Documentación de NetApp Data Classification

NetApp Data Classification

NetApp
February 06, 2026

Tabla de contenidos

Documentación de NetApp Data Classification

Notas de la versión

Novedades en la NetApp Data Classification

Conozca las novedades en NetApp Data Classification.

14 de enero de 2026

Versión 1.50

Esta versión de Clasificación de datos incluye correcciones de errores y las siguientes actualizaciones:

Mejoras en la clasificación personalizada

La clasificación de datos ahora admite la creación de categorías personalizadas para sus datos. Puede cargar archivos para ajustar un modelo de IA que la clasificación de datos utiliza para aplicar el marcador de categoría a los datos. Se ha mejorado la interfaz para todas las clasificaciones personalizadas.

Para obtener más información, consulte "Crear una clasificación personalizada".

Definición personalizada de datos obsoletos

La clasificación de datos ahora le permite personalizar la definición de datos obsoletos para que se adapte a las necesidades de su organización. Anteriormente, los datos obsoletos se definían como cualquier dato que se hubiera modificado por última vez hacía tres años. Ahora, los datos obsoletos pueden identificarse según cuándo se accedió a ellos por última vez o cuándo se modificaron por última vez; el período de tiempo puede variar desde hace 6 meses hasta hace 10 años.

Para obtener más información, consulte "Personalizar la definición de datos obsoletos".

Mejor rendimiento

Se han acortado los tiempos de carga de todas las páginas de Clasificación de datos, el informe de mapeo de datos y los filtros en la página de Investigación.

Tiempo estimado para los informes de investigación

Cuando descarga un informe de investigación, la Clasificación de datos ahora muestra el tiempo estimado para completar la descarga.

08 de diciembre de 2025

Versión 1.49

Esta versión de Clasificación de datos incluye correcciones de errores y las siguientes actualizaciones:

Supervise las métricas y el rendimiento en el panel de control de salud

La clasificación de datos ahora proporciona un panel de control de monitoreo de estado, que permite monitorear en tiempo real sus recursos e información sobre el uso de memoria, uso de disco, utilización de disco y más. Con la información del panel de monitoreo de estado, puede revisar la infraestructura de su implementación y obtener información para optimizar el almacenamiento y el rendimiento.

Para obtener más información, consulte "Monitorear la salud de la clasificación de datos".

Rendimiento de carga mejorado

Se ha mejorado el rendimiento de carga de todas las páginas en Clasificación de datos para crear una experiencia de usuario más eficiente.

10 de noviembre de 2025

Versión 1.48

Esta versión de Data Classification incluye correcciones de errores, mejoras de seguridad y mejoras de rendimiento.

Mayor claridad en el progreso del escaneo

Las configuraciones de escaneo ahora incluyen información mejorada sobre la finalización del escaneo. Anteriormente, la barra de progreso solo se mostraba mientras el escaneo estaba en curso. Ahora, la barra de progreso permanece visible después de la finalización para confirmar que los escaneos se completaron correctamente. También puedes ver el número de archivos mapeados y escaneados.

Para obtener más información sobre la configuración de escaneo, consulte "Cambie la configuración del análisis de NetApp Data Classification para sus repositorios".

6 de octubre de 2025

Versión 1.47

La BlueXP classification ahora es NetApp Data Classification

La BlueXP classification ha pasado a llamarse NetApp Data Classification. Además del cambio de nombre, se ha mejorado la interfaz de usuario.

BlueXP ahora es NetApp Console

BlueXP ha sido renombrado y rediseñado para reflejar mejor su función en la gestión de su infraestructura de datos.

La NetApp Console proporciona una gestión centralizada de servicios de almacenamiento y datos en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada.

Para obtener más detalles sobre lo que ha cambiado, consulte la "Notas de la versión de la NetApp Console" .

Experiencia de investigación mejorada

Encuentre y comprenda sus datos más rápido con nuevos filtros de búsqueda, recuentos de resultados por valor, información en tiempo real que resume los hallazgos clave y una tabla de resultados actualizada con columnas personalizables y un panel de detalles deslizable.

Para obtener más información, consulte "Investigar datos" .

Nuevos paneles de gobernanza y cumplimiento

Obtenga información importante más rápido con widgets intuitivos, imágenes más claras y un rendimiento de carga mejorado. Para obtener más información, consulte"Revise la información de gobernanza sobre sus datos" y"Ver información de cumplimiento sobre sus datos" .

Políticas para consultas guardadas (vista previa)

La clasificación de datos ahora le permite automatizar la gobernanza con acciones condicionales. Puede crear reglas de retención con eliminación automática y configurar notificaciones periódicas por correo electrónico, todo ello administrado desde una página de consultas guardadas actualizada.

Para obtener más información, consulte "Crear políticas" .

Acciones (vista previa)

Tome el control directo desde la página de Investigación: elimine, mueva, copie o etiquete archivos individualmente o en masa, para una gestión y remediación de datos eficiente.

Para obtener más información, consulte "Investigar datos" .

Compatibilidad con Google Cloud NetApp Volumes

La clasificación de datos ahora admite el escaneo en Google Cloud NetApp Volumes. Agregue fácilmente Google Cloud NetApp Volumes desde la NetApp Console para lograr una clasificación y un escaneo de datos sin inconvenientes. Para obtener más información, consulte "Escanear Google Cloud NetApp Volumes".

11 de agosto de 2025

Versión 1.46

Esta versión de clasificación de datos incluye correcciones de errores y las siguientes actualizaciones:

Información mejorada sobre eventos de escaneo en la página de auditoría

La página Auditoría ahora admite información mejorada sobre los eventos de escaneo para la BlueXP classification. La página Auditoría ahora muestra cuándo comienza el análisis de un sistema, los estados de los sistemas y cualquier problema. Los estados de los recursos compartidos y de los sistemas solo están disponibles para los escaneos de mapeo.

Para obtener más información sobre la página de Auditoría, consulte"Supervisar las operaciones de la NetApp Console" .

Compatibilidad con RHEL 9.6

Esta versión agrega soporte para Red Hat Enterprise Linux v9.6 para la instalación manual local de la BlueXP classification, incluidas las implementaciones de sitios oscuros.

Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión de BlueXP classification 1.30 o superior: Red Hat Enterprise Linux versiones 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 y 9.5.

14 de julio de 2025

Versión 1.45

Esta versión de BlueXP classification incluye cambios de código que optimizan la utilización de recursos y:

Flujo de trabajo mejorado para agregar recursos compartidos de archivos para escanear

Se ha simplificado el flujo de trabajo para agregar recursos compartidos de archivos a un grupo de recursos compartidos de archivos. El proceso ahora también diferencia la compatibilidad del protocolo CIFS según el tipo de autenticación (Kerberos o NTLM).

Para obtener más información, consulte "Escanear recursos compartidos de archivos" .

Información mejorada del propietario del archivo

Ahora puede ver más información sobre los propietarios de los archivos capturados en la pestaña Investigación. Al visualizar los metadatos de un archivo en la pestaña Investigación, ubique al propietario del archivo y luego seleccione **Ver detalles** para ver el nombre de usuario, el correo electrónico y el nombre de la

cuenta SAM. También puedes ver otros artículos que pertenecen a este usuario. Esta función solo está disponible para entornos de trabajo con Active Directory.

Para obtener más información, consulte "Investigue los datos almacenados en su organización" .

10 de junio de 2025

Versión 1.44

Esta versión de BlueXP classification incluye:

Tiempos de actualización mejorados para el panel de gobernanza

Se han mejorado los tiempos de actualización de los componentes individuales del panel de Gobernanza. La siguiente tabla muestra la frecuencia de actualizaciones de cada componente.

Componente	Horarios de actualización
La era de los datos	24 horas
Categorías	24 horas
Descripción general de los datos	5 minutos
Archivos duplicados	2 horas
Tipos de archivos	24 horas
Datos no comerciales	2 horas
Permisos abiertos	24 horas
Búsquedas guardadas	2 horas
Datos confidenciales y amplios permisos	24 horas
Tamaño de los datos	24 horas
Datos obsoletos	2 horas
Principales repositorios de datos por nivel de sensibilidad	2 horas

Puede ver la hora de la última actualización y actualizar manualmente los componentes Archivos duplicados, Datos no comerciales, Búsquedas guardadas, Datos obsoletos y Repositorios de datos principales por nivel de sensibilidad. Para obtener más información sobre el panel de gobernanza, consulte"Ver detalles de gobernanza sobre los datos almacenados en su organización" .

Mejoras de rendimiento y seguridad

Se han realizado mejoras para mejorar el rendimiento, el consumo de memoria y la seguridad de la clasificación BlueXP .

Corrección de errores

Redis se ha actualizado para mejorar la confiabilidad de la BlueXP classification. La BlueXP classification ahora utiliza Elasticsearch para mejorar la precisión de los informes de recuento de archivos durante los escaneos.

12 de mayo de 2025

Versión 1.43

Esta versión de clasificación de BlueXP incluye:

Priorizar los escaneos de clasificación

La clasificación de datos permite priorizar los escaneos de Mapa y clasificación además de los escaneos de solo mapeo, lo que le permite seleccionar qué escaneos se completan primero. Se admite la priorización de los escaneos de Mapa y Clasificación durante y antes de que comiencen los escaneos. Si decide priorizar un escaneo mientras está en progreso, se priorizarán tanto los escaneos de mapeo como los de clasificación.

Para obtener más información, consulte "Priorizar los escaneos" .

Compatibilidad con categorías de datos de información de identificación personal (PII) canadienses

Los escaneos de clasificación de datos identifican categorías de datos PII canadienses. Estas categorías incluyen información bancaria, números de pasaporte, números de seguro social, números de licencia de conducir y números de tarjetas de salud de todas las provincias y territorios canadienses.

Para obtener más información, consulte "Categorías de datos personales" .

Clasificación personalizada (vista previa)

La clasificación de datos admite clasificaciones personalizadas para escaneos de Mapa y Clasificación. Con clasificaciones personalizadas, puede adaptar los escaneos de clasificación de datos para capturar datos específicos de su organización utilizando expresiones regulares. Esta función se encuentra actualmente en versión preliminar.

Para obtener más información, consulte "Agregar clasificaciones personalizadas" .

Pestaña de búsquedas guardadas

La pestaña **Políticas** ha cambiado de nombre**"Búsquedas guardadas"** . La funcionalidad no cambia.

Enviar eventos de escaneo a la página de Auditoría

La clasificación de datos permite enviar eventos de clasificación (cuando se inicia un escaneo y cuando finaliza) a"Página de auditoría de NetApp Consle" .

Actualizaciones de seguridad

- Se ha actualizado el paquete Keras, mitigando vulnerabilidades (BDSA-2025-0107 y BDSA-2025-1984).
- Se ha actualizado la configuración de los contenedores Docker. El contenedor ya no tiene acceso a las interfaces de red del host para crear paquetes de red sin procesar. Al reducir el acceso innecesario, la actualización mitiga los posibles riesgos de seguridad.

Mejoras de rendimiento

Se han implementado mejoras de código para reducir el uso de RAM y mejorar el rendimiento general de la clasificación de datos.

Corrección de errores

Se han corregido errores que causaban que los escaneos de StorageGRID fallaran, que las opciones de filtro de la página de investigación no se cargaran y que la Evaluación de descubrimiento de datos no se descargara para evaluaciones de gran volumen.

14 de abril de 2025

Versión 1.42

Esta versión de BlueXP classification incluye:

Escaneo masivo para entornos de trabajo

La BlueXP classification admite operaciones masivas para entornos de trabajo. Puede elegir habilitar escaneos de mapeo, habilitar escaneos de mapeo y clasificación, deshabilitar escaneos o crear una configuración personalizada en todos los volúmenes en el entorno de trabajo. Si realiza una selección para un volumen individual, anulará la selección masiva. Para realizar una operación masiva, navegue a la página **Configuración** y haga su selección.

Descargar informe de investigación localmente

La BlueXP classification admite la posibilidad de descargar informes de investigación de datos localmente para verlos en el navegador. Si elige la opción local, la investigación de datos solo estará disponible en formato CSV y solo mostrará las primeras 10 000 filas de datos.

Para obtener más información, consulte "Investigue los datos almacenados en su organización con la BlueXP classification" .

10 de marzo de 2025

Versión 1.41

Esta versión de BlueXP classification incluye mejoras generales y correcciones de errores. También incluye:

Estado del escaneo

La BlueXP classification rastrea el progreso en tiempo real de los escaneos de clasificación y mapeo *iniciales* en un volumen. Barras progresivas separadas rastrean los escaneos de mapeo y clasificación, presentando un porcentaje del total de archivos escaneados. También puede pasar el cursor sobre una barra de progreso para ver la cantidad de archivos escaneados y el total de archivos. El seguimiento del estado de sus escaneos genera información más profunda sobre el progreso del escaneo, lo que le permite planificar mejor sus escaneos y comprender la asignación de recursos.

Para ver el estado de sus escaneos, navegue a **Configuración** en la BlueXP classification y luego seleccione **Configuración del entorno de trabajo**. El progreso se muestra en línea para cada volumen.

19 de febrero de 2025

Versión 1.40

Esta versión de BlueXP classification incluye las siguientes actualizaciones.

Compatibilidad con RHEL 9.5

Esta versión proporciona soporte para Red Hat Enterprise Linux v9.5 además de las versiones compatibles anteriormente. Esto se aplica a cualquier instalación local manual de la BlueXP classification, incluidas las implementaciones de sitios oscuros.

Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión de BlueXP classification 1.30 o superior: Red Hat Enterprise Linux versiones 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 y 9.5.

Priorizar los escaneos de solo mapeo

Al realizar escaneos de solo mapeo, puede priorizar los escaneos más importantes. Esta función es útil cuando tienes muchos entornos de trabajo y quieres garantizar que los escaneos de alta prioridad se completen primero.

De forma predeterminada, los escaneos se ponen en cola según el orden en el que se inician. Con la capacidad de priorizar los escaneos, puede moverlos al frente de la cola. Se pueden priorizar múltiples escaneos. La prioridad se designa en un orden de primero en entrar, primero en salir, lo que significa que el primer escaneo que prioriza pasa al frente de la cola; el segundo escaneo que prioriza pasa al segundo en la cola, y así sucesivamente.

La prioridad se concede por única vez. Los escaneos automáticos de datos cartográficos se realizan en el orden predeterminado.

La priorización se limita a"escaneos de solo mapeo" ; no está disponible para escaneos de mapas y clasificación.

Para obtener más información, consulte "Priorizar los escaneos" .

Reintentar todos los escaneos

La BlueXP classification admite la capacidad de reintentar por lotes todos los escaneos fallidos.

Puede volver a intentar los escaneos en una operación por lotes con la función **Reintentar todo**. Si los escaneos de clasificación fallan debido a un problema temporal, como una interrupción de la red, puede volver a intentar todos los escaneos al mismo tiempo con un botón en lugar de volver a intentarlos individualmente. Los escaneos se pueden volver a intentar tantas veces como sea necesario.

Para volver a intentar todos los escaneos:

1. Desde el menú de BlueXP classification , seleccione **Configuración**.
2. Para volver a intentar todos los escaneos fallidos, seleccione **Reintentar todos los escaneos**.

Precisión mejorada del modelo de categorización

La precisión del modelo de aprendizaje automático para"categorías predefinidas" Ha mejorado un 11%.

22 de enero de 2025

Versión 1.39

Esta versión de BlueXP classification actualiza el proceso de exportación del informe de investigación de datos. Esta actualización de exportación es útil para realizar análisis adicionales en sus datos, crear visualizaciones adicionales en los datos o compartir los resultados de su investigación de datos con otros.

Anteriormente, la exportación del informe de investigación de datos estaba limitada a 10 000 filas. Con esta versión, se ha eliminado el límite para que puedas exportar todos tus datos. Este cambio le permite exportar más datos de sus informes de investigación de datos, lo que le proporciona más flexibilidad en su análisis de datos.

Puede elegir el entorno de trabajo, los volúmenes, la carpeta de destino y el formato JSON o CSV. El nombre del archivo exportado incluye una marca de tiempo para ayudarle a identificar cuándo se exportaron los datos.

Los entornos de trabajo compatibles incluyen:

- Cloud Volumes ONTAP

- FSx para ONTAP
- ONTAP
- Grupo compartido

La exportación de datos del informe de investigación de datos tiene las siguientes limitaciones:

- El número máximo de registros a descargar es 500 millones por tipo (archivos, directorios y tablas).
- Se espera que exportar un millón de registros tome aproximadamente 35 minutos.

Para obtener más detalles sobre la investigación de datos y el informe, consulte "Investigar los datos almacenados en su organización" .

16 de diciembre de 2024

Versión 1.38

Esta versión de BlueXP classification incluye mejoras generales y correcciones de errores.

4 de noviembre de 2024

Versión 1.37

Esta versión de BlueXP classification incluye las siguientes actualizaciones.

Compatibilidad con RHEL 8.10

Esta versión proporciona soporte para Red Hat Enterprise Linux v8.10 además de las versiones compatibles anteriormente. Esto se aplica a cualquier instalación local manual de la BlueXP classification, incluidas las implementaciones de sitios oscuros.

Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión de BlueXP classification 1.30 o superior: Red Hat Enterprise Linux versiones 8.8, 8.10, 9.0, 9.1, 9.2, 9.3 y 9.4.

Obtenga más información sobre "BlueXP classification" .

Compatibilidad con NFS v4.1

Esta versión proporciona soporte para NFS v4.1 además de las versiones compatibles anteriormente.

Obtenga más información sobre "BlueXP classification" .

10 de octubre de 2024

Versión 1.36

Compatibilidad con RHEL 9.4

Esta versión proporciona soporte para Red Hat Enterprise Linux v9.4 además de las versiones compatibles anteriormente. Esto se aplica a cualquier instalación local manual de la BlueXP classification, incluidas las implementaciones de sitios oscuros.

Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión de BlueXP classification 1.30 o superior: Red Hat Enterprise Linux versiones 8.8, 9.0, 9.1, 9.2, 9.3 y 9.4.

Obtenga más información sobre "Descripción general de las implementaciones de BlueXP classification" .

Rendimiento de escaneo mejorado

Esta versión proporciona un rendimiento de escaneo mejorado.

2 de septiembre de 2024

Versión 1.35

Escanear datos de StorageGRID

La BlueXP classification admite el escaneo de datos en StorageGRID.

Para más detalles, consulte"Escanear datos de StorageGRID" .

5 de agosto de 2024

Versión 1.34

Esta versión de BlueXP classification incluye la siguiente actualización.

Cambiar de CentOS a Ubuntu

La BlueXP classification ha actualizado su sistema operativo Linux para Microsoft Azure y Google Cloud Platform (GCP) de CentOS 7.9 a Ubuntu 22.04.

Para obtener detalles sobre la implementación, consulte "Instalar en un host Linux con acceso a Internet y preparar el sistema host Linux" .

1 de julio de 2024

Versión 1.33

Compatible con Ubuntu

Esta versión es compatible con la plataforma Linux Ubuntu 24.04.

Los escaneos de mapeo recopilan metadatos

Los siguientes metadatos se extraen de los archivos durante los escaneos de mapeo y se muestran en los paneles de Gobernanza, Cumplimiento e Investigación:

- Entorno de trabajo
- Tipo de entorno de trabajo
- Repositorio de almacenamiento
- Tipo de archivo
- Capacidad utilizada
- Número de archivos
- Tamaño del archivo
- Creación de archivos
- Último acceso al archivo
- Archivo modificado por última vez
- Hora de descubrimiento del archivo

- Extracción de permisos

Datos adicionales en los paneles de control

Esta versión actualiza los datos que aparecen en los paneles de Gobernanza, Cumplimiento e Investigación durante los análisis de mapeo.

Para obtener más información, consulte "¿Cuál es la diferencia entre los escaneos de mapeo y de clasificación?" .

5 de junio de 2024

Versión 1.32

Nueva columna de estado de mapeo en la página de Configuración

Esta versión ahora muestra una nueva columna de estado de mapeo en la página de Configuración. La nueva columna le ayuda a identificar si el mapeo está en ejecución, en cola, en pausa o más.

Para obtener explicaciones sobre los estados, consulte "Cambiar la configuración de escaneo" .

15 de mayo de 2024

Versión 1.31

La clasificación está disponible como un servicio principal dentro de BlueXP

La BlueXP classification ahora está disponible como una capacidad principal dentro de BlueXP sin costo adicional para hasta 500 TiB de datos escaneados por conector. No se requiere licencia de clasificación ni suscripción paga. Como centramos la funcionalidad de BlueXP classification en el escaneo de sistemas de almacenamiento NetApp con esta nueva versión, algunas funciones heredadas solo estarán disponibles para los clientes que previamente hayan pagado una licencia. El uso de esas funciones heredadas expirará cuando el contrato pago llegue a su fecha de finalización.

La clasificación de datos no impone un límite en la cantidad de datos que puede escanear. Cada agente de consola admite el escaneo y la visualización de 500 TiB de datos. Para escanear más de 500 TiB de datos,"instalar otro agente de consola" entonces"Implementar otra instancia de clasificación de datos" . + La interfaz de usuario de la consola muestra datos de un solo conector. Para obtener sugerencias sobre cómo ver datos de varios agentes de la consola, consulte"Trabajar con múltiples agentes de consola" .

1 de abril de 2024

Versión 1.30

Se agregó soporte para la BlueXP classification de RHEL v8.8 y v9.3

Esta versión proporciona soporte para Red Hat Enterprise Linux v8.8 y v9.3 además de la versión 9.x previamente compatible, que requiere Podman, en lugar del motor Docker. Esto se aplica a cualquier instalación manual local de la BlueXP classification.

Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión de BlueXP classification 1.30 o superior: Red Hat Enterprise Linux versiones 8.8, 9.0, 9.1, 9.2 y 9.3.

Obtenga más información sobre "Descripción general de las implementaciones de BlueXP classification" .

La BlueXP classification es compatible si instala el conector en un host RHEL 8 o 9 que reside localmente. No es compatible si el host RHEL 8 o 9 reside en AWS, Azure o Google Cloud.

Se eliminó la opción para activar la recopilación de registros de auditoría

Se ha deshabilitado la opción para activar la recopilación de registros de auditoría.

Se mejoró la velocidad de escaneo

Se ha mejorado el rendimiento del escaneo en los nodos del escáner secundario. Puede agregar más nodos de escáner si necesita potencia de procesamiento adicional para sus escaneos. Para más detalles, consulte "Instalar la BlueXP classification en un host que tenga acceso a Internet" .

Actualizaciones automáticas

Si implementó la BlueXP classification en un sistema con acceso a Internet, el sistema se actualiza automáticamente. Anteriormente, la actualización se producía después de transcurrido un tiempo específico desde la última actividad del usuario. Con esta versión, la BlueXP classification se actualiza automáticamente si la hora local está entre la 1:00 a. m. y las 5:00 a. m. Si la hora local está fuera de este horario, la actualización se produce después de que transcurra un tiempo específico desde la última actividad del usuario. Para más detalles, consulte "Instalar en un host Linux con acceso a Internet" .

Si implementó la BlueXP classification sin acceso a Internet, deberá actualizarla manualmente. Para más detalles, consulte "Instalar la BlueXP classification en un host Linux sin acceso a Internet" .

4 de marzo de 2024

Versión 1.29

Ahora puede excluir el escaneo de datos que residen en determinados directorios de fuentes de datos

Si desea que la BlueXP classification excluya los datos de escaneo que residen en determinados directorios de fuentes de datos, puede agregar estos nombres de directorio a un archivo de configuración que procesa la BlueXP classification . Esta función le permite evitar escanear directorios que no son necesarios o que podrían arrojar resultados de datos personales falsos positivos.

"Más información" .

La compatibilidad con instancias extra grandes ahora está calificada

Si necesita la BlueXP classification para escanear más de 250 millones de archivos, puede utilizar una instancia Extra Grande en su implementación en la nube o instalación local. Este tipo de sistema puede escanear hasta 500 millones de archivos.

"Más información" .

10 de enero de 2024

Versión 1.27

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

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

Configurar ID de grupo adicionales como "Abierto a la organización"

Ahora puede configurar los ID de grupo en NFS para que se consideren como "Abierto a la organización" directamente desde la BlueXP classification si el grupo no se había configurado inicialmente con ese permiso.

Cualquier archivo o carpeta que tenga estos ID de grupo adjuntos se mostrará como "Abierto a la organización" en la página Detalles de la investigación. Vea cómo"Agregar ID de grupo adicionales como "abierto a la organización"" .

14 de diciembre de 2023

Versión 1.26.6

Esta versión incluye algunas mejoras menores.

El lanzamiento también eliminó las siguientes opciones:

- Se ha deshabilitado la opción para activar la recopilación de registros de auditoría.
- Durante la investigación de Directorios, la opción para calcular la cantidad de datos de información personal identificable (PII) por Directorios no está disponible. Consulte "Investigue los datos almacenados en su organización" .
- Se ha deshabilitado la opción para integrar datos mediante etiquetas de Azure Information Protection (AIP).

6 de noviembre de 2023

Versión 1.26.3

Los siguientes problemas se han solucionado en esta versión

- Se corrigió una inconsistencia al presentar la cantidad de archivos escaneados por el sistema en los paneles de control.
- Se mejoró el comportamiento del 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 instalaciones locales de la BlueXP classification en RHEL versión 9

Las versiones 8 y 9 de Red Hat Enterprise Linux no admiten el motor Docker, que era necesario para la instalación de la BlueXP classification . Ahora admitimos la instalación de la BlueXP classification en RHEL 9.0, 9.1 y 9.2 utilizando Podman versión 4 o superior como infraestructura de contenedor. Si su entorno requiere el uso de las versiones más nuevas de RHEL, ahora puede instalar la BlueXP classification (versión 1.26 o superior) al usar Podman.

En este momento no admitimos instalaciones de sitios oscuros ni entornos de escaneo distribuido (que utilizan un escáner maestro y remoto) cuando se utiliza RHEL 9.x.

5 de septiembre de 2023

Versión 1.25

Implementaciones pequeñas y medianas temporalmente no disponibles

Cuando implementa una instancia de BlueXP classification en AWS, la opción para seleccionar **Implementar > Configuración** y elegir una instancia de tamaño pequeño o mediano no está disponible en este momento. Aún puedes implementar la instancia utilizando el tamaño de instancia grande seleccionando **Implementar >**

Implementar.

Aplique etiquetas en hasta 100.000 elementos desde la página de Resultados de la investigación

En el pasado, solo se podían aplicar etiquetas a una sola página a la vez en la página Resultados de la investigación (20 elementos). Ahora puede seleccionar **todos** los elementos en las páginas de Resultados de la investigación y aplicar etiquetas a todos los elementos (hasta 100 000 elementos a la vez).

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

La BlueXP classification se utiliza para identificar archivos duplicados solo cuando los archivos tienen 50 MB o más. Ahora se pueden identificar archivos duplicados que comiencen con 1 MB. Puede utilizar los filtros de la página de Investigación "Tamaño de archivo" junto con "Duplicados" para ver qué archivos de un tamaño determinado están duplicados en su entorno.

17 de julio de 2023

Versión 1.24

La BlueXP classification identifica dos nuevos tipos de datos personales alemanes

La BlueXP classification puede identificar y categorizar archivos que contienen los siguientes tipos de datos:

- Identificación alemana (Personalausweisnummer)
- Número de seguridad social alemán (Sozialversicherungsnummer)

"Vea todos los tipos de datos personales que la BlueXP classification puede identificar en sus datos" .

La BlueXP classification es totalmente compatible en modo restringido y modo privado

La BlueXP classification ahora es totalmente compatible en sitios sin acceso a Internet (modo privado) y con acceso a Internet saliente limitado (modo restringido). "Obtenga más información sobre los modos de implementación de BlueXP para el conector" .

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

Ahora puedes actualizar a una versión más nueva de la BlueXP classification incluso si no es secuencial. Esto significa que la limitación actual de actualizar la BlueXP classification de una versión a la vez ya no es necesaria. Esta característica es relevante a partir de la versión 1.24.

La API de BlueXP classification ya está disponible

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

"Obtenga más información sobre las API de BlueXP classification" .

6 de junio de 2023

Versión 1.23

Ahora se admite el japonés al buscar nombres de interesados

Ahora se pueden ingresar nombres japoneses al buscar el nombre de un sujeto en respuesta a una Solicitud de acceso de sujeto de datos (DSAR). Puedes generar un"Informe de solicitud de acceso del interesado" con la información resultante. También puedes introducir nombres japoneses en el"Filtro "Sujeto de datos" en la

página de Investigación de datos" para identificar archivos que contienen el nombre del sujeto.

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

Ubuntu 22.04 ha sido calificado como un sistema operativo compatible con la BlueXP classification. Puede instalar la BlueXP classification en un host Ubuntu Linux en su red, o en un host Linux en la nube cuando utilice la versión 1.23 del instalador. "Vea cómo instalar la BlueXP classification en un host con Ubuntu instalado" .

Red Hat Enterprise Linux 8.6 y 8.7 ya no son compatibles con las nuevas instalaciones de BlueXP classification

Estas versiones no son compatibles con nuevas implementaciones porque Red Hat ya no admite Docker, lo cual es un requisito previo. Si tiene una máquina de BlueXP classification existente que se ejecuta en RHEL 8.6 o 8.7, NetApp seguirá brindando soporte para su configuración.

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

Puede habilitar que se recopilen registros de auditoría de acceso a archivos en su sistema de BlueXP classification para eventos de acceso a archivos detectados en volúmenes en sus entornos de trabajo. La BlueXP classification puede capturar los siguientes tipos de eventos FPolicy y los usuarios que realizaron las acciones en sus archivos: crear, leer, escribir, eliminar, cambiar nombre, cambiar propietario/permisos y cambiar SACL/DACL.

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

Ahora puede cargar su licencia BYOL de Data Sense en la BlueXP digital wallet en un sitio oscuro para que se le notifique cuando su licencia esté baja.

03 de abril de 2023

Versión 1.22

Nuevo informe de evaluación del descubrimiento de datos

El Informe de evaluación de descubrimiento de datos proporciona un análisis de alto nivel de su entorno escaneado para resaltar los hallazgos del sistema y mostrar áreas de preocupación y posibles pasos de remediación. El objetivo de este informe es generar conciencia sobre las preocupaciones en materia de gobernanza de datos, las exposiciones de seguridad de datos y las brechas de cumplimiento de datos de su conjunto de datos. "Vea cómo generar y utilizar el Informe de evaluación de descubrimiento de datos" .

Capacidad de implementar la BlueXP classification en instancias más pequeñas en la nube

Al implementar la BlueXP classification desde un conector BlueXP en un entorno de AWS, ahora puede seleccionar entre dos tipos de instancias más pequeñas que las disponibles con la instancia predeterminada. Si está escaneando un entorno pequeño, esto puede ayudarle a ahorrar en costos de la nube. Sin embargo, existen algunas restricciones al utilizar la instancia más pequeña. "Consulte los tipos de instancias disponibles y sus limitaciones" .

Ahora está disponible un script independiente para calificar su sistema Linux antes de la instalación de la BlueXP classification

Si desea verificar que su sistema Linux cumple con todos los requisitos previos independientemente de ejecutar la instalación de BlueXP classification , hay un script separado que puede descargar que solo prueba los requisitos previos. "Vea cómo comprobar si su host Linux está listo para instalar la BlueXP classification" .

7 de marzo de 2023

Versión 1.21

Nueva funcionalidad para agregar sus propias categorías personalizadas desde la interfaz de BlueXP classification

La BlueXP classification ahora le permite agregar sus propias categorías personalizadas para que la BlueXP classification identifique los archivos que encajan en esas categorías. La BlueXP classification tiene muchas "categorías predefinidas" , por lo que esta función le permite agregar categorías personalizadas para identificar dónde se encuentra la información que es exclusiva de su organización en sus datos.

Ahora puedes agregar palabras clave personalizadas desde la interfaz de BlueXP classification

La BlueXP classification ha tenido la capacidad de agregar palabras clave personalizadas que la BlueXP classification identificará en escaneos futuros durante un tiempo. Sin embargo, era necesario iniciar sesión en el host Linux de BlueXP classification y utilizar una interfaz de línea de comandos para agregar las palabras clave. En esta versión, la capacidad de agregar palabras clave personalizadas está en la interfaz de usuario de BlueXP classification , lo que hace que sea muy fácil agregar y editar estas palabras clave.

Capacidad de que la BlueXP classification no escanee archivos cuando se cambie la "hora del último acceso"

De forma predeterminada, si la BlueXP classification no tiene permisos de "escritura" adecuados, el sistema no escaneará los archivos en sus volúmenes porque la BlueXP classification no puede revertir la "hora del último 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 anular este comportamiento en la página de Configuración para que la BlueXP classification escanee los volúmenes independientemente de los permisos.

Junto con esta capacidad, se ha agregado un nuevo filtro llamado "Evento de análisis de escaneo" para que pueda ver los archivos que no se clasificaron porque la BlueXP classification no pudo revertir la hora del último acceso, o los archivos que se clasificaron aunque la BlueXP classification no pudo revertir la hora del último acceso.

"Obtenga más información sobre la "Marca de tiempo del último acceso" y los permisos que requiere la BlueXP classification" .

La BlueXP classification identifica tres nuevos tipos de datos personales

La BlueXP classification puede identificar y categorizar archivos que contienen los siguientes tipos de datos:

- Número de tarjeta de identidad de Botswana (Omang)
- Número de pasaporte de Botsuana
- Tarjeta de Identidad de Registro Nacional de Singapur (NRIC)

"Vea todos los tipos de datos personales que la BlueXP classification puede identificar en sus datos" .

Funcionalidad actualizada para directorios

- La opción "Informe CSV ligero" para los informes de investigación de datos ahora incluye información de los directorios.
- El filtro de tiempo "Último acceso" ahora muestra el tiempo del último acceso tanto para archivos como para directorios.

Mejoras en la instalación

- El instalador de BlueXP classification para sitios sin acceso a Internet (sitios oscuros) ahora realiza una verificación previa para asegurarse de que su sistema y los requisitos de red estén en su lugar para una

instalación exitosa.

- Los archivos de registro de auditoría de instalación ahora se guardan; se escriben en `/ops/netapp/install_logs` .

05 de febrero de 2023

Versión 1.20

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

En versiones anteriores de la BlueXP classification, podía enviar alertas por correo electrónico a los usuarios de BlueXP de su cuenta cuando ciertas políticas críticas devolvían resultados. Esta función le permite recibir notificaciones para proteger sus datos cuando no está en línea. Ahora también puedes enviar alertas por correo electrónico desde Políticas a cualquier otro usuario (hasta 20 direcciones de correo electrónico) que no esté en tu cuenta de BlueXP .

"Obtenga más información sobre cómo enviar alertas por correo electrónico según los resultados de las políticas" .

Ahora puedes agregar patrones personales desde la interfaz de BlueXP classification

La BlueXP classification ha tenido durante un tiempo la capacidad de agregar "datos personales" personalizados que la BlueXP classification identificará en futuros escaneos. Sin embargo, era necesario iniciar sesión en el host Linux de BlueXP classification y usar una línea de comando para agregar los patrones personalizados. En esta versión, la capacidad de agregar patrones personales usando una expresión regular está en la interfaz de usuario de BlueXP classification , lo que hace que sea muy fácil agregar y editar estos patrones personalizados.

Capacidad de mover 15 millones de archivos utilizando la BlueXP classification

En el pasado, la BlueXP classification podía mover un máximo de 100 000 archivos de origen a cualquier recurso compartido NFS. Ahora puedes mover hasta 15 millones de archivos a la vez.

Capacidad de ver la cantidad de usuarios que tienen acceso a los archivos de SharePoint Online

El filtro "Número de usuarios con acceso" ahora admite archivos almacenados en repositorios de SharePoint Online. En el pasado, solo se admitían archivos en recursos compartidos CIFS. Tenga en cuenta que los grupos de SharePoint que no estén basados en el directorio activo no se contarán en este filtro en este momento.

Se ha agregado el nuevo estado "Éxito parcial" al panel Estado de acción.

El nuevo estado "Éxito parcial" indica que una acción de BlueXP classification ha finalizado y algunos elementos fallaron y otros tuvieron éxito, por ejemplo, cuando se mueven o eliminan 100 archivos. Además, el estado "Terminado" ha cambiado de nombre a "Éxito". En el pasado, el estado "Terminado" podía enumerar acciones que tuvieron éxito y acciones que fallaron. Ahora el estado "Éxito" significa que todas las acciones se realizaron correctamente en todos los elementos. "Vea cómo ver el panel Estado de acciones" .

9 de enero de 2023

Versión 1.19

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

El panel de gobernanza ha agregado una nueva área *Datos confidenciales y permisos amplios* que proporciona un mapa de calor de archivos que contienen datos confidenciales (incluidos datos personales

confidenciales y sensibles) y que son demasiado permisivos. Esto puede ayudarle a ver dónde puede haber algunos riesgos con datos confidenciales. "Más información" .

Hay tres nuevos filtros disponibles en la página de 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 para una determinada cantidad de usuarios. Puede elegir un rango de números para refinar los resultados; por ejemplo, para ver qué archivos son accesibles para 51-100 usuarios.
- Los filtros "Hora de creación", "Hora de descubrimiento", "Última modificación" y "Último acceso" ahora le permiten crear un rango de fechas personalizado en lugar de solo seleccionar un rango de días predefinido. Por ejemplo, puede buscar archivos con una "Hora de creación" "más antigua que 6 meses" o con una fecha de "Última modificación" dentro de los "últimos 10 días".
- El filtro "Ruta de archivo" ahora le permite especificar las rutas que desea excluir de los resultados de la consulta filtrada. Si ingresa rutas para incluir y excluir ciertos datos, la BlueXP classification busca primero todos los archivos en las rutas incluidas, luego elimina los archivos de las rutas excluidas y luego muestra los resultados.

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

La BlueXP classification puede identificar el Número Individual Japonés

La BlueXP classification puede identificar y categorizar archivos que contienen el Número Individual Japonés (también conocido como Mi Número). Esto incluye tanto el Número Personal como el Corporativo. "Vea todos los tipos de datos personales que la BlueXP classification puede identificar en sus datos" .

Limitaciones conocidas en la NetApp Data Classification

Las limitaciones conocidas identifican funciones que no son compatibles o no interoperan correctamente en esta versión. Revise estas limitaciones cuidadosamente.

Opciones deshabilitadas de NetApp Data Classification

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

- Se ha deshabilitado la opción para activar la recopilación de registros de auditoría.
- Durante la investigación de Directorios, la opción para calcular la cantidad de datos de información de identificación personal (PII) por Directorios no está disponible.
- Se ha deshabilitado la opción para integrar datos mediante etiquetas de Azure Information Protection (AIP).

Escaneo de clasificación de datos

Las siguientes limitaciones ocurren con los escaneos de clasificación de datos.

La clasificación de datos escanea solo un recurso compartido en un volumen

Si tiene varios recursos compartidos de archivos bajo un solo volumen, la clasificación de datos escanea el recurso compartido con la jerarquía más alta. Por ejemplo, si tiene acciones como las siguientes:

- /A

- /A/B
- /DO
- /DELAWARE

En esta configuración, solo se escanean los datos en /A. Los datos en /C y /D no se escanean.

Solución alternativa

Existe una solución alternativa para asegurarse de estar escaneando datos de todos los recursos compartidos en su volumen. Siga estos pasos:

1. En el sistema, agregue el volumen a escanear.
2. Una vez que la clasificación de datos haya terminado de escanear el volumen, vaya a la página *Investigación de datos* y cree un filtro para ver qué recurso compartido se está escaneando:

   Filtre los datos por "Nombre del sistema" 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 que pueda ver cuáles recursos compartidos no se están escaneando.
4. "Agregue las acciones restantes a un grupo de acciones" .

   Agregue todas las acciones individualmente, por ejemplo:

   ```
   /C
   /D
   ```

5. Realice estos pasos para cada volumen del sistema que tenga múltiples recursos compartidos.

Marca de tiempo del último acceso

Cuando la clasificación de datos realiza un escaneo de un directorio, el escaneo impacta el campo **Último acceso** del directorio. Cuando ve el campo **Último acceso**, esos metadatos reflejan la fecha y hora del escaneo o la última vez que un usuario accedió al directorio.

Empezar

Obtenga más información sobre la NetApp Data Classification

NetApp Data Classification es un servicio de gobernanza de datos para la NetApp Console que escanea sus fuentes de datos locales y en la nube corporativas para mapear y clasificar datos e identificar información privada. Esto puede ayudar a reducir el riesgo de seguridad y cumplimiento, disminuir los costos de almacenamiento y ayudarlo con sus proyectos de migración de datos.

A partir de la versión 1.31, la clasificación de datos está disponible como una capacidad principal dentro de la NetApp Console. No hay ningún cargo adicional No se requiere licencia de clasificación ni suscripción. + Si ha estado utilizando la versión heredada 1.30 o anterior, esa versión estará disponible hasta que expire su suscripción.

NetApp Console

Se puede acceder a la clasificación de datos a través de la NetApp Console.

La NetApp Console proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp . Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp . Sin embargo, algunos servicios de datos de NetApp accesibles desde la consola requieren licencia o suscripción.

Obtenga más información sobre el"NetApp Console" .

Funciones

La clasificación de datos utiliza inteligencia artificial (IA), procesamiento del lenguaje natural (PLN) y aprendizaje automático (ML) para comprender el contenido que escanea con el fin de extraer entidades y categorizar el contenido en consecuencia. Esto permite que la clasificación de datos proporcione las siguientes áreas de funcionalidad.

"Conozca los casos de uso para la clasificación de datos" .

Mantener el cumplimiento

La clasificación de datos proporciona varias herramientas que pueden ayudarle con sus esfuerzos de cumplimiento. Puede utilizar la clasificación de datos para:

- Identificar información de identificación personal (PII).
- Identifique un amplio alcance de información personal confidencial según lo exigen las regulaciones de privacidad GDPR, CCPA, PCI y HIPAA.

- Responder a las solicitudes de acceso del titular de los datos (DSAR) basadas en el nombre o la dirección de correo electrónico.

Fortalecer la seguridad

La clasificación de datos puede identificar datos que potencialmente corren el riesgo de ser accedidos con fines delictivos. Puede utilizar la clasificación de datos para:

- Identifique todos los archivos y directorios (recursos compartidos y carpetas) con permisos abiertos que estén expuestos a toda su organización o al público.
- Identifique datos confidenciales que residen fuera de la ubicación inicial dedicada.
- Cumplir con las políticas de retención de datos.
- Utilice *Políticas* para detectar automáticamente nuevos problemas de seguridad para que el personal de seguridad pueda tomar medidas de inmediato.

Optimizar el uso del almacenamiento

La clasificación de datos proporciona herramientas que pueden ayudarle con el costo total de propiedad (TCO) de su almacenamiento. Puede utilizar la clasificación de datos para:

- Aumente la eficiencia del almacenamiento identificando datos duplicados o no relacionados con el negocio.
- Ahorre costos de almacenamiento identificando datos inactivos que puede clasificar en un almacenamiento de objetos menos costoso. "Obtenga más información sobre la organización en niveles de los sistemas Cloud Volumes ONTAP" . "Obtenga más información sobre la organización en niveles de los sistemas ONTAP locales" .

Sistemas y fuentes de datos compatibles

La clasificación de datos puede escanear y analizar datos estructurados y no estructurados de los siguientes tipos de sistemas y fuentes de datos:

Sistemas

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP (implementado en AWS, Azure o GCP)
- Clústeres ONTAP locales
- StorageGRID
- Google Cloud NetApp Volumes

Fuentes de datos

- Recursos compartidos de archivos de NetApp
- Bases de datos:
  - Servicio de base de datos relacional de Amazon (Amazon RDS)
  - MongoDB
  - MySQL
  - Oráculo

- PostgreSQL
- SAP HANA
- Servidor SQL (MSSQL)

La clasificación de datos admite las versiones NFS 3.x, 4.0 y 4.1, y las versiones CIFS 1.x, 2.0, 2.1 y 3.0.

Costo

La clasificación de datos es de uso gratuito. No se requiere licencia de clasificación ni suscripción paga.

Costos de infraestructura

- La instalación de Data Classification en la nube requiere implementar una instancia en la nube, lo que genera cargos por parte del proveedor de la nube donde se implementa. Ver el tipo de instancia que se implementa para cada proveedor de nube . No hay ningún costo si instala Data Classification en un sistema local.
- Para la clasificación de datos es necesario que haya implementado un agente de consola. En muchos casos, ya tienes un agente de consola debido a otro almacenamiento y servicios que estás usando en la consola. La instancia del agente de consola genera cargos del proveedor de la nube donde se implementa. Ver el "tipo de instancia que se implementa para cada proveedor de nube" . No hay ningún costo si instala el agente de consola en un sistema local.

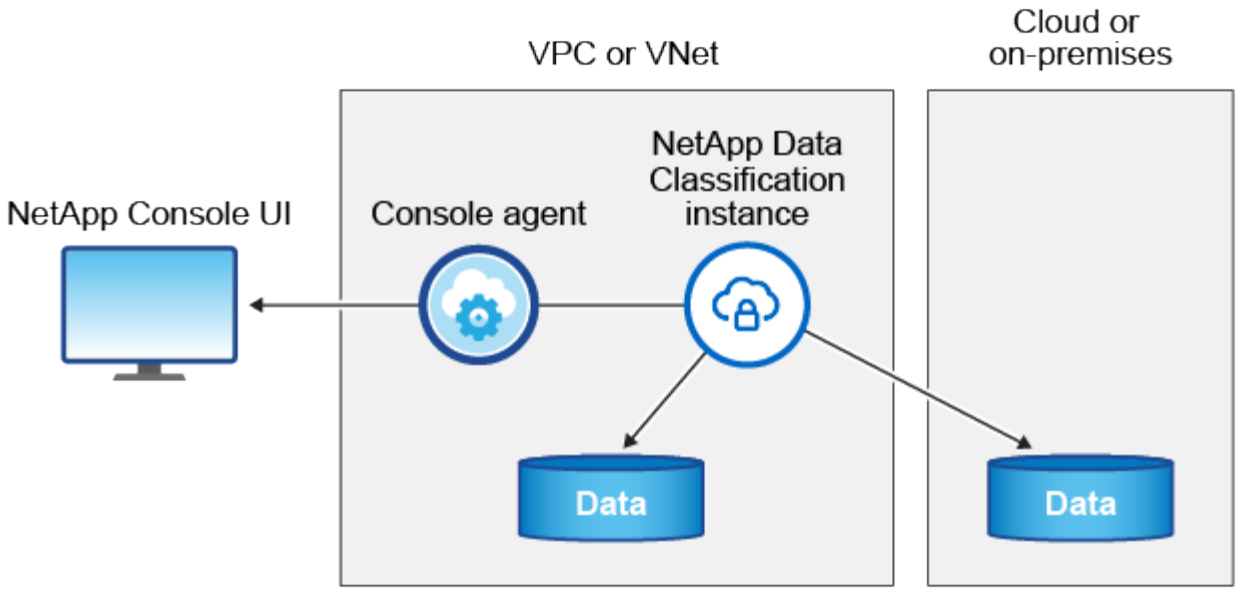
Costos de transferencia de datos

Los costos de transferencia de datos dependen de su configuración. Si la instancia de clasificación de datos y la fuente de datos están en la misma zona de disponibilidad y región, no hay costos de transferencia de datos. Pero si la fuente de datos, como un sistema Cloud Volumes ONTAP , está en una zona de disponibilidad o región *diferente*, su proveedor de nube le cobrará los costos de transferencia de datos. Consulte estos enlaces para obtener más detalles:

- "AWS: Precios de Amazon Elastic Compute Cloud (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 Datos

Cuando implementa la clasificación de datos en la nube, la consola implementa la instancia en la misma subred que el agente de la consola. "Obtenga más información sobre el agente de consola."



Tenga en cuenta lo siguiente sobre la instancia predeterminada:

- En AWS, la clasificación de datos se ejecuta en un "instancia m6i.4xlarge" con un disco GP2 de 500 GiB. La imagen del sistema operativo es Amazon Linux 2. Al implementar en AWS, puede elegir un tamaño de instancia más pequeño si está escaneando una pequeña cantidad de datos.
- En Azure, la clasificación de datos se ejecuta en un"Standard_D16s_v3 VM" con un disco de 500 GiB. La imagen del sistema operativo es Ubuntu 22.04.
- En GCP, la clasificación de datos se ejecuta en un"Máquina virtual n2-standard-16" con un disco persistente estándar de 500 GiB. La imagen del sistema operativo es Ubuntu 22.04.
- En las regiones donde la instancia predeterminada no está disponible, la clasificación de datos se ejecuta en una instancia alternativa. "Ver los tipos de instancias alternativos" .
- La instancia se llama *CloudCompliance* con un hash generado (UUID) concatenado a ella. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Solo se implementa una instancia de clasificación de datos por agente de consola.

También puede implementar la clasificación de datos en un host Linux en sus instalaciones o en un host en su 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 datos se automatizan siempre que la instancia tenga acceso a Internet.

La instancia debe permanecer en ejecución en todo momento porque la clasificación de datos escanea continuamente los datos.

Implementar en diferentes tipos de instancias

Revise las siguientes especificaciones para los tipos de instancias:

Tamaño del sistema	Especificaciones	Limitaciones
Extra grande	32 CPU, 128 GB de RAM, 1 TiB SSD	Puede escanear hasta 500 millones de archivos.

Tamaño del sistema	Especificaciones	Limitaciones
Grande (predeterminado)	16 CPU, 64 GB de RAM, SSD de 500 GiB	Puede escanear hasta 250 millones de archivos.

Al implementar la clasificación de datos en Azure o GCP, envíe un correo electrónico a ng-contact-data-sense@netapp.com para obtener ayuda si desea utilizar un tipo de instancia más pequeño.

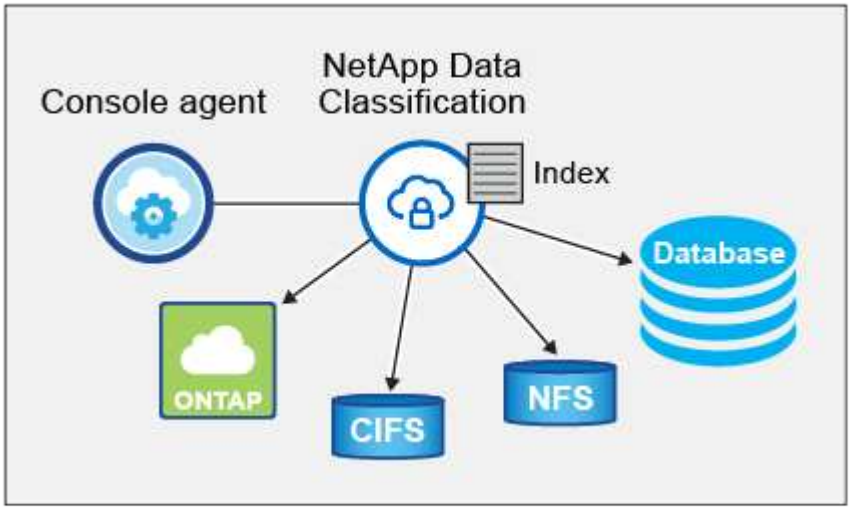
Cómo funciona el escaneo de clasificación de datos

A un alto nivel, el escaneo de clasificación de datos funciona así:

1. Implementa una instancia de Clasificación de datos en la consola.
2. Habilita el mapeo de alto nivel (llamados escaneos *Solo mapeo*) o el escaneo de nivel profundo (llamados escaneos *Mapeo y clasificación*) en una o más fuentes de datos.
3. La clasificación de datos escanea datos utilizando un proceso de aprendizaje de IA.
4. Puede utilizar los paneles y las herramientas de generación de informes proporcionados para ayudarle en sus esfuerzos de cumplimiento y gobernanza.

Después de habilitar la Clasificación de datos y seleccionar los repositorios que desea escanear (estos son los volúmenes, esquemas de bases de datos u otros datos de usuario), inmediatamente comienza a escanear los datos para identificar datos personales y confidenciales. En la mayoría de los casos, debe centrarse en escanear datos de producción en vivo en lugar de copias de seguridad, espejos o sitios de recuperación ante desastres. Luego, la clasificación de datos mapea los datos de su organización, categoriza cada archivo e identifica y extrae entidades y patrones predefinidos en los datos. El resultado del escaneo es un índice de información personal, información personal confidencial, categorías de datos y tipos de archivos.

La clasificación de datos se conecta a los datos como cualquier otro cliente montando volúmenes NFS y CIFS. A los volúmenes NFS se accede automáticamente como de solo lectura, mientras que es necesario proporcionar credenciales de Active Directory para escanear volúmenes CIFS.



Después del escaneo inicial, la clasificación de datos escanea continuamente sus datos de manera rotatoria para detectar cambios incrementales. Por eso es importante mantener la instancia en ejecución.

Puede habilitar y deshabilitar escaneos a nivel de volumen o a nivel de esquema de base de datos.

La clasificación de datos no impone un límite en la cantidad de datos que puede escanear. Cada agente de consola admite el escaneo y la visualización de 500 TiB de datos. Para escanear más de 500 TiB de datos,"instalar otro agente de consola" entonces"Implementar otra instancia de clasificación de datos" . + La interfaz de usuario de la consola muestra datos de un solo conector. Para obtener sugerencias sobre cómo ver datos de varios agentes de la consola, consulte"Trabajar con múltiples agentes de consola" .

¿Cuál es la diferencia entre los escaneos de mapeo y clasificación?

Puede realizar dos tipos de escaneos en Clasificación de datos:

- Los escaneos de solo mapeo brindan únicamente una descripción general de alto nivel de sus datos y se realizan en fuentes de datos seleccionadas. Los escaneos de solo mapeo toman menos tiempo que los escaneos de mapas y clasificación porque no acceden a los archivos para ver los datos dentro de ellos. Es posible que desees hacer esto inicialmente para identificar áreas de investigación y luego realizar un escaneo de Mapa y Clasificación en esas áreas.
- **Los escaneos de mapas y clasificación** proporcionan un escaneo de nivel profundo de sus datos.

Para obtener detalles sobre las diferencias entre los escaneos de mapeo y clasificación, consulte"¿Cuál es la diferencia entre los escaneos de mapeo y clasificación?" .

Información que la clasificación de datos categoriza

La clasificación de datos recopila, indexa y asigna categorías a los siguientes datos:

- **Metadatos estándar** sobre los archivos: el tipo de archivo, su tamaño, fechas de creación y modificación, etc.
- **Datos personales**: Información de identificación personal (PII), como direcciones de correo electrónico, números de identificación o números de tarjetas de crédito, que la clasificación de datos identifica mediante palabras, cadenas y patrones específicos en los archivos. "Obtenga más información sobre los datos personales" .
- **Datos personales sensibles**: Tipos especiales de información personal sensible (IPS), como datos de salud, origen étnico u opiniones políticas, según lo define el Reglamento General de Protección de Datos (RGPD) y otras regulaciones de privacidad. "Obtenga más información sobre datos personales sensibles" .
- **Categorías**: La clasificación de datos toma los datos que escanea y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. "Obtenga más información sobre las categorías".
- **Reconocimiento de entidades de nombre**: la clasificación de datos utiliza IA para extraer los nombres naturales de las personas de los documentos. "Obtenga información sobre cómo responder a las solicitudes de acceso de los interesados" .

Descripción general de la red

Data Classification implementa un solo servidor o clúster donde usted elija: en la nube o en las instalaciones. Los servidores se conectan a través de protocolos estándar a las fuentes de datos e indexan los resultados en un clúster Elasticsearch, que también está implementado en los mismos servidores. Esto permite compatibilidad con entornos multicloud, cross-cloud, cloud privado y locales.

La consola implementa la instancia de clasificación de datos con un grupo de seguridad que habilita conexiones HTTP entrantes desde el agente de la consola.

Cuando usa la consola en modo SaaS, la conexión a la consola se proporciona a través de HTTPS y los datos privados enviados entre su navegador y la instancia de clasificación de datos están protegidos con cifrado de extremo a extremo mediante TLS 1.2, lo que significa que NetApp y terceros no pueden leerlos.

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

Si tiene requisitos de red estrictos,"Obtenga información sobre los puntos finales con los que se comunica la clasificación de datos" .

Acceso a la NetApp Data Classification

Puede acceder a la NetApp Data Classification a través de la NetApp Console.

Para iniciar sesión en la consola, puede usar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la NetApp Console usando su correo electrónico y una contraseña. "Obtenga más información sobre cómo iniciar sesión en la consola" .

Tareas específicas requieren roles de usuario de consola específicos. "Obtenga información sobre los roles de acceso a la consola para todos los servicios" .

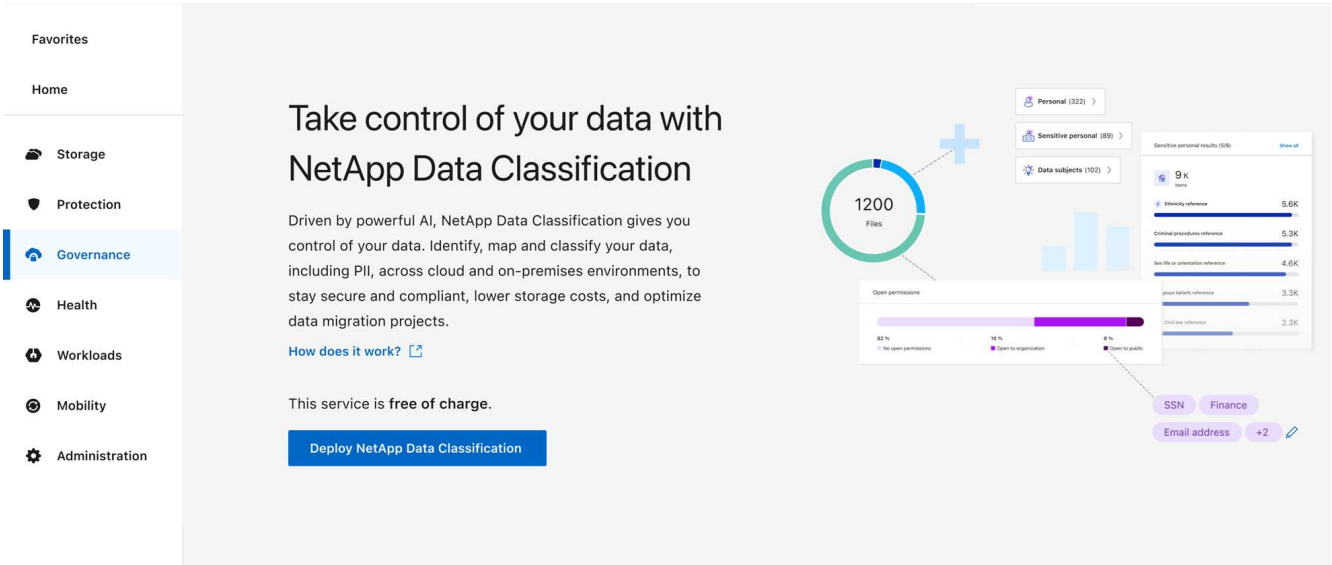
Antes de empezar

- "Debes agregar un agente de consola."
- "Comprenda qué estilo de implementación de clasificación de datos se adapta a su carga de trabajo."

Pasos

1. En un navegador web, navegue hasta el"Consola" .
2. Inicie sesión en la consola.
3. Desde la página principal de la NetApp Console, seleccione **Gobernanza** > **Clasificación de datos**.
4. Si es la primera vez que accede a Clasificación de datos, aparecerá la página de destino.

   Seleccione **Implementar clasificación local o en la nube** para comenzar a implementar su instancia de clasificación. Para obtener más información, consulte"¿Qué implementación de clasificación de datos debería utilizar?"



De lo contrario, aparecerá el Panel de clasificación de datos.

Implementar la clasificación de datos

¿Qué implementación de NetApp Data Classification debería utilizar?

Puede implementar NetApp Data Classification de diferentes maneras. Conozca qué método se adapta a sus necesidades.

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

- "Implementar en la nube usando la consola" . La consola implementa la instancia de clasificación de datos en la misma red del proveedor de nube que el agente de la consola.
- "Instalar en un host Linux con acceso a Internet" . Instale Data Classification en un host Linux en su red, o en un host Linux en la nube, que tenga acceso a Internet. Este tipo de instalación puede ser una buena opción si prefiere escanear sistemas ONTAP locales utilizando una instancia de clasificación de datos que también se encuentre en las instalaciones, aunque esto no es un requisito.
- "Instalar 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, no tiene conectividad con la capa SaaS de la consola.

> El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada. Para obtener documentación del modo privado en la interfaz heredada de BlueXP , consulte"Documentación en PDF para el modo privado de BlueXP" .

Tanto la instalación en un host Linux con acceso a Internet como la instalación local en un host Linux sin acceso a Internet utilizan un script de instalación. El script comienza verificando 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 ejecutar la instalación de Clasificación de datos, hay un paquete de software separado que puede descargar que solo prueba los requisitos previos.

Consulte "Compruebe que su host Linux esté listo para instalar Data Classification" .

Implemente la NetApp Data Classification en la nube mediante la NetApp Console

Puede implementar NetApp Data Classification en la nube con la NetApp Console. La consola implementa la instancia de clasificación de datos en la misma red del proveedor de nube que el agente de la consola.

Tenga en cuenta que también puede"Instalar Data Classification en un host Linux que tenga acceso a Internet" . Este tipo de instalación puede ser una buena opción si prefiere escanear sistemas ONTAP locales utilizando una instancia de clasificación de datos que también se encuentra 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

Comience rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener detalles completos.

Crear un agente de consola

Si aún no tiene un agente de consola, cree uno. Ver"Creación de un agente de consola en AWS" ,"Creación de un agente de consola en Azure" , o"Creación de un agente de consola en GCP" .

También puedes"Instalar el agente de consola local" en un host Linux de su red o en un host Linux en la nube.

Prerrequisitos

Asegúrate de que tu entorno puede cumplir los requisitos previos. Esto incluye acceso saliente a internet para la instancia, conectividad entre el agente de la Console y Data Classification por el puerto 443 y más. Ver la lista completa.

Implementar la clasificación de datos

Inicie el asistente de instalación para implementar la instancia de Clasificación de datos en la nube.

Crear un agente de consola

Si aún no tiene un agente de consola, cree uno en su proveedor de nube. Ver "Creación de un agente de consola en AWS" o "Creación de un agente de consola en Azure" , o "Creación de un agente de consola en GCP" . En la mayoría de los casos, probablemente ya tendrá configurado un agente de consola antes de intentar activar la clasificación de datos, ya que la mayoría "Las funciones de la consola requieren un agente de consola" , pero hay casos en los que necesitarás configurarlo ahora.

Hay algunos escenarios en los que es necesario utilizar un agente de consola implementado en un proveedor de nube específico:

- Al escanear datos en Cloud Volumes ONTAP en AWS o Amazon FSx para buckets de ONTAP , se utiliza un agente de consola en AWS.
- Al escanear datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, se utiliza un agente de consola en Azure.
  - Para Azure NetApp Files, debe implementarse en la misma región que los volúmenes que desea escanear.
- Al escanear datos en Cloud Volumes ONTAP en GCP, se utiliza un agente de consola en GCP.

Los sistemas ONTAP locales, los recursos compartidos de archivos de NetApp y las bases de datos se pueden escanear al usar cualquiera de estos agentes de consola en la nube.

Ten en cuenta que también puedes "Instalar el agente de consola local" en un host Linux de su red o en la nube. Algunos usuarios que planean instalar Data Classification localmente también pueden optar por instalar el agente de consola localmente.

Puede haber situaciones en las que necesites usar "varios agentes de consola" .

La clasificación de datos no impone un límite en la cantidad de datos que puede escanear. Cada agente de consola admite el escaneo y la visualización de 500 TiB de datos. Para escanear más de 500 TiB de datos,"instalar otro agente de consola" entonces"Implementar otra instancia de clasificación de datos" . + La interfaz de usuario de la consola muestra datos de un solo conector. Para obtener sugerencias sobre cómo ver datos de varios agentes de la consola, consulte"Trabajar con múltiples agentes de consola" .

Apoyo de la región gubernamental

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

"Obtenga información sobre cómo implementar el agente de consola en una región gubernamental.".

Prerrequisitos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de implementar la clasificación de datos en la nube. Cuando implementa la clasificación de datos en la nube, se ubica en la misma subred que el agente de consola.

Habilitar el acceso a Internet saliente desde la Clasificación de datos

La clasificación de datos requiere acceso a Internet saliente. Si su red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de clasificación de datos tenga acceso a Internet saliente para contactar los siguientes puntos finales. El proxy no debe ser transparente. Los servidores proxy transparentes no son compatibles actualmente.

Revise la tabla correspondiente a continuación según si está implementando la clasificación de datos en AWS, Azure o GCP.

Puntos finales necesarios para AWS

Puntos finales	Objetivo
\ https://api.console.netapp.com	Comunicación con el servicio de consola, que incluye cuentas de NetApp .
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	Comunicación con el sitio web de la consola para la autenticación centralizada de usuarios.
\ 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 de software, manifiestos y plantillas.
\ 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 que la clasificación de datos acceda y descargue manifiestos y plantillas, y envíe registros y métricas.

Puntos de conexión necesarios para Azure

Puntos finales	Objetivo
\ https://api.console.netapp.com	Comunicación con el servicio de consola, que incluye cuentas de NetApp .
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	Comunicación con el sitio web de la consola para la autenticación centralizada de usuarios.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y permite enviar registros y métricas.
\ https://support.compliance.api.console.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.

Puntos finales necesarios para GCP

Puntos finales	Objetivo
\ https://api.console.netapp.com	Comunicación con el servicio de consola, que incluye cuentas de NetApp .
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	Comunicación con el sitio web de la consola para la autenticación centralizada de usuarios.

Puntos finales	Objetivo
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y permite enviar registros y métricas.
\ https://support.compliance.api.console.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.

Asegúrese de que la clasificación de datos tenga los permisos necesarios

Asegúrese de que la clasificación de datos tenga permisos para implementar recursos y crear grupos de seguridad para la instancia de clasificación de datos.

- "Permisos de Google Cloud"
- "Permisos de AWS"
- "Permisos de Azure"

Asegúrese de que el agente de la consola pueda acceder a la clasificación de datos

Asegúrese de la conectividad entre el agente de la consola y la instancia de clasificación de datos. El grupo de seguridad del agente de consola debe permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de clasificación de datos. Esta conexión permite la implementación de la instancia de Clasificación de datos y le permite ver información en las pestañas Cumplimiento y Gobernanza. La clasificación de datos es compatible con las regiones gubernamentales en AWS y Azure.

Se requieren reglas de grupo de seguridad entrantes y salientes adicionales para las implementaciones de AWS y AWS GovCloud. Ver "Reglas para el agente de consola en AWS" Para más detalles.

Se requieren reglas de grupo de seguridad entrantes y salientes adicionales para las implementaciones de Azure y Azure Government. Ver "Reglas para el agente de consola en Azure" Para más detalles.

Asegúrese de poder mantener la clasificación de datos en funcionamiento

La instancia de Clasificación de datos debe permanecer activada para escanear continuamente sus datos.

Asegúrese de que el navegador web esté conectado a la clasificación de datos.

Una vez habilitada la clasificación de datos, asegúrese de que los usuarios accedan a la interfaz de la consola desde un host que tenga una conexión a la instancia de clasificación de datos.

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

Comprueba los límites de tu vCPU

Asegúrese de que el límite de vCPU de su proveedor de nube permita la implementación de una instancia con la cantidad necesaria de núcleos. Necesitará verificar el límite de vCPU para la familia de instancias relevante en la región donde se ejecuta la consola. "Ver los tipos de instancia requeridos" .

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

- "Documentación de AWS: Cuotas de servicio de Amazon EC2"
- "Documentación de Azure: Cuotas de vCPU de máquinas virtuales"
- "Documentación de Google Cloud: Cuotas de recursos"

Implementar la clasificación de datos en la nube

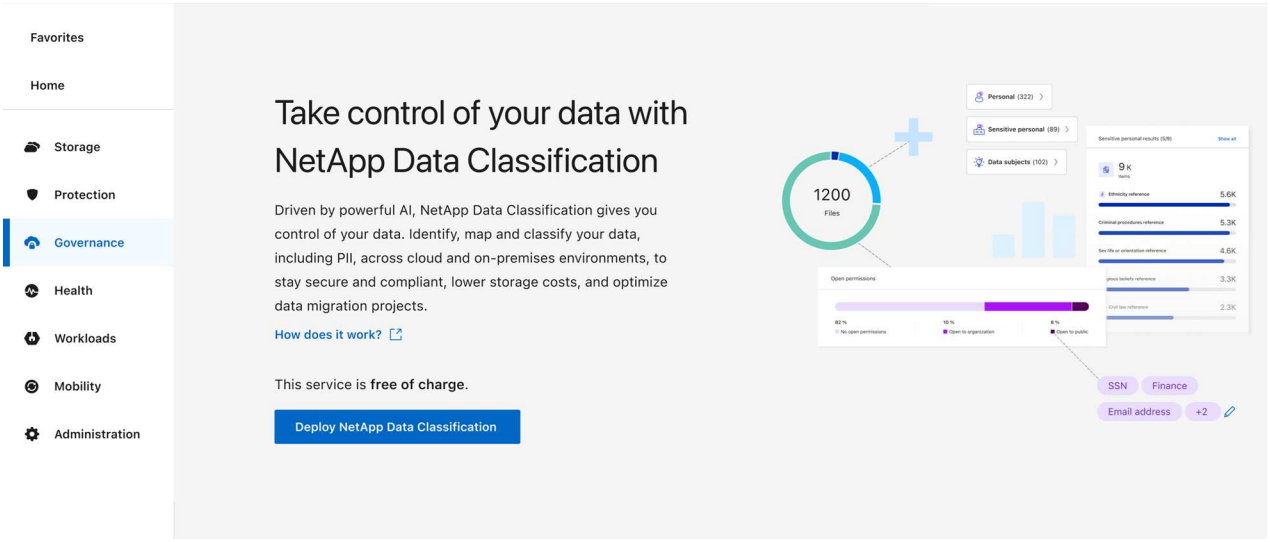
Siga estos pasos para implementar una instancia de Clasificación de datos en la nube. El agente de la consola implementará la instancia en la nube y luego instalará el software de clasificación de datos en esa instancia.

En las regiones donde el tipo de instancia predeterminado no está disponible, la clasificación de datos se ejecuta en un"tipo de instancia alternativo" .

Implementar en AWS

Pasos

1. Desde la página principal de Clasificación de datos, seleccione **Implementar clasificación en las instalaciones o en la nube**.

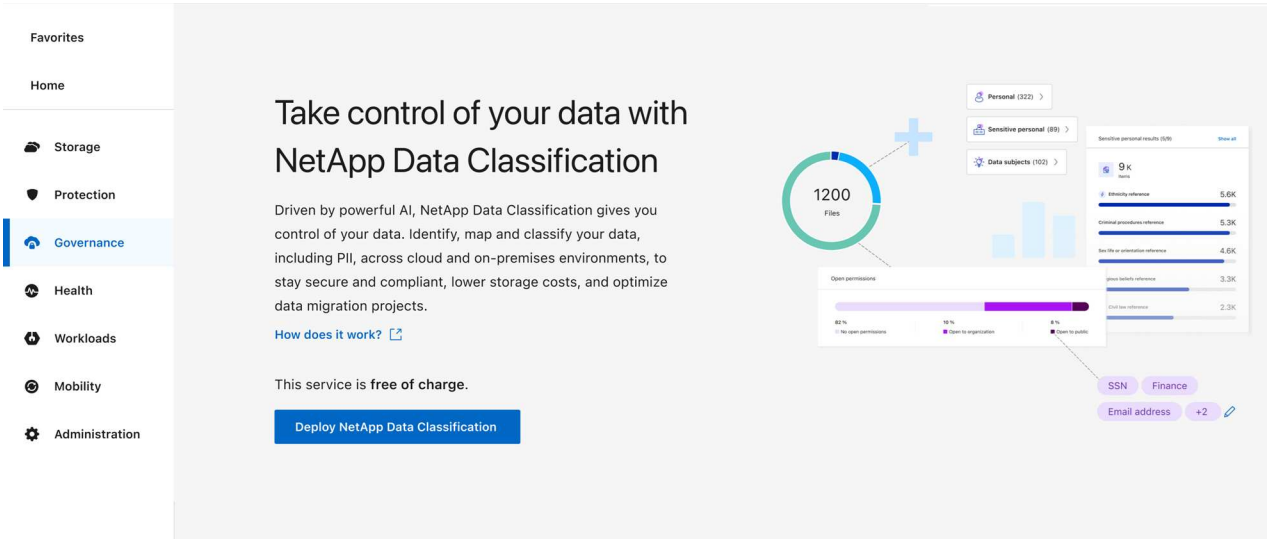


2. Desde la página *Instalación*, seleccione **Implementar > Implementar** para usar el tamaño de instancia "Grande" e iniciar el asistente de implementación en la nube.
3. El asistente muestra el progreso a medida que avanza en los pasos de implementación. Cuando se requieren entradas o si surgen problemas, se le solicitará información.
4. Cuando se implementa la instancia y se instala la Clasificación de datos, seleccione **Continuar con la configuración** para ir a la página *Configuración*.

Implementar en Azure

Pasos

1. Desde la página principal de Clasificación de datos, seleccione **Implementar clasificación en las instalaciones o en la nube**.



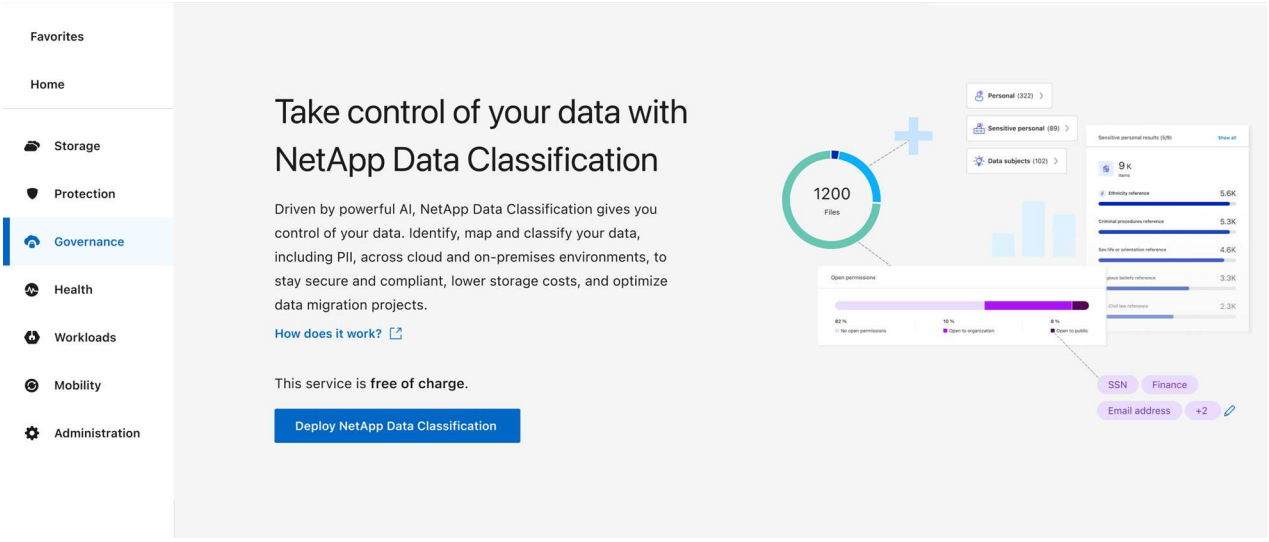
2. Seleccione **Implementar** para iniciar el asistente de implementación en la nube.

3. El asistente muestra el progreso a medida que avanza en los pasos de implementación. Se detendrá y solicitará información si surge algún problema.
4. Cuando se implementa la instancia y se instala la Clasificación de datos, seleccione **Continuar con la configuración** para ir a la página *Configuración*.

Implementar en Google Cloud

Pasos

1. Desde la página principal de Clasificación de datos, seleccione **Gobernanza > Clasificación**.
2. Seleccione **Implementar clasificación local o en la nube**.



3. Seleccione **Implementar** para iniciar el asistente de implementación en la nube.
4. El asistente muestra el progreso a medida que avanza en los pasos de implementación. Se detendrá y solicitará información si surge algún problema.
5. Cuando se implementa la instancia y se instala la Clasificación de datos, seleccione **Continuar con la configuración** para ir a la página *Configuración*.

Resultado

La consola implementa la instancia de clasificación de datos en su proveedor de nube.

Las actualizaciones del agente de consola y del software de clasificación de datos se automatizan siempre que las instancias tengan conectividad a Internet.

¿Qué sigue?

Desde la página de Configuración puede seleccionar las fuentes de datos que desea escanear.

Instalar NetApp Data Classification en un host que tenga acceso a Internet

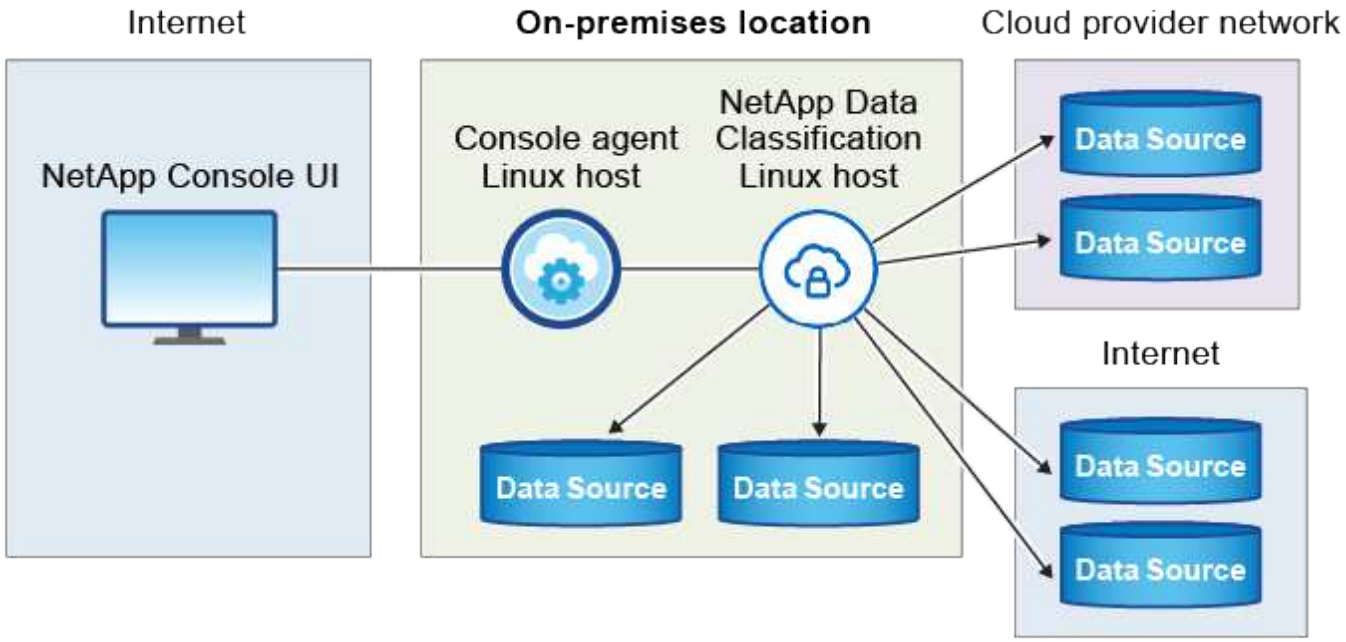
Para implementar NetApp Data Classification en un host Linux en su red o en un host Linux en la nube que tenga acceso a Internet, debe implementar el host Linux manualmente en su red o en la nube.

La instalación local es una buena opción si prefiere escanear sistemas ONTAP locales utilizando una instancia de clasificación de datos que también se encuentra en las instalaciones. Esto no es un requisito. El software

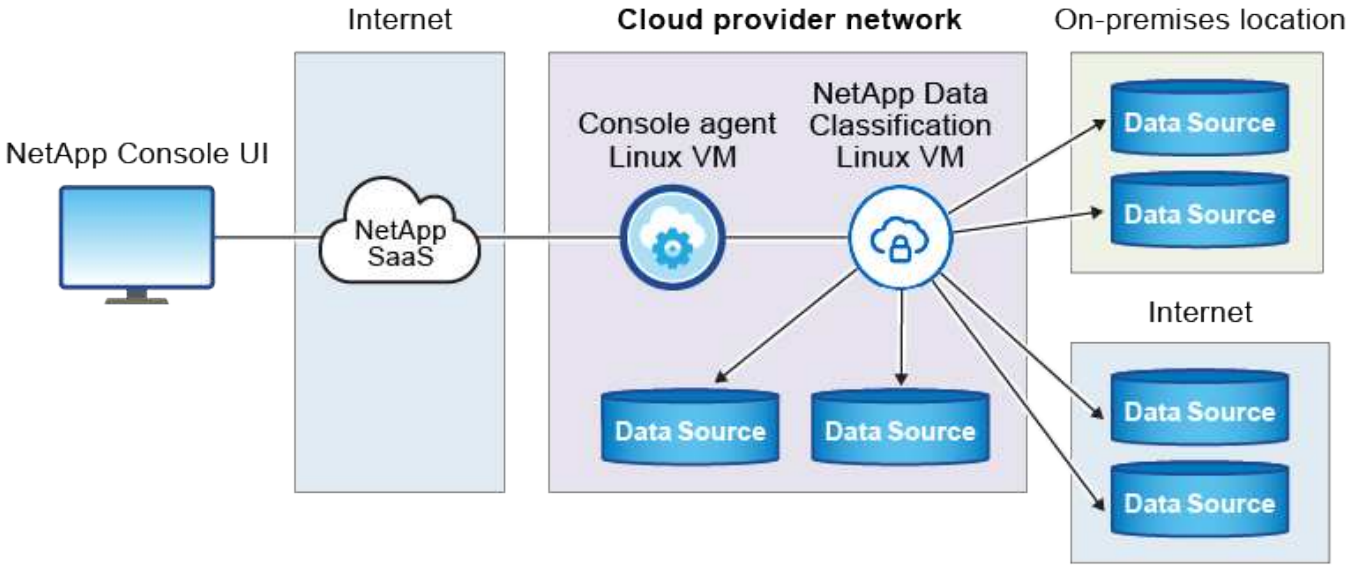
funciona de la misma manera independientemente del método de instalación que elija.

El script de instalación de Clasificación de datos comienza verificando si el sistema y el entorno cumplen los requisitos previos requeridos. Si se cumplen todos los requisitos previos, se inicia la instalación. Si desea verificar los requisitos previos independientemente de ejecutar la instalación de Clasificación de datos, hay un paquete de software separado que puede descargar que solo prueba los requisitos previos. "Vea cómo comprobar si su host Linux está listo para instalar la Clasificación de Datos" .

La instalación típica en un host Linux *en sus instalaciones* tiene los siguientes componentes y conexiones.



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



Inicio rápido

Comience rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener detalles completos.

1 Crear un agente de consola

Si aún no tienes un agente de consola, "Implementar el agente de consola localmente" en un host Linux en su red o en un host Linux en la nube.

También puedes crear un agente de consola con tu proveedor de nube. Ver "Creación de un agente de consola en AWS" , "Creación de un agente de consola en Azure" , o "Creación de un agente de consola en GCP" .

2 Revisar los prerrequisitos

Asegúrese de que su entorno pueda cumplir con los requisitos previos. Esto incluye acceso a Internet saliente para la instancia, conectividad entre el agente de la consola y la clasificación de datos a través del puerto 443 y más. Ver la lista completa .

También necesitas un sistema Linux que cumpla con los requisitossiguientes requisitos .

3 Descargar e implementar la clasificación de datos

Descargue el software Cloud Data Classification del sitio de soporte de NetApp y copie el archivo de instalación en el host Linux que planea utilizar. Luego, inicie el asistente de instalación y siga las instrucciones para implementar la instancia de Clasificación de datos.

Crear un agente de consola

Se requiere un agente de consola antes de poder instalar y utilizar la clasificación de datos. En la mayoría de los casos, probablemente tendrá un agente de consola configurado antes de intentar activar la clasificación de datos porque la mayoría "Las funciones de la consola requieren un agente de consola" , pero habrá casos en los que necesitarás configurar uno ahora.

Para crear uno en su entorno de proveedor de nube, consulte "Creación de un agente de consola en AWS" , "Creación de un agente de consola en Azure" , o "Creación de un agente de consola en GCP" .

Hay algunos escenarios en los que es necesario utilizar un agente de consola implementado en un proveedor de nube específico:

- Al escanear datos en Cloud Volumes ONTAP en AWS o Amazon FSx para ONTAP, se utiliza un agente de consola en AWS.
- Al escanear datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, se utiliza un agente de consola en Azure.

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

- Al escanear datos en Cloud Volumes ONTAP en GCP, se utiliza un agente de consola en GCP.

Los sistemas ONTAP locales, los recursos compartidos de archivos de NetApp y las cuentas de bases de datos se pueden escanear utilizando cualquiera de estos agentes de consola en la nube.

Tenga en cuenta que también puede "Implementar el agente de consola localmente" en un host Linux en su red o en un host Linux en la nube. Algunos usuarios que planean instalar Data Classification en sus instalaciones también pueden optar por instalar el agente de consola en sus instalaciones.

Necesitará la dirección IP o el nombre de host del sistema del agente de consola al instalar Clasificación de datos. Tendrás esta información si instalaste el agente de consola en tus instalaciones. Si el agente de la consola está implementado en la nube, puede encontrar esta información en la consola: seleccione el ícono Ayuda, luego **Soporte** y luego **Agente de consola**.

Preparar el sistema host Linux

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

Asegúrese de poder mantener la clasificación de datos en ejecución. La máquina de clasificación de datos debe permanecer encendida para escanear continuamente sus datos.

- La clasificación de datos debe realizarse en un host dedicado. El host no se puede compartir con otras aplicaciones o software de terceros, como antivirus.
- Elija el tamaño que se alinee con el conjunto de datos que planea escanear con Clasificación de datos.

Tamaño del sistema	UPC	RAM (la memoria de intercambio debe estar deshabilitada)	Disco
Extra grande	32 CPU	128 GB de RAM	• SSD de 1 TiB en /, o 100 GiB disponibles en /opt • 895 GiB disponibles en /var/lib/docker • 5 GiB en /tmp • **Para Podman, 30 GB en /var/tmp**
Grande	16 CPU	64 GB de RAM	• SSD de 500 GiB en /, o 100 GiB disponibles en /opt • 400 GiB disponibles en /var/lib/docker o para Podman /var/lib/containers • 5 GiB en /tmp • **Para Podman, 30 GB en /var/tmp**

- Al implementar una instancia de cómputo en la nube para su instalación de Clasificación de datos, se recomienda utilizar un sistema que cumpla con los requisitos del sistema "Grande" mencionados anteriormente:
  - **Tipo de instancia de Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Ver tipos de instancias de AWS adicionales" .
  - **Tamaño de máquina virtual de Azure**: "Standard_D16s_v3". "Ver tipos de instancias de Azure adicionales" .
  - **Tipo de máquina GCP**: "n2-standard-16". "Ver tipos de instancias de GCP adicionales" .
- **Permisos de carpeta UNIX**: Se requieren los siguientes permisos mínimos de UNIX:

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

- **Sistema operativo**:
  - Los siguientes sistemas operativos requieren el uso del motor de contenedores Docker:
    - Red Hat Enterprise Linux versión 7.8 y 7.9
    - Ubuntu 22.04 (requiere la versión 1.23 o superior de Data Classification)
    - Ubuntu 24.04 (requiere la versión 1.23 o superior de Data Classification)
  - Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión 1.30 o superior de Data Classification:
    - Red Hat Enterprise Linux versiones 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 y 9.6.
  - Las extensiones vectoriales avanzadas (AVX2) deben estar habilitadas en el sistema host.
- **Gestión de suscripciones de Red Hat**: el host debe estar registrado en Gestión de suscripciones de Red Hat. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación.
- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Classification:
  - Dependiendo del sistema operativo que estés usando, necesitas instalar uno de los motores de contenedores:
    - Docker Engine versión 19.3.1 o superior. "Ver instrucciones de instalación" .
    - Podman versión 4 o superior. Para instalar Podman, ingrese(`sudo yum install podman netavark -y`).
- Versión de Python 3.6 o superior. "Ver instrucciones de instalación" .
  - **Consideraciones sobre NTP**: NetApp recomienda configurar el sistema de clasificación de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La hora debe estar sincronizada entre el sistema de clasificación de datos y el sistema del agente de consola.
- **Consideraciones sobre Firewalld**: Si planea utilizar `firewalld` Le recomendamos que lo habilite antes de instalar Data Classification. Ejecute los siguientes comandos para configurar `firewalld` para que sea compatible con la Clasificación de Datos:

```
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 planea utilizar hosts de clasificación de datos adicionales como nodos de escáner, agregue estas reglas a su 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` ajustes.

La dirección IP del sistema host de clasificación de datos no se puede cambiar después de la instalación.

Habilitar el acceso a Internet saliente desde la Clasificación de datos

La clasificación de datos requiere acceso a Internet saliente. Si su red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de clasificación de datos tenga acceso a Internet saliente para contactar los siguientes puntos finales.

Puntos finales	Objetivo
\ https://api.console.netapp.com	Comunicación con la consola, que incluye cuentas de NetApp .
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	Comunicación con el sitio web de la consola para la autenticación centralizada de usuarios.
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 permite 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://packages.ubuntu.com/ \ http://archive.ubuntu.com	Proporciona paquetes de requisitos previos para la instalación de Ubuntu.

Verifique que todos los puertos requeridos estén habilitados

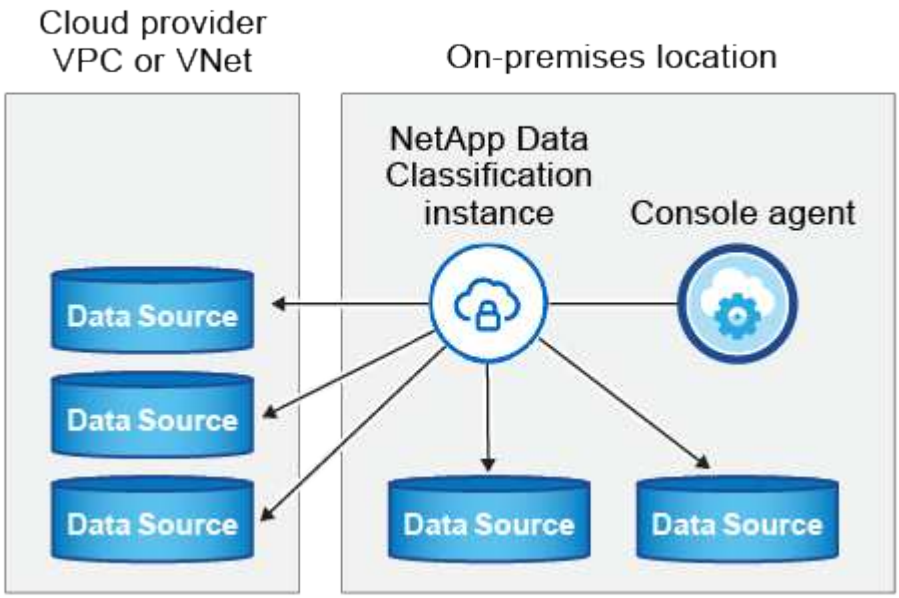
Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el agente de la consola, la clasificación de datos, Active Directory y sus fuentes de datos.

Tipo de conexión	Puertos	Descripción
Agente de consola <> Clasificación de datos	8080 (TCP), 443 (TCP) y 80. 9000	Las reglas de firewall o enrutamiento para el agente de la consola deben permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de clasificación de datos. Asegúrese de que el puerto 8080 esté abierto para que pueda ver el progreso de la instalación en la consola. Si se utiliza un firewall en el host Linux, se requiere el puerto 9000 para los procesos internos dentro de un servidor Ubuntu.
Agente de consola <> clúster ONTAP (NAS)	443 (TCP)	La consola descubre clústeres ONTAP mediante HTTPS. Si utiliza políticas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del agente de la consola debe permitir el acceso HTTPS saliente a través del puerto 443. Si el agente de la consola está en la nube, toda comunicación saliente está permitida por el firewall predefinido o las reglas de enrutamiento. • El clúster ONTAP debe permitir el acceso HTTPS entrante a través del puerto 443. La política de firewall predeterminada "mgmt" permite el acceso HTTPS entrante desde todas las direcciones IP. Si modificó esta política predeterminada o si creó su propia política de firewall, debe asociar el protocolo HTTPS con esa política y habilitar el acceso desde el host del agente de la Consola.
Clasificación de datos <> Clúster ONTAP	• Para NFS - 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS - 139 (TCP\UDP) y 445 (TCP\UDP)	La clasificación de datos necesita una conexión de red a cada subred de Cloud Volumes ONTAP o al sistema ONTAP local. Los firewalls o las reglas de enrutamiento para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de clasificación de datos. Asegúrese de que estos puertos estén abiertos para la instancia de clasificación de datos: • Para NFS - 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volumen NFS deben permitir el acceso desde la instancia de clasificación de datos.

Tipo de conexión	Puertos	Descripción
Clasificación de datos <> Active Directory	389 (TCP y UDP), 636 (TCP), 3268 (TCP) y 3269 (TCP)	Debe tener un Directorio Activo ya configurado para los usuarios de su empresa. Además, la clasificación de datos necesita credenciales de Active Directory para escanear volúmenes CIFS. Debes tener la información del Directorio Activo: • Dirección IP del servidor DNS o varias direcciones IP • Nombre de usuario y contraseña para el servidor • Nombre de dominio (nombre de Active Directory) • Ya sea que esté utilizando LDAP seguro (LDAPS) o no • Puerto del servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

Instalar la clasificación de datos en el host Linux

Para configuraciones típicas, instalará el software en un solo sistema host. Vea esos pasos aquí .



VerPreparación del sistema host Linux yRevisión de prerrequisitos para obtener la lista completa de requisitos antes de implementar la clasificación de datos.

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

Actualmente, la clasificación de datos no puede escanear depósitos S3, Azure NetApp Files o FSx para ONTAP cuando el software está instalado en las instalaciones. En estos casos, necesitará implementar un agente de consola independiente y una instancia de clasificación de datos en la nube y "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 datos en un solo host local.

"Mira este vídeo"para ver cómo instalar Clasificación de Datos.

Tenga en cuenta que todas las actividades de instalación se registran al instalar Data Classification. Si surge algún problema durante la instalación, puede ver el contenido del registro de auditoría de la instalación. Esta escrito para `/opt/netapp/install_logs/` .

Antes de empezar

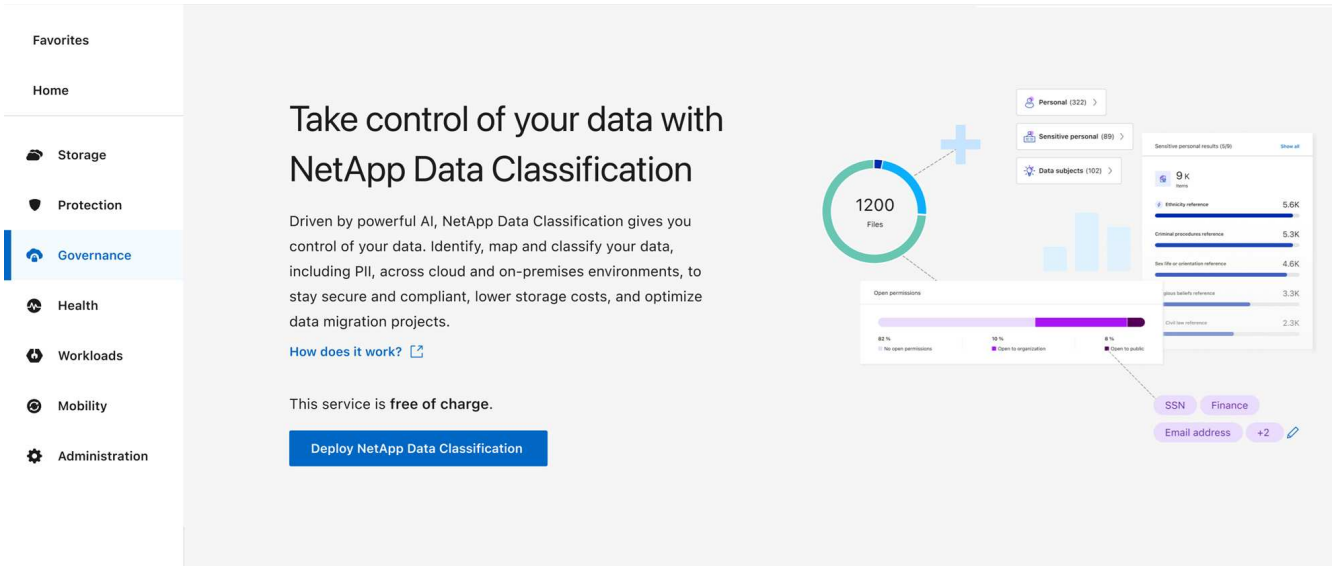
- Verifique que su sistema Linux cumpla con losrequisitos del anfitrión .
- Verifique que el sistema tenga instalados los dos paquetes de software necesarios (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de root en el sistema Linux.
- Si está utilizando un proxy para acceder a 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 realiza la interceptación de TLS, necesitará saber la ruta en el sistema Linux de clasificación de datos donde se almacenan los certificados CA de TLS.
  - El proxy no debe ser transparente. Actualmente, la clasificación de datos no admite servidores proxy transparentes.
  - El usuario debe ser un usuario local. Los usuarios del dominio no son compatibles.
- Verifique que su entorno fuera de línea cumpla con los requisitospermisos y conectividad .

Pasos

1. Descargue el software de clasificación de datos desde "Sitio de soporte de NetApp" . El archivo que debe seleccionar se llama **DATASENSE-INSTALLER-<versión>.tar.gz**.
2. Copie el archivo de instalación en el host Linux que planea utilizar (usando `scp` o algún otro método).
3. Descomprima el archivo de instalación en la máquina host, por ejemplo:

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

4. En la consola, seleccione **Gobernanza > Clasificación**.
5. Seleccione **Implementar clasificación local o en la nube**.



6. Dependiendo de si está instalando Data Classification en una instancia que preparó en la nube o en una instancia que preparó en sus instalaciones, seleccione la opción **Implementar** adecuada para iniciar la instalación de Data Classification.
7. Se muestra el cuadro de diálogo *Implementar clasificación de datos en las instalaciones*. Copie el comando proporcionado (por ejemplo: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) y pégalo en un archivo de texto para que puedas usarlo más tarde. Luego seleccione **Cerrar** para cerrar el cuadro de diálogo.
8. En la máquina host, ingrese el comando que copió y luego siga una serie de indicaciones, o puede proporcionar el comando completo incluidos todos los parámetros requeridos como argumentos de la línea de comando.

   Tenga en cuenta que el instalador realiza una verificación previa para asegurarse de que los requisitos del sistema y de la red estén cumplidos para una instalación exitosa. "Mira este vídeo" Para comprender los mensajes previos a la verificación y sus implicaciones.

Introduzca los parámetros según se le solicite:	Introduzca el comando completo:
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 nube (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 datos para que el sistema del agente de la consola pueda acceder a ella. c. Ingrese la dirección IP o el nombre de host de la máquina host del agente de consola para que el sistema de clasificación de datos pueda acceder a ella. d. Introduzca los detalles del proxy cuando se le solicite. Si su agente de consola ya utiliza un proxy, no es necesario ingresar esta información nuevamente aquí ya que la clasificación de datos utilizará automáticamente el proxy utilizado por el agente de consola.	Alternativamente, puede crear todo el comando 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 variables:

- *account_id* = ID de cuenta de NetApp
- *client_id* = ID de cliente del agente de consola (agregue el sufijo "clients" 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 datos.
- *cm_host* = dirección IP o nombre de host del sistema del agente de consola.
- *cloud_provider* = Al instalar en una instancia de nube, ingrese "AWS", "Azure" o "Gcp" según el 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* = Esquema de conexión: https o http (predeterminado http).
- *proxy_user* = Usuario autenticado para conectarse al servidor proxy, si se requiere autenticación básica. El usuario debe ser un usuario local (no se admiten usuarios de dominio).
- *proxy_password* = Contraseña para el nombre de usuario que usted especificó.
- *ca_cert_dir* = Ruta en el sistema Linux de clasificación de datos que contiene paquetes de certificados CA TLS adicionales. Solo es necesario si el proxy está realizando intercepción TLS.

Resultado

El instalador de Data Classification instala paquetes, registra la instalación e instala Data Classification. La instalación puede tardar entre 10 y 20 minutos.

Si hay conectividad a través del puerto 8080 entre la máquina host y la instancia del agente de la consola, verá el progreso de la instalación en la pestaña Clasificación de datos en la consola.

¿Qué sigue?

Desde la página de Configuración puede seleccionar las fuentes de datos que desea escanear.

Instalar NetApp Data Classification en un host Linux sin acceso a Internet

La instalación de NetApp Data Classification en un host Linux en un sitio local que no tiene acceso a Internet se conoce como *modo privado*. Este tipo de instalación, que utiliza un script de instalación, no tiene conectividad con la capa SaaS de la NetApp Console .

> El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada. Para obtener documentación del modo privado en la interfaz heredada de BlueXP , consulte"Documentación en PDF para el modo privado de BlueXP" .

Compruebe que su host Linux esté listo para instalar NetApp Data Classification

Antes de instalar NetApp Data Classification manualmente en un host Linux, opcionalmente ejecute un script en el host para verificar que todos los requisitos previos estén cumplidos para instalar Data Classification. Puede ejecutar este script en un host Linux en su red o en un host Linux en la nube. El host puede estar conectado a Internet o puede residir en un sitio que no tenga acceso a Internet (un *sitio oscuro*).

El script de instalación de Clasificación de datos incluye un script de prueba para garantizar que su entorno cumpla con los requisitos. Puede ejecutar este script por separado para verificar la preparación del host Linux antes de ejecutar el script de instalación.

Empezando

Realizarás las siguientes tareas:

- Opcionalmente, instale un agente de consola si aún no tiene uno instalado. Puede ejecutar el script de prueba sin tener un agente de consola instalado, pero el script verifica la conectividad entre el agente de consola y la máquina host de clasificación de datos, por lo que se recomienda que tenga un agente de consola.
- Prepare la máquina host y verifique que cumpla con todos los requisitos.
- Habilitar el acceso a Internet saliente desde la máquina host de clasificación de datos.
- Verifique que todos los puertos necesarios estén habilitados en todos los sistemas.
- Descargue y ejecute el script de prueba de prerrequisitos.

Crear un agente de consola

Se requiere un agente de consola antes de poder instalar y utilizar la clasificación de datos. Sin embargo, puede ejecutar el script de Requisitos previos sin un agente de consola.

Puede "Instalar el agente de consola local" en un host Linux en su red o en un host Linux en la nube. También puede instalar Clasificación de datos localmente si el agente de Consola está instalado localmente.

Para crear un agente de consola en su entorno de proveedor de nube, consulte:

- "Creación de un agente de consola en AWS"
- "Creación de un agente de consola en Azure"
- "Creación de un agente de consola en GCP"

Necesita la dirección IP o el nombre de host del sistema del agente de la consola al ejecutar el script de requisitos previos. Tienes esta información si instalaste el agente de consola en tus instalaciones. Si el agente de la Consola está implementado en la nube, puede encontrar esta información desde la Consola: seleccione el ícono Ayuda y luego **Soporte**; en la sección Agente y Auditoría, seleccione **Ir al agente**.

Verificar los requisitos del host

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

- La clasificación de datos debe realizarse en un host dedicado. El host no se puede compartir con otras aplicaciones o software de terceros, como antivirus.
- Elija el tamaño que se alinee con el conjunto de datos que planea escanear con Clasificación de datos.

Tamaño del sistema	UPC	RAM (la memoria de intercambio debe estar deshabilitada)	Disco
Extra grande	32 CPU	128 GB de RAM	• SSD de 1 TiB en /, o 100 GiB disponibles en /opt • 895 GiB disponibles en /var/lib/docker • 5 GiB en /tmp • **Para Podman, 30 GB en /var/tmp**
Grande	16 CPU	64 GB de RAM	• SSD de 500 GiB en /, o 100 GiB disponibles en /opt • 400 GiB disponibles en /var/lib/docker o para Podman /var/lib/containers • 5 GiB en /tmp • **Para Podman, 30 GB en /var/tmp**

- Al implementar una instancia de cómputo en la nube para su instalación de Clasificación de datos, se recomienda utilizar un sistema que cumpla con los requisitos del sistema "Grande" mencionados anteriormente:
  - **Tipo de instancia de Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Ver tipos de instancias de AWS adicionales" .

- **Tamaño de máquina virtual de Azure**: "Standard_D16s_v3". "Ver tipos de instancias de Azure adicionales" .
- **Tipo de máquina GCP**: "n2-standard-16". "Ver tipos de instancias de GCP adicionales" .

- **Permisos de carpeta UNIX**: Se requieren los siguientes permisos mínimos de UNIX:

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

- **Sistema operativo**:
  - Los siguientes sistemas operativos requieren el uso del motor de contenedores Docker:
    - Red Hat Enterprise Linux versión 7.8 y 7.9
    - Ubuntu 22.04 (requiere la versión 1.23 o superior de Data Classification)
    - Ubuntu 24.04 (requiere la versión 1.23 o superior de Data Classification)
  - Los siguientes sistemas operativos requieren el uso del motor de contenedores Podman y requieren la versión 1.30 o superior de Data Classification:
    - Red Hat Enterprise Linux versiones 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 y 9.6.
  - Las extensiones vectoriales avanzadas (AVX2) deben estar habilitadas en el sistema host.
- **Gestión de suscripciones de Red Hat**: el host debe estar registrado en Gestión de suscripciones de Red Hat. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación.
- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Classification:
  - Dependiendo del sistema operativo que estés usando, necesitas instalar uno de los motores de contenedores:
    - Docker Engine versión 19.3.1 o superior. "Ver instrucciones de instalación" .
    - Podman versión 4 o superior. Para instalar Podman, ingrese(`sudo yum install podman netavark -y`).
- Versión de Python 3.6 o superior. "Ver instrucciones de instalación" .
  - **Consideraciones sobre NTP**: NetApp recomienda configurar el sistema de clasificación de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La hora debe estar sincronizada entre el sistema de clasificación de datos y el sistema del agente de consola.
- **Consideraciones sobre Firewalld**: Si planea utilizar `firewalld` Le recomendamos que lo habilite antes de instalar Data Classification. Ejecute los siguientes comandos para configurar `firewalld` para que sea compatible con la Clasificación de Datos:

```
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 planea utilizar hosts de clasificación de datos adicionales como nodos de escáner (en un modelo distribuido), agregue estas reglas a su 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` ajustes.

Habilitar el acceso a Internet saliente desde la Clasificación de datos

La clasificación de datos requiere acceso a Internet saliente. Si su red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de clasificación de datos tenga acceso a Internet saliente para contactar los siguientes puntos finales.

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

Puntos finales	Objetivo
\ https://api.console.netapp.com	Comunicación con el servicio de consola, que incluye cuentas de NetApp .
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	Comunicación con el sitio web de la consola para la autenticación centralizada de usuarios.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y permite enviar registros y métricas.
\ https://support.compliance.api.console.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	Objetivo
\ http://packages.ubuntu.com/ \ http://archive.ubuntu.com	Proporciona paquetes de requisitos previos para la instalación de Ubuntu.

Verifique que todos los puertos requeridos estén habilitados

Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el agente de la consola, la clasificación de datos, Active Directory y sus fuentes de datos.

Tipo de conexión	Puertos	Descripción
Agente de consola <> Clasificación de datos	8080 (TCP), 443 (TCP) y 80. 9000	Las reglas de firewall o enrutamiento para el agente de la consola deben permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de clasificación de datos. Asegúrese de que el puerto 8080 esté abierto para que pueda ver el progreso de la instalación en la consola. Si se utiliza un firewall en el host Linux, se requiere el puerto 9000 para los procesos internos dentro de un servidor Ubuntu.
Agente de consola <> clúster ONTAP (NAS)	443 (TCP)	La consola descubre clústeres ONTAP mediante HTTPS. Si utiliza políticas de firewall personalizadas, el host del agente de la consola debe permitir el acceso HTTPS saliente a través del puerto 443. Si el agente de la consola está en la nube, toda comunicación saliente está permitida por el firewall predefinido o las reglas de enrutamiento.

Ejecute el script de requisitos previos de clasificación de datos

Siga estos pasos para ejecutar el script de requisitos previos de clasificación de datos.

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

Antes de empezar

- Verifique que su sistema Linux cumpla con losrequisitos del anfitrión .
- Verifique que el sistema tenga instalados los dos paquetes de software necesarios (Docker Engine o Podman y Python 3).
- Asegúrese de tener privilegios de root en el sistema Linux.

Pasos

1. Descargue el script de Requisitos previos de clasificación de datos desde "Sitio de soporte de NetApp" . El archivo que debe seleccionar se llama **standalone-pre-requisite-tester-<version>**.
2. Copie el archivo al host Linux que planea utilizar (usando `scp` o algún otro método).
3. Asignar permisos para ejecutar el script.

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

4. Ejecute el script utilizando el siguiente comando.

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

   Agregue la opción "--darksite" solo si está ejecutando el script en un host que no tiene acceso a Internet. Se omiten ciertas pruebas de requisitos previos cuando el host no está conectado a Internet.

5. El script le solicita la dirección IP de la máquina host de clasificación de datos.
   - Introduzca la dirección IP o el nombre de host.
6. El script le preguntará si tiene un agente de consola instalado.
   - Ingrese **N** si no tiene un agente de consola instalado.
   - Ingrese **Y** si tiene un agente de consola instalado. Y luego ingrese la dirección IP o el nombre de host del agente de la consola para que el script de prueba pueda probar esta conectividad.
7. El script ejecuta una variedad de pruebas en el sistema y muestra resultados a medida que avanza. Cuando termina, 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 Data Classification en el host cuando esté listo.

Si se descubre algún problema, se clasifica como "Recomendado" o "Obligatorio" para su solución. Los problemas recomendados suelen ser elementos que harían que las tareas de categorización y escaneo de clasificación de datos se ejecuten más lentamente. No es necesario corregir estos elementos, pero es posible que quieras abordarlos.

Si tiene algún problema "Obligatorio", debe solucionarlo y ejecutar nuevamente el script de prueba de requisitos previos.

Activar el escaneo en sus fuentes de datos

Escanee fuentes de datos con NetApp Data Classification

NetApp Data Classification escanea los datos en los repositorios (los volúmenes, esquemas de bases de datos u otros datos de usuario) que seleccione para identificar datos personales y confidenciales. Luego, la clasificación de datos mapea los datos de su organización, categoriza cada archivo e identifica patrones predefinidos en los datos. El resultado del escaneo es un índice de información personal, información personal confidencial, categorías de datos y tipos de archivos.

Después del escaneo inicial, la clasificación de datos escanea continuamente sus datos de manera rotatoria para detectar cambios incrementales. Por eso es importante mantener la instancia en ejecución.

Puede habilitar y deshabilitar escaneos a nivel de volumen o a nivel de esquema de base de datos.

¿Cuál es la diferencia entre los escaneos de mapeo y clasificación?

Puede realizar dos tipos de escaneos en Clasificación de datos:

- Los escaneos de solo mapeo brindan únicamente una descripción general de alto nivel de sus datos y se realizan en fuentes de datos seleccionadas. Los escaneos de solo mapeo toman menos tiempo que los escaneos de mapas y clasificación porque no acceden a los archivos para ver los datos dentro. Es posible que desees hacer esto inicialmente para identificar áreas de investigación y luego realizar un escaneo de Mapa y Clasificación en esas áreas.
- **Los escaneos de mapas y clasificación** proporcionan un escaneo de nivel profundo de sus datos.

La siguiente tabla muestra algunas de las diferencias:

Característica	Mapear y clasificar escaneos	Escaneos de solo mapeo
Velocidad de escaneo	Lento	Rápido
Precios	Gratis	Gratis
Capacidad	Limitado a 500 TiB*	Limitado a 500 TiB*
Lista de tipos de archivos y capacidad utilizada	Sí	Sí
Número de archivos y capacidad utilizada	Sí	Sí
Edad y tamaño de los archivos	Sí	Sí
Capacidad para ejecutar un"Informe de mapeo 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
Crear"consultas guardadas" que proporcionan resultados de búsqueda personalizados	Sí	No
Capacidad de ejecutar otros informes	Sí	No
Capacidad de ver metadatos de archivos**	No	Sí

* La clasificación de datos no impone un límite en la cantidad de datos que puede escanear. Cada agente de consola admite el escaneo y la visualización de 500 TiB de datos. Para escanear más de 500 TiB de datos,"instalar otro agente de consola" entonces"Implementar otra instancia de clasificación de datos" . + La interfaz de usuario de la consola muestra datos de un solo conector. Para obtener sugerencias sobre cómo ver datos de varios agentes de la consola, consulte"Trabajar con múltiples agentes de consola" .

** Los siguientes metadatos se extraen de los archivos durante los escaneos de mapeo:

- Sistema
- Tipo de sistema
- Repositorio de almacenamiento
- Tipo de archivo
- Capacidad utilizada
- Número de archivos

- Tamaño del archivo
- Creación de archivos
- Último acceso al archivo
- Archivo modificado por última vez
- Hora de descubrimiento del archivo
- Extracción de permisos

Diferencias en el panel de gobernanza:

Característica	Mapa y clasificación	Mapa
Datos obsoletos	Sí	Sí
Datos no comerciales	Sí	Sí
Archivos duplicados	Sí	Sí
Consultas guardadas predefinidas	Sí	No
Consultas guardadas predeterminadas	Sí	Sí
Informe de la DDA	Sí	Sí
Informe de mapeo	Sí	Sí
Detección del nivel de sensibilidad	Sí	No
Datos sensibles con amplios permisos	Sí	No
Permisos abiertos	Sí	Sí
La era de los datos	Sí	Sí
Tamaño de los datos	Sí	Sí
Categorías	Sí	No
Tipos de archivos	Sí	Sí

Diferencias en el panel de cumplimiento:

Característica	Mapa y clasificación	Mapa
Información personal	Sí	No
Información personal sensible	Sí	No
Informe de evaluación de riesgos de privacidad	Sí	No
Informe HIPAA	Sí	No
Informe PCI DSS	Sí	No

Diferencias en los filtros de investigación:

Característica	Mapa y clasificación	Mapa
Consultas guardadas	Sí	Sí
Tipo de sistema	Sí	Sí
Sistema	Sí	Sí
Repositorio de almacenamiento	Sí	Sí
Tipo de archivo	Sí	Sí
Tamaño del archivo	Sí	Sí
Hora de creación	Sí	Sí
Tiempo descubierto	Sí	Sí
Última modificación	Sí	Sí
Último acceso	Sí	Sí
Permisos abiertos	Sí	Sí
Ruta del directorio de archivos	Sí	Sí
Categoría	Sí	No
Nivel de sensibilidad	Sí	No
Número de identificadores	Sí	No
Datos personales	Sí	No
Datos personales sensibles	Sí	No
Titular de los datos	Sí	No
Duplicados	Sí	Sí
Estado de clasificación	Sí	El estado siempre es "Perspectivas limitadas"
Evento de análisis de escaneo	Sí	Sí
Hash de archivo	Sí	Sí
Número de usuarios con acceso	Sí	Sí
Permisos de usuario/grupo	Sí	Sí
Propietario del archivo	Sí	Sí
Tipo de directorio	Sí	Sí

Escanee Amazon FSx en busca de volúmenes ONTAP con la NetApp Data Classification

Complete unos pocos pasos para escanear Amazon FSx en busca de volúmenes ONTAP con NetApp Data Classification.

Antes de empezar

- Necesita un agente de consola activo en AWS para implementar y administrar la clasificación de datos.
- El grupo de seguridad que seleccionó al crear el sistema debe permitir el tráfico desde la instancia de Clasificación de datos. Puede encontrar el grupo de seguridad asociado utilizando el ENI conectado al sistema de archivos FSx para ONTAP y editarlo utilizando la Consola de administración de AWS.

  "Grupos de seguridad de AWS para instancias de Linux"

  "Grupos de seguridad de AWS para instancias de Windows"

  "Interfaces de red elásticas (ENI) de AWS"

- Asegúrese de que los siguientes puertos estén abiertos para la instancia de clasificación de datos:
  - Para NFS: puertos 111 y 2049.
  - Para CIFS: puertos 139 y 445.

Implementar la instancia de clasificación de datos

"Implementar la clasificación de datos"si aún no hay una instancia implementada.

Debe implementar la clasificación de datos en la misma red de AWS que el agente de consola para AWS y los volúmenes FSx que desea escanear.

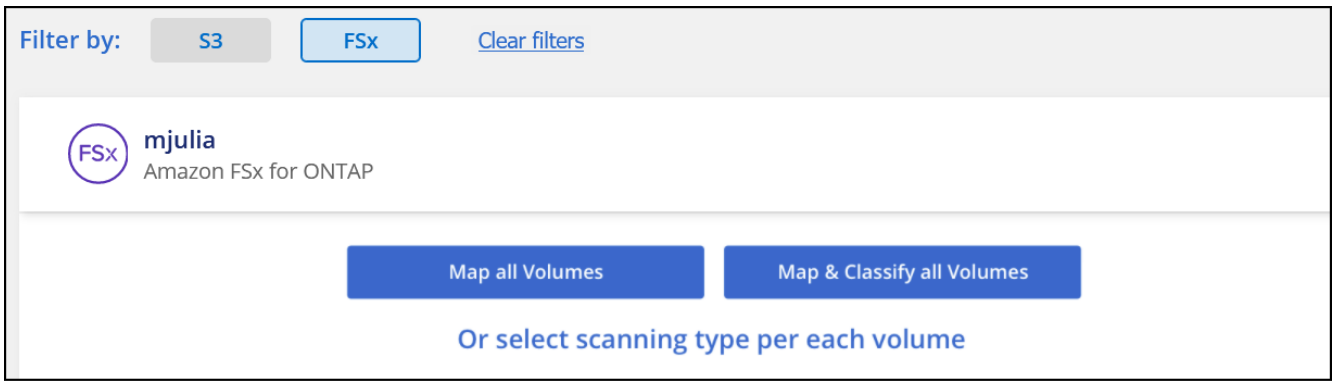
Nota: Actualmente, no se admite la implementación de la clasificación de datos en una ubicación local al escanear volúmenes FSx.

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

Habilite la clasificación de datos en sus sistemas

Puede habilitar la clasificación de datos para FSx para volúmenes ONTAP .

1. Desde la NetApp Console, **Gobernanza > Clasificación**.
2. Desde el menú Clasificación de datos, seleccione **Configuración**.



3. Seleccione cómo desea escanear los volúmenes en cada sistema. "Aprenda sobre escaneos de mapeo y clasificación":
   - Para mapear todos los volúmenes, seleccione **Mape todos los volúmenes**.

- Para mapear y clasificar todos los volúmenes, seleccione **Mapear y clasificar todos los volúmenes**.
- Para personalizar el escaneo para cada volumen, seleccione **O seleccione el tipo de escaneo para cada volumen** y luego elija los volúmenes que desea mapear y/o clasificar.

4. En el cuadro de diálogo de confirmación, seleccione **Aprobar** para que la Clasificación de datos comience a escanear sus volúmenes.

Resultado

La clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados estarán disponibles en el panel de Cumplimiento tan pronto como la Clasificación de Datos finalice los escaneos iniciales. El tiempo que lleva depende de la cantidad de datos: pueden ser unos minutos u horas. Puede seguir el progreso del escaneo inicial navegando al menú **Configuración** y luego seleccionando **Configuración del sistema**. Realice un seguimiento del progreso de cada escaneo en la barra de progreso; puede pasar el cursor sobre la barra de progreso para ver la cantidad de archivos escaneados en relación con el total de archivos en el volumen.

- De forma predeterminada, si la clasificación de datos no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos en sus volúmenes porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, seleccione **O seleccione el tipo de escaneo para cada volumen**. La página resultante tiene una configuración que puede habilitar para que la Clasificación de datos escanee los volúmenes independientemente de los permisos.
- La clasificación de datos escanea solo un recurso compartido de archivos bajo un volumen. Si tiene varias acciones en sus volúmenes, deberá escanear esas otras acciones por separado como un grupo de acciones. "Ver más detalles sobre esta limitación de clasificación de datos" .

Verificar que la clasificación de datos tenga acceso a los volúmenes

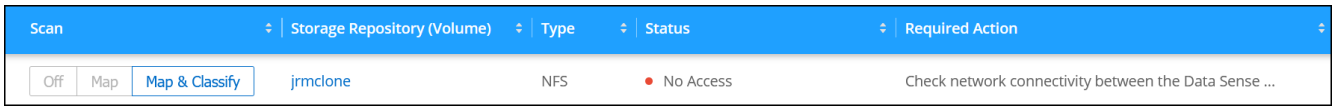
Asegúrese de que la clasificación de datos pueda acceder a los volúmenes verificando su red, grupos de seguridad y políticas de exportación.

Necesitará proporcionar a Data Classification las credenciales CIFS para que pueda acceder a los volúmenes CIFS.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. En la página de Configuración, seleccione **Ver detalles** para revisar el estado y corregir cualquier error.

   Por ejemplo, la siguiente imagen muestra un volumen que la clasificación de datos no puede escanear debido a problemas de conectividad de red entre la instancia de clasificación de datos y el volumen.



3. Asegúrese de que haya una conexión de red entre la instancia de clasificación de datos y cada red que incluya volúmenes para FSx para ONTAP.

   Para FSx para ONTAP, la clasificación de datos puede escanear volúmenes solo en la misma región que la consola.

4. Asegúrese de que las políticas de exportación de volumen NFS incluyan la dirección IP de la instancia de clasificación de datos para que pueda acceder a los datos de cada volumen.
5. Si utiliza CIFS, proporcione a Clasificación de datos credenciales de Active Directory para que pueda escanear volúmenes CIFS.

    a. Desde el menú Clasificación de datos, seleccione **Configuración**.

    b. Para cada sistema, seleccione **Editar credenciales CIFS** e ingrese el nombre de usuario y la contraseña que la clasificación de datos necesita para acceder a los volúmenes CIFS en el sistema.

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

        Si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de datos, se recomienda que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, configure el usuario de Active Directory como parte de un grupo principal en la organización que tenga permisos para todos los archivos.

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

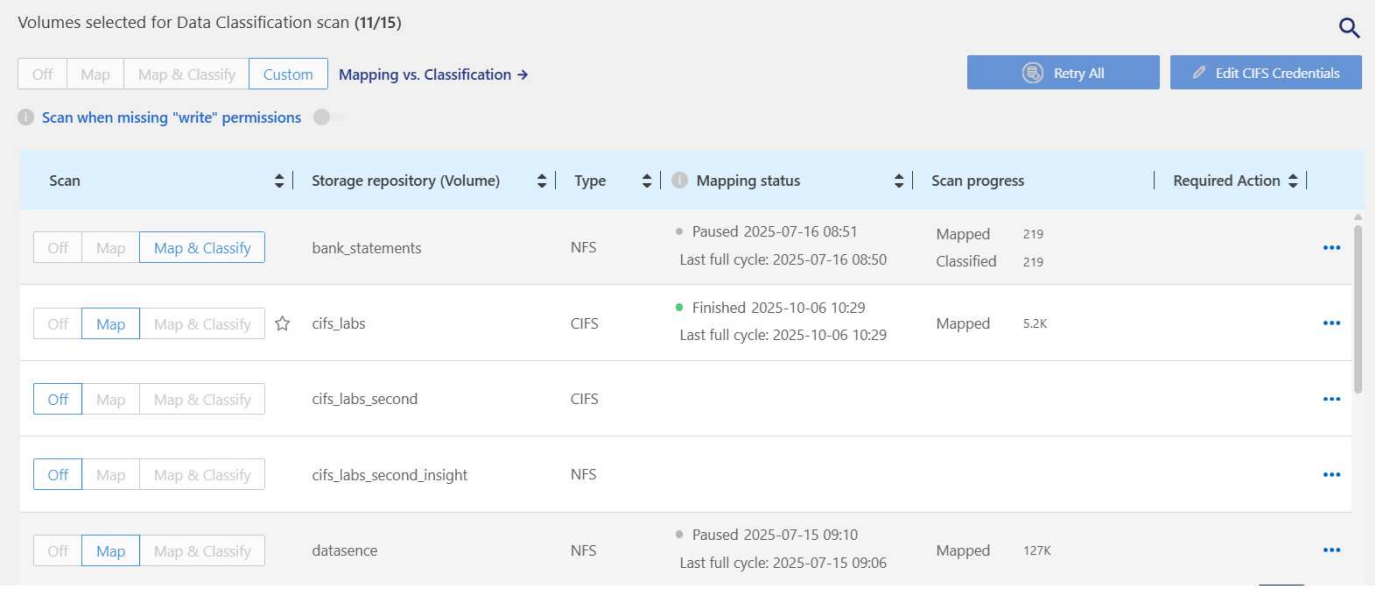
Habilitar y deshabilitar escaneos en volúmenes

Puede iniciar o detener análisis en cualquier sistema en cualquier momento desde la página de Configuración. También puede cambiar los escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa. Se recomienda escanear todos los volúmenes de un sistema.

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha seleccionado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando lo configure en **Personalizado** o **Desactivado** en el área de encabezado, deberá activar el mapeo y/o el escaneo completo en cada nuevo volumen que agregue al sistema.

El interruptor en la parte superior de la página para **Escanear cuando faltan permisos de "escritura"** está deshabilitado de manera predeterminada. Esto significa que si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, active el interruptor y se escanearán todos los archivos independientemente de los permisos. "Más información".

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha configurado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando la configuración para todos los volúmenes es **Personalizada** o **Desactivada**, deberá activar el escaneo manualmente para cada nuevo volumen que agregue.



Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione un sistema y luego seleccione **Configuración**.
3. Para habilitar o deshabilitar los escaneos para todos los volúmenes, seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** en el encabezado sobre todos los volúmenes.

   Para habilitar o deshabilitar los escaneos de volúmenes individuales, busque los volúmenes en la lista y luego seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** junto al nombre del volumen.

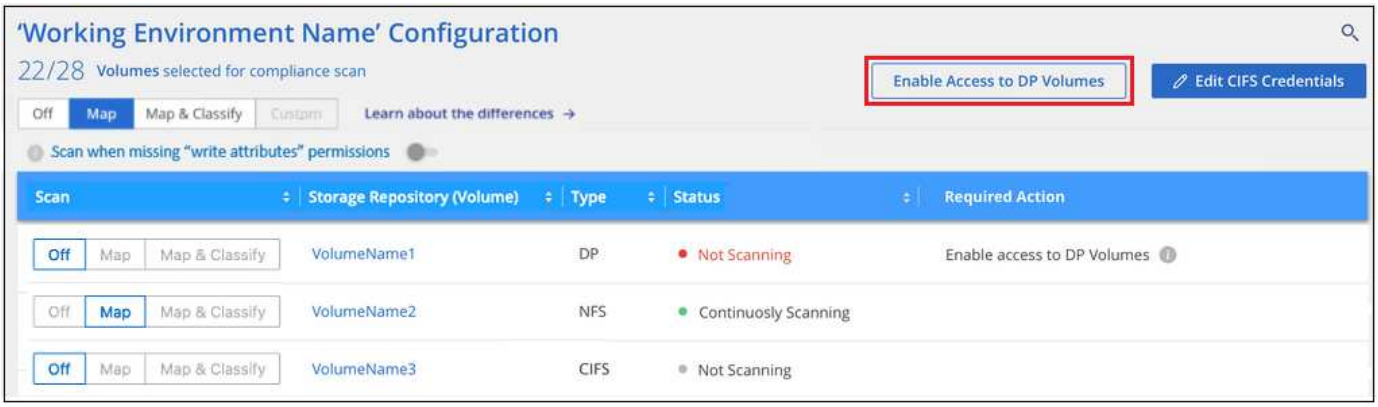
Resultado

Cuando habilita el escaneo, la clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados comienzan a aparecer en el panel de Cumplimiento tan pronto como la Clasificación de datos inicia el escaneo. El tiempo de finalización del escaneo depende de la cantidad de datos y puede variar entre minutos y horas.

Escanear volúmenes de protección de datos

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

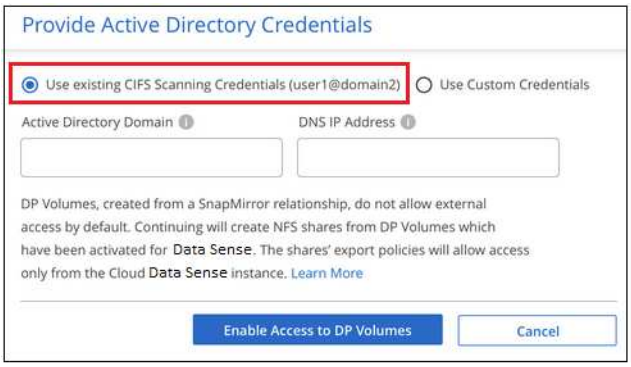
Inicialmente, la lista de volúmenes identifica estos volúmenes como *Tipo* **DP** con el *Estado* **No escaneando** y la *Acción requerida* **Habilitar acceso a volúmenes DP**.

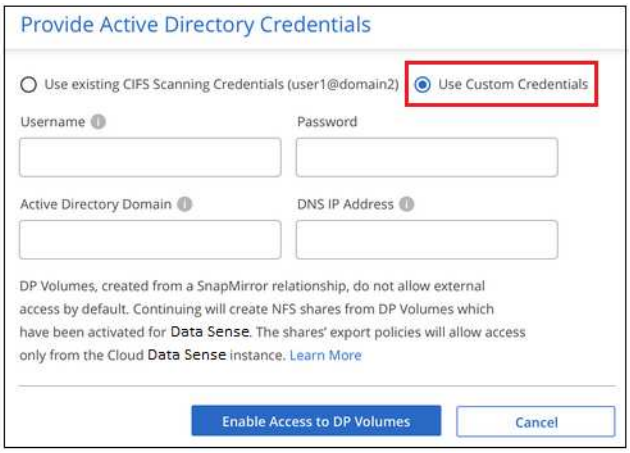


Pasos

Si desea escanear estos volúmenes de protección de datos:

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione **Habilitar acceso a volúmenes DP** en la parte superior de la página.
3. Revise el mensaje de confirmación y seleccione **Habilitar acceso a volúmenes DP** nuevamente.
   - Se habilitan los volúmenes que se crearon inicialmente como volúmenes NFS en el sistema de archivos de origen FSx para ONTAP .
   - Los volúmenes que se crearon inicialmente como volúmenes CIFS en el sistema de archivos de origen FSx para ONTAP requieren que ingrese credenciales CIFS para escanear esos volúmenes DP. Si ya ingresó las credenciales de Active Directory para que la Clasificación de datos pueda escanear volúmenes CIFS, puede usar esas credenciales o puede especificar un conjunto diferente de credenciales de administrador.





4. Active cada volumen DP que desee escanear.

Resultado

Una vez habilitada, la clasificación de datos crea un recurso compartido NFS de cada volumen DP que se activó para el escaneo. Las políticas de exportación de acciones solo permiten el acceso desde la instancia de Clasificación de datos.

Si no tenía volúmenes de protección de datos CIFS cuando habilitó inicialmente el acceso a los volúmenes DP y luego agregó algunos, el botón **Habilitar acceso a CIFS DP** aparece en la parte superior de la página de Configuración. Seleccione este botón y agregue credenciales CIFS para habilitar el acceso a estos volúmenes DP CIFS.

Las credenciales de Active Directory se registran solo en la VM de almacenamiento del primer volumen DP CIFS, por lo que se escanearán todos los volúmenes DP en esa SVM. Cualquier volumen que resida en otras SVM no tendrá las credenciales de Active Directory registradas, por lo que esos volúmenes de DP no se escanearán.

Escanee volúmenes de Azure NetApp Files con NetApp Data Classification

Complete unos pocos pasos para comenzar a utilizar NetApp Data Classification para Azure NetApp Files.

Descubra el sistema de Azure NetApp Files que desea escanear

Si el sistema de Azure NetApp Files que desea escanear aún no se encuentra en la NetApp Console como sistema,"agréguelo en la página de Sistemas" .

Implementar la instancia de clasificación de datos

"Implementar la clasificación de datos"si aún no hay una instancia implementada.

La clasificación de datos debe implementarse en la nube al escanear volúmenes de Azure NetApp Files y debe implementarse en la misma región que los volúmenes que desea escanear.

Nota: Actualmente, no se admite la implementación de la clasificación de datos en una ubicación local al escanear volúmenes de Azure NetApp Files .

Habilite la clasificación de datos en sus sistemas

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

1. Desde el menú Clasificación de datos, seleccione **Configuración**.

2. Seleccione cómo desea escanear los volúmenes en cada sistema. "Aprenda sobre escaneos de mapeo y clasificación":
   - Para mapear todos los volúmenes, seleccione **Mape todos los volúmenes**.
   - Para mapear y clasificar todos los volúmenes, seleccione **Mapear y clasificar todos los volúmenes**.
   - Para personalizar el escaneo de cada volumen, seleccione **O seleccione el tipo de escaneo para cada volumen** y luego elija los volúmenes que desea mapear o mapear y clasificar.

     VerHabilitar o deshabilitar escaneos en volúmenes Para más detalles.

3. En el cuadro de diálogo de confirmación, seleccione **Aprobar**.

Resultado

La clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados están disponibles en el panel de Cumplimiento tan pronto como la Clasificación de datos finaliza los escaneos iniciales. El tiempo que lleva depende de la cantidad de datos: pueden ser unos minutos u horas. Puede seguir el progreso del escaneo inicial navegando al menú **Configuración** y luego seleccionando **Configuración del sistema**. La clasificación de datos muestra una barra de progreso para cada escaneo. Puede pasar el cursor sobre la barra de progreso para ver la cantidad de archivos escaneados en relación con la cantidad total de archivos en el volumen.

- De forma predeterminada, si la clasificación de datos no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos en sus volúmenes porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, seleccione **O seleccione el tipo de escaneo para cada volumen**. La página resultante tiene una configuración que puede habilitar para que la Clasificación de datos escanee los volúmenes independientemente de los permisos.
- La clasificación de datos escanea solo un recurso compartido de archivos bajo un volumen. Si tiene varias acciones en sus volúmenes, deberá escanear esas otras acciones por separado como un grupo de acciones. "Conozca esta limitación de clasificación de datos" .

Verificar que la clasificación de datos tenga acceso a los volúmenes

Asegúrese de que la clasificación de datos pueda acceder a los volúmenes verificando su red, grupos de seguridad y políticas de exportación. Debe proporcionar a la clasificación de datos credenciales CIFS para que pueda acceder a los volúmenes CIFS.

Para Azure NetApp Files, la clasificación de datos solo puede escanear volúmenes en la misma región que la consola.

Lista de verificación

- Asegúrese de que haya una conexión de red entre la instancia de Clasificación de datos y cada red que incluya volúmenes para Azure NetApp Files.
- Asegúrese de que los siguientes puertos estén abiertos para la instancia de clasificación de datos:
  - Para NFS: puertos 111 y 2049.
  - Para CIFS: puertos 139 y 445.
- Asegúrese de que las políticas de exportación de volumen NFS incluyan la dirección IP de la instancia de clasificación de datos para que pueda acceder a los datos de cada volumen.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.

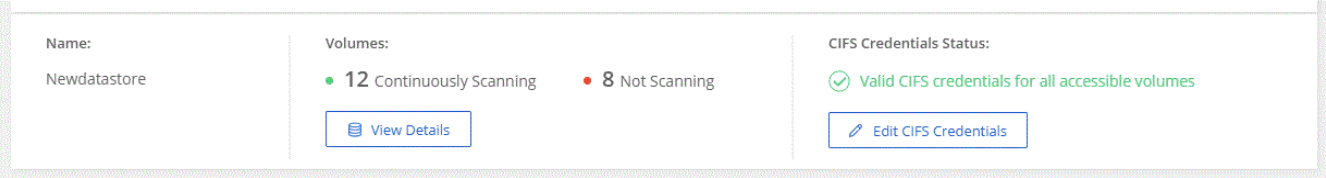
   a. Si utiliza CIFS (SMB), asegúrese de que las credenciales de Active Directory sean correctas. Para cada sistema, seleccione **Editar credenciales CIFS** y luego ingrese el nombre de usuario y la contraseña que la clasificación de datos necesita para acceder a los volúmenes CIFS en el sistema.

      Las credenciales pueden ser de solo lectura; proporcionar credenciales de administrador garantiza que Data Classification pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de datos.

      Si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de datos, se recomienda que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, configure el usuario de

Active Directory como parte de un grupo principal en la organización que tenga permisos para todos los archivos.

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



2. En la página de Configuración, seleccione **Ver detalles** para revisar el estado de cada volumen CIFS y NFS. Si es necesario, corrija cualquier error como problemas de conectividad de red.

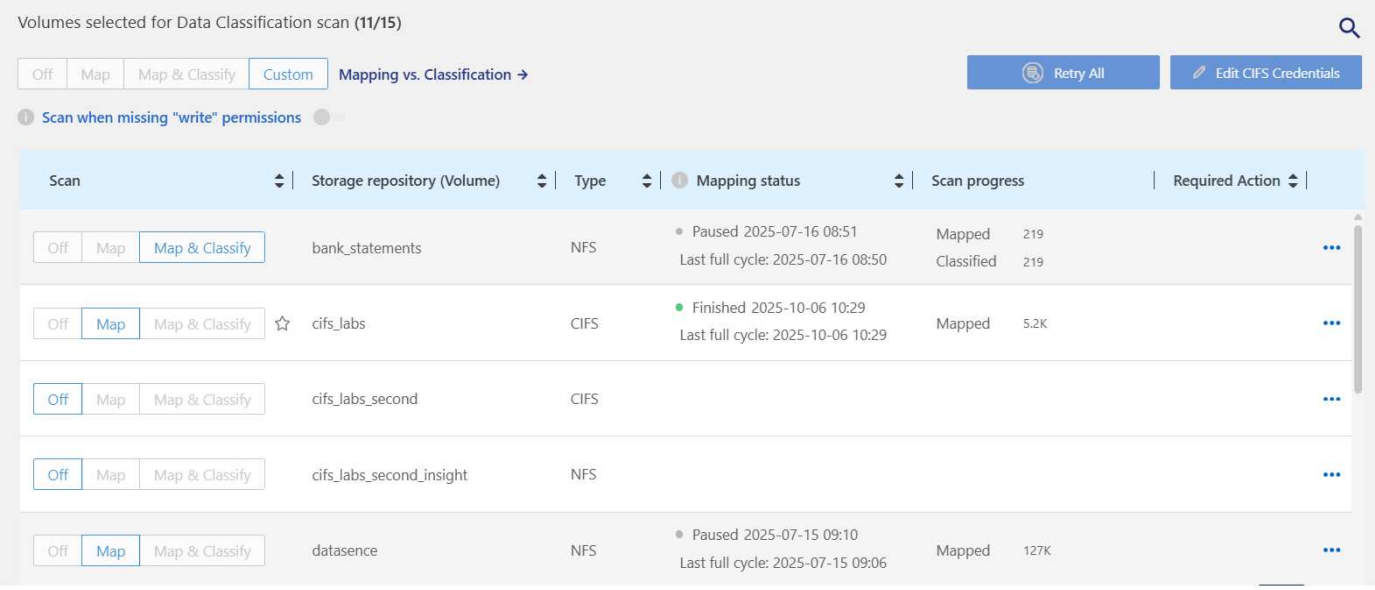
Habilitar o deshabilitar escaneos en volúmenes

Puede iniciar o detener análisis en cualquier sistema en cualquier momento desde la página de Configuración. También puede cambiar los escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa. Se recomienda escanear todos los volúmenes de un sistema.

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha seleccionado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando lo configure en **Personalizado** o **Desactivado** en el área de encabezado, deberá activar el mapeo y/o el escaneo completo en cada nuevo volumen que agregue al sistema.

El interruptor en la parte superior de la página para **Escanear cuando faltan permisos de "escritura"** está deshabilitado de manera predeterminada. Esto significa que si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, active el interruptor y se escanearán todos los archivos independientemente de los permisos. "Más información".

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha configurado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando la configuración para todos los volúmenes es **Personalizada** o **Desactivada**, deberá activar el escaneo manualmente para cada nuevo volumen que agregue.



Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione un sistema y luego seleccione **Configuración**.
3. Para habilitar o deshabilitar los escaneos para todos los volúmenes, seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** en el encabezado sobre todos los volúmenes.

   Para habilitar o deshabilitar los escaneos de volúmenes individuales, busque los volúmenes en la lista y luego seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** junto al nombre del volumen.

Resultado

Cuando habilita el escaneo, la clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados comienzan a aparecer en el panel de Cumplimiento tan pronto como la Clasificación de datos inicia el escaneo. El tiempo de finalización del escaneo depende de la cantidad de datos y puede variar entre minutos y horas.

Escanee Cloud Volumes ONTAP y volúmenes ONTAP locales con NetApp Data Classification

Complete unos pocos pasos para comenzar a escanear sus Cloud Volumes ONTAP y volúmenes ONTAP locales utilizando NetApp Data Classification.

Prerrequisitos

Antes de habilitar la Clasificación de datos, asegúrese de tener una configuración compatible.

- Si está escaneando Cloud Volumes ONTAP y sistemas ONTAP locales a los que se puede acceder a través de Internet, puede"Implementar la clasificación de datos en la nube" o"En una ubicación local que tenga acceso a Internet" .
- Si está escaneando sistemas ONTAP locales que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe"Implementar la clasificación de datos en la misma ubicación local que no tiene acceso a Internet" . Esto requiere que el agente de consola se implemente en la misma ubicación local.

Verificar que la clasificación de datos tenga acceso a los volúmenes

Asegúrese de que la clasificación de datos pueda acceder a los volúmenes verificando su red, grupos de seguridad y políticas de exportación. Necesitará proporcionar a Data Classification las credenciales CIFS para que pueda acceder a los volúmenes CIFS.

Lista de verificación

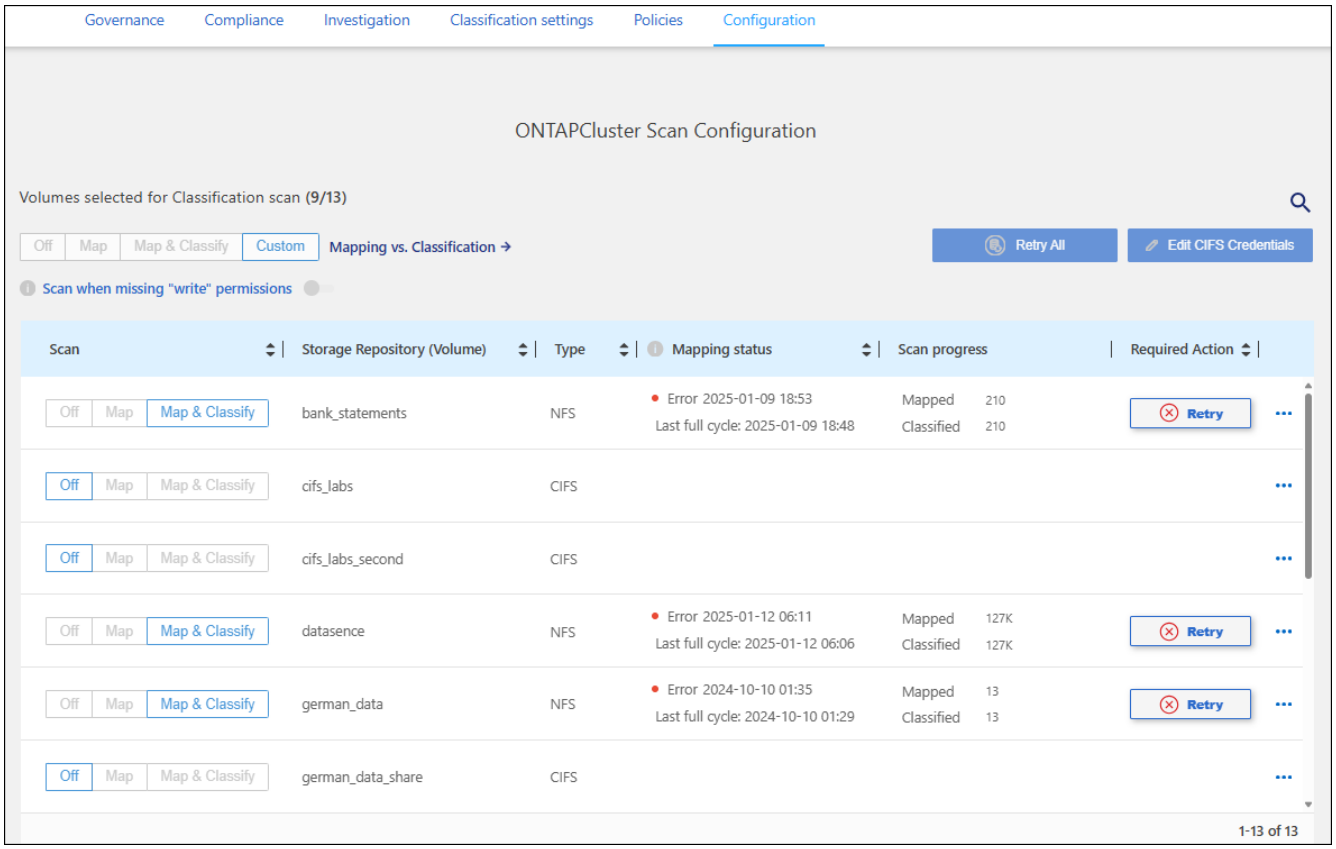
- Asegúrese de que haya una conexión de red entre la instancia de clasificación de datos y cada red que incluya volúmenes para Cloud Volumes ONTAP o clústeres ONTAP locales.
- Asegúrese de que el grupo de seguridad de Cloud Volumes ONTAP permita el tráfico entrante desde la instancia de clasificación de datos.

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

- Asegúrese de que las políticas de exportación de volumen NFS incluyan la dirección IP de la instancia de clasificación de datos para que pueda acceder a los datos de cada volumen.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.



2. Si utiliza CIFS, proporcione a Clasificación de datos credenciales de Active Directory para que pueda escanear volúmenes CIFS. Para cada sistema, seleccione **Editar credenciales CIFS** e ingrese el nombre de usuario y la contraseña que la clasificación de datos necesita para acceder a los volúmenes CIFS en el sistema.

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

Si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de datos, se recomienda que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, configure el usuario de Active Directory como parte de un grupo principal en la organización que tenga permisos para todos los archivos.

Si ingresó las credenciales correctamente, un mensaje confirmará que todos los volúmenes CIFS se autenticaron exitosamente.

3. En la página Configuración, seleccione **Configuración** para revisar el estado de cada volumen CIFS y NFS y corregir cualquier error.

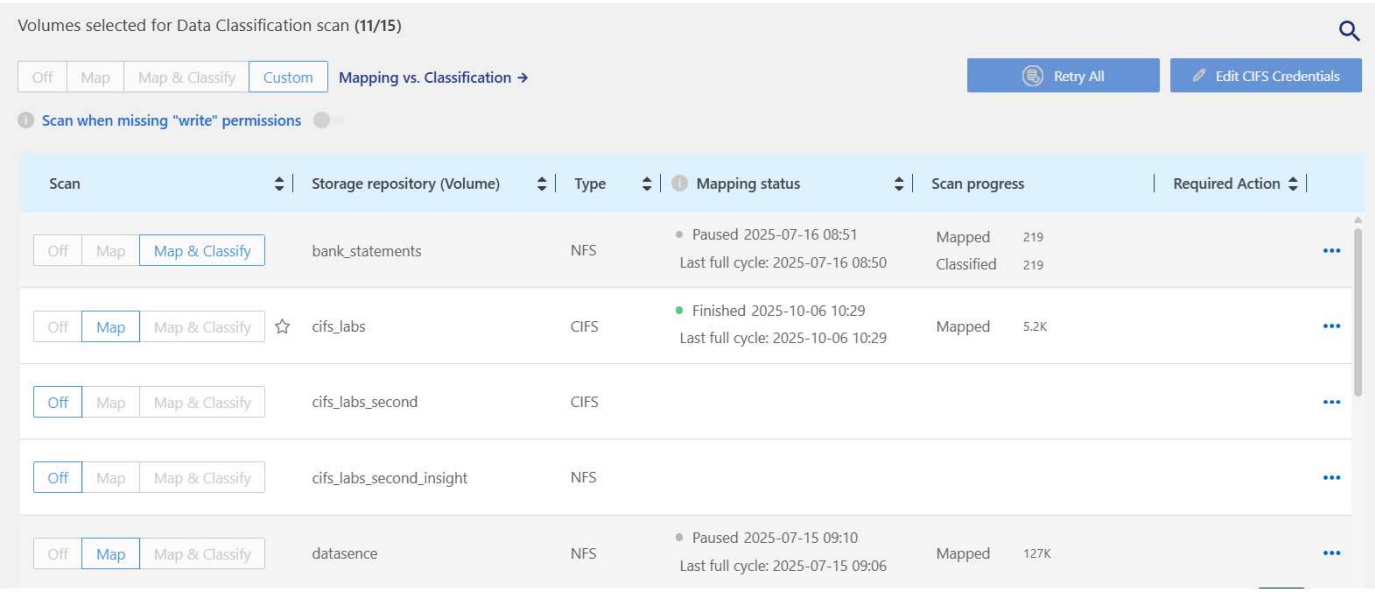
Habilitar o deshabilitar escaneos en volúmenes

Puede iniciar o detener análisis en cualquier sistema en cualquier momento desde la página de Configuración. También puede cambiar los escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa. Se recomienda escanear todos los volúmenes de un sistema.

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha seleccionado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando lo configure en **Personalizado** o **Desactivado** en el área de encabezado, deberá activar el mapeo y/o el escaneo completo en cada nuevo volumen que agregue al sistema.

El interruptor en la parte superior de la página para **Escanear cuando faltan permisos de "escritura"** está deshabilitado de manera predeterminada. Esto significa que si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, active el interruptor y se escanearán todos los archivos independientemente de los permisos. "Más información".

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha configurado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando la configuración para todos los volúmenes es **Personalizada** o **Desactivada**, deberá activar el escaneo manualmente para cada nuevo volumen que agregue.



Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione un sistema y luego seleccione **Configuración**.
3. Para habilitar o deshabilitar los escaneos para todos los volúmenes, seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** en el encabezado sobre todos los volúmenes.

   Para habilitar o deshabilitar los escaneos de volúmenes individuales, busque los volúmenes en la lista y luego seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** junto al nombre del volumen.

Resultado

Cuando habilita el escaneo, la clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados comienzan a aparecer en el panel de Cumplimiento tan pronto como la Clasificación de datos inicia el escaneo. El tiempo de finalización del escaneo depende de la cantidad de datos y puede variar entre minutos y horas.

La clasificación de datos escanea solo un recurso compartido de archivos bajo un volumen. Si tiene varias acciones en sus volúmenes, deberá escanear esas otras acciones por separado como un grupo de acciones. "Ver más detalles sobre esta limitación de clasificación de datos" .

Escanee esquemas de bases de datos con NetApp Data Classification

Complete unos pocos pasos para comenzar a escanear sus esquemas de base de datos con NetApp Data Classification.

Revisar los prerrequisitos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar la Clasificación de datos.

Bases de datos compatibles

La clasificación de datos puede escanear esquemas de las siguientes bases de datos:

- Servicio de base de datos relacional de Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oráculo
- PostgreSQL
- SAP HANA
- Servidor SQL (MSSQL)

La función de recopilación de estadísticas **debe estar habilitada** en la base de datos.

Requisitos de la base de datos

Se puede escanear cualquier base de datos con conectividad a la instancia de Clasificación de Datos, independientemente de dónde esté alojada. Solo necesitas la siguiente información para conectarte 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 acceso de lectura a los esquemas

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

Para MongoDB, se requiere un rol de administrador de solo lectura.

Implementar la instancia de clasificación de datos

Implementar la clasificación de datos si aún no hay una instancia implementada.

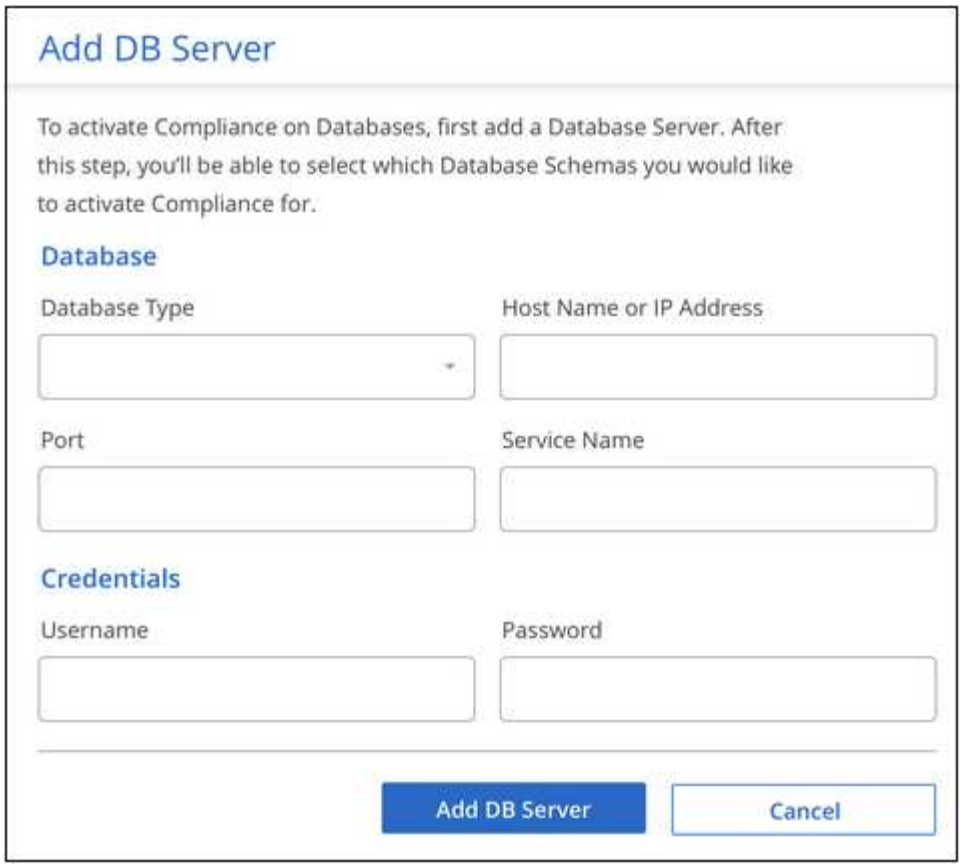
Si está escaneando esquemas de bases de datos a los que se puede acceder a través de Internet, puede"Implementar la clasificación de datos en la nube" o"Implementar la clasificación de datos en una ubicación local que tenga acceso a Internet" .

Si está escaneando esquemas de bases de datos que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe"Implementar la clasificación de datos en la misma ubicación local que no tiene acceso a Internet" . Esto también requiere que el agente de consola esté implementado en esa misma ubicación local.

Agregar el servidor de base de datos

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

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la página de Configuración, seleccione **Agregar sistema** > **Agregar servidor de base de datos**.
3. Ingrese la información requerida para identificar el servidor de base de datos.
   a. Seleccione el tipo de base de datos.
   b. Introduzca el puerto y el nombre de host o dirección IP para conectarse a la base de datos.
   c. Para las bases de datos Oracle, ingrese el nombre del servicio.
   d. Introduzca las credenciales para que Clasificación de Datos pueda acceder al servidor.
   e. Seleccione **Agregar servidor de base de datos**.



La base de datos se agrega a la lista de sistemas.

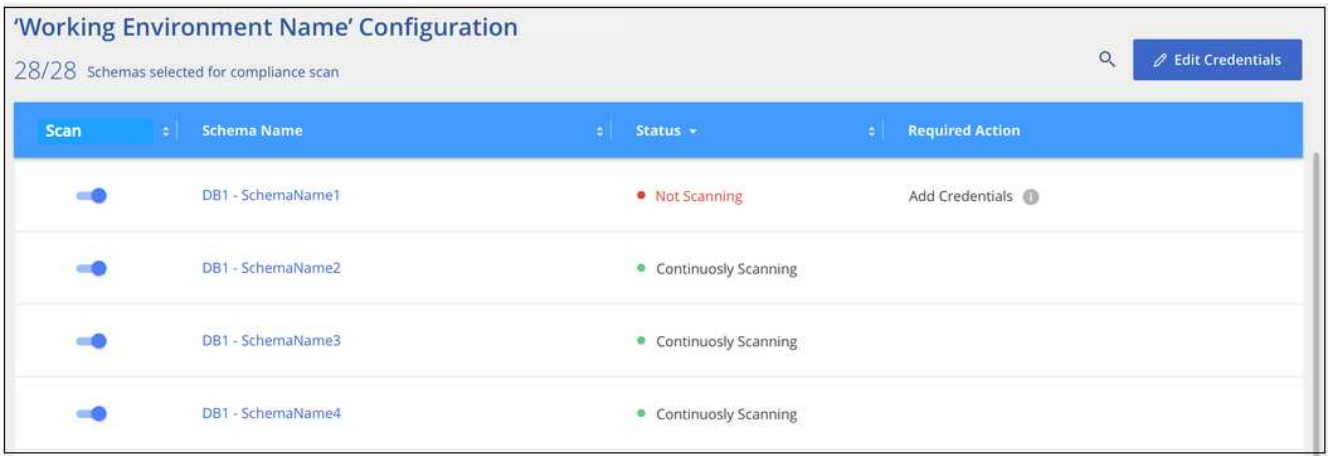
Habilitar y deshabilitar escaneos en esquemas de bases de datos

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

No existe ninguna opción para seleccionar escaneos de solo mapeo para esquemas de base de datos.

1. Desde la página de Configuración, seleccione el botón **Configuración** para la base de datos que desea configurar.

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



Resultado

La clasificación de datos comienza a escanear los esquemas de base de datos que usted habilitó. Puede seguir el progreso del escaneo inicial navegando al menú **Configuración** y luego seleccionando **Configuración del sistema**. El progreso de cada escaneo se muestra como una barra de progreso. También puede pasar el cursor sobre la barra de progreso para ver la cantidad de archivos escaneados en relación con la cantidad total de archivos en el volumen. Si hay algún error, aparecerá en la columna Estado, junto con las acciones necesarias para solucionarlo.

La clasificación de datos escanea sus bases de datos una vez al día; las bases de datos no se escanean continuamente como otras fuentes de datos.

Escanee Google Cloud NetApp Volumes con la NetApp Data Classification

NetApp Data Classification admite Google Cloud NetApp Volumes como sistema. Aprenda a escanear su sistema Google Cloud NetApp Volumes .

Descubra el sistema Google Cloud NetApp Volumes que desea escanear

Si el sistema de Google Cloud NetApp Volumes que desea escanear aún no se encuentra en la NetApp Console como sistema,"agréguelo a la página de Sistemas" .

Implementar la instancia de clasificación de datos

"Implementar la clasificación de datos"si aún no hay una instancia implementada.

La clasificación de datos debe implementarse en la nube al escanear Google Cloud NetApp Volumes y debe implementarse en la misma región que los volúmenes que desea escanear.

Nota: Actualmente, no se admite la implementación de la clasificación de datos en una ubicación local al escanear Google Cloud NetApp Volumes.

Habilite la clasificación de datos en sus sistemas

Puede habilitar la clasificación de datos en su sistema Google Cloud NetApp Volumes .

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione cómo desea escanear los volúmenes en cada sistema. "Aprenda sobre escaneos de mapeo y clasificación":

- Para mapear todos los volúmenes, seleccione **Mape todos los volúmenes**.
- Para mapear y clasificar todos los volúmenes, seleccione **Mapear y clasificar todos los volúmenes**.
- Para personalizar el escaneo para cada volumen, seleccione **O seleccione el tipo de escaneo para cada volumen** y luego elija los volúmenes que desea mapear y/o clasificar.

  VerHabilitar y deshabilitar escaneos en volúmenes Para más detalles.

3. En el cuadro de diálogo de confirmación, seleccione **Aprobar**.

Resultado

La clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados están disponibles en el panel de Cumplimiento tan pronto como la Clasificación de datos finaliza los escaneos iniciales. El tiempo que tarda depende de la cantidad de datos: desde unos minutos hasta unas horas. Puede seguir el progreso del escaneo inicial en la sección **Configuración del sistema** del menú **Configuración**. La clasificación de datos muestra una barra de progreso para cada escaneo. También puede pasar el cursor sobre la barra de progreso para ver la cantidad de archivos escaneados en relación con el total de archivos en el volumen.

- De forma predeterminada, si la clasificación de datos no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos en sus volúmenes porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, seleccione **O seleccione el tipo de escaneo para cada volumen**. La página resultante tiene una configuración que puede habilitar para que la Clasificación de datos escanee los volúmenes independientemente de los permisos.
- La clasificación de datos escanea solo un recurso compartido de archivos bajo un volumen. Si tiene varias acciones en sus volúmenes, deberá escanear esas otras acciones por separado como un grupo de acciones. "Conozca esta limitación de clasificación de datos".

Verificar que la clasificación de datos tenga acceso a los volúmenes

Asegúrese de que la clasificación de datos pueda acceder a los volúmenes verificando su red, grupos de seguridad y políticas de exportación. Para los volúmenes CIFS, debe proporcionar Clasificación de datos con credenciales CIFS.

Para los Google Cloud NetApp Volumes, la clasificación de datos solo puede escanear volúmenes en la misma región que la consola.

Lista de verificación

- Asegúrese de que haya una conexión de red entre la instancia de Clasificación de datos y cada red que incluya volúmenes para Google Cloud NetApp Volumes.
- Asegúrese de que los siguientes puertos estén abiertos para la instancia de clasificación de datos:
  - Para NFS: puertos 111 y 2049.
  - Para CIFS: puertos 139 y 445.
- Asegúrese de que las políticas de exportación de volumen NFS incluyan la dirección IP de la instancia de clasificación de datos para que pueda acceder a los datos de cada volumen.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.

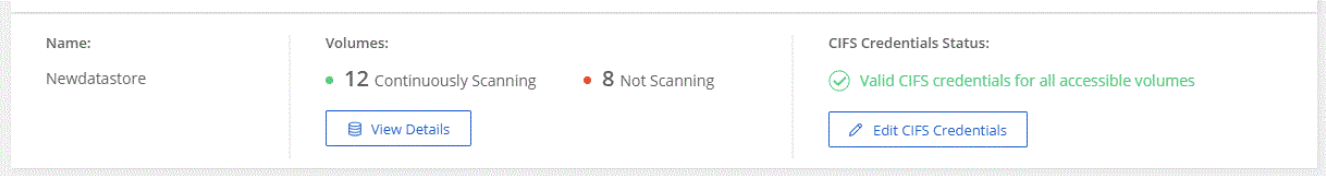
   a. Si utiliza CIFS (SMB), asegúrese de que las credenciales de Active Directory sean correctas. Para

cada sistema, seleccione **Editar credenciales CIFS** y luego ingrese el nombre de usuario y la contraseña que la clasificación de datos necesita para acceder a los volúmenes CIFS en el sistema.

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

Si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de datos, se recomienda que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, configure el usuario de Active Directory como parte de un grupo principal en la organización que tenga permisos para todos los archivos.

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



2. En la página de Configuración, seleccione **Ver detalles** para revisar el estado de cada volumen CIFS y NFS y corregir cualquier error.

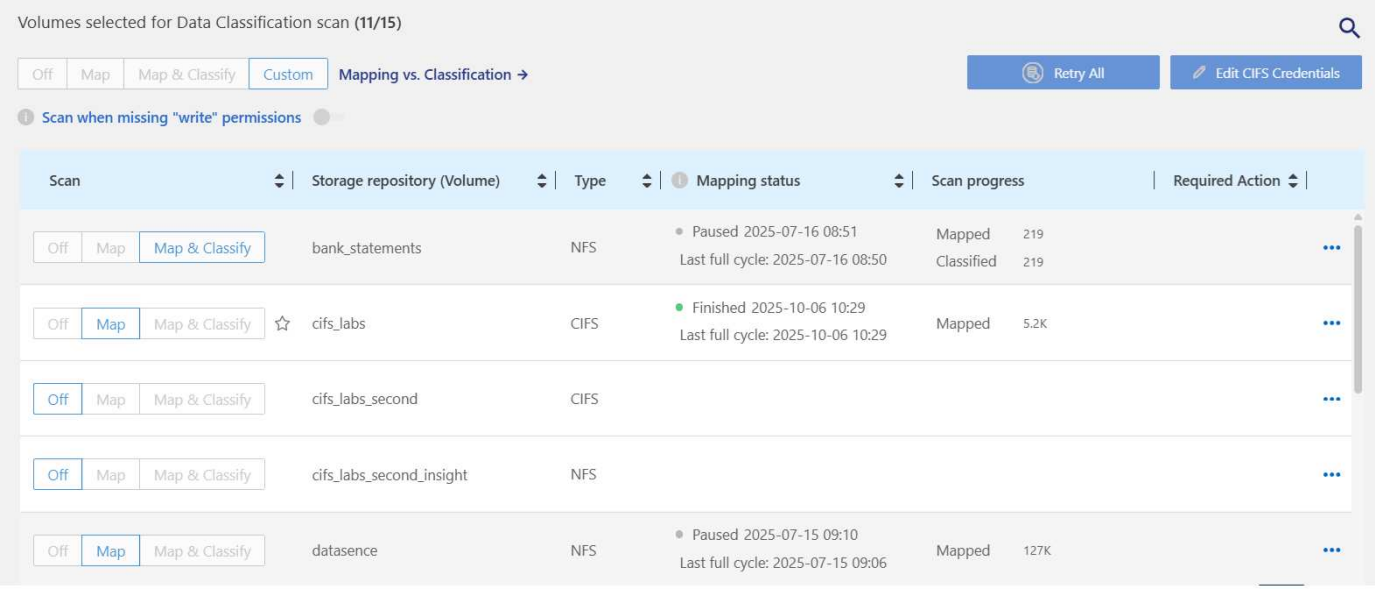
Habilitar y deshabilitar escaneos en volúmenes

Puede iniciar o detener análisis en cualquier sistema en cualquier momento desde la página de Configuración. También puede cambiar los escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa. Se recomienda escanear todos los volúmenes de un sistema.

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha seleccionado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando lo configure en **Personalizado** o **Desactivado** en el área de encabezado, deberá activar el mapeo y/o el escaneo completo en cada nuevo volumen que agregue al sistema.

El interruptor en la parte superior de la página para **Escanear cuando faltan permisos de "escritura"** está deshabilitado de manera predeterminada. Esto significa que si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. Si no le importa si se restablece el último tiempo de acceso, active el interruptor y se escanearán todos los archivos independientemente de los permisos. "Más información".

Los nuevos volúmenes agregados al sistema se escanean automáticamente solo cuando usted ha configurado la configuración **Mapa** o **Mapa y clasificar** en el área de encabezado. Cuando la configuración para todos los volúmenes es **Personalizada** o **Desactivada**, deberá activar el escaneo manualmente para cada nuevo volumen que agregue.



Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione un sistema y luego seleccione **Configuración**.
3. Para habilitar o deshabilitar los escaneos para todos los volúmenes, seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** en el encabezado sobre todos los volúmenes.

   Para habilitar o deshabilitar los escaneos de volúmenes individuales, busque los volúmenes en la lista y luego seleccione **Mapa**, **Mapa y clasificar** o **Desactivado** junto al nombre del volumen.

Resultado

Cuando habilita el escaneo, la clasificación de datos comienza a escanear los volúmenes que seleccionó en el sistema. Los resultados comienzan a aparecer en el panel de Cumplimiento tan pronto como la Clasificación de datos inicia el escaneo. El tiempo de finalización del escaneo depende de la cantidad de datos y puede variar entre minutos y horas.

Escanee recursos compartidos de archivos con NetApp Data Classification

Para escanear recursos compartidos de archivos, primero debe crear un grupo de recursos compartidos de archivos en NetApp Data Classification. Los grupos de recursos compartidos de archivos son para recursos compartidos NFS o CIFS (SMB) alojados localmente o en la nube.

La versión principal de Clasificación de datos no admite el escaneo de datos de recursos compartidos de archivos que no sean de NetApp .

Prerrequisitos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar la Clasificación de datos.

- Las acciones se pueden alojar en cualquier lugar, incluso en la nube o en las instalaciones locales. Los recursos compartidos CIFS de sistemas de almacenamiento NetApp 7-Mode más antiguos se pueden escanear como recursos compartidos de archivos.

- La clasificación de datos no puede extraer permisos ni la "hora del último acceso" de los sistemas 7-Mode.
- Debido a un problema conocido entre algunas versiones de Linux y los recursos compartidos CIFS en sistemas 7-Mode, debe configurar el recurso compartido para usar solo SMBv1 con la autenticación NTLM habilitada.

- Debe haber conectividad de red entre la instancia de clasificación de datos y los recursos compartidos.
- Puede agregar un recurso compartido DFS (sistema de archivos distribuido) como un recurso compartido CIFS normal. Debido a que la clasificación de datos no sabe que el recurso compartido está construido sobre múltiples servidores/volúmenes combinados como un único recurso compartido CIFS, es posible que reciba errores de permiso o conectividad acerca del recurso compartido cuando el mensaje en realidad solo se aplica a una de las carpetas/recursos compartidos que se encuentra en un servidor/volumen diferente.
- Para los recursos compartidos CIFS (SMB), asegúrese de tener credenciales de Active Directory que proporcionen acceso de lectura a los recursos compartidos. Se prefieren las credenciales de administrador en caso de que la clasificación de datos necesite escanear datos que requieran permisos elevados.

  Si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de datos, se recomienda que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, configure el usuario de Active Directory como parte de un grupo principal en la organización que tenga permisos para todos los archivos.

- Todos los recursos compartidos de archivos CIFS de un grupo deben utilizar las mismas credenciales de Active Directory.
- Puede combinar recursos compartidos NFS y CIFS (utilizando Kerberos o NTLM). Debes agregar las acciones al grupo por separado. Es decir, debes completar el proceso dos veces: una por protocolo.
  - No se puede crear un grupo de recursos compartidos de archivos que combine tipos de autenticación CIFS (Kerberos y NTLM).
- Si utiliza CIFS con autenticación Kerberos, asegúrese de que la dirección IP proporcionada sea accesible para la clasificación de datos. No se pueden agregar archivos compartidos si la dirección IP no es accesible.

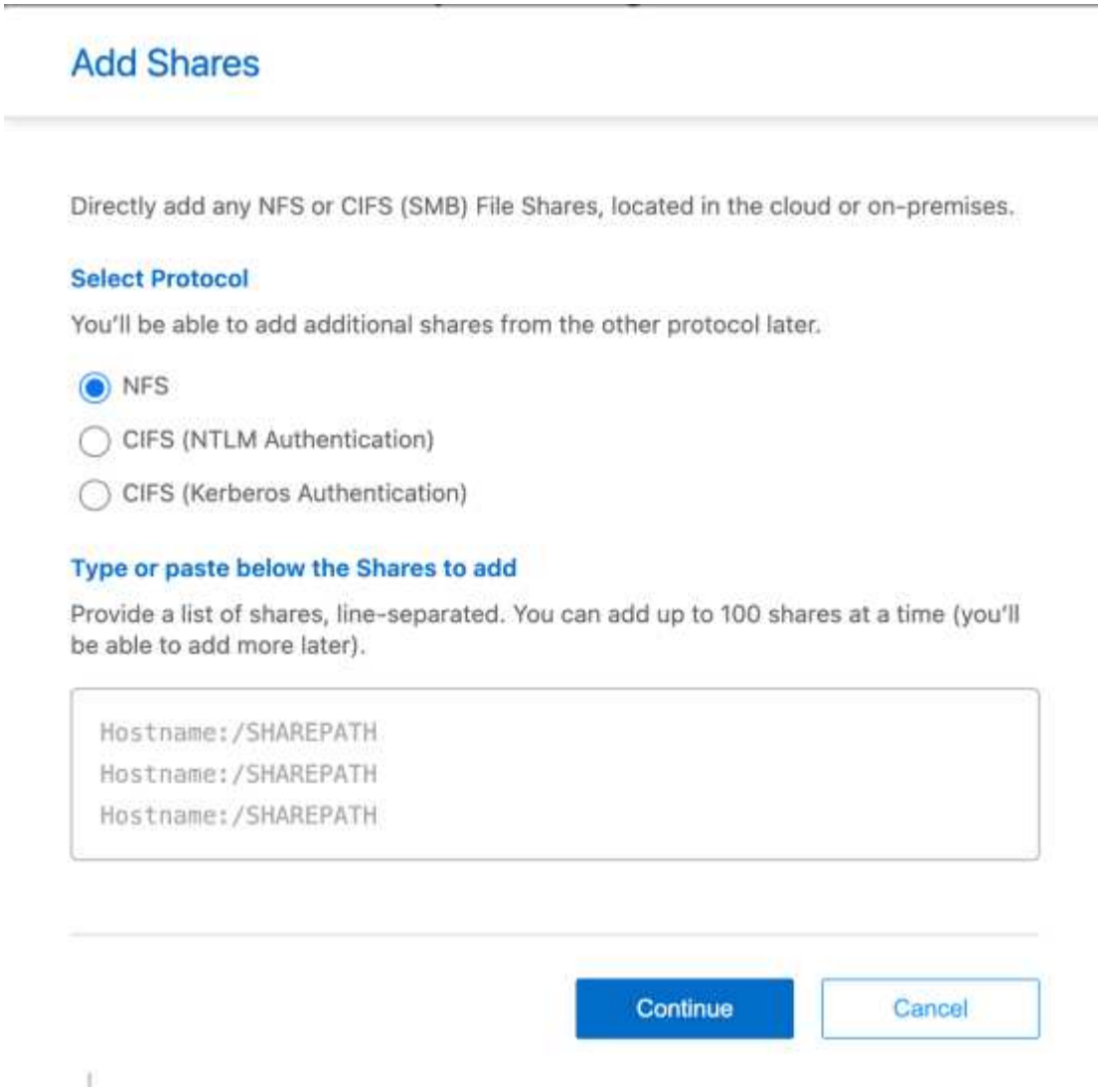
Crear un grupo de recursos compartidos de archivos

Cuando agregue recursos compartidos de archivos al grupo, debe utilizar el formato `<host_name>:/<share_path>`.

Puede agregar recursos compartidos de archivos individualmente o puede ingresar una lista separada por líneas de los recursos compartidos de archivos que desea escanear. Puedes agregar hasta 100 acciones a la vez.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la página de Configuración, seleccione **Agregar sistema** > **Agregar grupo de recursos compartidos de archivos**.
3. En el cuadro de diálogo Agregar grupo de recursos compartidos de archivos, ingrese el nombre del grupo de recursos compartidos y luego seleccione **Continuar**.
4. Seleccione el protocolo para los recursos compartidos de archivos que está agregando.



a. Si está agregando recursos compartidos CIFS con autenticación NTLM, ingrese las credenciales de Active Directory para acceder a los volúmenes CIFS. Aunque se admiten credenciales de solo lectura, se recomienda proporcionar acceso completo con credenciales de administrador. Seleccione **Guardar**.

5. Agregue los recursos compartidos de archivos que desea escanear (un recurso compartido de archivos por línea). Luego seleccione **Continuar**.
6. Un cuadro de diálogo de confirmación muestra la cantidad de acciones que se agregaron.

   Si el cuadro de diálogo enumera recursos compartidos que no se pudieron agregar, capture esta información para poder resolver el problema. Si el problema está relacionado con una convención de nomenclatura, puede volver a agregar el recurso compartido con un nombre corregido.

7. Configurar el escaneo en el volumen:
   - Para habilitar escaneos de solo mapeo en recursos compartidos de archivos, seleccione **Mapa**.
   - Para habilitar escaneos completos en recursos compartidos de archivos, seleccione **Mapear y clasificar**.
   - Para deshabilitar el escaneo en recursos compartidos de archivos, seleccione **Desactivado**.

El interruptor en la parte superior de la página para **Escanear cuando faltan permisos de "atributos de escritura"** está deshabilitado de manera predeterminada. Esto significa que si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no escaneará los archivos porque la clasificación de datos no puede revertir la "hora del último acceso" a la marca de tiempo original. + Si cambia **Escanear cuando faltan permisos de "atributos de escritura"** a **Activado**, el escaneo restablece la última hora de acceso y escanea todos los archivos independientemente de los permisos. + Para obtener más información sobre la marca de tiempo del último acceso, consulte"Metadatos recopilados de fuentes de datos en la clasificación de datos" .

Resultado

La clasificación de datos comienza a escanear los archivos en los recursos compartidos de archivos que agregó. PuedeSeguimiento del progreso del escaneo y ver los resultados del escaneo en el **Panel de Control**.

Si el escaneo no se completa exitosamente para una configuración CIFS con autenticación Kerberos, verifique la pestaña **Configuración** para ver si hay errores.

Editar un grupo de recursos compartidos de archivos

Después de crear un grupo de recursos compartidos de archivos, puede editar el protocolo CIFS o agregar y eliminar recursos compartidos de archivos.

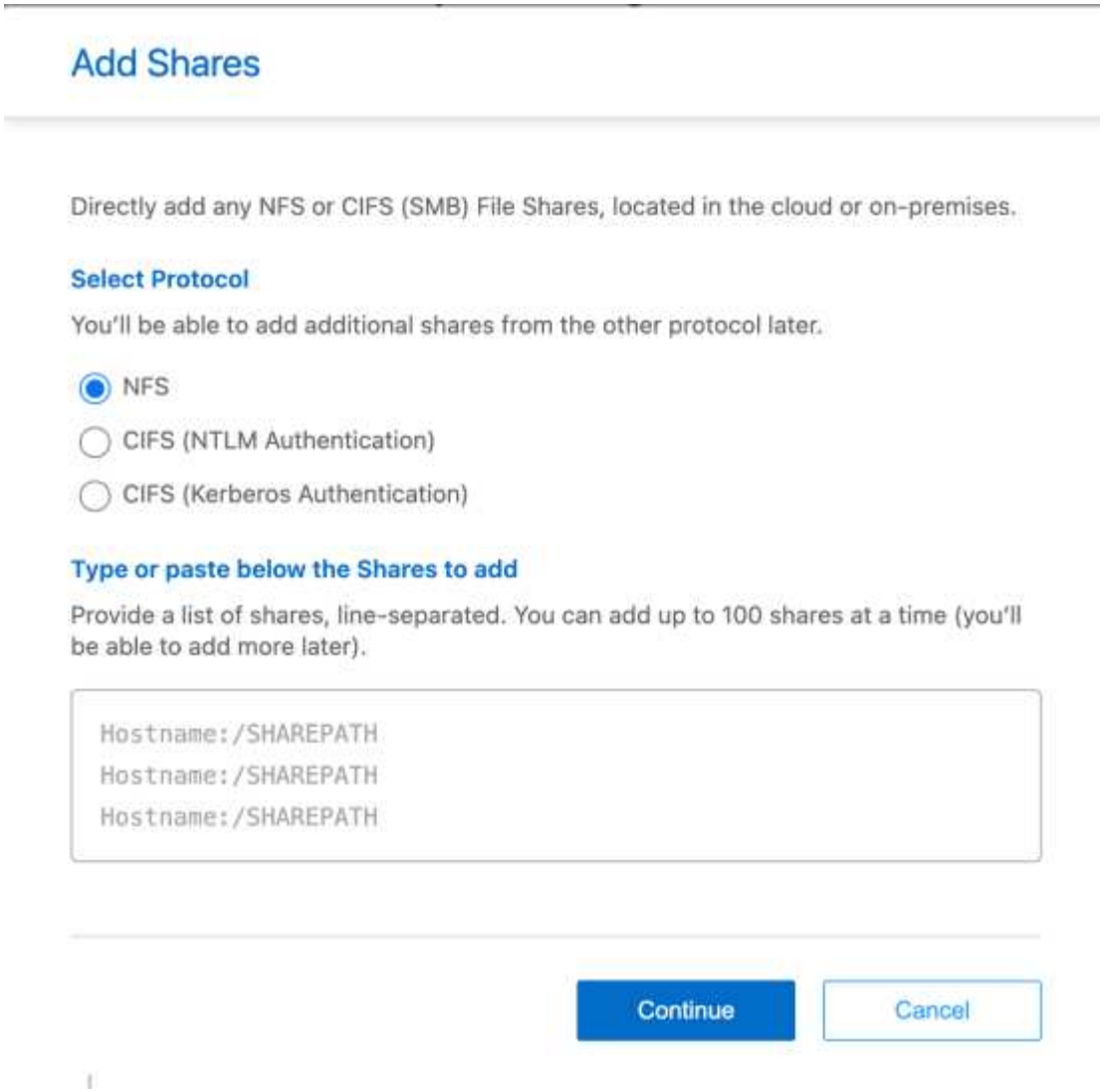
Editar la configuración del protocolo CIFS

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la página de Configuración, seleccione el grupo de recursos compartidos de archivos que desea modificar.
3. Seleccione **Editar credenciales CIFS**.

4. Elija el método de autenticación: **NTLM** o **Kerberos**.
5. Ingrese el **nombre de usuario** y la **contraseña** del Directorio Activo.
6. Seleccione **Guardar** para completar el proceso.

Agregar recursos compartidos de archivos a los escaneos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la página de Configuración, seleccione el grupo de recursos compartidos de archivos que desea modificar.
3. Seleccione **+ Agregar acciones**.
4. Seleccione el protocolo para los recursos compartidos de archivos que está agregando.



Si está agregando recursos compartidos de archivos a un protocolo que ya ha configurado, no se requieren cambios.

Si está agregando recursos compartidos de archivos con un segundo protocolo, asegúrese de haber configurado correctamente la autenticación como se detalla en"prerrequisitos" .

5. Agregue los recursos compartidos de archivos que desea escanear (un recurso compartido de archivos por línea) utilizando el formato `<host_name>:/<share_path>` .
6. Seleccione **Continuar** para completar la adición de los recursos compartidos de archivos.

Eliminar un recurso compartido de archivos de los análisis

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione el sistema del cual desea eliminar los recursos compartidos de archivos.
3. Seleccione **Configuración**.
4. Desde la página de Configuración, seleccione Acciones ••• para el recurso compartido de archivos que desea eliminar.
5. En el menú Acciones, seleccione **Eliminar recurso compartido**.

Seguimiento del progreso del escaneo

Puede realizar un seguimiento del progreso del escaneo inicial.

1. Seleccione el menú **Configuración**.
2. Seleccione la **Configuración del sistema**.
3. Para el repositorio de almacenamiento, consulte la columna Progreso del escaneo para ver su estado.

Escanee datos de StorageGRID con la NetApp Data Classification

Complete unos pocos pasos para comenzar a escanear datos dentro de StorageGRID directamente con NetApp Data Classification.

Revisar los requisitos de StorageGRID

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar la Clasificación de datos.

- Debe tener la URL del punto final para conectarse con el servicio de almacenamiento de objetos.
- Debe tener la clave de acceso y la clave secreta de StorageGRID para que la clasificación de datos pueda acceder a los depósitos.

Implementar la instancia de clasificación de datos

Implementar la clasificación de datos si aún no hay una instancia implementada.

Si está escaneando datos de StorageGRID a los que se puede acceder a través de Internet, puede"Implementar la clasificación de datos en la nube" o"Implementar la clasificación de datos en una ubicación local que tenga acceso a Internet" .

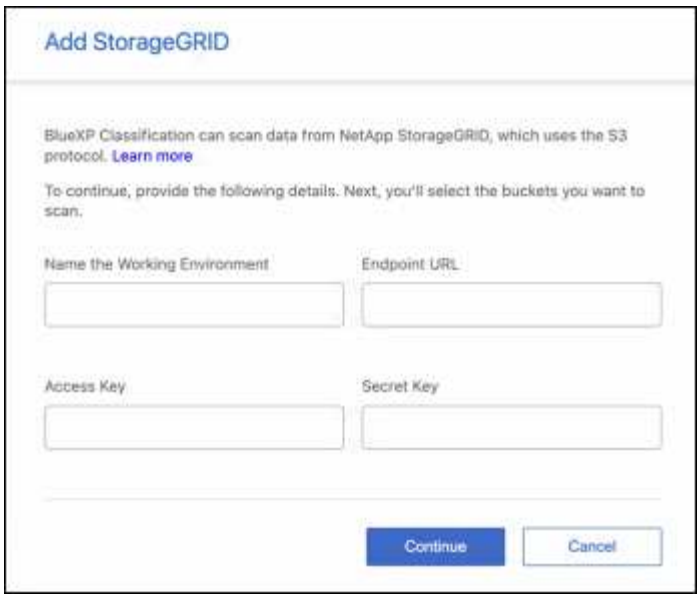
Si está escaneando datos de StorageGRID que se instaló en un sitio oscuro que no tiene acceso a Internet, debe"Implementar la clasificación de datos en la misma ubicación local que no tiene acceso a Internet" . Esto también requiere que el agente de consola esté implementado en esa misma ubicación local.

Agregue el servicio StorageGRID a la clasificación de datos

Agregue el servicio StorageGRID .

Pasos

1. Desde el menú Clasificación de datos, seleccione la opción **Configuración**.
2. Desde la página de Configuración, seleccione **Agregar sistema** > **Agregar StorageGRID**.
3. En el cuadro de diálogo Agregar servicio StorageGRID , ingrese los detalles del servicio StorageGRID y seleccione **Continuar**.
   a. Introduzca el nombre que desea utilizar para el Sistema. Este nombre debe reflejar el nombre del servicio StorageGRID al que se está conectando.
   b. Introduzca la URL del punto final para acceder al servicio de almacenamiento de objetos.
   c. Ingrese la clave de acceso y la clave secreta para que la clasificación de datos pueda acceder a los depósitos en StorageGRID.



Resultado

StorageGRID se agrega a la lista de sistemas.

Habilitar y deshabilitar escaneos en depósitos StorageGRID

Después de habilitar la Clasificación de datos en StorageGRID, el siguiente paso es configurar los depósitos que desea escanear. La clasificación de datos descubre esos grupos y los muestra en el sistema que usted creó.

Pasos

1. En la página de Configuración, busque el sistema StorageGRID .
2. En el mosaico del sistema StorageGRID , seleccione **Configuración**.
3. Complete uno de los siguientes pasos para habilitar o deshabilitar el escaneo:
   - Para habilitar escaneos de solo mapeo en un bucket, seleccione **Mapa**.
   - Para habilitar escaneos completos en un bucket, seleccione **Mapear y clasificar**.
   - Para deshabilitar el escaneo en un depósito, seleccione **Desactivado**.

Resultado

La clasificación de datos comienza a escanear los grupos que usted habilitó. Puede seguir el progreso del escaneo inicial navegando al menú **Configuración** y luego seleccionando **Configuración del sistema**. El progreso de cada escaneo se muestra como una barra de progreso. También puede pasar el cursor sobre la barra de progreso para ver la cantidad de archivos escaneados en relación con el total de archivos en el volumen. Si hay algún error, aparecerá en la columna Estado, junto con la acción necesaria para solucionarlo.

Integre su Active Directory con NetApp Data Classification

Puede integrar un Active Directory global con NetApp Data Classification para mejorar los resultados que Data Classification informa sobre los propietarios de archivos y qué usuarios y grupos tienen acceso a sus archivos.

Cuando configura ciertas fuentes de datos (enumeradas a continuación), debe ingresar las credenciales de Active Directory para que la clasificación de datos escanee los volúmenes CIFS. Esta integración proporciona

clasificación de datos con detalles del propietario del archivo y permisos para los datos que residen en esas fuentes de datos. El Active Directory ingresado para esas fuentes de datos puede ser diferente de las credenciales de Active Directory globales que ingrese aquí. La clasificación de datos buscará detalles de usuarios y permisos en todos los directorios activos integrados.

Esta integración proporciona información adicional en las siguientes ubicaciones en Clasificación de datos:

- Puedes utilizar el "Propietario del archivo""filtrar" y ver los resultados en los metadatos del archivo en el panel Investigación. En lugar de que el propietario del archivo contenga el SID (identificador de seguridad), se completa con el nombre de usuario real.

  También puede ver más detalles sobre el propietario del archivo: nombre de la cuenta, dirección de correo electrónico y nombre de la cuenta SAM, o ver los elementos que pertenecen a ese usuario.

- Ya puedes ver"permisos de archivo completos" para cada archivo y directorio cuando hace clic en el botón "Ver todos los permisos".
- En el"Panel de gobernanza" , el panel Permisos abiertos mostrará un mayor nivel de detalle sobre sus datos.

Los SID de usuarios locales y los SID de dominios desconocidos no se traducen al nombre de usuario real.

Fuentes de datos compatibles

Una integración de Active Directory con clasificación de datos puede identificar datos de las siguientes fuentes de datos:

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

Conéctese a su servidor de Active Directory

Una vez que haya implementado la Clasificación de datos y haya activado el escaneo en sus fuentes de datos, puede integrar la Clasificación de datos con su Active Directory. Se puede acceder a Active Directory mediante una dirección IP de servidor DNS o una dirección IP de servidor LDAP.

Las credenciales de Active Directory pueden ser de solo lectura, pero proporcionar credenciales de administrador garantiza que Data Classification pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de clasificación de datos.

Para volúmenes CIFS/recursos compartidos de archivos, si desea asegurarse de que los "últimos tiempos de acceso" de sus archivos no se modifiquen mediante los análisis de clasificación de clasificación de datos, el usuario debe tener permiso de escritura de atributos. Si es posible, recomendamos hacer que el usuario configurado de Active Directory sea parte de un grupo principal en la organización que tenga permisos para todos los archivos.

Requisitos

- Debe tener un Directorio Activo ya configurado para los usuarios de su empresa.
- Debes tener la información del Directorio Activo:

- 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)
- Ya sea que esté utilizando LDAP seguro (LDAPS) o no
- Puerto del servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)

- Los siguientes puertos deben estar abiertos para la comunicación saliente por parte de la instancia de clasificación de datos:

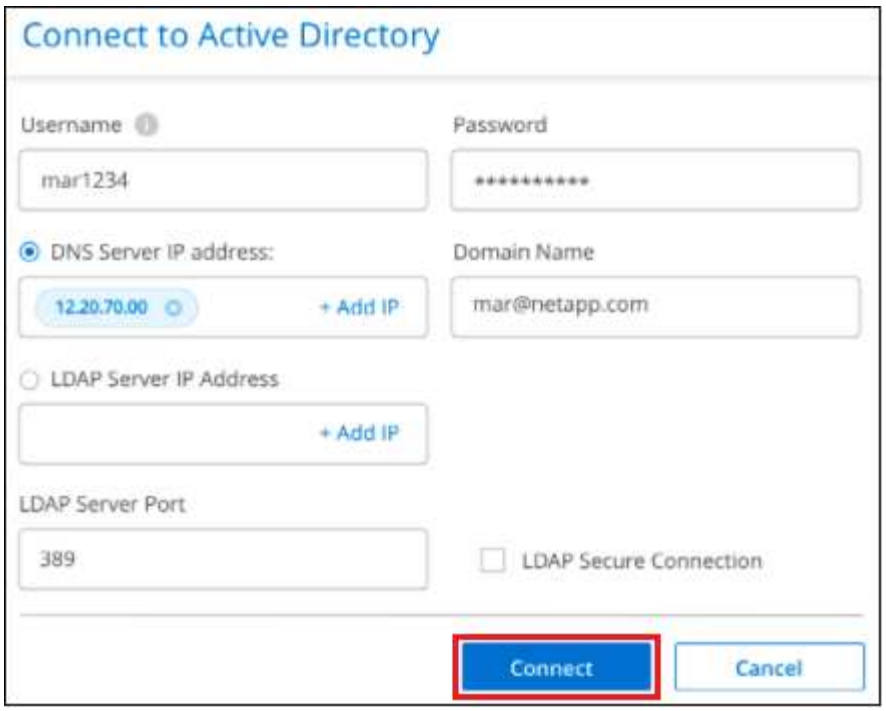
Protocolo	Puerto	Destino	Objetivo
TCP y UDP	389	Directorio activo	LDAP
TCP	636	Directorio activo	LDAP sobre SSL
TCP	3268	Directorio activo	Catálogo global
TCP	3269	Directorio activo	Catálogo global sobre SSL

Pasos

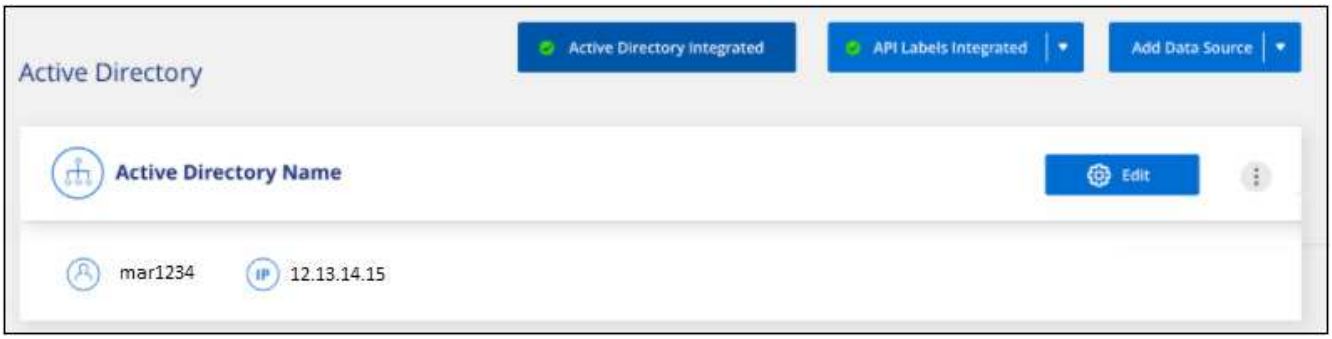
1. Desde la página Configuración de clasificación de datos, haga clic en **Agregar Active Directory**.

2. En el cuadro de diálogo Conectar a Active Directory, ingrese los detalles de Active Directory y haga clic en **Conectar**.

   Puede agregar varias direcciones IP, si es necesario, seleccionando **Agregar IP**.



La clasificación de datos se integra al Directorio Activo y se agrega una nueva sección a la página de Configuración.



Administre su integración de Active Directory

Si necesita modificar algún valor en su integración de Active Directory, haga clic en el botón **Editar** y realice los cambios.

También puedes eliminar la integración seleccionando la opción botón y luego **Eliminar Active Directory**.

Utilizar la clasificación de datos

Vea los detalles de gobernanza sobre los datos almacenados en su organización con NetApp Data Classification

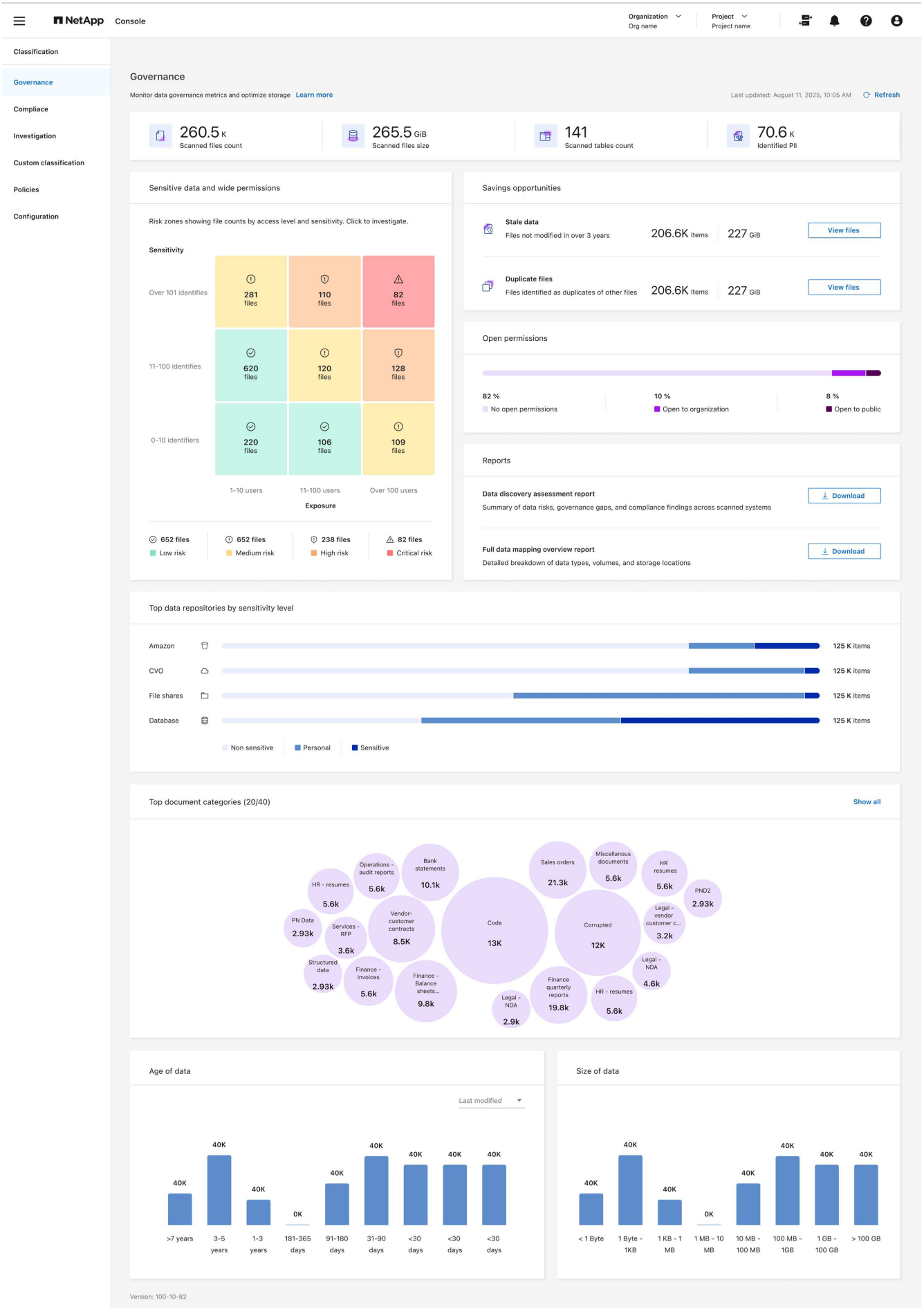
Obtenga control de los costos relacionados con los datos en los recursos de almacenamiento de su organización. La NetApp Data Classification identifica la cantidad de datos obsoletos, archivos duplicados y archivos muy grandes en sus sistemas para que pueda decidir si desea eliminar o agrupar algunos archivos en un almacenamiento de objetos menos costoso.

Aquí es donde debes comenzar tu investigación. Desde el panel de Gobernanza, puede seleccionar un área para realizar una investigación más profunda.

Además, si planea migrar datos desde ubicaciones locales a la nube, puede ver el tamaño de los datos y si alguno de ellos contiene información confidencial antes de moverlos.

Revisar el panel de gobernanza

El panel de gobernanza proporciona información para que pueda aumentar la eficiencia y controlar los costos relacionados con los datos almacenados en sus recursos de almacenamiento.


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

Pasos

1. Desde el menú de la NetApp Console , seleccione **Gobernanza > Clasificación**.
2. Seleccione **Gobernanza**.

   Aparece el panel de gobernanza.

Revisar oportunidades de ahorro

El componente *Oportunidades de ahorro* muestra datos que puede eliminar o almacenar en un almacenamiento de objetos menos costoso. Los datos en *Saving Opportunities* se actualizan cada 2 horas. También puede actualizar los datos manualmente.

Pasos

1. En el menú Clasificación de datos, seleccione **Gobernanza**.
2. Dentro de cada mosaico de Oportunidades de ahorro del panel de Gobernanza, seleccione **Optimizar almacenamiento** para ver los resultados filtrados en la página de Investigación. Para descubrir qué datos debe eliminar o transferir a un almacenamiento menos costoso, investigue las *Oportunidades de ahorro*.
   - **Datos obsoletos**: de forma predeterminada, los datos se consideran obsoletos si se modificaron por última vez hace más de 3 años. Puede [personalizar la definición de datos obsoletos](task-stale-data.html).
   - **Archivos duplicados**: archivos que están duplicados en otras ubicaciones en las fuentes de datos que está escaneando. "Vea qué tipos de archivos duplicados se muestran" .

Si alguna de sus fuentes de datos implementa niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos se pueden identificar en la categoría *Datos obsoletos*.

Crear el informe de evaluación de descubrimiento de datos

El informe de evaluación de descubrimiento de datos proporciona un análisis de alto nivel del entorno escaneado para mostrar áreas de preocupación y posibles pasos de remediación. Los resultados se basan tanto en el mapeo como en la clasificación de sus datos. El objetivo de este informe es crear conciencia sobre tres aspectos importantes de su conjunto de datos:

Característica	Descripción
Preocupaciones sobre la gobernanza de datos	Una imagen detallada de todos los datos que posee y las áreas en las que puede reducir la cantidad de datos para ahorrar costos.
Exposiciones de seguridad de datos	Áreas donde sus datos son accesibles a ataques internos o externos debido a amplios permisos de acceso.
Brechas de cumplimiento de datos	Dónde se encuentra su información personal o información personal confidencial, tanto por motivos de seguridad como para las DSAR (solicitudes de acceso de interesados).

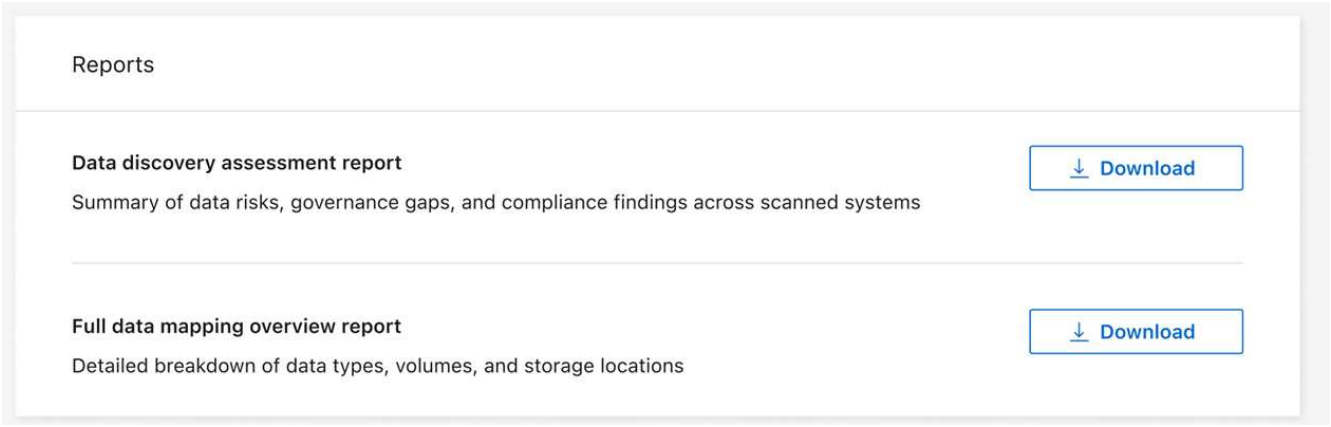
Con el informe podrás realizar las siguientes acciones:

- Reduzca los costos de almacenamiento modificando su política de retención o moviendo o eliminando ciertos datos (datos obsoletos o duplicados).
- Proteja sus datos que tienen permisos amplios revisando las políticas de administración de grupos globales.

- Proteja sus datos que contienen información personal o confidencial moviendo PII a almacenes de datos más seguros.

Pasos

1. En Clasificación de datos, seleccione **Gobernanza**.
2. En el mosaico de informes, seleccione **Informe de evaluación de descubrimiento de datos**.



Resultado

La clasificación de datos genera un informe en PDF que puedes revisar y compartir.

Crear el informe de descripción general del mapeo de datos

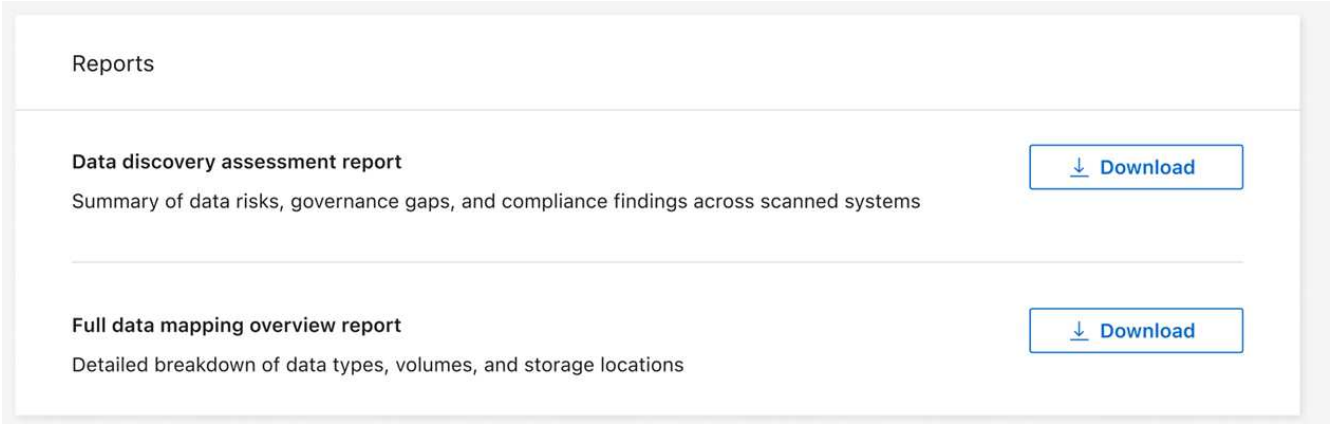
El informe de descripción general de mapeo de datos proporciona una descripción general de los datos almacenados en sus fuentes de datos corporativas para ayudarlo con las decisiones sobre procesos de migración, respaldo, seguridad y cumplimiento. El informe resume todos los sistemas y fuentes de datos. También proporciona un análisis para cada sistema.

El informe incluye la siguiente información:

Categoría	Descripción
Capacidad de uso	Para todos los sistemas: enumera la cantidad de archivos y la capacidad utilizada para cada sistema. Para sistemas individuales: enumera los archivos que utilizan la mayor capacidad.
La era de los datos	Proporciona tres cuadros y gráficos que indican cuándo se crearon los archivos, cuándo se modificaron por última vez o cuándo se accedió por última vez. Enumera la cantidad de archivos y su capacidad utilizada, en función de determinados rangos de fechas.
Tamaño de los datos	Enumera la cantidad de archivos que existen dentro de ciertos rangos de tamaño en sus sistemas.

Pasos

1. En Clasificación de datos, seleccione **Gobernanza**.
2. En el mosaico de informes, seleccione **Informe de descripción general de mapeo de datos completo**.



Resultado

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Si el informe tiene más de 1 MB, el archivo PDF se conserva en la instancia de Clasificación de datos y verá un mensaje emergente sobre la ubicación exacta. Cuando Data Classification está instalado en una máquina Linux en sus instalaciones o en una máquina Linux implementada en la nube, puede navegar directamente al archivo PDF. Cuando se implementa la clasificación de datos en la nube, es necesario autorizar con SSH la instancia de clasificación de datos para descargar el archivo PDF.

Revise los principales repositorios de datos enumerados por sensibilidad de datos

El área *Principales repositorios de datos por nivel de sensibilidad* del informe Descripción general de mapeo de datos enumera los cuatro principales repositorios de datos (sistemas y fuentes de datos) que contienen los elementos más sensibles. El gráfico de barras de cada sistema se divide en:

- Datos no sensibles
- Datos personales
- Datos personales sensibles

Estos datos se actualizan cada dos horas y se pueden actualizar manualmente.

Pasos

1. Para ver el número total de elementos en cada categoría, coloque el cursor sobre cada sección de la barra.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione cada área en la barra e investigue más.

Revisar datos confidenciales y permisos amplios

El área *Datos confidenciales y permisos amplios* del panel de Gobernanza muestra los recuentos de archivos que contienen datos confidenciales y tienen permisos amplios. La tabla muestra los siguientes tipos de permisos:

- Desde los permisos más restrictivos hasta las restricciones más permisivas en el eje horizontal.
- Desde los datos menos sensibles hasta los más sensibles en el eje vertical.

Pasos

1. Para ver el número total de archivos en cada categoría, coloque el cursor sobre cada cuadro.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione una casilla e investigue más.

Revisar los datos enumerados por tipos de permisos abiertos

El área *Permisos abiertos* del informe Descripción general de asignación de datos muestra el porcentaje de cada tipo de permisos que existen para todos los archivos que se están escaneando. El gráfico muestra los siguientes tipos de permisos:

- Sin permisos abiertos
- Abierto a la Organización
- Abierto al público
- Acceso desconocido

Pasos

1. Para ver el número total de archivos en cada categoría, coloque el cursor sobre cada cuadro.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione una casilla e investigue más.

Revisar la edad y el tamaño de los datos

Puede investigar los elementos en los gráficos *Edad* y *Tamaño* del informe Descripción general de mapeo de datos para ver si hay datos que debería eliminar o colocar en un nivel de almacenamiento de objetos menos costoso.

Pasos

1. En el gráfico Era de los Datos, para ver detalles sobre la edad de los datos, coloque el cursor sobre un punto del gráfico.
2. Para filtrar por rango de edad o tamaño, seleccione esa edad o tamaño.
    - **Gráfico de antigüedad de los datos**: clasifica los datos según el momento en que se crearon, la última vez que se accedió a ellos o la última vez que se modificaron.
    - **Gráfico de tamaño de datos**: clasifica los datos según su tamaño.

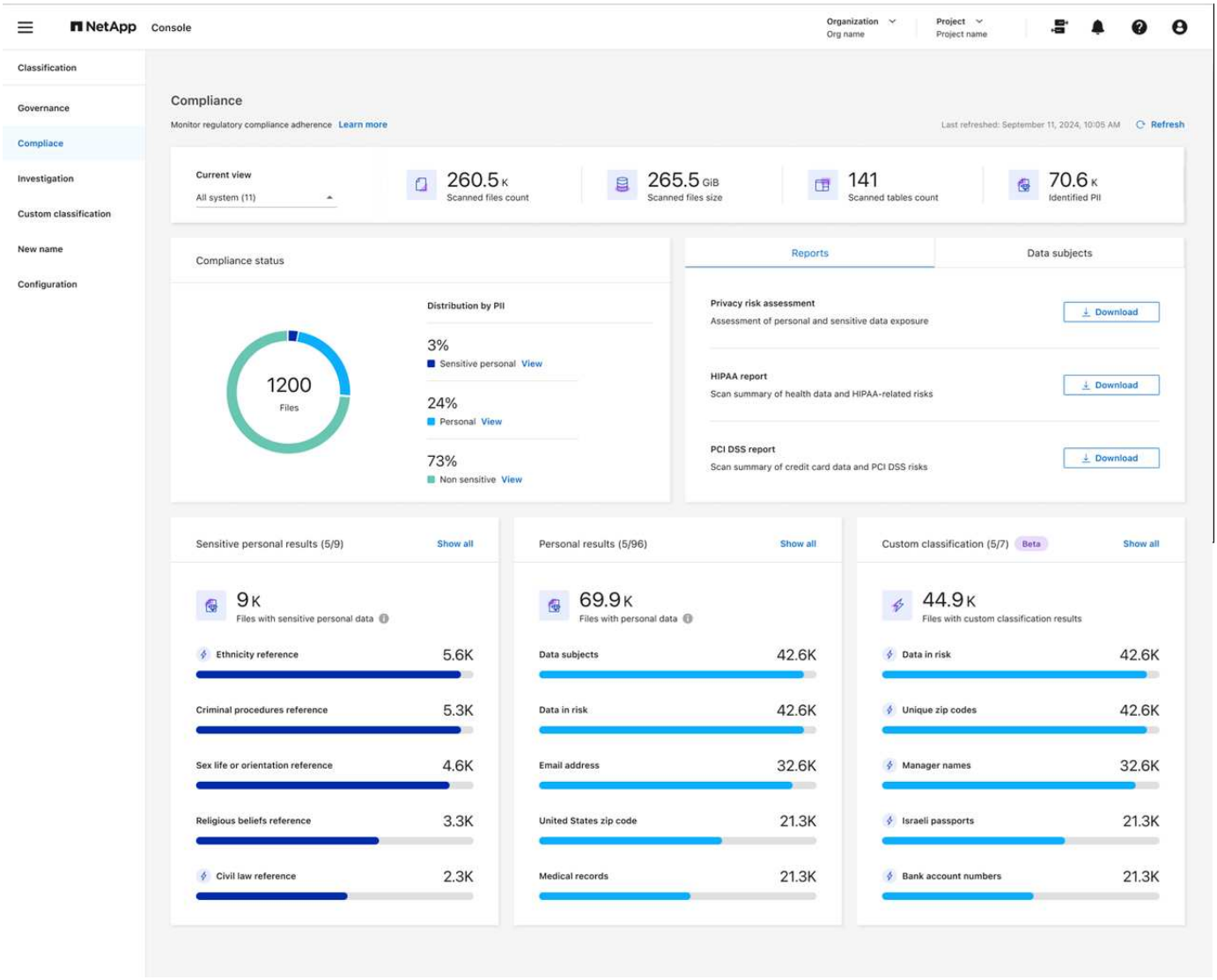
> Si alguna de sus fuentes de datos implementa niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos podrían identificarse en el gráfico *Antigüedad de los datos*.

Vea los detalles de cumplimiento sobre los datos privados almacenados en su organización con NetApp Data Classification

Obtenga control de sus datos privados al ver detalles sobre los datos personales (PII) y los datos personales confidenciales (SPII) de su organización. También puede obtener visibilidad al revisar las categorías y los tipos de archivos que NetApp Data Classification encontró en sus datos.

Los detalles de cumplimiento a nivel de archivo solo están disponibles si realiza un análisis de clasificación completo. Los escaneos de solo mapeo no brindan detalles a nivel de archivo.

De forma predeterminada, el panel de Clasificación de datos muestra datos de cumplimiento de todos los sistemas y bases de datos. Para ver los datos de sólo algunos de los sistemas, selecciónelos.



Puede filtrar los resultados desde la página Investigación de datos y descargar un informe de los resultados como un archivo CSV. Ver"Filtrado de datos en la página Investigación de datos" Para más detalles.

Ver archivos que contienen datos personales

La clasificación de datos identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. "Por ejemplo, números de tarjetas de crédito, números de seguro social, números de cuentas bancarias, contraseñas y más."La clasificación de datos identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

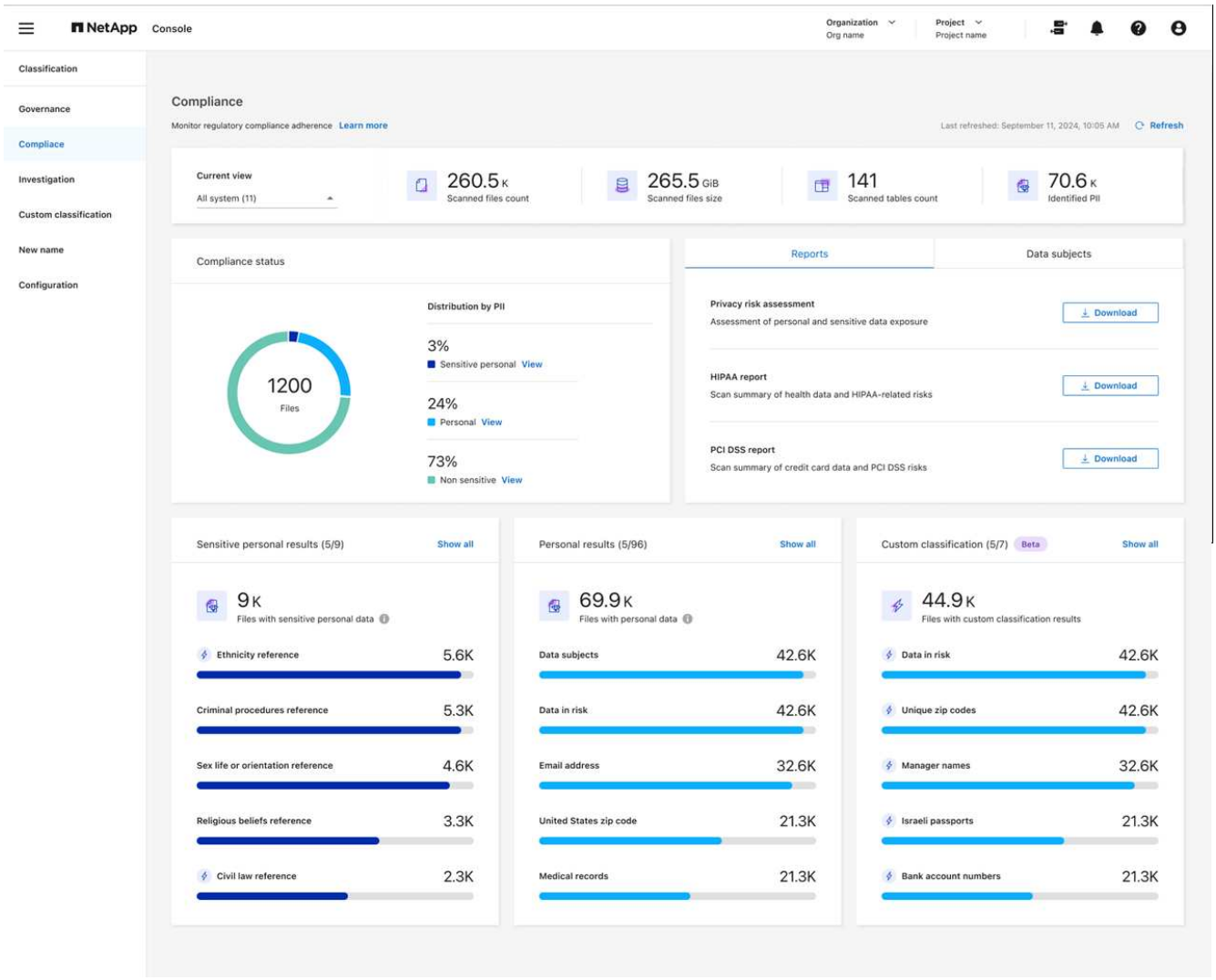
También puede crear términos de búsqueda personalizados para identificar datos personales específicos de su organización. Para obtener más información, consulte "Crear una clasificación personalizada" .

Para algunos tipos de datos personales, la clasificación de datos utiliza *validación de proximidad* para validar

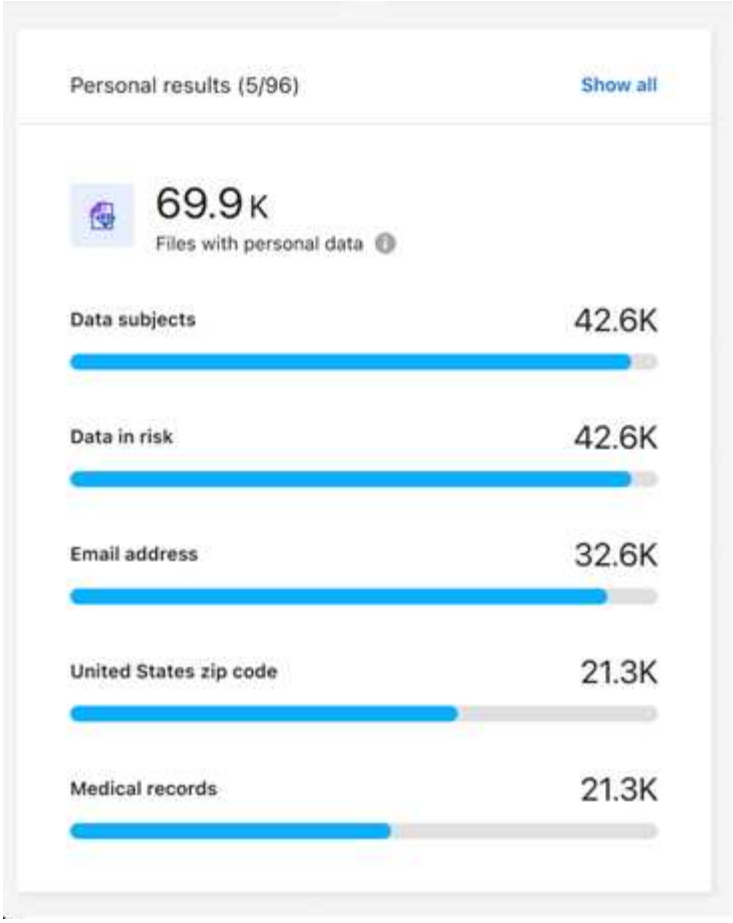
sus hallazgos. La validación se realiza mediante la búsqueda de una o más palabras clave predefinidas en proximidad a los datos personales encontrados. Por ejemplo, la clasificación de datos identifica un número de seguro social (SSN) de EE. UU. como un SSN si ve una palabra de proximidad junto a él, por ejemplo, *SSN* o *seguridad social*. "La tabla de datos personales" muestra cuándo la clasificación de datos utiliza la validación de proximidad.

Pasos

1. Desde el menú Clasificación de datos, seleccione la pestaña **Cumplimiento**.
2. Para investigar los detalles de todos los datos personales, seleccione el ícono junto al porcentaje de datos personales.

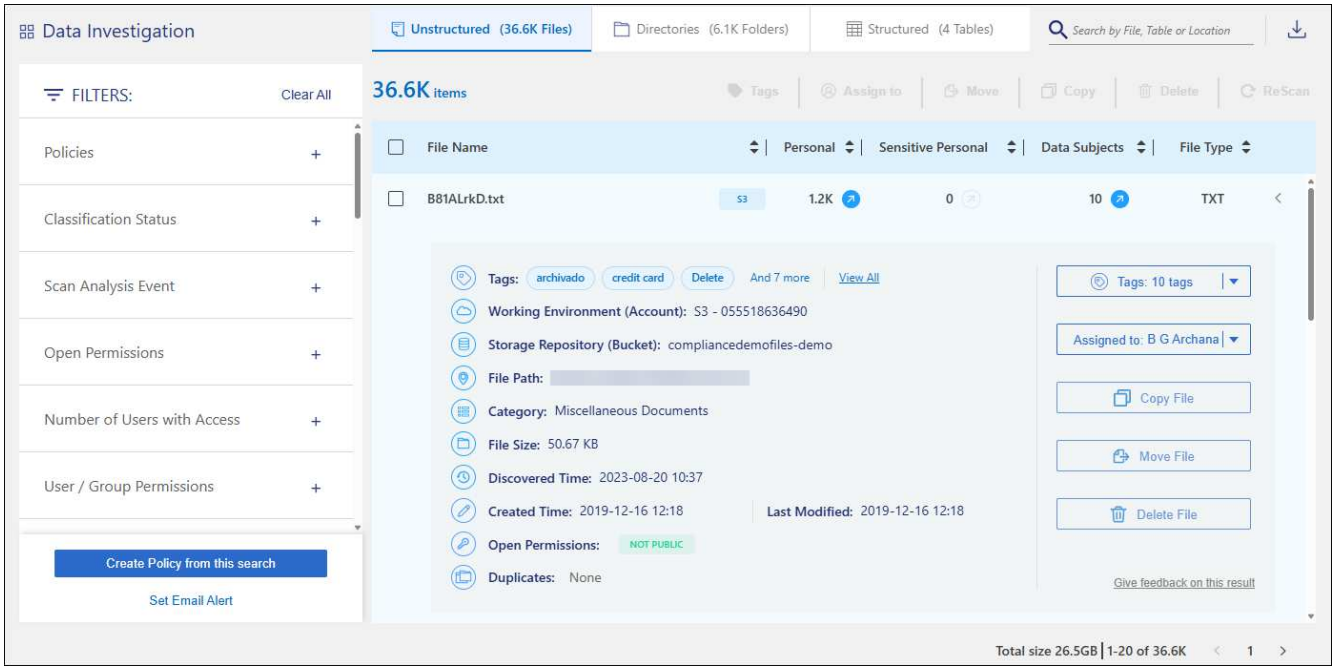


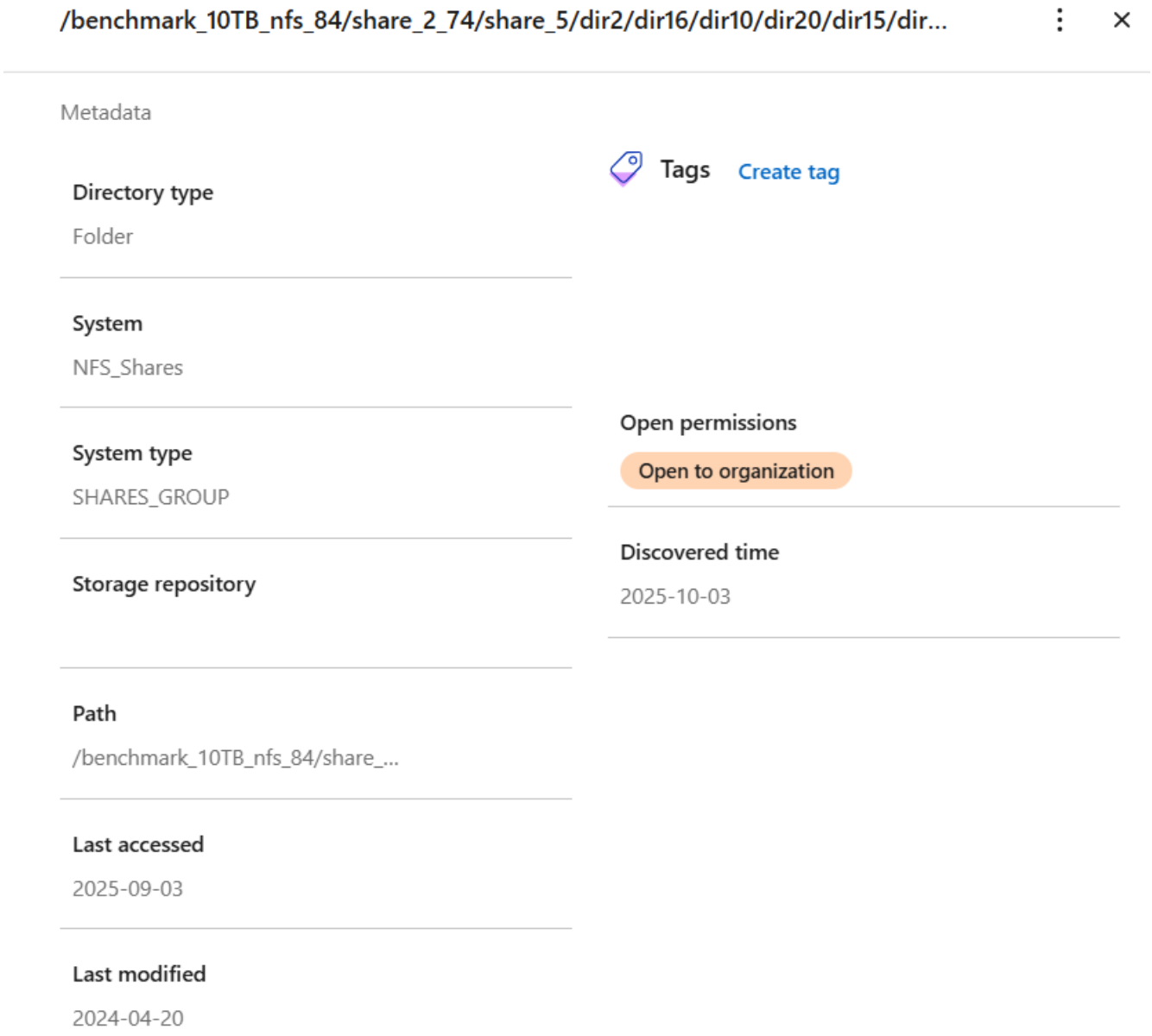
3. Para investigar los detalles de un tipo específico de datos personales, seleccione **Ver todo** y luego seleccione el ícono de flecha **Investigar resultados** para un tipo específico de datos personales, por ejemplo, direcciones de correo electrónico.



4. Investigue los datos buscando, ordenando, expandiendo detalles de un archivo específico, seleccionando la flecha **Investigar resultados** para ver información enmascarada o descargando la lista de archivos.

   Las siguientes imágenes muestran datos personales encontrados en un directorio (archivos compartidos y carpetas). En la pestaña **Estructurado**, puede ver los datos personales que se encuentran en las bases de datos. En la pestaña **No estructurado**, puede ver datos a nivel de archivo.





Ver archivos que contienen datos personales confidenciales

La clasificación de datos identifica automáticamente tipos especiales de información personal confidencial, según lo definen las regulaciones de privacidad, como "artículos 9 y 10 del RGPD" . Por ejemplo, información sobre la salud de una persona, su origen étnico o su orientación sexual. "Ver la lista completa" . La clasificación de datos identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

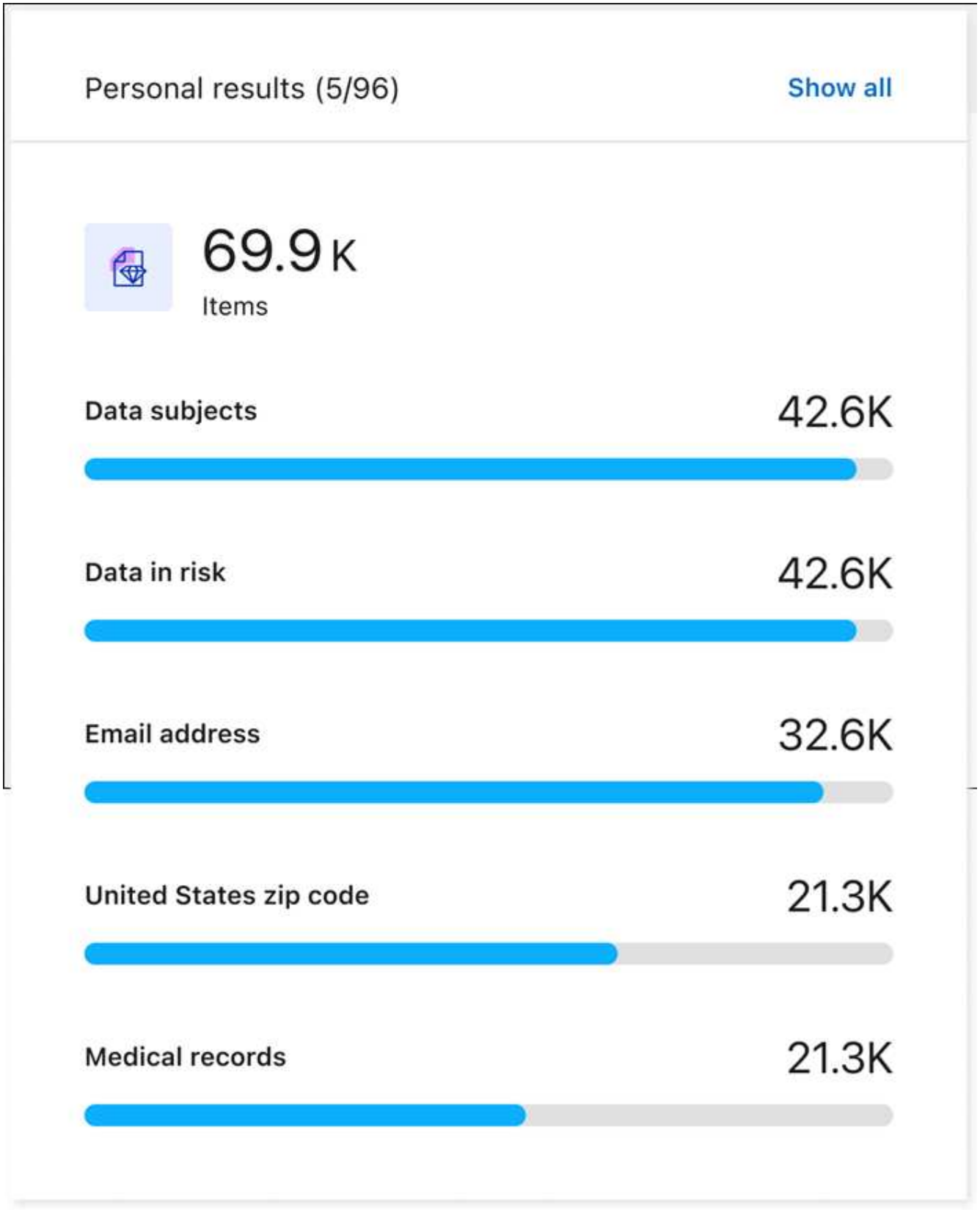
La clasificación de datos utiliza IA, procesamiento del lenguaje natural (PLN), aprendizaje automático (ML) y computación cognitiva (CC) para comprender el significado del contenido que escanea con el fin de extraer entidades y categorizarlo en consecuencia.

Por ejemplo, una categoría de datos sensibles del RGPD es el origen étnico. Gracias a sus capacidades de PNL, Data Classification puede distinguir la diferencia entre una frase que dice "George es mexicano" (lo que indica datos confidenciales según lo especificado en el artículo 9 del RGPD) y "George está comiendo comida mexicana".

Al escanear datos personales confidenciales solo se admite el idioma inglés. Más adelante se añadirá soporte para más idiomas.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Para investigar los detalles de todos los datos personales confidenciales, busque la tarjeta **Resultados personales confidenciales** y luego seleccione **Mostrar todo**.



.

3. Para investigar los detalles de un tipo específico de datos personales confidenciales, seleccione **Ver todo** y luego seleccione el ícono de flecha **Investigar resultados** para un tipo específico de datos personales confidenciales.
4. Investigue los datos buscando, ordenando, expandiendo detalles de un archivo específico, haciendo clic

en **Investigar resultados** para ver información enmascarada o descargando la lista de archivos.

Categorías de datos privados en la NetApp Data Classification

Hay muchos tipos de datos privados que NetApp Data Classification puede identificar en sus volúmenes y bases de datos.

La clasificación de datos identifica dos tipos de datos personales:

- **Información de identificación personal (PII)**
- **Información personal sensible (SPII)**

Si necesita clasificación de datos para identificar otros tipos de datos privados, como números de identificación nacional adicionales o identificadores de atención médica, comuníquese con su gerente de cuenta.

Tipos de datos personales

Los datos personales, o *información de identificación personal* (PII), que se encuentran en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna de la tabla a continuación identifica si la clasificación de datos utiliza"validación de proximidad" para validar sus hallazgos para el identificador.

En la tabla se identifican los idiomas en los que se pueden reconocer estos elementos.

Tipo	Identificador	¿Validación de proximidad?	Inglés	Alemán	Español	Francés	japonés
General	Número de Tarjeta de Crédito	Sí	✓	✓	✓		✓
	Titulares de los datos	No	✓	✓	✓		
	Dirección de correo electrónico	No	✓	✓	✓		✓
	Número IBAN (Número de cuenta bancaria internacional)	No	✓	✓	✓		✓
	Dirección IP	No	✓	✓	✓		✓
	Password	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

Tipo	Identificador	¿Validación de proximidad?	Inglés	Alemán	Español	Francés	japonés

Tipo	Identificador	¿Validación de proximidad?	Inglés	Alemán	Español	Francés	japonés
	Identificación del Reino Unido (NINO)	Sí	✓	✓	✓		
	Licencia de conducir de California, EE. UU.	Sí	✓	✓	✓		
	Licencia de conducir de Indiana, EE. UU.	Sí	✓	✓	✓		
	Licencia de conducir de Nueva York, EE. UU.	Sí	✓	✓	✓		
	Licencia de conducir de Texas, EE. UU.	Sí	✓	✓	✓		
	Número de Seguro Social de EE. UU. (SSN)	Sí	✓	✓	✓		

Tipos de datos personales sensibles

La clasificación de datos puede encontrar la siguiente información personal confidencial (SPII) en los archivos.

Los siguientes SPII actualmente solo se pueden reconocer en inglés:

- **Referencia de Procedimientos Penales**: Datos relativos a condenas y delitos penales de una persona física.
- **Referencia étnica**: Datos relativos al origen racial o étnico de una persona física.
- **Referencia de Salud**: Datos relativos a la salud de una persona física.
- **Códigos médicos CIE-9-CM**: Códigos utilizados en la industria médica y de la salud.
- **Códigos médicos CIE-10-CM**: Códigos utilizados en la industria médica y de la salud.
- **Referencia de creencias filosóficas**: Datos relativos a las creencias filosóficas de una persona física.
- **Referencia de opiniones políticas**: Datos relativos a las opiniones políticas de una persona física.
- **Referencia de creencias religiosas**: Datos relativos a las creencias religiosas de una persona física.
- **Referencia sobre la vida sexual o la orientación sexual**: Datos relativos a la vida sexual o la orientación sexual de una persona física.

Tipos de categorías

La clasificación de datos categoriza sus datos de la siguiente manera.

La mayoría de estas categorías se pueden reconocer en inglés, alemán y español.

Categoría	Tipo	Inglés	Alemán	Español
Finanzas	Balances generales	✓	✓	✓
	Órdenes de compra	✓	✓	✓
	Facturas	✓	✓	✓
	Informes trimestrales	✓	✓	✓

Categoría	Tipo	Inglés	Alemán	Español
HORA	Verificación de antecedentes	✓		✓
	Planes de compensación	✓	✓	✓
	Contratos de empleados	✓		✓
	Reseñas de empleados	✓		✓
	Salud	✓		✓
	Currículums	✓	✓	✓
Legal	Acuerdos de confidencialidad	✓	✓	✓
	Contratos entre proveedor y cliente	✓	✓	✓
Marketing	Campañas	✓	✓	✓
	Conferencias	✓	✓	✓
Operaciones	Informes de auditoría	✓	✓	✓
Ventas	Órdenes de venta	✓	✓	
Servicios	Solicitud de información	✓		✓
	Solicitud de propuestas	✓		✓
	SEMBRAR	✓	✓	✓
	Formación	✓	✓	✓
Soporte	Quejas y tickets	✓	✓	✓

Los siguientes metadatos también están categorizados e identificados en los mismos idiomas admitidos:

- Datos de la aplicación
- Archivos de archivo
- Audio
- Migas de pan de datos de aplicaciones empresariales de clasificación de datos
- Archivos CAD
- Código
- Corrupto
- Archivos de base de datos e índice
- Archivos de diseño
- Datos de la aplicación de correo electrónico
- Cifrados (archivos con una puntuación de entropía alta)
- Ejecutables
- Datos de aplicaciones financieras
- Datos de la aplicación de salud

- Imágenes
- Registros
- Documentos varios
- Presentaciones varias
- Hojas de cálculo varias
- Misceláneo "Desconocido"
- Archivos protegidos con contraseña
- Datos estructurados
- Vídeos
- Archivos de cero bytes

Tipos de archivos

La clasificación de datos escanea todos los archivos en busca de información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección de tipos de archivos del panel. Cuando la clasificación de datos detecta información de identificación personal (PII) o cuando realiza una búsqueda DSAR, solo se admiten los siguientes formatos de archivo:

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

Exactitud de la información encontrada

NetApp no puede garantizar el 100 % de precisión de los datos personales y los datos personales confidenciales que identifica la clasificación de datos. Siempre debes validar la información revisando los datos.

Según nuestras pruebas, la siguiente tabla muestra la precisión de la información que encuentra la clasificación de datos. Lo desglosamos por *precisión* y *recuperación*:

Precisión
: La probabilidad de que lo que encuentra la Clasificación de Datos haya sido identificado correctamente. Por ejemplo, una tasa de precisión del 90% para datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal, en realidad contienen información personal. 1 de cada 10 archivos sería un falso positivo.

Recordar
: La probabilidad de que la clasificación de datos encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70% para datos personales significa que la clasificación de datos puede identificar 7 de cada 10 archivos que realmente contienen información personal en su organización. La clasificación de datos perdería el 30% de los datos y no aparecerán en el panel de control.

Estamos mejorando constantemente la precisión de nuestros resultados. Estas mejoras estarán disponibles automáticamente en futuras versiones de Clasificación de datos.

Tipo	Precisión	Recordar
Datos personales - General	90%-95%	60%-80%

Tipo	Precisión	Recordar
Datos personales - Identificadores de país	30%-60%	40%-60%
Datos personales sensibles	80%-95%	20%-30%
Categorías	90%-97%	60%-80%

Cree una clasificación personalizada en NetApp Data Classification

La NetApp Data Classification le permite crear categorías personalizadas o identificadores personales para identificar datos específicos según los requisitos normativos y de cumplimiento de su organización.

La clasificación de datos admite dos tipos de clasificadores personalizados: categorías e identificadores personales. Las categorías personalizadas se crean en función de un conjunto de archivos que usted carga, desde los cuales Data Classification crea un modelo de IA para identificar datos similares en su organización (por ejemplo, una empresa de investigación de salud podría crear una categoría de análisis clínico). Los identificadores personales personalizados se crean utilizando listas de palabras clave o una expresión regular (regex) para identificar información específica de su organización que pueda representar un riesgo de cumplimiento.

Todas las clasificaciones personalizadas están disponibles en el panel de clasificación personalizada.

Crear un identificador personal personalizado

La clasificación de datos le permite crear un identificador personal personalizado utilizando palabras clave contextuales o una expresión regular para identificar datos exclusivos de su organización.

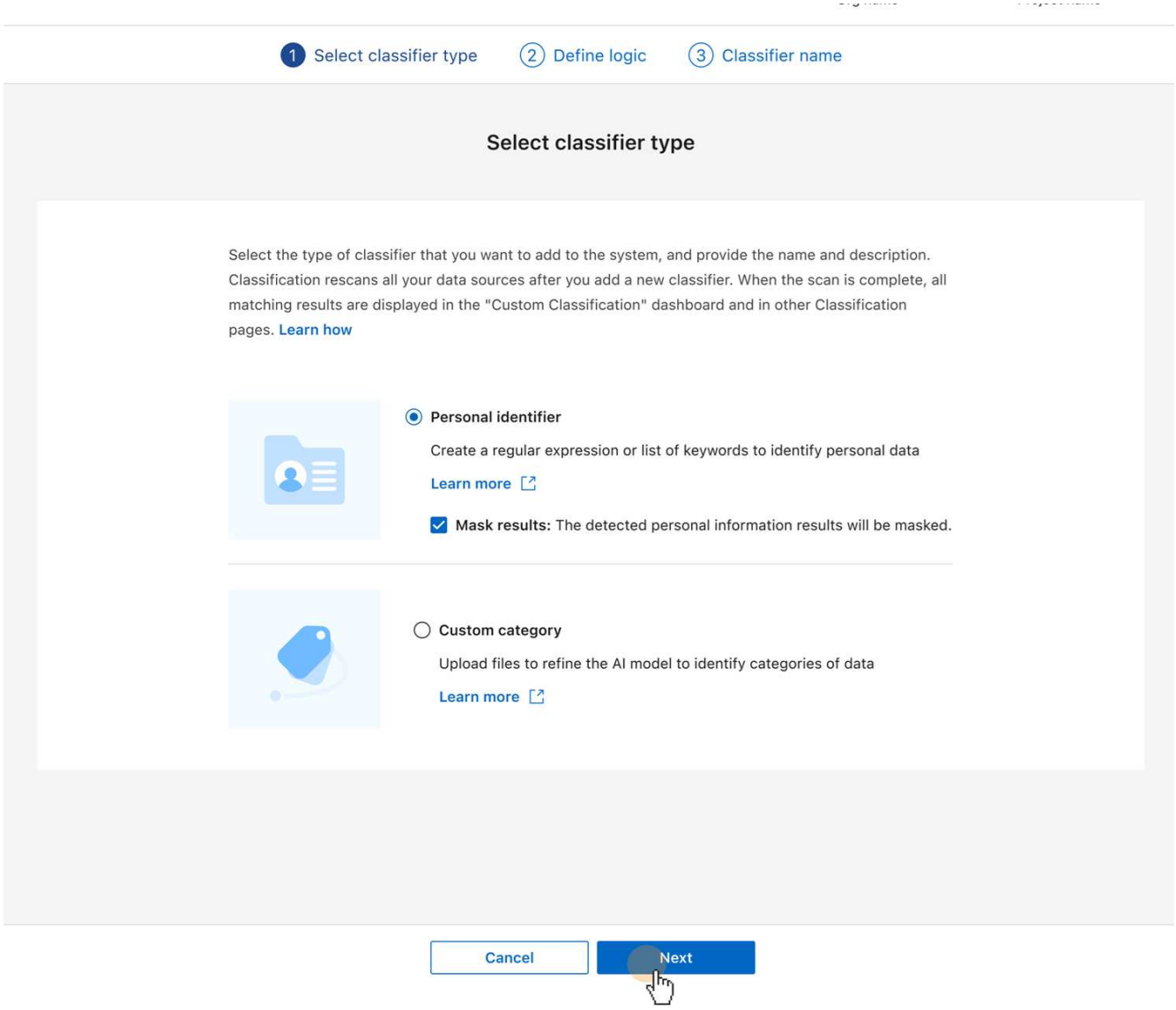
Requisitos para palabras clave

Si está creando su identificador personal con una lista de palabras clave, la lista debe cumplir los siguientes requisitos:

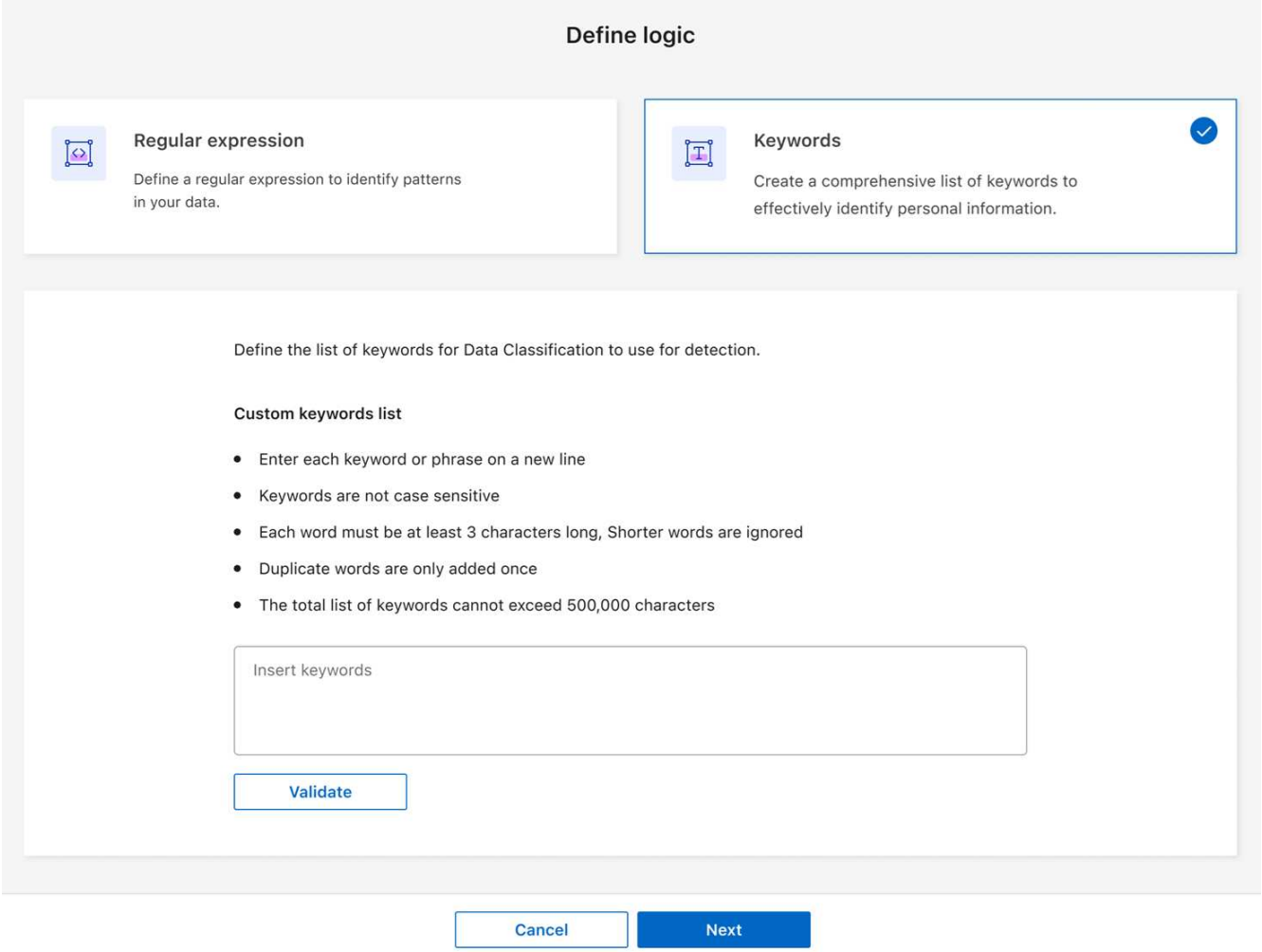
- Las entradas de palabras clave no distinguen entre mayúsculas y minúsculas.
- Las palabras clave deben tener al menos tres caracteres. Cualquier palabra con menos de tres caracteres será ignorada.
- Las palabras duplicadas solo se agregan una vez.
- La lista total de palabras clave no puede superar los 500.000 caracteres. La lista debe incluir al menos una palabra clave.

Pasos

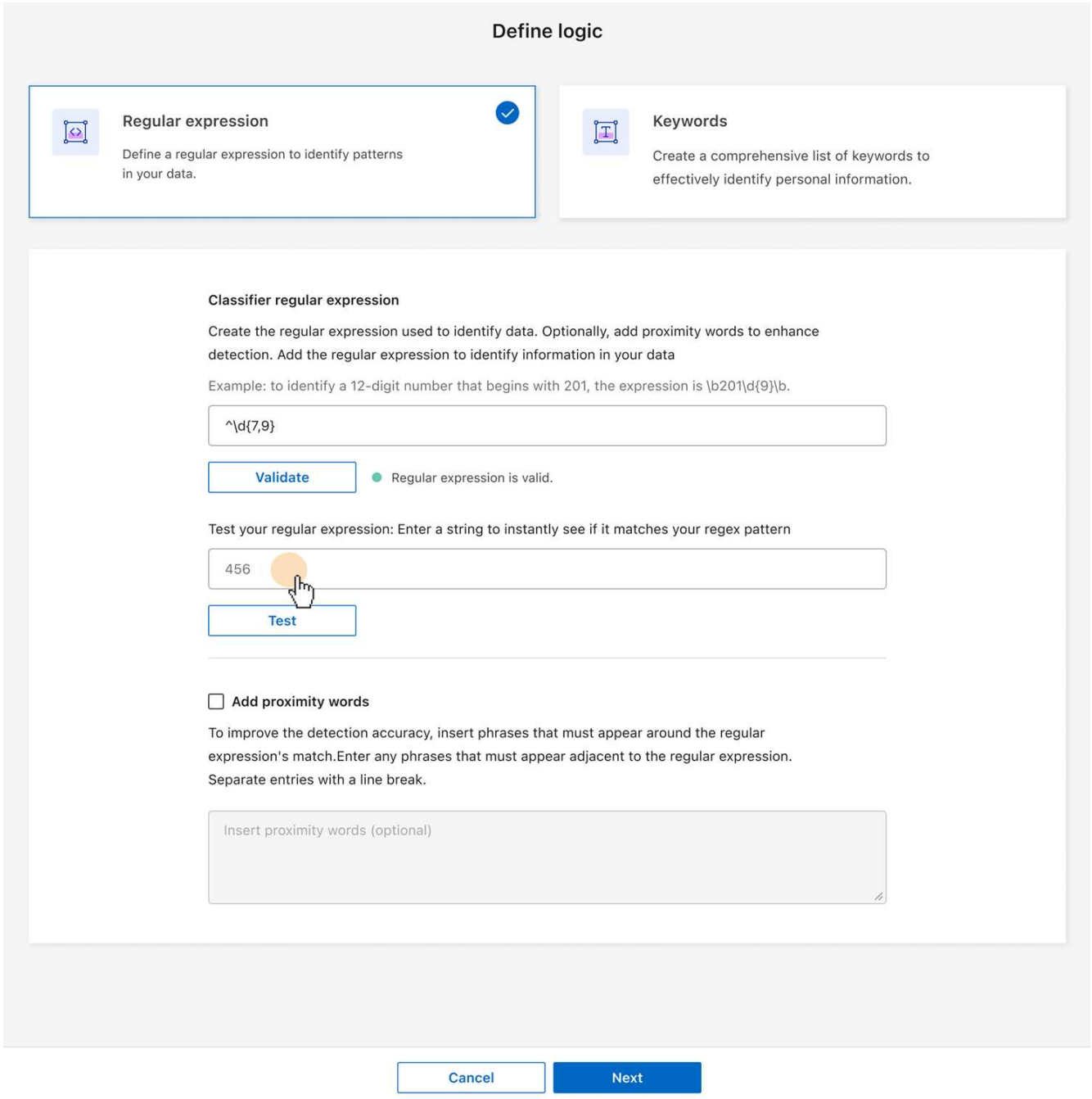
1. Seleccione la pestaña **Clasificación personalizada**.
2. Seleccione **+ Nuevo clasificador** para crear el clasificador personalizado.
3. Seleccione **Identificador personal**. Opcionalmente, seleccione **Ocultar resultados** para enmascarar los datos personales detectados.
4. Seleccione **Siguiente**.



5. Para agregar el clasificador con palabras clave, seleccione **Palabras clave**. Introduzca una lista de palabras clave, con cada entrada en una línea separada. Asegúrese de que las palabras clave cumplan con los requisitos.



Para agregar el clasificador como una expresión regular, seleccione **Expresión regular** y luego agregue un patrón para detectar la información específica de sus datos. Seleccione **Validar** para confirmar la sintaxis de su entrada.



a. Opcionalmente, ingrese una cadena de muestra que debe coincidir con su patrón de expresión regular y luego seleccione **Probar** para comprobarlo.

b. Opcionalmente, agregue palabras de proximidad. Si agrega palabras de proximidad, la clasificación de datos solo marca el patrón de expresión regular si las palabras de proximidad están adyacentes a la cadena coincidente.

6. Seleccione **Siguiente**.
7. Ingrese un **Nombre de clasificador** y una **Descripción** para identificar la categoría personalizada en su panel.
8. Seleccione **Guardar** para crear el identificador personal personalizado.

Después de crear un identificador personal personalizado, sus resultados se capturan en el próximo escaneo programado. Para capturar resultados antes, realice un análisis a pedido. Para ver los resultados, consulte

Generar informes de cumplimiento.

Crear una categoría personalizada

Con categorías personalizadas, puede categorizar datos específicos de su organización. Las categorías personalizadas se crean en función de los archivos de texto que usted carga, desde los cuales Data Classification crea un modelo de IA para identificar información similar en otros archivos.

Requisitos de datos de entrenamiento

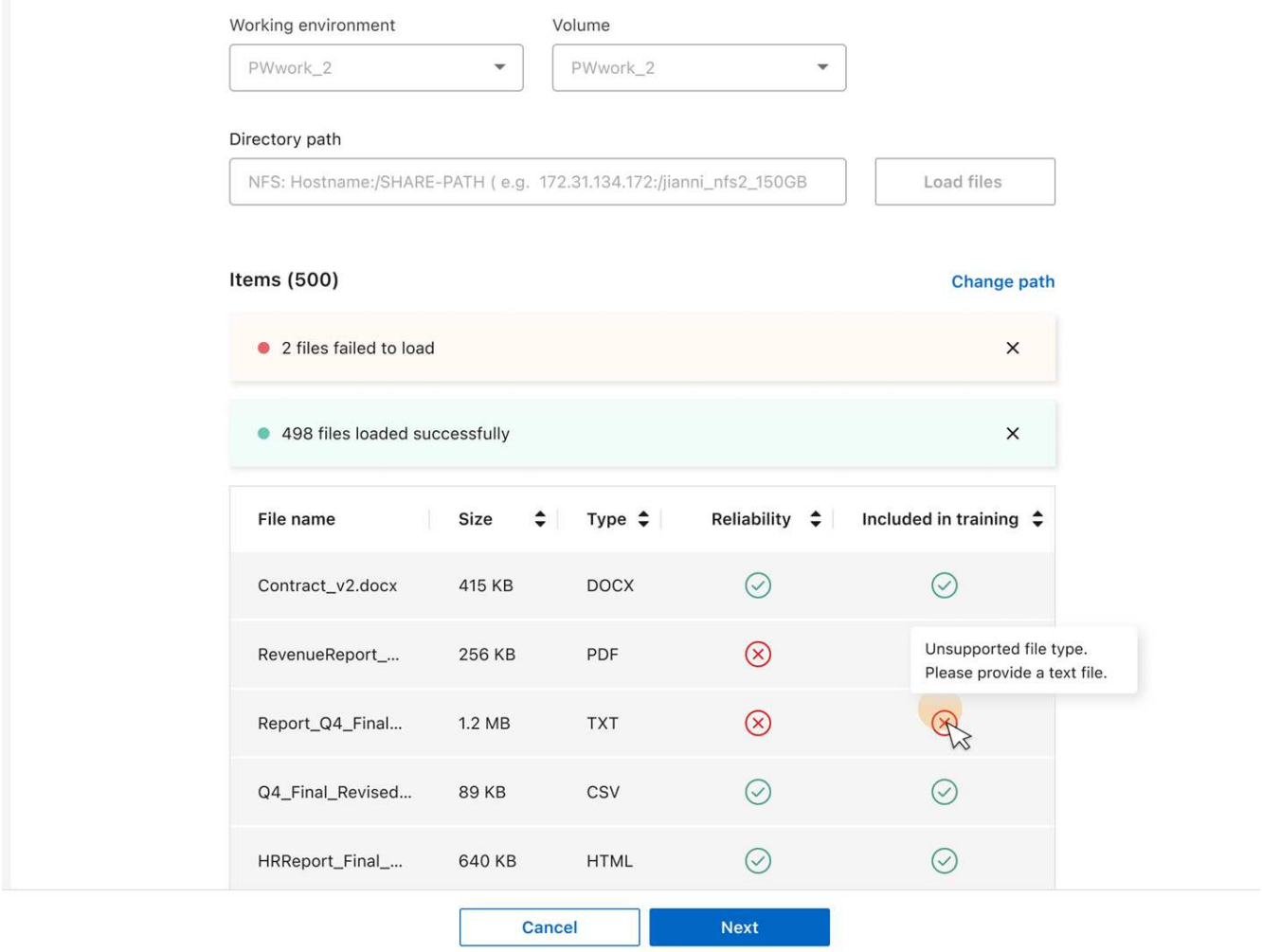
- El conjunto de datos de entrenamiento debe contener un mínimo de 25 archivos. El número máximo de archivos es 1000.
- Todos los archivos deben estar ubicados directamente en la ruta de archivo que usted proporcione.
- Todos los archivos deben tener más de 100 bytes.
- Los datos de entrenamiento de clasificación de datos deben ser uno de los siguientes tipos de archivos: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS o XLSX. Puede cargar una combinación de todos los tipos de archivos admitidos.

Pasos

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.
2. Seleccione **+ Nuevo clasificador**.
3. Seleccione **Categoría personalizada** como su tipo de clasificador y luego **Siguiente**.
4. Define la lógica de tu categoría personalizada con una colección de archivos basados en texto. Proporcione la dirección IP de la **Dirección de trabajo** y luego seleccione el **Volumen** en el menú desplegable.

   Ingrese la **Ruta del directorio** para el directorio que contiene los datos de entrenamiento.

5. Seleccione **Cargar archivos** para Clasificación de datos para realizar una verificación de los archivos. Puede revisar el resumen de los archivos, que enumera el nombre del archivo, el tamaño, el tipo y las notas si el archivo se consideró aceptable para la capacitación.



a. Para cambiar la ruta del archivo o volver a cargar archivos, seleccione **Cambiar ruta**, luego ingrese los datos y cargue los archivos nuevamente.

6. Cuando esté satisfecho con los archivos cargados, seleccione **Siguiente**.
7. Ingrese un **Nombre de clasificador** y una **Descripción** para identificar la categoría personalizada en su panel.
8. Seleccione **Guardar** para crear la categoría personalizada.

Resultado

Después de crear una categoría personalizada, sus resultados se capturan en el próximo análisis programado. Para capturar resultados antes, inicie el escaneo manualmente.

Editar un clasificador personalizado

Puede modificar la lógica de un identificador personal después de crearlo. No puede cambiar el tipo de identificador personal ni el tipo de lógica; por ejemplo, no puede cambiar una categoría personalizada a un identificador personal personalizado. Tampoco puedes cambiar un identificador personalizado basado en palabras clave a un identificador personalizado basado en expresiones regulares.

Pasos

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.
2. Identifique el clasificador que desea eliminar y luego seleccione el menú de acciones … al final de su fila.

3. Seleccione **Editar lógica**.
4. Si está modificando palabras clave, agregue, elimine o edite las palabras clave adecuadas. Si está modificando una expresión regular, ingrese la nueva expresión regular y valídela. Opcionalmente, agregue palabras clave de proximidad.
5. Seleccione **Guardar** para aplicar los cambios.

Eliminar un clasificador personalizado

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.
2. Identifique el clasificador que desea eliminar y luego seleccione el menú de acciones … al final de su fila.
3. Seleccione **Eliminar clasificador**.

Próximos pasos

- Generar informes de cumplimiento

Investigue los datos almacenados en su organización con NetApp Data Classification

El panel de investigación de datos muestra información a nivel de archivo y directorio sobre sus datos, lo que le permite ordenar y filtrar los resultados. La página Investigación de datos presenta información sobre metadatos y permisos de archivos y directorios, además de identificar archivos duplicados. Con información a nivel de archivo, directorio y base de datos, puede tomar medidas para mejorar el cumplimiento de su organización y ahorrar espacio de almacenamiento. La página Investigación de datos también admite mover, copiar y eliminar archivos.

Para obtener información de la página Investigación, debe realizar un análisis de clasificación completo de sus fuentes de datos. Las fuentes de datos que han tenido un escaneo de solo mapeo no muestran detalles a nivel de archivo.

Estructura de la investigación de datos

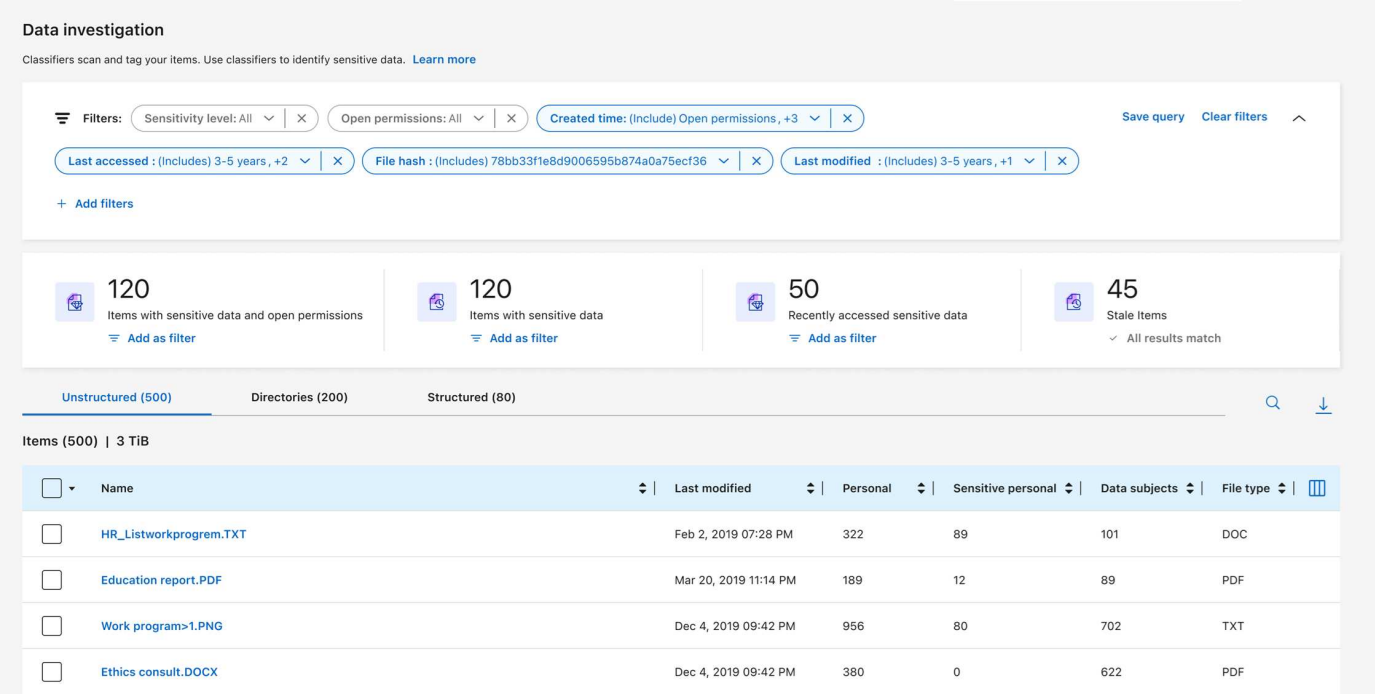
La página Investigación de datos clasifica los datos en tres pestañas:

- **Datos no estructurados**: datos de archivo
- **Directorios**: carpetas y recursos compartidos de archivos
- **Estructurado**: base de datos

Filtros de datos

La página de Investigación de datos proporciona numerosos filtros para ordenar sus datos para que pueda encontrar lo que necesita. Puedes utilizar varios filtros en conjunto.

Para agregar un filtro, seleccione el botón **Agregar filtro**.



Sensibilidad y contenido del filtro

Utilice los siguientes filtros para ver cuánta información confidencial contienen sus datos.

Filtrar	Detalles
Categoría	Seleccione el"tipos de categorías" .
Nivel de sensibilidad	Seleccione el nivel de sensibilidad: Personal, Personal sensible o No sensible.
Número de identificadores	Seleccione el rango de identificadores sensibles detectados por archivo. Incluye datos personales y datos personales sensibles. Al filtrar en directorios, la clasificación de datos totaliza las coincidencias de todos los archivos en cada carpeta (y subcarpetas). NOTA: La versión de diciembre de 2023 (versión 1.26.6) eliminó la opción para calcular la cantidad de datos de información personal identificable (PII) por directorios.
Datos personales	Seleccione el"tipos de datos personales" .
Datos personales sensibles	Seleccione el"tipos de datos personales sensibles" .
Titular de los datos	Introduzca el nombre completo o un identificador conocido del interesado. "Obtenga más información sobre los interesados aquí" .

Filtrar propietario de usuario y permisos de usuario

Utilice los siguientes filtros para ver los propietarios de archivos y los permisos para acceder a sus datos.

Filtrar	Detalles
Permisos abiertos	Seleccione el tipo de permisos dentro de los datos y dentro de las carpetas/recursos compartidos.

Filtrar	Detalles
Permisos de usuario/grupo	Seleccione uno o varios nombres de usuario y/o nombres de grupo, o ingrese 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 para una determinada cantidad de usuarios.

Filtrar cronológicamente

Utilice los siguientes filtros para ver datos según criterios de tiempo.

Filtrar	Detalles
Tiempo creado	Seleccione un rango de tiempo cuando se creó el archivo. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda.
Tiempo descubierto	Seleccione un rango de tiempo cuando la Clasificación de datos descubrió el archivo. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda.
Última modificación	Seleccione un rango de tiempo cuando el archivo fue modificado por última vez. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda.
Último acceso	Seleccione un rango de tiempo cuando se accedió por última vez al archivo o directorio*. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda. Para los tipos de archivos que Data Classification escanea, esta es la última vez que Data Classification escaneó el archivo.

* La hora del último acceso a un directorio solo está disponible para recursos compartidos NFS o CIFS.

Filtrar metadatos

Utilice los siguientes filtros para ver datos según ubicación, tamaño y directorio o tipo de archivo.

Filtrar	Detalles
Ruta del archivo	Ingrese hasta 20 rutas parciales o completas que desee incluir o excluir de la consulta. Si ingresa rutas de inclusión y rutas de exclusión, la Clasificación de datos busca primero todos los archivos en las rutas incluidas, luego elimina los archivos de las rutas excluidas y luego 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 bajo un recurso compartido configurado.
Tipo de directorio	Seleccione el tipo de directorio; "Compartir" o "Carpeta".
Tipo de archivo	Seleccione el"tipos de archivos" .
Tamaño del archivo	Seleccione el rango de tamaño del archivo.

Filtrar	Detalles
Hash de archivo	Ingrese el hash del archivo para encontrar un archivo específico, incluso si el nombre es diferente.

Tipo de almacenamiento de filtro

Utilice los siguientes filtros para ver los datos por tipo de almacenamiento.

Filtrar	Detalles
Tipo de sistema	Seleccione el tipo de sistema.
Nombre del entorno del sistema	Seleccione sistemas específicos.
Repositorio de almacenamiento	Seleccione el repositorio de almacenamiento, por ejemplo, un volumen o un esquema.

Consulta de filtro

Utilice el siguiente filtro para ver los datos por consultas guardadas.

Filtrar	Detalles
Consulta guardada	Seleccione una consulta guardada o varias. Ir a la"pestaña de consultas guardadas" para ver la lista de consultas guardadas existentes y crear otras nuevas.
Etiquetas	Seleccionar"la etiqueta o etiquetas" que están asignados a sus archivos.

Estado del análisis del filtro

Utilice el siguiente filtro para ver los datos según el estado del escaneo de clasificación de datos.

Filtrar	Detalles
Estado del análisis	Seleccione una opción para mostrar la lista de archivos que están pendientes de primer escaneo, cuyo escaneo se completó, pendientes de reescaneo o cuyo escaneo no se pudo realizar.
Evento de análisis de escaneo	Seleccione si desea ver los archivos que no se clasificaron porque la Clasificación de datos no pudo revertir la hora del último acceso, o los archivos que se clasificaron aunque la Clasificación de datos no pudo revertir la hora del último acceso.

"Ver detalles sobre la marca de tiempo de "último acceso""para obtener más información sobre los elementos que aparecen en la página Investigación al filtrar mediante el Evento de análisis de escaneo.

Filtrar datos por duplicados

Utilice el siguiente filtro para ver los archivos que están duplicados en su almacenamiento.

Filtrar	Detalles
Duplicados	Seleccione si el archivo está duplicado en los repositorios.

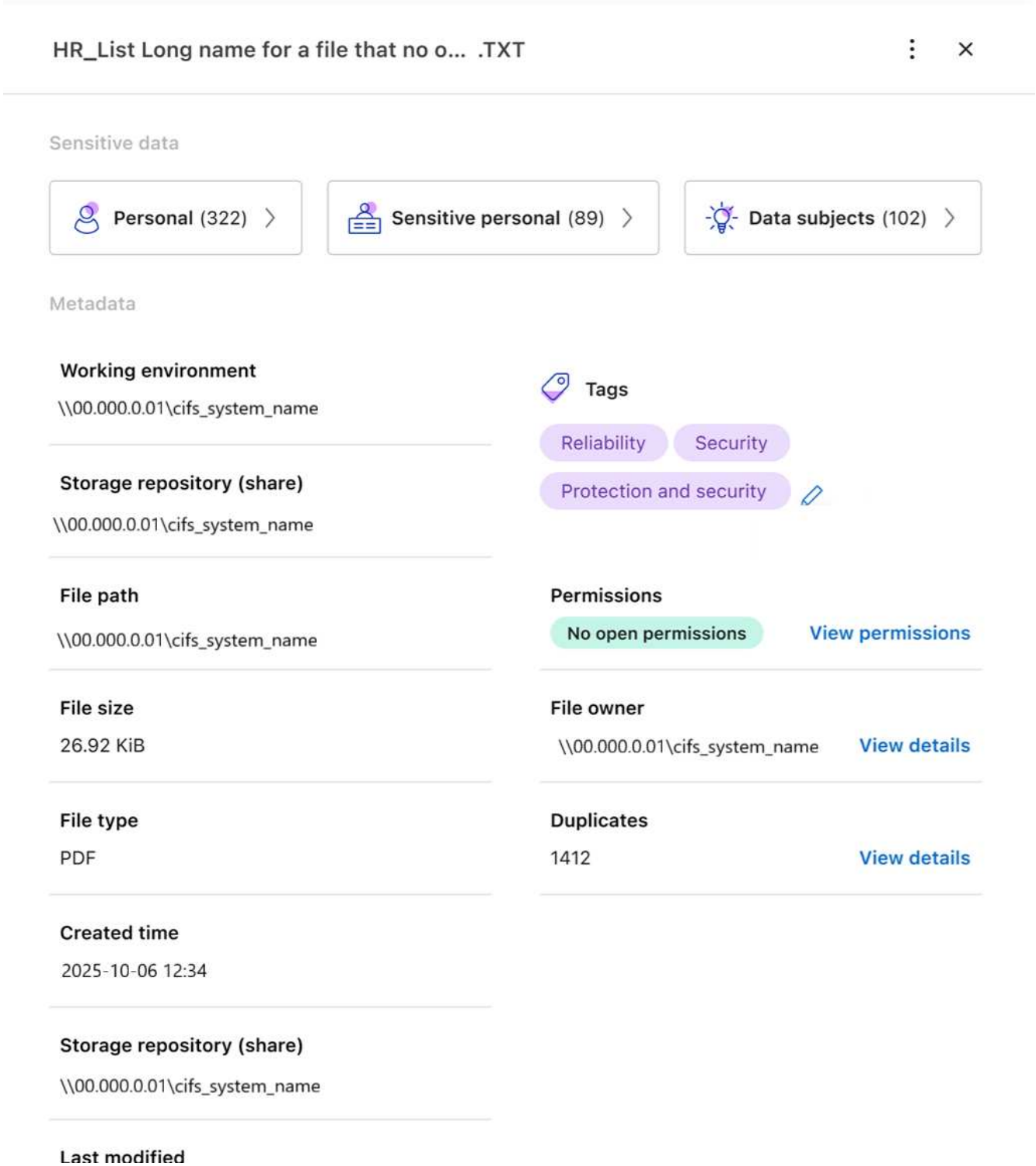
Ver metadatos del archivo

Además de mostrarle el sistema y el volumen donde reside el archivo, los metadatos muestran mucha más información, incluidos los permisos del archivo, el propietario del archivo y si hay duplicados de este archivo. Esta información es útil si estás planeando"crear consultas guardadas" porque podrás ver toda la información que puedes utilizar para filtrar tus datos.

La disponibilidad de la información depende de la fuente de datos. Por ejemplo, el nombre del volumen y los permisos no se comparten para los archivos de base de datos.

Pasos

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos a la derecha, seleccione el símbolo de cursor hacia abajo a la derecha para cualquier archivo individual para ver los metadatos del archivo.



3. Opcionalmente, puede crear o agregar una etiqueta al archivo con el botón **Crear etiqueta**. Seleccione una etiqueta existente del menú desplegable o agregue una nueva etiqueta con el botón **+ Agregar**. Las etiquetas se pueden utilizar para filtrar datos.

Ver permisos de usuario 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, seleccione **Ver todos los permisos**. Esta opción solo está disponible para datos en recursos compartidos CIFS.

Si utiliza identificadores de seguridad (SID) en lugar de nombres de usuarios y grupos, debe integrar su Active Directory en la clasificación de datos. Para obtener más información, consulte "Agregar Active Directory a la clasificación de datos" .

Pasos

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos a la derecha, seleccione el símbolo de cursor hacia abajo a la derecha para cualquier archivo individual para ver los metadatos del archivo.
3. 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, en el campo Permisos abiertos, seleccione **Ver todos los permisos**.

   La clasificación de datos muestra hasta 100 usuarios en la lista.

4. Seleccione el cursor hacia abajo Botón para que cualquier grupo vea la lista de usuarios que forman parte del grupo.

   Puedes expandir un nivel del grupo para ver los usuarios que forman parte del grupo.

5. Seleccione el nombre de un usuario o grupo para actualizar la página de Investigación para que pueda ver todos los archivos y directorios a los que el usuario o grupo tiene acceso.

Compruebe si hay archivos duplicados en sus sistemas de almacenamiento

Puede comprobar si se están almacenando archivos duplicados en sus sistemas de almacenamiento. Esto es útil si desea identificar áreas donde puede ahorrar espacio de almacenamiento. También es bueno asegurarse de que ciertos archivos que tienen permisos específicos o información confidencial no se dupliquen innecesariamente en sus sistemas de almacenamiento.

La clasificación de datos compara todos los archivos (excluidas las bases de datos) en busca de duplicados si son:

- 1 MB o lager
- O contienen información personal o información personal sensible.

La clasificación de datos utiliza tecnología hash para determinar archivos duplicados. Si dos archivos tienen el mismo código hash que otros, son duplicados exactos aunque sus nombres sean diferentes.

Pasos

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En el panel Filtro, seleccione "Tamaño de archivo" junto con "Duplicados" ("Tiene duplicados") para ver qué archivos de un determinado rango de tamaño están duplicados en su entorno.
3. Opcionalmente, descargue la lista de archivos duplicados y envíela a su administrador de almacenamiento para que pueda decidir qué archivos, si hay alguno, se pueden eliminar.
4. Opcionalmente, puede eliminar, etiquetar o mover los archivos duplicados. Seleccione los archivos en los que desea realizar una acción y luego seleccione la acción adecuada.

Ver si un archivo específico está duplicado

Puede ver si un solo archivo tiene duplicados.

Pasos

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos, seleccione ⌄ a la derecha para cualquier archivo individual para ver los metadatos del archivo.

   Si existen duplicados para un archivo, esta información aparece junto al campo *Duplicados*.

3. Para ver la lista de archivos duplicados y dónde se encuentran, seleccione **Ver detalles**.
4. En la página siguiente, seleccione **Ver duplicados** para ver los archivos en la página de Investigación.
5. Opcionalmente, puede eliminar, etiquetar o mover los archivos duplicados. Seleccione los archivos en los que desea realizar una acción y luego seleccione la acción adecuada.

> Puede utilizar el valor de "hash de archivo" proporcionado en esta página e ingresarlo directamente en la página de Investigación para buscar un archivo duplicado específico en cualquier momento, o puede usarlo en una consulta guardada.

Descargue su informe

Puede descargar sus resultados filtrados en formato CSV o JSON.

Se pueden descargar hasta tres archivos de informe si la clasificación de datos escanea archivos (datos no estructurados), directorios (carpetas y recursos compartidos de archivos) y bases de datos (datos estructurados).

Los archivos se dividen en archivos con un número fijo de filas o registros:

- JSON: 100.000 registros por informe que tarda unos 5 minutos en generarse
- CSV: 200.000 registros por informe que tarda aproximadamente 4 minutos en generarse

> Puede descargar una versión del archivo CSV para verlo en este navegador. Esta versión está limitada a 10.000 registros.

Qué incluye el informe descargable

El **Informe de datos de archivos no estructurados** incluye la siguiente información sobre sus archivos:

- Nombre del archivo
- Tipo de ubicación
- Nombre del sistema
- Repositorio de almacenamiento (por ejemplo, un volumen, un depósito, recursos compartidos)
- Tipo de repositorio
- Ruta del archivo
- Tipo de archivo
- Tamaño del archivo (en MB)
- Hora de creación
- Última modificación
- Último acceso

- Propietario del archivo
  - Los datos del propietario del archivo incluyen el nombre de la cuenta, el nombre de la cuenta SAM y la dirección de correo electrónico cuando se configura Active Directory.
- Categoría
- Información personal
- Información personal sensible
- Permisos abiertos
- Error de análisis de escaneo
- Fecha de detección de eliminación

  La 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 archivos confidenciales. Los archivos eliminados no contribuyen al recuento de números de archivos que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

El **Informe de datos de directorios no estructurados** incluye la siguiente información sobre sus carpetas y recursos compartidos de archivos:

- Tipo de sistema
- Nombre del sistema
- Nombre del directorio
- Repositorio de almacenamiento (por ejemplo, una carpeta o recursos compartidos de archivos)
- Propietario del directorio
- Hora de creación
- Tiempo descubierto
- Última modificación
- Último acceso
- Permisos abiertos
- Tipo de directorio

El **Informe de datos estructurados** incluye la siguiente información sobre las tablas de su base de datos:

- Nombre de la tabla de la base de datos
- Tipo de ubicación
- Nombre del sistema
- Repositorio de almacenamiento (por ejemplo, un esquema)
- Recuento de columnas
- Recuento de filas
- Información personal
- Información personal sensible

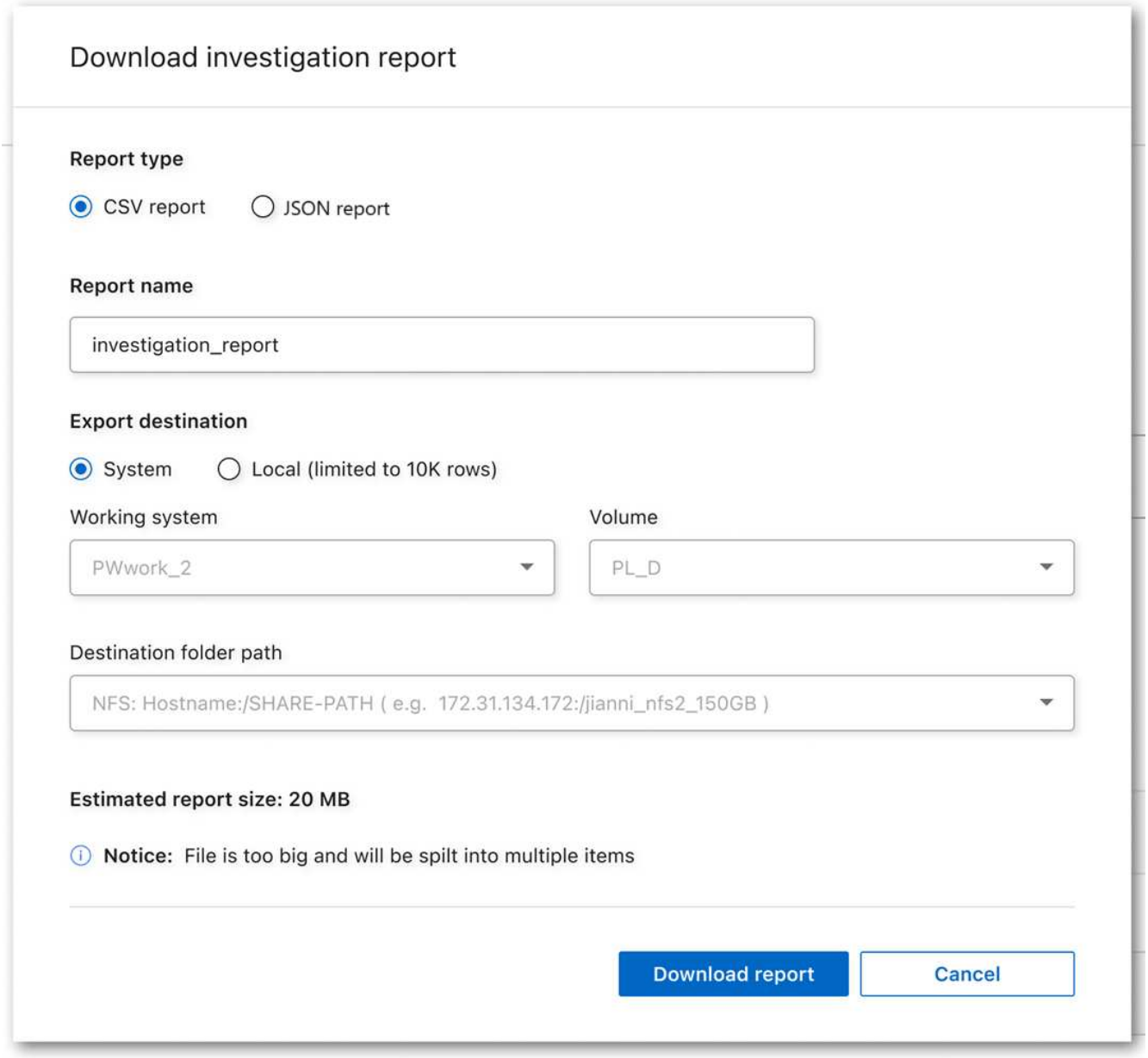
Pasos para generar el informe

1. Desde la página Investigación de datos, seleccione el Botón en la parte superior derecha de la página.

2. Elija el tipo de informe: CSV o JSON.
3. Introduzca un **nombre de informe**.
4. Para descargar el informe completo, seleccione **Sistema** y luego elija **Sistema** y **Volumen** en los respectivos menús desplegables. Proporcione una **Ruta de carpeta de destino**.

   Para descargar el informe en el navegador, seleccione **Local** . Tenga en cuenta que esta opción limita el informe a las primeras 10 000 filas y está limitada al formato **CSV**. No es necesario completar ningún otro campo si selecciona **Local**.

5. Seleccione **Descargar informe**.



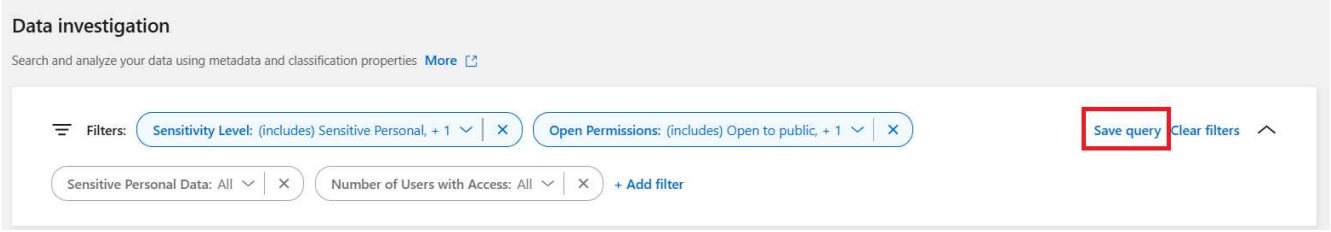
Resultado

Un cuadro de diálogo muestra un mensaje que indica que se están descargando los informes.

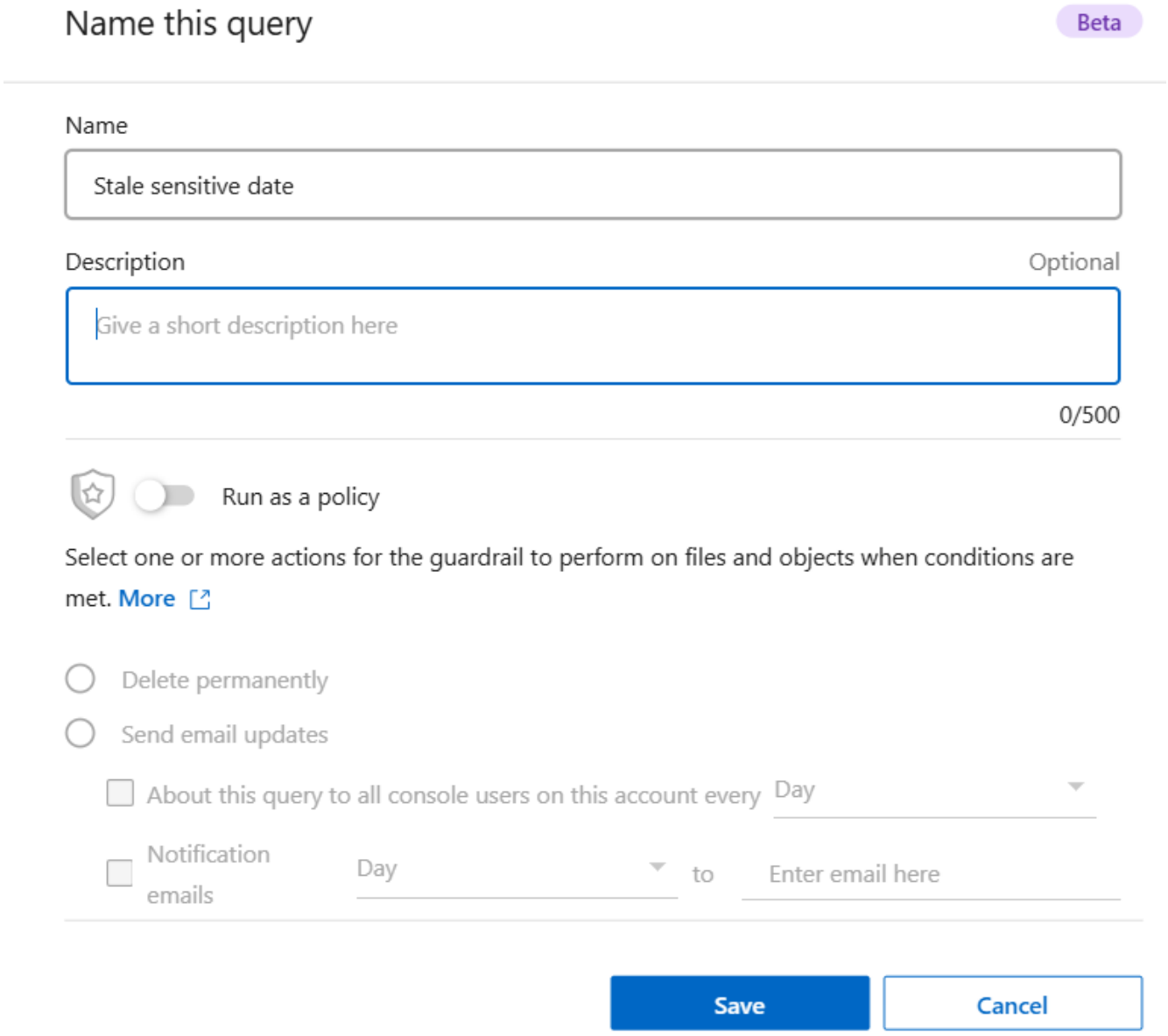
Crear una consulta guardada basada en filtros seleccionados

Pasos

1. En la pestaña Investigación, defina una búsqueda seleccionando los filtros que desea utilizar. Ver"Filtrado de datos en la página de Investigación" Para más detalles.
2. Una vez que tenga todas las características del filtro configuradas a su gusto, seleccione **Guardar consulta**.



3. Nombra la consulta guardada y agrega una descripción. El nombre debe ser único.
4. Opcionalmente, puede guardar la consulta como política:
   a. Para guardar la consulta como una política, cambie el interruptor **Ejecutar como política**.
   b. Elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.
5. Seleccione **Guardar**.



Una vez que haya creado la búsqueda o política, podrá verla en la pestaña **Consultas guardadas**.

Los resultados pueden tardar hasta 15 minutos en aparecer en la página Consultas guardadas.

Administre consultas guardadas con NetApp Data Classification

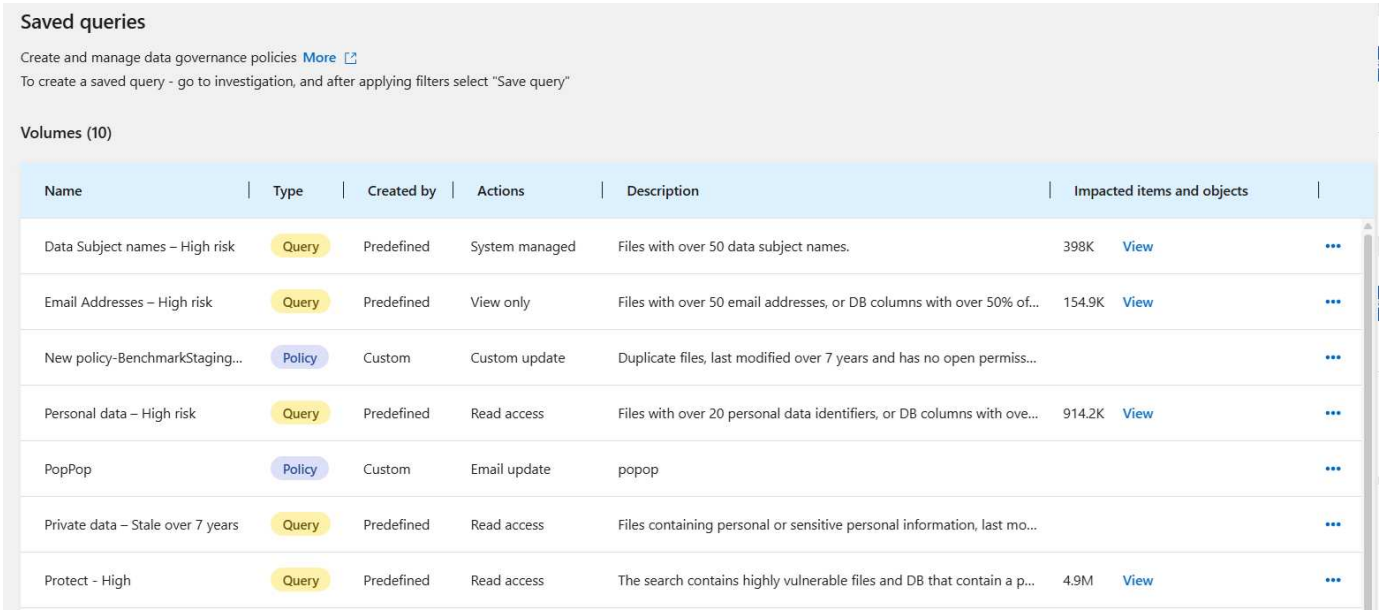
La clasificación de datos de NetaApp permite guardar sus consultas de búsqueda. Con una consulta guardada, puede crear filtros personalizados para ordenar las consultas frecuentes de su página de investigación de datos. La clasificación de datos también incluye consultas guardadas predefinidas basadas en solicitudes comunes.

La pestaña **Consultas guardadas** en el panel de Cumplimiento enumera todas las consultas guardadas

predefinidas y personalizadas disponibles en esta instancia de Clasificación de datos.

Las consultas guardadas también se pueden guardar como **políticas**. Mientras que las consultas filtran datos, las políticas le permiten actuar sobre los datos. Con una política: puede eliminar datos descubiertos o enviar actualizaciones por correo electrónico sobre los datos descubiertos.

Las consultas guardadas también aparecen en la lista de filtros en la página Investigación.



Ver los resultados de las consultas guardadas en la página de Investigación

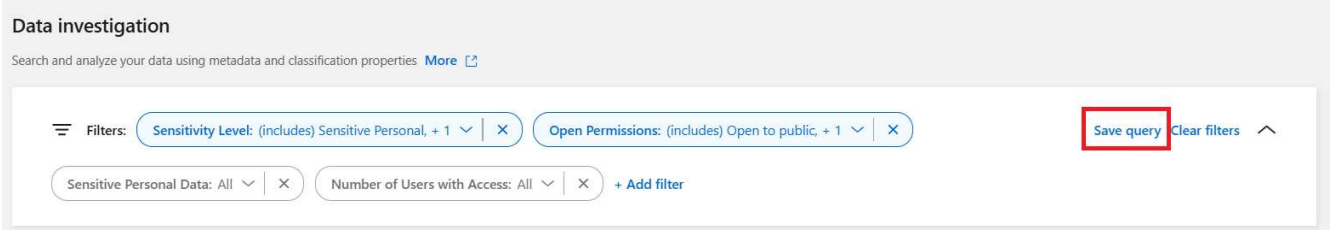
Para mostrar los resultados de una consulta guardada en la página Investigación, seleccione el icono Botón para una búsqueda específica y luego seleccione **Investigar resultados**.

Crear consultas y políticas guardadas

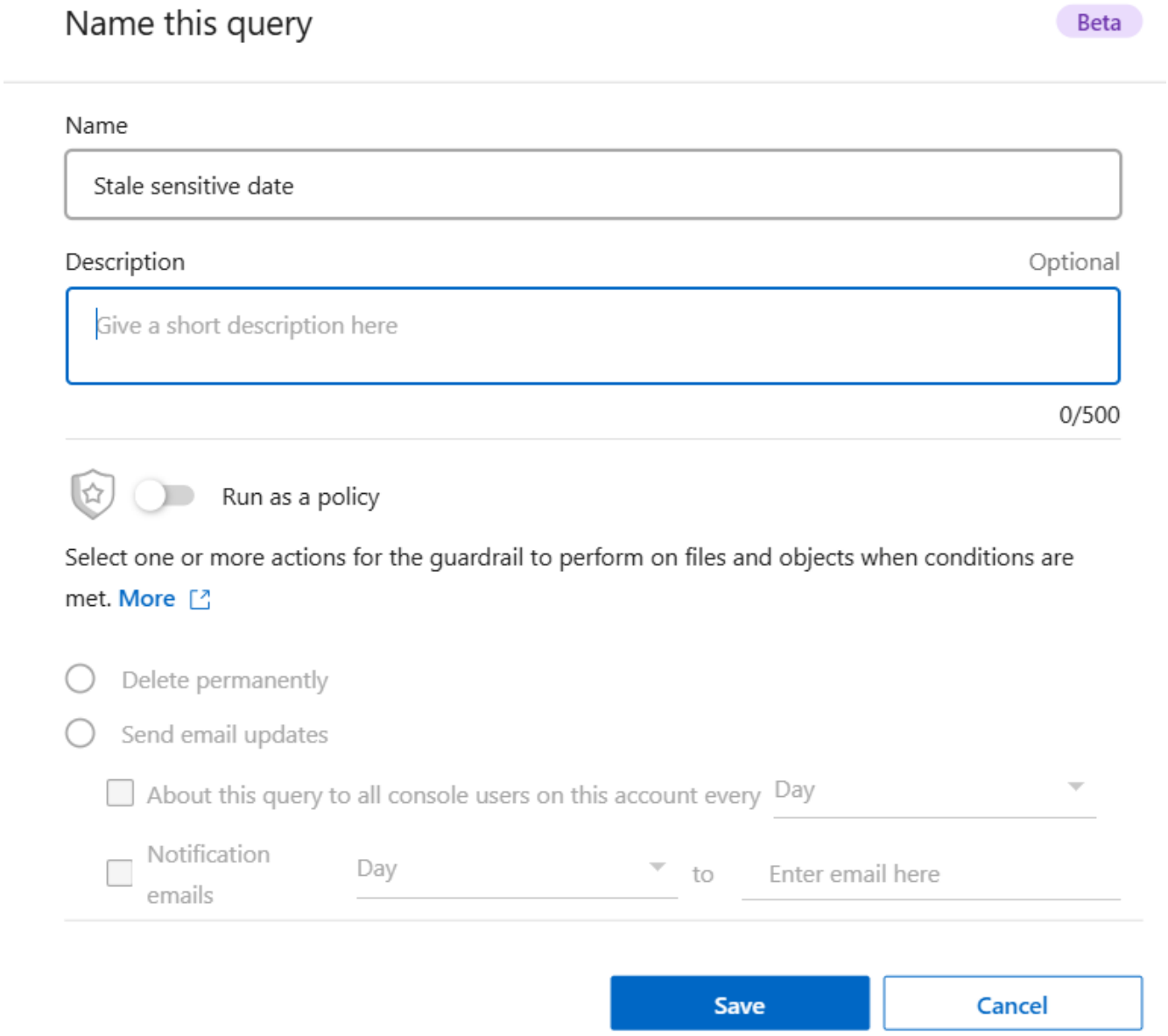
Puede crear sus propias consultas guardadas personalizadas que proporcionen resultados para consultas específicas de su organización. Se devuelven resultados para todos los archivos y directorios (recursos compartidos y carpetas) que coinciden con los criterios de búsqueda.

Pasos

1. En la pestaña Investigación, defina una búsqueda seleccionando los filtros que desea utilizar. Ver"Filtrado de datos en la página de Investigación" Para más detalles.
2. Una vez que tenga todas las características del filtro configuradas a su gusto, seleccione **Guardar consulta**.



3. Nombra la consulta guardada y agrega una descripción. El nombre debe ser único.
4. Opcionalmente, puede guardar la consulta como política:
   a. Para guardar la consulta como una política, cambie el interruptor **Ejecutar como política**.
   b. Elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.
5. Seleccione **Guardar**.



Una vez que haya creado la búsqueda o política, podrá verla en la pestaña **Consultas guardadas**.

Editar consultas o políticas guardadas

Puede modificar el nombre y la descripción de una consulta guardada. También puede convertir una consulta en una política y viceversa.

No se pueden modificar las consultas guardadas predeterminadas. No se pueden modificar los filtros de una consulta guardada. Alternativamente, puede ver los resultados de la investigación de una consulta guardada, cambiar o modificar los filtros y luego guardarla como una nueva consulta o política.

Pasos

1. Desde la página Consultas guardadas, seleccione **Editar búsqueda** para la búsqueda que desea cambiar.

2. Realice los cambios en los campos de nombre y descripción. Para cambiar únicamente los campos de nombre y descripción.

   Opcionalmente, puede convertir la consulta en una política o convertir la política en una consulta guardada. Cambie el interruptor **Ejecutar como política** según sea necesario. .. Si está convirtiendo la consulta en una política, elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.

3. Seleccione **Guardar** para completar los cambios.

Eliminar consultas guardadas

Puede eliminar cualquier consulta o política guardada personalizada si ya no la necesita. No puedes eliminar las consultas guardadas predeterminadas.

Para eliminar una consulta guardada, seleccione el Botón para una búsqueda específica, seleccione **Eliminar consulta**, luego seleccione **Eliminar consulta** nuevamente en el cuadro de diálogo de confirmación.

Consultas predeterminadas

La clasificación de datos proporciona las siguientes consultas de búsqueda definidas por el sistema:

- **Nombres de los interesados - Alto riesgo**

  Archivos con más de 50 nombres de interesados

- **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

- **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

- **Datos privados - Obsoletos durante más de 7 años**

  Archivos que contienen información personal o información personal sensible, modificados por última vez hace más de 7 años

- **Protección - Alta**

  Archivos o columnas de base de datos que contienen una contraseña, información de tarjeta de crédito, número IBAN o número de seguro social

- **Protección - Baja**

  Archivos a los que no se ha accedido durante más de 3 años

- **Protección - Media**

  Archivos que contienen archivos o columnas de bases de datos con identificadores de datos personales, incluidos números de identificación, números de identificación fiscal, números de licencia de conducir, identificaciones médicas o números de pasaporte

- **Datos personales sensibles - 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

Cambie la configuración del análisis de NetApp Data Classification para sus repositorios

Puede administrar cómo se escanean sus datos en cada uno de sus sistemas y fuentes de datos. Puede realizar los cambios sobre la base de un "repositorio", lo que significa que puede realizar cambios para cada volumen, esquema, usuario, etc., dependiendo del tipo de fuente de datos que esté escaneando.

Algunas de las cosas que puede cambiar son si se escanea o no un repositorio y si NetApp Data Classification está realizando una"escaneo de mapeo o escaneo de mapeo y clasificación" . También puede pausar y reanudar el escaneo, por ejemplo, si necesita dejar de escanear un volumen por un período de tiempo.

Ver el estado del escaneo de sus repositorios

Puede ver los repositorios individuales que NetApp Data Classification está escaneando (volúmenes, depósitos, etc.) para cada sistema y fuente de datos. También puedes ver cuántos han sido "Mapeados" y cuántos han sido "Clasificados". La clasificación lleva más tiempo porque la identificación completa de la IA se realiza en todos los datos.

Puede ver el estado de escaneo de cada entorno de trabajo en la página de Configuración:

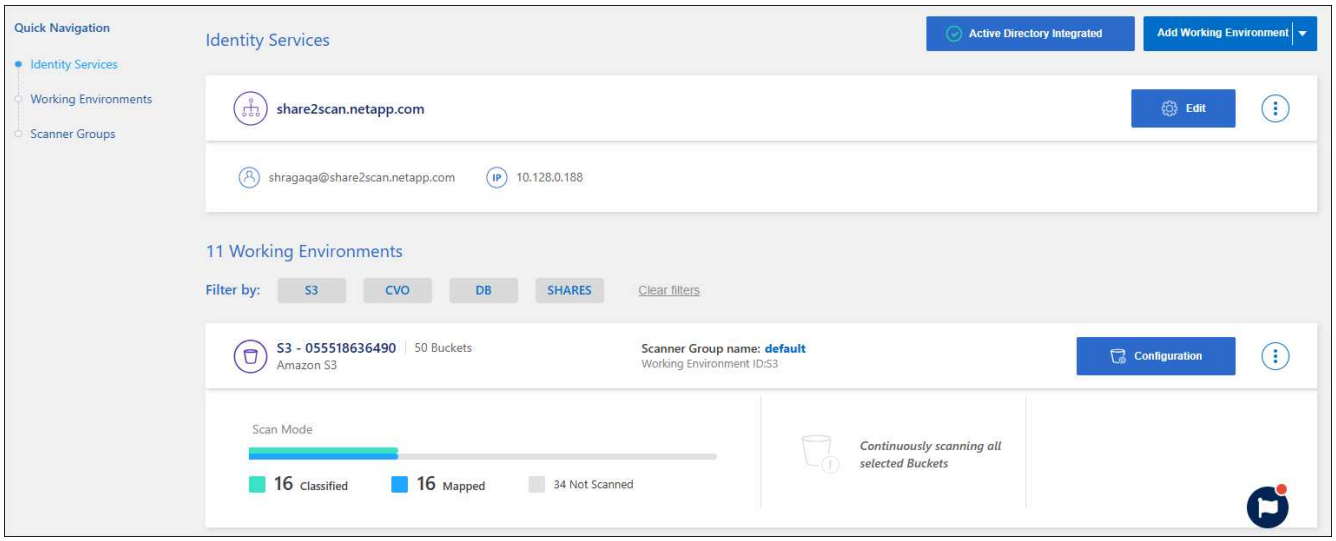
- **Inicializando** (punto azul claro): La configuración del mapa o clasificación está activada. Esto aparece brevemente antes de pasar al estado de "cola pendiente".
- **Cola pendiente** (punto naranja): la tarea de escaneo está esperando a ser incluida en la cola de escaneo.
- **En cola** (punto naranja): La tarea se agregó correctamente a la cola de escaneo. El sistema comenzará a mapear o clasificar el volumen cuando llegue su turno en la cola.
- **En ejecución** (punto verde): la tarea de escaneo, que estaba en la cola, está en progreso activo en el repositorio de almacenamiento seleccionado.
- **Terminado** (punto verde): El escaneo del repositorio de almacenamiento está completo.
- **Pausa** (punto gris): Has pausado el escaneo. Aunque los cambios en el volumen no se muestran en el sistema, la información obtenida mediante el escaneo permanece disponible.
- **Error** (punto rojo): El escaneo no puede completarse porque encontró problemas. Si necesita completar una acción, el error aparece en la información sobre herramientas debajo de la columna “Acción requerida”. De lo contrario, el sistema muestra un estado de “error” e intenta recuperarse. Cuando termina

el estado cambia.

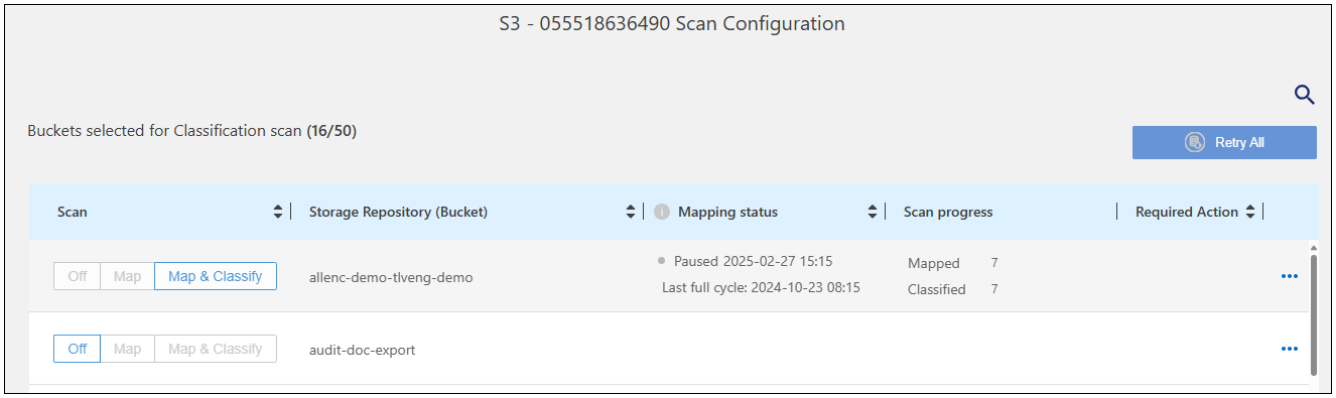
- **No escanea**: Se seleccionó la configuración de volumen “Desactivado” y el sistema no está escaneando el volumen.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.



2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.
3. En la página Configuración de escaneo, vea las configuraciones de escaneo para todos los repositorios.



4. Durante un escaneo, coloque el cursor sobre la barra de progreso en la columna *Estado de mapeo* para ver la cantidad de archivos en la cola que se deben mapear o clasificar para ese repositorio.

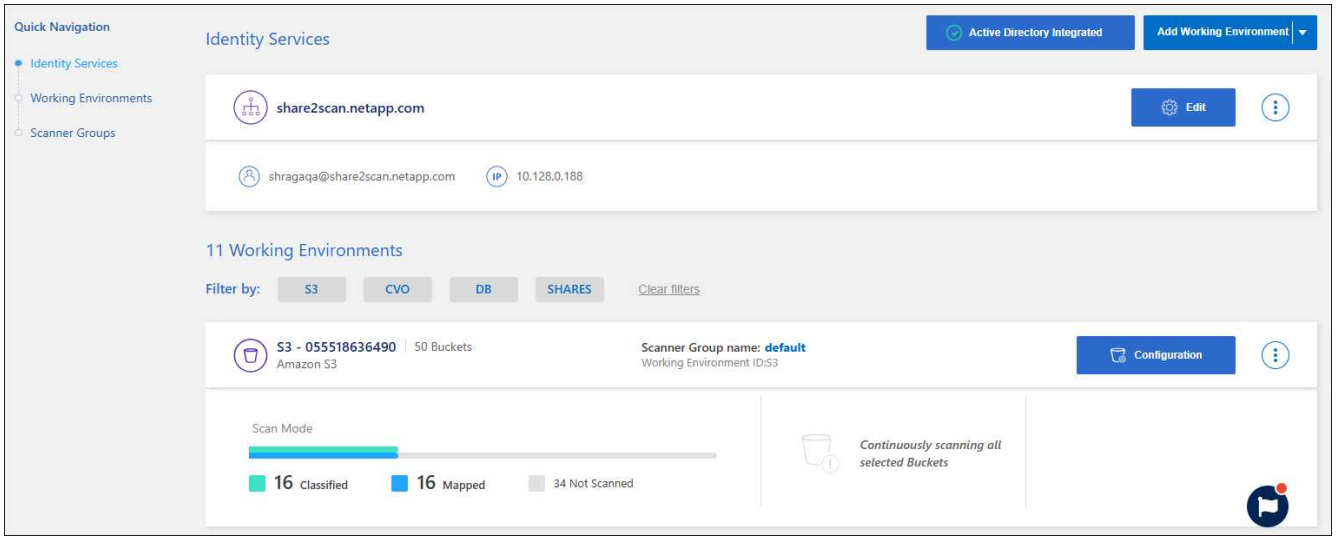
Cambiar el tipo de escaneo de un repositorio

Puede iniciar o detener escaneos de solo mapeo, o escaneos de mapeo y clasificación, en un sistema en cualquier momento desde la página de Configuración. También puede cambiar de escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa.

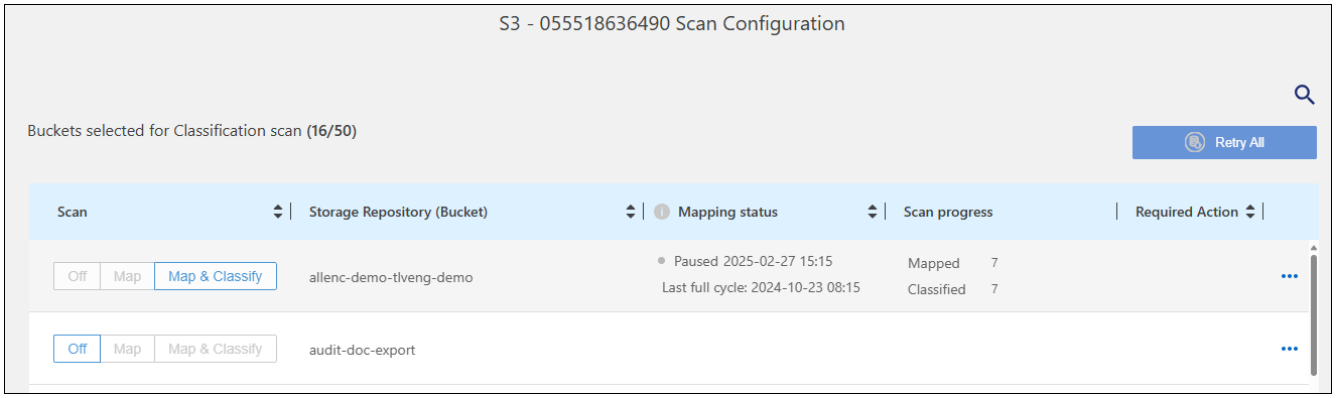
Las bases de datos no se pueden configurar para realizar exploraciones de solo mapeo. El escaneo de la base de datos puede estar Desactivado o Activado; donde Activado es equivalente a Mapear y clasificar.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.

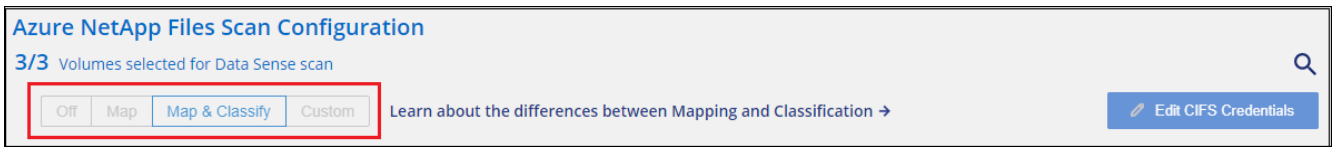


3. En la página Configuración de escaneo, cambie cualquiera de los repositorios (depósitos en este ejemplo) para realizar escaneos **Map** o **Map & Classify**.



Ciertos tipos de sistemas le permiten cambiar el tipo de escaneo globalmente para todos los repositorios usando una barra de botones en la parte superior de la página. Esto es válido para Cloud Volumes ONTAP, ONTAP local, Azure NetApp Files y Amazon FSx para sistemas ONTAP .

El siguiente ejemplo muestra esta barra de botones para un sistema Azure NetApp Files .



Priorizar los escaneos

Puede priorizar los escaneos de solo mapeo más importantes o mapear y clasificar los escaneos para garantizar que los escaneos de alta prioridad se completen primero.

De forma predeterminada, los escaneos se ponen en cola según el orden en el que se inician. Con la capacidad de priorizar los escaneos, puede moverlos al frente de la cola. Se pueden priorizar múltiples

escaneos. La prioridad se designa en un orden de primero en entrar, primero en salir, lo que significa que el primer escaneo que prioriza pasa al frente de la cola; el segundo escaneo que prioriza pasa al segundo en la cola, y así sucesivamente.

La prioridad se concede por única vez. Los escaneos automáticos de datos cartográficos se realizan en el orden predeterminado.

Pasos

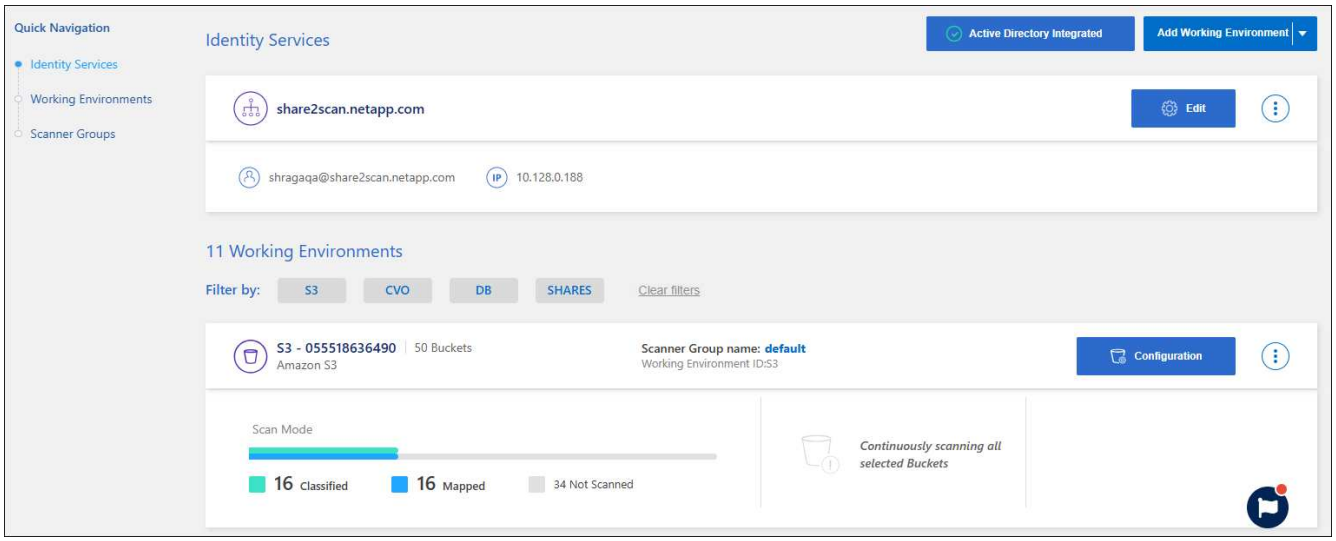
1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione los recursos que desea priorizar.
3. De las acciones … opción, seleccione **Priorizar escaneo**.

Detener la búsqueda de un repositorio

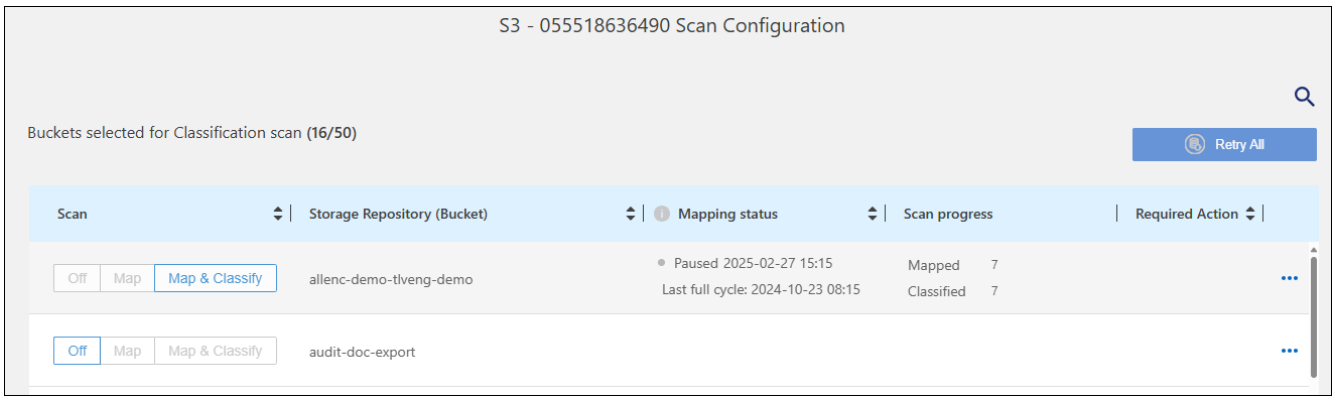
Puede dejar de escanear un repositorio (por ejemplo, un volumen) si ya no necesita supervisarlo para verificar su cumplimiento. Puedes hacer esto desactivando el escaneo. Cuando se desactiva el escaneo, se eliminan del sistema toda la indexación y la información sobre ese volumen y se detiene el cobro por escanear los datos.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.



3. En la página Configuración de escaneo, seleccione **Desactivado** para detener el escaneo de un depósito en particular.



Pausar y reanudar el escaneo de un repositorio

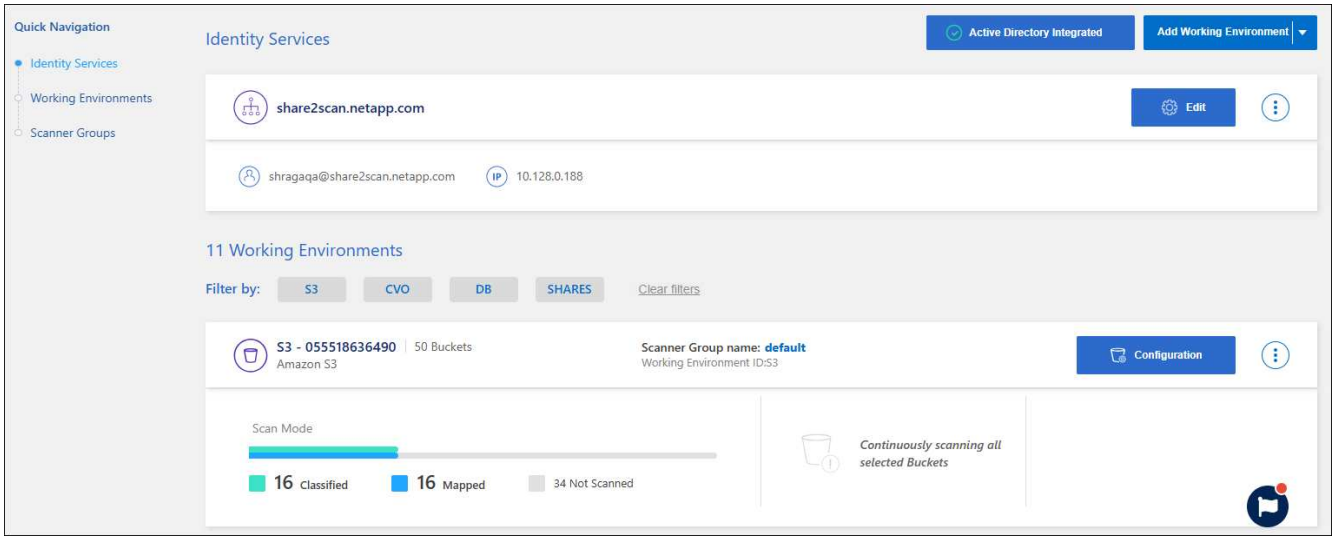
Puede "pausar" el escaneo en un repositorio si desea detener temporalmente el escaneo de cierto contenido. Pausar el escaneo significa que la Clasificación de Datos no realizará más escaneos para detectar cambios o adiciones al repositorio. Todos los resultados de escaneo actuales permanecen accesibles en la Clasificación de datos.

Si pausas los escaneos, no se eliminan los cargos de facturación porque los datos aún están en el sistema.

Puede reanudar el escaneo en cualquier momento.

Pasos

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.



3. En la página Configuración de escaneo, seleccione Acciones ••• icono.
4. Seleccione **Pausa** para pausar el escaneo de un volumen, o seleccione **Reanudar** para reanudar el escaneo de un volumen que se había pausado previamente.

Ver informes de cumplimiento de NetApp Data Classification

La NetApp Data Classification proporciona informes que puede utilizar para comprender mejor el estado del programa de privacidad de datos de su organización.

De forma predeterminada, los paneles de clasificación de datos muestran datos de cumplimiento y gobernanza de todos los sistemas, bases de datos y fuentes de datos. Si desea ver informes que contienen datos solo de algunos de los sistemas, puede filtrar para ver solo esos.

- Los informes de cumplimiento solo están disponibles si realiza un análisis de clasificación completo en sus fuentes de datos. Las fuentes de datos que hayan tenido un escaneo de solo mapeo solo pueden generar el Informe de mapeo de datos.
- NetApp no puede garantizar la precisión del 100% de los datos personales y los datos personales confidenciales que identifica la clasificación de datos. Siempre debes validar la información revisando los datos.

Los siguientes informes están disponibles para la clasificación de datos:

- **Informe de evaluación de descubrimiento de datos**: proporciona un análisis de alto nivel del entorno escaneado para resaltar los hallazgos del sistema y mostrar áreas de preocupación y posibles pasos de remediación. Este informe está disponible en el panel de Gobernanza.
- **Informe general de mapeo de datos completo**: proporciona información sobre el tamaño y la cantidad de archivos en sus sistemas. Esto incluye la capacidad de uso, la antigüedad de los datos, el tamaño de los datos y los tipos de archivos. Este informe está disponible en el panel de Gobernanza.
- **Informe de solicitud de acceso del interesado**: le permite extraer un informe de todos los archivos que contienen información sobre el nombre específico o un identificador personal del interesado. Este informe está disponible en el panel de Cumplimiento.
- **Informe HIPAA**: le ayuda a identificar la distribución de información de salud en sus archivos. Este informe está disponible en el panel de Cumplimiento.
- **Informe PCI DSS**: le ayuda a identificar la distribución de la información de tarjetas de crédito en sus archivos. Este informe está disponible en el panel de Cumplimiento.
- **Informe de evaluación de riesgos de privacidad**: proporciona información sobre la privacidad de sus datos y una puntuación de riesgo de privacidad. Este informe está disponible en el panel de Cumplimiento.
- **Informes sobre un tipo de información específico**: Se encuentran disponibles informes que incluyen detalles sobre los archivos identificados que contienen datos personales y datos personales sensibles. También puedes ver los archivos desglosados por categoría y tipo de archivo.

Seleccione los sistemas para los informes

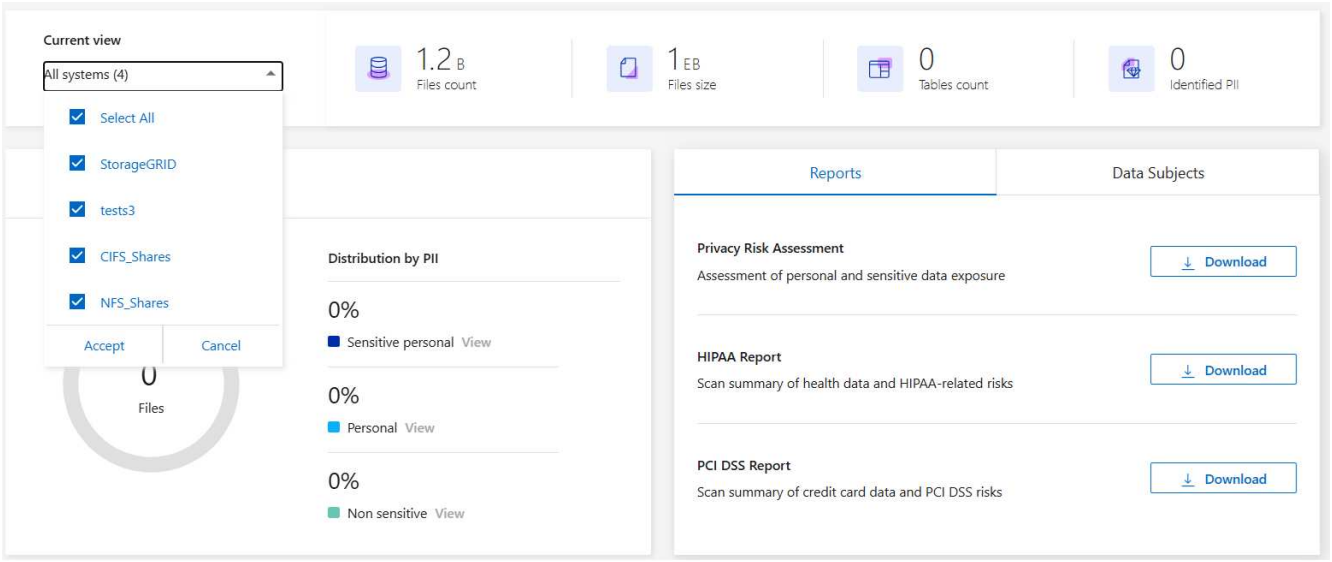
Puede filtrar el contenido del panel de Cumplimiento de clasificación de datos para ver los datos de cumplimiento de todos los sistemas y bases de datos, o solo de sistemas específicos.

Al filtrar el panel, la Clasificación de datos limita los datos de cumplimiento y los informes solo a aquellos sistemas que usted seleccionó.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.

2. Seleccione el filtro de sistemas en el menú desplegable y luego seleccione los sistemas.
3. Seleccione **Aceptar** para confirmar su selección.



Informe de solicitud de acceso del interesado

Las regulaciones de privacidad como el RGPD europeo otorgan a los interesados (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un interesado solicita esta información, esto se conoce como DSAR (solicitud de acceso al interesado). Las organizaciones están obligadas a responder a estas solicitudes "sin demoras indebidas" y, a más tardar, dentro del mes siguiente a su recepción.

Puede responder a una DSAR buscando el nombre completo de un sujeto o un identificador conocido (como una dirección de correo electrónico) y luego descargando un informe. El informe está diseñado para ayudar a su organización a cumplir con el requisito de GDPR o leyes de privacidad de datos similares.

¿Cómo puede la clasificación de datos ayudarle a responder a una DSAR?

Cuando se realiza una búsqueda de un interesado, la Clasificación de datos encuentra todos los archivos que contienen el nombre o identificador de esa persona. La clasificación de datos verifica los últimos datos preindexados en busca del nombre o identificador. No inicia un nuevo escaneo.

Una vez completada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso del interesado. El informe recopila información de los datos y la expresa en términos legales que usted puede enviar a la persona.

Actualmente no se admite la búsqueda de interesados en las bases de datos.

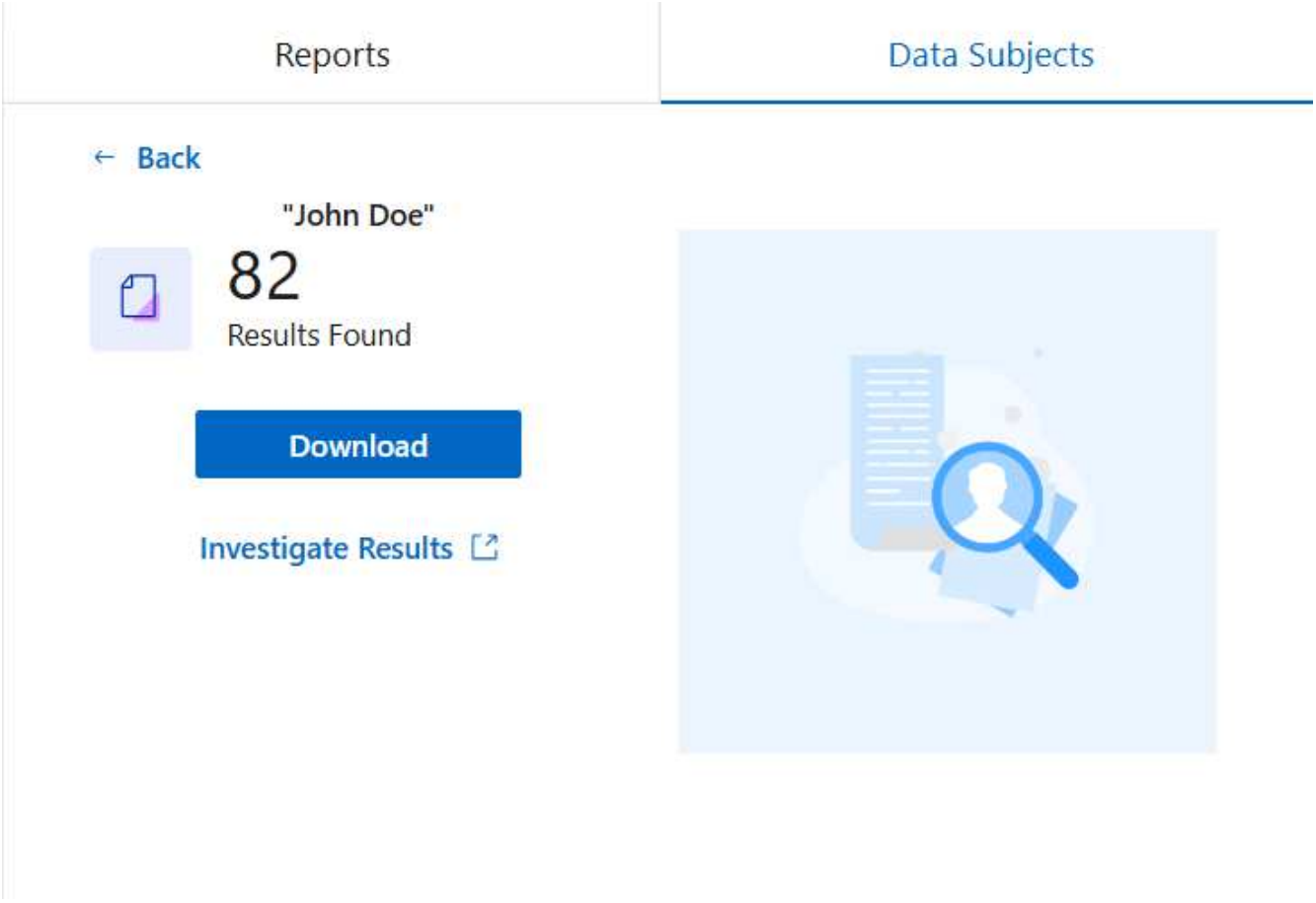
Búsqueda de interesados y descarga de informes

Busque el nombre completo del interesado o un identificador conocido y luego descargue un informe de lista de archivos o un informe DSAR. Puedes buscar por"cualquier tipo de información personal" .

Al buscar nombres de interesados se admiten los idiomas inglés, alemán, japonés y español. Más adelante se añadirá soporte para más idiomas.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Desde la página de Cumplimiento, busque la pestaña **Sujetos de datos**.
3. En la sección **Sujetos de datos**, ingrese un nombre o identificador conocido y luego seleccione **Buscar**.
4. Cuando se complete la búsqueda, seleccione **Descargar** para acceder a la respuesta a la solicitud de acceso del interesado. Seleccione **Investigar resultados** para ver más información en la página Investigación de
datos.



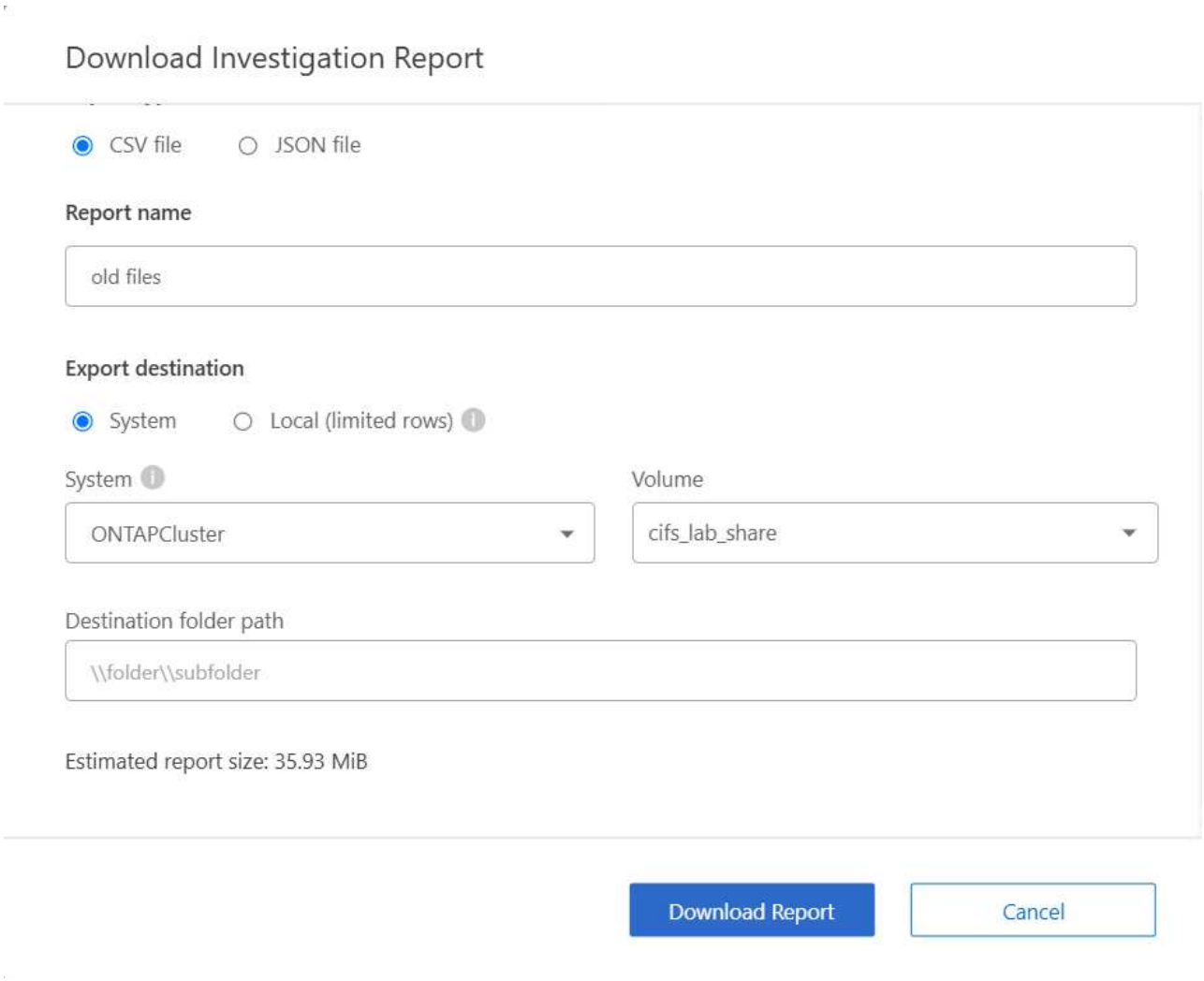
5. Revise los resultados en Clasificación de datos o descárguelos como informe seleccionando el ícono de descarga.

   a. Cuando seleccione el icono de descarga, configure sus ajustes de descarga:
      - Elija el formato de la película: CSV o JSON
      - Introduzca un **Nombre del informe**
      - Elija el destino de la exportación: **Sistema** o su máquina **Local**.

        Si elige sistema, se descargarán todos los datos. También debe seleccionar la ruta de **Sistema**, **Volumen** y **Carpeta de destino**.

   Si elige **Local**, limitará el informe a las primeras 10 000 filas de datos no estructurados; 5000 filas de datos no estructurados y 1000 filas de datos estructurados.

   a. Seleccione **Descargar informe** para iniciar la descarga.



Informe de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)

El Informe de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) puede ayudarle a identificar archivos que contienen información de salud. Está diseñado para ayudar a su organización a cumplir con los requisitos de privacidad de datos de HIPAA. La información que busca la clasificación de datos incluye:

- Patrón de referencia de salud
- Código médico CIE-10-CM
- Código médico CIE-9-CM
- RRHH - Categoría Salud
- Categoría de datos de aplicaciones de salud

El informe incluye la siguiente información:

- Descripción general: ¿Cuántos archivos contienen información de salud y en qué sistemas?
- Cifrado: el porcentaje de archivos que contienen información de salud que se encuentran en sistemas cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.
- Protección contra ransomware: el porcentaje de archivos que contienen información de salud que se encuentran en sistemas que tienen o no habilitada la protección contra ransomware. Esta información es

específica de Cloud Volumes ONTAP.

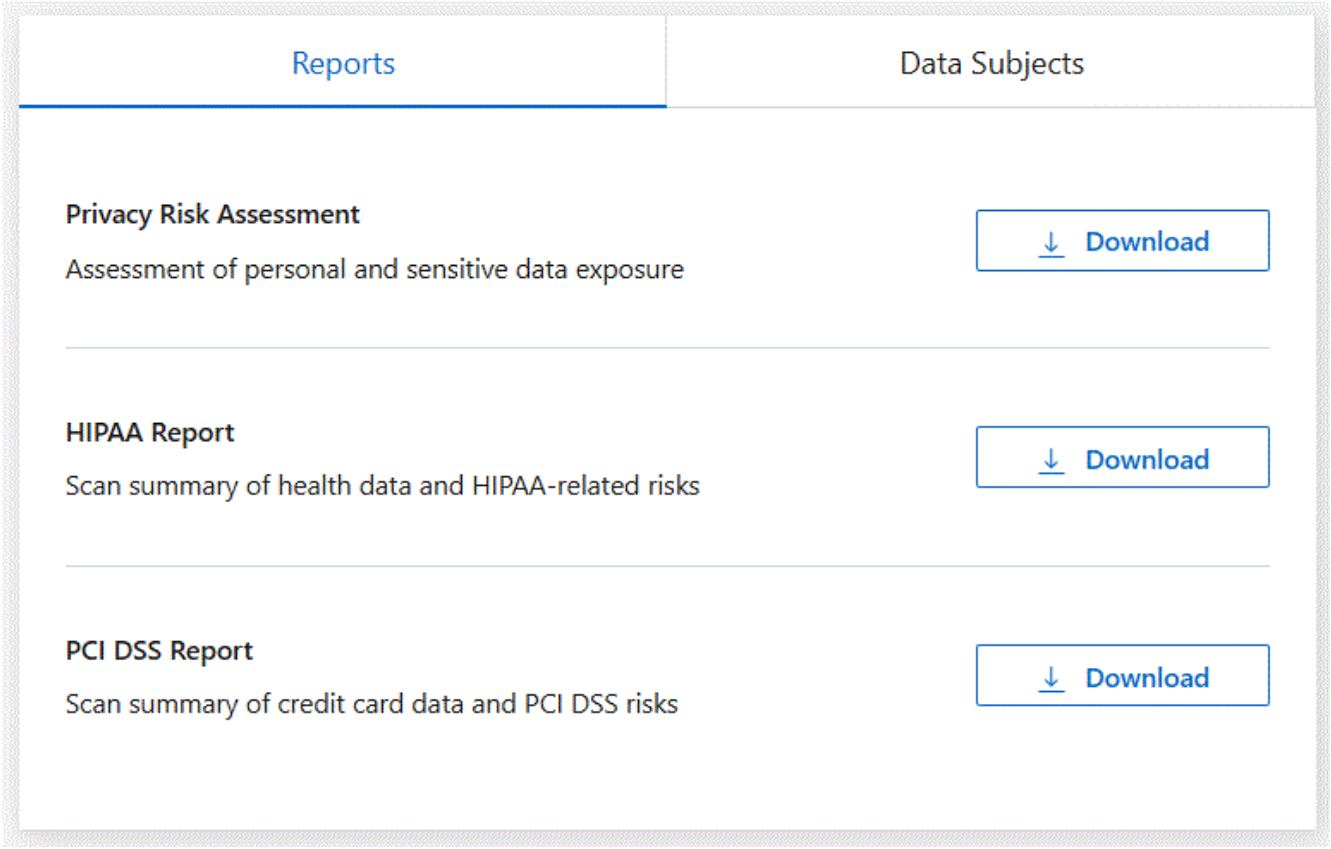
- Retención: El período de tiempo en el que se modificaron los archivos por última vez. Esto es útil porque no debe conservar la información de salud durante más tiempo del necesario para procesarla.
- Distribución de información de salud: los sistemas donde se encontró la información de salud y si el cifrado y la protección contra ransomware están habilitados.

Generar el informe HIPAA

Vaya a la pestaña Cumplimiento para generar el informe.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el ícono de descarga junto a **Informe HIPAA**.



Resultado

La clasificación de datos genera un informe en PDF.

Informe sobre el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

El informe del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) puede ayudarle a identificar la distribución de la información de tarjetas de crédito en sus archivos.

El informe incluye la siguiente información:

- Descripción general: ¿Cuántos archivos contienen información de tarjetas de crédito y en qué sistemas?

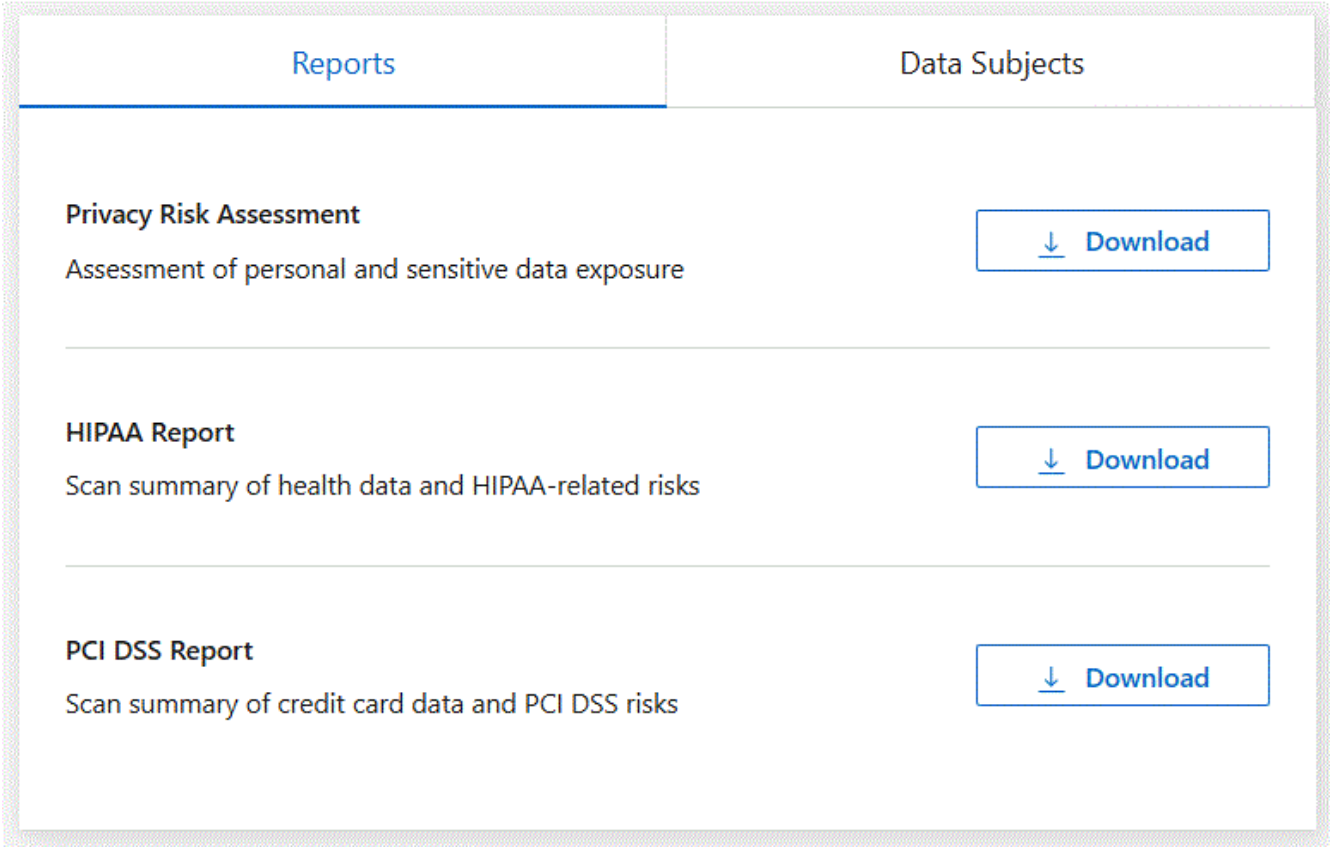
- Cifrado: el porcentaje de archivos que contienen información de tarjetas de crédito que se encuentran en sistemas cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.
- Protección contra ransomware: el porcentaje de archivos que contienen información de tarjetas de crédito que se encuentran en sistemas que tienen o no habilitada la protección contra ransomware. Esta información es específica de Cloud Volumes ONTAP.
- Retención: El período de tiempo en el que se modificaron los archivos por última vez. Esto es útil porque no debe conservar la información de la tarjeta de crédito durante más tiempo del necesario para procesarla.
- Distribución de información de tarjetas de crédito: los sistemas donde se encontró la información de la tarjeta de crédito y si el cifrado y la protección contra ransomware están habilitados.

Generar el informe PCI DSS

Vaya a la pestaña Cumplimiento para generar el informe.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el icono de descarga junto a **Informe PCI DSS**.



Resultado

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Informe de evaluación de riesgos de privacidad

El Informe de evaluación de riesgos de privacidad proporciona una descripción general del estado de riesgo de privacidad de su organización, según lo exigen las regulaciones de privacidad como GDPR y CCPA.

El informe incluye la siguiente información:

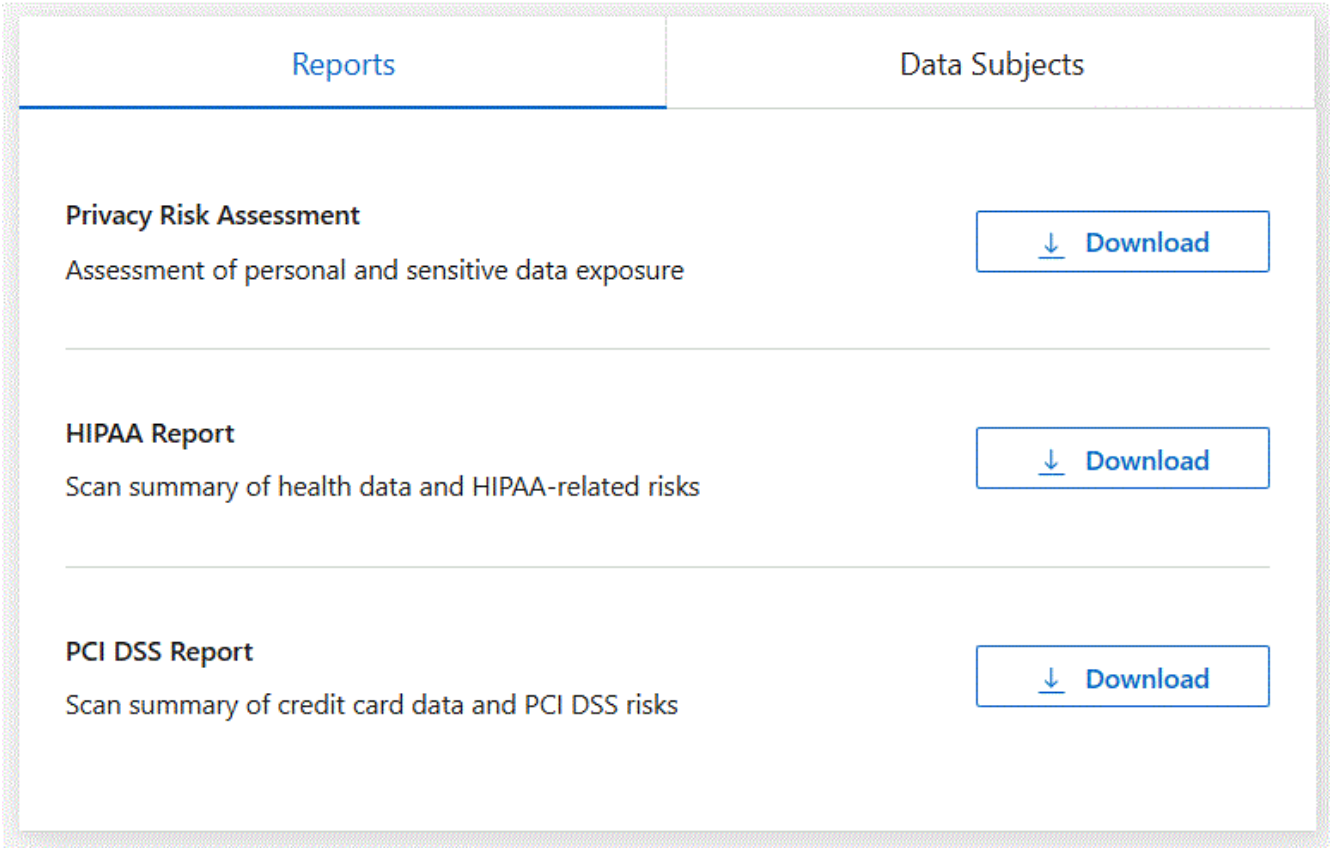
- Estado de cumplimiento: una puntuación de gravedad y la distribución de datos, ya sean no confidenciales, personales o personales confidenciales.
- Descripción general de la evaluación: un desglose de los tipos de datos personales encontrados, así como las categorías de datos.
- Sujetos de datos en esta evaluación: El número de personas, por ubicación, para las que se encontraron identificadores nacionales.

Generar el Informe de Evaluación de Riesgos de Privacidad

Vaya a la pestaña Cumplimiento para generar el informe.

Pasos

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el icono de descarga junto a **Informe de evaluación de riesgos de privacidad**.



Resultado

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Puntuación de gravedad

La clasificación de datos calcula la puntuación de gravedad del Informe de evaluación de riesgos de privacidad basándose en tres variables:

- El porcentaje de datos personales sobre todos los datos.
- El porcentaje de datos personales sensibles sobre todos los datos.
- El porcentaje de archivos que incluyen interesados, determinado por identificadores nacionales como documentos de identidad nacionales, números de seguridad 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 al 3%
3	Dos de las variables son mayores al 3%
4	Tres de las variables son mayores que 3%
5	Una de las variables es mayor al 6%
6	Dos de las variables son mayores al 6%
7	Tres de las variables son mayores al 6%
8	Una de las variables es mayor al 15%
9	Dos de las variables son mayores al 15%
10	Tres de las variables son mayores al 15%

Supervisar el estado de la NetApp Data Classification

El panel de control del estado de NetApp Data Classification proporciona supervisión en tiempo real e información sobre el rendimiento. El Monitor de salud captura información sobre su infraestructura de clasificación de datos, el estado del sistema, las métricas de uso y los datos de utilización, lo que le permite identificar y solucionar problemas.

Información sobre el Monitor de Salud

El panel de control del Monitor de salud presenta información en cuatro categorías.

- **Estado de la infraestructura**

  Ver información, incluido el estado de la versión, la estabilidad del sistema, el tipo de implementación y la escala de la máquina.

- **Contenedores problemáticos**

  Revise el campo de contenedores problemáticos para obtener información sobre los contenedores que se detienen o se reinician con frecuencia. Utilice esta información para investigar los contenedores

específicos.

- **Información del sistema**

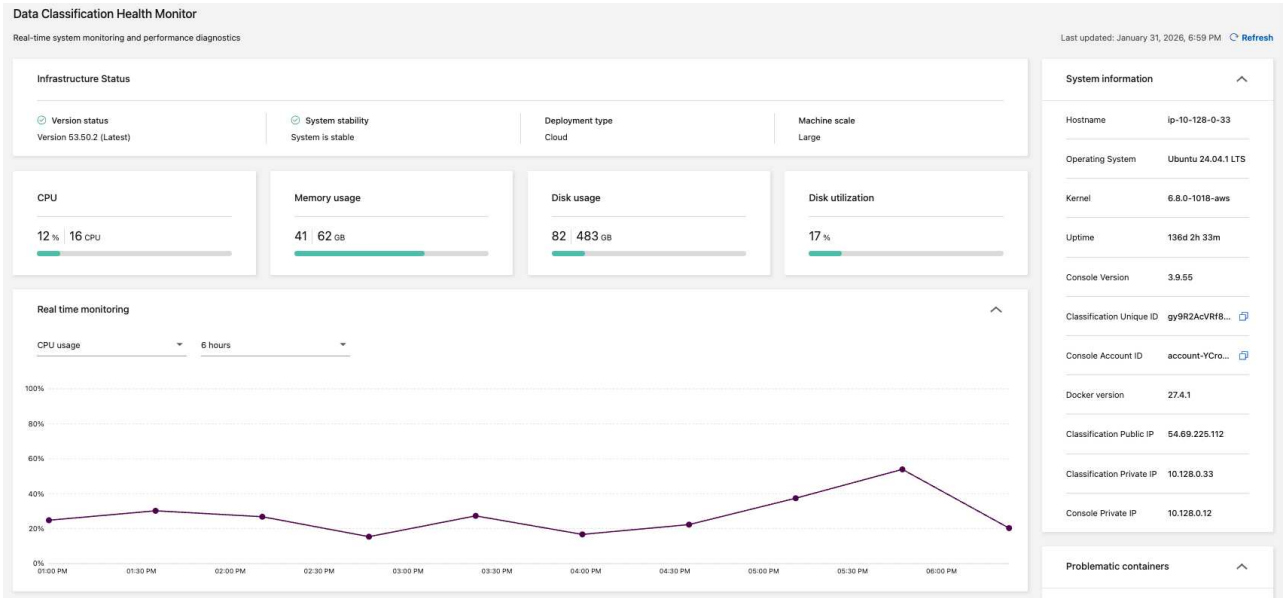
  El panel de información del sistema captura información crítica sobre la NetApp Console y la clasificación de datos, como las direcciones IP públicas y privadas, el nombre del host, el sistema operativo, la versión de la consola y el ID de la consola.

- **Uso y utilización**

  Revise el uso de la CPU, el uso del disco, el uso del disco y el uso de la memoria. Estos valores se muestran en unidades de almacenamiento (GB) o porcentajes del uso total. Si algún campo muestra una advertencia, selecciónela para obtener información y recomendaciones de solución.

Acceda al panel de control del Monitor de salud

1. En Clasificación de datos, seleccione **Configuración**.
2. En el encabezado **Configuración**, seleccione **Monitor de estado de clasificación de datos**.
3. En el panel de control del Monitor de salud, puedes:
   - Revisar el uso y utilización. Si alguna métrica de uso o utilización muestra advertencias, seleccione la advertencia para obtener recomendaciones para resolver el problema.
   - Alterne el gráfico para mostrar el uso de la CPU, el uso del disco, el uso del disco y el uso de la memoria. Puede cambiar el eje x para mostrar el contenido en horas (6, 12 o 24) o días (2, 7 o 14).
   - Actualice el panel para ver las métricas de datos más recientes.



Administrar la clasificación de datos

Excluir directorios específicos de los análisis de NetApp Data Classification

Si desea que NetApp Data Classification excluya directorios específicos de los análisis, puede agregar estos nombres de directorio a un archivo de configuración. Después de aplicar este cambio, el motor de clasificación de datos excluye esos directorios de los análisis.

De forma predeterminada, los análisis de clasificación de datos excluyen los datos de instantáneas de volumen, que son idénticos a su origen en el volumen.

Fuentes de datos compatibles

La exclusión de directorios específicos de los análisis de clasificación de datos es compatible con recursos compartidos NFS y CIFS en las siguientes fuentes de datos:

- ONTAP local
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Recursos compartidos de archivos generales

Define los directorios que se excluirán del escaneo

Antes de poder excluir directorios del escaneo de clasificación, debe iniciar sesión en el sistema de clasificación de datos para poder editar un archivo de configuración y ejecutar un script. Vea cómo"Iniciar sesión en el sistema de clasificación de datos" dependiendo de si instaló manualmente el software en una máquina Linux o si implementó la instancia en la nube.

Consideraciones

- Puede excluir un máximo de 50 rutas de directorio por sistema de clasificación de datos.
- La exclusión de rutas de directorio puede afectar los tiempos de escaneo.

Pasos

1. En el sistema de clasificación de datos, vaya a "/opt/netapp/config/custom_configuration" y luego abra el archivo `data_provider.yaml` .
2. En la sección "data_providers", debajo de la línea "exclude:", ingrese las rutas de directorio que desea excluir. Por ejemplo:

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

No modifique 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 envía los directorios que se excluirán del escaneo al motor de clasificación.

Resultado

Todos los escaneos posteriores de sus datos excluirán el escaneo de aquellos directorios especificados.

Puede agregar, editar o eliminar elementos de la lista de exclusión siguiendo estos mismos pasos. La lista de exclusión revisada se actualizará después de ejecutar el script para confirmar los cambios.

Ejemplos

Configuración 1:

Cualquier carpeta que contenga "carpeta1" en cualquier parte del nombre será excluida de todas las fuentes de datos.

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

Resultados esperados para las rutas que se excluirán:

- /CVO1/carpeta1
- /CVO1/nombrecarpeta1
- /CVO1/carpeta10
- /CVO1/*carpeta1
- /CVO1/+nombrecarpeta1
- /CVO1/nocarpeta10
- /CVO22/carpeta1
- /CVO22/nombrecarpeta1
- /CVO22/carpeta10

Ejemplos de rutas que no se excluirán:

- /CVO1/*carpeta
- /CVO1/nombredecarpeta
- /CVO22/*carpeta20

Configuración 2:

Se excluirá cualquier carpeta que contenga "*folder1" sólo al comienzo del nombre.

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

Resultados esperados para las rutas que se excluirán:

- /CVO/*carpeta1
- /CVO/*nombredecarpeta1
- /CVO/*carpeta10

Ejemplos de rutas que no se excluirán:

- /CVO/carpeta1
- /CVO/nombrecarpeta1
- /CVO/no*carpeta10

Configuración 3:

Se excluirá cualquier carpeta en la fuente de datos "CVO22" que contenga "carpeta1" en cualquier parte del nombre.

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

Resultados esperados para las rutas que se excluirán:

- /CVO22/carpeta1
- /CVO22/nombrecarpeta1
- /CVO22/carpeta10

Ejemplos de rutas que no se excluirán:

- /CVO1/carpeta1
- /CVO1/nombrecarpeta1
- /CVO1/carpeta10

Cómo escapar 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 del análisis, deberá utilizar la secuencia de escape \\ antes del nombre de la carpeta.

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

Ruta en la fuente: `/project/*not_to_scan`

Sintaxis en archivo de exclusión: `"\\*not_to_scan"`

Ver la lista de exclusiones actual

Es posible que el contenido de la `data_provider.yaml` archivo de configuración para que sea diferente de lo que realmente se confirmó después de ejecutar el `update_data_providers_from_config_file.sh` guion. Para ver la lista actual de directorios que ha excluido del análisis de clasificación de datos, ejecute el siguiente comando desde "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Definir identificadores de grupo adicionales como abiertos a la organización en la NetApp Data Classification

Cuando los identificadores de grupo (GID) se adjuntan a archivos o carpetas en recursos compartidos de archivos NFS, definen los permisos para el archivo o la carpeta; por ejemplo, si están "abiertos para la organización". Si algunos GID no están configurados inicialmente con el nivel de permiso "Abierto a la 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 NetApp Data Classification vuelva a escanear sus 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 muestren los permisos de archivos.

Para activar esta funcionalidad, debe iniciar sesión en el sistema de clasificación de datos para poder editar un archivo de configuración y ejecutar un script. Vea cómo"Iniciar sesión en el sistema de clasificación de datos" dependiendo de si instaló manualmente el software en una máquina Linux o si implementó la instancia en la nube.

Agregue el permiso "abierto a la organización" a los ID de grupo

Debe tener los números de identificación de grupo (GID) antes de comenzar esta tarea.

Pasos

1. En el sistema de clasificación de datos, vaya a "/opt/netapp/config/custom_configuration" y abra el archivo `data_provider.yaml` .
2. En la línea "organization_group_ids: []" agregue los ID del 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 envía los permisos de ID de grupo revisados al motor de clasificación.

Resultado

Todos los análisis posteriores de sus datos identificarán los archivos o carpetas que tengan 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 siguiendo 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 que el contenido de la `data_provider.yaml` archivo de configuración para que difiera de lo que realmente se ha confirmado después de ejecutar el `update_data_providers_from_config_file.sh` guion. Para ver la lista actual de ID de grupo que ha agregado a Clasificación de datos, ejecute el siguiente comando desde "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Personalice la definición de datos obsoletos en NetApp Data Classification

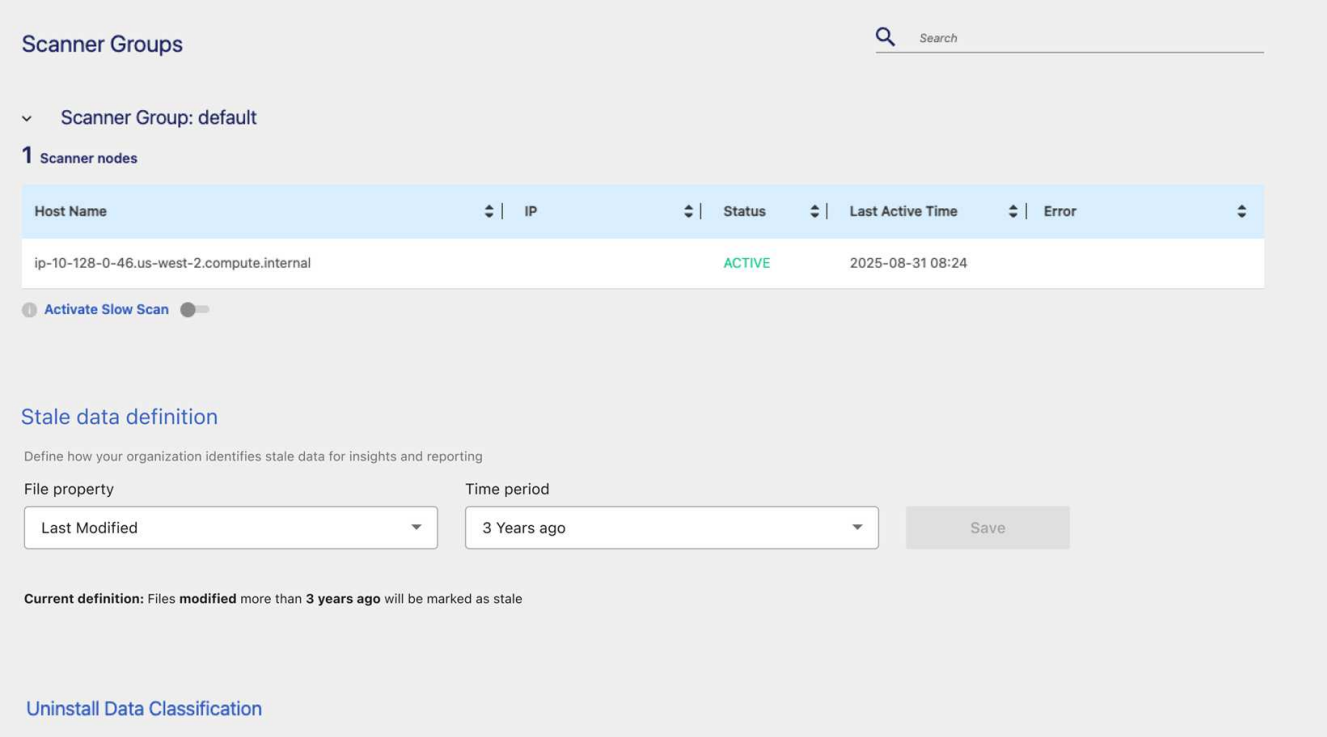
La NetApp Data Classification identifica datos obsoletos para ayudarlo a identificar oportunidades de ahorro y riesgos de gobernanza. Debido a que la definición de datos obsoletos puede variar según los diferentes contextos organizacionales, puede personalizar el modo en que la Clasificación de datos define los datos obsoletos.

Los datos obsoletos se pueden definir en función de cuándo se *accedió a ellos por última vez* o cuándo se *modificó por última vez*. Las selecciones del período de tiempo varían desde hace 6 meses hasta hace 10 años.

De forma predeterminada, los datos se consideran obsoletos si se modificaron por última vez hace tres años.

Definir datos obsoletos

1. En Ransomware Resilience, seleccione **Configuración**.
2. En la página de Configuración, desplácese hasta el encabezado **Definición de datos obsoletos**.
3. En el menú desplegable **Propiedades de archivo**, elija si desea definir datos obsoletos según cuándo se accedió por última vez o se modificó por última vez.
4. Seleccione el período de tiempo para la definición de datos obsoletos.



5. Seleccione **Guardar**.

Eliminar fuentes de datos de NetApp Data Classification

Si es necesario, puede detener que NetApp Data Classification escanee uno o más sistemas, bases de datos o grupos de recursos compartidos de archivos.

Desactivar los análisis de un sistema

Cuando desactiva los escaneos, la Clasificación de datos ya no escanea los datos en el sistema y elimina la información indexada de la instancia de Clasificación de datos. Los datos del propio sistema no se eliminan.

1. Desde la página *Configuración*, seleccione la botón en la fila del sistema y luego **Desactivar clasificación de datos**.

> También puede deshabilitar los análisis de un sistema desde el panel Servicios cuando selecciona el sistema.

Eliminar una base de datos de Clasificación de datos

Si ya no necesita escanear una determinada base de datos, puede eliminarla de la interfaz de Clasificación de datos y detener todos los escaneos.

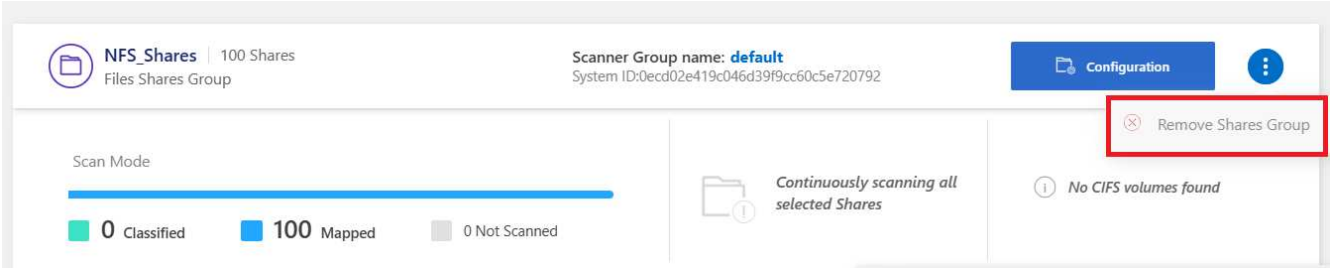
1. Desde la página *Configuración*, seleccione la botón en la fila de la base de datos y luego **Eliminar servidor de base de datos**.

Eliminar un grupo de recursos compartidos de archivos de la Clasificación de datos

Si ya no desea escanear archivos de usuario de un grupo de recursos compartidos de archivos, puede eliminar el grupo de recursos compartidos de archivos de la interfaz de Clasificación de datos y detener todos los escaneos.

Pasos

1. Desde la página *Configuración*, seleccione la botón en la fila del grupo de recursos compartidos de archivos y luego **Eliminar grupo de recursos compartidos de archivos**.



2. Seleccione **Eliminar grupo de acciones** en el cuadro de diálogo de confirmación.

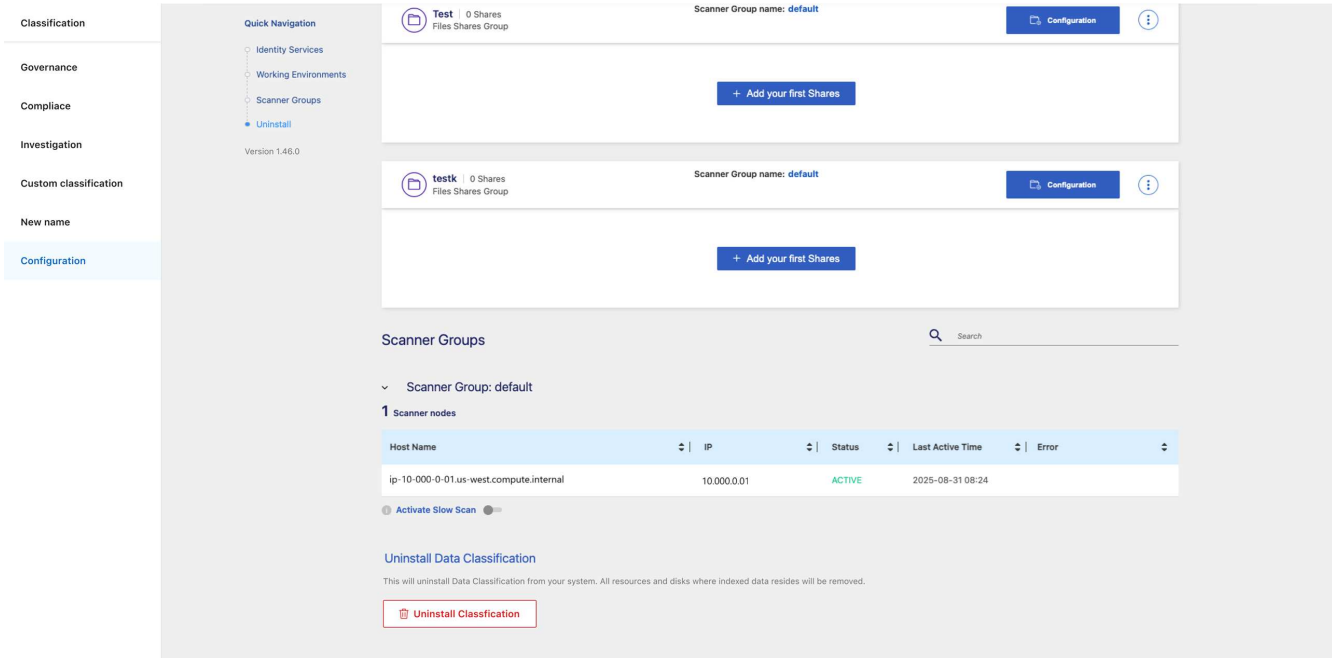
Desinstalar NetApp Data Classification

Puede desinstalar NetApp Data Classification para solucionar problemas o eliminar permanentemente el software del host. Al eliminar la instancia también se eliminan los discos asociados donde residen los datos indexados, lo que significa que toda la información que Data Classification ha escaneado se eliminará de forma permanente.

Los pasos que debes seguir dependen de si implementaste la clasificación de datos en la nube o en un host local.

Desinstalar la clasificación de datos de un proveedor de nube

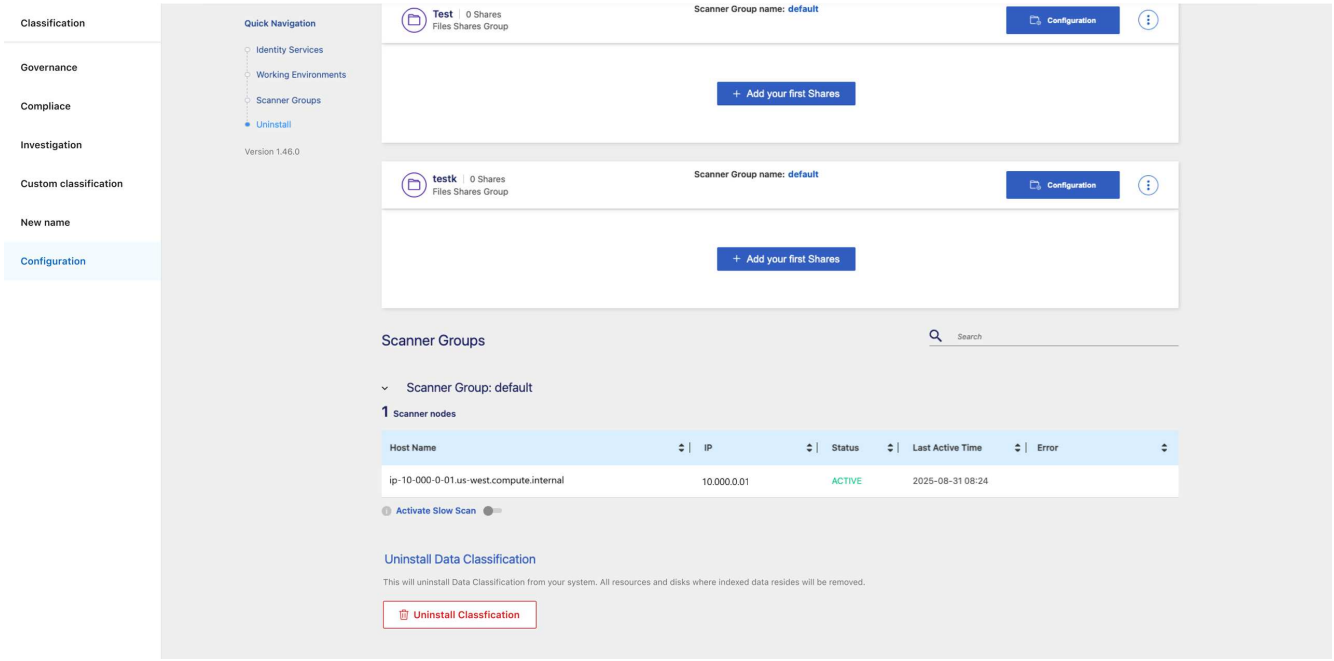
1. Desde Clasificación de datos, seleccione **Configuración**.
2. En la parte inferior de la página de configuración, seleccione **Desinstalar clasificación**.



3. En el cuadro de diálogo, ingrese "desinstalar" para continuar con la desconexión de la instancia de Clasificación de datos del agente de Consola. Seleccione **Desinstalar** para confirmar.
4. En el cuadro de diálogo *Desinstalar clasificación*, escriba **uninstall** para confirmar que desea desconectar la instancia de Clasificación de datos del agente de Consola y luego seleccione **Desinstalar**.
5. Para finalizar el proceso de desinstalación, vaya a la consola de su proveedor de nube y elimine la instancia de Clasificación de datos. La instancia se llama *CloudCompliance* con un hash generado (UUID) concatenado a ella. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Desinstalar la clasificación de datos de una implementación local

1. Desde Clasificación de datos, seleccione **Configuración**.
2. En la parte inferior de la página de configuración, seleccione **Desinstalar clasificación**.



3. En el cuadro de diálogo, ingrese "desinstalar" para continuar con la desconexión de la instancia de Clasificación de datos del agente de Consola. Seleccione **Desinstalar** para confirmar.
4. Para desinstalar el software del host, ejecute el `cleanup.sh` script en la máquina host de clasificación de datos, por ejemplo:

   ```
   cleanup.sh
   ```

   El guión se encuentra en el `/install/light_probe/onprem_installer/cleanup.sh` directorio. Vea cómo"Inicie sesión en la máquina host de clasificación de datos" .

Referencia

Tipos de instancias de NetApp Data Classification compatibles

El software de NetApp Data Classification debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, requisitos de RAM, requisitos de software, etc. Al implementar la clasificación de datos en la nube, recomendamos utilizar un sistema con características "grandes" para obtener una funcionalidad completa.

Puede implementar la clasificación de datos en un sistema con menos CPU y menos RAM, pero existen algunas limitaciones al utilizar estos sistemas menos potentes. "Conozca estas limitaciones" .

En las siguientes tablas, si el sistema marcado como "predeterminado" no está disponible en la región donde está instalando Data Classification, se implementará el siguiente sistema de la tabla.

Tipos de instancias de AWS

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, 1 TiB gp3 SSD	"m6i.8xlarge"(por defecto)
Grande	16 CPU, 64 GB de RAM, SSD de 500 GiB	"m6i.4xlarge"(predeterminado) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Medio	8 CPU, 32 GB de RAM, SSD de 200 GiB	"m6i.2xlarge"(predeterminado) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Pequeño	8 CPU, 16 GB de RAM, SSD de 100 GiB	"c6a.2xlarge"(predeterminado) c5a.2xlarge c5.2xlarge c4.2xlarge

Tipos de instancias de Azure

Tamaño del sistema	Especificaciones	Tipo de instancia
Extra grande	32 CPU, 128 GB de RAM, disco de SO (2048 GiB, rendimiento mínimo de 250 MB/s) y disco de datos (SSD de 1 TiB, rendimiento mínimo de 750 MB/s)	"Standard_D32_v3"(por defecto)
Grande	16 CPU, 64 GB de RAM, SSD de 500 GiB	"Standard_D16s_v3"(por defecto)

Tipos de instancias de GCP

Tamaño del sistema	Especificaciones	Tipo de instancia
Grande	16 CPU, 64 GB de RAM, SSD de 500 GiB	"n2-estándar-16"(predeterminado) n2d-standard-16 n1-standard-16

Metadatos recopilados de fuentes de datos en NetApp Data Classification

NetApp Data Classification recopila ciertos metadatos al realizar escaneos de clasificación en los datos de sus fuentes de datos y sistemas. La clasificación de datos puede acceder a la mayoría de los metadatos que necesitamos para clasificar sus datos, pero hay algunas fuentes en las que no podemos acceder a los datos que necesitamos.

	Metadatos	CIFS	No sé
Marcas de tiempo	*Hora de creación*	Disponible	No disponible (no compatible con Linux)
	Hora del último acceso	Disponible	Disponible
	Hora de la última modificación	Disponible	Disponible
Permisos	*Permisos abiertos*	Si el grupo "TODOS" tiene acceso al archivo, se considera "Abierto a la organización".	Si "Otros" tiene 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 normalmente se administran localmente en el servidor, por lo tanto, el mismo individuo puede tener un UID diferente en cada servidor)

- La clasificación de datos no extrae la "hora del último acceso" de las fuentes de datos de la base de datos.
- Las versiones anteriores del sistema operativo Windows (por ejemplo, Windows 7 y Windows 8) deshabilitan la recopilación del atributo "hora del último acceso" de forma predeterminada porque puede afectar el rendimiento del sistema. Cuando no se recopila este atributo, los análisis de clasificación de datos que se basan en la "hora del último acceso" se verán afectados. Puede habilitar la recopilación de la hora del último acceso en estos sistemas Windows más antiguos si es necesario.

Marca de tiempo del último acceso

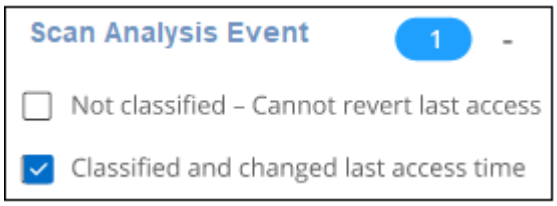
Cuando la clasificación de datos extrae datos de recursos compartidos de archivos, el sistema operativo considera que está accediendo a los datos y cambia la "hora del último acceso" en consecuencia. Después del escaneo, la clasificación de datos intenta revertir la última hora de acceso a la marca de tiempo original. Si la clasificación de datos no tiene permisos de escritura de atributos en CIFS o permisos de escritura en NFS, el sistema no puede revertir la última hora de acceso a la marca de tiempo original. Los volúmenes ONTAP configurados con SnapLock tienen permisos de solo lectura y tampoco pueden revertir la última hora de acceso a la marca de tiempo original.

De forma predeterminada, si la clasificación de datos no tiene estos permisos, el sistema no escaneará esos archivos en sus volúmenes porque la clasificación de datos no puede revertir la "hora del último 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 seleccionar el interruptor **Escanear cuando faltan permisos de "atributos de escritura"** en la parte inferior de la página de Configuración para que la Clasificación de datos escanee los volúmenes independientemente de los permisos.

Esta funcionalidad es aplicable a sistemas ONTAP locales, Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for NetApp ONTAP y recursos compartidos de archivos de terceros.

Hay un filtro en la página de Investigación llamado *Evento de análisis de escaneo* que le permite mostrar los archivos que no se clasificaron porque la Clasificación de datos no pudo revertir la última hora de acceso, o los archivos que se clasificaron aunque la Clasificación de datos no pudo revertir la última hora de acceso.



Las selecciones de filtro son:

- "No clasificado: no se puede revertir la última hora de acceso": esto muestra los archivos que no se clasificaron debido a la falta de permisos de escritura.
- "Hora del último acceso clasificado y actualizado": muestra los archivos que fueron clasificados y la Clasificación de datos no pudo restablecer la hora del último acceso a la fecha original. Este filtro es relevante solo para entornos en los que activó la opción **Escanear cuando faltan permisos de "atributos de escritura"**.

Si es necesario, puede exportar estos resultados a un informe para ver qué archivos se están escaneando o no debido a los permisos. "Obtenga más información sobre los informes de investigación de datos".

Inicie sesión en el sistema de NetApp Data Classification

Debe iniciar sesión en el sistema de NetApp Data Classification para poder acceder a los archivos de registro o editar los archivos de configuración.

Cuando Data Classification está instalado en una máquina Linux en sus instalaciones o en una máquina Linux implementada en la nube, puede acceder directamente al archivo de configuración y al script.

Cuando se implementa la clasificación de datos en la nube, es necesario acceder mediante SSH a la instancia de clasificación de datos. Puede acceder al sistema mediante SSH ingresando el usuario y la contraseña, o utilizando la clave SSH que proporcionó durante la instalación del agente de consola. El comando SSH es:

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

- `<path_to_the_ssh_key>`= ubicación de las claves de autenticación ssh
- `<machine_user>`:
  - Para AWS: utilice <ec2-user>
  - Para Azure: use el usuario creado para la instancia de consola
  - Para GCP: utilice el usuario creado para la instancia de la consola
- `<datasense_ip>`= Dirección IP de la instancia de la máquina virtual

Debe modificar las reglas de entrada del grupo de seguridad para acceder al sistema en la nube. Para más detalles, consulte:

- "Reglas de grupo de seguridad en AWS"
- "Reglas de grupo de seguridad en Azure"
- "Reglas de firewall en Google Cloud"

API de NetApp Data Classification

Las capacidades de NetApp Data Classification disponibles a través de la interfaz de usuario web también están disponibles a través de la API REST.

Hay cuatro categorías definidas dentro de Clasificación de datos que corresponden a las pestañas de la interfaz de usuario:

- Investigación
- Cumplimiento
- Gobernancia
- Configuración

Las API en la documentación de Swagger le permiten buscar, agregar datos, rastrear sus escaneos y realizar acciones que incluyen copiar, mover y eliminar.

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 excepción de los informes)
  - Los datos se exportan en formato JSON (fácil de analizar y enviar a aplicaciones de terceros, como Splunk)
- Cree consultas utilizando declaraciones "AND" y "OR", incluya y excluya información, y más.

  Por ejemplo, puede localizar archivos *sin* información personal identificable (PII) específica (funcionalidad no disponible en la interfaz de usuario). También puede excluir campos específicos para la operación de exportación.

- Realizar acciones

- Actualizar las credenciales de CIFS
- Ver y cancelar acciones
- Volver a escanear directorios
- Exportar datos

La API es segura y utiliza el mismo método de autenticación que la UI. Puede encontrar información sobre la autenticación en el"Documentación de REST API" .

Acceder a la referencia de la API de Swagger

Para ingresar a Swagger, necesitará la dirección IP de su instancia de clasificación de datos. En el caso de una implementación en la nube, utilizará la dirección IP pública. Luego tendrás que acceder a este punto final:

https://<ip_de_clasificación>/documentación

Ejemplo de uso de las API

El siguiente ejemplo muestra una llamada API para copiar archivos.

Solicitud de API

Inicialmente necesitará obtener todos los campos y opciones relevantes para que un sistema pueda ver todos los filtros en la pestaña de 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": "system-type",
      "operators": [
```

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

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

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

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

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

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

Usaremos esa respuesta en nuestros parámetros de solicitud para filtrar los archivos que queremos copiar.

Puede aplicar una acción a varios elementos. Los tipos de acciones admitidos incluyen: mover, eliminar y copiar.

Crearemos la acción de copia:

Solicitud de API

La siguiente API es la API de acción y le 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, por lo que puede utilizar las API de obtención y eliminación 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 obtener soporte de la NetApp Console

Es necesario registrarse para recibir soporte técnico específico para la NetApp Console y sus soluciones de almacenamiento y servicios de datos. También es necesario registrarse para obtener soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP .

Registrarse para recibir soporte no habilita el soporte de NetApp para un servicio de archivos de un proveedor de nube. Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de ese producto.

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

Descripción general del registro de soporte

Existen dos formas de registro para activar el derecho a recibir ayuda:

- Registrar el número de serie de su cuenta de la NetApp Console (su número de serie 960xxxxxxxx de 20 dígitos ubicado en la página Recursos de soporte en la consola).

  Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de la Consola. Cada cuenta de consola debe estar registrada.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de nube (son números de serie 909201xxxxxxxx de 20 dígitos).

  Estos números de serie se conocen comúnmente como *números de serie PAYGO* y son generados por la NetApp Console en el momento de la implementación de Cloud Volumes ONTAP .

El registro de ambos tipos de números de serie permite funciones como la apertura de tickets de soporte y la generación automática de casos. El registro se completa agregando cuentas del sitio de soporte de NetApp (NSS) a la consola como se describe a continuación.

Registrar la NetApp Console para obtener soporte de NetApp

Para registrarse para recibir soporte y activar el derecho a soporte, un usuario de su cuenta de NetApp Console debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de consola. La forma de registrarse para el soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta NSS

Si es cliente de NetApp con una cuenta NSS, simplemente necesita registrarse para recibir soporte a través de la consola.

Pasos

1. Seleccione **Administración** > **Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga las instrucciones de autenticación del Sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro fue exitoso, seleccione el ícono de Ayuda y seleccione **Soporte**.

   La página **Recursos** debería mostrar que su cuenta de consola está registrada para recibir soporte.

   Tenga en cuenta que otros usuarios de la consola 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. Sin embargo, eso no significa que su cuenta no esté registrada para recibir soporte. Siempre que un usuario de la organización haya seguido estos pasos, su cuenta quedará registrada.

Soy cliente actual pero no tengo cuenta NSS

Si es un cliente existente de NetApp con licencias y números de serie existentes pero *no* una cuenta NSS, debe crear una cuenta NSS y asociarla con su inicio de sesión de la consola.

Pasos

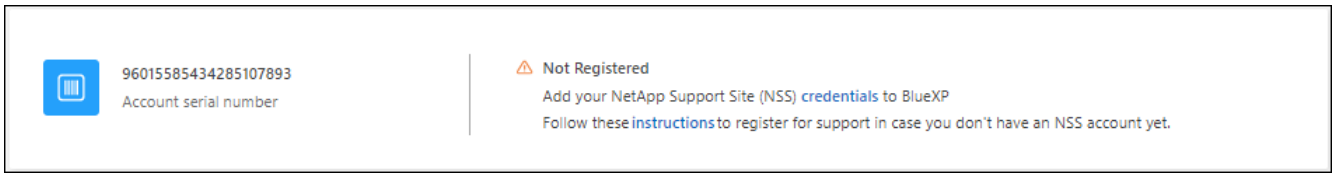
1. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta de la consola (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento de la cuenta.
2. Asocie su nueva cuenta NSS con su inicio de sesión de la consola completando los pasos a continuaciónCliente existente con una cuenta NSS .

Completamente nuevo en NetApp

Si es nuevo en NetApp y no tiene una cuenta NSS, siga cada paso a continuación.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.
2. Localice el número de serie de su ID de cuenta en la página de Registro de soporte.



3. Navegar a "Sitio de registro de soporte de NetApp" y seleccione *No soy un cliente registrado de NetApp *.
4. Llene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **Línea de productos**, seleccione **Administrador de nube** y luego seleccione su proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta del paso 2 anterior, complete la verificación de seguridad y luego confirme que leyó la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrese de revisar sus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirme la acción desde el correo electrónico.

   Al confirmar, se envía su solicitud a NetApp y se recomienda que cree una cuenta en el sitio de soporte de NetApp .

8. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento.

Después de terminar

NetApp debería comunicarse con usted durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tenga su cuenta del sitio de soporte de NetApp , asocie la cuenta con su inicio de sesión de consola completando los pasos a continuación.Cliente existente con una cuenta NSS .

Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de consola para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para obtener soporte

  Es necesario proporcionar su cuenta NSS para activar el soporte para su sistema y obtener acceso a los recursos de soporte técnico de NetApp .

- Implementación de Cloud Volumes ONTAP cuando trae su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que la consola pueda cargar su clave de licencia y habilitar la suscripción por el período que compró. Esto incluye actualizaciones automáticas para renovaciones de plazos.

- Actualización del software Cloud Volumes ONTAP a la última versión

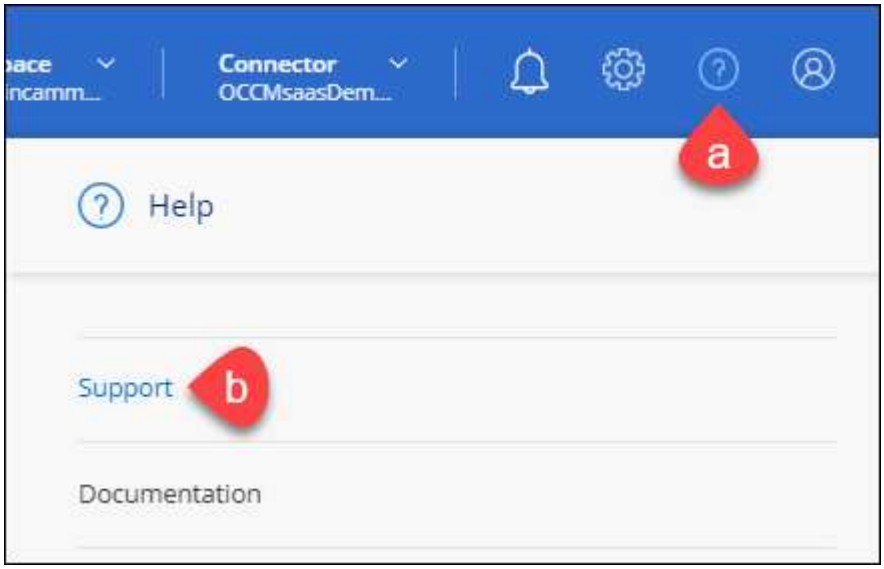
La asociación de credenciales NSS con su cuenta de NetApp Console es diferente a la asociación de una cuenta NSS con un inicio de sesión de usuario de consola.

Estas credenciales de NSS están asociadas con su ID de cuenta de consola específica. Los usuarios que pertenecen a la organización de la Consola pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

- Si tiene una cuenta de nivel de cliente, puede agregar una o más cuentas NSS.
- Si tiene una cuenta de socio o revendedor, puede agregar una o más cuentas NSS, pero no se pueden agregar junto con cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta NSS**.
3. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación específicos de soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp para realizar el proceso de autenticación.

   Estas acciones permiten que la consola utilice 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 NSS a nivel de cliente.
   - Solo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de socio. Si intenta agregar cuentas NSS de nivel de cliente y existe una cuenta de nivel de socio, recibirá el siguiente mensaje de error:

     "El tipo de cliente NSS no está permitido para esta cuenta porque ya hay usuarios NSS de otro tipo".

   Lo mismo ocurre si tiene cuentas NSS de nivel de cliente preexistentes e intenta agregar una cuenta de nivel de socio.

   - Tras iniciar sesión correctamente, NetApp almacenará el nombre de usuario NSS.

     Esta es una identificación generada por el sistema que se asigna a su correo electrónico. En la página **Administración de NSS**, puede mostrar su correo electrónico desde el ••• menú.

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en el ••• menú.

     Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de

estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

Obtenga ayuda para la NetApp Data Classification

NetApp proporciona soporte para NetApp Console y sus servicios en la nube de diversas maneras. Hay amplias opciones de autoayuda gratuitas disponibles las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimientos (KB) y un foro comunitario. Su registro de soporte incluye soporte técnico remoto mediante tickets web.

Obtenga soporte para un servicio de archivos de un proveedor de nube

Para obtener soporte técnico relacionado con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte la documentación de ese producto.

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

Para recibir soporte técnico específico para NetApp y sus soluciones de almacenamiento y servicios de datos, utilice las opciones de soporte que se describen a continuación.

Utilice opciones de autosuficiencia

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

  La documentación de la NetApp Console que estás viendo actualmente.

- "Base de conocimientos"

  Busque en la base de conocimientos de NetApp para encontrar artículos útiles para solucionar problemas.

- "Comunidades"

  Únase a la comunidad de la NetApp Console para seguir las discusiones en curso o crear otras nuevas.

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.

Antes de empezar

- Para utilizar la función **Crear un caso**, primero debe asociar sus credenciales del sitio de soporte de NetApp con su inicio de sesión de la consola. "Aprenda a administrar las credenciales asociadas con su inicio de sesión en la consola" .
- Si está abriendo un caso para un sistema ONTAP que tiene un número de serie, entonces su cuenta NSS debe estar asociada con el número de serie de ese sistema.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

   a. Seleccione **Llámenos** si desea hablar con alguien por teléfono. Serás dirigido a una página en netapp.com que enumera los números de teléfono a los que puedes llamar.

   b. Seleccione **Crear un caso** para abrir un ticket con un especialista de soporte de NetApp :

      - **Servicio**: Seleccione el servicio con el que está asociado el problema. Por ejemplo, * NetApp Console* cuando es específico de un problema de soporte técnico con flujos de trabajo o funcionalidad dentro de la consola.
      - **Sistema**: si corresponde al almacenamiento, seleccione * Cloud Volumes ONTAP* o **On-Prem** y luego el entorno de trabajo asociado.

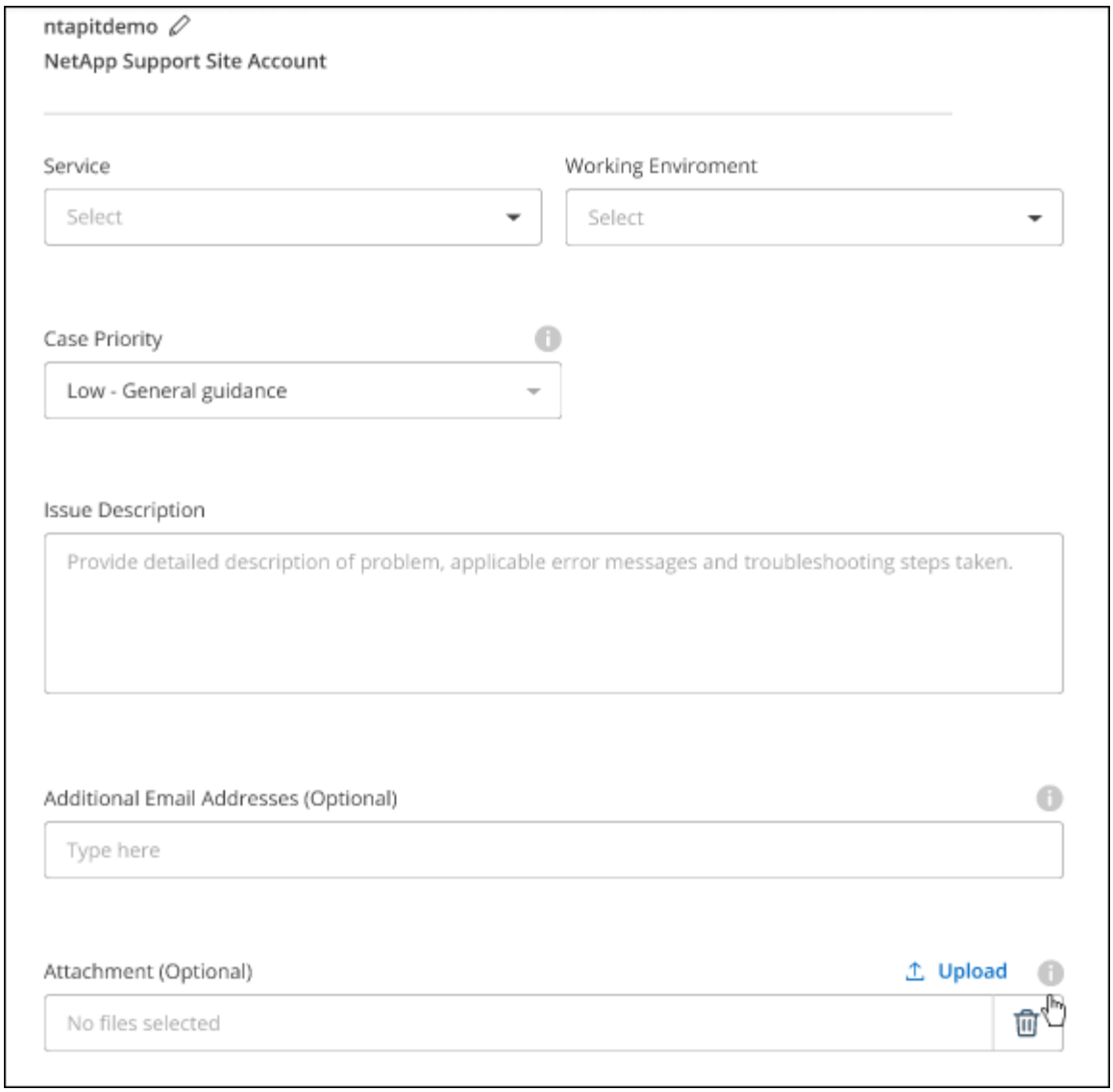
        La lista de sistemas está dentro del alcance de la organización de la consola y del agente de consola que ha seleccionado en el banner superior.

      - **Prioridad del caso**: elija la prioridad del caso, que puede ser Baja, Media, Alta o Crítica.

        Para obtener más detalles sobre estas prioridades, pase el mouse sobre el ícono de información junto al nombre del campo.

      - **Descripción del problema**: proporcione una descripción detallada de su problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que realizó.
      - **Direcciones de correo electrónico adicionales**: Ingrese direcciones de correo electrónico adicionales si desea informar a otra persona sobre este problema.
      - **Adjunto (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 su número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y se comunicará con usted pronto.

Para obtener un historial de sus casos de soporte, puede seleccionar **Configuración > Cronología** y buscar acciones llamadas "crear caso de soporte". Un botón en el extremo derecho le permite ampliar la acción para ver detalles.

Es posible que encuentres el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso contra el servicio seleccionado"

Este error podría significar que la cuenta NSS y la empresa registrada con la que está asociada no son la misma empresa registrada para el número de serie de la cuenta de la NetApp Console (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede buscar ayuda utilizando una de las siguientes opciones:

- Envíe un caso no técnico a https://mysupport.netapp.com/site/help

Gestione sus casos de soporte

Puede ver y administrar casos de soporte activos y resueltos directamente desde la Consola. Podrás gestionar los casos asociados a tu cuenta NSS y a tu empresa.

Tenga en cuenta lo siguiente:

- El panel 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 usted proporcionó.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su empresa en función de su cuenta de usuario NSS.

  Los resultados en la tabla reflejan los casos relacionados con la vista que usted seleccionó.
- Puede agregar o eliminar columnas de interés y puede filtrar el contenido de columnas como Prioridad y Estado. Otras columnas sólo proporcionan capacidades de clasificación.

  Vea los pasos a continuación para obtener más detalles.
- A nivel de caso, ofrecemos la posibilidad de actualizar notas de caso o cerrar un caso que aún no esté en estado Cerrado o Pendiente de cierre.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. Seleccione **Administración de casos** y, si se le solicita, agregue su cuenta NSS a la consola.

   La página **Administración de casos** muestra los casos abiertos relacionados con la cuenta NSS que está asociada con su cuenta de usuario de la consola. Esta es la misma cuenta NSS que aparece en la parte superior de la página de **administración de NSS**.
3. Modifique opcionalmente la información que se muestra en la tabla:
   - En **Casos de la organización**, seleccione **Ver** para ver todos los casos asociados a su empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un período de tiempo diferente.
   - Filtrar el contenido de las columnas.
   - Cambie las columnas que aparecen en la tabla seleccionando y luego elegir las columnas que desea mostrar.
4. Gestionar un caso existente seleccionando y seleccionando una de las opciones disponibles:
   - **Ver caso**: Ver detalles completos sobre un caso específico.
   - **Actualizar notas del 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**: proporcione detalles sobre el motivo por el cual está cerrando el caso y seleccione **Cerrar caso**.

Preguntas frecuentes sobre la NetApp Data Classification

Estas preguntas frecuentes pueden ayudarte si simplemente buscas una respuesta rápida a una pregunta.

NetApp Data Classification

Las siguientes preguntas proporcionan una comprensión general de la clasificación de datos.

¿Cómo funciona la clasificación de datos?

La clasificación de datos implementa otra capa de IA junto con su sistema de NetApp Console y sus sistemas de almacenamiento. Luego escanea los datos de volúmenes, depósitos, bases de datos y otras cuentas de almacenamiento e indexa la información que encuentra. La clasificación de datos aprovecha tanto la inteligencia artificial como el procesamiento del lenguaje natural, a diferencia de las soluciones alternativas que comúnmente se basan en expresiones regulares y coincidencia de patrones.

La clasificación de datos utiliza IA para proporcionar una comprensión contextual de los datos para una detección y clasificación precisas. Está impulsado por IA porque está diseñado para tipos de datos y escalas modernas. También comprende el contexto de los datos para proporcionar un descubrimiento y una clasificación sólidos y precisos.

"Obtenga más información sobre cómo funciona la clasificación de datos" .

¿Data Classification tiene una API REST y funciona con herramientas de terceros?

Sí, Data Classification tiene una API REST para las funciones compatibles con la versión de Data Classification que forma parte de la plataforma central de Console. Ver "Documentación de API" .

¿La clasificación de datos está disponible a través de los mercados en la nube?

La clasificación de datos es parte de las funciones principales de la NetApp Console , por lo que no es necesario utilizar los mercados para este servicio.

Escaneo y análisis de clasificación de datos

Las siguientes preguntas se relacionan con el rendimiento del escaneo y el análisis de clasificación de datos.

¿Con qué frecuencia Data Classification escanea mis datos?

Si bien el escaneo inicial de sus datos puede llevar un poco de tiempo, los escaneos posteriores solo inspeccionan los cambios incrementales, lo que reduce los tiempos de escaneo del sistema. La clasificación de datos escanea sus datos de manera continua, en forma rotatoria, en seis repositorios a la vez, de modo que todos los datos modificados se clasifican muy rápidamente.

"Aprenda cómo funcionan los escaneos" .

La clasificación de datos escanea las bases de datos solo una vez al día; las bases de datos no se escanean continuamente como otras fuentes de datos.

Los escaneos de datos tienen un impacto insignificante en sus sistemas de almacenamiento y en sus datos.

¿Varía el rendimiento del escaneo?

El rendimiento del escaneo puede variar según el ancho de banda de la red y el tamaño de archivo promedio en su entorno. También puede depender de las características de tamaño del sistema host (ya sea en la nube o en las instalaciones). Consulte "La instancia de Clasificación de Datos" y "Implementación de la clasificación de datos" Para más información.

Al agregar inicialmente nuevas fuentes de datos, también puede elegir realizar solo un escaneo de "mapeo" (Solo mapeo) en lugar de un escaneo de "clasificación" completo (Mapear y clasificar). El mapeo se puede realizar en sus fuentes de datos muy rápidamente porque no es necesario acceder a los archivos para ver los datos dentro de ellos. "Vea la diferencia entre un escaneo de mapeo y uno de clasificación" .

¿Puedo buscar mis datos utilizando la clasificación de datos?

La clasificación de datos ofrece amplias capacidades de búsqueda que facilitan la búsqueda de un archivo o pieza de datos específicos en todas las fuentes conectadas. La clasificación de datos permite a los usuarios buscar más allá de lo que reflejan los metadatos. Es un servicio independiente del lenguaje que también puede leer los archivos y analizar una multitud de tipos de datos confidenciales, como nombres e identificaciones. Por ejemplo, los usuarios pueden buscar en almacenes de datos estructurados y no estructurados para encontrar datos que pueden haberse filtrado de las bases de datos a los archivos de usuario, en violación de la política corporativa. Las búsquedas se pueden guardar para más tarde y se pueden crear políticas para buscar y tomar medidas sobre los resultados con una frecuencia determinada.

Una vez que se encuentran los archivos de interés, se pueden enumerar las características, incluidas las etiquetas, la cuenta del sistema, el depósito, la ruta del archivo, la categoría (de la clasificación), el tamaño del archivo, la última modificación, el estado del permiso, los duplicados, el nivel de sensibilidad, los datos personales, los tipos de datos sensibles dentro del archivo, el propietario, el tipo de archivo, el tamaño del archivo, la hora de creación, el hash del archivo, si los datos se asignaron a alguien que buscaba su atención y más. Se pueden aplicar filtros para descartar características que no sean pertinentes.

La clasificación de datos también tiene control de acceso basado en roles (RBAC) para permitir que se muevan o eliminen archivos, si existen los permisos adecuados. Si no existen los permisos adecuados, las tareas se pueden asignar a alguien de la organización que sí tenga los permisos adecuados.

Gestión de la clasificación de datos y privacidad

Las siguientes preguntas proporcionan información sobre cómo administrar la clasificación de datos y la configuración de privacidad.

¿Cómo activo o desactivo la clasificación de datos?

Primero debe implementar una instancia de Clasificación de datos en la consola o en un sistema local. Una vez que la instancia esté en ejecución, puede habilitar el servicio en sistemas, bases de datos y otras fuentes de datos existentes desde la pestaña **Configuración** o seleccionando un sistema específico. "Aprenda cómo empezar" .

La activación de la clasificación de datos en una fuente de datos da como resultado un escaneo inicial inmediato. Los resultados del escaneo se muestran poco después.

Puede deshabilitar la Clasificación de datos para que no escanee un sistema individual, una base de datos o un grupo de recursos compartidos de archivos desde la página Configuración de Clasificación de datos. Ver

"Eliminar fuentes de datos de la Clasificación de datos" .

Para eliminar por completo la instancia de Clasificación de datos, elimine manualmente la instancia de Clasificación de datos del portal de su proveedor de nube o de la ubicación local.

¿Puede el servicio excluir el escaneo de datos en ciertos directorios?

Sí. Si desea que la clasificación de datos excluya los datos escaneados que residen en determinados directorios de fuentes de datos, puede proporcionar esa lista al motor de clasificación. Después de aplicar ese cambio, la clasificación de datos excluirá el escaneo de datos en los directorios especificados. "Más información" .

¿Se escanean las instantáneas que residen en volúmenes ONTAP ?

No. La clasificación de datos no escanea instantáneas porque el contenido es idéntico al contenido del volumen.

¿Qué sucede si la clasificación de datos está habilitada en sus volúmenes ONTAP ?

Cuando la clasificación de datos escanea volúmenes que tienen datos fríos organizados en niveles de almacenamiento de objetos mediante escaneos de solo mapeo, escanea todos los datos: datos que están en discos locales y datos fríos organizados en niveles de almacenamiento de objetos. Esto también es válido para productos que no son de NetApp pero que implementan niveles.

El escaneo de solo mapeo no calienta los datos fríos: permanecen fríos y permanecen en el almacenamiento de objetos. Por otro lado, si realiza el escaneo de Mapa y Clasificación, algunas configuraciones podrían calentar los datos fríos.

Tipos de sistemas fuente y tipos de datos

Las siguientes preguntas se relacionan con los tipos de almacenamiento que se pueden escanear y los tipos de datos que se escanean.

¿Existen restricciones al desplegarse en una región gubernamental?

La clasificación de datos se admite cuando el agente de la consola se implementa en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD), también conocido como "modo restringido".

¿Qué fuentes de datos puedo escanear si instalo Data Classification en un sitio sin acceso a Internet?

> El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada. Para obtener documentación del modo privado en la interfaz heredada de BlueXP , consulte"Documentación en PDF para el modo privado de BlueXP" .

La clasificación de datos solo puede escanear datos de fuentes de datos que sean locales en el sitio local. En este momento, la clasificación de datos puede escanear las siguientes fuentes de datos locales en "modo privado", también conocido como sitio "oscuro":

- Sistemas ONTAP locales
- Esquemas de bases de datos
- Almacenamiento de objetos que utiliza el protocolo de Servicio de almacenamiento simple (S3)

¿Qué tipos de archivos son compatibles?

La clasificación de datos escanea todos los archivos en busca de información sobre categorías y metadatos, y muestra todos los tipos de archivos en la sección de tipos de archivos del panel.

Cuando la clasificación de datos detecta información de identificación personal (PII) o cuando realiza una búsqueda DSAR, solo se admiten los siguientes formatos de archivo:

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

¿Qué tipos de datos y metadatos captura la clasificación de datos?

La clasificación de datos le permite ejecutar un escaneo de "mapeo" general o un escaneo de "clasificación" completo en sus fuentes de datos. El mapeo proporciona solo una descripción general de alto nivel de sus datos, mientras que la clasificación proporciona un escaneo de nivel profundo de sus datos. El mapeo se puede realizar en sus fuentes de datos muy rápidamente porque no es necesario acceder a los archivos para ver los datos dentro de ellos.

- **Escaneo de mapeo de datos (Escaneo de solo mapeo)**: La clasificación de datos escanea solo los metadatos. Esto es útil para la administración y gobernanza de datos generales, la determinación rápida del alcance de proyectos, patrimonios muy grandes y la priorización. El mapeo de datos se basa en metadatos y se considera un escaneo **rápido**.

  Después de un escaneo rápido, puede generar un informe de mapeo de datos. Este informe es una descripción general de los datos almacenados en sus fuentes de datos corporativas para ayudarlo a tomar decisiones sobre la utilización de recursos, la migración, la copia de seguridad, la seguridad y los procesos de cumplimiento.

- **Escaneo profundo de clasificación de datos (escaneo de mapa y clasificación)**: La clasificación de datos escanea los datos utilizando protocolos estándar y permisos de solo lectura en todos sus entornos. Se abren y escanean archivos seleccionados para buscar datos comerciales confidenciales, información privada y problemas relacionados con ransomware.

  Después de un análisis completo, hay muchas funciones de clasificación de datos adicionales que puede aplicar a sus datos, como ver y refinar datos en la página de investigación de datos, buscar nombres dentro de archivos, copiar, mover y eliminar archivos de origen, y más.

La clasificación de datos captura metadatos como: nombre de 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 datos puede identificar muchos tipos de datos privados, como información personal (PII) e información personal confidencial (SPII). Para obtener más detalles sobre los datos privados, consulteCategorías de datos privados que escanea la Clasificación de Datos .

¿Puedo limitar la información de clasificación de datos a usuarios específicos?

Sí, la clasificación de datos está completamente integrada con la NetApp Console. Los usuarios de la NetApp Console solo pueden ver la información de los sistemas que pueden ver según sus permisos.

Además, si desea permitir que ciertos usuarios solo vean los resultados del análisis de Clasificación de datos sin tener la capacidad de administrar las configuraciones de Clasificación de datos, puede asignar a esos usuarios el rol de **Visor de clasificación** (cuando use la NetApp Console en modo estándar) o el rol de **Visor de cumplimiento** (cuando use la NetApp Console en modo restringido). "Más información" .

¿Alguien puede acceder a los datos privados enviados entre mi navegador y Data Classification?

No. Los datos privados enviados entre su navegador y la instancia de clasificación de datos están protegidos con cifrado de extremo a extremo mediante TLS 1.2, lo que significa que ni NetApp ni NetApp pueden leerlos. La clasificación de datos no compartirá ningún dato ni resultado con NetApp a menos que usted solicite y apruebe el acceso.

Los datos que se escanean permanecen dentro de su entorno.

¿Cómo se manejan los datos sensibles?

NetApp no tiene acceso a datos confidenciales y no los muestra en la interfaz de usuario. Los datos sensibles se enmascaran, por ejemplo, se muestran los últimos cuatro números de la información de la tarjeta de crédito.

¿Dónde se almacenan los datos?

Los resultados del escaneo se almacenan en Elasticsearch dentro de su instancia de clasificación de datos.

¿Cómo se accede a los datos?

La clasificación de datos accede a los datos almacenados en Elasticsearch a través de llamadas API, que requieren autenticación y están encriptadas mediante AES-128. Para acceder directamente a Elasticsearch se requiere acceso root.

Licencias y costos

La siguiente pregunta se relaciona con las licencias y los costos de uso de la Clasificación de Datos.

¿Cuánto cuesta la clasificación de datos?

La clasificación de datos es una capacidad central de la NetApp Console . No está cargado

Implementación del agente de consola

Las siguientes preguntas se relacionan con el agente de consola.

¿Qué es el agente de consola?

El agente de consola es un software que se ejecuta en una instancia de cómputo, ya sea dentro de su cuenta en la nube o en sus instalaciones, y que permite que la NetApp Console administre de forma segura los

recursos de la nube. Debe implementar un agente de consola para utilizar la clasificación de datos.

¿Dónde se debe instalar el agente de consola?

Al escanear datos, el agente de consola de NetApp Console debe instalarse en las siguientes ubicaciones:

- Para Cloud Volumes ONTAP en AWS o Amazon FSx para ONTAP: el agente de consola está en AWS.
- Para Cloud Volumes ONTAP en Azure o en Azure NetApp Files: el agente de consola está en Azure.
- Para Cloud Volumes ONTAP en GCP: el agente de consola está en GCP.
- Para sistemas ONTAP locales: el agente de consola está local.

Si tiene datos en estas ubicaciones, es posible que necesite utilizar "varios agentes de consola" .

¿La clasificación de datos requiere acceso a credenciales?

La clasificación de datos por sí sola no recupera las credenciales de almacenamiento. En cambio, se almacenan dentro del agente de la consola.

La clasificación de datos utiliza credenciales del plano de datos, por ejemplo, credenciales CIFS, para montar recursos compartidos antes de escanear.

¿La comunicación entre el servicio y el agente de la consola utiliza HTTP?

Sí, la clasificación de datos se comunica con el agente de la consola mediante HTTP.

Implementación de clasificación de datos

Las siguientes preguntas se relacionan con la instancia de Clasificación de datos independiente.

¿Qué modelos de implementación admite la clasificación de datos?

La NetApp Console permite al usuario escanear e informar sobre sistemas prácticamente en cualquier lugar, incluidos entornos locales, en la nube e híbridos. La clasificación de datos normalmente se implementa utilizando un modelo SaaS, en el que el servicio se habilita a través de la interfaz de la consola y no requiere instalación de hardware o software. Incluso en este modo de implementación de hacer clic y ejecutar, la gestión de datos se puede realizar independientemente de si los almacenes de datos están en las instalaciones o en la nube pública.

¿Qué tipo de instancia o máquina virtual se requiere para la clasificación de datos?

Cuando"implementado en la nube" :

- En AWS, la clasificación de datos se ejecuta en una instancia m6i.4xlarge con un disco GP2 de 500 GiB. Puede seleccionar un tipo de instancia más pequeña durante la implementación.
- En Azure, la clasificación de datos se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 500 GiB.
- En GCP, la clasificación de datos se ejecuta en una máquina virtual n2-standard-16 con un disco persistente estándar de 500 GiB.

"Obtenga más información sobre cómo funciona la clasificación de datos" .

¿Puedo implementar la clasificación de datos en mi propio host?

Sí. Puede instalar el software de clasificación de datos en un host Linux que tenga acceso a Internet en su red o en la nube. Todo funciona de la misma manera y usted continúa administrando la configuración y los resultados del escaneo a través de la Consola. Ver"Implementación de la clasificación de datos en las instalaciones" para conocer los requisitos del sistema y los detalles de instalación.

¿Qué pasa con los sitios seguros sin acceso a Internet?

Sí, eso también es compatible. Puede"Implementar la clasificación de datos en un sitio local que no tiene acceso a Internet" para sitios completamente seguros.

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

"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. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

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

Patentes

Puede encontrar una lista actualizada 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 aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

- "Aviso para la NetApp Console"
- "Aviso sobre la NetApp Data Classification"