Manos a la obra

Cloud Data Sense

NetApp
March 08, 2023

Tabla de Contenido

Manos a la obra

Más información acerca de Cloud Data Sense

Cloud Data Sense es un servicio de regulación de datos para BlueXP (anteriormente Cloud Manager) que analiza sus fuentes de datos corporativas, tanto en las instalaciones como en el cloud para asignar y clasificar los datos, así como para identificar información privada. Esto puede ayudarle a reducir los riesgos de seguridad y de cumplimiento de normativas, a reducir los costes de almacenamiento y a facilitar los proyectos de migración de datos.

"Obtenga más información acerca de los casos de uso de Cloud Data Sense".

Funciones

Cloud Data Sense usa la inteligencia artificial (IA), el procesamiento de lenguaje natural (NLP) y el aprendizaje automático (ML) para entender el contenido que analiza con el fin de extraer entidades y clasificar el contenido de manera acorde. Esto permite que Data Sense proporcione las siguientes áreas de funcionalidad.

Mantenga el cumplimiento normativo

Data sense proporciona varias herramientas que le ayudan en sus tareas de cumplimiento de normativas. Puede utilizar el sentido de los datos para:

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

Refuerce la seguridad

La detección de datos puede identificar datos que podrían estar en riesgo de acceder a ellos por motivos criminales. Puede utilizar el sentido de los datos para:

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

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

Optimice la utilización del almacenamiento

El sentido de los datos proporciona herramientas que pueden ayudar a obtener el coste total de propiedad (TCO) de su almacenamiento. Puede utilizar el sentido de los datos para:

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

Acelere la migración de datos

El sentido de los datos se puede utilizar para analizar sus datos en las instalaciones antes de migrarlos al cloud público o privado. Puede utilizar el sentido de los datos para:

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

Orígenes de datos compatibles

Cloud Data Sense puede analizar y analizar datos estructurados y no estructurados de los siguientes tipos de fuentes de datos:

NetApp:

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

No NetApp:

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

Cloud:

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

Bases de datos:

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

Data sense admite las versiones 3.x, 4.0 y 4.1 de NFS, y las versiones 1.x, 2.0, 2.1 y 3.0 de CIFS.

Coste

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

  "Descubra cómo otorgar licencias a Cloud Data Sense".

- La instalación de Cloud Data Sense en el cloud requiere la puesta en marcha de una instancia de cloud, lo cual resulta en cargos del proveedor de cloud en el que está puesta en marcha. Consulte el tipo de instancia que se pone en marcha en cada cloud proveedor. No tiene coste si instala Data Sense en un sistema local.
- Cloud Data Sense requiere que haya implementado un conector BlueXP. En muchos casos ya tiene un conector debido a otros servicios y almacenamiento que está utilizando en BlueXP. La instancia de Connector representa cargos del proveedor de cloud en el que se ha puesto en marcha. Consulte "tipo de instancia que se pone en marcha para cada proveedor de cloud". No hay costo si instala el conector en un sistema local.

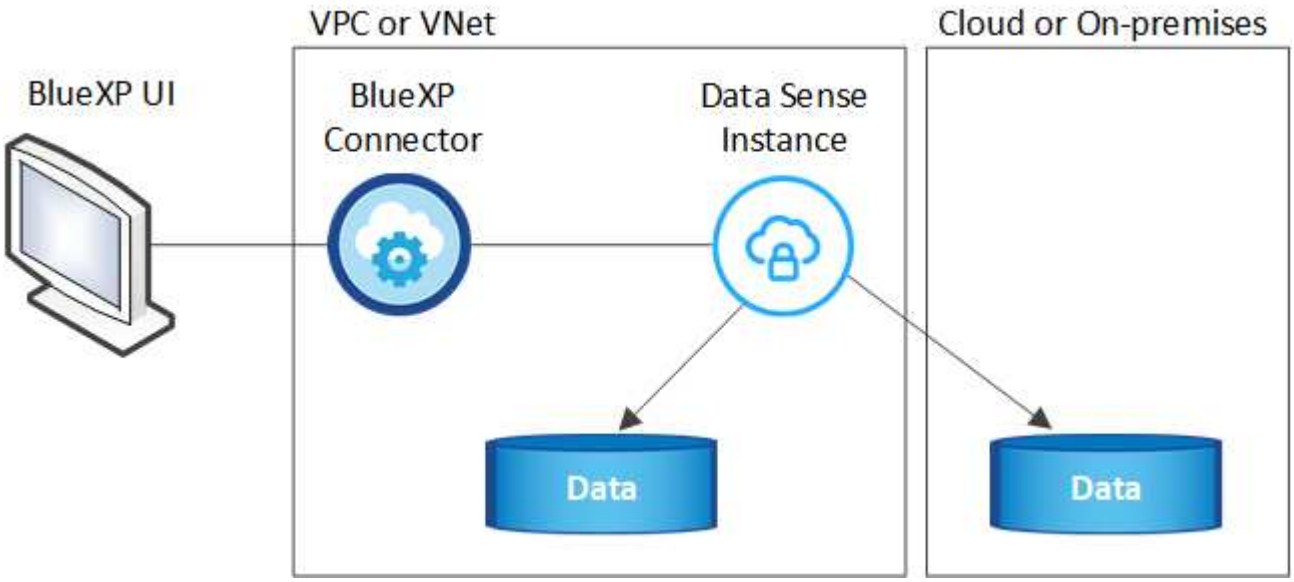
Costes de transferencia de datos

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

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

La instancia de Cloud Data Sense

Al implementar detección de datos en la nube, BlueXP despliega la instancia en la misma subred que Connector. "Más información sobre conectores."



Tenga en cuenta lo siguiente acerca de la instancia predeterminada:

- En AWS, Cloud Data SENSE se ejecuta en una "instancia m5.4xlarge" Con un disco GP2 de 500 GB. La imagen del sistema operativo es Amazon Linux 2 (Red Hat 7.3.1).

  En regiones donde no está disponible m5.4xLarge, Data Sense se ejecuta en una instancia m4.4xLarge en su lugar.

- En Azure, Cloud Data Sense se ejecuta en una "VM Standard_D16s_v3" Con un disco de 512 GB. La imagen del sistema operativo es CentOS 7.8.
- En GCP, Cloud Data Sense se ejecuta en una "n2-Standard-16 VM" Con un disco persistente estándar de 512 GB. La imagen del sistema operativo es CentOS 7.9.

  En regiones donde no está disponible n2-standard-16, Data Sense se ejecuta en un equipo virtual n2d-standard-16 o n1-standard-16.

- La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Sólo se despliega una instancia de detección de datos por conector.

También puede poner en marcha Data Sense en un host Linux en sus instalaciones o en un host de su proveedor de cloud preferido. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija. Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga acceso a Internet.

La instancia debe permanecer en ejecución en todo momento debido a que Cloud Data Sense analiza continuamente los datos.

Con un tipo de instancia más pequeño

Puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero hay algunas limitaciones al utilizar estos sistemas menos potentes.

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

Al implementar Data Sense en el cloud, envíe un correo electrónico a ng-contact-data-sense@netapp.com para obtener ayuda si desea usar uno de estos sistemas más pequeños. Tendremos que trabajar con usted para poner en marcha estas configuraciones de cloud más pequeñas.

Al poner en marcha la detección de datos en las instalaciones, solo tiene que utilizar un host Linux con las especificaciones más pequeñas. No necesita ponerse en contacto con NetApp para obtener ayuda.

Cómo funciona el Cloud Data Sense

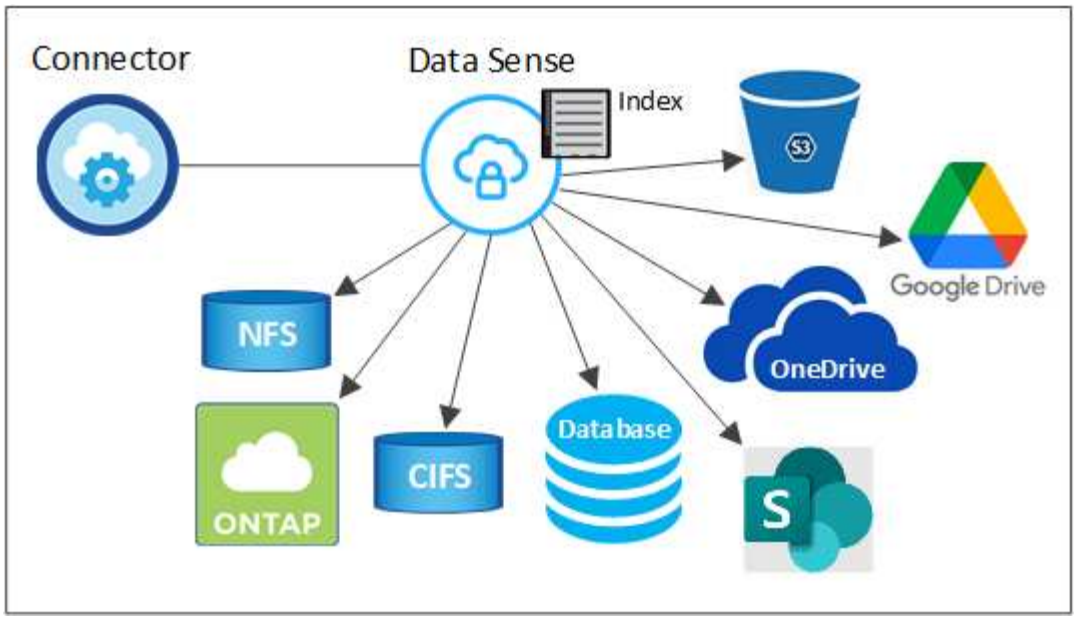
En un entorno de alto nivel, Cloud Data Sense funciona así:

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

Cómo funcionan las exploraciones

Después de habilitar Cloud Data SENSE y seleccionar los volúmenes, bloques, esquemas de base de datos, o los datos de usuario de OneDrive o SharePoint que desea analizar, comienza de inmediato a analizar los datos para identificar datos personales y confidenciales. Asigna los datos de la organización, categoriza cada archivo e identifica y extrae entidades y patrones predefinidos en los datos. El resultado de la exploración es un índice de información personal, información personal confidencial, categorías de datos y tipos de archivo.

El sentido de los datos se conecta a los datos como cualquier otro cliente mediante el montaje de volúmenes NFS y CIFS. Se accede automáticamente a los volúmenes NFS como de solo lectura, mientras que se necesitan proporcionar credenciales de Active Directory para analizar volúmenes CIFS.



Después del análisis inicial, Data Sense analiza continuamente los datos para detectar cambios incrementales (por eso es importante mantener la instancia en ejecución).

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

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

Cloud Data Sense permite ejecutar un análisis general de "asignación" en orígenes de datos seleccionados. La asignación sólo ofrece una descripción general de alto nivel de los datos, mientras que la clasificación proporciona un análisis profundo de los datos. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro.

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

En la siguiente tabla se muestran algunas de las diferencias:

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

Función	Clasificación	Asignación
Categorice los datos mediante etiquetas AIP y etiquetas de estado	Sí	No
Copie, elimine y mueva los archivos de origen	Sí	No
Capacidad para ejecutar otros informes	Sí	No

¿Con qué rapidez se analizan los datos del análisis de detección de datos

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

- Al realizar exploraciones de mapas, Data Sense puede escanear entre 100-150 TIBs de datos por día, por nodo de escáner.
- Al realizar exploraciones de clasificación, Data Sense puede escanear entre 15-40 TIBs de datos por día, por nodo de escáner.

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

Información que índices Cloud Data SENSE

Data Sense recopila, indexa y asigna categorías a sus datos (archivos). Los datos que indexan Data Sense incluyen los siguientes:

Metadatos estándar
: Cloud Data Sense recopila metadatos estándar sobre archivos: El tipo de archivo, su tamaño, fechas de creación y modificación, etc.

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

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

Categorías
: Cloud Data Sense toma los datos que ha analizado 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. "Más información sobre categorías".

Tipos
: Cloud Data Sense toma los datos que ha analizado y los divide por tipo de archivo. "Obtenga más información sobre los tipos".

Reconocimiento de entidad de nombre
: Cloud Data Sense utiliza la IA para extraer los nombres de las personas naturales de los documentos. "Obtenga información sobre cómo responder a las solicitudes de acceso a sujetos de datos".

Información general sobre redes

BlueXP implementa la instancia de Cloud Data Sense con un grupo de seguridad que permite conexiones HTTP entrantes desde la instancia de Connector.

Al utilizar BlueXP en modo SaaS, la conexión a BlueXP se ofrece mediante HTTPS y los datos privados que se envían entre su navegador y la instancia de Data Sense están protegidos con cifrado completo, lo que significa que NetApp y terceros no pueden leerla.

Las reglas salientes están completamente abiertas. Se necesita acceso a Internet para instalar y actualizar el software Data Sense y para enviar mediciones de uso.

Si tiene requisitos estrictos de red, "Descubra los extremos que los contactos de Cloud Data Sense".

Acceso de los usuarios a la información de cumplimiento

La función a la que se ha asignado cada usuario proporciona distintas funcionalidades dentro de BlueXP y Cloud Data Sense:

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

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

Ponga en marcha Cloud Data Sense

Ponga en marcha Cloud Data en el cloud

Complete unos pasos para poner en marcha Cloud Data en el cloud. La instancia de detección de datos se pondrá en marcha en la misma red de proveedores de cloud que BlueXP Connector.

Tenga en cuenta que también puede "Instale Data Sense en un host Linux que tenga acceso a Internet". Este tipo de instalación puede ser una buena opción si prefiere analizar sistemas ONTAP en las instalaciones mediante una instancia de Data Sense que también está ubicada en las instalaciones — pero esto no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

Inicio rápido

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

1 Cree un conector

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

También puede hacerlo "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube.

2 Revise los requisitos previos

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Data SENSE a través del puerto 443, entre otros. Vea la lista completa.

La configuración predeterminada requiere 16 vCPU para la instancia de Cloud Data Sense. Consulte "más detalles acerca del tipo de instancia".

3 Ponga en marcha Cloud Data Sense

Inicie el asistente de instalación para implementar la instancia de Cloud Data Sense en el cloud.

4 Suscríbase al servicio Cloud Data Sense

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

Cree un conector

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

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

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

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

Tenga en cuenta que también puede "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube. Algunos usuarios que planean instalar Data Sense on-prem también pueden optar por instalar el conector on-prem.

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

Apoyo del Gobierno en las regiones

Cloud Data Sense es compatible cuando el conector se ha puesto en marcha en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD). Cuando se implementa de esta manera, Data Sense tiene las siguientes restricciones:

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

Revise los requisitos previos

Revise los siguientes requisitos previos para asegurarse de que dispone de una configuración compatible antes de implementar Cloud Data Sense en el cloud.

Habilite el acceso a Internet de salida desde Cloud Data Sense

Cloud Data Sense requiere acceso saliente a Internet. Si la red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de detección de datos tiene acceso saliente a Internet para contactar con los siguientes puntos finales. Al implementar Data Sense en la nube, se encuentra en la misma subred que el conector.

Revise la siguiente tabla según cuál sea su caso, ya se esté poniendo en marcha Cloud Data Sense en AWS, Azure o GCP.

extremos necesarios para implementaciones de AWS:

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Permite que Cloud Data Sense acceda y descargue manifiestos y plantillas, así como para enviar registros y métricas.

Extremos necesarios para implementaciones de Azure y GCP:

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

Asegúrese de que BlueXP tiene los permisos necesarios

Asegúrese de que BlueXP tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Data Sense. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".

Compruebe sus límites de vCPU

Compruebe que el límite de vCPU de su proveedor de cloud permita poner en marcha una instancia con 16 núcleos. Deberá verificar el límite de vCPU para la familia de instancias correspondiente en la región donde se está ejecutando BlueXP. "Consulte los tipos de instancia necesarios".

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

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

  Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

Asegúrese de que BlueXP Connector puede acceder a Cloud Data Sense

Asegure la conectividad entre el conector y la instancia de Cloud Data Sense. El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Esta conexión permite la implementación de la instancia de Data Sense y permite ver información en las fichas cumplimiento y Gobierno. Cloud Data Sense es compatible en regiones gubernamentales de AWS y Azure.

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

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

Asegúrese de que puede mantener en funcionamiento Cloud Data Sense

La instancia de Cloud Data Sense tiene que seguir para poder analizar sus datos de forma continua.

Garantice la conectividad del navegador web con Cloud Data Sense

Después de habilitar Cloud Data Sense, asegúrese de que los usuarios acceden a la interfaz BlueXP desde un host que tiene una conexión a la instancia de detección de datos.

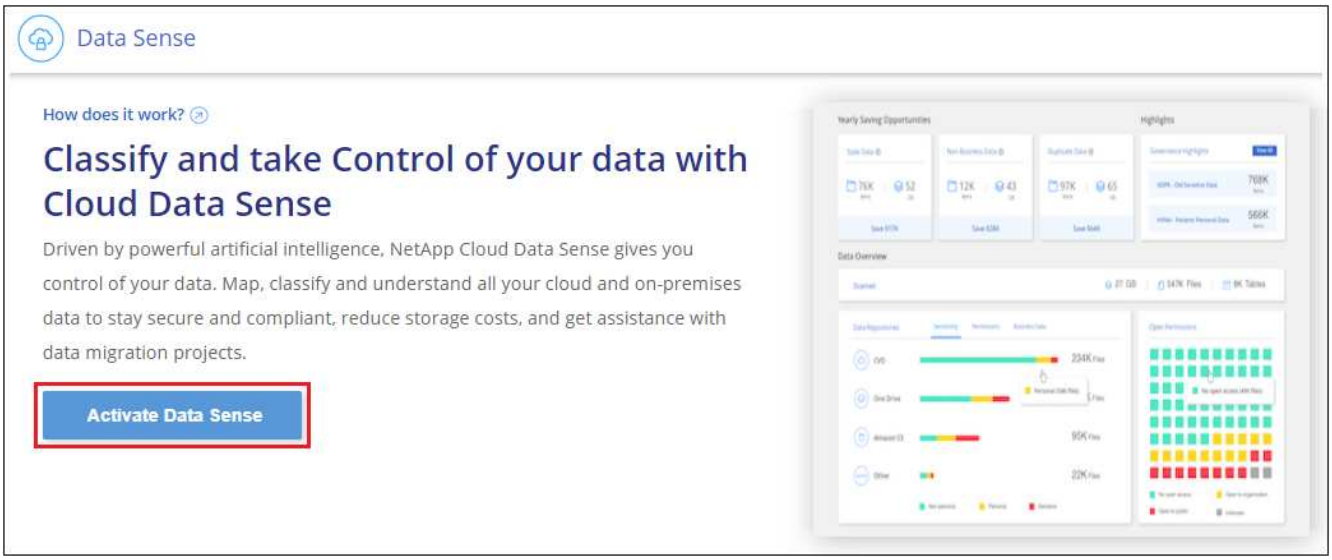
La instancia de detección de datos utiliza una dirección IP privada para garantizar que los datos indexados no sean accesibles a Internet. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esa conexión puede provenir de una conexión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

Ponga en marcha el sentido de los datos en el cloud

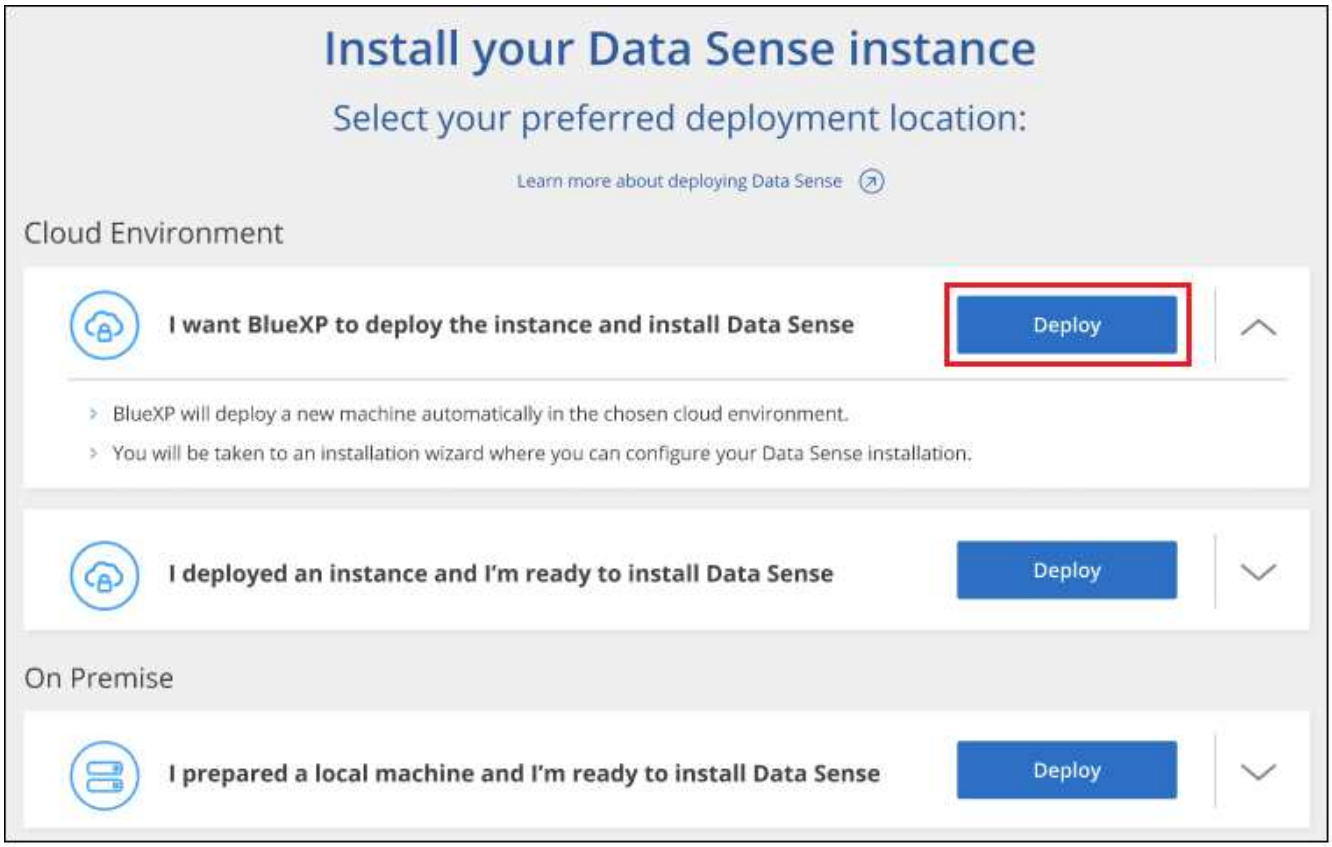
Siga estos pasos para poner en marcha una instancia de Cloud Data Sense en el cloud.

Pasos

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



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



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

5. Cuando se despliegue la instancia, haga clic en **continuar con la configuración** para ir a la página *Configuration*.

Resultado

BlueXP pone en marcha la instancia de Cloud Data Sense en su proveedor de cloud.

Las actualizaciones al conector BlueXP y al software de detección de datos se automatizan siempre que las instancias tengan conexión a Internet.

El futuro

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

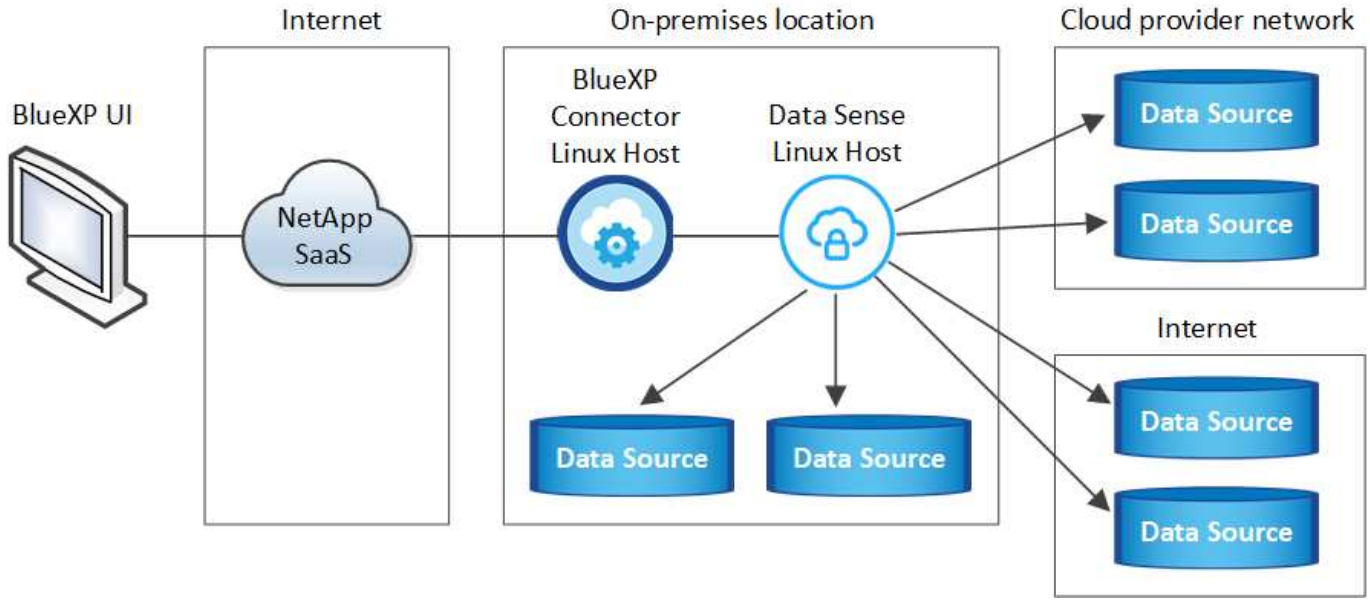
También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Ponga en marcha Cloud Data Sense en un host que tiene acceso a Internet

Complete unos pasos para implementar Cloud Data Sense en un host Linux de su red, o en un host Linux en la nube, que tenga acceso a Internet.

La instalación en las instalaciones puede ser una buena opción si prefiere analizar sistemas ONTAP en las instalaciones mediante una instancia de detección de datos que también está ubicada en las instalaciones, pero esto no es un requisito. El software funciona exactamente de la misma manera, independientemente del método de instalación que elija.

La instalación típica en las instalaciones tiene los siguientes componentes y conexiones.



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

Tenga en cuenta que también puede "Ponga en marcha la detección de datos en un sitio en las instalaciones que no tenga acceso a Internet" para ubicaciones completamente seguras.

Inicio rápido

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

1 Cree un conector

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

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

"Creación de un conector en Azure", o. "Creación de un conector en GCP".

2 Revise los requisitos previos

Asegúrese de que el entorno pueda cumplir con los requisitos previos. Esto incluye acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Data SENSE a través del puerto 443, entre otros. Vea la lista completa.

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

3 Descargue e implemente Cloud Data Sense

Descargue el software Cloud Data Sense del sitio de soporte de NetApp y copie el archivo del instalador en el host Linux que tiene pensado utilizar. A continuación, inicie el asistente de instalación y siga las instrucciones para implementar la instancia de detección de datos.

4 Suscríbase al servicio Cloud Data Sense

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

Cree un conector

Se necesita un conector BlueXP para poder instalar y utilizar Data Sense. En la mayoría de los casos, es probable que tenga un conector configurado antes de intentar activar Cloud Data Sense porque la mayoría "Las funciones de BlueXP requieren un conector", pero hay casos en los que necesitará configurar uno ahora.

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

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

- Cuando se escanear datos en Cloud Volumes ONTAP en AWS, Amazon FSX para ONTAP o en bloques AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.

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

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

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

Tenga en cuenta que también puede "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube. Algunos usuarios que planean instalar Data Sense on-prem también pueden optar por instalar el conector on-prem.

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

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

Prepare el sistema host Linux

El software de detección de datos debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de software, etc. El host Linux puede estar en su red o en la nube. No se admite la detección de datos en un host que se comparte con otras aplicaciones; el host debe ser un host dedicado.

Asegúrese de que puede mantener en funcionamiento Cloud Data Sense. El equipo Cloud Data Sense tiene que seguir para analizar sus datos de forma continua.

- **CPU**: 16 núcleos
- **RAM**: 64 GB (la memoria de intercambio debe estar desactivada en el host)
- **Disco**: SSD con 500 GIB disponibles en /, o.
  - 100 GIB disponibles en /opt
  - 400 GIB disponibles en /var
  - 5 GIB en /tmp

    Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.
- **Tipo de instancia de AWS EC2**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "m5.4xgrande".
- **Tamaño de máquina virtual de Azure**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "Standard_D16s_v3".
- **Tipo de máquina GCP**: Tipo de instancia que cumple los requisitos de CPU y RAM anteriores. Lo recomendamos "n2-estándar-16".
- **Sistema operativo**: Red Hat Enterprise Linux o CentOS versiones 8.0 a 8.7
  - CentOS Stream 8 también es compatible
  - Se pueden utilizar las versiones 7.8 o 7.9, pero la versión de kernel de Linux debe ser 4.0 o posterior
  - El sistema operativo debe ser capaz de instalar el motor del docker
- **Red Hat Subscription Management**: Un sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación.
- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Sense:
  - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".
  - Python 3 versión 3.6 o posterior. "Ver las instrucciones de instalación".
- * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Le recomendamos que lo habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

```
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 tiene pensado utilizar hosts de detección de datos adicionales como nodos de escáner, agregue estas reglas al 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
```

Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

La dirección IP del sistema host Data Sense no se puede cambiar tras la instalación.

Habilite el acceso a Internet de salida desde Cloud Data Sense

Cloud Data Sense requiere acceso saliente a Internet. Si la red virtual o física utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de detección de datos tiene acceso saliente a Internet para contactar con los siguientes puntos finales.

Puntos finales	Específico
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con el sitio Web de BlueXP para la autenticación centralizada del usuario.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes de software, manifiestos, plantillas y para enviar registros y métricas.
https://support.compliance.api.bluexp.netapp.com/	Permite a NetApp transmitir datos desde registros de auditoría.
https://github.com/docker https://download.docker.com http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Proporciona paquetes de requisitos previos para la instalación.

Verifique que todos los puertos necesarios estén habilitados

Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el conector, detección de datos, Active Directory y sus orígenes de datos.

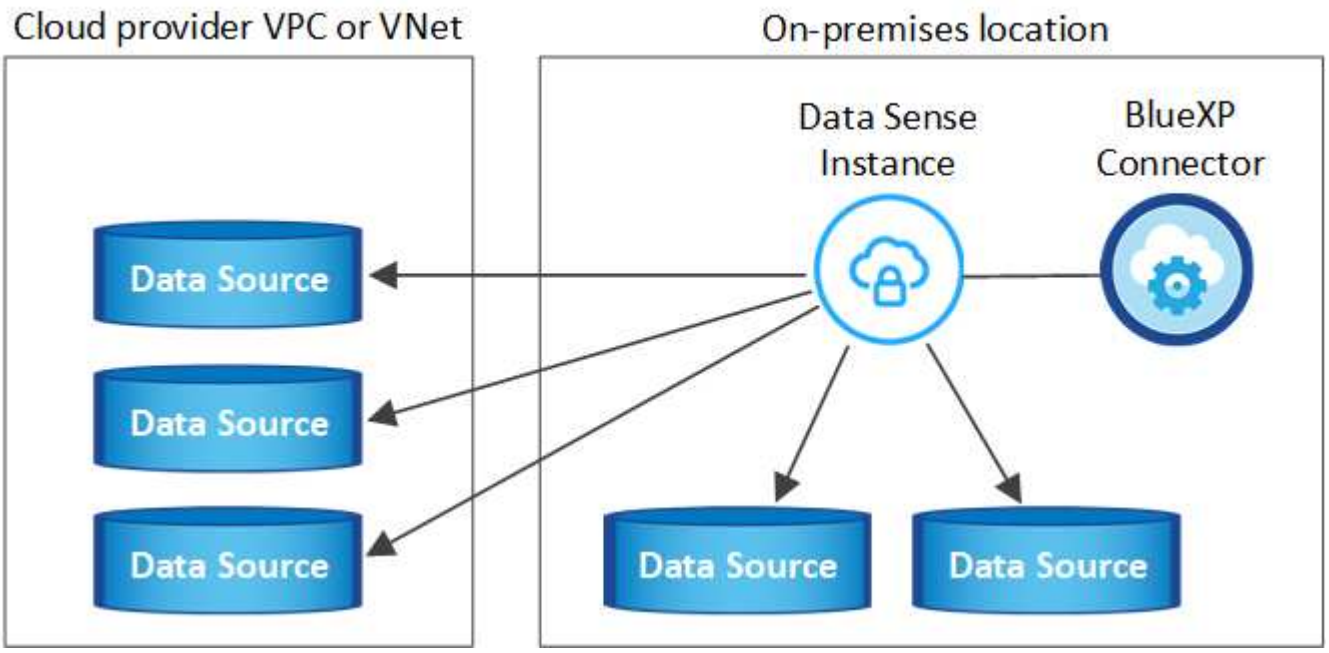
Tipo de conexión	Puertos	Descripción
Conector <> detección de datos	8080 (TCP), 443 (TCP) y 80	El firewall o las reglas de enrutamiento del conector deben permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, todas las comunicaciones salientes se permiten mediante el firewall predefinido o las reglas de enrutamiento. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.
Detección de los datos <> clúster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	Data Sense necesita una conexión de red a cada subred de Cloud Volumes ONTAP o a cada sistema ONTAP en las instalaciones. Los firewalls o las reglas de enrutamiento para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de detección de datos. Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.

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

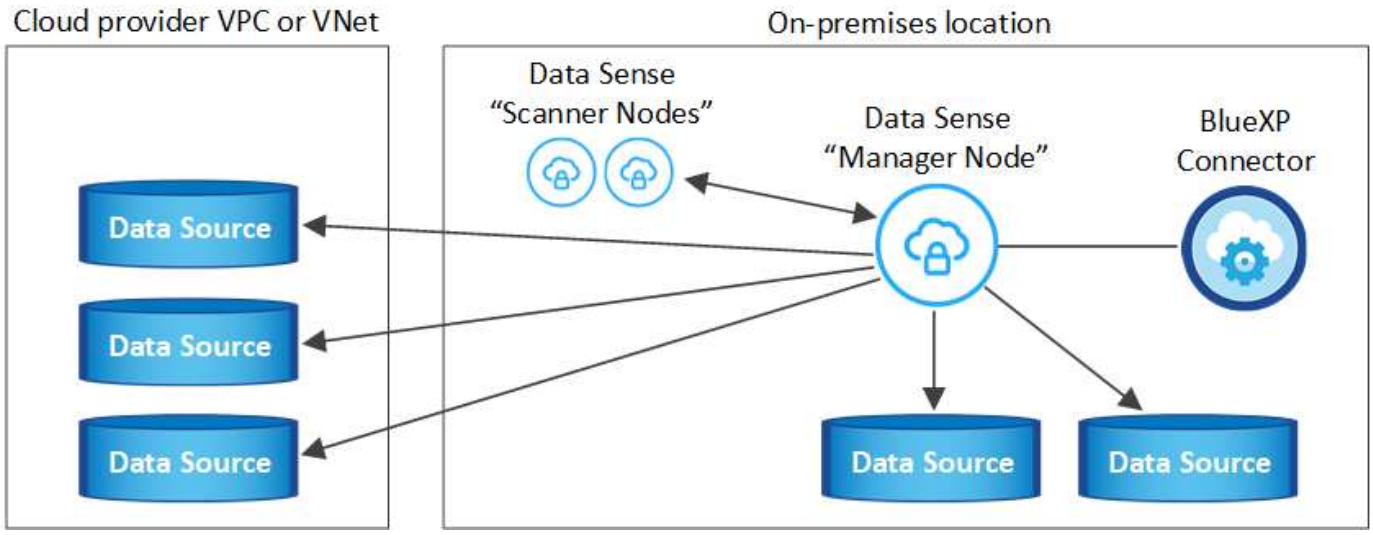
Si utiliza varios hosts de detección de datos para proporcionar potencia de procesamiento adicional para analizar sus fuentes de datos, tendrá que habilitar puertos y protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Ponga en marcha la detección de datos en las instalaciones

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



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



Consulte Preparar el sistema host Linux y.. Revisión de requisitos previos Para ver la lista completa de requisitos antes de poner en marcha Cloud Data Sense.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Cloud Data Sense no puede analizar actualmente bloques de S3, Azure NetApp Files o FSX para ONTAP cuando el software está instalado en las instalaciones. En estos casos, deberá poner en marcha un conector e instancia aparte de detección de datos en el cloud y en "Cambiar entre conectores" para sus diferentes fuentes de datos.

Instalación de un solo host para configuraciones típicas

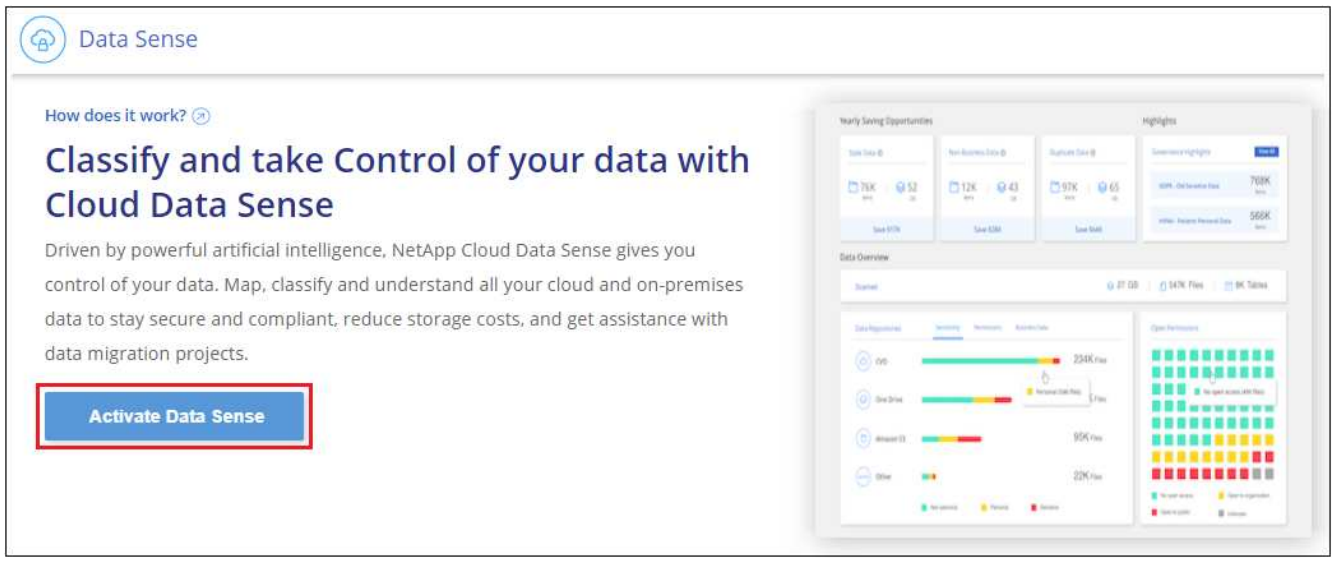
Siga estos pasos al instalar el software Data Sense en un solo host local.

Lo que necesitará

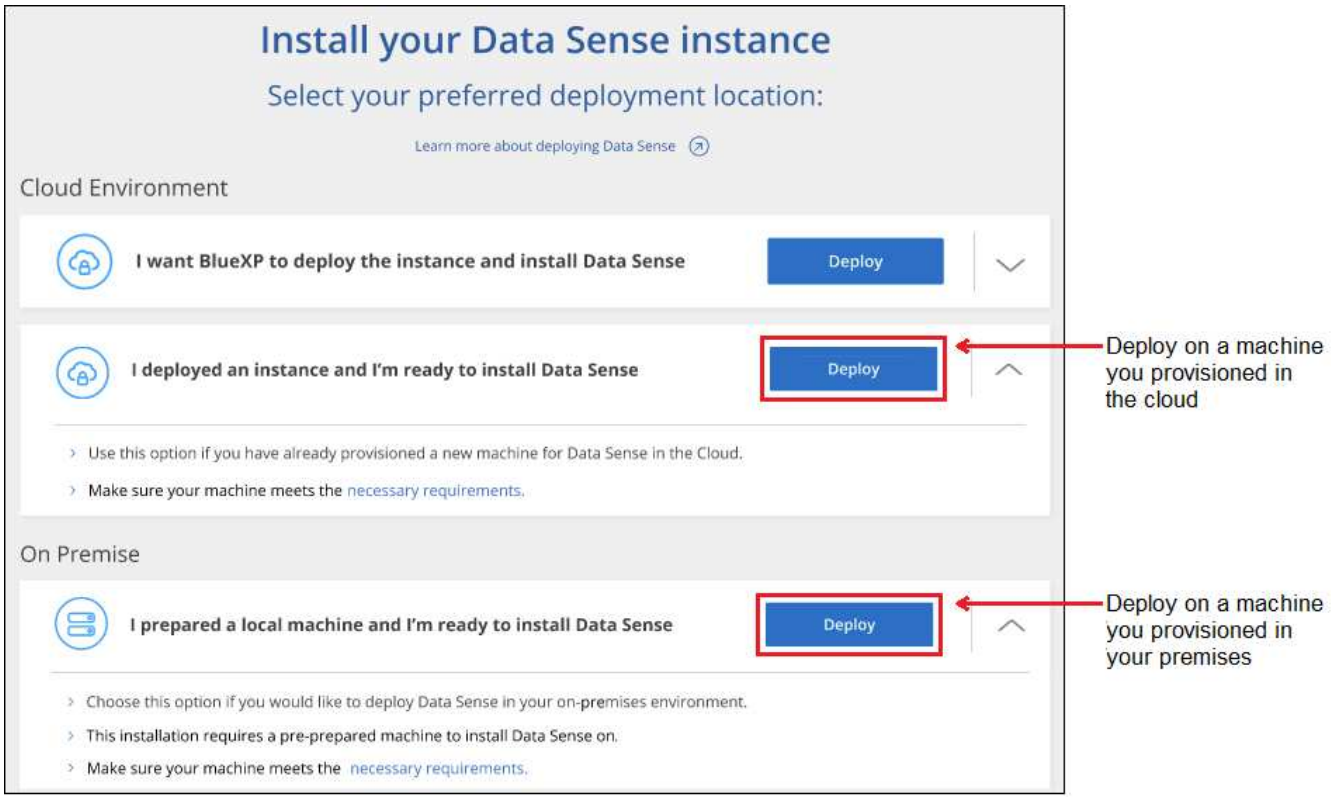
- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que el sistema tiene instalados los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.
- Si utiliza un proxy y está realizando intercepción TLS, deberá conocer la ruta en el sistema Data Sense Linux donde están almacenados los certificados de CA TLS.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

Pasos

1. Descargue el software Cloud Data Sense del "Sitio de soporte de NetApp". El archivo que debe seleccionar se denomina **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copie el archivo del instalador en el host Linux que tiene previsto utilizar (mediante `scp` o algún otro método).
3. En BlueXP, seleccione **Gobierno > Clasificación**.
4. Haga clic en **Activar detección de datos**.



5. En función de si está implementando una instancia en la nube o una instancia en sus instalaciones, haga clic en el botón **Deploy** correspondiente para iniciar el asistente de implementación de Data Sense.



6. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado y péguelo en un archivo de texto para poder usarlo más tarde y haga clic en **Cerrar**. Por ejemplo:

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Descomprima el archivo del instalador en el equipo host; por ejemplo:

```
tar -xzf DATASENSE-INSTALLER-V1.21.0.tar.gz
```

8. Cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de mensajes o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador.

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

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue la información que ha copiado del paso 6: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token>` b. Introduzca la dirección IP o el nombre de host del equipo host de Data Sense para que pueda accederse a él mediante la instancia de Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host de BlueXP Connector para que pueda accederse a ella mediante la instancia de detección de datos. d. Introduzca los detalles del proxy según se le solicite. Si su conector BlueXP ya utiliza un proxy, no es necesario volver a introducir esta información ya que detección de datos utilizará automáticamente el proxy utilizado por el conector.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host y proxy necesarios: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Agent_id* = ID del conector
   - *token* = token de usuario jwt
   - *DS_host* = dirección IP o nombre de host del sistema Data Sense Linux.
   - *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.
   - *proxy_host* = IP o nombre de host del servidor proxy si el host está detrás de un servidor proxy.
   - *proxy_Port* = Puerto para conectarse al servidor proxy (predeterminado 80).
   - *Proxy_Scheme* = combinación de conexiones: https o http (valor predeterminado http).
   - *proxy_USER* = Usuario autenticado para conectarse al servidor proxy, si se requiere autenticación básica.
   - *proxy_password* = Contraseña del nombre de usuario especificado.
   - *CA_cert_dir* = Ruta en el sistema Data Sense Linux que contiene paquetes de certificados de CA TLS adicionales. Sólo es necesario si el proxy está realizando intercepción TLS.

Resultado

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

Si hay conectividad sobre el puerto 8080 entre el equipo host y la instancia de conector, verá el progreso de instalación en la ficha detección de datos de BlueXP.

El futuro

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

También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

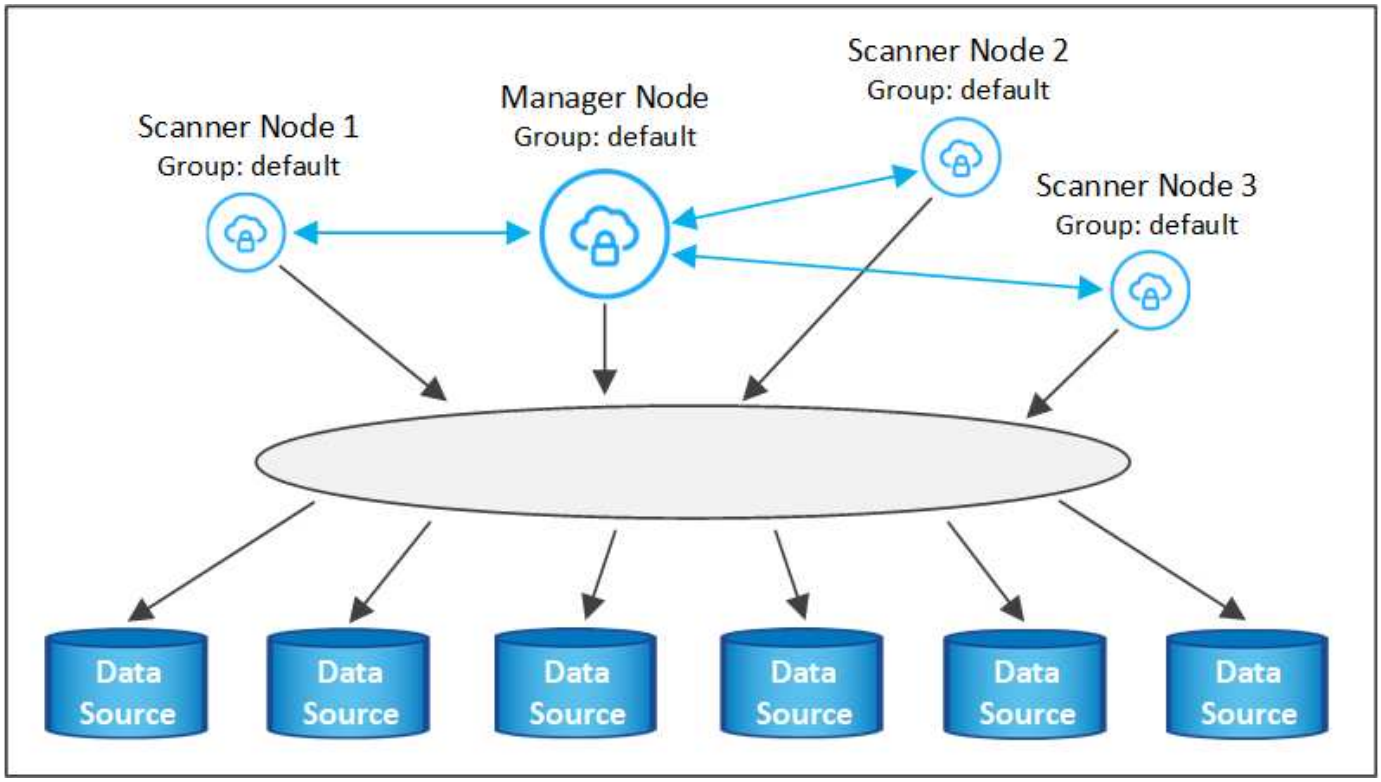
Agregar nodos de escáner a una implementación existente

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

Existen dos formas de añadir nodos de escáner adicionales:

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

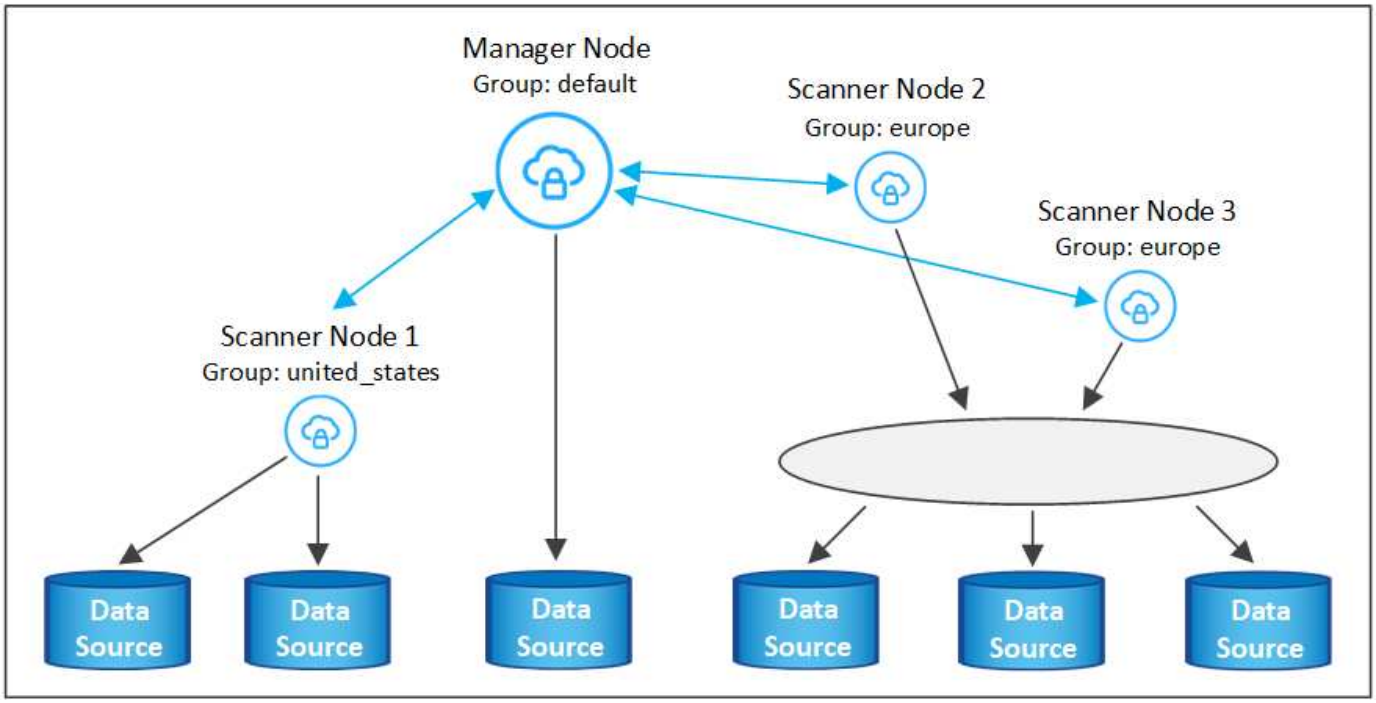
De forma predeterminada, los nuevos nodos de escáner que agregue se agregarán al pool general de recursos de digitalización. Esto se denomina "grupo de escáner predeterminado". En la siguiente imagen, hay 1 nodo de administrador y 3 nodos de escáner en el grupo "predeterminado" que están analizando todos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



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

de administrador y 3 nodos de escáner.

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



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

Puede elegir los grupos de escáneres que desea agregar a Data Sense y elegir sus nombres. El sentido de datos no impone que un nodo asignado a un grupo de escáner llamado "europa" se implemente en Europa.

Siga estos pasos para instalar nodos adicionales del escáner de detección de datos:

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

Lo que necesitará

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

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

- Si está utilizando `firewalld` En sus máquinas de Data Sense, le recomendamos que la habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

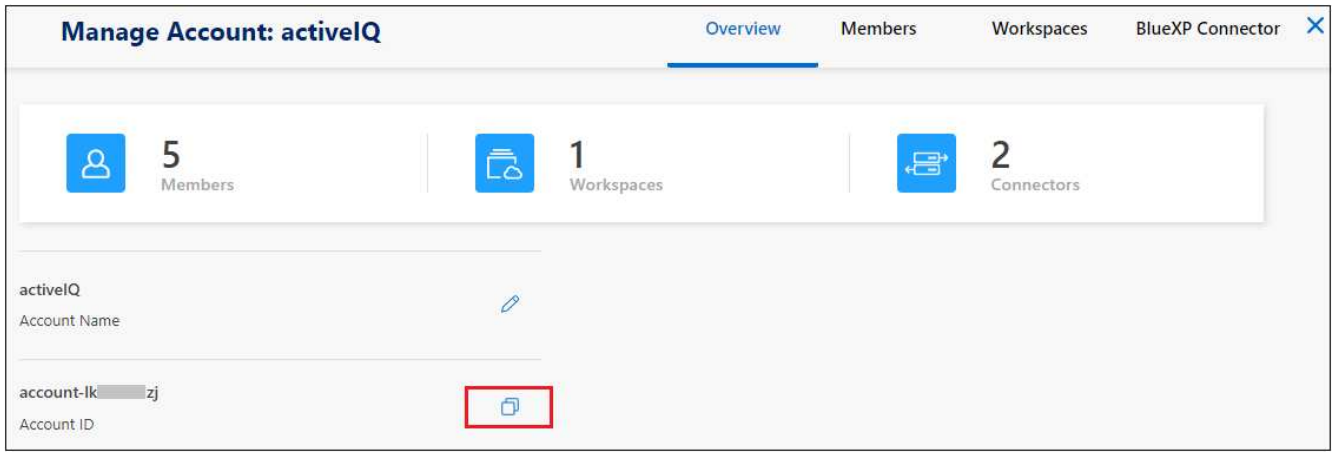
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

  Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

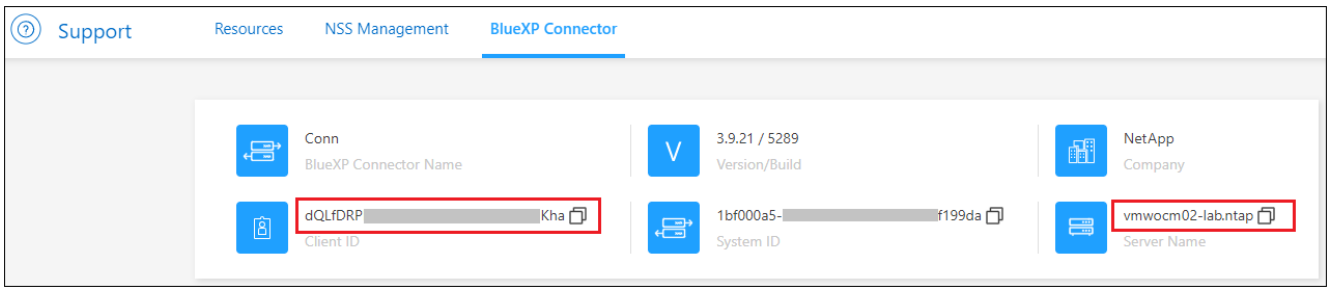
Requisitos previos

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

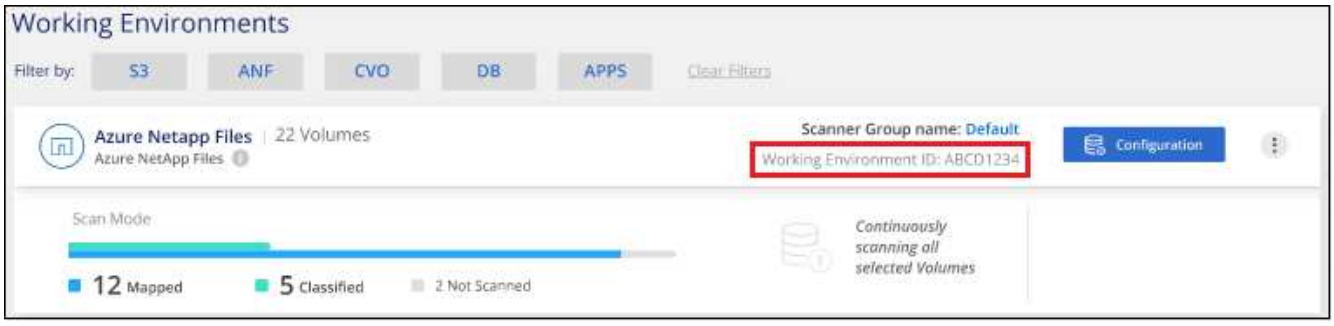
1. En la barra de menús de BlueXP, haga clic en **cuenta > Administrar cuentas**.



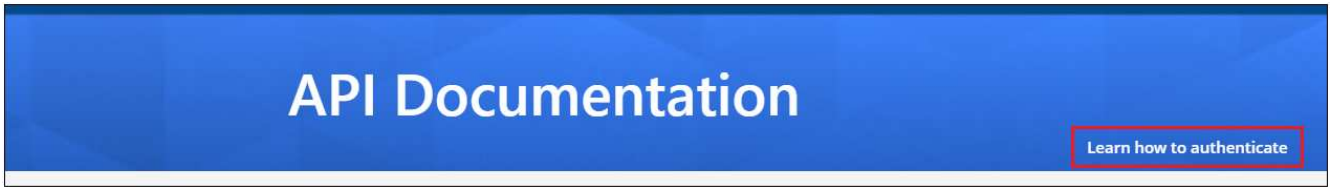
2. Copie el *ID de cuenta*.
3. En la barra de menús de BlueXP, haga clic en **Ayuda > Soporte > conector BlueXP**.



4. Copie el conector *Client ID* y el *Server Name*.
5. Si tiene previsto utilizar grupos de escáneres, en la ficha Configuración de detección de datos , copie el identificador de entorno de trabajo de cada entorno de trabajo que desee agregar a un grupo de escáneres.



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



7. Siga las instrucciones de autenticación y copie el *access token* de la respuesta.

Pasos

1. En el nodo de Data Sense Manager, ejecute el script "add_scanner_node.sh". Por ejemplo, este comando añade 2 nodos de escáner:

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

   Valores de variable:

   - *account_id* = ID de cuenta de NetApp
   - *Client_id* = ID de cliente del conector
   - *Cm_host* = dirección IP o nombre de host del sistema conector
   - *DS_Manager_ip* = Dirección IP privada del sistema de nodos de Data Sense Manager
   - *Node_Private_ip* = direcciones IP de los sistemas de nodos del escáner de detección de datos (varias IP de nodos del escáner están separadas por una coma)
   - *USER_token* = token de acceso de usuario JWT

2. Antes de que finalice la secuencia de comandos add_scanner_node, aparecerá un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j
   ```

3. En el host **cada nodo del escáner**:

   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).

   b. Descomprima el archivo del instalador.

   c. Pegue y ejecute el comando que copió en el paso 2.

   d. Si desea agregar un nodo de escáner a un "grupo de escáner", agregue el parámetro **-r <scanner_group_name>** al comando. De lo contrario, el nodo del escáner se agrega al grupo "predeterminado".

      Cuando la instalación termina en todos los nodos del escáner y se han Unido al nodo del administrador, el script "add_scanner_node.sh" también finaliza. La instalación puede tardar entre 10 y 20 minutos.

4. Si ha agregado algún nodo de escáner a un grupo de escáner, vuelva al nodo Administrador y realice las dos tareas siguientes:

   a. Abra el archivo "/opt/netapp/Datashense/working_Environment_to_scanner_group_config.yml" e introduzca la asignación para la que los grupos de escáneres exploran entornos de trabajo específicos. Deberá tener el *ID de entorno de trabajo* para cada origen de datos. Por ejemplo, las siguientes entradas agregan 2 entornos de trabajo al grupo de escáneres "europa" y 2 al grupo de escáneres "estados Unidos":

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

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

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

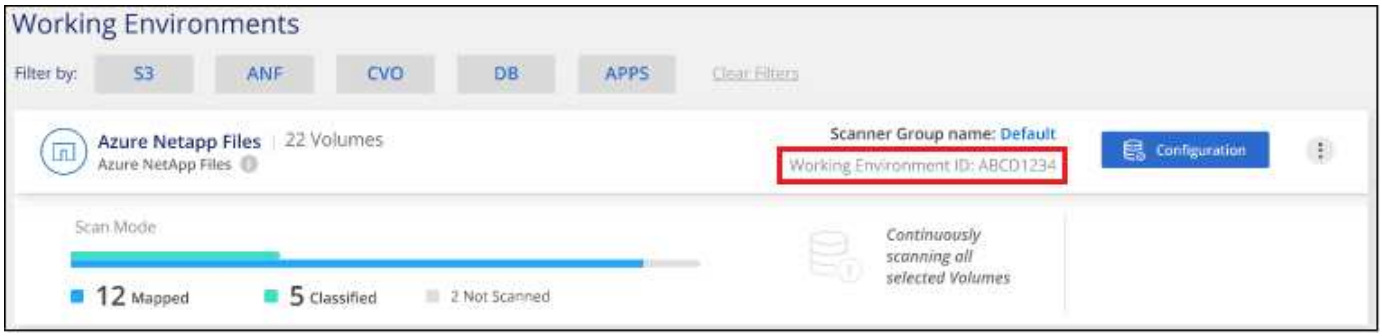
Resultado

Data Sense se configura con los nodos Manager y Scanner para analizar todos sus orígenes de datos.

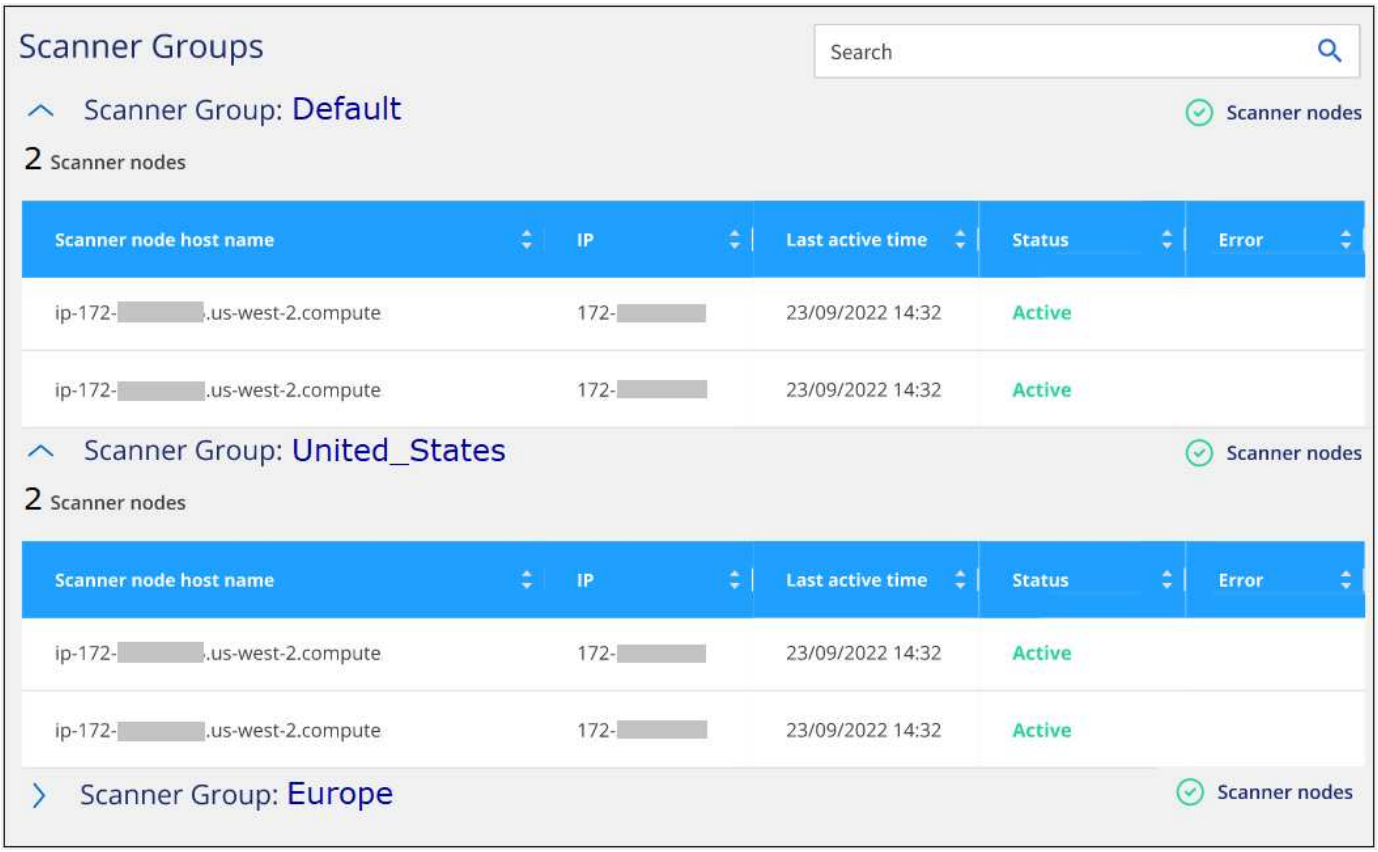
El futuro

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

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



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



Puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Instalación de varios hosts para configuraciones grandes

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

Siga estos pasos cuando instale software Data Sense en varios hosts locales al mismo tiempo. Tenga en cuenta que no puede utilizar "grupos de escáneres" al implementar varios hosts de esta forma.

Lo que necesitará

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

Puerto	Protocolos	Descripción
2377	TCP	Comunicaciones de gestión de clústeres

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

Pasos

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

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

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
   --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy-host
   <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy
   -user <proxy_user> --proxy-password <proxy_password>
   ```
3. Antes de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
   ```
4. En el host **cada nodo del escáner**:
   a. Copie el archivo de instalación de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) en el equipo host (usando `scp` o algún otro método).
   b. Descomprima el archivo del instalador.
   c. Pegue y ejecute el comando que copió en el paso 3.

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

Resultado

El instalador de Cloud Data Sense finaliza la instalación de los paquetes y registra la instalación. La instalación puede tardar entre 10 y 20 minutos.

El futuro

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

También puede hacerlo "Configure la licencia de Cloud Data Sense" en este momento. No se le cobrará hasta que finalice su prueba gratuita de 30 días.

Implemente Cloud Data Sense en un host sin acceso a Internet

Complete unos pasos para poner en marcha Cloud Data Sense en un host en un sitio local que no tiene acceso a Internet. Este tipo de instalación es perfecta para sus sitios seguros.

Tenga en cuenta que también puede "Ponga en marcha el sentido de los datos en un sitio local con acceso a Internet".

Orígenes de datos compatibles

Cuando se instala de esta manera (a veces denominado sitio "sin conexión" o "oscuro"), Data Sense solo puede analizar datos de orígenes de datos que también son locales del sitio local. En este momento, Data Sense puede analizar las siguientes fuentes de datos **locales**:

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

En situaciones especiales en las que necesita una instalación BlueXP muy segura, pero también desea analizar datos locales de cuentas de OneDrive o de cuentas de SharePoint Online, puede utilizar el instalador sin conexión de Data Sense y proporcionar acceso a Internet a unos pocos extremos seleccionados. Consulte Requisitos especiales para SharePoint y OneDrive para obtener más detalles.

Actualmente no hay compatibilidad para escanear cuentas Cloud Volumes ONTAP, Azure NetApp Files, FSX para ONTAP, AWS S3 o Google Drive cuando Data Sense se implementa en un sitio oscuro.

Limitaciones

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

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

  Tanto el conector BlueXP como el sensor de datos requerirán actualizaciones manuales periódicas para habilitar nuevas funciones. Puede ver la versión de Data Sense en la parte inferior de las páginas de la interfaz de usuario de Data Sense. Compruebe la "Notas de la versión de Cloud Data Sense" para ver las nuevas funciones de cada versión y si desea esas funciones. A continuación, puede seguir los pasos a.

"Actualice el conector BlueXP" y.. Actualice su software de detección de datos.

Inicio rápido

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

Instale el conector BlueXP

Si aún no tiene un conector instalado en su sitio local sin conexión, "Despliegue el conector" Ahora en un host Linux.

Revise los requisitos previos de detección de datos

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

Descargue e implemente Data Sense

Descargue el software Cloud Data Sense del sitio de soporte de NetApp y copie el archivo del instalador en el host Linux que tiene pensado utilizar. A continuación, inicie el asistente de instalación y siga las indicaciones para implementar la instancia de Cloud Data Sense.

Suscríbase al servicio Cloud Data Sense

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

Instale el conector BlueXP

Si aún no tiene un conector BlueXP instalado en su sitio local fuera de línea, "Despliegue el conector" En un host Linux del sitio sin conexión.

Prepare el sistema host Linux

El software de detección de datos debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de software, etc. No se admite la detección de datos en un host que se comparte con otras aplicaciones; el host debe ser un host dedicado.

- **Sistema operativo**: Red Hat Enterprise Linux o CentOS versiones 8.0 a 8.7
  - CentOS Stream 8 también es compatible
  - Se pueden utilizar las versiones 7.8 o 7.9, pero la versión de kernel de Linux debe ser 4.0 o posterior
  - El sistema operativo debe ser capaz de instalar Docker Engine
- **Disco**: SSD con 500 GIB disponibles en /, o.
  - 100 GIB disponibles en /opt
  - 400 GIB disponibles en /var
  - 5 GIB en /tmp

- **RAM**: 64 GB (la memoria de intercambio debe estar desactivada en el host)
- **CPU**: 16 núcleos

  Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

- **Software adicional**: Debe instalar el siguiente software en el host antes de instalar Data Sense:
  - Docker Engine versión 19.3.1 o posterior. "Ver las instrucciones de instalación".
  - Python 3 versión 3.6 o posterior. "Ver las instrucciones de instalación".
- * Consideraciones de Firewalld*: Si usted está planeando utilizar `firewalld`, Le recomendamos que lo habilite antes de instalar Data Sense. Ejecute los siguientes comandos para configurar `firewalld` Para que sea compatible con Data Sense:

  ```
  firewall-cmd --permanent --add-service=http
  firewall-cmd --permanent --add-service=https
  firewall-cmd --permanent --add-service=mysql
  firewall-cmd --permanent --add-port=80/tcp
  firewall-cmd --permanent --add-port=8080/tcp
  firewall-cmd --permanent --add-port=443/tcp
  firewall-cmd --permanent --add-port=555/tcp
  firewall-cmd --permanent --add-port=3306/tcp
  firewall-cmd --reload
  ```

  Si activa `firewalld` Después de instalar Data Sense, debe reiniciar docker.

La dirección IP del sistema host Data Sense no se puede cambiar tras la instalación.

Verifique los requisitos previos de BlueXP y Data Sense

Revise los siguientes requisitos previos para asegurarse de que dispone de una configuración compatible antes de implementar Cloud Data Sense.

- Asegúrese de que Connector tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Data Sense. Puede encontrar los últimos permisos de BlueXP en "Las políticas proporcionadas por NetApp".
- Asegúrese de que puede mantener en funcionamiento Cloud Data Sense. La instancia de Cloud Data Sense tiene que seguir para poder analizar sus datos de forma continua.
- Garantice la conectividad del navegador web con Cloud Data Sense. Después de habilitar Cloud Data Sense, asegúrese de que los usuarios acceden a la interfaz BlueXP desde un host que tiene una conexión a la instancia de detección de datos.

  La instancia de Data Sense utiliza una dirección IP privada para garantizar que los datos indexados no sean accesibles para otros. Como resultado, el navegador web que utiliza para acceder a BlueXP debe tener una conexión a esa dirección IP privada. Esta conexión puede provenir de un host que está dentro de la misma red que la instancia de Data Sense.

Verifique que todos los puertos necesarios estén habilitados

Debe asegurarse de que todos los puertos necesarios estén abiertos para la comunicación entre el conector, detección de datos, Active Directory y sus orígenes de datos.

Tipo de conexión	Puertos	Descripción
Conector <> detección de datos	8080 (TCP), 443 (TCP) y 80	El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 443 hacia y desde la instancia de detección de datos. Asegúrese de que el puerto 8080 está abierto para que pueda ver el progreso de la instalación en BlueXP.
Conector <> clúster ONTAP (NAS)	443 (TCP)	BlueXP detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos: • El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443. Si el conector está en la nube, el grupo de seguridad predefinido permite todas las comunicaciones salientes. • El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443. La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.
Detección de los datos <> clúster de ONTAP	• Para NFS: 111 (TCP\UDP) y 2049 (TCP\UDP) • Para CIFS: 139 (TCP\UDP) y 445 (TCP\UDP)	Data Sense necesita una conexión de red a cada subred de Cloud Volumes ONTAP o a cada sistema ONTAP en las instalaciones. Los grupos de seguridad para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de detección de datos. Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense: • Para NFS: 111 y 2049 • Para CIFS - 139 y 445 Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.

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

Si utiliza varios hosts de detección de datos para proporcionar potencia de procesamiento adicional para analizar sus fuentes de datos, tendrá que habilitar puertos y protocolos adicionales. "Consulte los requisitos de puerto adicionales".

Requisitos especiales para SharePoint y OneDrive

Cuando se implementa BlueXP y Data Sense en un sitio sin acceso a Internet, puede analizar archivos en cuentas de SharePoint Online y OneDrive proporcionando acceso a Internet a unos pocos extremos seleccionados.

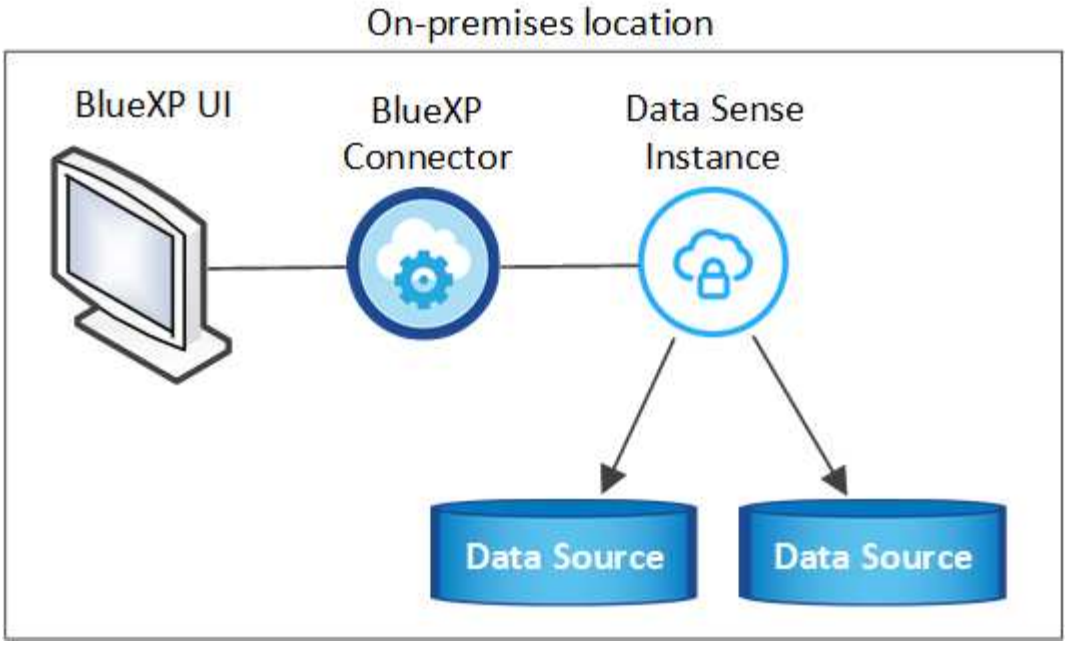
Las cuentas locales de SharePoint instaladas localmente se pueden analizar sin proporcionar acceso a Internet.

Puntos finales	Específico
\login.microsoft.com \graph.microsoft.com	Comunicación con los servidores de Microsoft para iniciar sesión en el servicio en línea seleccionado.
https://api.bluexp.netapp.com	Comunicación con el servicio BlueXP, que incluye cuentas de NetApp.

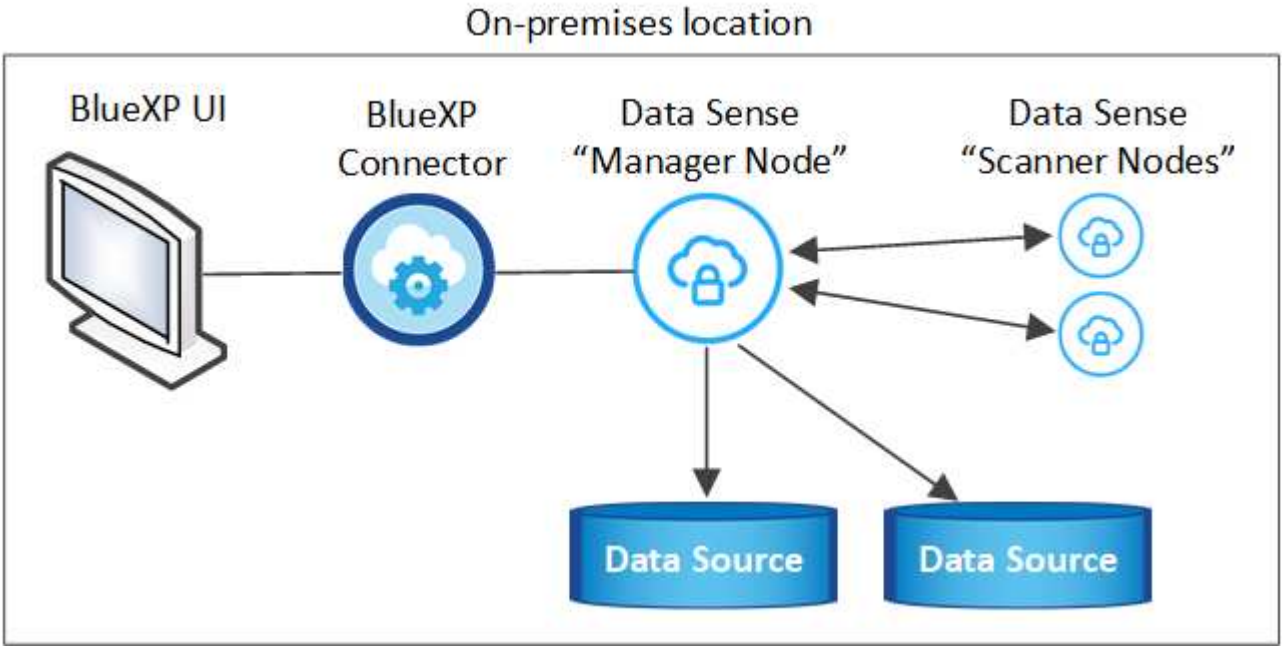
Sólo se requiere acceso a *api.bluexp.netapp.com* durante las conexiones iniciales con estos servicios externos.

Ponga en marcha Data Sense

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



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



Instalación de un solo host para configuraciones típicas

Siga estos pasos al instalar el software Data Sense en un solo host local en un entorno sin conexión.

Lo que necesitará

- Compruebe que su sistema Linux cumple con el requisitos del host.
- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine y Python 3).
- Asegúrese de tener privilegios de usuario raíz en el sistema Linux.

- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.

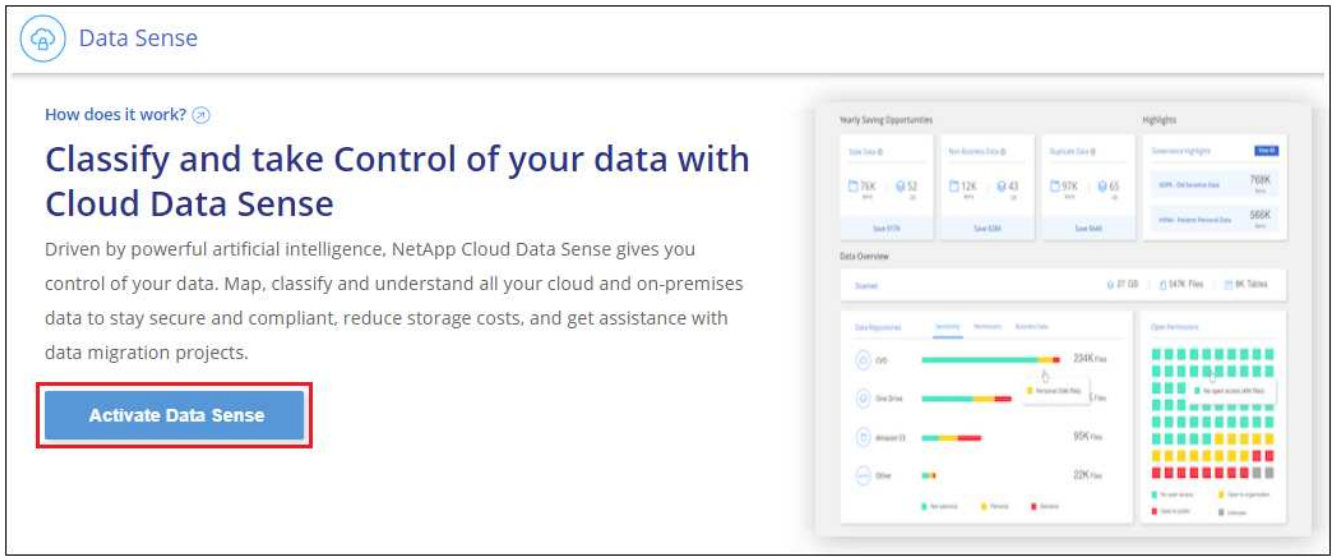
Pasos

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

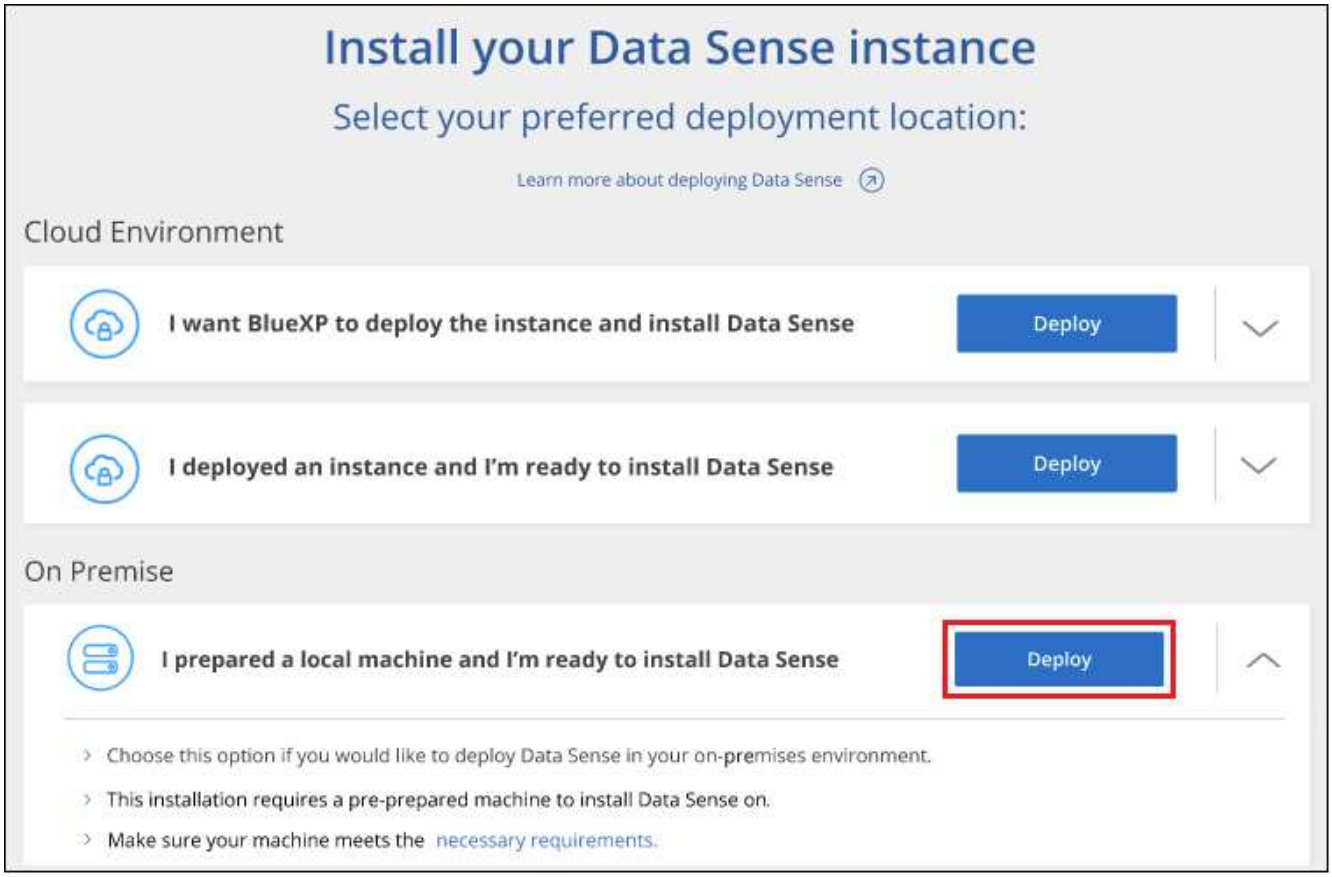
```
tar -xzf DataSense-offline-bundle-v1.21.0.tar.gz
```

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

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



6. Haga clic en **desplegar** para iniciar el asistente de implementación en las instalaciones.



7. Aparece el cuadro de diálogo *Deploy Data Sense on local*. Copie el comando proporcionado y péguelo en un archivo de texto para poder usarlo más tarde y haga clic en **Cerrar**. Por ejemplo:

   ```
   sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite
   ```

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

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

9. Cuando el instalador lo solicite, puede introducir los valores necesarios en una serie de mensajes o puede proporcionar los parámetros necesarios como argumentos de línea de comandos al instalador:

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

Introduzca los parámetros según se le solicite:	Introduzca el comando Full:
a. Pegue la información que ha copiado del paso 7: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --darksite` b. Introduzca la dirección IP o el nombre de host del equipo host de Data Sense para que pueda accederse a él mediante la instancia de Connector. c. Introduzca la dirección IP o el nombre de host de la máquina host de BlueXP Connector para que pueda accederse a ella mediante la instancia de detección de datos.	También puede crear el comando completo por adelantado, proporcionando los parámetros de host necesarios: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

Valores de variable:

- *account_id* = ID de cuenta de NetApp
- *Agent_id* = ID del conector
- *token* = token de usuario jwt
- *DS_host* = dirección IP o nombre de host del sistema Data Sense Linux.
- *Cm_host* = dirección IP o nombre de host del sistema BlueXP Connector.

Resultado

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

Si hay conectividad sobre el puerto 8080 entre el equipo host y la instancia de conector, verá el progreso de instalación en la ficha detección de datos de BlueXP.

El futuro

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

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

Instalación de varios hosts para configuraciones grandes

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

Siga estos pasos cuando instale software Data Sense en varios hosts locales en un entorno sin conexión.

Lo que necesitará

- Verifique que todos los sistemas Linux para los nodos Manager y Scanner se adapten al requisitos del host.
- Compruebe que ha instalado los dos paquetes de software de requisitos previos (Docker Engine y Python

3).

- Asegúrese de tener privilegios de usuario raíz en los sistemas Linux.
- Compruebe que su entorno sin conexión cumple con las necesidades permisos y conectividad.
- Debe tener las direcciones IP de los hosts de nodos de escáner que desee utilizar.
- Deben habilitarse los siguientes puertos y protocolos en todos los hosts:

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

Pasos

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

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

   Por ejemplo, este comando añade 3 nodos de escáner:
   ```
   sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
   --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy
   --darksite
   ```

3. Antes de que se complete la instalación del nodo de gestión, se mostrará un cuadro de diálogo con el comando de instalación necesario para los nodos del escáner. Copie el comando y guárdelo en un archivo de texto. Por ejemplo:

   ```
   sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
   ```

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

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

Resultado

El instalador de Cloud Data Sense finaliza la instalación de los paquetes y registra la instalación. La instalación puede tardar entre 15 y 25 minutos.

El futuro

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

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

Actualice el software de detección de datos

Dado que el software Data Sense se actualiza regularmente con las nuevas funciones, debe entrar en una rutina para comprobar si hay nuevas versiones periódicamente para asegurarse de que está utilizando el software y las funciones más recientes. Deberá actualizar el software Data Sense manualmente porque no hay conectividad a Internet para realizar la actualización automáticamente.

Antes de empezar

- El software de detección de datos puede actualizarse una versión principal cada vez. Por ejemplo, si tiene instalada la versión 1.18.x, sólo podrá actualizar a 1.19.x. Si tiene varias versiones principales detrás, tendrá que actualizar el software varias veces.
- Compruebe que el software del conector en las instalaciones se ha actualizado a la versión más reciente disponible. "Consulte los pasos de actualización del conector".

Pasos

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

   ```
   tar -xvf DataSense-offline-bundle-v1.21.0.tar.gz
   ```

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

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

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

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

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

   ```
   start_darksite_upgrade.sh
   ```

Resultado

El software Data Sense se actualiza en el host. La actualización puede tardar entre 5 y 10 minutos.

Tenga en cuenta que no es necesaria ninguna actualización en los nodos de escáner si ha implementado Data Sense en varios sistemas host para analizar configuraciones muy grandes.

Puede verificar que el software se ha actualizado comprobando la versión en la parte inferior de las páginas de la interfaz de usuario de detección de datos.

Active el análisis en sus orígenes de datos

Introducción a Cloud Data Sense para Cloud Volumes ONTAP y ONTAP en las instalaciones

Complete algunos pasos para empezar a analizar sus volúmenes de Cloud Volumes ONTAP y ONTAP en las instalaciones con Cloud Data Sense.

Inicio rápido

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

Descubra los orígenes de datos que desea analizar

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

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

Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

Habilite Cloud Data Sense y seleccione los volúmenes que desea analizar

Haga clic en **detección de datos**, seleccione la ficha **Configuración** y active las exploraciones de cumplimiento para volúmenes en entornos de trabajo específicos.

Garantice el acceso a los volúmenes

Ahora que Cloud Data Sense está habilitado, asegúrese de que pueda acceder a todos los volúmenes.

- La instancia de Cloud Data Sense necesita una conexión de red a cada subred de Cloud Volumes ONTAP o sistema ONTAP en las instalaciones.
- Los grupos de seguridad para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de detección de datos.
- Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense:
  - Para NFS: Puertos 111 y 2049.
  - Para CIFS: Puertos 139 y 445.

- Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.
- La detección de datos necesita credenciales de Active Directory para analizar volúmenes CIFS.

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

5 Gestione los volúmenes que desea analizar

Seleccione o anule la selección de los volúmenes que desea analizar y Cloud Data Sense iniciará o dejará de analizarlos.

Detección de los orígenes de datos que desea analizar

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

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

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

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

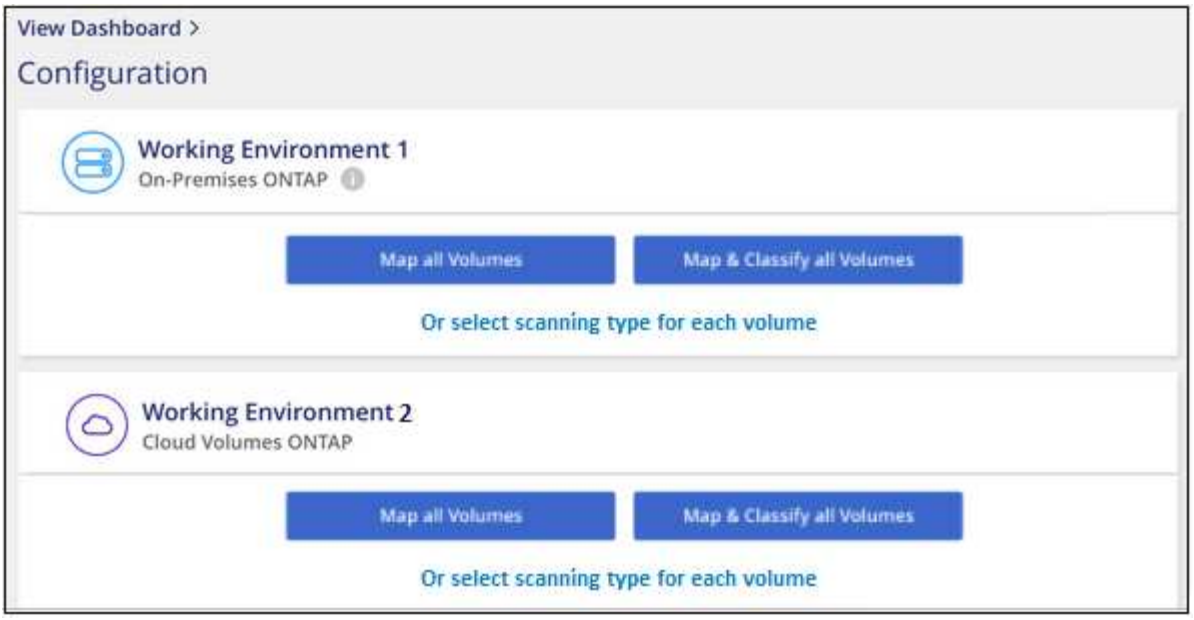
Si está escaneando en las instalaciones sistemas ONTAP que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Implemente Cloud Data Sense en la misma ubicación en las instalaciones que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar el sentido de los datos en el cloud en sus entornos de trabajo

Puede habilitar la detección de datos en el cloud en sistemas Cloud Volumes ONTAP de cualquier proveedor de cloud compatible y en clústeres de ONTAP en las instalaciones.

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



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

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

3. En el cuadro de diálogo de confirmación, haga clic en **aprobar** para que Data SENSE empiece a analizar los volúmenes.

Resultado

Cloud Data Sense comienza a analizar los volúmenes seleccionados en el entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento tan pronto como Cloud Data Sense termine los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

De forma predeterminada, si Data sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos de los volúmenes, ya que el detección de datos no puede revertir la "última hora de acceso" a la Marca de hora original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. Esa página tiene un valor que se puede habilitar para que Data Sense analice los volúmenes sin tener en cuenta los permisos.

Comprobar que Cloud Data Sense tiene acceso a volúmenes

Asegúrese de que Cloud Data Sense pueda acceder a los volúmenes mediante la comprobación de la red, los grupos de seguridad y las políticas de exportación. Deberá proporcionar la detección de datos con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que hay una conexión de red entre la instancia de Cloud Data Sense y cada red que incluye

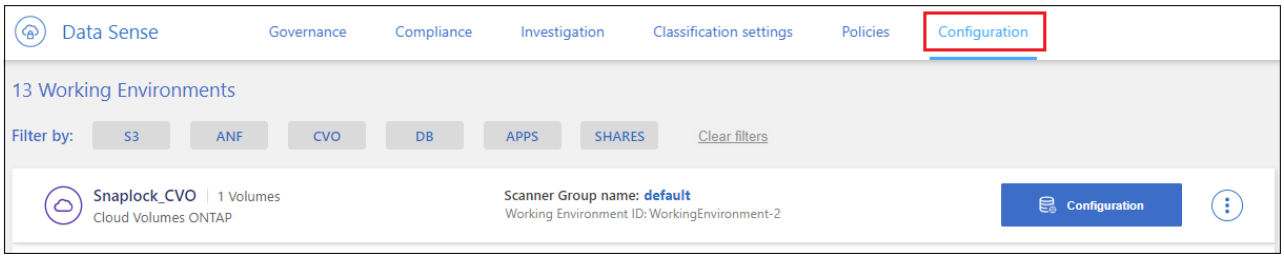
volúmenes para clústeres Cloud Volumes ONTAP o ONTAP en las instalaciones.

2. Asegúrese de que el grupo de seguridad para Cloud Volumes ONTAP permite el tráfico entrante desde la instancia de detección de datos.

   Puede abrir el grupo de seguridad para el tráfico desde la dirección IP de la instancia de Data Sense, o bien puede abrir el grupo de seguridad para todo el tráfico desde dentro de la red virtual.

3. Asegúrese de que los siguientes puertos están abiertos a la instancia de Data Sense:
   - Para NFS: Puertos 111 y 2049.
   - Para CIFS: Puertos 139 y 445.
4. Compruebe que las políticas de exportación de volúmenes NFS incluyan la dirección IP de la instancia de Data Sense para poder acceder a los datos de cada volumen.
5. Si utiliza CIFS, proporcione detección de datos con credenciales de Active Directory para poder analizar volúmenes CIFS.

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

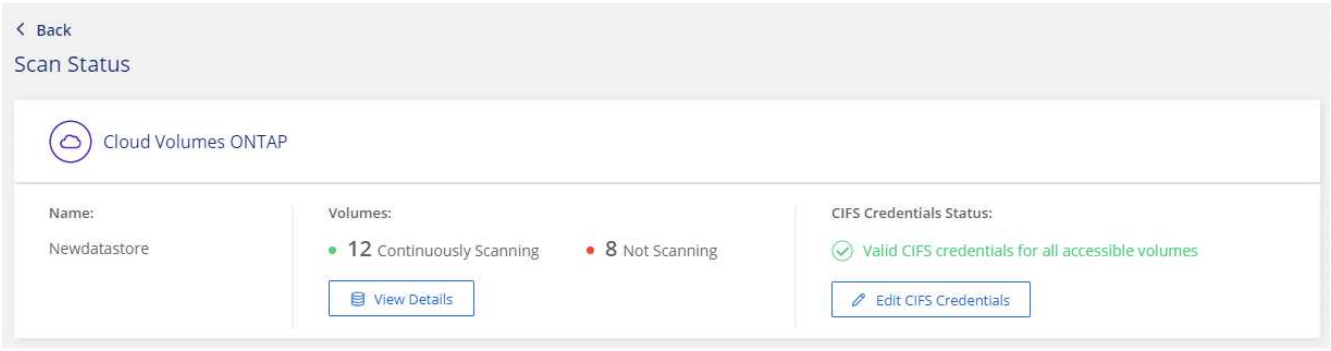


   b. Para cada entorno de trabajo, haga clic en **Editar credenciales CIFS** e introduzca el nombre de usuario y la contraseña que necesita Data Sense para acceder a los volúmenes CIFS en el sistema.

      Las credenciales pueden ser de sólo lectura, pero si se proporcionan credenciales de administrador, se garantiza que Data Sense pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de Cloud Data Sense.

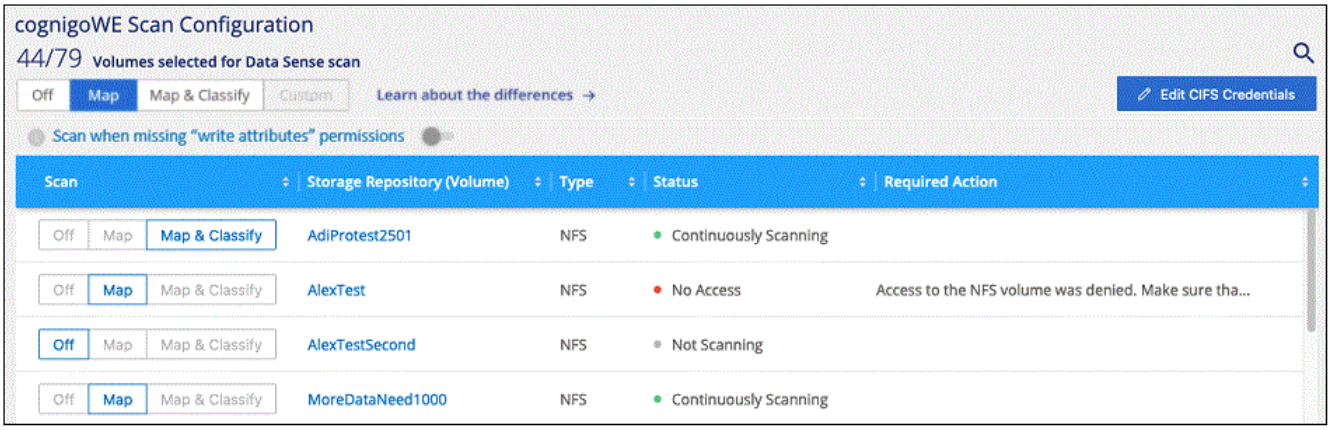
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

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



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

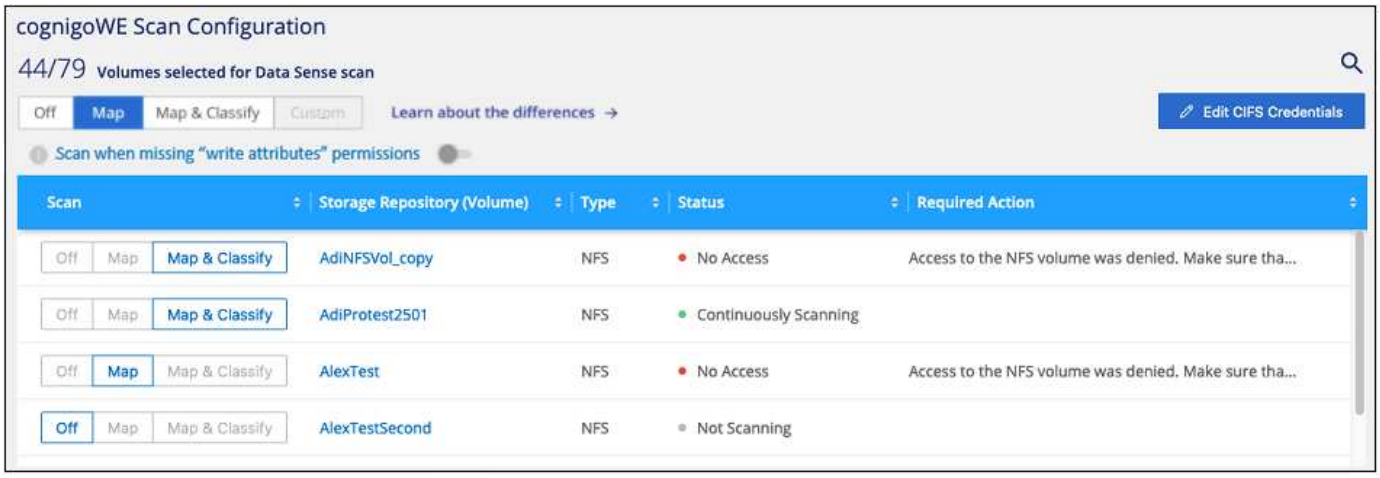
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes; uno de los cuales no puede analizar Cloud Data Sense debido a problemas de conectividad de red entre la instancia de detección de datos y el volumen.



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

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

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que si Data Sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos porque el sentido de datos no puede revertir la Marca de hora original a la "hora del último acceso". Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



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

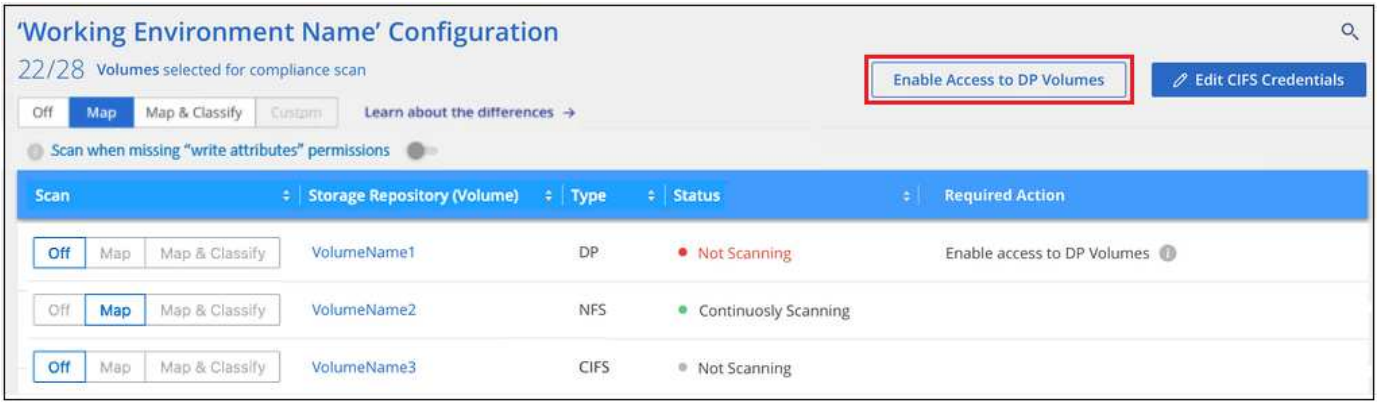
Para:	Haga lo siguiente:
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**
Active análisis de sólo asignación en todos los volúmenes	En el área de encabezado, haga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

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

Análisis de volúmenes de protección de datos

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

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

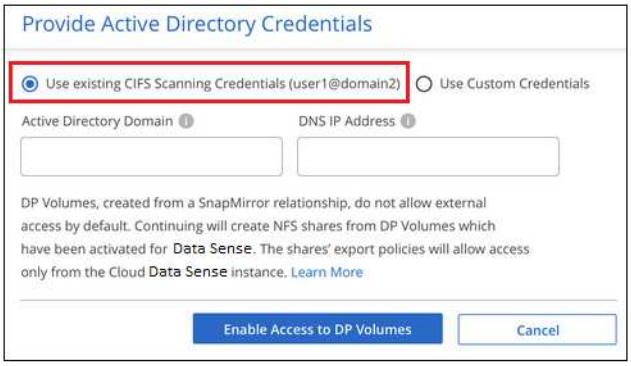


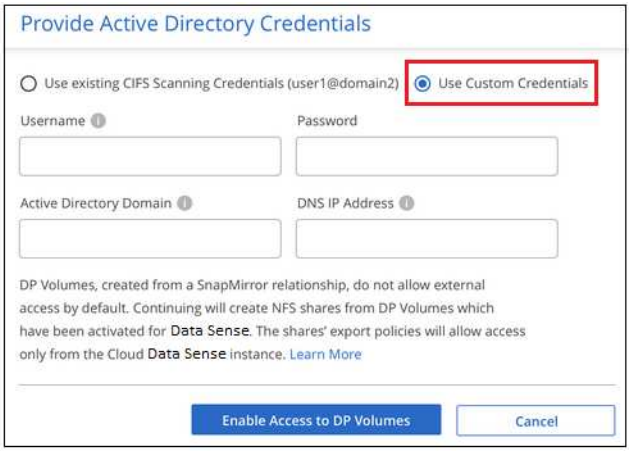
Pasos

Si desea analizar estos volúmenes de protección de datos:

1. Haga clic en **Activar acceso a volúmenes DP** en la parte superior de la página.
2. Revise el mensaje de confirmación y vuelva a hacer clic en **Activar acceso a volúmenes DP**.
   - Se habilitan los volúmenes que se crearon inicialmente como volúmenes NFS en el sistema ONTAP de origen.
   - Los volúmenes que se crearon inicialmente como volúmenes CIFS en el sistema ONTAP de origen requieren la introducción de credenciales CIFS para analizar dichos volúmenes DP. Si ya introdujo credenciales de Active Directory para que Cloud Data Sense pueda analizar volúmenes de CIFS,

puede usar esas credenciales o puede especificar un conjunto diferente de credenciales de administrador.





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

Resultado

Una vez habilitado, Cloud Data Sense crea un recurso compartido de NFS de cada volumen DP que se ha activado para el análisis. Las políticas de exportación de recursos compartidos solo permiten el acceso desde la instancia de detección de datos.

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

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

Introducción a Cloud Data Sense para Azure NetApp Files

Complete unos pasos para empezar a usar Cloud Data Sense para Azure NetApp Files.

Inicio rápido

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

Descubra los sistemas Azure NetApp Files que desea analizar

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

Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense en BlueXP" si aún no hay una instancia implementada.

3 Habilite Cloud Data Sense y seleccione los volúmenes que desea analizar

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

4 Garantice el acceso a los volúmenes

Ahora que Cloud Data Sense está habilitado, asegúrese de que pueda acceder a todos los volúmenes.

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

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

5 Gestione los volúmenes que desea analizar

Seleccione o anule la selección de los volúmenes que desea analizar y Cloud Data Sense iniciará o dejará de analizarlos.

Detección del sistema Azure NetApp Files que desea analizar

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

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

Implementar la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

El sentido de los datos se debe implementar en el cloud al analizar volúmenes de Azure NetApp Files y debe ponerse en marcha en la misma región que los volúmenes que desea analizar.

Nota: actualmente no se admite la implementación de la detección de datos en la nube en una ubicación local al analizar volúmenes Azure NetApp Files.

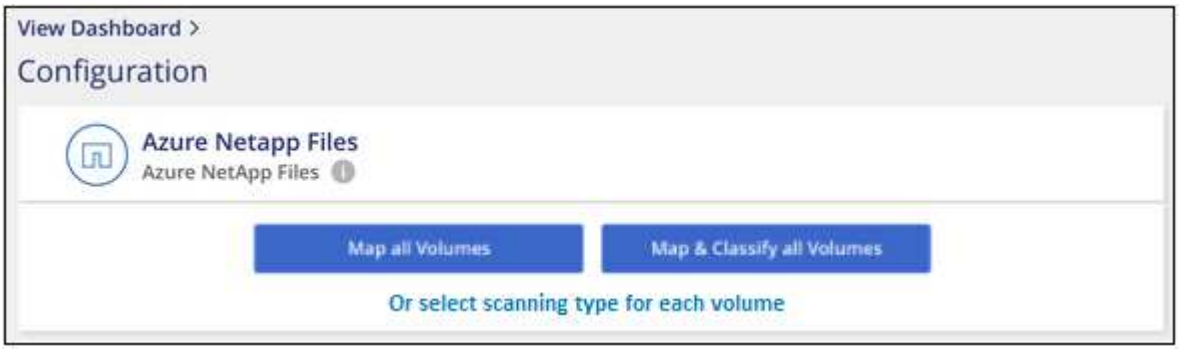
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar el sentido de los datos en el cloud en sus entornos de trabajo

Puede habilitar la detección de datos en el cloud en Azure NetApp Files Volumes.

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

ficha **Configuración**.



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

     Consulte Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes para obtener más detalles.
3. En el cuadro de diálogo de confirmación, haga clic en **aprobar** para que Data SENSE empiece a analizar los volúmenes.

Resultado

Cloud Data Sense comienza a analizar los volúmenes seleccionados en el entorno de trabajo. Los resultados estarán disponibles en el panel de cumplimiento tan pronto como Data Sense termine las exploraciones iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

De forma predeterminada, si Data sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos de los volúmenes, ya que el detección de datos no puede revertir la "última hora de acceso" a la Marca de hora original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. Esa página tiene un valor que se puede habilitar para que Data Sense analice los volúmenes sin tener en cuenta los permisos.

Comprobar que Cloud Data Sense tiene acceso a volúmenes

Asegúrese de que Cloud Data Sense pueda acceder a los volúmenes mediante la comprobación de la red, los grupos de seguridad y las políticas de exportación. Deberá proporcionar la detección de datos con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que haya una conexión de red entre la instancia de Cloud Data Sense y cada red que incluya los volúmenes para Azure NetApp Files.

   Para Azure NetApp Files, Cloud Data Sense solo puede analizar volúmenes que se encuentran en la misma región que BlueXP.

2. Asegúrese de que los siguientes puertos están abiertos a la instancia de Data Sense:
   - Para NFS, puertos 111 y 2049.
   - Para CIFS, puertos 139 y 445.
3. Compruebe que las políticas de exportación de volúmenes NFS incluyan la dirección IP de la instancia de Data Sense para poder acceder a los datos de cada volumen.
4. Si utiliza CIFS, proporcione detección de datos con credenciales de Active Directory para poder analizar volúmenes CIFS.

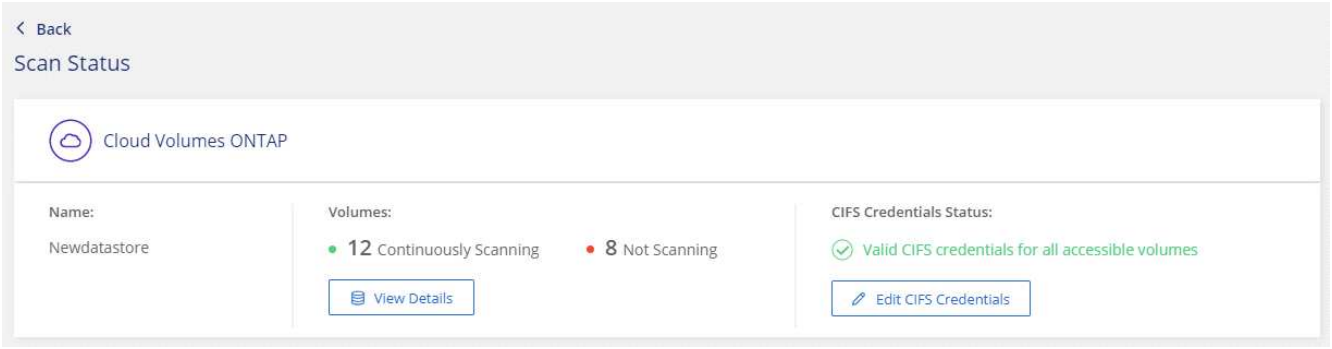
   a. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.

   b. Para cada entorno de trabajo, haga clic en **Editar credenciales CIFS** e introduzca el nombre de usuario y la contraseña que necesita Data Sense para acceder a los volúmenes CIFS en el sistema.

      Las credenciales pueden ser de sólo lectura, pero si se proporcionan credenciales de administrador, se garantiza que Data Sense pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de Cloud Data Sense.

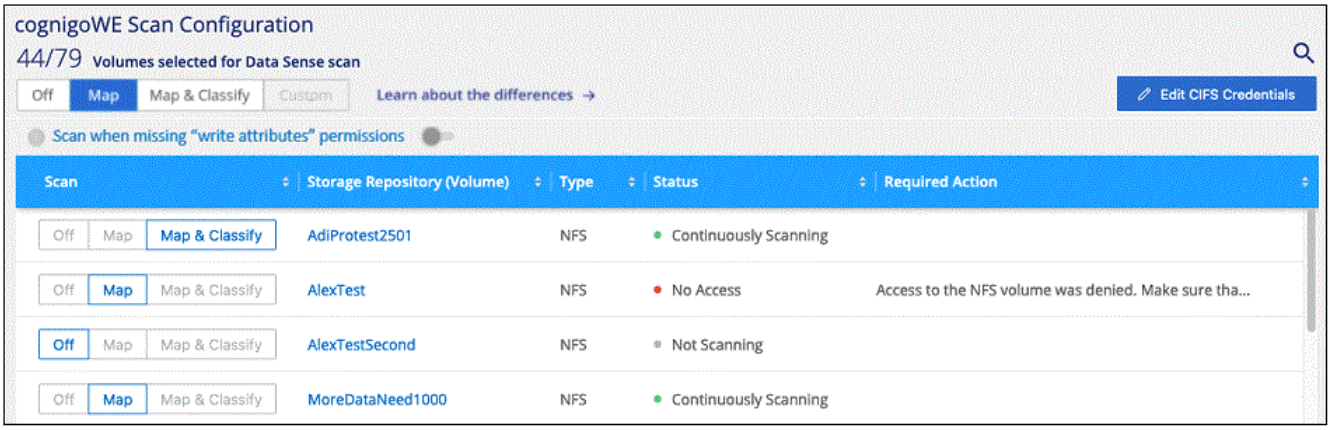
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

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



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

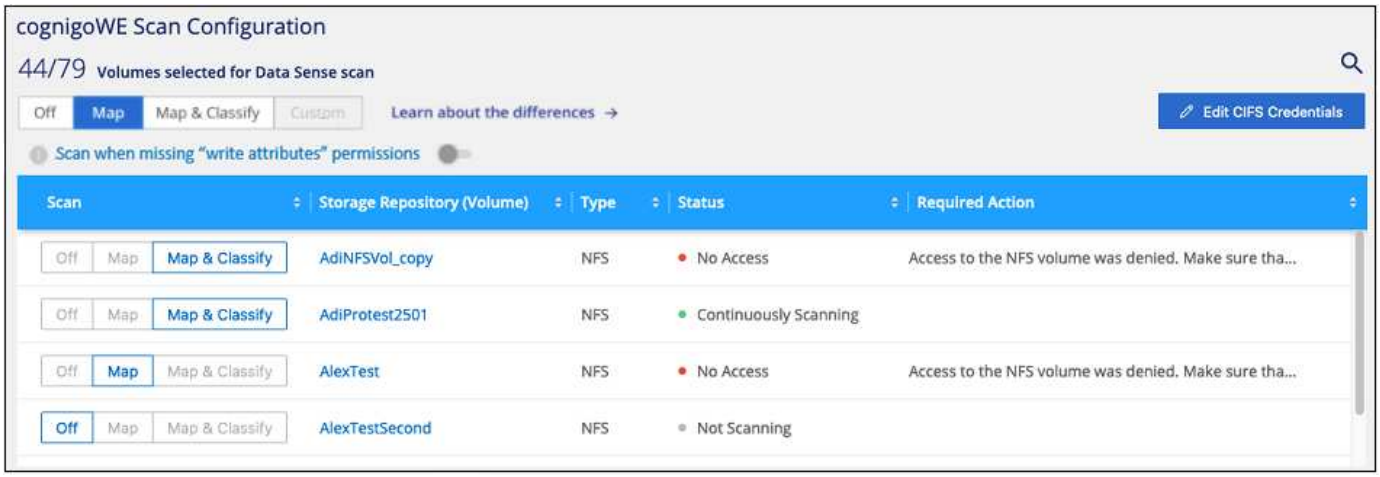
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes; uno de los cuales no puede analizar Cloud Data Sense debido a problemas de conectividad de red entre la instancia de detección de datos y el volumen.



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

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

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que si Data Sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos porque el sentido de datos no puede revertir la Marca de hora original a la "hora del último acceso". Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



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

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

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

Comience a utilizar Cloud Data Sense para Amazon FSX para ONTAP

Complete unos pasos para comenzar a analizar el volumen de Amazon FSX para ONTAP con Cloud Data Sense.

Antes de empezar

- Necesita un conector activo en AWS para implementar y gestionar Data Sense.
- El grupo de seguridad seleccionado al crear el entorno de trabajo debe permitir el tráfico desde la instancia de Cloud Data Sense. Puede buscar el grupo de seguridad asociado mediante ENI conectado al FSX para el sistema de archivos ONTAP y editarlo mediante la consola de gestión de AWS.

  "Grupos de seguridad de AWS para instancias de Linux"

  "Grupos de seguridad de AWS para instancias de Windows"

  "Interfaces de red elásticas de AWS (ENI)"

Inicio rápido

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

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

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

2 Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense en BlueXP" si aún no hay una instancia implementada.

3 Habilite Cloud Data Sense y seleccione los volúmenes que desea analizar

Haga clic en **detección de datos**, seleccione la ficha **Configuración** y active las exploraciones de cumplimiento para volúmenes en entornos de trabajo específicos.

4 Garantice el acceso a los volúmenes

Ahora que Cloud Data Sense está habilitado, asegúrese de que pueda acceder a todos los volúmenes.

- La instancia de Cloud Data Sense necesita una conexión de red a cada subred FSX para ONTAP.
- Asegúrese de que los siguientes puertos están abiertos a la instancia de Data Sense:
  - Para NFS, puertos 111 y 2049.
  - Para CIFS, puertos 139 y 445.
- Las políticas de exportación de volúmenes NFS deben permitir el acceso desde la instancia de Data Sense.
- La detección de datos necesita credenciales de Active Directory para analizar volúmenes CIFS. + haga clic en **cumplimiento** > **Configuración** > **Editar credenciales CIFS** y proporcione las credenciales.

5 Gestione los volúmenes que desea analizar

Seleccione o anule la selección de los volúmenes que desea analizar y Cloud Data Sense iniciará o dejará de analizarlos.

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

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

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

Implementar la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

Debe implementar el sentido de datos en la misma red de AWS que Connector for AWS y los volúmenes FSX que desea analizar.

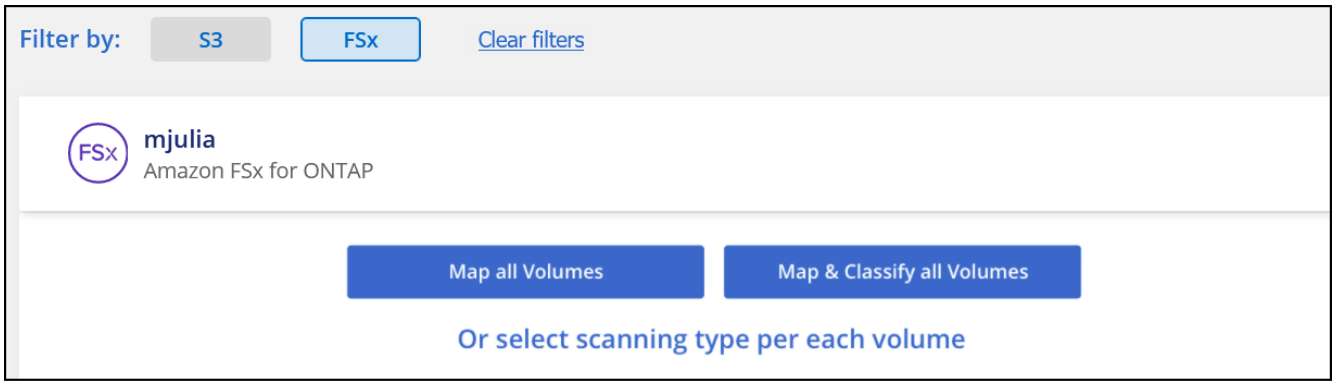
Nota: actualmente no se admite la implementación de Cloud Data Sense en una ubicación en las instalaciones al analizar volúmenes FSX.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Habilitar el sentido de los datos en el cloud en sus entornos de trabajo

Puede habilitar Cloud Data Sense para FSX para volúmenes de ONTAP.

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



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

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

3. En el cuadro de diálogo de confirmación, haga clic en **aprobar** para que Data SENSE empiece a analizar los volúmenes.

Resultado

Cloud Data Sense comienza a analizar los volúmenes seleccionados en el entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento tan pronto como Cloud Data Sense termine los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

> De forma predeterminada, si Data sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos de los volúmenes, ya que el detección de datos no puede revertir la "última hora de acceso" a la Marca de hora original. Si no le importa si se restablece la última hora de acceso, haga clic en **o seleccione el tipo de exploración para cada volumen**. Esa página tiene un valor que se puede habilitar para que Data Sense analice los volúmenes sin tener en cuenta los permisos.

Comprobar que Cloud Data Sense tiene acceso a volúmenes

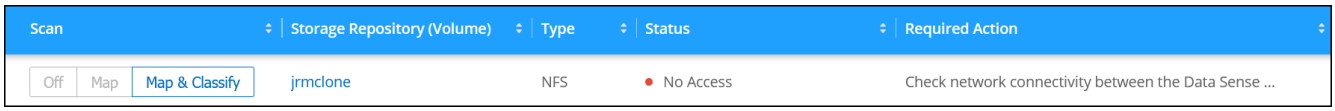
Asegúrese de que Cloud Data Sense pueda acceder a los volúmenes mediante la comprobación de las redes, los grupos de seguridad y las políticas de exportación.

Deberá proporcionar la detección de datos con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

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

   Por ejemplo, la siguiente imagen muestra que un volumen Cloud Data Sense no puede analizar debido a problemas de conectividad de red entre la instancia de detección de datos y el volumen.



2. Asegúrese de que hay una conexión de red entre la instancia de Cloud Data Sense y cada red que incluya volúmenes para FSX para ONTAP.

   Para FSX para ONTAP, Cloud Data Sense puede analizar volúmenes sólo en la misma región que BlueXP.

3. Asegúrese de que los siguientes puertos están abiertos a la instancia de detección de datos.
   - Para NFS, puertos 111 y 2049.
   - Para CIFS, puertos 139 y 445.
4. Compruebe que las políticas de exportación de volúmenes NFS incluyan la dirección IP de la instancia de Data Sense para poder acceder a los datos de cada volumen.
5. Si utiliza CIFS, proporcione detección de datos con credenciales de Active Directory para poder analizar volúmenes CIFS.

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

   b. Para cada entorno de trabajo, haga clic en **Editar credenciales CIFS** e introduzca el nombre de usuario y la contraseña que necesita Data Sense para acceder a los volúmenes CIFS en el sistema.

      Las credenciales pueden ser de sólo lectura, pero si se proporcionan credenciales de administrador, se garantiza que Data Sense pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de Cloud Data Sense.

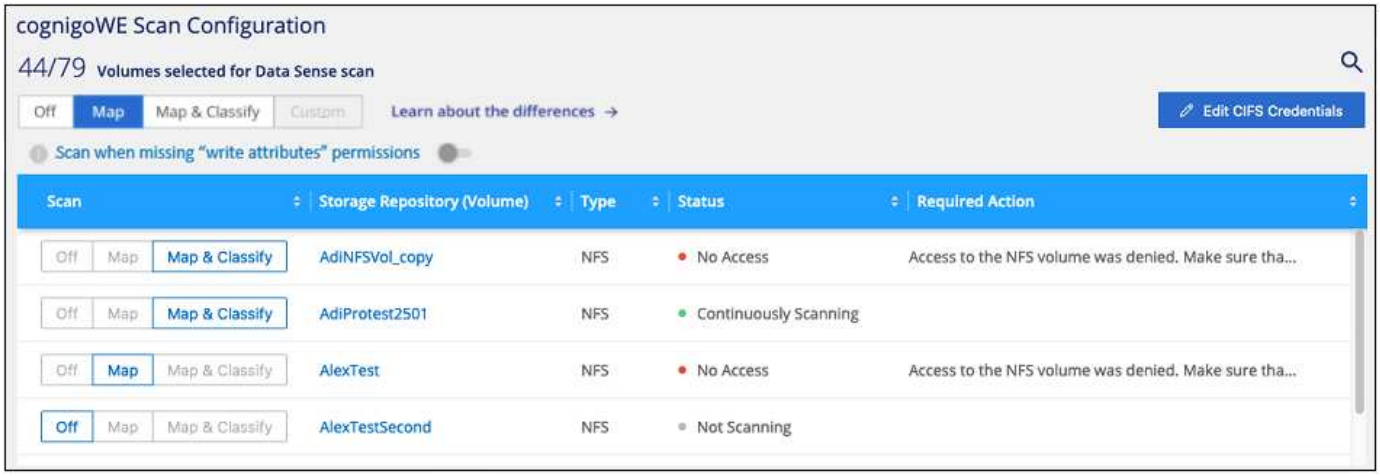
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

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

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

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

El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que si Data Sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos porque el sentido de datos no puede revertir la Marca de hora original a la "hora del último acceso". Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".



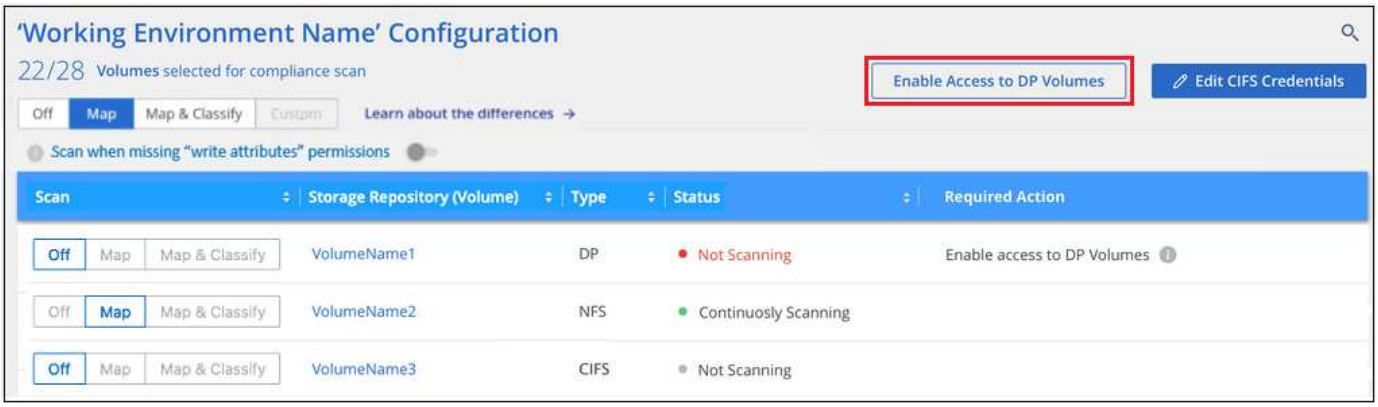
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en un volumen	En el área de volumen, haga clic en **Mapa**
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**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

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

Análisis de volúmenes de protección de datos

De manera predeterminada, los volúmenes de protección de datos (DP) no se analizan porque no se exponen externamente y en Cloud Data Sense no pueden acceder a ellos. Estos son los volúmenes de destino de las operaciones de SnapMirror desde un FSX para el sistema de archivos ONTAP.

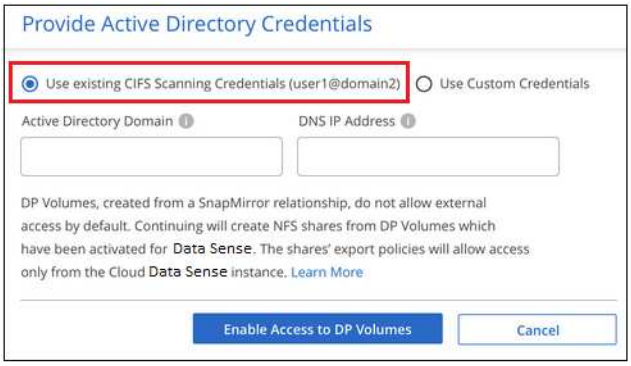
Inicialmente, la lista de volúmenes identifica estos volúmenes como *Type* **DP** con el *Status* **no Scanning** y el *Required Action* **Enable Access to DP Volumes**.

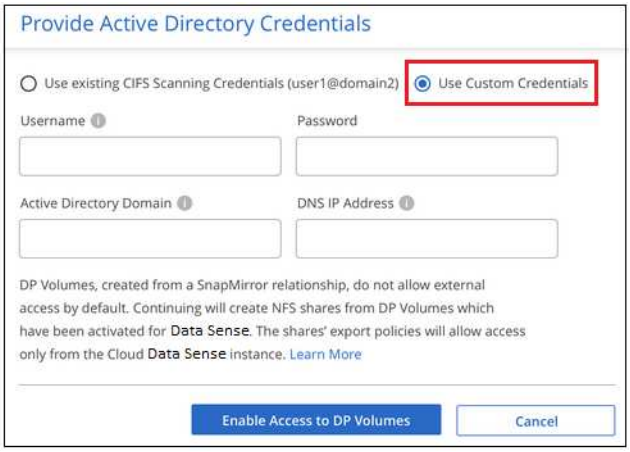


Pasos

Si desea analizar estos volúmenes de protección de datos:

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





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

Resultado

Una vez habilitado, Cloud Data Sense crea un recurso compartido de NFS de cada volumen DP que se ha activado para el análisis. Las políticas de exportación de recursos compartidos solo permiten el acceso desde la instancia de detección de datos.

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

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

Introducción a Cloud Data Sense para Amazon S3

Cloud Data Sense puede analizar sus buckets de Amazon S3 para identificar los datos personales y confidenciales que se encuentran en el almacenamiento de objetos S3. Cloud Data Sense puede analizar cualquier bloque de la cuenta, independientemente de si se ha creado para una solución de NetApp.

Inicio rápido

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

1 Configure los requisitos de S3 en su entorno de cloud

Asegúrese de que su entorno cloud pueda satisfacer los requisitos del Cloud Data Sense, incluida la preparación de un rol IAM y la configuración de la conectividad de Data Sense a S3. Vea la lista completa.

2 Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

3 Active Data Sense en su entorno de trabajo de S3

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

4 Seleccione los cucharones que desea escanear

Seleccione los cubos que desea analizar y Cloud Data Sense empezará a escanear.

Revisión de los requisitos previos de S3

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

Configure una función IAM para la instancia de Cloud Data Sense

Cloud Data Sense necesita permisos para conectarse a los bloques de S3 de su cuenta y para analizarlos. Configure un rol de IAM que incluya los permisos que se indican a continuación. BlueXP le solicita que seleccione una función de IAM al habilitar la detección de datos en el entorno de trabajo de Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Proporcione conectividad desde Cloud Data Sense a Amazon S3

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

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

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

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

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

Implementar la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense en BlueXP" si aún no hay una instancia implementada.

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

Nota: actualmente no se admite la implantación de Cloud Data Sense en una ubicación en las instalaciones al escanear cubos S3.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

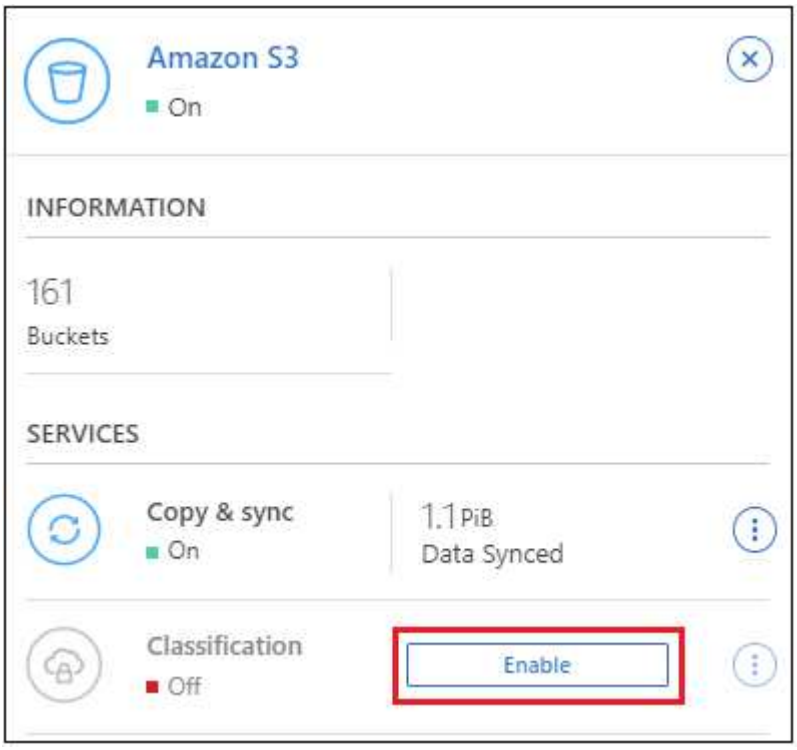
Activar el sentido de datos en su entorno de trabajo de S3

Habilite Cloud Data Sense en Amazon S3 después de verificar los requisitos previos.

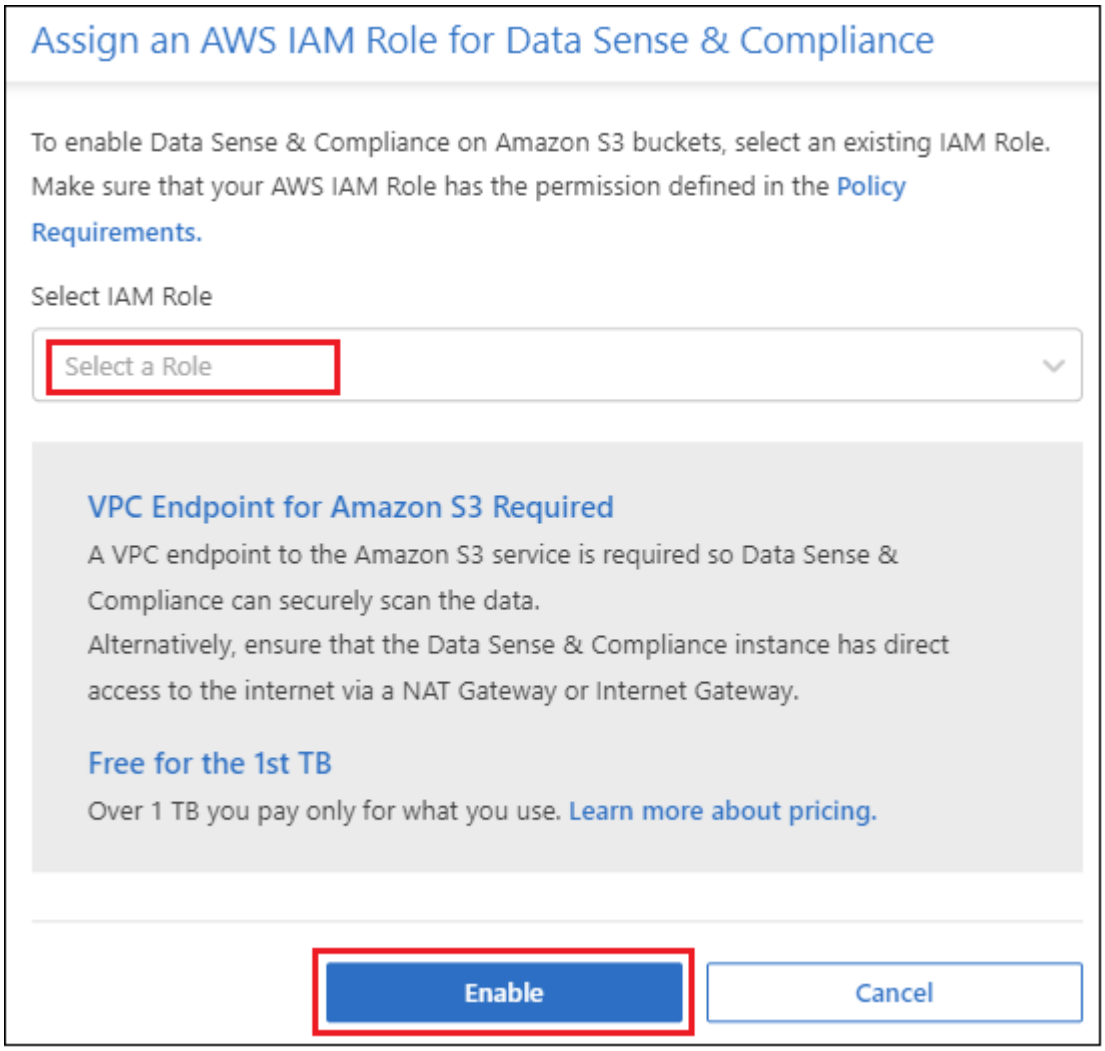
Pasos

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

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



4. Cuando se le solicite, asigne una función IAM a la instancia de detección de datos en la nube que tiene los permisos necesarios.



5. Haga clic en **Activar**.

También puede habilitar análisis de cumplimiento de un entorno de trabajo desde la página Configuración haciendo clic en Y seleccione **Activar detección de datos**.

Resultado

BlueXP asigna la función IAM a la instancia.

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

Después de que BlueXP habilita Cloud Data Sense en Amazon S3, el paso siguiente es configurar los bloques que desea analizar.

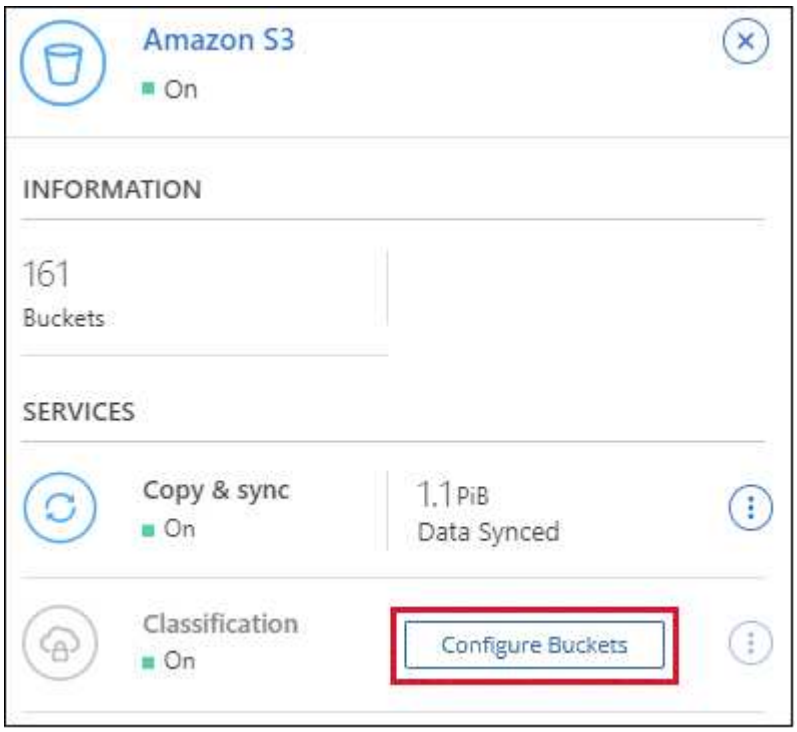
Cuando BlueXP se ejecuta en la cuenta de AWS que tiene los bloques de S3 que desea analizar, detecta esos bloques y los muestra en un entorno de trabajo de Amazon S3.

El sentido de los datos en cloud también puede ser Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS.

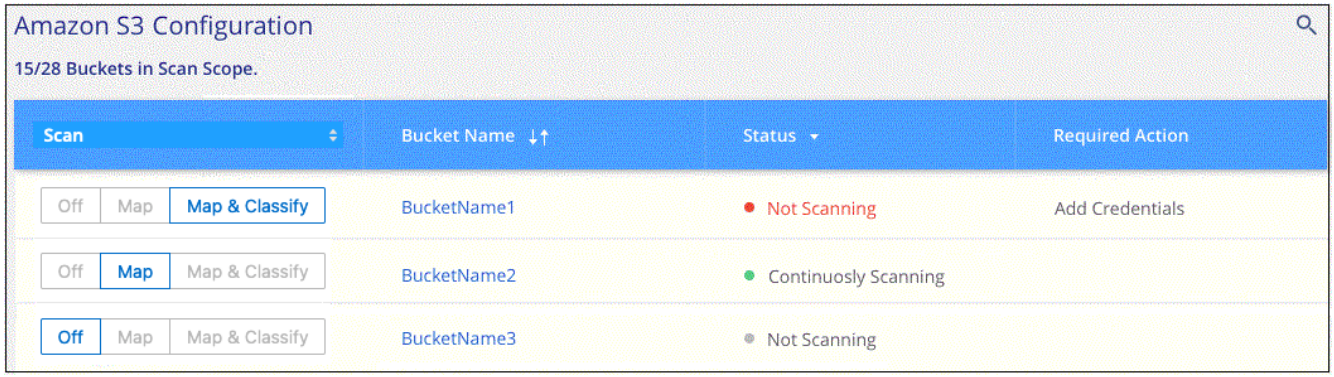
Pasos

1. Seleccione el entorno de trabajo de Amazon S3.

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



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



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

Resultado

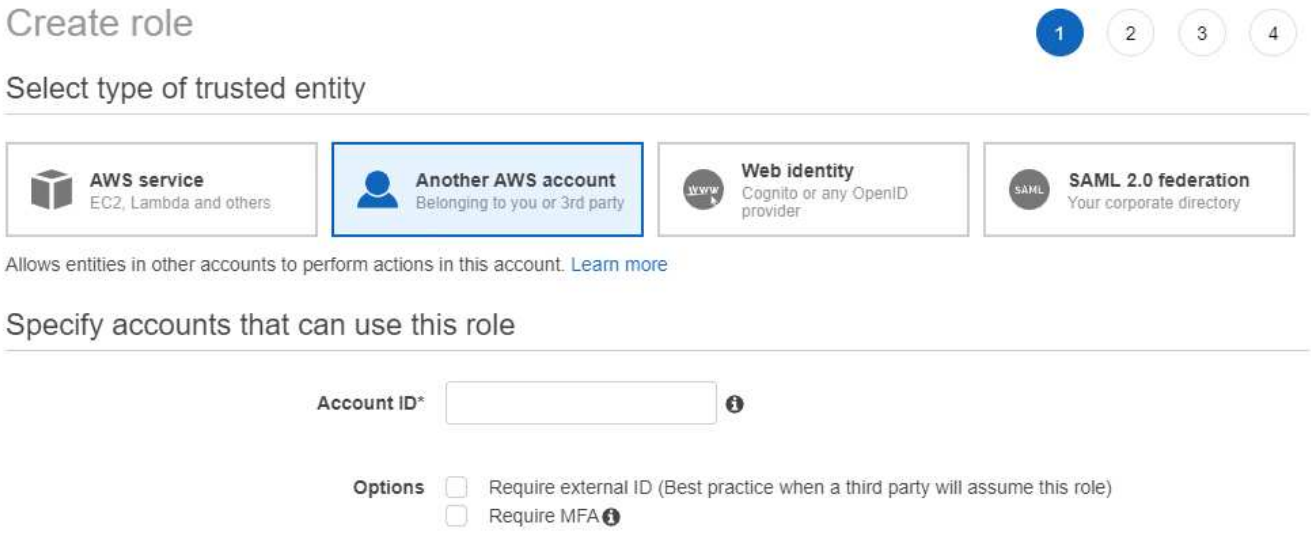
Cloud Data Sense comienza a analizar los cubos de S3 que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Escaneando bloques de cuentas de AWS adicionales

Puede analizar bloques de S3 que se encuentran en una cuenta de AWS diferente asignando un rol de esa cuenta para acceder a la instancia existente de Cloud Data Sense.

Pasos

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



   No olvide hacer lo siguiente:

   - Introduzca el ID de la cuenta en la que reside la instancia de Cloud Data Sense.
   - Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
   - Adjunte la política de detección de datos en el cloud IAM. Asegúrese de que tiene los permisos necesarios.

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

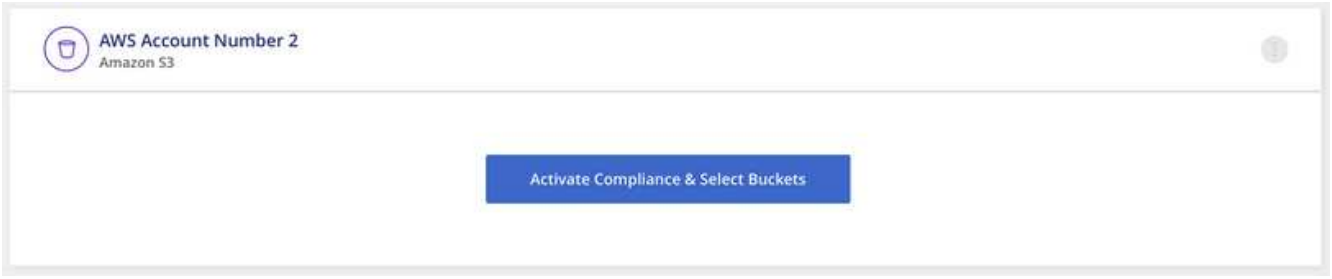
2. Vaya a la cuenta AWS de origen donde se encuentra la instancia de detección de datos y seleccione la función IAM asociada a la instancia.
   a. Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
   b. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.

c. Cree una directiva que incluya la acción "sts:AssumeRole" y especifique el ARN del rol que creó en la cuenta de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

La cuenta del perfil de instancia de Cloud Data Sense tiene ahora acceso a la cuenta adicional de AWS.

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



4. Haga clic en **Activar detección de datos y Seleccionar cucharones** y seleccione los cucharones que desea escanear.

Resultado

Cloud Data Sense comienza a analizar los nuevos bloques de S3 que ha habilitado.

Analizando esquemas de base de datos

Realice algunos pasos para empezar a analizar sus esquemas de base de datos con Cloud Data Sense.

Inicio rápido

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

Revisar los requisitos previos de la base de datos

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

Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

Agregue el servidor de la base de datos

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

Seleccione los esquemas

Seleccione los esquemas que desea analizar.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Data Sense.

Bases de datos compatibles

Cloud Data Sense es capaz de analizar esquemas de las siguientes bases de datos:

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

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

Requisitos de base de datos

Es posible analizar cualquier base de datos con conectividad a la instancia de Cloud Data Sense, independientemente de dónde esté alojada. Sólo necesita la siguiente información para conectarse a la base de datos:

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

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

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

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

Si está analizando esquemas de base de datos a los que se puede acceder a través de Internet, puede hacerlo "Ponga en marcha Cloud Data en el cloud" o. "Implemente el software de detección de datos en una ubicación local con acceso a Internet".

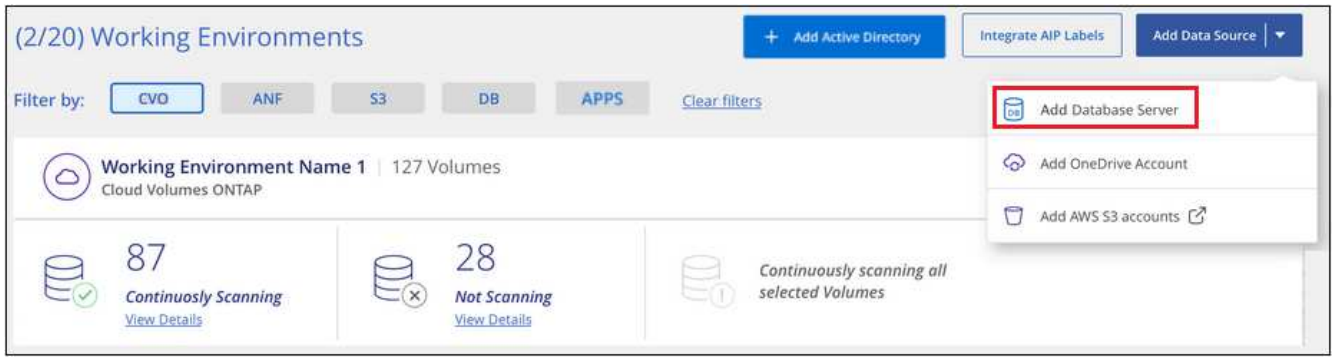
Si está analizando esquemas de base de datos que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Implemente Cloud Data Sense en la misma ubicación en las instalaciones que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Agregando el servidor de la base de datos

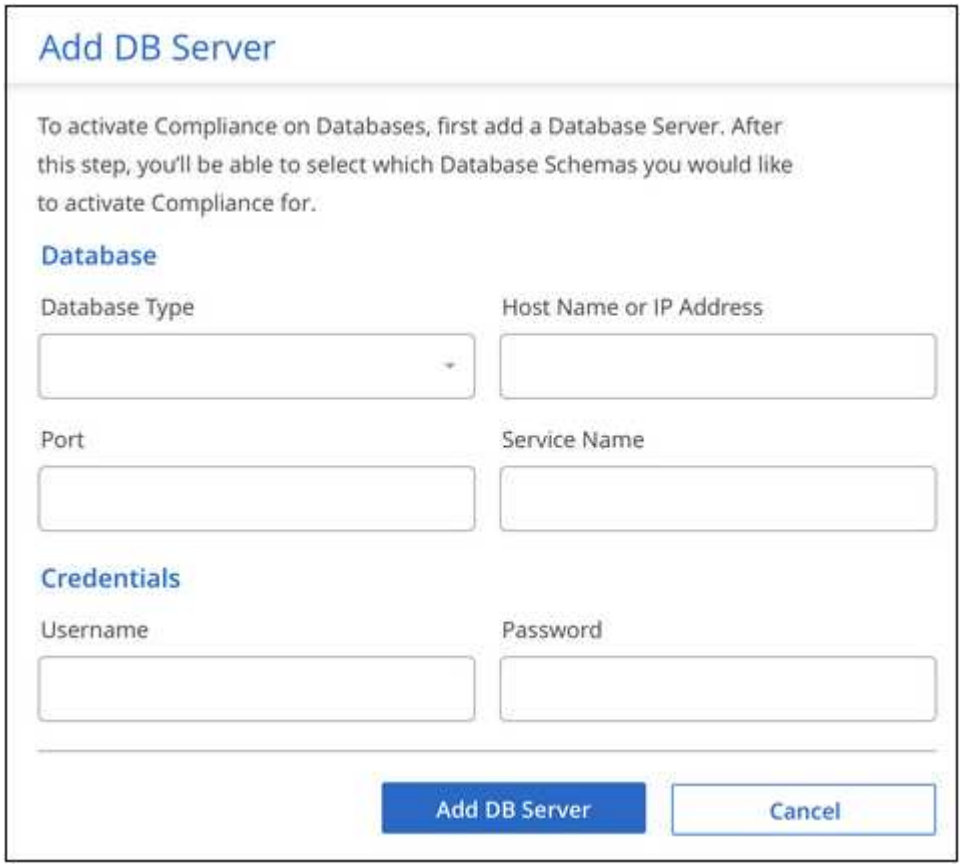
Agregue el servidor de base de datos donde residen los esquemas.

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



2. Introduzca la información necesaria para identificar el servidor de bases de datos.

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



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

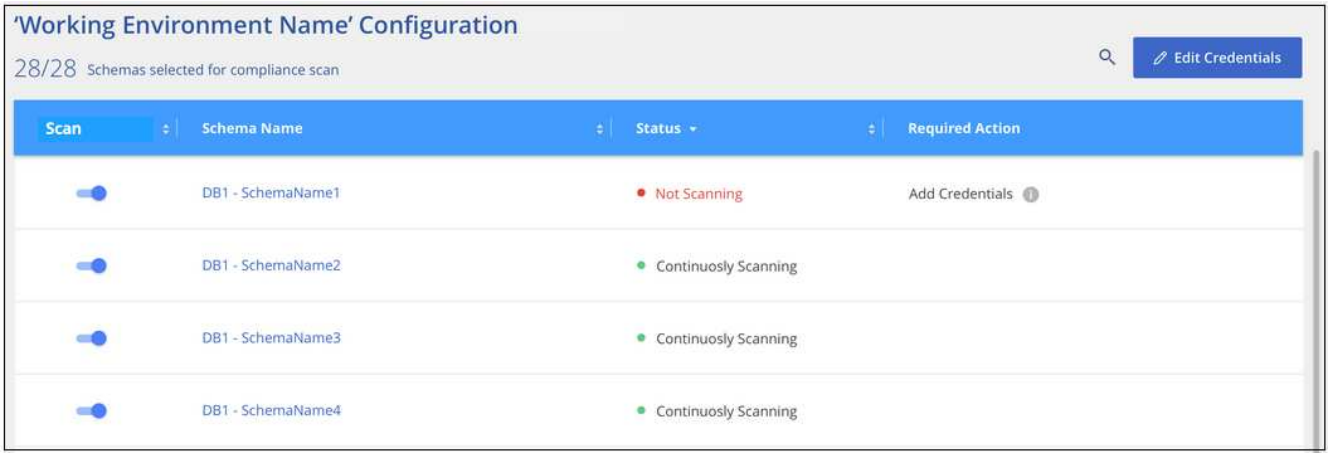
Habilitar y deshabilitar los análisis de cumplimiento de normativas en esquemas de base de datos

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

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

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

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



Resultado

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

Analizando cuentas de OneDrive

Complete unos pasos para empezar a analizar archivos en las carpetas de OneDrive de su usuario con Cloud Data Sense.

Inicio rápido

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

Revise los requisitos previos de OneDrive

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

Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

Añada la cuenta de OneDrive

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

4 Agregue los usuarios y seleccione el tipo de análisis

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

Revisión de los requisitos de OneDrive

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Data Sense.

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

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

El sentido de los datos puede ser "implementado en el cloud" o. "en una ubicación en el hotel que tiene acceso a internet".

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

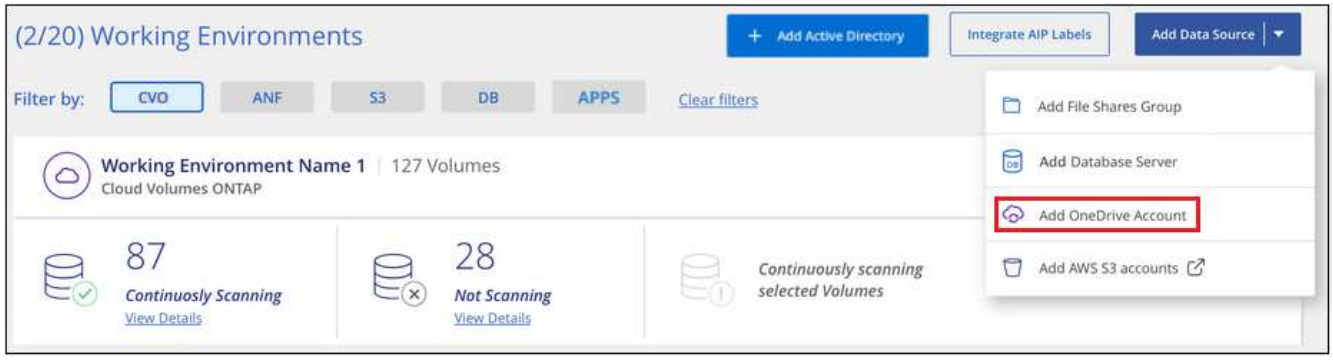
La detección de datos también puede ser "se implementa en una ubicación local que no tiene acceso a internet". Sin embargo, deberá proporcionar acceso a Internet a unos pocos extremos seleccionados para analizar sus archivos de OneDrive locales. "Consulte la lista de puntos finales necesarios aquí".

Adición de la cuenta de OneDrive

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

Pasos

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



2. En el cuadro de diálogo Agregar cuenta de OneDrive, haga clic en **Iniciar sesión en OneDrive**.

3. En la página de Microsoft que aparece, seleccione la cuenta de OneDrive e introduzca el usuario y la contraseña del administrador necesarios y, a continuación, haga clic en **Aceptar** para permitir que Cloud Data Sense lea datos de esta cuenta.

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

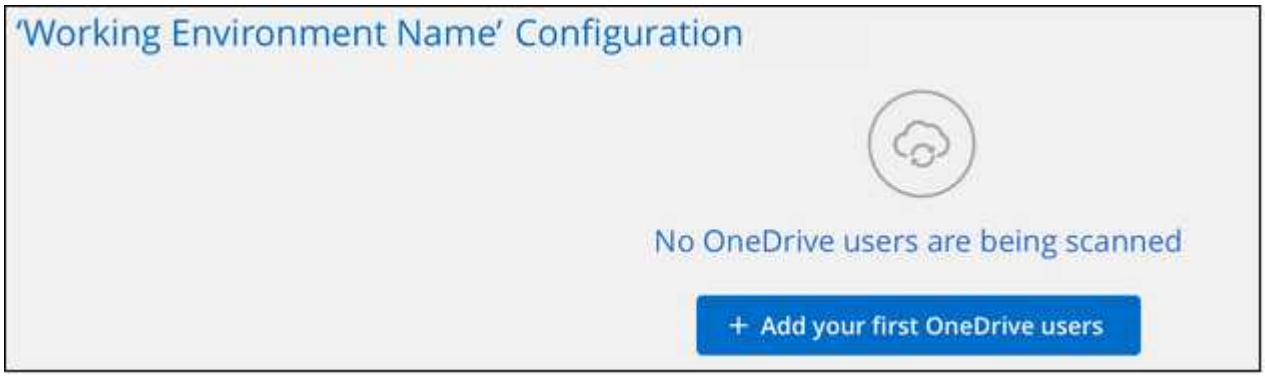
Añadir usuarios de OneDrive a los análisis de cumplimiento de normativas

Puede añadir usuarios individuales de OneDrive o todos sus usuarios de OneDrive para que sus archivos se puedan analizar mediante Cloud Data Sense.

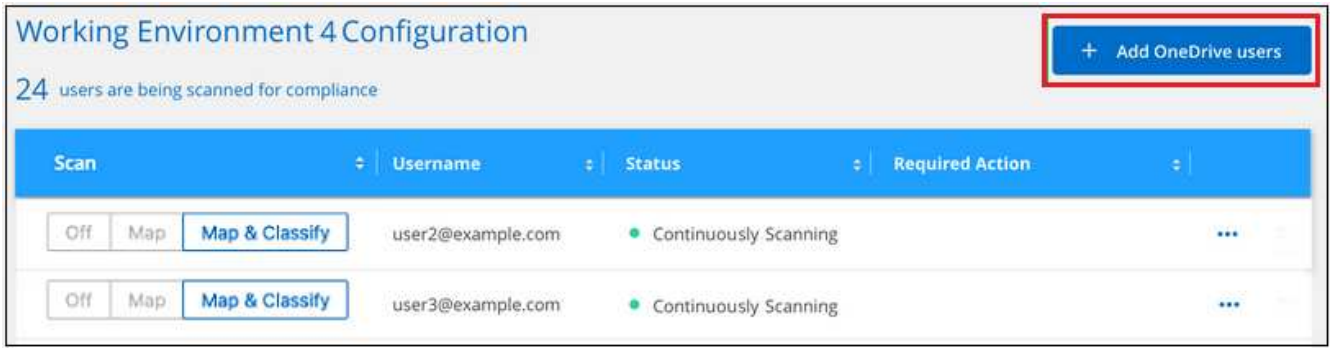
Pasos

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

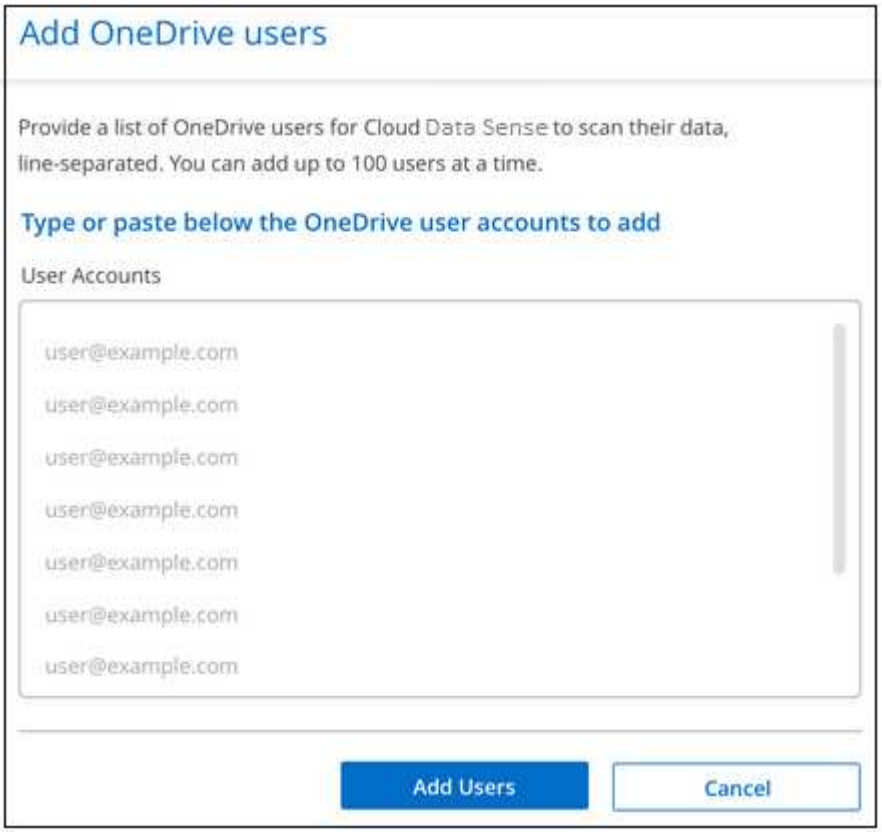
2. Si es la primera vez que añade usuarios para esta cuenta de OneDrive, haga clic en **Agregar sus primeros usuarios de OneDrive**.



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



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



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

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

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

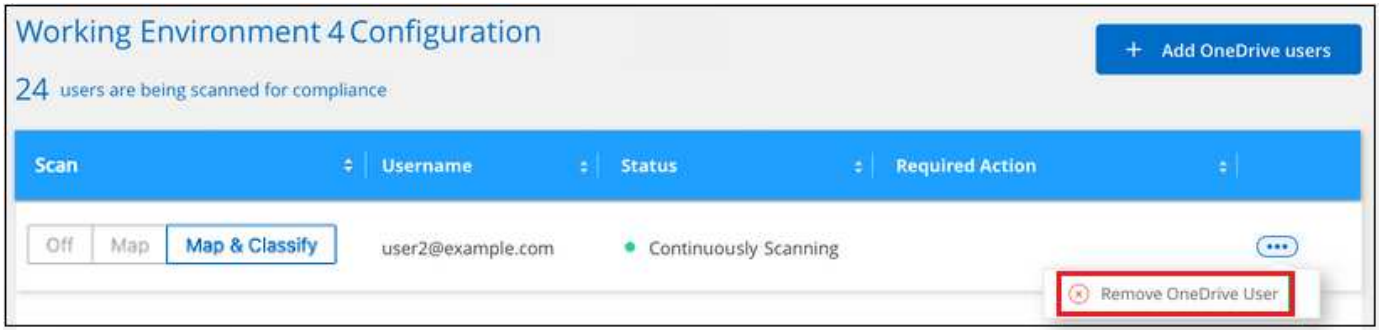
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en los archivos de usuario	Haga clic en **Mapa**
Activar análisis completos en archivos de usuario	Haga clic en **Mapa y clasificación**
Desactive el análisis en archivos de usuario	Haga clic en **Desactivado**

Resultado

Cloud Data Sense comienza a analizar los archivos de los usuarios agregados y los resultados se muestran en el Panel y en otras ubicaciones.

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

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



Tenga en cuenta que puede "Elimine toda la cuenta de OneDrive de Data Sense" Si ya no desea analizar ningún dato de usuario desde la cuenta de OneDrive.

Analizando cuentas de SharePoint

Realice unos pasos para comenzar a analizar archivos en sus cuentas de SharePoint Online y SharePoint en las instalaciones con Cloud Data Sense.

Inicio rápido

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

1 **Revise los requisitos previos de SharePoint**

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

2 **Ponga en marcha la instancia de Cloud Data Sense**

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

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

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

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

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

Revisar los requisitos de SharePoint

Revise los siguientes requisitos previos para asegurarse de que está preparado para activar Cloud Data Sense en una cuenta de SharePoint.

- Debe tener las credenciales de inicio de sesión de usuario administrador para la cuenta de SharePoint que proporciona acceso de lectura a todos los sitios de SharePoint.

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

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

- Para SharePoint Online, el sentido de los datos puede ser "implementado en el cloud" o. "se instala en una ubicación local con acceso a internet".

  La detección de datos también puede ser "se implementa en una ubicación local que no tiene acceso a internet". Sin embargo, deberá proporcionar acceso a Internet a unos pocos puntos finales seleccionados para analizar sus archivos de SharePoint Online. "Consulte la lista de puntos finales necesarios aquí".

- Para SharePoint en las instalaciones, se puede instalar Data Sense "en una ubicación en el hotel que tiene acceso a internet" o. "en una ubicación en el hotel que no tiene acceso a internet".

Cuando se instala detección de datos en un sitio sin acceso a Internet, el conector BlueXP también debe instalarse en ese mismo sitio sin acceso a Internet. "Leer más".

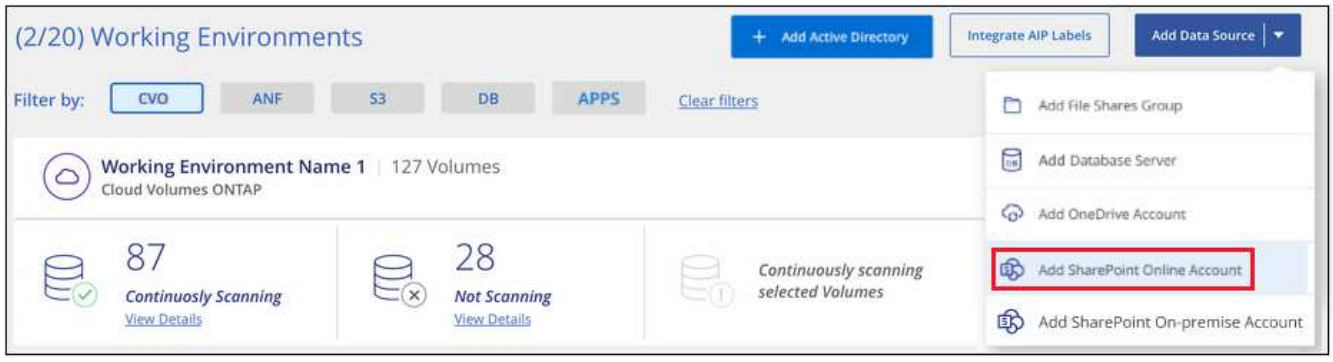
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Agregar una cuenta de SharePoint Online

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

Pasos

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



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

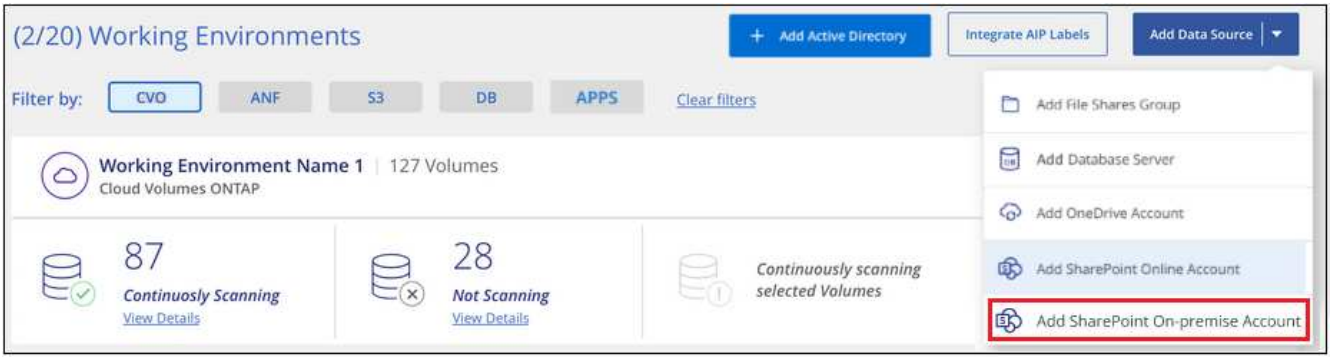
La cuenta de SharePoint Online se agrega a la lista de entornos de trabajo.

Adición de una cuenta de SharePoint en las instalaciones

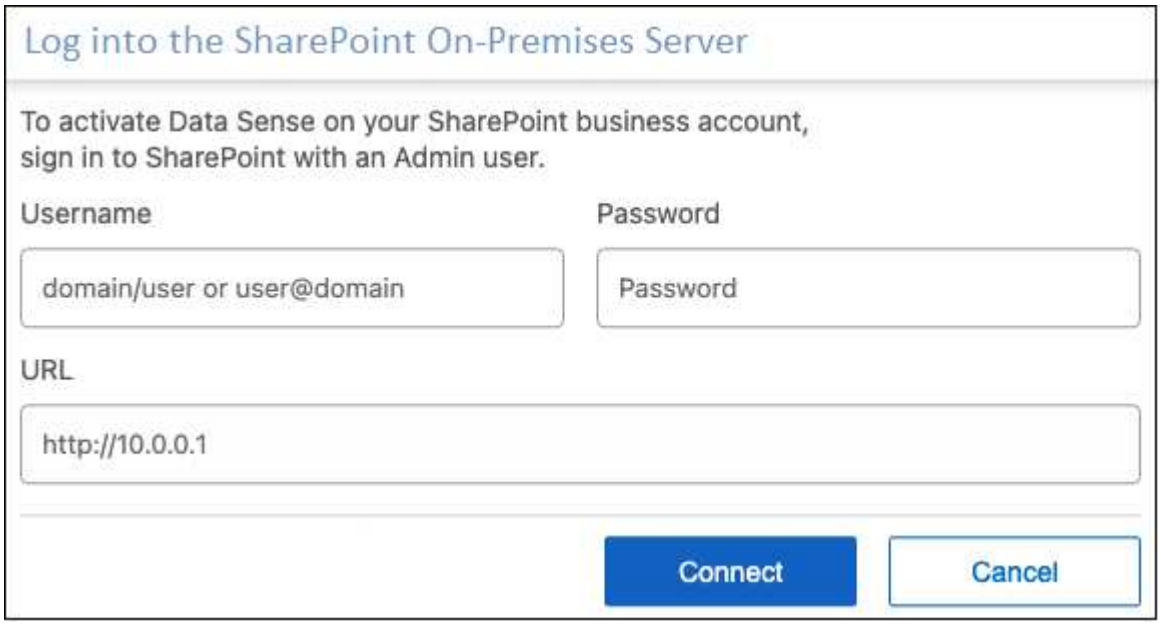
Agregue la cuenta de SharePoint en las instalaciones donde residen los archivos de usuario.

Pasos

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



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



3. Haga clic en **conectar**.

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

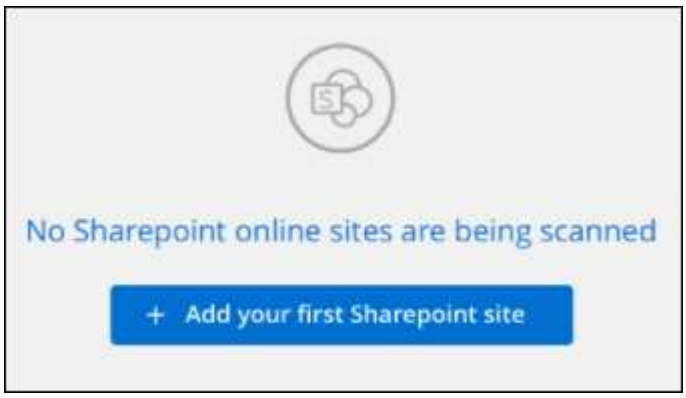
Agregar sitios de SharePoint a los análisis de cumplimiento

Puede agregar sitios de SharePoint individuales o todos los sitios de SharePoint de la cuenta para que los archivos asociados sean analizados por Cloud Data Sense. Los pasos son los mismos al agregar sitios locales de SharePoint Online o SharePoint.

Pasos

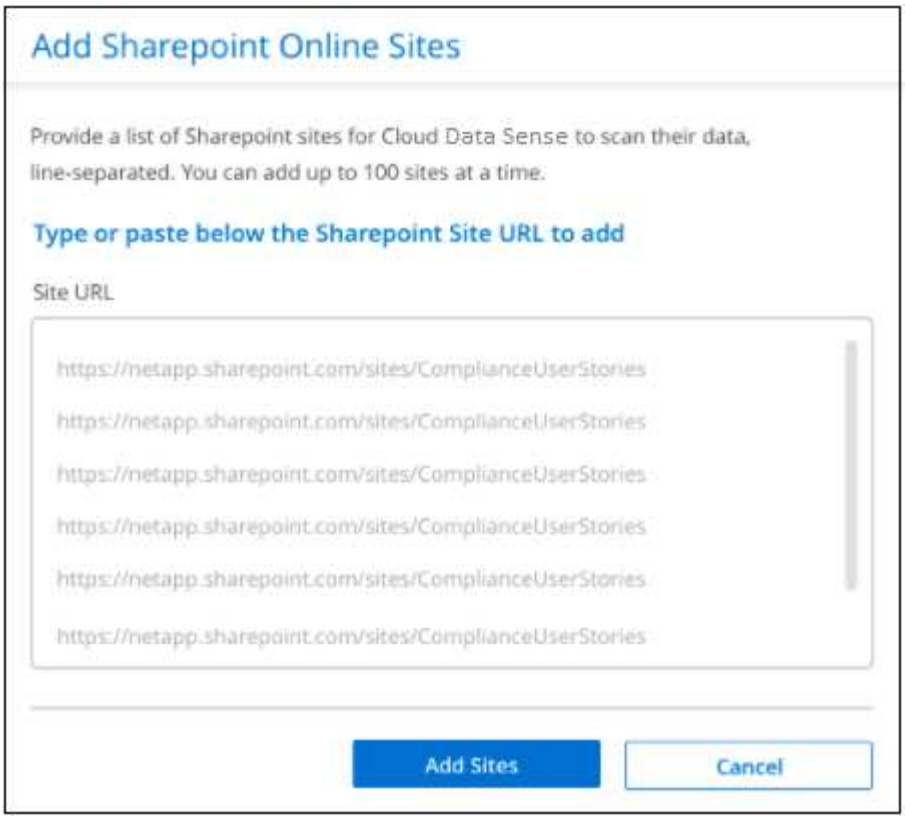
1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de SharePoint.

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



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

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



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

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

4. Habilite los análisis de sólo asignación, o los análisis de asignación y clasificación, en los archivos de los sitios de SharePoint.

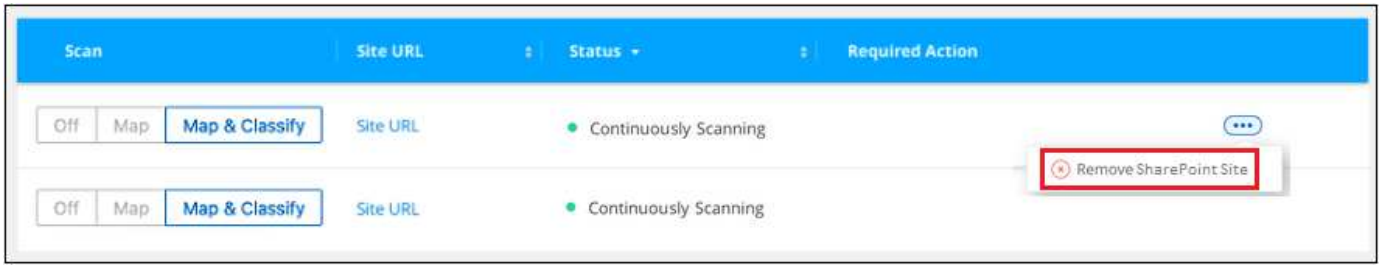
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en archivos	Haga clic en **Mapa**
Active los análisis completos en los archivos	Haga clic en **Mapa y clasificación**
Desactive el análisis en archivos	Haga clic en **Desactivado**

Resultado

Cloud Data Sense comienza a analizar los archivos de los sitios de SharePoint agregados y los resultados se muestran en el Panel y en otras ubicaciones.

Quitar un sitio de SharePoint de los análisis de cumplimiento

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



Tenga en cuenta que puede "Elimine toda la cuenta de SharePoint de Data Sense" Si ya no desea analizar los datos de usuario desde la cuenta de SharePoint.

Analizando cuentas de Google Drive

Realice algunos pasos para empezar a analizar archivos de usuario en sus cuentas de Google Drive con Cloud Data Sense.

Inicio rápido

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

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

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

2. **Ponga en marcha Cloud Data Sense**

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

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

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

4. **Seleccione el tipo de análisis de los archivos de usuario**

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

Revisión de los requisitos de Google Drive

Revise los siguientes requisitos previos para asegurarse de que está listo para habilitar Cloud Data Sense en una cuenta de Google Drive.

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

Restricciones actuales

Las siguientes funciones de detección de datos no son compatibles actualmente con los archivos de Google Drive:

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

Poner en marcha Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

El sentido de los datos puede ser "implementado en el cloud" o. "en una ubicación en el hotel que tiene acceso a internet".

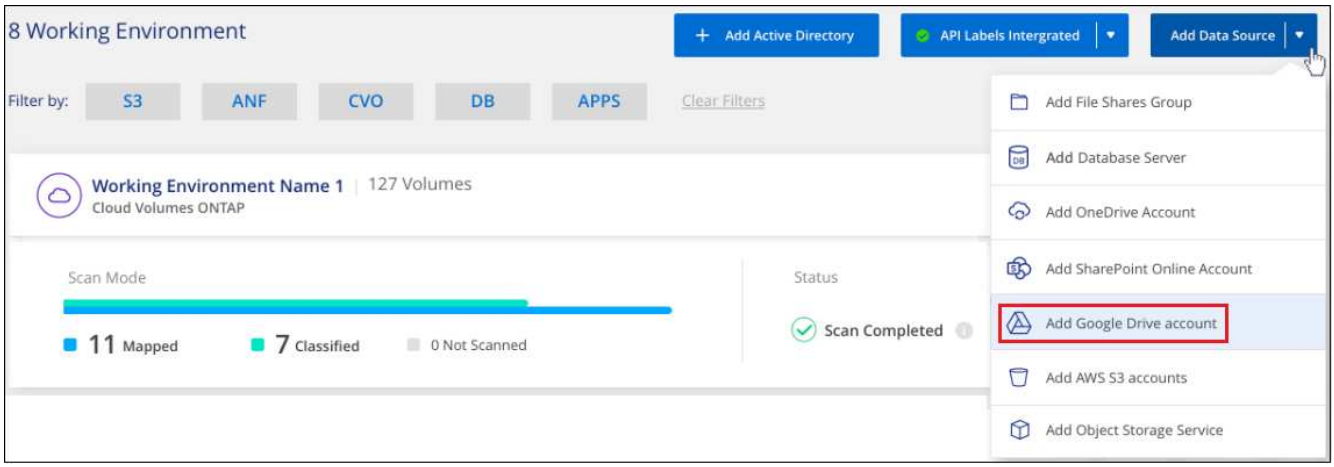
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Adición de la cuenta de Google Drive

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

Pasos

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



2. En el cuadro de diálogo Agregar una cuenta de Google Drive, haga clic en **Iniciar sesión en Google Drive**.
3. En la página de Google que aparece, seleccione la cuenta de Google Drive e introduzca el usuario y la contraseña de administrador necesarios y, a continuación, haga clic en **Aceptar** para permitir que detección de datos en la nube lea datos de esta cuenta.

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

Selección del tipo de análisis para los datos del usuario

Seleccione el tipo de análisis que Cloud Data Sense realizará en los datos del usuario.

Pasos

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

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

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

Resultado

Cloud Data Sense comienza a analizar los archivos de la cuenta de Google Drive que agregó, y los resultados se muestran en el Panel y en otras ubicaciones.

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

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

Analizando recursos compartidos de archivos

Complete unos pasos para empezar a analizar recursos compartidos de archivos NFS o CIFS no de NetApp directamente con Cloud Data Sense. Estos recursos compartidos de archivos pueden residir en las instalaciones o en el cloud.

Inicio rápido

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

1 Revise los requisitos previos para compartir archivos

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

2 Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

3 Cree un grupo que contenga los recursos compartidos de archivos

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

4 Añada los recursos compartidos de archivos y seleccione los recursos compartidos que desea analizar

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

Revisión de los requisitos de uso compartido de archivos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Data Sense.

- Los recursos compartidos se pueden alojar en cualquier lugar, incluso en el cloud o en las instalaciones. Son recursos compartidos de archivos que residen en sistemas de almacenamiento que no son de NetApp.
- Debe haber conectividad de red entre la instancia de detección de datos y los recursos compartidos.
- Asegúrese de que estos puertos estén abiertos a la instancia de Data Sense:
  - Para NFS, puertos 111 y 2049.
  - Para CIFS, puertos 139 y 445.
- Necesitará la lista de recursos compartidos que desea añadir en el formato `<host_name>:/<share_path>`. Puede introducir los recursos compartidos individualmente o proporcionar una lista separada por líneas de los recursos compartidos de archivos que desea escanear.
- En el caso de los recursos compartidos CIFS (SMB), asegúrese de tener credenciales de Active Directory con acceso de lectura a los recursos compartidos. Las credenciales de administración son preferidas en caso de que Cloud Data Sense necesite analizar cualquier dato que requiera permisos elevados.

  Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

Si va a analizar recursos compartidos de archivos NFS o CIFS de otros proveedores a los que se puede acceder a través de Internet, puede hacerlo "Ponga en marcha Cloud Data en el cloud" o. "Implemente el software de detección de datos en una ubicación local con acceso a Internet".

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

Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

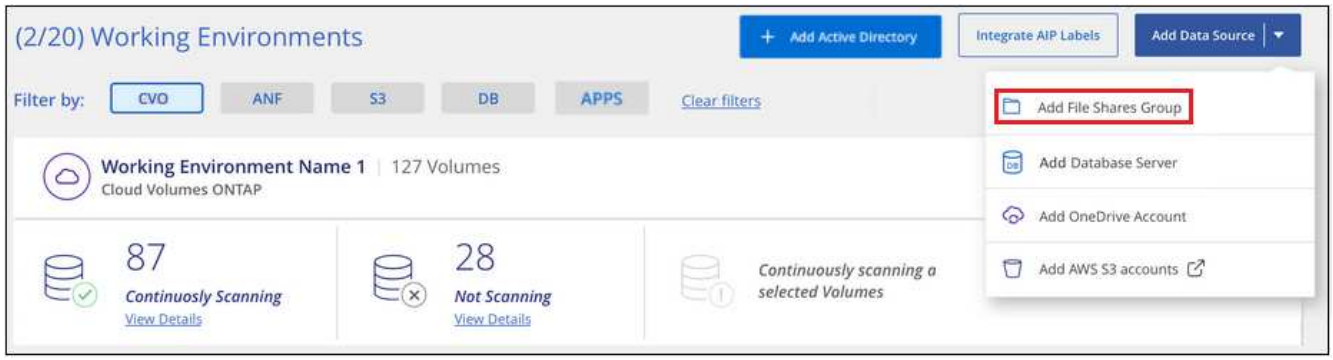
Creación del grupo para los recursos compartidos de archivos

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

Puede mezclar los recursos compartidos de NFS y CIFS en el mismo grupo, sin embargo, todos los recursos compartidos de archivos CIFS de un grupo deben utilizar las mismas credenciales de Active Directory. Si va a añadir recursos compartidos CIFS que utilizan credenciales diferentes, debe crear un grupo independiente para cada conjunto único de credenciales.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar grupo de recursos compartidos de archivos**.



2. En el cuadro de diálogo Agregar grupo de recursos compartidos de archivos, introduzca el nombre del grupo de recursos compartidos y haga clic en **continuar**.

El nuevo grupo de archivos compartidos se agrega a la lista de entornos de trabajo.

Agregar recursos compartidos de archivos a un grupo

Se agregan recursos compartidos de archivos al grupo de recursos compartidos de archivos para que Cloud Data Sense analice estos archivos en esos recursos compartidos. Los recursos compartidos se añaden con el formato `<host_name>:/<share_path>`.

Puede agregar recursos compartidos de archivos individuales o puede proporcionar una lista separada por

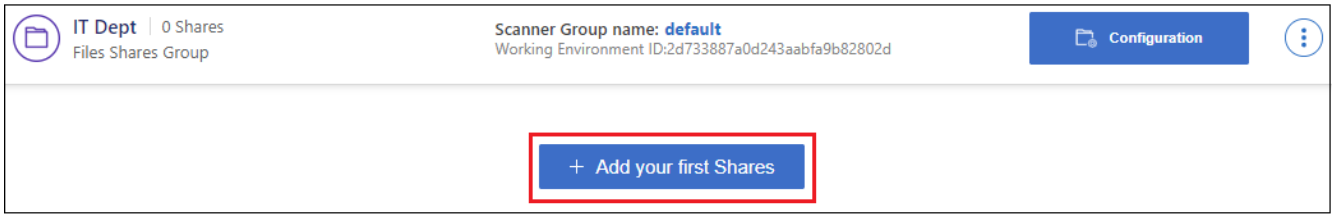
líneas de los recursos compartidos de archivos que desea analizar. Puede añadir hasta 100 recursos compartidos al mismo tiempo.

Al añadir ambos recursos compartidos NFS y CIFS en un único grupo, deberá realizar el proceso dos veces, una vez que añada recursos compartidos NFS y, a continuación, vuelva a añadir los recursos compartidos CIFS.

Pasos

1. En la página *Working Environments*, haga clic en el botón **Configuración** del grupo de recursos compartidos de archivos.

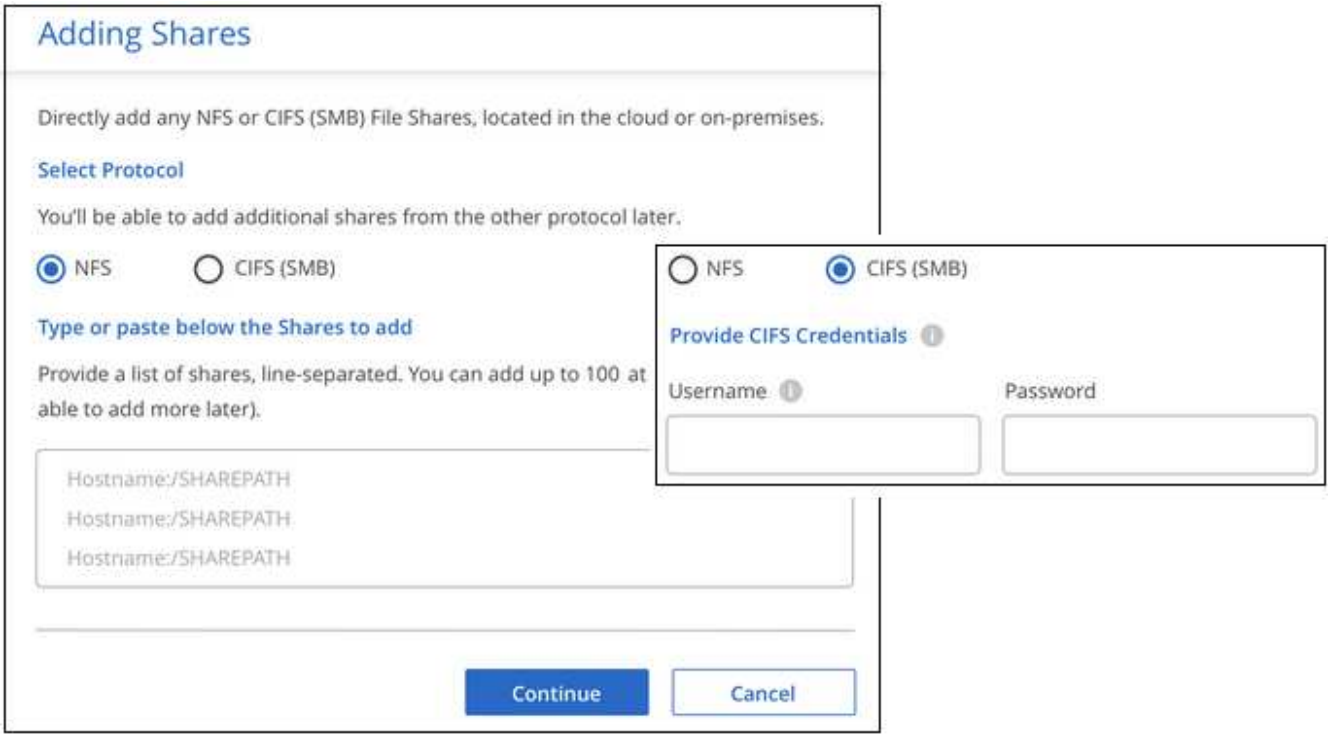
2. Si es la primera vez que añade archivos compartidos para este grupo de archivos compartidos, haga clic en **Agregar sus primeros recursos compartidos**.



   Si va a agregar archivos compartidos a un grupo existente, haga clic en **Agregar recursos compartidos**.

3. Seleccione el protocolo para los recursos compartidos de archivos que va a agregar, agregue los recursos compartidos de archivos que desea analizar - un recurso compartido de archivos por línea - y haga clic en **continuar**.

   Cuando se añaden recursos compartidos CIFS (SMB), debe introducir las credenciales de Active Directory con acceso de lectura a los recursos compartidos. Se prefieren las credenciales de administrador.



Un cuadro de diálogo de confirmación muestra el número de recursos compartidos que se han añadido.

Si el cuadro de diálogo enumera los recursos compartidos que no se han podido agregar, capture esta información para que pueda resolver el problema. En algunos casos, es posible volver a añadir el recurso compartido con un nombre de host o un nombre de recurso compartido corregidos.

4. Active análisis de sólo asignación o análisis de asignación y clasificación en cada recurso compartido de archivos.

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

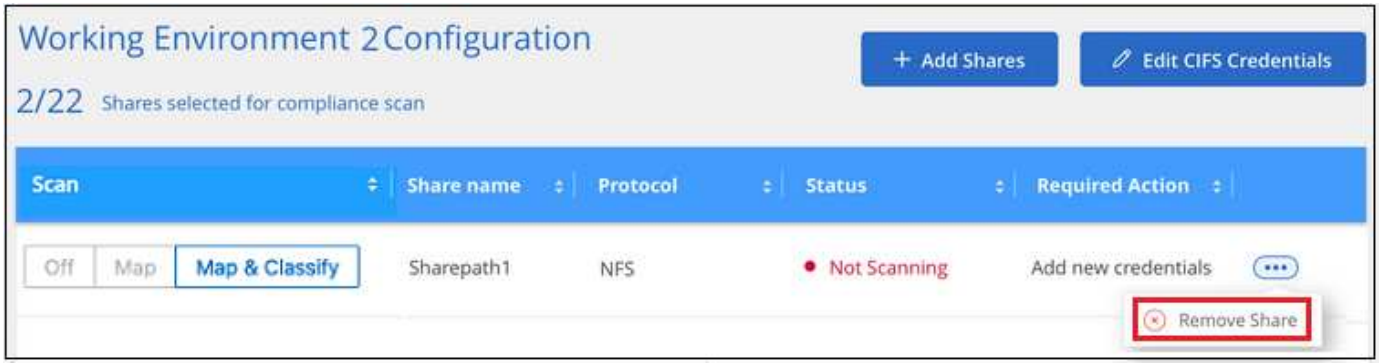
El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que si Data Sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará los archivos porque el sentido de datos no puede revertir la Marca de hora original a la "hora del último acceso". Si no le importa si se restablece la última hora de acceso, ENCIENDA el conmutador y se explorarán todos los archivos independientemente de los permisos. "Leer más".

Resultado

Cloud Data Sense comienza a analizar los archivos de los recursos compartidos de archivos agregados y los resultados se muestran en el Panel y en otras ubicaciones.

Quitar un recurso compartido de archivos de los análisis de cumplimiento de normativas

Si ya no necesita analizar determinados recursos compartidos de archivos, puede eliminar los recursos compartidos de archivos individuales para que los analice en cualquier momento. Haga clic en **Quitar recurso compartido** en la página Configuración.



Analizando el almacenamiento de objetos que utiliza el protocolo S3

Complete unos pasos para empezar a analizar datos en el almacenamiento de objetos directamente con Cloud Data Sense. El sentido de los datos puede analizar datos desde cualquier servicio de almacenamiento de objetos que utilice el protocolo simple Storage Service (S3). Entre ellas se incluyen StorageGRID de NetApp, IBM Cloud Object Store, Azure Blob (Using Minio), Linode, B2 Cloud Storage, Amazon S3, etc.

Inicio rápido

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

1 Revise los requisitos previos de almacenamiento del objeto

Debe tener la URL del extremo para conectarse con el servicio de almacenamiento de objetos.

Debe tener la clave de acceso y la clave secreta del proveedor de almacenamiento de objetos para que Cloud Data Sense pueda acceder a los bloques.

2 Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense" si aún no hay una instancia implementada.

3 Añada el servicio de almacenamiento de objetos

Añada el servicio de almacenamiento de objetos al Cloud Data Sense.

4 Seleccione los cucharones que desea escanear

Seleccione los cubos que desea analizar y Cloud Data Sense empezará a escanear.

Revisión de requisitos de almacenamiento de objetos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Data Sense.

- Debe tener la URL del extremo para conectarse con el servicio de almacenamiento de objetos.
- Debe tener la clave de acceso y la clave secreta del proveedor de almacenamiento de objetos para que Data Sense pueda acceder a los bloques.
- La compatibilidad con Azure Blob requiere que utilice el "Servicio de Minio".

Implementar la instancia de Cloud Data Sense

Si todavía no hay una instancia implementada, implemente Cloud Data Sense.

Si va a analizar datos de un almacenamiento de objetos S3 al que se puede acceder a través de Internet, puede hacerlo "Ponga en marcha Cloud Data en el cloud" o. "Implemente el software de detección de datos en una ubicación local con acceso a Internet".

Si va a analizar datos del almacenamiento de objetos S3 que se ha instalado en un sitio oscuro que no tiene acceso a Internet, deberá hacerlo "Implemente Cloud Data Sense en la misma ubicación en las instalaciones que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

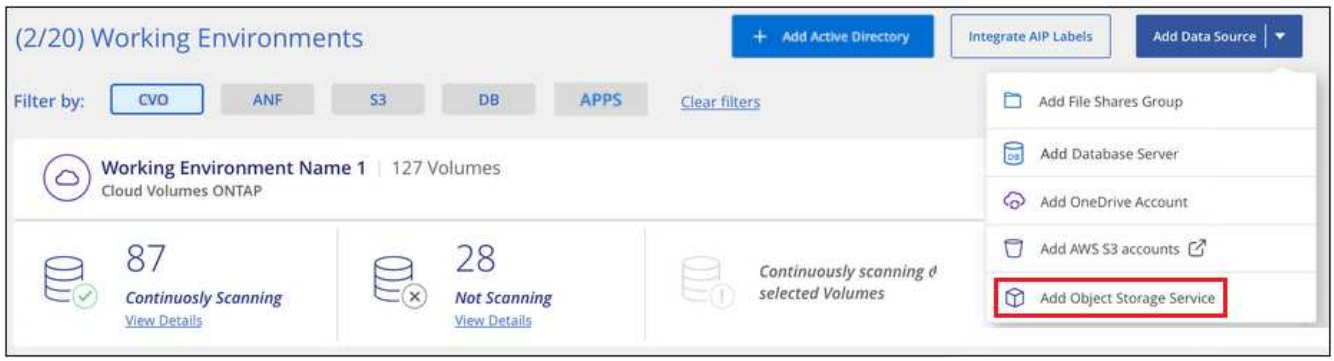
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

Adición del servicio de almacenamiento de objetos al Cloud Data Sense

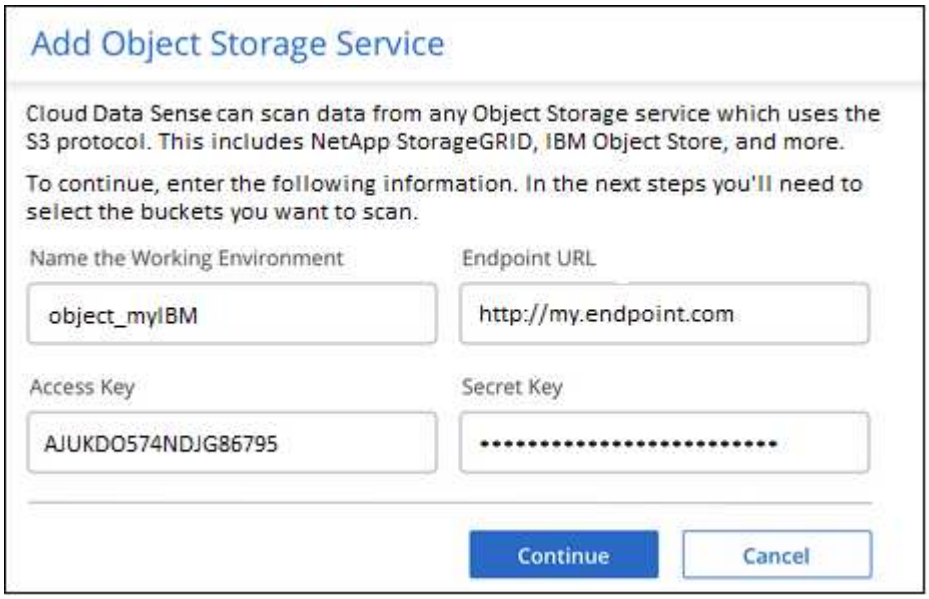
Añada el servicio de almacenamiento de objetos.

Pasos

1. En la página Configuración de entornos de trabajo, haga clic en **Agregar origen de datos** > **Agregar servicio de almacenamiento de objetos**.



2. En el cuadro de diálogo Add Object Storage Service, introduzca los detalles del servicio de almacenamiento de objetos y haga clic en **continuar**.
   a. Introduzca el nombre que desea utilizar para el entorno de trabajo. Este nombre debe reflejar el nombre del servicio de almacenamiento de objetos al que se conecta.
   b. Introduzca la URL de extremo para acceder al servicio de almacenamiento de objetos.
   c. Introduzca la clave de acceso y la clave secreta para que Cloud Data Sense pueda acceder a los bloques del almacenamiento de objetos.



Resultado

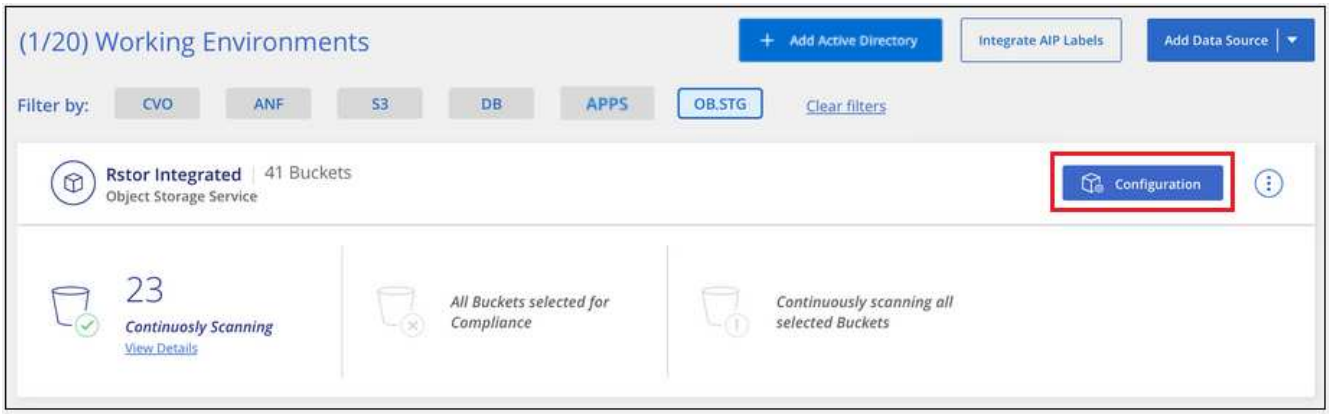
El nuevo Servicio de almacenamiento de objetos se añade a la lista de entornos de trabajo.

Habilitación y deshabilitación de análisis de cumplimiento de normativas en bloques de almacenamiento de objetos

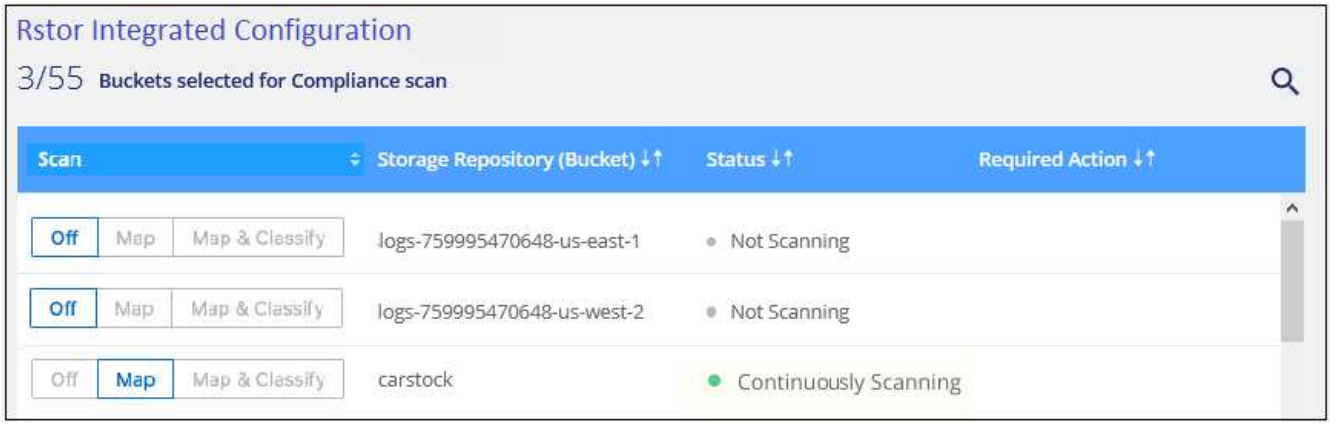
Después de habilitar Cloud Data Sense en el Servicio de almacenamiento de objetos, el siguiente paso es configurar los bloques que desea analizar. El sentido de los datos detecta esos bloques y los muestra en el entorno de trabajo que ha creado.

Pasos

1. En la página Configuración, haga clic en **Configuración** en el entorno de trabajo Servicio de almacenamiento de objetos.



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



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

Resultado

Cloud Data Sense comienza a analizar los bloques que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Integre su Active Directory con Cloud Data Sense

Puede integrar un Active Directory global con Cloud Data Sense para mejorar los resultados de los informes de detección de datos sobre los propietarios de archivos y qué usuarios y grupos tienen acceso a sus archivos.

Al configurar determinados orígenes de datos (que se enumeran a continuación), debe introducir credenciales de Active Directory para que Data Sense analice volúmenes CIFS. Esta integración proporciona Data Sense con el propietario del archivo y los detalles de permisos para los datos que residen en esos orígenes de datos. El directorio activo introducido para esos orígenes de datos puede ser diferente de las credenciales globales de Active Directory especificadas aquí. Data sense buscará en todos los directorios activos integrados para los detalles de permisos y usuarios.

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

- Puede utilizar el "propietario del archivo" "filtro" Y consulte los resultados en los metadatos del archivo en el panel Investigación. En lugar del propietario del archivo que contiene el SID (identificador de seguridad), se rellena con el nombre de usuario real.
- Puede ver "permisos completos de archivos" Para cada archivo y directorio al hacer clic en el botón "Ver todos los permisos".
- En la "Consola de gobernanza", El panel permisos abiertos mostrará un mayor nivel de detalle acerca de los datos.

Los SID del usuario local y los SID de dominios desconocidos no se traducen al nombre de usuario real.

Orígenes de datos compatibles

Una integración de Active Directory con Cloud Data Sense puede identificar datos procedentes de los siguientes orígenes de datos:

- Sistemas ONTAP en las instalaciones
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX para ONTAP
- Recursos compartidos de archivos CIFS de otros proveedores (no recursos compartidos de archivos NFS)

No se ofrece compatibilidad para identificar la información de usuarios y permisos de esquemas de base de datos, cuentas de OneDrive, cuentas de SharePoint, cuentas de Google Drive, cuentas de Amazon S3, O almacenamiento de objetos que utiliza el protocolo simple Storage Service (S3).

Conectarse al servidor de Active Directory

Después de implementar detección de datos y haber activado el análisis en sus orígenes de datos, puede integrar detección de datos con Active Directory. Se puede acceder a Active Directory mediante una dirección IP del servidor DNS o una dirección IP del servidor LDAP.

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

En el caso de volúmenes CIFS/recursos compartidos de archivos, si desea asegurarse de que los análisis de clasificación de detección de datos no modifican los archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permiso atributos de escritura. Si es posible, recomendamos que el usuario configurado de Active Directory sea parte de un grupo padre en la organización que tenga permisos para todos los archivos.

Requisitos

- Debe tener un Active Directory ya configurado para los usuarios de su empresa.
- Debe tener la información de Active Directory:
  - Dirección IP del servidor DNS o varias direcciones IP

    o.

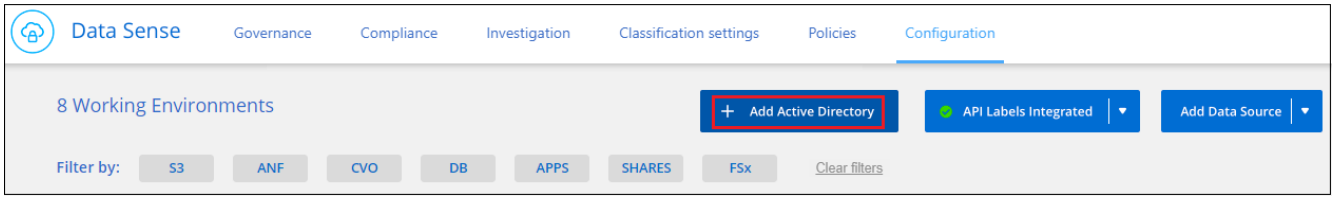
  Dirección IP del servidor LDAP o varias direcciones IP
  - Nombre de usuario y contraseña para acceder al servidor
  - Nombre de dominio (nombre de Active Directory)
  - Si utiliza o no un LDAP seguro (LDAPS)
  - Puerto de servidor LDAP (normalmente 389 para LDAP y 636 para LDAP seguro)
- La instancia de detección de datos debe abrir los siguientes puertos para la comunicación saliente:

Protocolo	Puerto	Destino	Específico
TCP Y UDP	389	Active Directory	LDAP

Protocolo	Puerto	Destino	Específico
TCP	636	Active Directory	LDAP sobre SSL
TCP	3268	Active Directory	Catálogo global
TCP	3269	Active Directory	Catálogo global sobre SSL

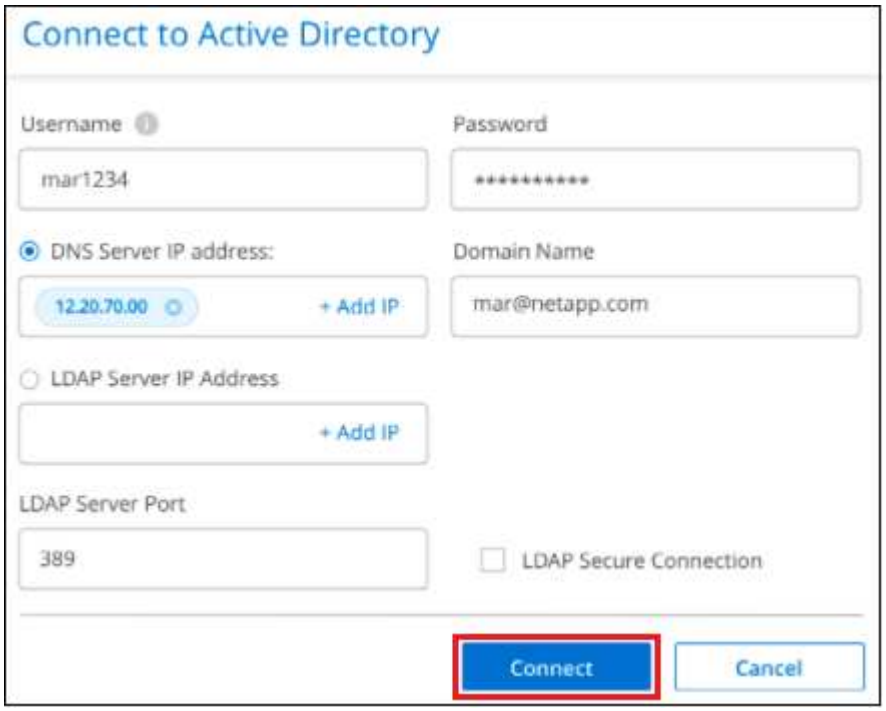
Pasos

1. En la página Configuración de detección de datos en la nube, haga clic en **Agregar Active Directory**.

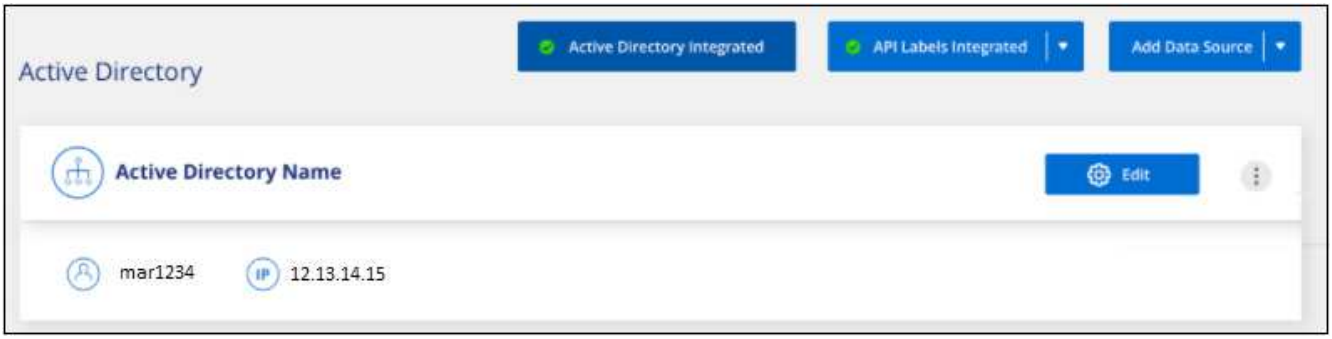


2. En el cuadro de diálogo conectarse a Active Directory, introduzca los detalles de Active Directory y haga clic en **conectar**.

   Si es necesario, puede agregar varias direcciones IP haciendo clic en **Agregar IP**.



   Data Sense se integra en Active Directory y se agrega una nueva sección a la página Configuration.



Administración de la integración con Active Directory

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

También puede eliminar la integración si ya no la necesita haciendo clic en el Y a continuación **Quitar Active Directory**.

Configure la licencia de Cloud Data Sense

Los primeros 1 TB de datos que Cloud Data Sense analiza en un espacio de trabajo BlueXP se pueden disponer de forma gratuita durante 30 días. Debe seguir analizando los datos después de ese momento una licencia BYOL de NetApp o una suscripción al mercado de su proveedor de cloud.

Antes de leer más:

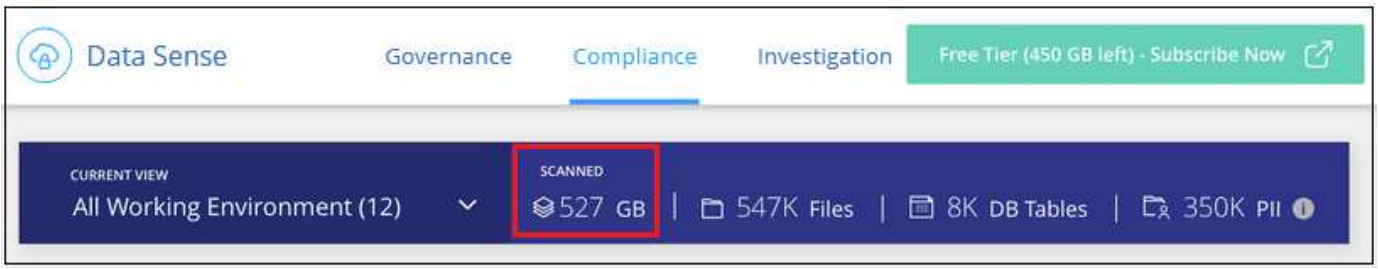
- Si ya está suscrito a la suscripción de pago por uso (PAYGO, por sus siglas en inglés) de BlueXP en el mercado de su proveedor de la nube, entonces también estará suscrito automáticamente a Cloud Data Sense. No tendrá que volver a suscribirse.
- Cloud Data Sense Bring-Your-Own-License (BYOL) es una licencia *floating* que puede utilizar en todos los entornos de trabajo y orígenes de datos del espacio de trabajo que tiene pensado analizar. Verá una suscripción activa en Digital Wallet.

"Obtenga más información acerca de las licencias y los costes relacionados con Cloud Data Sense".

Utilice una suscripción a Cloud Data Sense PAYGO

Las suscripciones de pago por uso del mercado de su proveedor de cloud le permiten obtener la licencia del uso de sistemas Cloud Volumes ONTAP y de muchos servicios de datos en el cloud, como Cloud Data Sense.

Puede suscribirse en cualquier momento y no se le cobrará hasta que finalice la prueba de 30 días o la cantidad de datos supere 1 TB. Siempre puede ver la cantidad total de datos que se van a analizar desde el panel de detección de datos. Y el botón *Subscribe Now* facilita la suscripción cuando esté listo.



Pasos

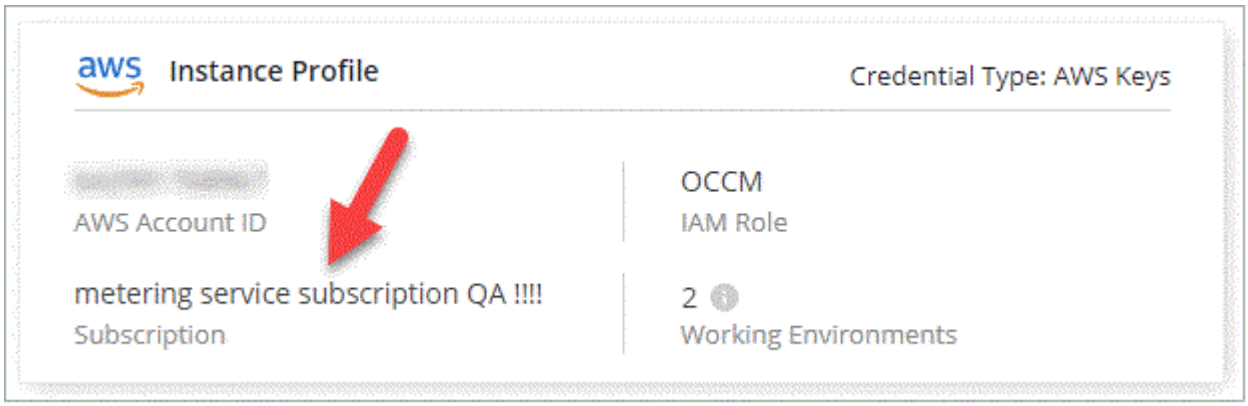
Un usuario que tenga la función *Account Admin* debe completar estos pasos.

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.

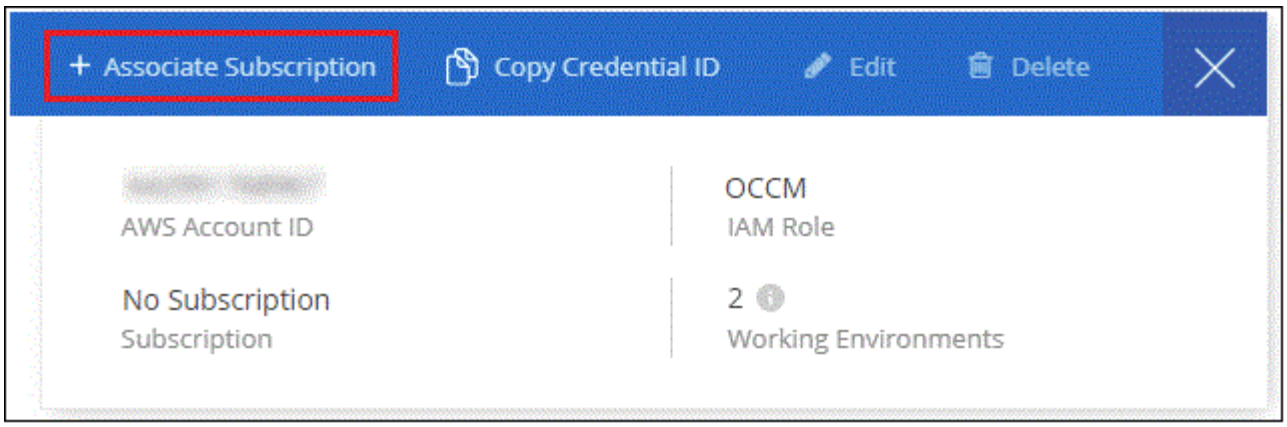
2. Busque las credenciales de AWS Instance Profile, Azure Managed Service Identity o Google Project.

   La suscripción se debe agregar al perfil de instancia, la identidad de servicio gestionado o Google Project. La carga no funcionará de otro modo.

   Si ya tiene una suscripción a BlueXP (que se muestra a continuación para AWS), entonces está preparado, no hay nada más que hacer.



3. Si todavía no tiene una suscripción, pase el cursor sobre las credenciales, haga clic en el menú de acciones y haga clic en **Suscripción asociada**.



4. Seleccione una suscripción existente y haga clic en **asociado**, o haga clic en **Agregar suscripción** y siga los pasos.

   El siguiente vídeo muestra cómo asociar un "Mercado AWS" Suscripción a una suscripción a AWS:

   ► https://docs.netapp.com/es-es/cloud-manager-data-sense//media/video_subscribing_aws.mp4 *(video)*

   El siguiente vídeo muestra cómo asociar un "Azure Marketplace" Suscripción a una suscripción de Azure:

   ► https://docs.netapp.com/es-es/cloud-manager-data-sense//media/video_subscribing_azure.mp4 *(video)*

   El siguiente vídeo muestra cómo asociar un "Mercado para GCP" Suscripción a una suscripción a GCP:

   ► https://docs.netapp.com/es-es/cloud-manager-data-sense//media/video_subscribing_gcp.mp4 *(video)*

Use una licencia BYOL de Cloud Data Sense

Las licencias que traiga sus propias de NetApp proporcionan períodos de 1, 2 o 3 años. La licencia BYOL **Cloud Data Sense** es una licencia *flotante* donde la capacidad total se comparte entre **todos** de sus entornos de trabajo y fuentes de datos, lo que facilita las licencias y la renovación iniciales.

Si no tiene una licencia de Cloud Data Sense, póngase en contacto con nosotros para adquirir una:

- Mailto:ng-contact-data-sense@netapp.com?Subject=Licensing[Enviar correo electrónico para adquirir una licencia].
- Haga clic en el icono de chat situado en la parte inferior derecha de BlueXP para solicitar una licencia.

De manera opcional, si tiene una licencia basada en nodo sin asignar para Cloud Volumes ONTAP que no usará, puede convertirla en una licencia de Cloud Data Sense con la misma equivalencia en dólares y la misma fecha de caducidad. "Vaya aquí para obtener más información".

La página de Digital Wallet de BlueXP se utiliza para gestionar licencias BYOL de Cloud Data Sense. Puede añadir licencias nuevas y actualizar las licencias existentes.

Obtenga su archivo de licencia de Cloud Data Sense

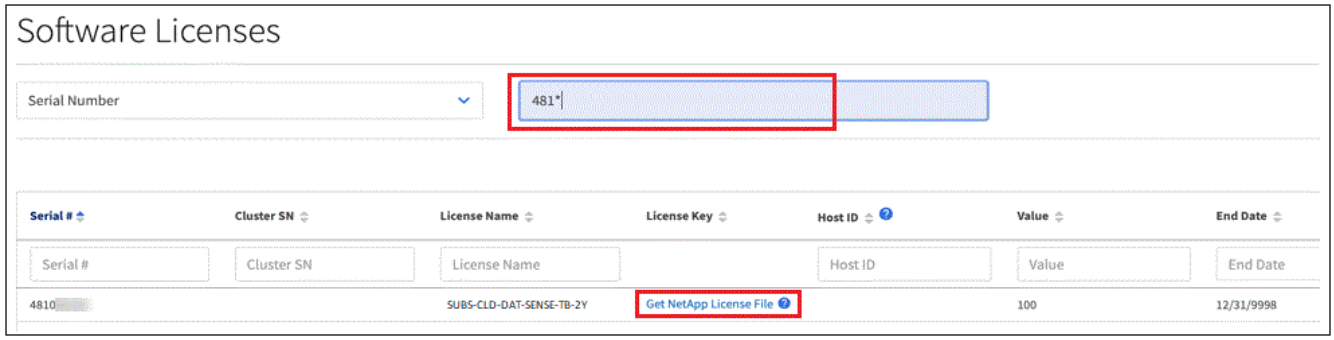
Después de adquirir la licencia de Cloud Data Sense, activa la licencia en BlueXP introduciendo el número de serie y la cuenta NSS de Cloud Data Sense o cargando el archivo de licencia de NLF. Los pasos a continuación muestran cómo obtener el archivo de licencia de NLF si planea utilizar ese método.

Si ha implementado Cloud Data Sense en un host de un sitio en las instalaciones que no tiene acceso a

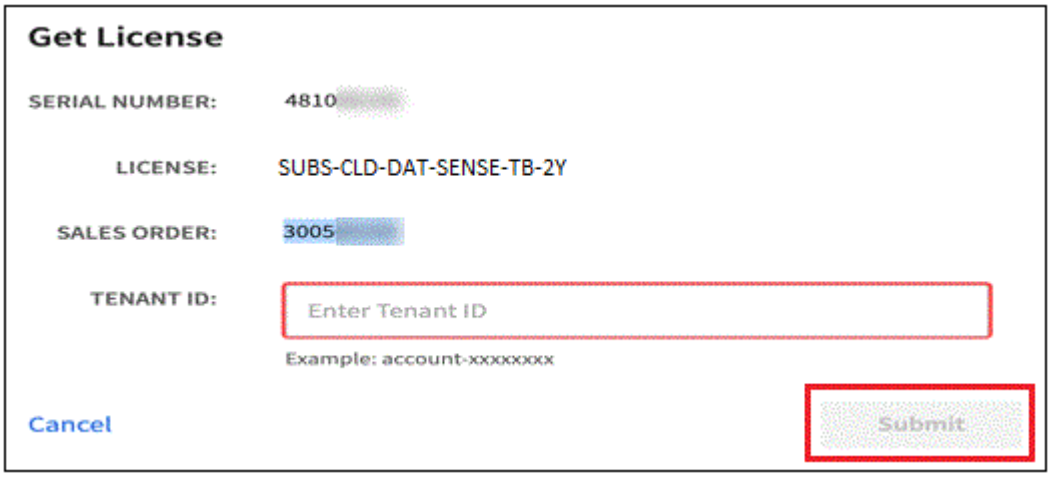
Internet, necesitará obtener el archivo de licencia de un sistema conectado a Internet. La activación de la licencia mediante el número de serie y la cuenta de NSS no está disponible para las instalaciones de sitios oscuros.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp" Y haga clic en **sistemas > licencias de software**.
2. Introduzca el número de serie de la licencia de Cloud Data Sense.



3. En **clave de licencia**, haga clic en **obtener archivo de licencia de NetApp**.
4. Introduzca su ID de cuenta de BlueXP (esto se denomina ID de inquilino en el sitio de soporte) y haga clic en **Enviar** para descargar el archivo de licencia.



Puede encontrar su ID de cuenta de BlueXP seleccionando el menú desplegable **cuenta** de la parte superior de BlueXP y, a continuación, haciendo clic en **Administrar cuenta** junto a su cuenta. Su ID de cuenta se encuentra en la ficha Descripción general.

Añada licencias BYOL de Cloud Data Sense a su cuenta

Después de adquirir una licencia de Cloud Data Sense para su cuenta de BlueXP, debe agregar la licencia a BlueXP para utilizar el servicio de detección de datos.

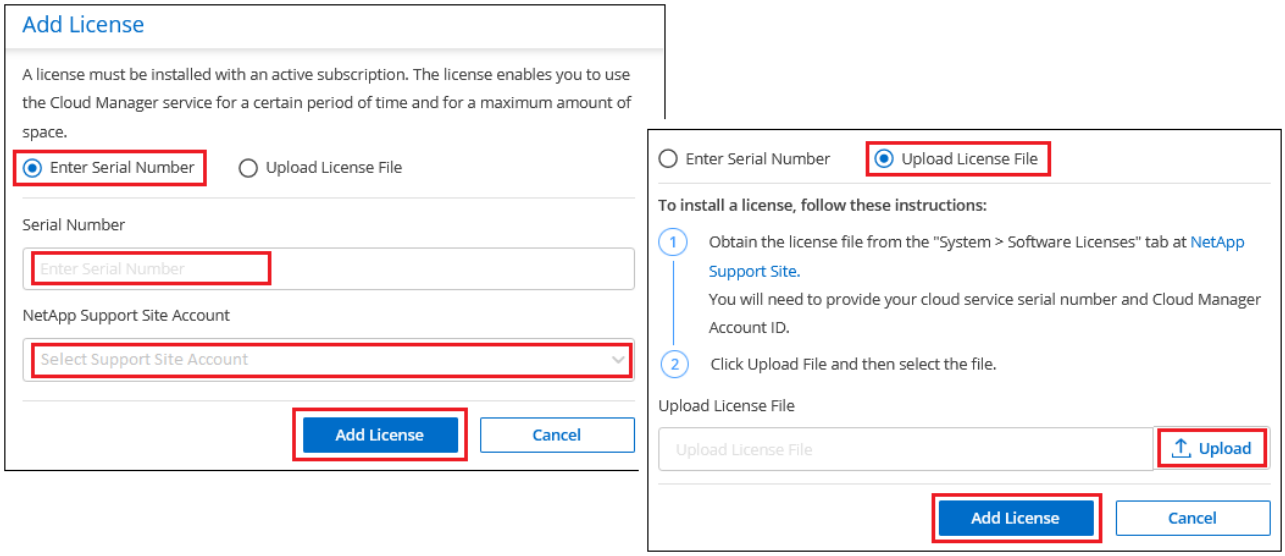
Pasos

1. En el menú BlueXP, haga clic en **Gobierno > cartera digital** y, a continuación, seleccione la ficha **licencias de servicios de datos**.
2. Haga clic en **Agregar licencia**.
3. En el cuadro de diálogo *Add License*, introduzca la información de la licencia y haga clic en **Add License**:

- Si tiene el número de serie de la licencia de Data Sense y conoce su cuenta de NSS, seleccione la opción **introducir número de serie** e introduzca esa información.

  Si su cuenta del sitio de soporte de NetApp no está disponible en la lista desplegable, "Agregue la cuenta NSS a BlueXP".

- Si tiene el archivo de licencia de Data Sense (requerido cuando está instalado en un sitio oscuro), seleccione la opción **cargar archivo de licencia** y siga las indicaciones para adjuntar el archivo.



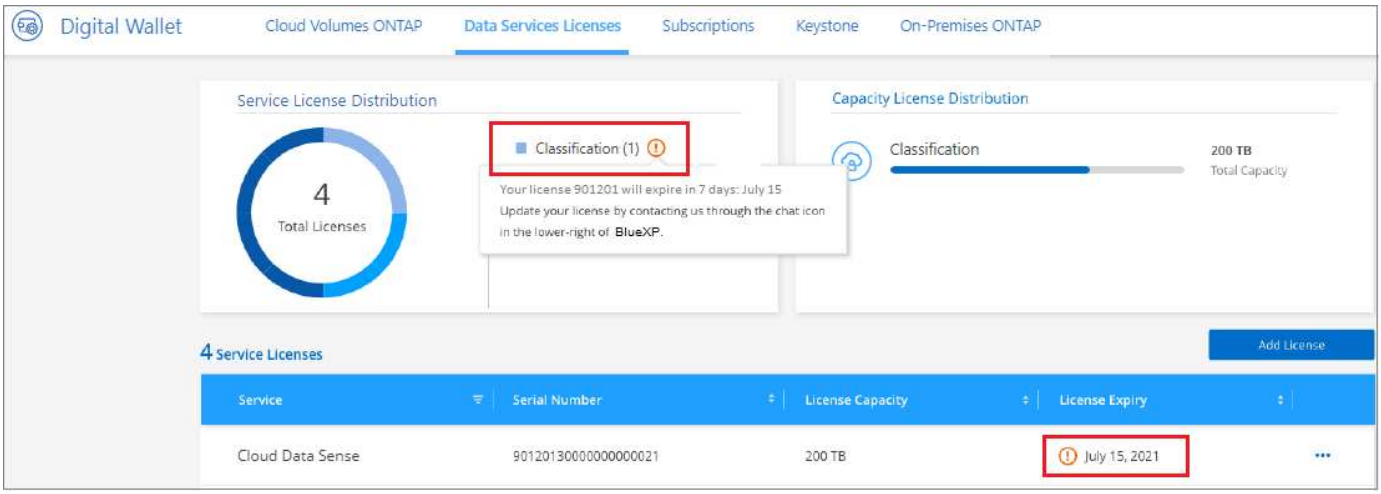
Resultado

BlueXP agrega la licencia para que su servicio Cloud Data Sense esté activo.

Actualice una licencia BYOL de Cloud Data Sense

Si el término con licencia se acerca a la fecha de vencimiento o si la capacidad con licencia alcanza el límite, se le notificará en Cloud Data Sense.

Este estado también aparece en la cartera digital.



Puede actualizar su licencia de Cloud Data Sense antes de que caduque para que no se interrumpa su capacidad para acceder a los datos analizados.

Pasos

1. Haga clic en el icono de chat situado en la parte inferior derecha de BlueXP para solicitar una extensión de su término o capacidad adicional a su licencia de Cloud Data Sense para el número de serie concreto. También puede enviar un correo electrónico para solicitar una actualización a su licencia.

   Tras pagar la licencia y registrarse en el sitio de soporte de NetApp, BlueXP actualiza automáticamente la licencia en la cartera digital y la página licencias de servicios de datos reflejarán el cambio en 5 a 10 minutos.

2. Si BlueXP no puede actualizar automáticamente la licencia (por ejemplo, cuando está instalada en un sitio oscuro), deberá cargar manualmente el archivo de licencia.

   a. Puede hacerlo Obtenga el archivo de licencia del sitio de soporte de NetApp.

   b. En la página cartera digital de la ficha *Data Services Licenses*, haga clic en ••• Para el número de serie del servicio que está actualizando y haga clic en **Actualizar licencia**.

   c. En la página *Update License*, cargue el archivo de licencia y haga clic en **Actualizar licencia**.

Resultado

BlueXP actualiza la licencia para que su servicio Cloud Data Sense siga activo.

Consideraciones sobre la licencia de BYOL

Al utilizar una licencia BYOL de Cloud Data Sense, BlueXP muestra una advertencia en la interfaz de usuario de Data Sense y en la interfaz de usuario de Digital Wallet cuando el tamaño de todos los datos que está

analizando se acerca al límite de capacidad o se acerca a la fecha de caducidad de la licencia. Recibe estas advertencias:

- Cuando la cantidad de datos que está analizando ha alcanzado el 80% de la capacidad con licencia y, de nuevo, cuando ha alcanzado el límite
- 30 días antes de que caduque una licencia, y de nuevo cuando caduque la licencia

Utilice el icono de chat situado en la parte inferior derecha de la interfaz de BlueXP para renovar su licencia cuando vea estas advertencias.

Si la licencia caduca, Data Sense continúa ejecutándose, pero el acceso a los paneles está bloqueado para que no pueda ver información sobre ninguno de los datos analizados. Solo la página *Configuration* está disponible en caso de que se desee reducir la cantidad de volúmenes que se van a analizar para lograr que su uso de capacidad esté dentro del límite de licencia.

Una vez que renueve su licencia BYOL, BlueXP actualiza automáticamente la licencia de Digital Wallet y ofrece acceso completo a todas las consolas. Si BlueXP no puede acceder al archivo de licencia a través de la conexión segura a Internet (por ejemplo, cuando está instalado en un sitio oscuro), puede obtener el archivo usted mismo y cargarlo manualmente en BlueXP. Para ver instrucciones, consulte cómo actualizar una licencia de Cloud Data Sense.

Si la cuenta que está utilizando tiene una licencia BYOL y una suscripción a PAYGO, Data Sense _no pasará a la suscripción a PAYGO cuando caduque la licencia BYOL. Debe renovar la licencia de BYOL.

Preguntas frecuentes acerca de Cloud Data Sense

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Servicio Cloud Data Sense

Las siguientes preguntas constituyen un conocimiento general de la utilidad de detección de datos en el cloud.

¿Qué es lo mejor de los datos en el cloud?

Cloud Data Sense es una oferta de cloud que utiliza la tecnología basada en la inteligencia artificial (IA) para ayudarle a comprender el contexto de los datos e identificar los datos confidenciales en sus sistemas de almacenamiento. Los sistemas pueden ser entornos de trabajo que has añadido al lienzo BlueXP y muchos tipos de fuentes de datos a los que Data Sense puede acceder a través de tus redes. "Consulte la lista completa a continuación".

Cloud Data Sense ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para abordar nuevas normativas de cumplimiento de normativas sobre privacidad y sensibilidad de los datos, como GDPR, CCPA, HIPAA, etc.

¿Cómo funciona Cloud Data?

Cloud Data Sense implementa otra capa de inteligencia artificial junto a su sistema y sistemas de almacenamiento de BlueXP. A continuación, analiza los datos en volúmenes, bloques, bases de datos y otras cuentas de almacenamiento e indexa las estadísticas de datos que se encuentran. Data Sense aprovecha tanto la inteligencia artificial como el procesamiento de lenguaje natural, en lugar de soluciones alternativas

que se crean comúnmente alrededor de expresiones regulares y correspondencia de patrones.

Cloud Data Sense utiliza la IA para proporcionar un conocimiento contextual de los datos para una detección y clasificación precisas. Está impulsada por la IA porque está diseñada para los tipos de datos y la escala actuales. También comprende el contexto de los datos a fin de proporcionar datos sólidos, precisos, de detección y clasificación.

"Obtenga más información sobre el funcionamiento de Cloud Data Sense".

¿Cuáles son los casos de uso comunes de Cloud Data Sense?

- Identificación de la Información personal de identificación (PII).
- Localice con facilidad y cree informes sobre datos específicos en respuesta a sujetos de datos, según lo requiera el RGPD, la CCPA, la HIPAA y otras normativas de privacidad de los datos.
- Cumpla con las normativas de privacidad de datos nuevas y futuras.
- Cumpla con las normativas sobre privacidad y cumplimiento de normativas de datos.
- Migrar los datos de los sistemas heredados al cloud.
- Cumpla con las políticas de retención de datos.

"Obtenga más información acerca de los casos de uso de Cloud Data Sense".

¿Qué pasa con la arquitectura detección de datos en el cloud?

Cloud Data Sense pone en marcha un único servidor o clúster, sin importar dónde elija, en el cloud o en las instalaciones. Los servidores se conectan mediante protocolos estándar a los orígenes de datos e indexan los hallazgos de un clúster Elasticsearch, que también se implementa en los mismos servidores. Esto permite la compatibilidad con entornos multicloud, entre cloud, cloud privado y en las instalaciones.

¿Qué proveedores de cloud son compatibles?

Cloud Data Sense funciona como parte de BlueXP y es compatible con AWS, Azure y GCP. Esto proporciona a su organización una visibilidad de privacidad unificada a través de distintos proveedores de cloud.

¿Cloud Data tiene sentido una API REST? ¿Funciona con herramientas de terceros?

BlueXP admite las funcionalidades de la API DE REST para sus servicios. Si BlueXP no es el punto de gestión preferido, servicios como Cloud Data Sense también pueden usarse a través de una API REST. Cada acción del usuario tiene una API REST que se puede integrar con sistemas de terceros.

¿Cloud Data Sense está disponible a través de las plataformas?

Sí, BlueXP y Cloud Data Sense están disponibles en las plataformas AWS, Azure y GCP.

Análisis y análisis de Cloud Data

Las siguientes preguntas están relacionadas con el rendimiento del análisis de detección de datos en el cloud y los análisis disponibles para los usuarios.

¿Con qué frecuencia Cloud Data Sense analiza mis datos?

Los datos cambian con frecuencia; Cloud Data Sense analiza los datos de forma continua y sin impacto en los datos. Aunque el análisis inicial de los datos puede tardar más tiempo, los análisis posteriores sólo analizan

los cambios incrementales, lo que reduce los tiempos de análisis del sistema.

"Descubra cómo funcionan las exploraciones".

Los análisis de datos tienen un impacto insignificante en los sistemas de almacenamiento y en los datos. Sin embargo, si le preocupa incluso un impacto muy pequeño, puede configurar Data Sense para realizar exploraciones "lentas". "Descubra cómo reducir la velocidad de escaneado".

¿Puedo buscar mis datos con Cloud Data Sense?

Cloud Data Sense ofrece amplias funcionalidades de búsqueda que facilitan la búsqueda de un archivo o pieza de datos específicos de todas las fuentes conectadas. El sentido de los datos permite a los usuarios buscar más allá de solo lo que reflejan los metadatos. Es un servicio que no depende del lenguaje que también puede leer los archivos y analizar una multitud de tipos de datos confidenciales, como nombres e ID. Por ejemplo, los usuarios pueden buscar en almacenes de datos estructurados y no estructurados para buscar datos que se hayan filtrado desde bases de datos a archivos de usuario, en violación de la política corporativa. Las búsquedas se pueden guardar más adelante y se pueden crear políticas para buscar y realizar acciones sobre los resultados a una frecuencia establecida.

Una vez que se han encontrado los archivos de interés, se pueden enumerar las características, incluyendo etiquetas, cuenta de entorno de trabajo, bloque, ruta de archivo, categoría (de clasificación), tamaño de archivo, última modificación, estado de permisos, duplicados, nivel de sensibilidad, datos personales, tipos de datos confidenciales dentro del archivo, propietario, tipo de archivo, tamaño de archivo, hora de creación, hash de archivo, si los datos se asignaron a alguien que busca atención y mucho más. Los filtros pueden aplicarse para eliminar las características que no son pertinentes. La detección de datos también cuenta con controles RBAC para permitir mover o eliminar archivos, en caso de que haya los permisos adecuados. Si no hay permisos correctos, las tareas se pueden asignar a alguien de la organización que tenga los permisos adecuados.

¿Qué tipo de análisis proporciona Cloud Data Sense?

Las fuentes de datos se pueden representar visualmente y las relaciones se definen y se representan gráficamente. Por ejemplo, los administradores pueden ver todos los datos desfasados, duplicados y no relacionados con el negocio en todos los orígenes de datos de toda la empresa (sistemas locales, bases de datos, recursos compartidos de archivos, almacenes S3, OneDrive, etc.). Luego pueden copiar, mover, eliminar y gestionar los datos para optimizar los costes en almacenamiento y reducir los riesgos. Los usuarios pueden reducir el riesgo viendo qué datos confidenciales se pueden exponer y pueden crear trabajos para gestionar permisos para una protección de datos sólida. El sentido de los datos también clasifica todos los distintos tipos de datos, de modo que los administradores pueden investigar los datos por tipo y ver qué acciones se han tomado sobre los datos, y cuándo.

¿Cloud Data Sense ofrece informes?

Sí. La información que ofrece Cloud Data Sense puede ser relevante para otras partes interesadas de sus organizaciones y así permitirle generar informes que compartan la información. Los siguientes informes están disponibles para Data Sense:

Informe de evaluación de riesgos de privacidad

Proporciona información sobre la privacidad de sus datos y una puntuación de riesgo para la privacidad. "Leer más".

Informe de solicitud de acceso de asunto de datos

Le permite extraer un informe de todos los archivos que contienen información sobre el nombre o identificador personal específico de un sujeto de datos. "Leer más".

Informe PCI DSS

Le ayuda a identificar la distribución de la información de la tarjeta de crédito a través de sus archivos. "Leer más".

Informe HIPAA

Le ayuda a identificar la distribución de información médica a través de sus archivos. "Leer más".

Informe asignación de datos

Proporciona información acerca del tamaño y el número de archivos en los entornos de trabajo. Esto incluye la capacidad de uso, la antigüedad de los datos, el tamaño de los datos y los tipos de archivos. "Leer más".

Informa sobre un tipo de información específico

Hay informes disponibles que incluyen detalles sobre los archivos identificados que contienen datos personales y datos personales confidenciales. También puede ver los archivos desglosados por categoría y tipo de archivo. "Leer más".

¿el rendimiento del análisis varía?

El rendimiento del análisis puede variar en función del ancho de banda de la red y del tamaño medio de los archivos del entorno. También puede depender del tamaño del sistema host (ya sea en el cloud o en las instalaciones). Consulte "La instancia de Cloud Data Sense" y.. "Poner en marcha Cloud Data Sense" si quiere más información.

Al agregar inicialmente nuevos orígenes de datos, también puede elegir realizar sólo una exploración de "asignación" en lugar de una exploración de "clasificación" completa. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro. "Vea la diferencia entre una exploración de mapeo y clasificación".

Cloud Data SENSE, gestión y privacidad

Las siguientes preguntas ofrecen información sobre cómo gestionar la configuración de sentido y privacidad de datos en el cloud.

¿Cómo puedo habilitar el sentido de los datos en el cloud?

En primer lugar, necesita poner en marcha una instancia de Cloud Data Sense en BlueXP o en un sistema local. Una vez que la instancia se esté ejecutando, puede habilitar el servicio en entornos de trabajo existentes, bases de datos y otros orígenes de datos desde la ficha **detección de datos** o seleccionando un entorno de trabajo específico.

"Aprenda cómo empezar".

La activación de Cloud Data Sense en una fuente de datos da como resultado un análisis inicial inmediato. Los resultados de la exploración se muestran poco después.

¿Cómo se deshabilita el sentido de Cloud Data?

Puede deshabilitar Cloud Data Sense para poder analizar un entorno de trabajo individual, base de datos, grupo de recursos compartidos de archivos, cuenta de OneDrive o cuenta de SharePoint en la página Data Sense Configuration.

"Leer más".

Para eliminar por completo la instancia de Cloud Data Sense, puede eliminar manualmente la instancia de Data Sense del portal de su proveedor de cloud o su ubicación local.

¿Puedo personalizar el servicio según las necesidades de mi organización?

Cloud Data Sense proporciona información inmediata a sus datos. Estos conocimientos se pueden extraer y utilizar para las necesidades de su organización.

Además, Data Sense ofrece muchas formas de agregar una lista personalizada de "datos personales" que el sensor de datos identificará en los análisis, lo que le proporciona una imagen completa sobre dónde residen los datos potencialmente confidenciales en los archivos de su organización.

- Puede agregar identificadores únicos basados en columnas específicas en las bases de datos que está explorando. Llamamos a esto **Data Fusion**.
- Puede agregar palabras clave personalizadas desde un archivo de texto.
- Puede agregar patrones personalizados utilizando una expresión regular (regex).

"Leer más".

¿Puedo limitar la información de Cloud Data Sense a usuarios específicos?

Sí, Cloud Data Sense está totalmente integrado con BlueXP. Los usuarios de BlueXP sólo pueden ver información sobre los entornos de trabajo que pueden ver según sus privilegios de área de trabajo.

Además, si desea permitir que determinados usuarios sólo vean los resultados del análisis de detección de datos sin tener la capacidad de administrar la configuración de detección de datos, puede asignar a esos usuarios la función Visor de cumplimiento de normativas de la nube.

"Leer más".

¿Puede alguien acceder a los datos privados enviados entre mi navegador y Data Sense?

No Los datos privados enviados entre su navegador y la instancia de Data Sense están protegidos gracias al cifrado integral, lo que significa que NetApp y terceros no pueden leerlos. Data Sense no compartirá ningún dato ni resultado con NetApp a menos que solicite y apruebe el acceso.

¿Qué sucede si la organización en niveles de datos está habilitada en sus volúmenes de ONTAP?

Es posible que desee habilitar Cloud Data Sense en sistemas ONTAP que organice los datos inactivos en niveles en el almacenamiento de objetos. Si se habilita la organización en niveles de datos, Data Sense analiza todos los datos, tanto de los discos como de los datos inactivos organizados en niveles para el almacenamiento de objetos.

El análisis de cumplimiento de normativas no calienta los datos inactivos: Permanece frío y organizado en niveles en el almacenamiento de objetos.

¿Cloud Data Sense puede enviar notificaciones a mi organización?

Sí. Junto con la función Directivas, puede enviar alertas por correo electrónico a los usuarios de BlueXP (diariamente, semanalmente o mensualmente) o a cualquier otra dirección de correo electrónico, cuando una Política devuelva los resultados para que pueda obtener notificaciones para proteger sus datos. Más información acerca de "Normativas".

También puede descargar informes de estado desde la página Gobierno y la página Investigación que puede compartir internamente en su organización.

¿Puede Cloud Data Sense funcionar con las etiquetas AIP que he incorporado en mis archivos?

Sí. Puede administrar etiquetas AIP en los archivos que detección de datos en la nube está analizando si se ha suscrito "Protección de información de Azure (AIP)". Puede ver las etiquetas que ya están asignadas a los archivos, agregar etiquetas a los archivos y cambiar las etiquetas existentes.

"Leer más".

Tipos de sistemas y tipos de datos de origen

Las siguientes preguntas están relacionadas con los tipos de almacenamiento que se pueden analizar y los tipos de datos que se analizan.

¿Qué orígenes de datos se pueden analizar con detección de datos?

Cloud Data Sense puede analizar datos de entornos de trabajo que ha añadido al BlueXP Canvas y de muchos tipos de fuentes de datos estructuradas y no estructuradas a las que Data Sense puede acceder a través de sus redes.

Entornos de trabajo:

- Cloud Volumes ONTAP (implementado en AWS, Azure o GCP)
- Clústeres de ONTAP en las instalaciones
- Azure NetApp Files
- Amazon FSX para ONTAP
- Amazon S3

Fuentes de datos:

- Recursos compartidos de archivos que no son de NetApp
- Almacenamiento de objetos (que utiliza el protocolo S3)
- Bases de datos (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL y SAP HANA, SQL SERVER)
- Cuentas de OneDrive
- Cuentas en línea y en las instalaciones de SharePoint
- Cuentas de Google Drive

Data sense admite las versiones 3.x, 4.0 y 4.1 de NFS, y las versiones 1.x, 2.0, 2.1 y 3.0 de CIFS.

¿Existen restricciones cuando se implementa en una región gubernamental?

Cloud Data Sense es compatible cuando el conector se ha puesto en marcha en una región gubernamental (AWS GovCloud, Azure Gov o Azure DoD). Cuando se implementa de esta manera, Data Sense tiene las siguientes restricciones:

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

¿Qué fuentes de datos puedo analizar si instalo Data Sense en un sitio sin acceso a Internet?

Data Sense solo puede analizar datos de orígenes de datos locales del sitio local. En este momento, Data Sense puede analizar los siguientes orígenes de datos locales en un sitio "oscuro":

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

¿Qué tipos de archivo son compatibles?

Cloud Data SENSE analiza todos los archivos para obtener información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Cuando Data Sense detecta Información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo:

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

¿Qué tipos de datos y metadatos captura Cloud Data SENSE?

Cloud Data Sense permite ejecutar un análisis general de "asignación" o un análisis completo de "clasificación" en sus orígenes de datos. La asignación sólo ofrece una descripción general de alto nivel de los datos, mientras que la clasificación proporciona un análisis profundo de los datos. La asignación se puede realizar en sus orígenes de datos muy rápidamente porque no tiene acceso a los archivos para ver los datos dentro.

- Exploración de asignación de datos.

  El análisis de detección de datos solo analiza los metadatos. Esto resulta útil para la gestión y el gobierno generales de los datos, el dimensionamiento rápido de los proyectos, las estatales de gran tamaño y la priorización. La asignación de datos se basa en metadatos y se considera una exploración **rápida**.

  Después de un análisis rápido, puede generar un informe de asignación de datos. Este informe es una descripción general de los datos almacenados en sus orígenes de datos corporativos para ayudarle a tomar decisiones sobre la utilización de los recursos, la migración, el backup, la seguridad y los procesos de cumplimiento de normativas.

- Exploración de clasificación de datos (profunda).

  Los análisis de detección de datos utilizan protocolos estándar y permisos de solo lectura en todos los entornos. Algunos archivos se abren y se analizan en busca de datos confidenciales relacionados con el negocio, información privada y problemas relacionados con el ransomware.

  Después de un análisis completo hay muchas características adicionales de Data Sense que puede aplicar a sus datos, como ver y afinar datos en la página Investigación de datos, buscar nombres dentro de archivos, copiar, mover y eliminar archivos de origen, y mucho más.

Licencias y costes

Las siguientes preguntas están relacionadas con las licencias y los costes de uso de Cloud Data Sense.

¿Cuánto cuesta Cloud Data?

El coste de utilizar Cloud Data Sense depende de la cantidad de datos que se van a analizar. Los primeros 1 TB de datos que analiza Data Sense en un espacio de trabajo BlueXP son gratuitos durante 30 días. Después de alcanzar cualquiera de los límites, necesitará uno de los siguientes para continuar con el análisis de datos:

- Una suscripción a la lista de BlueXP Marketplace de su proveedor de la nube, o.
- A bring-your-own-license (BYOL) de NetApp

Consulte "precios" para obtener más detalles.

¿Qué sucede si he alcanzado el límite de capacidad de su licencia?

Si alcanza un límite de capacidad BYOL, Data Sense continúa ejecutándose, pero el acceso a los paneles está bloqueado para que no pueda ver información sobre ninguno de los datos analizados. Solo la página Configuration está disponible en caso de que se desee reducir la cantidad de volúmenes que se van a analizar para potencialmente traer su uso de capacidad bajo el límite de licencia. Debe renovar su licencia de BYOL para volver a obtener acceso completo a Data Sense.

Despliegue del conector

Las siguientes preguntas se refieren al conector BlueXP.

¿Qué es el conector?

Connector es un software que se ejecuta en una instancia informática dentro de su cuenta cloud o en las instalaciones, que permite a BlueXP gestionar de forma segura los recursos cloud. Debe implementar un conector para usar Cloud Data Sense.

¿Dónde se debe instalar el conector?

- Cuando se escanear datos en Cloud Volumes ONTAP en AWS, Amazon FSX para ONTAP o en bloques AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.
- Al analizar datos en Cloud Volumes ONTAP en GCP, se utiliza un conector en GCP.
- Al analizar datos en sistemas ONTAP en las instalaciones, recursos compartidos de archivos que no son de NetApp, almacenamiento de objetos S3 genérico, bases de datos, carpetas de OneDrive, cuentas de SharePoint y cuentas de Google Drive, puede utilizar un conector en cualquiera de estas ubicaciones de cloud.

Por tanto, si tiene datos en muchas de estas ubicaciones, es posible que tenga que utilizarlos "Múltiples conectores".

¿Puedo desplegar el conector en mi propio host?

Sí. Puede hacerlo "Ponga en marcha el conector en las instalaciones" En un host Linux en su red o en la nube. Si tiene pensado poner en marcha Data Sense en las instalaciones, es posible que también desee

instalar el conector en las instalaciones; pero no es necesario.

¿Qué pasa con sitios seguros sin acceso a Internet?

Sí, también es compatible. Puede hacerlo "Implemente el conector en un host Linux local que no tenga acceso a Internet". Después puede detectar clústeres de ONTAP en las instalaciones y otros orígenes de datos locales y analizar los datos con Data Sense.

Puesta en marcha de detección de datos

Las siguientes preguntas se refieren a la instancia de detección de datos independiente.

¿Qué modelos de implementación son compatibles con Cloud Data Sense?

BlueXP permite al usuario analizar y generar informes sobre sistemas prácticamente en cualquier parte, incluidos entornos locales, de cloud e híbridos. Cloud Data SENSE se implementa normalmente mediante un modelo SaaS, en el que el servicio se activa a través de la interfaz BlueXP y no requiere ninguna instalación de hardware o software. Incluso en este modo de puesta en marcha con un clic y una ejecución, la gestión de datos se puede realizar sin importar si los almacenes de datos están en las instalaciones o en el cloud público.

¿Qué tipo de instancia o máquina virtual se requiere para Cloud Data Sense?

Cuando "implementado en el cloud":

- En AWS, Cloud Data Sense se ejecuta en una instancia de mp5.4 x grande con un disco GP2 de 500 GB.
- En Azure, Cloud Data Sense se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 512 GB.
- En GCP, Cloud Data Sense se ejecuta en una máquina virtual n2-estándar-16 con un disco persistente estándar de 512 GB.

Tenga en cuenta que puede implementar la detección de datos en un sistema con menos CPU y menos RAM, pero existen limitaciones al utilizar estos sistemas. Consulte "Con un tipo de instancia más pequeño" para obtener más detalles.

"Obtenga más información sobre el funcionamiento de Cloud Data Sense".

¿Puedo implementar el sentido de los datos en mi propio host?

Sí. Puede instalar el software Data Sense en un host Linux que tenga acceso a Internet en su red o en la nube. Todo funciona igual y continúa gestionando la configuración de exploración y los resultados a través de BlueXP. Consulte "Poner en marcha el sentido de datos en el cloud en las instalaciones" para conocer los requisitos del sistema y los detalles de la instalación.

¿Qué pasa con sitios seguros sin acceso a Internet?

Sí, también es compatible. Puede hacerlo "Ponga en marcha la detección de datos en un sitio en las instalaciones que no tenga acceso a Internet" para ubicaciones completamente seguras.