Active el análisis en sus orígenes de datos

Cloud Data Sense

NetApp
March 08, 2023

This PDF was generated from https://docs.netapp.com/es-es/cloud-manager-data-sense/task-getting-started-compliance.html on March 08, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

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".

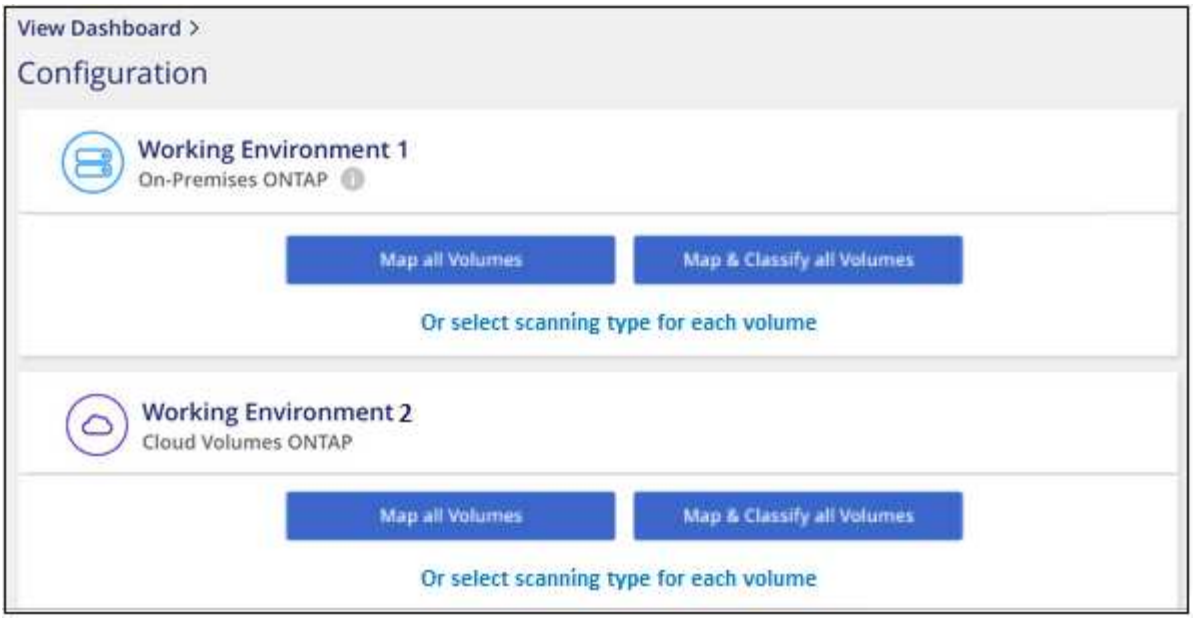
Si está escaneando en las instalaciones sistemas ONTAP que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Implemente Cloud Data Sense en la misma ubicación en las instalaciones que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue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

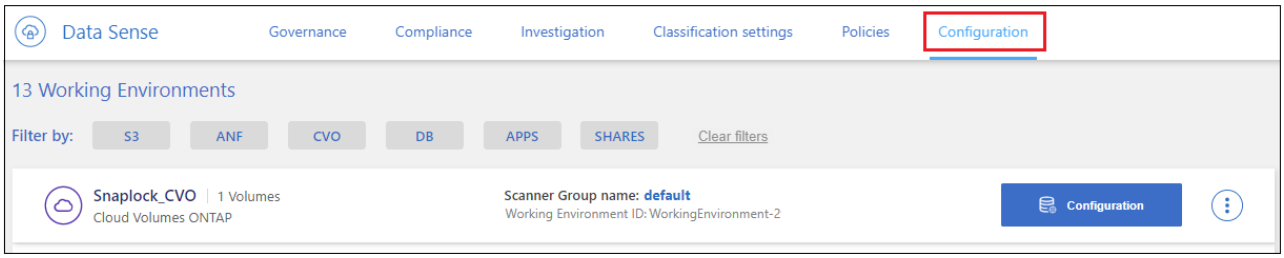
volúmenes para clústeres Cloud Volumes ONTAP o ONTAP en las instalaciones.

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**.

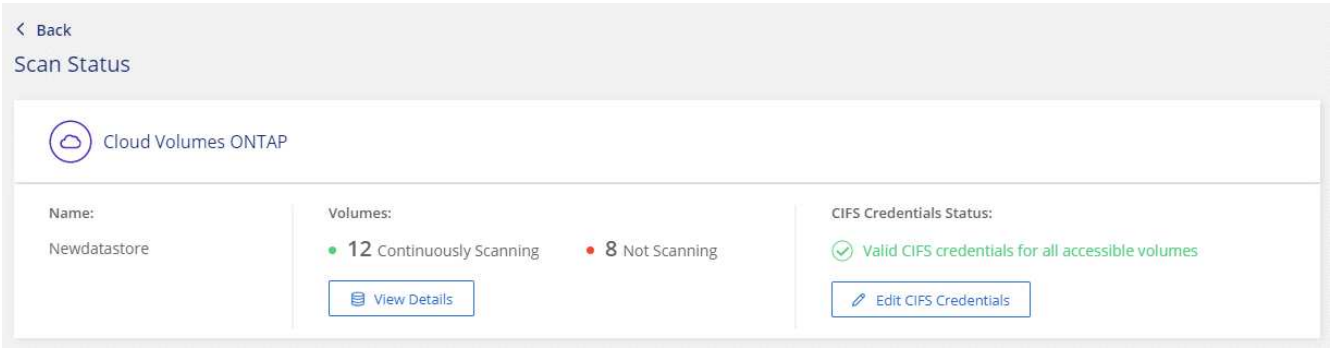


   b. Para cada entorno de trabajo, haga clic en **Editar credenciales CIFS** e introduzca el nombre de usuario y la contraseña que necesita Data Sense para acceder a los volúmenes CIFS en el sistema.

      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.

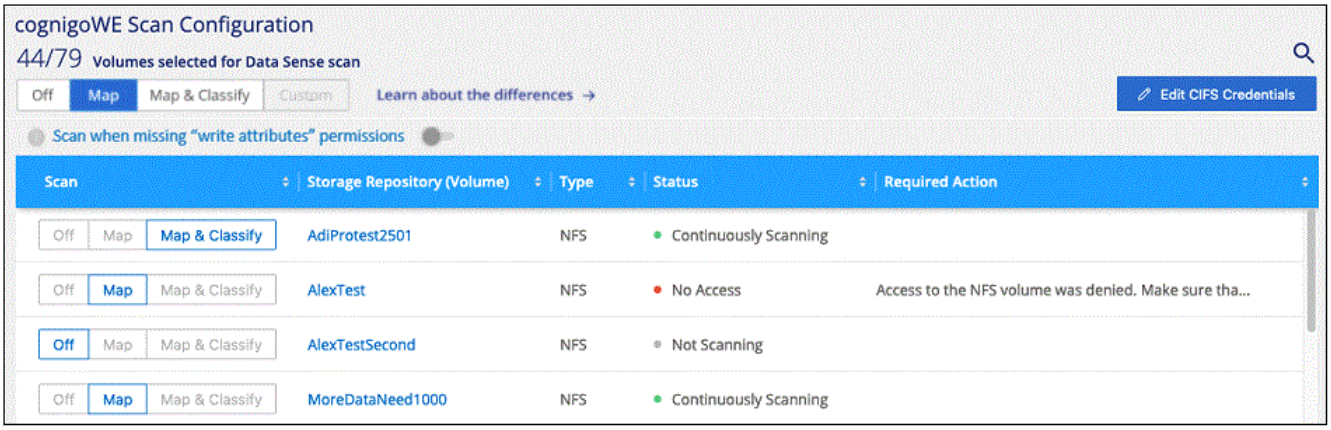
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario 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.

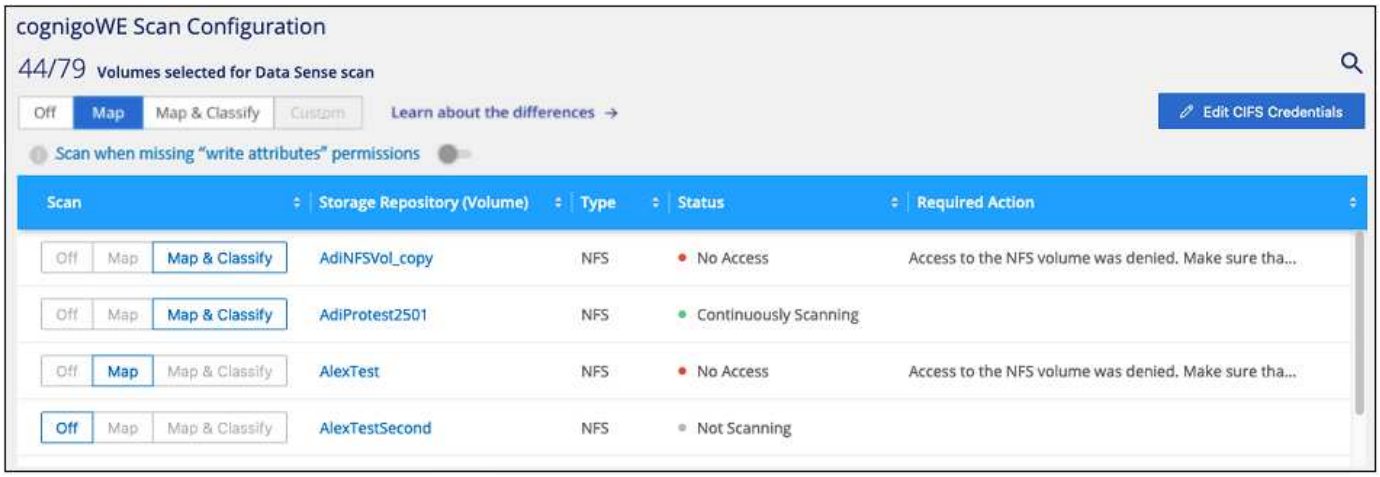
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes; uno de los cuales no puede analizar Cloud Data Sense debido a problemas de conectividad de red entre la instancia de detección de datos y el volumen.



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**

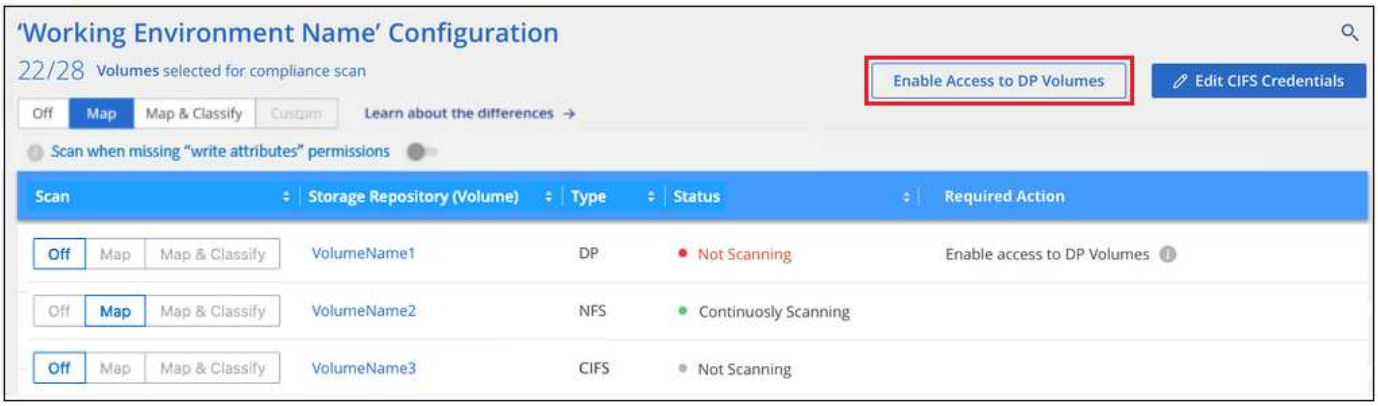
Para:	Haga lo siguiente:
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**
Active análisis de sólo asignación en todos los volúmenes	En el área de encabezado, haga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

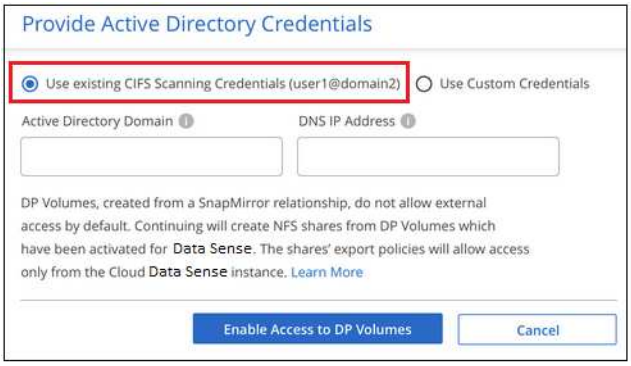


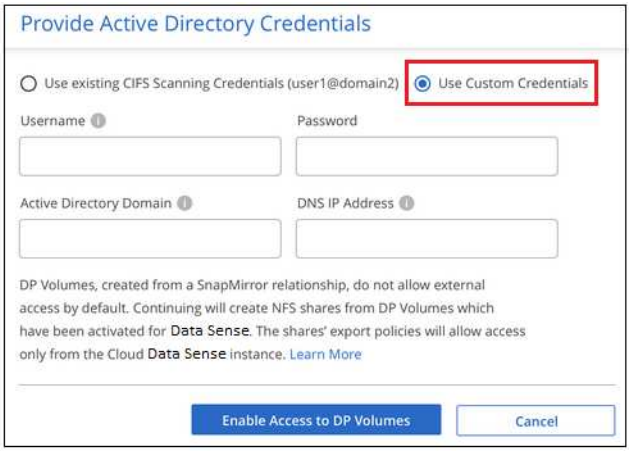
Pasos

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.

1 Descubra los sistemas Azure NetApp Files que desea analizar

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

2 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.

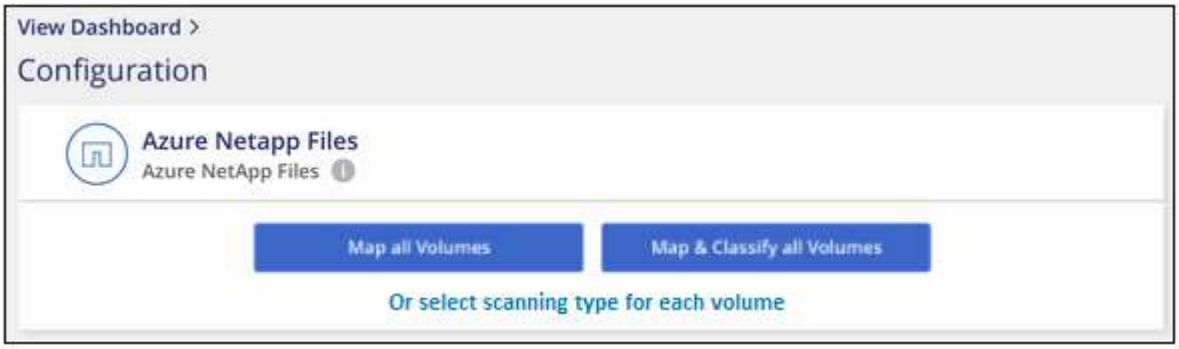
Nota: actualmente no se admite la implementación de la detección de datos en la nube en una ubicación local al analizar volúmenes Azure NetApp Files.

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.

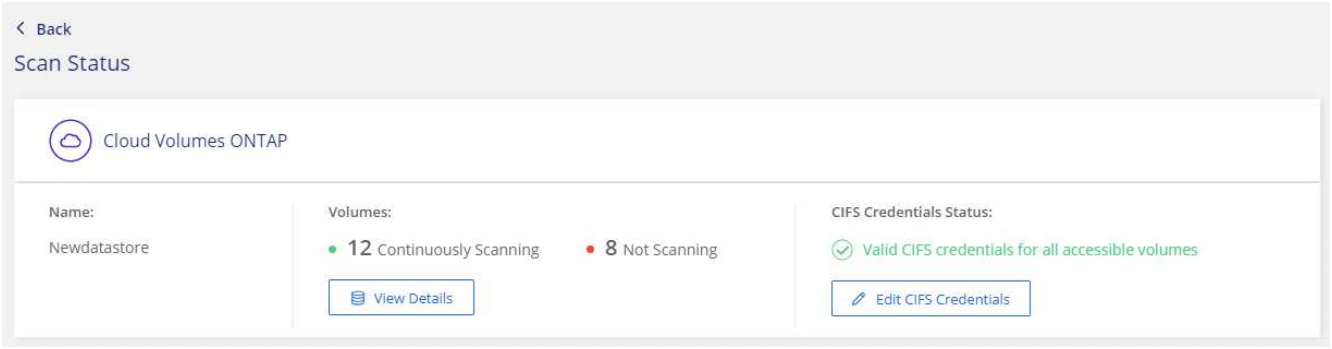
   a. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y seleccione la ficha **Configuración**.

   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.

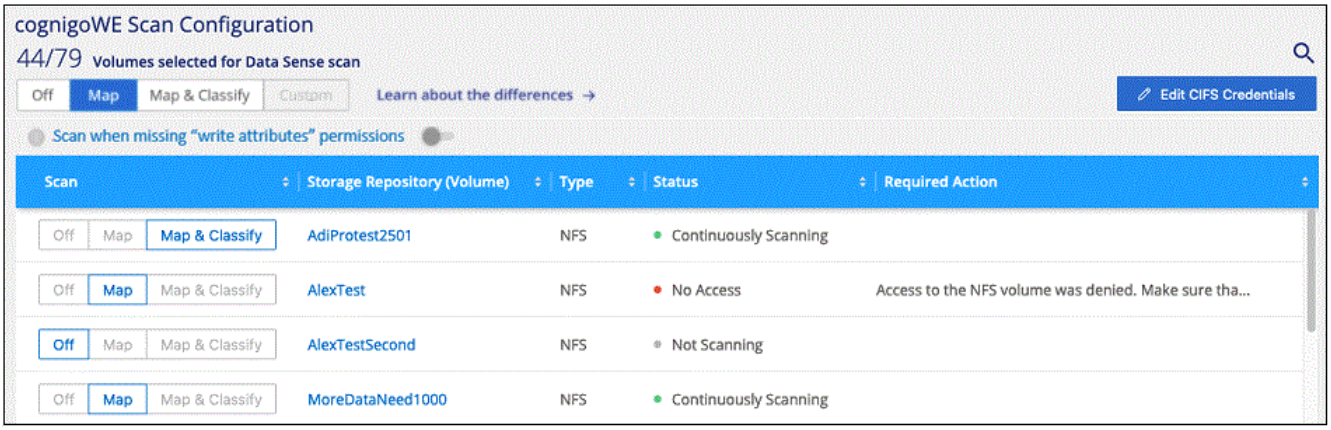
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario 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.

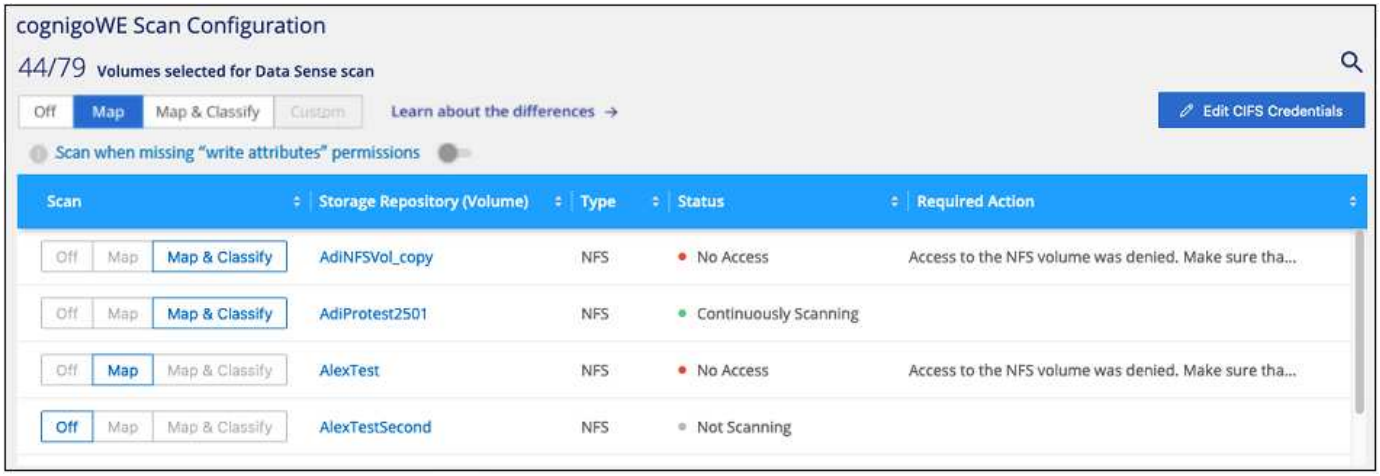
   Por ejemplo, la siguiente imagen muestra cuatro volúmenes; uno de los cuales no puede analizar Cloud Data Sense debido a problemas de conectividad de red entre la instancia de detección de datos y el volumen.



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.

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".

Ponga en marcha la instancia de Cloud Data Sense

"Ponga en marcha Cloud Data Sense en BlueXP" 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 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.

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.

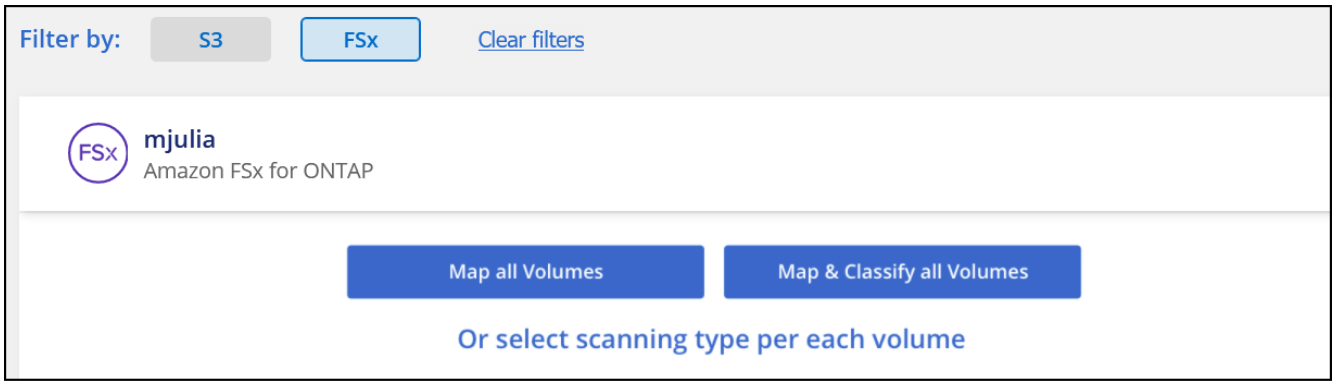
Nota: actualmente no se admite la implementación de Cloud Data Sense en una ubicación en las instalaciones al analizar volúmenes FSX.

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

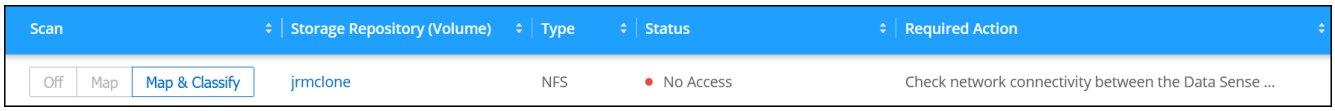
Asegúrese de que Cloud Data Sense pueda acceder a los volúmenes mediante la comprobación de las redes, los grupos de seguridad y las políticas de exportación.

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.

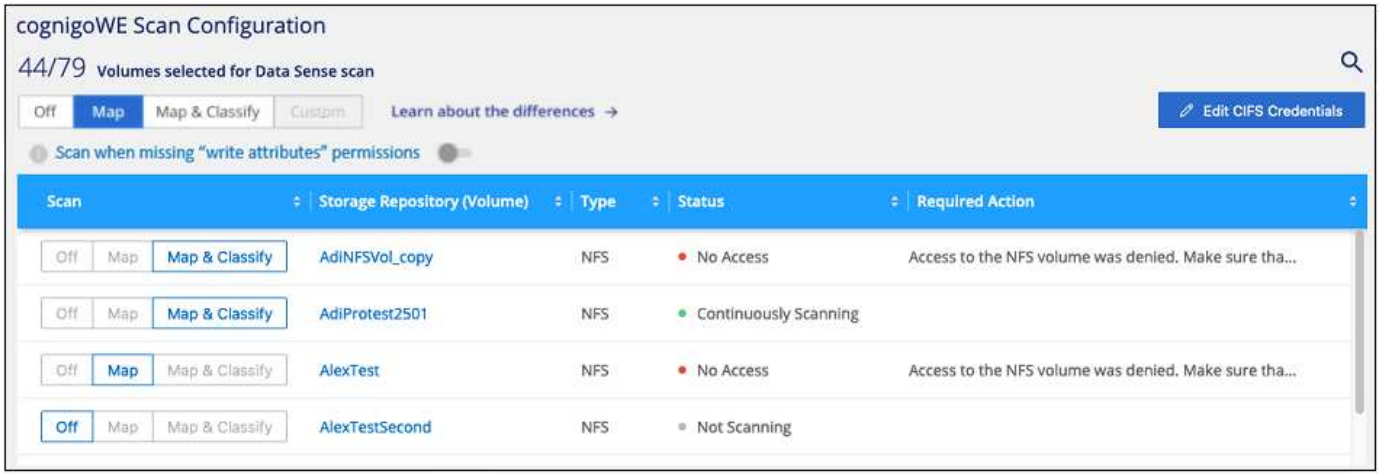
      Si desea asegurarse de que los análisis de clasificación de detección de datos no modifican sus archivos “horas a las que se accedió por última vez”, recomendamos que el usuario tenga permisos de atributos de escritura en CIFS o permisos de escritura en NFS. Si es posible, recomendamos que el usuario 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".



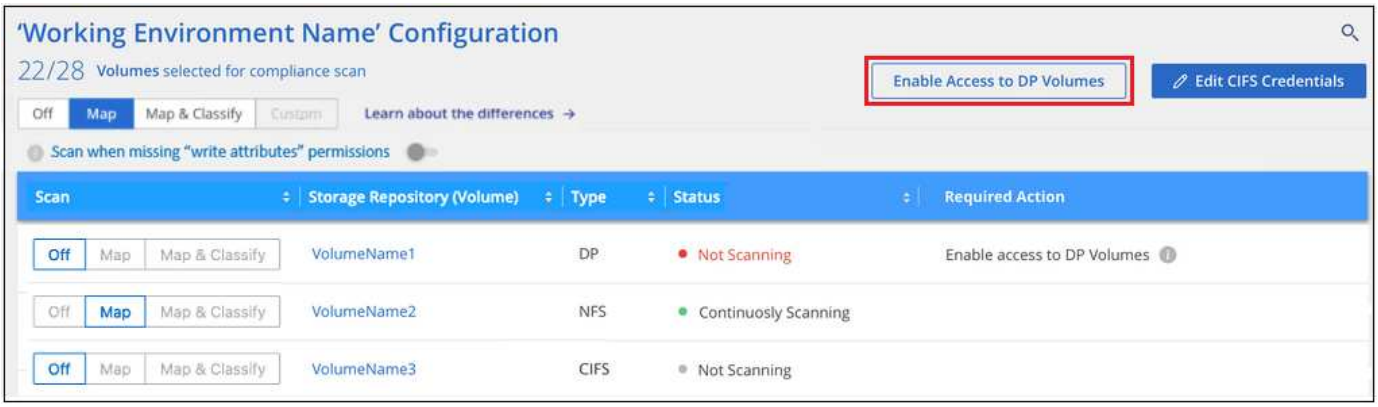
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en un volumen	En el área de volumen, haga clic en **Mapa**
Active el análisis completo en un volumen	En el área de volumen, haga clic en **Mapa y clasificación**
Desactive el análisis en un volumen	En el área de volumen, haga clic en **Desactivado**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

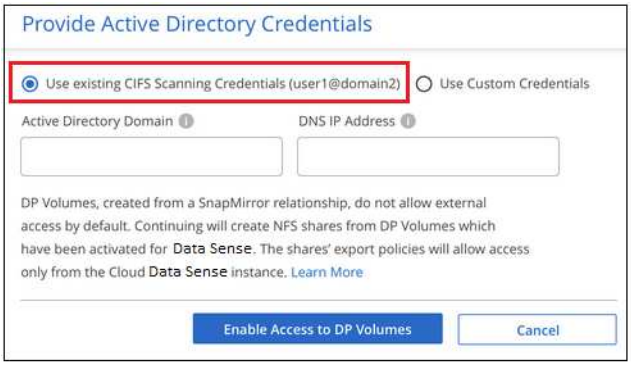
Inicialmente, la lista de volúmenes identifica estos volúmenes como *Type* **DP** con el *Status* **no Scanning** y el *Required Action* **Enable Access to DP Volumes**.

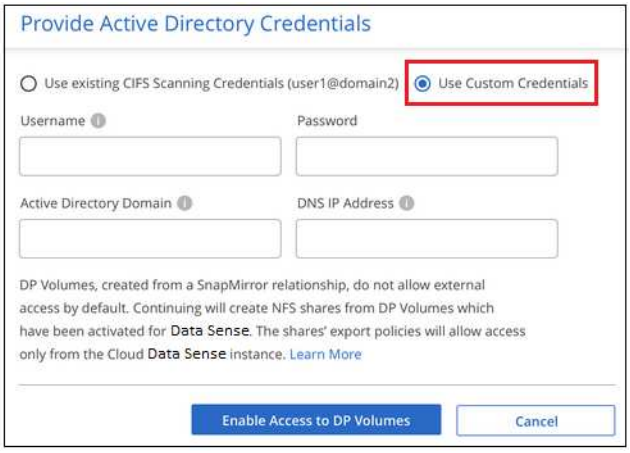


Pasos

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.

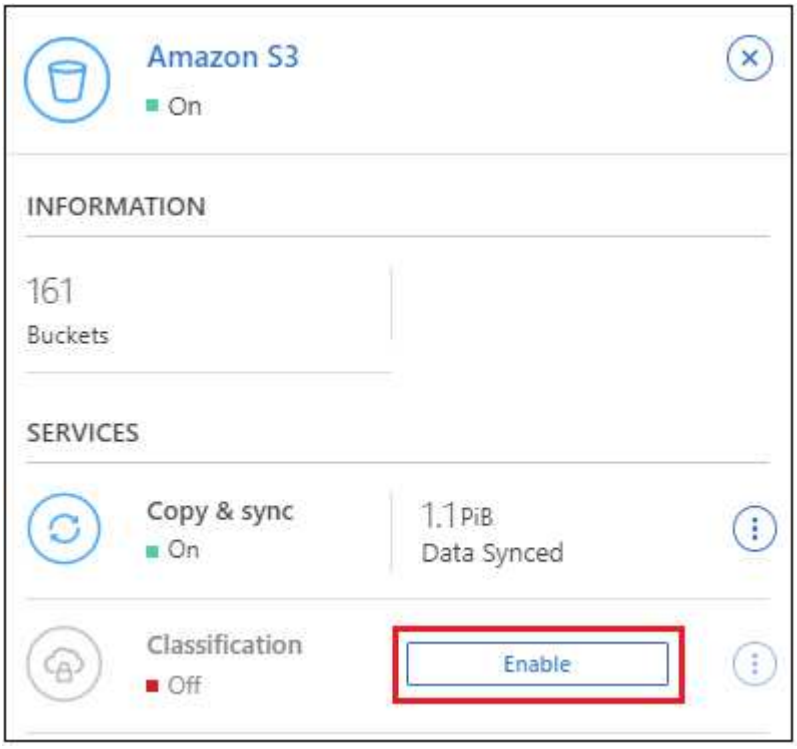
Activar el sentido de datos en su entorno de trabajo de S3

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

Pasos

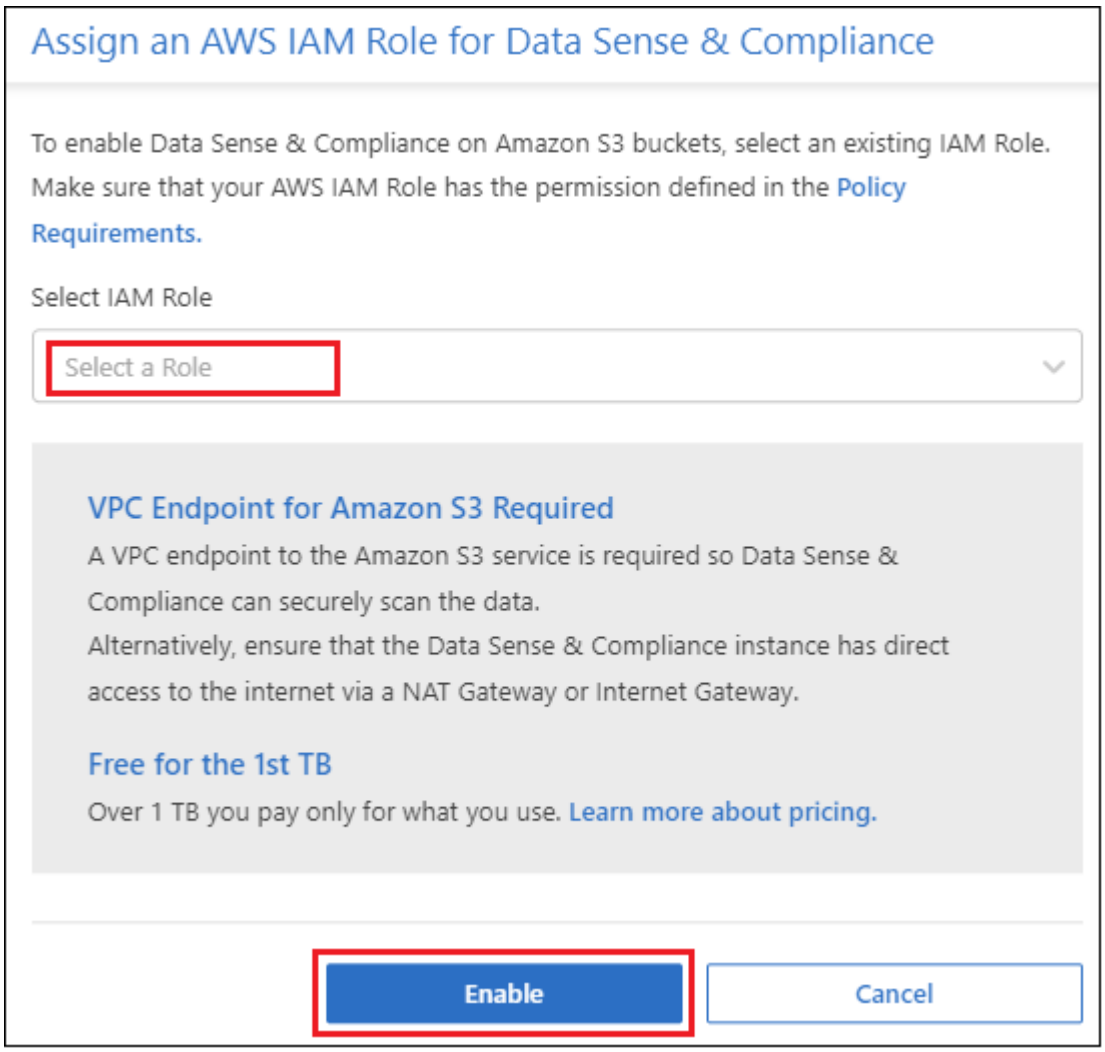
1. En el menú de navegación izquierdo de BlueXP, haga clic en **almacenamiento > lienzo**.
2. Seleccione el entorno de trabajo de Amazon S3.

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

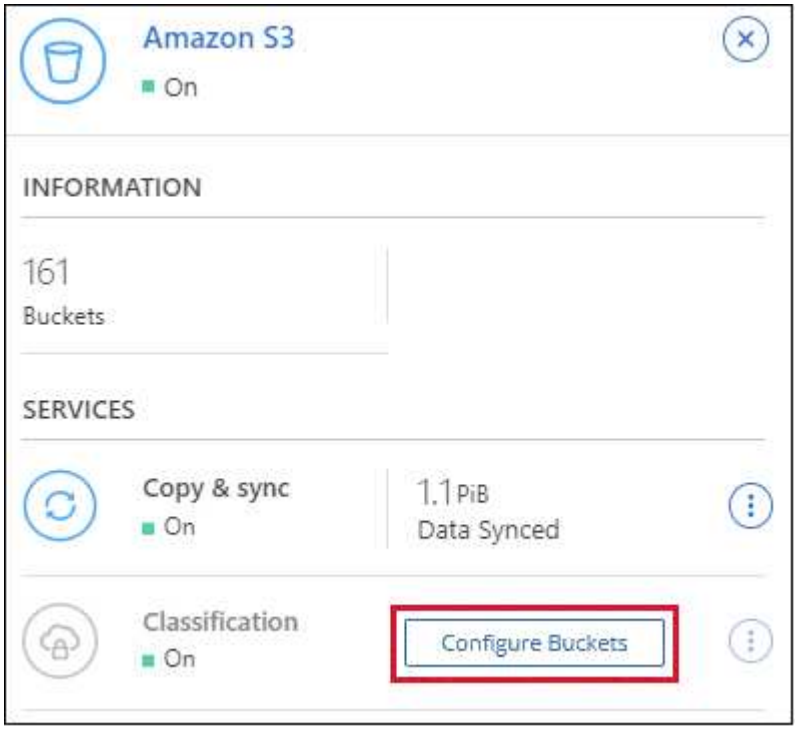
Después de que BlueXP habilita Cloud Data Sense en Amazon S3, el paso siguiente es configurar los bloques que desea analizar.

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.

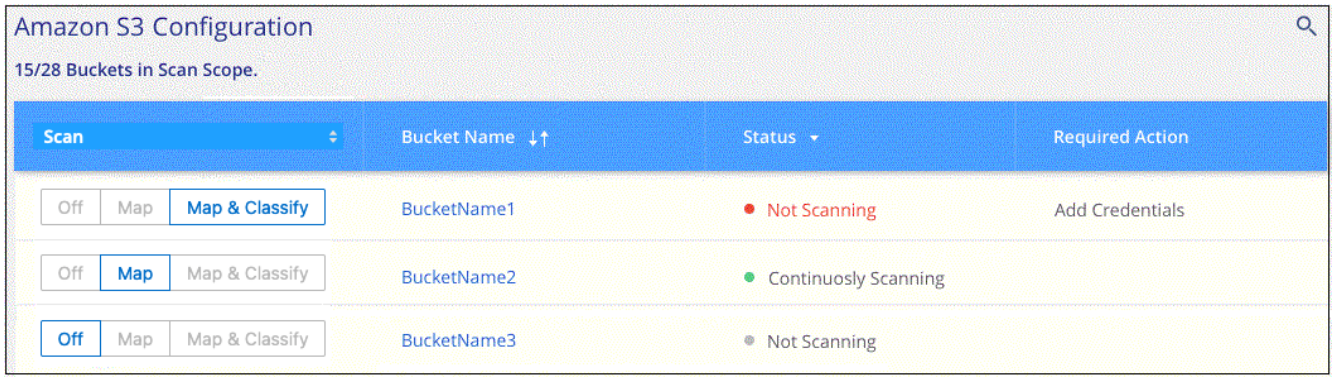
El sentido de los datos en cloud también puede ser Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS.

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

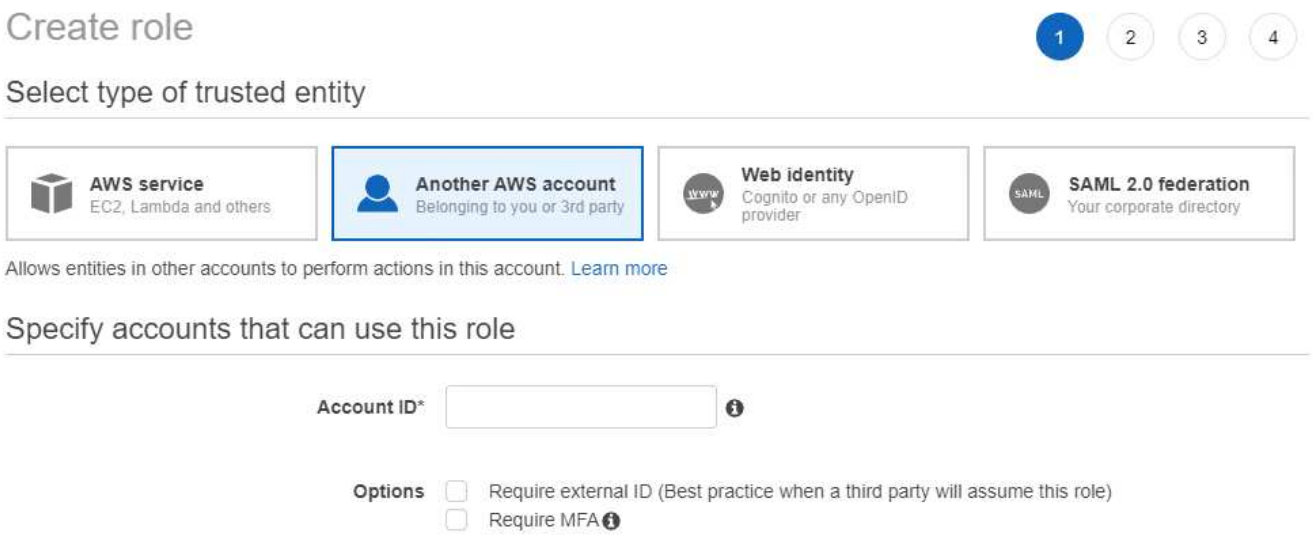
Cloud Data Sense comienza a analizar los cubos de S3 que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

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.

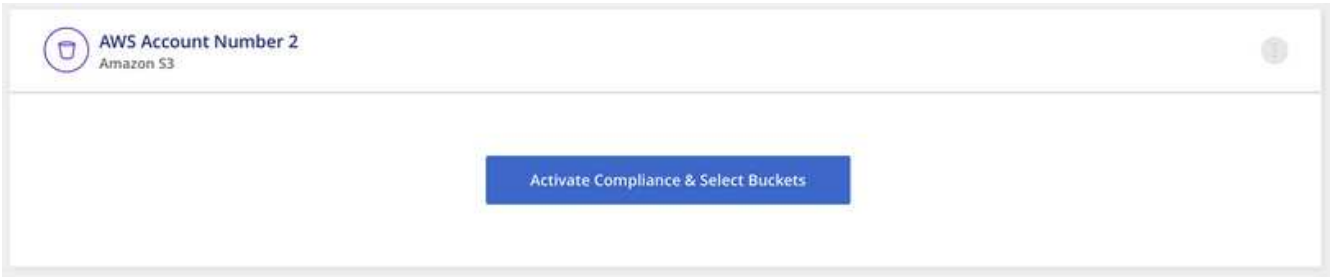
b. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.

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".

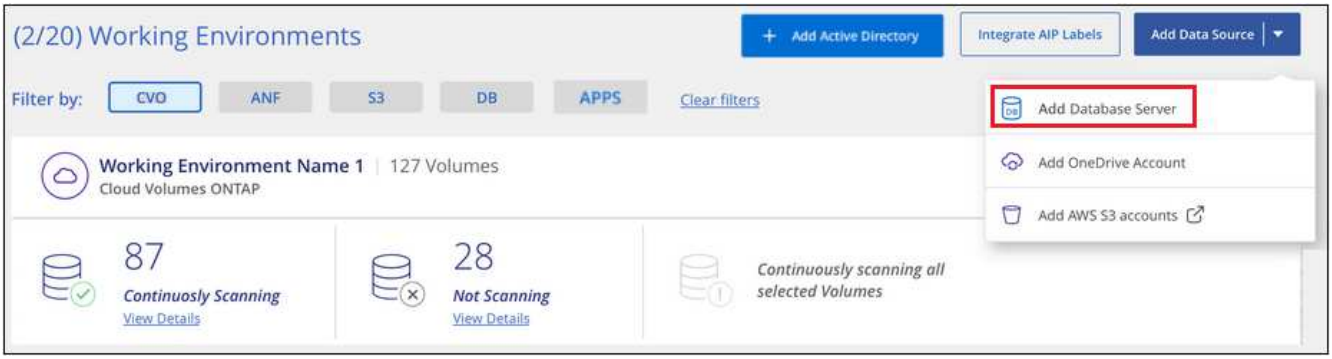
Si está analizando esquemas de base de datos que se han instalado en un sitio oscuro que no tiene acceso a Internet, debe hacerlo "Implemente Cloud Data Sense en la misma ubicación en las instalaciones que no tiene acceso a Internet". Esto también requiere que el conector BlueXP se despliegue en esa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

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

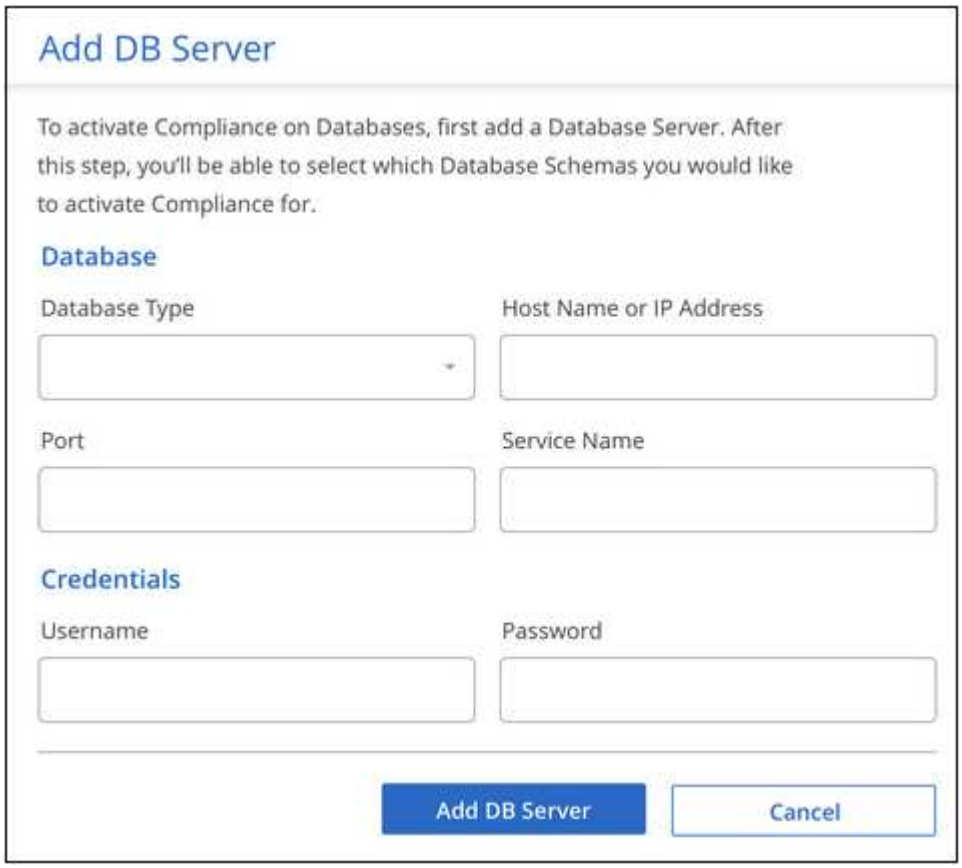
Agregando el servidor de la base de datos

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.

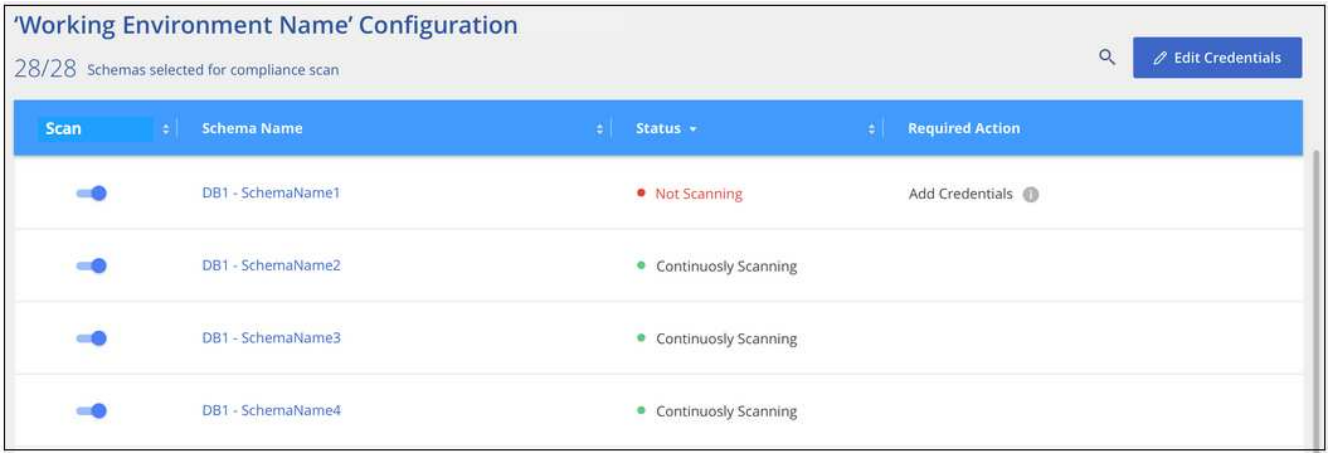
Habilitar y deshabilitar los análisis de cumplimiento de normativas en esquemas de base de datos

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.

1 Revise los requisitos previos de OneDrive

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

2 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.

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.

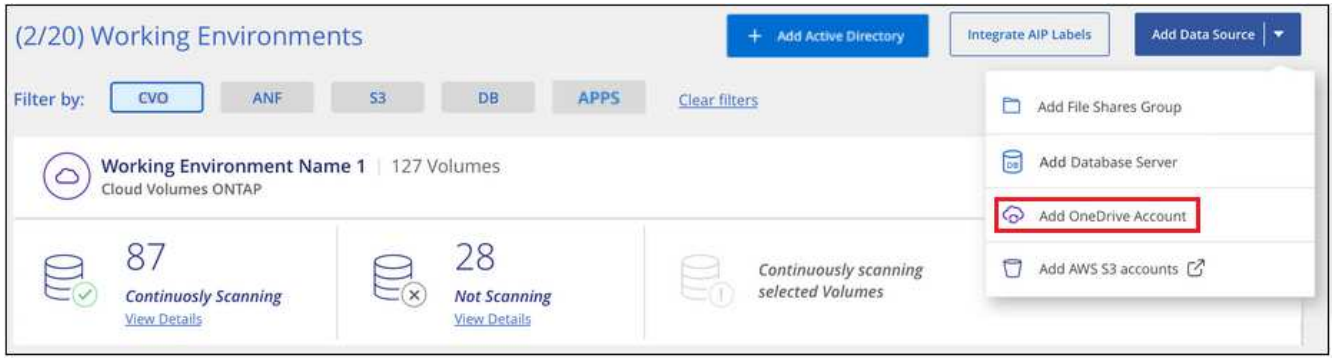
La detección de datos también puede ser "se implementa en una ubicación local que no tiene acceso a internet". Sin embargo, deberá proporcionar acceso a Internet a unos pocos extremos seleccionados para analizar sus archivos de OneDrive locales. "Consulte la lista de puntos finales necesarios aquí".

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.

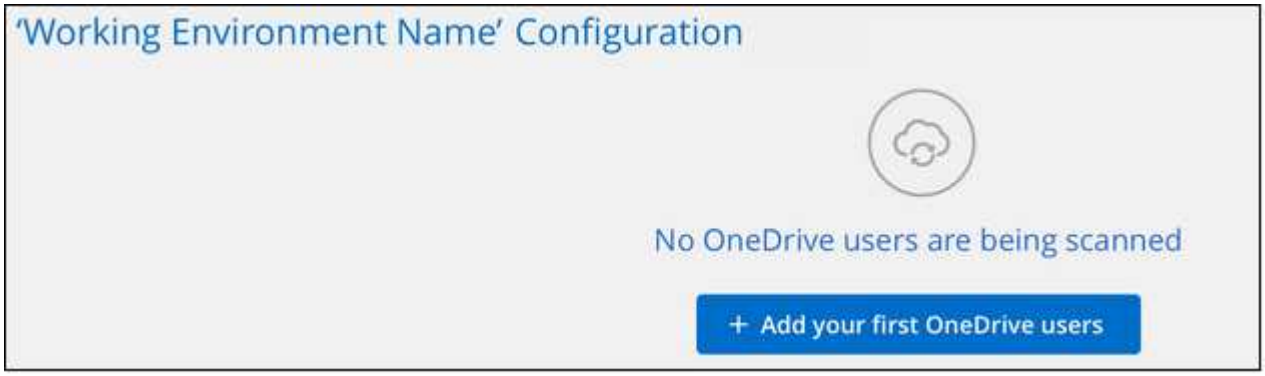
Añadir usuarios de OneDrive a los análisis de cumplimiento de normativas

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

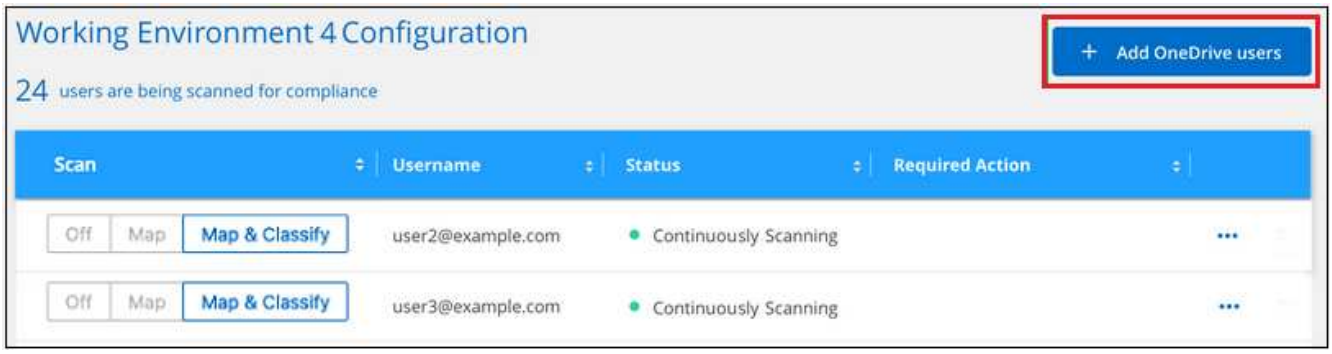
Pasos

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

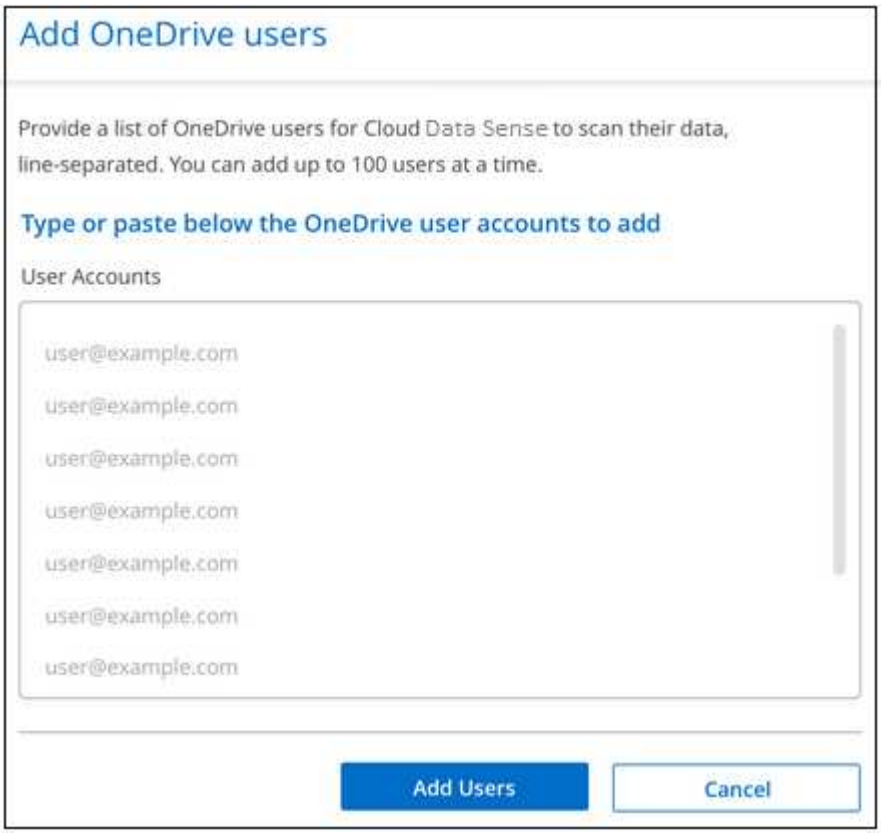
2. Si es la primera vez que añade usuarios para esta cuenta de OneDrive, haga clic en **Agregar sus primeros usuarios de OneDrive**.



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**

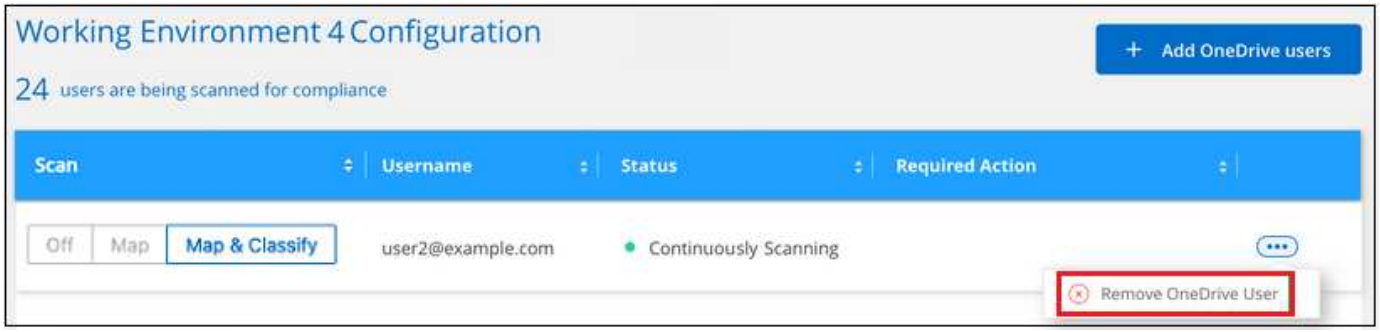
Para:	Haga lo siguiente:
Desactive el análisis en archivos de usuario	Haga clic en **Desactivado**

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".

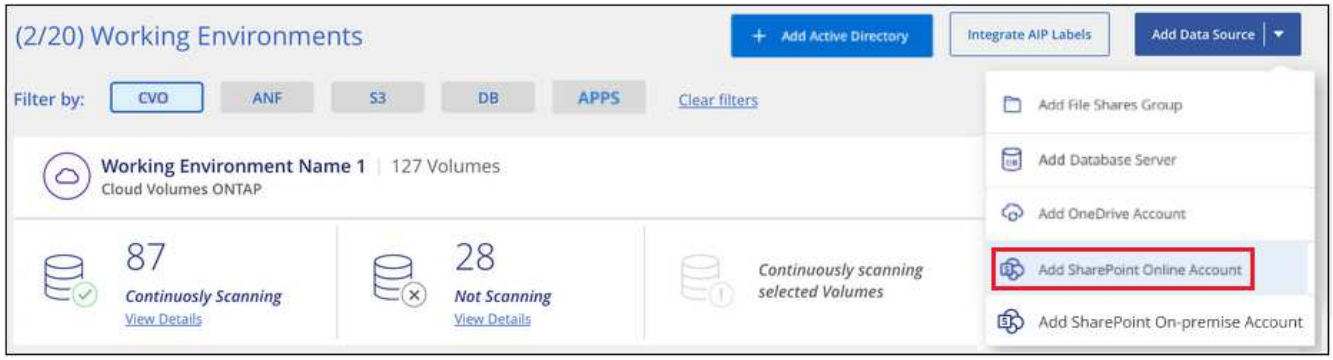
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

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.

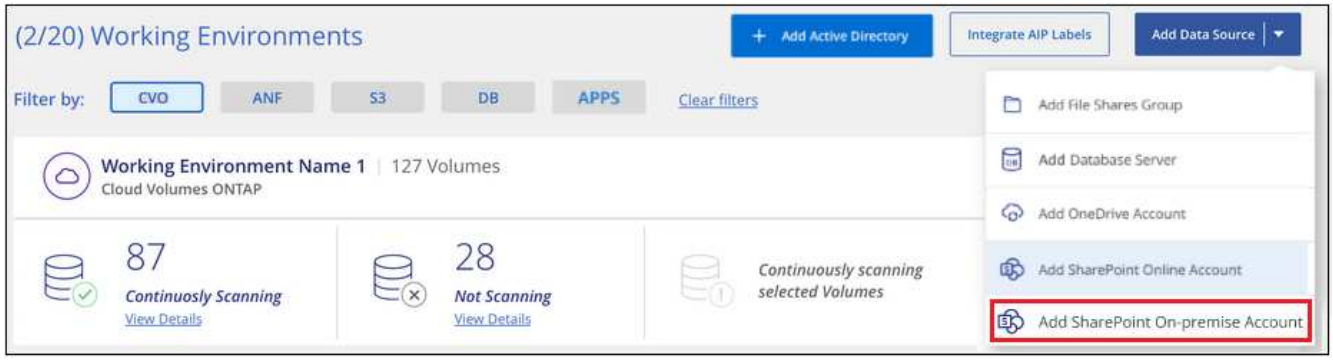
La cuenta de SharePoint Online se agrega a la lista de entornos de trabajo.

Adición de una cuenta de SharePoint en las instalaciones

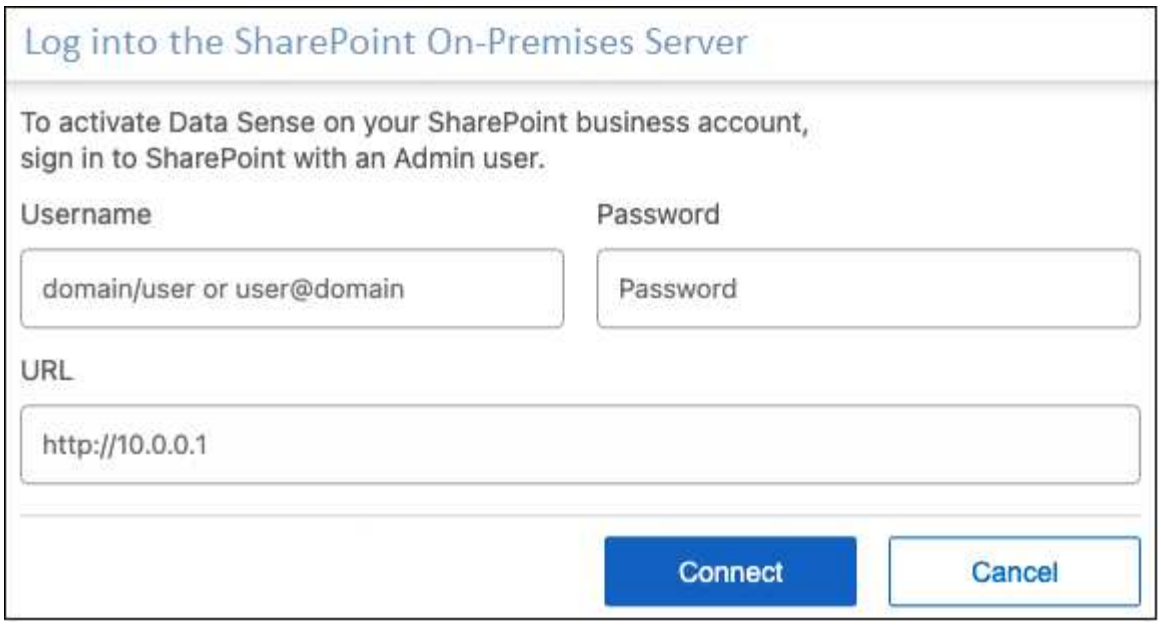
Agregue la cuenta de SharePoint en las instalaciones donde residen los archivos de usuario.

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.

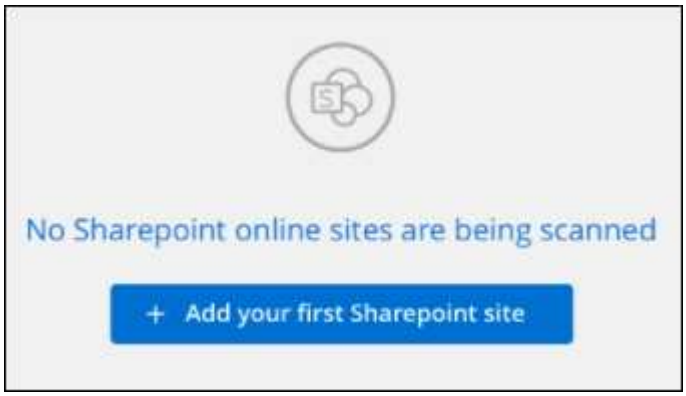
Agregar sitios de SharePoint a los análisis de cumplimiento

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

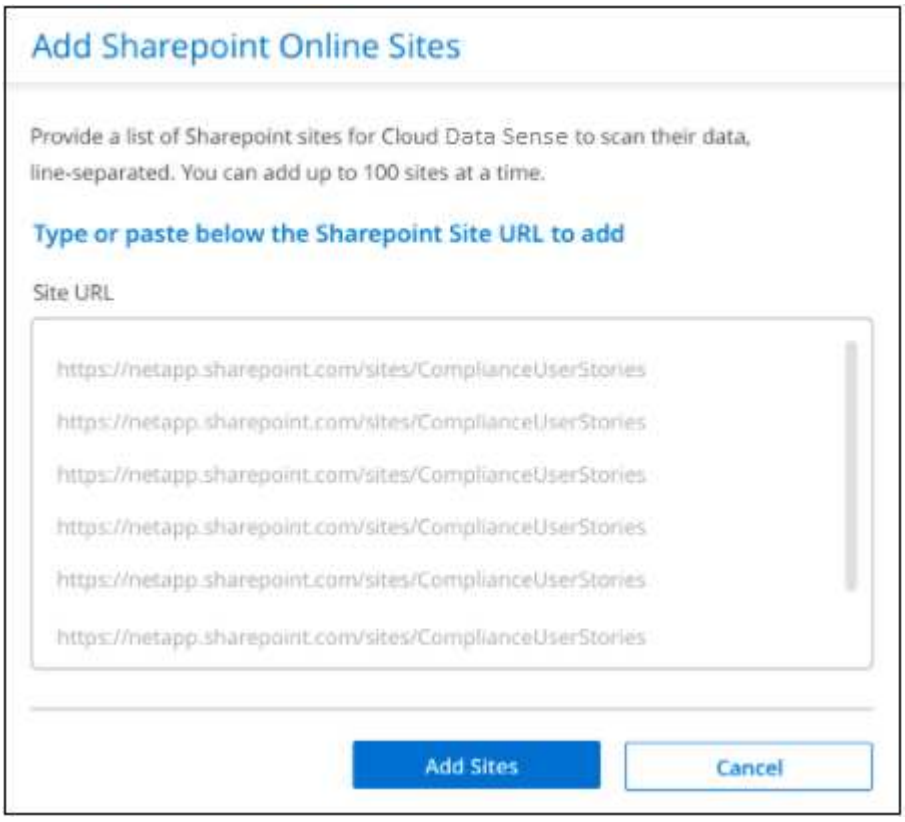
1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de SharePoint.

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.

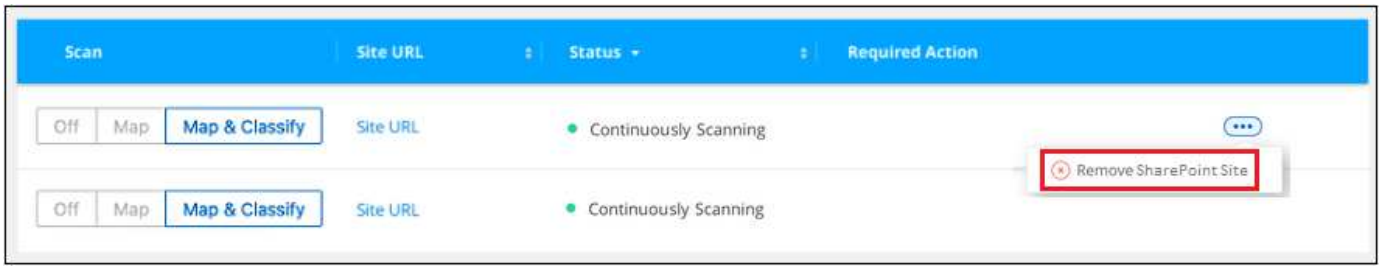
Para:	**Haga lo siguiente:**
Active los análisis de sólo asignación en archivos	Haga clic en **Mapa**
Active los análisis completos en los archivos	Haga clic en **Mapa y clasificación**
Desactive el análisis en archivos	Haga clic en **Desactivado**

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".

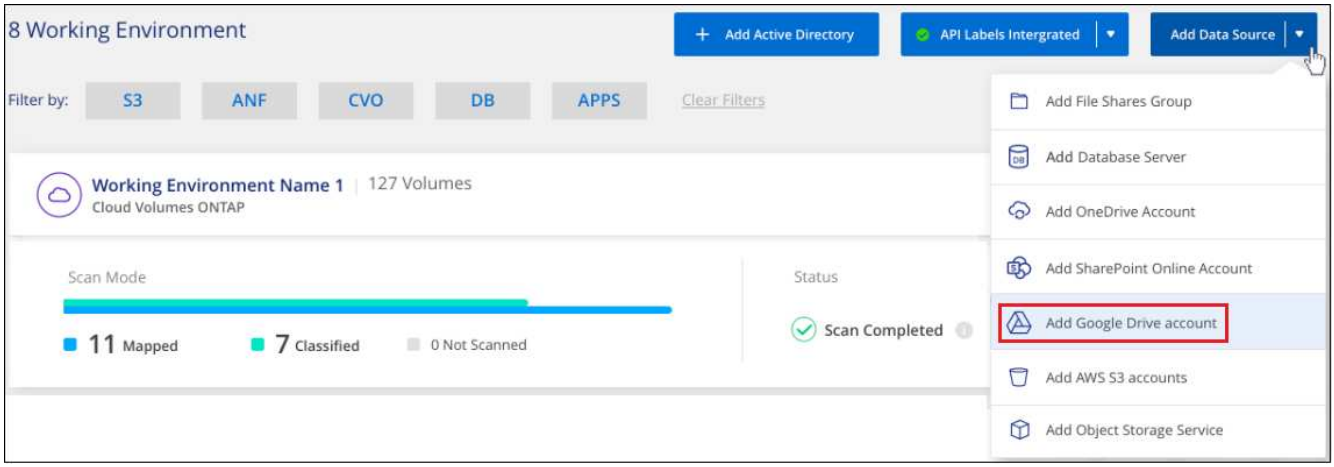
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

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.

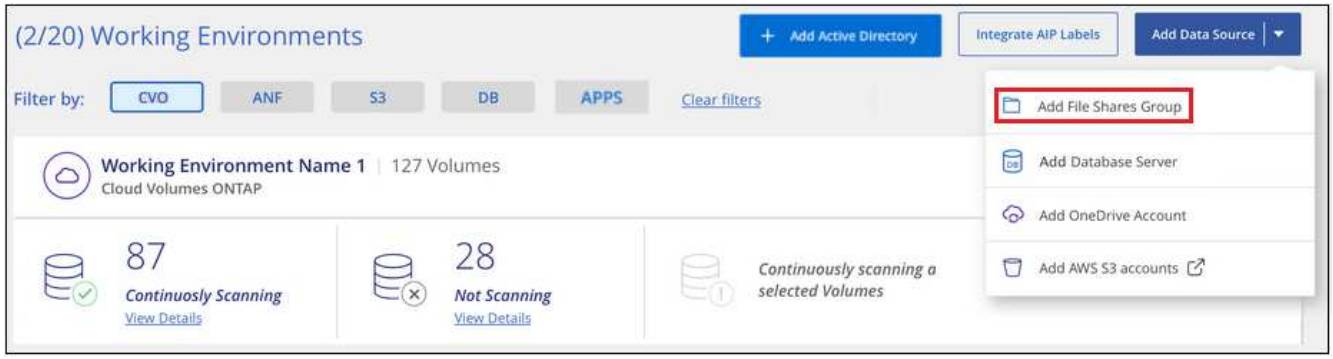
Creación del grupo para los recursos compartidos de archivos

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>`.

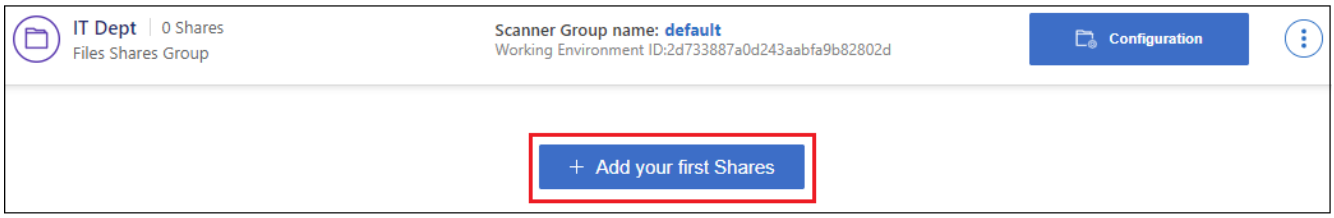
Puede agregar recursos compartidos de archivos individuales o puede proporcionar una lista separada por líneas de los recursos compartidos de archivos que desea analizar. Puede añadir hasta 100 recursos compartidos al mismo tiempo.

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.

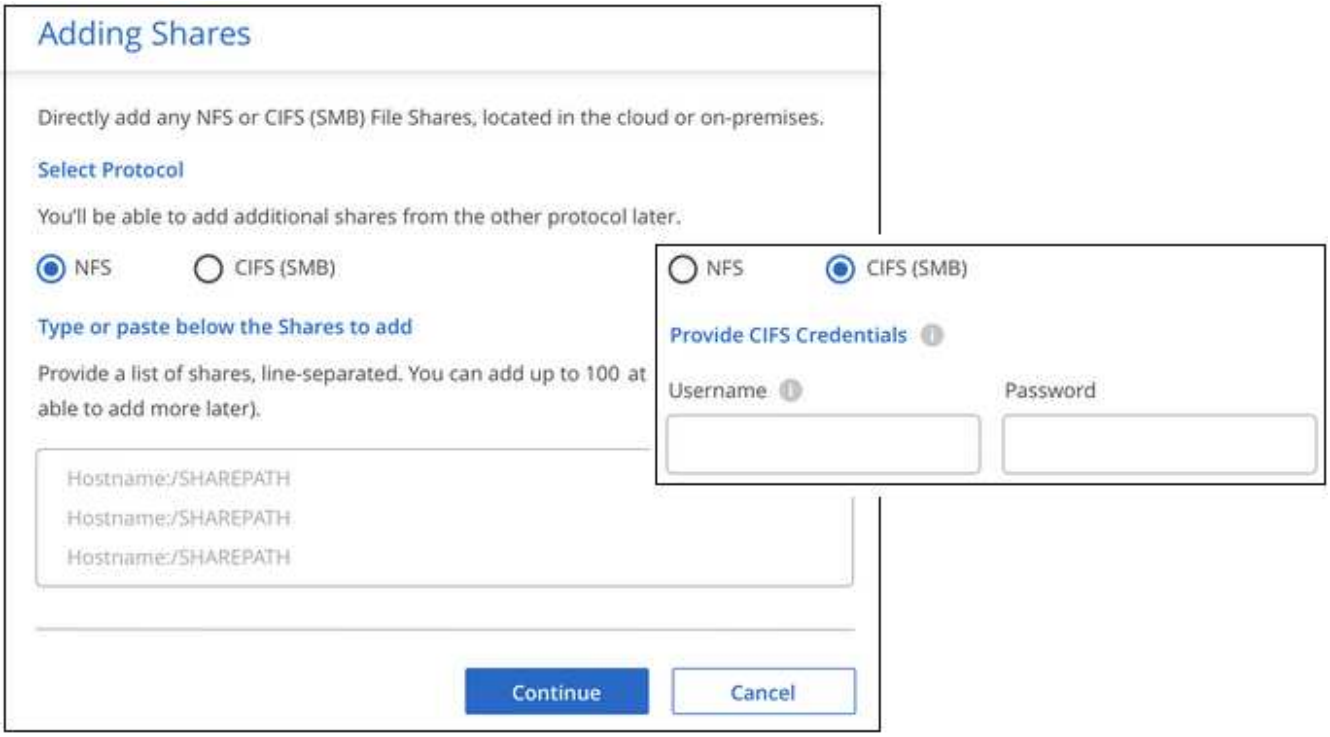
2. Si es la primera vez que añade archivos compartidos para este grupo de archivos compartidos, haga clic en **Agregar sus primeros recursos compartidos**.



   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**

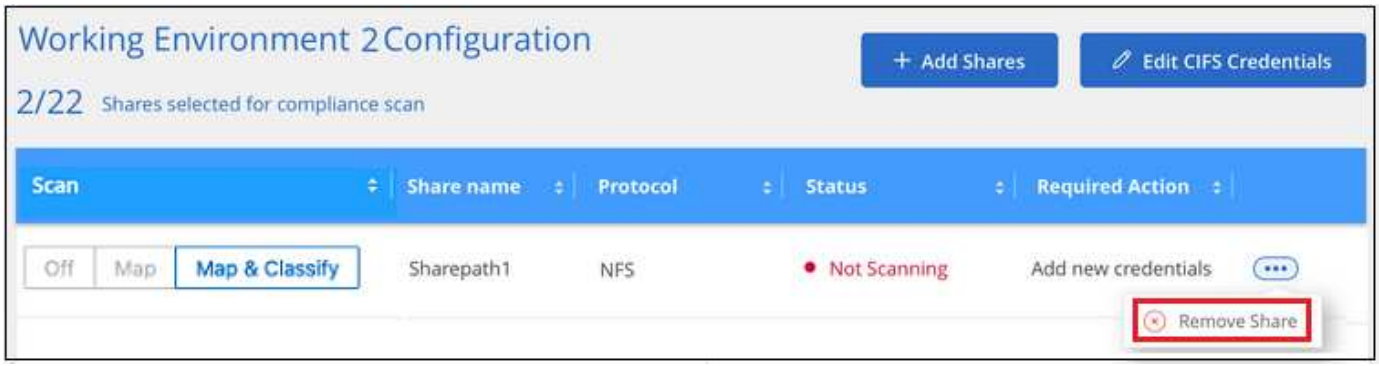
El conmutador situado en la parte superior de la página para **Buscar cuando faltan los permisos de "atributos de escritura"** está desactivado de forma predeterminada. Esto significa que si Data Sense no tiene permisos de atributos de escritura en CIFS o permisos de escritura en NFS, el sistema no analizará 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.

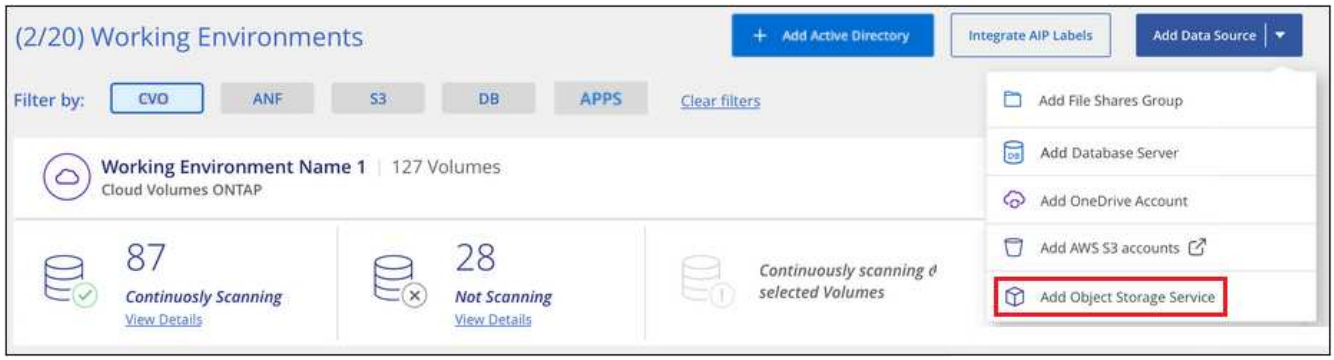
Las actualizaciones del software Data Sense se automatizan siempre que la instancia tenga conectividad a Internet.

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**.

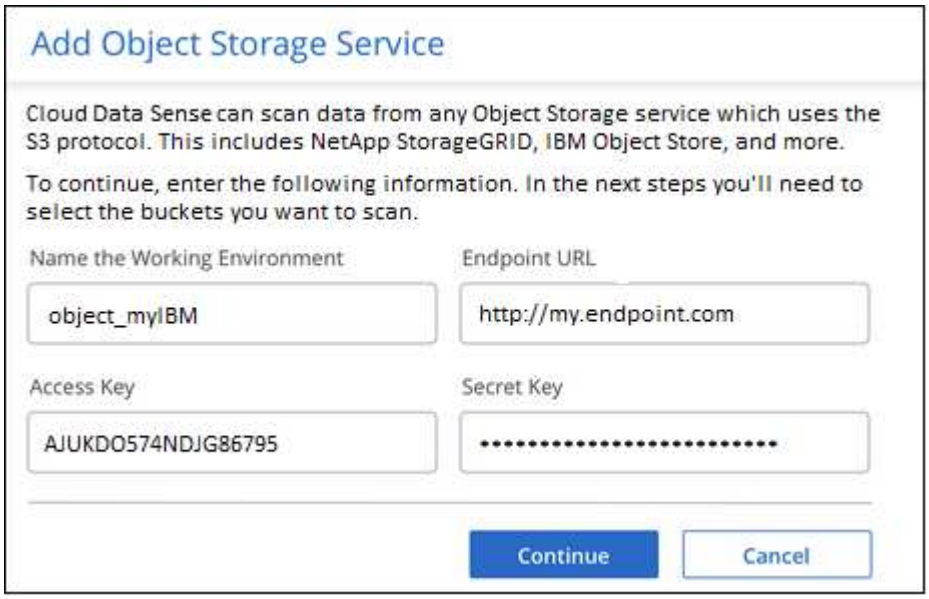


2. En el cuadro de diálogo Add Object Storage Service, introduzca los detalles del servicio de almacenamiento de objetos y haga clic en **continuar**.

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

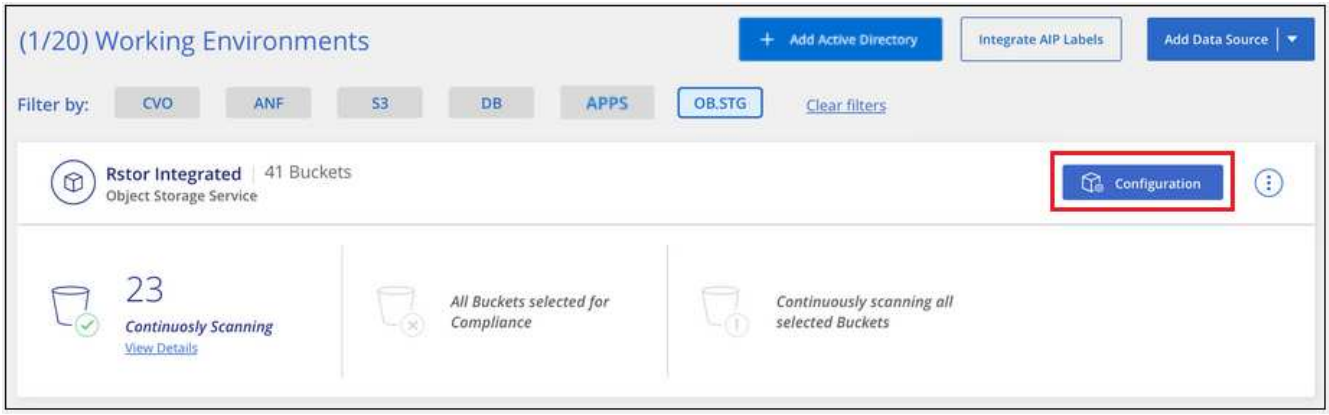
El nuevo Servicio de almacenamiento de objetos se añade a la lista de entornos de trabajo.

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

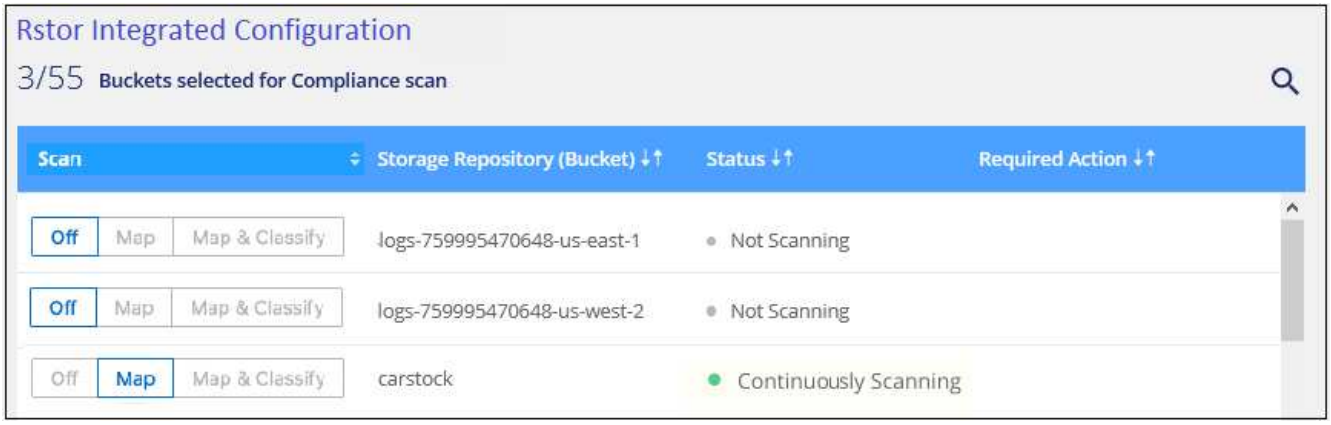
Después de habilitar Cloud Data Sense en el Servicio de almacenamiento de objetos, el siguiente paso es configurar los bloques que desea analizar. El sentido de los datos detecta esos bloques y los muestra en el entorno de trabajo que ha creado.

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.

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.