração, clique em **Configuração** no ambiente de trabalho Serviço de armazenamento de objetos.



2. Ative digitalizações apenas de mapeamento ou digitalizações de mapeamento e classificação nos seus buckets.



Para:	Faça isso:
Ative digitalizações apenas de mapeamento num balde	Clique em **mapa**
Ative digitalizações completas num balde	Clique em **Map & Classify**
Desative a digitalização em um balde	Clique em **Off**

Resultado

A classificação BlueXP começa a digitalizar os intervalos que você ativou. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Gerencie as depreciações de dados

Veja detalhes de governança sobre seus dados usando o painel Governança

Controle os custos relacionados aos dados sobre os recursos de storage da sua organização. A classificação do BlueXP identifica a quantidade de dados obsoletos, dados não comerciais, arquivos duplicados e arquivos muito grandes em seus sistemas. Assim, você pode decidir se deseja remover ou categorizar alguns arquivos para um storage de objetos mais econômico.

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

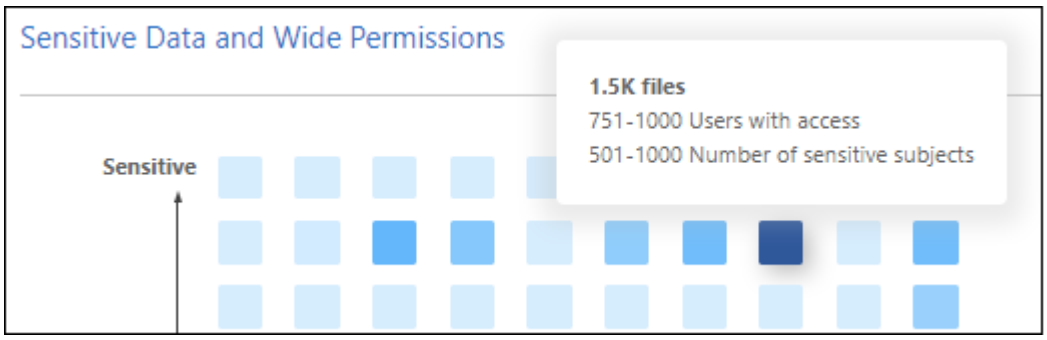
NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Dados listados por sensibilidade e permissões amplas no painel Governança

A área *dados confidenciais e permissões amplas* no painel de governança fornece um mapa de calor de arquivos que contêm dados confidenciais (incluindo dados pessoais confidenciais e confidenciais) e que são excessivamente permissivos. Isso pode ajudá-lo a ver onde você pode ter alguns riscos com dados confidenciais.

Isto aplica-se às versões de classificação BlueXP 1,30 e anteriores.

Os arquivos são classificados com base no número de usuários com permissão para acessar os arquivos no eixo X (menor para maior) e no número de identificadores sensíveis dentro dos arquivos no eixo Y (menor para maior). Os blocos representam o número de arquivos que correspondem aos itens dos eixos X e Y. O bloco colorido mais claro é bom; com menos usuários capazes de acessar os arquivos e com menos identificadores sensíveis por arquivo. Os blocos mais escuros são os itens que você pode querer investigar. Por exemplo, a tela abaixo mostra o texto da dica de ferramenta para o bloco azul escuro. Ele mostra que você tem 1.500 arquivos onde 751-100 usuários têm acesso e onde há 501-100 identificadores sensíveis por arquivo.



Você pode clicar no bloco em que está interessado para ver os resultados filtrados dos arquivos afetados na página de investigação para que você possa investigar mais.

Nenhum dado será exibido neste painel se você não tiver integrado um serviço de identidade com a classificação BlueXP . "Veja como integrar seu serviço do ative Directory com a classificação do BlueXP ".

Esse painel oferece suporte a arquivos em compartilhamentos CIFS, OneDrive e fontes de dados do SharePoint. Atualmente, não há suporte para bancos de dados, Google Drive, Amazon S3 e armazenamento de objetos genéricos.

Área de classificação no painel mostrando rótulos AIP

A área *classificação* no painel fornece uma lista das etiquetas AIP (proteção de informações do Azure) mais identificadas nos seus dados digitalizados.

Se você se inscreveu no Azure Information Protection (AIP), poderá classificar e proteger documentos e arquivos aplicando rótulos ao conteúdo. A revisão dos rótulos AIP mais usados atribuídos a arquivos permite ver quais rótulos são mais usados em seus arquivos.

Consulte "Etiquetas AIP" para obter mais informações.

Organize os seus dados privados

A classificação BlueXP fornece muitas maneiras de gerenciar e organizar seus dados privados. Isso facilita a visualização dos dados mais importantes para você.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores. A versão de dezembro de 2023 (v1.26.6) removeu a opção de integrar dados usando rótulos AIP (proteção de informações do Azure).

- Se você está inscrito "Proteção de informações do Azure (AIP)" para classificar e proteger seus arquivos, você pode usar a classificação BlueXP para gerenciar esses rótulos AIP.

- Você pode adicionar Tags a arquivos que deseja marcar para a organização ou para algum tipo de acompanhamento.
- Você pode atribuir um usuário do BlueXP a um arquivo específico ou a vários arquivos, para que a pessoa possa ser responsável pelo gerenciamento do arquivo.
- Usando a funcionalidade "Política", você pode criar suas próprias consultas de pesquisa personalizadas para que você possa ver facilmente os resultados clicando em um botão.
- Você pode enviar alertas de e-mail para usuários do BlueXP ou qualquer outro endereço de e-mail quando certas políticas críticas retornam resultados.

As capacidades descritas nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma varredura somente de mapeamento não mostram detalhes no nível do arquivo.

Devo usar tags ou rótulos?

Abaixo está uma comparação entre a marcação de classificação BlueXP e a rotulagem de proteção de informações do Azure.

Tags	Etiquetas
Tags de arquivo são uma parte integrada da classificação BlueXP .	Requer que você se inscreveu no Azure Information Protection (AIP).
A tag só é mantida no banco de dados de classificação BlueXP - não é gravada no arquivo. Ele não altera o arquivo, nem o arquivo acessado ou modificado vezes.	O rótulo faz parte do arquivo e, quando o rótulo muda, o arquivo muda. Essa alteração também altera os horários acessados e modificados do arquivo.
Você pode ter várias tags em um único arquivo.	Você pode ter um rótulo em um único arquivo.
A tag pode ser usada para a ação interna de classificação do BlueXP , como copiar, mover, excluir, executar uma política, etc.	Outros sistemas que podem ler o arquivo podem ver o rótulo - que pode ser usado para automação adicional.
Apenas uma única chamada de API é usada para ver se um arquivo tem uma tag.	

Categorize seus dados usando rótulos AIP

Você pode gerenciar rótulos AIP nos arquivos que a classificação do BlueXP está digitalizando se você se inscreveu "Proteção de informações do Azure (AIP)" no . O AIP permite classificar e proteger documentos e arquivos aplicando rótulos ao conteúdo. A classificação BlueXP permite exibir os rótulos que já estão atribuídos a arquivos, adicionar rótulos a arquivos e alterar rótulos quando um rótulo já existe.

A classificação BlueXP suporta etiquetas AIP nos seguintes tipos de arquivo: .DOC, .DOCX, .PDF, .PPTX, .xls, .xlsx.

- Atualmente, não é possível alterar rótulos em arquivos com mais de 30 MB. Para contas do OneDrive, SharePoint e Google Drive, o tamanho máximo do arquivo é de 4 MB.
- Se um arquivo tem um rótulo que não existe mais no AIP, a classificação BlueXP considera-o como um arquivo sem um rótulo.
- Se você implantou a classificação do BlueXP em uma região do governo ou em um local local local que não tenha acesso à Internet (também conhecido como um site escuro), a funcionalidade de rótulo AIP não estará disponível.

Integre rótulos AIP em seu projeto ou área de trabalho

Antes de gerenciar rótulos AIP, você precisa integrar a funcionalidade de rótulo AIP na classificação do BlueXP , fazendo login na sua conta existente do Azure. Uma vez ativado, você pode gerenciar rótulos AIP em arquivos para todos "fontes de dados" no seu projeto ou área de trabalho do BlueXP .

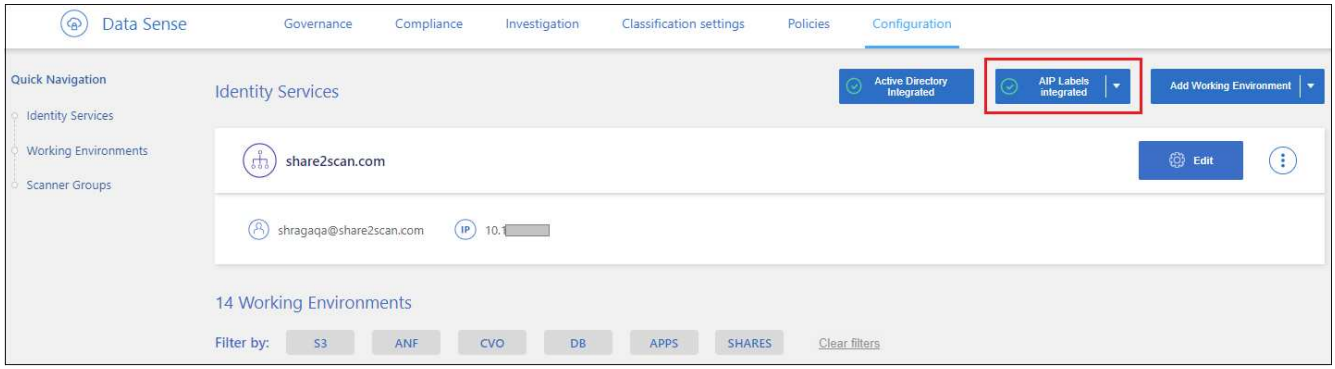
Requisitos

- Você deve ter uma conta e uma licença de proteção de informações do Azure.
- Tem de ter as credenciais de início de sessão para a conta Azure.
- Se você planeja alterar rótulos em arquivos que residem nos buckets do Amazon S3, verifique se a permissão `s3:PutObject` está incluída na função IAM. "Configurando a função do IAM"Consulte .

Passos

1. Na página Configuração de classificação do BlueXP , clique em **integrar rótulos AIP**.

2. Na caixa de diálogo integrar rótulos AIP, clique em **entrar no Azure**.
3. Na página da Microsoft exibida, selecione a conta e insira as credenciais necessárias.
4. Retorne à guia classificação do BlueXP e você verá a mensagem "*AIP rótulos foram integrados com êxito com o Account <account_name>*".
5. Clique em **Fechar** e você verá o texto *rótulos AIP integrados* na parte superior da página.



Resultado

Você pode exibir e atribuir rótulos AIP a partir do painel de resultados da página de investigação. Você

também pode atribuir rótulos AIP a arquivos usando políticas.

Veja etiquetas AIP em seus arquivos

Você pode exibir o rótulo AIP atual atribuído a um arquivo.

No painel resultados da investigação de dados, clique em para o ficheiro para expandir os detalhes dos metadados do ficheiro.

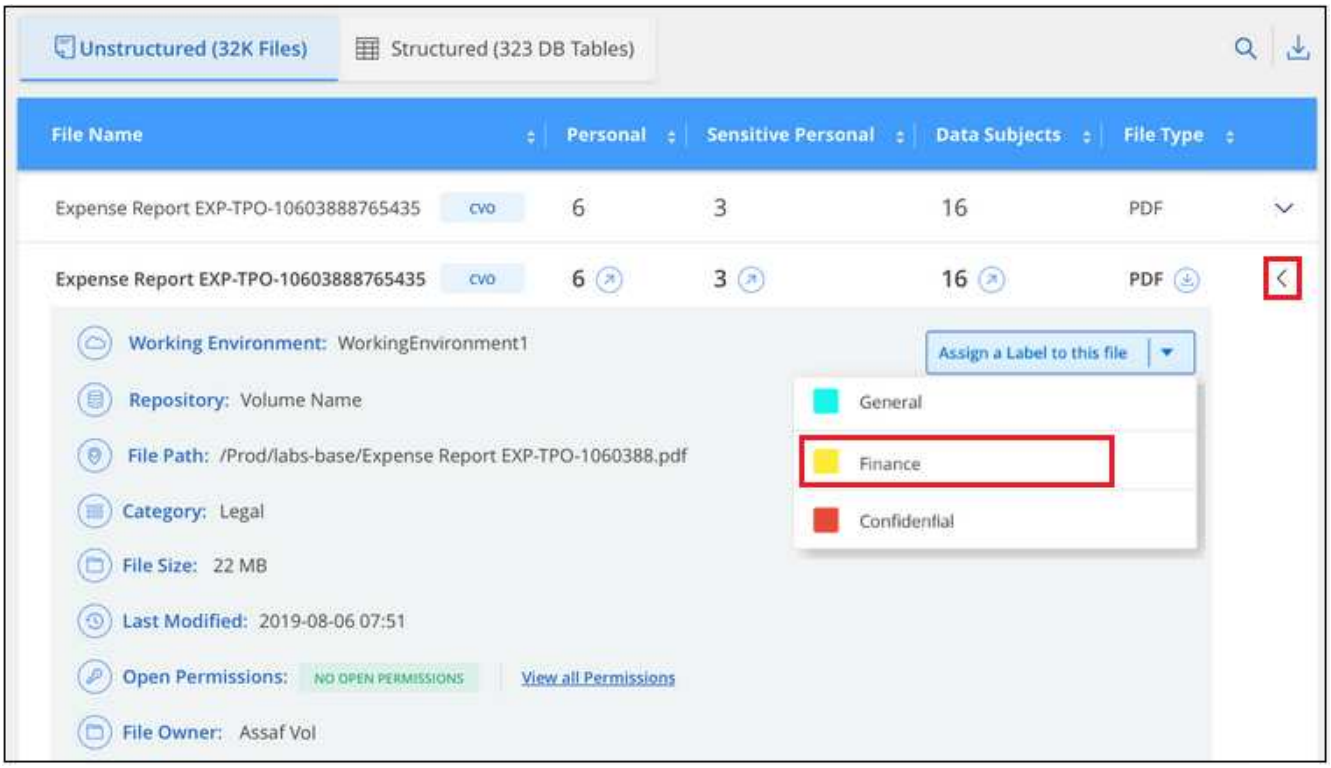
Atribua etiquetas AIP manualmente

Você pode adicionar, alterar e remover rótulos AIP de seus arquivos usando a classificação BlueXP .

Siga estas etapas para atribuir um rótulo AIP a um único arquivo.

Passos

1. No painel resultados da investigação de dados, clique em para o ficheiro para expandir os detalhes dos metadados do ficheiro.



2. Clique em **Assign a Label to this file** (atribuir um rótulo a este arquivo*) e, em seguida, selecione o rótulo.

   O rótulo aparece nos metadados do arquivo.

Siga estas etapas para atribuir um rótulo AIP a vários arquivos. Observe que você pode atribuir um rótulo AIP a um máximo de 20 arquivos de cada vez (uma página na IU).

Passos

1. No painel resultados da investigação de dados, selecione o arquivo ou os arquivos que você deseja rotular.

   - Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
   - Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).

2. Na barra de botões, clique em **Label** e selecione o rótulo AIP:

O rótulo AIP é adicionado aos metadados para todos os arquivos selecionados.

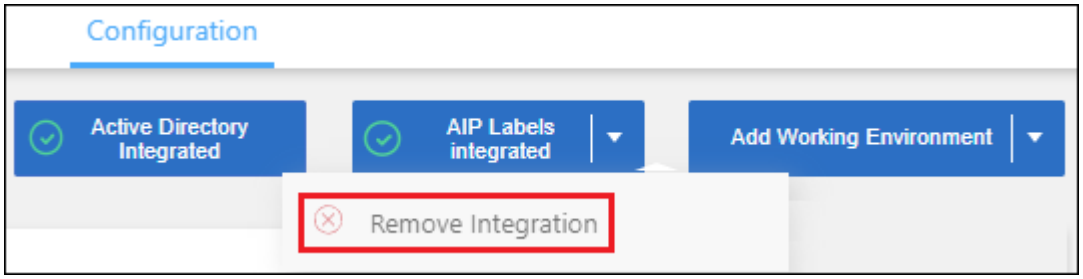
Remova a integração AIP

Se você não quiser mais a capacidade de gerenciar rótulos AIP em arquivos, você pode remover a conta AIP da interface de classificação do BlueXP .

Observe que não são feitas alterações nos rótulos que você adicionou usando a classificação BlueXP . Os rótulos que existem nos arquivos permanecerão como eles existem atualmente.

Passos

1. Na página *Configuration*, clique em **AIP Labels Integrated > Remove Integration** (etiquetas AIP integradas > Remover integração).



2. Clique em **Remover integração** na caixa de diálogo de confirmação.

Aplique tags para gerenciar seus arquivos digitalizados

Você pode adicionar uma tag aos arquivos que deseja marcar para algum tipo de acompanhamento. Por exemplo, você pode ter encontrado alguns arquivos duplicados e deseja excluir um deles, mas você precisa verificar qual deles deve ser excluído. Você pode adicionar uma tag de "Check to delete" ao arquivo para que você saiba que esse arquivo requer alguma pesquisa e algum tipo de ação futura.

A classificação BlueXP permite visualizar as tags atribuídas a arquivos, adicionar ou remover tags de arquivos e alterar o nome ou excluir uma tag existente.

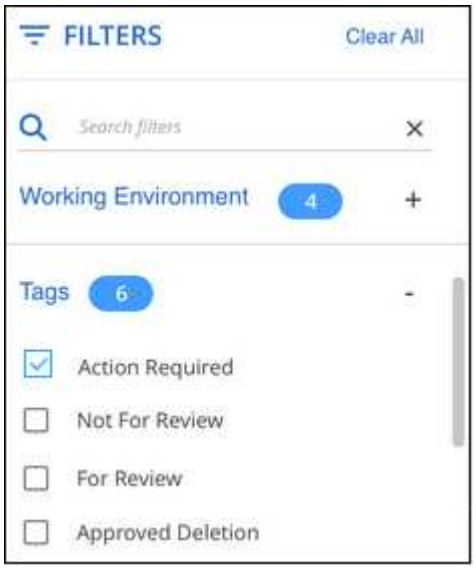
Observe que a tag não é adicionada ao arquivo da mesma forma que as etiquetas AIP fazem parte dos metadados do arquivo. A tag é vista apenas pelos usuários do BlueXP usando a classificação BlueXP para que você possa ver se um arquivo precisa ser excluído ou verificado para algum tipo de acompanhamento.

As tags atribuídas a arquivos na classificação BlueXP não estão relacionadas às tags que você pode adicionar a recursos, como volumes ou instâncias de máquina virtual. As tags de classificação BlueXP são aplicadas no nível do arquivo.

Exibir arquivos que têm certas tags aplicadas

Você pode visualizar todos os arquivos que têm tags específicas atribuídas.

1. Clique no separador **Investigation** da classificação BlueXP .
2. Na página Investigação de dados, clique em **Tags** no painel filtros e selecione as tags necessárias.



O painel resultados da investigação exibe todos os arquivos que têm essas tags atribuídas.

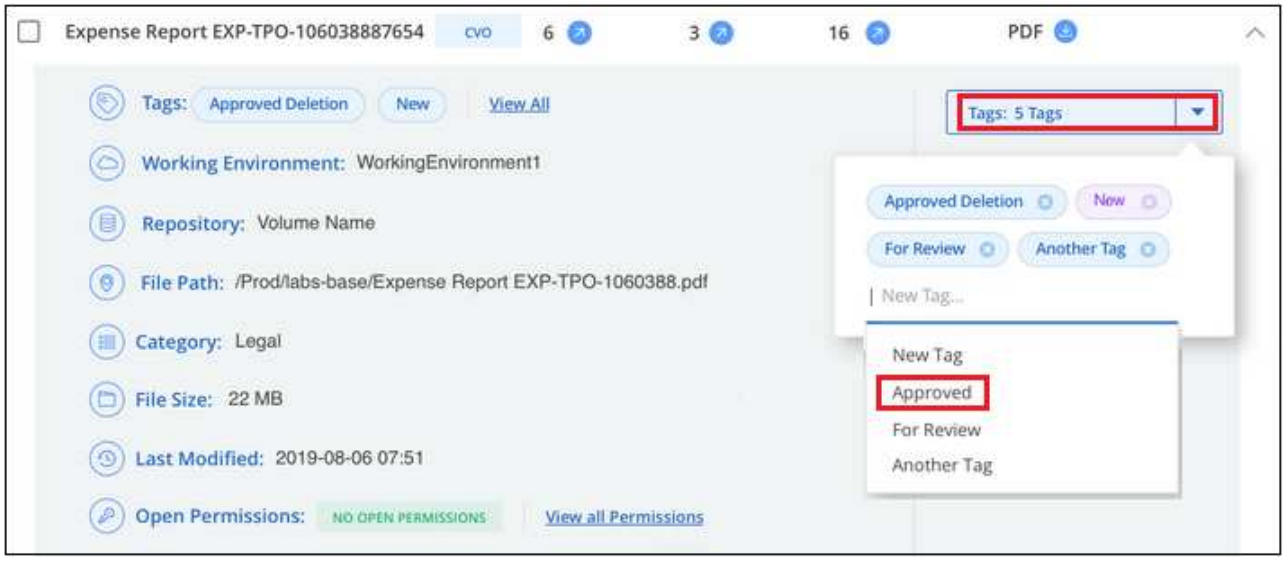
Atribuir tags a arquivos

Você pode adicionar tags a um único arquivo ou a um grupo de arquivos.

Para adicionar uma tag a um único arquivo:

Passos

1. No painel resultados da investigação de dados, clique em para o ficheiro para expandir os detalhes dos metadados do ficheiro.
2. Clique no campo **Tags** e as tags atualmente atribuídas serão exibidas.
3. Adicione a tag ou tags:
   - Para atribuir uma tag existente, clique no campo **New Tag…** e comece a digitar o nome da tag. Quando a tag que você está procurando for exibida, selecione-a e pressione **Enter**.
   - Para criar uma nova tag e atribuí-la ao arquivo, clique no campo **New Tag…**, digite o nome da nova tag e pressione **Enter**.



A tag aparece nos metadados do arquivo.

Para adicionar uma tag a vários arquivos:

Passos

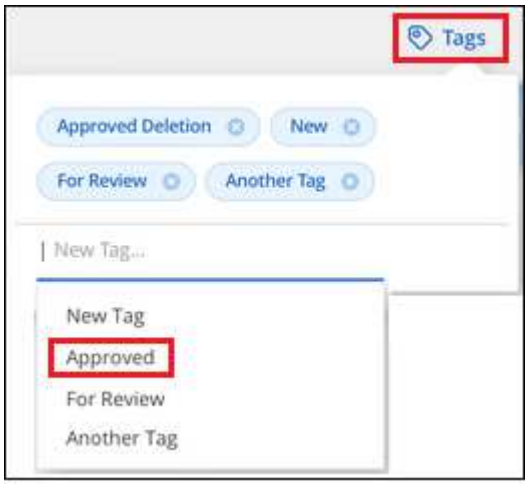
1. No painel resultados da investigação de dados, selecione o arquivo ou os arquivos que você deseja marcar.

   - Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
   - Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).
   - Para selecionar todos os arquivos em todas as páginas, marque a caixa na linha de título (File Name) e, em seguida, na mensagem pop-up All **20** Items on this page selected Select all Items in list (63K Items), clique em **Selecionar todos os itens na lista (itens xxx)**.

     Você pode aplicar tags a um máximo de 100.000 arquivos de cada vez.

2. Na barra de botões, clique em **Tags** e as tags atualmente atribuídas são exibidas.
3. Adicione a tag ou tags:
   - Para atribuir uma tag existente, clique no campo **New Tag…** e comece a digitar o nome da tag. Quando a tag que você está procurando for exibida, selecione-a e pressione **Enter**.

◦ Para criar uma nova tag e atribuí-la ao arquivo, clique no campo **New Tag…**, digite o nome da nova tag e pressione **Enter**.



4. Aprovar a adição das tags na caixa de diálogo de confirmação e as tags são adicionadas aos metadados para todos os arquivos selecionados.

Excluir tags de arquivos

Você pode excluir uma tag se não precisar mais usá-la.

Basta clicar no **x** para obter uma tag existente.

Se você selecionou vários arquivos, a tag será removida de todos os arquivos.

Atribua usuários para gerenciar determinados arquivos

Você pode atribuir um usuário do BlueXP a um arquivo específico ou a vários arquivos, para que a pessoa possa ser responsável por quaisquer ações de acompanhamento que precisam ser feitas no arquivo. Esse recurso é frequentemente usado com o recurso para adicionar tags de status personalizadas a um arquivo.

Por exemplo, você pode ter um arquivo que contém certos dados pessoais que permite que muitos usuários leiam e gravem o acesso (permissões abertas). Assim, você pode atribuir a tag Status "alterar permissões" e atribuir este arquivo ao usuário "Joan Smith" para que eles possam decidir como corrigir o problema. Quando eles corrigirem o problema, eles poderiam alterar a tag Status para "Completed" (Concluído).

Observe que o nome de usuário não é adicionado ao arquivo como parte dos metadados do arquivo - ele é visto apenas pelos usuários do BlueXP ao usar a classificação BlueXP .

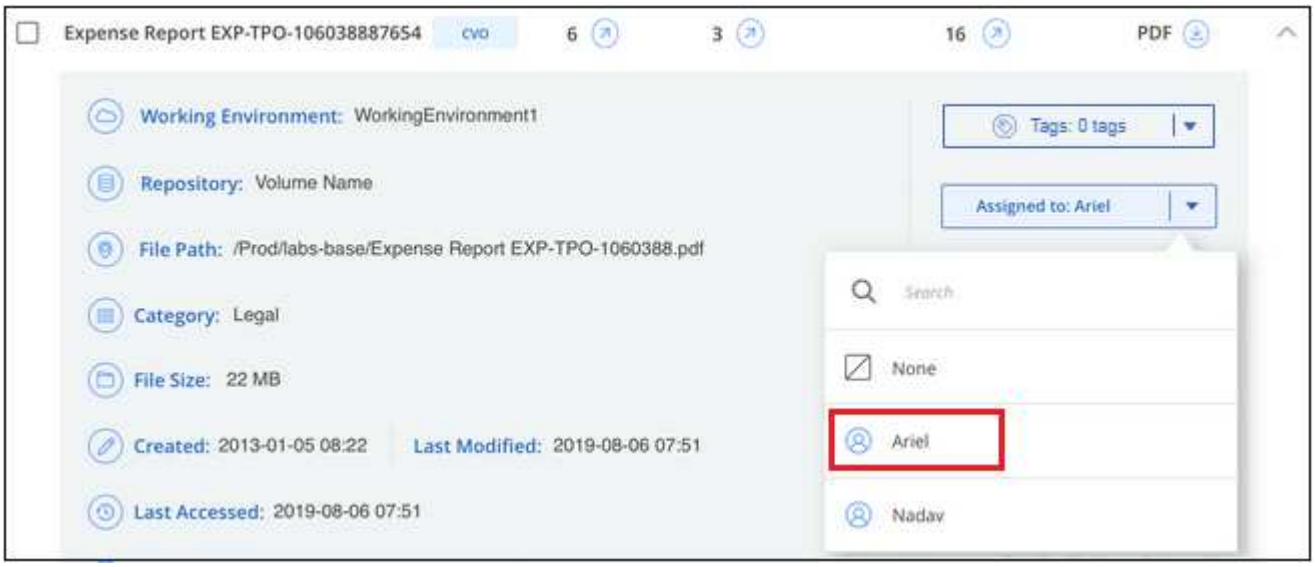
Um novo filtro na página de investigação permite visualizar facilmente todos os ficheiros que têm a mesma pessoa no campo "atribuído a".

Siga estas etapas para atribuir um usuário a um único arquivo.

Passos

1. No painel resultados da investigação de dados, clique em para o ficheiro para expandir os detalhes dos metadados do ficheiro.

2. Clique no campo **Assigned to** e selecione o nome de usuário.



O Nome de utilizador aparece nos metadados do ficheiro.

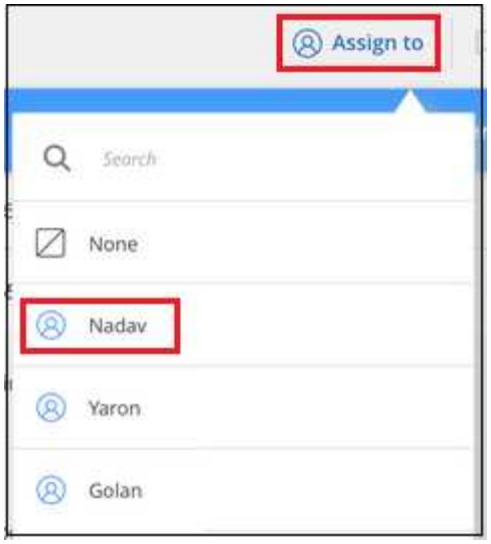
Siga estas etapas para atribuir um usuário a vários arquivos. Observe que você pode atribuir um usuário a um máximo de 20 arquivos de cada vez (uma página na IU).

Passos

1. No painel resultados da investigação de dados, selecione o ficheiro ou os ficheiros que pretende atribuir a um utilizador.

- Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
- Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).

2. Na barra de botões, clique em **Assign to** e selecione o nome de usuário:



O usuário é adicionado aos metadados para todos os arquivos selecionados.

Gerencie seus dados privados

A classificação do BlueXP fornece várias maneiras de gerenciar seus dados privados. Algumas funcionalidades facilitam a preparação para a migração dos seus dados, enquanto outras funcionalidades permitem-lhe fazer alterações nos dados.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

- Você pode copiar arquivos para um compartilhamento NFS de destino se quiser fazer uma cópia de certos dados e movê-los para um local NFS diferente.
- Você pode clonar um volume ONTAP para um novo volume, incluindo apenas arquivos selecionados do volume de origem no novo volume clonado. Isso é útil para situações em que você está migrando dados e deseja excluir certos arquivos do volume original.
- Você pode copiar e sincronizar arquivos de um repositório de origem para um diretório em um local de destino específico. Isso é útil para situações em que você está migrando dados de um sistema de origem para outro, enquanto ainda há alguma atividade final nos arquivos de origem.
- Você pode mover arquivos de origem que a classificação do BlueXP está digitalizando para qualquer compartilhamento NFS.
- Você pode excluir arquivos que parecem inseguros ou muito arriscados para deixar em seu sistema de armazenamento, ou que você identificou como duplicados.

- As capacidades descritas nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma varredura somente de mapeamento não mostram detalhes no nível do arquivo.
- Os dados das contas do Google Drive não podem usar nenhum desses recursos no momento.

Copiar ficheiros de origem

Você pode copiar qualquer arquivo de origem que a classificação BlueXP esteja digitalizando. Existem três tipos de operações de cópia dependendo do que você está tentando realizar:

- **Copie arquivos** do mesmo ou de diferentes volumes ou fontes de dados para um compartilhamento NFS de destino.

  Isso é útil se você quiser fazer uma cópia de certos dados e movê-los para um local NFS diferente.

- **Clonar um volume ONTAP** para um novo volume no mesmo agregado, mas incluir somente arquivos selecionados do volume de origem no novo volume clonado.

  Isso é útil para situações em que você está migrando dados e deseja excluir certos arquivos do volume original. Esta ação usa a "NetApp FlexClone" funcionalidade para duplicar rapidamente o volume e, em seguida, remover os arquivos que você **não** selecionou.

- **Copie e sincronize arquivos** de um único repositório de origem (volume ONTAP, bucket S3, compartilhamento NFS, etc.) para um diretório em um local de destino específico (destino).

  Isso é útil para situações em que você está migrando dados de um sistema de origem para outro. Após a cópia inicial, o serviço sincroniza todos os dados alterados com base na programação definida. Esta ação usa a "Cópia e sincronização do NetApp BlueXP " funcionalidade para copiar e sincronizar dados de uma origem para um destino.

Copiar arquivos de origem para um compartilhamento NFS

Você pode copiar arquivos de origem que a classificação do BlueXP está digitalizando para qualquer compartilhamento NFS. O compartilhamento NFS não precisa ser integrado à classificação BlueXP , basta saber o nome do compartilhamento NFS onde todos os arquivos selecionados serão copiados no formato `<host_name>:/<share_path>`.

Você não pode copiar arquivos que residem em bancos de dados.

Requisitos

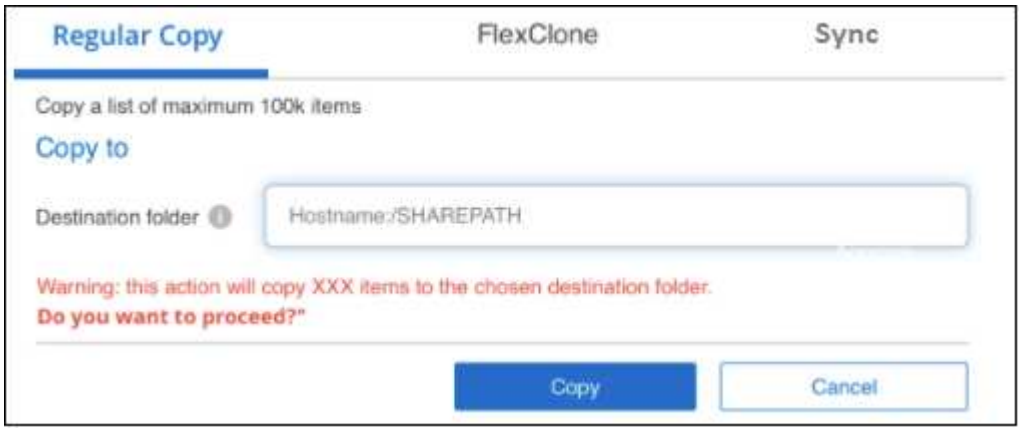
- Você deve ter permissões para copiar arquivos. "Saiba mais sobre o acesso do usuário às informações de conformidade".
- A cópia de arquivos requer que o compartilhamento NFS de destino permita o acesso a partir da instância de classificação BlueXP .
- Você pode copiar entre 1 e 100.000 arquivos de cada vez.

Passos

1. No painel resultados da investigação de dados, selecione o arquivo ou os arquivos que deseja copiar e clique em **Copiar**.

- Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
- Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).
- Para selecionar todos os arquivos em todas as páginas, marque a caixa na linha de título (File Name) e, em seguida, na mensagem pop-up All **20** Items on this page selected Select all Items in list (63K Items), clique em **Selecionar todos os itens na lista (itens xxx)**.

2. Na caixa de diálogo *Copiar arquivos*, selecione a guia **cópia regular**.



3. Digite o nome do compartilhamento NFS onde todos os arquivos selecionados serão copiados no formato `<host_name>:/<share_path>`e clique em **Copiar**.

   É apresentada uma caixa de diálogo com o estado da operação de cópia.

Pode ver o progresso da operação de cópia no "Painel Status ações".

Observe que você também pode copiar um arquivo individual ao exibir os detalhes dos metadados de um arquivo. Basta clicar em **Copiar ficheiro**.

Clone dados de volume para um novo volume

Você pode clonar um volume ONTAP existente que a classificação BlueXP está digitalizando usando a funcionalidade NetApp *FlexClone*. Isso permite que você duplique rapidamente o volume, incluindo apenas os arquivos selecionados. Isso é útil se você estiver migrando dados e quiser excluir certos arquivos do volume original ou se quiser criar uma cópia de um volume para teste.

O novo volume é criado no mesmo agregado que o volume de origem. Certifique-se de que tem espaço suficiente para este novo volume no agregado antes de iniciar esta tarefa. Contacte o administrador de armazenamento, se necessário.

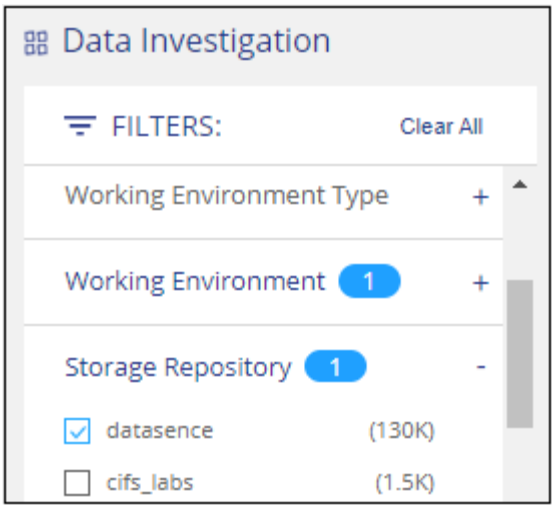
Nota: os volumes FlexGroup não podem ser clonados porque não são suportados pelo FlexClone.

Requisitos

- Você deve ter permissões para copiar arquivos. "Saiba mais sobre o acesso do usuário às informações de conformidade".
- Você deve selecionar um mínimo de 20 arquivos.
- Todos os arquivos selecionados devem ter o mesmo volume e o volume deve estar on-line.
- O volume deve ser de um sistema Cloud Volumes ONTAP ou ONTAP no local. Nenhuma outra fonte de dados é suportada atualmente.
- A licença FlexClone deve ser instalada no cluster. Esta licença é instalada por padrão em sistemas Cloud Volumes ONTAP.

Passos

1. No painel Investigação de dados, crie um filtro selecionando um único **ambiente de trabalho** e um único **Repositório de armazenamento** para garantir que todos os arquivos sejam do mesmo volume ONTAP.

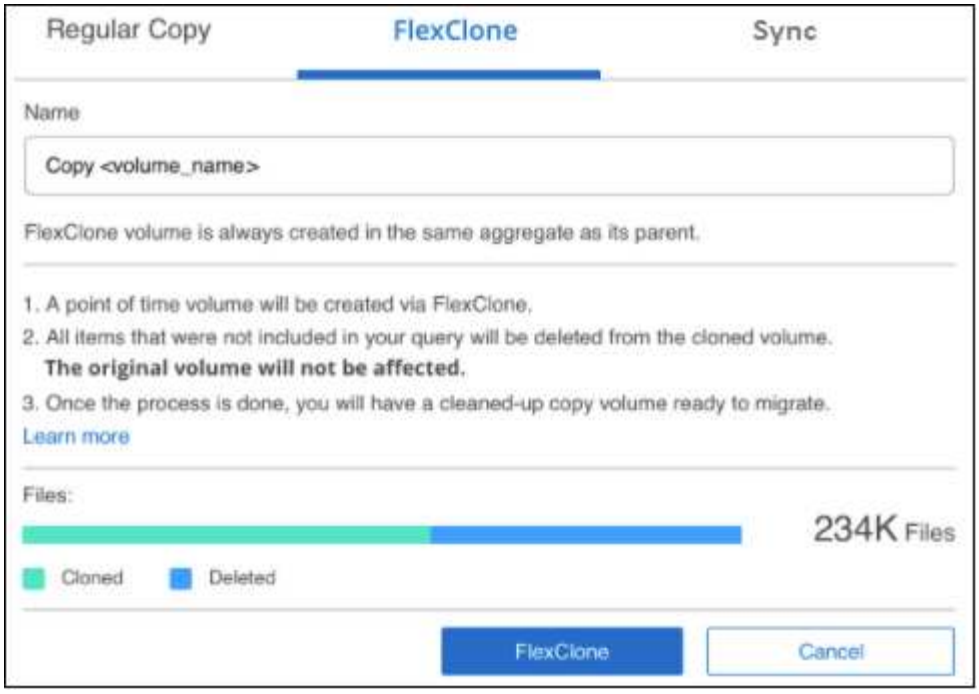


Aplique outros filtros para que você veja apenas os arquivos que deseja clonar para o novo volume.

2. No painel resultados da investigação, selecione os arquivos que deseja clonar e clique em **Copiar**.

- Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
- Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).
- Para selecionar todos os arquivos em todas as páginas, marque a caixa na linha de título (File Name) e, em seguida, na mensagem pop-up All **20** Items on this page selected Select all Items in list (63K Items), clique em **Selecionar todos os itens na lista (itens xxx)**.

3. Na caixa de diálogo *Copiar arquivos*, selecione a guia **FlexClone**. Esta página mostra o número total de arquivos que serão clonados do volume (os arquivos selecionados) e o número de arquivos que não estão incluídos/excluídos (os arquivos que você não selecionou) do volume clonado.



4. Digite o nome do novo volume e clique em **FlexClone**.

   É apresentada uma caixa de diálogo com o estado da operação clone.

Resultado

O novo volume clonado é criado no mesmo agregado que o volume de origem.

É possível visualizar o progresso da operação de clone no "Painel Status ações".

Se você selecionou inicialmente **Mapear todos os volumes** ou **mapear e classificar todos os volumes** quando você ativou a classificação BlueXP para o ambiente de trabalho em que o volume de origem reside, a classificação BlueXP verificará o novo volume clonado automaticamente. Se você não usou nenhuma dessas seleções inicialmente, então, se quiser digitalizar esse novo volume, será necessário "ative a digitalização no volume manualmente".

Copie e sincronize arquivos de origem para um sistema de destino

Você pode copiar arquivos de origem que a classificação BlueXP está digitalizando de qualquer fonte de dados não estruturados suportada para um diretório em um local de ("Locais de destino compatíveis com cópia e sincronização do BlueXP "destino específico). Após a cópia inicial, todos os dados alterados nos arquivos são sincronizados com base na programação configurada.

Isso é útil para situações em que você está migrando dados de um sistema de origem para outro. Esta ação usa a "Cópia e sincronização do NetApp BlueXP " funcionalidade para copiar e sincronizar dados de uma origem para um destino.

Não é possível copiar e sincronizar arquivos que residem em bancos de dados, contas do OneDrive ou contas do SharePoint.

Requisitos

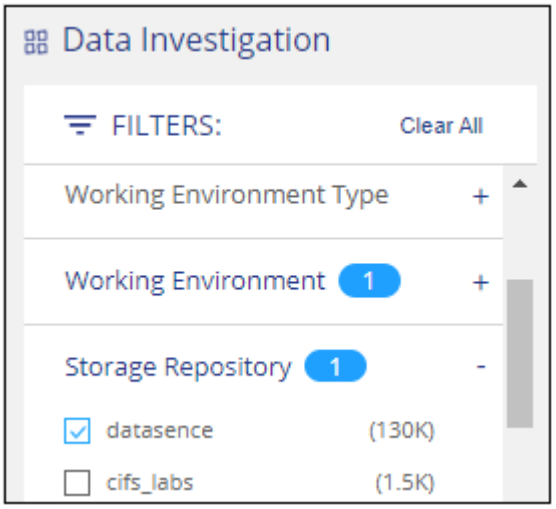
- Você deve ter permissões para copiar e sincronizar arquivos. "Saiba mais sobre o acesso do usuário às informações de conformidade".

- Você deve selecionar um mínimo de 20 arquivos.
- Todos os arquivos selecionados devem ser do mesmo repositório de origem (volume ONTAP, bucket do S3, compartilhamento NFS ou CIFS, etc.).
- Você precisará ativar o serviço de cópia e sincronização do BlueXP e configurar um mínimo de um agente de dados que pode ser usado para transferir arquivos entre os sistemas de origem e destino. Reveja os requisitos de cópia e sincronização do BlueXP a partir do "Descrição de início rápido".

  Observe que o serviço de cópia e sincronização do BlueXP tem taxas de serviço separadas para seus relacionamentos de sincronização e incorrerá em cobranças de recursos se você implantar o agente de dados na nuvem.

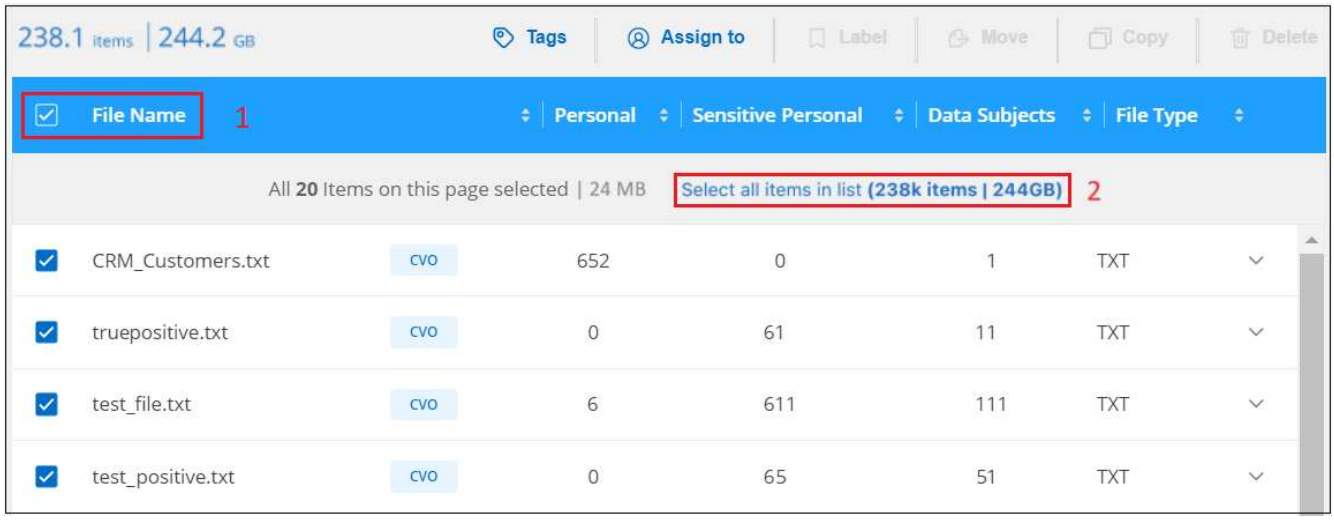
Passos

1. No painel Investigação de dados, crie um filtro selecionando um único **ambiente de trabalho** e um único **Repositório de armazenamento** para garantir que todos os arquivos sejam do mesmo repositório.

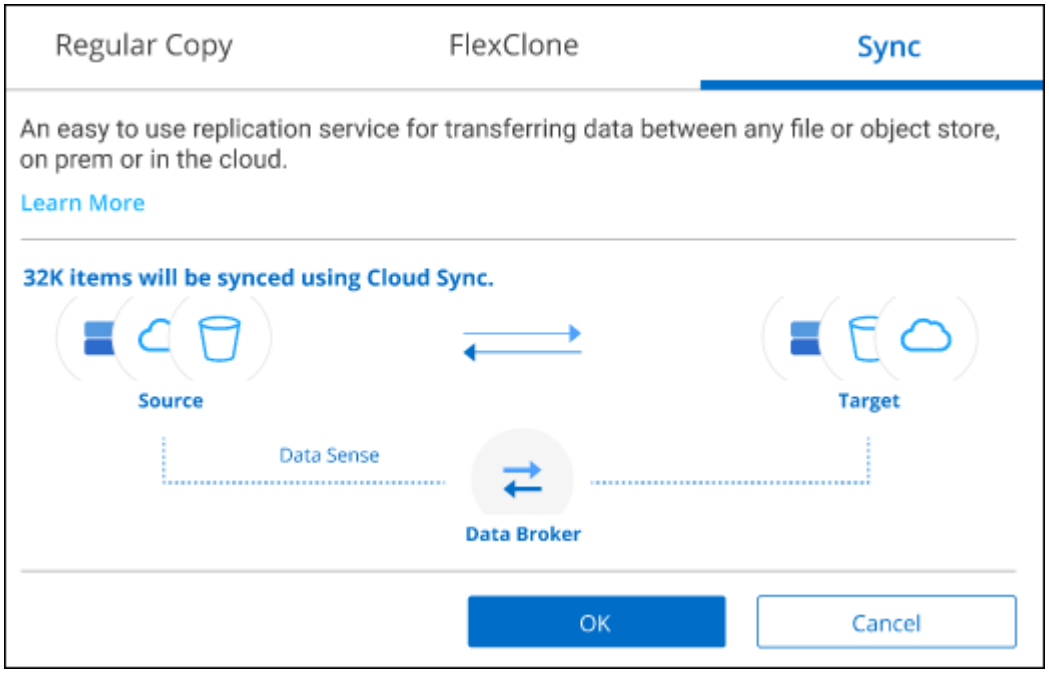


   Aplique outros filtros para que você veja apenas os arquivos que deseja copiar e sincronizar com o sistema de destino.

2. No painel resultados da investigação, selecione todos os arquivos em todas as páginas marcando a caixa na linha de título (File Name), na mensagem pop-up All **20** Items on this page selected Select all Items in list **(63K Items)**clique em **Selecione todos os itens na lista (itens xxx)** e clique em **Copiar**.



3. Na caixa de diálogo *Copy Files*, selecione a guia **Sync**.



4. Se tiver certeza de que deseja sincronizar os arquivos selecionados para um local de destino, clique em **OK**.

   A IU de cópia e sincronização do BlueXP é aberta no BlueXP .

   É-lhe pedido que defina a relação de sincronização. O sistema de origem é pré-preenchido com base no repositório e nos ficheiros que já selecionou na classificação BlueXP .

5. Você precisará selecionar o sistema de destino e, em seguida, selecionar (ou criar) o Data Broker que você pretende usar. Reveja os requisitos de cópia e sincronização do BlueXP a partir do "Descrição de início rápido".

Resultado

Os arquivos são copiados para o sistema de destino e serão sincronizados com base na programação que você definir. Se você selecionar uma sincronização única, os arquivos serão copiados e sincronizados apenas uma vez. Se você escolher uma sincronização periódica, os arquivos serão sincronizados com base na

programação. Observe que se o sistema de origem adicionar novos arquivos que correspondam à consulta criada usando filtros, esses arquivos *new* serão copiados para o destino e sincronizados no futuro.

Observe que algumas das operações de cópia e sincronização BlueXP usuais são desativadas quando são invocadas a partir da classificação BlueXP :

- Não é possível usar os botões **Excluir arquivos na origem** ou **Excluir arquivos no destino**.
- A execução de um relatório está desativada.

Mover arquivos de origem para um compartilhamento NFS

Você pode mover arquivos de origem que a classificação do BlueXP está digitalizando para qualquer compartilhamento NFS. O compartilhamento NFS não precisa ser integrado à classificação BlueXP .

Opcionalmente, você pode deixar um arquivo de breadcrumb no local do arquivo movido. Um arquivo de breadcrumb ajuda seus usuários a entender por que um arquivo foi movido de seu local original. Para cada arquivo movido, o sistema cria um arquivo de breadcrumb no local de origem `<filename>-breadcrumb-<date>.txt` chamado . Você pode adicionar texto na caixa de diálogo que será adicionado ao arquivo de breadcrumb para indicar o local onde o arquivo foi movido e o usuário que moveu o arquivo.

Observe que a estrutura de subdiretório do arquivo de origem é recriada no compartilhamento de destino quando o arquivo é movido, então é mais fácil entender de onde o arquivo foi movido. Se existir um ficheiro com o mesmo nome no local de destino, o ficheiro não será movido.

Você não pode mover arquivos que residem em bancos de dados.

Requisitos

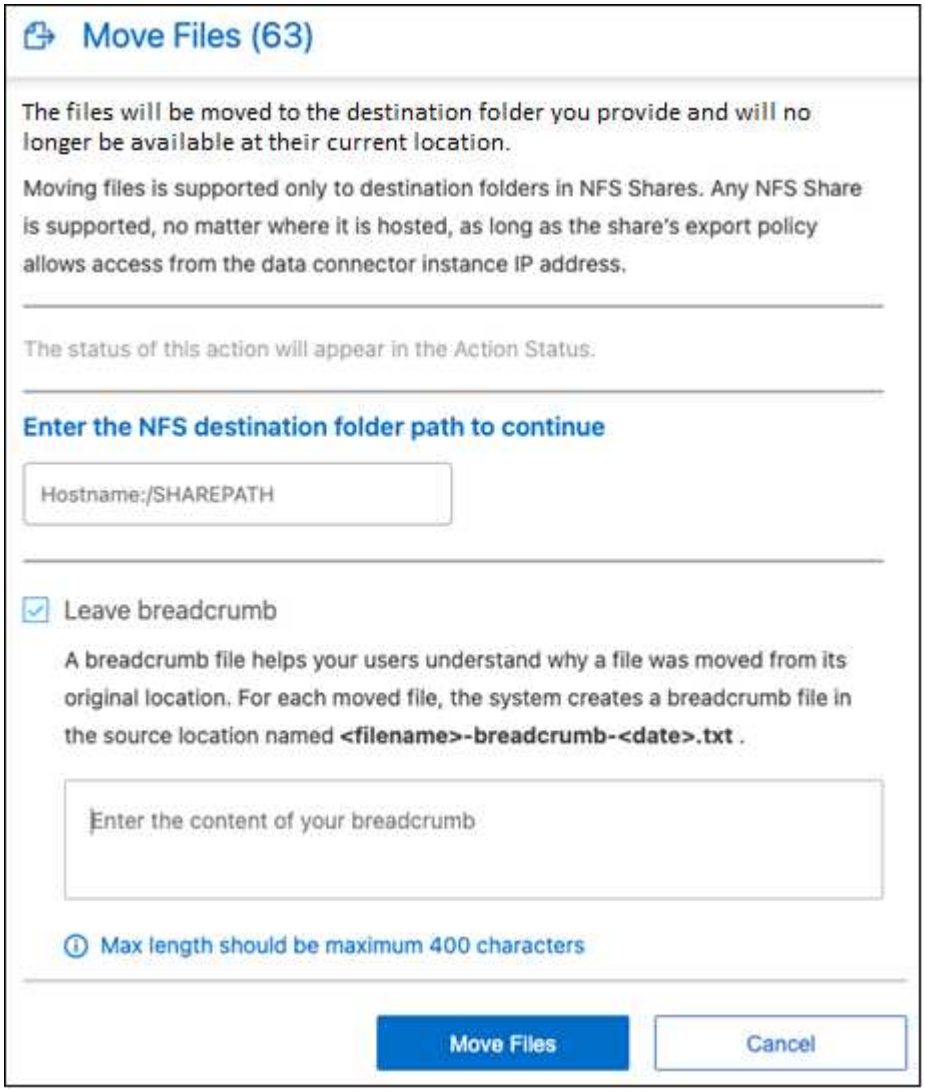
- Você deve ter permissões para mover arquivos. "Saiba mais sobre o acesso do usuário às informações de conformidade".
- Os arquivos de origem podem estar localizados nas seguintes fontes de dados: ONTAP on-premises, Cloud Volumes ONTAP, Azure NetApp Files, compartilhamentos de arquivos e SharePoint Online.
- Você pode mover um máximo de 15 milhões de arquivos de cada vez.
- Apenas os ficheiros com 50 MB ou menos são movidos.
- O compartilhamento NFS de destino deve permitir o acesso a partir do endereço IP da instância de classificação BlueXP .

Passos

1. No painel resultados da investigação de dados, selecione o ficheiro ou os ficheiros que pretende mover.

- Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
- Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).
- Para selecionar todos os arquivos em todas as páginas, marque a caixa na linha de título (File Name) e, em seguida, na mensagem pop-up All **20** Items on this page selected Select all Items in list (63K Items), clique em **Selecionar todos os itens na lista (itens xxx)**.

2. Na barra de botões, clique em **mover**.



3. Na caixa de diálogo *mover arquivos*, digite o nome do compartilhamento NFS onde todos os arquivos selecionados serão movidos no formato `<host_name>:/<share_path>`.
4. Se você quiser deixar um arquivo de breadcrumb, marque a caixa *deixar breadcrumb*. Você pode inserir texto na caixa de diálogo para indicar o local onde o arquivo foi movido e o usuário que moveu o arquivo, e qualquer outra informação, como o motivo pelo qual o arquivo foi movido.
5. Clique em **mover ficheiros**.

Observe que você também pode mover um arquivo individual ao exibir os detalhes dos metadados de um arquivo. Basta clicar em **mover ficheiro**.

Eliminar ficheiros de origem

Você pode remover permanentemente arquivos de origem que parecem inseguros ou muito arriscados para sair em seu sistema de armazenamento, ou que você identificou como uma duplicata. Esta ação é permanente e não há desfazer ou restaurar.

Você pode excluir arquivos manualmente do painel de investigação ou "Usando políticas automaticamente".

Não é possível excluir arquivos que residem em bancos de dados. Todas as outras fontes de dados são suportadas.

A exclusão de arquivos requer as seguintes permissões:

- Para dados NFS - a política de exportação precisa ser definida com permissões de gravação.
- Para dados CIFS - as credenciais CIFS precisam ter permissões de gravação.
- Para dados S3 - a função IAM deve incluir a seguinte permissão: `s3:DeleteObject`.

Excluir arquivos de origem manualmente

Requisitos

- Você deve ter permissões para excluir arquivos. "Saiba mais sobre o acesso do usuário às informações de conformidade".
- Pode eliminar um máximo de 100.000 ficheiros de cada vez.

Passos

1. No painel resultados da investigação de dados, selecione o ficheiro ou os ficheiros que pretende eliminar.

- Para selecionar arquivos individuais, marque a caixa para cada arquivo (Volume_1).
- Para selecionar todos os arquivos na página atual, marque a caixa na linha de título (File Name).
- Para selecionar todos os arquivos em todas as páginas, marque a caixa na linha de título (File Name) e, em seguida, na mensagem pop-up All **20** Items on this page selected Select all Items in list (63K Items), clique em **Selecionar todos os itens na lista (itens xxx)**.

2. Na barra de botões, clique em **Excluir**.
3. Como a operação de exclusão é permanente, você deve digitar "**permanentemente delete**" na caixa de diálogo *Delete File* subsequente e clicar em **Delete File**.

Pode ver o progresso da operação de eliminação no "Painel Status ações".

Observe que você também pode excluir um arquivo individual ao exibir os detalhes dos metadados de um arquivo. Basta clicar em **Excluir arquivo**.

Adicione identificadores de dados pessoais às suas análises de classificação do BlueXP

A classificação BlueXP fornece muitas maneiras de adicionar uma lista personalizada de "dados pessoais" que a classificação BlueXP identificará em futuras verificações, dando a você uma visão completa sobre onde os dados potencialmente confidenciais residem em *all* arquivos de suas organizações.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

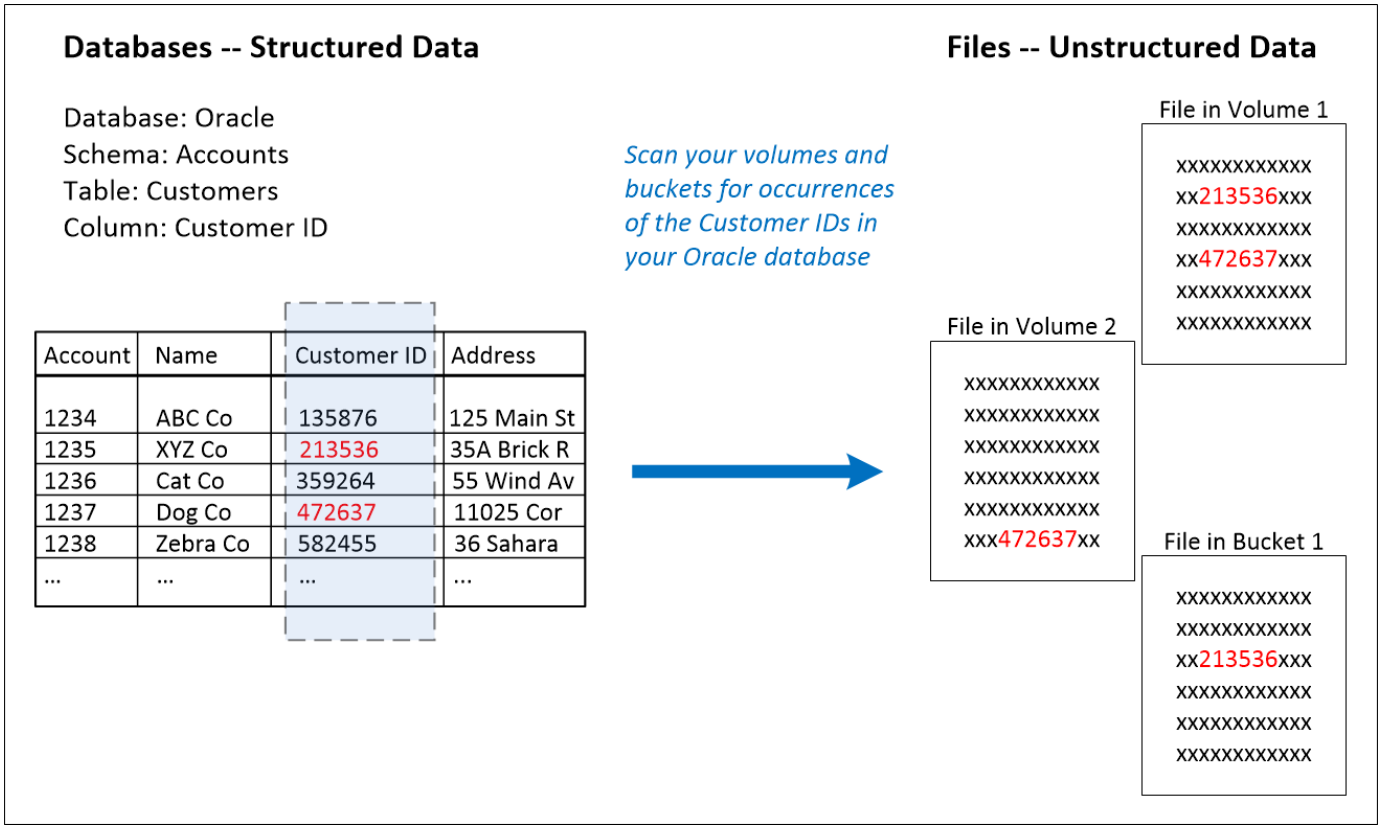
- Você pode adicionar identificadores exclusivos com base em colunas específicas em bancos de dados que você está digitalizando.
- Você pode adicionar palavras-chave personalizadas a partir de um arquivo de texto - essas palavras são identificadas dentro de seus dados.
- Você pode adicionar um padrão pessoal usando uma expressão regular (regex) — o regex é adicionado aos padrões predefinidos existentes.
- Você pode adicionar categorias personalizadas para identificar onde categorias específicas de informações são encontradas em seus dados.

Todos esses mecanismos para adicionar critérios de digitalização personalizados são suportados em todos os idiomas.

As capacidades descritas nesta secção só estão disponíveis se tiver optado por efetuar uma análise de classificação completa nas suas fontes de dados. As fontes de dados que tiveram uma varredura somente de mapeamento não mostram detalhes no nível do arquivo.

Adicione identificadores de dados pessoais personalizados a partir de seus bancos de dados

Um recurso que chamamos *Data Fusion* permite que você analise os dados de suas organizações para identificar se identificadores exclusivos de seus bancos de dados são encontrados em qualquer uma de suas outras fontes de dados. Você pode escolher os identificadores adicionais que a classificação do BlueXP procurará em suas verificações selecionando uma coluna específica, ou colunas, em uma tabela de banco de dados. Por exemplo, o diagrama abaixo mostra como o Data Fusion é usado para verificar seus volumes, buckets e bancos de dados para ocorrências de todas as suas IDs de cliente do seu banco de dados Oracle.



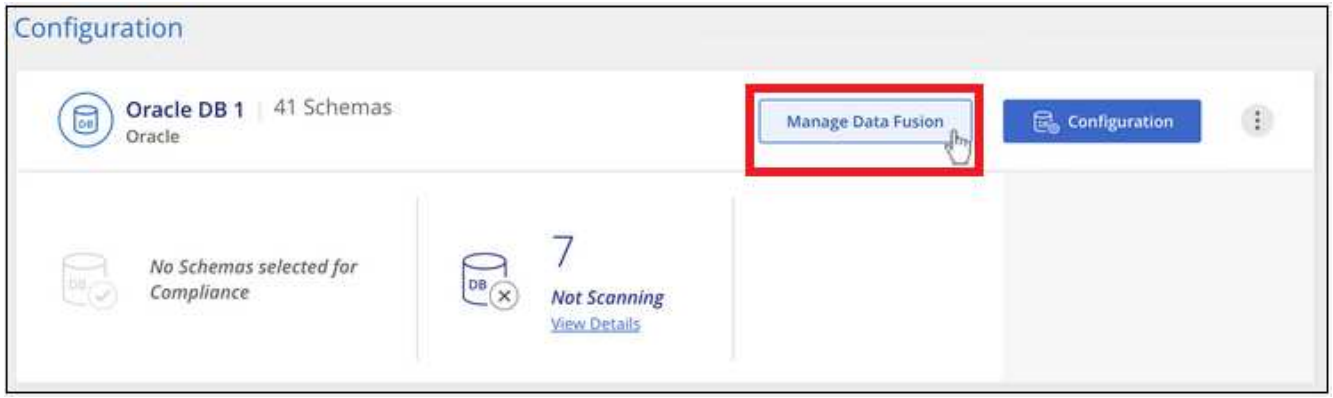
Como você pode ver, dois IDs de cliente exclusivos foram encontrados em dois volumes e em um bucket do S3. Quaisquer correspondências em tabelas de banco de dados também serão identificadas.

Observe que, uma vez que você está digitalizando seus próprios bancos de dados, qualquer idioma em que seus dados estejam armazenados será usado para identificar dados em futuras análises de classificação do BlueXP .

Passos

É necessário ter "adicionado pelo menos um servidor de banco de dados" que classificar BlueXP antes de poder adicionar fontes de dados Fusion.

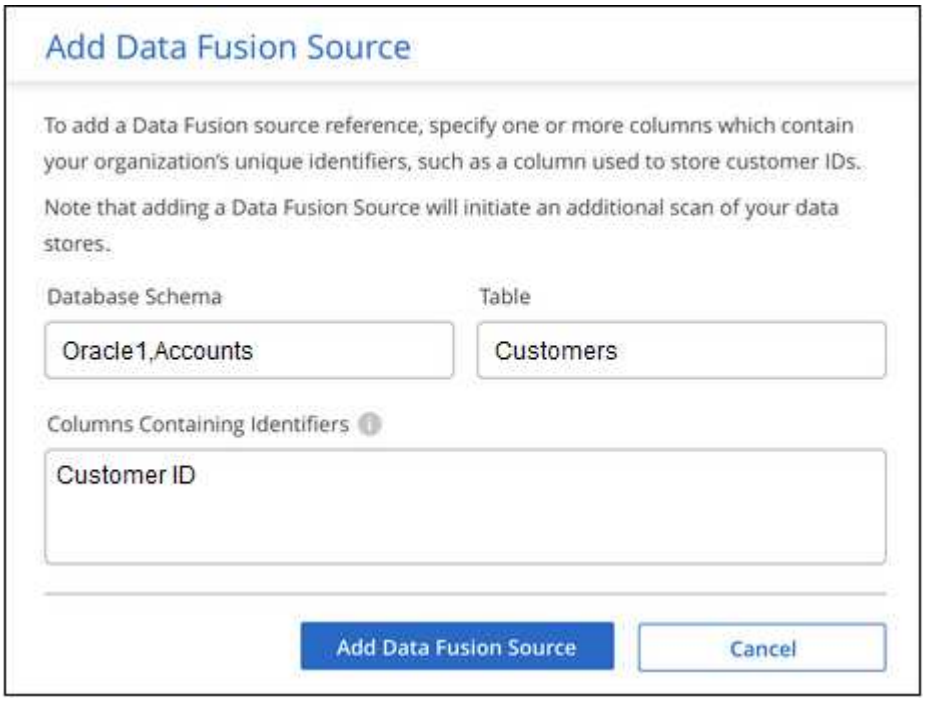
1. Na página Configuração, clique em **Manage Data Fusion** no banco de dados onde residem os dados de origem.



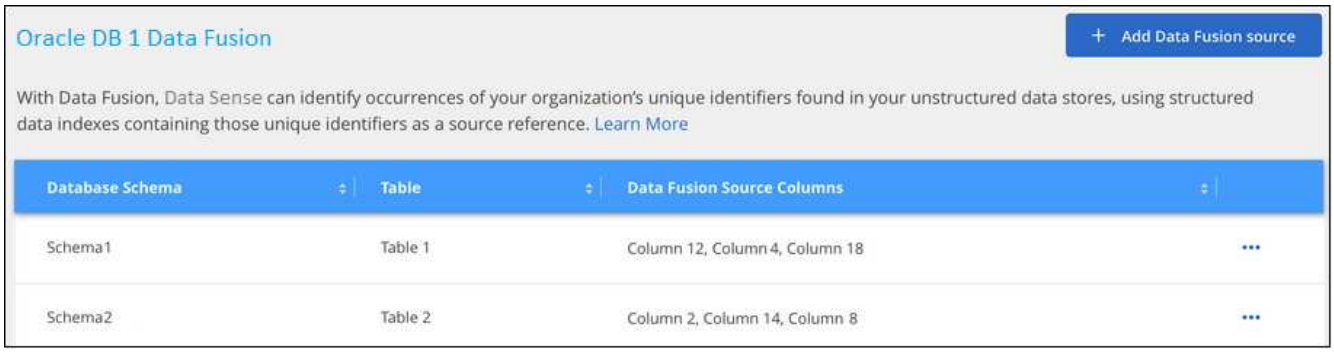
2. Clique em **Adicionar fonte de dados Fusion** na próxima página.
3. Na página *Adicionar origem do Fusion de dados*:

a. Selecione o esquema do banco de dados no menu suspenso.
b. Insira o nome da tabela nesse esquema.
c. Insira a coluna, ou colunas, que contêm os identificadores exclusivos que você deseja usar.

   Ao adicionar várias colunas, insira o nome de cada coluna ou nome de exibição de tabela em uma linha separada.

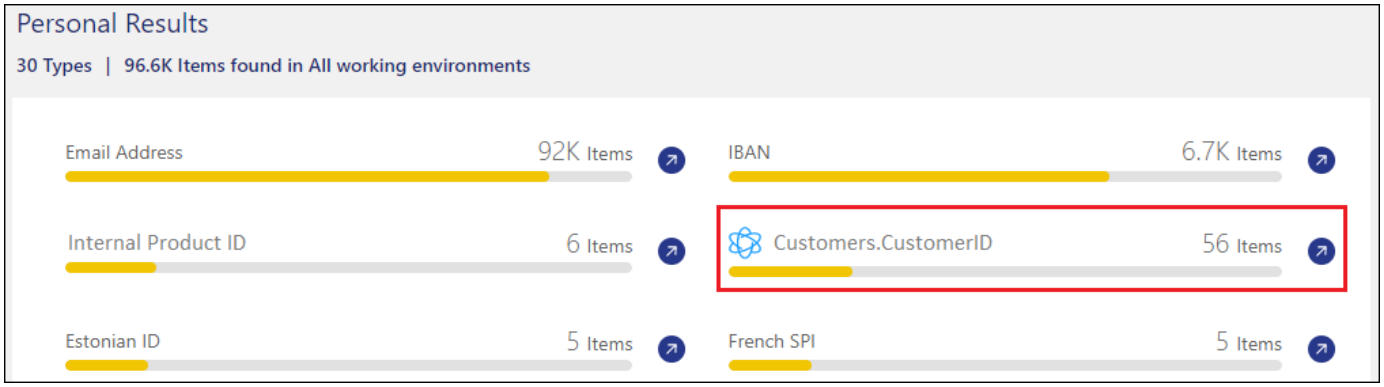


4. Clique em **Adicionar fonte de Fusion de dados**.



Resultados

Após a próxima verificação, os resultados incluirão essas novas informações no Painel de conformidade, na seção "resultados pessoais", e na página de investigação no filtro "dados pessoais". O nome usado para o classificador aparece na lista de filtros, por `Customers.CustomerID` exemplo .



Excluir uma fonte de Data Fusion

Se, em algum momento, você decidir não digitalizar seus arquivos usando uma determinada fonte de dados Fusion, você pode selecionar a linha de origem na página de inventário do Data Fusion e clicar em **Excluir fonte de dados Fusion**.

Adicione palavras-chave personalizadas a partir de uma lista de palavras

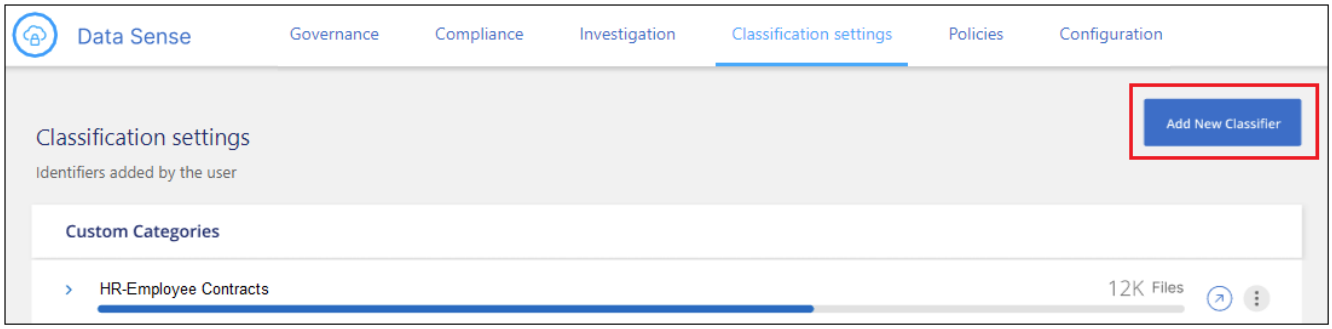
Você pode adicionar palavras-chave personalizadas à classificação do BlueXP para que ele identifique onde essas informações são encontradas em seus dados. Você adiciona as palavras-chave apenas inserindo cada palavra que você quer que a classificação BlueXP reconheça. As palavras-chave são adicionadas às palavras-chave pré-definidas existentes que a classificação BlueXP já usa, e os resultados serão visíveis na seção padrões pessoais.

Por exemplo, você pode querer ver onde nomes de produto internos são mencionados em todos os seus arquivos para garantir que esses nomes não estejam acessíveis em locais que não sejam seguros.

Depois de atualizar as palavras-chave personalizadas, a classificação BlueXP reiniciará a digitalização de todas as fontes de dados. Após a conclusão do exame, os novos resultados serão apresentados no Painel de controlo de conformidade da classificação do BlueXP , na secção "resultados pessoais", e na página de investigação no filtro "dados pessoais".

Passos

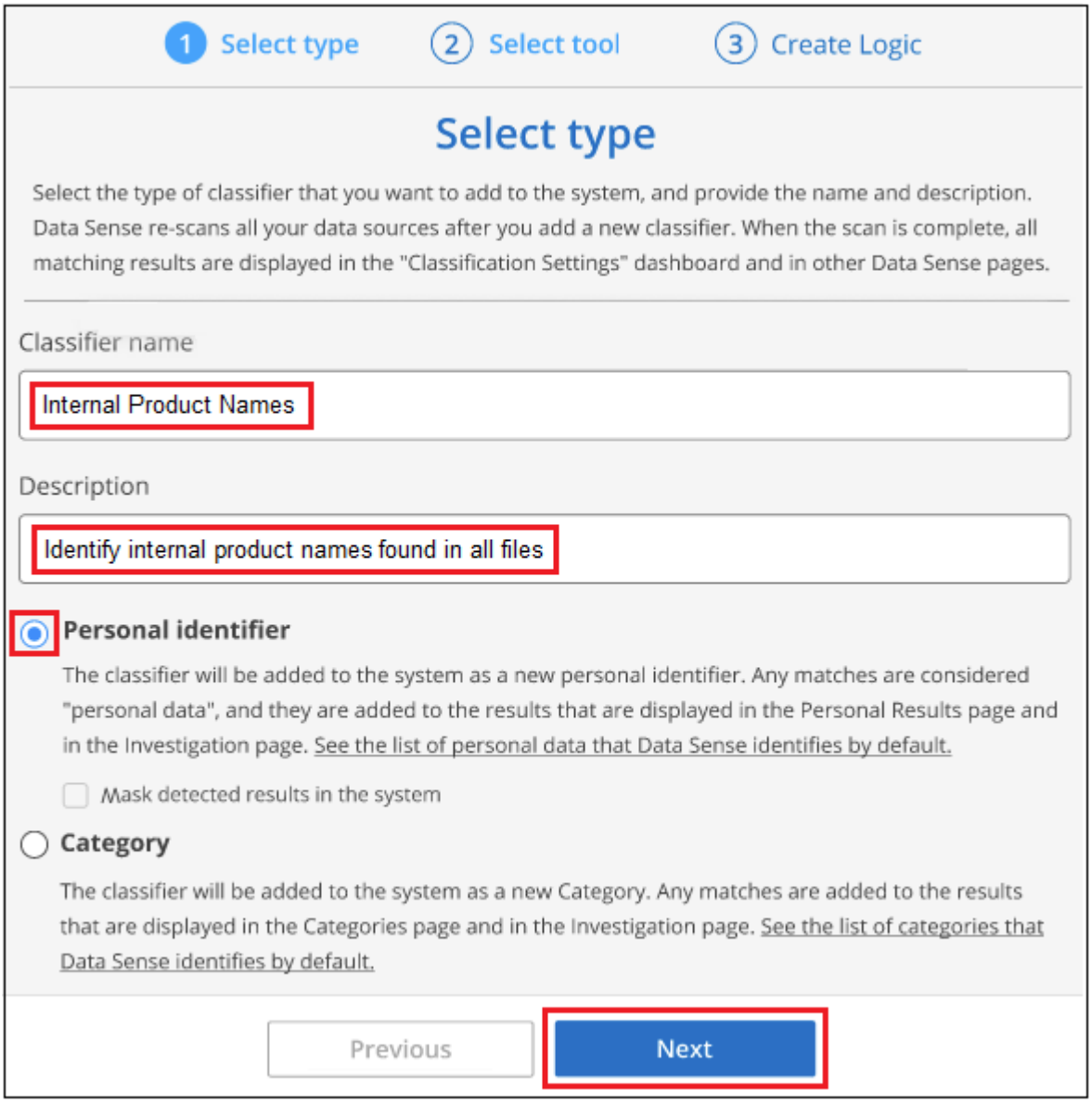
1. Na guia *Configurações de classificação*, clique em **Adicionar novo classificador** para iniciar o assistente *Adicionar classificador personalizado*.



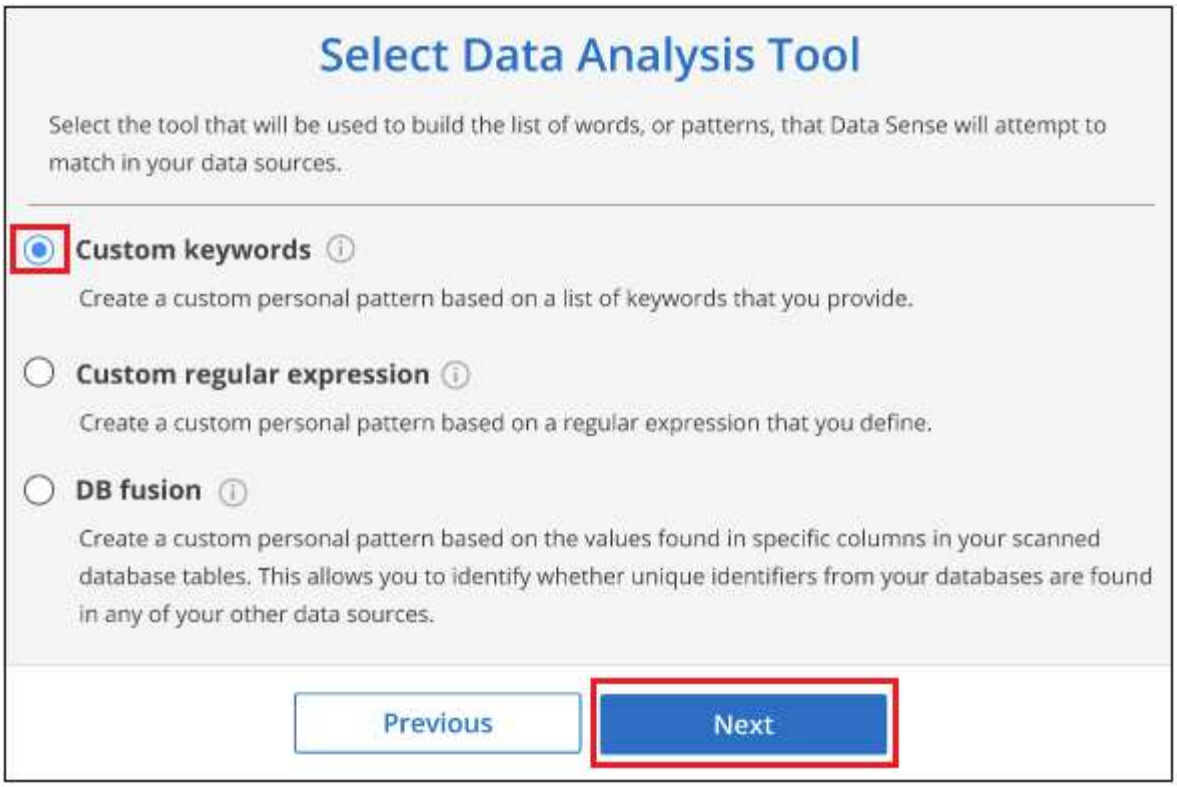
2. Na página *Selecionar tipo*, digite o nome do classificador, forneça uma breve descrição, selecione **Identificador Pessoal** e clique em **Avançar**.

   O nome inserido aparecerá na IU de classificação do BlueXP como o título dos arquivos digitalizados que correspondem aos requisitos do classificador e como o nome do filtro na página de investigação.

   Você também pode marcar a caixa "Máscara de resultados detetados no sistema" para que o resultado completo não apareça na IU. Por exemplo, você pode querer fazer isso para ocultar números completos de cartão de crédito ou dados pessoais semelhantes (a máscara aparecerá na interface do usuário como esta: "Pass:[**] **** ******" 3434).

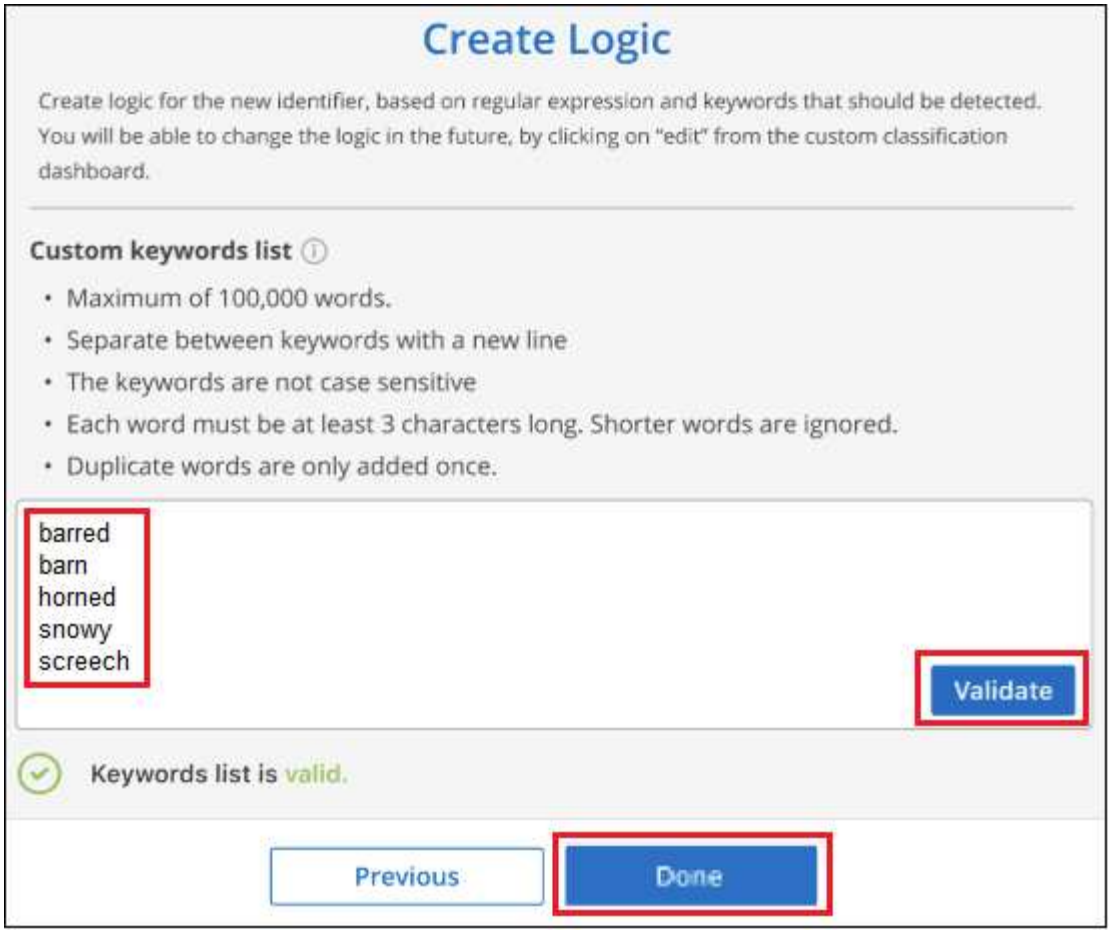


3. Na página *Select Data Analysis Tool*, selecione **Custom Keywords** como o método que você deseja usar para definir o classificador e clique em **Next**.



4. Na página *Create Logic*, insira as palavras-chave que deseja reconhecer - cada palavra em uma linha separada - e clique em **Validar**.

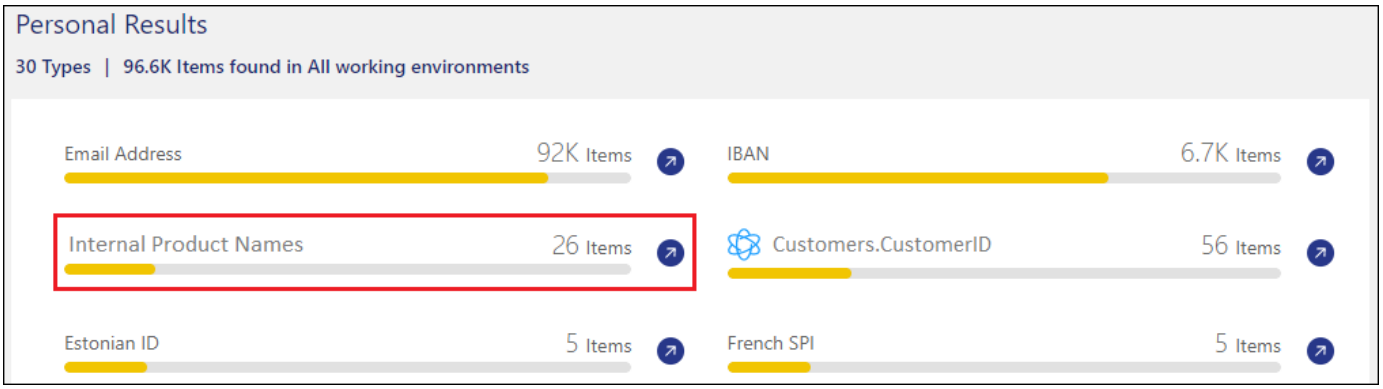
   A captura de tela abaixo mostra os nomes de produto internos (diferentes tipos de corujas). A pesquisa de classificação BlueXP para esses itens não é sensível a maiúsculas e minúsculas.



5. Clique em **Done** e a classificação BlueXP começa a redigitalizar seus dados.

Resultados

Após a conclusão da verificação, os resultados incluirão essas novas informações no Painel de conformidade, na seção "resultados pessoais", e na página de investigação no filtro "dados pessoais".



Como você pode ver, o nome do classificador é usado como o nome no painel resultados pessoais. Desta forma, você pode ativar muitos grupos diferentes de palavras-chave e ver os resultados para cada grupo.

Adicione identificadores de dados pessoais personalizados usando uma regex

Você pode adicionar um padrão pessoal para identificar informações específicas em seus dados usando uma expressão regular personalizada (regex). Isso permite que você crie uma nova regex personalizada para identificar novos elementos de informações pessoais que ainda não existem no sistema. O regex é adicionado

aos padrões pré-definidos existentes que a classificação BlueXP já usa, e os resultados serão visíveis na seção padrões pessoais.

Por exemplo, você pode querer ver onde suas IDs de produto internas são mencionadas em todos os seus arquivos. Se a ID do produto tiver uma estrutura clara, por exemplo, é um número de 12 dígitos que começa com 201, você pode usar o recurso regex personalizado para pesquisá-lo em seus arquivos. A expressão regular para este exemplo é * B201 d'9*.

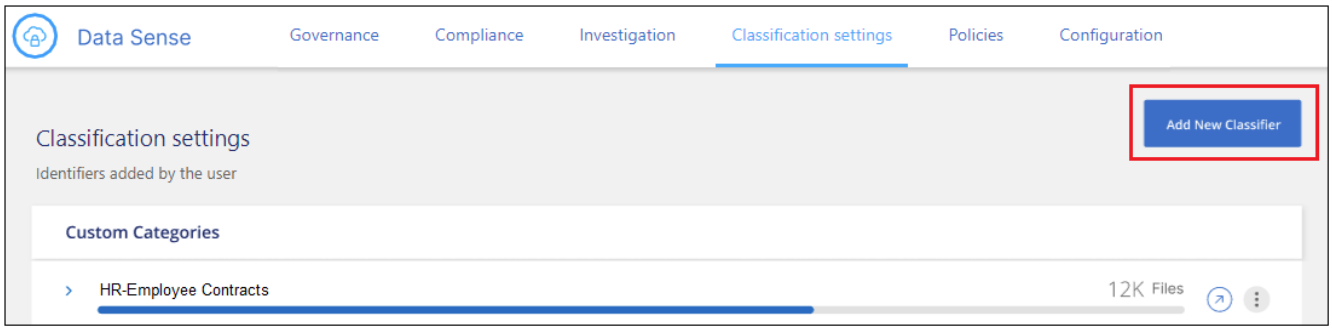
Depois de adicionar o regex, a classificação BlueXP reiniciará a digitalização de todas as fontes de dados. Após a conclusão do exame, os novos resultados serão apresentados no Painel de controlo de conformidade da classificação do BlueXP , na secção "resultados pessoais", e na página de investigação no filtro "dados pessoais".

Se você precisar de ajuda para construir a expressão regular, "Expressões regulares 101" consulte . Escolha **Python** para o sabor para ver os tipos de resultados a classificação BlueXP irá corresponder a partir da expressão regular. O "Página do Python Regex Tester" também é útil ao exibir uma representação gráfica de seus padrões.

Atualmente não permitimos o uso de sinalizadores de padrão ao criar um regex - isso significa que você não deve usar "/".

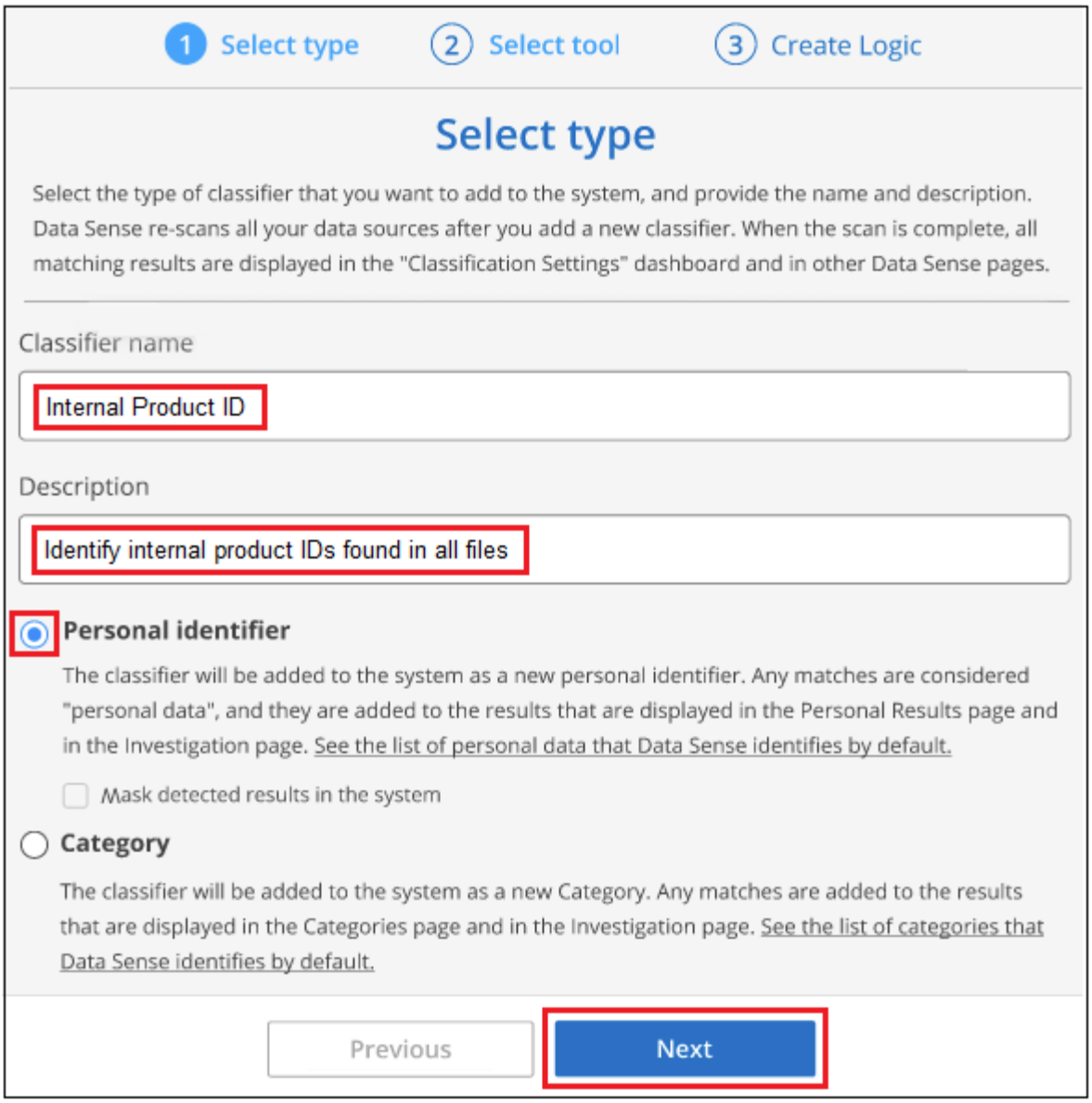
Passos

1. Na guia *Configurações de classificação*, clique em **Adicionar novo classificador** para iniciar o assistente *Adicionar classificador personalizado*.

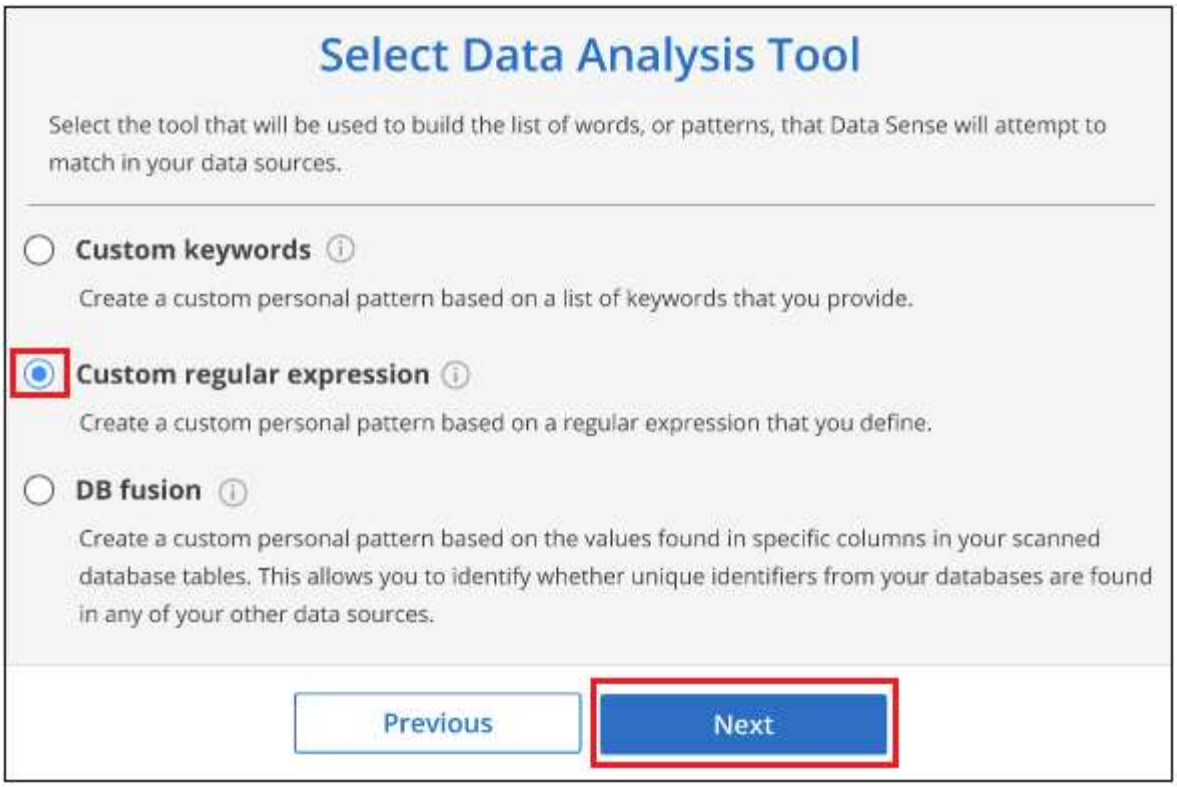


2. Na página *Selecionar tipo*, digite o nome do classificador, forneça uma breve descrição, selecione **Identificador Pessoal** e clique em **Avançar**.

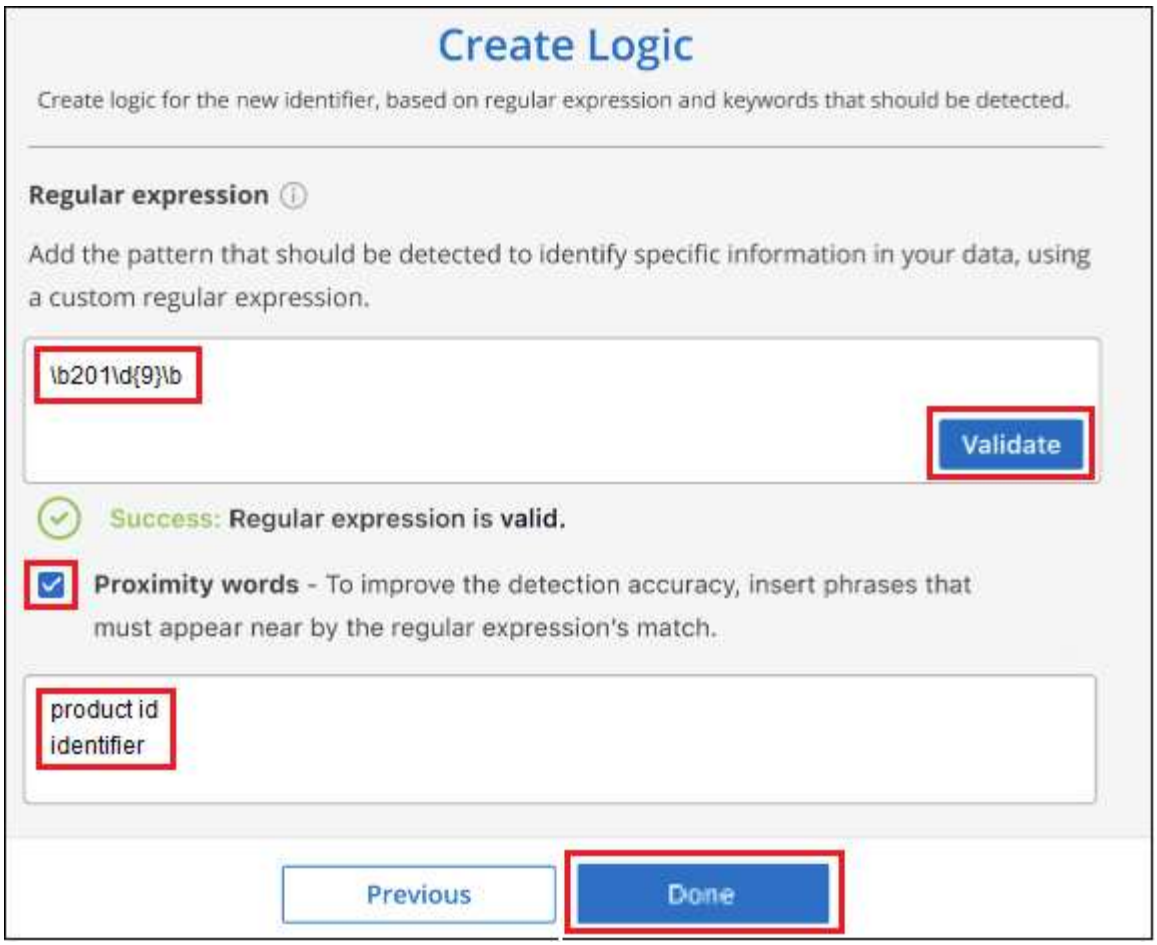
   O nome inserido aparecerá na IU de classificação do BlueXP como o título dos arquivos digitalizados que correspondem aos requisitos do classificador e como o nome do filtro na página de investigação. Você também pode marcar a caixa "Máscara de resultados detetados no sistema" para que o resultado completo não apareça na IU. Por exemplo, você pode querer fazer isso para ocultar números completos de cartão de crédito ou dados pessoais semelhantes.



3. Na página *Select Data Analysis Tool*, selecione **Custom regular expression** como o método que você deseja usar para definir o classificador e clique em **Next**.

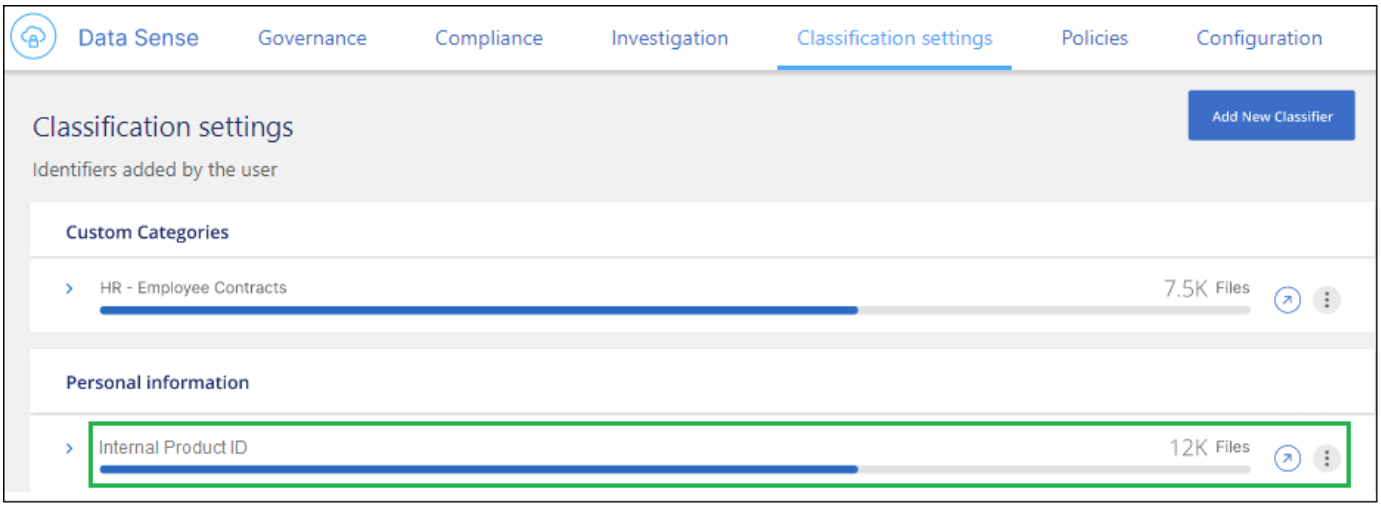


4. Na página *Create Logic*, insira a expressão regular e quaisquer palavras de proximidade e clique em **Done**.
   a. Você pode inserir qualquer expressão regular legal. Clique no botão **Validar** para que a classificação BlueXP verifique se a expressão regular é válida e se ela não é muito ampla — o que significa que retornará muitos resultados.
   b. Opcionalmente, você pode inserir algumas palavras de proximidade para ajudar a refinar a precisão dos resultados. Estas são palavras que normalmente serão encontradas dentro de 300 carateres do padrão que você está procurando (antes ou depois do padrão encontrado). Introduza cada palavra ou frase numa linha separada.



Resultados

O classificador é adicionado e a classificação BlueXP começa a redigitalizar todas as suas fontes de dados. Você será retornado à página Classifiers personalizados, onde você pode exibir o número de arquivos que correspondem ao seu novo classificador. Os resultados da digitalização de todas as suas fontes de dados demorarão algum tempo, dependendo do número de arquivos que precisam ser digitalizados.



Adicionar categorias personalizadas

A classificação BlueXP leva os dados que digitaliza e divide-os em diferentes tipos de categorias. Categorias são tópicos baseados na análise de inteligência artificial do conteúdo e metadados de cada arquivo. "Consulte

a lista de categorias predefinidas".

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

Você pode adicionar categorias personalizadas à classificação do BlueXP para que você possa identificar onde categorias de informações exclusivas para o seu data Estate são encontradas em seus dados. Você adiciona cada categoria criando arquivos de "treinamento" que contêm as categorias de dados que você deseja identificar e, em seguida, fazer com que a classificação BlueXP analise esses arquivos para "aprender" através da IA para que ele possa identificar esses dados em suas fontes de dados. As categorias são adicionadas às categorias predefinidas existentes que a classificação BlueXP já identifica e os resultados são visíveis na seção categorias.

Por exemplo, você pode querer ver onde os arquivos de instalação compatados no formato .gz estão localizados em seus arquivos para que você possa removê-los, se necessário.

Depois de atualizar as categorias personalizadas, a classificação BlueXP reiniciará a digitalização de todas as fontes de dados. Após a conclusão do exame, os novos resultados serão apresentados no Painel de controlo de conformidade da classificação BlueXP , na secção "categorias", e na página de investigação no filtro "Categoria". "Veja como exibir arquivos por categorias".

O que você vai precisar

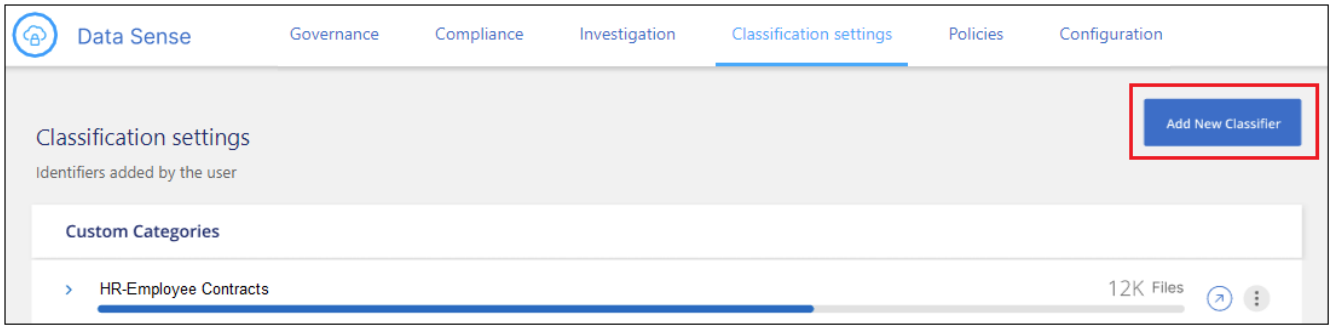
Você precisará criar um mínimo de 25 arquivos de treinamento que contenham amostras das categorias de dados que você deseja que a classificação BlueXP reconheça. Os seguintes tipos de arquivo são suportados:

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

Os arquivos devem ter no mínimo 100 bytes e devem estar localizados em uma pasta acessível pela classificação BlueXP .

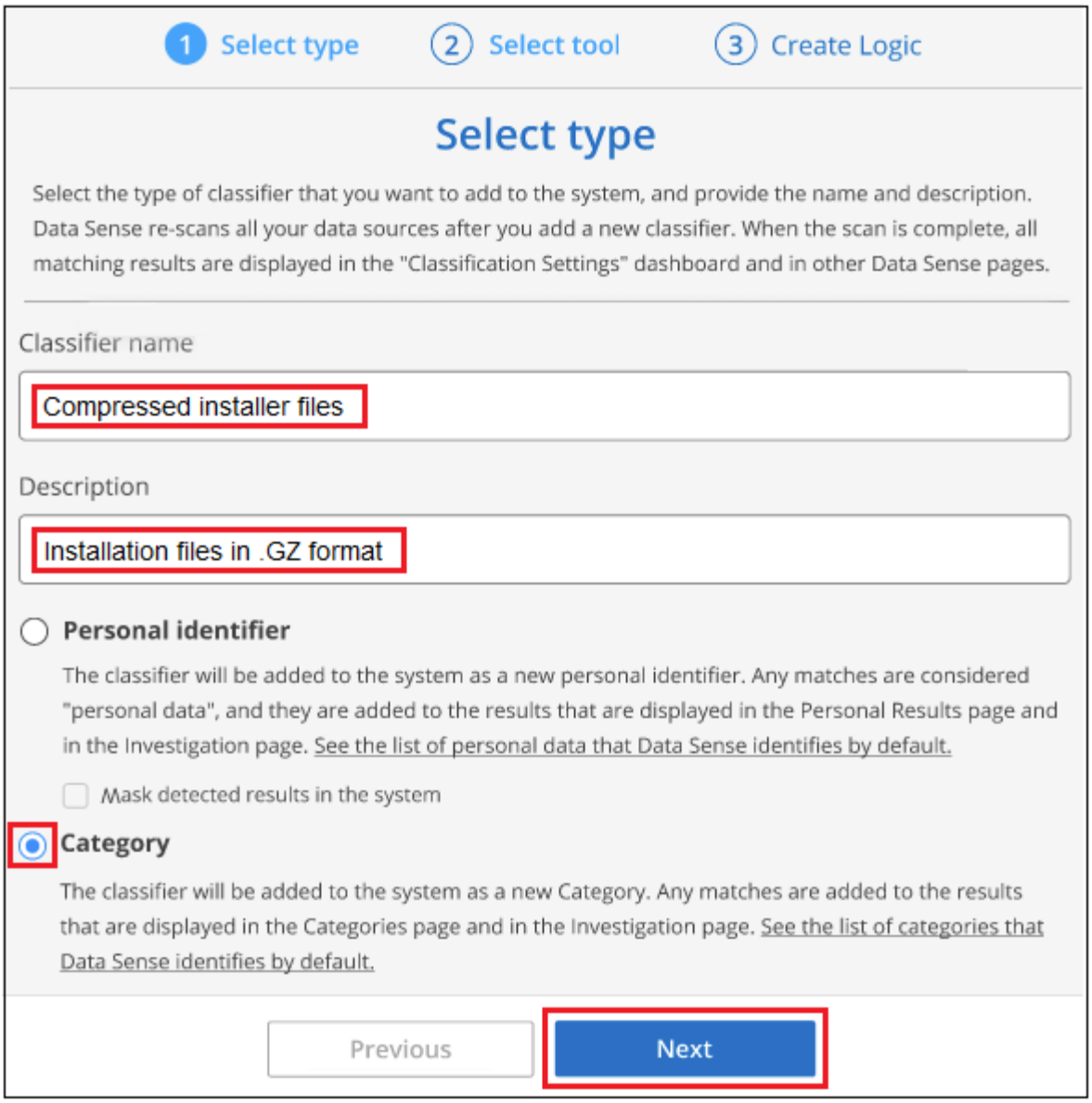
Passos

1. Na guia *Configurações de classificação*, clique em **Adicionar novo classificador** para iniciar o assistente *Adicionar classificador personalizado*.

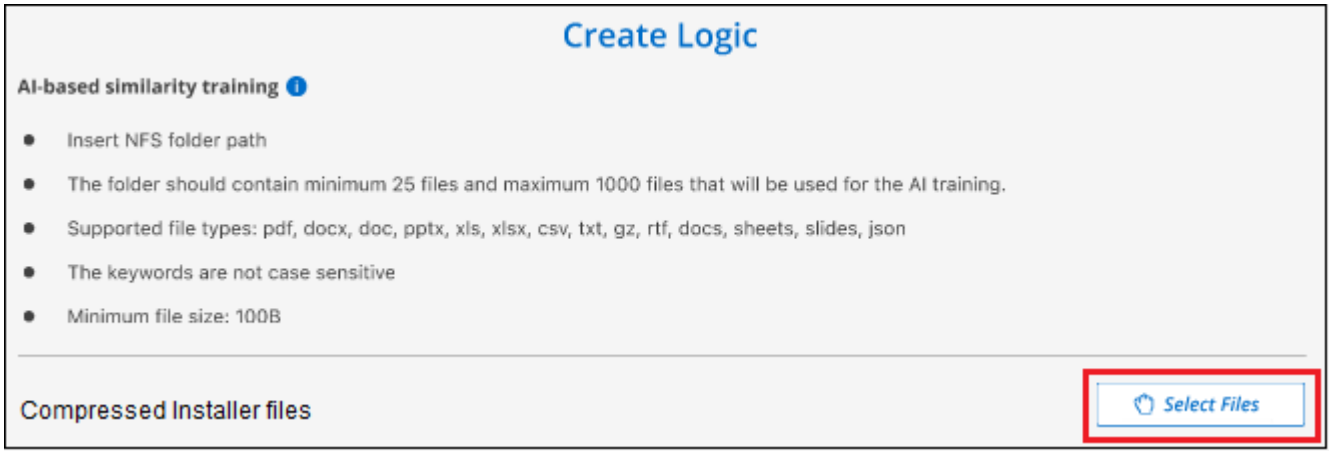


2. Na página *Selecionar tipo*, digite o nome do classificador, forneça uma breve descrição, selecione **Categoria** e clique em **Avançar**.

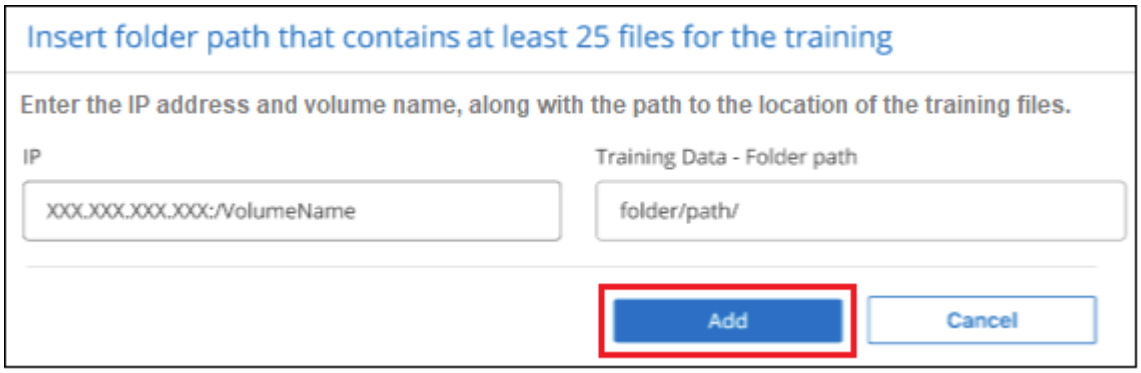
   O nome inserido aparecerá na IU de classificação do BlueXP como o título dos arquivos digitalizados que correspondem à categoria de dados que você está definindo e como o nome do filtro na página de investigação.



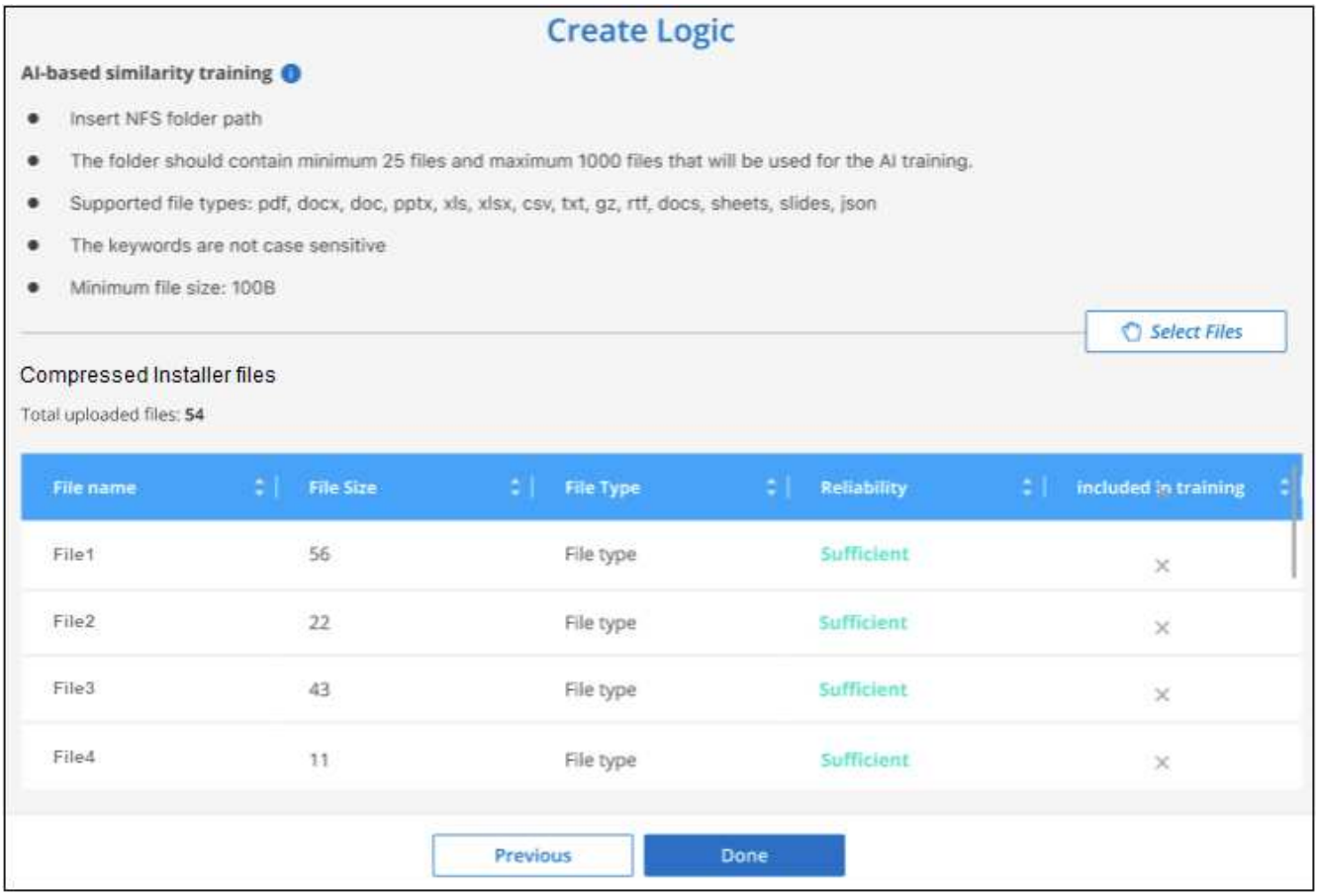
3. Na página *Create Logic*, certifique-se de que os arquivos de aprendizagem estão preparados e clique em **Select Files**.



4. Introduza o endereço IP do volume e o caminho em que os ficheiros de formação estão localizados e clique em **Add**.



5. Verifique se os arquivos de treinamento foram reconhecidos pela classificação BlueXP . Clique no **x** para remover quaisquer arquivos de treinamento que não atendam aos requisitos. Em seguida, clique em **Concluído**.

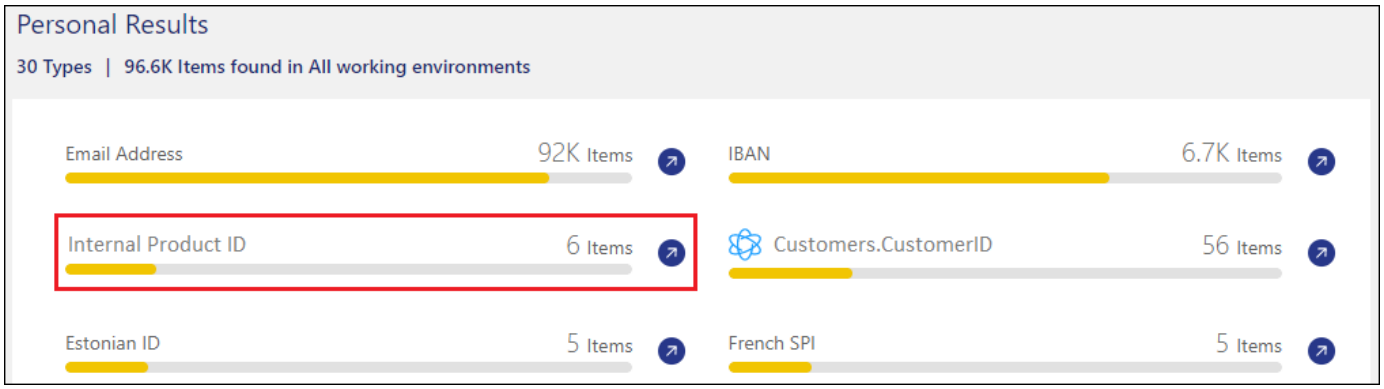


Resultados

A nova categoria é criada conforme definido pelos arquivos de treinamento e adicionada à classificação BlueXP . Em seguida, a classificação BlueXP começa a redigitalizar todas as suas fontes de dados para identificar arquivos que se encaixam nesta nova categoria. Você será retornado à página Classifiers personalizados, onde você pode ver o número de arquivos que correspondem à sua nova categoria. Os resultados da digitalização de todas as suas fontes de dados demorarão algum tempo, dependendo do número de arquivos que precisam ser digitalizados.

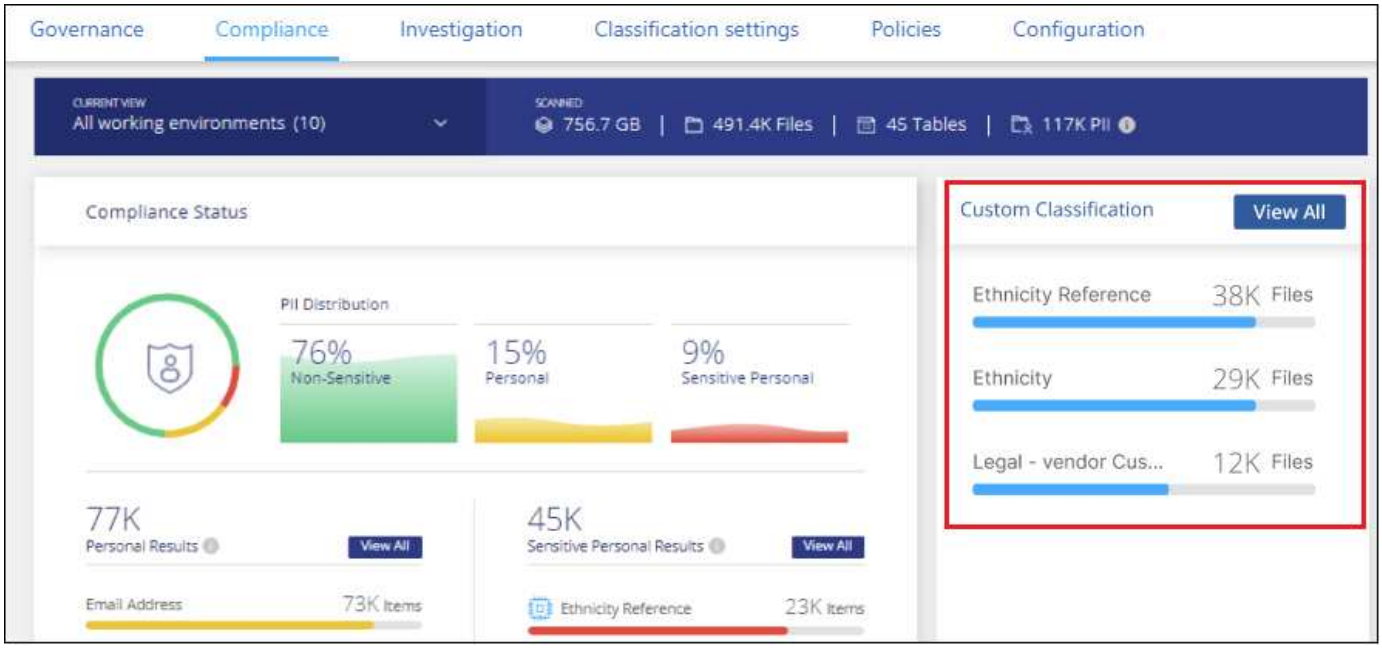
Veja os resultados dos seus classificadores personalizados

Você pode exibir os resultados de qualquer um dos seus classificadores personalizados no Painel de conformidade e na página de investigação. Por exemplo, esta captura de tela mostra as informações correspondentes no Painel de conformidade na seção "resultados pessoais".



Clique no botão para ver os resultados detalhados na página de investigação.

Além disso, todos os resultados do classificador personalizado aparecem na guia classificadores personalizados e os 6 melhores resultados do classificador personalizado são exibidos no Painel de conformidade, conforme mostrado abaixo.

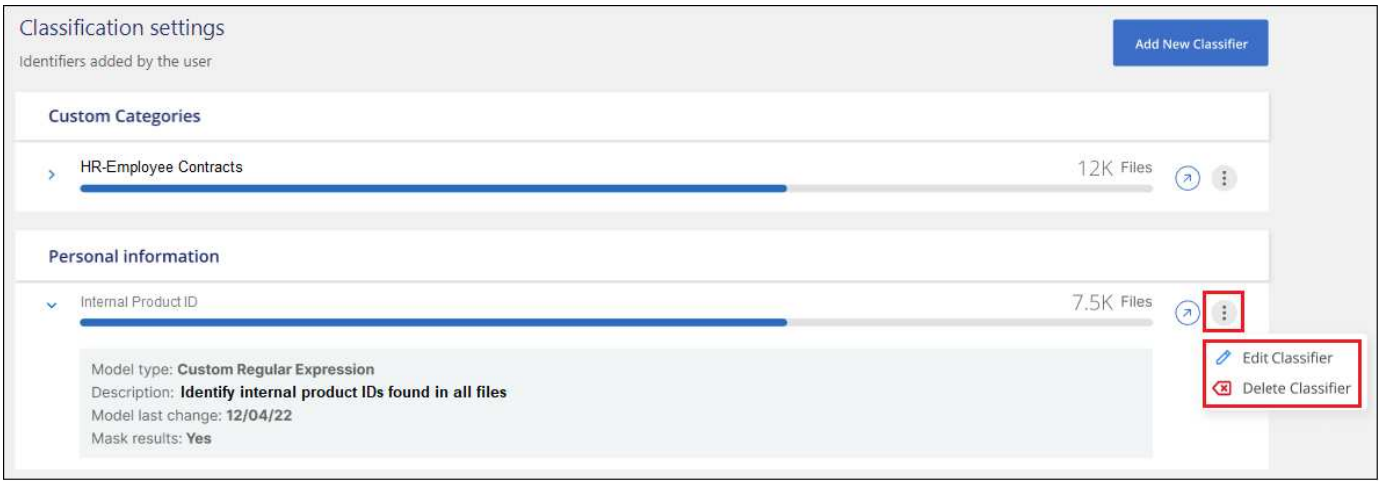


Gerenciar classificadores personalizados

Você pode alterar qualquer um dos classificadores personalizados que você criou usando o botão **Editar classificador**.

Neste momento, não é possível editar classificadores Data Fusion.

E se você decidir, em algum momento posterior, que não precisa da classificação do BlueXP para identificar os padrões personalizados que você adicionou, você pode usar o botão **Excluir classificador** para remover cada item.



Visualização do status de suas ações de conformidade

Quando você executa uma ação assíncrona do painel de resultados da investigação em muitos arquivos, por exemplo, mover ou excluir arquivos 100, o processo pode levar algum tempo. Você pode monitorar o status dessas ações no painel *Action Status* para saber quando ele foi aplicado a todos os arquivos.

Isso permite que você veja as ações que foram concluídas com sucesso, as que estão em andamento e as que falharam para que você possa diagnosticar e corrigir quaisquer problemas. Observe que operações curtas que são concluídas rapidamente, como mover um único arquivo, não aparecem no painel Status das ações.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

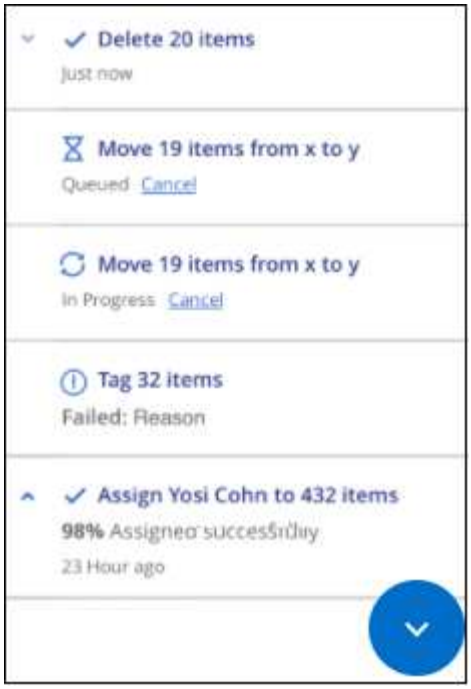
O estado pode ser:

- Sucesso - Uma ação de classificação BlueXP está concluída e todos os itens foram bem-sucedidos.
- Sucesso parcial - Uma ação de classificação BlueXP está concluída e alguns itens falharam e alguns foram bem-sucedidos.
- Em curso - a ação ainda está em andamento.
- Em fila de espera - a ação não foi iniciada.
- Cancelado - a ação foi cancelada.
- Falha - a ação falhou.

Observe que você pode cancelar quaisquer ações que tenham o status "em fila" ou "em andamento".

Passos

1. Na parte inferior direita da IU de classificação do BlueXP , você pode ver o botão **Status das ações**  .
2. Clique neste botão e as ações 20 mais recentes são listadas.



Pode clicar no nome de uma ação para ver os detalhes correspondentes a essa operação.

Auditar o histórico das ações de classificação do BlueXP

As atividades de gerenciamento de Registros de classificação do BlueXP que foram executadas em arquivos de todos os ambientes de trabalho e fontes de dados que a classificação do BlueXP está digitalizando. A classificação BlueXP também Registra as atividades ao implantar a instância de classificação BlueXP .

Você pode visualizar o conteúdo dos arquivos de log de auditoria de classificação do BlueXP ou baixá-los para ver quais alterações de arquivo ocorreram e quando. Por exemplo, você pode ver qual solicitação foi emitida, a hora da solicitação e detalhes como localização de origem no caso de um arquivo ser excluído ou localização de origem e destino no caso de um arquivo ser movido.

NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Conteúdo do ficheiro de registo

Cada linha no log de auditoria contém informações neste formato:

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Data e hora - carimbo de data/hora completo para o evento
- Estado - INFORMAÇÃO, AVISO
- Tipo de ação (excluir, copiar, mover, criar política, atualizar política, redigitalizar arquivos, baixar relatório JSON, etc.)

- Nome do ficheiro (se a ação for relevante para um ficheiro)
- Detalhes para a ação - o que foi feito: Depende da ação
  - Nome da política
  - Para mover - origem e destino
  - Para copiar - origem e destino
  - Para tag - nome da tag
  - Para atribuir a - nome de utilizador
  - Para alerta por e-mail - endereço de e-mail / conta

Por exemplo, as linhas a seguir do arquivo de log mostram uma operação de cópia bem-sucedida e uma operação de cópia com falha.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Localizações dos ficheiros de registo

Os arquivos de log de auditoria de gerenciamento estão localizados na máquina de classificação BlueXP em: `/opt/netapp/audit_logs/`

Os arquivos de log de auditoria de instalação são gravados `/opt/netapp/install_logs/`

Cada ficheiro de registo pode ter um tamanho máximo de 10 MB. Quando esse limite é atingido, um novo arquivo de log é iniciado. Os arquivos de log são denominados "DataSense_audit.log", "DataSense_audit.log.1", "DataSense_audit.log.2", e assim por diante. Um máximo de 100 ficheiros de registo são retidos no sistema - os ficheiros de registo mais antigos são eliminados automaticamente após o máximo ter sido atingido.

Aceder aos ficheiros de registo

Você precisará fazer login no sistema de classificação BlueXP para acessar os arquivos de log. Veja como "Inicie sessão no sistema de classificação BlueXP "dependendo se você instalou manualmente o software em uma máquina Linux ou se implantou a instância na nuvem.

Reduzir a velocidade de digitalização da classificação BlueXP

As verificações de dados têm um impactos insignificante nos sistemas de storage e nos dados. No entanto, se você estiver preocupado com até mesmo um impactos muito pequeno, você pode configurar a classificação BlueXP para executar verificações "lentas".

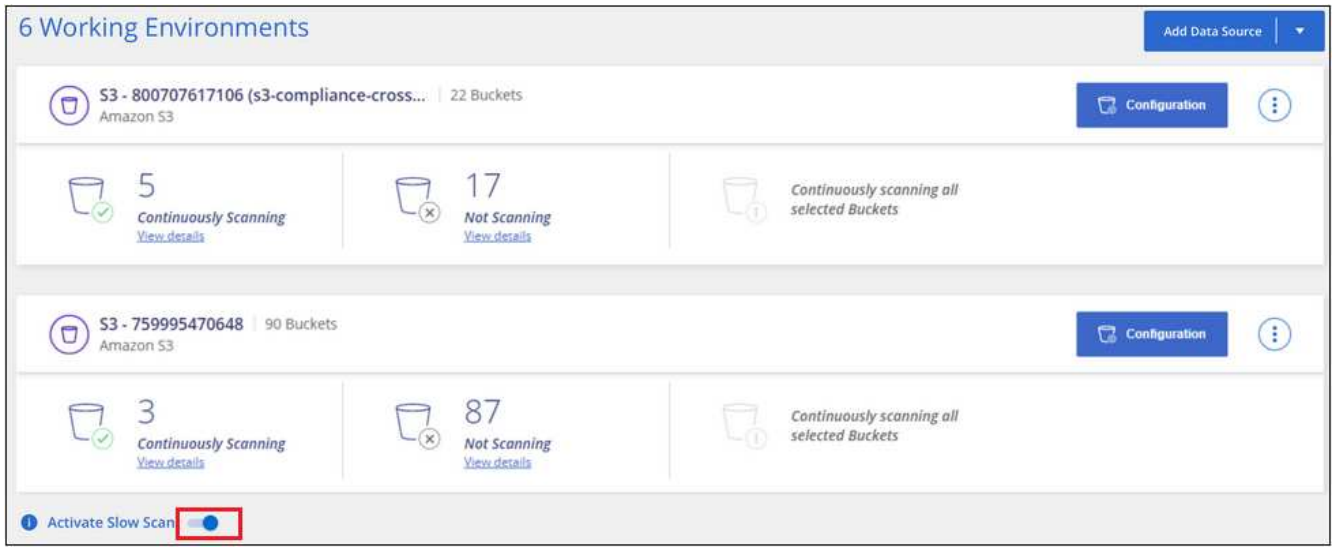
Quando ativado, a digitalização lenta é usada em todas as fontes de dados - você não pode configurar a digitalização lenta para um único ambiente de trabalho ou fonte de dados.

A velocidade de digitalização não pode ser reduzida ao digitalizar bases de dados.

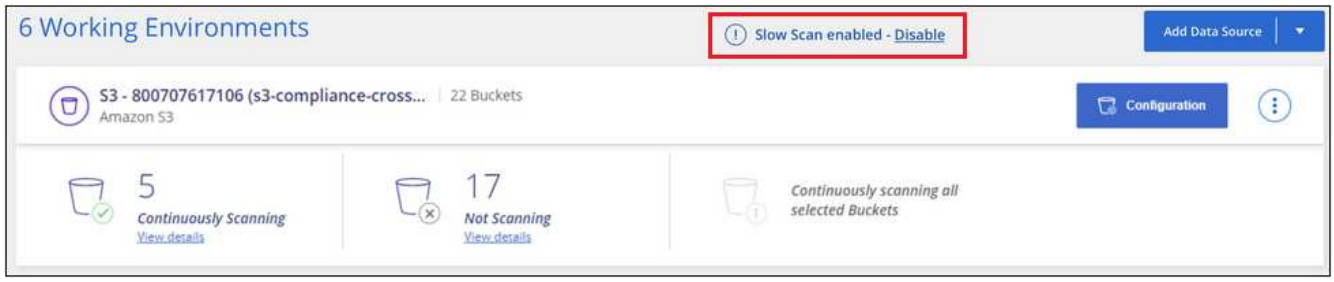
NOTA esta informação é relevante apenas para a classificação BlueXP versões antigas 1,30 e anteriores.

Passos

1. Na parte inferior da página *Configuration*, mova o controle deslizante para a direita para ativar a varredura lenta.



A parte superior da página Configuração indica que a digitalização lenta está ativada.



2. Você pode desativar a varredura lenta clicando em **Disable** nesta mensagem.

Remova uma conta do OneDrive, SharePoint ou Google Drive da classificação do BlueXP

Se você não quiser mais analisar arquivos de usuário de uma determinada conta do OneDrive, de uma conta específica do SharePoint ou de uma conta do Google Drive, você pode excluir a conta da interface de classificação do BlueXP e parar todas as verificações.

Passos

1. Na página *Configuração*, clique no botão na linha da conta OneDrive, SharePoint ou Google Drive e clique em **Remover conta OneDrive**, **Remover conta SharePoint** ou **Remover conta Google Drive**.

2. Clique em **Excluir conta** na caixa de diálogo de confirmação.

Referência

Tipos de instância de classificação BlueXP compatíveis

O software de classificação BlueXP deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de software etc. Ao implantar a classificação do BlueXP na nuvem, recomendamos que você use um sistema com as caraterísticas "grandes" para obter a funcionalidade completa.

Você pode implantar a classificação BlueXP em um sistema com menos CPUs e menos RAM, mas há algumas limitações ao usar esses sistemas menos poderosos. "Saiba mais sobre essas limitações".

Nas tabelas a seguir, se o sistema marcado como "padrão" não estiver disponível na região onde você está instalando a classificação BlueXP , 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" (predefinição)
Grande	16 CPUs, 64 GB de RAM, 500 GiB SSD	"m6i.4xlarge" (predefinição) m6a.4xlarge m5a.4xlarge m5,4xlarge m4,4xlarge
Média	8 CPUs, 32 GB de RAM, 200 GiB SSD	"m6i.2xlarge" (predefinição) m6a.2xlarge m5a.2xlarge m5,2xlarge m4,2xlarge
Pequeno	8 CPUs, 16 GB de RAM, 100 GiB SSD	"c6a.2xlarge" (predefinição) 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" (predefinição)
Grande	16 CPUs, 64 GB de RAM, 500 GiB SSD	"Standard_D16s_v3" (predefinição)

Tipos de instância do GCP

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

Metadados coletados de fontes de dados

A classificação do BlueXP coleta determinados metadados ao executar verificações de classificação nos dados de suas fontes de dados e ambientes de trabalho. A classificação BlueXP pode acessar a maioria dos metadados de que precisamos para classificar seus dados, mas existem algumas fontes nas quais não podemos acessar os dados de que precisamos.

	Metadados	CIFS	NFS
Carimbos de hora	*Tempo de criação*	Disponível	Não disponível (não suportado no Linux)
	Último tempo de acesso	Disponível	Disponível
	Último tempo de modificação	Disponível	Disponível
Permissões	*Permissões abertas*	Se o grupo "TODOS" tem acesso ao arquivo, é considerado "aberto à organização"	Se "outros" tem acesso ao arquivo, é considerado "aberto à organização"
	Usuários/acesso de grupo	As informações de usuários e grupos são retiradas do LDAP	Não disponível (os usuários NFS geralmente são gerenciados localmente no servidor, portanto, o mesmo indivíduo pode ter um UID diferente em cada servidor)

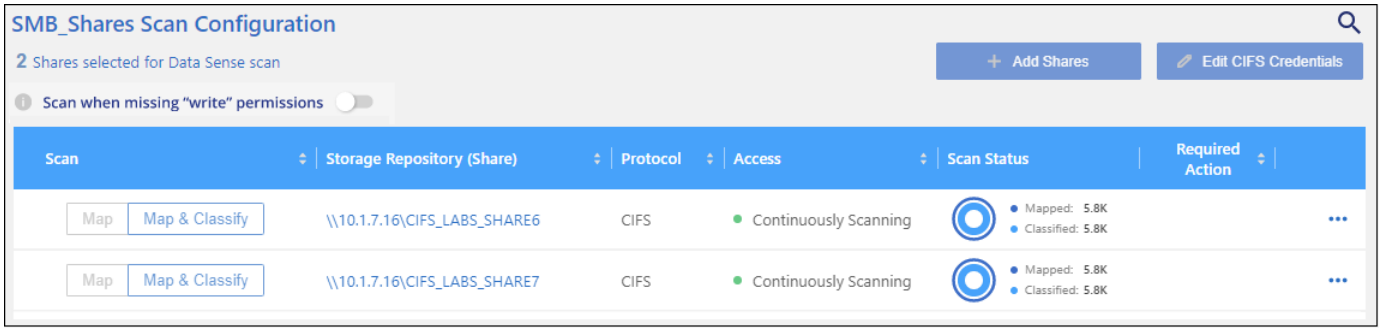
- A classificação BlueXP não extrai o "último tempo acessado" das fontes de dados do banco de dados.
- Versões mais antigas do sistema operacional Windows (por exemplo, Windows 7 e Windows 8) desabilitam a coleção do atributo "última hora acessada" por padrão, porque ele pode afetar o desempenho do sistema. Quando esse atributo não for coletado, a análise de classificação do BlueXP baseada no "último tempo acessado" será impactada. Você pode ativar a coleção do último tempo de acesso nesses sistemas Windows mais antigos, se necessário.

Data/hora do último acesso

Quando a classificação BlueXP extrai dados de compartilhamentos de arquivo, o sistema operacional considera-os como acessando os dados e altera o "último tempo de acesso" em conformidade. Após a digitalização, a classificação BlueXP tenta reverter a última hora de acesso ao carimbo de data/hora original. Se a classificação do BlueXP não tiver permissões de atributos de gravação no CIFS ou permissões de gravação no NFS, o sistema não poderá reverter o último tempo de acesso ao carimbo de data/hora original. Os volumes ONTAP configurados com SnapLock têm permissões somente leitura e também não podem reverter o último tempo de acesso ao carimbo de data/hora original.

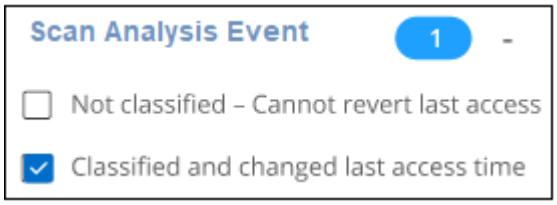
Por padrão, se a classificação do BlueXP não tiver essas permissões, o sistema não verificará esses arquivos em seus volumes porque a classificação do BlueXP não pode reverter o "último tempo de acesso" para o timestamp original. No entanto, se você não se importa se o último tempo de acesso é redefinido para a hora original em seus arquivos, você pode clicar na opção **Escanear quando faltar permissões de "escrever atributos"** na parte inferior da página Configuração para que a classificação BlueXP digitalize os volumes

independentemente das permissões.



Esse recurso é aplicável a sistemas ONTAP locais, Cloud Volumes ONTAP, Azure NetApp Files, FSX for ONTAP e compartilhamentos de arquivos de terceiros.

Observe que há um filtro na página de investigação chamado *Scan Analysis Event* que permite exibir os arquivos que não foram classificados porque a classificação do BlueXP não pôde reverter o último tempo acessado ou os arquivos que foram classificados, mesmo que a classificação do BlueXP não pudesse reverter o último tempo de acesso.



As seleções de filtro são:

- "Not Classified — cannot revert last access time" (não classificado — não é possível reverter o último tempo de acesso) - mostra os ficheiros que não foram classificados devido a permissões de gravação em falta.
- "Classificado e atualizado último tempo de acesso" - mostra os ficheiros que foram classificados e a classificação BlueXP não conseguiu repor o último tempo de acesso à data original. Este filtro é relevante apenas para ambientes em que você ativou **Escanear quando faltar permissões de "atributos de gravação"**.

Se necessário, você pode exportar esses resultados para um relatório para que você possa ver quais arquivos estão ou não sendo digitalizados por causa das permissões. "Saiba mais sobre o Relatório de Investigação de dados".

Inicie sessão no sistema de classificação BlueXP

Às vezes, você pode precisar fazer login no sistema de classificação BlueXP para que você possa acessar arquivos de log ou editar arquivos de configuração.

Quando a classificação do BlueXP é instalada em uma máquina Linux no local ou em uma máquina Linux implantada na nuvem, você pode acessar o arquivo de configuração e o script diretamente.

Quando a classificação do BlueXP é implantada na nuvem, você precisa fazer SSH para a instância de classificação do BlueXP . Você faz o SSH para o sistema inserindo o usuário e a senha, ou usando a chave SSH fornecida durante a instalação do BlueXP Connector. 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 Azure: Use o usuário criado para a instância do BlueXP
** Para o GCP: Use o usuário criado para a instância do BlueXP

- <datasense_ip>: Endereço IP da instância da máquina virtual

Observe que você precisará modificar as regras de entrada do grupo de segurança para acessar o sistema na nuvem. Para obter detalhes, consulte:

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

APIs de classificação BlueXP

Os recursos de classificação do BlueXP que estão disponíveis através da IU da Web também estão disponíveis através da API Swagger.

Existem quatro categorias definidas na classificação BlueXP que correspondem às guias na IU:

- Investigação
- Conformidade
- Governança
- Configuração

As APIs na documentação do Swagger permitem que você pesquise, agregue dados, rastreie suas varreduras e crie ações como copiar, mover e muito mais.

Visão geral

A API permite que você execute as seguintes funções:

- Exportar informações
  - Tudo o que está disponível na IU pode ser exportado através da API (com exceção de relatórios)
  - Os dados são exportados em um formato JSON (fácil de analisar e enviar para aplicativos de 3rd partes, como Splunk)
- Crie consultas usando declarações "E" e "OU", 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). Também pode excluir campos específicos para a operação de exportação.

- Execute ações
  - Atualizar credenciais CIFS
  - Ver e cancelar ações
  - Volte a verificar diretórios
  - Exportar dados

A API é segura e usa o mesmo método de autenticação que a interface do usuário. Você pode encontrar informações sobre a autenticação em: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Acessando a referência da API Swagger

Para entrar no Swagger, você precisará do endereço IP da instância de classificação do seu BlueXP . No caso de uma implantação na nuvem, você usará o endereço IP público. Então você precisará entrar nesse endpoint:

https://<classification_ip>/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 um ambiente de trabalho para exibir todos os filtros na guia 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": "Working Environment Type",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ENVIRONMENT",
    "name": "Working Environment",
    "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, copiar, atribuir a, FlexClone, exportar dados, redigitalizar e rotular.

Vamos criar a ação de cópia:

Solicitação de API

Esta próxima API é a API de ação e permite que você crie várias 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, para que você possa usar as APIs GET e DELETE para obter status sobre a 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 apoio

Registre-se para obter suporte

O Registro de suporte é necessário para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage. O Registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP.

O Registro para suporte não ativa o suporte do NetApp para um serviço de arquivos de provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Visão geral do Registro de suporte

Existem duas formas de Registro para ativar o direito de suporte:

- Registar o número de série da sua conta BlueXP (o número de série 960xxxxxxxx de 20 dígitos localizado na página recursos de suporte no BlueXP).

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

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

  Esses números de série são comumente referidos como *PAYGO serial numbers* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP.

Registrar ambos os tipos de números de série permite recursos como abrir tickets de suporte e geração automática de casos. O Registro é concluído adicionando contas do site de suporte da NetApp (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para obter suporte ao NetApp

Para se Registrar para obter suporte e ativar o direito de suporte, um usuário em sua organização (ou conta) do BlueXP deve associar uma conta do site de suporte da NetApp ao login do BlueXP . A forma como você se Registra no suporte da NetApp depende se você já tem uma conta do site de suporte da NetApp (NSS).

Cliente existente com uma conta NSS

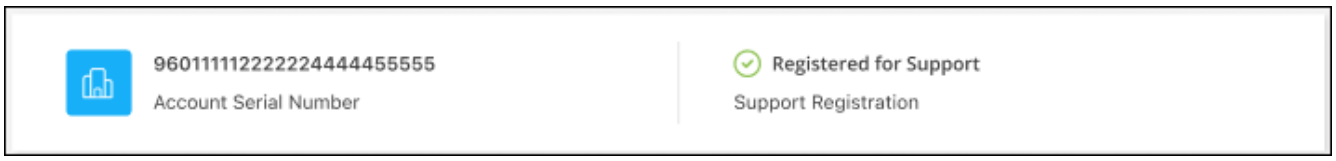
Se você é um cliente da NetApp com uma conta NSS, você simplesmente precisa se Registrar para obter suporte através do BlueXP .

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (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 organização do BlueXP está registrada para suporte.



   Observe que outros usuários do BlueXP não verão esse mesmo status de Registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização do BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido esses passos, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é um cliente NetApp com licenças e números de série existentes, mas *no* conta NSS, você precisa criar uma conta NSS e associá-la ao seu login no BlueXP .

Passos

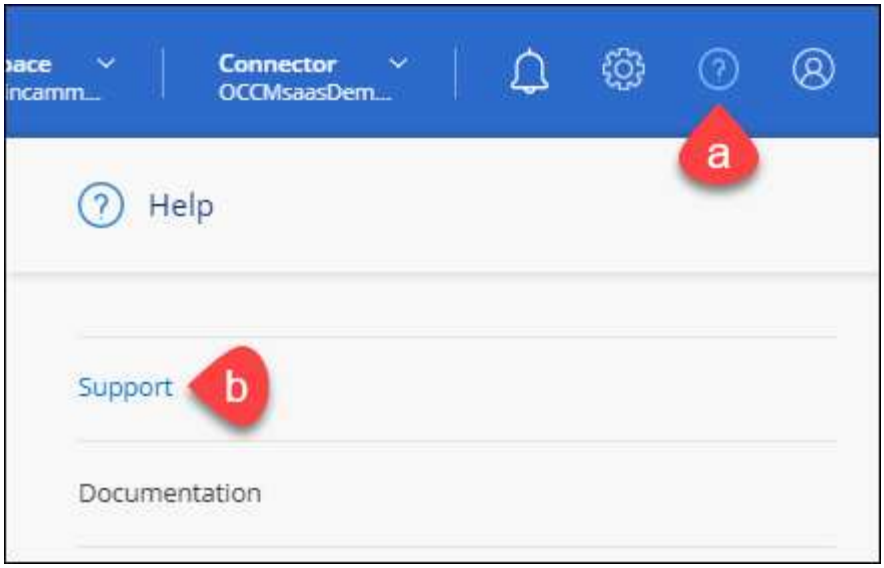
1. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento da conta.
2. Associe a sua nova conta NSS ao seu login no BlueXP executando as etapas em Cliente existente com uma conta NSS.

Novo na NetApp

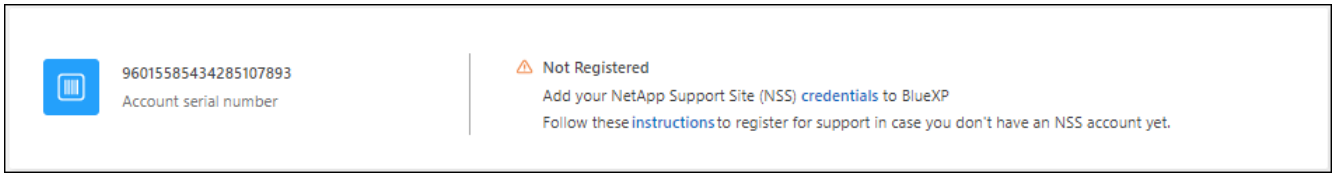
Se você é novo no NetApp e não tem uma conta NSS, siga cada passo abaixo.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Localize o número de série da ID da conta na página Registro de suporte.



3. Navegue "Site de Registro de suporte da NetApp" e selecione **não sou um Cliente NetApp registado**.
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 a partir da etapa 2 acima, complete a verificação de segurança e confirme se leu a Política de Privacidade de dados globais da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam se o e-mail de validação não chegar em poucos minutos.

7. Confirme a ação a partir do e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta do site de suporte da NetApp.

8. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento.

Depois de terminar

O NetApp deve entrar em Contato com você durante esse processo. Este é um exercício de integração única para novos usuários.

Depois de ter sua conta do site de suporte da NetApp, associe a conta ao login do BlueXP , executando as

etapas em Cliente existente com uma conta NSS.

Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

A associação das credenciais do site de suporte da NetApp à sua organização do BlueXP é necessária para ativar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

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

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

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

  É necessário fornecer a sua conta NSS para que o BlueXP possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

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

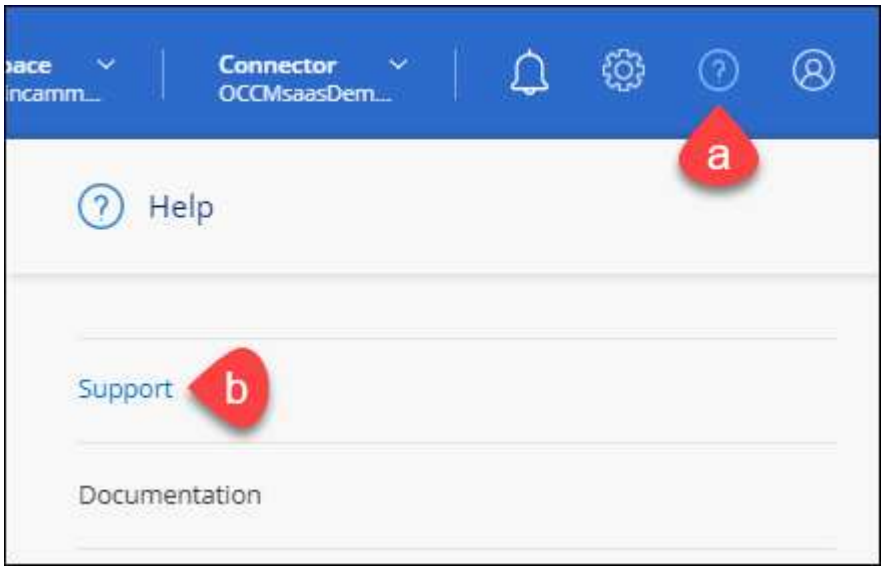
Associar credenciais NSS à sua organização do BlueXP é diferente da conta NSS associada a um login de usuário do BlueXP .

Essas credenciais do NSS estão associadas ao ID específico da organização do BlueXP . Os utilizadores que pertencem à organização BlueXP podem aceder a estas credenciais a partir de **suporte > Gestão NSS**.

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O 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 executar o processo de autenticação.

   Essas ações permitem que o BlueXP use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

   Observe o seguinte:

   - A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

   O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do 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 o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ••• menu.

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

     Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

Obtenha ajuda

A NetApp oferece suporte ao BlueXP e seus serviços de nuvem de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. O seu registo de suporte inclui suporte técnico remoto através de Bilheteira na Web.

Obtenha suporte para um serviço de arquivos do provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage, use as opções de suporte descritas abaixo.

Use opções de suporte autônomo

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

- Documentação

  A documentação do BlueXP que você está visualizando no momento.

- "Base de conhecimento"

  PESQUISE na base de conhecimento do BlueXP para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Junte-se à comunidade BlueXP para seguir as discussões em curso ou criar novas.

Crie um caso com o suporte do NetApp

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

Antes de começar

- Para usar o recurso **criar um caso**, primeiro você deve associar suas credenciais do site de suporte da NetApp ao login do BlueXP . "Saiba como gerenciar credenciais associadas ao seu login no BlueXP".
- Se você estiver abrindo um caso para um sistema ONTAP com um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

Passos

1. No BlueXP , 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 no telefone. Você será direcionado para uma página no NetApp.com que lista os números de telefone que você pode ligar.

   b. Selecione **criar um caso** para abrir um ticket com um especialista em suporte da NetApp:

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, BlueXP quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do serviço.
      - **Ambiente de trabalho**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **no local** e, em seguida, o ambiente de trabalho associado.

        A lista de ambientes de trabalho está dentro do escopo da organização (ou conta) do BlueXP , do projeto (ou da área de trabalho) e do conetor que você selecionou no banner superior do serviço.

      - **Prioridade do caso**: Escolha a prioridade para o caso, que pode ser baixa, média, alta ou Crítica.

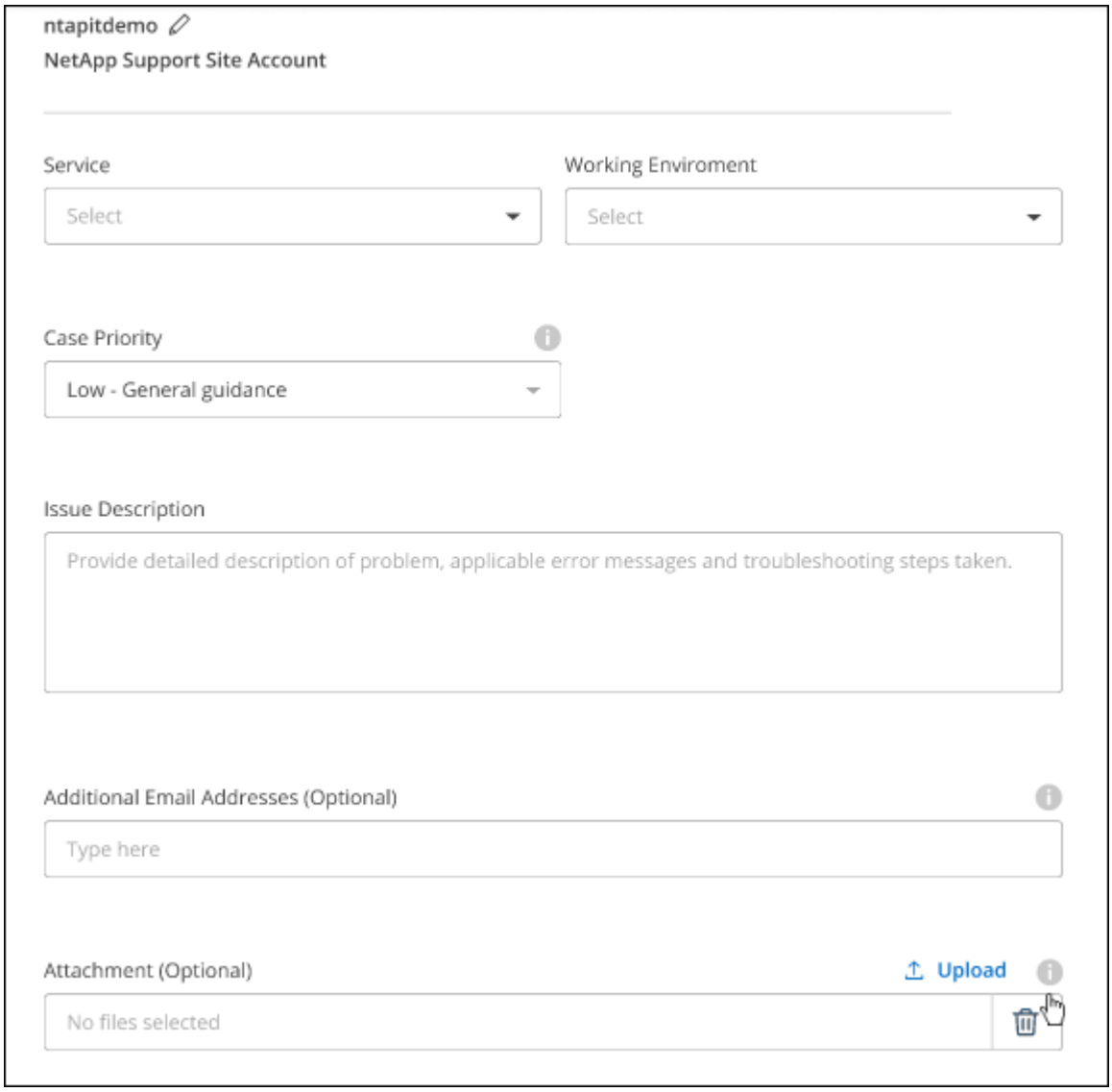
        Para saber mais detalhes sobre essas prioridades, passe o Mouse sobre o ícone de informações ao lado do nome do campo.

      - **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 você quiser que outra

pessoa saiba sobre esse problema.

- **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

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



Depois de terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp irá rever o seu caso e voltar para você em breve.

Para obter um histórico de seus casos de suporte, você pode selecionar **Configurações > linha do tempo** e procurar ações chamadas "criar caso de suporte". Um botão à 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 de Registro com a qual está associada não são a mesma empresa de Registro para o número de série da conta BlueXP (ou seja. 960xxxx) ou o número de

série do ambiente de trabalho. Pode procurar assistência utilizando uma das seguintes opções:

- Use o chat no produto
- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerenciar seus casos de suporte (prévia)

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

O gerenciamento de casos está disponível como uma prévia. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A vista à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta do usuário NSS que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses ao nível da sua empresa com base na sua conta NSS de utilizador.

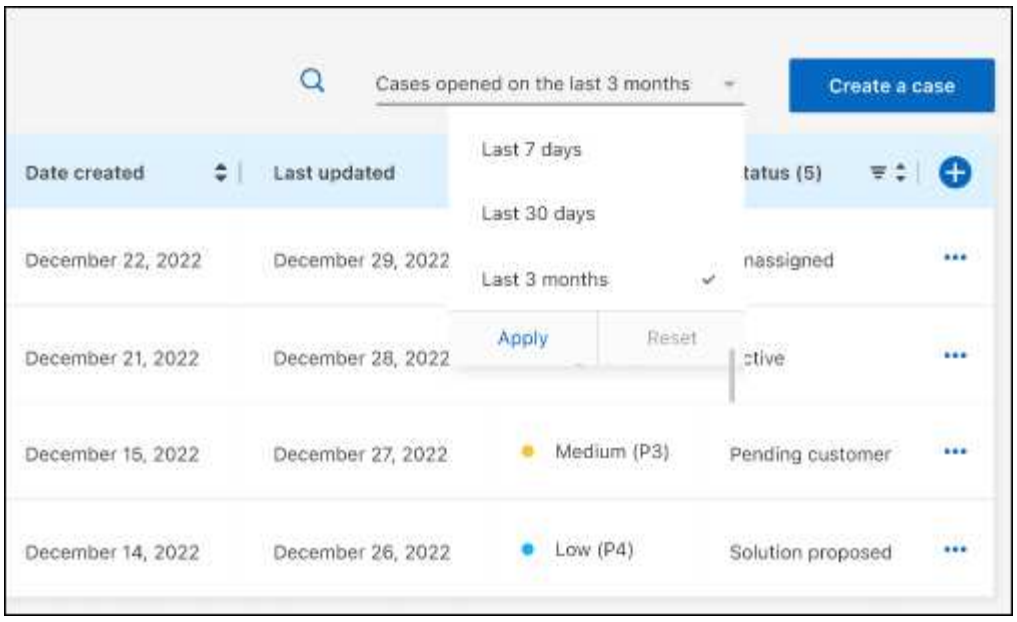
  Os resultados na tabela refletem os casos relacionados à exibição selecionada.
- Você pode adicionar ou remover colunas de interesse e pode filtrar o conteúdo de colunas como prioridade e Status. Outras colunas fornecem apenas capacidades de ordenação.

  Veja os passos abaixo para obter mais detalhes.
- Em um nível por caso, oferecemos a capacidade de atualizar notas de caso ou fechar um caso que ainda não esteja no status fechado ou pendente fechado.

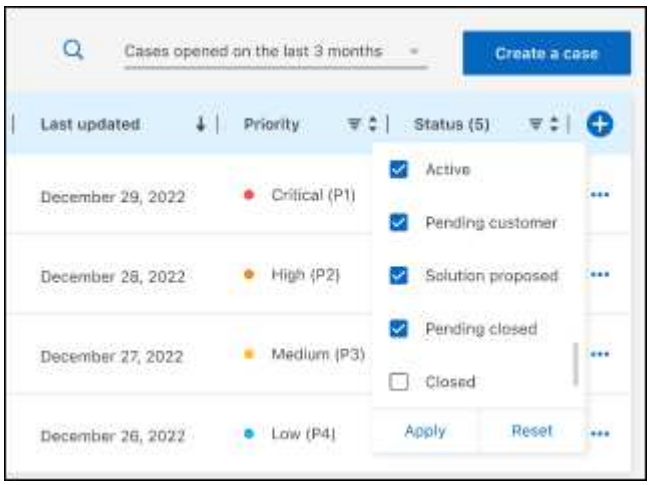
Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Selecione **Gerenciamento de casos** e, se for solicitado, adicione sua conta NSS ao BlueXP .

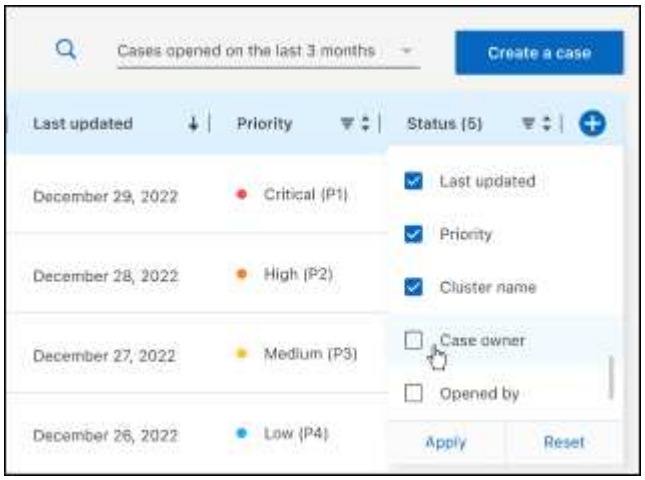
   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à conta de usuário do BlueXP . Esta é a mesma conta NSS que aparece na parte superior da página **NSS Management**.
3. Opcionalmente, modifique as informações exibidas na tabela:
   - Em **casos da organização**, selecione **Exibir** para ver todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um intervalo de tempo diferente.



- Filtre o conteúdo das colunas.



- Altere as colunas que aparecem na tabela selecionando e escolhendo as colunas que você deseja exibir.

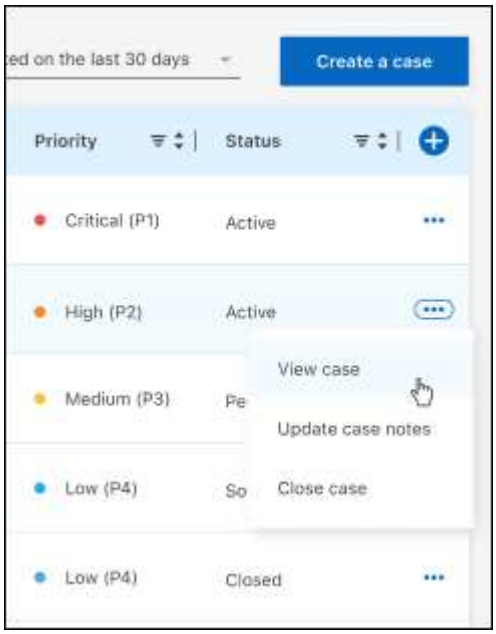


4. Gerencie um caso existente •••selecionando e selecionando uma das opções disponíveis:

   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - * Atualizar notas de caso*: Forneça detalhes adicionais sobre o seu problema ou selecione **carregar arquivos** para anexar até um máximo de cinco arquivos.

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

   - * Fechar caso*: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.



Avisos legais

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

Direitos de autor

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

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos 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 de terceiros e licenças usadas no software NetApp.

- "Aviso para BlueXP"
- "Aviso para classificação BlueXP "

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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