Documentación de clasificación de BlueXP

BlueXP classification

NetApp
April 03, 2024

Tabla de contenidos

Documentación de clasificación de BlueXP

Notas de la versión

Novedades de la clasificación de BlueXP

Descubre las novedades de la clasificación de BlueXP (Cloud Data Sense).

1 de abril de 2024 (Versión 1,30)

Compatibilidad añadida para la clasificación de BlueXP de RHEL v8,8 y v9,3

Esta versión es compatible con Red Hat Enterprise Linux v8,8 y v9,3, además de la versión 9.x admitida anteriormente, que requiere Podman, en lugar del motor Docker. Esto es aplicable a cualquier instalación manual en las instalaciones de la clasificación de BlueXP.

Los siguientes sistemas operativos deben utilizar el motor de contenedor Podman y requieren la versión de clasificación de BlueXP 1,30 o posterior: Red Hat Enterprise Linux versiones 8,8, 9,0, 9,1, 9,2 y 9,3.

Más información acerca de "Información general sobre las puestas en marcha de clasificación de BlueXP".

Se quitó la opción para activar la recogida del registro de auditoría

Se deshabilitó la opción para activar la recogida de registros de auditoría.

Velocidad de escaneo mejorada

Se ha mejorado el rendimiento de escaneo en nodos de escáner secundarios. Puede agregar más nodos de escáner si necesita potencia de procesamiento adicional para sus escaneos. Para obtener más información, consulte "Instala la clasificación de BlueXP en un host que tenga acceso a Internet".

Actualizaciones automáticas

Si implementaste la clasificación de BlueXP en un sistema con acceso a Internet, el sistema se actualizará automáticamente. Anteriormente, la actualización se produjo después de un tiempo específico transcurrido desde la última actividad del usuario. Con esta versión, la clasificación de BlueXP se actualiza automáticamente si la hora local es entre las 1:00 y las 5:00:00. Si la hora local está fuera de estas horas, la actualización se produce después de que transcurra un tiempo específico desde la última actividad del usuario. Para obtener más información, consulte "Instale en un host Linux con acceso a Internet".

Si implementaste la clasificación de BlueXP sin acceso a Internet, tendrás que actualizar manualmente. Para obtener más información, consulte "Instala la clasificación BlueXP en un host Linux sin acceso a Internet".

4 de marzo de 2024 (versión 1,29)

Ahora puede excluir los datos de escaneo que residen en ciertos directorios de origen de datos

Si desea que la clasificación de BlueXP excluya los datos de análisis que residen en determinados directorios de orígenes de datos, puede añadir estos nombres de directorio a un archivo de configuración que procese la clasificación de BlueXP. Esta función le permite evitar el escaneo de directorios que no son necesarios, o que daría lugar a la devolución de resultados de datos personales falsos positivos.

"Leer más".

El soporte de instancias extra grandes ya está cualificado

Si necesitas la clasificación de BlueXP para analizar más de 250 millones de archivos, puedes utilizar una instancia de Extra Large en la puesta en marcha de la nube o en la instalación on-premises. Este tipo de sistema puede escanear hasta 500 millones de archivos.

"Leer más".

10 de enero de 2024 (versión 1,27)

Los resultados de la página de investigación ahora muestran el tamaño total además del número total de elementos

Los resultados filtrados en la página de investigación ahora muestran el tamaño total de los elementos además del número total de archivos. Esto puede ayudar al mover archivos, eliminar archivos y más.

Configurar IDs de grupo adicionales como abiertos para la organización

Ahora puede configurar los ID de grupo en NFS para que se consideren «abiertos a la organización» directamente desde la clasificación de BlueXP si el grupo no se había establecido inicialmente con ese permiso. Todos los archivos y carpetas que tengan estos ID de grupo adjuntos se mostrarán como abiertos a la organización en la página Detalles de la investigación. Descubra cómo "Agregar ID de grupo adicionales como abiertos a la organización".

14 de diciembre de 2023 (versión 1.26.6)

Esta versión incluye algunas mejoras menores.

La versión también eliminó temporalmente las siguientes opciones:

- Se deshabilitó la opción para activar la recogida de registros de auditoría. Consulte "Supervise y gestione eventos de acceso a archivos".
- Durante la investigación de directorios, la opción de calcular el número de datos de información personal identificable (PII) por directorios no está disponible. Consulte "Investigue los datos almacenados en su organización".
- Se ha desactivado la opción de integrar datos mediante etiquetas de Azure Information Protection (AIP). Consulte "Organice sus datos privados".

6 de noviembre de 2023 (versión 1.26.3)

Los siguientes problemas se han solucionado en esta versión

- Se ha corregido una inconsistencia al presentar el número de archivos escaneados por el sistema en los paneles de control.
- Se ha mejorado el comportamiento de escaneo al manejar e informar sobre archivos y directorios con caracteres especiales en el nombre y los metadatos.

4 de octubre de 2023 (versión 1,26)

Compatibilidad con las instalaciones on-premises de la clasificación de BlueXP en la versión 9 de RHEL

Red Hat Enterprise Linux, las versiones 8 y 9 no son compatibles con el motor Docker; se requería para la instalación de la clasificación de BlueXP. Ahora admitimos la instalación de clasificación de BlueXP en RHEL 9,0, 9,1 y 9,2 mediante Podman versión 4 o posterior como infraestructura de contenedores. Si tu entorno requiere el uso de las versiones más recientes de RHEL, ahora puedes instalar la clasificación de BlueXP (versión 1,26 o posterior) cuando utilizas Podman.

En este momento, no admitimos instalaciones de sitios oscuros ni entornos de análisis distribuidos (con nodos de escáner maestro y remoto) cuando se usa RHEL 9.x.

5 de septiembre de 2023 (versión 1,25)

Implementaciones pequeñas y medianas no disponibles temporalmente

Cuando implementas una instancia de clasificación de BlueXP en AWS, la opción de seleccionar **Desplegar > Configuración** y elegir una instancia pequeña o mediana no estará disponible en este momento. Aún puede implementar la instancia utilizando el tamaño de instancia grande seleccionando **Desplegar > Desplegar**.

Aplique etiquetas a un máximo de 100.000 elementos desde la página de resultados de la investigación

En el pasado, sólo se podían aplicar etiquetas a una sola página a la vez en la página de resultados de la investigación (20 elementos). Ahora puede seleccionar **todos** elementos en las páginas de resultados de la investigación y aplicar etiquetas a todos los elementos - hasta 100.000 elementos a la vez. "Descubra cómo".

Identifique archivos duplicados con un tamaño de archivo mínimo de 1 MB

Clasificación de BlueXP utilizada para identificar los archivos duplicados solo cuando los archivos tenían 50 MB o más. Ahora se pueden identificar los archivos duplicados que comienzan con 1 MB. Puedes usar los filtros de página de investigación “Tamaño de archivo” junto con “Duplicados” para ver qué archivos de un determinado tamaño están duplicados en tu entorno.

17 de julio de 2023 (versión 1,24)

Dos nuevos tipos de datos personales alemanes se identifican por la clasificación de BlueXP

La clasificación de BlueXP puede identificar y categorizar los archivos que contengan los siguientes tipos de datos:

- Identificación alemana (Personalausweisnummer)
- Número de Seguro Social Alemán (Sozialversicherungsnummer)

"Consulta todos los tipos de datos personales que la clasificación de BlueXP puede identificar en tus datos".

La clasificación de BlueXP es totalmente compatible con el modo restringido y el modo privado

La clasificación de BlueXP ahora es totalmente compatible en sitios sin acceso a Internet (modo privado) y con acceso a Internet saliente limitado (modo restringido). "Obtén más información sobre los modos de puesta en marcha de BlueXP para Connector".

Capacidad de omitir versiones al actualizar una instalación en modo privado de la clasificación de BlueXP

Ahora puedes actualizar a una versión más reciente de la clasificación de BlueXP incluso si no es secuencial. Esto significa que ya no es necesaria la limitación actual para actualizar la clasificación de BlueXP de una versión a la vez. Esta función es relevante a partir de la versión 1,24 en adelante.

La API de clasificación de BlueXP ya está disponible

La API de clasificación de BlueXP permite realizar acciones, crear consultas y exportar información sobre los datos que está escaneando. La documentación interactiva se encuentra disponible mediante Swagger. La documentación se divide en varias categorías, incluidas Investigación, Cumplimiento, Gobernanza y Configuración. Cada categoría es una referencia a las pestañas de la interfaz de usuario de clasificación de BlueXP.

"Obtén más información sobre las API de clasificación de BlueXP".

6 de junio de 2023 (versión 1,23)

Ahora se admite el japonés al buscar nombres de sujetos de datos

Ahora se pueden introducir nombres en japonés al buscar el nombre de un sujeto en respuesta a una solicitud de acceso a los datos del interesado (DSAR). Puede generar un "Informe de solicitud de acceso de asunto de datos" con la información resultante. También puede introducir nombres japoneses en la "Filtro de sujeto de datos en la página Investigación de datos" para identificar los archivos que contienen el nombre del sujeto.

Ubuntu ahora es una distribución Linux compatible en la que puedes instalar la clasificación de BlueXP

Ubuntu 22,04 ha sido calificado como un sistema operativo compatible para la clasificación BlueXP. Puede instalar la clasificación de BlueXP en un host Ubuntu Linux de su red o en un host Linux en el cloud cuando utilice la versión 1,23 del instalador. "Descubre cómo instalar la clasificación de BlueXP en un host con Ubuntu instalado".

Red Hat Enterprise Linux 8,6 y 8,7 ya no son compatibles con las nuevas instalaciones de clasificación de BlueXP

Estas versiones no son compatibles con nuevas implementaciones porque Red Hat ya no es compatible con Docker, lo cual es un requisito previo. Si ya tienes un equipo de clasificación de BlueXP en RHEL 8,6 o 8,7, NetApp seguirá admitiendo tu configuración.

La clasificación de BlueXP se puede configurar como un recopilador de FPolicy para recibir eventos de FPolicy de sistemas ONTAP

Es posible habilitar los registros de auditoría de acceso a archivos para que se recopilen en el sistema de clasificación de BlueXP para los eventos de acceso a archivos detectados en volúmenes en tus entornos de trabajo. La clasificación de BlueXP puede capturar los siguientes tipos de eventos de FPolicy y los usuarios que realizaron las acciones en sus archivos: Crear, leer, escribir, eliminar, cambiar el nombre, Cambie el propietario/permisos y cambie SACL/DACL. "Vea cómo supervisar y gestionar eventos de acceso a archivos".

Las licencias BYOL de Data Sense son ahora compatibles en sitios oscuros

Ahora puedes cargar la licencia BYOL de Data Sense en la cartera digital de BlueXP en un sitio oscuro para que se te notifique cuando tu licencia esté baja. "Vea cómo obtener y cargar su licencia BYOL de Data Sense".

3 de abril de 2023 (versión 1.22)

Nuevo informe de evaluación de detección de datos

El informe de evaluación de detección de datos proporciona un análisis de alto nivel del entorno escaneado para resaltar los resultados obtenidos por el sistema y mostrar las áreas de preocupación y los posibles pasos para solucionarlos. El objetivo de este informe es dar a conocer las preocupaciones sobre la gobernanza de datos, las amenazas a la seguridad de los datos y los vacíos de cumplimiento de normativas en relación con los datos de su conjunto de datos. "Descubra cómo generar y utilizar el Informe de evaluación de detección de datos".

Capacidad de poner en marcha la clasificación de BlueXP en instancias más pequeñas en el cloud

Al implementar la clasificación de BlueXP desde un conector BlueXP en un entorno AWS, ahora puedes elegir entre dos tipos de instancia menores de los que hay disponibles con la instancia predeterminada. Si está analizando un entorno pequeño, esto puede ayudarle a ahorrar costes en la nube. Sin embargo, hay algunas restricciones al utilizar la instancia más pequeña. "Vea los tipos de instancia y las limitaciones disponibles".

El script independiente ya está disponible para calificar tu sistema Linux antes de instalar la clasificación de BlueXP

Si desea verificar que su sistema Linux cumpla todos los requisitos previos independientemente de ejecutar la instalación de la clasificación de BlueXP, hay un script independiente que puede descargar y que solo prueba los requisitos previos. "Descubre cómo comprobar si tu host Linux está listo para instalar la clasificación de BlueXP".

7 de marzo de 2023 (versión 1.21)

Nueva funcionalidad para añadir tus propias categorías personalizadas desde la interfaz de usuario de clasificación de BlueXP

Ahora, la clasificación de BlueXP te permite añadir tus propias categorías personalizadas de forma que la clasificación de BlueXP identifique los archivos que se adaptan a esas categorías. La clasificación de BlueXP tiene muchas "categorías predefinidas", por lo tanto, esta característica permite agregar categorías personalizadas para identificar dónde se encuentra la información que es única para la organización en los datos.

"Leer más".

Ahora puedes añadir palabras clave personalizadas desde la interfaz de usuario de clasificación de BlueXP

La clasificación de BlueXP ha tenido la capacidad de añadir palabras clave personalizadas que la clasificación de BlueXP identificará en futuros análisis durante algún tiempo. Sin embargo, tienes que iniciar sesión en el host Linux de clasificación BlueXP y utilizar una interfaz de línea de comandos para añadir las palabras clave. En esta versión, la capacidad de añadir palabras clave personalizadas se encuentra en la interfaz de usuario de clasificación de BlueXP, por lo que es muy fácil añadir y editar estas palabras clave.

"Obtén más información sobre cómo añadir palabras clave personalizadas en la interfaz de usuario de clasificación de BlueXP".

Posibilidad de que la clasificación de BlueXP no escanee los archivos cuando se cambie la “última hora de acceso”

De forma predeterminada, si la clasificación de BlueXP no tiene permisos de «escritura» adecuados, el sistema no analizará los archivos de tus volúmenes, porque la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Sin embargo, si no le importa si la última hora de acceso se restablece a la hora original de sus archivos, puede anular este comportamiento en la página Configuration para que la clasificación de BlueXP analice los volúmenes con independencia de los permisos.

Junto con esta funcionalidad, se ha añadido un nuevo filtro llamado «Scan Analysis Event» para que puedas ver los archivos que no se clasificaron porque la clasificación de BlueXP no pudo revertir el último acceso o los archivos clasificados aunque la clasificación de BlueXP no pudo revertir el último acceso.

"Obtén más información sobre la «marca de tiempo de último acceso» y los permisos que requiere la clasificación de BlueXP".

Existen tres nuevos tipos de datos personales identificados por la clasificación de BlueXP

La clasificación de BlueXP puede identificar y categorizar los archivos que contengan los siguientes tipos de datos:

- Número de tarjeta de identidad de Botswana (Omang)
- Número de pasaporte de Botswana
- Tarjeta de identidad de registro nacional de Singapur (NRIC)

"Consulta todos los tipos de datos personales que la clasificación de BlueXP puede identificar en tus datos".

Funcionalidad actualizada para directorios

- La opción "Informe CSV claro" para Informes de investigación de datos ahora incluye información de los directorios.
- El filtro de tiempo "último acceso" muestra ahora la última hora a la que se accedió tanto para archivos como para directorios.

Mejoras en la instalación

- El instalador de clasificación de BlueXP para sitios sin acceso a Internet (sitios oscuros) ahora realiza una comprobación previa para asegurarse de que se cumplen los requisitos de red y del sistema para que la instalación se realice correctamente.
- Los archivos de registro de auditoría de la instalación se guardan ahora y se escriben en `/ops/netapp/install_logs`.

5 de febrero de 2023 (versión 1.20)

Posibilidad de enviar correos electrónicos de notificación basados en políticas a cualquier dirección de correo electrónico

En versiones anteriores de la clasificación de BlueXP, puedes enviar alertas por correo electrónico a los usuarios de BlueXP en tu cuenta cuando ciertas Políticas críticas devuelvan resultados. Esta función le permite obtener notificaciones para proteger sus datos cuando no está en línea. Ahora también puede enviar alertas de correo electrónico desde Directivas a cualquier otro usuario - hasta 20 direcciones de correo electrónico - que no se encuentren en su cuenta de BlueXP.

"Obtenga más información sobre el envío de alertas por correo electrónico basadas en los resultados de la directiva".

Ahora puedes añadir patrones personales desde la interfaz de usuario de clasificación de BlueXP

La clasificación de BlueXP ha tenido la capacidad de añadir «datos personales» personalizados que la clasificación de BlueXP identificará en futuros análisis durante algún tiempo. Sin embargo, tenía que iniciar sesión en el host Linux de clasificación de BlueXP y utilizar una línea de comandos para añadir los patrones personalizados. En esta versión, la capacidad de añadir patrones personales con un regex se encuentra en la interfaz de usuario de clasificación de BlueXP, lo que facilita la adición y edición de estos patrones personalizados.

"Obtén más información sobre cómo añadir patrones personalizados en la interfaz de usuario de clasificación de BlueXP".

Capacidad para mover 15 millones de archivos con la clasificación de BlueXP

Anteriormente, la clasificación de BlueXP podía mover un máximo de 100.000 archivos de origen a cualquier recurso compartido NFS. Ahora puede mover hasta 15 millones de archivos a la vez. "Más información sobre mover archivos de origen con la clasificación de BlueXP".

Capacidad para ver el número de usuarios que tienen acceso a archivos de SharePoint Online

El filtro "número de usuarios con acceso" ahora admite archivos almacenados en repositorios en línea de SharePoint. Anteriormente, solo se admitía los ficheros con recursos compartidos CIFS. Tenga en cuenta que los grupos de SharePoint que no están basados en directorios activos no se contarán en este filtro en este momento.

Se ha agregado un nuevo estado "éxito parcial" al panel Estado de acción

El nuevo estado «Correcto parcial» indica que una acción de clasificación de BlueXP ha finalizado y que algunos elementos han fallado y algunos elementos se han realizado correctamente, por ejemplo, cuando mueve o elimina archivos 100. Además, se ha cambiado el nombre del estado "terminado" por "correcto". En el pasado, el estado "terminado" podría incluir acciones que se han realizado correctamente y que han fallado. Ahora el estado "éxito" significa que todas las acciones se han realizado correctamente en todos los elementos. "Consulte cómo ver el panel Estado de acciones".

9 de enero de 2023 (versión 1.19)

Capacidad para ver un gráfico de archivos que contienen datos confidenciales y que son excesivamente permisivos

El panel de control de gobierno ha agregado un área nueva *sensible Data y permisos amplios* que proporciona un mapa térmico de archivos que contienen datos confidenciales (incluidos datos personales confidenciales y confidenciales) y que son demasiado permisivos. Esto puede ayudarle a ver dónde puede tener algunos riesgos con datos confidenciales. "Leer más".

Hay tres filtros nuevos disponibles en la página Investigación de datos

Hay nuevos filtros disponibles para refinar los resultados que se muestran en la página Investigación de datos:

- El filtro "número de usuarios con acceso" muestra qué archivos y carpetas están abiertos a un determinado número de usuarios. Puede elegir un intervalo de números para refinar los resultados, por ejemplo, para ver los archivos a los que pueden acceder 51-100 usuarios.

- Los filtros "Hora de creación", "Hora descubierta", "última modificación" y "último acceso" ahora permiten crear un intervalo de fechas personalizado en lugar de sólo seleccionar un intervalo de días predefinido. Por ejemplo, puede buscar archivos con una "hora creada" "más de 6 meses" o con una fecha "última modificación" dentro de los "últimos 10 días".
- El filtro "Ruta de acceso" le permite especificar rutas que desea excluir de los resultados de la consulta filtrada. Si introduce rutas para incluir y excluir determinados datos, primero la clasificación de BlueXP busca todos los archivos en las rutas incluidas, luego quita los archivos de las rutas excluidas y, a continuación, muestra los resultados.

"Consulte la lista de todos los filtros que puede utilizar para investigar los datos".

La clasificación de BlueXP puede identificar el número individual japonés

La clasificación de BlueXP puede identificar y categorizar los archivos que contengan el número individual japonés (también conocido como My Number). Esto incluye tanto el número personal como el número de mi corporativo. "Consulta todos los tipos de datos personales que la clasificación de BlueXP puede identificar en tus datos".

Limitaciones conocidas

Las limitaciones conocidas identifican funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

El lanzamiento de clasificación de BlueXP eliminó temporalmente las opciones

La versión de diciembre de 2023 (versión 1.26.6) eliminó temporalmente las siguientes opciones:

- Se deshabilitó la opción para activar la recogida de registros de auditoría.
- Durante la investigación de directorios, la opción de calcular el número de datos de información personal identificable (PII) por directorios no está disponible.
- Se ha desactivado la opción de integrar datos mediante etiquetas de Azure Information Protection (AIP).

Limitaciones de análisis de clasificación de BlueXP

La clasificación de BlueXP solo analiza un recurso compartido de un volumen

Si tienes varios recursos compartidos de archivos en un solo volumen, la clasificación de BlueXP analiza el recurso compartido con la jerarquía más alta. Por ejemplo, si tiene recursos compartidos como los siguientes:

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

A continuación, se escanearán los datos de /A. Los datos en /C y /D no se escanearán.

Solución alternativa

Hay una solución para asegurarse de que está escaneando datos de todos los recursos compartidos del volumen. Siga estos pasos:

1. En el entorno de trabajo, agregue el volumen que se va a escanear.
2. Una vez que la clasificación de BlueXP haya completado el análisis del volumen, vaya a la página *Data Investigation* y cree un filtro para ver qué recurso compartido se está analizando:

   Filtrará los datos por «Nombre del entorno de trabajo» y «Tipo de directorio = Compartir» para ver qué recurso compartido se está escaneando.

3. Obtenga la lista completa de recursos compartidos que existen en el volumen para poder ver qué recursos compartidos no se están analizando.
4. "Agregue los recursos compartidos restantes a un grupo de recursos compartidos".

   Deberá agregar todos los recursos compartidos de forma individual, por ejemplo:

   ```
   /C
   /D
   ```

5. Realice estos pasos para cada volumen del entorno de trabajo que tenga varios recursos compartidos.

Manos a la obra

Más información sobre la clasificación de BlueXP

La clasificación de BlueXP (Cloud Data Sense) es un servicio de gobernanza de datos para BlueXP que analiza tus fuentes de datos corporativas on-premises y en la nube para asignar y clasificar datos, así como para identificar la información privada. Esto puede ayudarle a reducir los riesgos de seguridad y de cumplimiento de normativas, a reducir los costes de almacenamiento y a facilitar los proyectos de migración de datos.

Funciones

La clasificación de BlueXP utiliza la inteligencia artificial (IA), el procesamiento del lenguaje natural (NLP) y el aprendizaje automático (ML) para entender el contenido que escanea y, así, extraer entidades y categorizar el contenido debidamente. Esto permite la clasificación de BlueXP para proporcionar las siguientes áreas de funcionalidad.

"Obtén más información sobre los casos de uso para la clasificación de BlueXP".

Mantenga el cumplimiento normativo

La clasificación de BlueXP proporciona varias herramientas que pueden ayudarte en tus tareas de cumplimiento de normativas. Puedes usar la clasificación de BlueXP para lo siguiente:

- Identificación de la Información personal de identificación (PII).
- Identificar un amplio alcance de información personal confidencial según las normativas de privacidad del RGPD, la CCPA, el PCI y la HIPAA.
- Responda a las solicitudes de acceso de sujetos de datos (DSAR) en función del nombre o la dirección de correo electrónico.
- Identifica si se encuentran identificadores únicos de tus bases de datos en archivos de otros repositorios, básicamente creando tu propia lista de «datos personales» que se identifican en los análisis de clasificación de BlueXP.
- Notificar a determinados usuarios por correo electrónico cuando los archivos contienen un PII determinado (definir este criterio mediante "Normativas") para que pueda decidir sobre un plan de acción.

Refuerce la seguridad

La clasificación de BlueXP puede identificar los datos a los que podría correr riesgo de acceder con fines criminales. Puedes usar la clasificación de BlueXP para lo siguiente:

- Identifique todos los archivos y directorios (recursos compartidos y carpetas) con permisos abiertos que se exponen a toda la organización o al público.
- Identifique los datos confidenciales que se encuentran fuera de la ubicación inicial dedicada.
- Cumpla con las políticas de retención de datos.
- Utilice *Policies* para notificar automáticamente al personal de seguridad sobre nuevos problemas de seguridad y que puedan actuar inmediatamente.
- Agregue etiquetas personalizadas a los archivos (por ejemplo, "hay que mover") y asigne un usuario de BlueXP para que esa persona pueda tener actualizaciones en los archivos.

- Ver y modificar "Etiquetas de Azure Information Protection (AIP)" en sus archivos.

Optimice la utilización del almacenamiento

La clasificación de BlueXP proporciona herramientas que pueden ayudarte con el TCO (TCO) de tu almacenamiento. Puedes usar la clasificación de BlueXP para lo siguiente:

- Aumente la eficiencia del almacenamiento identificando datos duplicados o no relacionados con la empresa. Puede utilizar esta información para decidir si desea mover o eliminar determinados archivos.
- Elimine los archivos que parezcan poco seguros o demasiado arriesgados a dejar en el sistema de almacenamiento o que haya identificado como duplicados. Puede utilizar *Policies* para eliminar automáticamente los archivos que coincidan con determinados criterios.
- Ahorre en costes de almacenamiento identificando los datos inactivos que puede establecer niveles en almacenamiento de objetos más económico. "Obtenga más información sobre la organización en niveles en sistemas Cloud Volumes ONTAP". "Obtenga más información acerca de la organización en niveles desde sistemas ONTAP en las instalaciones".

Acelere la migración de datos

La clasificación de BlueXP puede utilizarse para analizar tus datos on-premises antes de migrarlos a la nube pública o privada. Puedes usar la clasificación de BlueXP para lo siguiente:

- Consulte el tamaño de los datos y si alguno de ellos contiene información confidencial antes de moverlos.
- Filtre los datos de origen (según más de 25 tipos de criterios) para que pueda mover sólo los archivos necesarios al destino. No se mueven los datos innecesarios.
- Mueva, copie y sincronice automáticamente y continuamente solo los datos necesarios en el repositorio en el cloud.

Orígenes de datos compatibles

La clasificación de BlueXP puede analizar y analizar datos estructurados y no estructurados a partir de los siguientes tipos de orígenes de datos:

NetApp:

- Cloud Volumes ONTAP (implementado en AWS, Azure o GCP)
- Clústeres de ONTAP en las instalaciones
- StorageGRID
- Azure NetApp Files
- Amazon FSX para ONTAP
- Cloud Volumes Service para Google Cloud

No NetApp:

- Isilon de Dell EMC
- Pure Storage
- Nutanix
- Cualquier otro proveedor de almacenamiento

Cloud:

- Amazon S3
- Google Cloud Storage
- OneDrive
- SharePoint online
- SharePoint en las instalaciones (SharePoint Server)
- Unidad de Google

Bases de datos:

- Servicio de bases de datos relacionales de Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- Servidor SQL (MSSQL)

La clasificación de BlueXP es compatible con las versiones de NFS 3.x y CIFS 1.x, 2,0, 2,1 y 3,0.

Coste

- El coste de utilizar la clasificación de BlueXP depende de la cantidad de datos que se estén escaneando. Los primeros 1 TB de datos que analiza la clasificación de BlueXP en un espacio de trabajo de BlueXP son gratis durante 30 días. Esto incluye todos los datos de todos los entornos de trabajo y orígenes de datos. Debe haber una suscripción a AWS, Azure o GCP Marketplace o una licencia con su propia licencia de NetApp para seguir analizando datos después de ese punto. Consulte "precios" para obtener más detalles.

  "Descubre cómo licenciar la clasificación de BlueXP".

- Para instalar la clasificación de BlueXP en la nube, es necesario poner en marcha una instancia de nube, lo que se genera en los cargos del proveedor de nube en el que se la pone en marcha. Consulte el tipo de instancia que se pone en marcha en cada cloud proveedor. No hay coste si instalas la clasificación de BlueXP en un sistema on-premises.
- Para la clasificación de BlueXP es necesario que hayas puesto en marcha un conector BlueXP. En muchos casos ya tiene un conector debido a otros servicios y almacenamiento que está utilizando en BlueXP. La instancia de Connector representa cargos del proveedor de cloud en el que se ha puesto en marcha. Consulte "tipo de instancia que se pone en marcha para cada proveedor de cloud". No hay costo si instala el conector en un sistema local.

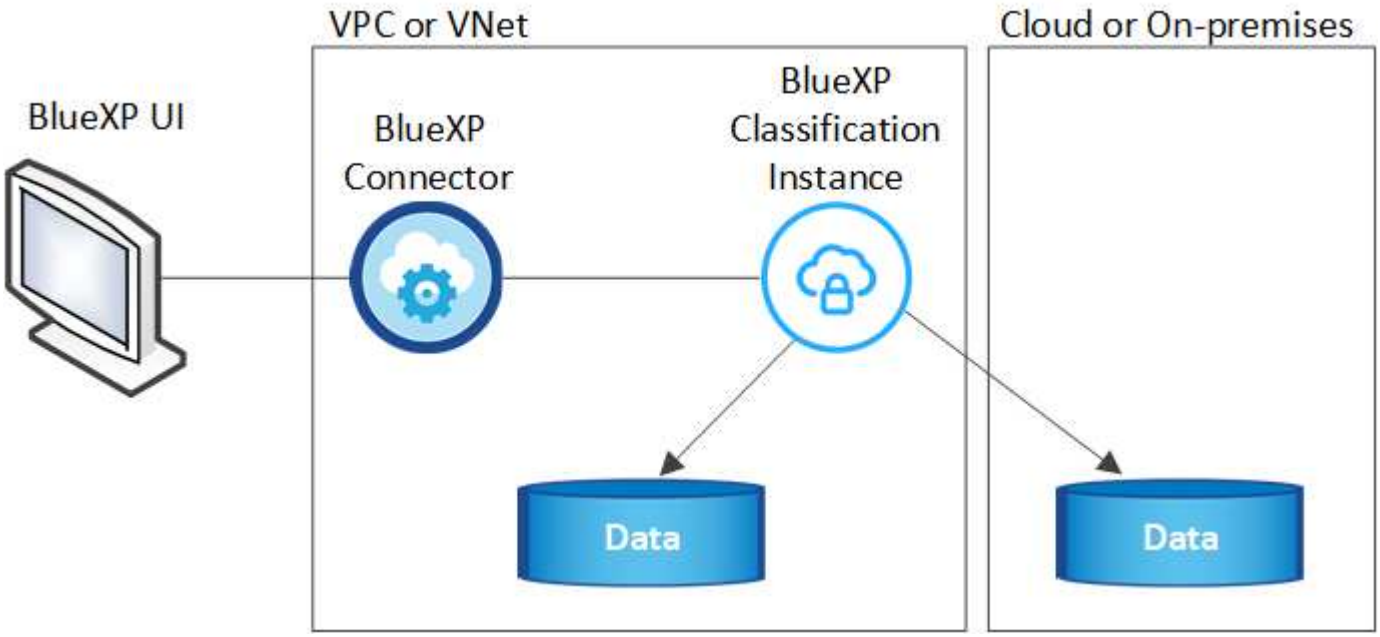
Costes de transferencia de datos

Los costes de la transferencia de datos dependen de su configuración. Si la instancia de clasificación y el origen de datos de BlueXP se encuentran en la misma zona y región de disponibilidad, no hay costes de transferencia de datos. Pero si el origen de los datos, como un sistema Cloud Volumes ONTAP o un bloque S3, está en una región o zona de disponibilidad *diferente*, su proveedor cloud le cobrará los costes de transferencia de datos. Consulte estos enlaces para obtener más información:

- "AWS: Precios de Amazon EC2"
- "Microsoft Azure: Detalles de precios del ancho de banda"
- "Google Cloud: Precios del servicio de transferencia de almacenamiento"

La instancia de clasificación de BlueXP

Cuando pones en marcha la clasificación de BlueXP en la nube, BlueXP pone en marcha la instancia en la misma subred que Connector. "Más información sobre conectores."



Tenga en cuenta lo siguiente acerca de la instancia predeterminada:

- En AWS, la clasificación de BlueXP se ejecuta en un "instancia m6i.4xlarge" Con un disco GP2 de 500 GIB. La imagen del sistema operativo es Amazon Linux 2. Cuando se implementa en AWS, puede elegir un tamaño de instancia más pequeño si va a escanear una pequeña cantidad de datos.
- En Azure, la clasificación de BlueXP se ejecuta en A. "VM Standard_D16s_v3" Con un disco de 500 GIB. La imagen del sistema operativo es CentOS 7.9.
- En GCP, la clasificación de BlueXP se ejecuta en un "n2-Standard-16 VM" Con un disco persistente estándar de 500 GIB. La imagen del sistema operativo es CentOS 7.9.
- En las regiones en las que la instancia predeterminada no está disponible, la clasificación de BlueXP se ejecuta en una instancia alternativa. "Consulte los tipos de instancia alternativa".
- La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Solo se pone en marcha una instancia de clasificación de BlueXP por cada Connector.

También puedes poner en marcha la clasificación de BlueXP en un host Linux on-premises o en un host de tu proveedor de nube preferido. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija. Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga acceso a Internet.

La instancia debe permanecer ejecutándose en todo momento porque la clasificación de BlueXP analiza los datos de forma continua.

Con un tipo de instancia más pequeño

Puedes poner en marcha la clasificación de BlueXP en un sistema con menos CPU y menos RAM, pero existen algunas limitaciones al usar estos sistemas menos potentes.

Tamaño del sistema	Especificaciones	Limitaciones
Extra grande	32 CPU, 128 GB de RAM, SSD de 1 TiB	Puede escanear hasta 500 millones de archivos.
Grande (predeterminado)	16 CPU, 64 GB de RAM, 500 GIB de SSD	Puede escanear hasta 250 millones de archivos.
Mediano	8 CPU, 32 GB de RAM, 200 GIB de SSD	El análisis es más lento y sólo puede analizar un millón de archivos.
Pequeño	8 CPU, 16 GB de RAM, 100 GIB de SSD	Las mismas limitaciones que "Medio", más la capacidad de identificar "nombres de asunto de los datos" los archivos internos están desactivados.

Al poner en marcha la clasificación de BlueXP en la nube en AWS, puedes elegir una instancia grande, mediana o pequeña. Al implementar la clasificación de BlueXP en Azure o GCP, envía un correo electrónico a ng-contact-data-sense@netapp.com para obtener ayuda si quieres utilizar uno de estos sistemas alternativos. Tendremos que trabajar con usted para poner en marcha estas otras configuraciones de cloud.

Cuando ponga en marcha la clasificación de BlueXP en las instalaciones, solo tiene que utilizar un host Linux con las especificaciones alternativas. No necesita ponerse en contacto con NetApp para obtener ayuda.

Funcionamiento de la clasificación de BlueXP

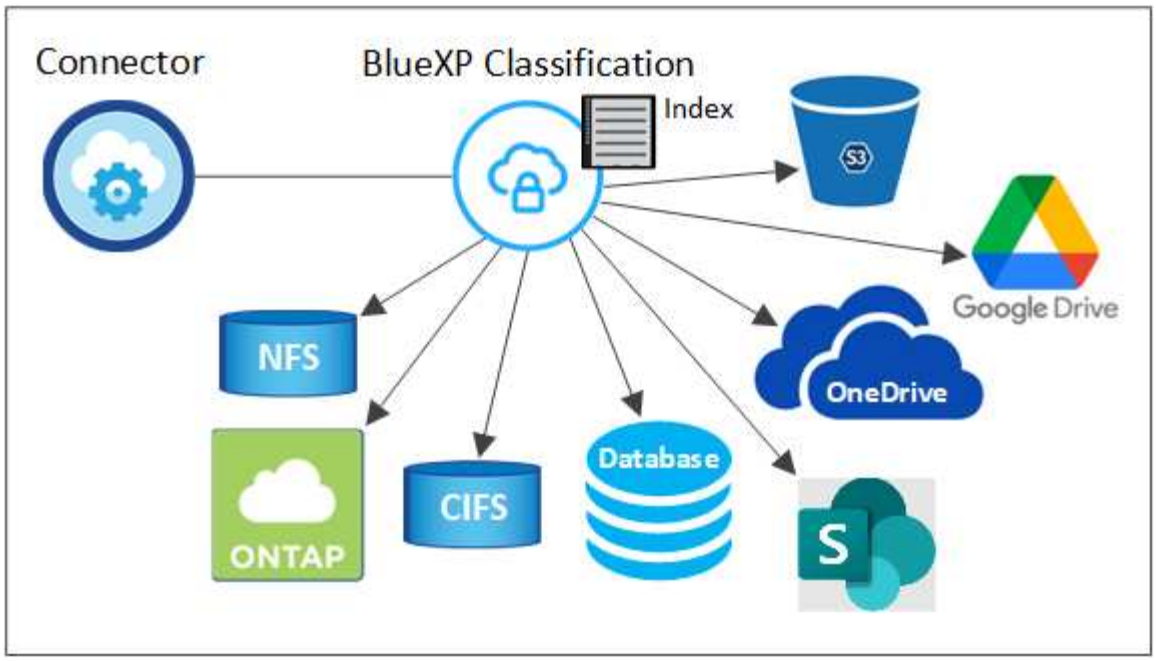
En un nivel alto, la clasificación de BlueXP funciona así:

1. Implementas una instancia de clasificación de BlueXP en BlueXP.
2. Puede activar la asignación de alto nivel o el análisis de alto nivel en uno o más orígenes de datos.
3. La clasificación de BlueXP analiza los datos mediante un proceso de aprendizaje de IA.
4. Utilice las consolas y herramientas de informes que se proporcionan con el fin de ayudarle en sus esfuerzos de cumplimiento de normativas y gobierno.

Cómo funcionan las exploraciones

Después de habilitar la clasificación de BlueXP y seleccionar los repositorios que desea analizar (estos son los volúmenes, los bloques, los esquemas de la base de datos o los datos de usuario de OneDrive o SharePoint), comienza inmediatamente a analizar los datos para identificar los datos personales y confidenciales. Debería centrarse en analizar los datos de producción en directo en la mayoría de los casos en lugar de realizar backups, duplicados o sitios de recuperación ante desastres. A continuación, la clasificación de BlueXP asigna sus datos de organización, categoriza cada archivo e identifica y extrae entidades y patrones predefinidos en los datos. El resultado de la exploración es un índice de información personal, información personal confidencial, categorías de datos y tipos de archivo.

La clasificación de BlueXP se conecta a los datos igual que cualquier otro cliente ya que se monta en los volúmenes de NFS y CIFS. Se accede automáticamente a los volúmenes NFS como de solo lectura, mientras que se necesitan proporcionar credenciales de Active Directory para analizar volúmenes CIFS.



Tras el análisis inicial, la clasificación de BlueXP analiza continuamente los datos por turnos para detectar los cambios incrementales (por este motivo es importante mantener la instancia en ejecución).

Puede habilitar y deshabilitar los análisis a nivel del volumen, en el nivel de bloque, en el nivel de esquema de base de datos, en el nivel de usuario de OneDrive y en el nivel del sitio de SharePoint.

¿Cuál es la diferencia entre las exploraciones de asignación y clasificación

La clasificación de BlueXP te permite ejecutar un análisis general de «asignaciones» en fuentes de datos seleccionadas. La asignación sólo ofrece una descripción general de alto nivel de los datos, mientras que la clasificación proporciona un análisis profundo de los datos. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro.

A muchos usuarios les gusta esta funcionalidad porque quieren analizar rápidamente sus datos para identificar los orígenes de datos que requieren más investigación y, a continuación, pueden habilitar análisis de clasificación solo en los orígenes o volúmenes de datos necesarios.

En la siguiente tabla se muestran algunas de las diferencias:

Función	Clasificación	Asignación
Velocidad de escaneado	Lento	Y rápido
Lista de tipos de archivo y capacidad utilizada	Sí	Sí
Número de archivos y capacidad utilizada	Sí	Sí
Antigüedad y tamaño de los archivos	Sí	Sí
Capacidad de ejecutar una "Informe de asignación de datos"	Sí	Sí
Página de investigación de datos para ver los detalles del archivo	Sí	No
Buscar nombres dentro de los archivos	Sí	No

Función	Clasificación	Asignación
Cree "normativas" que proporcionan resultados de búsqueda personalizados	Sí	No
Categorice los datos mediante etiquetas AIP y etiquetas de estado	Sí	No
Copie, elimine y mueva los archivos de origen	Sí	No
Capacidad para ejecutar otros informes	Sí	No

Con qué rapidez escanea los datos de clasificación de BlueXP

La velocidad de análisis se ve afectada por la latencia de la red, la latencia del disco, el ancho de banda de la red, el tamaño del entorno y los tamaños de distribución de archivos.

- Cuando se realizan escaneos de mapeo, la clasificación de BlueXP puede analizar entre 100-150 TIBs de datos al día, por nodo de escáner.
- Cuando se realizan análisis de clasificación, la clasificación de BlueXP puede analizar entre 15-40 TIBs de datos al día, por nodo de escáner.

"Obtenga más información sobre la implementación de varios nodos de escáner para analizar los datos".

Información que indexa la clasificación de BlueXP

La clasificación de BlueXP recopila, indexa y asigna categorías a tus datos (archivos). Los datos que indexa la clasificación de BlueXP incluyen los siguientes:

Metadatos estándar

La clasificación de BlueXP recopila metadatos estándar sobre archivos: El tipo de archivo, su tamaño, fechas de creación y modificación, etc.

Datos personales

Información de identificación personal, como direcciones de correo electrónico, números de identificación o números de tarjetas de crédito. "Más información sobre datos personales".

Datos personales confidenciales

Tipos especiales de información confidencial, como datos sanitarios, origen étnico o opiniones políticas, según lo define el RGPD y otras regulaciones de privacidad. "Más información sobre datos personales confidenciales".

Categorías

La clasificación de BlueXP toma los datos que ha escaneado y los divide en distintos tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. "Más información sobre categorías".

Tipos

La clasificación de BlueXP toma los datos que ha escaneado y los desglosa por según el tipo de archivo. "Obtenga más información sobre los tipos".

Reconocimiento de entidad de nombre

La clasificación de BlueXP usa la IA para extraer los nombres de las personas físicas de los documentos. "Obtenga información sobre cómo responder a las solicitudes de acceso a sujetos de datos".

Información general sobre redes

BlueXP implementa la instancia de clasificación de BlueXP con un grupo de seguridad que permite las conexiones HTTP de entrada desde la instancia de Connector.

Cuando se utiliza BlueXP en el modo SaaS, la conexión a BlueXP se establece a través de HTTPS, y los datos privados que se envían entre su navegador y la instancia de clasificación de BlueXP se protegen con un cifrado integral mediante TLS 1,2, lo que significa que NetApp y terceros no podrán leerlo.

Las reglas salientes están completamente abiertas. Se necesita acceso a Internet para instalar y actualizar el software de clasificación de BlueXP y para enviar las métricas de uso.

Si tiene requisitos estrictos de red, "Obtén más información sobre los extremos que contactos de clasificación de BlueXP".

Acceso de los usuarios a la información de cumplimiento

El rol asignado a cada usuario proporciona diferentes funcionalidades dentro de BlueXP y dentro de la clasificación de BlueXP:

- Un **Administrador de cuentas** puede administrar la configuración de cumplimiento y ver la información de cumplimiento de todos los entornos de trabajo.
- **Workspace Admin** puede administrar la configuración de cumplimiento y ver la información de cumplimiento sólo para los sistemas a los que tienen permisos de acceso. Si un administrador de espacio de trabajo no puede acceder a un entorno de trabajo en BlueXP, no podrá ver ninguna información de cumplimiento de normativas del entorno de trabajo en la pestaña de clasificación de BlueXP.
- Los usuarios con la función **Compliance Viewer** sólo pueden ver información de cumplimiento y generar informes para los sistemas a los que tienen permiso de acceso. Estos usuarios no pueden habilitar o deshabilitar el análisis de volúmenes, bloques o esquemas de base de datos. Estos usuarios no pueden copiar, mover ni eliminar archivos.

"Más información sobre los roles de BlueXP" y cómo "añadir usuarios con roles específicos".

Implementa la clasificación de BlueXP

¿Qué puesta en marcha de clasificación de BlueXP deberías utilizar?

Puedes poner en marcha la clasificación de BlueXP de distintas formas. Aprende qué método satisface tus necesidades.

La clasificación de BlueXP se puede implementar de las siguientes maneras:

- "Póngalo en marcha en la nube con BlueXP". BlueXP pondrá en marcha la instancia de clasificación de BlueXP en la misma red de proveedores de cloud que BlueXP Connector.
- "Instale en un host Linux con acceso a Internet". Instala la clasificación de BlueXP en un host Linux de tu red o en un host Linux en el cloud que tenga acceso a Internet. Este tipo de instalación puede ser una buena opción si prefieres analizar sistemas ONTAP on-premises mediante una instancia de clasificación de BlueXP que también está ubicada en las instalaciones, pero este no es un requisito.
- "Instale en un host Linux en un sitio local sin acceso a Internet", También conocido como *modo privado.* Este tipo de instalación, que utiliza un script de instalación, es bueno para sus sitios seguros.

Tanto la instalación en un host Linux con acceso a Internet como la instalación en las instalaciones en un host Linux sin acceso a Internet utilizan un script de instalación. El script comienza comprobando si el sistema y el entorno cumplen los requisitos previos. Si se cumplen los requisitos previos, se inicia la instalación. Si desea verificar los requisitos previos independientemente de la ejecución de la instalación de la clasificación de BlueXP, puede descargar un paquete de software independiente que solo prueba los requisitos previos.

Consulte "Compruebe que su host Linux esté listo para instalar la clasificación de BlueXP".

Pon en marcha la clasificación de BlueXP en el cloud con BlueXP

Completa unos pasos para poner en marcha la clasificación de BlueXP en la nube. BlueXP pondrá en marcha la instancia de clasificación de BlueXP en la misma red de proveedores de cloud que BlueXP Connector.

Tenga en cuenta que también puede "Instala la clasificación de BlueXP en un host Linux que tenga acceso a Internet". Este tipo de instalación puede ser una buena opción si prefieres escanear los sistemas ONTAP on-premises usando una instancia de clasificación de BlueXP que también está ubicada en las instalaciones, pero esto no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Cree un conector**

Si aún no tiene un conector, cree un conector ahora. Consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

También puede hacerlo "Instale el conector en las instalaciones" En un host Linux de su red o en un host Linux del cloud.

2. **Revise los requisitos previos**

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso a Internet saliente para la instancia, conectividad entre Connector y la clasificación de BlueXP a través del puerto 443, y mucho más. Vea la lista completa.

3. **Implementa la clasificación de BlueXP**

Inicia el asistente de instalación para implementar la instancia de clasificación de BlueXP en la nube.

4. **Suscríbete al servicio de clasificación de BlueXP**

Los primeros 1 TB de datos que analiza la clasificación de BlueXP en BlueXP son gratuitos durante 30 días. Debe haber una suscripción a BlueXP a través de su plataforma de proveedores de cloud o una licencia BYOL de NetApp para continuar analizando los datos después de ese punto.

Cree un conector

Si aún no tiene un conector, cree un conector en su proveedor de cloud. Consulte "Creación de un conector en AWS" o. "Creación de un conector en Azure", o. "Creación de un conector en GCP". En la mayoría de los casos, es probable que tengas configurado un Connector antes de intentar activar la clasificación de BlueXP porque la mayoría "Las funciones de BlueXP requieren un conector", pero hay casos en los que necesitará configurar uno ahora.

Existen algunas situaciones en las que debe utilizar un conector implementado en un proveedor de cloud específico:

- Cuando escanea datos en Cloud Volumes ONTAP en AWS, Amazon FSx para ONTAP o en buckets AWS S3, usa un conector en AWS.
- Al escanear datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, se utiliza un conector en Azure.
  - Para Azure NetApp Files, debe implementarse en la misma región que los volúmenes que desea analizar.
- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.

Los sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos genéricos de S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive se pueden analizar al utilizar cualquiera de estos conectores de cloud.

Tenga en cuenta que también puede "Instale el conector en las instalaciones" En un host Linux en su red o en la nube. Algunos usuarios que planean instalar la clasificación de BlueXP en las instalaciones también pueden optar por instalar el conector en las instalaciones.

Como puede ver, puede que haya algunas situaciones en las que necesite utilizar "Múltiples conectores".

Apoyo del Gobierno en las regiones

La clasificación BlueXP se admite cuando Connector se implementa en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD). Cuando se implementa de esta manera, la clasificación de BlueXP tiene las siguientes restricciones:

- Las cuentas de OneDrive, cuentas de SharePoint y cuentas de Google Drive no se pueden analizar.
- La funcionalidad de etiqueta de Microsoft Azure Information Protection (AIP) no se puede integrar.

"Consulte más información sobre el despliegue del conector en una región gubernamental".

Revise los requisitos previos

Revise los siguientes requisitos previos para asegurarse de que tiene una configuración compatible antes de poner en marcha la clasificación de BlueXP en el cloud. Al poner en marcha la clasificación de BlueXP en el cloud, estará ubicada en la misma subred que Connector.

Habilita el acceso a Internet saliente desde la clasificación de BlueXP

La clasificación de BlueXP requiere acceso a Internet saliente. Si tu red física o virtual utiliza un servidor proxy para acceder a Internet, asegúrese de que la instancia de clasificación de BlueXP tenga acceso a Internet saliente para contactar con los siguientes extremos. El proxy debe ser no transparente; actualmente no admitimos proxies transparentes.

Revisa la tabla correspondiente a continuación en función de si vas a poner en marcha la clasificación de

BlueXP en AWS, Azure o GCP.

Extremos necesarios para AWS

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
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/	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
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 la clasificación de BlueXP para acceder a manifiestos y plantillas y descargarlos, así como enviar registros y métricas.

Extremos necesarios para Azure

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
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/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.

Puntos finales necesarios para GCP

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.

Puntos finales	Específico
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/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.

Asegúrese de que BlueXP tiene los permisos necesarios

Asegúrate de que BlueXP tenga permisos para implementar recursos y crear grupos de seguridad para la instancia de clasificación de BlueXP. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".

Asegúrate de que BlueXP Connector pueda acceder a la clasificación de BlueXP

Garantiza la conectividad entre el Connector y la instancia de clasificación de BlueXP. El grupo de seguridad de Connector debe permitir el tráfico de entrada y salida a través del puerto 443 hacia y desde la instancia de clasificación de BlueXP. Esta conexión permite la implementación de la instancia de clasificación de BlueXP y permite ver información en las pestañas Cumplimiento y gobernanza. La clasificación de BlueXP es compatible con las regiones gubernamentales de AWS y Azure.

Se requieren reglas adicionales de grupos de seguridad entrantes y salientes para las implementaciones de AWS GovCloud. Consulte "Reglas para el conector en AWS" para obtener más detalles.

Se requieren reglas adicionales de grupos de seguridad entrantes y salientes para implementaciones gubernamentales de Azure y Azure. Consulte "Reglas para Connector en Azure" para obtener más detalles.

Asegúrate de que puedes mantener en funcionamiento la clasificación de BlueXP

La instancia de clasificación de BlueXP tiene que permanecer en la para analizar tus datos de forma continua.

Garantice la conectividad del explorador web con la clasificación de BlueXP

Después de habilitar la clasificación de BlueXP, asegúrese de que los usuarios accedan a la interfaz de BlueXP desde un host que tiene una conexión a la instancia de clasificación de BlueXP.

La instancia de clasificación de BlueXP usa una dirección IP privada para garantizar que Internet no pueda acceder a los datos indexados. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esa conexión puede proceder de una conexión directa con su proveedor de cloud (por ejemplo, una VPN), o de un host que esté dentro de la misma red que la instancia de clasificación de BlueXP.

Compruebe sus límites de vCPU

Asegúrese de que el límite de vCPU de su proveedor de cloud permita poner en marcha una instancia con el número necesario de núcleos. Deberá verificar el límite de vCPU para la familia de instancias correspondiente en la región donde se está ejecutando BlueXP. "Consulte los tipos de instancia necesarios".

Consulte los siguientes enlaces para obtener más información sobre los límites de vCPU:

- "Documentación de AWS: Cuotas de servicio de Amazon EC2"
- "Documentación de Azure: Cuotas de vCPU de máquina virtual"
- "Documentación de Google Cloud: Cuotas de recursos"

Tenga en cuenta que puede poner en marcha la clasificación de BlueXP en una instancia en entornos de cloud de AWS con menos CPU y menos RAM, pero hay limitaciones cuando se utilizan estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

Pon en marcha la clasificación de BlueXP en el cloud

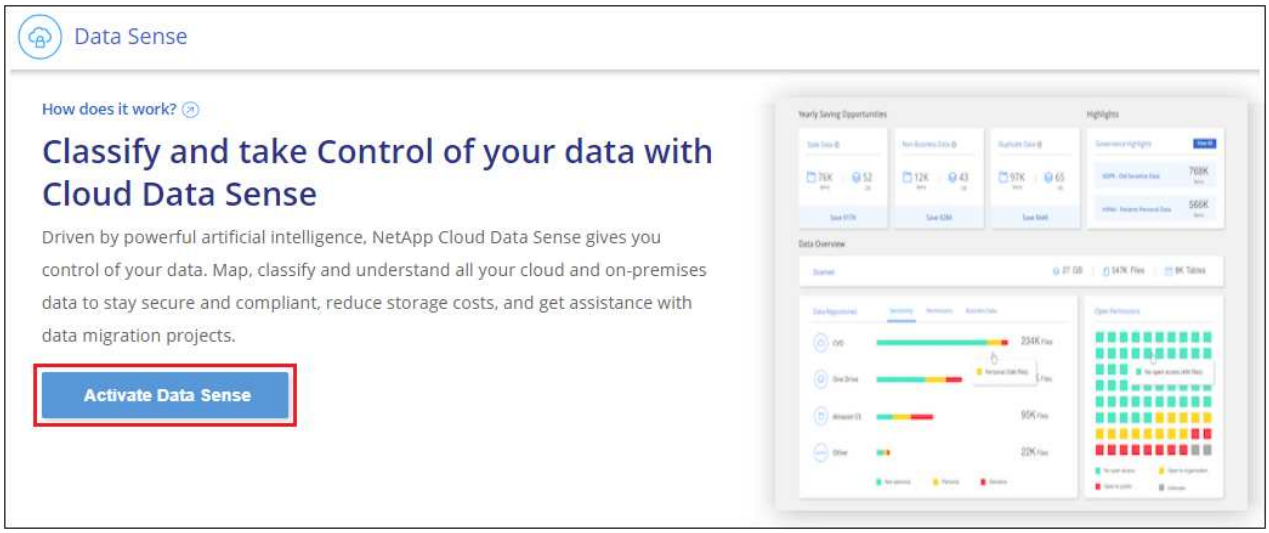
Sigue estos pasos para implementar una instancia de clasificación de BlueXP en la nube. Connector pondrá en marcha la instancia en la nube y, a continuación, instalará el software de clasificación BlueXP en esa instancia.

Tenga en cuenta que cuando implemente la clasificación de BlueXP desde un conector BlueXP en un entorno AWS, puede seleccionar el tamaño de instancia predeterminado o puede seleccionar entre dos tipos de instancia menores. "Vea los tipos de instancia y las limitaciones disponibles". En las regiones en las que el tipo de instancia predeterminado no está disponible, la clasificación de BlueXP se ejecuta en A. "tipo de instancia alternativa".

Implemente en AWS

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación**.



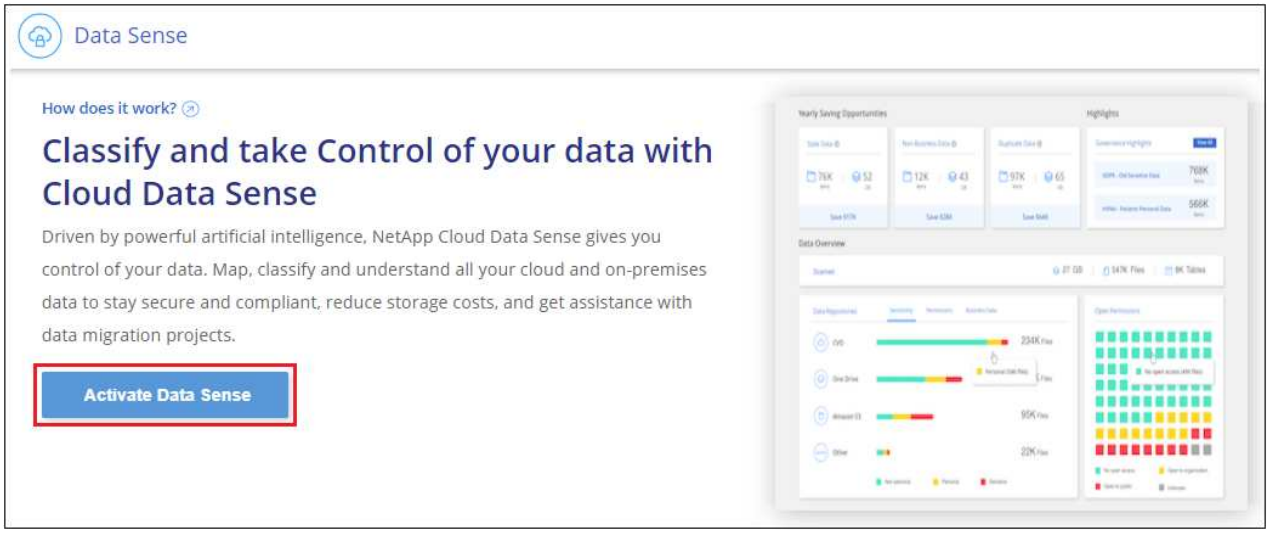
2. Haga clic en **Activar detección de datos**.
3. En la página *Installation*, haga clic en **deploy > Deploy** para utilizar el tamaño de instancia "grande" e iniciar el asistente de implementación de la nube.
4. El asistente muestra el progreso a medida que avanza por los pasos de implementación. Se detendrá y pedirá información si se produce algún problema.

5. Cuando la instancia esté implementada y la clasificación de BlueXP esté instalada, haga clic en **Continuar con la configuración** para ir a la página *Configuration*.

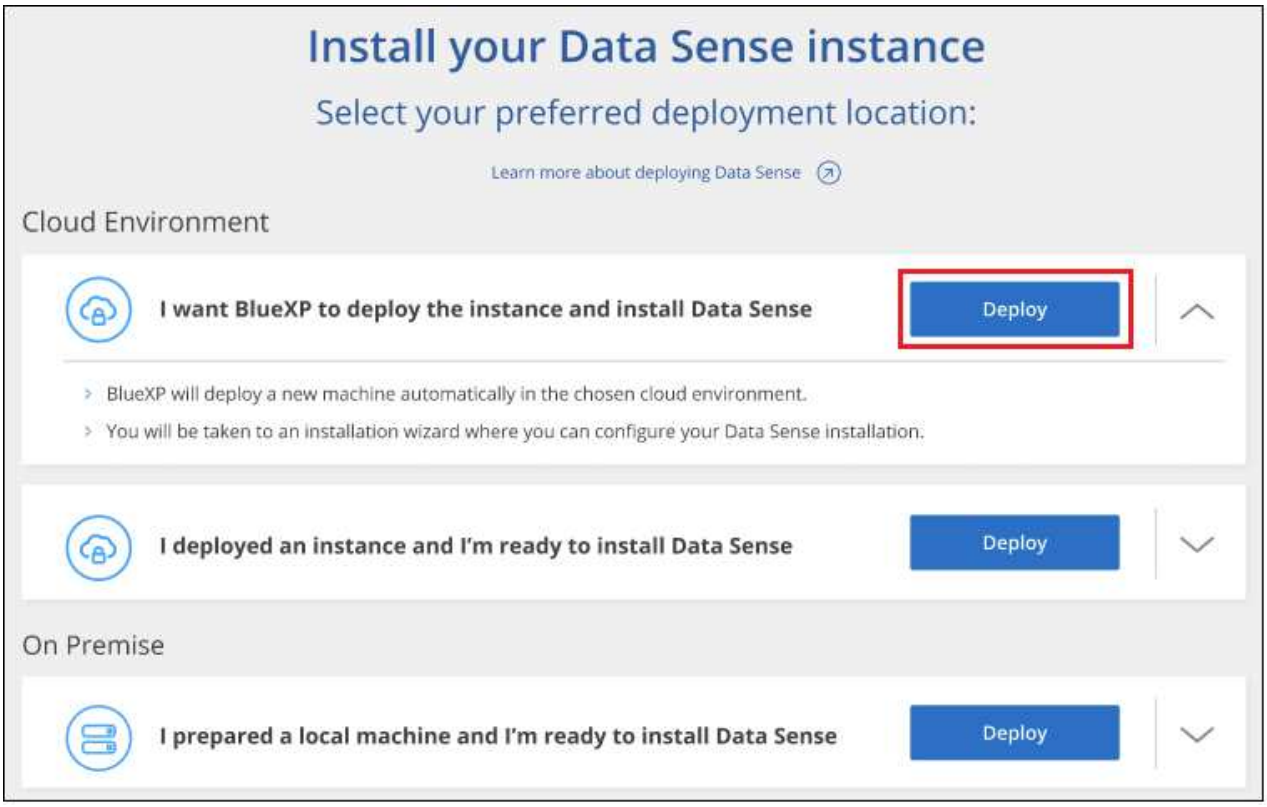
Implemente en Azure

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Activar detección de datos**.



3. Haga clic en **desplegar** para iniciar el asistente de implementación de la nube.



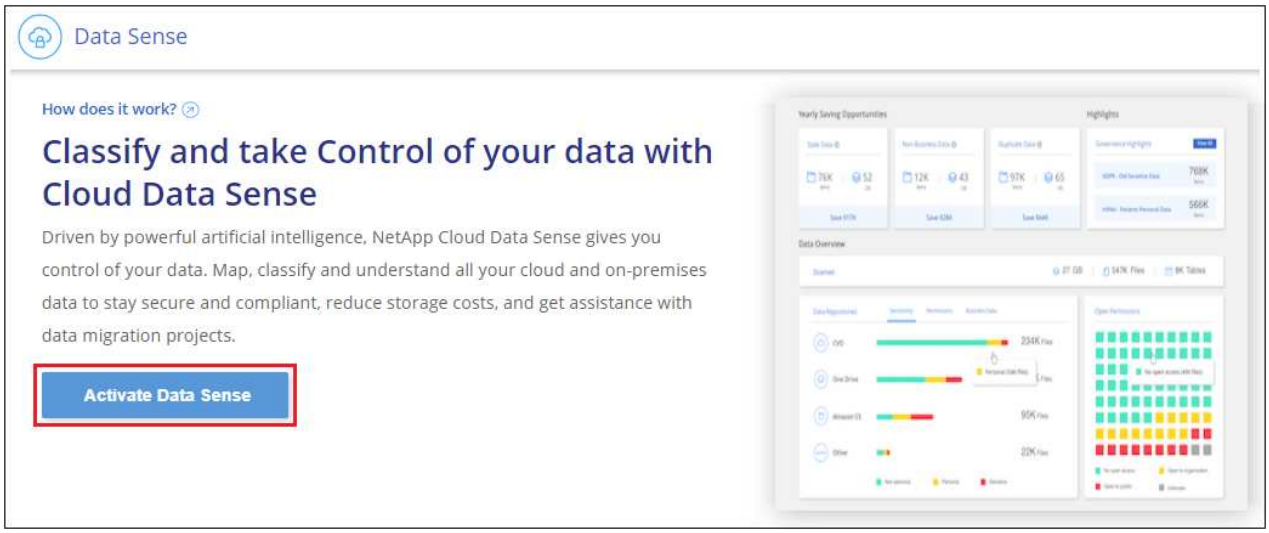
4. El asistente muestra el progreso a medida que avanza por los pasos de implementación. Se detendrá y pedirá información si se produce algún problema.

5. Cuando la instancia esté implementada y la clasificación de BlueXP esté instalada, haga clic en **Continuar con la configuración** para ir a la página *Configuration*.

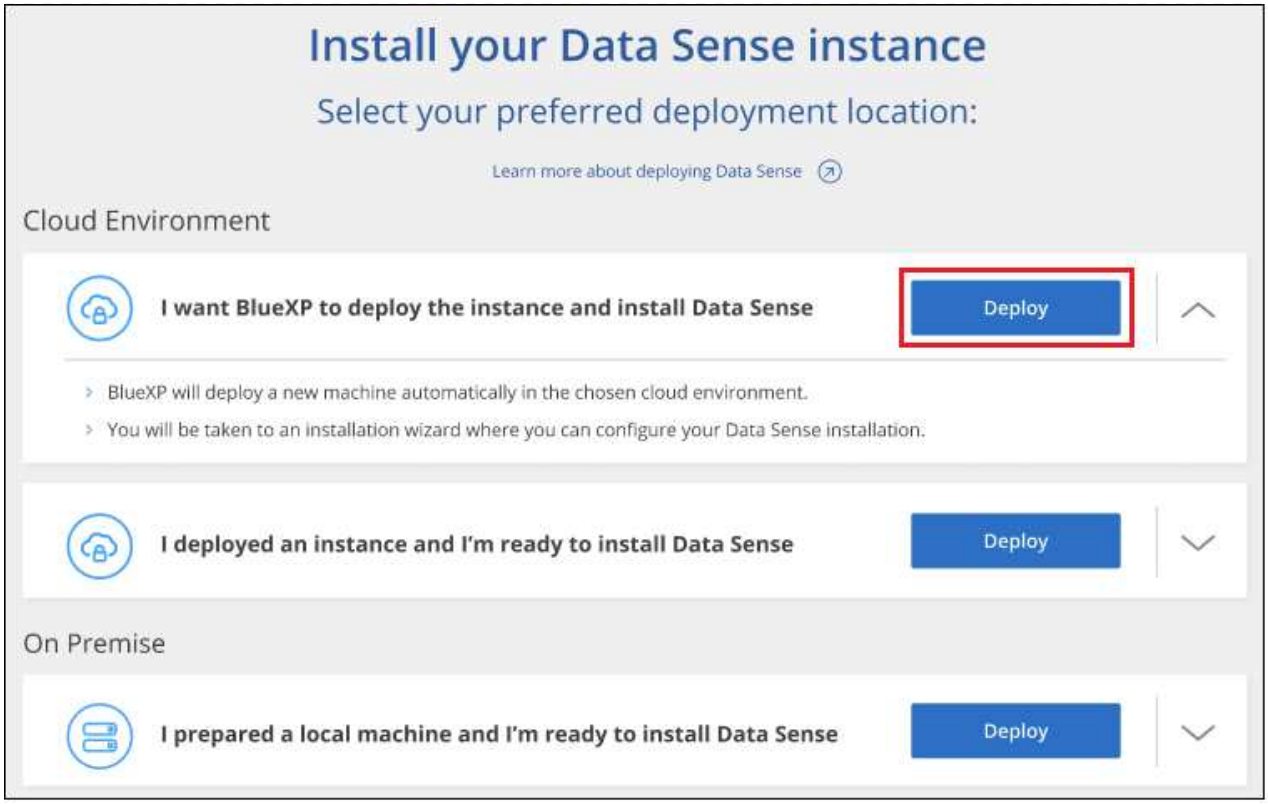
Realice puestas en marcha en Google Cloud

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Activar detección de datos**.



3. Haga clic en **desplegar** para iniciar el asistente de implementación de la nube.



4. El asistente muestra el progreso a medida que avanza por los pasos de implementación. Se detendrá y pedirá información si se produce algún problema.

5. Cuando la instancia esté implementada y la clasificación de BlueXP esté instalada, haga clic en **Continuar con la configuración** para ir a la página *Configuration*.

Resultado

BlueXP pone en marcha la instancia de clasificación de BlueXP en su proveedor de cloud.

Las actualizaciones en BlueXP Connector y el software de clasificación BlueXP se automatizan siempre que las instancias tengan conectividad a Internet.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

También puede hacerlo "Configura las licencias para la clasificación de BlueXP" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

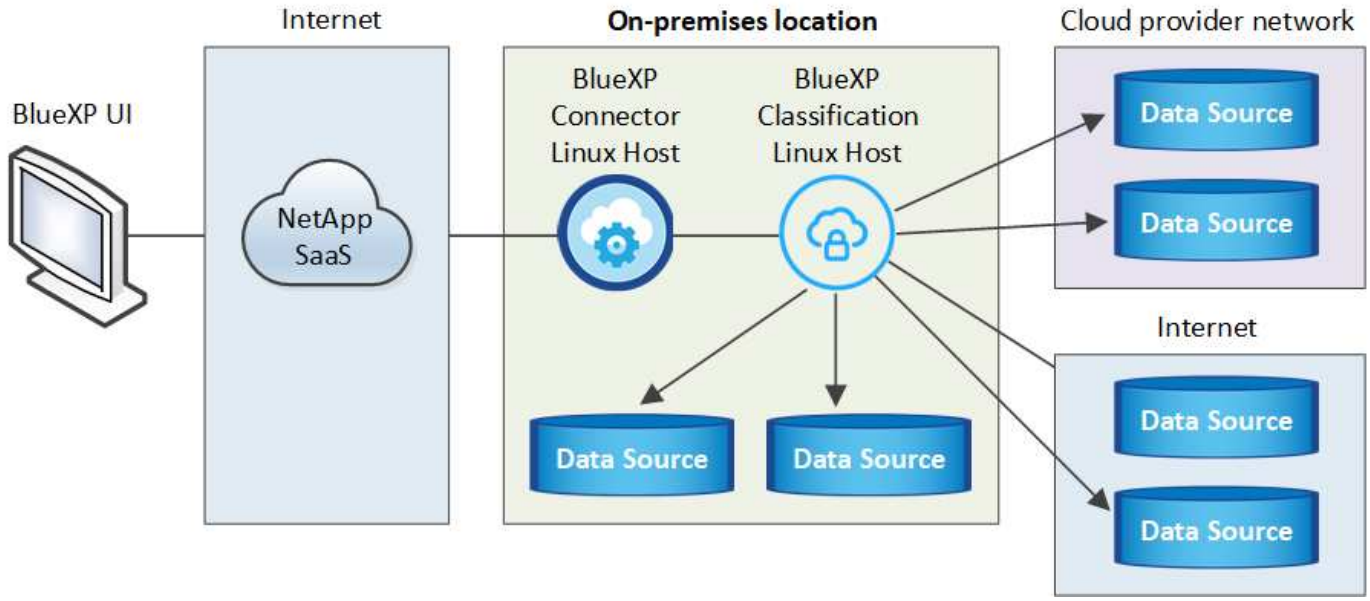
Instala la clasificación de BlueXP en un host que tenga acceso a Internet

Completa unos pasos para instalar la clasificación de BlueXP en un host Linux en tu red o en un host Linux en la nube que tenga acceso a Internet. Deberá implementar el host Linux manualmente en su red o en el cloud como parte de esta instalación.

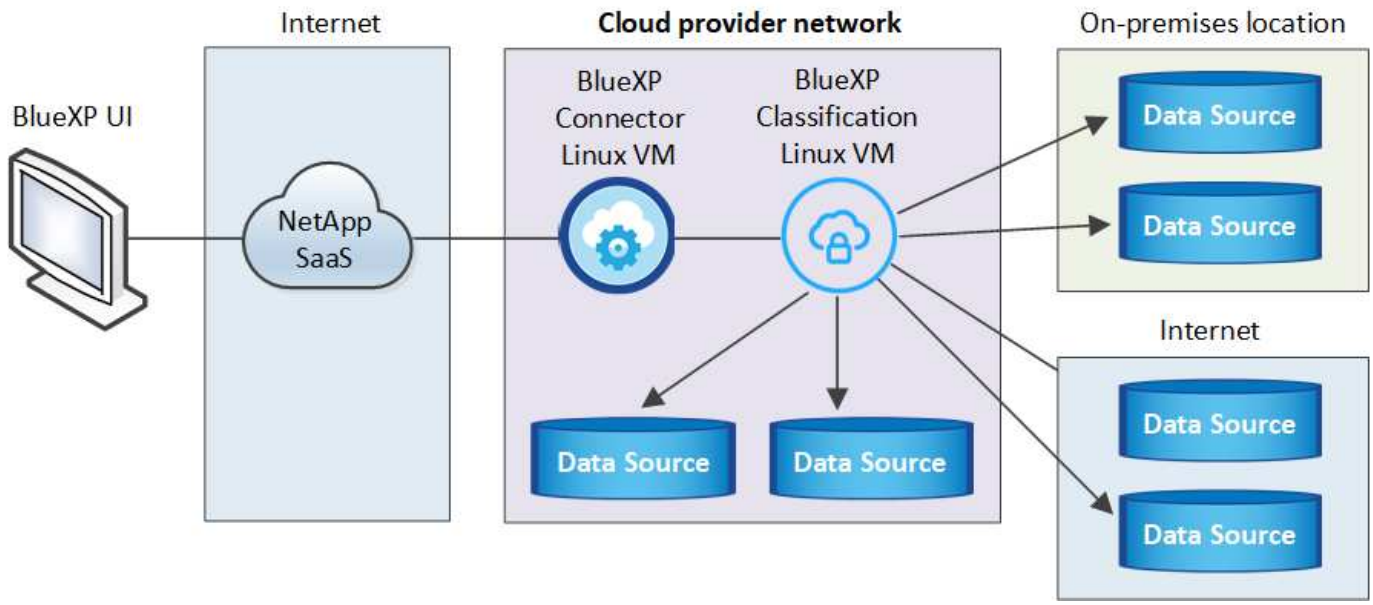
La instalación en las instalaciones puede ser una buena opción si prefieres analizar los sistemas de ONTAP on-premises mediante una instancia de clasificación de BlueXP que también está ubicada en las instalaciones, pero este no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

El script de instalación de clasificación de BlueXP comienza comprobando si el sistema y el entorno cumplen los requisitos previos necesarios. Si se cumplen todos los requisitos previos, se inicia la instalación. Si desea verificar los requisitos previos independientemente de la ejecución de la instalación de la clasificación de BlueXP, puede descargar un paquete de software independiente que solo prueba los requisitos previos. "Descubre cómo comprobar si tu host Linux está listo para instalar la clasificación de BlueXP".

La instalación típica en un host Linux *in your local* tiene los siguientes componentes y conexiones.



La instalación típica en un host Linux *en la nube* tiene los siguientes componentes y conexiones.



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Tenga en cuenta que también puede "Instala la clasificación de BlueXP en un sitio on-premises que no tenga acceso a Internet" para ubicaciones completamente seguras.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Cree un conector

Si aún no tiene un conector, "Ponga en marcha el conector en las instalaciones" En un host Linux de su red o en un host Linux del cloud.

También puede crear un conector con su proveedor de cloud. Consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

2 Revise los requisitos previos

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso a Internet saliente para la instancia, conectividad entre Connector y la clasificación de BlueXP a través del puerto 443, y mucho más. Vea la lista completa.

También necesita un sistema Linux que cumpla con el siga los requisitos.

3 Descarga e implementa la clasificación de BlueXP

Descarga el software de clasificación de Cloud BlueXP en el sitio de soporte de NetApp y copia el archivo del instalador en el host Linux que tengas que utilizar. A continuación, inicie el asistente de instalación y siga las

indicaciones para implementar la instancia de clasificación de BlueXP.

4 Suscríbete al servicio de clasificación de BlueXP

Los primeros 1 TB de datos que analiza la clasificación de BlueXP en BlueXP son gratuitos durante 30 días. Debe suscribirse a su mercado de proveedores de cloud o una licencia de BYOL de NetApp para continuar analizando los datos después de ese punto.

Cree un conector

Es necesario un conector BlueXP para poder instalar y utilizar la clasificación de BlueXP. En la mayoría de los casos, es probable que tengas configurado un Connector antes de intentar activar la clasificación de BlueXP debido a que en la mayoría de los casos "Las funciones de BlueXP requieren un conector", pero hay casos en los que necesitará configurar uno ahora.

Para crear una en su entorno de proveedor de cloud, consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

Existen algunas situaciones en las que debe utilizar un conector implementado en un proveedor de cloud específico:

- Cuando escanea datos en Cloud Volumes ONTAP en AWS, Amazon FSx para ONTAP o en buckets AWS S3, usa un conector en AWS.
- Al escanear datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, se utiliza un conector en Azure.

  Para Azure NetApp Files, debe implementarse en la misma región que los volúmenes que desea analizar.

- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.

Los sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos genérico de S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive se pueden analizar con cualquiera de estos conectores de cloud.

Tenga en cuenta que también puede "Ponga en marcha el conector en las instalaciones" En un host Linux de su red o en un host Linux del cloud. Algunos usuarios que planean instalar la clasificación de BlueXP en las instalaciones también pueden optar por instalar el conector en las instalaciones.

Como puede ver, puede que haya algunas situaciones en las que necesite utilizar "Múltiples conectores".

Necesitarás la dirección IP o el nombre de host del sistema Connector al instalar la clasificación de BlueXP. Tendrá esta información si instaló el conector en sus instalaciones. Si el conector está implementado en la nube, puede encontrar esta información desde la consola BlueXP: Haga clic en el icono Ayuda, seleccione **Soporte** y haga clic en **conector BlueXP**.

Prepare el sistema host Linux

El software de clasificación de BlueXP debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, los requisitos de RAM, los requisitos de software, etc. El host Linux puede estar en su red o en la nube.

Asegúrate de que puedes mantener en funcionamiento la clasificación de BlueXP. La máquina de clasificación de BlueXP tiene que permanecer en ella para analizar tus datos de forma continua.

- La clasificación de BlueXP no se admite en un host compartido con otras aplicaciones; el host debe ser un host dedicado.
- Al crear el sistema host en tus instalaciones, puedes elegir entre tres tamaños de sistema en función del tamaño del conjunto de datos que tengas pensado analizar la clasificación de BlueXP.

Tamaño del sistema	CPU	RAM (la memoria de intercambio debe estar desactivada)	Disco
* Extra grande*	32 CPU	128 GB DE MEMORIA RAM	1 TiB SSD en /, o. - 100 GiB disponible en /opt - 895 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Grande	16 CPU	64 GB DE MEMORIA RAM	500 GiB SSD en /, o. - 100 GiB disponible en /opt - 395 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Media	8 CPU	32 GB DE MEMORIA RAM	200 GiB SSD en /, o. - 50 GiB disponible en /opt - 145 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Pequeño	8 CPU	16 GB DE MEMORIA RAM	100 GiB SSD en /, o. - 50 GiB disponible en /opt - 45 GiB disponible en /var/lib/docker - 5 GiB en /tmp

Tenga en cuenta que existen limitaciones cuando se utilizan sistemas más pequeños. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

- A la hora de poner en marcha una instancia de computación en la nube para la instalación de tu clasificación de BlueXP, te recomendamos un sistema que cumpla los requisitos «grandes» del sistema anteriores:
  - **Tipo de instancia de AWS EC2**: Recomendamos "m6i.4xlarge". "Consulte tipos de instancia de AWS adicionales".
  - **Azure VM size**: Recomendamos "Standard_D16s_v3". "Consulte tipos de instancia de Azure adicionales".
  - **Máquina GCP tipo**: Recomendamos "n2-standard-16". "Consulte tipos de instancia de GCP adicionales".
- **Permisos de carpeta UNIX**: Se requieren los siguientes permisos mínimos de UNIX:

Carpeta	Permisos mínimos
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`

Carpeta	Permisos mínimos
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **sistema operativo**:
  - Los siguientes sistemas operativos requieren el uso del motor de contenedor Docker:
    - Red Hat Enterprise Linux versiones 7,8 y 7,9
    - CentOS versión 7,8 y 7,9
    - Ubuntu 22,04 (requiere la versión de clasificación de BlueXP 1,23 o posterior)
  - Los siguientes sistemas operativos requieren el uso del motor de contenedor Podman y requieren la versión de clasificación de BlueXP 1,30 o posterior:
    - Red Hat Enterprise Linux versiones 8,8, 9,0, 9,1, 9,2 y 9,3

      Tenga en cuenta que las siguientes funciones no son compatibles actualmente con RHEL 8.x y RHEL 9.x:

      - Instalación en un sitio oscuro
      - Escaneo distribuido; utilizando un nodo de escáner maestro y nodos de escáner remoto
- **Red Hat Subscription Management**: El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de 3rd partes necesario durante la instalación.
- **Software adicional**: Debes instalar el siguiente software en el host antes de instalar la clasificación BlueXP:
  - Dependiendo del sistema operativo que esté utilizando, deberá instalar uno de los motores de contenedores:
    - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".

      "Vea este vídeo" Para obtener una demostración rápida de la instalación de Docker en CentOS.

    - Podman versión 4 o superior. Para instalar Podman, actualice los paquetes del sistema (`sudo yum update -y`) Y, a continuación, instale Podman (`sudo yum install netavark -y`).
- Python versión 3,6 o superior. "Ver las instrucciones de instalación".
  - **Consideraciones sobre NTP**: NetApp recomienda configurar el sistema de clasificación BlueXP para usar un servicio de Protocolo de hora de red (NTP). La hora debe sincronizarse entre el sistema de clasificación de BlueXP y el sistema BlueXP Connector.
  - * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Te recomendamos que lo habilites antes de instalar la clasificación de BlueXP. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con la clasificación de 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
```

Si tienes pensado usar hosts de clasificación de BlueXP adicionales como nodos de análisis, añade estas reglas a tu sistema principal en este 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
```

+
Tenga en cuenta que debe reiniciar Docker o Podman cada vez que habilite o actualice `firewalld` configuración.

> La dirección IP del sistema host de clasificación de BlueXP no se puede cambiar tras la instalación.

Habilita el acceso a Internet saliente desde la clasificación de BlueXP

La clasificación de BlueXP requiere acceso a Internet saliente. Si tu red física o virtual utiliza un servidor proxy para acceder a Internet, asegúrese de que la instancia de clasificación de BlueXP tenga acceso a Internet saliente para contactar con los siguientes extremos.

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
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/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.
https://github.com/docker https://download.docker.com	Proporciona paquetes de requisitos previos para la instalación de Docker.

Puntos finales	Específico
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Proporciona paquetes de requisitos previos para la instalación de CentOS.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Proporciona paquetes de requisitos previos para la instalación de Ubuntu.

Verifique que todos los puertos necesarios estén habilitados

Debes asegurarte de que todos los puertos requeridos estén abiertos para la comunicación entre el conector, la clasificación de BlueXP, Active Directory y los orígenes de datos.

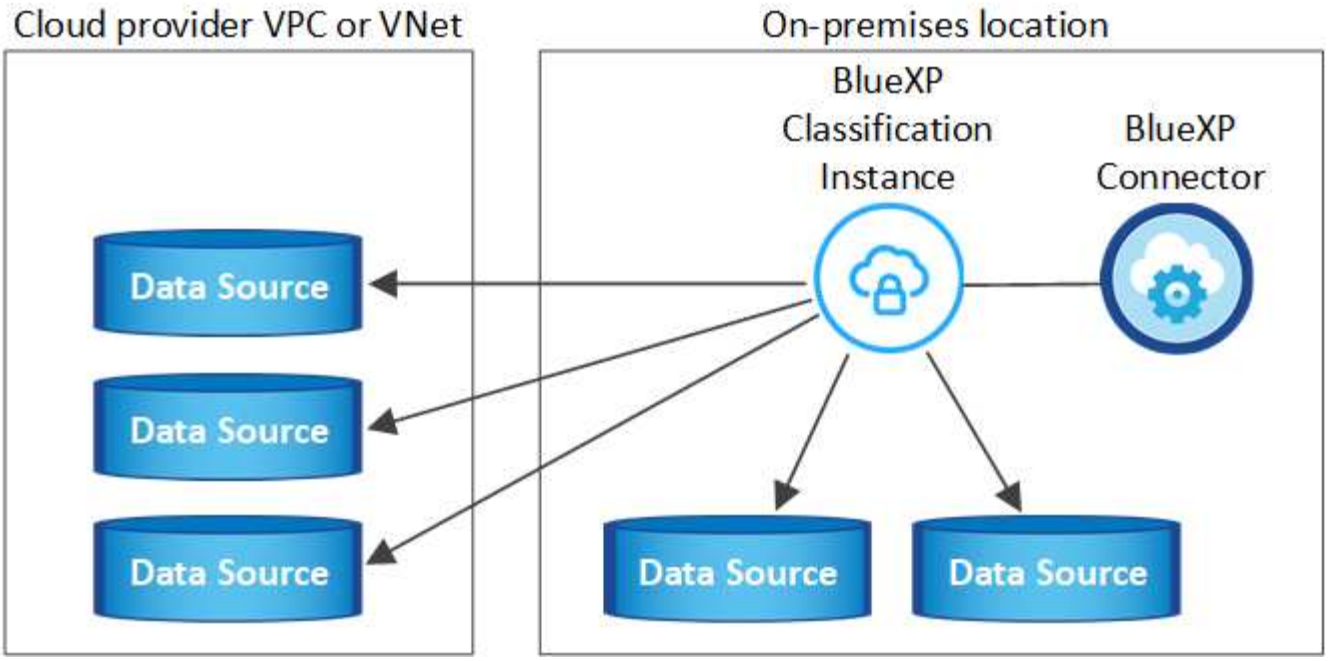
Tipo de conexión	Puertos	Descripción
Conector Clasificación de <> BlueXP	8080 (TCP), 443 (TCP) y 80	El firewall o las reglas de enrutamiento para Connector deben permitir el tráfico de entrada y salida a través del puerto 443 hacia y desde la instancia de clasificación de BlueXP. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, todas las comunicaciones salientes se permiten mediante el firewall predefinido o las reglas de enrutamiento. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.

Tipo de conexión	Puertos	Descripción
Clasificación de BlueXP <> Cluster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	La clasificación de BlueXP necesita una conexión de red con cada subred Cloud Volumes ONTAP o sistema ONTAP en las instalaciones. Los firewalls o las reglas de enrutamiento para Cloud Volumes ONTAP deben permitir las conexiones entrantes desde la instancia de clasificación de BlueXP. Asegúrate de que estos puertos estén abiertos a la instancia de clasificación de BlueXP: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de clasificación de BlueXP.
Clasificación de BlueXP <> Active Directory	389 (TCP Y UDP), 636 (TCP), 3268 (TCP) Y 3269 (TCP)	Debe tener un Active Directory ya configurado para los usuarios de su empresa. Además, la clasificación de BlueXP necesita credenciales de Active Directory para analizar los volúmenes de CIFS. Debe tener la información de Active Directory: • DNS Server IP Address o varias direcciones IP • Nombre de usuario y contraseña para el servidor • Nombre de dominio (nombre de Active Directory) • Si utiliza o no un LDAP seguro (LDAPS) • Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

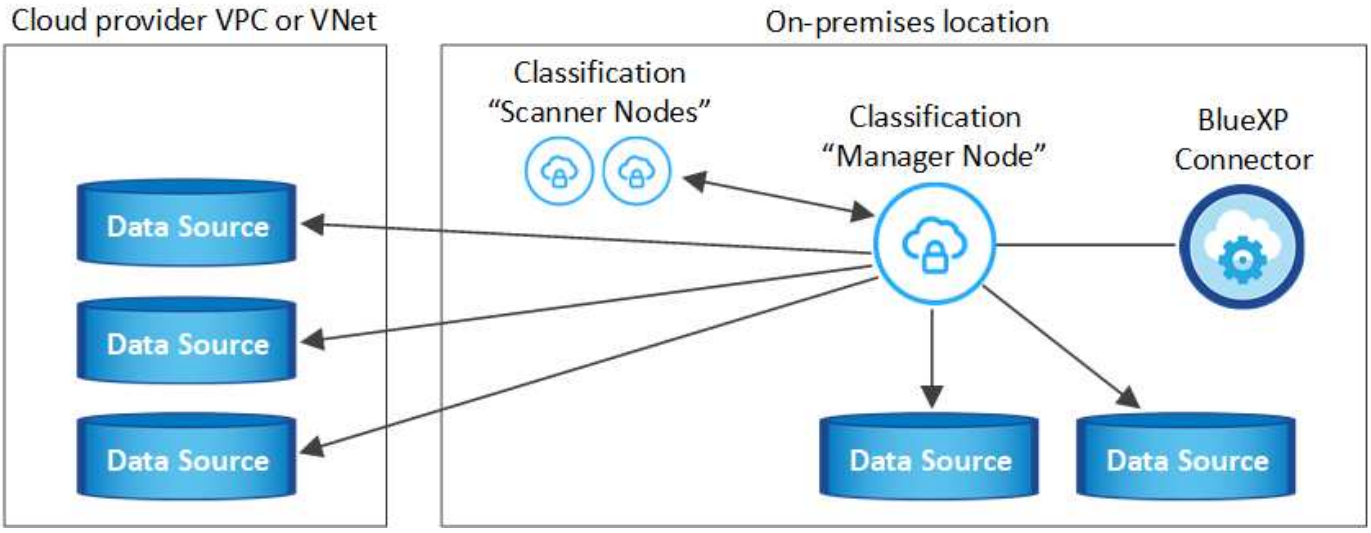
Si utilizas varios hosts de clasificación de BlueXP para obtener una capacidad de procesamiento adicional para analizar tus orígenes de datos, tendrás que habilitar puertos/protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Instale la clasificación BlueXP en el host Linux

En configuraciones típicas, instalará el software en un único sistema host. Consulte estos pasos aquí.



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Consulte estos pasos aquí.



Consulte Preparar el sistema host Linux y.. Revisión de requisitos previos Para consultar la lista completa de requisitos antes de poner en marcha la clasificación de BlueXP.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

> La clasificación de BlueXP no puede analizar los buckets de S3, Azure NetApp Files o FSx para ONTAP cuando el software está instalado en las instalaciones. En estos casos, tendrás que poner en marcha un Connector independiente y una instancia de la clasificación de BlueXP en la nube y en la nube "Cambiar entre conectores" para sus diferentes fuentes de datos.

Instalación de un solo host para configuraciones típicas

Revise los requisitos y siga estos pasos al instalar el software de clasificación de BlueXP en un único host local.

"Vea este vídeo" Para ver cómo instalar la clasificación de BlueXP.

Tenga en cuenta que todas las actividades de instalación se registran al instalar la clasificación de BlueXP. Si tiene algún problema durante la instalación, puede ver el contenido del registro de auditoría de la instalación. Está escrito en `/opt/netapp/install_logs/`. "Consulte más detalles aquí".

Lo que necesitará

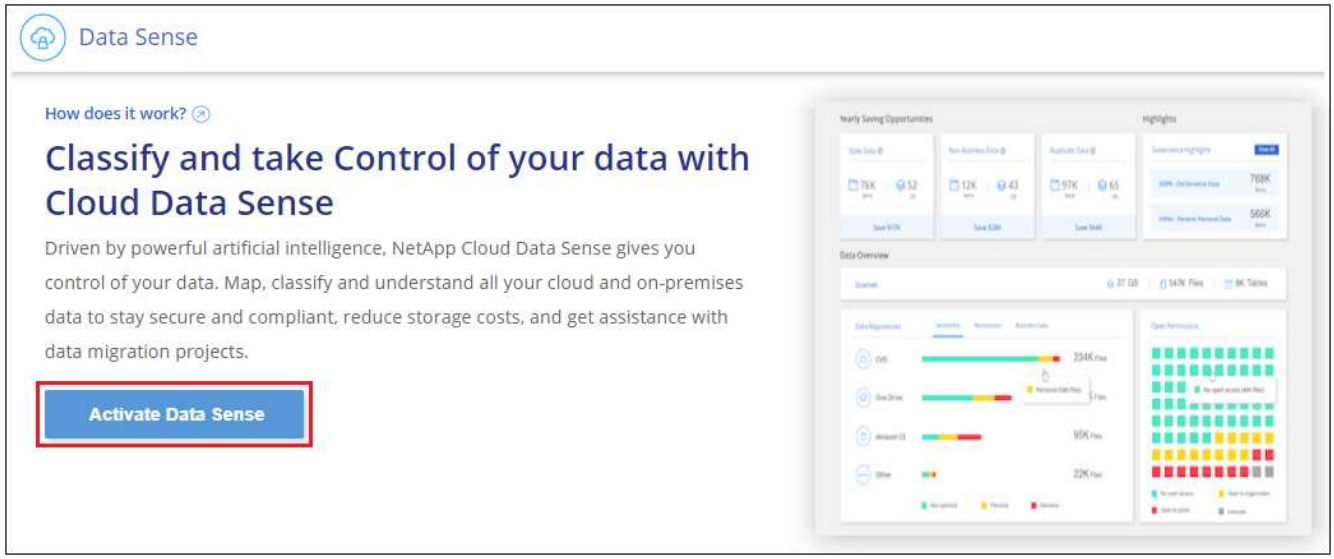
- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que el sistema tiene instalados los dos paquetes de software de requisitos previos (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.
- Si utiliza un proxy para acceder a Internet:
  - Necesitará la información del servidor proxy (dirección IP o nombre de host, puerto de conexión, esquema de conexión: https o http, nombre de usuario y contraseña).
  - Si el proxy ejecuta la intercepción TLS, deberá conocer la ruta en el sistema Linux de clasificación BlueXP donde se almacenan los certificados de CA TLS.
  - El proxy debe ser no transparente; actualmente no admitimos proxies transparentes.
  - El usuario debe ser un usuario local. Los usuarios de dominio no son compatibles.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

Pasos

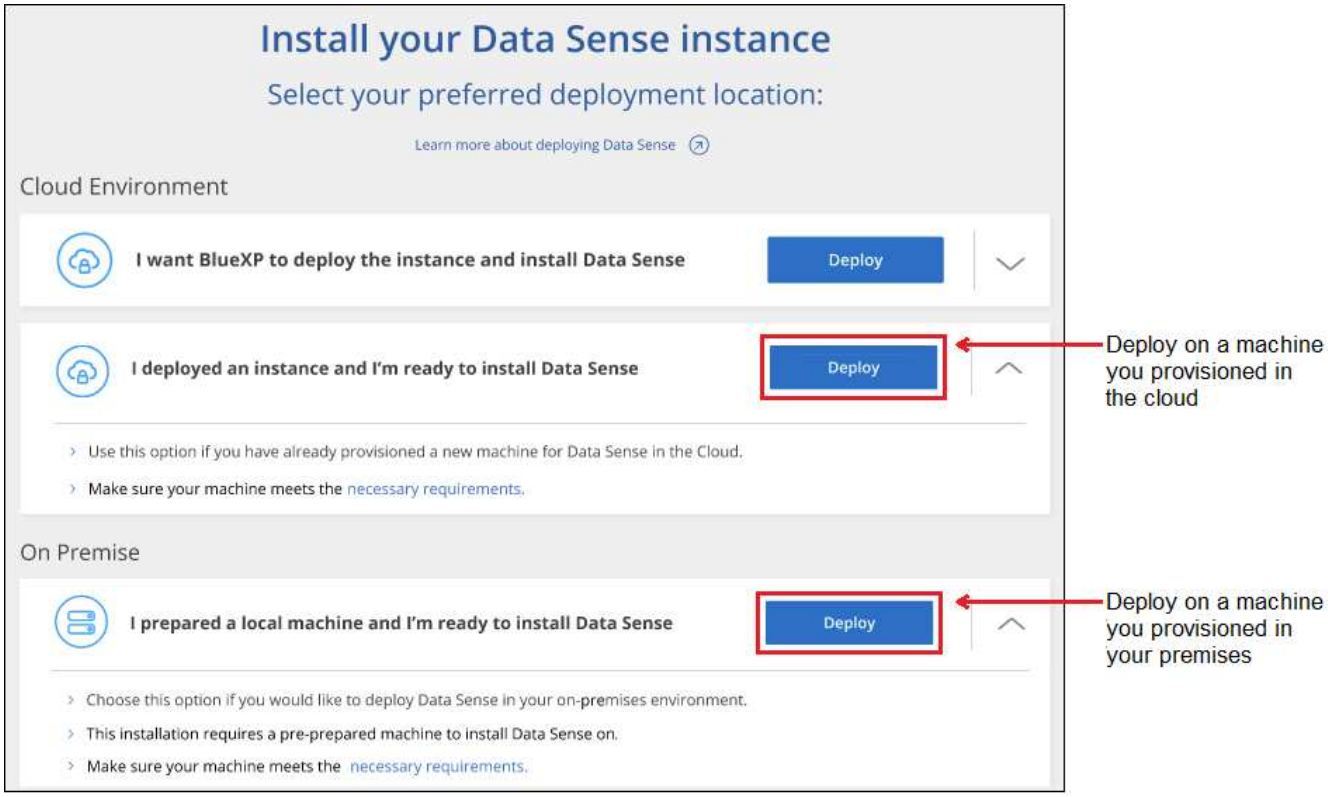
1. Descargue el software de clasificación de BlueXP en la "Sitio de soporte de NetApp". El archivo que debe seleccionar se denomina **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copie el archivo del instalador en el host Linux que tiene previsto utilizar (mediante `scp` o algún otro método).
3. Descomprima el archivo del instalador en el equipo host; por ejemplo:

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

4. En BlueXP, seleccione **Gobierno > Clasificación**.
5. Haga clic en **Activar detección de datos**.



6. En función de si vas a instalar la clasificación de BlueXP en una instancia que preparaste en la nube o en una instancia que preparaste en tus instalaciones, haz clic en el botón **Deploy** adecuado para iniciar la instalación de la clasificación de BlueXP.



7. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado (por ejemplo: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) y péguela en un archivo de texto para que pueda usarlo más tarde. A continuación, haga clic en **Cerrar** para descartar el cuadro de diálogo.
8. En el equipo host, escriba el comando que copió y luego siga una serie de avisos, o bien puede proporcionar el comando completo incluyendo todos los parámetros necesarios como argumentos de línea de comandos.

   Tenga en cuenta que el instalador realiza una comprobación previa para asegurarse de que el sistema y los requisitos de red están en su lugar para una instalación correcta. "Vea este vídeo" para comprender los

mensajes e implicaciones de comprobación previa.

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue el comando que copió del paso 7: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` Si está instalando en una instancia de cloud (no en sus instalaciones), agregue `--manual -cloud-install <cloud_provider>`. b. Introduzca la dirección IP o el nombre de host de la máquina host de clasificación de BlueXP para que se pueda acceder a ella desde el sistema Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host del conector de BlueXP para que el sistema de clasificación de BlueXP pueda acceder a ellos. d. Introduzca los detalles del proxy según se le solicite. Si tu BlueXP Connector ya utiliza un proxy, no es necesario volver a introducir esta información aquí, ya que la clasificación de BlueXP usará automáticamente el proxy que utilizará The Connector.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host y proxy necesarios: `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 de variable:

- *account_id* = ID de cuenta de NetApp
- *Client_id* = Identificador de cliente de conector (agregue el sufijo “clientes” al ID de cliente si aún no está allí)
- *USER_token* = token de acceso de usuario JWT
- *ds_host* = dirección IP o nombre de host del sistema Linux de clasificación de BlueXP.
- *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.
- *CLOUD_PROVEEDOR* = Cuando se instala en una instancia de nube, ingresa “AWS”, “Azure” o “GCP” dependiendo del proveedor de nube.
- *proxy_host* = IP o nombre de host del servidor proxy si el host está detrás de un servidor proxy.
- *proxy_Port* = Puerto para conectarse al servidor proxy (predeterminado 80).
- *Proxy_Scheme* = combinación de conexiones: https o http (valor predeterminado http).
- *proxy_USER* = Usuario autenticado para conectarse al servidor proxy, si se requiere autenticación básica. El usuario debe ser un usuario local: Los usuarios de dominio no son compatibles.
- *proxy_password* = Contraseña del nombre de usuario especificado.
- *Ca_cert_dir* = Ruta en el sistema Linux de clasificación BlueXP que contiene paquetes de certificados TLS CA adicionales. Sólo es necesario si el proxy está realizando intercepción TLS.

Resultado

El instalador de clasificación de BlueXP instala los paquetes, registra la instalación e instala la clasificación de BlueXP. La instalación puede tardar entre 10 y 20 minutos.

Si hay conectividad por el puerto 8080 entre el equipo host y la instancia de Connector, verás el progreso de la instalación en la pestaña de clasificación de BlueXP de BlueXP.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

También puede hacerlo "Configura las licencias para la clasificación de BlueXP" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

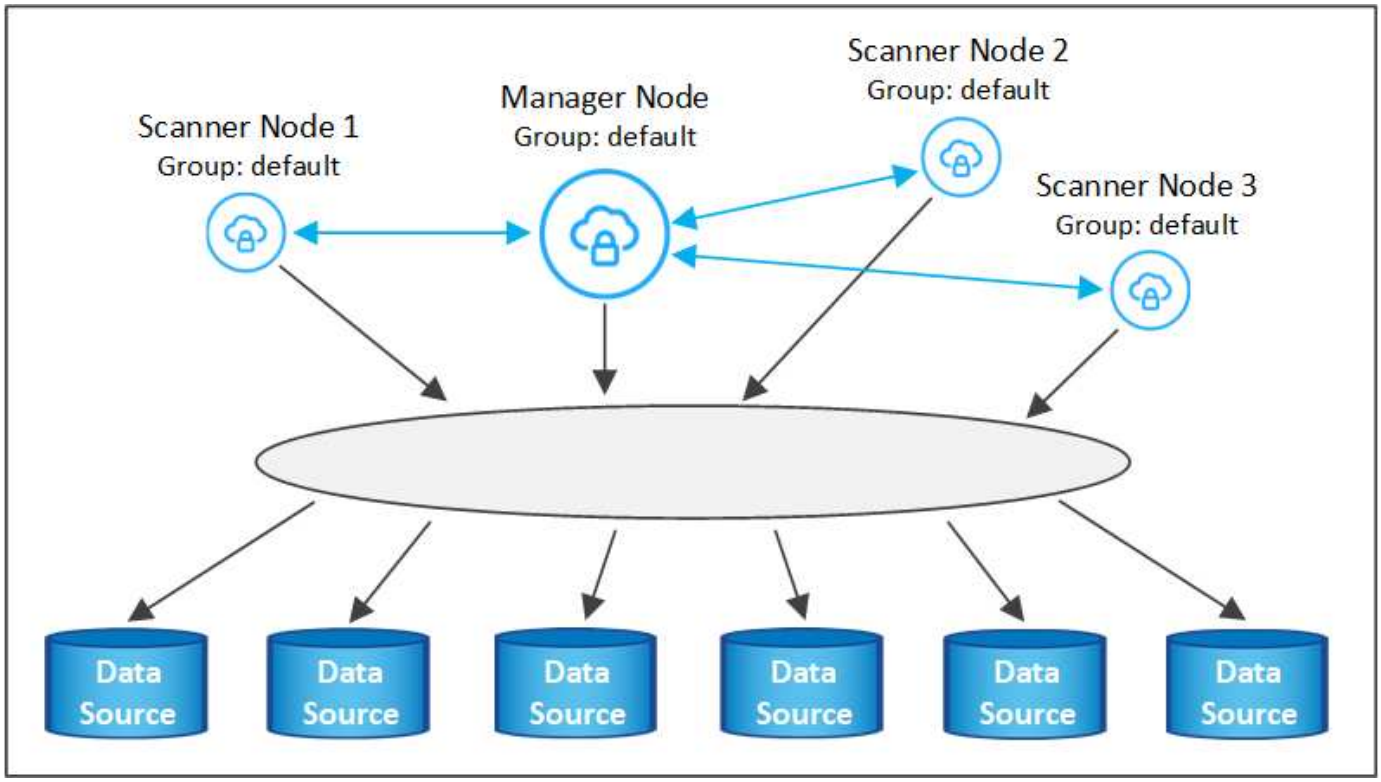
Agregar nodos de escáner a una implementación existente

Puede añadir más nodos de escáner si necesita más potencia de procesamiento de escaneado para analizar sus orígenes de datos. Puede añadir los nodos del escáner inmediatamente después de instalar el nodo Manager, o bien puede añadir un nodo de escáner más adelante. Por ejemplo, si se da cuenta de que la cantidad de datos de uno de sus orígenes de datos se ha duplicado o triplicado en tamaño después de 6 meses, puede añadir un nuevo nodo de escáner para ayudar con el análisis de datos.

Existen dos formas de añadir nodos de escáner adicionales:

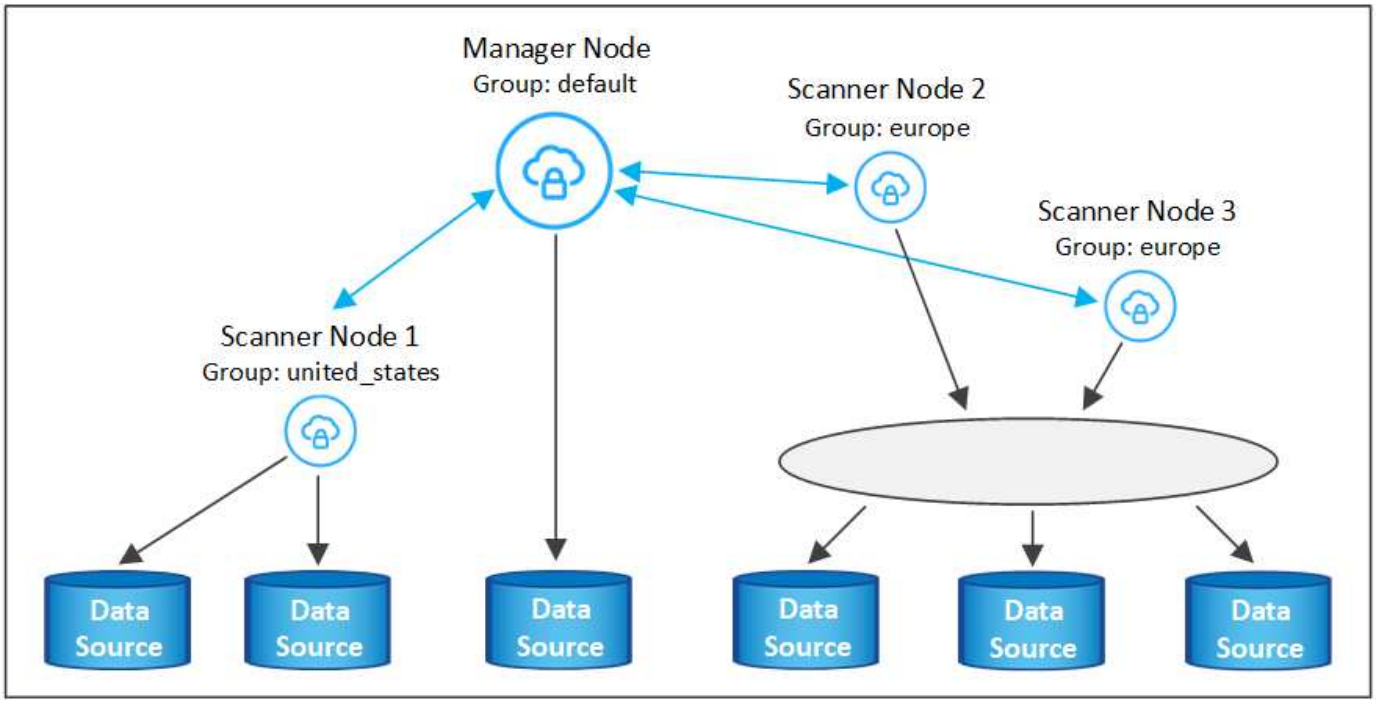
- agregue un nodo para ayudarle a analizar todos los orígenes de datos
- agregar un nodo para ayudarle a escanear un origen de datos específico o un grupo específico de orígenes de datos (normalmente basado en la ubicación)

De forma predeterminada, los nuevos nodos de escáner que agregue se agregarán al pool general de recursos de digitalización. Esto se denomina "grupo de escáner predeterminado". En la siguiente imagen, hay 1 nodo de administrador y 3 nodos de escáner en el grupo "predeterminado" que están analizando todos los datos de los 6 orígenes de datos.



Si tiene ciertos orígenes de datos que desea analizar mediante nodos de escáner que están físicamente más cercanos a los orígenes de datos, puede definir un nodo de escáner o un grupo de nodos de escáner, para analizar un origen de datos específico o un grupo de orígenes de datos. En la siguiente imagen, hay 1 nodo de administrador y 3 nodos de escáner.

- El nodo Administrador está en el grupo "predeterminado" y está analizando 1 origen de datos
- El nodo 1 del escáner se encuentra en el grupo "estados Unidos" y está analizando 2 orígenes de datos
- Los nodos de escáner 2 y 3 se encuentran en el grupo "europa" y comparten las tareas de escaneo para 3 fuentes de datos



Los grupos de análisis de clasificación de BlueXP pueden definirse como áreas geográficas independientes en las que se almacenan los datos. Puedes poner en marcha varios nodos de escáner de clasificación de BlueXP en todo el mundo y elegir un grupo de escáner para cada nodo. De esta forma, cada nodo de escáner analizará los datos más cercanos. Cuanto más cerca esté el nodo del escáner de los datos, mejor será porque reduce la latencia de red tanto como sea posible mientras escanea datos.

Puedes elegir qué grupos de escáneres añadir a la clasificación de BlueXP y puedes elegir sus nombres. La clasificación de BlueXP no obliga a que se ponga en marcha en Europa un nodo asignado a un grupo de escáner llamado «europa».

Seguirás estos pasos para instalar nodos adicionales de escáner de clasificación de BlueXP:

1. Prepare los sistemas host Linux que actuarán como nodos del escáner
2. Descargue el software Data Sense en estos sistemas Linux
3. Ejecute un comando en el nodo Administrador para identificar los nodos del escáner
4. Siga los pasos para implementar el software en los nodos del escáner (y para definir opcionalmente un "grupo de escáner" para determinados nodos del escáner)
5. Si ha definido un grupo de escáner, en el nodo Administrador:
    a. Abra el archivo "working_Environment_to_scanner_group_config.yml" y defina los entornos de trabajo que explorarán cada grupo de escáneres

b. Ejecute la siguiente secuencia de comandos para registrar esta información de asignación en todos los nodos del escáner: `update_we_scanner_group_from_config_file.sh`

Lo que necesitará

- Compruebe que todos los sistemas Linux para los nodos del escáner cumplen con el requisitos del host.
- Compruebe que los sistemas tienen instalados los dos paquetes de software de requisitos previos (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts del nodo Scanner que desea añadir.
- Debe tener la dirección IP del sistema host del nodo del gestor de clasificación de BlueXP
- Debe tener la dirección IP o el nombre de host del sistema Connector, su ID de cuenta de NetApp, su identificador de cliente conector y el token de acceso de usuario. Si tiene previsto utilizar grupos de escáner, deberá conocer el identificador de entorno de trabajo de cada origen de datos de su cuenta. Consulte los pasos ***Prerrequisito*** siguientes para obtener esta información.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

- Si está utilizando `firewalld` En tus máquinas de clasificación de BlueXP, te recomendamos habilitarla antes de instalar la clasificación de BlueXP. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con la clasificación de 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 --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
firewall-cmd --reload
```

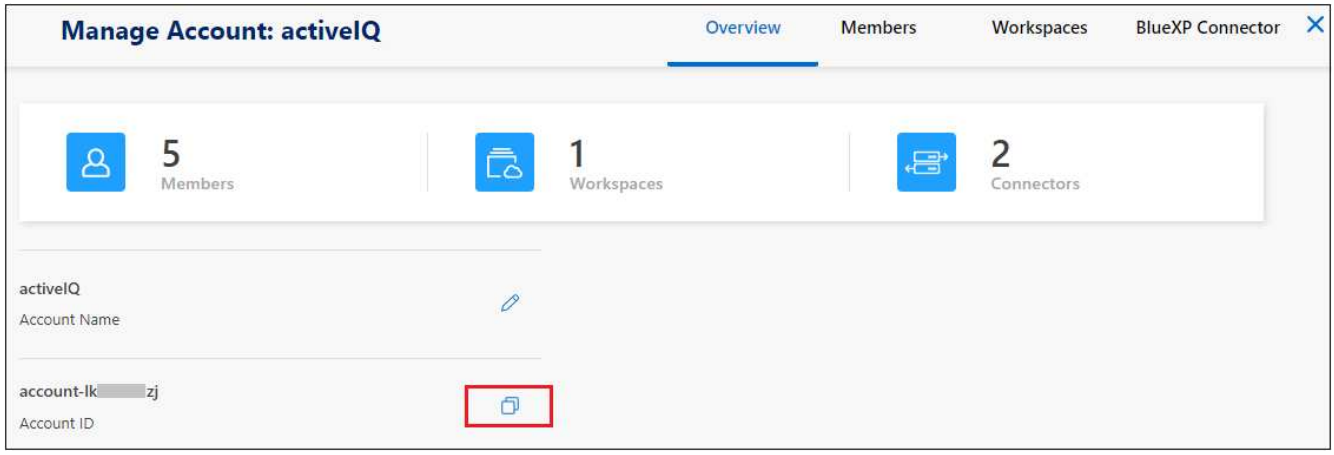
Tenga en cuenta que debe reiniciar Docker o Podman cada vez que habilite o actualice `firewalld`

configuración.

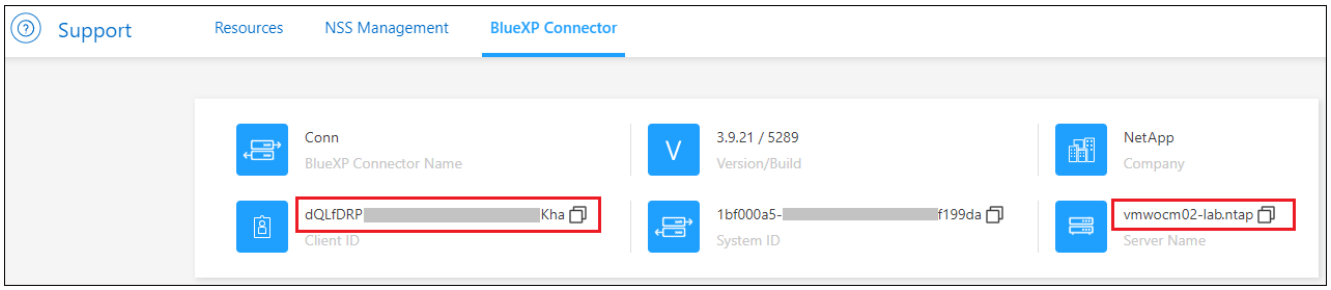
Requisitos previos

Siga estos pasos para obtener el identificador de cuenta de NetApp, el identificador de cliente del conector, el nombre de servidor del conector y el token de acceso de usuario necesarios para añadir nodos de escáner.

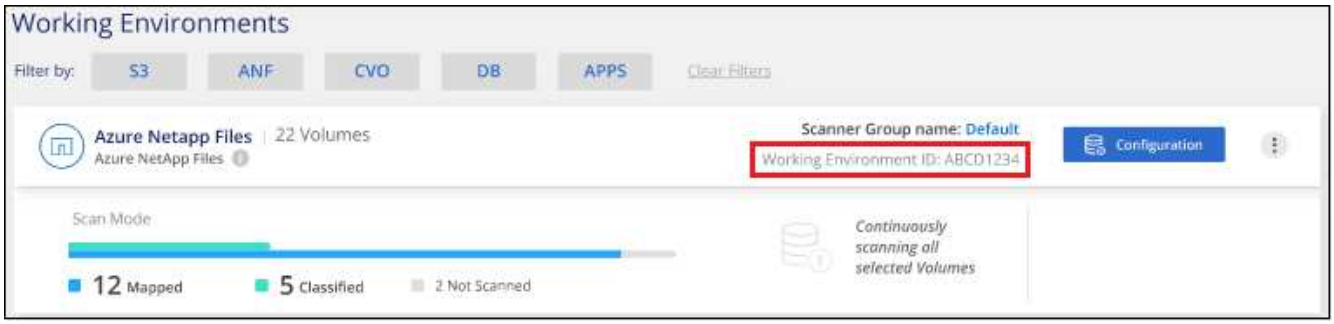
1. En la barra de menús de BlueXP, haga clic en **cuenta > Administrar cuentas**.



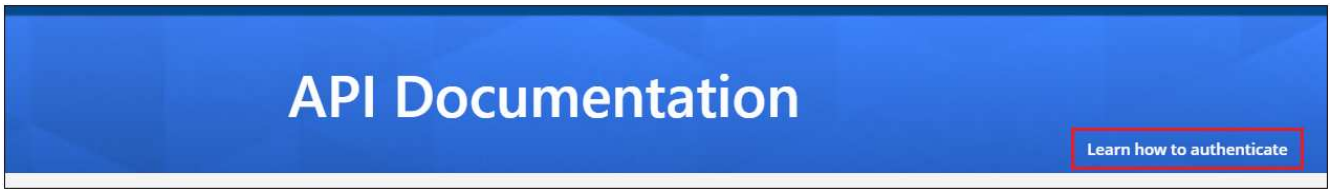
2. Copie el *ID de cuenta*.
3. En la barra de menús de BlueXP, haga clic en **Ayuda > Soporte > conector BlueXP**.



4. Copie el conector *Client ID* y el *Server Name*.
5. Si tienes pensado usar grupos de escáner, en la pestaña Configuración de clasificación de BlueXP, copia el ID de entorno de trabajo de cada entorno de trabajo que quieras añadir a un grupo de escáner.



6. Vaya a la "Centro de desarrollo de documentación de API" Y haga clic en **aprender a autenticar**.



7. Siga las instrucciones de autenticación, usando el nombre de usuario y la contraseña del administrador de la cuenta en los parámetros «nombre de usuario» y «contraseña».
8. A continuación, copie el token *ACCESS* de la respuesta.

Pasos

1. En el nodo del gestor de clasificación de BlueXP, ejecute el script «add_scanner_node.sh». Por ejemplo, este comando añade 2 nodos de escáner:

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Client_id* = Identificador de cliente de conector (agregue el sufijo «Clientes» al ID de cliente que copió en los pasos de requisito previo)
   - *Cm_host* = dirección IP o nombre de host del sistema conector
   - *ds_manager_ip* = Dirección IP privada del sistema de nodos del Gestor de clasificación de BlueXP
   - *Node_private_ip* = direcciones IP de los sistemas de nodos del escáner de clasificación de BlueXP (varias IP de los nodos del escáner están separadas con comas)
   - *USER_token* = token de acceso de usuario JWT
2. Antes de que finalice la secuencia de comandos add_scanner_node, aparecerá un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando (por ejemplo: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) y guárdelo en un archivo de texto.
3. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 2.
   d. Si desea agregar un nodo de escáner a un "grupo de escáner", agregue el parámetro **-r <scanner_group_name>** al comando. De lo contrario, el nodo del escáner se agrega al grupo "predeterminado".

      Cuando la instalación termina en todos los nodos del escáner y se han Unido al nodo del administrador, el script "add_scanner_node.sh" también finaliza. La instalación puede tardar entre 10 y 20 minutos.
4. Si ha agregado algún nodo de escáner a un grupo de escáner, vuelva al nodo Administrador y realice las dos tareas siguientes:
   a. Abra el archivo «/opt/netapp/config/custom_configuration/working_environment_to_scanner_group_config.yml» e

introduzca la asignación para la que los grupos de escáneres explorarán entornos de trabajo específicos. Deberá tener el *ID de entorno de trabajo* para cada origen de datos. Por ejemplo, las siguientes entradas agregan 2 entornos de trabajo al grupo de escáneres "europa" y 2 al grupo de escáneres "estados Unidos":

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

El grupo "predeterminado" analiza cualquier entorno de trabajo que no se agregue a la lista; debe tener al menos un nodo de administrador o escáner en el grupo "predeterminado".

b. Ejecute la siguiente secuencia de comandos para registrar esta información de asignación en todos los nodos del escáner: `/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

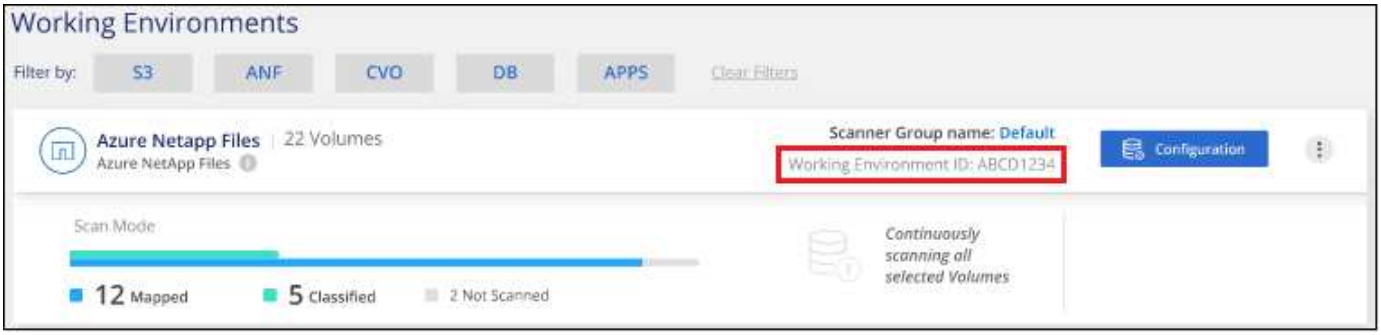
Resultado

La clasificación de BlueXP se configura con nodos Manager y Scanner para analizar todas tus fuentes de datos.

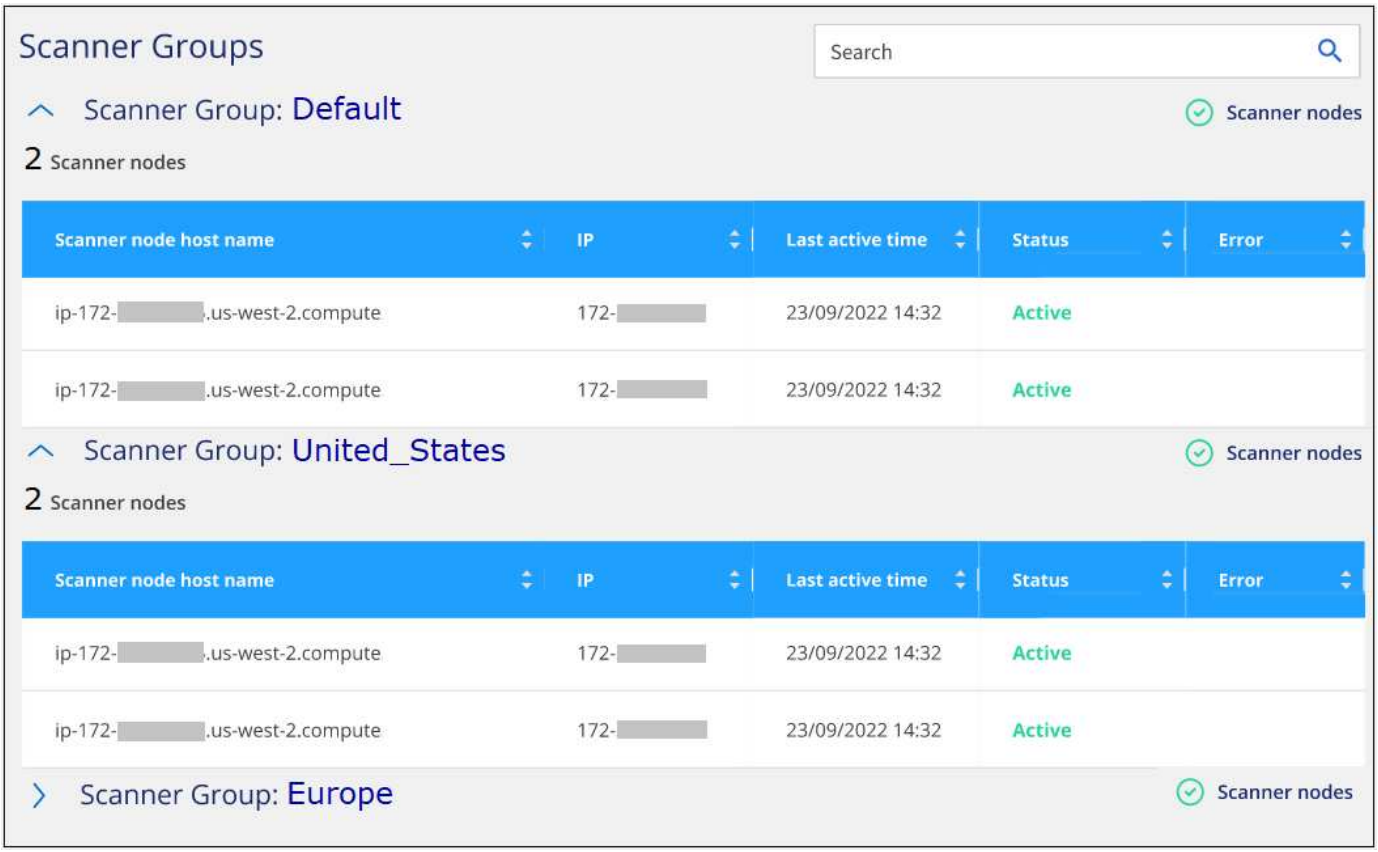
El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar, si aún no lo ha hecho. Si ha creado grupos de escáner, los nodos de escáner del grupo correspondiente escanean cada origen de datos.

Puede ver el nombre del grupo de escáneres de cada entorno de trabajo en la página Configuración.



También puede ver la lista de todos los grupos de escáneres junto con la dirección IP y el estado de cada nodo de escáner del grupo en la parte inferior de la página Configuración.



Puede hacerlo "Configura las licencias para la clasificación de BlueXP" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instalación de varios hosts para configuraciones grandes

En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Sigue estos pasos cuando instales el software de clasificación BlueXP en varios hosts on-premises a la vez. Tenga en cuenta que no puede utilizar "grupos de escáneres" al implementar varios hosts de esta forma.

Lo que necesitará

- Verifique que todos los sistemas Linux para los nodos Manager y Scanner se adapten al requisitos del host.
- Compruebe que los sistemas tienen instalados los dos paquetes de software de requisitos previos (Docker o Podman Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts de nodos de escáner que desee utilizar.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres

Puerto	Protocolos	Descripción
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

Pasos

1. Siga los pasos 1 a 7 de la Instalación de un solo host en el nodo de gestión.
2. Como se muestra en el paso 8, cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de peticiones o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

   Además de las variables disponibles para una instalación de un solo host, se utiliza una nueva opción **-n <node_ip>** para especificar las direcciones IP de los nodos del escáner. Las varias IP de nodos de escáner están separadas por una coma.

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   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> --proxy
   -host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
   --proxy-user <proxy_user> --proxy-password <proxy_password>
   ```
3. Antes de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copiar el comando (por ejemplo, `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) y guárdelo en un archivo de texto.
4. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 3.

      Cuando la instalación finalice en todos los nodos de escáner y se han Unido al nodo de gestión, también se completa la instalación del nodo de gestión.

Resultado

El instalador de clasificación de BlueXP finalizará la instalación de paquetes y registrará la instalación. La instalación puede tardar entre 10 y 20 minutos.

El futuro

En la página Configuración puede seleccionar los orígenes de datos que desea analizar.

También puede hacerlo "Configura las licencias para la clasificación de BlueXP" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instala la clasificación BlueXP en un host Linux sin acceso a Internet

Completa unos pocos pasos para instalar la clasificación de BlueXP en un host Linux en un sitio local que no tenga acceso a Internet, también conocido como *modo privado*. Este tipo de instalación es perfecta para sus sitios seguros.

"Obtén más información sobre los distintos modos de puesta en marcha para el conector de BlueXP y la clasificación de BlueXP".

Tenga en cuenta que también puede "Pon en marcha la clasificación de BlueXP en un sitio local que tenga acceso a Internet".

El script de instalación de clasificación de BlueXP comienza comprobando si el sistema y el entorno cumplen los requisitos previos necesarios. Si se cumplen todos los requisitos previos, se inicia la instalación. Si desea verificar los requisitos previos independientemente de la ejecución de la instalación de la clasificación de BlueXP, puede descargar un paquete de software independiente que solo prueba los requisitos previos. "Descubre cómo comprobar si tu host Linux está listo para instalar la clasificación de BlueXP".

Orígenes de datos compatibles

Cuando se instala en modo privado (a veces llamado sitio «sin conexión» u «oscuro»), la clasificación de BlueXP solo puede analizar los datos de orígenes de datos locales en el sitio local. En este momento, la clasificación de BlueXP puede escanear las siguientes fuentes de datos **locales**:

- Sistemas ONTAP en las instalaciones
- Esquemas de base de datos
- Cuentas locales de SharePoint (SharePoint Server)
- Recursos compartidos de archivos NFS o CIFS de terceros
- Almacenamiento de objetos que utiliza el protocolo simple Storage Service (S3)

Actualmente no hay soporte para escanear Cloud Volumes ONTAP, Azure NetApp Files, FSx para ONTAP, AWS S3 o Google Drive, OneDrive o cuentas de SharePoint Online cuando la clasificación de BlueXP está puesta en marcha en modo privado.

Limitaciones

La mayoría de las funciones de clasificación de BlueXP funcionan cuando se implementa en un sitio sin acceso a Internet. Sin embargo, algunas funciones que requieren acceso a Internet no son compatibles, por ejemplo:

- Administración de etiquetas de Microsoft Azure Information Protection (AIP)
- Envío de alertas por correo electrónico a usuarios de BlueXP cuando determinadas políticas críticas devuelven resultados
- Configuración de funciones de BlueXP para usuarios diferentes (por ejemplo, Administrador de cuentas o Visor de cumplimiento)
- Copiar y sincronizar archivos de origen mediante la copia y sincronización de BlueXP
- Recibiendo comentarios de usuarios
- Actualizaciones de software automatizadas desde BlueXP

  Tanto el conector de BlueXP como la clasificación de BlueXP requerirán actualizaciones manuales

periódicas para permitir nuevas funciones. Puedes ver la versión de clasificación de BlueXP en la parte inferior de las páginas de interfaz de usuario de clasificación de BlueXP. Compruebe la "Notas de la versión de clasificación de BlueXP" para ver las nuevas funciones de cada versión y si desea esas funciones. A continuación, puede seguir los pasos a. "Actualice el conector BlueXP" y.. Actualiza tu software de clasificación BlueXP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Instale el conector BlueXP

Si aún no tiene un conector instalado en modo privado, "Despliegue el conector" Ahora en un host Linux.

2 Revisa los requisitos previos de clasificación de BlueXP

Compruebe que su sistema Linux cumple con el requisitos del host, que tiene todo el software necesario instalado y que su entorno sin conexión cumple con el necesario permisos y conectividad.

3 Descarga e implementa la clasificación de BlueXP

Descarga el software de clasificación de BlueXP desde el sitio de soporte de NetApp y copia el archivo del instalador en el host Linux que tengas que utilizar. A continuación, inicie el asistente de instalación y siga las indicaciones para implementar la instancia de clasificación de BlueXP.

4 Suscríbete al servicio de clasificación de BlueXP

Los primeros 1 TB de datos que analiza la clasificación de BlueXP en BlueXP son gratuitos durante 30 días. Se requiere una licencia BYOL de NetApp para continuar con el análisis de los datos después de ese punto.

Instale el conector BlueXP

Si aún no tienes un conector BlueXP instalado en modo privado, "Despliegue el conector" En un host Linux del sitio sin conexión.

Prepare el sistema host Linux

El software de clasificación de BlueXP debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, los requisitos de RAM, los requisitos de software, etc.

- La clasificación de BlueXP no se admite en un host compartido con otras aplicaciones; el host debe ser un host dedicado.
- Al crear el sistema host en tus instalaciones, puedes elegir entre tres tamaños de sistema en función del tamaño del conjunto de datos que tengas pensado analizar la clasificación de BlueXP.

Tamaño del sistema	CPU	RAM (la memoria de intercambio debe estar desactivada)	Disco
* Extra grande*	32 CPU	128 GB DE MEMORIA RAM	1 TiB SSD en /, o. - 100 GiB disponible en /opt - 895 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Grande	16 CPU	64 GB DE MEMORIA RAM	500 GiB SSD en /, o. - 100 GiB disponible en /opt - 395 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Media	8 CPU	32 GB DE MEMORIA RAM	200 GiB SSD en /, o. - 50 GiB disponible en /opt - 145 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Pequeño	8 CPU	16 GB DE MEMORIA RAM	100 GiB SSD en /, o. - 50 GiB disponible en /opt - 45 GiB disponible en /var/lib/docker - 5 GiB en /tmp

Tenga en cuenta que existen limitaciones cuando se utilizan sistemas más pequeños. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

- A la hora de poner en marcha una instancia de computación en la nube para la instalación de tu clasificación de BlueXP, te recomendamos un sistema que cumpla los requisitos «grandes» del sistema anteriores:
  - **Tipo de instancia de AWS EC2**: Recomendamos "m6i.4xlarge". "Consulte tipos de instancia de AWS adicionales".
  - **Azure VM size**: Recomendamos "Standard_D16s_v3". "Consulte tipos de instancia de Azure adicionales".
  - **Máquina GCP tipo**: Recomendamos "n2-standard-16". "Consulte tipos de instancia de GCP adicionales".
- **Permisos de carpeta UNIX**: Se requieren los siguientes permisos mínimos de UNIX:

Carpeta	Permisos mínimos
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **sistema operativo**:
  - Los siguientes sistemas operativos requieren el uso del motor de contenedor Docker:

        - Red Hat Enterprise Linux versiones 7,8 y 7,9
        - CentOS versión 7,8 y 7,9
        - Ubuntu 22,04 (requiere la versión de clasificación de BlueXP 1,23 o posterior)
    - Los siguientes sistemas operativos requieren el uso del motor de contenedor Podman y requieren la versión de clasificación de BlueXP 1,30 o posterior:
        - Red Hat Enterprise Linux versiones 8,8, 9,0, 9,1, 9,2 y 9,3

          Tenga en cuenta que las siguientes funciones no son compatibles actualmente con RHEL 8.x y RHEL 9.x:

            - Instalación en un sitio oscuro
            - Escaneo distribuido; utilizando un nodo de escáner maestro y nodos de escáner remoto
- **Red Hat Subscription Management**: El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de 3rd partes necesario durante la instalación.
- **Software adicional**: Debes instalar el siguiente software en el host antes de instalar la clasificación BlueXP:
    - Dependiendo del sistema operativo que esté utilizando, deberá instalar uno de los motores de contenedores:
        - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".

          "Vea este vídeo" Para obtener una demostración rápida de la instalación de Docker en CentOS.

        - Podman versión 4 o superior. Para instalar Podman, actualice los paquetes del sistema (`sudo yum update -y`) Y, a continuación, instale Podman (`sudo yum install netavark -y`).
- Python versión 3,6 o superior. "Ver las instrucciones de instalación".
    - **Consideraciones sobre NTP**: NetApp recomienda configurar el sistema de clasificación BlueXP para usar un servicio de Protocolo de hora de red (NTP). La hora debe sincronizarse entre el sistema de clasificación de BlueXP y el sistema BlueXP Connector.
    - * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Te recomendamos que lo habilites antes de instalar la clasificación de BlueXP. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con la clasificación de 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
      ```

      Tenga en cuenta que debe reiniciar Docker o Podman cada vez que habilite o actualice `firewalld` configuración.

> La dirección IP del sistema host de clasificación de BlueXP no se puede cambiar tras la instalación.

Comprueba los requisitos previos de clasificación de BlueXP y BlueXP

Revise los siguientes requisitos previos para asegurarse de que tiene una configuración compatible antes de implementar la clasificación de BlueXP.

- Compruebe que Connector tenga permisos para implementar recursos y crear grupos de seguridad para la instancia de clasificación de BlueXP. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".
- Asegúrate de que puedes mantener en funcionamiento la clasificación de BlueXP. La instancia de clasificación de BlueXP tiene que permanecer en la para analizar tus datos de forma continua.
- Garantice la conectividad del explorador web con la clasificación de BlueXP. Después de habilitar la clasificación de BlueXP, asegúrese de que los usuarios accedan a la interfaz de BlueXP desde un host que tiene una conexión a la instancia de clasificación de BlueXP.

  La instancia de clasificación de BlueXP usa una dirección IP privada para garantizar que los datos indexados no sean accesibles para nadie más. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esa conexión puede proceder de un host que está dentro de la misma red que la instancia de clasificación de BlueXP.

Verifique que todos los puertos necesarios estén habilitados

Debes asegurarte de que todos los puertos requeridos estén abiertos para la comunicación entre el conector, la clasificación de BlueXP, Active Directory y los orígenes de datos.

Tipo de conexión	Puertos	Descripción
Conector Clasificación de <> BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) Y 80	El grupo de seguridad del Connector debe permitir el tráfico de entrada y salida a través de los puertos 6000 y 443 hacia y desde la instancia de clasificación de BlueXP. • Se requiere el puerto 6000 para que la licencia BYOL de clasificación de BlueXP funcione en un sitio oscuro. • El puerto 8080 debería estar abierto para que puedas ver el progreso de la instalación en BlueXP.

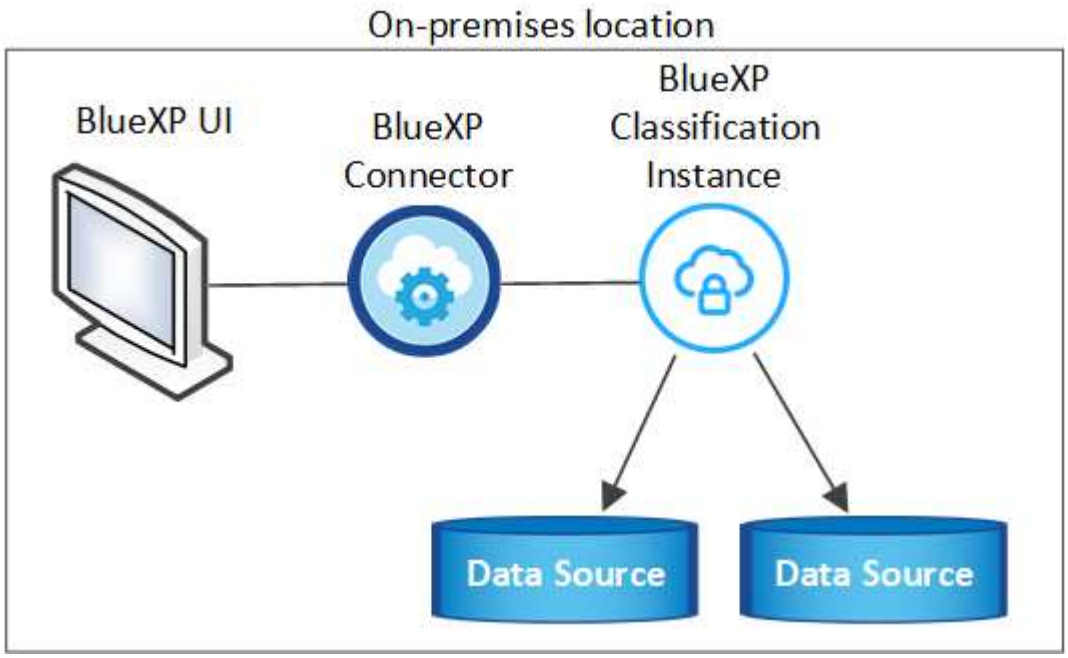
Tipo de conexión	Puertos	Descripción
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, el grupo de seguridad predefinido permite todas las comunicaciones salientes. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.
Clasificación de BlueXP <> Cluster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	La clasificación de BlueXP necesita una conexión de red con cada subred Cloud Volumes ONTAP o sistema ONTAP en las instalaciones. Los grupos de seguridad de Cloud Volumes ONTAP deben permitir las conexiones entrantes desde la instancia de clasificación de BlueXP. Asegúrate de que estos puertos estén abiertos a la instancia de clasificación de BlueXP: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de clasificación de BlueXP.

Tipo de conexión	Puertos	Descripción
Clasificación de BlueXP <> Active Directory	389 (TCP Y UDP), 636 (TCP), 3268 (TCP) Y 3269 (TCP)	Debe tener un Active Directory ya configurado para los usuarios de su empresa. Además, la clasificación de BlueXP necesita credenciales de Active Directory para analizar los volúmenes de CIFS. Debe tener la información de Active Directory: • DNS Server IP Address o varias direcciones IP • Nombre de usuario y contraseña para el servidor • Nombre de dominio (nombre de Active Directory) • Si utiliza o no un LDAP seguro (LDAPS) • Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

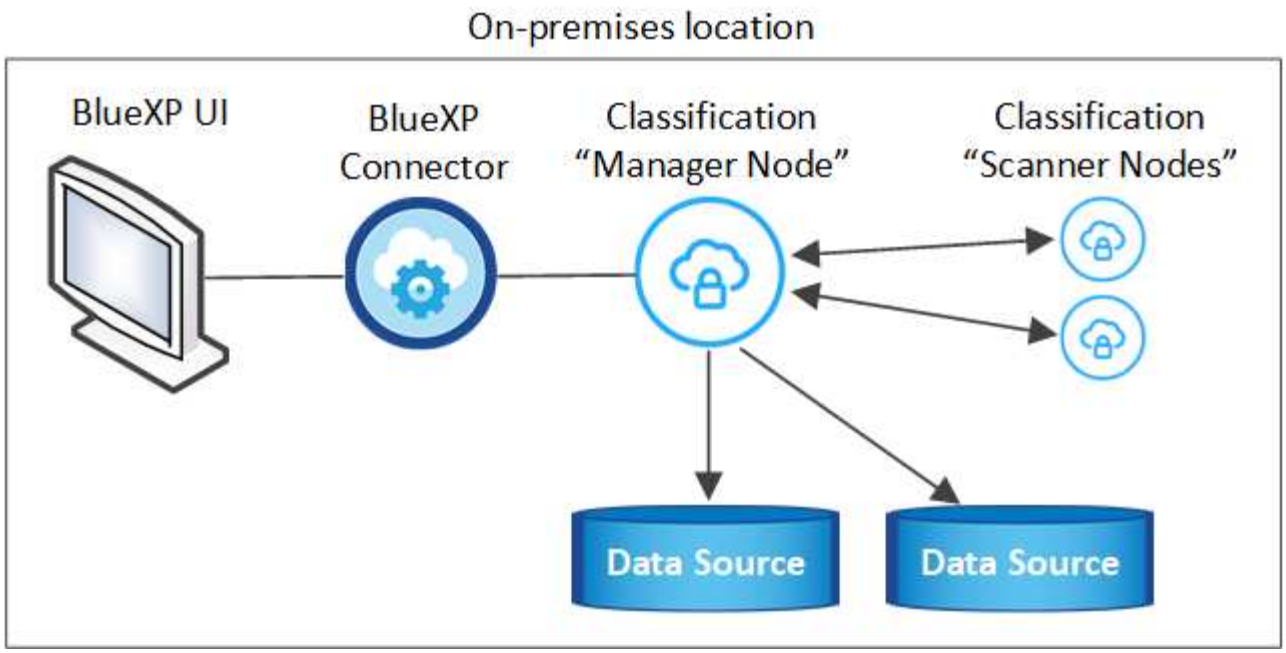
Si utilizas varios hosts de clasificación de BlueXP para obtener una capacidad de procesamiento adicional para analizar tus orígenes de datos, tendrás que habilitar puertos/protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Instale la clasificación BlueXP en el host Linux local

En configuraciones típicas, instalará el software en un único sistema host. "Consulte estos pasos aquí".



En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. "Consulte estos pasos aquí".



Instalación de un solo host para configuraciones típicas

Siga estos pasos al instalar el software de clasificación de BlueXP en un único host local en un entorno sin conexión.

Tenga en cuenta que todas las actividades de instalación se registran al instalar la clasificación de BlueXP. Si tiene algún problema durante la instalación, puede ver el contenido del registro de auditoría de la instalación. Está escrito en `/opt/netapp/install_logs/`. "Consulte más detalles aquí".

Lo que necesitará

- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

Pasos

1. En un sistema configurado por Internet, descargue el software de clasificación de BlueXP en la "Sitio de soporte de NetApp". El archivo que debe seleccionar se llama **DataSense-offline-Bundle-<version>.tar.gz**.
2. Copie el paquete del instalador en el host Linux que desee utilizar en modo privado.
3. Descomprima el paquete del instalador en el equipo host; por ejemplo:

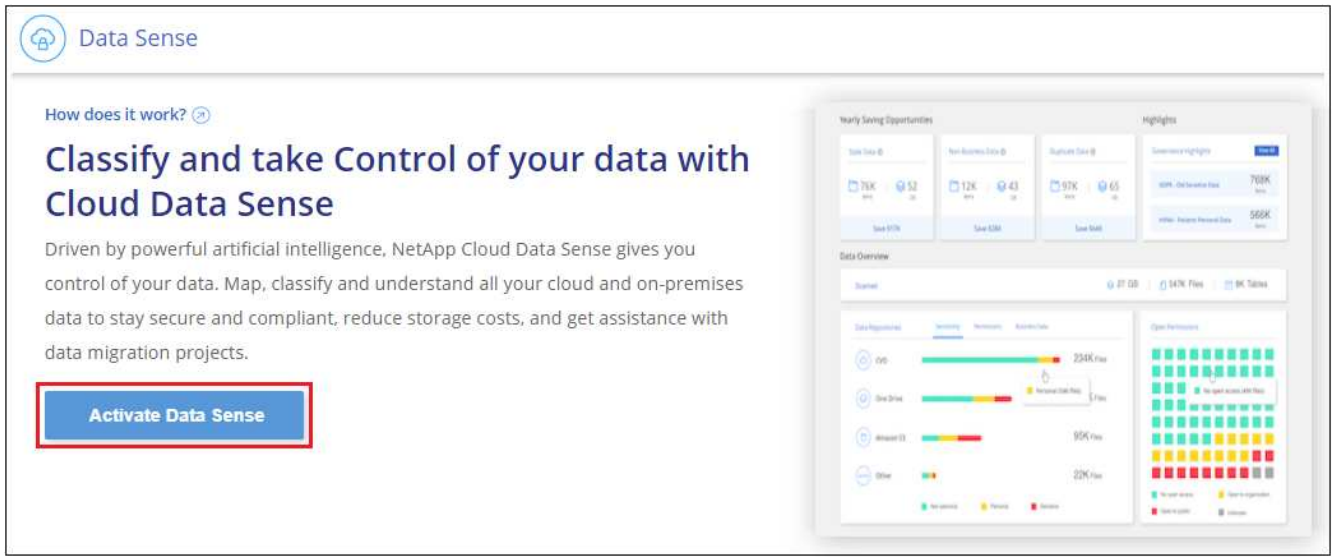
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   Esto extrae el software requerido y el archivo de instalación actual **cc_onprem_installer.tar.gz**.

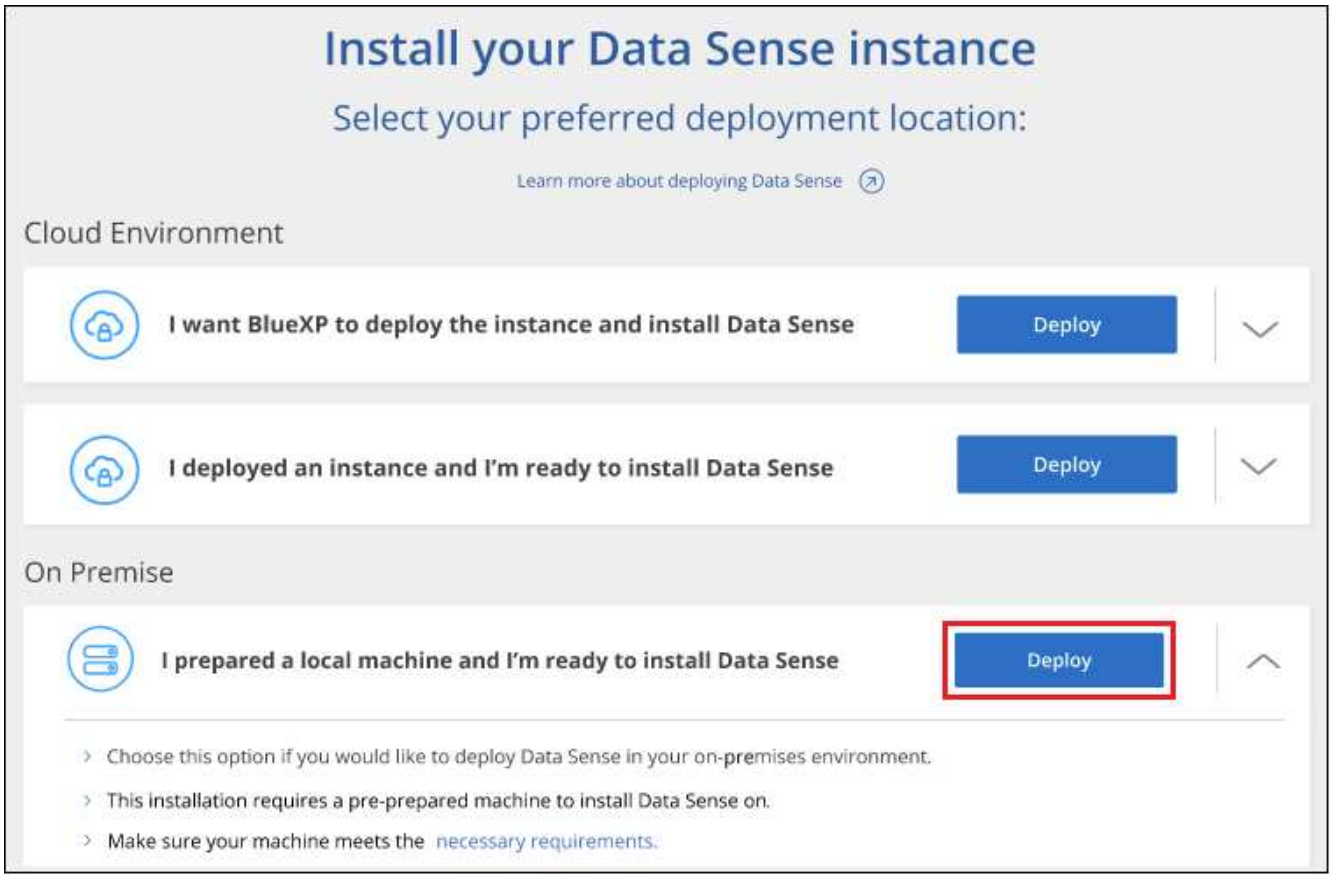
4. Descomprima el archivo de instalación en el equipo host; por ejemplo:

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

5. Inicie BlueXP y seleccione **Gobierno > Clasificación**.
6. Haga clic en **Activar detección de datos**.



7. Haga clic en **desplegar** para iniciar la instalación en las instalaciones.



8. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado (por ejemplo:

`sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) y péguela en un archivo de texto para que pueda usarlo más tarde. A continuación, haga clic en **Cerrar** para descartar el cuadro de diálogo.

9. En el equipo host, escriba el comando que copió y luego siga una serie de avisos, o bien puede proporcionar el comando completo incluyendo todos los parámetros necesarios como argumentos de línea de comandos.

   Tenga en cuenta que el instalador realiza una comprobación previa para asegurarse de que el sistema y los requisitos de red están en su lugar para una instalación correcta.

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue la información que ha copiado del paso 8: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. Introduzca la dirección IP o el nombre de host de la máquina host de clasificación de BlueXP para que se pueda acceder a ella desde el sistema Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host del conector de BlueXP para que el sistema de clasificación de BlueXP pueda acceder a ellos.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host necesarios: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Client_id* = Identificador de cliente de conector (agregue el sufijo “clientes” al ID de cliente si aún no está allí)
   - *USER_token* = token de acceso de usuario JWT
   - *ds_host* = dirección IP o nombre de host del sistema de clasificación de BlueXP.
   - *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.

Resultado

El instalador de clasificación de BlueXP instala los paquetes, registra la instalación e instala la clasificación de BlueXP. La instalación puede tardar entre 10 y 20 minutos.

Si hay conectividad por el puerto 8080 entre el equipo host y la instancia de Connector, verás el progreso de la instalación en la pestaña de clasificación de BlueXP de BlueXP.

El futuro

En la página Configuration puede seleccionar el local "Clústeres de ONTAP en las instalaciones" y.. "oracle" que desea escanear.

También puede hacerlo "Configura las licencias de BYOL para la clasificación de BlueXP" Desde la página de la cartera digital de BlueXP en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instalación de varios hosts para configuraciones grandes

En configuraciones de gran tamaño en las que va a escanear petabytes de datos, puede incluir varios hosts para proporcionar una capacidad de procesamiento adicional. Cuando se utilizan varios sistemas host, el sistema principal se denomina *Manager node* y los sistemas adicionales que proporcionan potencia de procesamiento adicional se denominan *Scanner Nodes*.

Siga estos pasos al instalar el software de clasificación BlueXP en varios hosts on-premises en un entorno sin conexión.

Lo que necesitará

- Verifique que todos los sistemas Linux para los nodos Manager y Scanner se adapten al requisitos del host.
- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts de nodos de escáner que desee utilizar.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres
7946	TCP, UDP	Comunicación entre nodos
4789	UDP	Superpone el tráfico de red
50	ESP	Tráfico de red de superposición (ESP) IPsec cifrada
111	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)
2049	TCP, UDP	Servidor NFS para compartir archivos entre los hosts (necesario de cada nodo de escáner al nodo de administración)

Pasos

1. Siga los pasos 1 a 8 de la "Instalación de un solo host" en el nodo de gestión.
2. Como se muestra en el paso 9, cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de peticiones o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

   Además de las variables disponibles para una instalación de un solo host, se utiliza una nueva opción **-n <node_ip>** para especificar las direcciones IP de los nodos del escáner. Las IP de varios nodos están separadas por una coma.

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   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 de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando (por ejemplo: `sudo`

`./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) y guárdelo en un archivo de texto.

4. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**cc_onprem_installer.tar.gz**) en el equipo host.
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 3.

      Cuando la instalación finalice en todos los nodos de escáner y se han Unido al nodo de gestión, también se completa la instalación del nodo de gestión.

Resultado

El instalador de clasificación de BlueXP finalizará la instalación de paquetes y registrará la instalación. La instalación puede tardar entre 15 y 25 minutos.

El futuro

En la página Configuration puede seleccionar el local "Clústeres de ONTAP en las instalaciones" y local "oracle" que desea escanear.

También puede hacerlo "Configura las licencias de BYOL para la clasificación de BlueXP" Desde la página de la cartera digital de BlueXP en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Actualiza el software de clasificación BlueXP

Dado que el software de clasificación BlueXP se actualiza con nuevas funciones de forma regular, deberías entrar en rutina para comprobar si hay nuevas versiones periódicamente y asegurarse de que estás usando el software y las funciones más recientes. Tendrás que actualizar el software de clasificación de BlueXP manualmente porque no hay conectividad a Internet para realizar la actualización de forma automática.

Antes de empezar

- Recomendamos que el software BlueXP Connector se actualice a la última versión disponible. "Consulte los pasos de actualización del conector".
- A partir de la versión de clasificación de BlueXP 1,24, puede realizar actualizaciones a cualquier futura versión del software.

  Si tu software de clasificación BlueXP ejecuta una versión anterior a la 1,24, solo puedes actualizar una versión principal cada vez. Por ejemplo, si tiene instalada la versión 1,21.x, solo puede actualizar a 1,22.x. Si tiene varias versiones principales detrás, tendrá que actualizar el software varias veces.

Pasos

1. En un sistema configurado por Internet, descargue el software de clasificación de BlueXP en la "Sitio de soporte de NetApp". El archivo que debe seleccionar se llama **DataSense-offline-Bundle-<version>.tar.gz**.
2. Copie el paquete de software en el host Linux donde esté instalada la clasificación de BlueXP en el sitio oscuro.
3. Descomprima el paquete de software en el equipo host; por ejemplo:

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

Esto extrae el archivo de instalación **cc_onprem_installer.tar.gz**.

4. Descomprima el archivo de instalación en el equipo host; por ejemplo:

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

Esto extrae la secuencia de comandos de actualización **start_darksite_upgrade.sh** y cualquier software de terceros requerido.

5. Ejecute el script de actualización en el equipo host, por ejemplo:

```
start_darksite_upgrade.sh
```

Resultado

El software de clasificación de BlueXP se actualiza en el host. La actualización puede tardar entre 5 y 10 minutos.

Tenga en cuenta que no es necesaria ninguna actualización en los nodos de escáner si ha implementado la clasificación de BlueXP en varios sistemas hosts para analizar configuraciones de gran tamaño.

Puede comprobar que el software se haya actualizado consultando la versión en la parte inferior de las páginas de interfaz de usuario de clasificación de BlueXP.

Compruebe que su host Linux esté listo para instalar la clasificación de BlueXP

Antes de instalar manualmente la clasificación de BlueXP en un host Linux, puede ejecutar un script en el host para comprobar que estén establecidos todos los requisitos previos para instalar la clasificación de BlueXP. Puede ejecutar este script en un host Linux de su red o en un host Linux de la nube. El host se puede conectar a Internet, o el host puede residir en un sitio que no tiene acceso a Internet (un *sitio oscuro*).

También hay un script de prueba de requisito previo que forma parte del script de instalación de clasificación de BlueXP. El script descrito aquí está específicamente diseñado para usuarios que quieren verificar el host Linux independientemente de ejecutar el script de instalación de la clasificación de BlueXP.

Primeros pasos

Realizará las siguientes tareas.

1. Opcionalmente, instale un conector BlueXP si aún no tiene uno instalado. Puede ejecutar el script de prueba sin tener instalado un Connector, pero el script comprueba la conectividad entre el Connector y el equipo host de clasificación de BlueXP, por lo que se recomienda tener un Connector.
2. Prepare el equipo host y compruebe que cumple todos los requisitos.
3. Habilita el acceso a Internet saliente desde el equipo host de clasificación de BlueXP.
4. Verifique que todos los puertos necesarios estén activados en todos los sistemas.
5. Descargue y ejecute el script de prueba de requisito previo.

Cree un conector

Es necesario un conector BlueXP para poder instalar y utilizar la clasificación de BlueXP. No obstante, puede ejecutar el script Prerequisites sin un conector.

Puede hacerlo "Instale el conector en las instalaciones" En un host Linux de su red o en un host Linux del cloud. Algunos usuarios que planean instalar la clasificación de BlueXP en las instalaciones también pueden optar por instalar el conector en las instalaciones.

Para crear un conector en su entorno de proveedor de cloud, consulte "Creación de un conector en AWS", "Creación de un conector en Azure", o. "Creación de un conector en GCP".

Necesitará la dirección IP o el nombre de host del sistema Connector cuando ejecute el script Prerequisites. Tendrá esta información si instaló el conector en sus instalaciones. Si el conector está implementado en la nube, puede encontrar esta información desde la consola BlueXP: Haga clic en el icono Ayuda, seleccione **Soporte** y haga clic en **conector BlueXP**.

Verifique los requisitos del host

El software de clasificación de BlueXP debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, los requisitos de RAM, los requisitos de software, etc.

- La clasificación de BlueXP no se admite en un host compartido con otras aplicaciones; el host debe ser un host dedicado.
- Al crear el sistema host en tus instalaciones, puedes elegir entre tres tamaños de sistema en función del tamaño del conjunto de datos que tengas pensado analizar la clasificación de BlueXP.

Tamaño del sistema	CPU	RAM (la memoria de intercambio debe estar desactivada)	Disco
* Extra grande*	32 CPU	128 GB DE MEMORIA RAM	1 TiB SSD en /, o. - 100 GiB disponible en /opt - 895 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Grande	16 CPU	64 GB DE MEMORIA RAM	500 GiB SSD en /, o. - 100 GiB disponible en /opt - 395 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Media	8 CPU	32 GB DE MEMORIA RAM	200 GiB SSD en /, o. - 50 GiB disponible en /opt - 145 GiB disponible en /var/lib/docker - 5 GiB en /tmp
Pequeño	8 CPU	16 GB DE MEMORIA RAM	100 GiB SSD en /, o. - 50 GiB disponible en /opt - 45 GiB disponible en /var/lib/docker - 5 GiB en /tmp

Tenga en cuenta que existen limitaciones cuando se utilizan sistemas más pequeños. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

- A la hora de poner en marcha una instancia de computación en la nube para la instalación de tu clasificación de BlueXP, te recomendamos un sistema que cumpla los requisitos «grandes» del sistema anteriores:
  - **Tipo de instancia de AWS EC2**: Recomendamos "m6i.4xlarge". "Consulte tipos de instancia de AWS adicionales".
  - **Azure VM size**: Recomendamos "Standard_D16s_v3". "Consulte tipos de instancia de Azure adicionales".
  - **Máquina GCP tipo**: Recomendamos "n2-standard-16". "Consulte tipos de instancia de GCP adicionales".
- **Permisos de carpeta UNIX**: Se requieren los siguientes permisos mínimos de UNIX:

Carpeta	Permisos mínimos
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **sistema operativo**:
  - Los siguientes sistemas operativos requieren el uso del motor de contenedor Docker:
    - Red Hat Enterprise Linux versiones 7,8 y 7,9
    - CentOS versión 7,8 y 7,9
    - Ubuntu 22,04 (requiere la versión de clasificación de BlueXP 1,23 o posterior)
  - Los siguientes sistemas operativos requieren el uso del motor de contenedor Podman y requieren la versión de clasificación de BlueXP 1,30 o posterior:
    - Red Hat Enterprise Linux versiones 8,8, 9,0, 9,1, 9,2 y 9,3

      Tenga en cuenta que las siguientes funciones no son compatibles actualmente con RHEL 8.x y RHEL 9.x:

      - Instalación en un sitio oscuro
      - Escaneo distribuido; utilizando un nodo de escáner maestro y nodos de escáner remoto
- **Red Hat Subscription Management**: El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de 3rd partes necesario durante la instalación.
- **Software adicional**: Debes instalar el siguiente software en el host antes de instalar la clasificación BlueXP:
  - Dependiendo del sistema operativo que esté utilizando, deberá instalar uno de los motores de contenedores:
    - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".

      "Vea este vídeo" Para obtener una demostración rápida de la instalación de Docker en CentOS.

    - Podman versión 4 o superior. Para instalar Podman, actualice los paquetes del sistema (`sudo yum update -y`) Y, a continuación, instale Podman (`sudo yum install netavark -y`).

- Python versión 3,6 o superior. "Ver las instrucciones de instalación".

  - **Consideraciones sobre NTP**: NetApp recomienda configurar el sistema de clasificación BlueXP para usar un servicio de Protocolo de hora de red (NTP). La hora debe sincronizarse entre el sistema de clasificación de BlueXP y el sistema BlueXP Connector.

  - * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Te recomendamos que lo habilites antes de instalar la clasificación de BlueXP. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con la clasificación de 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
```

    Si tienes pensado usar otros hosts de clasificación de BlueXP como nodos de escáner (en un modelo distribuido), añade estas reglas a tu sistema principal en este 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
```

+
Tenga en cuenta que debe reiniciar Docker o Podman cada vez que habilite o actualice `firewalld` configuración.

Habilita el acceso a Internet saliente desde la clasificación de BlueXP

La clasificación de BlueXP requiere acceso a Internet saliente. Si tu red física o virtual utiliza un servidor proxy para acceder a Internet, asegúrese de que la instancia de clasificación de BlueXP tenga acceso a Internet saliente para contactar con los siguientes extremos.

Esta sección no es necesaria para los sistemas host instalados en sitios sin conexión a Internet.

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.

Puntos finales	Específico
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/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.
https://github.com/docker https://download.docker.com	Proporciona paquetes de requisitos previos para la instalación de Docker.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Proporciona paquetes de requisitos previos para la instalación de CentOS.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Proporciona paquetes de requisitos previos para la instalación de Ubuntu.

Verifique que todos los puertos necesarios estén habilitados

Debes asegurarte de que todos los puertos requeridos estén abiertos para la comunicación entre el conector, la clasificación de BlueXP, Active Directory y los orígenes de datos.

Tipo de conexión	Puertos	Descripción
Conector Clasificación de <> BlueXP	8080 (TCP), 443 (TCP) y 80	El firewall o las reglas de enrutamiento para Connector deben permitir el tráfico de entrada y salida a través del puerto 443 hacia y desde la instancia de clasificación de BlueXP. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, el host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, todas las comunicaciones salientes se permiten mediante el firewall predefinido o las reglas de enrutamiento.

Ejecuta el script Prerequisites de clasificación de BlueXP

Sigue estos pasos para ejecutar el script de requisitos previos de clasificación de BlueXP.

"Vea este vídeo" Para ver cómo ejecutar el script de requisitos previos e interpretar los resultados.

Lo que necesitará

- Compruebe que su sistema Linux cumple con el requisitos del host.

- Compruebe que el sistema tiene instalados los dos paquetes de software de requisitos previos (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.

Pasos

1. Descargue el script de requisitos previos de clasificación de BlueXP desde la "Sitio de soporte de NetApp". El archivo que debe seleccionar se llama **Standalone-pre-requisito-tester-<version>**.
2. Copie el archivo en el host Linux que tiene previsto utilizar (mediante `scp` o algún otro método).
3. Asigne permisos para ejecutar el script.

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

4. Ejecute el script con el siguiente comando.

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

   Agregue la opción "--darksite" sólo si está ejecutando la secuencia de comandos en un host que no tiene acceso a Internet. Algunas pruebas de requisitos previos se omiten cuando el host no está conectado a Internet.

5. El script solicita la dirección IP del equipo host de clasificación de BlueXP.
   - Introduzca la dirección IP o el nombre de host.
6. La secuencia de comandos le indica si tiene un conector BlueXP instalado.
   - Introduzca **N** si no tiene un conector instalado.
   - Introduzca **y** si tiene un conector instalado. A continuación, introduzca la dirección IP o el nombre de host del conector BlueXP para que la secuencia de comandos de prueba pueda probar esta conectividad.
7. La secuencia de comandos ejecuta una variedad de pruebas en el sistema y muestra los resultados a medida que avanza. Cuando termine, escribe un registro de la sesión en un archivo llamado `prerequisites-test-<timestamp>.log` en el directorio `/opt/netapp/install_logs`.

Resultado

Si todas las pruebas de requisitos previos se ejecutaron correctamente, puede instalar la clasificación de BlueXP en el host cuando esté listo.

Si se detectan problemas, se clasifican como "recomendado" o "requerido" para ser solucionados. Los problemas recomendados normalmente son elementos que hacían que las tareas de análisis y categorización de la clasificación de BlueXP se ejecutaran más lentamente. No es necesario corregir estos elementos, pero es posible que desee abordarlos.

Si tiene algún problema "requerido", debe solucionar los problemas y volver a ejecutar el script de prueba de requisitos previos.

Active el análisis en sus orígenes de datos

Primeros pasos con la clasificación de BlueXP para Cloud Volumes ONTAP y ONTAP on-premises

Completa unos pasos para empezar a analizar tus volúmenes de ONTAP en Cloud Volumes ONTAP y on-premises mediante la clasificación de BlueXP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Descubra los orígenes de datos que desea analizar**

Para poder analizar volúmenes, debe agregar los sistemas como entornos de trabajo en BlueXP:

- Para sistemas Cloud Volumes ONTAP, estos entornos de trabajo deberían estar ya disponibles en BlueXP
- Para sistemas ONTAP en las instalaciones, "BlueXP debe detectar los clústeres de ONTAP"

2. **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Habilita la clasificación de BlueXP y selecciona los volúmenes que deseas escanear**

Seleccione la pestaña **Configuración** y active los escaneos de cumplimiento para volúmenes en entornos de trabajo específicos.

4. **Garantice el acceso a los volúmenes**

Ahora que la clasificación de BlueXP está habilitada, asegúrate de que puede acceder a todos los volúmenes.

- La instancia de clasificación de BlueXP necesita una conexión de red con cada subred de Cloud Volumes ONTAP o sistema ONTAP en las instalaciones.
- Los grupos de seguridad de Cloud Volumes ONTAP deben permitir las conexiones entrantes desde la instancia de clasificación de BlueXP.
- Asegúrate de que estos puertos estén abiertos a la instancia de clasificación de BlueXP:
  - Para NFS: Puertos 111 y 2049.
  - Para CIFS: Puertos 139 y 445.
- Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de clasificación de BlueXP.
- La clasificación de BlueXP necesita credenciales de Active Directory para analizar los volúmenes de CIFS.

  Haga clic en **cumplimiento** > **Configuración** > **Editar credenciales CIFS** y proporcione las credenciales.

5. **Gestione los volúmenes que desea analizar**

Selecciona o anula la selección de los volúmenes que quieres analizar y la clasificación de BlueXP iniciará o detendrá su análisis.

Detección de los orígenes de datos que desea analizar

Si los orígenes de datos que desea analizar no están ya en su entorno de BlueXP, puede añadirlos al lienzo en este momento.

Sus sistemas Cloud Volumes ONTAP ya deben estar disponibles en el lienzo de BlueXP. Para los sistemas ONTAP en las instalaciones, es necesario que lo tenga "BlueXP descubre estos clústeres".

Implementar la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

Si está escaneando sistemas Cloud Volumes ONTAP y ONTAP locales a los que se puede acceder a través de Internet, puede hacerlo "Pon en marcha la clasificación de BlueXP en el cloud" o. "en una ubicación en el hotel que tiene acceso a internet".

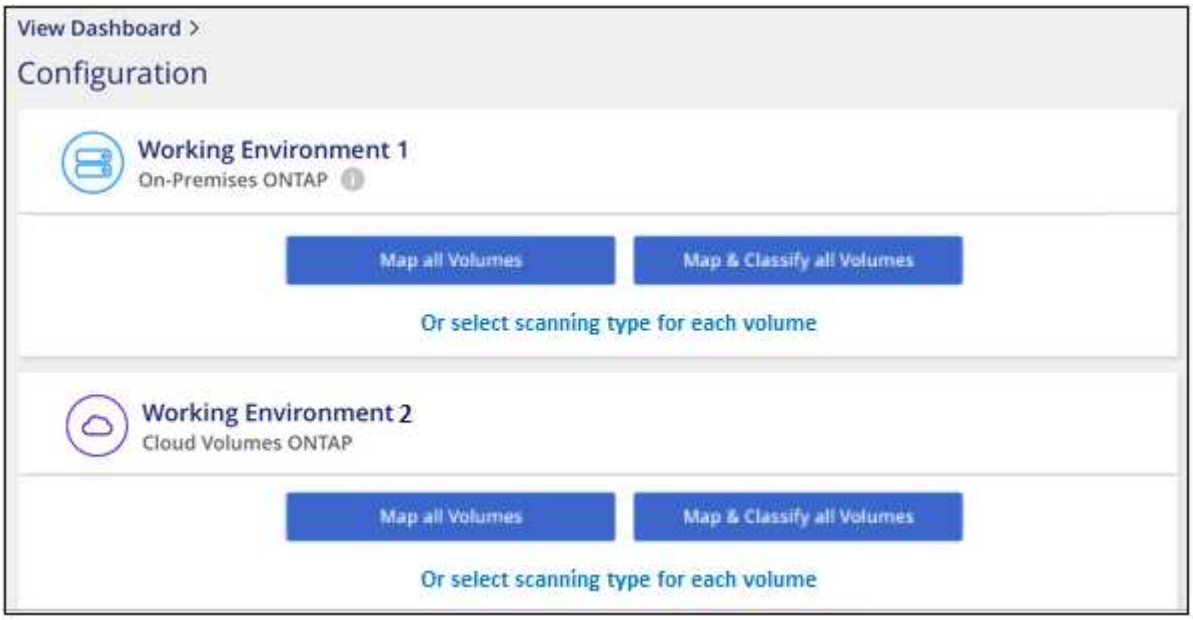
Si está escaneando en las instalaciones sistemas ONTAP que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Pon en marcha la clasificación de BlueXP en la misma ubicación on-premises que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar la clasificación de BlueXP en tus entornos de trabajo

Puedes habilitar la clasificación de BlueXP en sistemas Cloud Volumes ONTAP en cualquier proveedor de nube compatible y en clústeres de ONTAP on-premises.

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.



2. Seleccione cómo desea analizar los volúmenes en cada entorno de trabajo. "Obtenga más información

sobre las exploraciones de clasificación y mapeo":

- Para asignar todos los volúmenes, haga clic en **asignar todos los volúmenes**.
- Para asignar y clasificar todos los volúmenes, haga clic en **asignar y clasificar todos los volúmenes**.
- Para personalizar la exploración de cada volumen, haga clic en **o seleccione el tipo de exploración para cada volumen** y, a continuación, elija los volúmenes que desea asignar y/o clasificar.

  Consulte Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes para obtener más detalles.

3. En el cuadro de diálogo de confirmación, haz clic en **Aprobar** para que la clasificación de BlueXP comience a escanear tus volúmenes.

Resultado

La clasificación de BlueXP comienza a analizar los volúmenes que seleccionaste en el entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento en cuanto la clasificación de BlueXP finalice los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

- De forma predeterminada, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS u permisos de escritura en NFS, el sistema no analizará los archivos de tus volúmenes, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. La página resultante tiene un ajuste que se puede habilitar para que la clasificación de BlueXP analice los volúmenes independientemente de los permisos.
- La clasificación de BlueXP solo analiza un recurso compartido de archivos en un volumen. Si tiene varios recursos compartidos en sus volúmenes, deberá escanear los otros recursos compartidos por separado como un grupo de recursos compartidos. "Consulta más detalles sobre esta limitación de clasificación de BlueXP".

Verificar que la clasificación de BlueXP tenga acceso a los volúmenes

Asegúrese de que la clasificación de BlueXP pueda acceder a los volúmenes comprobando la red, los grupos de seguridad y las políticas de exportación. Tendrás que ofrecer la clasificación de BlueXP con credenciales CIFS para que pueda acceder a los volúmenes de CIFS.

Pasos

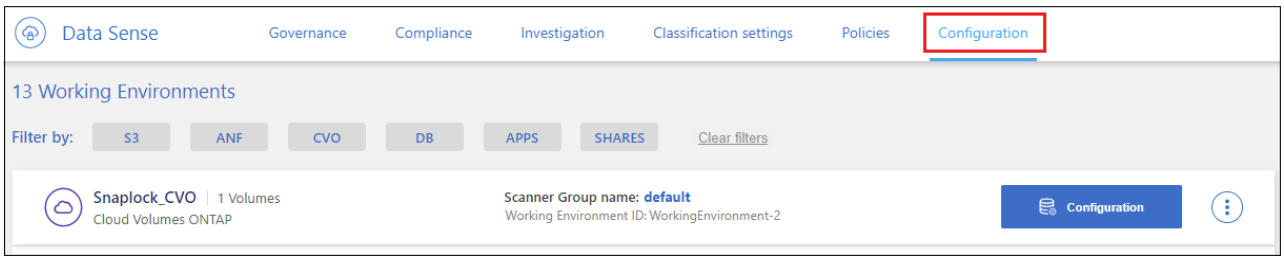
1. Asegúrese de que haya una conexión de red entre la instancia de clasificación de BlueXP y cada red que incluya volúmenes para los clústeres de Cloud Volumes ONTAP o de ONTAP en las instalaciones.
2. Compruebe que el grupo de seguridad de Cloud Volumes ONTAP permita el tráfico entrante de la instancia de clasificación de BlueXP.

   Puede abrir el grupo de seguridad para el tráfico desde la dirección IP de la instancia de clasificación de BlueXP o bien abrir el grupo de seguridad para todo el tráfico desde dentro de la red virtual.

3. Compruebe que los siguientes puertos estén abiertos en la instancia de clasificación de BlueXP:
   - Para NFS: Puertos 111 y 2049.
   - Para CIFS: Puertos 139 y 445.
4. Compruebe que las políticas de exportación de volúmenes de NFS incluyan la dirección IP de la instancia de clasificación de BlueXP para que pueda acceder a los datos de cada volumen.

5. Si usas CIFS, proporciona una clasificación de BlueXP con credenciales de Active Directory para que pueda analizar los volúmenes de CIFS.

   a. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.

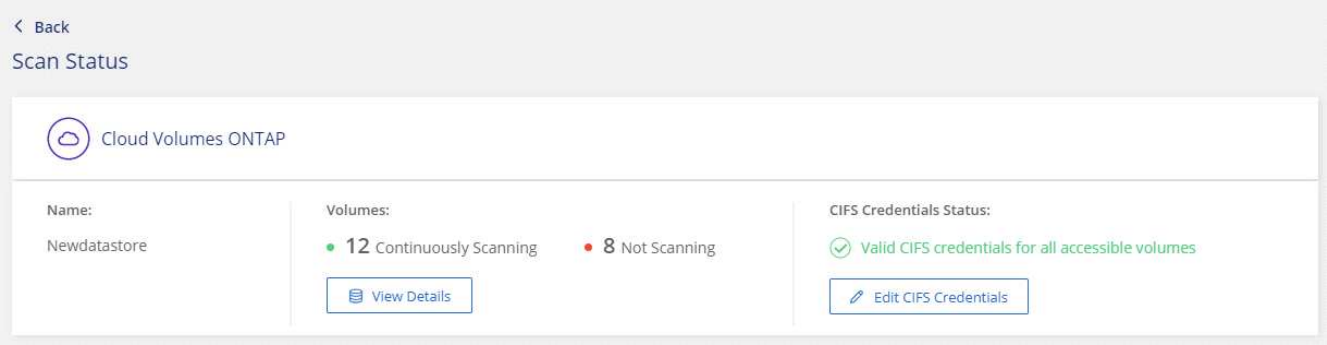


   b. Para cada entorno de trabajo, haga clic en **Edit CIFS Credentials** e introduzca el nombre de usuario y la contraseña que la clasificación de BlueXP necesita para acceder a los volúmenes CIFS del sistema.

      Las credenciales pueden ser de solo lectura, pero al proporcionar credenciales de administrador se garantiza que la clasificación de BlueXP pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de BlueXP.

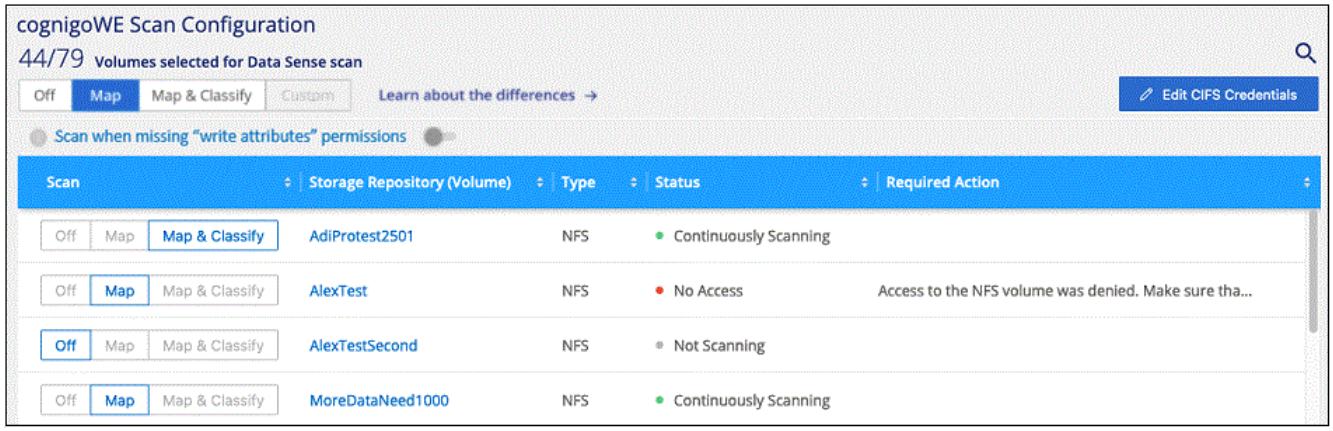
      Si quieres asegurarte de que las «horas de último acceso» no cambian debido a los análisis de clasificación de BlueXP, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

      Después de introducir las credenciales, debe ver un mensaje que indica que todos los volúmenes CIFS se autenticaron correctamente.



6. En la página *Configuration*, haga clic en **View Details** para revisar el estado de cada volumen CIFS y NFS y corregir los errores.

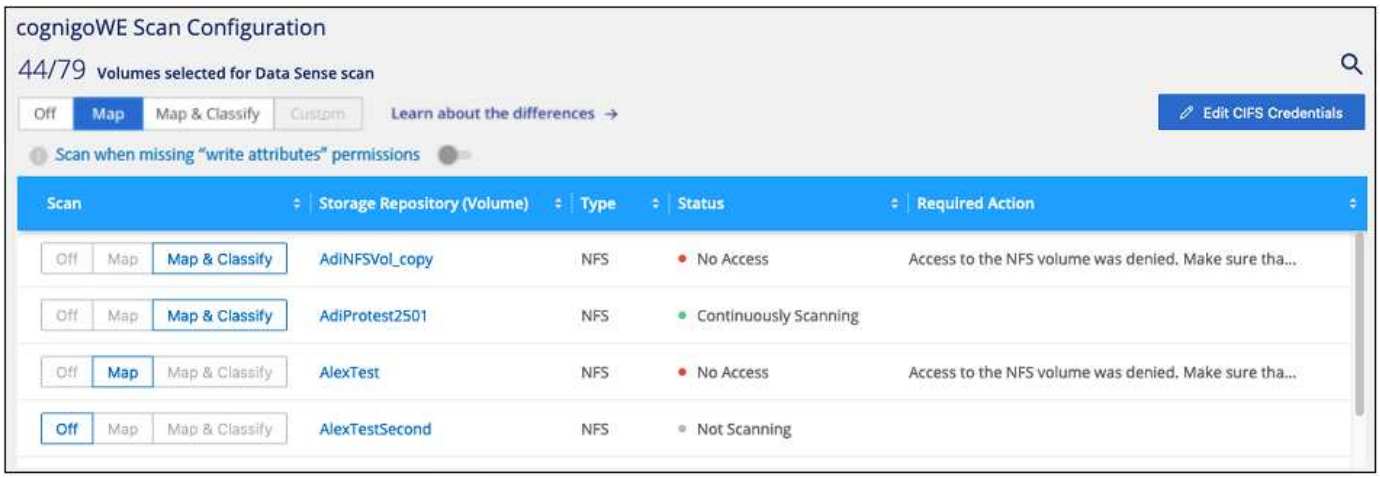
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes, uno de los cuales la clasificación de BlueXP no puede analizar debido a problemas de conectividad de red entre la instancia de clasificación de BlueXP y el volumen.



Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes

Puede iniciar o detener exploraciones de sólo asignación, o bien análisis de asignación y clasificación, en un entorno de trabajo en cualquier momento desde la página Configuración. También puede cambiar de exploraciones de sólo asignación a exploraciones de asignación y clasificación, y viceversa. Le recomendamos que analice todos los volúmenes.

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



Para:	Haga lo siguiente:
Active los análisis de sólo asignación en un volumen	En el área de volumen, haga clic en **Mapa**
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**
Active análisis de sólo asignación en todos los volúmenes	En el área de encabezado, haga clic en **Mapa**

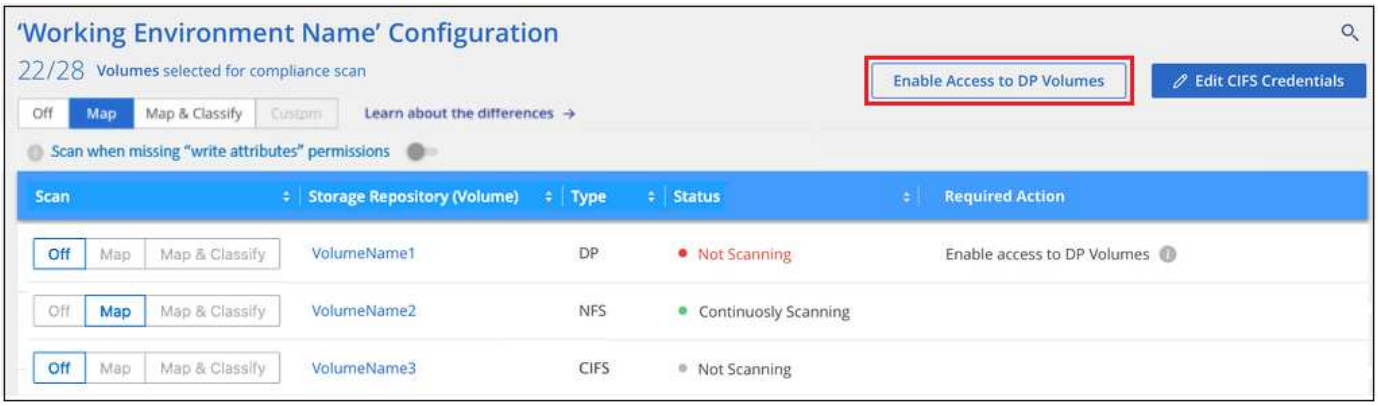
Para:	Haga lo siguiente:
Active el análisis completo en todos los volúmenes	En el área de encabezado, haga clic en **Mapa y clasificación**
Desactive el análisis en todos los volúmenes	En el área encabezado, haga clic en **Desactivado**

> Los nuevos volúmenes agregados al entorno de trabajo sólo se analizan automáticamente cuando se ha establecido el ajuste **Mapa** o **Mapa y clasificación** en el área de rumbo. Cuando se establece en **personalizado** o **Desactivado** en el área rumbo, deberá activar la asignación y/o la exploración completa en cada volumen nuevo que agregue en el entorno de trabajo.

Análisis de volúmenes de protección de datos

De forma predeterminada, los volúmenes de protección de datos (DP) no se analizan porque no se exponen externamente y la clasificación de BlueXP no puede acceder a ellos. Se trata de los volúmenes de destino de las operaciones de SnapMirror desde un sistema ONTAP en las instalaciones o desde un sistema Cloud Volumes ONTAP.

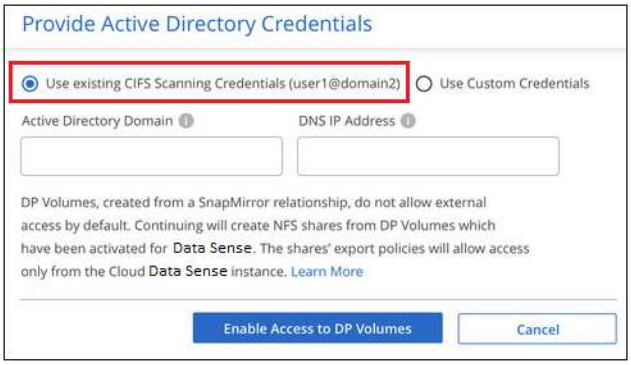
Inicialmente, la lista de volúmenes identifica estos volúmenes como *Type* **DP** con el *Status* **no Scanning** y el *Required Action* **Enable Access to DP Volumes**.

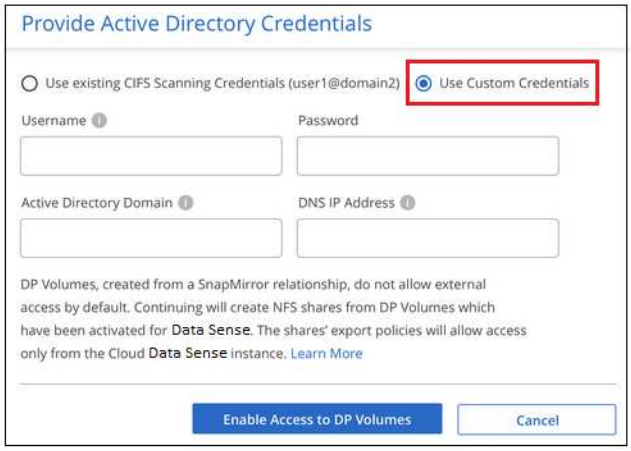


Pasos

Si desea analizar estos volúmenes de protección de datos:

1. Haga clic en **Activar acceso a volúmenes DP** en la parte superior de la página.
2. Revise el mensaje de confirmación y vuelva a hacer clic en **Activar acceso a volúmenes DP**.
   - Se habilitan los volúmenes que se crearon inicialmente como volúmenes NFS en el sistema ONTAP de origen.
   - Los volúmenes que se crearon inicialmente como volúmenes CIFS en el sistema ONTAP de origen requieren la introducción de credenciales CIFS para analizar dichos volúmenes DP. Si ya has introducido credenciales de Active Directory para que la clasificación de BlueXP pueda analizar los volúmenes de CIFS, pueda usar esas credenciales o puede especificar un conjunto diferente de credenciales de administrador.





3. Active cada volumen DP que desee analizar del mismo modo que se habilitaron otros volúmenes.

Resultado

Una vez habilitada, la clasificación de BlueXP crea un recurso compartido NFS de cada volumen de DP que se activó para el análisis. Las políticas de exportación de recursos compartidos solo permiten el acceso desde la instancia de clasificación de BlueXP.

Nota: Si no ha tenido volúmenes de protección de datos CIFS cuando ha activado inicialmente el acceso a volúmenes DP y, más tarde, agregue algunos, el botón **Activar acceso a CIFS DP** aparece en la parte superior de la página Configuración. Haga clic en este botón y añada credenciales CIFS para habilitar el acceso a estos volúmenes CIFS DP.

> Las credenciales de Active Directory solo están registradas en la máquina virtual de almacenamiento del primer volumen CIFS DP, por lo que se analizarán todos los volúmenes de DP en esa SVM. Cualquier volumen que resida en otras SVM no tendrá registradas las credenciales de Active Directory; por lo tanto, esos volúmenes de DP no se analizarán.

Primeros pasos con la clasificación de BlueXP para Azure NetApp Files

Completa unos pasos para empezar a usar la clasificación de BlueXP para Azure NetApp Files.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 **Descubra los sistemas Azure NetApp Files que desea analizar**

Antes de poder analizar volúmenes Azure NetApp Files, "Debe configurar BlueXP para descubrir la configuración".

2 **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP en BlueXP" si aún no hay una instancia implementada.

3 Habilita la clasificación de BlueXP y selecciona los volúmenes que deseas escanear

Haga clic en **cumplimiento**, seleccione la ficha **Configuración** y active los análisis de cumplimiento para volúmenes en entornos de trabajo específicos.

4 Garantice el acceso a los volúmenes

Ahora que la clasificación de BlueXP está habilitada, asegúrate de que puede acceder a todos los volúmenes.

- La instancia de clasificación de BlueXP necesita una conexión de red con cada subred Azure NetApp Files.
- Asegúrate de que estos puertos estén abiertos a la instancia de clasificación de BlueXP:
  - Para NFS, puertos 111 y 2049.
  - Para CIFS, puertos 139 y 445.
- Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de clasificación de BlueXP.
- La clasificación de BlueXP necesita credenciales de Active Directory para analizar los volúmenes de CIFS.

  Haga clic en **cumplimiento** > **Configuración** > **Editar credenciales CIFS** y proporcione las credenciales.

5 Gestione los volúmenes que desea analizar

Selecciona o anula la selección de los volúmenes que quieres analizar y la clasificación de BlueXP iniciará o detendrá su análisis.

Detección del sistema Azure NetApp Files que desea analizar

Si el sistema Azure NetApp Files que desea escanear no está ya en BlueXP como entorno de trabajo, puede agregarlo al lienzo en este momento.

"Descubra cómo descubrir el sistema Azure NetApp Files en BlueXP".

Implementar la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

La clasificación de BlueXP debe ponerse en marcha en la nube al analizar los volúmenes de Azure NetApp Files y debe implementarse en la misma región que los volúmenes que deseas analizar.

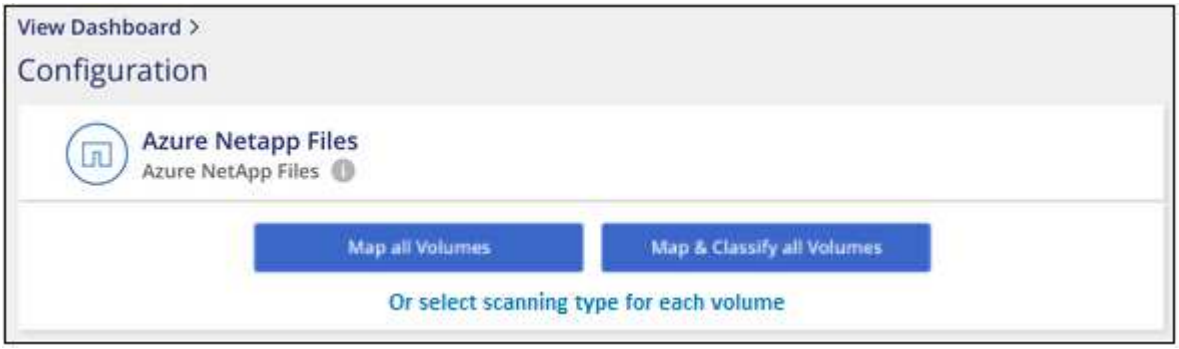
Nota: La implementación de la clasificación de BlueXP en una ubicación local no es compatible actualmente al analizar volúmenes de Azure NetApp Files.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar la clasificación de BlueXP en tus entornos de trabajo

Puede habilitar la clasificación de BlueXP en sus volúmenes de Azure NetApp Files.

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.



2. Seleccione cómo desea analizar los volúmenes en cada entorno de trabajo. "Obtenga más información sobre las exploraciones de clasificación y mapeo":
   - Para asignar todos los volúmenes, haga clic en **asignar todos los volúmenes**.
   - Para asignar y clasificar todos los volúmenes, haga clic en **asignar y clasificar todos los volúmenes**.
   - Para personalizar la exploración de cada volumen, haga clic en **o seleccione el tipo de exploración para cada volumen** y, a continuación, elija los volúmenes que desea asignar y/o clasificar.

     Consulte Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes para obtener más detalles.

3. En el cuadro de diálogo de confirmación, haz clic en **Aprobar** para que la clasificación de BlueXP comience a escanear tus volúmenes.

Resultado

La clasificación de BlueXP comienza a analizar los volúmenes que seleccionaste en el entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento en cuanto la clasificación de BlueXP finalice los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

- De forma predeterminada, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS u permisos de escritura en NFS, el sistema no analizará los archivos de tus volúmenes, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. La página resultante tiene un ajuste que se puede habilitar para que la clasificación de BlueXP analice los volúmenes independientemente de los permisos.
- La clasificación de BlueXP solo analiza un recurso compartido de archivos en un volumen. Si tiene varios recursos compartidos en sus volúmenes, deberá escanear los otros recursos compartidos por separado como un grupo de recursos compartidos. "Consulta más detalles sobre esta limitación de clasificación de BlueXP".

Verificar que la clasificación de BlueXP tenga acceso a los volúmenes

Asegúrese de que la clasificación de BlueXP pueda acceder a los volúmenes comprobando la red, los grupos de seguridad y las políticas de exportación. Tendrás que ofrecer la clasificación de BlueXP con credenciales CIFS para que pueda acceder a los volúmenes de CIFS.

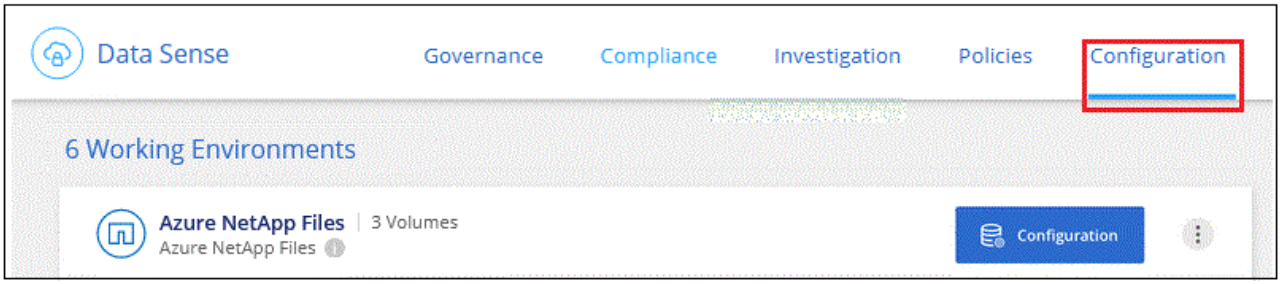
Pasos

1. Asegúrate de que haya una conexión de red entre la instancia de clasificación de BlueXP y cada red que incluya volúmenes para Azure NetApp Files.

> Para Azure NetApp Files, la clasificación de BlueXP solo puede analizar volúmenes que estén en la misma región que BlueXP.

2. Compruebe que los siguientes puertos estén abiertos en la instancia de clasificación de BlueXP:
   - Para NFS, puertos 111 y 2049.
   - Para CIFS, puertos 139 y 445.
3. Compruebe que las políticas de exportación de volúmenes de NFS incluyan la dirección IP de la instancia de clasificación de BlueXP para que pueda acceder a los datos de cada volumen.
4. Si usas CIFS, proporciona una clasificación de BlueXP con credenciales de Active Directory para que pueda analizar los volúmenes de CIFS.

   a. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.

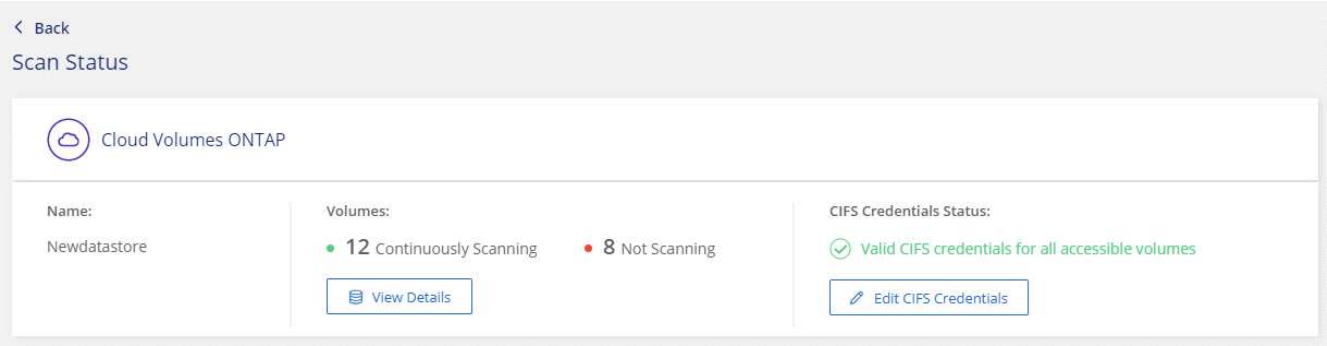


   b. Para cada entorno de trabajo, haga clic en **Edit CIFS Credentials** e introduzca el nombre de usuario y la contraseña que la clasificación de BlueXP necesita para acceder a los volúmenes CIFS del sistema.

      Las credenciales pueden ser de solo lectura, pero al proporcionar credenciales de administrador se garantiza que la clasificación de BlueXP pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de BlueXP.

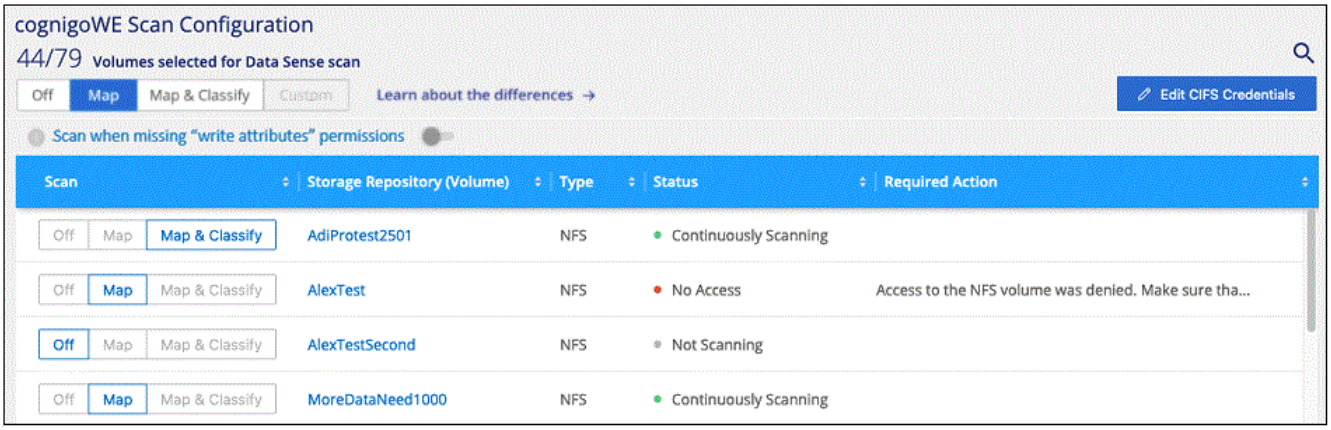
      Si quieres asegurarte de que las «horas de último acceso» no cambian debido a los análisis de clasificación de BlueXP, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

      Después de introducir las credenciales, debe ver un mensaje que indica que todos los volúmenes CIFS se autenticaron correctamente.



5. En la página *Configuration*, haga clic en **View Details** para revisar el estado de cada volumen CIFS y NFS y corregir los errores.

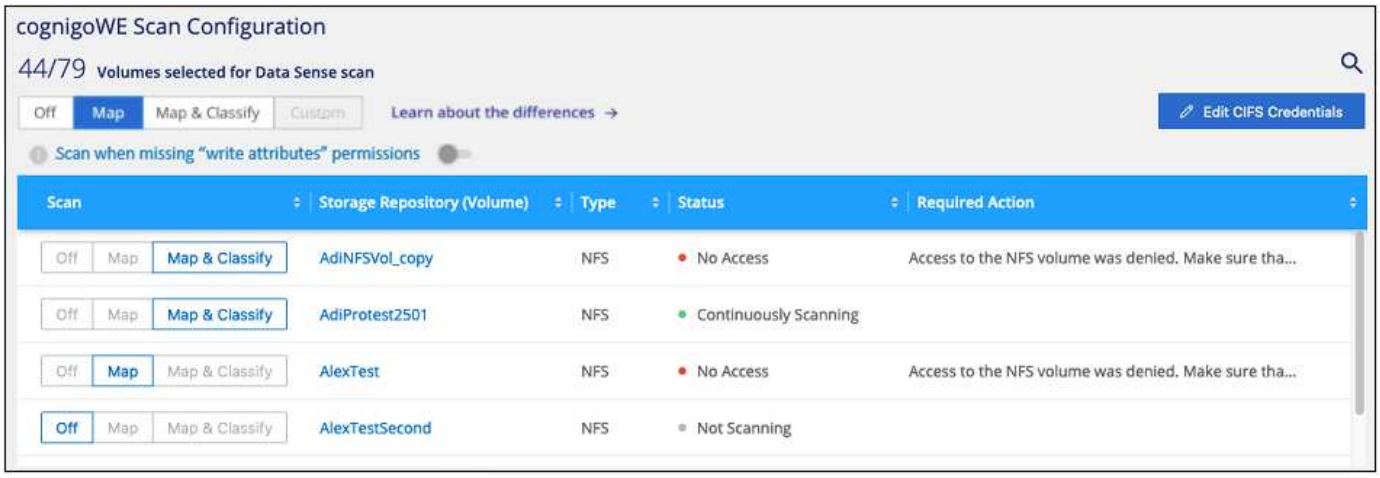
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes, uno de los cuales la clasificación de BlueXP no puede analizar debido a problemas de conectividad de red entre la instancia de clasificación de BlueXP y el volumen.



Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes

Puede iniciar o detener exploraciones de sólo asignación, o bien análisis de asignación y clasificación, en un entorno de trabajo en cualquier momento desde la página Configuración. También puede cambiar de exploraciones de sólo asignación a exploraciones de asignación y clasificación, y viceversa. Le recomendamos que analice todos los volúmenes.

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



Para:	Haga lo siguiente:
Active los análisis de sólo asignación en un volumen	En el área de volumen, haga clic en **Mapa**

Para:	Haga lo siguiente:
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**
Active análisis de sólo asignación en todos los volúmenes	En el área de encabezado, haga clic en **Mapa**
Active el análisis completo en todos los volúmenes	En el área de encabezado, haga clic en **Mapa y clasificación**
Desactive el análisis en todos los volúmenes	En el área encabezado, haga clic en **Desactivado**

Los nuevos volúmenes agregados al entorno de trabajo sólo se analizan automáticamente cuando se ha establecido el ajuste **Mapa** o **Mapa y clasificación** en el área de rumbo. Cuando se establece en **personalizado** o **Desactivado** en el área rumbo, deberá activar la asignación y/o la exploración completa en cada volumen nuevo que agregue en el entorno de trabajo.

Comienza a usar la clasificación de BlueXP para Amazon FSx para ONTAP

Completa unos pasos para empezar a analizar volúmenes de Amazon FSx para ONTAP con la clasificación de BlueXP.

Antes de empezar

- Necesitas un conector activo en AWS para poner en marcha y gestionar la clasificación de BlueXP.
- El grupo de seguridad que haya seleccionado al crear el entorno de trabajo debe permitir el tráfico desde la instancia de clasificación de BlueXP. Puede buscar el grupo de seguridad asociado mediante ENI conectado al FSX para el sistema de archivos ONTAP y editarlo mediante la consola de gestión de AWS.

  "Grupos de seguridad de AWS para instancias de Linux"

  "Grupos de seguridad de AWS para instancias de Windows"

  "Interfaces de red elásticas de AWS (ENI)"

Inicio rápido

Comience rápidamente siguiendo estos pasos o desplácese hacia abajo para obtener todos los detalles.

1 Descubra el FSX para los sistemas de archivos ONTAP que desea analizar

Antes de poder analizar volúmenes FSX para ONTAP, "Debe tener un entorno de trabajo FSX con volúmenes configurados".

2 Implementa la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP en BlueXP" si aún no hay una instancia implementada.

3 Habilita la clasificación de BlueXP y selecciona los volúmenes que deseas escanear

Seleccione la pestaña **Configuración** y active los escaneos de cumplimiento para volúmenes en entornos de trabajo específicos.

4 Garantice el acceso a los volúmenes

Ahora que la clasificación de BlueXP está habilitada, asegúrate de que puede acceder a todos los volúmenes.

- La instancia de clasificación de BlueXP necesita una conexión de red con cada subred de FSx para ONTAP.
- Asegúrate de que los siguientes puertos estén abiertos a la instancia de clasificación de BlueXP:
  - Para NFS, puertos 111 y 2049.
  - Para CIFS, puertos 139 y 445.
- Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de clasificación de BlueXP.
- La clasificación de BlueXP necesita credenciales de Active Directory para analizar los volúmenes de CIFS. + haga clic en **cumplimiento** > **Configuración** > **Editar credenciales CIFS** y proporcione las credenciales.

5 Gestione los volúmenes que desea analizar

Seleccione o anule la selección de los volúmenes que desea analizar y la clasificación de BlueXP iniciará o detendrá su análisis.

Descubrir el FSX para el sistema de archivos ONTAP que desea analizar

Si el sistema de archivos FSX para ONTAP que desea analizar no está ya en BlueXP como entorno de trabajo, puede agregarlo al lienzo en este momento.

"Descubra cómo descubrir o crear el sistema de archivos FSX para ONTAP en BlueXP".

Implementar la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

Debes poner en marcha la clasificación de BlueXP en la misma red de AWS que el conector para AWS y los volúmenes FSx que desees analizar.

Nota: Implementar la clasificación de BlueXP en una ubicación local no es compatible actualmente al escanear volúmenes de FSX.

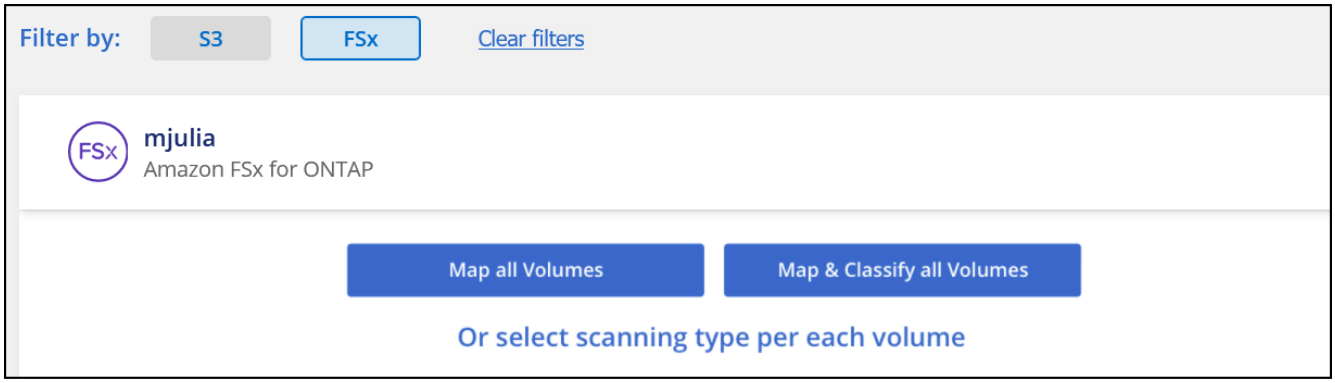
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar la clasificación de BlueXP en tus entornos de trabajo

Puedes habilitar la clasificación de BlueXP para FSx para volúmenes de ONTAP.

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la

ficha **Configuración**.



2. Seleccione cómo desea analizar los volúmenes en cada entorno de trabajo. "Obtenga más información sobre las exploraciones de clasificación y mapeo":
   - Para asignar todos los volúmenes, haga clic en **asignar todos los volúmenes**.
   - Para asignar y clasificar todos los volúmenes, haga clic en **asignar y clasificar todos los volúmenes**.
   - Para personalizar la exploración de cada volumen, haga clic en **o seleccione el tipo de exploración para cada volumen** y, a continuación, elija los volúmenes que desea asignar y/o clasificar.

     Consulte Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes para obtener más detalles.

3. En el cuadro de diálogo de confirmación, haz clic en **Aprobar** para que la clasificación de BlueXP comience a escanear tus volúmenes.

Resultado

La clasificación de BlueXP comienza a analizar los volúmenes que seleccionaste en el entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento en cuanto la clasificación de BlueXP finalice los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

- De forma predeterminada, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS u permisos de escritura en NFS, el sistema no analizará los archivos de tus volúmenes, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. La página resultante tiene un ajuste que se puede habilitar para que la clasificación de BlueXP analice los volúmenes independientemente de los permisos.
- La clasificación de BlueXP solo analiza un recurso compartido de archivos en un volumen. Si tiene varios recursos compartidos en sus volúmenes, deberá escanear los otros recursos compartidos por separado como un grupo de recursos compartidos. "Consulta más detalles sobre esta limitación de clasificación de BlueXP".

Verificar que la clasificación de BlueXP tenga acceso a los volúmenes

Para asegurarse de que la clasificación de BlueXP pueda acceder a los volúmenes, compruebe la red, los grupos de seguridad y las políticas de exportación.

Tendrás que ofrecer la clasificación de BlueXP con credenciales CIFS para que pueda acceder a los volúmenes de CIFS.

Pasos

1. En la página *Configuration*, haga clic en **View Details** para revisar el estado y corregir los errores.

   Por ejemplo, la siguiente imagen muestra una clasificación de BlueXP de volúmenes que no se puede analizar debido a problemas de conectividad de red entre la instancia de clasificación de BlueXP y el volumen.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. Asegúrate de que haya una conexión de red entre la instancia de clasificación de BlueXP y cada red que incluya volúmenes para FSx para ONTAP.

   Para FSx para ONTAP, la clasificación de BlueXP puede analizar volúmenes solo en la misma región que BlueXP.

3. Compruebe que los siguientes puertos estén abiertos en la instancia de clasificación de BlueXP.
   - Para NFS, puertos 111 y 2049.
   - Para CIFS, puertos 139 y 445.
4. Compruebe que las políticas de exportación de volúmenes de NFS incluyan la dirección IP de la instancia de clasificación de BlueXP para que pueda acceder a los datos de cada volumen.
5. Si usas CIFS, proporciona una clasificación de BlueXP con credenciales de Active Directory para que pueda analizar los volúmenes de CIFS.

   a. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.

   b. Para cada entorno de trabajo, haga clic en **Edit CIFS Credentials** e introduzca el nombre de usuario y la contraseña que la clasificación de BlueXP necesita para acceder a los volúmenes CIFS del sistema.

      Las credenciales pueden ser de solo lectura, pero al proporcionar credenciales de administrador se garantiza que la clasificación de BlueXP pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de BlueXP.

      Si quieres asegurarte de que las «horas de último acceso» no cambian debido a los análisis de clasificación de BlueXP, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

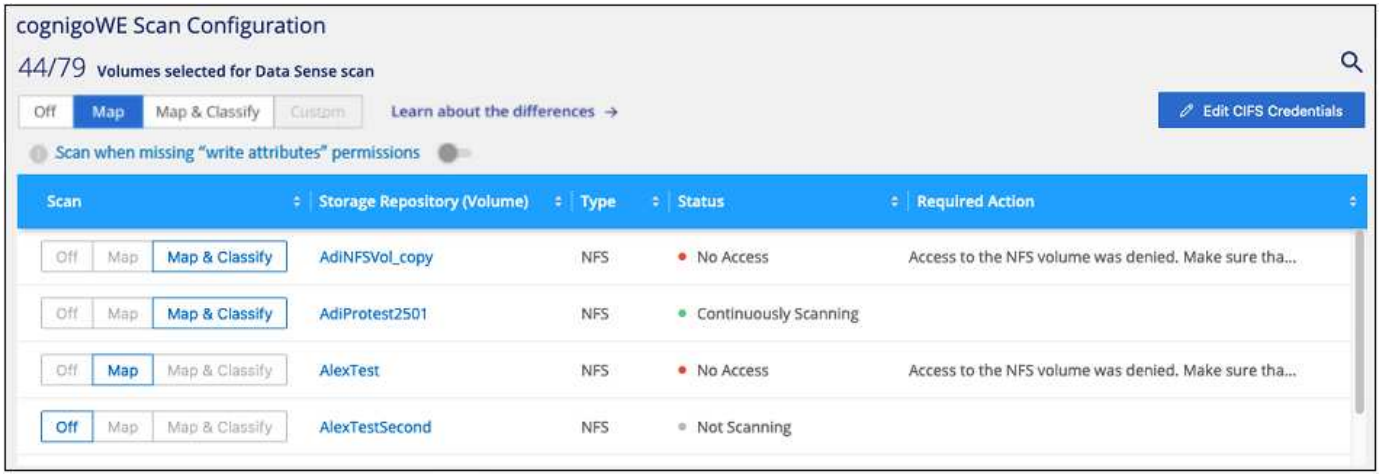
   Después de introducir las credenciales, debe ver un mensaje que indica que todos los volúmenes CIFS se autenticaron correctamente.

Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes

Puede iniciar o detener exploraciones de sólo asignación, o bien análisis de asignación y clasificación, en un entorno de trabajo en cualquier momento desde la página Configuración. También puede cambiar de exploraciones de sólo asignación a exploraciones de asignación y clasificación, y viceversa. Le recomendamos que analice todos los volúmenes.

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de**

"atributos de escritura" está desactivado de forma predeterminada. Esto significa que, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



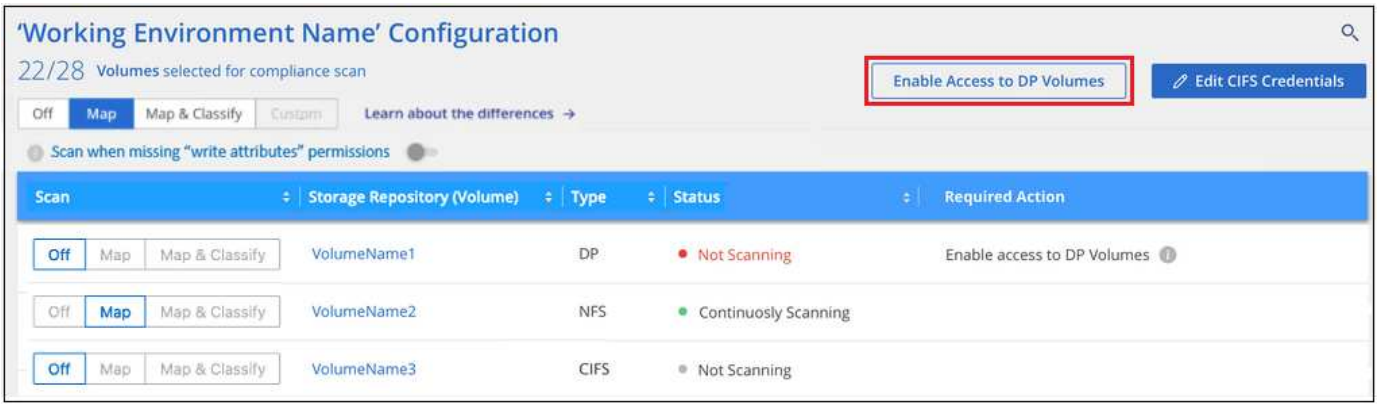
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en un volumen	En el área de volumen, haga clic en **Mapa**
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**
Active análisis de sólo asignación en todos los volúmenes	En el área de encabezado, haga clic en **Mapa**
Active el análisis completo en todos los volúmenes	En el área de encabezado, haga clic en **Mapa y clasificación**
Desactive el análisis en todos los volúmenes	En el área encabezado, haga clic en **Desactivado**

Los nuevos volúmenes agregados al entorno de trabajo sólo se analizan automáticamente cuando se ha establecido el ajuste **Mapa** o **Mapa y clasificación** en el área de rumbo. Cuando se establece en **personalizado** o **Desactivado** en el área rumbo, deberá activar la asignación y/o la exploración completa en cada volumen nuevo que agregue en el entorno de trabajo.

Análisis de volúmenes de protección de datos

De forma predeterminada, los volúmenes de protección de datos (DP) no se analizan porque no se exponen externamente y la clasificación de BlueXP no puede acceder a ellos. Estos son los volúmenes de destino de las operaciones de SnapMirror desde un FSX para el sistema de archivos ONTAP.

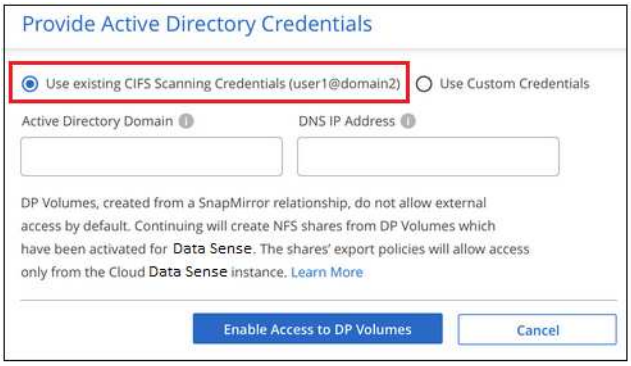
Inicialmente, la lista de volúmenes identifica estos volúmenes como *Type* **DP** con el *Status* **no Scanning** y el *Required Action* **Enable Access to DP Volumes**.

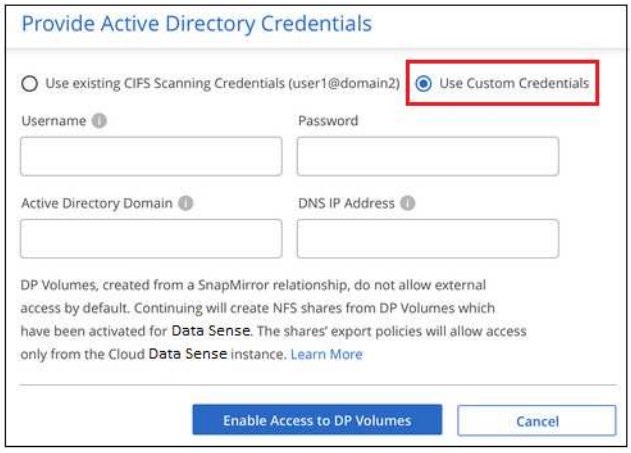


Pasos

Si desea analizar estos volúmenes de protección de datos:

1. Haga clic en **Activar acceso a volúmenes DP** en la parte superior de la página.
2. Revise el mensaje de confirmación y vuelva a hacer clic en **Activar acceso a volúmenes DP**.
   - Se habilitaron los volúmenes creados inicialmente como volúmenes NFS en el FSX de origen para el sistema de archivos ONTAP.
   - Los volúmenes creados inicialmente como volúmenes CIFS en el FSX de origen para el sistema de archivos ONTAP requieren que introduzca credenciales CIFS para analizar esos volúmenes DP. Si ya has introducido credenciales de Active Directory para que la clasificación de BlueXP pueda analizar los volúmenes de CIFS, pueda usar esas credenciales o puede especificar un conjunto diferente de credenciales de administrador.





3. Active cada volumen DP que desee analizar del mismo modo que se habilitaron otros volúmenes.

Resultado

Una vez habilitada, la clasificación de BlueXP crea un recurso compartido NFS de cada volumen de DP que se activó para el análisis. Las políticas de exportación de recursos compartidos solo permiten el acceso desde la instancia de clasificación de BlueXP.

Nota: Si no ha tenido volúmenes de protección de datos CIFS cuando ha activado inicialmente el acceso a volúmenes DP y, más tarde, agregue algunos, el botón **Activar acceso a CIFS DP** aparece en la parte superior de la página Configuración. Haga clic en este botón y añada credenciales CIFS para habilitar el acceso a estos volúmenes CIFS DP.

Las credenciales de Active Directory solo están registradas en la máquina virtual de almacenamiento del primer volumen CIFS DP, por lo que se analizarán todos los volúmenes de DP en esa SVM. Cualquier volumen que resida en otras SVM no tendrá registradas las credenciales de Active Directory; por lo tanto, esos volúmenes de DP no se analizarán.

Primeros pasos con la clasificación de BlueXP para Amazon S3

La clasificación de BlueXP puede analizar tus buckets de Amazon S3 para identificar los datos personales y confidenciales que residen en el almacenamiento de objetos S3. La clasificación de BlueXP puede analizar cualquier bloque de la cuenta, independientemente de si se ha creado para una solución de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Configure los requisitos de S3 en su entorno de cloud**

Asegúrate de que tu entorno de nube pueda cumplir los requisitos de la clasificación de BlueXP, incluida la preparación de un rol de IAM y la configuración de la conectividad desde la clasificación de BlueXP a S3. Vea la lista completa.

2. **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Activa la clasificación de BlueXP en tu entorno de trabajo S3**

Seleccione el entorno de trabajo de Amazon S3, haga clic en **Habilitar** y seleccione una función IAM que incluya los permisos necesarios.

4. **Seleccione los cucharones que desea escanear**

Selecciona los bloques que quieres escanear y la clasificación de BlueXP comenzará a escanearlos.

Revisión de los requisitos previos de S3

Los siguientes requisitos son específicos para el análisis de bloques de S3.

Configura un rol de IAM para la instancia de clasificación de BlueXP

La clasificación de BlueXP necesita permisos para conectarse a los bloques de S3 de tu cuenta y analizarlos. Configure un rol de IAM que incluya los permisos que se indican a continuación. BlueXP te pide que selecciones un rol de IAM al habilitar la clasificación de BlueXP en el entorno de trabajo de 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/*"
          ]
      }
  ]
}
```

Proporciona conectividad desde la clasificación de BlueXP a Amazon S3

La clasificación de BlueXP necesita una conexión con Amazon S3. La mejor forma de proporcionar esa conexión es mediante un extremo VPC con el servicio S3. Para ver instrucciones, consulte "Documentación de AWS: Crear un extremo de puerta de enlace".

Al crear el extremo de VPC, asegúrese de seleccionar la región, la VPC y la tabla de rutas que correspondan a la instancia de clasificación de BlueXP. También debe modificar el grupo de seguridad para añadir una regla de HTTPS de salida que habilite el tráfico hacia el extremo de S3. De lo contrario, la clasificación de BlueXP no podrá conectarse al servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿Por qué no se puede conectar a un bloque de S3 mediante un extremo VPC de puerta de enlace?"

Una alternativa es proporcionar la conexión utilizando una puerta de enlace NAT.

No se puede usar un proxy para acceder a S3 a través de Internet.

Implementar la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP en BlueXP" si aún no hay una instancia implementada.

Debe implementar la instancia con un conector puesto en marcha en AWS para que BlueXP detecte automáticamente los cubos de S3 de esta cuenta de AWS y los muestre en un entorno de trabajo de Amazon S3.

Nota: La implementación de la clasificación de BlueXP en una ubicación local no es compatible actualmente al analizar cubos S3.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

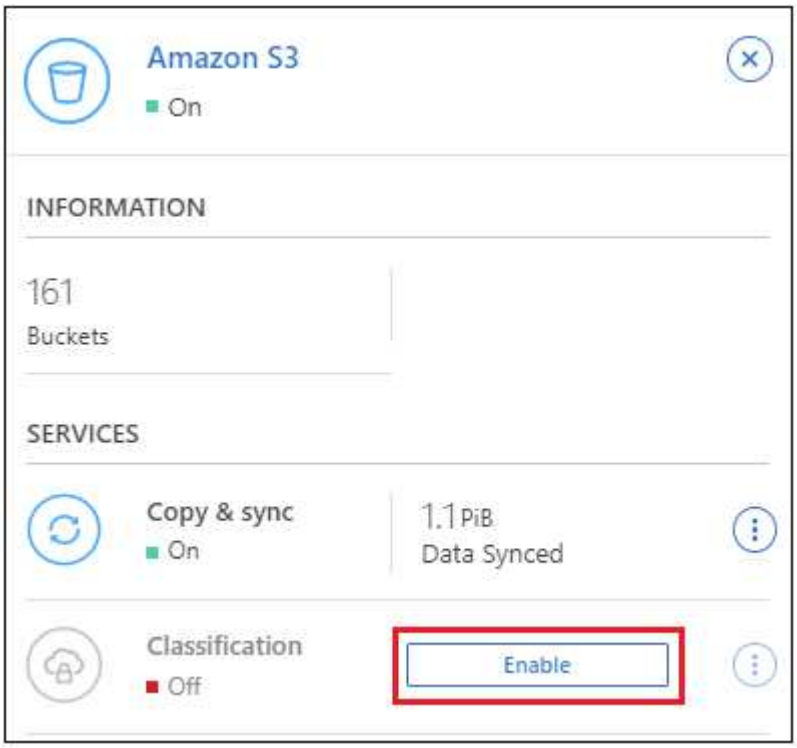
Activar la clasificación de BlueXP en tu entorno de trabajo S3

Habilita la clasificación de BlueXP en Amazon S3 después de verificar los requisitos previos.

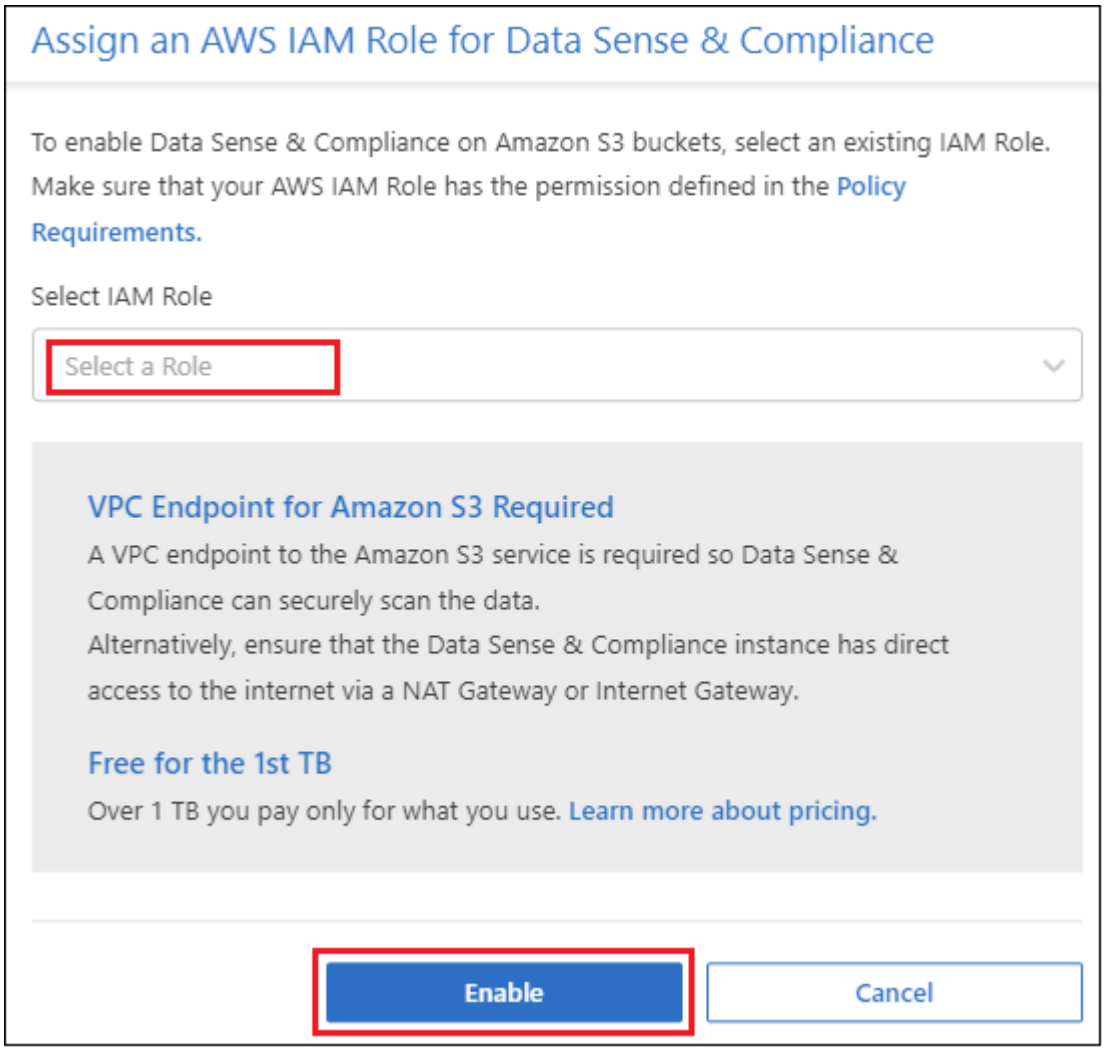
Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **almacenamiento > lienzo**.
2. Seleccione el entorno de trabajo de Amazon S3.

3. En el panel Servicios de la derecha, haga clic en **Activar** junto a **Clasificación**.



4. Cuando se le solicite, asigne un rol de IAM a la instancia de clasificación de BlueXP que tenga los permisos necesarios.



5. Haga clic en **Activar**.

> También puede habilitar análisis de cumplimiento de un entorno de trabajo desde la página Configuración haciendo clic en ⋮ Y seleccionando **Activar clasificación de BlueXP**.

Resultado

BlueXP asigna la función IAM a la instancia.

Habilitar y deshabilitar los análisis de cumplimiento de normativas en bloques S3

Después de que BlueXP habilita la clasificación de BlueXP en Amazon S3, el paso siguiente es configurar los bloques que quieres analizar.

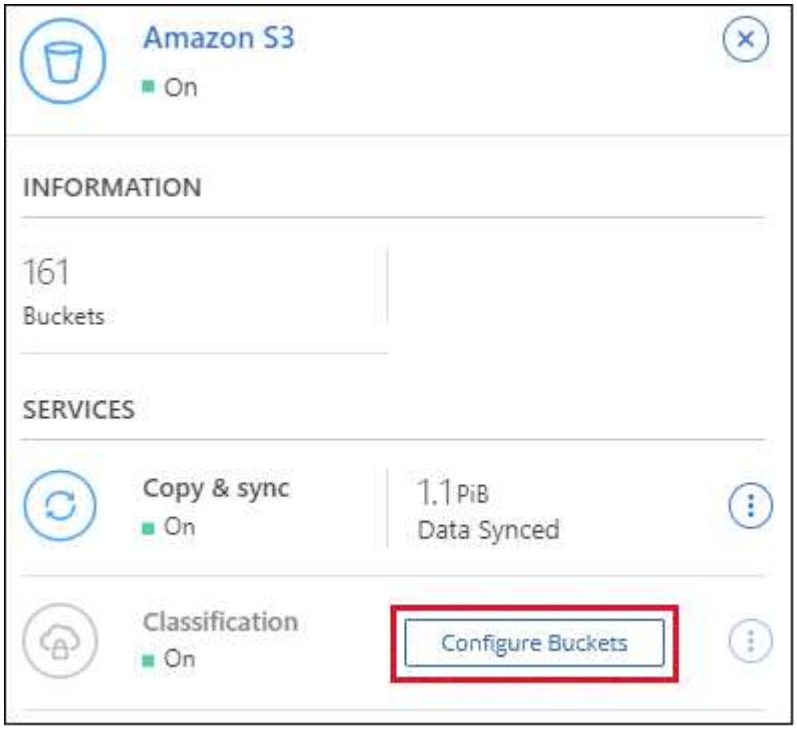
Cuando BlueXP se ejecuta en la cuenta de AWS que tiene los bloques de S3 que desea analizar, detecta esos bloques y los muestra en un entorno de trabajo de Amazon S3.

La clasificación de BlueXP también puede Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS.

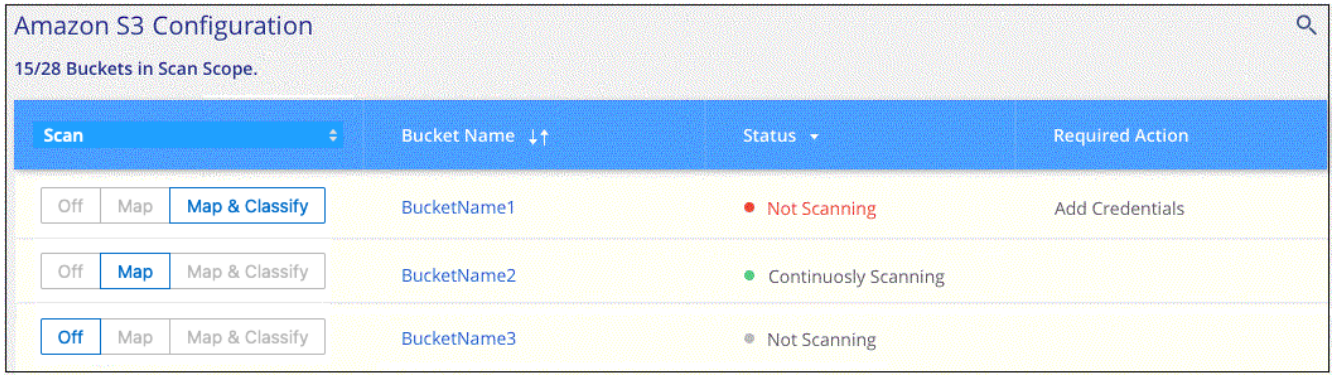
Pasos

1. Seleccione el entorno de trabajo de Amazon S3.

2. En el panel Servicios de la derecha, haga clic en **Configurar cucharones**.



3. Active escaneos de sólo asignación o escaneos de asignación y clasificación en los bloques.



Para:	Haga lo siguiente:
Habilite los análisis de sólo asignación en un bloque	Haga clic en **Mapa**
Activar exploraciones completas en un bloque	Haga clic en **Mapa y clasificación**
Desactivar el análisis en un bloque	Haga clic en **Desactivado**

Resultado

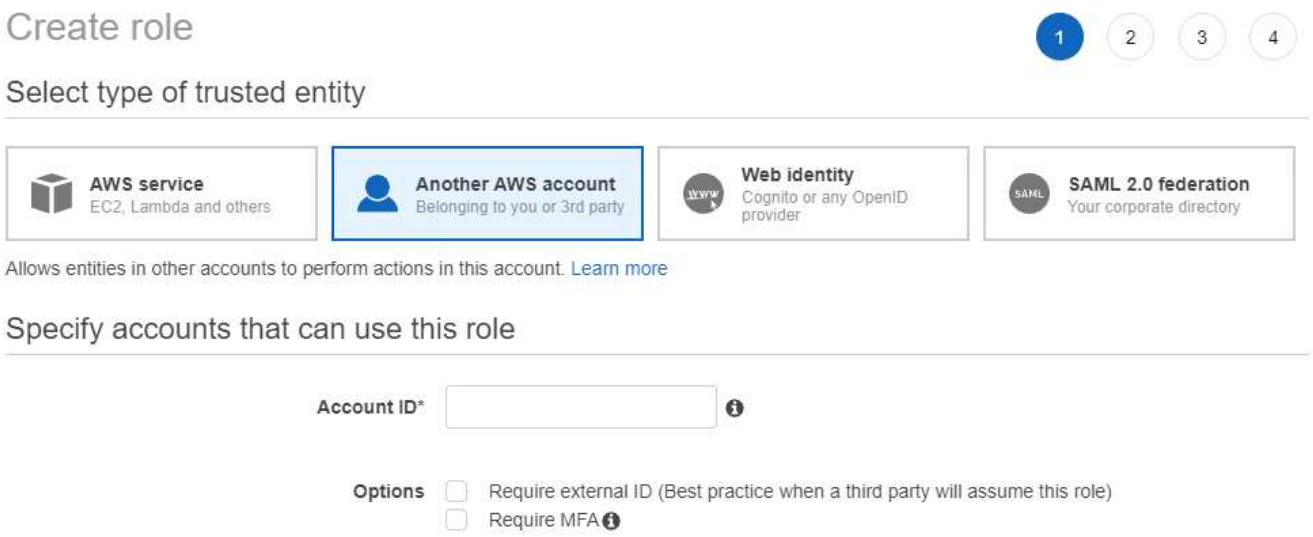
La clasificación de BlueXP comienza a analizar los bloques de S3 que has habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Escaneando bloques de cuentas de AWS adicionales

Puede analizar bloques de S3 que están con una cuenta de AWS diferente asignando un rol de esa cuenta para acceder a la instancia de clasificación existente de BlueXP.

Pasos

1. Vaya a la cuenta AWS de destino donde desee explorar bloques S3 y crear un rol IAM seleccionando **otra cuenta de AWS**.



   No olvide hacer lo siguiente:

   - Introduzca el ID de la cuenta en la que reside la instancia de clasificación de BlueXP.
   - Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
   - Adjunta la política de IAM de clasificación de BlueXP. Asegúrese de que tiene los permisos necesarios.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

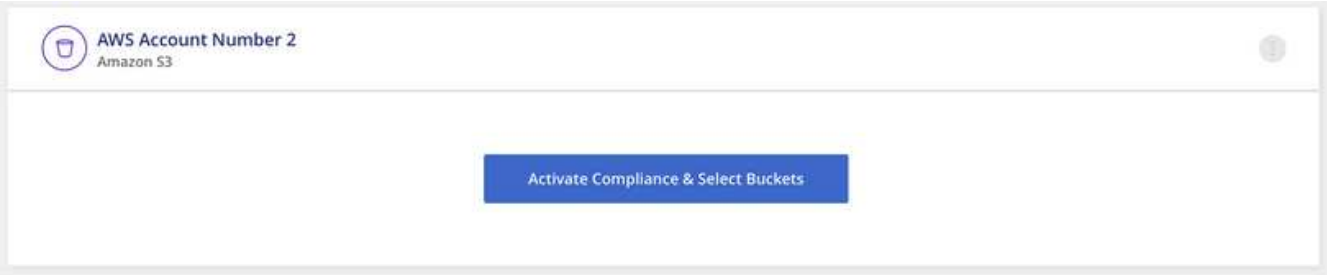
2. Ve a la cuenta de AWS de origen donde reside la instancia de clasificación de BlueXP y selecciona el rol IAM adjunto a la instancia.
   a. Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
   b. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.
   c. Cree una directiva que incluya la acción "sts:AssumeRole" y especifique el ARN del rol que creó en la

cuenta 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/*"
            ]
        }
    ]
}
```

La cuenta de perfil de instancia de clasificación de BlueXP ahora tiene acceso a la cuenta de AWS adicional.

3. Vaya a la página **Configuración de Amazon S3** y aparecerá la nueva cuenta de AWS. Ten en cuenta que la clasificación de BlueXP puede tardar unos minutos en sincronizar el entorno de trabajo de la nueva cuenta y mostrar esta información.



4. Haz clic en **Activar la clasificación de BlueXP y Select Buckets** y selecciona los bloques que deseas escanear.

Resultado

La clasificación de BlueXP comienza a analizar los nuevos bloques de S3 que ha habilitado.

Escanear esquemas de base de datos

Completa unos pasos para empezar a analizar tus esquemas de base de datos con la clasificación de BlueXP.

Tenga en cuenta que después de habilitar el análisis de bases de datos, puede agregar identificadores únicos que la clasificación de BlueXP identificará en todos sus orígenes de datos en función de columnas específicas de sus bases de datos. Esto se denomina función *Data Fusion*. "Aprenda a agregar identificadores de datos personales personalizados de sus bases de datos".

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Revisar los requisitos previos de la base de datos**

Asegúrese de que la base de datos es compatible y de que dispone de la información necesaria para conectarse a la base de datos.

2. **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Agregue el servidor de la base de datos**

Agregue el servidor de base de datos al que desea acceder.

4. **Seleccione los esquemas**

Seleccione los esquemas que desea analizar.

Revise los requisitos previos

Revise los siguientes requisitos previos para comprobar que tiene una configuración compatible antes de habilitar la clasificación de BlueXP.

Bases de datos compatibles

La clasificación de BlueXP puede analizar esquemas de las siguientes bases de datos:

- Servicio de bases de datos relacionales de Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA

- Servidor SQL (MSSQL)

> La característica de recopilación de estadísticas **debe estar activada** en la base de datos.

Requisitos de base de datos

Se puede analizar cualquier base de datos con conectividad a la instancia de clasificación de BlueXP, independientemente de dónde esté alojada. Sólo necesita la siguiente información para conectarse a la base de datos:

- Dirección IP o nombre de host
- Puerto
- Nombre del servicio (sólo para acceder a bases de datos Oracle)
- Credenciales que permiten el acceso de lectura a los esquemas

  Al seleccionar un nombre de usuario y una contraseña, es importante elegir uno que tenga permisos de lectura completos para todos los esquemas y tablas que desee analizar. Le recomendamos que cree un usuario dedicado para el sistema de clasificación de BlueXP con todos los permisos necesarios.

Nota: para MongoDB, se requiere una función de administrador de sólo lectura.

Implementa la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

Si está analizando esquemas de base de datos a los que se puede acceder a través de Internet, puede hacerlo "Pon en marcha la clasificación de BlueXP en el cloud" o. "Pon en marcha la clasificación de BlueXP en una ubicación on-premises que tenga acceso a Internet".

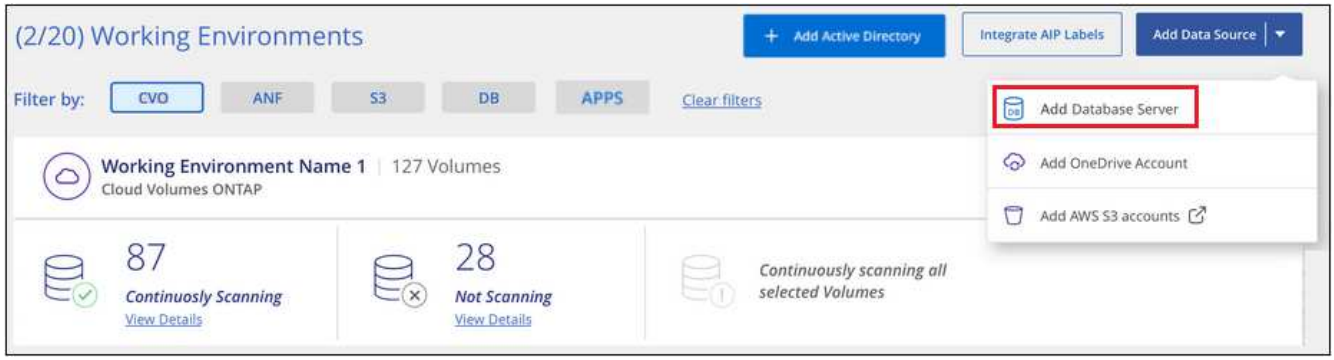
Si está analizando esquemas de base de datos que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Pon en marcha la clasificación de BlueXP en la misma ubicación on-premises que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

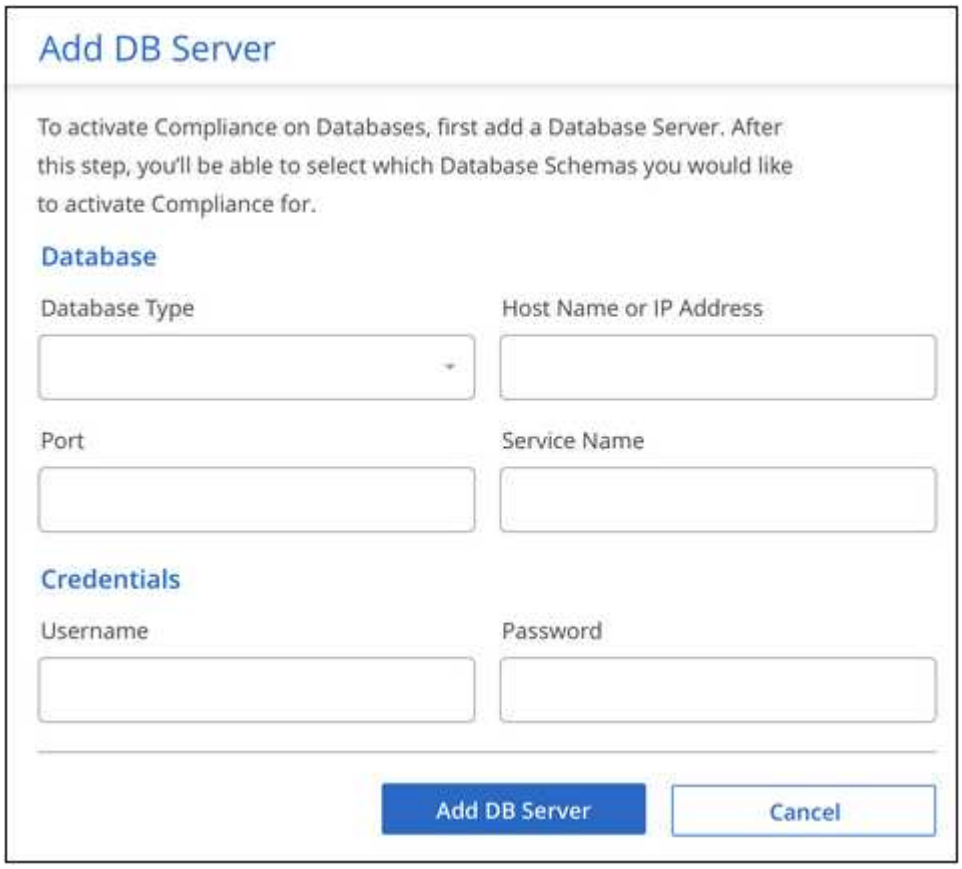
Agregue el servidor de la base de datos

Agregue el servidor de base de datos donde residen los esquemas.

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar servidor de base de datos**.



2. Introduzca la información necesaria para identificar el servidor de bases de datos.
   a. Seleccione el tipo de base de datos.
   b. Introduzca el puerto y el nombre de host o la dirección IP para conectarse a la base de datos.
   c. Para las bases de datos de Oracle, introduzca el nombre del servicio.
   d. Introduzca las credenciales para que la clasificación de BlueXP pueda acceder al servidor.
   e. Haga clic en **Agregar servidor de base de datos**.



La base de datos se agrega a la lista de entornos de trabajo.

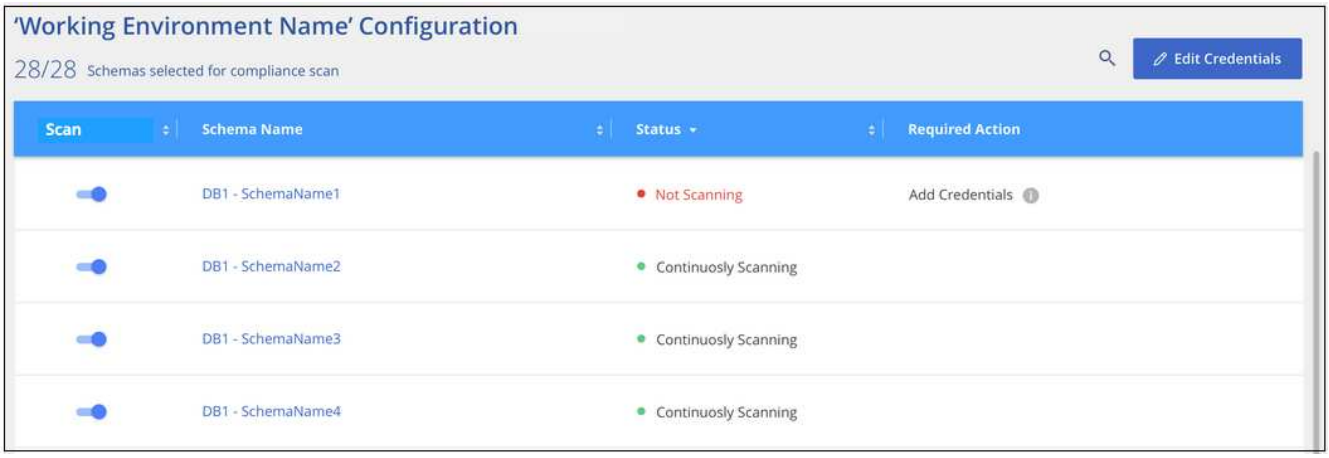
Activar y desactivar exploraciones de cumplimiento en esquemas de base de datos

Puede detener o iniciar el análisis completo de sus esquemas en cualquier momento.

No existe ninguna opción para seleccionar los análisis de sólo asignación para esquemas de base de datos.

1. En la página *Configuration*, haga clic en el botón **Configuration** de la base de datos que desea configurar.

2. Seleccione los esquemas que desea analizar moviendo el control deslizante hacia la derecha.



Resultado

La clasificación de BlueXP comienza a analizar los esquemas de base de datos que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Ten en cuenta que la clasificación de BlueXP analiza tus bases de datos una vez al día: Las bases de datos no se analizan continuamente, como otras fuentes de datos.

Analizando cuentas de OneDrive

Completa unos pasos para comenzar a escanear archivos en las carpetas de OneDrive de tu usuario con la clasificación de BlueXP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 **Revise los requisitos previos de OneDrive**

Compruebe que tiene las credenciales de administrador para iniciar sesión en la cuenta de OneDrive.

Implementa la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

Añada la cuenta de OneDrive

Con las credenciales de usuario de administrador, inicie sesión en la cuenta de OneDrive a la que desee acceder para que se agregue como nuevo entorno de trabajo.

Agregue los usuarios y seleccione el tipo de análisis

Agregue la lista de usuarios de la cuenta de OneDrive que desee analizar y seleccione el tipo de análisis. Puede añadir hasta 100 usuarios al mismo tiempo.

Revisión de los requisitos de OneDrive

Revise los siguientes requisitos previos para comprobar que tiene una configuración compatible antes de habilitar la clasificación de BlueXP.

- Debe tener las credenciales de inicio de sesión de administrador para la cuenta de OneDrive para la Empresa que proporcione acceso de lectura a los archivos del usuario.
- Necesitará una lista separada por líneas de las direcciones de correo electrónico para todos los usuarios cuyas carpetas de OneDrive desee analizar.

Implementar la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

La clasificación de BlueXP puede ser "implementado en el cloud" o. "en una ubicación en el hotel que tiene acceso a internet".

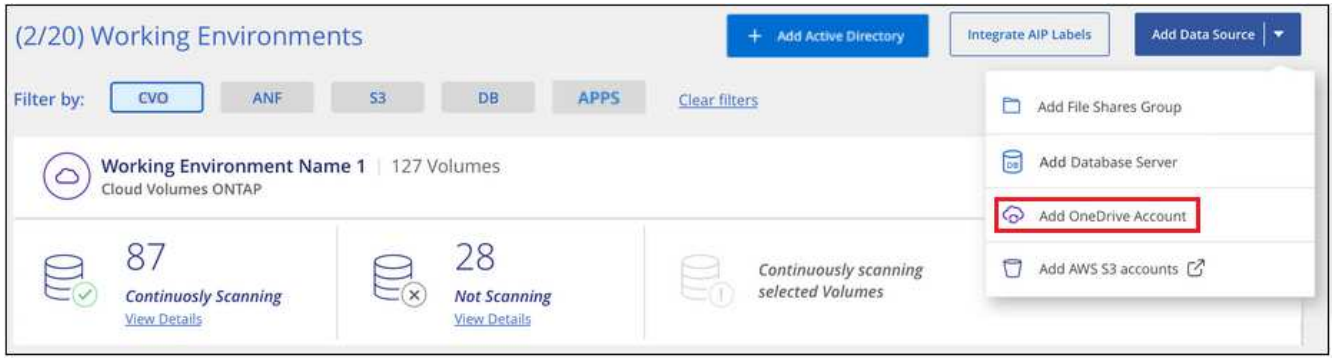
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Adición de la cuenta de OneDrive

Agregue la cuenta de OneDrive donde residen los archivos de usuario.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar cuenta de OneDrive**.



2. En el cuadro de diálogo Agregar cuenta de OneDrive, haga clic en **Iniciar sesión en OneDrive**.
3. En la página de Microsoft que aparece, selecciona la cuenta de OneDrive e introduce el usuario y la contraseña de administrador necesarios, luego haz clic en **Aceptar** para permitir que la clasificación de BlueXP lea los datos de esta cuenta.

La cuenta de OneDrive se agrega a la lista de entornos de trabajo.

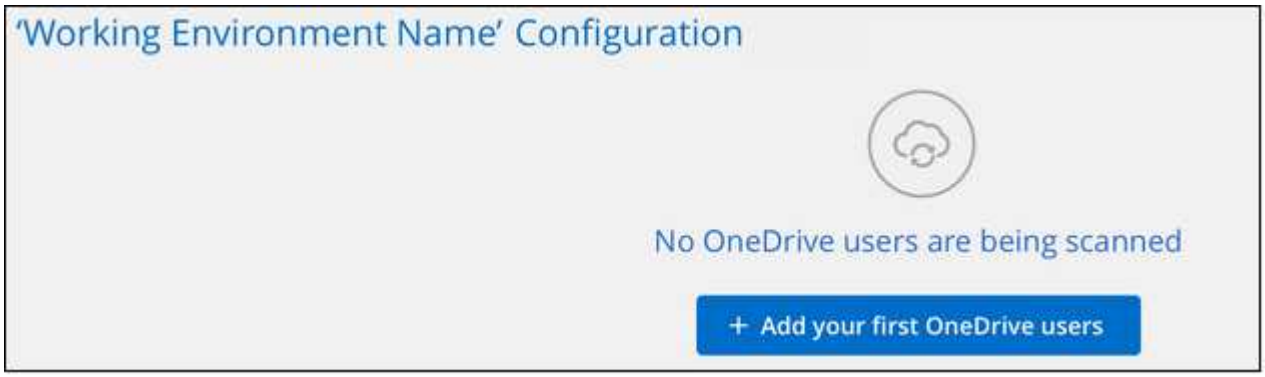
Añadir usuarios de OneDrive a los análisis de cumplimiento de normativas

Puede añadir usuarios individuales de OneDrive, o todos sus usuarios de OneDrive, de manera que sus archivos se analizarán mediante la clasificación de BlueXP.

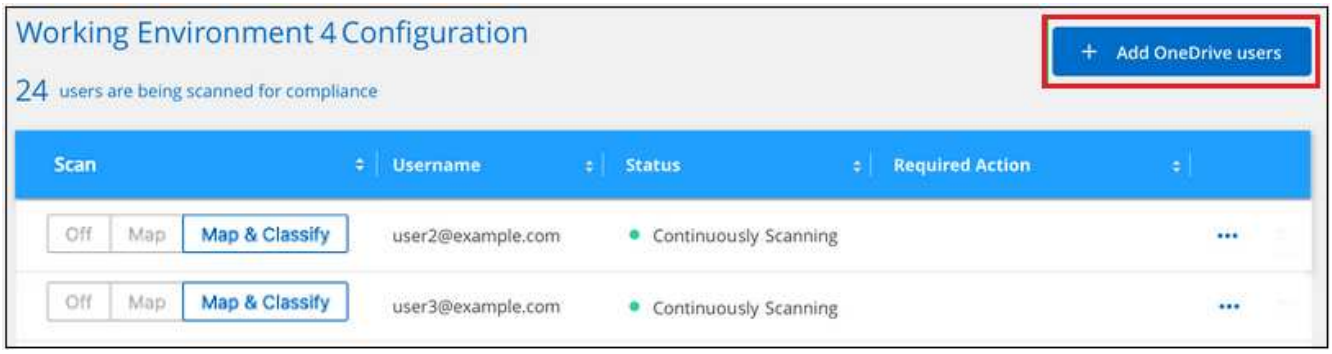
Pasos

1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de OneDrive.

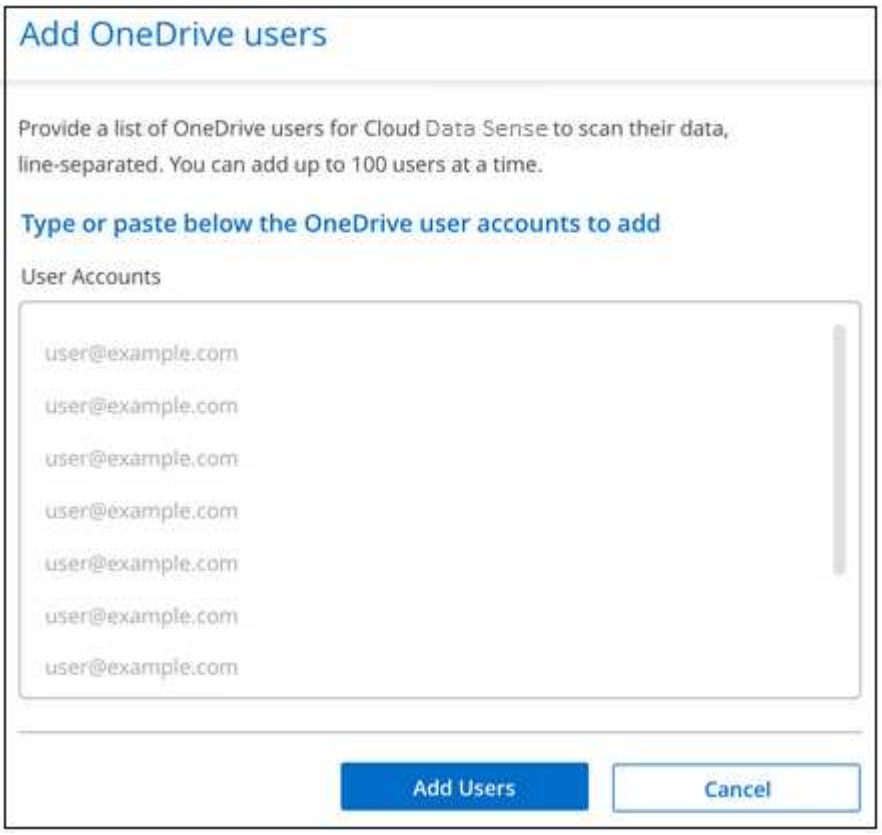
2. Si es la primera vez que añade usuarios para esta cuenta de OneDrive, haga clic en **Agregar sus primeros usuarios de OneDrive**.



Si va a agregar usuarios adicionales desde una cuenta de OneDrive, haga clic en **Agregar usuarios de OneDrive**.



3. Agregue las direcciones de correo electrónico de los usuarios cuyos archivos desea escanear - una dirección de correo electrónico por línea (hasta 100 máximo por sesión) - y haga clic en **Agregar usuarios**.



Un cuadro de diálogo de confirmación muestra el número de usuarios que se han agregado.

Si el cuadro de diálogo enumera los usuarios que no se han podido agregar, capture esta información para que pueda resolver el problema. En algunos casos, puede volver a agregar al usuario con una dirección de correo electrónico corregida.

4. Active análisis de sólo asignación o análisis de asignación y clasificación en archivos de usuario.

Para:	Haga lo siguiente:
Active los análisis de sólo asignación en los archivos de usuario	Haga clic en **Mapa**
Activar análisis completos en archivos de usuario	Haga clic en **Mapa y clasificación**

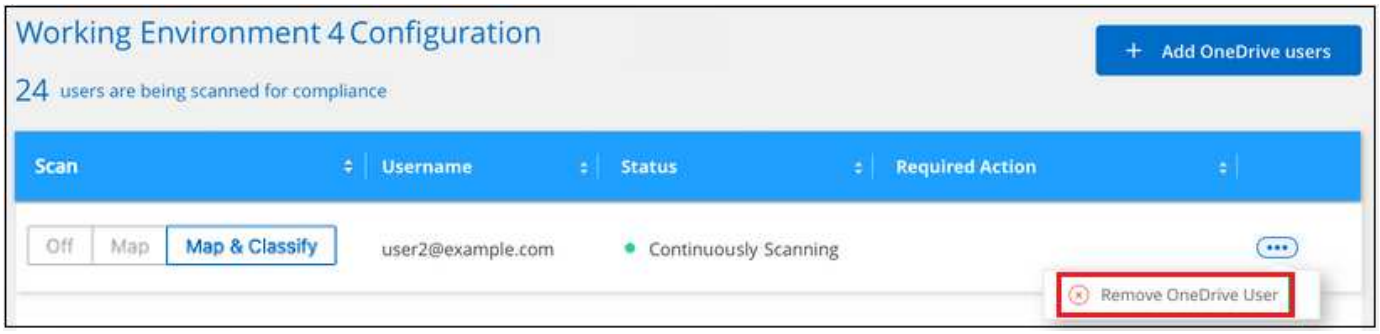
Para:	Haga lo siguiente:
Desactive el análisis en archivos de usuario	Haga clic en **Desactivado**

Resultado

La clasificación de BlueXP comienza a analizar los archivos para los usuarios que has añadido; los resultados se muestran en el Dashboard y en otras ubicaciones.

La eliminación de un usuario de OneDrive de los análisis de cumplimiento de normativas

Si dejan la compañía o cambia su dirección de correo electrónico, puede eliminar a usuarios individuales de OneDrive para que puedan analizar sus archivos en cualquier momento. Sólo tiene que hacer clic en **Eliminar usuario de OneDrive** en la página Configuración.



Tenga en cuenta que puede "Elimina toda la cuenta de OneDrive de la clasificación de BlueXP" Si ya no desea analizar ningún dato de usuario desde la cuenta de OneDrive.

Analizando cuentas de SharePoint

Complete unos pasos para empezar a analizar archivos en sus cuentas on-premise de SharePoint Online y SharePoint con clasificación de BlueXP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Revise los requisitos previos de SharePoint**

Asegúrese de que tiene credenciales completas para iniciar sesión en la cuenta de SharePoint y de que tiene las direcciones URL de los sitios de SharePoint que desea analizar.

2. **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Inicie sesión en la cuenta de SharePoint**

Con credenciales de usuario completas, inicie sesión en la cuenta de SharePoint a la que desea acceder para que se agregue como nuevo origen de datos/entorno de trabajo.

4 Agregue las direcciones URL del sitio de SharePoint que desea analizar

Agregue la lista de direcciones URL del sitio de SharePoint que desea analizar en la cuenta de SharePoint y seleccione el tipo de análisis. Puede agregar hasta 100 URL a la vez, y hasta 1.000 sitios en total por cada cuenta.

Revisar los requisitos de SharePoint

Revisa los siguientes requisitos previos para asegurarte de que estás listo para activar la clasificación BlueXP en una cuenta de SharePoint.

- Debe tener las credenciales de inicio de sesión de usuario administrador para la cuenta de SharePoint que proporciona acceso de lectura a todos los sitios de SharePoint.
  - Para SharePoint Online puede utilizar una cuenta que no sea de administrador, pero ese usuario debe tener permiso para tener acceso a todos los sitios de SharePoint que desea analizar.
- Para SharePoint en las instalaciones, también necesitará la dirección URL de SharePoint Server.
- Necesitará una lista separada por líneas de las direcciones URL del sitio de SharePoint para todos los datos que desee analizar.

Implementar la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

- Para SharePoint Online, la clasificación de BlueXP puede ser "implementado en el cloud".
- En el caso de SharePoint en las instalaciones, se puede instalar la clasificación de BlueXP "en una ubicación en el hotel que tiene acceso a internet" o. "en una ubicación en el hotel que no tiene acceso a internet".

Cuando se instala la clasificación de BlueXP en un sitio sin acceso a Internet, también se debe instalar BlueXP Connector en ese mismo sitio sin acceso a Internet. "Leer más".

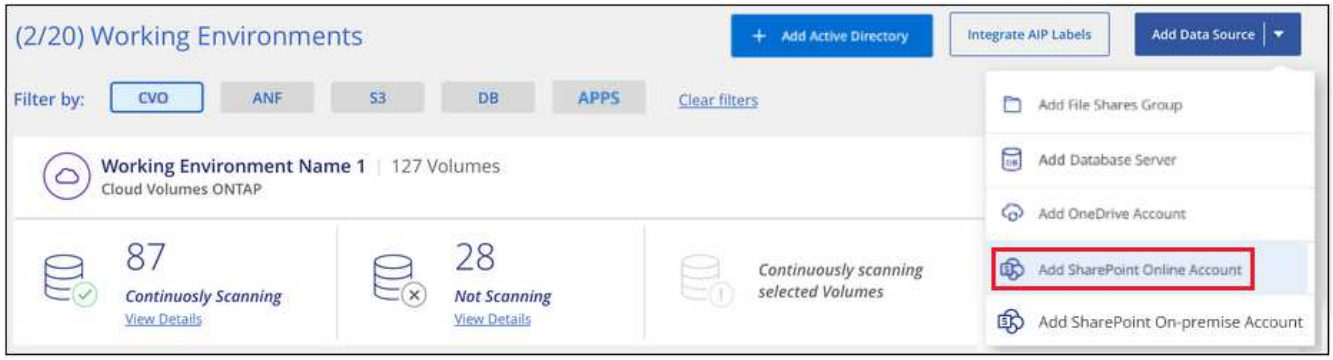
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Agregar una cuenta de SharePoint Online

Agregue la cuenta de SharePoint Online donde residen los archivos de usuario.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar cuenta en línea de SharePoint**.



2. En el cuadro de diálogo Agregar una cuenta en línea de SharePoint, haga clic en **Iniciar sesión en SharePoint**.
3. En la página de Microsoft que aparece, seleccione la cuenta de SharePoint e introduzca el usuario y la contraseña (usuario administrador u otro usuario con acceso a los sitios de SharePoint) y, a continuación, haga clic en **Aceptar** para permitir que la clasificación de BlueXP lea los datos de esta cuenta.

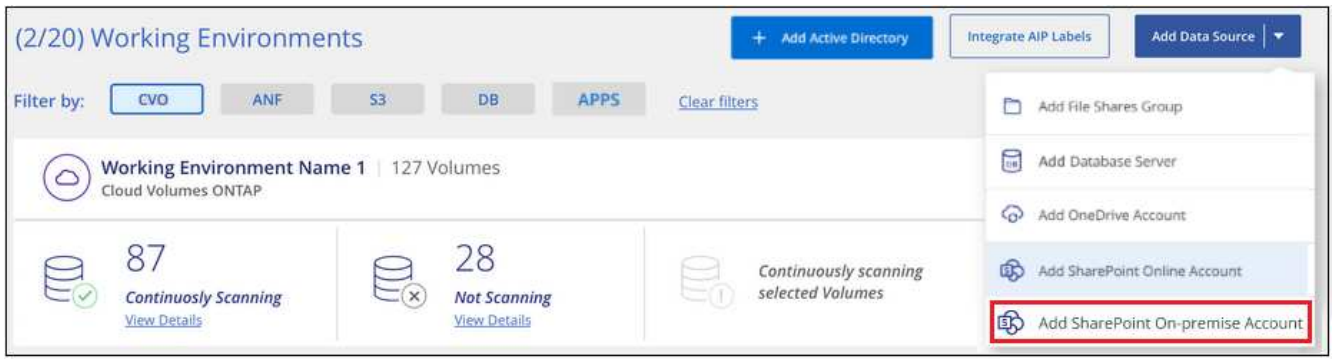
La cuenta de SharePoint Online se agrega a la lista de entornos de trabajo.

Adición de una cuenta de SharePoint en las instalaciones

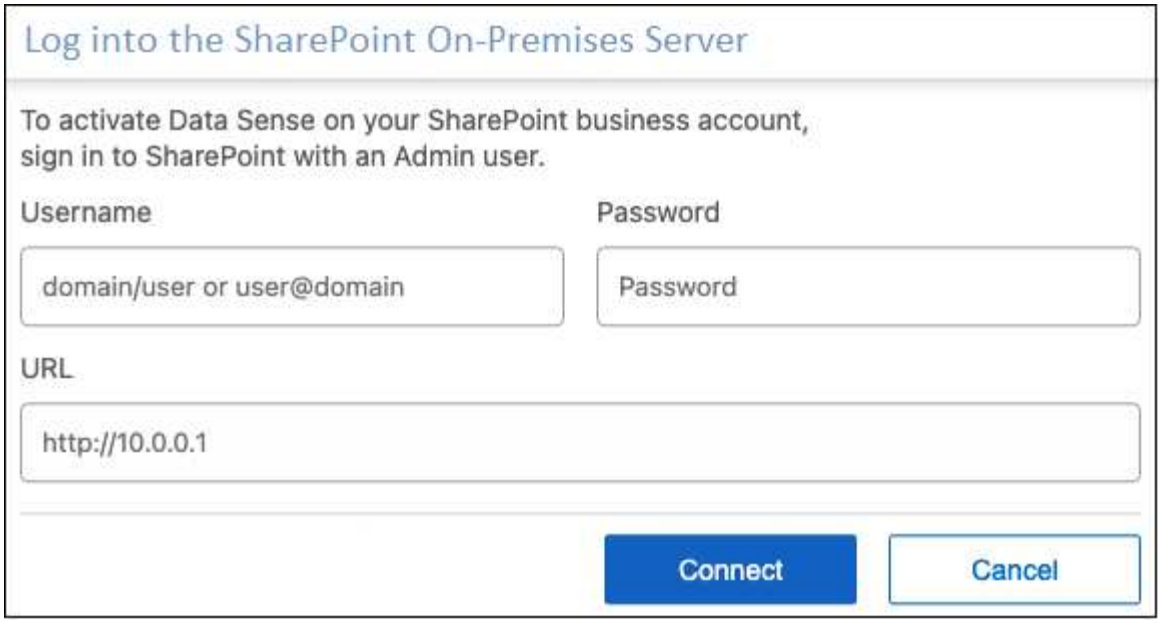
Agregue la cuenta de SharePoint en las instalaciones donde residen los archivos de usuario.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar cuenta de SharePoint en las instalaciones**.



2. En el cuadro de diálogo Iniciar sesión en el servidor local de SharePoint, introduzca la siguiente información:
   - Usuario administrador con el formato "dominio/usuario" o "usuario@dominio" y contraseña de administrador
   - URL de SharePoint Server



3. Haga clic en **conectar**.

La cuenta de SharePoint en las instalaciones se agrega a la lista de entornos de trabajo.

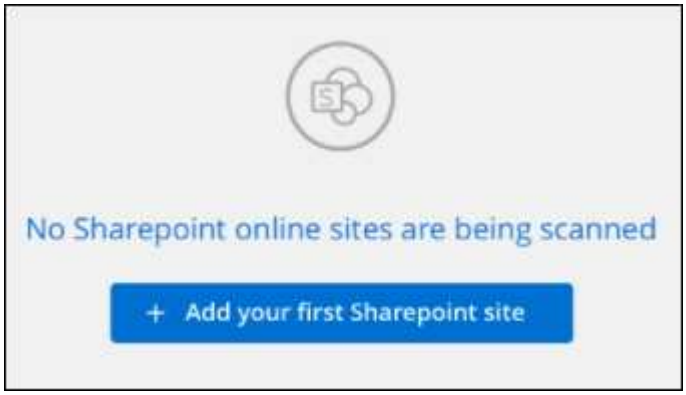
Agregar sitios de SharePoint a los análisis de cumplimiento

Puede añadir sitios de SharePoint individuales, o hasta 1.000 sitios de SharePoint en la cuenta, de modo que la clasificación de BlueXP analice los archivos asociados. Los pasos son los mismos si agrega sitios de SharePoint Online o de SharePoint en las instalaciones.

Pasos

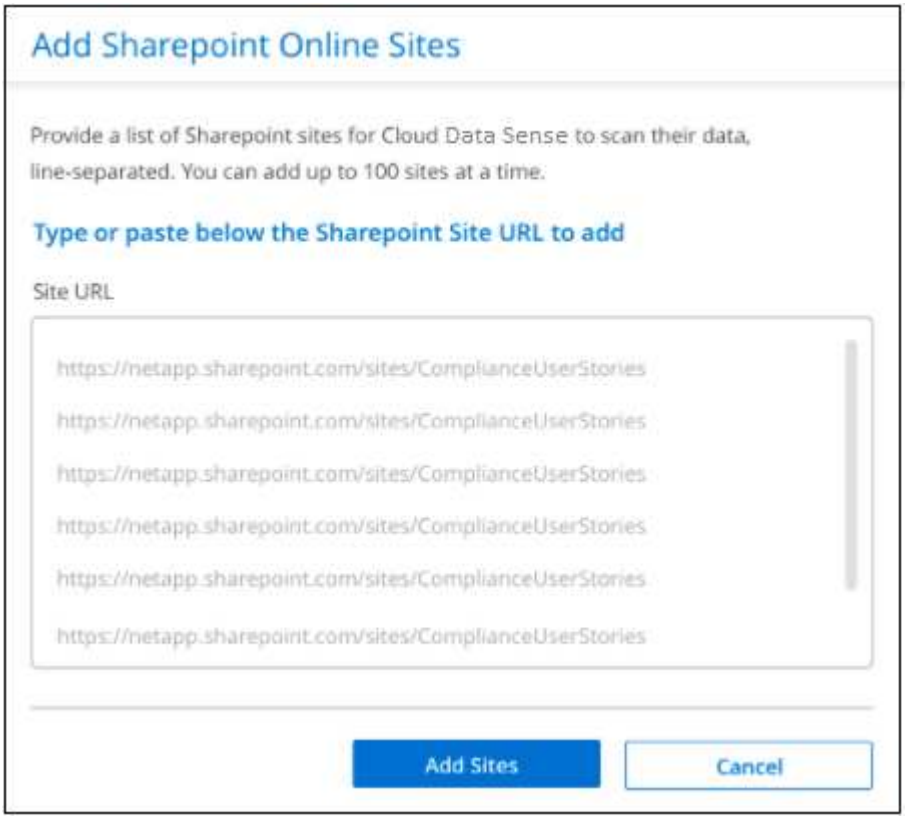
1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de SharePoint.

2. Si es la primera vez que agrega sitios para esta cuenta de SharePoint, haga clic en **Agregar su primer sitio de SharePoint**.



Si va a agregar usuarios adicionales desde una cuenta de SharePoint, haga clic en **Agregar sitios de SharePoint**.

3. Agregue las direcciones URL de los sitios cuyos archivos desea explorar - una dirección URL por línea (hasta un máximo de 100 por sesión) - y haga clic en **Agregar sitios**.



Un cuadro de diálogo de confirmación muestra el número de sitios que se han agregado.

Si el cuadro de diálogo enumera los sitios que no se han podido agregar, capture esta información para que pueda resolver el problema. En algunos casos, puede volver a agregar el sitio con una dirección URL corregida.

4. Si necesita agregar más de 100 sitios para esta cuenta, simplemente haga clic en **Agregar sitios de SharePoint** nuevamente hasta que haya agregado todos sus sitios para esta cuenta (hasta 1.000 sitios en total para cada cuenta).
5. Habilite los análisis de sólo asignación, o los análisis de asignación y clasificación, en los archivos de los sitios de SharePoint.

Para:	Haga lo siguiente:
Active los análisis de sólo asignación en archivos	Haga clic en **Mapa**

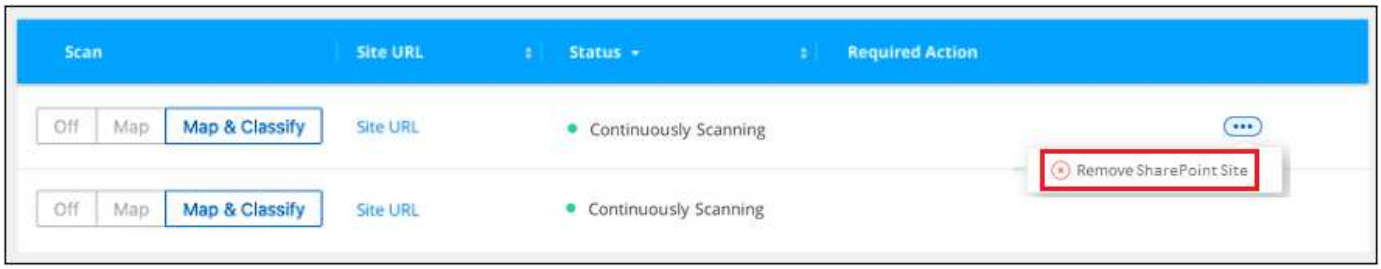
Para:	Haga lo siguiente:
Active los análisis completos en los archivos	Haga clic en **Mapa y clasificación**
Desactive el análisis en archivos	Haga clic en **Desactivado**

Resultado

La clasificación de BlueXP comienza a analizar los archivos en los sitios de SharePoint que ha agregado y los resultados se muestran en el Dashboard y en otras ubicaciones.

Quitar un sitio de SharePoint de los análisis de cumplimiento

Si quita un sitio de SharePoint en el futuro o decide no analizar archivos en un sitio de SharePoint, puede eliminar sitios de SharePoint individuales para que sus archivos se analicen en cualquier momento. Haga clic en **Quitar sitio de SharePoint** de la página Configuración.



Tenga en cuenta que puede "Elimina toda la cuenta de SharePoint de la clasificación de BlueXP" Si ya no desea analizar los datos de usuario desde la cuenta de SharePoint.

Analizando cuentas de Google Drive

Completa unos pocos pasos para comenzar a escanear archivos de usuario en tus cuentas de Google Drive con la clasificación de BlueXP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Revise los requisitos previos de Google Drive**

Asegúrese de que tiene las credenciales de administrador para iniciar sesión en la cuenta de Google Drive.

2. **Implementa la clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Inicie sesión en la cuenta de Google Drive**

Con las credenciales de usuario Admin, inicie sesión en la cuenta de Google Drive a la que desee acceder para que se agregue como nuevo origen de datos.

4 Seleccione el tipo de análisis de los archivos de usuario

Seleccione el tipo de análisis que desea realizar en los archivos de usuario; asignación o asignación y clasificación.

Revisión de los requisitos de Google Drive

Revisa los siguientes requisitos previos para asegurarte de estar listo para habilitar la clasificación BlueXP en una cuenta de Google Drive.

- Debe tener las credenciales de inicio de sesión de administrador para la cuenta de Google Drive que proporciona acceso de lectura a los archivos del usuario

Restricciones actuales

Las siguientes funciones de clasificación de BlueXP no son compatibles con los archivos de Google Drive actualmente:

- Al ver archivos en la página Investigación de datos, las acciones de la barra de botones no están activas. No puede copiar, mover, eliminar, etc. ningún archivo.
- Los permisos no se pueden identificar dentro de los archivos de Google Drive, por lo que no se muestra ninguna información de permisos en la página Investigación.

Implementando la clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

La clasificación de BlueXP puede ser "implementado en el cloud" o. "en una ubicación en el hotel que tiene acceso a internet".

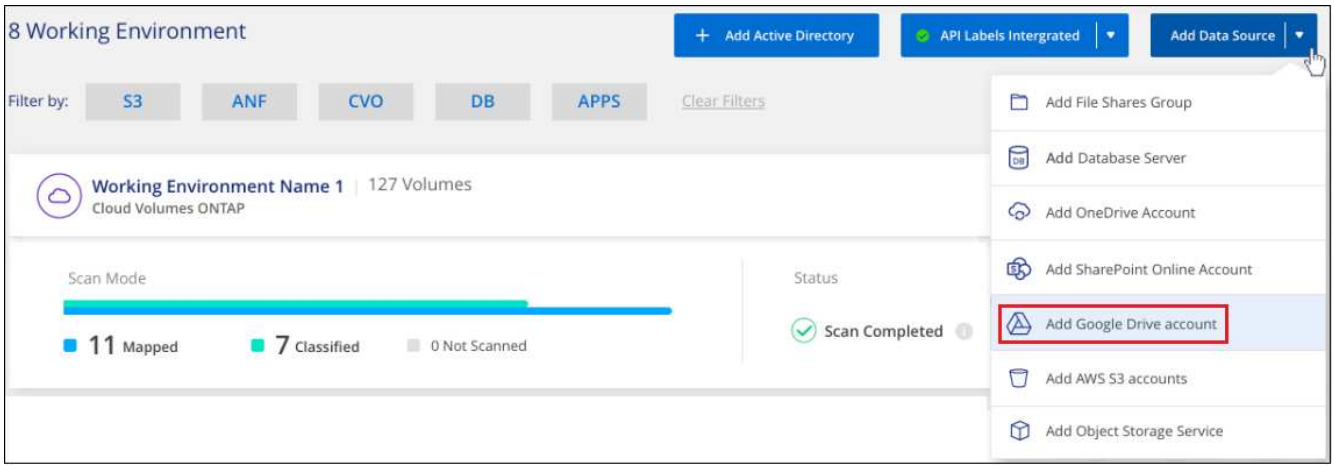
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Adición de la cuenta de Google Drive

Agregue la cuenta de Google Drive donde residen los archivos de usuario. Si desea analizar archivos de varios usuarios, tendrá que realizar este paso para cada usuario.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar cuenta de Google Drive**.



2. En el cuadro de diálogo Agregar una cuenta de Google Drive, haga clic en **Iniciar sesión en Google Drive**.
3. En la página de Google que aparece, selecciona la cuenta de Google Drive e introduce el usuario Admin y la contraseña necesarios, luego haz clic en **Aceptar** para permitir que la clasificación de BlueXP lea los datos de esta cuenta.

La cuenta de Google Drive se añade a la lista de entornos de trabajo.

Selección del tipo de análisis para los datos del usuario

Seleccione el tipo de análisis que realizará la clasificación de BlueXP en los datos del usuario.

Pasos

1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de Google Drive.

2. Active análisis de sólo asignación o análisis de asignación y clasificación en los archivos de la cuenta de Google Drive.

Para:	Haga lo siguiente:
Active los análisis de sólo asignación en archivos	Haga clic en **Mapa**
Active los análisis completos en los archivos	Haga clic en **Mapa y clasificación**
Desactive el análisis en archivos	Haga clic en **Desactivado**

Resultado

La clasificación de BlueXP comienza a analizar los archivos en la cuenta de Google Drive que agregaste y los resultados se muestran en el Dashboard y en otras ubicaciones.

Eliminación de una cuenta de Google Drive de los análisis de cumplimiento

Dado que sólo los archivos de Google Drive de un solo usuario forman parte de una única cuenta de Google Drive, si desea detener el análisis de archivos desde la cuenta de Google Drive de un usuario, entonces debería hacerlo "Elimina la cuenta de Google Drive de la clasificación de BlueXP".

Analizando recursos compartidos de archivos

Completa unos pasos para empezar a analizar recursos compartidos de archivos NFS o CIFS que no sean de NetApp directamente con la clasificación de BlueXP. Estos recursos compartidos de archivos pueden residir en las instalaciones o en el cloud.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1. **Revise los requisitos previos para compartir archivos**

Para los recursos compartidos CIFS (SMB), asegúrese de tener credenciales para acceder a los recursos compartidos.

2. **Implementa la instancia de clasificación de BlueXP**

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3. **Cree un grupo que contenga los recursos compartidos de archivos**

El grupo es un contenedor para los recursos compartidos de archivos que desea analizar y se utiliza como nombre del entorno de trabajo para esos archivos compartidos.

4. **Añada los recursos compartidos de archivos al grupo**

Agregue la lista de recursos compartidos de archivos que desea analizar y seleccione el tipo de análisis. Puede añadir hasta 100 archivos compartidos a la vez.

Revisión de los requisitos de uso compartido de archivos

Revise los siguientes requisitos previos para comprobar que tiene una configuración compatible antes de habilitar la clasificación de BlueXP.

- Los recursos compartidos se pueden alojar en cualquier lugar, incluso en el cloud o en las instalaciones. En la mayoría de los casos se trata de recursos compartidos de archivos que se encuentran en sistemas de almacenamiento que no son de NetApp. Sin embargo, los recursos compartidos de CIFS de los antiguos sistemas de almacenamiento NetApp 7-Mode se pueden analizar como recursos compartidos de archivos.

Tenga en cuenta que la clasificación de BlueXP no puede extraer permisos ni la «última hora de acceso» de los sistemas 7-Mode. Además, debido a un problema conocido entre algunas versiones de Linux y recursos compartidos CIFS en sistemas 7-Mode, debe configurar el recurso compartido para que utilice solo SMB v1 con la autenticación NTLM habilitada.

- Es necesario que haya conectividad de red entre la instancia de clasificación de BlueXP y los recursos compartidos.
- Asegúrate de que estos puertos estén abiertos a la instancia de clasificación de BlueXP:
  - Para NFS, puertos 111 y 2049.
  - Para CIFS, puertos 139 y 445.
- Puede agregar un recurso compartido DFS (sistema de archivos distribuidos) como un recurso compartido de CIFS normal. Sin embargo, como la clasificación de BlueXP no sabe que el recurso compartido se crea en varios servidores o volúmenes combinados como un único recurso compartido de CIFS, puede que reciba errores de permiso o conectividad sobre el recurso compartido cuando el mensaje solo se aplica a una de las carpetas o recursos compartidos que está ubicada en un servidor o volumen diferente.
- En el caso de los recursos compartidos CIFS (SMB), asegúrese de tener credenciales de Active Directory con acceso de lectura a los recursos compartidos. Se prefieren las credenciales de administrador en caso de que la clasificación de BlueXP deba analizar cualquier dato que requiera permisos elevados.

  Si quieres asegurarte de que las «horas de último acceso» no cambian debido a los análisis de clasificación de BlueXP, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

- Necesitará la lista de recursos compartidos que desea añadir en el formato `<host_name>:/<share_path>`. Puede introducir los recursos compartidos individualmente o proporcionar una lista separada por líneas de los recursos compartidos de archivos que desea escanear.

Implementar la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

Si va a analizar recursos compartidos de archivos NFS o CIFS de otros proveedores a los que se puede acceder a través de Internet, puede hacerlo "Pon en marcha la clasificación de BlueXP en el cloud" o. "Pon en marcha la clasificación de BlueXP en una ubicación on-premises que tenga acceso a Internet".

Si va a escanear recursos compartidos de archivos NFS o CIFS que no son de NetApp y que se han instalado en un sitio oscuro que no tiene acceso a Internet, necesita hacerlo "Pon en marcha la clasificación de BlueXP en la misma ubicación on-premises que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Creación del grupo para los recursos compartidos de archivos

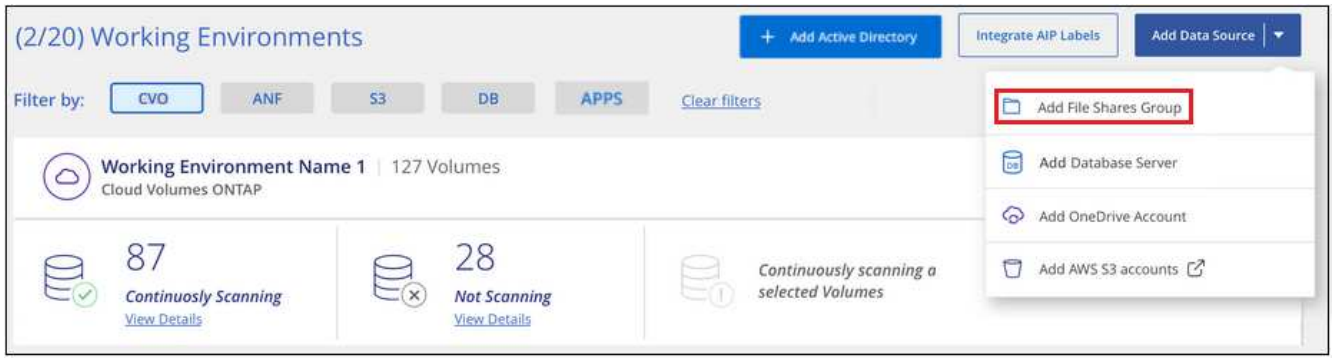
Debe agregar un "grupo" de archivos compartidos antes de poder agregar los archivos compartidos. El grupo es un contenedor para los recursos compartidos de archivos que desea analizar y el nombre del grupo se utiliza como nombre del entorno de trabajo para esos archivos compartidos.

Puede mezclar los recursos compartidos de NFS y CIFS en el mismo grupo, sin embargo, todos los recursos compartidos de archivos CIFS de un grupo deben utilizar las mismas credenciales de Active Directory. Si va a

añadir recursos compartidos CIFS que utilizan credenciales diferentes, debe crear un grupo independiente para cada conjunto único de credenciales.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar grupo de recursos compartidos de archivos**.



2. En el cuadro de diálogo Agregar grupo de recursos compartidos de archivos, introduzca el nombre del grupo de recursos compartidos y haga clic en **continuar**.

El nuevo grupo de archivos compartidos se agrega a la lista de entornos de trabajo.

Agregar recursos compartidos de archivos a un grupo

Añades archivos compartidos al grupo File Shares para que los archivos de esos recursos compartidos se analicen mediante la clasificación de BlueXP. Los recursos compartidos se añaden con el formato `<host_name>:/<share_path>`.

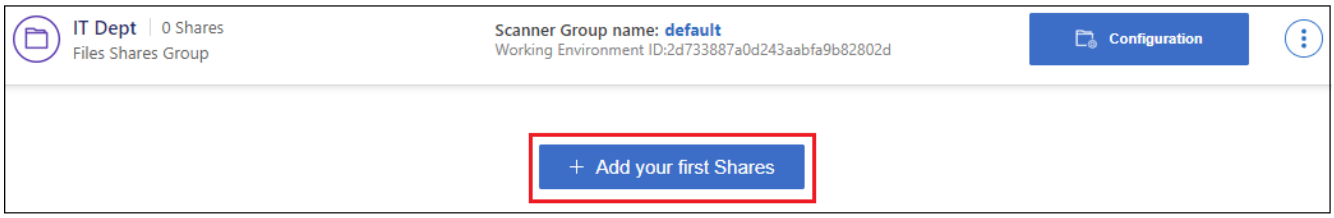
Puede agregar recursos compartidos de archivos individuales o puede proporcionar una lista separada por líneas de los recursos compartidos de archivos que desea analizar. Puede añadir hasta 100 recursos compartidos al mismo tiempo.

Al añadir ambos recursos compartidos NFS y CIFS en un único grupo, deberá realizar el proceso dos veces, una vez que añada recursos compartidos NFS y, a continuación, vuelva a añadir los recursos compartidos CIFS.

Pasos

1. En la página *Working Environments*, haga clic en el botón **Configuración** del grupo de recursos compartidos de archivos.

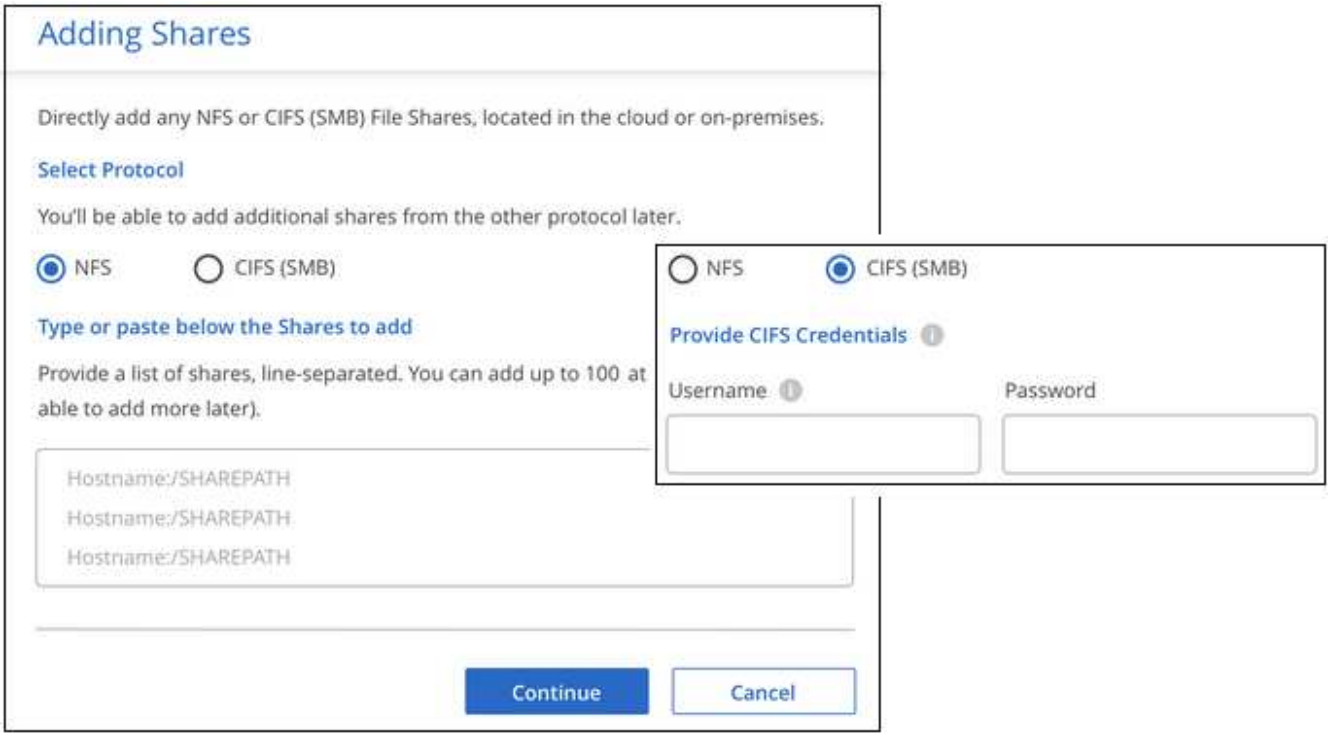
2. Si es la primera vez que añade archivos compartidos para este grupo de archivos compartidos, haga clic en **Agregar sus primeros recursos compartidos**.



Si va a agregar archivos compartidos a un grupo existente, haga clic en **Agregar recursos compartidos**.

3. Seleccione el protocolo para los recursos compartidos de archivos que va a agregar, agregue los recursos compartidos de archivos que desea analizar - un recurso compartido de archivos por línea - y haga clic en **continuar**.

   Cuando se añaden recursos compartidos CIFS (SMB), debe introducir las credenciales de Active Directory con acceso de lectura a los recursos compartidos. Se prefieren las credenciales de administrador.



Un cuadro de diálogo de confirmación muestra el número de recursos compartidos que se han añadido.

Si el cuadro de diálogo enumera los recursos compartidos que no se han podido agregar, capture esta información para que pueda resolver el problema. En algunos casos, es posible volver a añadir el recurso compartido con un nombre de host o un nombre de recurso compartido corregidos.

4. Active análisis de sólo asignación o análisis de asignación y clasificación en cada recurso compartido de archivos.

Para:	Haga lo siguiente:
Active análisis de sólo asignación en recursos compartidos de archivos	Haga clic en **Mapa**
Active análisis completos en recursos compartidos de archivos	Haga clic en **Mapa y clasificación**
Desactive el análisis en recursos compartidos de archivos	Haga clic en **Desactivado**

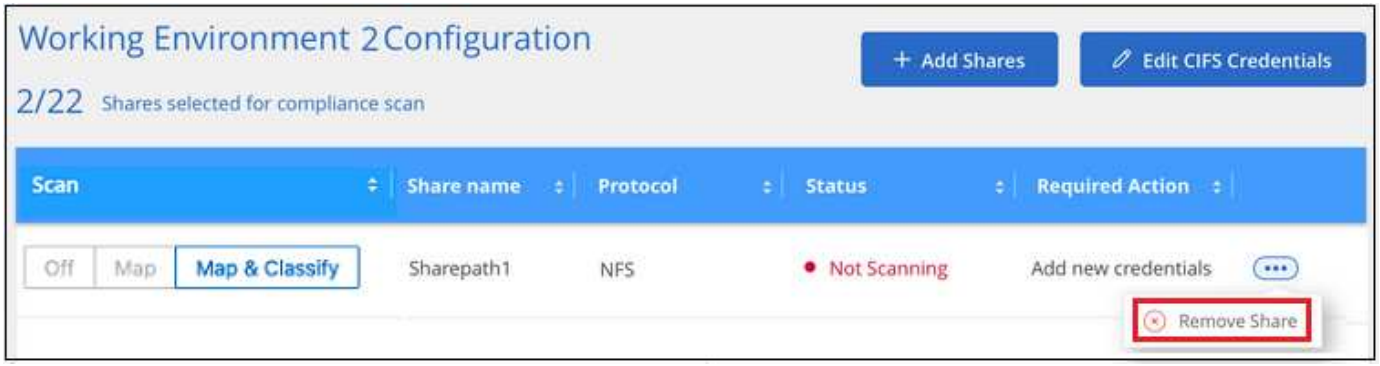
El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que, si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos, ya que la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".

Resultado

La clasificación de BlueXP comienza a analizar los archivos en los recursos compartidos de archivos que ha añadido y los resultados se muestran en la consola y en otras ubicaciones.

Quitar un recurso compartido de archivos de los análisis de cumplimiento de normativas

Si ya no necesita analizar determinados recursos compartidos de archivos, puede eliminar los recursos compartidos de archivos individuales para que los analice en cualquier momento. Haga clic en **Quitar recurso compartido** en la página Configuración.



Analizando el almacenamiento de objetos que utiliza el protocolo S3

Completa unos pasos para empezar a analizar datos en el almacenamiento de objetos directamente con la clasificación de BlueXP. La clasificación de BlueXP puede analizar datos de cualquier servicio de almacenamiento de objetos que use el protocolo Simple Storage Service (S3). Entre ellas se incluyen NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3, etc.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Revise los requisitos previos de almacenamiento del objeto

Debe tener la URL del extremo para conectarse con el servicio de almacenamiento de objetos.

Debe tener la clave de acceso y la clave secreta del proveedor de almacenamiento de objetos para que la clasificación de BlueXP pueda acceder a los bloques.

2 Implementa la instancia de clasificación de BlueXP

"Implementa la clasificación de BlueXP" si aún no hay una instancia implementada.

3 Añada el servicio de almacenamiento de objetos

Añade el servicio de almacenamiento de objetos a la clasificación de BlueXP.

4 Seleccione los cucharones que desea escanear

Selecciona los bloques que quieres escanear y la clasificación de BlueXP comenzará a escanearlos.

Revisión de requisitos de almacenamiento de objetos

Revise los siguientes requisitos previos para comprobar que tiene una configuración compatible antes de habilitar la clasificación de BlueXP.

- Debe tener la URL del extremo para conectarse con el servicio de almacenamiento de objetos.
- Debe tener la clave de acceso y la clave secreta del proveedor de almacenamiento de objetos para que la clasificación de BlueXP pueda acceder a los bloques.

Implementar la instancia de clasificación de BlueXP

Pon en marcha la clasificación de BlueXP si aún no hay una instancia implementada.

Si va a analizar datos de un almacenamiento de objetos S3 al que se puede acceder a través de Internet, puede hacerlo "Pon en marcha la clasificación de BlueXP en el cloud" o. "Pon en marcha la clasificación de BlueXP en una ubicación on-premises que tenga acceso a Internet".

Si va a analizar datos del almacenamiento de objetos S3 que se ha instalado en un sitio oscuro que no tiene acceso a Internet, deberá hacerlo "Pon en marcha la clasificación de BlueXP en la misma ubicación on-premises que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

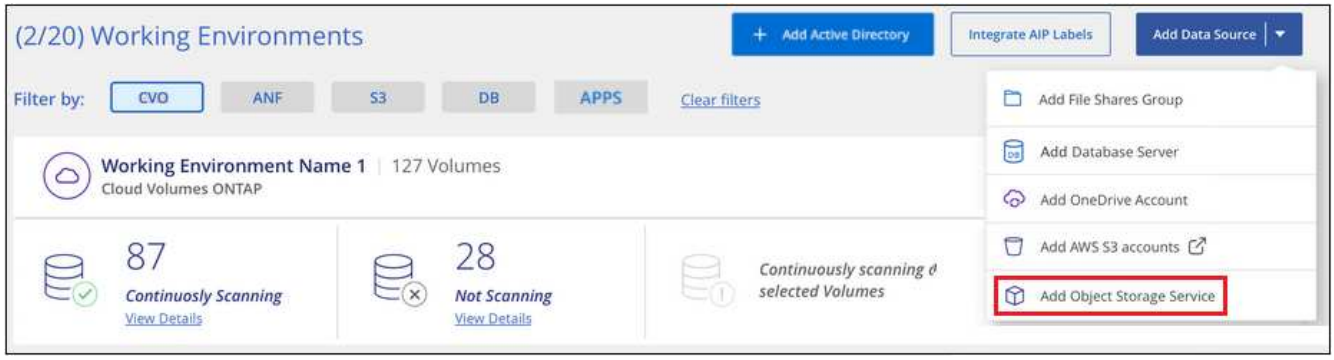
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Agregar el servicio de almacenamiento de objetos a la clasificación de BlueXP

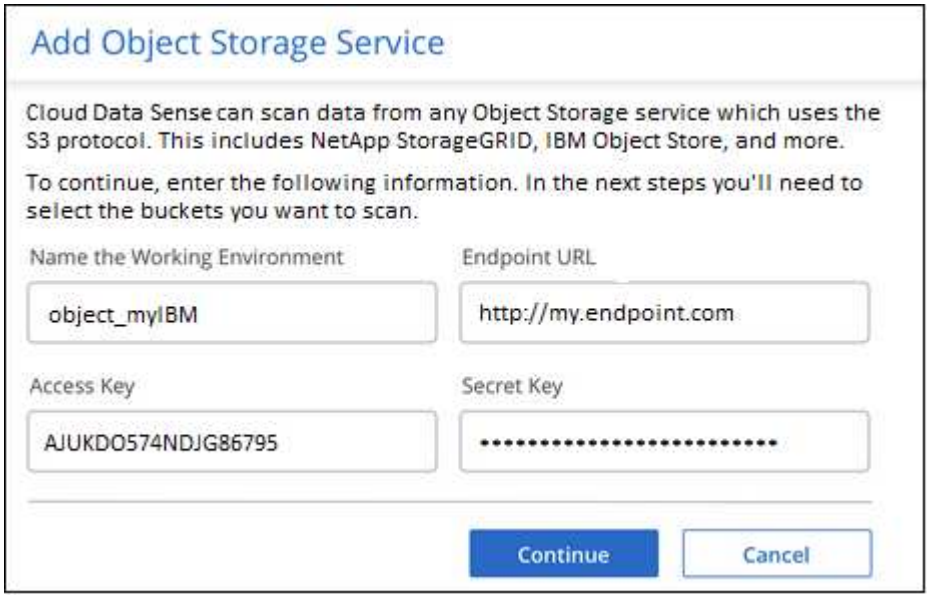
Añada el servicio de almacenamiento de objetos.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar servicio de almacenamiento de objetos**.



2. En el cuadro de diálogo Add Object Storage Service, introduzca los detalles del servicio de almacenamiento de objetos y haga clic en **continuar**.
   a. Introduzca el nombre que desea utilizar para el entorno de trabajo. Este nombre debe reflejar el nombre del servicio de almacenamiento de objetos al que se conecta.
   b. Introduzca la URL de extremo para acceder al servicio de almacenamiento de objetos.
   c. Introduzca la clave de acceso y la clave secreta para que la clasificación de BlueXP pueda acceder a los buckets del almacenamiento de objetos.



Resultado

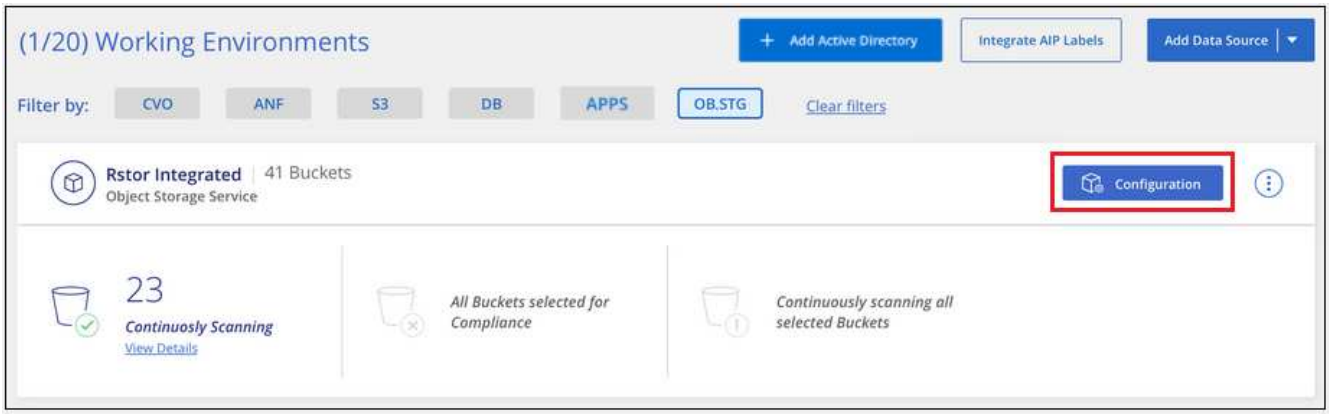
El nuevo Servicio de almacenamiento de objetos se añade a la lista de entornos de trabajo.

Habilitación y deshabilitación de análisis de cumplimiento de normativas en bloques de almacenamiento de objetos

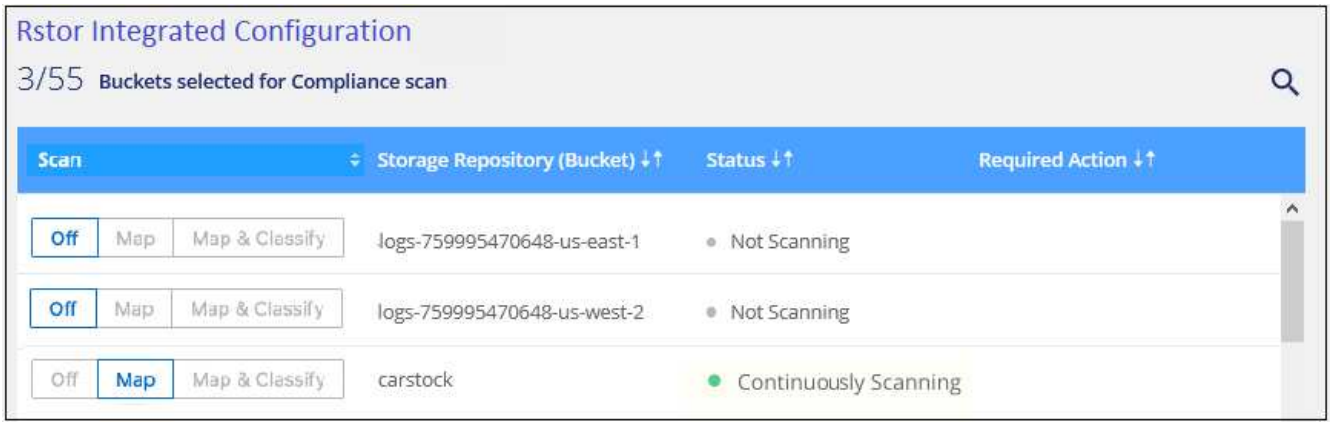
Después de habilitar la clasificación de BlueXP en tu servicio de almacenamiento de objetos, el paso siguiente es configurar los bloques que quieres analizar. La clasificación de BlueXP descubre esos buckets y los muestra en el entorno de trabajo que has creado.

Pasos

1. En la página Configuración, haga clic en **Configuración** en el entorno de trabajo Servicio de almacenamiento de objetos.



2. Active escaneos de sólo asignación o escaneos de asignación y clasificación en los bloques.



Para:	Haga lo siguiente:
Habilite los análisis de sólo asignación en un bloque	Haga clic en **Mapa**
Activar exploraciones completas en un bloque	Haga clic en **Mapa y clasificación**
Desactivar el análisis en un bloque	Haga clic en **Desactivado**

Resultado

La clasificación de BlueXP comienza a analizar los bloques que has habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Integra tu Active Directory con la clasificación de BlueXP

Puedes integrar un Active Directory global con la clasificación de BlueXP para mejorar los resultados que la clasificación de BlueXP informa sobre los propietarios de archivos y qué usuarios y grupos tienen acceso a tus archivos.

Cuando configuras ciertas fuentes de datos (que se enumeran a continuación), tienes que introducir las credenciales de Active Directory para que la clasificación de BlueXP analice los volúmenes de CIFS. Esta integración proporciona la clasificación de BlueXP con el propietario de archivo y los detalles de permisos para los datos que residen en esos orígenes de datos. El directorio activo introducido para esos orígenes de datos puede ser diferente de las credenciales globales de Active Directory especificadas aquí. La clasificación de BlueXP buscará en todos los directorios activos integrados para obtener información sobre los usuarios y los permisos.

Esta integración proporciona información adicional en las siguientes ubicaciones en la clasificación de BlueXP:

- Puede utilizar el "propietario del archivo" "filtro" Y consulte los resultados en los metadatos del archivo en el panel Investigación. En lugar del propietario del archivo que contiene el SID (identificador de seguridad), se rellena con el nombre de usuario real.
- Puede ver "permisos completos de archivos" Para cada archivo y directorio al hacer clic en el botón "Ver todos los permisos".
- En la "Consola de gobernanza", El panel permisos abiertos mostrará un mayor nivel de detalle acerca de los datos.

> Los SID del usuario local y los SID de dominios desconocidos no se traducen al nombre de usuario real.

Orígenes de datos compatibles

Una integración de Active Directory con la clasificación de BlueXP puede identificar datos procedentes de las siguientes fuentes de datos:

- Sistemas ONTAP en las instalaciones
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX para ONTAP
- Recursos compartidos de archivos CIFS de otros proveedores (no recursos compartidos de archivos NFS)
- Cuentas de OneDrive
- Cuentas de SharePoint

No se ofrece compatibilidad para identificar la información de usuarios y permisos de esquemas de base de datos, cuentas de Google Drive, cuentas de Amazon S3 o Object Storage que utilizan el protocolo simple Storage Service (S3).

Conéctese a su servidor de Active Directory

Después de implementar la clasificación de BlueXP y haber activado el análisis en tus fuentes de datos, puedes integrar la clasificación de BlueXP con Active Directory. Se puede acceder a Active Directory mediante una dirección IP del servidor DNS o una dirección IP del servidor LDAP.

Las credenciales de Active Directory pueden ser de solo lectura, pero ofrecer credenciales de administrador garantiza que la clasificación de BlueXP pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de BlueXP.

Para volúmenes/recursos compartidos de archivos CIFS, si deseas asegurarte de que los análisis de clasificación de BlueXP no cambien tus archivos, recomendamos que el usuario tenga permiso de atributos de escritura. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

Requisitos

- Debe tener un Active Directory ya configurado para los usuarios de su empresa.
- Debe tener la información de Active Directory:
  - Dirección IP del servidor DNS o varias direcciones IP

    o.

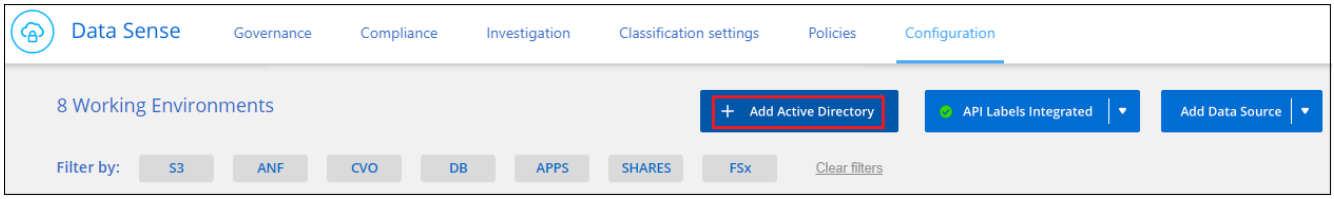
  Dirección IP del servidor LDAP o varias direcciones IP

  - Nombre de usuario y contraseña para acceder al servidor
  - Nombre de dominio (nombre de Active Directory)
  - Si utiliza o no un LDAP seguro (LDAPS)
  - Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)
- La instancia de clasificación de BlueXP debe tener abiertos los siguientes puertos para la comunicación saliente:

Protocolo	Puerto	Destino	Específico
TCP Y UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP sobre SSL
TCP	3268	Active Directory	Catálogo global
TCP	3269	Active Directory	Catálogo global sobre SSL

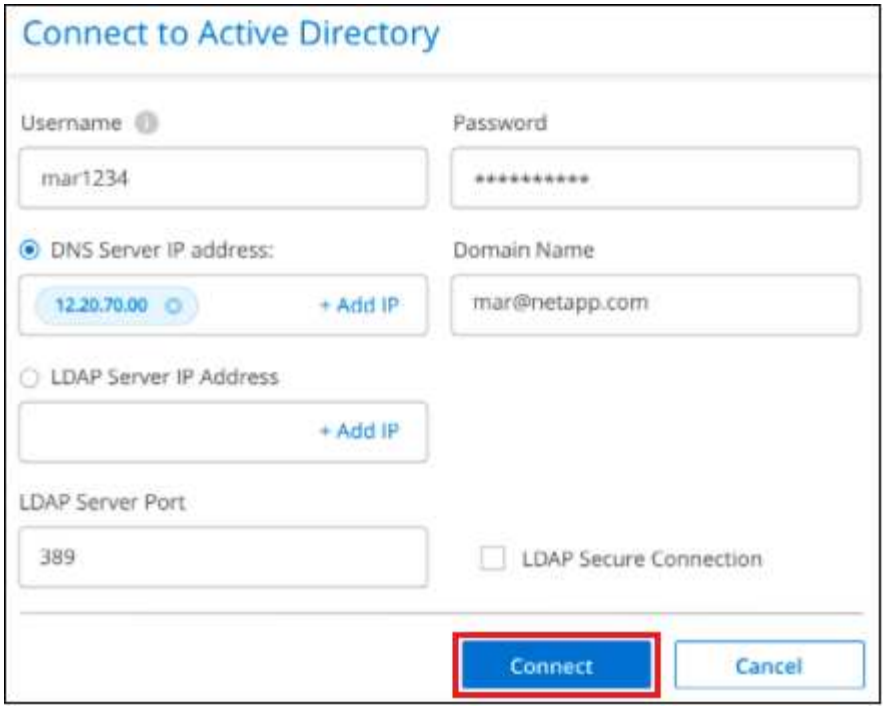
Pasos

1. En la página Configuración de clasificación de BlueXP, haz clic en **Add Active Directory**.

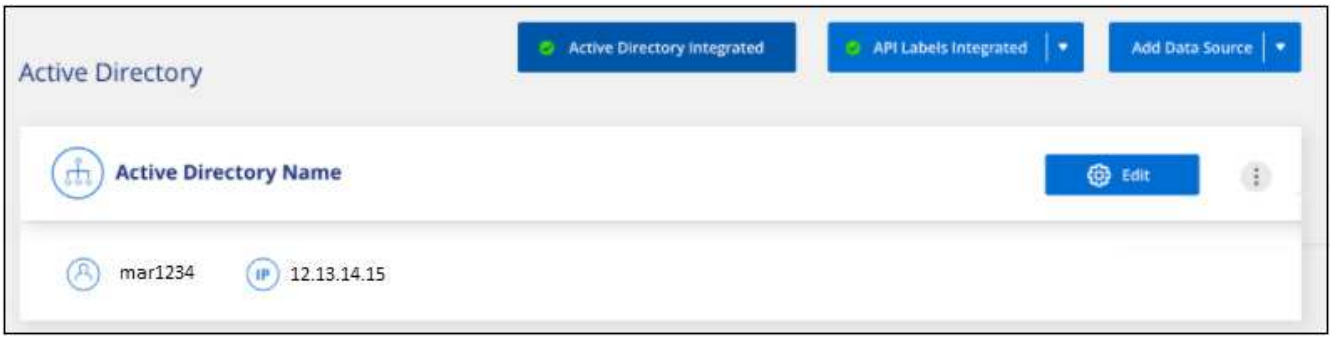


2. En el cuadro de diálogo conectarse a Active Directory, introduzca los detalles de Active Directory y haga clic en **conectar**.

   Si es necesario, puede agregar varias direcciones IP haciendo clic en **Agregar IP**.



La clasificación de BlueXP se integra en Active Directory y se añade una nueva sección a la página Configuración.



Gestione su integración con Active Directory

Si necesita modificar algún valor de su integración con Active Directory, haga clic en el botón **Editar** y realice los cambios.

También puede eliminar la integración si ya no la necesita haciendo clic en el ⋮ Y a continuación **Quitar Active Directory**.

Configura las licencias para la clasificación de BlueXP

Los primeros 1 TB de datos que analiza la clasificación de BlueXP en un espacio de trabajo de BlueXP son gratis durante 30 días. Debe seguir analizando los datos después de ese momento una licencia BYOL de NetApp o una suscripción al mercado de su proveedor de cloud.

Antes de leer más:

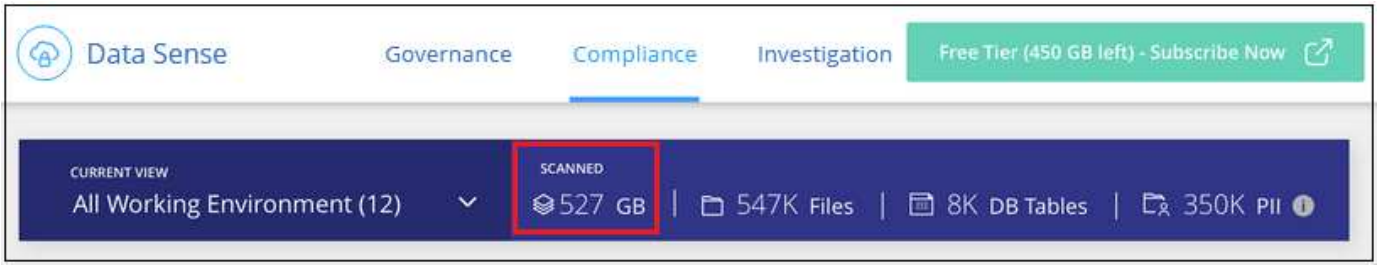
- Si ya te has suscrito a la suscripción de pago por uso (PAYGO) de BlueXP en el mercado de tu proveedor de cloud, también te suscribirás automáticamente a la clasificación de BlueXP. No tendrá que volver a suscribirse.
- La clasificación BYOL (bring-your-own-license) de BlueXP (Data Sense) es una licencia *flotante* que puedes utilizar en todos los entornos de trabajo y orígenes de datos del espacio de trabajo que planeas analizar. Verás una suscripción activa en la cartera digital de BlueXP.
- La cantidad de datos que se analizan se calcula en función del tamaño lógico de archivo, sin ninguna eficiencia del almacenamiento.

"Obtén más información sobre las licencias y los costes relacionados con la clasificación de BlueXP".

prueba gratuita de 30 días

Está disponible una prueba gratuita de 30 días para hasta 1 TB de datos que analiza la clasificación de BlueXP en un espacio de trabajo de BlueXP. Tendrá que comprar una licencia BYOL de NetApp o un registro para obtener una suscripción desde el mercado del proveedor de cloud para seguir escaneando los datos después de ese momento.

Puede suscribirse en cualquier momento y no se le cobrará hasta que finalice la prueba de 30 días o la cantidad de datos supere 1 TB. Siempre puedes ver la cantidad total de datos que se analizan en el Panel de gobernanza de clasificación de BlueXP. Y el botón *Subscribe Now* facilita la suscripción cuando esté listo.



Usa una suscripción PAYGO de clasificación de BlueXP

Las suscripciones de pago por uso desde el mercado de su proveedor de cloud permiten utilizar las licencias para usar los sistemas Cloud Volumes ONTAP y muchos servicios BlueXP, como la clasificación de BlueXP. Pagarás a tu proveedor de nube por la cantidad de datos que se analiza la clasificación de BlueXP por horas con una única suscripción.

La suscripción garantiza que no se produzca ninguna interrupción en el servicio una vez que finalice la prueba gratuita. Cuando finalice la prueba, se le cobrará cada hora según la cantidad de datos que esté escaneando. No se le cobrará por su suscripción durante su prueba gratuita.

Pasos

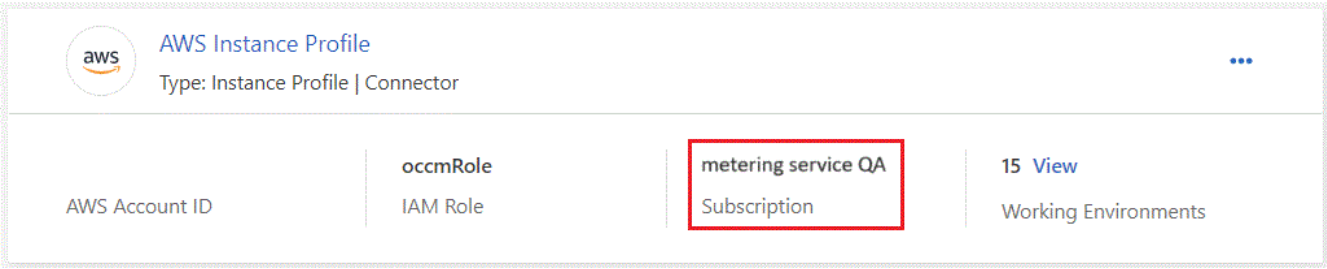
Un usuario que tenga la función *Account Admin* debe completar estos pasos.

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.

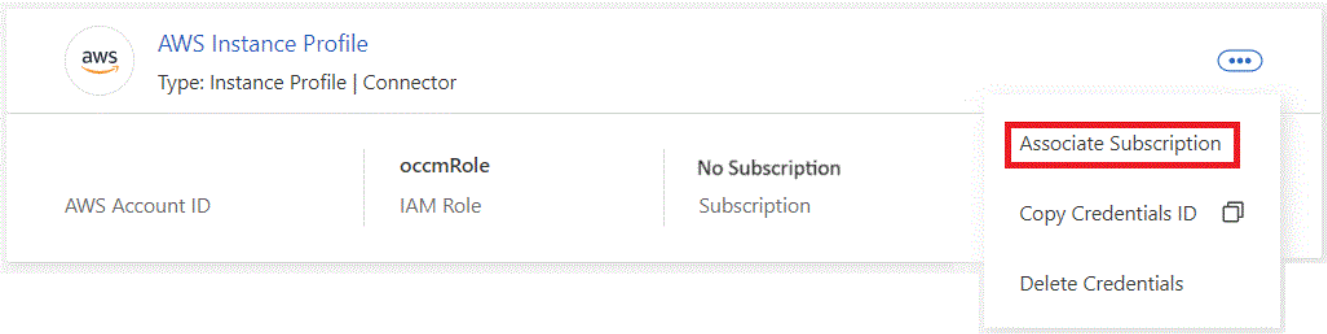
2. Haga clic en **Credenciales** y, a continuación, busque las credenciales para el perfil de instancia de AWS, la identidad de servicio gestionado de Azure o Google Project.

   La suscripción se debe agregar al perfil de instancia, la identidad de servicio gestionado o Google Project. La carga no funcionará de otro modo.

   Si ya tienes una suscripción a BlueXP (como se muestra a continuación para AWS), entonces ya estás todo listo: No hay nada más que tengas que hacer.



3. Si aún no tienes una suscripción, haz clic en el menú de acciones y haz clic en **Suscripción asociada**.



4. Seleccione una suscripción existente y haga clic en **asociado**, o haga clic en **Agregar suscripción** y siga los pasos.

   El siguiente vídeo muestra cómo asociar un "Mercado AWS" Suscripción a una suscripción a AWS:

   ► https://docs.netapp.com/es-es/bluexp-classification//media/video_subscribing_aws.mp4 *(video)*

   El siguiente vídeo muestra cómo asociar un "Azure Marketplace" Suscripción a una suscripción de Azure:

   ► https://docs.netapp.com/es-es/bluexp-classification//media/video_subscribing_azure.mp4 *(video)*

   El siguiente vídeo muestra cómo asociar un "Google Cloud Marketplace" Suscripción a una suscripción a GCP:

   ► https://docs.netapp.com/es-es/bluexp-classification//media/video_subscribing_gcp.mp4 *(video)*

Utilizar un contrato anual

Paga por la clasificación BlueXP cada año comprando un contrato anual. Están disponibles en plazos de 1, 2 o 3 años.

Si tienes un contrato anual en un mercado, todo el análisis de datos de clasificación de BlueXP se cobrará en función de ese contrato. No se puede mezclar y combinar un contrato anual de mercado con una licencia propia.

- AWS: "Vaya a la oferta de BlueXP Marketplace para obtener información sobre precios".
- Azure: "Vaya a la oferta de BlueXP Marketplace para obtener información sobre precios".
- Google Cloud: Póngase en contacto con su representante de ventas de NetApp para adquirir un contrato anual. El contrato está disponible como oferta privada en Google Cloud Marketplace. Después de que NetApp comparta la oferta privada contigo, puedes seleccionar el plan anual al suscribirte en el mercado de Google Cloud durante la activación de la clasificación de BlueXP.

Utiliza una licencia BYOL de clasificación de BlueXP

Las licencias que traiga sus propias de NetApp proporcionan períodos de 1, 2 o 3 años. La licencia de clasificación BYOL BlueXP (Data Sense) es una licencia *flotante* donde la capacidad total se comparte entre **todos** de tus entornos de trabajo y orígenes de datos, lo que facilita la renovación y la licencia iniciales.

Si no tienes una licencia de clasificación de BlueXP, ponte en contacto con nosotros para comprar una:

- Mailto:ng-contact-data-sense@netapp.com?Subject=Licensing[Enviar correo electrónico para adquirir una licencia].
- Haga clic en el icono de chat situado en la parte inferior derecha de BlueXP para solicitar una licencia.

Opcionalmente, si tiene una licencia basada en nodos sin asignar para Cloud Volumes ONTAP que no utilizará, puede convertirla en una licencia de clasificación de BlueXP que tenga la misma equivalencia de dólar y la misma fecha de caducidad. "Vaya aquí para obtener más información".

Utilizarás la cartera digital de BlueXP para gestionar las licencias de BYOL para la clasificación de BlueXP. Puedes añadir nuevas licencias, actualizar las licencias existentes y ver el estado de la licencia desde la cartera digital de BlueXP.

Obtenga el archivo de licencia de clasificación de BlueXP

Después de comprar tu licencia de clasificación de BlueXP (Data Sense), activa la licencia en BlueXP introduciendo el número de serie de la clasificación de BlueXP y la cuenta del sitio de soporte de NetApp (NSS) o cargando el archivo de licencia de NetApp (NLF). Los pasos a continuación muestran cómo obtener el archivo de licencia de NLF si planea utilizar ese método.

Si has implementado la clasificación de BlueXP en un host de un sitio local que no tiene acceso a Internet, lo que significa que has implementado el conector de BlueXP en "modo privado", necesitará obtener el archivo de licencia de un sistema conectado a internet. La activación de la licencia mediante el número de serie y la cuenta NSS no está disponible para instalaciones de modo privado.

Antes de empezar

Antes de comenzar, necesitará tener la siguiente información:

- Número de serie de clasificación de BlueXP

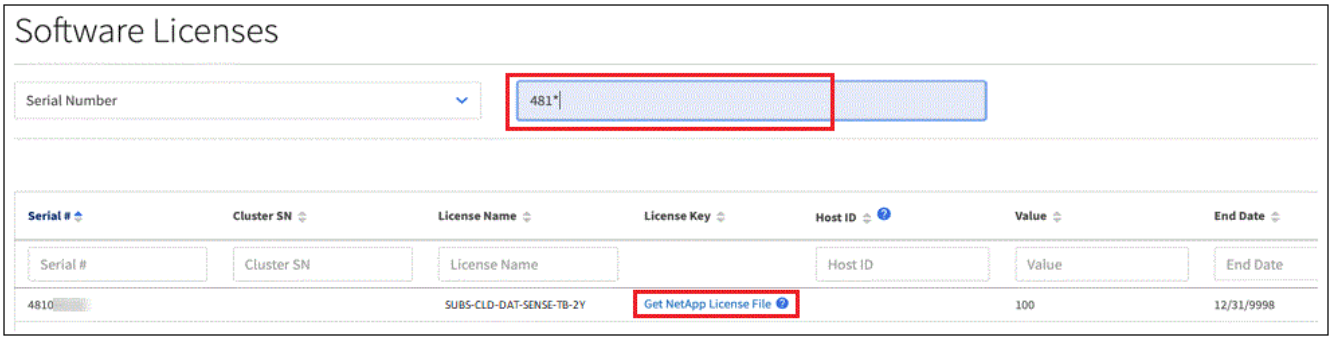
  Busque este número en su pedido de ventas o póngase en contacto con el equipo de cuentas para obtener esta información.

- ID de cuenta de BlueXP

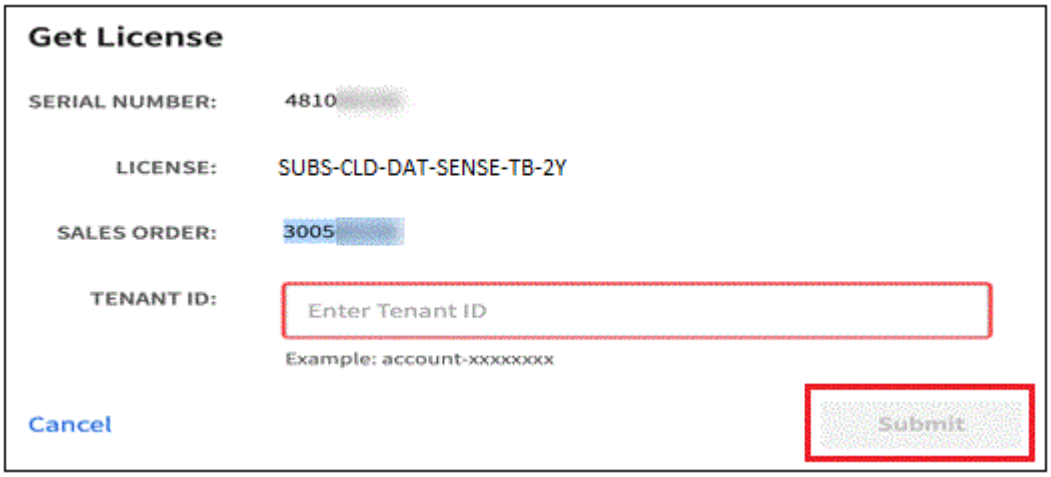
  Puede encontrar su ID de cuenta de BlueXP seleccionando el menú desplegable **cuenta** de la parte superior de BlueXP y, a continuación, haciendo clic en **Administrar cuenta** junto a su cuenta. Su ID de cuenta se encuentra en la ficha Descripción general. Para sitios de modo privado sin acceso a Internet, utilice **CUENTA-DARKSITE1**.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp" Y haga clic en **sistemas > licencias de software**.
2. Introduce el número de serie de la licencia de clasificación de BlueXP.



3. En la columna **Clave de licencia**, haz clic en **Obtener archivo de licencia de NetApp**.
4. Introduzca su ID de cuenta de BlueXP (esto se denomina ID de inquilino en el sitio de soporte) y haga clic en **Enviar** para descargar el archivo de licencia.



Añade licencias BYOL de clasificación de BlueXP a tu cuenta

Después de comprar una licencia de clasificación (Data Sense) de BlueXP para tu cuenta de BlueXP, tendrás que añadir la licencia a BlueXP para utilizar el servicio de clasificación de BlueXP.

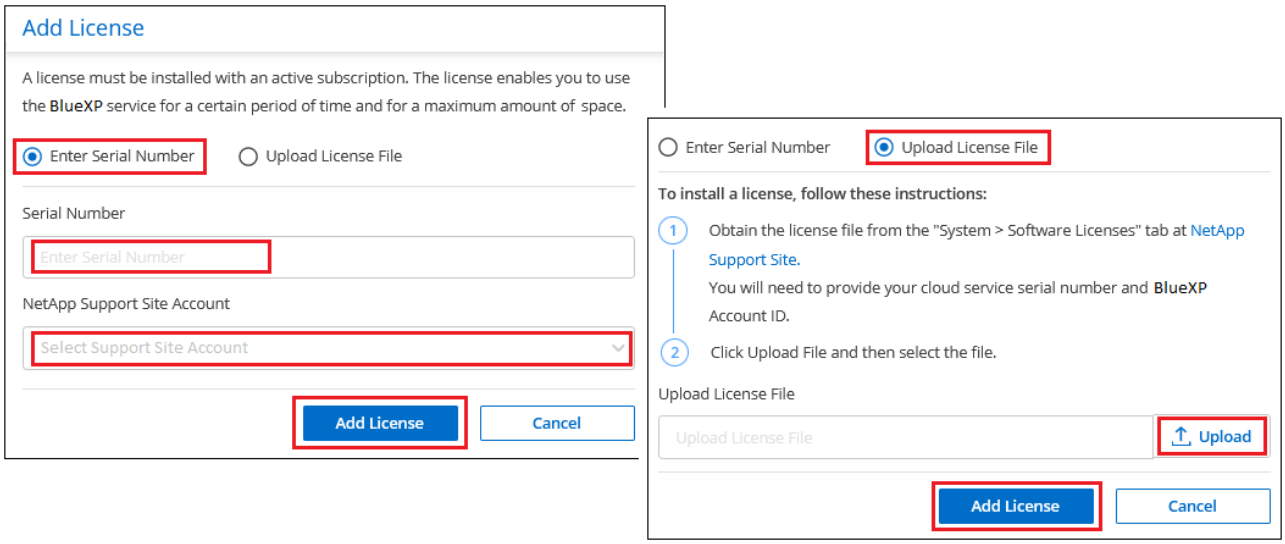
Pasos

1. En el menú BlueXP, haga clic en **Gobierno > cartera digital** y, a continuación, seleccione la ficha **licencias de servicios de datos**.
2. Haga clic en **Agregar licencia**.
3. En el cuadro de diálogo *Add License*, introduzca la información de la licencia y haga clic en **Add License**:
   - Si tienes el número de serie de la licencia de clasificación de BlueXP y conoces tu cuenta NSS, selecciona la opción **Enter Serial Number** e introduce esa información.

     Si su cuenta del sitio de soporte de NetApp no está disponible en la lista desplegable, "Agregue la cuenta NSS a BlueXP".

   - Si tienes el archivo de licencia de clasificación de BlueXP (necesario cuando se instala en un sitio oscuro), selecciona la opción **Cargar archivo de licencia** y sigue las indicaciones para adjuntar el

archivo.



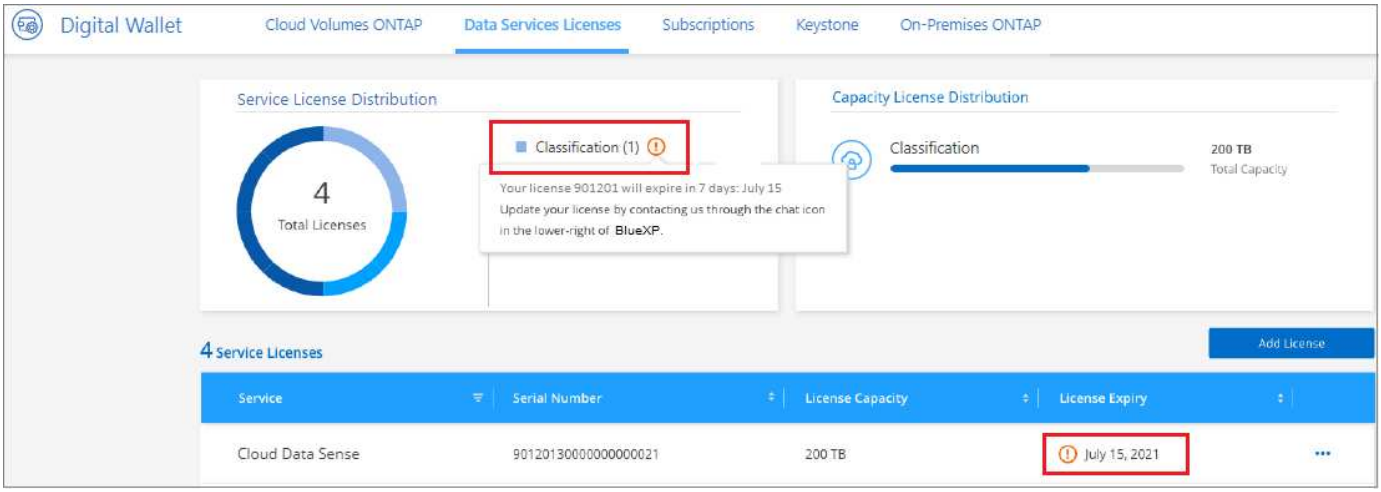
Resultado

BlueXP añade la licencia para que tu servicio de clasificación de BlueXP esté activo.

Actualizar una licencia BYOL de clasificación de BlueXP

Si el plazo que le otorga la licencia se acerca a la fecha de caducidad o si su capacidad con licencia está llegando al límite, se le notificará en la IU de clasificación.

Este estado también aparece en la cartera digital de BlueXP y en "Notificaciones".



Puedes actualizar tu licencia de clasificación de BlueXP antes de que caduque para que no se interrumpa tu capacidad de acceder a los datos escaneados.

Pasos

1. Haga clic en el icono de chat situado en la parte inferior derecha de BlueXP para solicitar una extensión de

su término o capacidad adicional a su licencia de Cloud Data Sense para el número de serie concreto. También puede enviar un correo electrónico para solicitar una actualización a su licencia.

Después de pagar la licencia y estar registrado en el sitio de soporte de NetApp, BlueXP actualiza automáticamente la licencia en la cartera digital de BlueXP y la página de licencias de servicios de datos reflejará el cambio que se ha producido en un plazo de 5 a 10 minutos.

2. Si BlueXP no puede actualizar automáticamente la licencia (por ejemplo, cuando está instalada en un sitio oscuro), deberá cargar manualmente el archivo de licencia.
   a. Puede hacerlo Obtenga el archivo de licencia del sitio de soporte de NetApp.
   b. En la página de Digital Wallet de BlueXP, en la ficha *Data Services Licenses*, haga clic en ••• Para el número de serie del servicio que está actualizando y haga clic en **Actualizar licencia**.

   c. En la página *Update License*, cargue el archivo de licencia y haga clic en **Actualizar licencia**.

Resultado

BlueXP actualiza la licencia para que tu servicio de clasificación de BlueXP siga estando activo.

Consideraciones sobre la licencia de BYOL

Cuando utiliza una licencia BYOL de clasificación (Data Sense) de BlueXP, BlueXP muestra una advertencia en la interfaz de usuario de clasificación de BlueXP y en la interfaz de usuario de cartera digital de BlueXP cuando el tamaño de todos los datos que escaneas se acerca al límite de capacidad o se acerca a la fecha de caducidad de la licencia. Recibe estas advertencias:

- Cuando la cantidad de datos que está analizando ha alcanzado el 80% de la capacidad con licencia y, de nuevo, cuando ha alcanzado el límite
- 30 días antes de que caduque una licencia, y de nuevo cuando caduque la licencia

Utilice el icono de chat situado en la parte inferior derecha de la interfaz de BlueXP para renovar su licencia cuando vea estas advertencias.

Si tu licencia caduca o has alcanzado el límite de tu propia licencia, la clasificación de BlueXP sigue ejecutándose, pero se bloquea el acceso a las consolas de forma que no puedas ver información sobre ninguno de los datos escaneados. Solo la página *Configuration* está disponible en caso de que se desee reducir la cantidad de volúmenes que se van a analizar para lograr que su uso de capacidad esté dentro del límite de licencia.

Cuando renuevas la licencia BYOL, BlueXP actualiza automáticamente la licencia en la cartera digital de BlueXP y proporciona acceso completo a todas las consolas. Si BlueXP no puede acceder al archivo de licencia a través de la conexión segura a Internet (por ejemplo, cuando está instalado en un sitio oscuro), puede obtener el archivo usted mismo y cargarlo manualmente en BlueXP. Para ver instrucciones, consulte

Cómo actualizar una licencia de clasificación de BlueXP.

> Si la cuenta que estás usando tiene una licencia BYOL y una suscripción PAYGO, la clasificación *NOT* de BlueXP pasará a la suscripción PAYGO cuando caduque la licencia BYOL. Debe renovar la licencia de BYOL.

Preguntas frecuentes sobre la clasificación de BlueXP

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Servicio de clasificación de BlueXP

Las preguntas siguientes proporcionan un conocimiento general de la clasificación de BlueXP.

¿Qué es la clasificación de BlueXP?

La clasificación de BlueXP es una oferta de cloud que usa tecnología impulsada por inteligencia artificial (IA) para ayudarte a comprender el contexto de los datos e identificar datos confidenciales en tus sistemas de almacenamiento. Los sistemas pueden ser entornos de trabajo que hayas añadido a BlueXP Canvas y muchos tipos de fuentes de datos a las que la clasificación de BlueXP puede acceder en tus redes. "Consulte la lista completa a continuación".

La clasificación de BlueXP ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para abordar las nuevas normativas de cumplimiento de normativas sobre privacidad y confidencialidad de los datos, como RGPD, CCPA, HIPAA, etc.

¿Cómo funciona la clasificación de BlueXP?

La clasificación de BlueXP pone en marcha otra capa de inteligencia artificial junto con su sistema y sistemas de almacenamiento BlueXP. A continuación, analiza los datos en volúmenes, bloques, bases de datos y otras cuentas de almacenamiento e indexa las estadísticas de datos que se encuentran. La clasificación de BlueXP aprovecha tanto la inteligencia artificial como el procesamiento del lenguaje natural, al contrario que soluciones alternativas que se construyen habitualmente en torno a expresiones regulares y coincidencia de patrones.

La clasificación de BlueXP utiliza la IA para ofrecer una comprensión contextual de los datos a fin de detectarlos y clasificarlos con precisión. Está impulsada por la IA porque está diseñada para los tipos de datos y la escala actuales. También comprende el contexto de los datos a fin de proporcionar datos sólidos, precisos, de detección y clasificación.

"Obtén más información sobre cómo funciona la clasificación de BlueXP".

¿Cuáles son los casos de uso más comunes para la clasificación de BlueXP?

- Identificación de la Información personal de identificación (PII).
- Localice con facilidad y cree informes sobre datos específicos en respuesta a sujetos de datos, según lo requiera el RGPD, la CCPA, la HIPAA y otras normativas de privacidad de los datos.
- Cumpla con las normativas de privacidad de datos nuevas y futuras.
- Cumpla con las normativas sobre privacidad y cumplimiento de normativas de datos.
- Migrar los datos de los sistemas heredados al cloud.

- Cumpla con las políticas de retención de datos.

"Obtén más información sobre los casos de uso para la clasificación de BlueXP".

¿Qué hay de la arquitectura de clasificación de BlueXP?

La clasificación de BlueXP pone en marcha un único servidor o clúster, donde quieras, tanto en la nube como on-premises. Los servidores se conectan mediante protocolos estándar a los orígenes de datos e indexan los hallazgos de un clúster Elasticsearch, que también se implementa en los mismos servidores. Esto permite la compatibilidad con entornos multicloud, entre cloud, cloud privado y en las instalaciones.

¿Qué proveedores de cloud son compatibles?

La clasificación de BlueXP funciona como parte de BlueXP y es compatible con AWS, Azure y GCP. Esto proporciona a su organización una visibilidad de privacidad unificada a través de distintos proveedores de cloud.

¿La clasificación de BlueXP tiene una API REST y funciona con herramientas de terceros?

BlueXP admite las funcionalidades de la API DE REST para sus servicios. Si BlueXP no es el punto preferido de gestión, servicios como la clasificación de BlueXP también se pueden usar a través de una API DE REST. Cada acción del usuario tiene una API REST que se puede integrar con sistemas de terceros. Consulte "API de clasificación de BlueXP" para obtener más detalles.

¿La clasificación de BlueXP está disponible en los mercados?

Sí, la clasificación de BlueXP y BlueXP está disponible en los mercados de AWS, Azure y GCP.

Análisis y análisis de clasificación de BlueXP

Las siguientes preguntas hacen referencia al rendimiento del análisis de clasificación de BlueXP y el análisis disponibles para los usuarios.

¿Con qué frecuencia escanea los datos la clasificación de BlueXP?

Si bien el análisis inicial de los datos puede tardar un poco de tiempo, los análisis posteriores solo inspeccionan los cambios incrementales, lo que reduce los tiempos de escaneo del sistema. La clasificación de BlueXP analiza los datos continuamente por turnos, seis repositorios cada vez, para que todos los datos modificados se clasifiquen muy rápidamente.

"Descubra cómo funcionan las exploraciones".

Tenga en cuenta que la clasificación de BlueXP analiza las bases de datos solo una vez al día: Las bases de datos no se analizan continuamente, como otras fuentes de datos.

Los análisis de datos tienen un impacto insignificante en los sistemas de almacenamiento y en los datos. Sin embargo, si te preocupa incluso un impacto muy pequeño, puedes configurar la clasificación de BlueXP para realizar análisis «lentos». "Descubra cómo reducir la velocidad de escaneado".

¿Puedo buscar mis datos usando la clasificación de BlueXP?

La clasificación de BlueXP ofrece amplias funciones de búsqueda que facilitan la búsqueda de un archivo o un fragmento de datos específico en todas las fuentes conectadas. La clasificación de BlueXP permite a los usuarios realizar búsquedas más profundas que lo que reflejan los metadatos. Es un servicio que no depende

del lenguaje que también puede leer los archivos y analizar una multitud de tipos de datos confidenciales, como nombres e ID. Por ejemplo, los usuarios pueden buscar en almacenes de datos estructurados y no estructurados para buscar datos que se hayan filtrado desde bases de datos a archivos de usuario, en violación de la política corporativa. Las búsquedas se pueden guardar más adelante y se pueden crear políticas para buscar y realizar acciones sobre los resultados a una frecuencia establecida.

Una vez que se han encontrado los archivos de interés, se pueden enumerar las características, incluyendo etiquetas, cuenta de entorno de trabajo, bloque, ruta de archivo, categoría (de clasificación), tamaño de archivo, última modificación, estado de permisos, duplicados, nivel de sensibilidad, datos personales, tipos de datos confidenciales dentro del archivo, propietario, tipo de archivo, tamaño de archivo, hora de creación, hash de archivo, si los datos se asignaron a alguien que busca atención y mucho más. Los filtros pueden aplicarse para eliminar las características que no son pertinentes. La clasificación de BlueXP también tiene controles de control de acceso basado en roles para permitir mover o eliminar los archivos si existen los permisos adecuados. Si no hay permisos correctos, las tareas se pueden asignar a alguien de la organización que tenga los permisos adecuados.

¿Qué tipo de análisis ofrece la clasificación de BlueXP?

Las fuentes de datos se pueden representar visualmente y las relaciones se definen y se representan gráficamente. Por ejemplo, los administradores pueden ver todos los datos desfasados, duplicados y no relacionados con el negocio en todos los orígenes de datos de toda la empresa (sistemas locales, bases de datos, recursos compartidos de archivos, almacenes S3, OneDrive, etc.). Luego pueden copiar, mover, eliminar y gestionar los datos para optimizar los costes en almacenamiento y reducir los riesgos. Los usuarios pueden reducir el riesgo viendo qué datos confidenciales se pueden exponer y pueden crear trabajos para gestionar permisos para una protección de datos sólida. La clasificación de BlueXP también clasifica todos los diferentes tipos de datos, de modo que los administradores pueden investigar datos por tipo y ver qué acciones se han llevado a cabo en los datos y cuándo.

¿La clasificación de BlueXP ofrece informes?

Sí. La información que ofrece la clasificación de BlueXP puede ser relevante para otras partes interesadas de tus organizaciones, por lo que te permitimos generar informes para compartir las perspectivas. Los siguientes informes están disponibles para la clasificación de BlueXP:

Informe de evaluación de riesgos de privacidad

Proporciona información sobre la privacidad de sus datos y una puntuación de riesgo para la privacidad. "Leer más".

Informe de solicitud de acceso de asunto de datos

Le permite extraer un informe de todos los archivos que contienen información sobre el nombre o identificador personal específico de un sujeto de datos. "Leer más".

Informe PCI DSS

Le ayuda a identificar la distribución de la información de la tarjeta de crédito a través de sus archivos. "Leer más".

Informe HIPAA

Le ayuda a identificar la distribución de información médica a través de sus archivos. "Leer más".

Informe asignación de datos

Proporciona información acerca del tamaño y el número de archivos en los entornos de trabajo. Esto incluye la capacidad de uso, la antigüedad de los datos, el tamaño de los datos y los tipos de archivos. "Leer más".

Informe de evaluación de detección de datos

Proporciona un análisis de alto nivel del entorno escaneado para resaltar los resultados del sistema y mostrar las áreas de preocupación y los posibles pasos para solucionarlos. "Modo de aprendizaje".

Informa sobre un tipo de información específico

Hay informes disponibles que incluyen detalles sobre los archivos identificados que contienen datos personales y datos personales confidenciales. También puede ver los archivos desglosados por categoría y tipo de archivo. "Leer más".

¿el rendimiento del análisis varía?

El rendimiento del análisis puede variar en función del ancho de banda de la red y del tamaño medio de los archivos del entorno. También puede depender del tamaño del sistema host (ya sea en el cloud o en las instalaciones). Consulte "La instancia de clasificación de BlueXP" y.. "Implementando la clasificación de BlueXP" si quiere más información.

Al agregar inicialmente nuevos orígenes de datos, también puede elegir realizar sólo una exploración de "asignación" en lugar de una exploración de "clasificación" completa. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro. "Vea la diferencia entre una exploración de mapeo y clasificación".

Privacidad y gestión de clasificación de BlueXP

Las siguientes preguntas ofrecen información sobre cómo gestionar la configuración de privacidad y clasificación de BlueXP.

¿Cómo habilito la clasificación de BlueXP?

Primero necesitas poner en marcha una instancia de clasificación de BlueXP en BlueXP o en un sistema on-premises. Una vez que la instancia se está ejecutando, puede habilitar el servicio en entornos de trabajo existentes, bases de datos y otras fuentes de datos desde la pestaña **Configuración** o seleccionando un entorno de trabajo específico.

"Aprenda cómo empezar".

> Si se activa la clasificación de BlueXP en un origen de datos, el análisis inicial se realiza inmediatamente. Los resultados de la exploración se muestran poco después.

¿Cómo deshabilito la clasificación de BlueXP?

Puede deshabilitar la clasificación de BlueXP para que no analice un entorno de trabajo, una base de datos, un grupo de recursos compartidos de archivos, una cuenta de OneDrive o una cuenta de SharePoint individuales desde la página Configuración de clasificación de BlueXP.

"Leer más".

> Para quitar por completo la instancia de clasificación de BlueXP, puedes quitar manualmente la instancia de clasificación de BlueXP del portal del proveedor de nube o la ubicación on-premises.

¿Puedo personalizar el servicio según las necesidades de mi organización?

La clasificación de BlueXP proporciona información inmediata sobre tus datos. Estos conocimientos se pueden extraer y utilizar para las necesidades de su organización.

Además, la clasificación de BlueXP ofrece muchas formas de añadir una lista personalizada de «datos personales» que identificará la clasificación de BlueXP en los análisis, lo que proporciona una imagen completa sobre dónde residen los datos potencialmente confidenciales en *todos* los archivos de su organización.

- Puede agregar identificadores únicos basados en columnas específicas en las bases de datos que está explorando. Llamamos a esto **Data Fusion**.
- Puede agregar palabras clave personalizadas desde un archivo de texto.
- Puede agregar patrones personalizados utilizando una expresión regular (regex).

"Leer más".

¿Puedo indicar al servicio que excluya los datos de escaneo en ciertos directorios?

Sí. Si desea que la clasificación de BlueXP excluya los datos de análisis que residen en determinados directorios de orígenes de datos, puede proporcionar esa lista al motor de clasificación. Después de aplicar ese cambio, la clasificación de BlueXP excluirá el análisis de datos en los directorios especificados.

"Leer más".

¿Se analizan copias Snapshot que residen en los volúmenes ONTAP?

No La clasificación de BlueXP no analiza las copias Snapshot porque el contenido es idéntico al contenido del volumen.

¿Qué sucede si la organización en niveles de datos está habilitada en sus volúmenes de ONTAP?

Cuando la clasificación de BlueXP analiza volúmenes que tienen datos inactivos organizados en niveles en el almacenamiento de objetos, analiza todos los datos que hay en los discos locales y los datos inactivos organizados en niveles en el almacenamiento de objetos. Esto también es aplicable a productos que no son de NetApp que implementan la organización en niveles.

El análisis no calienta los datos fríos: Permanecen inactivos y permanecen en el almacenamiento de objetos.

¿Puede la clasificación de BlueXP enviar notificaciones a mi organización?

Sí. Junto con la función Directivas, puede enviar alertas por correo electrónico a los usuarios de BlueXP (diariamente, semanalmente o mensualmente) o a cualquier otra dirección de correo electrónico, cuando una Política devuelva los resultados para que pueda obtener notificaciones para proteger sus datos. Más información acerca de "Normativas".

También puede descargar informes de estado desde la página Gobierno y la página Investigación que puede compartir internamente en su organización.

¿Puede la clasificación de BlueXP funcionar con las etiquetas AIP que he incrustado en mis archivos?

Sí. Puede gestionar etiquetas AIP en los archivos a los que está analizando la clasificación de BlueXP si ya se ha suscrito "Protección de información de Azure (AIP)". Puede ver las etiquetas que ya están asignadas a los archivos, agregar etiquetas a los archivos y cambiar las etiquetas existentes.

"Leer más".

Tipos de sistemas y tipos de datos de origen

Las siguientes preguntas están relacionadas con los tipos de almacenamiento que se pueden analizar y los tipos de datos que se analizan.

¿Qué fuentes de datos se pueden analizar con la clasificación de BlueXP?

La clasificación de BlueXP puede analizar los datos de los entornos de trabajo que haya añadido a BlueXP Canvas y de muchos tipos de fuentes de datos estructuradas y no estructuradas a las que puede acceder la clasificación de BlueXP en sus redes.

Entornos de trabajo:

- Cloud Volumes ONTAP (implementado en AWS, Azure o GCP)
- Clústeres de ONTAP en las instalaciones
- Azure NetApp Files
- Amazon FSX para ONTAP
- Amazon S3

Fuentes de datos:

- Recursos compartidos de archivos que no son de NetApp
- Almacenamiento de objetos (que utiliza el protocolo S3)
- Bases de datos (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL y SAP HANA, SQL SERVER)
- Cuentas de OneDrive
- Cuentas en línea y en las instalaciones de SharePoint
- Cuentas de Google Drive

La clasificación de BlueXP es compatible con las versiones de NFS 3.x y CIFS 1.x, 2,0, 2,1 y 3,0.

¿Existen restricciones cuando se implementa en una región gubernamental?

La clasificación de BlueXP se admite cuando Connector se pone en marcha en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD), también conocida como «modo restringido». Cuando se implementa de esta manera, la clasificación de BlueXP tiene las siguientes restricciones:

- Las cuentas de OneDrive, cuentas de SharePoint y cuentas de Google Drive no se pueden analizar.
- La funcionalidad de etiqueta de Microsoft Azure Information Protection (AIP) no se puede integrar.

¿Qué fuentes de datos puedo analizar si instalo la clasificación de BlueXP en un sitio sin acceso a Internet?

La clasificación de BlueXP solo puede analizar datos de orígenes de datos locales al sitio on-premises. En este momento, la clasificación de BlueXP puede analizar las siguientes fuentes de datos locales en «modo privado», también conocido como sitio «oscuro»:

- Sistemas ONTAP en las instalaciones

- Esquemas de base de datos
- Cuentas locales de SharePoint (SharePoint Server)
- Recursos compartidos de archivos NFS o CIFS de terceros
- Almacenamiento de objetos que utiliza el protocolo simple Storage Service (S3)

¿Qué tipos de archivo son compatibles?

La clasificación de BlueXP analiza todos los archivos para buscar información de categorías y metadatos y muestra todos los tipos de archivos en la sección Tipos de archivos de la consola.

Cuando la clasificación de BlueXP detecta información personal identificable (PII) o cuando realiza una búsqueda DSAR, solo son compatibles los siguientes formatos de archivo:

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

¿Qué tipos de datos y metadatos captura la clasificación de BlueXP?

La clasificación de BlueXP te permite ejecutar un análisis general de «asignaciones» o un análisis completo de «clasificación» en tus orígenes de datos. La asignación sólo ofrece una descripción general de alto nivel de los datos, mientras que la clasificación proporciona un análisis profundo de los datos. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro.

- Exploración de asignación de datos.

  La clasificación de BlueXP solo analiza los metadatos. Esto resulta útil para la gestión y el gobierno generales de los datos, el dimensionamiento rápido de los proyectos, las estatales de gran tamaño y la priorización. La asignación de datos se basa en metadatos y se considera una exploración **rápida**.

  Después de un análisis rápido, puede generar un informe de asignación de datos. Este informe es una descripción general de los datos almacenados en sus orígenes de datos corporativos para ayudarle a tomar decisiones sobre la utilización de los recursos, la migración, el backup, la seguridad y los procesos de cumplimiento de normativas.

- Exploración de clasificación de datos (profunda).

  Los análisis de clasificación de BlueXP usan protocolos estándar y permiso de solo lectura en todos tus entornos. Algunos archivos se abren y se analizan en busca de datos confidenciales relacionados con el negocio, información privada y problemas relacionados con el ransomware.

  Después de un análisis completo, hay muchas funciones adicionales de clasificación de BlueXP que puedes aplicar a tus datos, como ver y refinar datos en la página de Investigación de datos, buscar nombres dentro de los archivos, copiar, mover y eliminar archivos de origen, y mucho más.

La clasificación de BlueXP captura metadatos como: Nombre del archivo, permisos, hora de creación, último acceso y última modificación. Esto incluye todos los metadatos que aparecen en la página Detalles de investigación de datos y en los informes de investigación de datos.

La clasificación de BlueXP puede identificar muchos tipos de datos privados, como los datos personales y los datos personales confidenciales. Para obtener información detallada sobre los datos privados, consulte "Categorías de datos privados que escanea la clasificación de BlueXP".

¿Puedo limitar la información de clasificación de BlueXP a usuarios específicos?

Sí, la clasificación de BlueXP está totalmente integrada en BlueXP. Los usuarios de BlueXP sólo pueden ver información sobre los entornos de trabajo que pueden ver según sus privilegios de área de trabajo.

Además, si quieres permitir que determinados usuarios solo vean los resultados del análisis de clasificación de BlueXP sin tener la capacidad de administrar las configuraciones de clasificación de BlueXP, puedes asignar a esos usuarios el rol Cloud Compliance Viewer.

"Leer más".

¿Puede alguien acceder a los datos privados enviados entre mi navegador y la clasificación de BlueXP?

No Los datos privados que se envíen entre su explorador y la instancia de clasificación de BlueXP se mantienen seguros gracias al cifrado integral con TLS 1,2, lo que significa que ni NetApp ni terceros podrán leerlos. La clasificación de BlueXP no compartirá datos ni resultados con NetApp a menos que solicites y apruebes el acceso.

Los datos que se analizan permanecen dentro de su entorno.

¿Cómo se gestionan los datos confidenciales?

NetApp no tiene acceso a los datos confidenciales y no los muestra en la interfaz de usuario de. Los datos confidenciales están enmascarados; por ejemplo, los últimos cuatro números se muestran para obtener información sobre la tarjeta de crédito.

¿Dónde se almacenan los datos?

Los resultados del análisis se almacenan en Elasticsearch, dentro de tu instancia de clasificación de BlueXP.

¿Cómo se accede a los datos?

La clasificación de BlueXP accede a los datos almacenados en Elasticsearch mediante llamadas a API, que requieren autenticación y están cifrados mediante AES-128. Para acceder a Elasticsearch se necesita acceso de raíz directamente.

Licencias y costes

Las siguientes preguntas hacen referencia a las licencias y los costes para usar la clasificación de BlueXP.

¿Cuánto cuesta la clasificación de BlueXP?

El coste de utilizar la clasificación de BlueXP depende de la cantidad de datos que se estén escaneando. Los primeros 1 TB de datos que analiza la clasificación de BlueXP en un espacio de trabajo de BlueXP son gratis durante 30 días. Después de alcanzar cualquiera de los límites, necesitará uno de los siguientes para continuar con el análisis de datos:

- Una suscripción a la lista de BlueXP Marketplace de su proveedor de la nube, o.
- A bring-your-own-license (BYOL) de NetApp

Consulte "precios" para obtener más detalles.

¿Qué sucede si he alcanzado el límite de capacidad de su licencia?

Si alcanzas el límite de capacidad de tu propia licencia, la clasificación de BlueXP sigue ejecutándose, pero se bloquea el acceso a las consolas de forma que no puedas ver información sobre ninguno de los datos escaneados. Solo la página Configuration está disponible en caso de que se desee reducir la cantidad de volúmenes que se van a analizar para potencialmente traer su uso de capacidad bajo el límite de licencia. Debe renovar su licencia BYOL para recuperar el acceso total a la clasificación de BlueXP.

Despliegue del conector

Las siguientes preguntas se refieren al conector BlueXP.

¿Qué es el conector?

Connector es un software que se ejecuta en una instancia informática dentro de su cuenta cloud o en las instalaciones, que permite a BlueXP gestionar de forma segura los recursos cloud. Debes implementar un conector para usar la clasificación de BlueXP.

¿Dónde se debe instalar el conector?

- Cuando se escanear datos en Cloud Volumes ONTAP en AWS, Amazon FSX para ONTAP o en bloques AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.
- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.
- Al analizar datos en sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos S3 genérico, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive, puede utilizar un conector en cualquiera de estas ubicaciones de cloud.

Por tanto, si tiene datos en muchas de estas ubicaciones, es posible que tenga que utilizarlos "Múltiples conectores".

¿La clasificación de BlueXP requiere acceso a las credenciales?

La propia clasificación de BlueXP no recupera las credenciales de almacenamiento. En su lugar, se almacenan en el conector BlueXP.

La clasificación de BlueXP usa credenciales del plano de datos, por ejemplo, credenciales de CIFS para montar los recursos compartidos antes del análisis.

¿Puedo desplegar el conector en mi propio host?

Sí. Puede hacerlo "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en un host del cloud. Si tienes pensado implementar la clasificación de BlueXP en las instalaciones, es posible que desee instalar el conector también en las instalaciones, pero no es necesario.

¿La comunicación entre el servicio y el conector utiliza HTTP?

Sí, la clasificación de BlueXP se comunica con el conector de BlueXP mediante HTTP.

¿Qué pasa con sitios seguros sin acceso a Internet?

Sí, también es compatible. Puede hacerlo "Implemente el conector en un host Linux local que no tenga acceso a Internet". "Esto también se conoce como “modo privado”". A continuación, puedes detectar clústeres de ONTAP on-premises y otras fuentes de datos locales y analizar los datos mediante la clasificación de BlueXP.

Puesta en marcha de la clasificación de BlueXP

Las siguientes preguntas hacen referencia a la instancia de clasificación de BlueXP aparte.

¿Qué modelos de implementación son compatibles con la clasificación de BlueXP?

BlueXP permite al usuario analizar y generar informes sobre sistemas prácticamente en cualquier parte, incluidos entornos locales, de cloud e híbridos. La clasificación de BlueXP normalmente se pone en marcha mediante un modelo de SaaS, en el que el servicio se habilita a través de la interfaz de BlueXP y no requiere instalar ningún hardware o software. Incluso en este modo de puesta en marcha con un clic y una ejecución, la gestión de datos se puede realizar sin importar si los almacenes de datos están en las instalaciones o en el cloud público.

¿Qué tipo de instancia o máquina virtual es necesario para la clasificación de BlueXP?

Cuando "implementado en el cloud":

- En AWS, la clasificación de BlueXP se ejecuta en una instancia m6i.4xlarge con un disco de 500 GiB y GP2 GB. Es posible seleccionar un tipo de instancia menor durante la implementación.
- En Azure, la clasificación de BlueXP se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 500 GiB.
- En GCP, la clasificación de BlueXP se ejecuta en una VM n2 estándar 16 con un disco persistente estándar de 500 GiB.

Tenga en cuenta que puede poner en marcha la clasificación de BlueXP en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

"Obtén más información sobre cómo funciona la clasificación de BlueXP".

¿Puedo poner en marcha la clasificación de BlueXP en mi propio host?

Sí. Puede instalar el software de clasificación BlueXP en un host Linux que tenga acceso a Internet en su red o en el cloud. Todo funciona igual y continúa gestionando la configuración de exploración y los resultados a través de BlueXP. Consulte "Puesta en marcha de la clasificación de BlueXP en las instalaciones" para conocer los requisitos del sistema y los detalles de la instalación.

¿Qué pasa con sitios seguros sin acceso a Internet?

Sí, también es compatible. Puede hacerlo "Pon en marcha la clasificación de BlueXP en un sitio local que no tenga acceso a Internet" para ubicaciones completamente seguras.

Usa la clasificación de BlueXP

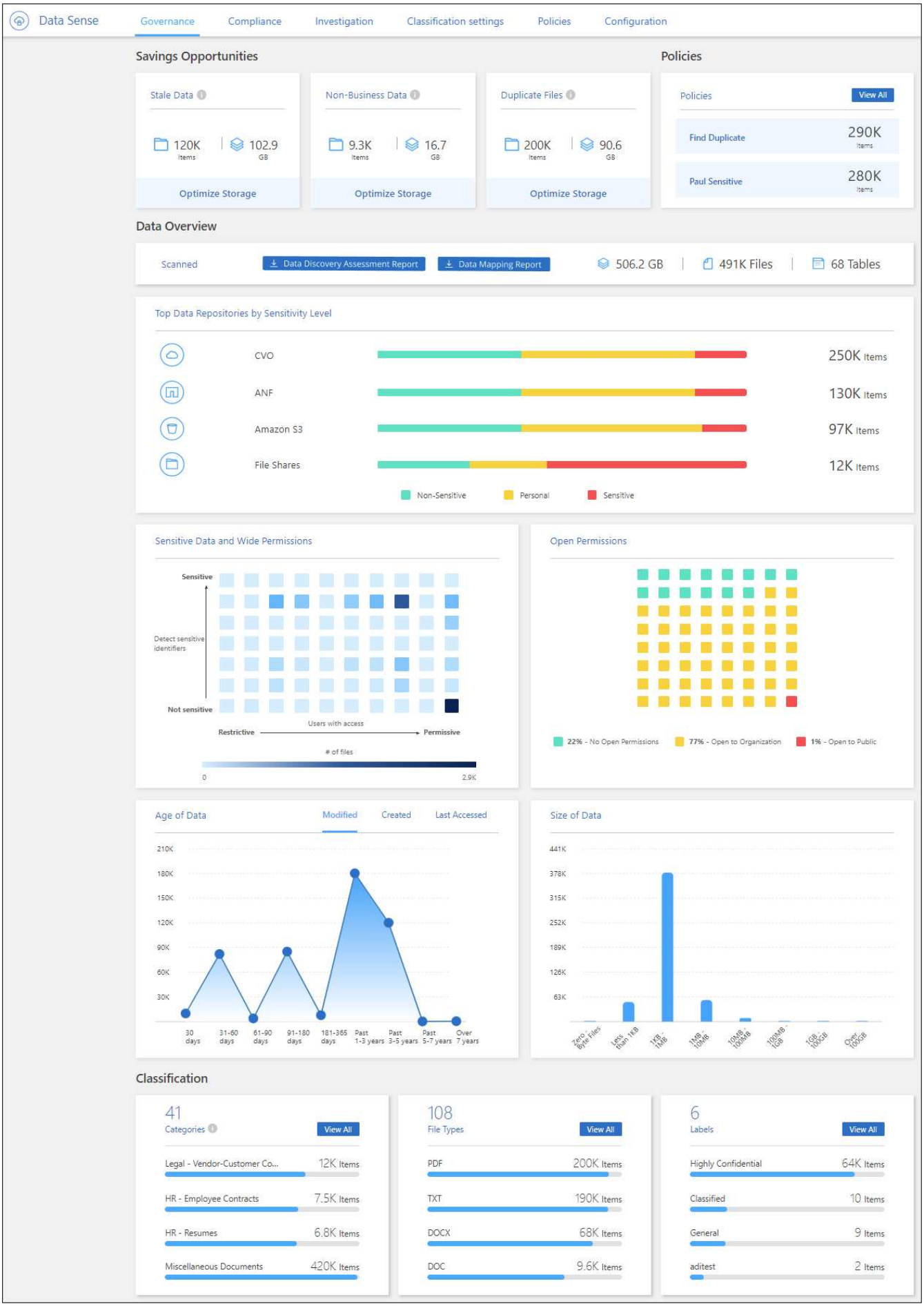
Ver detalles de gobierno sobre los datos almacenados en su organización

Controle los costes relacionados con los datos que residen en los recursos de almacenamiento de su organización. La clasificación de BlueXP identifica la cantidad de datos obsoletos, datos no empresariales, archivos duplicados y archivos muy grandes de tus sistemas, de modo que puedas decidir si quieres eliminar o organizar en niveles algunos archivos en un almacenamiento de objetos más barato.

Además, si tiene pensado migrar datos desde ubicaciones locales al cloud, puede visualizar el tamaño de los datos y si alguno de ellos contiene información confidencial antes de moverlos.

El panel de control de gobierno

La consola de gobernanza proporciona información para que pueda aumentar la eficiencia y controlar los costes relacionados con los datos almacenados en sus recursos de almacenamiento.


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

Guarde las oportunidades

Puede que desee investigar los elementos del área *Saving Opportunities* para ver si hay datos que debe eliminar o organizar en niveles un almacenamiento de objetos menos costoso. Haga clic en cada elemento para ver los resultados filtrados en la página Investigación.

- * Datos obsoletos* - datos que se modificaron por última vez hace 3 años.
- **Datos no profesionales** - datos que se consideran no relacionados con el negocio, en función de su categoría o tipo de archivo. Estos recursos incluyen:
  - Datos de aplicaciones
  - Audio
  - Ejecutables
  - Imágenes
  - Registros
  - Vídeos
  - Varios (categoría general "otros")
- **Duplicar archivos**: Archivos duplicados en otras ubicaciones de los orígenes de datos que está analizando. "Consulte qué tipos de archivos duplicados se muestran".

  NOTA

  Si alguno de sus orígenes de datos implementa una organización en niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos se pueden identificar en la categoría *datos obsoletos*.

Políticas con el mayor número de resultados

En el área *Policies*, las políticas con mayor número de resultados aparecen en la parte superior de la lista. Haga clic en el nombre de una directiva para mostrar los resultados en la página Investigación. Haga clic en **Ver todo** para ver la lista de todas las directivas disponibles.

Haga clic en "aquí" Para obtener más información acerca de las políticas.

Descripción general de los datos

La sección *Data Overview* proporciona una rápida descripción general de todos los datos que se están analizando. Haga clic en el botón para descargar un informe completo de asignación de datos que incluya capacidad de uso, antigüedad de los datos, tamaño de los datos y tipos de archivo para todos los entornos de trabajo y orígenes de datos. Consulte Informe de asignación de datos para obtener todos los detalles de este informe.

Principales repositorios de datos listados por sensibilidad de datos

El área *Top Data Repository by Sensitivity Level* enumera los cuatro principales repositorios de datos (entornos de trabajo y orígenes de datos) que contienen los elementos más sensibles. El gráfico de barras de cada entorno de trabajo se divide en:

- Datos no confidenciales
- Datos personales
- Datos personales confidenciales

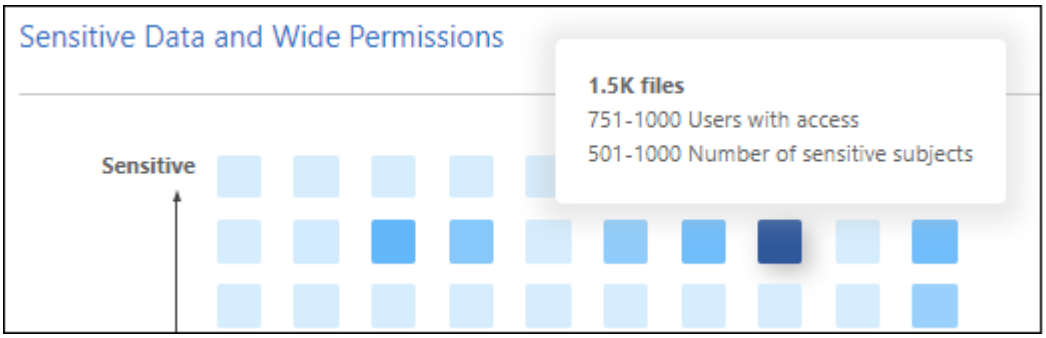
Puede pasar el ratón sobre cada sección para ver el número total de elementos de cada categoría.

Haga clic en cada área para ver los resultados filtrados en la página Investigación para que pueda seguir investigando.

Datos listados por sensibilidad y permisos amplios

El área *Sensitive Data y Wide Permissions* proporciona un mapa térmico de los archivos que contienen datos confidenciales (incluidos datos personales confidenciales y confidenciales) y que son demasiado permisivos. Esto puede ayudarle a ver dónde puede tener algunos riesgos con datos confidenciales.

Los archivos se clasifican en función del número de usuarios con permiso para acceder a los archivos del eje X (del más bajo al más alto) y del número de identificadores confidenciales dentro de los archivos del eje y (del más bajo al más alto). Los bloques representan el número de archivos que coinciden con los elementos de los ejes X e Y. El bloque de color más claro es bueno; con menos usuarios capaces de acceder a los archivos y con menos identificadores confidenciales por archivo. Los bloques más oscuros son los elementos que tal vez desee investigar. Por ejemplo, la siguiente pantalla muestra el texto de desplazamiento del bloque azul oscuro. Muestra que tiene 1,500 archivos en los que 751-100 usuarios tienen acceso y donde hay 501-100 identificadores confidenciales por archivo.



Puede hacer clic en el bloque en el que está interesado para ver los resultados filtrados de los archivos afectados en la página Investigación para poder seguir investigando.

No se muestran datos en este panel si no se ha integrado un servicio de identidades con la clasificación de BlueXP. "Descubre cómo integrar tu servicio de Active Directory con la clasificación de BlueXP".

> Este panel admite archivos en recursos compartidos de CIFS, OneDrive y orígenes de datos de SharePoint. Actualmente no se admite el almacenamiento de bases de datos, Google Drive, Amazon S3 y objetos genéricos.

Datos listados por tipos de permisos abiertos

El área *Open Permissions* muestra el porcentaje de cada tipo de permisos que existen para todos los archivos que se están analizando. El gráfico muestra los siguientes tipos de permisos:

- Sin permisos abiertos
- Abierto a la organización
- Abierto al público
- Acceso desconocido

Puede pasar el ratón sobre cada sección para ver el número total de archivos de cada categoría. Haga clic en cada área para ver los resultados filtrados en la página Investigación para que pueda seguir investigando.

Antigüedad de los datos y tamaño de los gráficos de datos

Puede que desee investigar los elementos de los gráficos *Age* y *Size* para ver si hay datos que debe eliminar o organizar en niveles un almacenamiento de objetos menos costoso.

Puede pasar el ratón sobre un punto de los gráficos para ver detalles sobre la antigüedad o el tamaño de los datos de esa categoría. Haga clic para ver todos los archivos filtrados por esa edad o rango de tamaño.

- * Edad del Gráfico de datos* - categoriza los datos en función de la hora en que se creó, la última vez que se accedió o la última vez que se modificó.
- * Tamaño del gráfico de datos* - categoriza los datos en función del tamaño.

NOTA

Si alguno de sus orígenes de datos implementa una organización en niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos se pueden identificar en el gráfico *Age of Data*.

La mayoría de las clasificaciones de datos identificadas

El área *Classification* proporciona una lista de los más identificados "Categorías", "Tipos de archivo", y. "Etiquetas AIP" en los datos escaneados.

Categorías

Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como "currículos" o "contratos de empleados" puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

Consulte "Ver archivos por categorías" si quiere más información.

Tipos de archivo

La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente.

Consulte "Visualización de tipos de archivo" si quiere más información.

Etiquetas AIP

Si se ha suscrito a la protección de información de Azure (AIP), puede clasificar y proteger documentos y archivos aplicando etiquetas al contenido. La revisión de las etiquetas AIP más utilizadas que se asignan a los archivos le permite ver qué etiquetas se utilizan más en sus archivos.

Consulte "Etiquetas AIP" si quiere más información.

Informe de asignación de datos

El informe de asignación de datos proporciona una descripción general de los datos que se almacenan en sus fuentes de datos empresariales para ayudarle en la toma de decisiones de migración, copia de seguridad, seguridad y procesos de cumplimiento de normativas. En el informe se enumera una descripción general que resume todos sus entornos de trabajo y orígenes de datos y, a continuación, proporciona un desglose para cada entorno de trabajo.

El informe incluye la siguiente información:

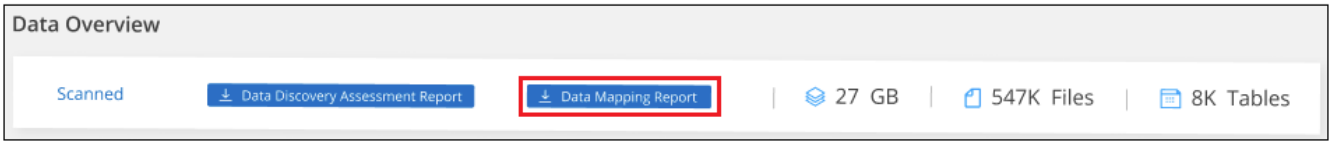
Categoría	Descripción
Capacidad de uso	Para todos los entornos de trabajo: Enumera el número de archivos y la capacidad utilizada para cada entorno de trabajo. Para entornos de trabajo individuales: Enumera los archivos que utilizan la mayor capacidad.
Antigüedad de los datos	Proporciona tres gráficos para cuándo se crearon los archivos, la última modificación o el último acceso. Enumera el número de archivos y su capacidad utilizada, en función de determinados rangos de fechas.
Tamaño de los datos	Enumera el número de archivos que existen dentro de determinados rangos de tamaño en los entornos de trabajo.
Tipos de archivo	Enumera el número total de archivos y la capacidad utilizada para cada tipo de archivo que se almacena en sus entornos de trabajo.

Generar el informe de asignación de datos

Este informe se genera desde la pestaña Gobernanza de la clasificación de BlueXP.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Gobierno** y, a continuación, haga clic en el botón **Informe de asignación de datos**.



Resultado

La clasificación de BlueXP genera un informe PDF que se puede revisar y enviar a otros grupos según sea necesario.

Si el informe tiene un tamaño superior a los 1 MB, el archivo PDF se conservará en la instancia de clasificación de BlueXP y verás un mensaje emergente sobre la ubicación exacta. Cuando se instala la clasificación de BlueXP en un equipo Linux en las instalaciones o en un equipo Linux puesto en marcha en el cloud, podrá acceder directamente al archivo PDF. Cuando la clasificación de BlueXP se ponga en marcha en la nube, necesitarás SSH en la instancia de clasificación de BlueXP para descargar el archivo PDF. "Consulte cómo acceder a los datos en la instancia de clasificación".

Tenga en cuenta que puede personalizar el nombre de la empresa que aparece en la primera página del informe desde la parte superior de la página de clasificación de BlueXP haciendo clic en Y, a continuación, haga clic en **Cambiar nombre de compañía**. La próxima vez que genere el informe, incluirá el nuevo nombre.

Informe de evaluación de identificación de datos

El informe de evaluación de detección de datos proporciona un análisis de alto nivel del entorno escaneado para resaltar los resultados obtenidos por el sistema y mostrar las áreas de preocupación y los posibles pasos de solución. Los resultados se basan en la asignación y clasificación de los datos. El objetivo de este informe es concienciar sobre tres aspectos importantes de su conjunto de datos:

Función	Descripción
Cuestiones relacionadas con el gobierno de los datos	Una imagen detallada de todos los datos de su propiedad y áreas en las que puede reducir la cantidad de datos para ahorrar costes.
Riesgos para la seguridad de los datos	Áreas en las que los datos son accesibles para ataques internos o externos debido a amplios permisos de acceso.
Lagunas de cumplimiento de normativas para los datos	Cuando su información personal personal personal personal o confidencial se encuentre para seguridad y para DSARs (solicitudes de acceso a sujetos de datos).

Tras la evaluación, este informe identifica las áreas en las que puede:

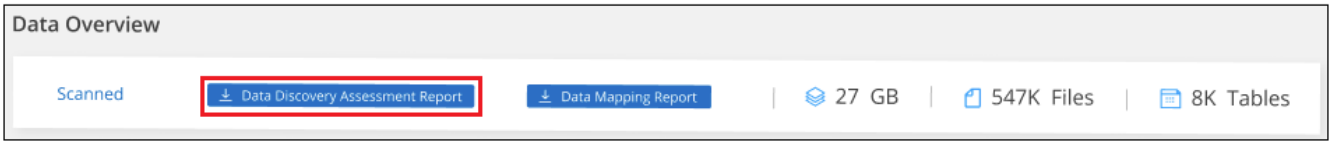
- Reducir los costes de almacenamiento cambiando la política de retención o moviendo o eliminando ciertos datos (datos obsoletos, duplicados o no empresariales).
- Proteja sus datos con amplios permisos mediante la revisión de las políticas de gestión de grupos globales
- Proteja sus datos con información personal o confidencial moviendo PII a almacenes de datos más seguros

Generar el informe de evaluación de detección de datos

Este informe se genera desde la pestaña Gobernanza de la clasificación de BlueXP.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Gobierno** y, a continuación, haga clic en el botón **Informe de evaluación de detección de datos**.



Resultado

La clasificación de BlueXP genera un informe PDF que se puede revisar y enviar a otros grupos según sea necesario.

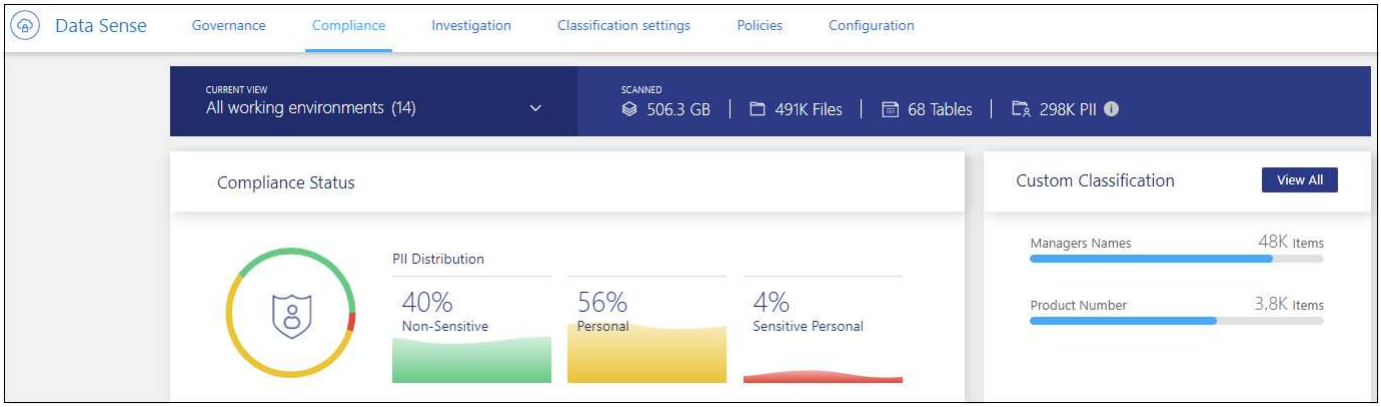
Tenga en cuenta que puede personalizar el nombre de la empresa que aparece en la primera página del informe desde la parte superior de la página de clasificación de BlueXP haciendo clic en Y, a continuación, haga clic en **Cambiar nombre de compañía**. La próxima vez que genere el informe, incluirá el nuevo nombre.

Consulte los detalles del cumplimiento de normativas sobre los datos almacenados en su organización

Controle sus datos privados al ver los detalles sobre los datos personales y los datos personales confidenciales de su empresa. También puedes obtener visibilidad revisando las categorías y los tipos de archivos que se encuentra en la clasificación de BlueXP en tus datos.

Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

De forma predeterminada, la consola de clasificación de BlueXP muestra los datos de cumplimiento de normativas de todos los entornos de trabajo y las bases de datos.



Si sólo desea ver datos para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

También puede filtrar los resultados desde la página Investigación de datos y descargar un informe de los resultados como un archivo CSV. Consulte "Filtrar datos en la página Investigación de datos" para obtener más detalles.

Ver archivos que contienen datos personales

La clasificación de BlueXP identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria, contraseñas, y sigue. "Consulte la lista completa". La clasificación de BlueXP identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

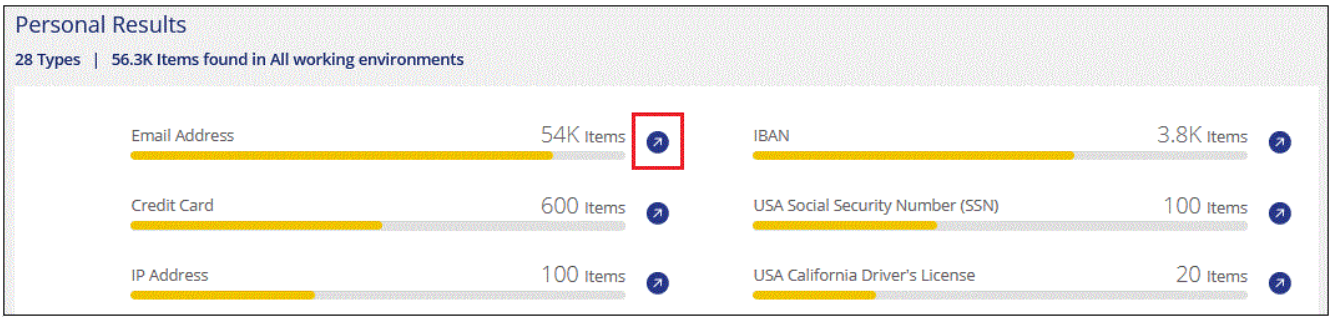
Además, si ha agregado un servidor de bases de datos para analizar, la función *Data Fusion* permite analizar los archivos para identificar si se encuentran identificadores únicos de las bases de datos en esos archivos u otras bases de datos. Consulte "Adición de identificadores de datos personales mediante Data Fusion" para obtener más detalles.

Para algunos tipos de datos personales, la clasificación de BlueXP utiliza *proximity validation* para validar sus descubrimientos. La validación se produce buscando una o más palabras clave predefinidas cerca de los datos personales encontrados. Por ejemplo, la clasificación de BlueXP identifica a un EE. UU Número de seguridad social (SSN) como un SSN si ve una palabra de proximidad junto a ella (por ejemplo, *SSN* o *seguridad social*). "La tabla de datos personales" Muestra cuándo la clasificación de BlueXP utiliza validación de proximidad.

Pasos

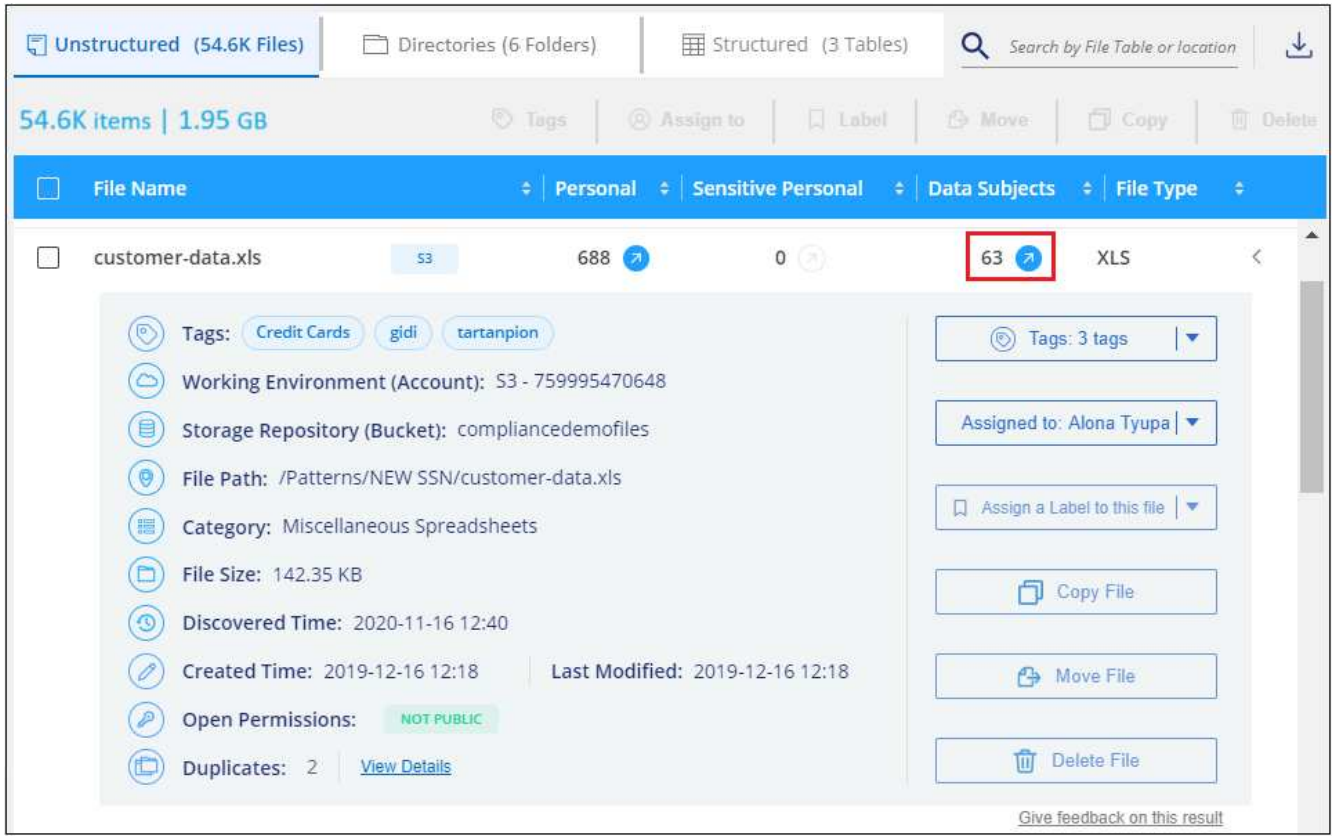
1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Para investigar los detalles de todos los datos personales, haga clic en el icono situado junto al porcentaje de datos personales.

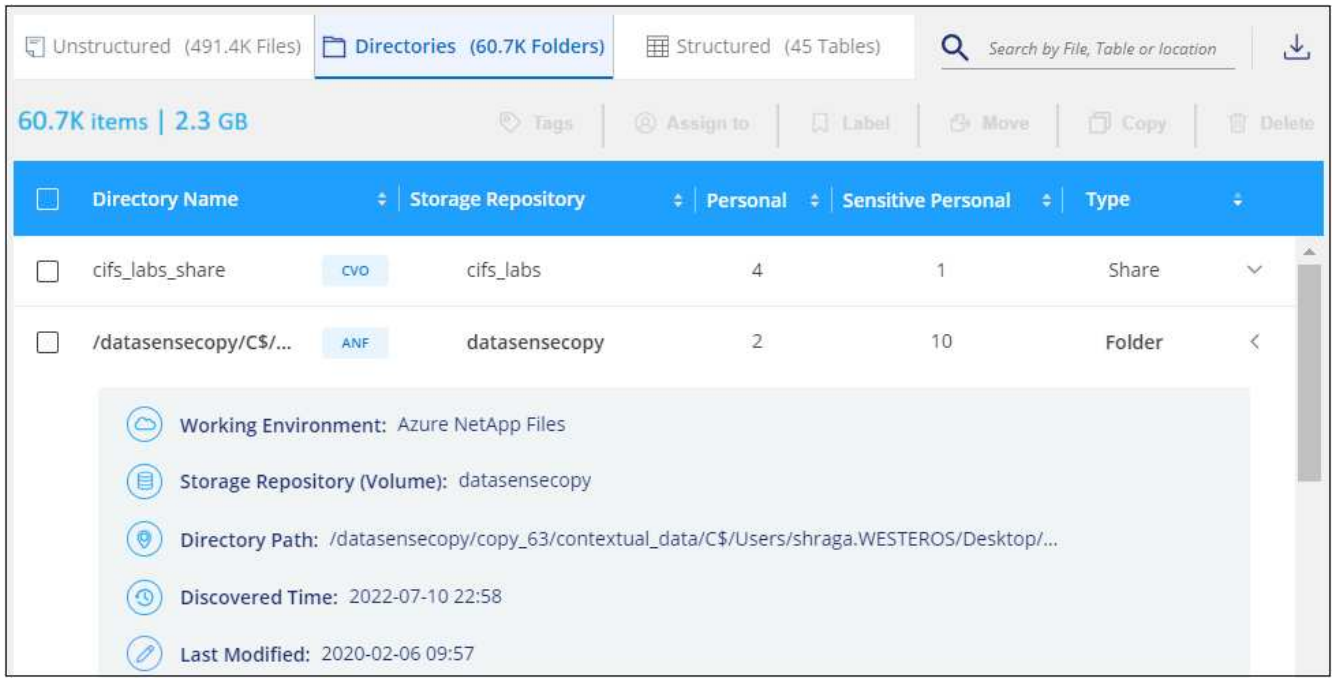
3. Para investigar los detalles de un tipo específico de datos personales, haga clic en **Ver todos** y, a continuación, en el icono **investigar resultados** para un tipo específico de datos personales; por ejemplo, direcciones de correo electrónico.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

   Las 2 capturas de pantalla siguientes muestran datos personales encontrados en archivos individuales y encontrados en archivos dentro de directorios (recursos compartidos y carpetas). También puede seleccionar la ficha **estructurado** para ver los datos personales encontrados en las bases de datos.





Ver archivos que contienen datos personales confidenciales

La clasificación de BlueXP identifica automáticamente tipos especiales de información personal confidencial, tal y como definen las normativas de privacidad como "Artículos 9 y 10 del RGPD". Por ejemplo, información sobre la salud, origen étnico o orientación sexual de una persona. "Consulte la lista completa". La clasificación de BlueXP identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

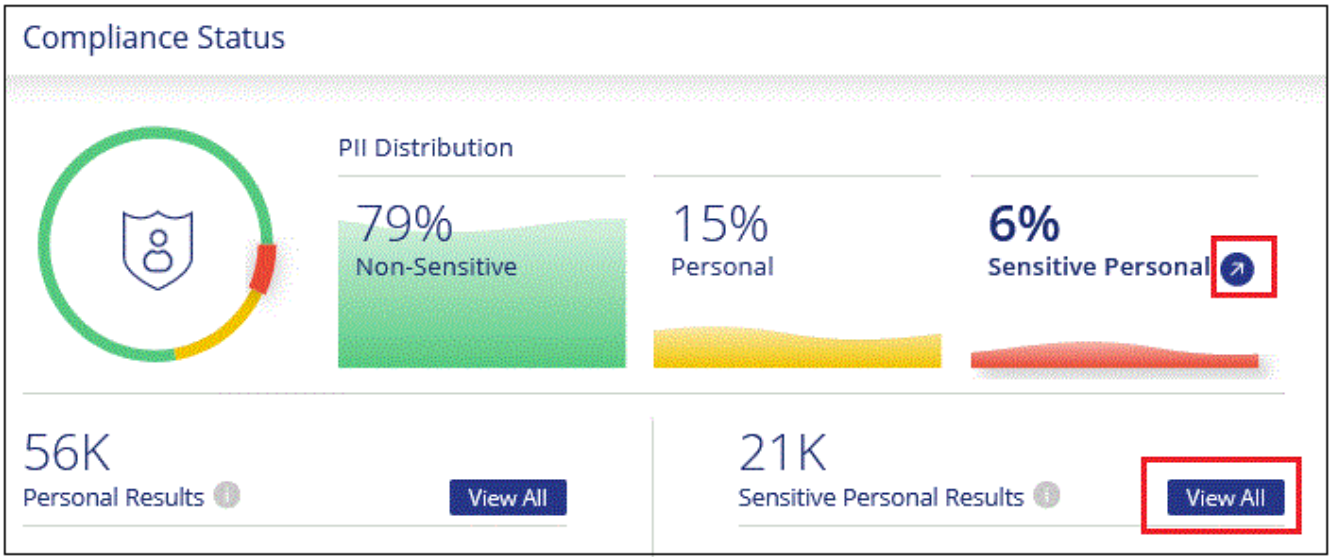
La clasificación de BlueXP utiliza la inteligencia artificial (IA), el procesamiento del lenguaje natural (NLP), el aprendizaje automático (ML) y la computación cognitiva (CC) para entender el significado del contenido que escanea para extraer entidades y categorizarlo adecuadamente.

Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Gracias a sus capacidades de PLN, la clasificación de BlueXP puede distinguir la diferencia entre una frase que sea «George es mexicano» (que indica datos confidenciales según el artículo 9 del RGPD) y otra que sea «George está comiendo comida mexicana».

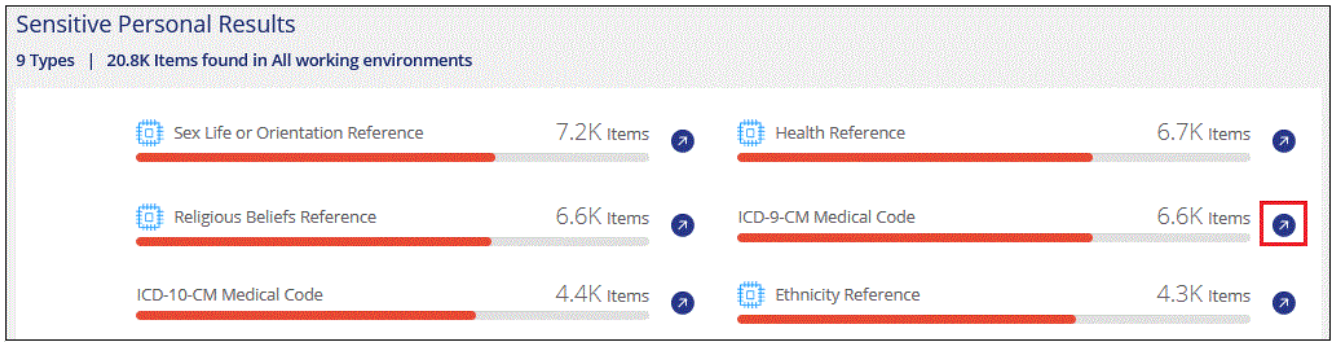
> Sólo se admite inglés cuando se escanea datos personales confidenciales. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Para investigar los detalles de todos los datos personales confidenciales, haga clic en el icono situado junto al porcentaje de datos personales confidenciales.



3. Para investigar los detalles de un tipo específico de datos personales confidenciales, haga clic en **Ver todo** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales confidenciales.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Ver archivos por categorías

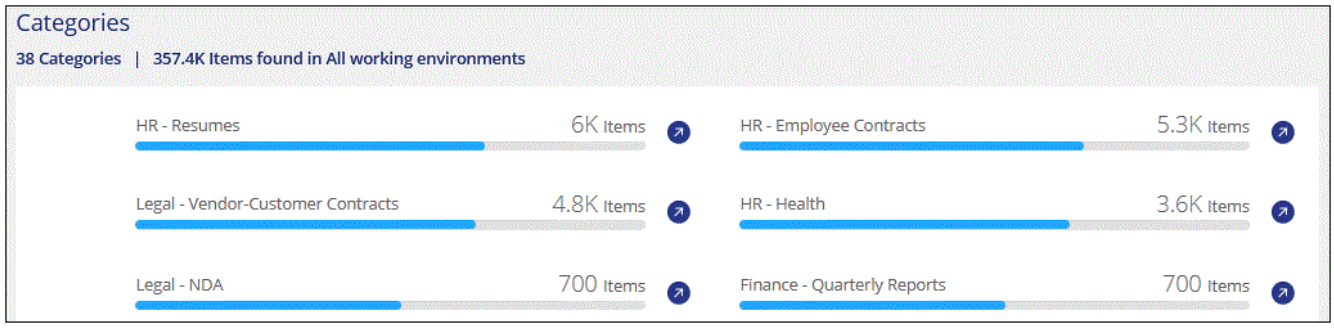
La clasificación de BlueXP toma los datos que ha escaneado y los divide en distintos tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. "Vea la lista de categorías".

Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

> Las categorías son: Inglés, alemán y español. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Haga clic en el icono **investigar resultados** de una de las 4 categorías principales directamente desde la pantalla principal, o haga clic en **Ver todos** y luego haga clic en el icono de cualquiera de las categorías.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

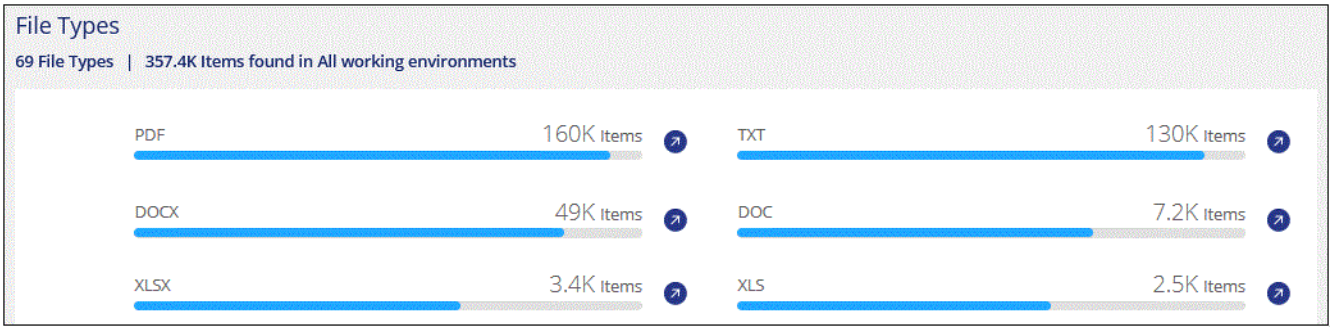
Ver archivos por tipos de archivo

La clasificación de BlueXP toma los datos que ha escaneado y los desglosa por según el tipo de archivo. La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente. "Consulte la lista de tipos de archivo".

Por ejemplo, puede almacenar archivos CAD que incluyan información muy confidencial sobre su organización. Si no está seguro, puede tomar el control de los datos confidenciales restringiendo permisos o moviendo los archivos a otra ubicación.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Haga clic en el icono **investigar resultados** de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y, a continuación, haga clic en el icono de cualquiera de los tipos de archivo.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

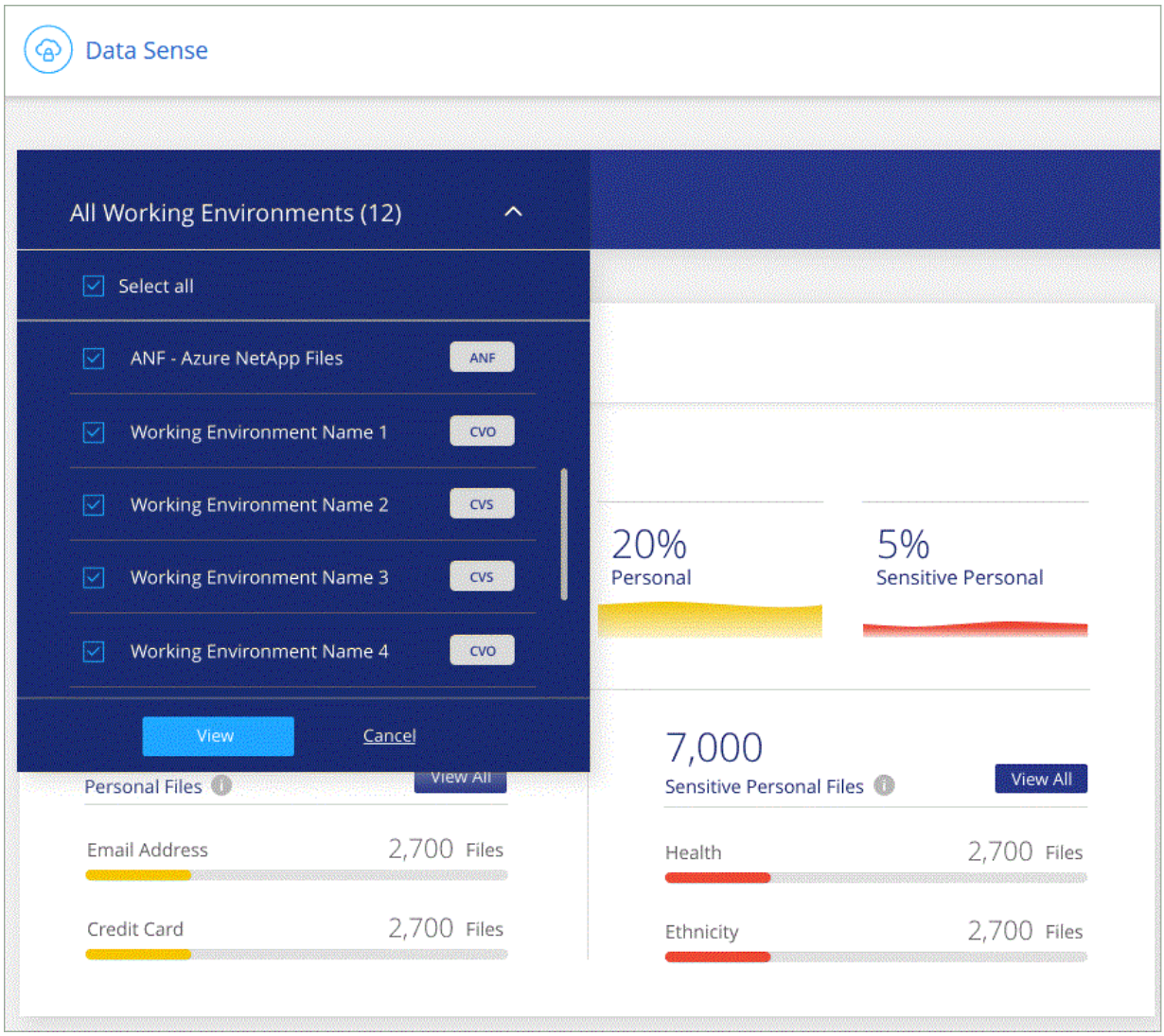
Ver datos del panel de control para entornos de trabajo específicos

Puedes filtrar el contenido de la consola de clasificación de BlueXP para ver los datos de cumplimiento de normativas de todos los entornos de trabajo y bases de datos, o simplemente para entornos de trabajo específicos.

Al filtrar la consola, la clasificación de BlueXP define los datos de cumplimiento y los informes solo a los entornos de trabajo que has seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Categorías de datos privados

Hay muchos tipos de datos privados que la clasificación de BlueXP puede identificar en tus volúmenes, bloques de Amazon S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint, etc. Y cuentas de Google Drive. Vea las categorías a continuación.

> Si necesita la clasificación de BlueXP para identificar otros tipos de datos privados, como números de identificación nacionales o identificadores sanitarios adicionales, envíe un correo electrónico a ng-contact-data-sense@netapp.com con su solicitud.

Tipos de datos personales

Los datos personales encontrados en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna de la siguiente tabla identifica si la clasificación de BlueXP lo utiliza "validación de proximidad" validar los resultados del identificador.

Los idiomas en los que se pueden reconocer estos elementos se identifican en la tabla.

Tenga en cuenta que puede agregar a la lista de datos personales que se encuentran en sus archivos. Si vas

a analizar un servidor de bases de datos, la función *Data Fusion* te permite elegir identificadores adicionales que buscará la clasificación de BlueXP en sus exploraciones seleccionando columnas en una tabla de base de datos. También puede agregar palabras clave personalizadas desde un archivo de texto o patrones personalizados utilizando una expresión regular. Consulte "Agregar identificadores de datos personales a tus análisis de clasificación de BlueXP" para obtener más detalles.

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
Generales	Número de tarjeta de crédito	No	✓	✓	✓		✓
	Datos sujetos	No	✓	✓	✓		
	Dirección de correo electrónico	No	✓	✓	✓		✓
	Número IBAN (número internacional de cuenta bancaria)	No	✓	✓	✓		✓
	Dirección IP	No	✓	✓	✓		✓
	Contraseña	Sí	✓	✓	✓		✓

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
Identificadores nacionales							

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
	ID esloveno (EMSO)	Sí	✓	✓	✓		
	ID sudafricano	Sí	✓	✓	✓		
	Número de identificación fiscal en español	Sí	✓	✓	✓		
	ID sueco	Sí	✓	✓	✓		
	Licencia de conducir de Texas	Sí	✓	✓	✓		
	REINO UNIDO ID (NINO)	Sí	✓	✓	✓		
	Licencia de conducir de Estados Unidos California	Sí	✓	✓	✓		
	Licencia de conducir de Estados Unidos Indiana	Sí	✓	✓	✓		
	Licencia de conducir de los Estados Unidos de Nueva York	Sí	✓	✓	✓		
	Número de Seguro Social de Estados Unidos (SSN)	Sí	✓	✓	✓		

Tipos de datos personales confidenciales

Los datos personales confidenciales que puede encontrar la clasificación de BlueXP en los archivos incluyen la siguiente lista.

Los elementos de esta categoría sólo se pueden reconocer en inglés en este momento.

Procedimientos penales referencia
Datos relativos a las condenas y delitos penales de una persona natural.

Referencia étnica
Datos relativos al origen racial o étnico de una persona natural.

Referencia de Salud
Datos relativos a la salud de una persona física.

Códigos médicos ICD-9-cm
Códigos utilizados en la industria médica y de la salud.

Códigos médicos ICD-10-cm
Códigos utilizados en la industria médica y de la salud.

Creencias filosóficas referencia
Datos relativos a las creencias filosóficas de una persona natural.

Opiniones políticas referencia
Datos relativos a las opiniones políticas de una persona natural.

Referencia de creencias religiosas
Datos relativos a las creencias religiosas de una persona natural.

Referencia de vida sexual o orientación
Datos relativos a la vida sexual o la orientación sexual de una persona natural.

Tipos de categorías

La clasificación de BlueXP categoriza los datos de la siguiente manera.

La mayoría de estas categorías pueden ser reconocidas en inglés, alemán y español.

Categoría	Tipo	Inglés	Alemán	Español
Finanzas	Hojas de balance	✓	✓	✓
	Órdenes de compra	✓	✓	✓
	Facturas	✓	✓	✓
	Informes trimestrales	✓	✓	✓
RR. HH	Comprobaciones de fondo	✓		✓
	Planes de compensación	✓	✓	✓
	Contratos de empleados	✓		✓
	Revisiones de empleados	✓		✓
	Salud	✓		✓
	Se reanudará	✓	✓	✓
Legal	NDAS	✓	✓	✓
	Contratos con el proveedor y el cliente	✓	✓	✓
Marketing	Campañas	✓	✓	✓
	Conferencias	✓	✓	✓
Operaciones	Informes de auditoría	✓	✓	✓
Ventas	Pedidos de ventas	✓	✓	
Servicios	RFI	✓		✓
	RFP	✓		✓
	CERDA	✓	✓	✓
	Entrenamiento	✓	✓	✓
Soporte técnico	Quejas y boletos	✓	✓	✓

Los siguientes metadatos también se categorizan y se identifican en los mismos idiomas compatibles:

- Datos de aplicaciones
- Archivos de archivo
- Audio
- Datos de aplicaciones de negocio
- Archivos CAD
- Codificación
- Dañado

- Archivos de base de datos e índice
- Breadcrumbs de clasificación de BlueXP
- Archivos de diseño
- Datos de aplicación de correo electrónico
- Cifrado (archivos con una puntuación de entropía alta)
- Ejecutables
- Datos de aplicaciones financieras
- Datos de aplicación de salud
- Imágenes
- Registros
- Documentos varios
- Presentaciones diversas
- Hojas de cálculo varias
- Varios "desconocidos"
- Archivos protegidos con contraseña
- Datos estructurados
- Vídeos
- Archivos de byte cero

Tipos de archivos

La clasificación de BlueXP analiza todos los archivos para buscar información de categorías y metadatos y muestra todos los tipos de archivos en la sección Tipos de archivos de la consola.

Pero cuando la clasificación de BlueXP detecta información personal identificable (PII) o cuando realiza una búsqueda DSAR, solo son compatibles los siguientes formatos de archivo:

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

Precisión de la información encontrada

NetApp no puede garantizar la precisión del 100 % de los datos personales y los datos personales confidenciales que identifica la clasificación de BlueXP. Siempre debe validar la información revisando los datos.

Según nuestras pruebas, la tabla siguiente muestra la precisión de la información que encuentra la clasificación de BlueXP. La dividiremos por *precision* y *RECALL*:

Precisión

La probabilidad de que lo que encuentra la clasificación de BlueXP se haya identificado correctamente. Por ejemplo, una tasa de precisión del 90% para los datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal contienen realmente información personal. 1 de cada 10 archivos sería un falso positivo.

Recuperar

La probabilidad de que la clasificación de BlueXP encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70 % de los datos personales significa que la clasificación de BlueXP puede identificar 7 de cada 10 archivos que contengan realmente información personal en tu organización. La clasificación de BlueXP faltaría el 30 % de los datos y no aparecerá en el panel.

Constantemente estamos mejorando la precisión de nuestros resultados. Esas mejoras estarán disponibles de forma automática en futuras versiones de clasificación de BlueXP.

Tipo	Precisión	Recuperar
Datos personales - General	90%-95%	60%-80%
Datos personales: Identificadores de país	30%-60%	40%-60%
Datos personales confidenciales	80%-95%	20%-30%
Categorías	90%-97%	60%-80%

Investigue los datos almacenados en su organización

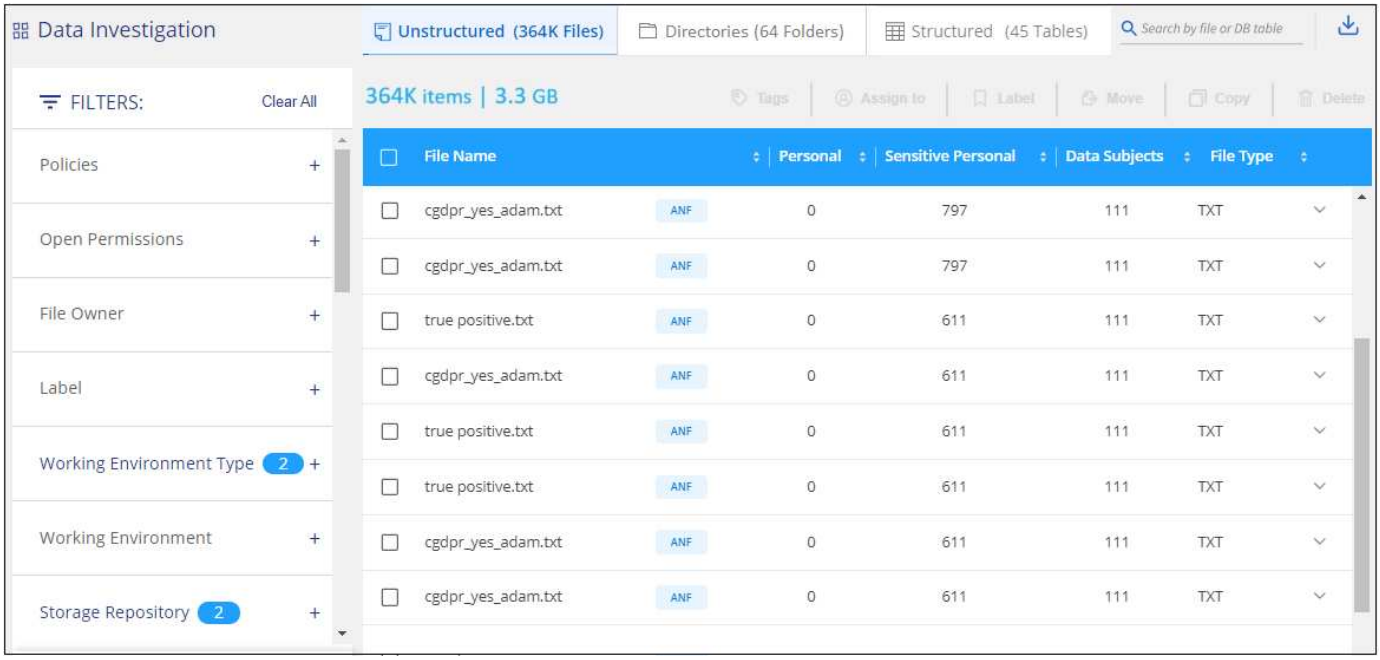
Puede investigar los datos de su organización visualizando los detalles en la página Investigación de datos. Puedes navegar a esta página desde muchas áreas de la interfaz de usuario de clasificación de BlueXP, incluidas las consolas de gobierno y cumplimiento de normativas.

Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

Filtrar datos en la página Investigación de datos

Puede filtrar el contenido de la página de investigación para que muestre solo los resultados que desea ver. Esta es una característica muy eficaz porque después de afinar los datos, puede utilizar la barra de botones en la parte superior de la página para realizar una variedad de acciones, incluyendo copiar archivos, mover archivos, agregar una etiqueta o etiqueta AIP a los archivos, y mucho más.

Si desea descargar el contenido de la página como un informe después de haberlo afinado, haga clic en botón. Vaya aquí para obtener detalles sobre el informe de investigación de datos.



- Las pestañas de nivel superior permiten ver datos de archivos (datos no estructurados), directorios (carpetas y recursos compartidos de archivos) o de bases de datos (datos estructurados).
- Los controles de la parte superior de cada columna permiten ordenar los resultados en orden numérico o alfabético.
- Los filtros del panel izquierdo permiten afinar los resultados seleccionando los atributos descritos en las secciones siguientes.

Filtrar datos por sensibilidad y contenido

Utilice los siguientes filtros para ver cuánta información confidencial contiene los datos.

Filtro	Detalles
Categoría	Seleccione la "tipos de categorías".
Nivel de sensibilidad	Seleccione el nivel de sensibilidad: Personal, personal sensible o no confidencial.
Número de identificadores	Seleccione el rango de identificadores confidenciales detectados por archivo. Incluye datos personales y datos personales confidenciales. Al filtrar en Directorios, la clasificación de BlueXP totaliza las coincidencias de todos los archivos de cada carpeta (y subcarpetas). NOTA: El lanzamiento de diciembre de 2023 (versión 1.26.6) eliminó temporalmente la opción de calcular el número de datos de información personal identificable (PII) por directorios.
Datos personales	Seleccione la "tipos de datos personales".
Datos personales confidenciales	Seleccione la "tipos de datos personales confidenciales".
Asunto de los datos	Introduzca el nombre completo o el identificador conocido de un sujeto de datos. "Obtenga más información sobre los temas de datos aquí".

Filtrar los datos por propietario y permisos de usuario

Utilice los siguientes filtros para ver los propietarios de archivos y los permisos para acceder a los datos.

Filtro	Detalles
Abra permisos	Seleccione el tipo de permisos dentro de los datos y dentro de carpetas o recursos compartidos.
Permisos de usuario/grupo	Seleccione uno o varios nombres de usuario y/o grupos, o introduzca un nombre parcial.
Propietario del archivo	Introduzca el nombre del propietario del archivo.
Número de usuarios con acceso	Seleccione uno o varios rangos de categorías para mostrar qué archivos y carpetas están abiertos a un determinado número de usuarios.

Filtrar los datos por tiempo

Utilice los siguientes filtros para ver datos según criterios de tiempo.

Filtro	Detalles
Hora de creación	Seleccione un intervalo de tiempo cuando se creó el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.
Hora de detección	Selecciona un intervalo de tiempo cuando la clasificación de BlueXP detecte el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.
Última modificación	Seleccione un intervalo de tiempo en el que se modificó por última vez el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.
Último acceso	Seleccione un intervalo de tiempo cuando se accedió por última vez al archivo o directorio (solo CIFS o NFS). También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda. Para los tipos de archivos que analiza la clasificación de BlueXP, esta es la última vez que la clasificación de BlueXP analizó el archivo. Tenga en cuenta que la clasificación de BlueXP no extrae el «tiempo de último acceso» de los siguientes orígenes de datos: SharePoint Online, SharePoint on-premises (SharePoint Server), OneDrive, Google Drive y Amazon S3.

Filtrar datos por metadatos

Utilice los siguientes filtros para ver los datos según la ubicación, el tamaño y el directorio o el tipo de archivo.

Filtro	Detalles
Ruta del archivo	Introduzca hasta 20 rutas parciales o completas que desee incluir o excluir de la consulta. Si introduces ambas rutas de inclusión y excluyes las rutas, la clasificación de BlueXP busca primero todos los archivos de las rutas incluidas, luego quita los archivos de las rutas excluidas y, a continuación, muestra los resultados. Tenga en cuenta que el uso de "*" en este filtro no tiene ningún efecto y que no puede excluir carpetas específicas del análisis; se analizarán todos los directorios y archivos de un recurso compartido configurado.
Tipo de directorio	Seleccione el tipo de directorio; "Compartir" o "carpeta".
Tipo de archivo	Seleccione la "tipos de archivos".
Tamaño de archivo	Seleccione el rango de tamaño del archivo.
Hash de archivo	Introduzca el hash del archivo para buscar un archivo específico, aunque el nombre sea diferente.

Filtre los datos por tipo de almacenamiento

Utilice los siguientes filtros para ver datos por tipo de almacenamiento.

Filtro	Detalles
Tipo de entorno de trabajo	Seleccione el tipo de entorno de trabajo. OneDrive, SharePoint y Google Drive están clasificados en "aplicaciones".
Nombre del entorno de trabajo	Seleccione entornos de trabajo específicos.
Repositorio de almacenamiento	Seleccione el repositorio de almacenamiento, por ejemplo, un volumen o un esquema.

Filtre los datos por etiquetas, usuarios asignados y políticas

Utilice los siguientes filtros para ver los datos por etiquetas o etiquetas AIP.

Filtro	Detalles
Normativas	Seleccione una política o políticas. Vaya "aquí" para ver la lista de directivas existentes y crear sus propias directivas personalizadas.
Etiqueta	Seleccione "Etiquetas AIP" que se asignan a sus archivos.
Etiquetas	Seleccione "la etiqueta o las etiquetas" que se asignan a sus archivos.
Asignado a.	Seleccione el nombre de la persona a la que se asigna el archivo.

Filtrar datos por estado de análisis

Use el siguiente filtro para ver los datos por el estado de escaneo de clasificación de BlueXP.

Filtro	Detalles
Estado del análisis	Seleccione una opción para mostrar la lista de archivos que están pendientes de primer análisis, que se han finalizado el análisis, que se han reescaneado pendiente o que no se han podido analizar.
Evento Análisis de exploración	Selecciona si quieres ver archivos que no estaban clasificados porque la clasificación de BlueXP no pudo revertir la hora del último acceso o los archivos que estaban clasificados aunque la clasificación de BlueXP no pudo revertir la última hora a la que se accedió.

"Consulte los detalles acerca de la Marca de hora "última en la que se accedió"" Para obtener más información acerca de los elementos que aparecen en la página Investigación al filtrar mediante el filtrado del evento Análisis de Análisis.

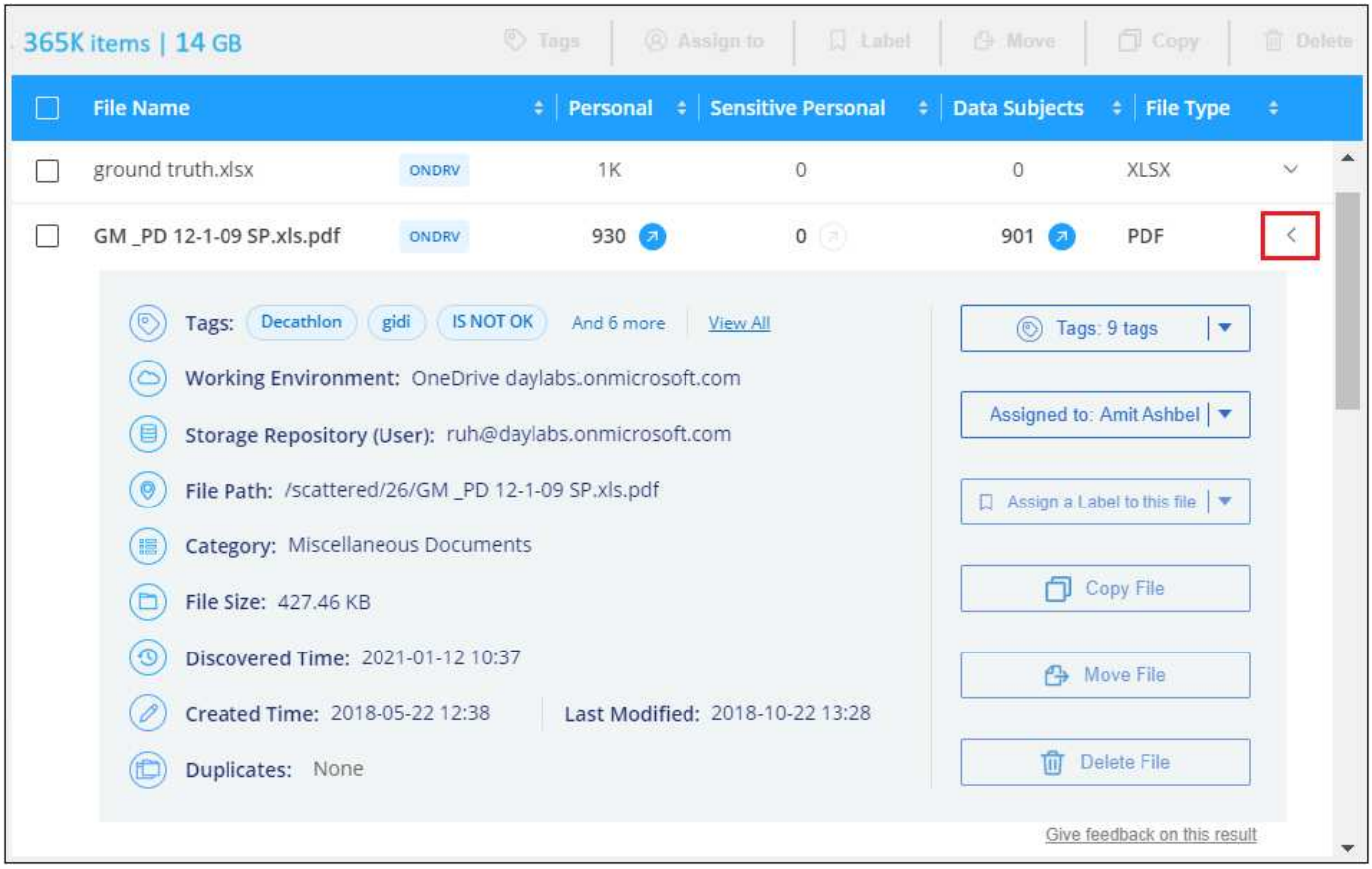
Filtrar datos por duplicados

Utilice el siguiente filtro para ver los archivos duplicados en su almacenamiento.

Filtro	Detalles
Duplicados	Seleccione si el archivo está duplicado en los repositorios.

Ver metadatos de archivo

En el panel resultados de la investigación de datos puede hacer clic en ⌄ para cualquier archivo individual para ver los metadatos del archivo.



Además de mostrarle el entorno de trabajo y el volumen en el que reside el archivo, los metadatos muestran mucha más información, incluidos los permisos de archivo, el propietario del archivo, si hay duplicados de este archivo y la etiqueta AIP asignada (si lo tiene "AIP integrado en la clasificación de BlueXP"). Esta información es útil si tiene previsto hacerlo "Crear políticas" porque puede ver toda la información que puede utilizar para filtrar sus datos.

Tenga en cuenta que no toda la información está disponible para todas las fuentes de datos - sólo lo que es apropiado para ese origen de datos. Por ejemplo, el nombre de volumen, los permisos y las etiquetas AIP no son relevantes para los archivos de la base de datos.

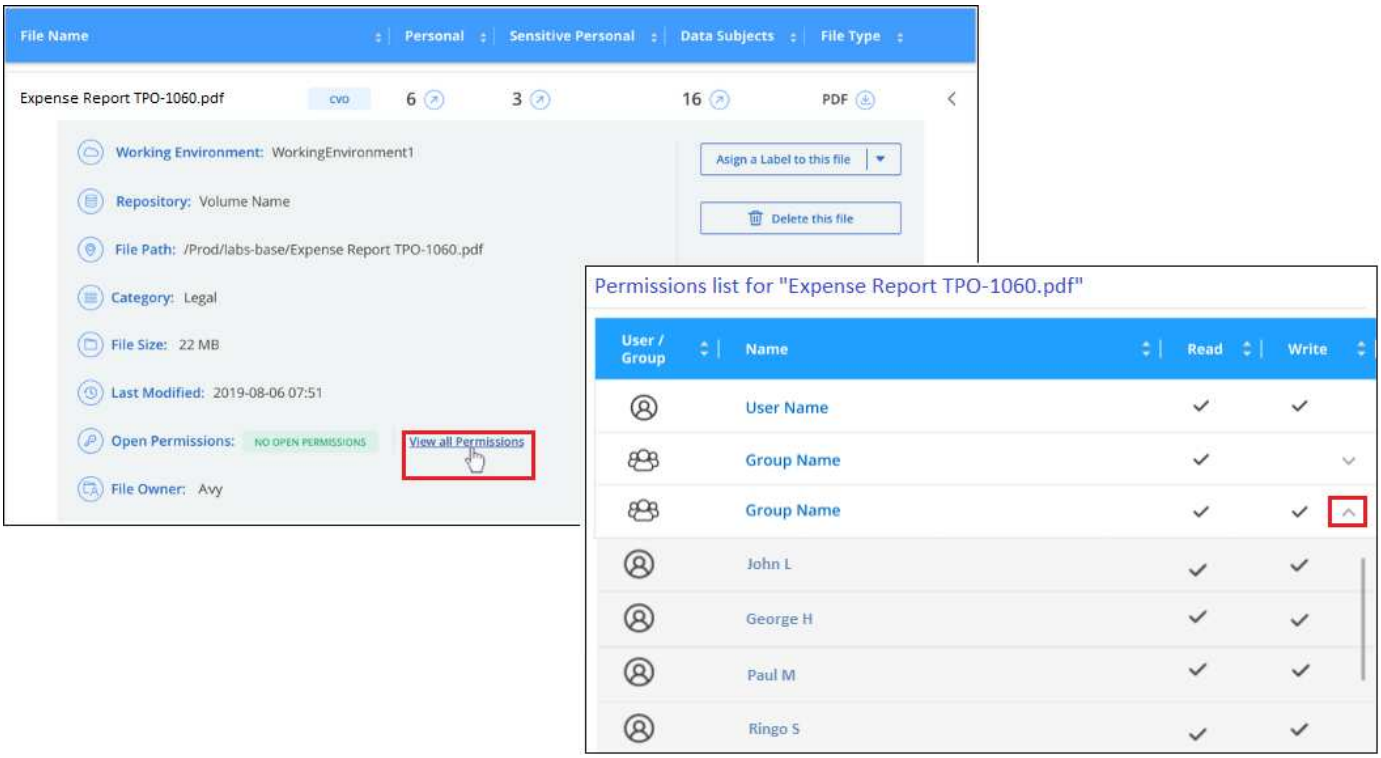
Al ver los detalles de un único archivo, hay algunas acciones que puede realizar en el archivo:

- Puede mover o copiar el archivo a cualquier recurso compartido NFS. Consulte "Mover archivos de origen a un recurso compartido NFS" y.. "Copiando archivos de origen a un recurso compartido NFS" para obtener más detalles.
- Puede eliminar el archivo. Consulte "Eliminando archivos de origen" para obtener más detalles.
- Puede asignar un estado determinado al archivo. Consulte "Aplicación de etiquetas" para obtener más detalles.
- Puede asignar el archivo a un usuario de BlueXP para que sea responsable de las acciones de seguimiento que se deban realizar en el archivo. Consulte "Asignar usuarios a un archivo" para obtener más detalles.
- Si has integrado etiquetas AIP con la clasificación de BlueXP, puedes asignar una etiqueta a este archivo o cambiarla a otra, si ya existe alguna. Consulte "Asignación manual de etiquetas AIP" para obtener más detalles.

Ver permisos para archivos y directorios

Para ver una lista de todos los usuarios o grupos que tienen acceso a un archivo o directorio y los tipos de permisos que tienen, haga clic en **Ver todos los permisos**. Este botón solo está disponible para datos en recursos compartidos CIFS, SharePoint Online, SharePoint en las instalaciones y OneDrive.

Tenga en cuenta que, si ve SID (identificadores de seguridad) en lugar de nombres de usuarios y grupos, debería integrar su Active Directory en la clasificación de BlueXP. "Descubra cómo hacerlo".



Puede hacer clic en ⌄ para que cualquier grupo vea la lista de usuarios que forman parte del grupo.

Además, Puede hacer clic en el nombre de un usuario o un grupo y la página de investigación se muestra con el nombre de ese usuario o grupo rellenado en el filtro “permisos de usuario/grupo” para poder ver todos los archivos y directorios a los que tiene acceso el usuario o grupo.

Compruebe si hay archivos duplicados en los sistemas de almacenamiento

Puede ver si se están almacenando ficheros duplicados en los sistemas de almacenamiento. Esto resulta útil para identificar áreas en las que puede ahorrar espacio de almacenamiento. También puede ser útil asegurarse de que determinados archivos que tienen permisos específicos o información confidencial no se dupliquen innecesariamente en sus sistemas de almacenamiento.

Todos los archivos (sin incluir las bases de datos) que son de 1 MB o más y que contienen información personal o personal confidencial, se comparan para ver si hay duplicados. Puedes usar los filtros de página de investigación “Tamaño de archivo” junto con “Duplicados” para ver qué archivos de un rango de tamaño determinado están duplicados en tu entorno.

La clasificación de BlueXP usa tecnología de hash para determinar los archivos duplicados. Si algún archivo tiene el mismo código hash que otro archivo, podemos estar 100% seguros de que los archivos son duplicados exactos, incluso si los nombres de archivo son diferentes.

Puede descargar la lista de archivos duplicados y enviarlos al administrador de almacenamiento para que puedan decidir qué archivos se pueden eliminar, si los hay. O usted puede "elimine el archivo" usted mismo si está seguro de que una versión específica del archivo no es necesaria.

Ver todos los archivos duplicados

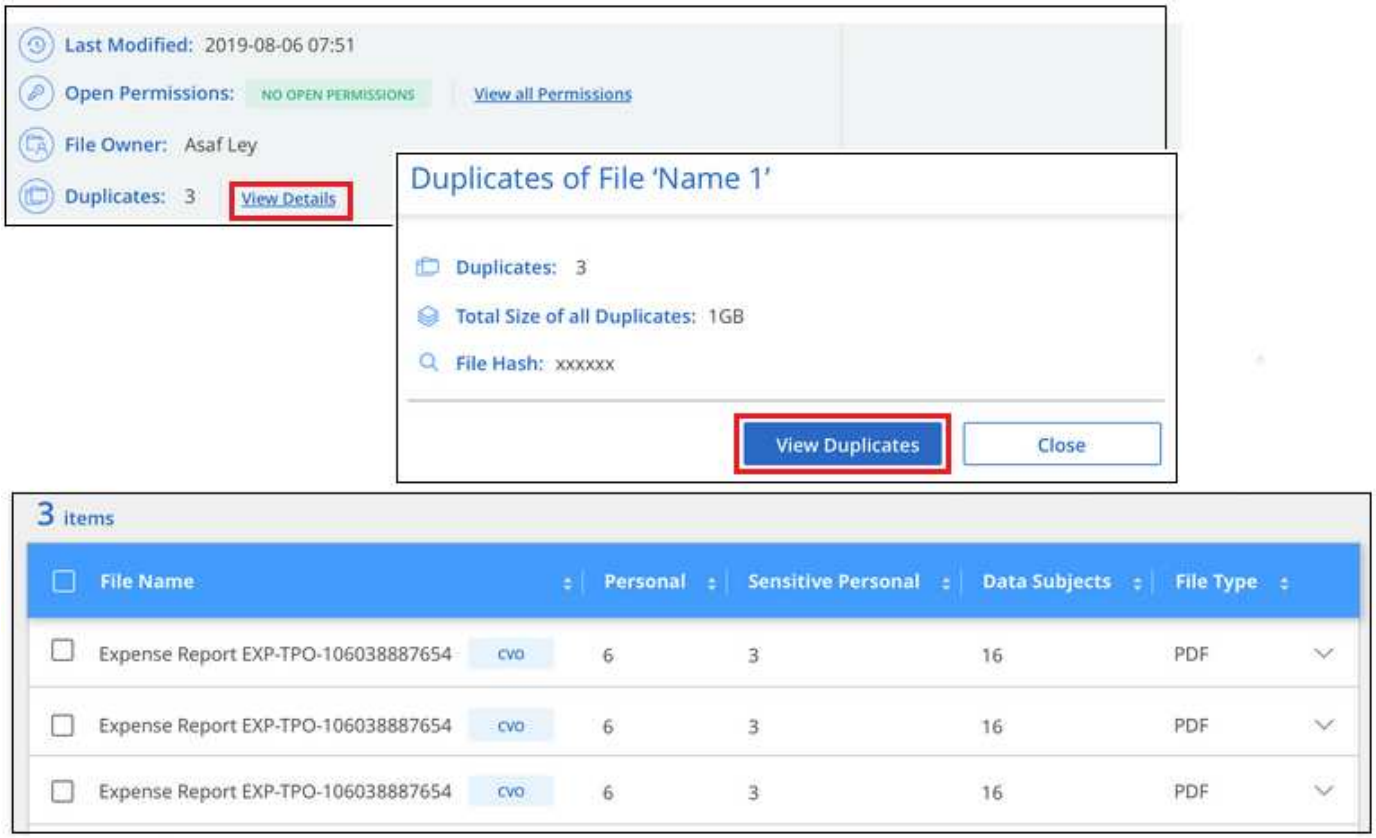
Si desea obtener una lista de todos los archivos duplicados en los entornos de trabajo y los orígenes de datos que está analizando, puede utilizar el filtro llamado **duplicados > tiene duplicados** en la página Investigación de datos.

Todos los archivos duplicados se muestran en la página de resultados.

Ver si un archivo específico está duplicado

Si desea ver si un único archivo tiene duplicados, en el panel resultados de investigación de datos puede hacer clic en ⌄ para cualquier archivo individual para ver los metadatos del archivo. Si hay duplicados de un archivo determinado, esta información aparece junto al campo *Duplicates*.

Para ver la lista de archivos duplicados y su ubicación, haga clic en **Ver detalles**. En la página siguiente, haga clic en **Ver duplicados** para ver los archivos en la página Investigación.



Puede usar el valor "hash de archivo" que se proporciona en esta página e introducirlo directamente en la página Investigación para buscar un archivo duplicado específico en cualquier momento, o puede usarlo en una directiva.

Informe de investigación de datos

El Informe de investigación de datos es una descarga del contenido filtrado de la página Investigación de datos.

El informe está disponible en dos formatos diferentes:

- Como archivo .CSV que se puede guardar en el equipo local.

  Este informe puede incluir un máximo de 10.000 filas de datos.

- Como un archivo .JSON que se exporta a un recurso compartido NFS.

  Si hay más de 250.000 filas de datos, se crean archivos .JSON adicionales.

Al exportar a un recurso compartido de archivos, asegúrese de que la clasificación de BlueXP tenga los permisos correctos para acceder a las exportaciones.

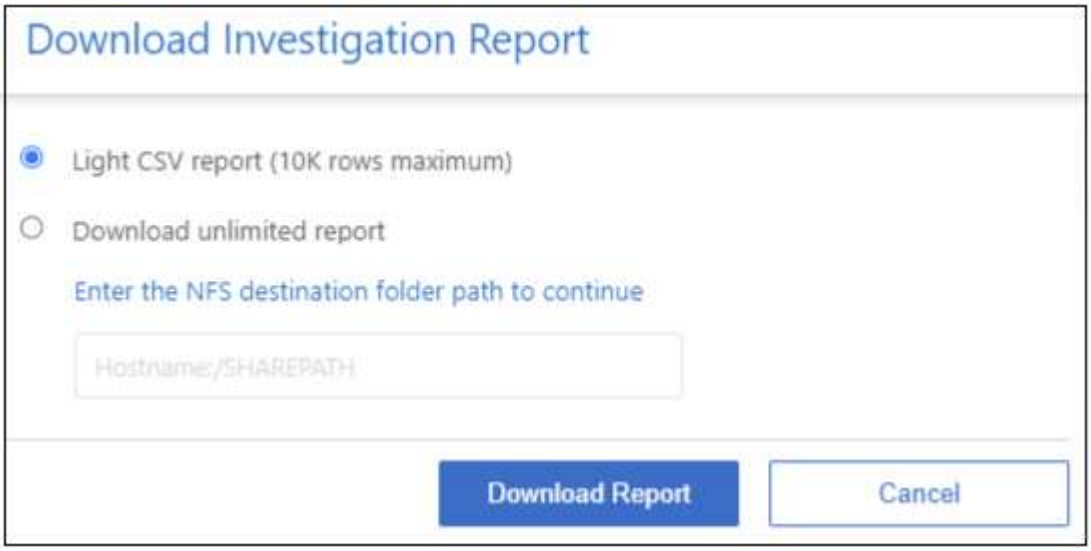
Puede haber hasta tres archivos de informes descargados si la clasificación de BlueXP está analizando archivos (datos no estructurados), directorios (carpetas y recursos compartidos de archivos) y bases de datos (datos estructurados).

Generar el informe de investigación de datos

Pasos

1. En la página Data Investigation, haga clic en en la parte superior derecha de la página.
2. Seleccione si desea descargar un informe .CSV o un informe .JSON de los datos y haga clic en **Descargar informe**.

   Al seleccionar un informe .JSON, introduzca el nombre del recurso compartido NFS al que se descargará el informe con el formato `<host_name>:/<share_path>`.



Resultado

Un cuadro de diálogo muestra un mensaje que indica que los informes se están descargando.

Puede ver el progreso de la generación de informes JSON en la "Panel Estado de acciones".

Lo que se incluye en cada informe de investigación de datos

El **Informe de datos de archivos no estructurados** incluye la siguiente información sobre sus archivos:

- Nombre de archivo
- Tipo de ubicación
- Nombre del entorno de trabajo
- Repositorio de almacenamiento (por ejemplo, un volumen, un bloque, recursos compartidos)
- Tipo de repositorio
- Ruta del archivo
- Tipo de archivo

- Tamaño de archivo (en MB)
- Hora de creación
- Última modificación
- Último acceso
- Propietario del archivo
- Categoría
- Información personal
- Información personal confidencial
- Permisos abiertos
- Error de análisis de adquisición
- Fecha de detección de eliminación

  Una fecha de detección de eliminación identifica la fecha en la que se eliminó o movió el archivo. Esto le permite identificar cuándo se han movido los archivos confidenciales. Los archivos eliminados no forman parte del recuento de números de archivo que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

Informe de datos de directorios no estructurados incluye la siguiente información sobre sus carpetas y recursos compartidos de archivos:

- Tipo de entorno de trabajo
- Nombre del entorno de trabajo
- Nombre del directorio
- Repositorio de almacenamiento (por ejemplo, una carpeta o archivos compartidos)
- Propietario del directorio
- Hora de creación
- Hora de detección
- Última modificación
- Último acceso
- Permisos abiertos
- Tipo de directorio

El **Informe de datos estructurados** incluye la siguiente información sobre las tablas de la base de datos:

- Nombre de tabla DE BASE de DATOS
- Tipo de ubicación
- Nombre del entorno de trabajo
- Repositorio de almacenamiento (por ejemplo, un esquema)
- Recuento de columnas
- Recuento de filas
- Información personal

- Información personal confidencial

Organice sus datos privados

La clasificación de BlueXP ofrece muchas formas de gestionar y organizar los datos privados. Esto le facilita ver los datos que más le importan.

- Si está suscrito a. "Protección de información de Azure (AIP)" Para clasificar y proteger tus archivos, puedes usar la clasificación de BlueXP para gestionar esas etiquetas de AIP.

> La versión de diciembre de 2023 (v1.26.6) eliminó temporalmente la opción de integrar datos mediante etiquetas de protección de información de Azure (AIP).

- Puede agregar etiquetas a los archivos que desee marcar para la organización o para algún tipo de seguimiento.
- Puede asignar un usuario de BlueXP a un archivo específico, o a varios archivos, para que la persona pueda ser responsable de administrar el archivo.
- Con la funcionalidad "Directiva" puede crear sus propias consultas de búsqueda personalizadas para que pueda ver fácilmente los resultados haciendo clic en un botón.
- Puede enviar alertas por correo electrónico a los usuarios de BlueXP o a cualquier otra dirección de correo electrónico, cuando ciertas políticas críticas devuelvan resultados.

> Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

¿Debo usar etiquetas o etiquetas?

A continuación se muestra una comparación del etiquetado de clasificación de BlueXP y el etiquetado de Azure Information Protection.

Etiquetas	Etiquetas
Las etiquetas de archivos son una parte integrada de la clasificación de BlueXP.	Requiere que se haya suscrito a la protección de información de Azure (AIP).
La etiqueta solo se conserva en la base de datos de clasificación de BlueXP: No se escribe en el archivo. No cambia el archivo, ni los tiempos de acceso o modificación del archivo.	La etiqueta forma parte del archivo y cuando la etiqueta cambia, el archivo cambia. Este cambio también cambia los tiempos de acceso y modificación del archivo.
Puede tener varias etiquetas en un único archivo.	Puede tener una etiqueta en un solo archivo.
La etiqueta se puede usar para la acción de clasificación interna de BlueXP, como copiar, mover, eliminar, ejecutar una política etc.	Otros sistemas que pueden leer el archivo pueden ver la etiqueta, que se puede utilizar para automatización adicional.
Sólo se utiliza una sola llamada API para ver si un archivo tiene una etiqueta.	

Categorice los datos mediante etiquetas AIP

Puede gestionar etiquetas AIP en los archivos a los que está analizando la clasificación de BlueXP si ya se ha suscrito "Protección de información de Azure (AIP)". AIP le permite clasificar y proteger documentos y archivos aplicando etiquetas al contenido. La clasificación de BlueXP te permite ver las etiquetas que ya están asignadas a archivos, agregar etiquetas a archivos y cambiar etiquetas cuando ya existe una etiqueta.

La clasificación de BlueXP admite etiquetas AIP en los siguientes tipos de archivos: .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX.

- Actualmente no puede cambiar etiquetas en archivos de más de 30 MB. Para las cuentas de OneDrive, SharePoint y Google Drive, el tamaño máximo del archivo es 4 MB.
- Si un archivo tiene una etiqueta que ya no existe en AIP, la clasificación de BlueXP lo considera como un archivo sin una etiqueta.
- Si has implementado la clasificación de BlueXP en una región gubernamental o en una ubicación on-premises que no tiene acceso a Internet (también conocida como sitio oscuro), la funcionalidad de etiqueta AIP no estará disponible.

Integre las etiquetas AIP en su espacio de trabajo

Para poder administrar etiquetas AIP, debes integrar la funcionalidad de etiqueta AIP en la clasificación de BlueXP iniciando sesión en tu cuenta de Azure existente. Una vez activado, puede administrar etiquetas AIP dentro de los archivos para todos "fuentes de datos" En el espacio de trabajo de BlueXP.

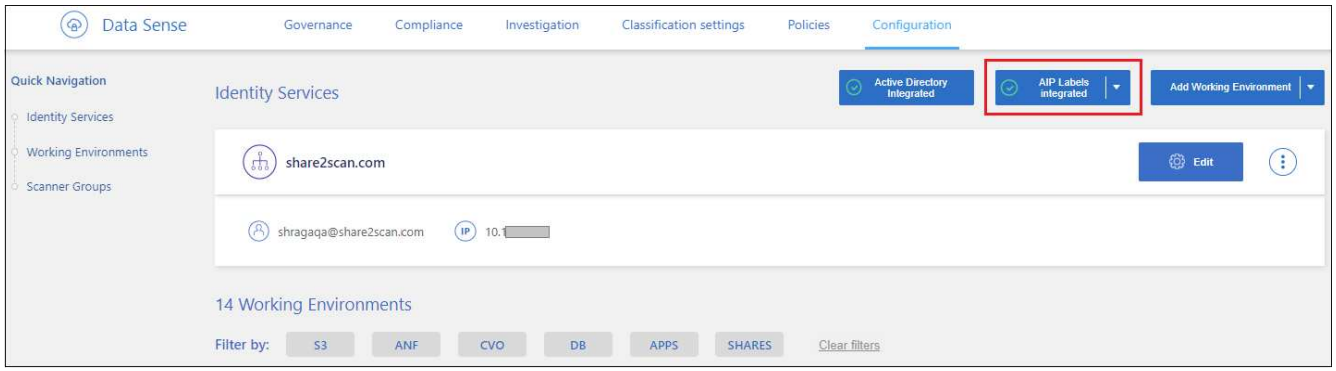
Requisitos

- Debe tener una cuenta y una licencia de Azure Information Protection.
- Debe tener las credenciales de inicio de sesión de la cuenta de Azure.
- Si planea cambiar las etiquetas de los archivos que residen en bloques de Amazon S3, asegúrese de que el permiso `s3:PutObject` Se incluye en el rol IAM. Consulte "Configuración del rol IAM".

Pasos

1. En la página Configuración de clasificación de BlueXP, haz clic en **Integrar etiquetas AIP**.

2. En el cuadro de diálogo integrar etiquetas AIP, haga clic en **Iniciar sesión en Azure**.
3. En la página de Microsoft que aparece, seleccione la cuenta e introduzca las credenciales necesarias.
4. Vuelve a la pestaña de clasificación de BlueXP y verás el mensaje «*AIP Labels se han integrado correctamente con la cuenta <account_name>*».
5. Haga clic en **Cerrar** y verá el texto *AIP Labels integrated* en la parte superior de la página.



Resultado

Puede ver y asignar etiquetas AIP desde el panel de resultados de la página Investigación. También puede asignar etiquetas AIP a archivos mediante directivas.

Vea las etiquetas AIP en sus archivos

Puede ver la etiqueta AIP actual que está asignada a un archivo.

En el panel resultados de la investigación de datos, haga clic en ⌄ para que el archivo expanda los detalles de metadatos del archivo.

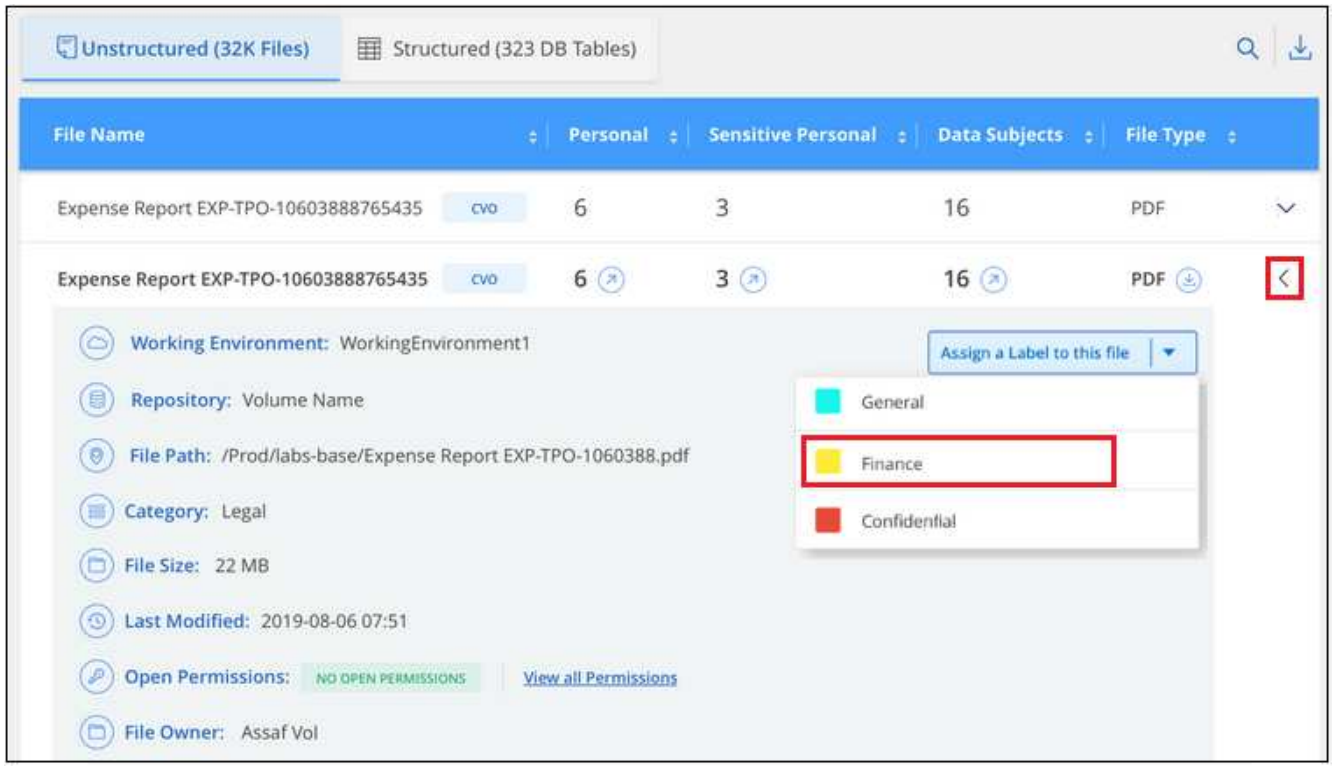
Asignar etiquetas AIP manualmente

Puedes añadir, cambiar y eliminar etiquetas AIP de tus archivos mediante la clasificación de BlueXP.

Siga estos pasos para asignar una etiqueta AIP a un único archivo.

Pasos

1. En el panel resultados de la investigación de datos, haga clic en ⌄ para que el archivo expanda los detalles de metadatos del archivo.



2. Haga clic en **asignar una etiqueta a este archivo** y, a continuación, seleccione la etiqueta.

   La etiqueta aparece en los metadatos del archivo.

Siga estos pasos para asignar una etiqueta AIP a varios archivos. Tenga en cuenta que puede asignar una etiqueta AIP a un máximo de 20 archivos a la vez (una página en la interfaz de usuario).

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea etiquetar.

   - Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
   - Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).

2. En la barra de botones, haga clic en **etiqueta** y seleccione la etiqueta AIP:

La etiqueta AIP se agrega a los metadatos de todos los archivos seleccionados.

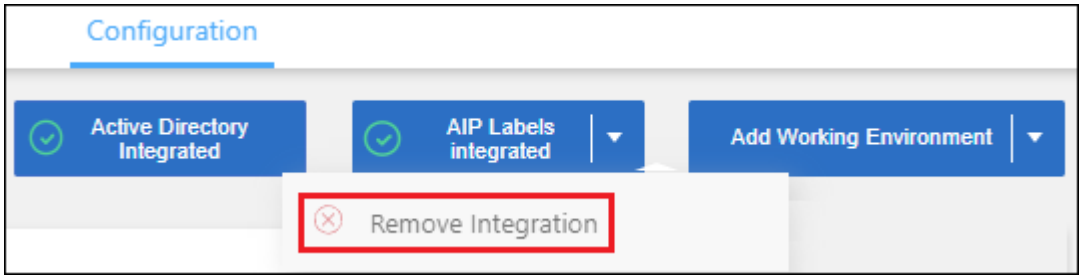
Elimine la integración AIP

Si ya no quieres tener la capacidad de administrar etiquetas AIP en archivos, puedes eliminar la cuenta AIP de la interfaz de clasificación de BlueXP.

Ten en cuenta que no se realizan cambios en las etiquetas que has añadido mediante la clasificación de BlueXP. Las etiquetas que existen en los archivos permanecerán tal como existen actualmente.

Pasos

1. En la página *Configuration*, haga clic en **Etiquetas AIP integradas > Eliminar integración**.



2. Haga clic en **Eliminar integración** en el cuadro de diálogo de confirmación.

Aplique etiquetas para gestionar los archivos escaneados

Puede agregar una etiqueta a los archivos que desee marcar para algún tipo de seguimiento. Por ejemplo, es posible que haya encontrado algunos archivos duplicados y desee eliminar uno de ellos, pero debe comprobar qué se debe eliminar. Puede agregar una etiqueta de "comprobar para eliminar" al archivo para que sepa que este archivo requiere algún tipo de investigación y acción futura.

La clasificación de BlueXP permite ver las etiquetas asignadas a archivos, añadir o quitar etiquetas de los archivos, y cambiar el nombre o eliminar una etiqueta existente.

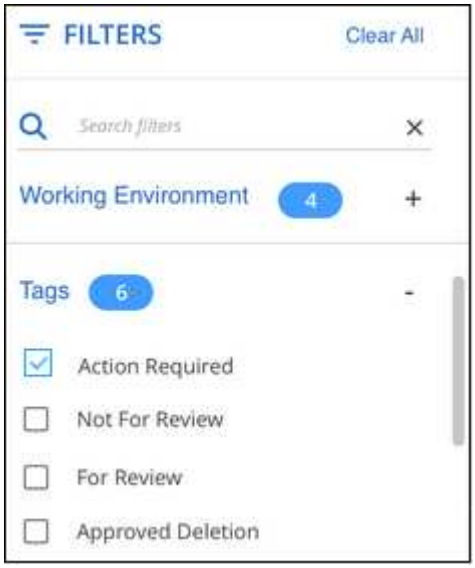
Tenga en cuenta que la etiqueta no se agrega al archivo de la misma manera que las etiquetas AIP forman parte de los metadatos del archivo. Los usuarios de BlueXP solo ven la etiqueta con la clasificación de BlueXP, para que puedas ver si es necesario eliminar o comprobar un archivo en cuanto a algún tipo de seguimiento.

Las etiquetas asignadas a archivos en la clasificación de BlueXP no están relacionadas con las etiquetas que se pueden añadir a recursos, como volúmenes o instancias de máquinas virtuales. Las etiquetas de clasificación de BlueXP se aplican a nivel de archivo.

Ver archivos que tienen determinadas etiquetas aplicadas

Puede ver todos los archivos que tienen asignadas etiquetas específicas.

1. Haga clic en la pestaña **Investigation** de la clasificación de BlueXP.
2. En la página Investigación de datos, haga clic en **Etiquetas** en el panel Filtros y, a continuación, seleccione las etiquetas necesarias.



El panel resultados de la investigación muestra todos los archivos que tienen asignadas esas etiquetas.

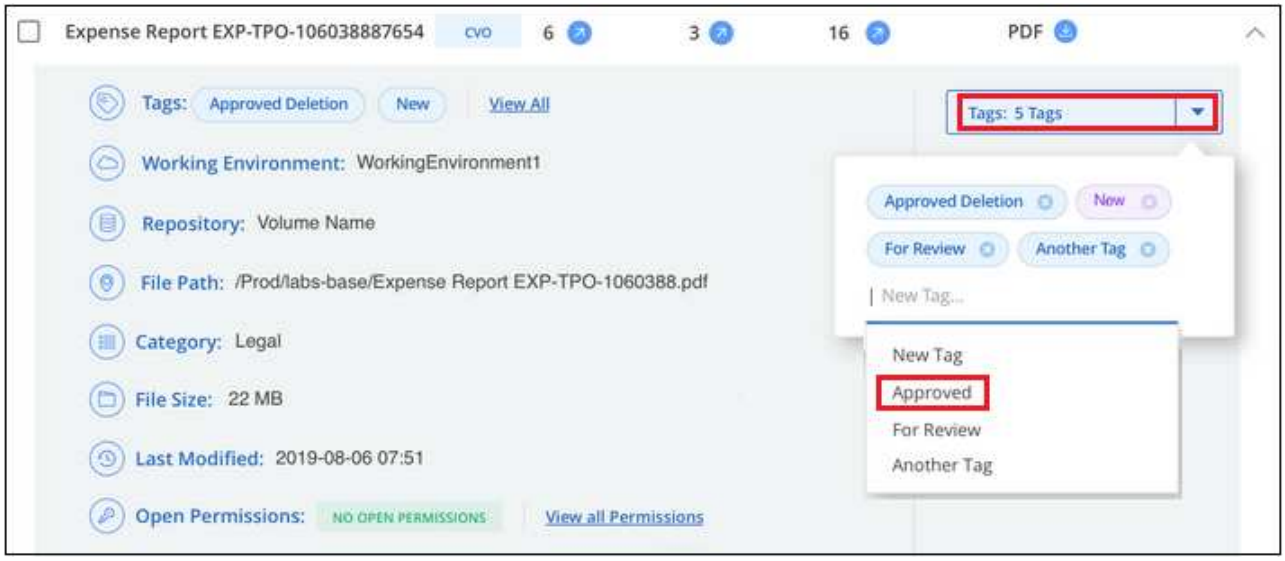
Asigne etiquetas a los archivos

Puede agregar etiquetas a un único archivo o a un grupo de archivos.

Para agregar una etiqueta a un único archivo:

Pasos

1. En el panel resultados de la investigación de datos, haga clic en ⌄ para que el archivo expanda los detalles de metadatos del archivo.
2. Haga clic en el campo **Etiquetas** y se mostrarán las etiquetas asignadas actualmente.
3. Agregue la etiqueta o las etiquetas:
   - Para asignar una etiqueta existente, haga clic en el campo **Nueva etiqueta…** y empiece a escribir el nombre de la etiqueta. Cuando aparezca la etiqueta que está buscando, selecciónela y pulse **Intro**.
   - Para crear una nueva etiqueta y asignarla al archivo, haga clic en el campo **Nueva etiqueta…**, escriba el nombre de la nueva etiqueta y pulse **Intro**.



La etiqueta aparece en los metadatos del archivo.

Para agregar una etiqueta a varios archivos:

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desee etiquetar.

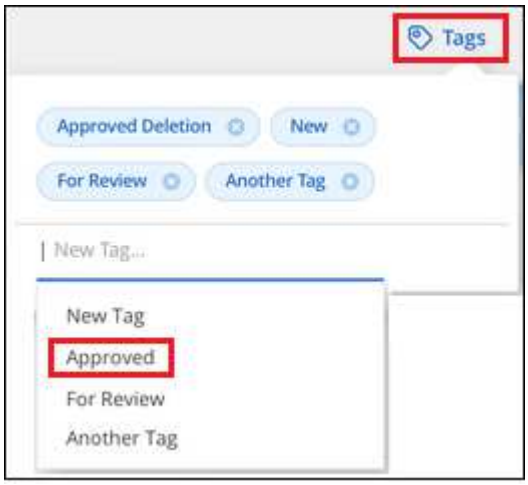
   - Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
   - Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).
   - Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (File Name) y, a continuación, en el mensaje emergente All **20** Items on this page selected Select all Items in list (63K Items), Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

     Puede aplicar etiquetas a un máximo de 100.000 archivos a la vez.

2. En la barra de botones, haga clic en **Etiquetas** y aparecerán las etiquetas asignadas actualmente.
3. Agregue la etiqueta o las etiquetas:
   - Para asignar una etiqueta existente, haga clic en el campo **Nueva etiqueta…** y empiece a escribir el

nombre de la etiqueta. Cuando aparezca la etiqueta que está buscando, selecciónela y pulse **Intro**.

- Para crear una nueva etiqueta y asignarla al archivo, haga clic en el campo **Nueva etiqueta…**, escriba el nombre de la nueva etiqueta y pulse **Intro**.



4. Apruebe la adición de etiquetas en el cuadro de diálogo de confirmación y las etiquetas se agregarán a los metadatos de todos los archivos seleccionados.

Eliminar etiquetas de los archivos

Puede eliminar una etiqueta si ya no necesita utilizarla.

Sólo tiene que hacer clic en **x** para ver una etiqueta existente.

Si ha seleccionado varios archivos, la etiqueta se elimina de todos los archivos.

Asigne usuarios para administrar ciertos archivos

Puede asignar un usuario de BlueXP a un archivo específico, o a varios archivos, para que pueda ser responsable de cualquier acción de seguimiento que necesite realizar en el archivo. Esta funcionalidad se suele utilizar con la función para agregar etiquetas de estado personalizadas a un archivo.

Por ejemplo, puede tener un archivo que contiene ciertos datos personales que permiten a demasiados usuarios acceso de lectura y escritura (permisos abiertos). Así que podría asignar la etiqueta de estado "Cambiar permisos" y asignar este archivo al usuario "Joan Smith" para que puedan decidir cómo solucionar el problema. Cuando hayan solucionado el problema, podrían cambiar la etiqueta de estado a "completado".

Tenga en cuenta que el nombre de usuario no se añade al archivo como parte de los metadatos del archivo; los usuarios de BlueXP lo ven cuando usan la clasificación de BlueXP.

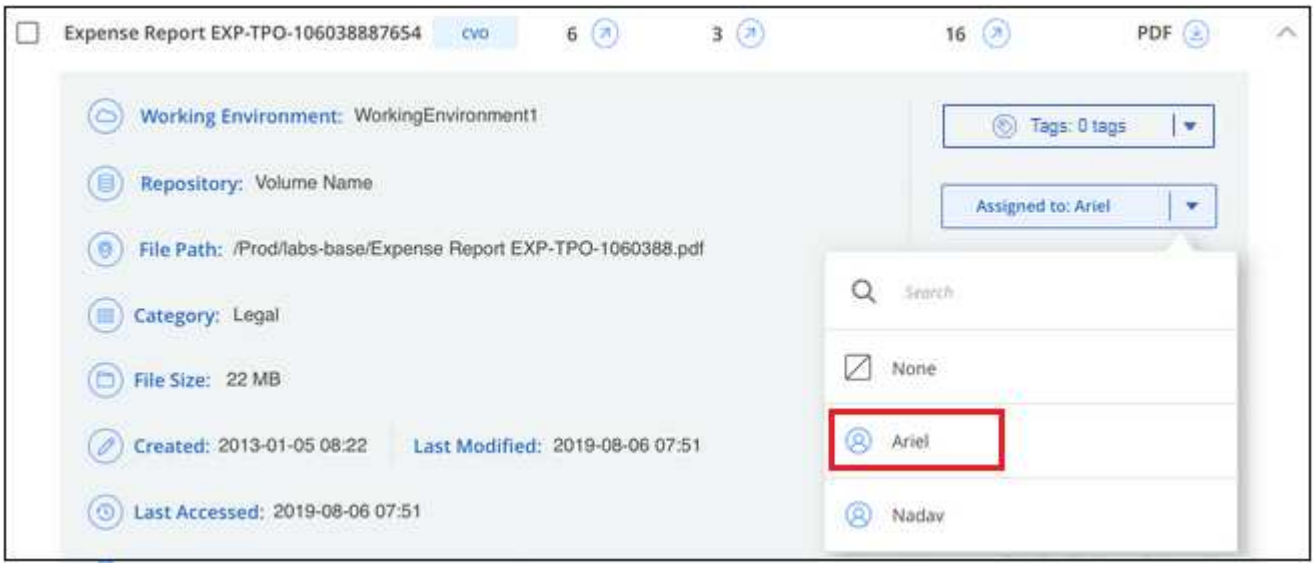
Un filtro nuevo en la página Investigación le permite ver fácilmente todos los archivos que tienen la misma persona en el campo "asignado a".

Siga estos pasos para asignar un usuario a un único archivo.

Pasos

1. En el panel resultados de la investigación de datos, haga clic en ⌄ para que el archivo expanda los detalles de metadatos del archivo.

2. Haga clic en el campo **asignado a** y seleccione el nombre de usuario.



El nombre de usuario aparece en los metadatos del archivo.

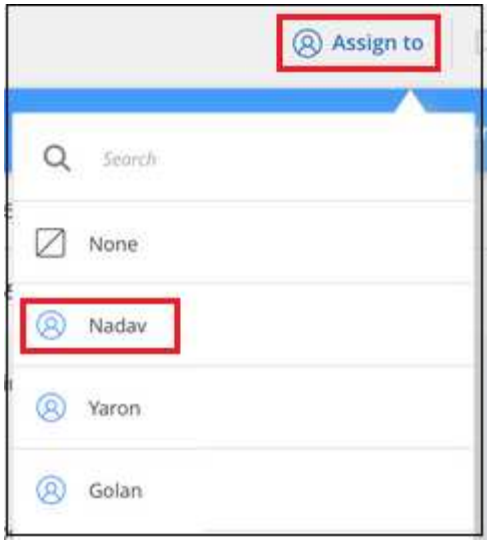
Siga estos pasos para asignar un usuario a varios archivos. Tenga en cuenta que puede asignar un usuario a un máximo de 20 archivos a la vez (una página en la interfaz de usuario).

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea asignar a un usuario.

   - Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
   - Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).

2. En la barra de botones, haga clic en **asignar a** y seleccione el nombre de usuario:



El usuario se agrega a los metadatos de todos los archivos seleccionados.

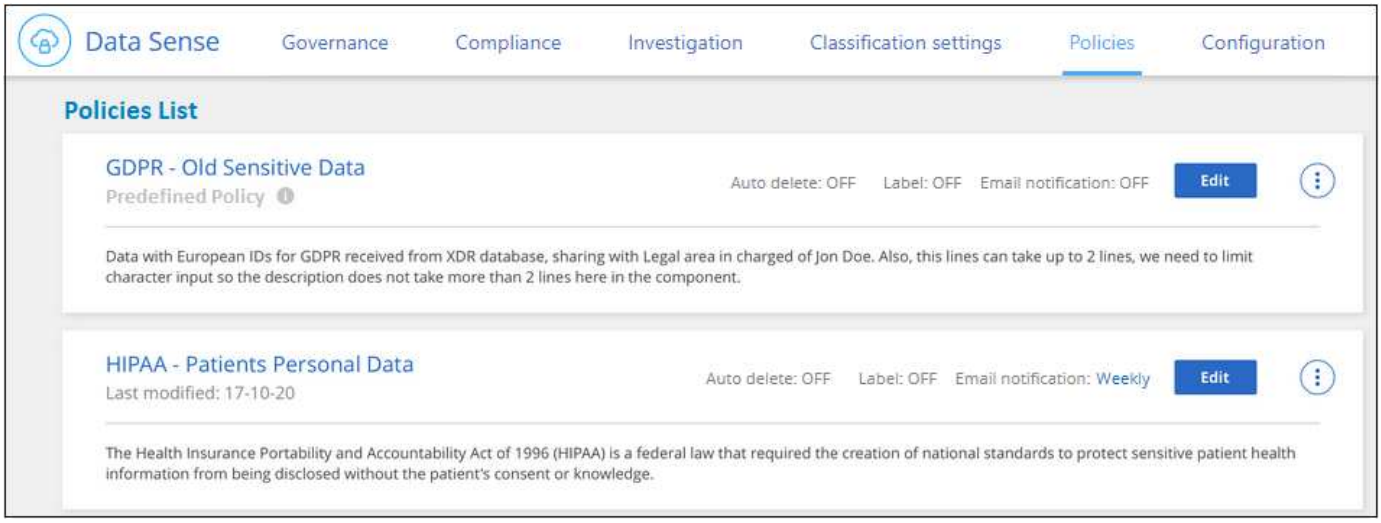
Asigne políticas a sus datos

Las directivas son como una lista de favoritos de filtros personalizados que proporcionan resultados de búsqueda en la página de investigación para consultas de cumplimiento solicitadas con frecuencia. La clasificación de BlueXP proporciona un conjunto de políticas predefinidas basadas en solicitudes habituales de los clientes. Puede crear directivas personalizadas que proporcionen resultados para búsquedas específicas de su organización.

Las políticas ofrecen la siguiente funcionalidad:

- Directivas predefinidas Desde NetApp según solicitudes de usuarios
- Capacidad de crear sus propias políticas personalizadas
- Inicie la página de investigación con los resultados de las políticas con un solo clic
- Envíe alertas por correo electrónico a los usuarios de BlueXP o a cualquier otra dirección de correo electrónico cuando determinadas políticas críticas devuelvan resultados para que pueda obtener notificaciones que protejan sus datos
- Asigne etiquetas AIP (Protección de información de Azure) automáticamente a todos los archivos que coincidan con los criterios definidos en una directiva
- Elimine archivos automáticamente (una vez al día) cuando determinadas directivas devuelvan resultados para que pueda proteger sus datos automáticamente

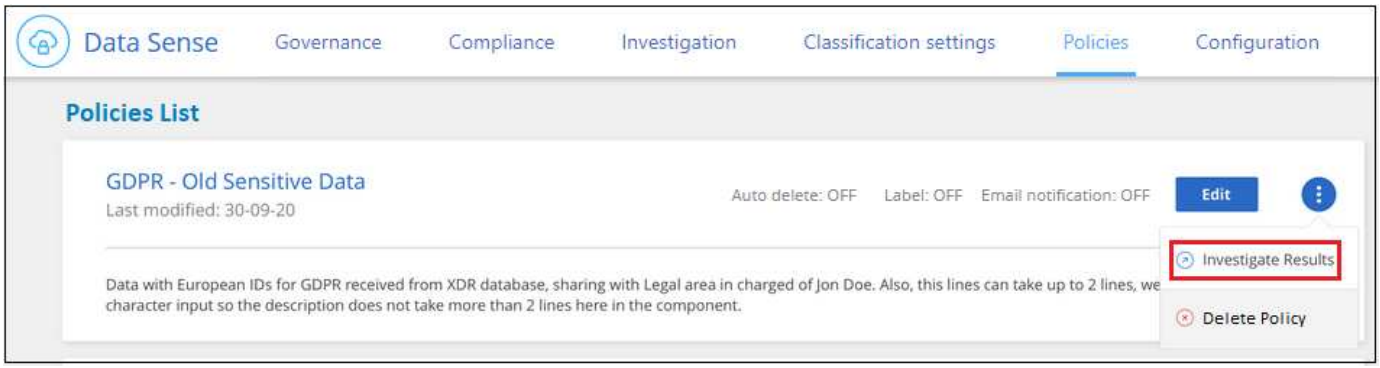
La pestaña **Políticas** del Panel de cumplimiento enumera todas las políticas predefinidas y personalizadas disponibles en esta instancia de clasificación de BlueXP.



Además, las políticas aparecen en la lista de filtros de la página Investigación.

Ver los resultados de la política en la página Investigación

Para mostrar los resultados de una directiva en la página Investigación, haga clic en ⋮ Para una política específica y, a continuación, seleccione **investigar resultados**.



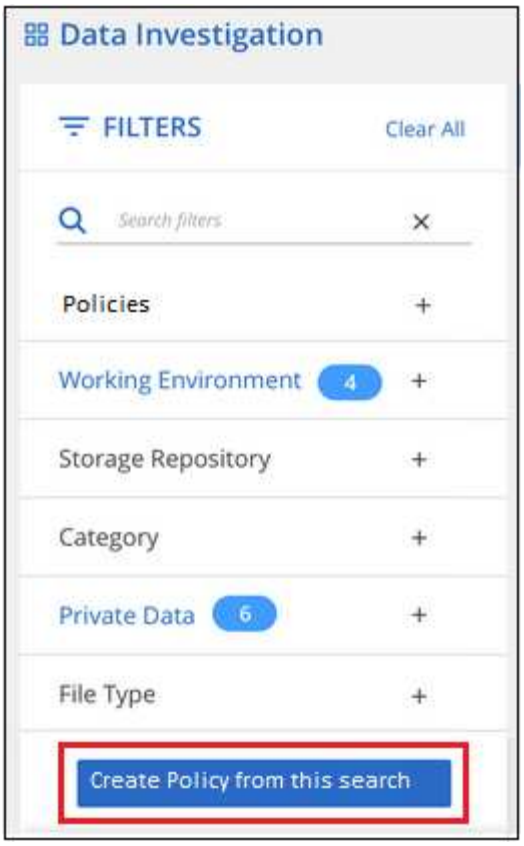
Crear políticas personalizadas

Puede crear sus propias directivas personalizadas que proporcionen resultados para búsquedas específicas de su organización. Los resultados se devuelven para todos los archivos y directorios (recursos compartidos y carpetas) que coincidan con los criterios de búsqueda.

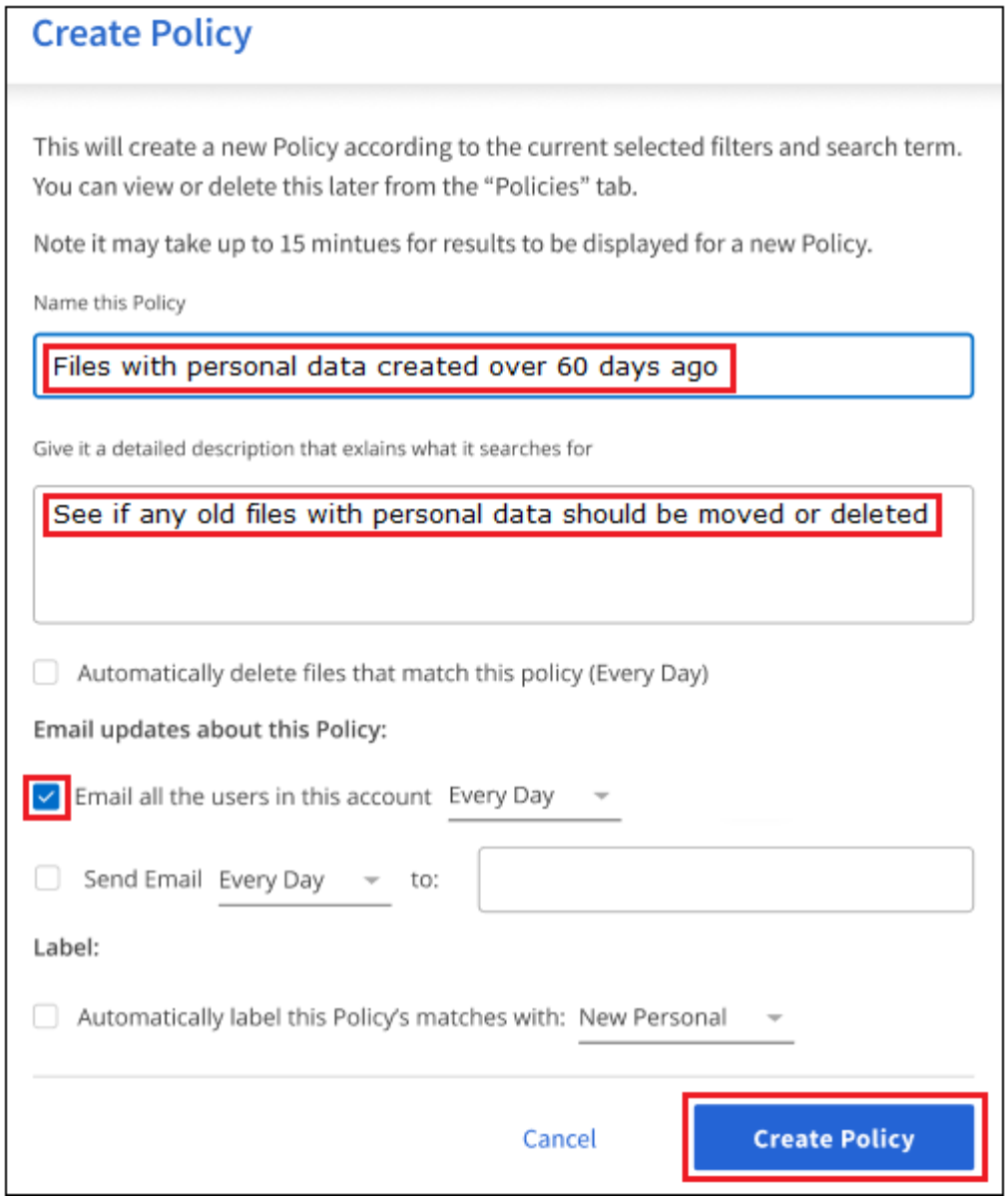
Tenga en cuenta que las acciones para eliminar datos y asignar etiquetas AIP basadas en los resultados de la directiva sólo son válidas para archivos. Los directorios que coinciden con los criterios de búsqueda no se pueden eliminar automáticamente ni asignar etiquetas AIP.

Pasos

1. En la página Investigación de datos, defina la búsqueda seleccionando todos los filtros que desee utilizar. Consulte "Filtrar datos en la página Investigación de datos" para obtener más detalles.
2. Una vez que tenga todas las características de filtro de la forma que desee, haga clic en **Crear directiva de esta búsqueda**.



3. Asigne un nombre a la directiva y seleccione otras acciones que ésta pueda realizar:
   a. Introduzca un nombre y una descripción únicos.
   b. Opcionalmente, marque la casilla para eliminar automáticamente los archivos que coincidan con los parámetros de directiva. Más información acerca de eliminación de archivos de origen mediante una directiva.
   c. Opcionalmente, marque la casilla si desea que se envíen correos electrónicos de notificación a usuarios de BlueXP en su cuenta y elija el intervalo en el que se envía el correo electrónico. Más información acerca de envío de alertas por correo electrónico basadas en los resultados de la política.
   d. Opcionalmente, marque la casilla si desea enviar correos electrónicos de notificación a otros usuarios, introduzca hasta 20 direcciones de correo electrónico y elija el intervalo en el que se envía el correo electrónico.
   e. Opcionalmente, active la casilla para asignar automáticamente etiquetas AIP a archivos que coincidan con los parámetros de directiva y seleccione la etiqueta. (Sólo si ya tiene etiquetas AIP integradas. Más información acerca de "Etiquetas AIP".)
   f. Haga clic en **Crear directiva**.



Resultado

La nueva directiva aparece en la ficha Directivas.

Enviar alertas de correo electrónico cuando se encuentren datos no conformes

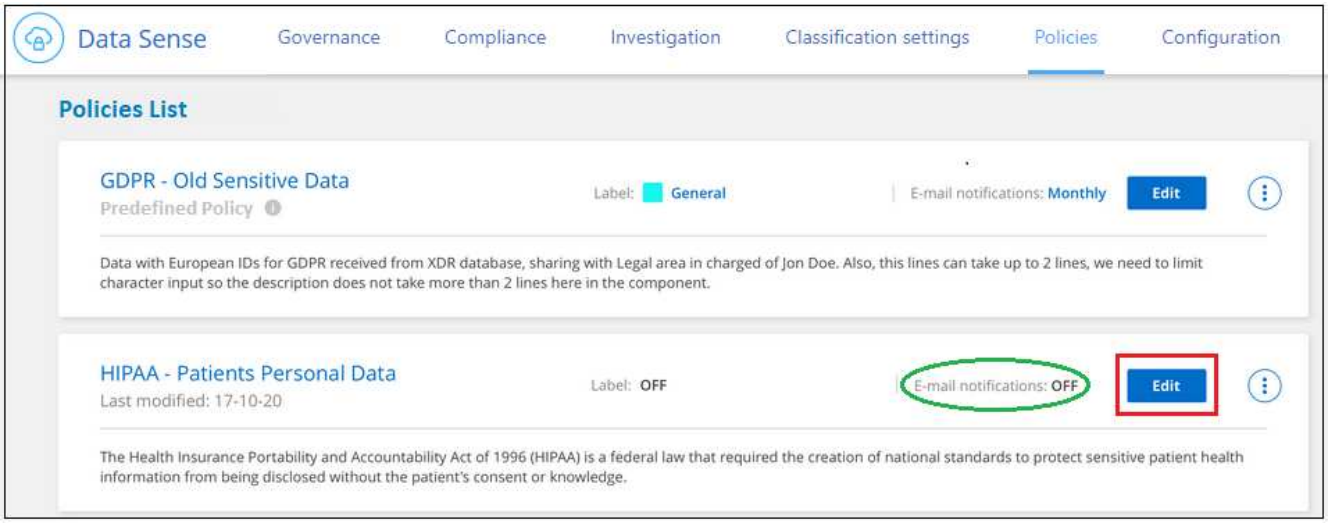
La clasificación de BlueXP puede enviar alertas por correo electrónico a los usuarios de BlueXP en tu cuenta cuando ciertas políticas críticas devuelvan resultados para que puedas recibir notificaciones que protejan tus datos. Puede optar por enviar las notificaciones por correo electrónico diariamente, semanalmente o mensualmente. También puede optar por enviar alertas de correo electrónico a cualquier otra dirección de correo electrónico - hasta 20 direcciones de correo electrónico - no en su cuenta de BlueXP.

Puede configurar esta configuración al crear la directiva o al editar cualquier directiva.

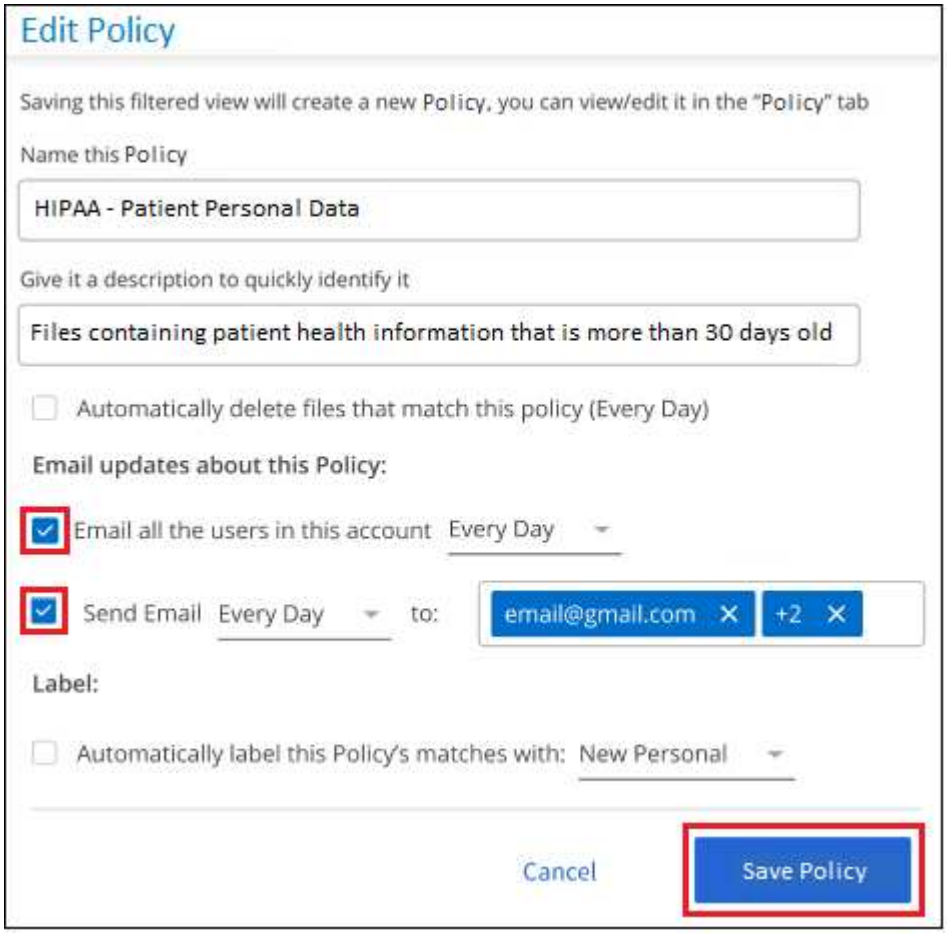
Siga estos pasos para agregar actualizaciones de correo electrónico a una directiva existente.

Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva en la que desea agregar (o cambiar) la configuración de correo electrónico.



2. En la página Edit Policy:
   a. Marque la casilla "Enviar por correo electrónico a todos los usuarios de esta cuenta" si desea enviar correos electrónicos de notificación a los usuarios de su cuenta de BlueXP y elija el intervalo en el que se envía el correo electrónico (por ejemplo, **todos los días**).
   b. Marque la casilla "Enviar correo electrónico" si desea enviar correos electrónicos de notificación a usuarios adicionales, seleccione el intervalo en el que se envía el correo electrónico e introduzca hasta 20 direcciones de correo electrónico.



3. Haga clic en **Guardar directiva** y el intervalo en el que se envía el correo electrónico aparecerá en la

descripción de la directiva.

Resultado

El primer correo electrónico se envía ahora si hay algún resultado de la Política, pero sólo si alguno de los archivos cumple los criterios de la Política. No se envía información personal en los correos electrónicos de notificación. El correo electrónico indica que hay archivos que coinciden con los criterios de directiva y proporciona un vínculo a los resultados de la directiva.

Eliminar archivos de origen automáticamente mediante Políticas

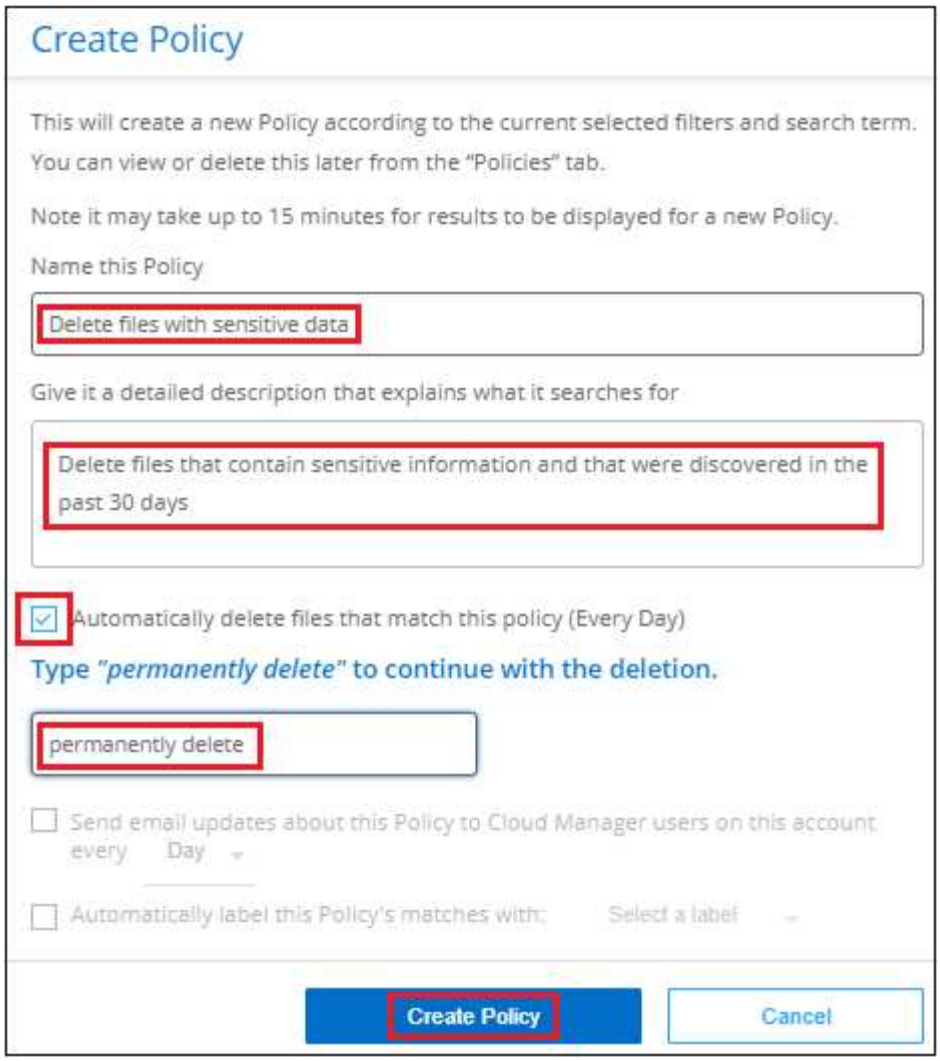
Puede crear una directiva personalizada para eliminar los archivos que coincidan con la directiva. Por ejemplo, puede que desee eliminar archivos que contienen información confidencial y que se han detectado por la clasificación de BlueXP en los últimos 30 días.

Sólo los administradores de cuentas pueden crear una directiva para eliminar archivos automáticamente.

> Todos los archivos que coincidan con la directiva se eliminarán de forma permanente una vez al día.

Pasos

1. En la página Investigación de datos, defina la búsqueda seleccionando todos los filtros que desee utilizar. Consulte "Filtrar datos en la página Investigación de datos" para obtener más detalles.
2. Una vez que tenga todas las características de filtro de la forma que desee, haga clic en **Crear directiva de esta búsqueda**.
3. Asigne un nombre a la directiva y seleccione otras acciones que ésta pueda realizar:
   a. Introduzca un nombre y una descripción únicos.
   b. Active la casilla para "eliminar automáticamente los archivos que coinciden con esta directiva" y escriba **eliminar permanentemente** para confirmar que desea que los archivos se eliminen de forma permanente mediante esta directiva.
   c. Haga clic en **Crear directiva**.



Resultado

La nueva directiva aparece en la ficha Directivas. Los archivos que coinciden con la directiva se eliminan una vez al día cuando se ejecuta la directiva.

Puede ver la lista de archivos que se han eliminado en "Panel Estado de acciones".

Asigne etiquetas AIP automáticamente con directivas

Puede asignar una etiqueta AIP a todos los archivos que cumplan los criterios de la directiva. Puede especificar la etiqueta AIP al crear la directiva, o puede agregar la etiqueta al editar cualquier directiva.

Las etiquetas se añaden o actualizan en los archivos continuamente a medida que la clasificación de BlueXP analiza los archivos.

En función de si una etiqueta ya se ha aplicado a un archivo y del nivel de clasificación de la etiqueta, se realizan las siguientes acciones al cambiar una etiqueta:

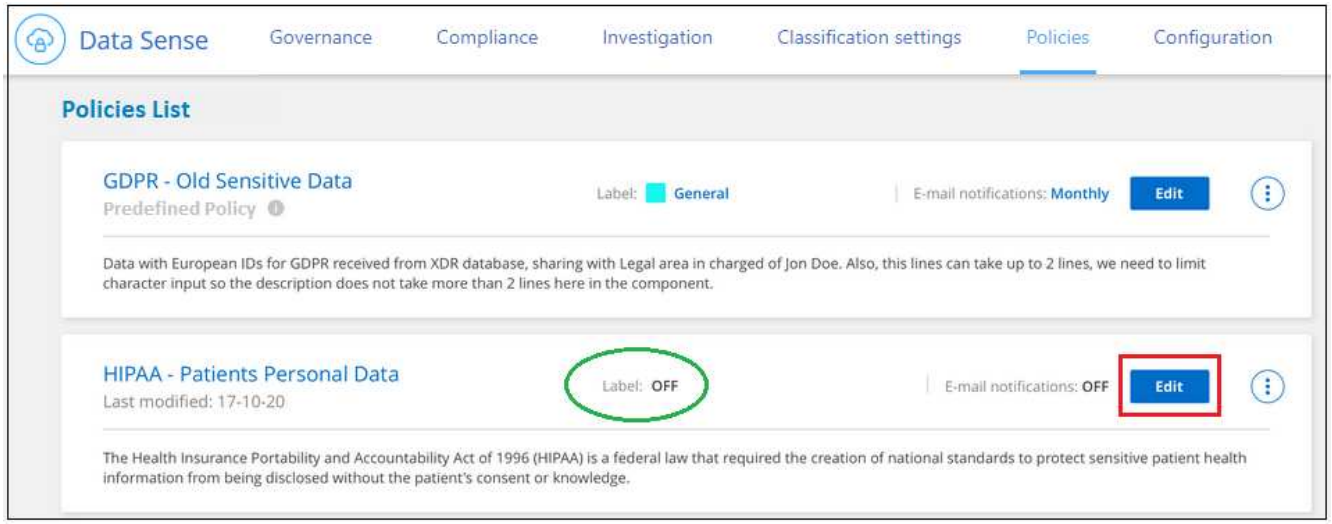
Si el archivo…	Realice lo siguiente…
No tiene etiqueta	Se agrega la etiqueta
Tiene una etiqueta de un nivel inferior de clasificación	Se agrega la etiqueta de nivel superior

Si el archivo…	Realice lo siguiente…
Tiene una etiqueta existente de un nivel superior de clasificación	Se mantiene la etiqueta de nivel superior
Se asigna una etiqueta tanto manualmente como por una directiva	Se agrega la etiqueta de nivel superior
Se asignan dos etiquetas diferentes mediante dos directivas	Se agrega la etiqueta de nivel superior

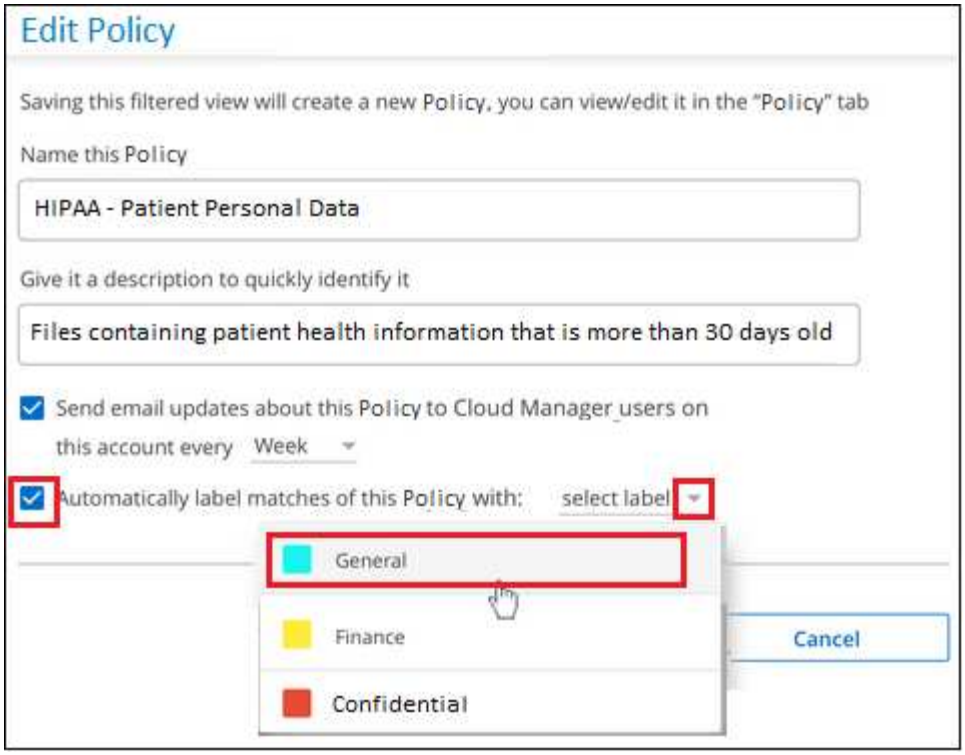
Siga estos pasos para agregar una etiqueta AIP a una directiva existente.

Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva en la que desea agregar (o cambiar) la etiqueta AIP.



2. En la página Editar directiva, active la casilla para habilitar etiquetas automáticas para los archivos que coincidan con los parámetros de directiva y seleccione la etiqueta (por ejemplo, **General**).



3. Haga clic en **Guardar directiva** y la etiqueta aparecerá en la descripción de la directiva.

> Si se ha configurado una directiva con una etiqueta, pero la etiqueta se ha eliminado de AIP, el nombre de la etiqueta se desactiva y la etiqueta ya no se asigna.

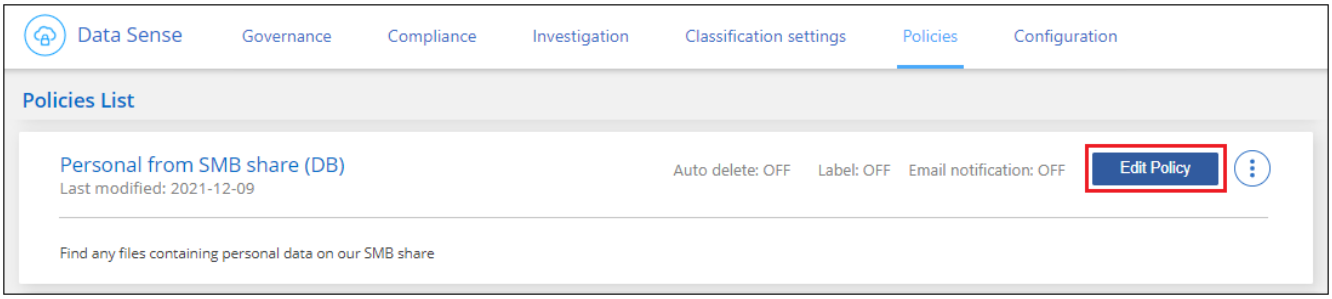
Editar políticas

Puede modificar cualquier criterio para una política existente que haya creado previamente. Esto puede resultar especialmente útil si desea cambiar la consulta (los elementos definidos mediante Filtros) para agregar o quitar determinados parámetros.

Tenga en cuenta que para directivas predefinidas, sólo puede modificar si se envían notificaciones de correo electrónico y si se agregan etiquetas AIP. No se pueden cambiar otros valores.

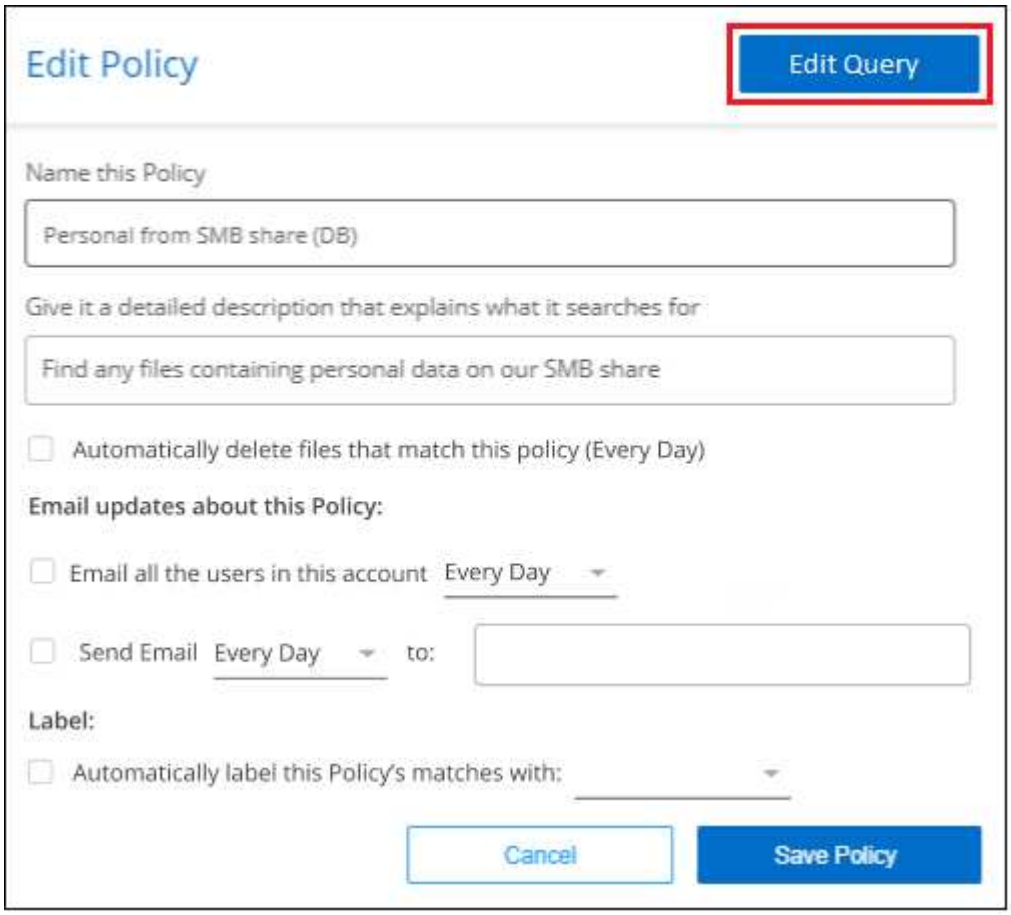
Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva que desea cambiar.

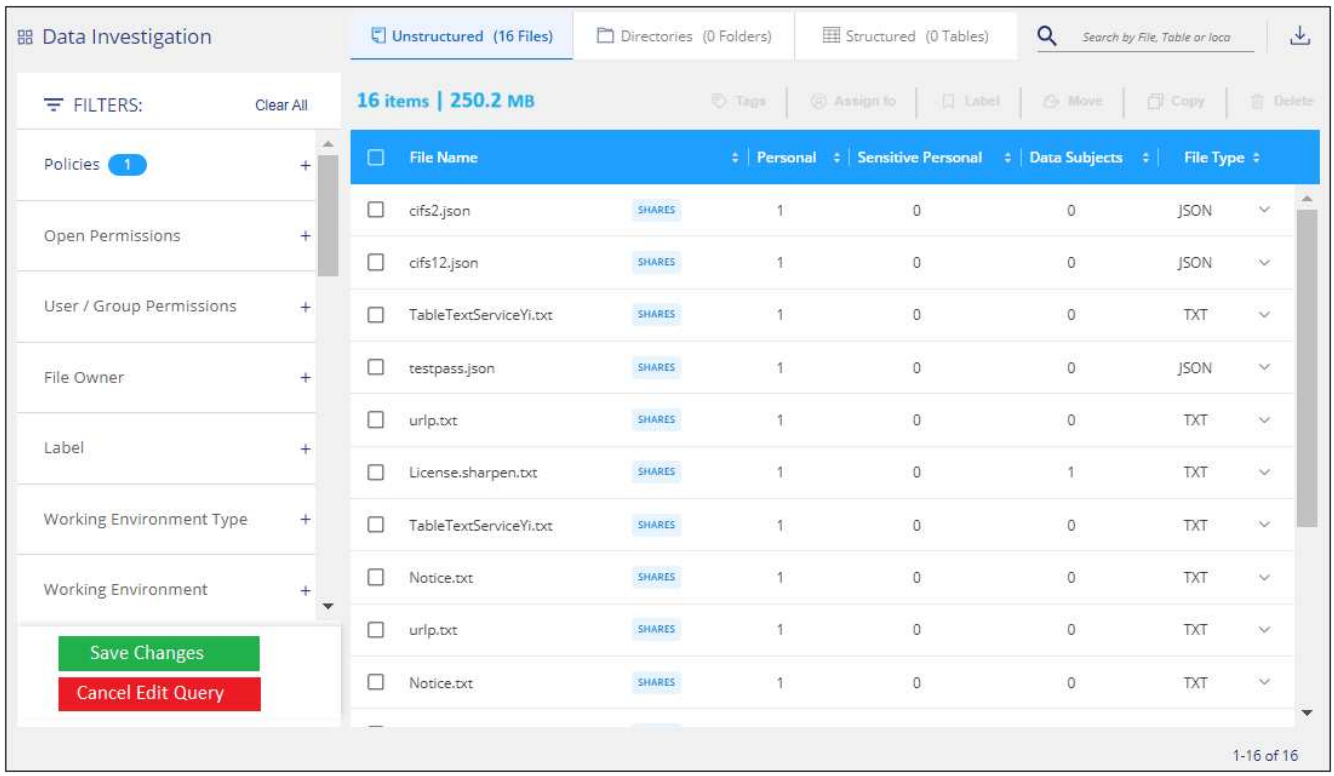


2. Si sólo desea cambiar los elementos de esta página (Nombre, Descripción, si se envían notificaciones de correo electrónico y si se agregan etiquetas AIP), realice el cambio y haga clic en **Guardar directiva**.

   Si desea cambiar los filtros de la consulta guardada, haga clic en **Editar consulta**.



3. En la página Investigación que define esa consulta, edite la consulta agregando, quitando o personalizando los filtros y haga clic en **Guardar cambios** .



Resultado

La directiva cambia inmediatamente. Cualquier acción definida para que esa directiva envíe un correo electrónico, agregue etiquetas AIP o elimine archivos tendrá lugar en el siguiente interno.

Eliminar políticas

Puede eliminar cualquier directiva personalizada que haya creado si ya no la necesita. No se puede eliminar ninguna de las directivas predefinidas.

Para eliminar una directiva, haga clic en Para una directiva específica, haga clic en **Eliminar directiva** y, a continuación, vuelva a hacer clic en **Eliminar directiva** en el cuadro de diálogo de confirmación.

Lista de directivas predefinidas

La clasificación de BlueXP proporciona las siguientes políticas definidas por el sistema:

Nombre	Descripción	Lógica
S3: Datos privados expuestos públicamente	S3 objetos que contienen información personal o confidencial, con acceso público de lectura abierto.	S3 Public y contiene información personal o confidencial
PCI DSS: Datos obsoletos durante 30 días	Archivos con información de tarjeta de crédito, modificado por última vez hace 30 días.	Contiene tarjeta de crédito y última modificación durante 30 días
HIPAA: Datos desfasados a lo largo de 30 días	Archivos que contienen información médica, modificada por última vez hace 30 días.	Contiene datos de salud (definidos de la misma forma que en el informe HIPAA) Y última modificación durante 30 días
Datos privados: Obsoletos a lo largo de 7 años	Archivos que contengan información personal o confidencial, modificado por última vez hace más de 7 años.	Archivos que contengan información personal o confidencial, modificado por última vez hace más de 7 años
RGPD: Ciudadanos europeos	Archivos que contienen más de 5 identificadores de ciudadanos de un país de la UE o tablas de DB que contienen identificadores de ciudadanos de un país de la UE.	Archivos que contienen más de 5 identificadores de una (una) tablas de ciudadanos o bases de datos de la UE que contienen filas con más del 15% de columnas con identificadores de la UE de un país. (Cualquiera de los identificadores nacionales de los países europeos. No incluye Brasil, California, Estados Unidos SSN, Israel, Sudáfrica)
CCPA - residentes de California	Archivos que contienen más de 10 identificadores de licencia de controlador de California o tablas de base de datos con este identificador.	Archivos que contienen más de 10 identificadores de Licencia de controlador de California O tablas de base de datos que contienen la licencia de controlador de California
Nombres de sujetos de datos: Alto riesgo	Archivos con más de 50 nombres de asunto de datos.	Archivos con más de 50 nombres de asunto de datos

Nombre	Descripción	Lógica
Direcciones de correo electrónico: Alto riesgo	Archivos con más de 50 direcciones de correo electrónico o columnas de base de datos con más del 50% de sus filas que contienen direcciones de correo electrónico	Archivos con más de 50 direcciones de correo electrónico o columnas de base de datos con más del 50% de sus filas que contienen direcciones de correo electrónico
Datos personales: Alto riesgo	Archivos con más de 20 identificadores de datos personales o columnas de base de datos con más del 50% de sus filas que contienen identificadores de datos personales.	Archivos con más de 20 columnas personales o de base de datos con más del 50% de sus filas que contienen personales
Datos personales confidenciales: Alto riesgo	Archivos con más de 20 identificadores de datos personales confidenciales, o columnas de base de datos con más del 50% de sus filas que contienen datos personales confidenciales.	Archivos con más de 20 columnas confidenciales personales o de base de datos con más del 50% de sus filas que contienen personal confidencial

Gestione sus datos privados

La clasificación de BlueXP ofrece muchas formas de gestionar los datos privados. Algunas funcionalidades facilitan la preparación para la migración de datos, mientras que otras permiten realizar cambios en los datos.

- Puede copiar archivos en un recurso compartido NFS de destino si desea realizar una copia de determinados datos y moverlos a una ubicación NFS diferente.
- Es posible clonar un volumen de ONTAP en un volumen nuevo, e incluir solo los archivos seleccionados del volumen de origen en el nuevo volumen clonado. Esto resulta útil en situaciones en las que se migran datos y se desean excluir determinados archivos del volumen original.
- Puede copiar y sincronizar archivos de un repositorio de origen a un directorio en una ubicación de destino específica. Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro mientras todavía hay alguna actividad final en los archivos de origen.
- Puede mover los archivos de origen que la clasificación de BlueXP esté analizando a cualquier recurso compartido NFS.
- Puede eliminar archivos que parecen poco seguros o demasiado arriesgados para dejar en el sistema de almacenamiento, o que ha identificado como duplicados.

- Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.
- Los datos de cuentas de Google Drive no pueden usar ninguna de estas funcionalidades en este momento.

Copie los archivos de origen

Puede copiar todos los archivos de origen que la clasificación de BlueXP esté analizando. Existen tres tipos de operaciones de copia en función de lo que intente lograr:

- **Copiar archivos** de los mismos volúmenes o orígenes de datos o diferentes a un recurso compartido NFS de destino.

  Esto resulta útil si se desea realizar una copia de ciertos datos y moverlos a una ubicación NFS diferente.

- **Clonar un volumen ONTAP** en un volumen nuevo del mismo agregado, pero incluir sólo los archivos seleccionados del volumen de origen en el nuevo volumen clonado.

  Esto resulta útil en situaciones en las que se migran datos y se desean excluir determinados archivos del volumen original. Esta acción utiliza "FlexClone de NetApp" funcionalidad para duplicar rápidamente el volumen y, a continuación, eliminar los archivos que **no** seleccionó.

- **Copiar y sincronizar archivos** desde un único repositorio de origen (volumen ONTAP, bloque S3, recurso compartido NFS, etc.) a un directorio en una ubicación de destino específica.

  Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro. Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya establecido. Esta acción utiliza "Copia y sincronización de NetApp BlueXP" funcionalidad para copiar y sincronizar datos de un origen en un destino.

Copie los archivos de origen en un recurso compartido NFS

Puede copiar los archivos de origen que la clasificación de BlueXP esté analizando en cualquier recurso compartido NFS. No es necesario integrar el recurso compartido de NFS con la clasificación de BlueXP, solo tienes que saber el nombre del recurso compartido de NFS en el que se copiarán todos los archivos seleccionados en formato `<host_name>:/<share_path>`.

No se pueden copiar archivos que residen en bases de datos.

Requisitos

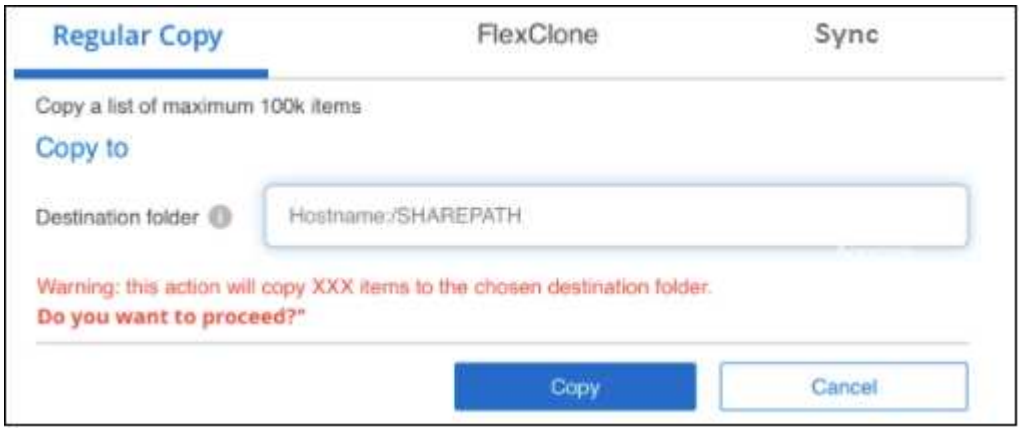
- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar archivos.
- Para copiar archivos es necesario que el recurso compartido NFS de destino permita el acceso desde la instancia de clasificación de BlueXP.
- Puede copiar entre 1 y 100,000 archivos a la vez.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea copiar y haga clic en **Copiar**.

- Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (File Name) y, a continuación, en el mensaje emergente All **20** Items on this page selected Select all Items in list (63K Items), Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

2. En el cuadro de diálogo *Copy Files*, seleccione la ficha **copia normal**.



3. Introduzca el nombre del recurso compartido NFS donde se copiarán todos los archivos seleccionados en el formato `<host_name>:/<share_path>`Y haga clic en **Copiar**.

   Se muestra un cuadro de diálogo con el estado de la operación de copia.

Puede ver el progreso de la operación de copia en "Panel Estado de acciones".

Tenga en cuenta que también puede copiar un archivo individual al ver los detalles de metadatos de un archivo. Haga clic en **Copiar archivo**.

Clone los datos de volúmenes en un volumen nuevo

Puede clonar un volumen de ONTAP existente que analice la clasificación de BlueXP mediante la funcionalidad *FlexClone* de NetApp. Esto le permite duplicar rápidamente el volumen e incluir únicamente los archivos seleccionados. Esto resulta útil si va a migrar datos y desea excluir determinados archivos del

volumen original o si desea crear una copia de un volumen para realizar las pruebas.

El nuevo volumen se creará en el mismo agregado que el volumen de origen. Asegúrese de tener suficiente espacio para este nuevo volumen en el agregado antes de iniciar esta tarea. Si es necesario, póngase en contacto con el administrador de almacenamiento.

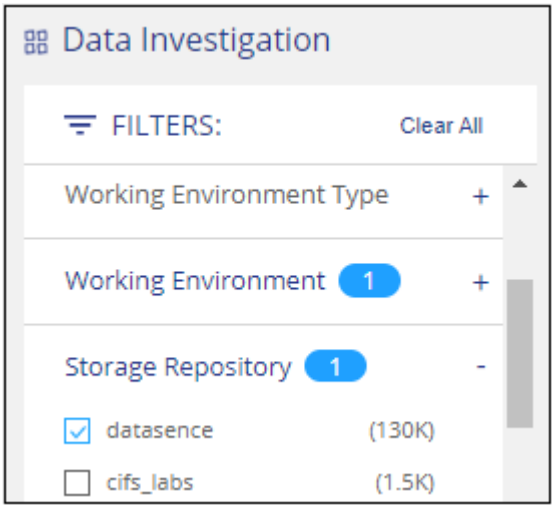
Nota: los volúmenes FlexGroup no se pueden clonar porque FlexClone no los admite.

Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar archivos.
- Debe seleccionar un mínimo de 20 archivos.
- Todos los archivos seleccionados deben ser del mismo volumen y el volumen debe estar en línea.
- El volumen debe ser de un sistema ONTAP Cloud Volumes ONTAP o en las instalaciones. Actualmente no se admiten otros orígenes de datos.
- Debe instalar la licencia de FlexClone en el clúster. Esta licencia se instala de manera predeterminada en sistemas Cloud Volumes ONTAP.

Pasos

1. En el panel Investigación de datos, cree un filtro seleccionando un solo **entorno de trabajo** y un único **repositorio de almacenamiento** para asegurarse de que todos los archivos pertenecen al mismo volumen ONTAP.

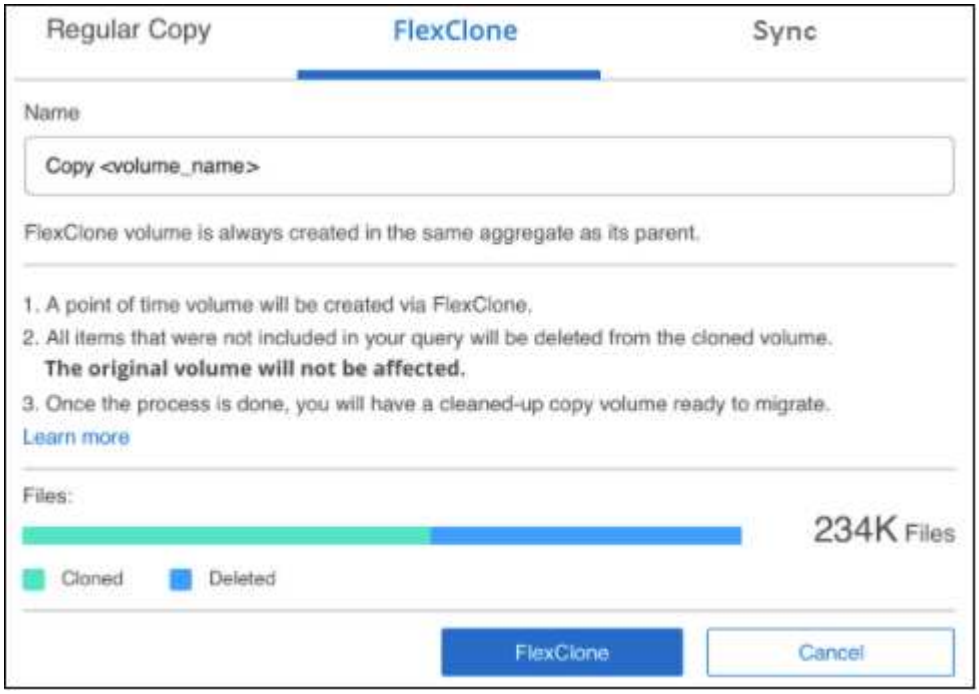


   Aplique otros filtros para ver solo los archivos que desea clonar en el nuevo volumen.

2. En el panel resultados de la investigación, seleccione los archivos que desea clonar y haga clic en **Copiar**.

- Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (File Name) y, a continuación, en el mensaje emergente All **20** Items on this page selected Select all Items in list (63K Items), Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

3. En el cuadro de diálogo *Copy Files*, seleccione la ficha **FlexClone**. Esta página muestra el número total de archivos que se clonarán desde el volumen (los archivos seleccionados) y el número de archivos que no se incluyen o eliminan (los archivos que no seleccionó) del volumen clonado.



4. Introduzca el nombre del nuevo volumen y haga clic en **FlexClone**.

   Se muestra un cuadro de diálogo con el estado de la operación de clonado.

Resultado

El nuevo volumen clonado se crea en el mismo agregado que el volumen de origen.

Puede ver el progreso de la operación de clonado en el "Panel Estado de acciones".

Si inicialmente seleccionaste **Asignar todos los volúmenes** o **Asignar y clasificar todos los volúmenes** cuando habilitaste la clasificación de BlueXP para el entorno de trabajo donde reside el volumen de origen, la clasificación de BlueXP escaneará el nuevo volumen clonado automáticamente. Si inicialmente no ha utilizado ninguna de estas selecciones, si desea explorar este nuevo volumen, deberá hacerlo "active la exploración en el volumen manualmente".

Copiar y sincronizar archivos de origen en un sistema de destino

Puede copiar archivos de origen que analiza la clasificación de BlueXP desde cualquier origen de datos no estructurados compatible a un directorio en una ubicación de destino específica ("Ubicaciones de destino que admiten la copia y sincronización de BlueXP"). Después de la copia inicial, los datos modificados en los archivos se sincronizan en función de la programación que configure.

Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro. Esta acción utiliza "Copia y sincronización de NetApp BlueXP" funcionalidad para copiar y sincronizar datos de un origen en un destino.

No se pueden copiar y sincronizar archivos que residen en cuentas de SharePoint, cuentas de OneDrive o bases de datos.

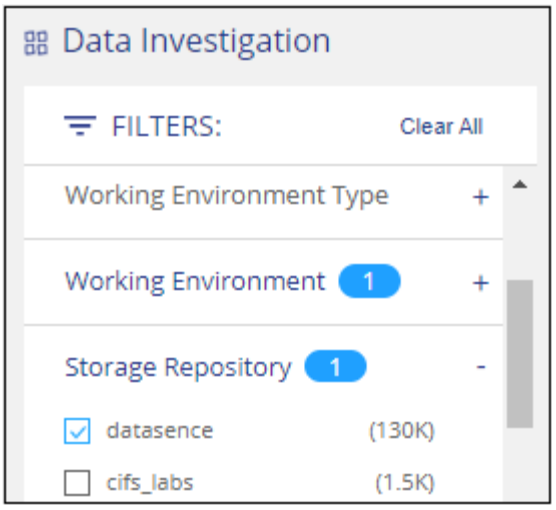
Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar y sincronizar archivos.
- Debe seleccionar un mínimo de 20 archivos.
- Todos los archivos seleccionados deben ser del mismo repositorio de origen (volumen ONTAP, bloque de S3, recurso compartido NFS o CIFS, etc.).
- Deberá activar el servicio de copia y sincronización de BlueXP y configurar un agente de datos como mínimo que se puede utilizar para transferir archivos entre los sistemas de origen y de destino. Revise los requisitos de copia y sincronización de BlueXP a partir del "Descripción de Inicio rápido".

  Tenga en cuenta que el servicio de copia y sincronización de BlueXP tiene distintos cargos de servicio para sus relaciones de sincronización y que incurrirá en cargos por los recursos si implementa el agente de datos en el cloud.

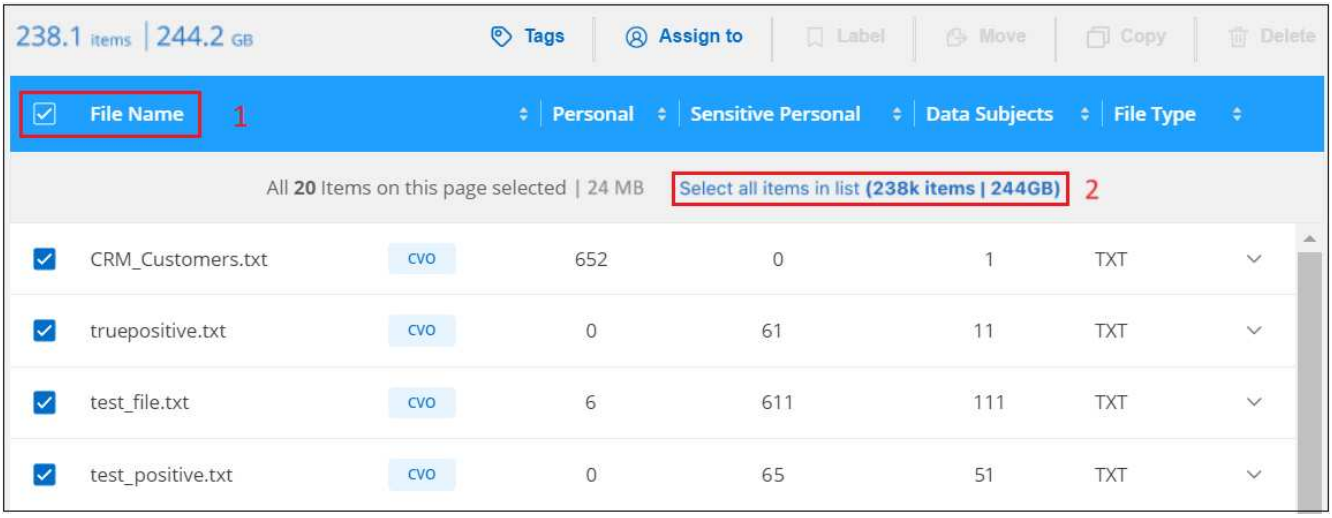
Pasos

1. En el panel Investigación de datos, cree un filtro seleccionando un solo **entorno de trabajo** y un único **repositorio de almacenamiento** para asegurarse de que todos los archivos están del mismo repositorio.

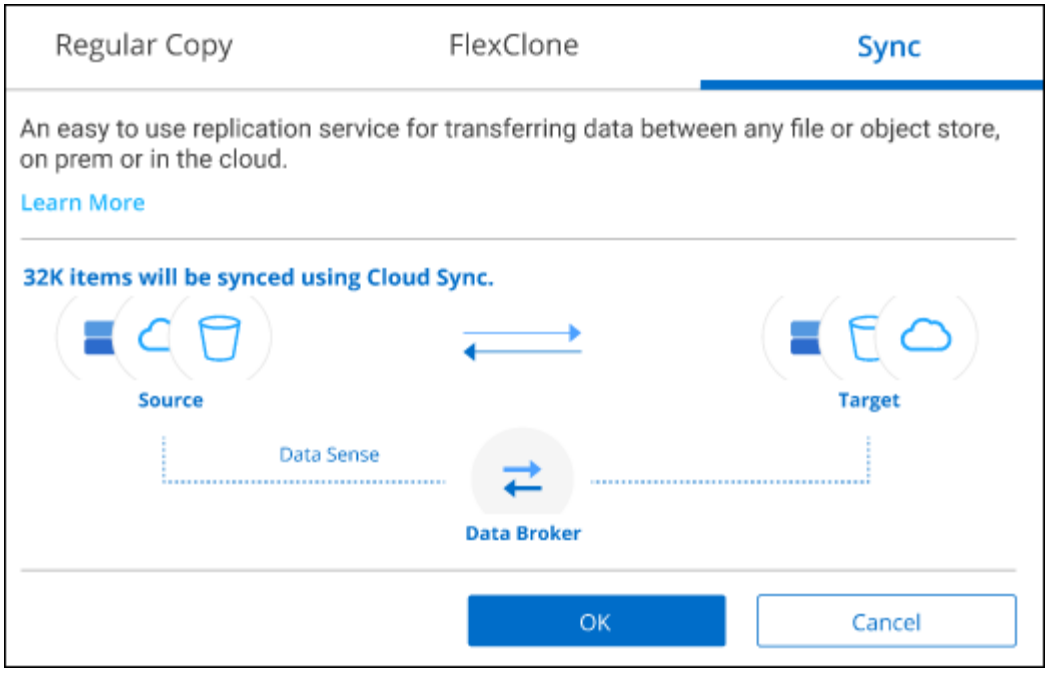


Aplique cualquier otro filtro para que sólo vea los archivos que desea copiar y sincronizar con el sistema de destino.

2. En el panel resultados de la investigación, seleccione todos los archivos de todas las páginas marcando la casilla de la fila de título (File Name), luego en el mensaje emergente All 20 Items on this page selected Select all Items in list (63K Items) Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)** y, a continuación, haga clic en **Copiar**.



3. En el cuadro de diálogo *Copy Files*, seleccione la ficha **Sync**.



4. Si está seguro de que desea sincronizar los archivos seleccionados con una ubicación de destino, haga clic en **Aceptar**.

   La IU de copia y sincronización de BlueXP se abre en BlueXP.

   Se le solicitará que defina la relación de sincronización. El sistema de origen se rellena automáticamente en función del repositorio y los archivos que ya hayas seleccionado en la clasificación de BlueXP.

5. Deberá seleccionar el sistema de destino y, a continuación, seleccionar (o crear) el agente de datos que desea utilizar. Revise los requisitos de copia y sincronización de BlueXP a partir del "Descripción de Inicio rápido".

Resultado

Los archivos se copian en el sistema de destino y se sincronizarán según la programación que defina. Si selecciona una sincronización única, los archivos se copiarán y sincronizarán una vez. Si elige una sincronización periódica, los archivos se sincronizan según la programación. Tenga en cuenta que si el sistema de origen agrega nuevos archivos que coinciden con la consulta creada mediante filtros, esos archivos *new* se copiarán en el destino y se sincronizarán en el futuro.

Tenga en cuenta que algunas de las operaciones de copia y sincronización habituales de BlueXP se deshabilitan cuando se invocan desde la clasificación de BlueXP:

- No puede utilizar los botones **Eliminar archivos en origen** o **Eliminar archivos en destino**.
- La ejecución de un informe está deshabilitada.

Mover archivos de origen a un recurso compartido NFS

Puede mover los archivos de origen que la clasificación de BlueXP esté analizando a cualquier recurso compartido NFS. La unidad de NFS no es necesario integrar con la clasificación de BlueXP.

De manera opcional, puede dejar un archivo de rastro en la ubicación del archivo movido. Un archivo de rastro ayuda a los usuarios a comprender por qué se trasladó un archivo desde su ubicación original. Para cada archivo movido, el sistema crea un archivo de rastro en la ubicación de origen llamada `<filename>-`

`breadcrumb-<date>.txt`. Puede añadir texto al cuadro de diálogo que se añadirá al archivo de rastro para indicar la ubicación donde se trasladó el archivo y el usuario que trasladó el archivo.

Tenga en cuenta que la estructura de subdirectorios del archivo de origen se vuelve a crear en el recurso compartido de destino cuando se mueve el archivo, de modo que es más fácil entender desde dónde se movió el archivo. Si existe un archivo con el mismo nombre en la ubicación de destino, el archivo no se moverá.

No se pueden mover los archivos que residen en las bases de datos.

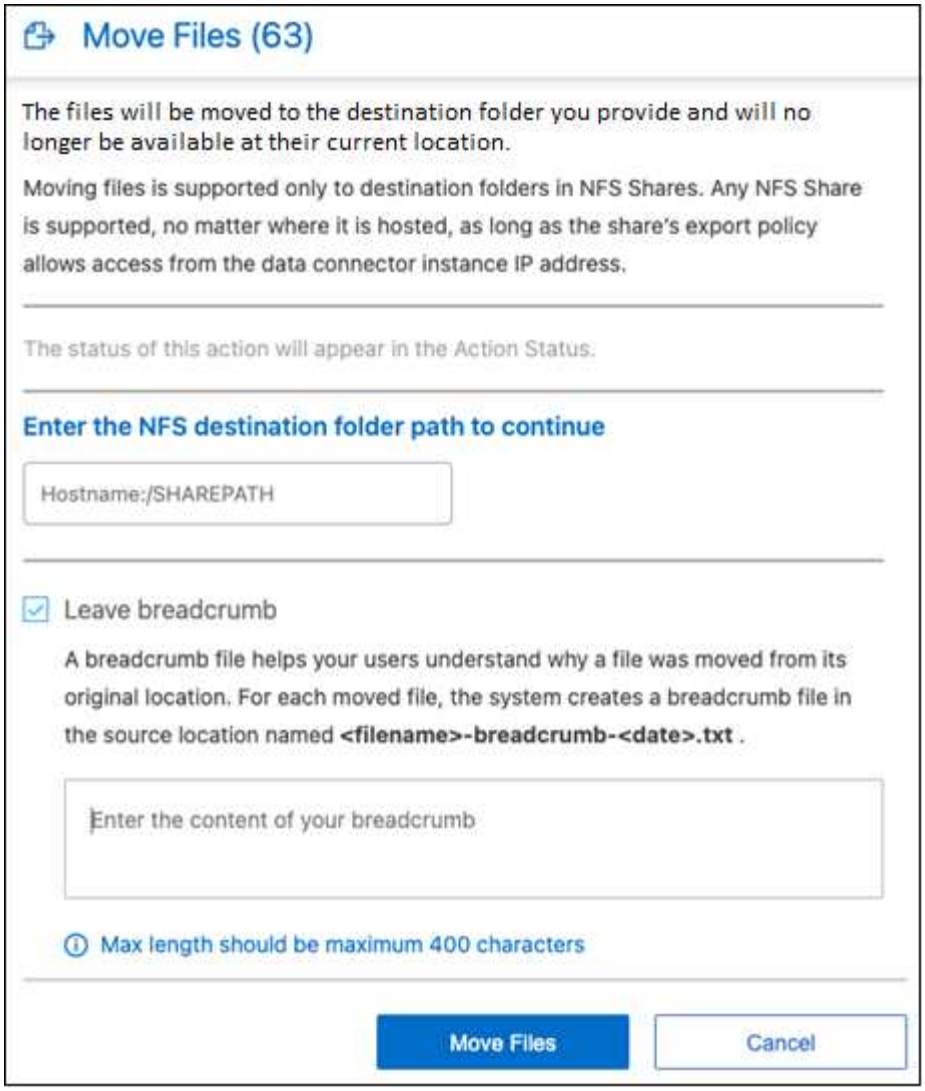
Requisitos

- Debe tener el rol Administrador de cuentas o Administrador de área de trabajo para mover archivos.
- Los archivos de origen se pueden ubicar en los siguientes orígenes de datos: ONTAP en las instalaciones, Cloud Volumes ONTAP, Azure NetApp Files, recursos compartidos de archivos y SharePoint Online.
- Puede mover un máximo de 15 millones de archivos al mismo tiempo.
- Solo se mueven los archivos de 50 MB o menos.
- El recurso compartido de NFS de destino debe permitir el acceso desde la dirección IP de la instancia de clasificación de BlueXP.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desee mover.

   - Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
   - Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).
   - Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (File Name) y, a continuación, en el mensaje emergente All **20** Items on this page selected Select all Items in list (63K Items), Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.
2. En la barra de botones, haga clic en **mover**.



3. En el cuadro de diálogo *Move Files*, escriba el nombre del recurso compartido NFS donde se moverán todos los archivos seleccionados en el formato `<host_name>:/<share_path>`.
4. Si desea dejar un archivo de rastro, marque la casilla *Leave wexploración*. Puede escribir texto en el cuadro de diálogo para indicar la ubicación en la que se ha movido el archivo y el usuario que lo ha movido, así como cualquier otra información, como el motivo por el que se ha movido el archivo.
5. Haga clic en **mover archivos**.

Tenga en cuenta que también puede mover un archivo individual al ver los detalles de los metadatos de un archivo. Simplemente haga clic en **mover archivo**.

Elimine los archivos de origen

Puede eliminar de forma permanente los archivos de origen que parezcan poco seguros o demasiado arriesgados para dejar su sistema de almacenamiento, o que haya identificado como duplicados. Esta acción es permanente y no hay deshacer ni restaurar.

Puede eliminar archivos manualmente desde el panel Investigación, o. "Uso automático de directivas".

> No se pueden eliminar los archivos que residen en las bases de datos. Se admiten todos los demás orígenes de datos.

Para eliminar archivos, es necesario contar con los siguientes permisos:

- Para datos NFS: La política de exportación debe definirse con permisos de escritura.
- Para datos CIFS: Las credenciales CIFS necesitan permisos de escritura.
- Para datos S3 - el rol IAM debe incluir el siguiente permiso: `s3:DeleteObject`.

Elimine los archivos de origen manualmente

Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para eliminar archivos.
- Puede eliminar un máximo de 100,000 archivos al mismo tiempo.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea eliminar.

- Para seleccionar archivos individuales, marque la casilla de cada archivo (Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (File Name) y, a continuación, en el mensaje emergente All **20** Items on this page selected Select all Items in list (63K Items), Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

2. En la barra de botones, haga clic en **Eliminar**.
3. Debido a que la operación de eliminación es permanente, debe escribir "**permanentemente delete**" en el diálogo posterior *Delete File* y hacer clic en **Delete File**.

Puede ver el progreso de la operación de eliminación en la "Panel Estado de acciones".

Tenga en cuenta que también puede eliminar un archivo individual al ver los detalles de metadatos de un archivo. Simplemente haga clic en **Eliminar archivo**.

Ver informes de cumplimiento

La clasificación de BlueXP ofrece informes que puede utilizar para comprender mejor el estado del programa de privacidad de los datos de su organización.

De forma predeterminada, las consolas de clasificación de BlueXP muestran los datos de cumplimiento y gobierno de todos los entornos de trabajo, las bases de datos y los orígenes de datos. Si desea ver informes que contengan datos sólo para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

- Los informes descritos en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación sólo pueden generar el informe de asignación de datos.
- NetApp no puede garantizar la precisión del 100 % de los datos personales y los datos personales confidenciales que identifica la clasificación de BlueXP. Siempre debe validar la información revisando los datos.

Informe de evaluación del riesgo de privacidad

El informe de evaluación de riesgos de privacidad ofrece una descripción general del estado de riesgo de privacidad de su organización, tal y como lo exigen las normativas de privacidad como el RGPD y la CCPA. El informe incluye la siguiente información:

Estado de cumplimiento

A. puntuación de gravedad y la distribución de los datos, ya sean personales, confidenciales o no confidenciales.

Descripción general de la evaluación

Desglose de los tipos de datos personales encontrados, así como de las categorías de datos.

Datos sujetos en esta evaluación

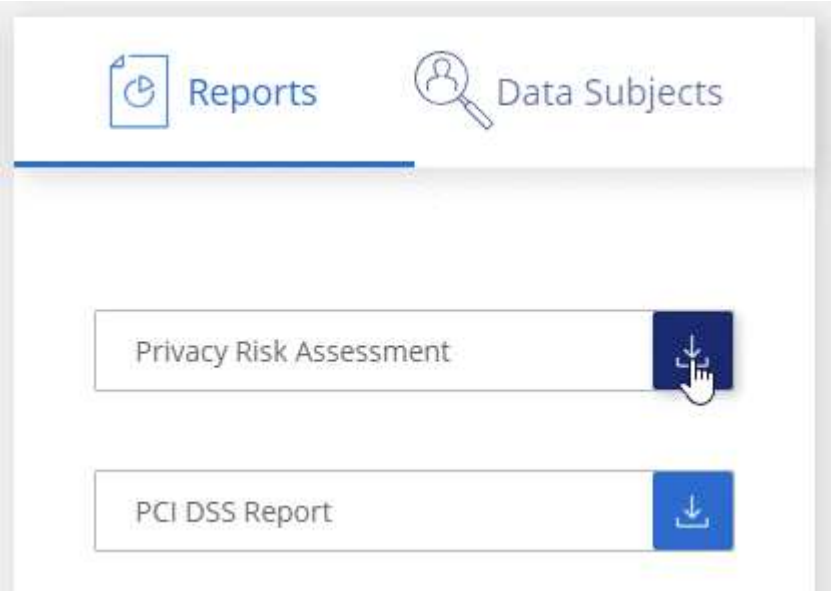
El número de personas, por ubicación, para las cuales se encontraron identificadores nacionales.

Genere el informe de evaluación de riesgos de privacidad

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **cumplimiento** y, a continuación, haga clic en el icono de descarga situado junto a **Evaluación de riesgo de privacidad** en **Informes**.



Resultado

La clasificación de BlueXP genera un informe PDF que se puede revisar y enviar a otros grupos según sea necesario.

Puntuación de gravedad

La clasificación de BlueXP calcula la puntuación de gravedad del informe de evaluación de riesgos de privacidad basándose en tres variables:

- El porcentaje de datos personales de todos los datos.
- El porcentaje de datos personales confidenciales de todos los datos.
- El porcentaje de archivos que incluyen temas de datos, determinado por identificadores nacionales como ID nacionales, números de Seguro Social y números de identificación fiscal.

La lógica utilizada para determinar la puntuación es la siguiente:

Puntuación de gravedad	Lógica
0	Las tres variables son exactamente 0 %
1	Una de las variables es mayor que 0 %
2	Una de las variables es mayor que el 3 %
3	Dos de las variables son mayores que el 3%
4	Tres de las variables son mayores que el 3%
5	Una de las variables es mayor que el 6 %
6	Dos de las variables son mayores que el 6%
7	Tres de las variables son mayores que el 6%
8	Una de las variables es mayor que el 15 %
9	Dos de las variables son mayores que el 15%
10	Tres de las variables son mayores que el 15%

Informe PCI DSS

El Informe de estándares de seguridad de datos del sector de la tarjeta de pago (PCI DSS) puede ayudarle a identificar la distribución de información de la tarjeta de crédito a través de sus archivos. El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información de tarjeta de crédito y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información de la tarjeta de crédito en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información de tarjetas de crédito en entornos de trabajo que tienen o no la protección contra ransomware habilitada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de la tarjeta de crédito por más tiempo de lo que necesita para procesarla.

Distribución de la información de la tarjeta de crédito

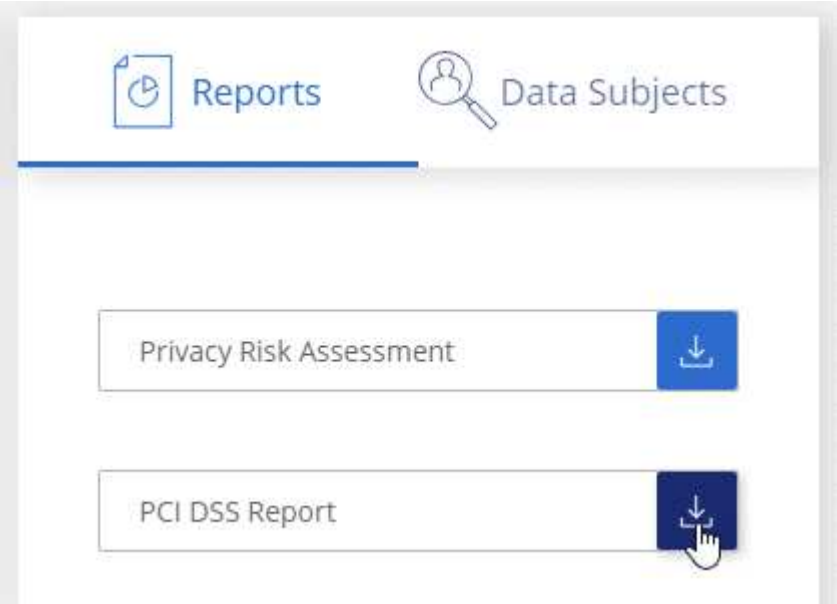
Entornos en los que se encontró la información de la tarjeta de crédito y si la protección mediante cifrado y ransomware están habilitadas.

Genere el informe PCI DSS

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **conformidad** y, a continuación, haga clic en el icono de descarga situado junto a **Informe DSS de PCI** en **Informes**.



Resultado

La clasificación de BlueXP genera un informe PDF que se puede revisar y enviar a otros grupos según sea necesario.

Informe HIPAA

El Informe de la Ley de Portabilidad y responsabilidad de los Seguros médicos (HIPAA) puede ayudarle a identificar archivos que contengan información médica. Se ha diseñado para ayudar en el requisito de su organización a cumplir las leyes de privacidad de datos HIPAA. La información que busca la clasificación de BlueXP incluye:

- Patrón de referencia de salud
- Código médico ICD-10-cm
- Código médico ICD-9-cm
- HR - Categoría de salud

- Datos de aplicación de Salud

El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información médica y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información médica en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información médica en entornos de trabajo que tienen o no la protección contra ransomware activada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de salud por más tiempo de lo que necesita para procesarla.

Distribución de la información de salud

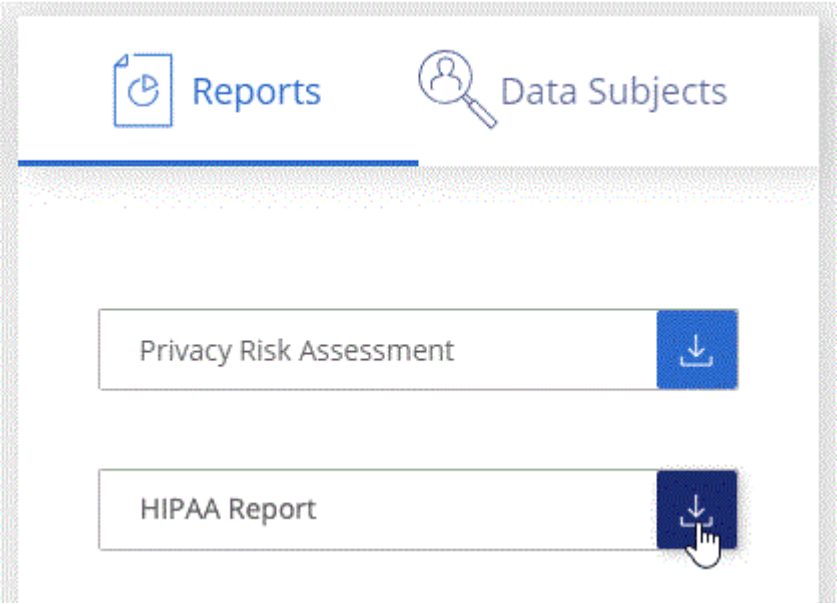
Entornos en los que se encontró la información médica y si está habilitada el cifrado y la protección contra ransomware.

Generar el informe HIPAA

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **cumplimiento** y, a continuación, haga clic en el icono de descarga situado junto a **Informe HIPAA** en **Informes**.



Resultado

La clasificación de BlueXP genera un informe PDF que se puede revisar y enviar a otros grupos según sea

necesario.

¿Qué es una solicitud de acceso de asunto de datos?

Las normas de privacidad, como el GDPR europeo, otorgan a sujetos de datos (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un sujeto de datos solicita esta información, se le conoce como DSAR (solicitud de acceso a sujetos de datos). Las organizaciones deben responder a estas solicitudes "sin demora indebida" y, a más tardar, en el plazo de un mes a partir de su recepción.

Puede responder a un DSAR buscando el nombre completo o el identificador conocido de un sujeto (como una dirección de correo electrónico) y, a continuación, descargando un informe. El informe está diseñado para ayudar en el requisito de su organización a cumplir con el RGPD o con leyes de privacidad de datos similares.

¿Cómo puede ayudarte la clasificación de BlueXP a responder a un DSAR?

Cuando realiza la búsqueda de los datos del sujeto, la clasificación de BlueXP busca todos los archivos, los bloques y las cuentas de OneDrive y SharePoint que tienen el nombre o el identificador de esa persona. La clasificación de BlueXP comprueba el nombre o el identificador de los datos preindexados más recientes. No inicia una nueva exploración.

Una vez finalizada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso a un sujeto de datos. El informe agrega información procedente de los datos y los coloca en términos legales de los que se puede enviar a la persona.

> La búsqueda de sujetos de datos no es compatible en las bases de datos en este momento.

Buscar temas de datos y descargar informes

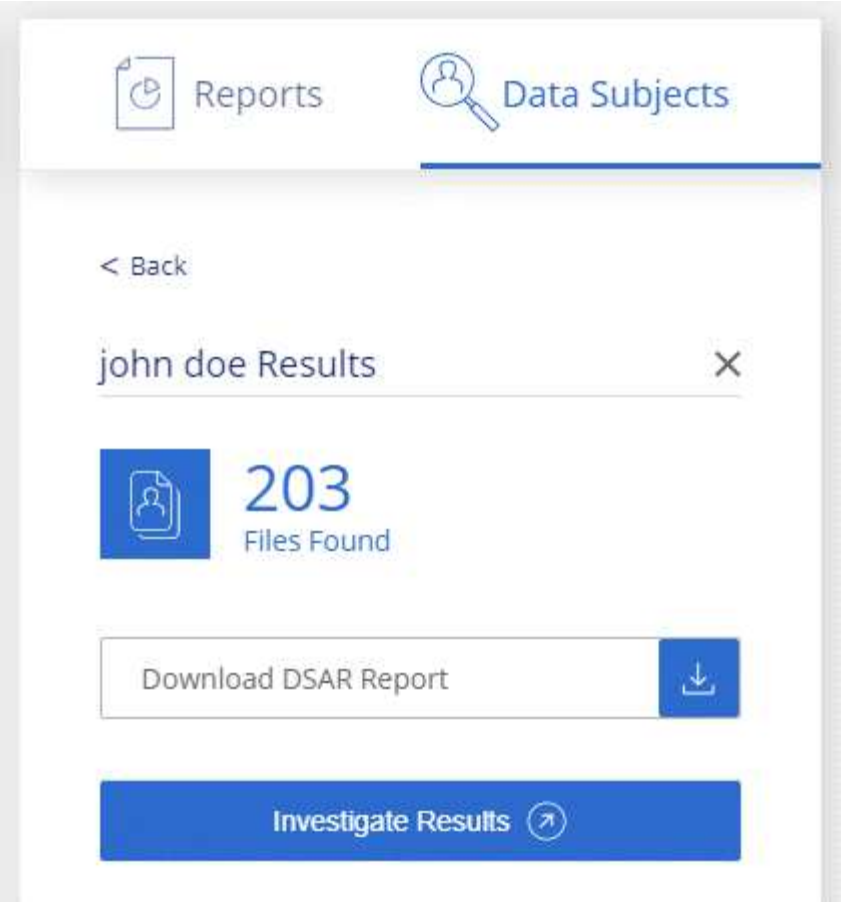
Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "cualquier tipo de información personal".

> El inglés, el alemán, el japonés y el español son compatibles al buscar los nombres de los sujetos de datos. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Temas de datos**.
3. Busque el nombre completo o el identificador conocido del sujeto de datos.

   A continuación se muestra un ejemplo que muestra una búsqueda del nombre *john doe*:



4. Elija una de las opciones disponibles:
   - **Descargar informe DSAR**: Respuesta formal a la solicitud de acceso que se puede enviar al sujeto de datos. Este informe contiene información generada automáticamente en función de los datos que se ha encontrado en la clasificación de BlueXP del interesado y que se ha diseñado para utilizarse como plantilla. Debe completar el formulario y revisarlo internamente antes de enviarlo al sujeto de datos.
   - **investigar resultados**: Página que permite investigar los datos mediante la búsqueda, clasificación, ampliación de los detalles de un archivo específico y descarga de la lista de archivos.

     Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista de archivos.

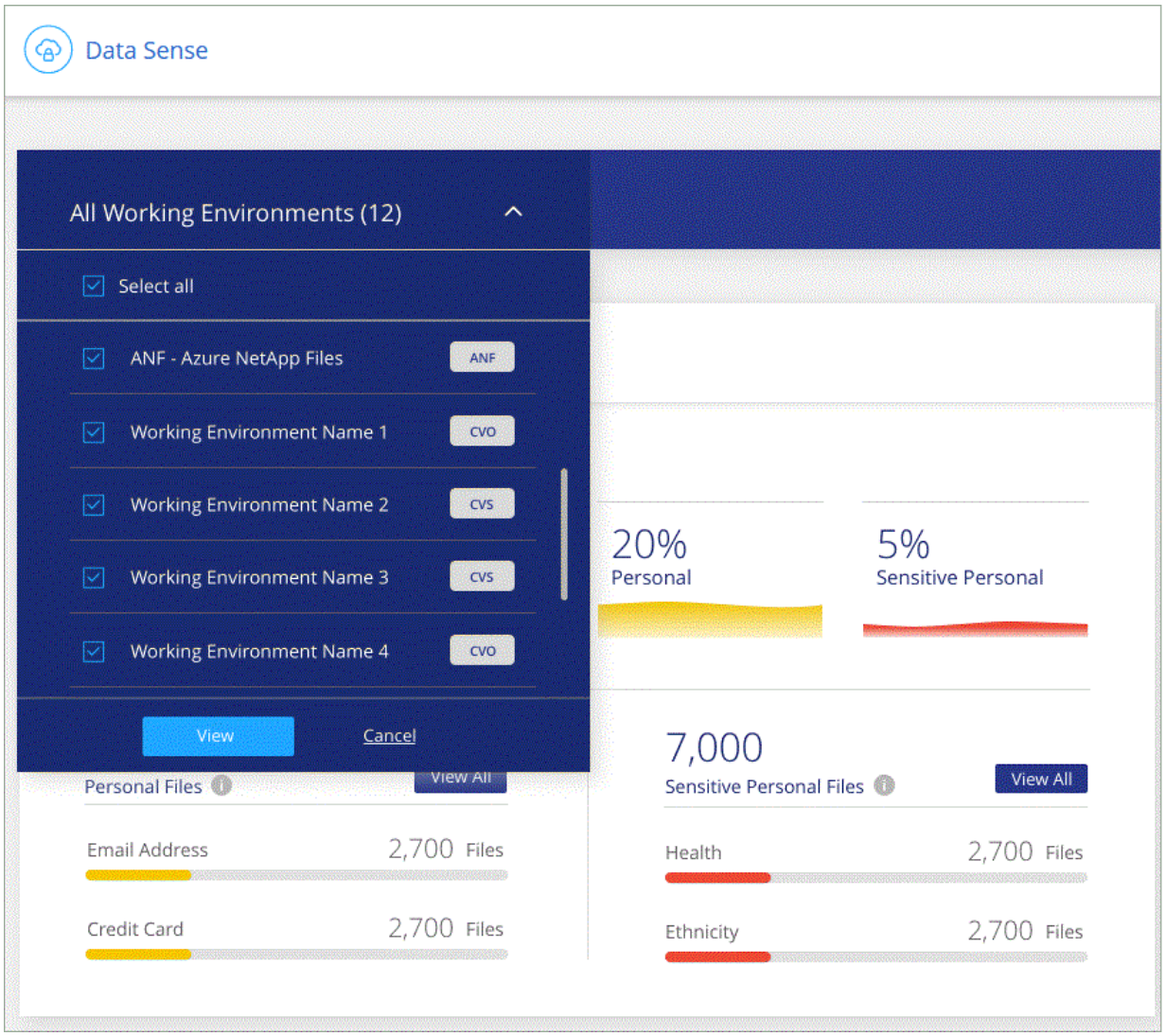
Seleccione los entornos de trabajo para los informes

Puedes filtrar el contenido de la consola de cumplimiento de normativas de clasificación de BlueXP para ver los datos de cumplimiento de todos los entornos de trabajo y bases de datos, o simplemente para entornos de trabajo específicos.

Al filtrar la consola, la clasificación de BlueXP define los datos de cumplimiento y los informes solo a los entornos de trabajo que has seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.


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

Gestiona la clasificación de BlueXP

Añade identificadores de datos personales a tus análisis de clasificación de BlueXP

La clasificación de BlueXP ofrece muchas formas de añadir una lista personalizada de «datos personales» que identificará la clasificación de BlueXP en futuros análisis, lo que te da una imagen completa sobre dónde residen los datos potencialmente confidenciales en *todos* los archivos de tu organización.

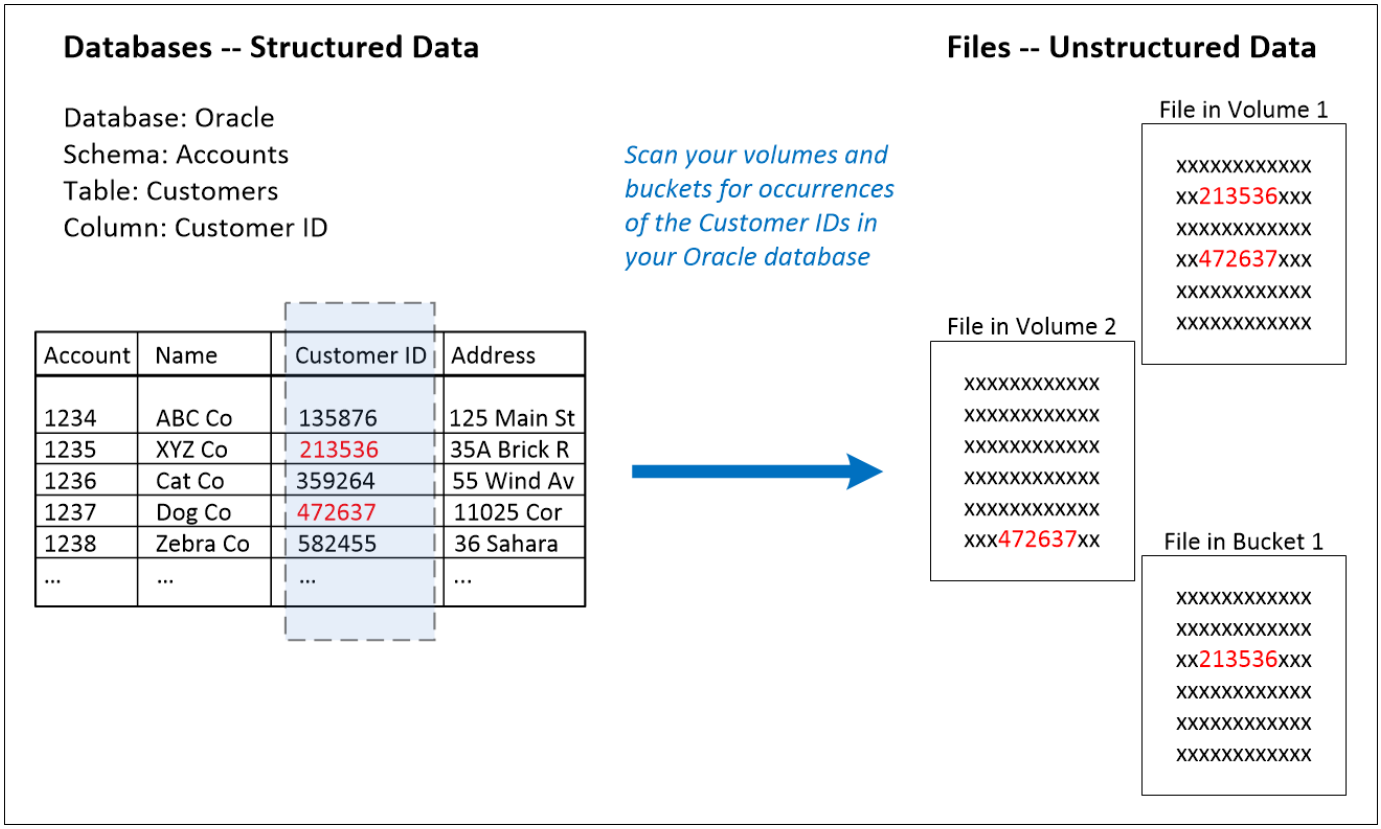
- Puede agregar identificadores únicos basados en columnas específicas de las bases de datos que está analizando.
- Puede agregar palabras clave personalizadas desde un archivo de texto: Estas palabras se identifican dentro de sus datos.
- Puede agregar un patrón personal utilizando una expresión regular (regex) — el regex se agrega a los patrones predefinidos existentes.
- Puede agregar categorías personalizadas para identificar dónde se encuentran determinadas categorías de información en los datos.

Todos estos mecanismos para agregar criterios de análisis personalizados se admiten en todos los idiomas.

> Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

Agregar identificadores de datos personales personalizados de las bases de datos

Una función que llamamos *Data Fusion* le permite analizar los datos de su organización para identificar si los identificadores únicos de sus bases de datos se encuentran en cualquiera de sus otros orígenes de datos. Puedes elegir los identificadores adicionales que buscará la clasificación de BlueXP en sus análisis si seleccionas una columna o columnas específicas en una tabla de base de datos. Por ejemplo, el siguiente diagrama muestra cómo se utilizan data Fusion para analizar los volúmenes, bloques y bases de datos en busca de apariciones de todos los ID de cliente de la base de datos de Oracle.



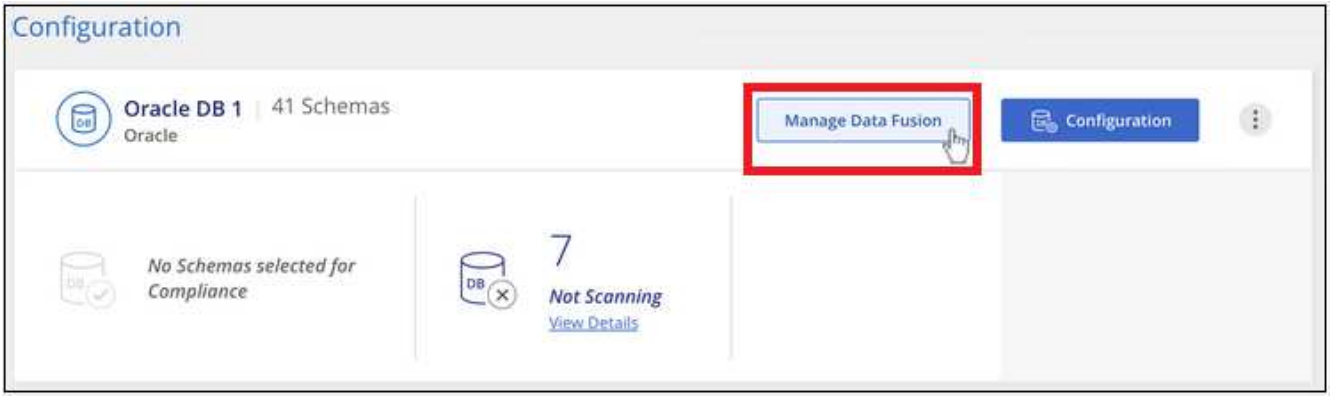
Como puede ver, se han encontrado dos ID de cliente únicos en dos volúmenes y en un bloque de S3. También se identificarán todas las coincidencias en las tablas de la base de datos.

Tenga en cuenta que, como escanea sus propias bases de datos, independientemente del idioma en el que se almacenen los datos se utilizará para identificar datos en futuros análisis de clasificación de BlueXP.

Pasos

Debe tener "se añadió al menos un servidor de base de datos" A la clasificación de BlueXP antes de poder añadir orígenes de datos Fusion.

1. En la página Configuración, haga clic en **Administrar Fusion de datos** en la base de datos donde residen los datos de origen.



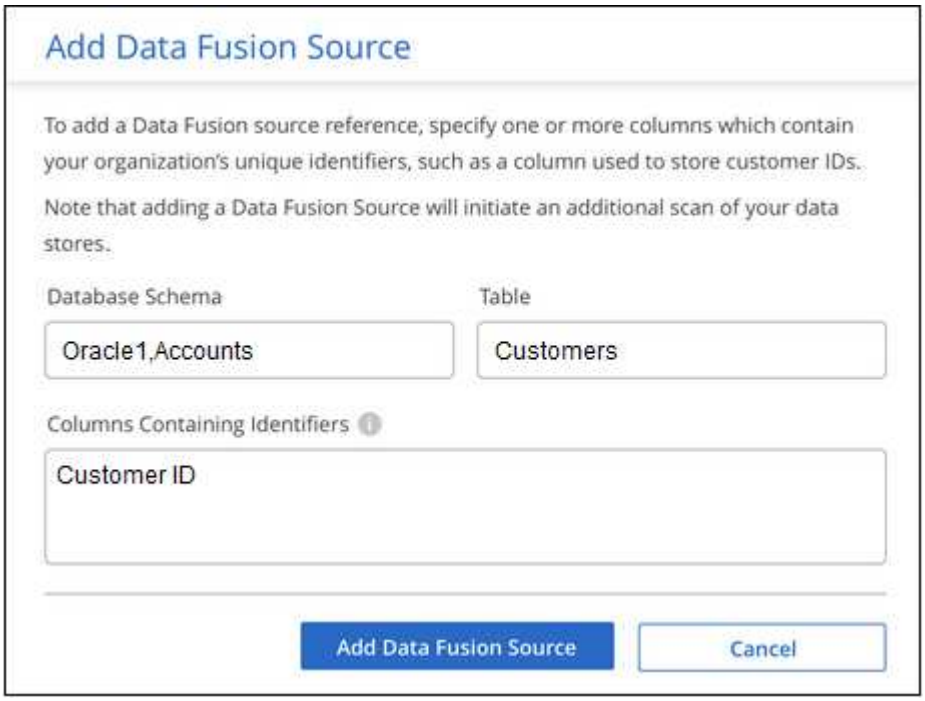
2. Haga clic en **Agregar origen de Fusion de datos** en la página siguiente.
3. En la página *Add Data Fusion Source*:

a. Seleccione el esquema de base de datos en el menú desplegable.

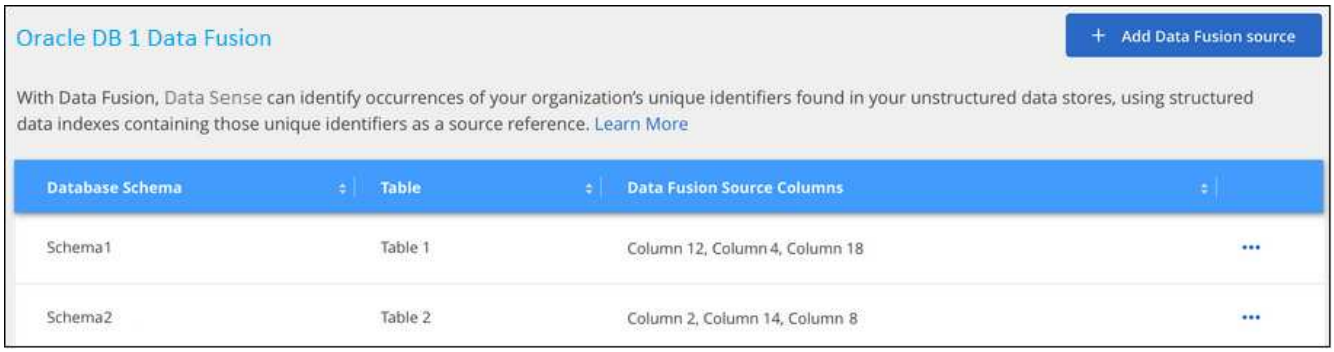
b. Introduzca el nombre de la tabla en ese esquema.

c. Introduzca la columna, o Columns, que contiene los identificadores únicos que desea utilizar.

   Al agregar varias columnas, introduzca cada nombre de columna o nombre de vista de tabla en una línea independiente.

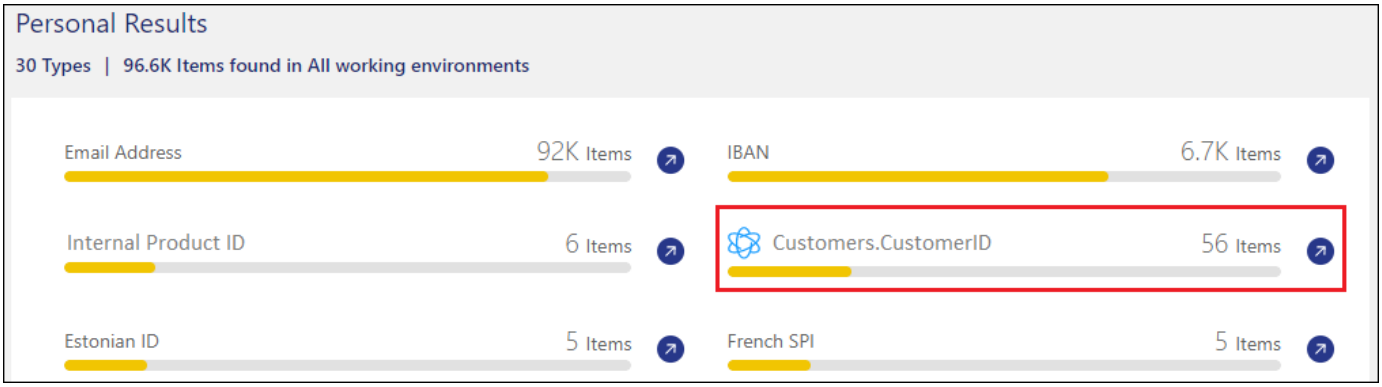


4. Haga clic en **Agregar origen de Fusion de datos**.



Resultados

Después del siguiente análisis, los resultados incluirán esta nueva información en el Panel de cumplimiento en la sección "resultados personales" y en la página Investigación del filtro "datos personales". El nombre utilizado para el clasificador aparece en la lista de filtros, por ejemplo `Customers.CustomerID`.



Eliminar un origen de Data Fusion

Si en algún momento decide no analizar sus archivos mediante un origen de Data Fusion determinado, puede seleccionar la fila de origen en la página de inventario de Data Fusion y hacer clic en **Eliminar origen de Data Fusion**.

Agregar palabras clave personalizadas de una lista de palabras

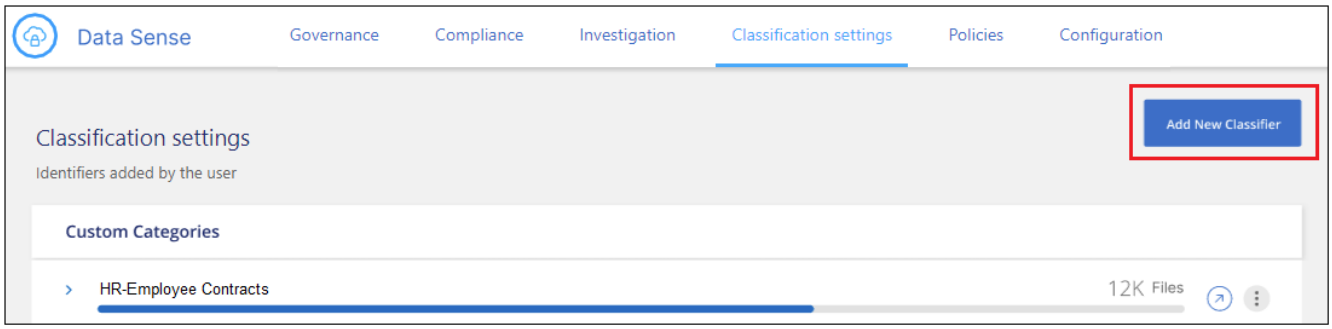
Puedes añadir palabras clave personalizadas a la clasificación de BlueXP para que identifique dónde se encuentra esa información en tus datos. Para añadir las palabras clave solo tienes que introducir las palabras que quieras que reconozca la clasificación de BlueXP. Las palabras clave se agregan a las palabras clave predefinidas existentes que ya usa la clasificación de BlueXP, y los resultados serán visibles en la sección Patrones personales.

Por ejemplo, es posible que desee ver dónde se mencionan los nombres internos de producto en todos los archivos para asegurarse de que estos nombres no están accesibles en ubicaciones que no son seguras.

Después de actualizar las palabras clave personalizadas, la clasificación de BlueXP reiniciará el análisis de todas las fuentes de datos. Una vez que el análisis se haya completado, los nuevos resultados aparecerán en el panel de cumplimiento de la clasificación de BlueXP, en la sección «Resultados personales», y en la página de investigación del filtro «Datos personales».

Pasos

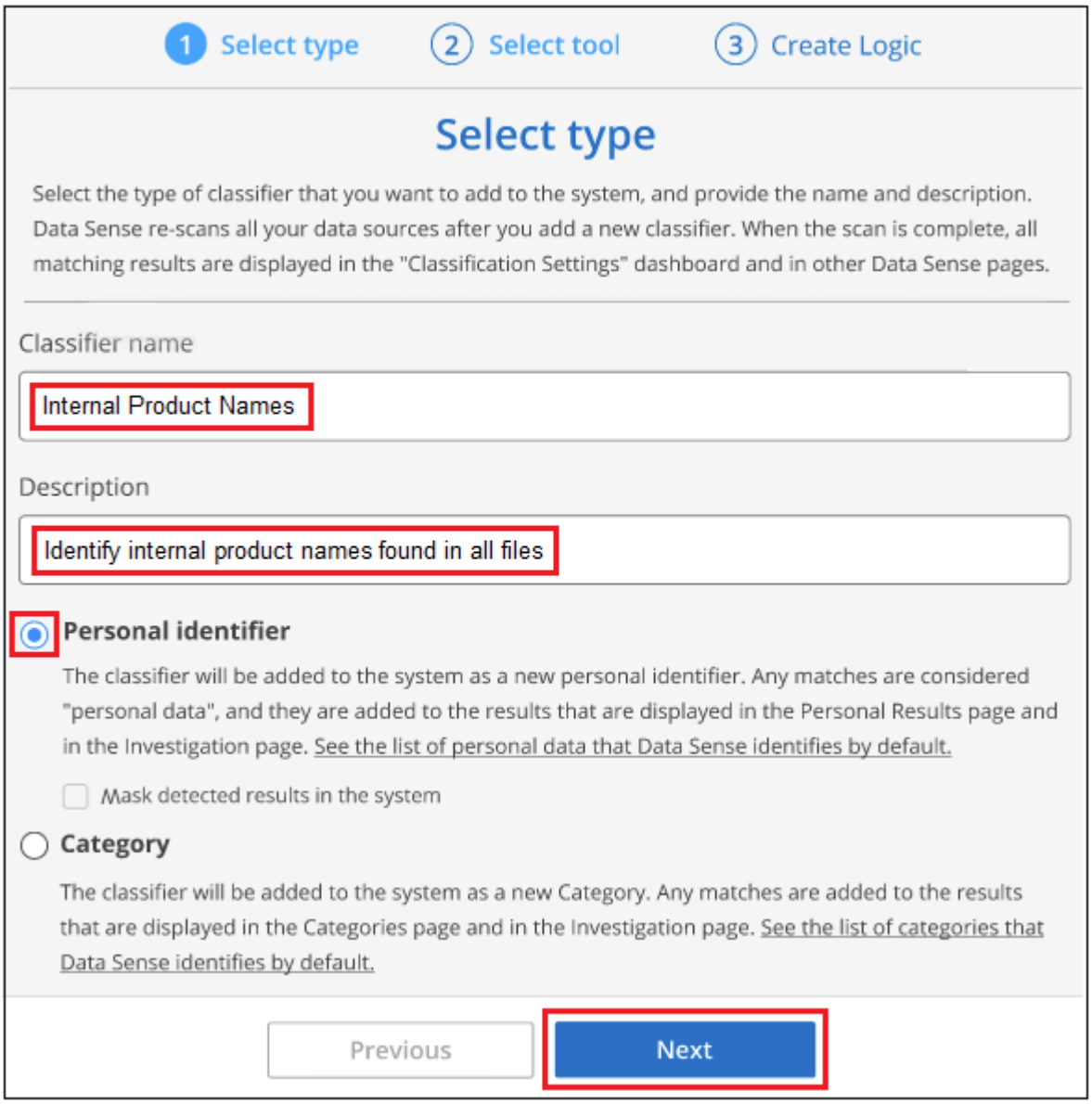
1. En la ficha *Classification settings*, haga clic en **Agregar nuevo clasificador** para iniciar el asistente *Add Custom Classifier*.



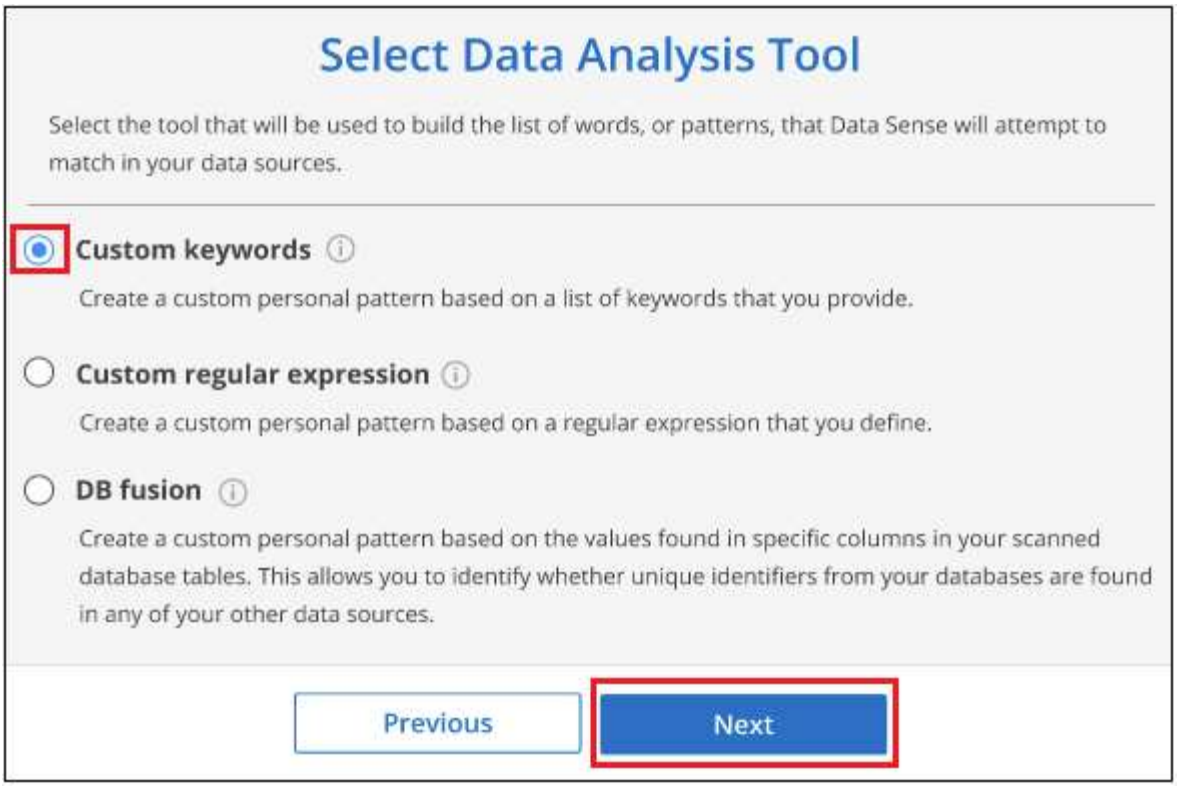
2. En la página *Select type*, escriba el nombre del clasificador, proporcione una breve descripción, seleccione **Identificador personal** y, a continuación, haga clic en **Siguiente**.

   El nombre que introduzcas aparecerá en la interfaz de usuario de clasificación de BlueXP como encabezado de los archivos escaneados que coincidan con los requisitos del clasificador, así como el nombre del filtro en la página de investigación.

   También puede marcar la casilla "Mask Detected results in the system" para que el resultado completo no aparezca en la interfaz de usuario. Por ejemplo, puede que desee hacer esto para ocultar los números completos de la tarjeta de crédito o datos personales similares (la máscara aparecerá en la IU de esta manera: "Pase:[***] pase:[] pase:[] pase:[***]" 3434).

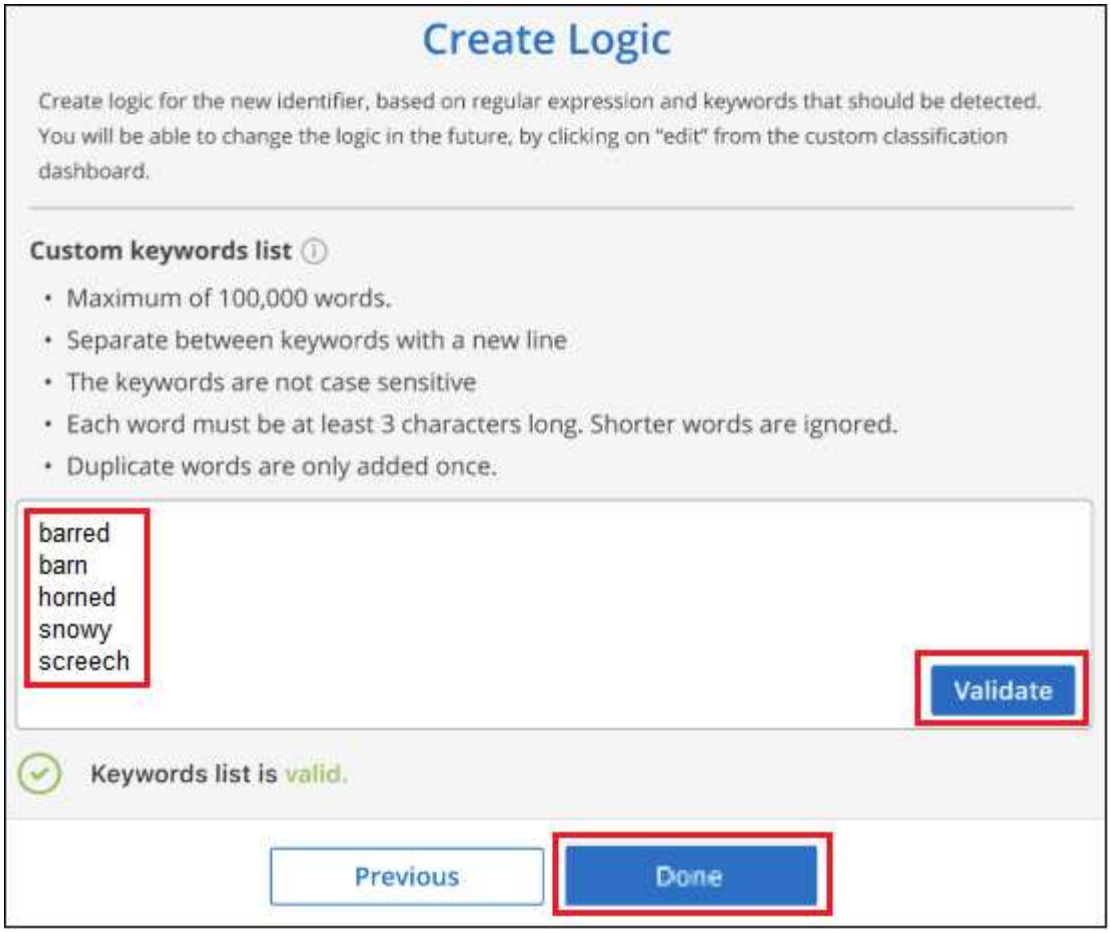


3. En la página *Select Data Analysis Tool*, seleccione **palabras clave personalizadas** como el método que desea utilizar para definir el clasificador y, a continuación, haga clic en **Siguiente**.



4. En la página *Create Logic*, introduzca las palabras clave que desee reconocer - cada palabra en una línea separada - y haga clic en **Validar**.

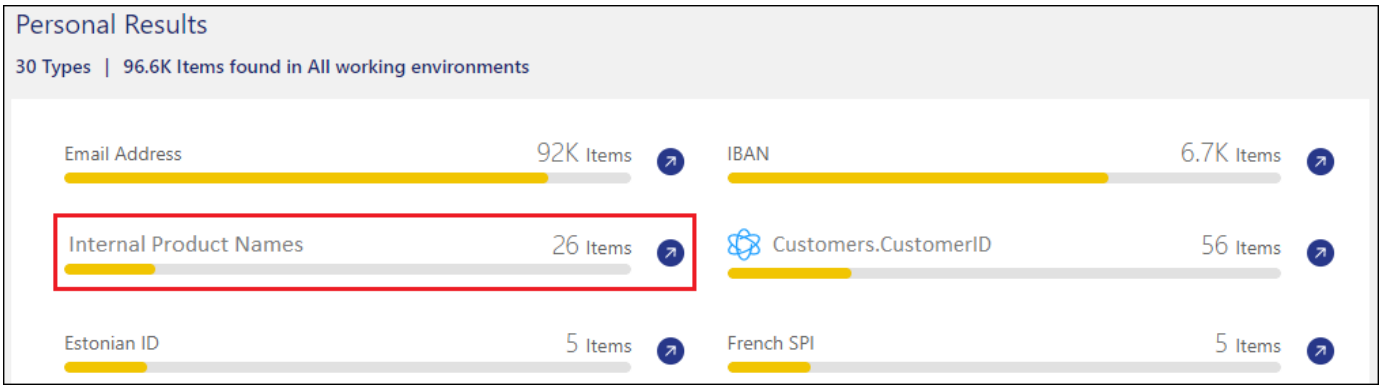
   La siguiente captura de pantalla muestra los nombres de productos internos (diferentes tipos de búhos). La búsqueda de clasificación de BlueXP para estos elementos no distingue mayúsculas de minúsculas.



5. Haz clic en **Listo** y la clasificación de BlueXP comienza a volver a analizar tus datos.

Resultados

Una vez finalizada la exploración, los resultados incluirán esta nueva información en el Panel de cumplimiento en la sección "resultados personales" y en la página Investigación del filtro "datos personales".



Como puede ver, el nombre del clasificador se utiliza como nombre en el panel resultados personales. De esta manera puede activar muchos grupos diferentes de palabras clave y ver los resultados de cada grupo.

Agregue identificadores de datos personales personalizados mediante un regex

Puede agregar un patrón personal para identificar información específica de los datos mediante una expresión regular personalizada (regex). Esto le permite crear un nuevo regex personalizado para identificar nuevos elementos de información personal que aún no existen en el sistema. El regex se agrega a los patrones

predefinidos existentes que ya usa la clasificación de BlueXP, y los resultados serán visibles en la sección Patrones personales.

Por ejemplo, puede que desee ver dónde se mencionan los ID de producto internos en todos sus archivos. Si el ID de producto tiene una estructura clara, por ejemplo, es un número de 12 dígitos que comienza con 201, puede utilizar la característica personalizada regex para buscarla en sus archivos. La expresión regular de este ejemplo es **\b201\d{9}\b**.

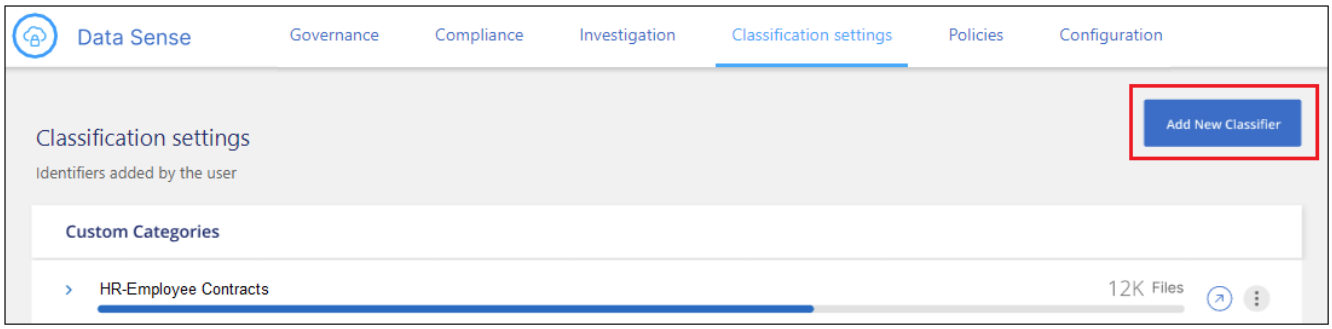
Después de añadir el regex, la clasificación de BlueXP reiniciará el análisis de todas las fuentes de datos. Una vez que el análisis se haya completado, los nuevos resultados aparecerán en el panel de cumplimiento de la clasificación de BlueXP, en la sección «Resultados personales», y en la página de investigación del filtro «Datos personales».

Si necesita ayuda para construir la expresión regular, consulte "Expresiones regulares 101". Elige **Python** para ver los tipos de resultados que la clasificación de BlueXP coincidirá con la expresión regular. La "Página de Python Regex Tester" también es útil al mostrar una representación gráfica de sus patrones.

> Actualmente no permitimos el uso de banderas de patrón al crear un regex - esto significa que no debe usar '/'.

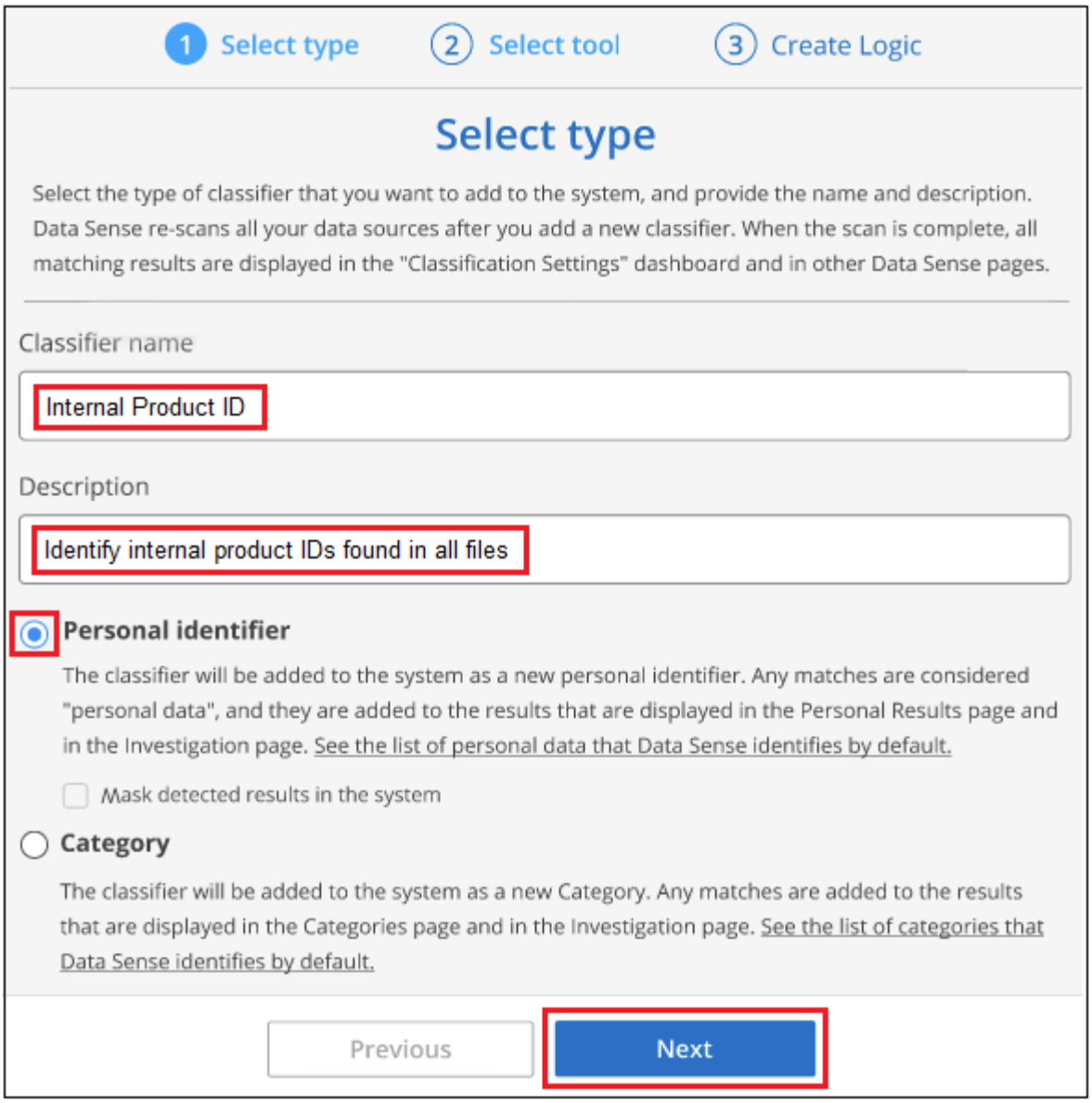
Pasos

1. En la ficha *Classification settings*, haga clic en **Agregar nuevo clasificador** para iniciar el asistente *Add Custom Classifier*.

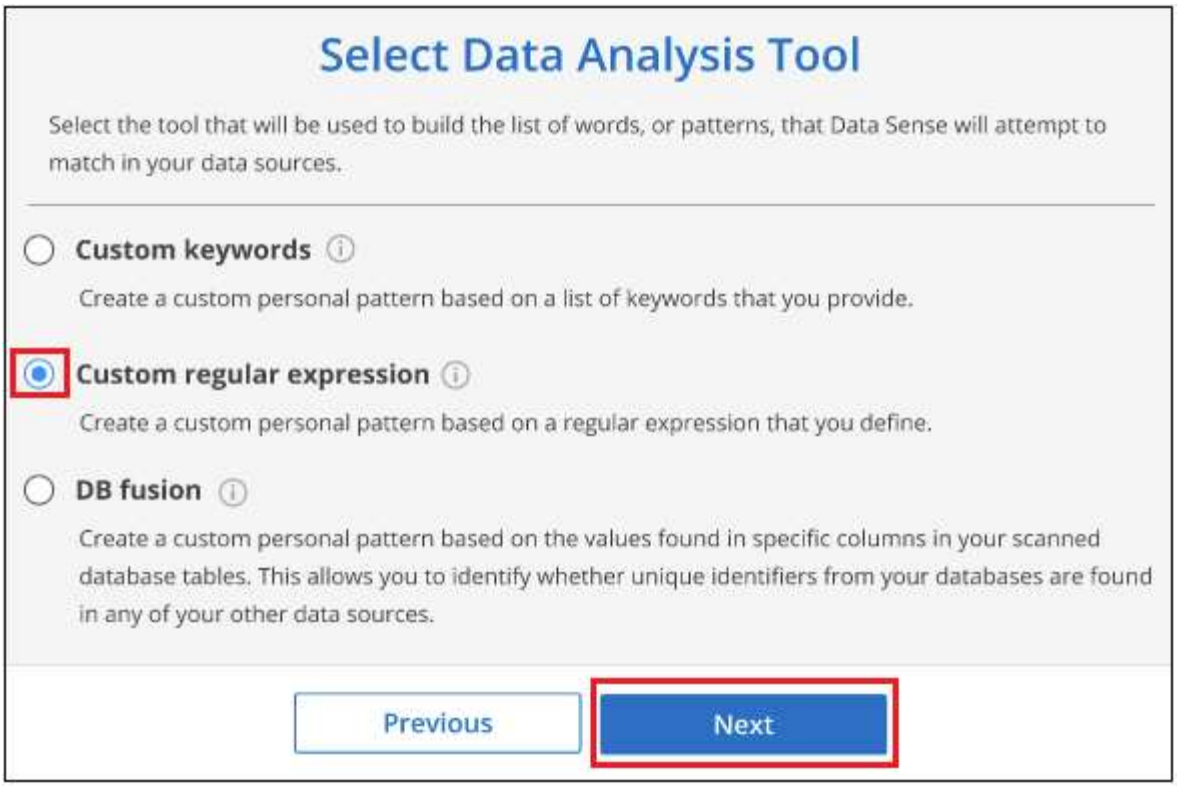


2. En la página *Select type*, escriba el nombre del clasificador, proporcione una breve descripción, seleccione **Identificador personal** y, a continuación, haga clic en **Siguiente**.

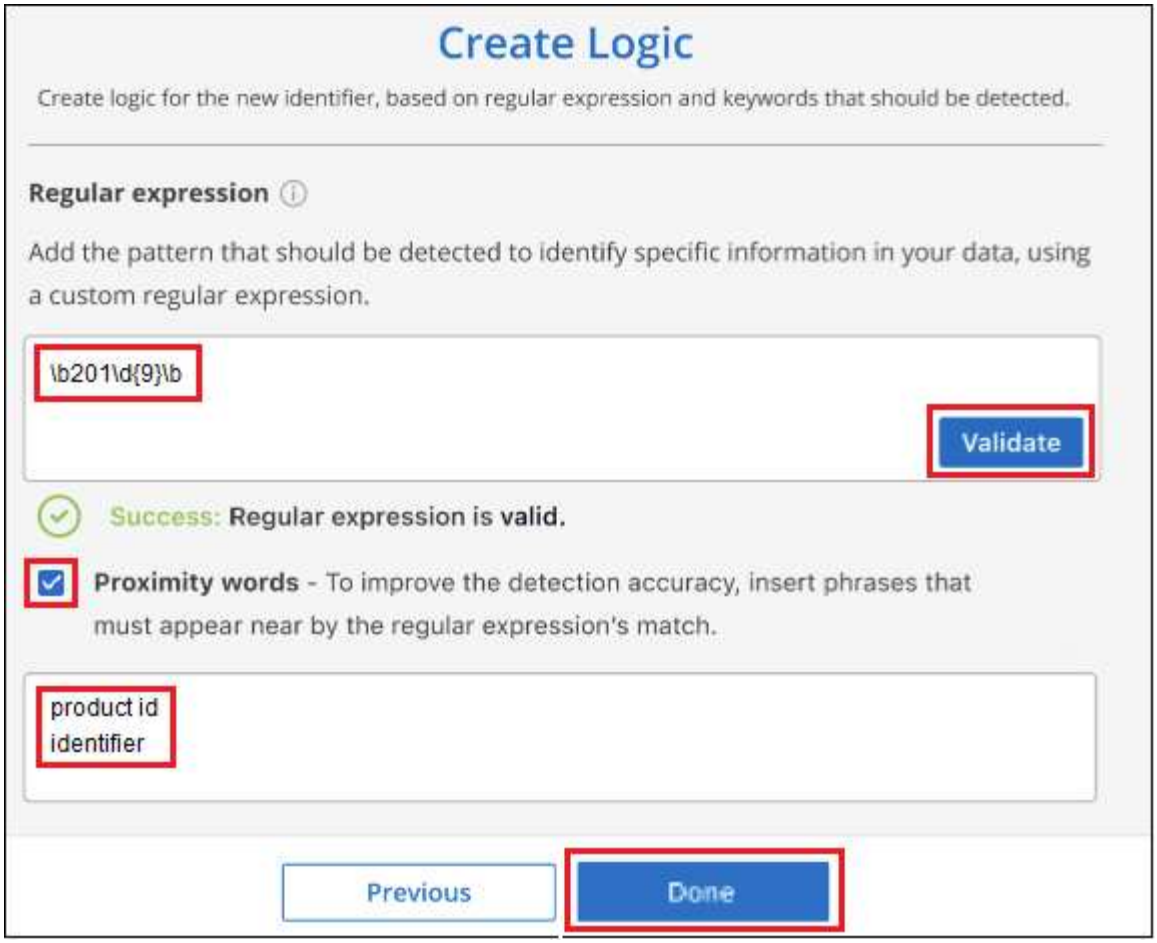
   El nombre que introduzcas aparecerá en la interfaz de usuario de clasificación de BlueXP como encabezado de los archivos escaneados que coincidan con los requisitos del clasificador, así como el nombre del filtro en la página de investigación. También puede marcar la casilla "Mask Detected results in the system" para que el resultado completo no aparezca en la interfaz de usuario. Por ejemplo, puede que desee hacer esto para ocultar los números completos de la tarjeta de crédito o datos personales similares.



3. En la página *Select Data Analysis Tool*, seleccione **expresión regular personalizada** como el método que desea utilizar para definir el clasificador y, a continuación, haga clic en **Siguiente**.

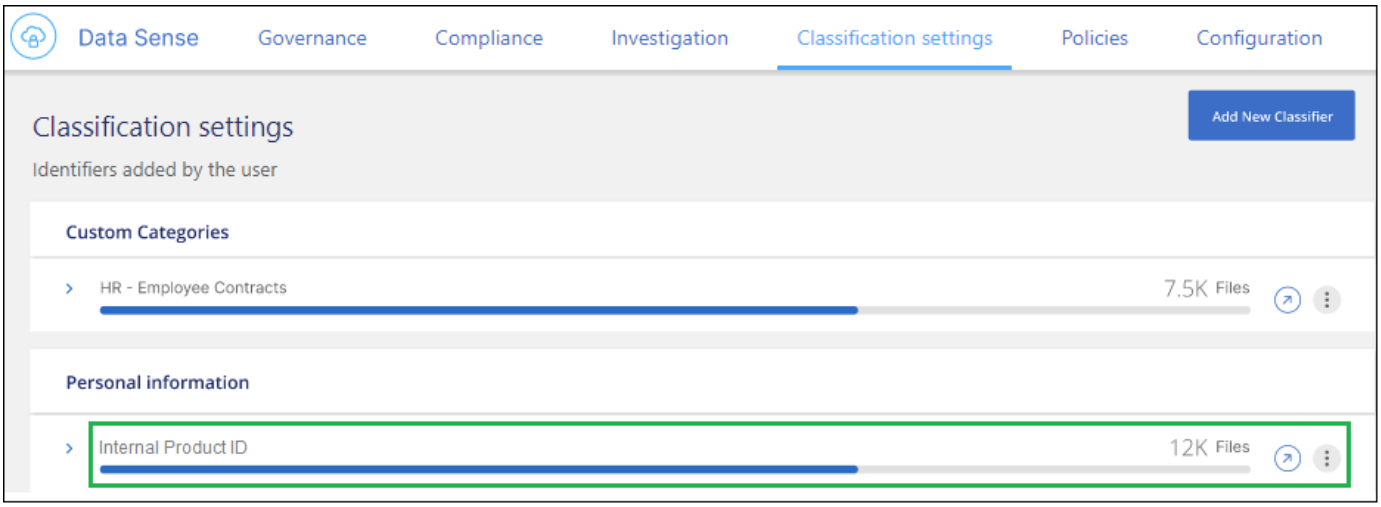


4. En la página *Create Logic*, introduzca la expresión regular y las palabras de proximidad y haga clic en **hecho**.
   a. Puede introducir cualquier expresión regular legal. Haz clic en el botón **Validar** para que la clasificación de BlueXP verifique que la expresión regular es válida y que no es demasiado amplia, lo que significa que devolverá demasiados resultados.
   b. Opcionalmente, puede introducir algunas palabras de proximidad para ayudar a refinar la precisión de los resultados. Estas son palabras que normalmente se encuentran dentro de los 300 caracteres del patrón que está buscando (antes o después del patrón encontrado). Introduzca cada palabra o frase en una línea diferente.



Resultados

Se añade el clasificador y la clasificación de BlueXP empieza a volver a analizar todas tus fuentes de datos. Volverá a la página Clasificadores personalizados, donde podrá ver el número de archivos que coinciden con el nuevo clasificador. Los resultados del análisis de todos los orígenes de datos tardarán un poco en función del número de archivos que se deban analizar.



Agregar categorías personalizadas

La clasificación de BlueXP toma los datos que escanea y los divide en distintos tipos de categorías. Las categorías son temas basados en el análisis de inteligencia artificial del contenido y los metadatos de cada

archivo. "Consulte la lista de categorías predefinidas".

Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como *resume* o *Employee Contracts* puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

Puedes agregar categorías personalizadas a la clasificación de BlueXP para que puedas identificar qué categorías de información son únicas para el conjunto de datos se encuentran en tus datos. Puedes añadir cada categoría creando archivos de «entrenamiento» que contengan las categorías de datos que quieres identificar y, a continuación, hacer que la clasificación de BlueXP analice esos archivos para «aprender» a través de la IA para que pueda identificar esos datos en tus fuentes de datos. Las categorías se añaden a las categorías predefinidas existentes que ya identifica la clasificación de BlueXP y los resultados se pueden ver en la sección Categorías.

Por ejemplo, es posible que desee ver dónde se encuentran los archivos de instalación comprimidos en formato .gz en sus archivos para que pueda eliminarlos, si es necesario.

Después de actualizar las categorías personalizadas, la clasificación de BlueXP reiniciará el análisis de todas las fuentes de datos. Una vez que se haya completado el análisis, los nuevos resultados aparecerán en la consola de cumplimiento de la clasificación de BlueXP, en la sección «Categorías» y en la página de investigación del filtro «Categoría». "Vea cómo ver archivos por categorías".

Lo que necesitará

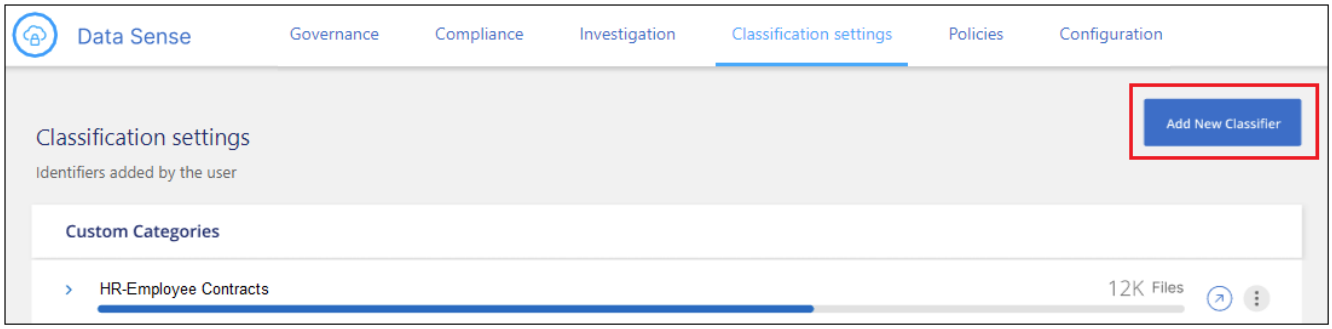
Tendrás que crear un mínimo de 25 archivos de entrenamiento que contengan muestras de las categorías de datos que quieres que reconozca la clasificación de BlueXP. Se admiten los siguientes tipos de archivo:

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

Los archivos deben tener un mínimo de 100 bytes y deben encontrarse en una carpeta a la que se pueda acceder mediante la clasificación de BlueXP.

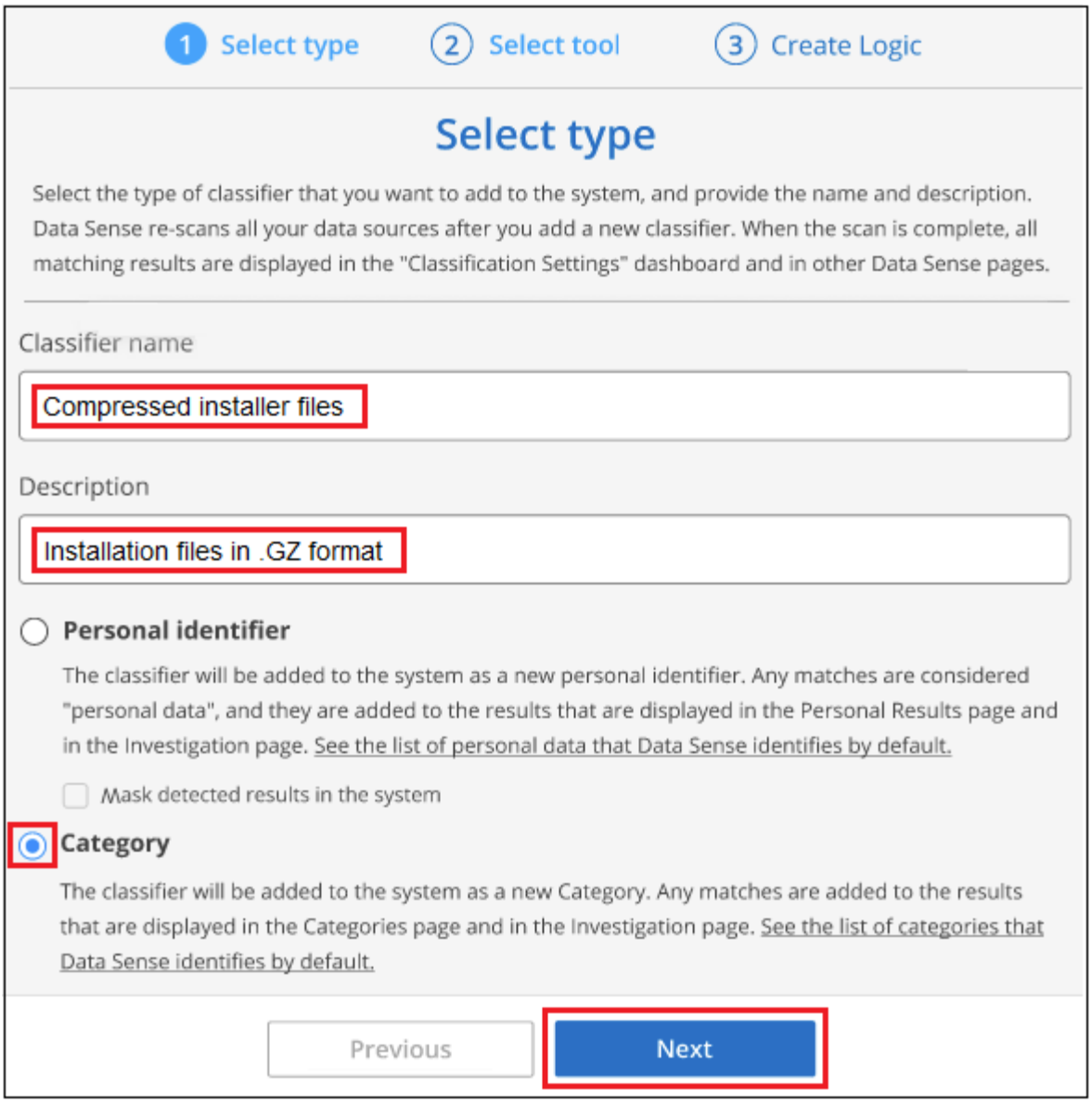
Pasos

1. En la ficha *Classification settings*, haga clic en **Agregar nuevo clasificador** para iniciar el asistente *Add Custom Classifier*.

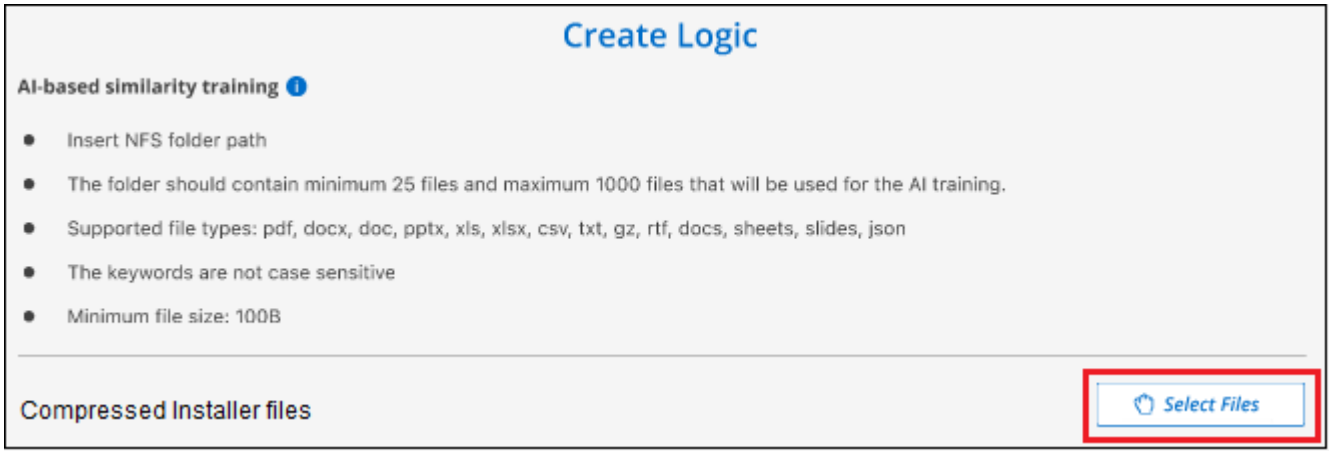


2. En la página *Select type*, introduzca el nombre del clasificador, proporcione una breve descripción, seleccione **Categoría** y, a continuación, haga clic en **Siguiente**.

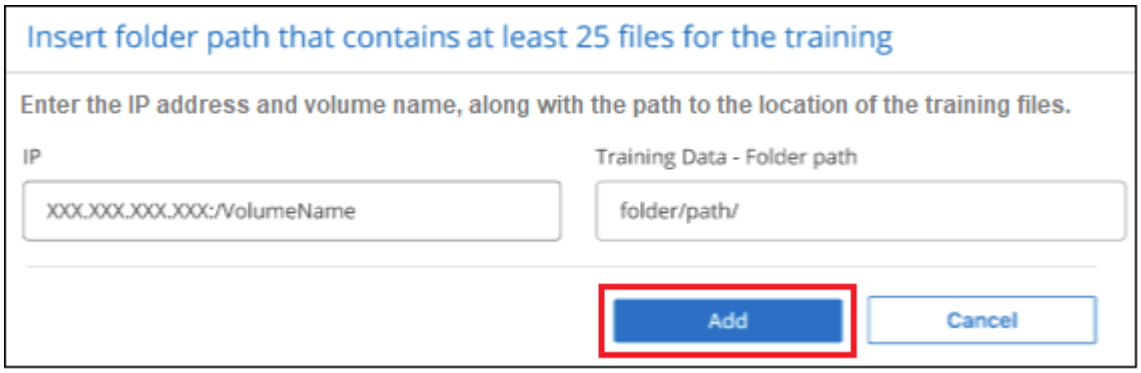
   El nombre que introduzcas aparecerá en la interfaz de usuario de clasificación de BlueXP como encabezado de los archivos escaneados que coincidan con la categoría de datos que vas a definir, y como nombre del filtro en la página de investigación.



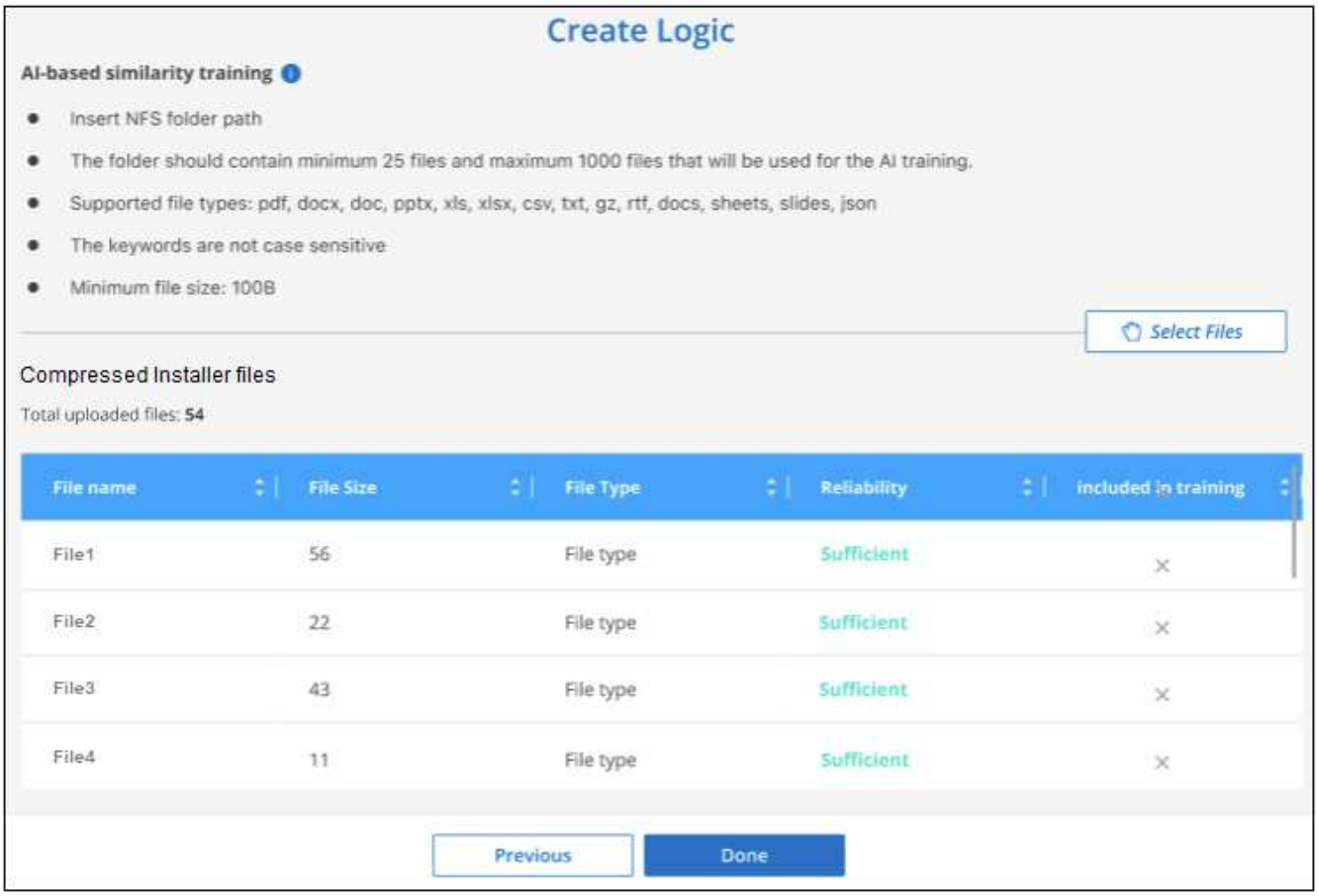
3. En la página *Create Logic*, asegúrese de que tiene preparados los archivos de aprendizaje y, a continuación, haga clic en **Seleccionar archivos**.



4. Introduzca la dirección IP del volumen y la ruta de acceso donde se encuentran los archivos de entrenamiento y haga clic en **Agregar**.



5. Comprueba que los archivos de entrenamiento se hayan reconocido mediante la clasificación de BlueXP. Haga clic en **x** para eliminar los archivos de entrenamiento que no cumplan los requisitos. A continuación, haga clic en **hecho**.

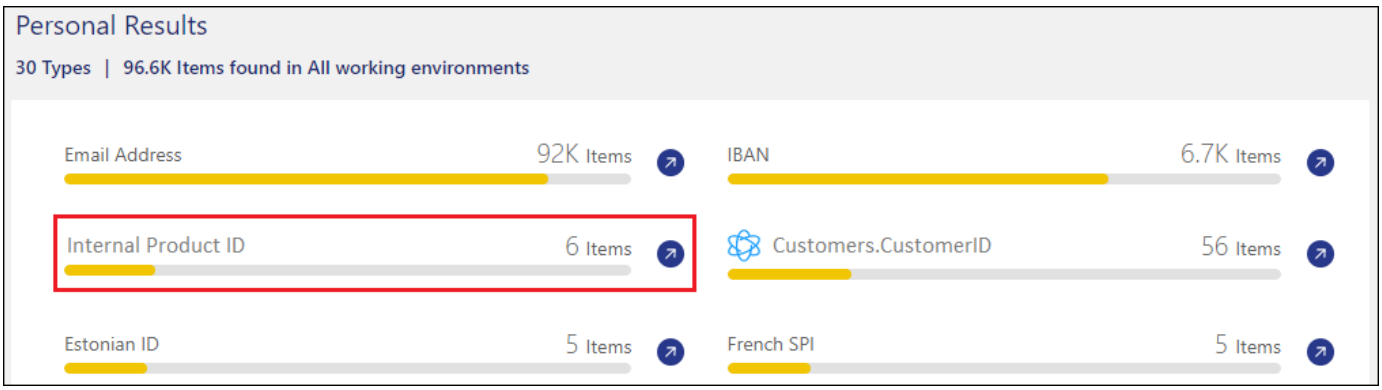


Resultados

La nueva categoría se crea tal y como se define en los archivos de entrenamiento y se agrega a la clasificación de BlueXP. A continuación, la clasificación de BlueXP empieza a volver a analizar todas tus fuentes de datos para identificar los archivos que se adaptan a esta nueva categoría. Volverá a la página Clasificadores personalizados, donde podrá ver el número de archivos que coinciden con la nueva categoría. Los resultados del análisis de todos los orígenes de datos tardarán un poco en función del número de archivos que se deban analizar.

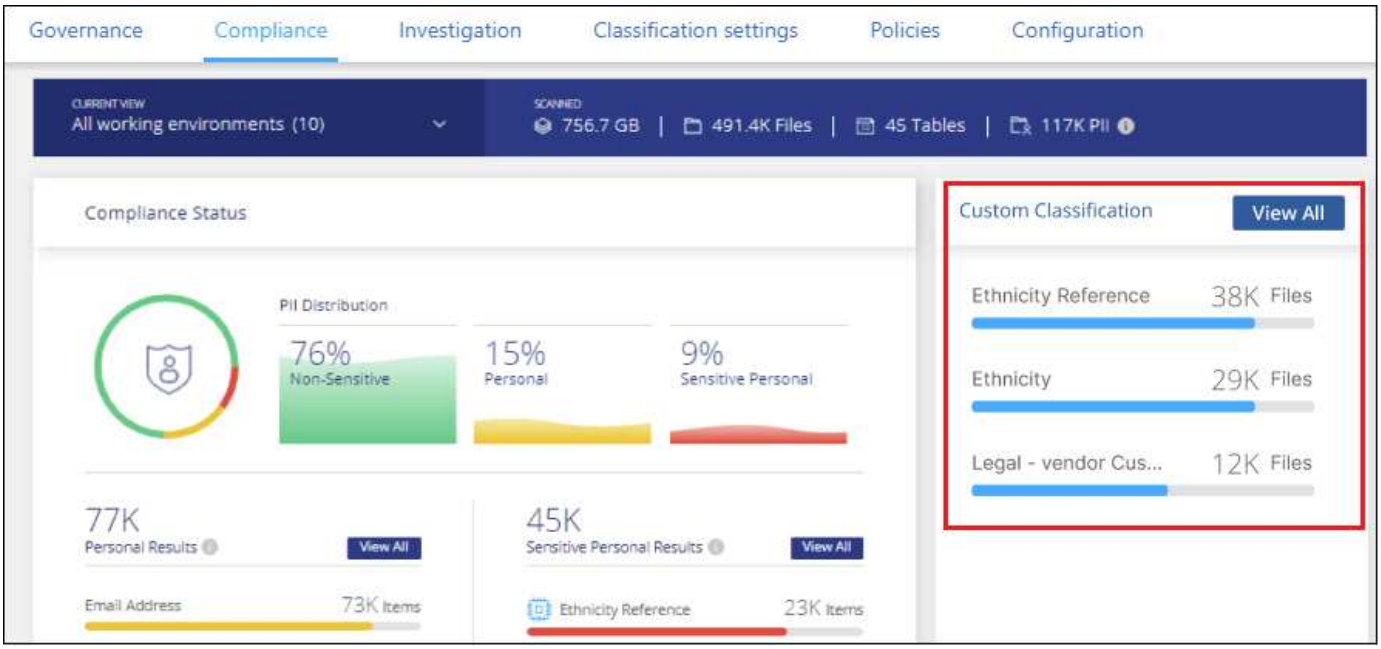
Vea los resultados de sus clasificadores personalizados

Puede ver los resultados desde cualquiera de los clasificadores personalizados en el Panel de cumplimiento y en la página Investigación. Por ejemplo, esta captura de pantalla muestra la información coincidente en el Panel de cumplimiento en la sección "resultados personales".



Haga clic en la Para ver los resultados detallados en la página Investigación.

Además, todos los resultados del clasificador personalizado aparecen en la ficha Clasificadores personalizados y los 6 resultados superiores del clasificador personalizado se muestran en el Panel de cumplimiento, como se muestra a continuación.



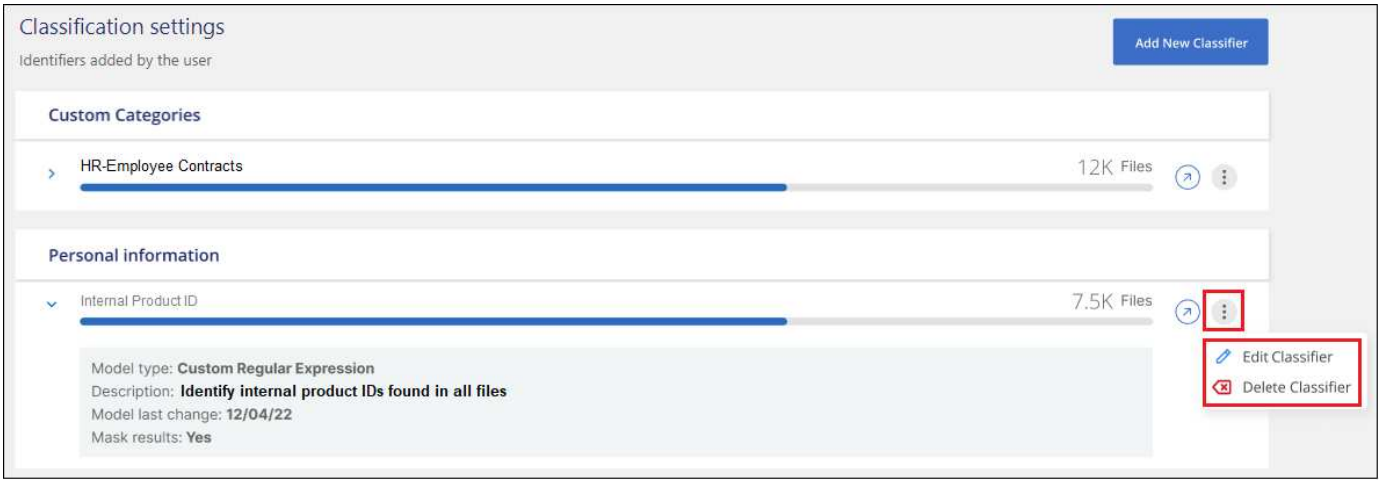
Administrar clasificadores personalizados

Puede cambiar cualquiera de los clasificadores personalizados que haya creado utilizando el botón **Editar clasificador**.

No puede editar los clasificadores de Data Fusion en este momento.

Y si decides en algún momento posterior que no necesitas la clasificación de BlueXP para identificar los patrones personalizados que agregaste, puedes usar el botón **Eliminar clasificador** para eliminar cada

elemento.



Excluye directorios específicos de las exploraciones de clasificación de BlueXP

Si desea que la clasificación de BlueXP excluya los datos de análisis que residen en determinados directorios de orígenes de datos, puede añadir estos nombres de directorio a un archivo de configuración. Después de aplicar este cambio, el motor de clasificación de BlueXP excluirá el análisis de datos en esos directorios.

Tenga en cuenta que la clasificación de BlueXP está configurada de forma predeterminada para excluir los datos de copias Snapshot de volumen de análisis porque el contenido es idéntico al contenido del volumen.

Esta funcionalidad está disponible en la clasificación de BlueXP versión 1,29 y posteriores (a partir de marzo de 2024).

Orígenes de datos compatibles

Se admite la exclusión de directorios específicos de los análisis de clasificación de BlueXP para los recursos compartidos NFS y CIFS en las siguientes fuentes de datos:

- ONTAP en las instalaciones
- Cloud Volumes ONTAP
- Amazon FSX para ONTAP de NetApp
- Azure NetApp Files
- Recursos generales para recursos compartidos de archivos

Defina los directorios que se excluirán de la exploración

Para poder excluir los directorios del análisis de clasificación, debe iniciar sesión en el sistema de clasificación de BlueXP para poder editar un archivo de configuración y ejecutar un script. Descubra cómo "Inicia sesión en el sistema de clasificación de BlueXP" Dependiendo de si instaló manualmente el software en una máquina Linux o si implementó la instancia en la nube.

- Puedes excluir un máximo de 50 rutas de directorio por sistema de clasificación de BlueXP.
- La exclusión de las rutas de acceso de directorio puede afectar a los tiempos de exploración.

Pasos

1. En el sistema de clasificación de BlueXP, vaya a «/opt/netapp/config/custom_configuration» y abra el archivo `data_provider.yaml`.
2. En la sección “data_providers”, bajo la línea “exclude:”, introduzca las rutas de acceso del directorio que desea excluir. Por ejemplo:

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

   No cambie nada más en este archivo.

3. Guarde los cambios en el archivo.
4. Vaya a «/opt/netapp/Datasense/tools/customer_configuration/data_providers» y ejecute el siguiente script:

   ```
   update_data_providers_from_config_file.sh
   ```

   Este comando confirma los directorios que se excluirán de la exploración en el motor de clasificación.

Resultado

Todos los escaneos posteriores de sus datos excluirán el escaneo de esos directorios especificados.

Puede agregar, editar o eliminar elementos de la lista de exclusión mediante estos mismos pasos. La lista de exclusión revisada se actualizará después de ejecutar el script para confirmar los cambios.

Ejemplos

Configuración 1:

Cada carpeta que contenga “folder1” en cualquier lugar del nombre será excluida de todas las fuentes de datos.

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

Resultados esperados para las rutas que se excluirán:

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

- /CVO1/*folder1
- /CVO1/+folder1name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Ejemplos de rutas que no se excluirán:

- /CVO1/*carpeta
- /CVO1/nombre de carpeta
- /CVO22/*folder20

Configuración 2:

Cada carpeta que contenga “*folder1” solo al inicio del nombre será excluida.

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

Resultados esperados para las rutas que se excluirán:

- /CVO/*folder1
- /CVO/*folder1name
- /CVO/*folder10

Ejemplos de rutas que no se excluirán:

- CVO/folder1
- CVO/folder1name
- /CVO/no*folder10

Configuración 3:

Todas las carpetas del origen de datos “CVO22” que contengan “folder1” en cualquier lugar del nombre serán excluidas.

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

Resultados esperados para las rutas que se excluirán:

- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Ejemplos de rutas que no se excluirán:

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

Escape de caracteres especiales en los nombres de carpetas

Si tiene un nombre de carpeta que contiene uno de los siguientes caracteres especiales y desea excluir los datos de esa carpeta de ser escaneados, deberá utilizar la secuencia de escape \\ antes del nombre de la carpeta.

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

Ruta de acceso en origen: `/project/*not_to_scan`

Sintaxis en el archivo de exclusión: `"\\*not_to_scan"`

Ver la lista de exclusión actual

Es posible para el contenido del `data_provider.yaml` el archivo de configuración debe ser diferente al que se ha confirmado después de ejecutar el `update_data_providers_from_config_file.sh` guión. Para ver la lista actual de directorios que ha excluido del análisis de clasificación de BlueXP, ejecute el siguiente comando en «/opt/netapp/Datasense/tools/customer_configuration/data_providers»:

```
get_data_providers_configuration.sh
```

Ver el estado de las acciones de cumplimiento

Cuando ejecuta una acción asincrónica desde el panel de resultados de la investigación en muchos archivos, por ejemplo, al mover o eliminar archivos 100, el proceso puede tardar algún tiempo. Puede supervisar el estado de estas acciones en el panel *Action Status* para saber cuándo se ha aplicado a todos los archivos.

Esto permite ver las acciones que se completaron correctamente, las que están en curso en ese momento y las que han fallado para poder diagnosticar y corregir cualquier problema. Tenga en cuenta que las operaciones cortas que se completan rápidamente, como mover un único archivo, no aparecen en el panel Estado de acciones.

El estado puede ser:

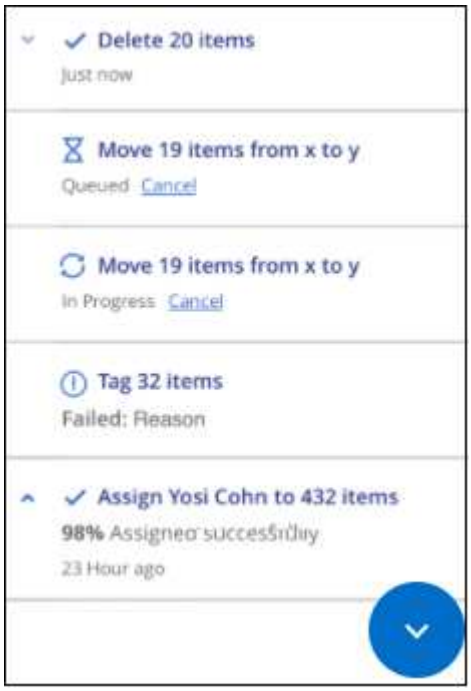
- Correcto: La acción de clasificación de BlueXP ha finalizado y todos los elementos se han realizado correctamente.
- Correcto parcial: Una acción de clasificación de BlueXP ha finalizado, algunos elementos han fallado y otros se han realizado correctamente.
- En curso: La acción sigue en curso.
- Queued: La acción no ha comenzado.

- Cancelado: La acción se ha cancelado.
- Error: La acción ha fallado.

Tenga en cuenta que puede cancelar cualquier acción que tenga el estado "en cola" o "en curso".

Pasos

1. En la parte inferior derecha de la interfaz de usuario de clasificación de BlueXP, puedes ver el botón **Actions Status** .
2. Haga clic en este botón y se muestran las 20 acciones más recientes.



Puede hacer clic en el nombre de una acción para ver los detalles correspondientes a esa operación.

Defina IDs de grupo adicionales como abiertos para la organización

Cuando se adjuntan ID de grupo (GID) a archivos o carpetas en recursos compartidos de archivos NFS, definen los permisos para el archivo o la carpeta; por ejemplo, si están «abiertos a la organización». Si algunos identificadores de grupo (GID) no se configuran inicialmente con el nivel de permiso «Abrir para organización», puede agregar ese permiso al GID para que todos los archivos y carpetas que tengan ese GID adjunto se consideren «abiertos a la organización».

Después de realizar este cambio y la clasificación de BlueXP vuelve a analizar los archivos y carpetas, todos los archivos y carpetas que tengan estos ID de grupo adjuntos mostrarán este permiso en la página Detalles de la investigación, y también aparecerán en los informes donde se muestran los permisos de archivo.

Para activar esta funcionalidad, debes iniciar sesión en el sistema de clasificación de BlueXP para poder editar un archivo de configuración y ejecutar un script. Descubra cómo "Inicia sesión en el sistema de

clasificación de BlueXP" Dependiendo de si instaló manualmente el software en una máquina Linux o si implementó la instancia en la nube.

Agregue el permiso de apertura a la organización a los ID de grupo

Debe tener los Núm.s de ID de grupo (GID) antes de iniciar esta tarea.

Pasos

1. En el sistema de clasificación de BlueXP, vaya a «/opt/netapp/config/custom_configuration» y abra el archivo `data_provider.yaml`.
2. En la línea ORGANIZATION_GROUP_ids: [], agregue los IDs de grupo. Por ejemplo:

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

   No cambie nada más en este archivo.

3. Guarde los cambios en el archivo.
4. Vaya a «/opt/netapp/Datasense/tools/customer_configuration/data_providers» y ejecute el siguiente script:

   ```
   update_data_providers_from_config_file.sh
   ```

   Este comando confirma los permisos de ID de grupo revisados en el motor de clasificación.

Resultado

Todos los escaneos posteriores de sus datos identificarán archivos o carpetas que tienen estos ID de grupo adjuntos como “abiertos a la organización”.

Puede editar la lista de ID de grupo y eliminar cualquier ID de grupo que haya agregado en el pasado mediante estos mismos pasos. La lista revisada de ID de grupo se actualizará después de ejecutar el script para confirmar los cambios.

Ver la lista actual de ID de grupo

Es posible para el contenido del `data_provider.yaml` el archivo de configuración debe ser diferente al que se ha confirmado después de ejecutar el `update_data_providers_from_config_file.sh` guión. Para ver la lista actual de ID de grupo que ha añadido a la clasificación de BlueXP, ejecute el siguiente comando en «/opt/netapp/Datasense/tools/customer_configuration/data_providers»:

```
get_data_providers_configuration.sh
```

Audita el historial de acciones de clasificación de BlueXP

Actividades de gestión de registros de clasificación de BlueXP que se han realizado en archivos de todos los entornos de trabajo y fuentes de datos que está analizando la clasificación de BlueXP. La clasificación de BlueXP también registra las actividades al

implementar la instancia de clasificación de BlueXP.

Puede ver el contenido de los archivos de registro de auditoría de clasificación de BlueXP o descargarlos, para ver qué cambios se han producido en los archivos y cuándo. Por ejemplo, puede ver qué solicitud se emitió, la hora de la solicitud y detalles como la ubicación de origen en caso de que se haya eliminado un archivo o la ubicación de origen y destino en caso de que se haya movido un archivo.

Contenido del archivo de registro

Cada línea del registro de auditoría contiene información con el siguiente formato:

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Fecha y hora: Marca de hora completa del evento
- Estado: INFORMACIÓN, AVISO
- Tipo de acción (eliminar, copiar, mover, crear política, actualizar política, Volver a analizar archivos, descargar informes JSON, etc.)
- Nombre de archivo (si la acción es relevante para un archivo)
- Detalles de la acción - lo que se hizo: Depende de la acción
  - Nombre de la política
  - Para mover: Origen y destino
  - Para copia - origen y destino
  - Para etiqueta: Nombre de etiqueta
  - Para asignar a: Nombre de usuario
  - Para alerta de correo electrónico: Dirección/cuenta de correo electrónico

Por ejemplo, las siguientes líneas del archivo de registro muestran una operación de copia correcta y una operación de copia con errores.

```
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
```

Ubicaciones de archivos de registro

Los archivos de registro de auditoría de gestión están ubicados en la máquina de clasificación de BlueXP en lo siguiente: `/opt/netapp/audit_logs/`

Los archivos de registro de auditoría de instalación se escriben en `/opt/netapp/install_logs/`

Cada archivo de registro puede tener un tamaño máximo de 10 MB. Cuando se alcanza ese límite, se inicia un nuevo archivo de registro. Los archivos de registro se denominan "DataSense_audit.log", "DataSense_audit.log.1", "DataSense_audit.log.2", etc. Un máximo de 100 archivos de registro se retienen en el sistema - los archivos de registro antiguos se eliminan automáticamente una vez alcanzado el máximo.

Acceder a los archivos de registro

Tendrás que iniciar sesión en el sistema de clasificación de BlueXP para acceder a los archivos de registro. Descubra cómo "Inicia sesión en el sistema de clasificación de BlueXP" Dependiendo de si instaló manualmente el software en una máquina Linux o si implementó la instancia en la nube.

Reducir la velocidad de exploración de clasificación de BlueXP

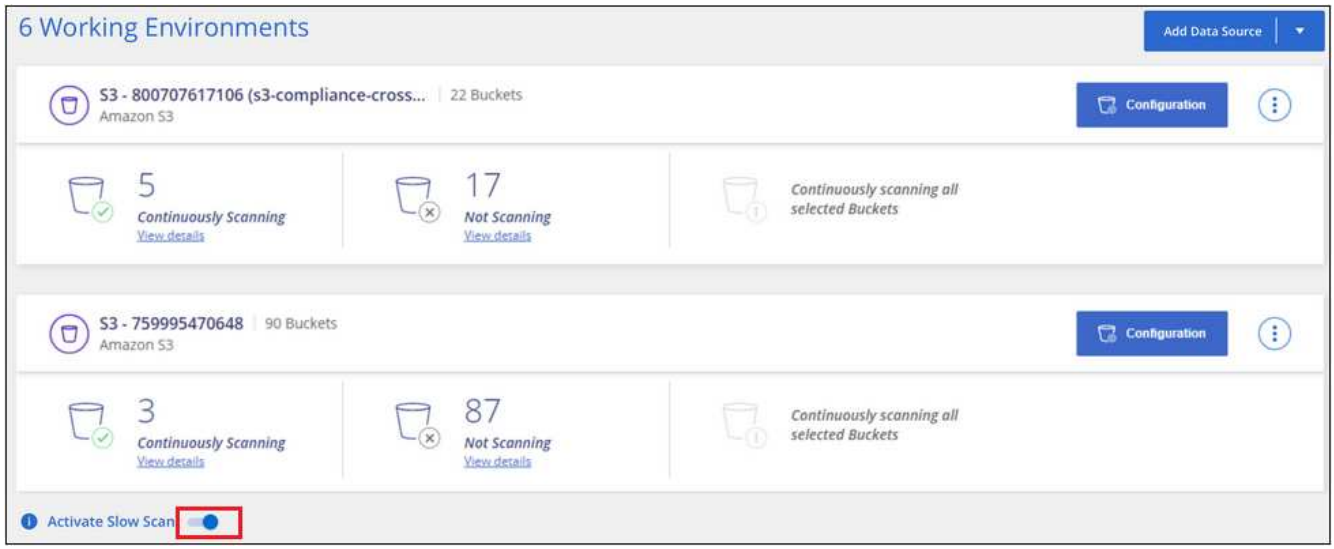
Los análisis de datos tienen un impacto insignificante en los sistemas de almacenamiento y en los datos. Sin embargo, si te preocupa incluso un impacto muy pequeño, puedes configurar la clasificación de BlueXP para realizar análisis «lentos».

Cuando está activada, el análisis lento se utiliza en todas las fuentes de datos; no puede configurar el análisis lento para un único entorno de trabajo o origen de datos.

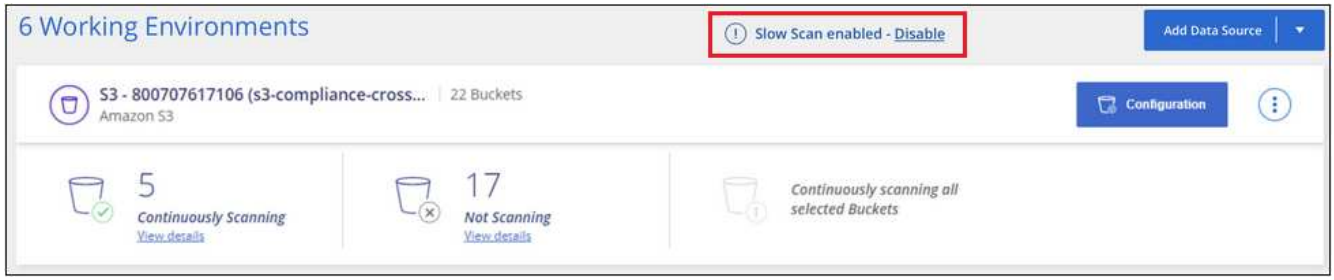
No se puede reducir la velocidad de análisis al analizar bases de datos.

Pasos

1. Desde la parte inferior de la página *Configuration*, mueva el control deslizante hacia la derecha para activar el análisis lento.



La parte superior de la página Configuración indica que se ha activado el escaneo lento.



2. Puede desactivar el escaneo lento haciendo clic en **Desactivar** en este mensaje.

Quitar fuentes de datos de la clasificación de BlueXP

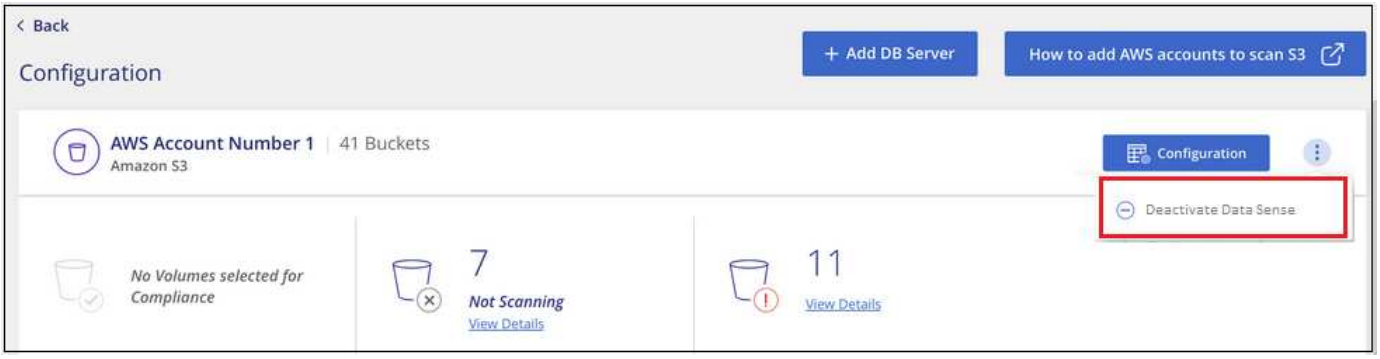
Si es necesario, puedes evitar que la clasificación de BlueXP analice uno o más entornos de trabajo, bases de datos, grupos de recursos compartidos de archivos, cuentas de OneDrive, cuentas de Google Drive, O cuentas de SharePoint.

La carga para escanear los datos se detiene cuando se elimina el origen de datos.

Desactivar los análisis de cumplimiento de normativas en un entorno de trabajo

Al desactivar los análisis, la clasificación de BlueXP ya no analiza los datos en el entorno de trabajo y elimina la información de cumplimiento indexado de la instancia de clasificación de BlueXP (los datos del entorno de trabajo en sí no se eliminan).

1. En la página *Configuration*, haga clic en ⋮ En la fila del entorno de trabajo y, a continuación, haga clic en **Desactivar detección de datos**.



También puede desactivar los análisis de cumplimiento de un entorno de trabajo desde el panel Servicios cuando seleccione el entorno de trabajo.

Eliminar una base de datos de la clasificación de BlueXP

Si ya no quieres analizar una determinada base de datos, puedes eliminarla de la interfaz de clasificación de BlueXP y detener todos los análisis.

1. En la página *Configuration*, haga clic en ⋮ En la fila de la base de datos y, a continuación, haga clic en **Quitar servidor de base de datos**.

Quitar una cuenta de OneDrive, SharePoint o Google Drive de la clasificación de BlueXP

Si ya no quieres analizar archivos de usuario de una determinada cuenta de OneDrive, desde una cuenta de SharePoint específica o desde una cuenta de Google Drive, puedes eliminar la cuenta de la interfaz de clasificación de BlueXP y detener todos los análisis.

Pasos

1. En la página *Configuration*, haga clic en ⋮ En la fila de la cuenta de OneDrive, SharePoint o Google Drive y, a continuación, haga clic en **Eliminar cuenta de OneDrive**, **Eliminar cuenta de SharePoint** o **Eliminar cuenta de Google Drive**.

2. Haga clic en **Eliminar cuenta** en el cuadro de diálogo de confirmación.

Eliminar un grupo de recursos compartidos de archivos de la clasificación de BlueXP

Si ya no desea analizar archivos de usuario de un grupo de recursos compartidos de archivos, puede eliminar el grupo File Shares de la interfaz de clasificación de BlueXP y detener todos los análisis.

Pasos

1. En la página *Configuration*, haga clic en ⋮ En la fila del grupo de recursos compartidos de archivos y, a continuación, haga clic en **Quitar grupo de recursos compartidos de archivos**.

2. Haga clic en **Eliminar grupo de recursos compartidos** en el cuadro de diálogo de confirmación.

Desinstalación de la clasificación de BlueXP

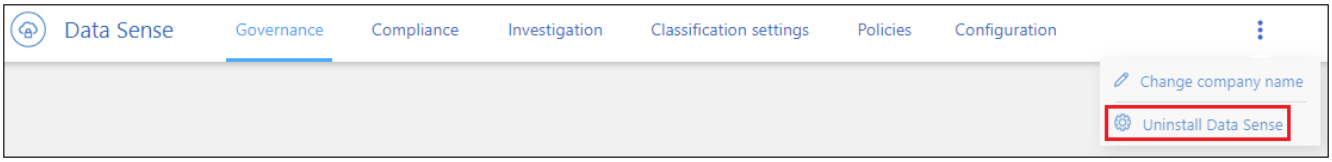
Puede desinstalar el software de clasificación de BlueXP para solucionar problemas o quitar de forma permanente el software del host. Al eliminar la instancia también se eliminan los discos asociados donde residen los datos indexados; toda la información que ha escaneado la clasificación de BlueXP se eliminará de forma permanente.

Los pasos que tienes que utilizar dependen de si has puesto en marcha la clasificación de BlueXP en la nube o en un host on-premises.

Desinstale la clasificación de BlueXP de una puesta en marcha de cloud

Puedes desinstalar y eliminar la instancia de clasificación de BlueXP del entorno de proveedor de nube si ya no quieres utilizar la clasificación de BlueXP.

1. En la parte superior de la página de clasificación de BlueXP, haga clic en Y, a continuación, haga clic en **Desinstalar detección de datos**.



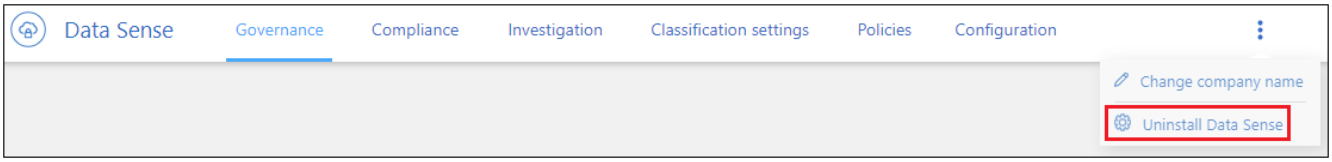
2. En el cuadro de diálogo *Uninstall Data Sense*, escriba **uninstall** para confirmar que desea desconectar la instancia de clasificación de BlueXP del conector BlueXP y, a continuación, haga clic en **Uninstall**.
3. Ve a la consola de tu proveedor de nube y elimina la instancia de clasificación de BlueXP. La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

   Esto elimina la instancia y todos los datos asociados que se recopilaron mediante la clasificación de BlueXP.

Desinstale la clasificación de BlueXP de una puesta en marcha en las instalaciones

Puede desinstalar la clasificación de BlueXP de un host si ya no quiere usar la clasificación de BlueXP o si tiene un problema que requiera la reinstalación.

1. En la parte superior de la página de clasificación de BlueXP, haga clic en Y, a continuación, haga clic en **Desinstalar detección de datos**.



2. En el cuadro de diálogo *Uninstall Data Sense*, escriba **uninstall** para confirmar que desea desconectar la instancia de clasificación de BlueXP del conector BlueXP y, a continuación, haga clic en **Uninstall**.

3. Para desinstalar el software del host, ejecute el `cleanup.sh` script en el equipo host, por ejemplo:

```
cleanup.sh
```

Descubra cómo "Inicia sesión en el equipo host de clasificación de BlueXP".

Referencia

Tipos de instancia de clasificación de BlueXP admitidos

El software de clasificación de BlueXP debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, los requisitos de RAM, los requisitos de software, etc. Al poner en marcha la clasificación de BlueXP en el cloud, le recomendamos que utilice un sistema con las características «grandes» para disfrutar de todas las funciones.

Puedes poner en marcha la clasificación de BlueXP en un sistema con menos CPU y menos RAM, pero existen algunas limitaciones al usar estos sistemas menos potentes. "Obtenga información sobre estas limitaciones".

En las siguientes tablas, si el sistema marcado como «predeterminado» no está disponible en la región donde instalas la clasificación de BlueXP, se implementará el siguiente sistema de la tabla.

Tipos de instancia de AWS

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, 1 TiB GP3 SSD	"m6i.8xlarge" (predeterminado)
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"m6i.4xgrande" (por defecto) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Mediano	8 CPU, 32 GB de RAM, 200 GIB de SSD	"m6i.2xgrande" (por defecto) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Pequeño	8 CPU, 16 GB de RAM, 100 GIB de SSD	"cera.2xlarge" (predeterminado) c5a.2xgrande c5.2xgrande c4.2xgrande

Tipos de instancia de Azure

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, disco de SO (2.048 GiB, rendimiento mínimo de 250 MB/s) y disco de datos (1 TiB SSD, rendimiento mínimo de 750 MB/s)	"Standard_D32_v3" (predeterminado)
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"Standard_D16s_v3" (predeterminado)

Tipos de instancia de GCP

Tamaño del sistema	Especificaciones	Tipo de instancia
Grande	16 CPU, 64 GB de RAM, 500 GIB de SSD	"n2-estándar-16" (predeterminado) n2d-standard-16 n1-standard-16

Metadatos recogidos de orígenes de datos

La clasificación de BlueXP recopila ciertos metadatos al realizar análisis de clasificación en los datos de tus orígenes de datos y entornos de trabajo. La clasificación de BlueXP puede acceder a la mayoría de los metadatos que necesitamos para clasificar los datos, pero hay algunas fuentes en las que no podemos acceder a los datos que necesitamos.

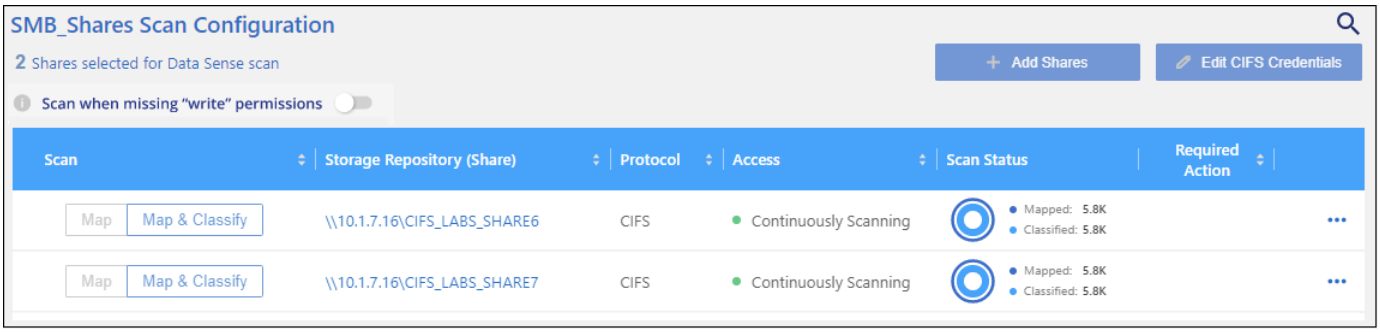
	Metadatos	CIFS	NFS
Sellos de tiempo	*Tiempo de creación*	Disponible	No disponible (no se admite en Linux)
	Hora del último acceso	Disponible	Disponible
	Hora de última modificación	Disponible	Disponible
Permisos	*Permisos abiertos*	Si el grupo "TODOS" tiene acceso al archivo, se considera "abierto a la organización"	Si "otros" tienen acceso al archivo, se considera "abierto a la organización"
	Acceso de usuarios/grupos	La información de usuarios y grupos se toma de LDAP	No disponible (los usuarios NFS suelen gestionarse localmente en el servidor; por tanto, el mismo individuo puede tener un UID diferente en cada servidor)

- La clasificación de BlueXP no extrae el «tiempo de último acceso» de los siguientes orígenes de datos: SharePoint Online, SharePoint on-premises (SharePoint Server), OneDrive, Google Drive y Amazon S3, y bases de datos.
- Las versiones anteriores del sistema operativo Windows (por ejemplo, Windows 7 y Windows 8) desactivan la recopilación del atributo de tiempo de último acceso de forma predeterminada porque puede afectar al rendimiento del sistema. Cuando no se recopila este atributo, se afectará el análisis de clasificación de BlueXP que se basa en el «tiempo de último acceso». Puede habilitar la recopilación de la última hora de acceso en estos sistemas Windows antiguos si es necesario.

Marca de hora del último acceso

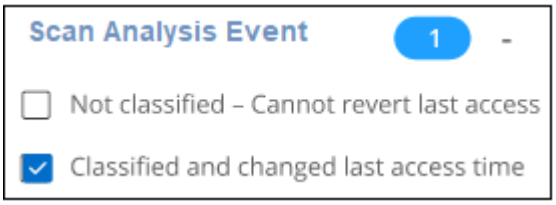
Cuando la clasificación de BlueXP extrae datos de recursos compartidos de archivos, el sistema operativo los considera accediendo a los datos y cambia la «última hora de acceso» conforme a ello. Tras el análisis, la clasificación de BlueXP intenta revertir la hora del último acceso a la marca de tiempo original. Si la clasificación de BlueXP no tiene permisos de atributos de escritura en CIFS, u permisos de escritura en NFS, el sistema no podrá revertir la hora del último acceso a la marca de tiempo original. Los volúmenes ONTAP configurados con SnapLock tienen permisos de solo lectura y además no pueden revertir la última hora de acceso a la marca de tiempo original.

De forma predeterminada, si la clasificación de BlueXP no tiene estos permisos, el sistema no analizará esos archivos en tus volúmenes porque la clasificación de BlueXP no puede revertir la «última hora de acceso» a la marca de tiempo original. Sin embargo, si no le importa si la última hora de acceso se restablece a la hora original en sus archivos, puede hacer clic en el interruptor **Escanear cuando faltan permisos de "atributos de escritura"** en la parte inferior de la página de configuración para que la clasificación de BlueXP escanee los volúmenes independientemente de los permisos.



Esta funcionalidad se puede aplicar a sistemas ONTAP en las instalaciones, Cloud Volumes ONTAP, Azure NetApp Files, FSX para ONTAP y recursos compartidos de archivos no de NetApp.

Tenga en cuenta que hay un filtro en la página de investigación llamado *Scan Analysis Event* que le permite mostrar los archivos que no se clasificaron porque la clasificación de BlueXP no pudo revertir la última hora a la que se accedió. O los archivos que estaban clasificados aunque la clasificación de BlueXP no pudieron revertir la última hora de acceso.



Las selecciones de filtro son:

- "No clasificado — no se puede revertir el tiempo del último acceso" - muestra los archivos que no se han clasificado debido a que faltan permisos de escritura.
- «Hora de último acceso clasificada y actualizada»: Muestra los archivos clasificados y la clasificación de BlueXP no pudo restablecer la fecha original de último acceso. Este filtro sólo es relevante para entornos en los que ha activado **Buscar cuando faltan permisos de "atributos de escritura"**.

Si es necesario, puede exportar estos resultados a un informe para poder ver qué archivos se están analizando o no debido a permisos. "Obtenga más información sobre el informe de investigación de datos".

Inicia sesión en el sistema de clasificación de BlueXP

A veces es posible que tengas que iniciar sesión en el sistema de clasificación de BlueXP para poder acceder a los archivos de registro o editar los archivos de configuración.

Cuando la clasificación de BlueXP está instalada en un equipo Linux en las instalaciones o en un equipo Linux implementado en la nube, puedes acceder al archivo de configuración y al script directamente.

Cuando se pone en marcha la clasificación de BlueXP en la nube, necesitas SSH para la instancia de

clasificación de BlueXP. Debe SSH al sistema introduciendo el usuario y la contraseña, o usando la clave SSH que ha proporcionado durante la instalación de BlueXP Connector. El comando SSH es:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = ubicación de claves de autenticación ssh
* <machine_user>.:
```

+
Para AWS: Utilice <ec2-user>
Para Azure: Utilice el usuario creado para la instancia de BlueXP
** Para GCP: Utilice el usuario creado para la instancia de BlueXP

- <datasense_ip> = dirección IP de la instancia de la máquina virtual

Tenga en cuenta que deberá modificar las reglas entrantes del grupo de seguridad para acceder al sistema en la nube. Para obtener más información, consulte:

- "Reglas del grupo de seguridad en AWS"
- "Reglas de grupos de seguridad en Azure"
- "Reglas de firewall en Google Cloud"

API de clasificación de BlueXP

Las funcionalidades de clasificación de BlueXP que están disponibles en la interfaz de usuario web también están disponibles en la API de Swagger.

Hay cuatro categorías definidas en la clasificación de BlueXP que se corresponden con las pestañas de la interfaz de usuario:

- Investigación
- Cumplimiento de normativas
- Gobernanza
- Configuración

Las API de la documentación de Swagger te permiten buscar, agregar datos, realizar un seguimiento de tus escaneos y crear acciones como copiar, mover y otras.

Descripción general

La API le permite realizar las siguientes funciones:

- Información de exportación
  - Todo lo que está disponible en la interfaz de usuario se puede exportar a través de la API (con la excepción de los informes)
  - Los datos se exportan en formato JSON (fácil de analizar y enviar a aplicaciones de 3rd partes, como Splunk).
- Cree consultas utilizando las sentencias AND y OR, incluya y excluya información y mucho más.

Por ejemplo, puede localizar archivos *sin* Información personal identificable específica (PII) (funcionalidad no disponible en la interfaz de usuario). También puede excluir campos específicos para la operación de exportación.

- Realice acciones
  - Actualice las credenciales de CIFS
  - Ver y cancelar acciones
  - Vuelva a explorar los directorios
  - Elimine, copie, etiquete y asigne usuarios a los datos
  - Clonar y copiar archivos
  - Exportar datos

La API es segura y utiliza el mismo método de autenticación que la interfaz de usuario. Puede encontrar información sobre la autenticación en: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Acceder a la referencia de API de Swagger

Para entrar en Swagger, necesitarás la dirección IP de tu instancia de clasificación de BlueXP. En el caso de una puesta en marcha de cloud, utilizará la dirección IP pública. Entonces tendrás que entrar en este punto final:

https://<classification_ip>/documentación

Ejemplo que utiliza las API

En el siguiente ejemplo se muestra una llamada API para copiar archivos.

Solicitud API

Inicialmente, necesitará obtener todos los campos y opciones relevantes para un entorno de trabajo para ver todos los filtros en la pestaña Investigación.

```
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"
```

Respuesta

```
{
  "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"
    }
  ]
}
```

Utilizaremos esa respuesta en nuestros parámetros de solicitud para filtrar los archivos deseados que queremos copiar.

Puede aplicar una acción en varios elementos. Los tipos de acción compatibles incluyen: Mover, eliminar, copiar, asignar a, FlexClone, exportar datos, volver a explorar y etiquetar.

Crearemos la acción de copia:

Solicitud API

Esta próxima API es esa API de acción y te permite crear múltiples acciones.

```
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"]}]}}"
```

Respuesta

La respuesta devolverá el objeto de acción, de modo que pueda utilizar las API GET y DELETE para obtener el estado de la acción o cancelarla.


```
{
  "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"
}
```

Conocimiento y apoyo

Regístrese para recibir soporte

Es necesario registrarse en soporte para recibir soporte técnico específico para BlueXP y sus servicios y soluciones de almacenamiento. También es necesario registrar soporte para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP.

Al registrarse para recibir soporte, no se habilita el soporte de NetApp para un servicio de archivos de proveedor de cloud. Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Información general del registro de soporte

Existen dos formas de registro para activar el derecho de asistencia:

- Registro de la suscripción al soporte de ID de cuenta de BlueXP (número de serie de 20 dígitos xxxx960xxxxx que se encuentra en la página Recursos de asistencia técnica de BlueXP).

  Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Debe registrarse cada suscripción de asistencia técnica a nivel de cuenta de BlueXP.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de cloud (estos son números de serie de 20 dígitos 909201xxxxxxxx).

  Estos números de serie se denominan comúnmente *PAYGO serial Numbers* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP.

El registro de ambos tipos de números de serie permite funcionalidades, como abrir tickets de soporte y la generación automática de casos. Para completar el registro, añade cuentas del sitio de soporte de NetApp (NSS) a BlueXP, como se describe a continuación.

Registra tu cuenta de BlueXP para recibir soporte de NetApp

Para registrarte para obtener soporte y activar el soporte, un usuario de tu cuenta de BlueXP debe asociar una cuenta en el sitio de soporte de NetApp a su inicio de sesión en BlueXP. La forma de registrarse para recibir soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta de NSS

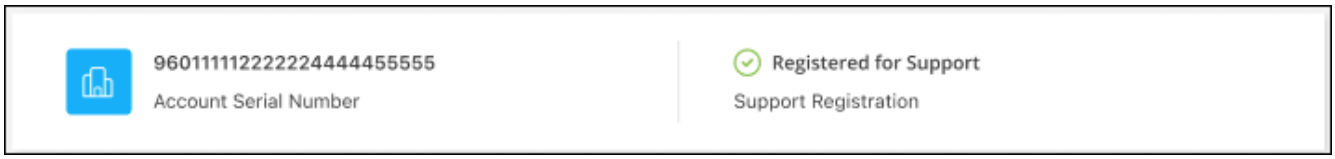
Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.

2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga el aviso de autenticación del sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro se ha realizado correctamente, seleccione el icono Ayuda y seleccione **Soporte**.

   La página **Recursos** debe mostrar que su cuenta está registrada para soporte.

   Tenga en cuenta que los otros usuarios de BlueXP no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP. Sin embargo, eso no significa que tu cuenta de BlueXP no esté registrada para el soporte técnico. Siempre y cuando un usuario de la cuenta haya seguido estos pasos, su cuenta se ha registrado.

Cliente existente pero no cuenta NSS

Si eres un cliente existente de NetApp con licencias y números de serie existentes, pero *no* NSS, deberás crear una cuenta NSS y asociarla al inicio de sesión de BlueXP.

Pasos

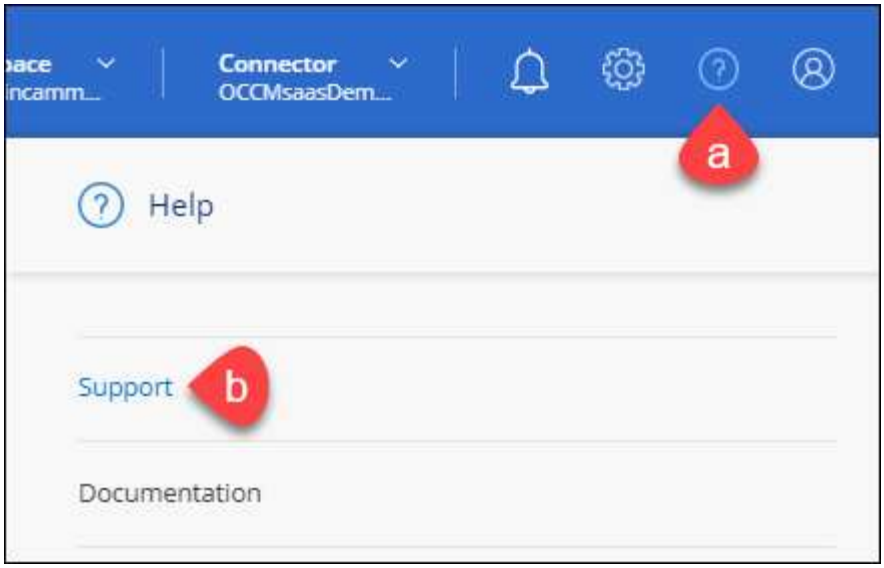
1. Complete el para crear una cuenta en la página de soporte de NetApp "Formulario de registro de usuarios del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
   b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.
2. Asocia tu nueva cuenta de NSS con tu inicio de sesión de BlueXP. Para ello, sigue los pasos que se muestran en Cliente existente con una cuenta de NSS.

Totalmente nuevo en NetApp

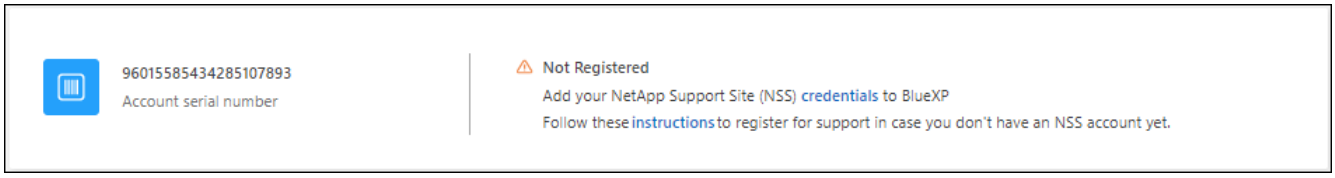
Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Busque el número de serie de su ID de cuenta en la página Support Registration.



3. Vaya a. "Sitio de registro de soporte de NetApp" Y seleccione **no soy un cliente registrado de NetApp**.
4. Rellene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **línea de productos**, seleccione **Cloud Manager** y, a continuación, seleccione el proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta desde el paso 2 anterior, complete la comprobación de seguridad y confirme que ha leído la Política de privacidad de datos global de NetApp.

   Se envía inmediatamente un correo electrónico al buzón de correo para finalizar esta transacción segura. Asegúrese de comprobar sus carpetas de spam si el correo electrónico de validación no llega en pocos minutos.

7. Confirme la acción desde el correo electrónico.

   Confirmar envía su solicitud a NetApp y recomienda que cree una cuenta en la página de soporte de NetApp.

8. Complete el para crear una cuenta en la página de soporte de NetApp "Formulario de registro de usuarios del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
   b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Después de terminar

NetApp debería ponerse en contacto con usted durante este proceso. Este es un ejercicio de incorporación puntual para nuevos usuarios.

Cuando tengas tu cuenta en el sitio de soporte de NetApp, asocia la cuenta con el inicio de sesión de BlueXP siguiendo los pasos que se muestran a continuación Cliente existente con una cuenta de NSS.

Asocie credenciales de NSS para soporte de Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de BlueXP para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para recibir soporte

  Se requiere que proporcione su cuenta de NSS para activar el soporte de su sistema y obtener acceso a los recursos de soporte técnico de NetApp.

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y activar la suscripción para el plazo que adquirió. Esto incluye actualizaciones automáticas para renovaciones de términos.

- Actualizar el software Cloud Volumes ONTAP a la versión más reciente

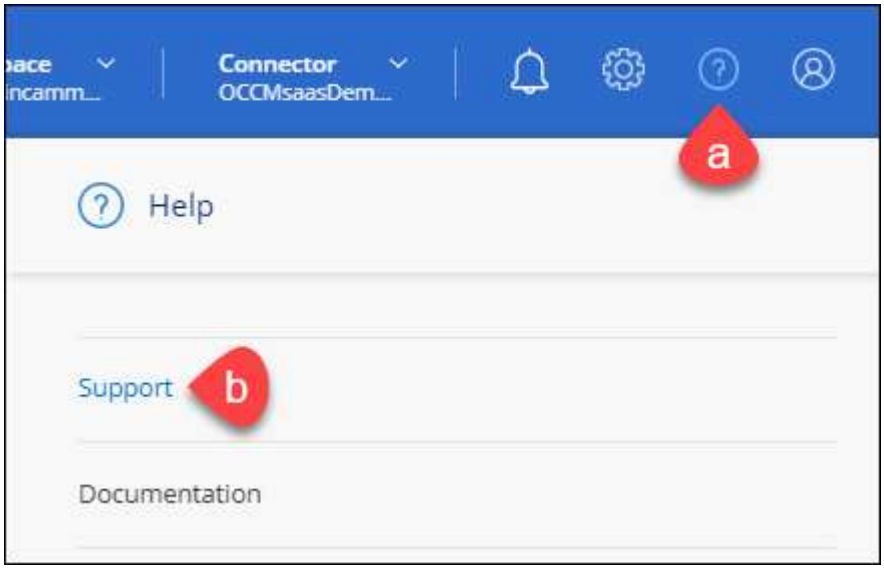
La asociación de credenciales de NSS con su cuenta de BlueXP es diferente de la cuenta de NSS asociada con un inicio de sesión de usuario de BlueXP.

Estas credenciales de NSS están asociadas con tu ID de cuenta de BlueXP específico. Los usuarios que pertenecen a la cuenta BlueXP pueden acceder a estas credenciales desde **Soporte > Gestión NSS**.

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de partner o distribuidor, puede añadir una o varias cuentas de NSS, pero no se podrán añadir junto con las cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de

Microsoft.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

   Estas acciones permiten a BlueXP utilizar su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

   Tenga en cuenta lo siguiente:

   - La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas de NSS en el nivel del cliente.
   - Sólo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de partner. Si intenta agregar cuentas de NSS de nivel de cliente y existe una cuenta de nivel de partner, obtendrá el siguiente mensaje de error:

     "El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de tipo diferente."

   Lo mismo sucede si tiene cuentas de NSS de nivel de cliente preexistentes e intenta añadir una cuenta de nivel de partner.

   - Después de iniciar sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

     Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde ••• de windows

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en la ••• de windows

     Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

Obtenga ayuda

NetApp ofrece soporte para BlueXP y sus servicios cloud de diversas maneras. Hay disponibles amplias opciones de auto soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un foro de la comunidad. Su registro de soporte incluye soporte técnico remoto a través de tickets web.

Obtenga soporte para un servicio de archivos de proveedores de cloud

Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"

- "Cloud Volumes Service para Google Cloud"

Para recibir soporte técnico específico sobre BlueXP y sus soluciones y servicios de almacenamiento, use las opciones de soporte descritas a continuación.

Utilice opciones de soporte automático

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

  La documentación de BlueXP que está viendo actualmente.

- "Base de conocimientos"

  Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para resolver problemas.

- "Comunidades"

  Únase a la comunidad de BlueXP para seguir los debates en curso o crear otros nuevos.

Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte de.

Antes de empezar

- Para utilizar la funcionalidad **Crear un caso**, primero debes asociar tus credenciales del sitio de soporte de NetApp con el inicio de sesión de BlueXP. "Descubre cómo gestionar las credenciales asociadas con tu inicio de sesión de BlueXP".
- Si abre un caso para un sistema ONTAP que tiene un número de serie, su cuenta de NSS deberá estar asociada con el número de serie de ese sistema.

Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

   a. Selecciona **Llámanos** si quieres hablar con alguien por teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.

   b. Selecciona **Crear un caso** para abrir un ticket con un especialista en Soporte NetApp:

      - **Servicio**: Seleccione el servicio con el que está asociado el problema. Por ejemplo, cuando BlueXP es específico de un problema de soporte técnico con flujos de trabajo o funcionalidades dentro del servicio.
      - **Entorno de trabajo**: Si se aplica al almacenamiento, seleccione **Cloud Volumes ONTAP** o **On-Prem** y, a continuación, el entorno de trabajo asociado.

        La lista de entornos de trabajo se encuentra dentro del ámbito de la cuenta BlueXP, el área de trabajo y el conector que ha seleccionado en el banner superior del servicio.

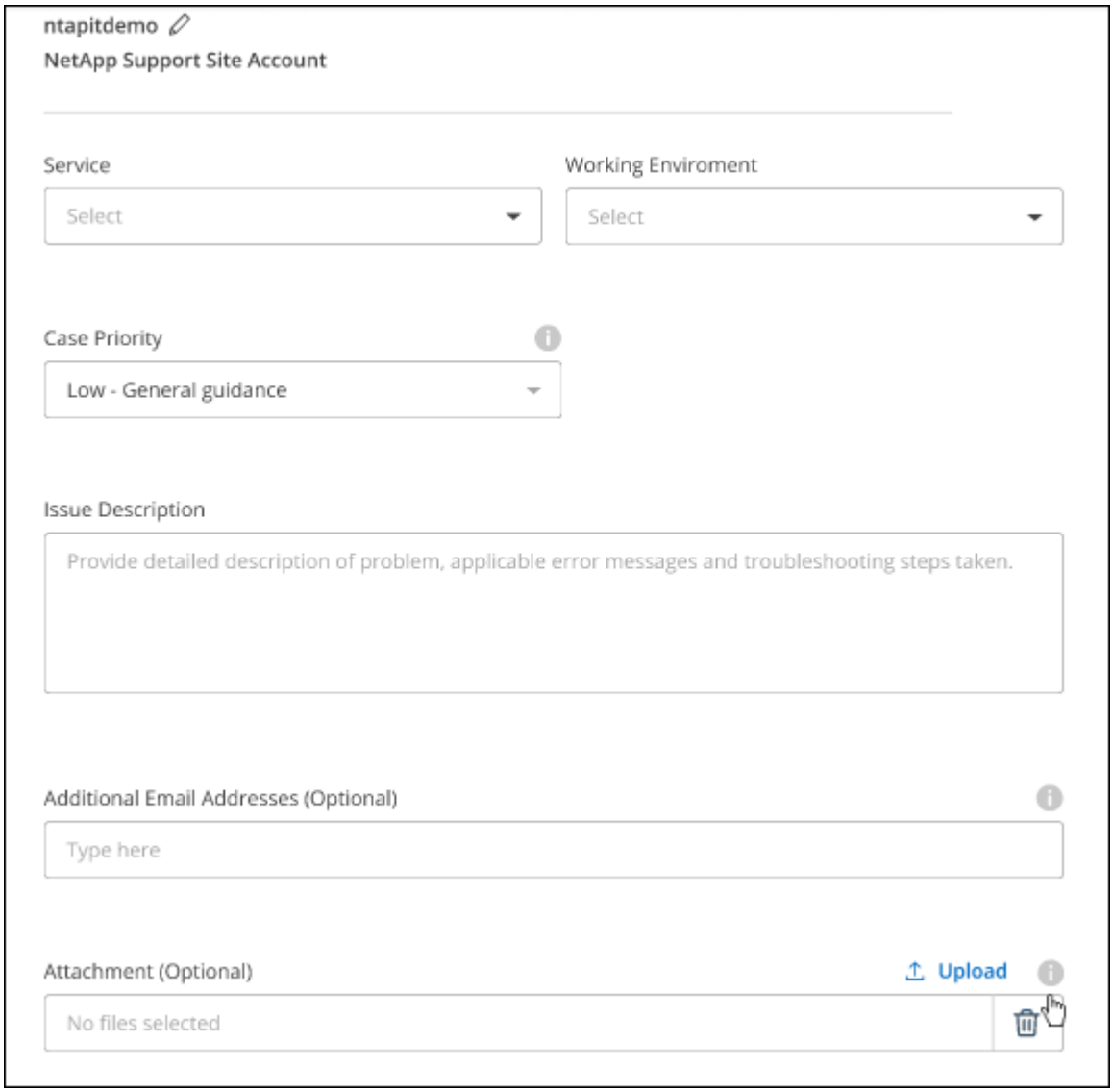
      - **Prioridad de caso**: Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

        Para obtener más información sobre estas prioridades, pase el ratón sobre el icono de información

situado junto al nombre del campo.

- **Descripción del problema**: Proporcione una descripción detallada del problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que haya realizado.
- **Direcciones de correo electrónico adicionales**: Introduzca direcciones de correo electrónico adicionales si desea que alguien más conozca este problema.
- **Accesorio (opcional)**: Cargue hasta cinco archivos adjuntos, uno a la vez.

  Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.



Después de terminar

Aparecerá una ventana emergente con el número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y le pondrá en contacto con usted próximamente.

Para obtener un historial de sus casos de soporte, puede seleccionar **Ajustes > Línea de tiempo** y buscar acciones denominadas “Crear caso de soporte”. Un botón situado en el extremo derecho le permite ampliar la acción para ver los detalles.

Es posible que se encuentre el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso en el servicio seleccionado"

Este error podría significar que la cuenta NSS y la compañía de registro con la que está asociada no es la misma compañía de registro para el número de serie de la cuenta de BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede solicitar ayuda utilizando una de las siguientes opciones:

- Usar el chat en el producto
- Envíe un caso no técnico en https://mysupport.netapp.com/site/help

Gestione sus casos de soporte (vista previa)

Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

La gestión de casos está disponible como vista previa. Tenemos pensado perfeccionar esta experiencia y añadir mejoras en próximos lanzamientos. Envíenos sus comentarios mediante el chat en el producto.

Tenga en cuenta lo siguiente:

- La consola de gestión de casos en la parte superior de la página ofrece dos vistas:
  - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que ha proporcionado.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su compañía en función de su cuenta NSS de usuario.

  Los resultados de la tabla reflejan los casos relacionados con la vista seleccionada.

- Puede agregar o quitar columnas de interés y filtrar el contenido de columnas como prioridad y estado. Otras columnas proporcionan funciones de clasificación.

  Consulte los pasos a continuación para obtener más información.

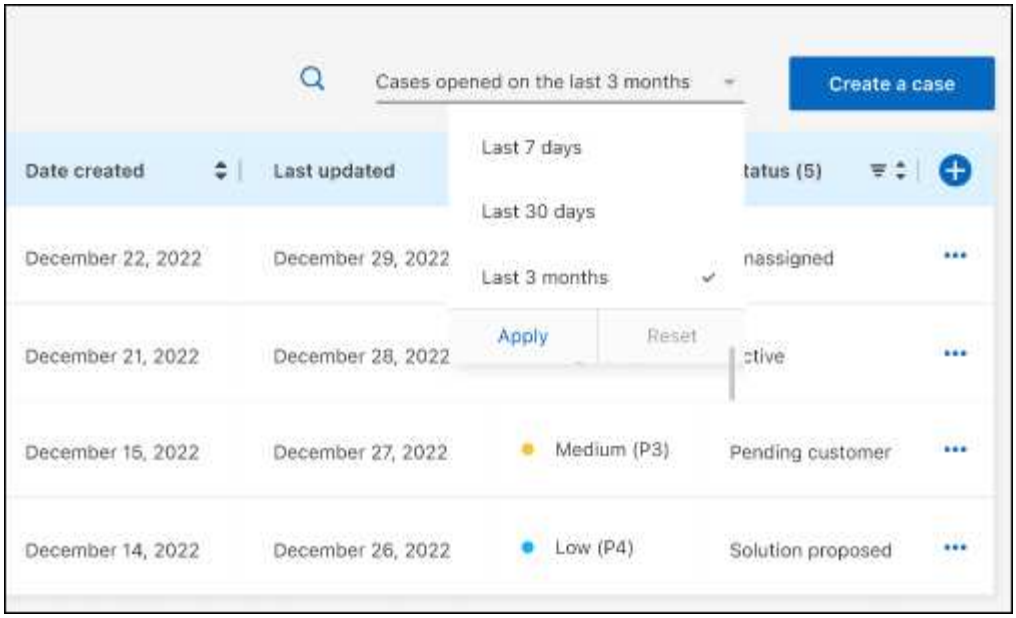
- En el nivel por caso, ofrecemos la posibilidad de actualizar las notas de un caso o cerrar un caso que no esté ya en estado cerrado o pendiente de cierre.

Pasos

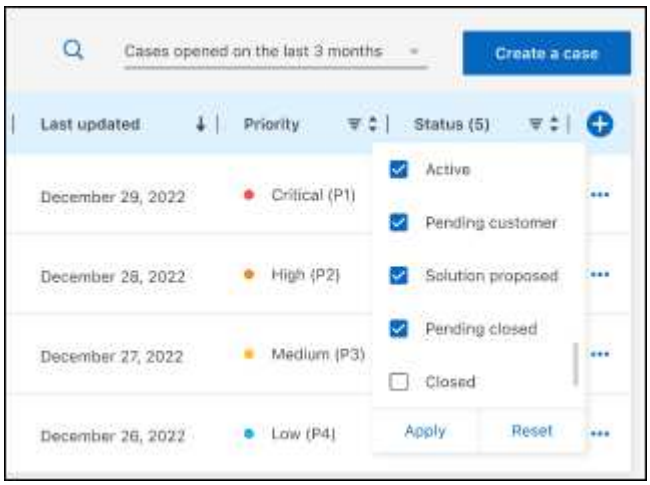
1. En BlueXP, selecciona **Ayuda > Soporte**.
2. Selecciona **Gestión de casos** y, si se te solicita, agrega tu cuenta de NSS a BlueXP.

   La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS asociada con su cuenta de usuario de BlueXP. Esta es la misma cuenta NSS que aparece en la parte superior de la página **NSS Management**.

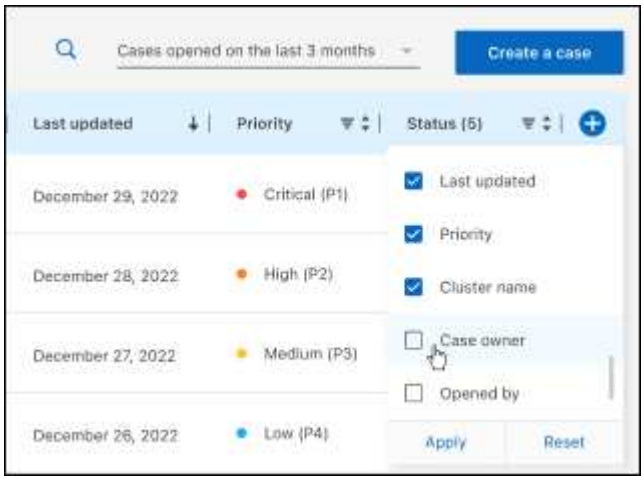
3. Si lo desea, puede modificar la información que se muestra en la tabla:
   - En **Casos de la organización**, selecciona **Ver** para ver todos los casos asociados a tu empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un marco de tiempo diferente.



- Filtre el contenido de las columnas.

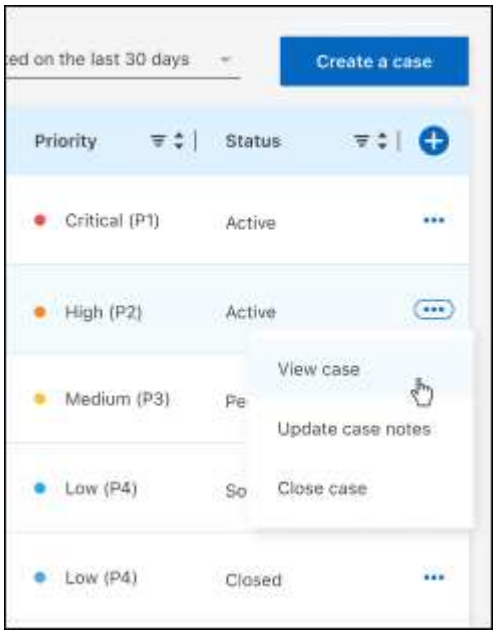


- Seleccione para cambiar las columnas que aparecen en la tabla y, a continuación, seleccione las columnas que desea mostrar.



4. Seleccione para gestionar un caso existente ••• y seleccione una de las opciones disponibles:
    - **Ver caso**: Ver todos los detalles sobre un caso específico.
    - **Actualizar notas de caso**: Proporcione detalles adicionales sobre su problema o seleccione **cargar archivos** para adjuntar hasta un máximo de cinco archivos.

      Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.
    - **Cerrar caso**: Proporciona detalles sobre por qué estás cerrando el caso y selecciona **Cerrar caso**.



Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

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

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

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

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

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

Política de privacidad

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

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- "Aviso para BlueXP"
- "Aviso para la clasificación de BlueXP"