



Rastreo de depreciaciones de datos

BlueXP classification

NetApp
June 14, 2024

Tabla de contenidos

- Rastreo de depreciaciones de datos 1
 - Escanee los buckets de Amazon S3 1
 - Escanear cuentas de OneDrive 8
 - Analizar cuentas de SharePoint 12
 - Analizar cuentas de Google Drive 17
 - Analice el almacenamiento de objetos que utiliza el protocolo S3 19

Rastreo de depreciaciones de datos

Escanee los buckets de Amazon S3

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

NOTA Esta información solo es relevante para las versiones heredadas de clasificación de BlueXP 1,30 y anteriores.

Inicio rápido

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

1

Configure los requisitos de S3 en su entorno de cloud

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

2

Implementa la instancia de clasificación de BlueXP

"[Implementa la clasificación de BlueXP](#)" si aún no hay una instancia implementada.

3

Activa la clasificación de BlueXP en tu entorno de trabajo S3

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

4

Seleccione los cucharones que desea escanear

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

Revisión de los requisitos previos de S3

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

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

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

```

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

```

Proporciona conectividad desde la clasificación de BlueXP a Amazon S3

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

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

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

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



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

Implementar la instancia de clasificación de BlueXP

["Implementa la clasificación de BlueXP en BlueXP"](#) si aún no hay una instancia implementada.

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

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

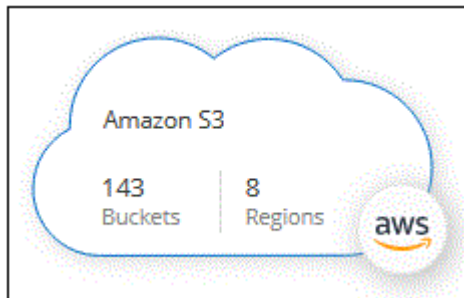
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Activar la clasificación de BlueXP en tu entorno de trabajo S3

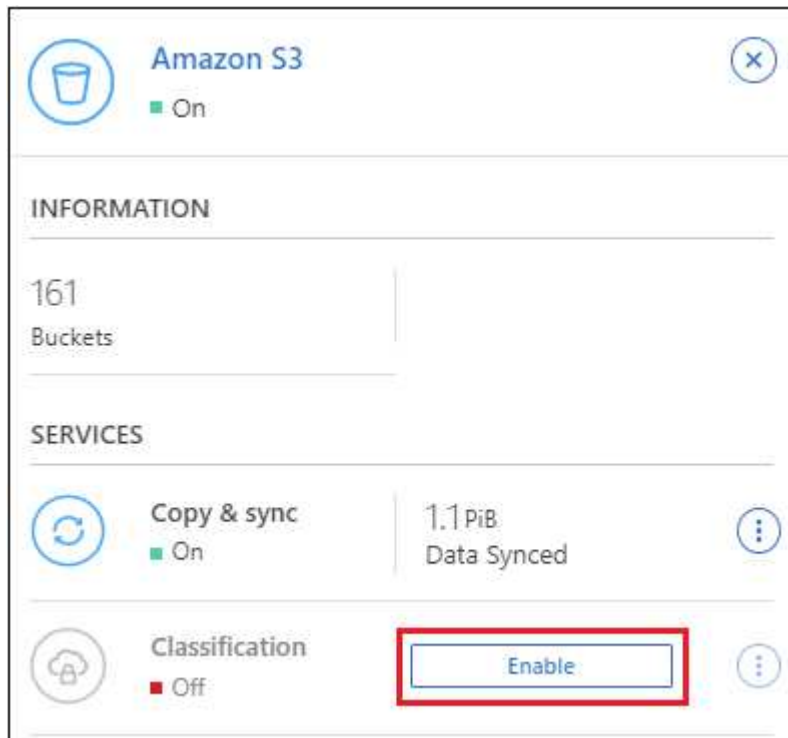
Habilita la clasificación de BlueXP en Amazon S3 después de verificar los requisitos previos.

Pasos

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



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



4. Cuando se le solicite, asigne un rol de IAM a la instancia de clasificación de BlueXP que tenga [los](#)

permisos necesarios.

Assign an AWS IAM Role for Data Sense & Compliance

To enable Data Sense & Compliance on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

Select a Role

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Data Sense & Compliance can securely scan the data.

Alternatively, ensure that the Data Sense & Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.


Free for the 1st TB

Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable **Cancel**

5. Haga clic en **Activar**.



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

Resultado

BlueXP asigna la función IAM a la instancia.

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

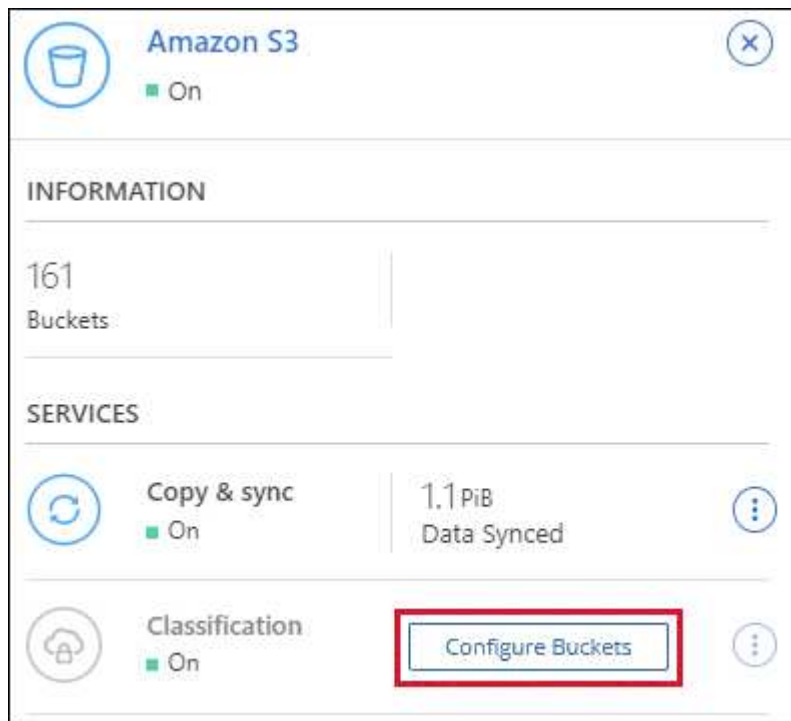
Después de que BlueXP habilita la clasificación de BlueXP en Amazon S3, el paso siguiente es configurar los bloques que quieres analizar.

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

La clasificación de BlueXP también puede [Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS](#).

Pasos

1. Seleccione el entorno de trabajo de Amazon S3.
2. En el panel Servicios de la derecha, haga clic en **Configurar cucharones**.



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

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuosly Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

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

Resultado

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

Escaneando bloques de cuentas de AWS adicionales

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





Pasos

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

Create role



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options**
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA ⓘ

No olvide hacer lo siguiente:

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

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

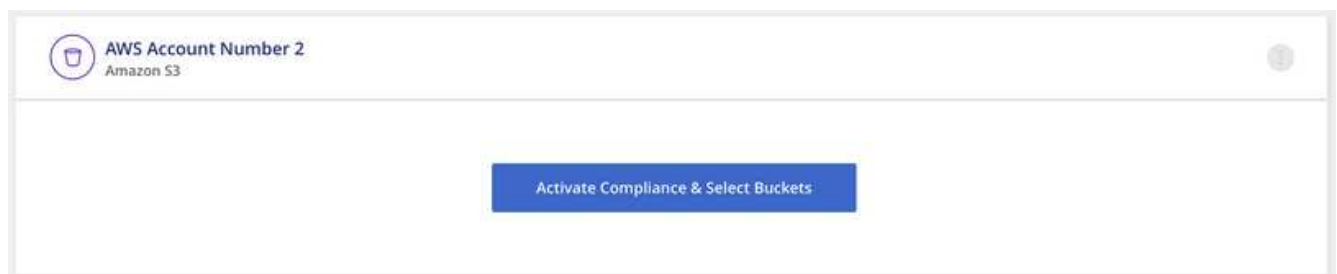
2. Ve a la cuenta de AWS de origen donde reside la instancia de clasificación de BlueXP y selecciona el rol IAM adjunto a la instancia.

- Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
- Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.
- Cree una directiva que incluya la acción "sts:AssumeRole" y especifique el ARN del rol que creó en la cuenta de destino.

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

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

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



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

Resultado

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

Escanear cuentas de OneDrive

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

NOTA Esta información solo es relevante para las versiones heredadas de clasificación de BlueXP 1,30 y anteriores.

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

Implementa la instancia de clasificación de BlueXP

"[Implementa la clasificación de BlueXP](#)" si aún no hay una instancia implementada.

3

Añada la cuenta de OneDrive

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

4

Agregue los usuarios y seleccione el tipo de análisis

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

Revisión de los requisitos de OneDrive

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

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

Implementar la instancia de clasificación de BlueXP

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

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

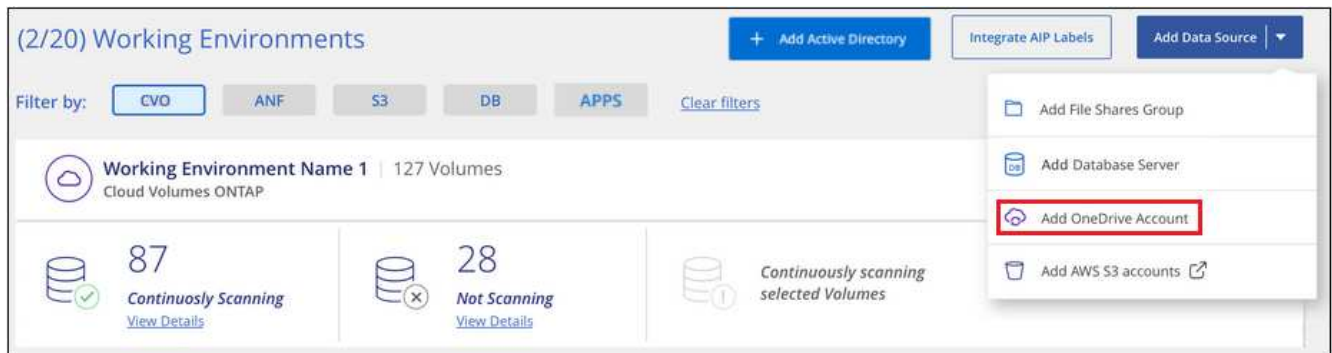
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Adición de la cuenta de OneDrive

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

Pasos

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



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

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

Añadir usuarios de OneDrive a los análisis de cumplimiento de normativas

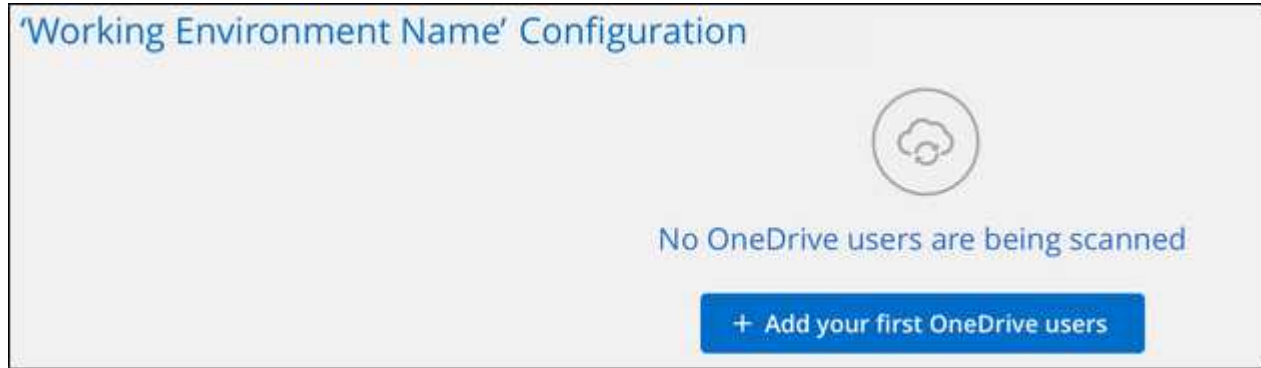
Puede añadir usuarios individuales de OneDrive, o todos sus usuarios de OneDrive, de manera que sus archivos se analizarán mediante la clasificación de BlueXP.

Pasos

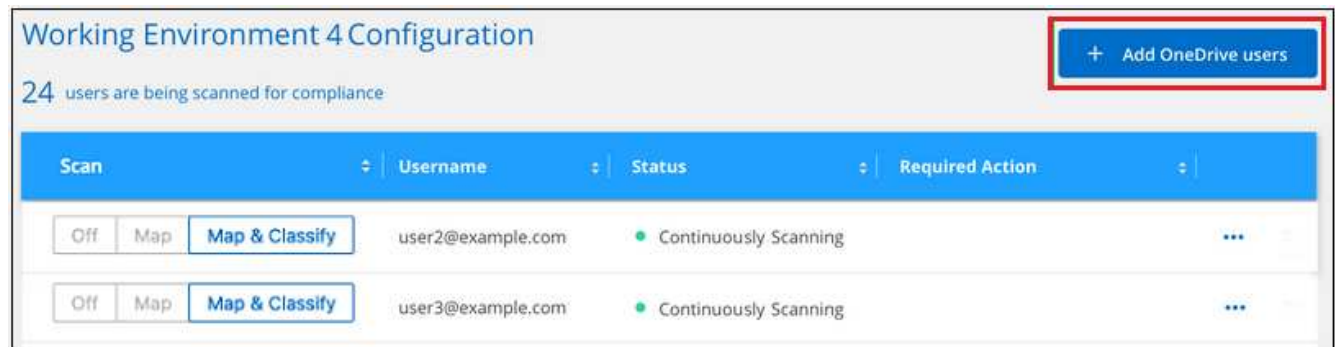
1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de OneDrive.



- 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**.



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

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

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

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

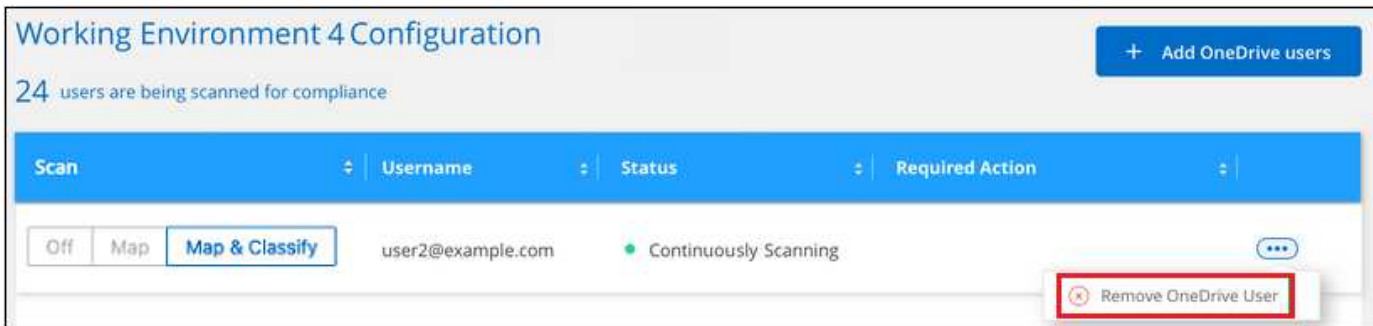
Para:	Haga lo siguiente:
Active los análisis de sólo asignación en los archivos de usuario	Haga clic en Mapa
Activar análisis completos en archivos de usuario	Haga clic en Mapa y clasificación
Desactive el análisis en archivos de usuario	Haga clic en Desactivado

Resultado

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

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

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



Analizar cuentas de SharePoint

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

NOTA Esta información solo es relevante para las versiones heredadas de clasificación de BlueXP 1,30 y anteriores.

Inicio rápido

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

1

Revise los requisitos previos de SharePoint

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

2

Implementa la instancia de clasificación de BlueXP

"[Implementa la clasificación de BlueXP](#)" si aún no hay una instancia implementada.

3

Inicie sesión en la cuenta de SharePoint

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

4

Agregue las direcciones URL del sitio de SharePoint que desea analizar

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

Revisar los requisitos de SharePoint

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

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

Implementa la instancia de clasificación de BlueXP

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

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

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

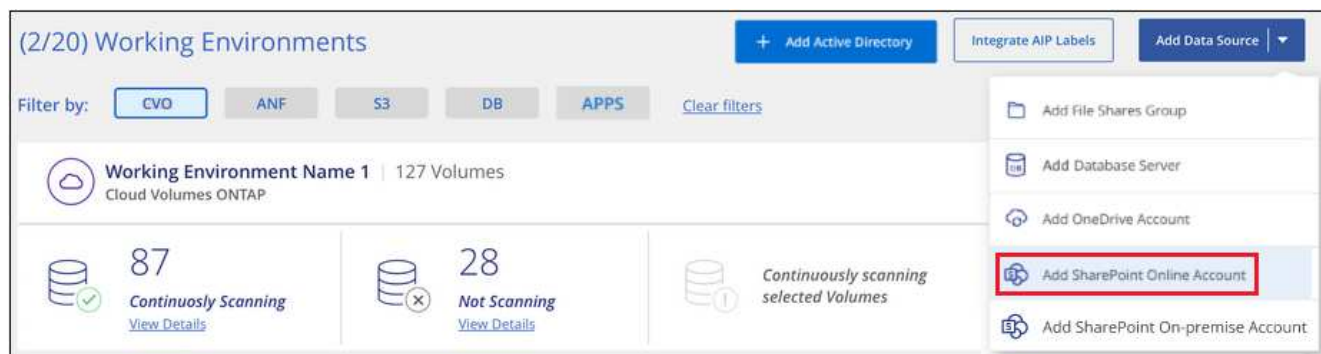
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Agregue una cuenta de SharePoint Online

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

Pasos

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



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

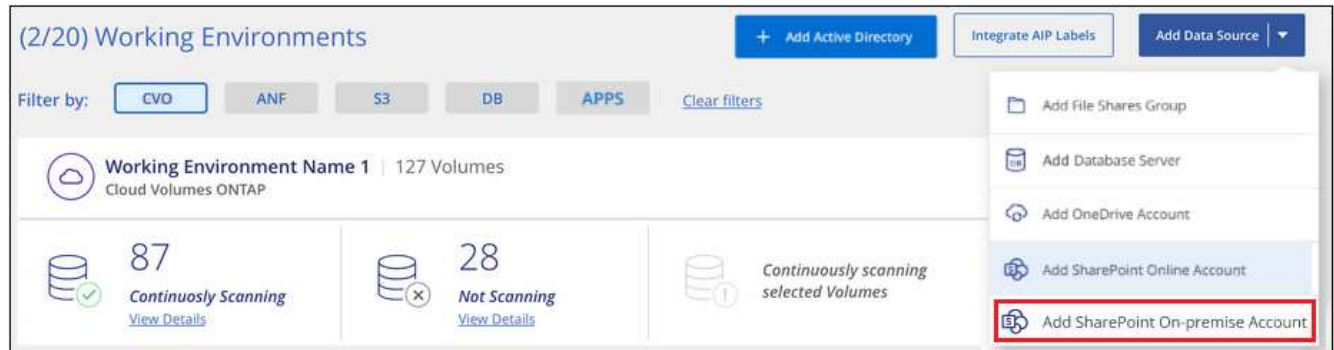
La cuenta de SharePoint Online se agrega a la lista de entornos de trabajo.

Agregue una cuenta de SharePoint On-Premise

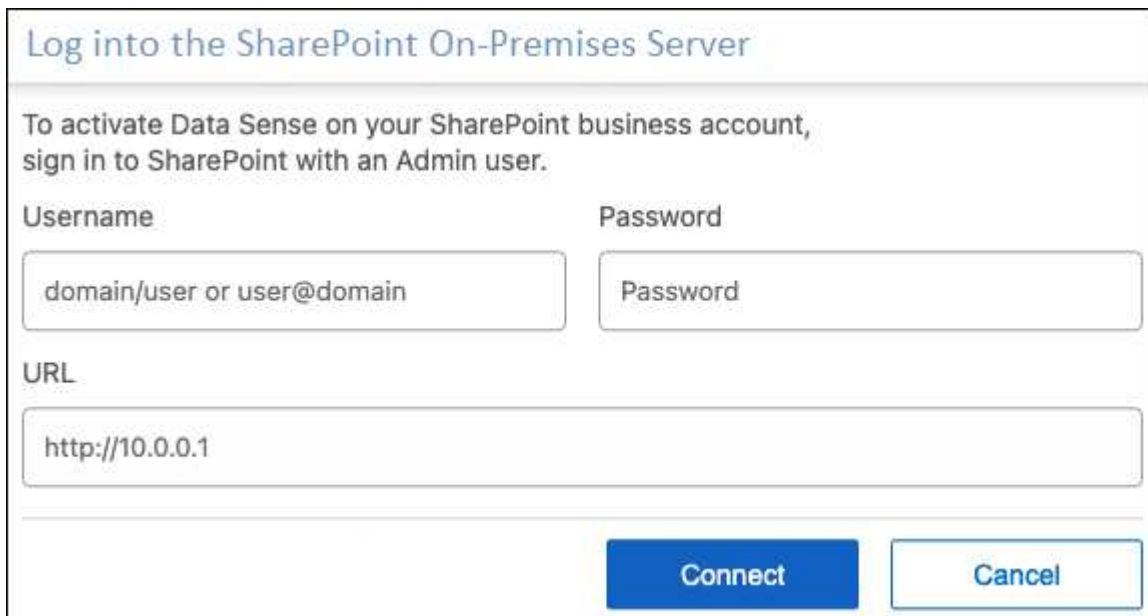
Agregue la cuenta de SharePoint en las instalaciones donde residen los archivos de usuario.

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

The image shows a dialog box titled 'Log into the SharePoint On-Premises Server'. The text inside says 'To activate Data Sense on your SharePoint business account, sign in to SharePoint with an Admin user.' There are three input fields: 'Username' with the placeholder 'domain/user or user@domain', 'Password' with the placeholder 'Password', and 'URL' with the placeholder 'http://10.0.0.1'. At the bottom, there are two buttons: 'Connect' (blue) and 'Cancel' (white with blue border).

3. Haga clic en **conectar**.

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

Agregue sitios de SharePoint a las exploraciones de cumplimiento

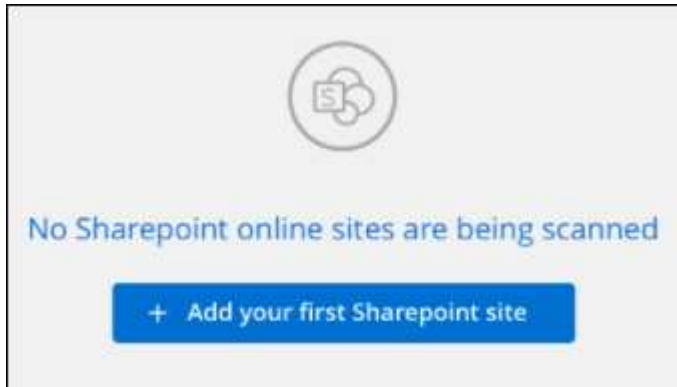
Puede añadir sitios de SharePoint individuales, o hasta 1.000 sitios de SharePoint en la cuenta, de modo que la clasificación de BlueXP analice los archivos asociados. Los pasos son los mismos si agrega sitios de SharePoint Online o de SharePoint en las instalaciones.

Pasos

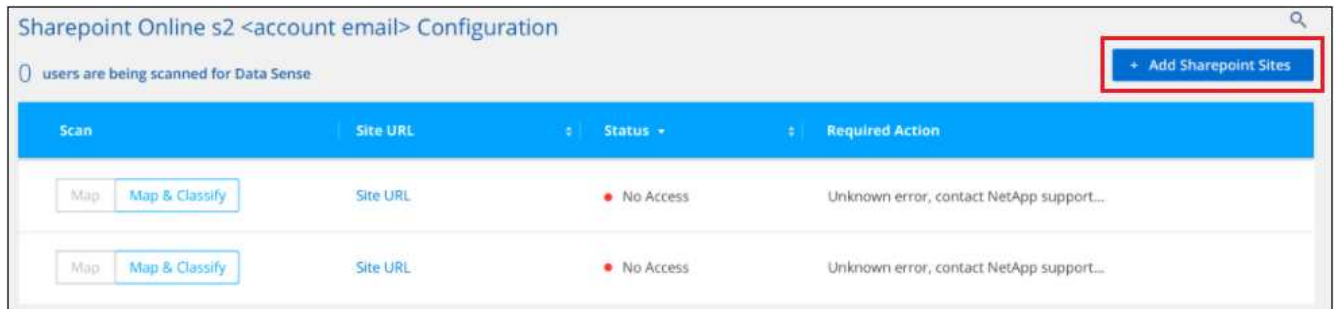
1. En la página *Configuration*, haga clic en el botón **Configuration** de la cuenta de SharePoint.



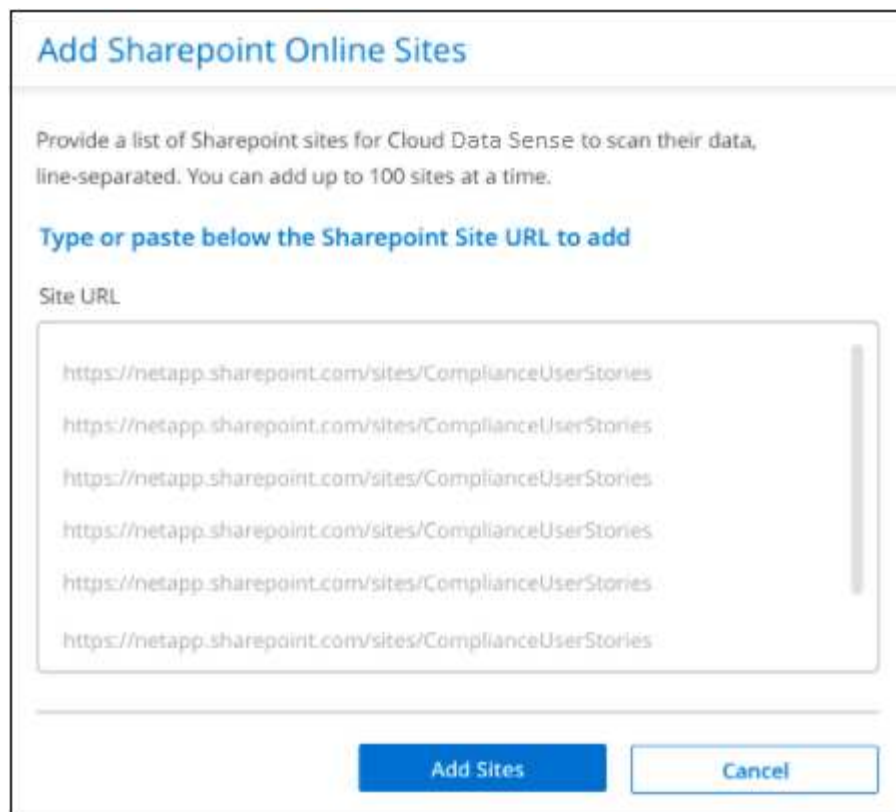
2. Si es la primera vez que agrega sitios para esta cuenta de SharePoint, haga clic en **Agregar su primer sitio de SharePoint**.



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



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



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

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

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

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

Resultado

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

Eliminar 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.

Scan	Site URL	Status	Required Action
Off Map Map & Classify	Site URL	Continuously Scanning	Remove SharePoint Site
Off Map Map & Classify	Site URL	Continuously Scanning	

Tenga en cuenta que puede ["Eliminar toda la cuenta de SharePoint de la clasificación de BlueXP"](#) Si ya no desea analizar los datos de usuario desde la cuenta de SharePoint.

Analizar cuentas de Google Drive

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

NOTA Esta información solo es relevante para las versiones heredadas de clasificación de BlueXP 1,30 y anteriores.

Inicio rápido

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

1

Revise los requisitos previos de Google Drive

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

2

Implementa la clasificación de BlueXP

"[Implementa la clasificación de BlueXP](#)" si aún no hay una instancia implementada.

3

Inicie sesión en la cuenta de Google Drive

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

4

Seleccione el tipo de análisis de los archivos de usuario

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

Revisa los requisitos de Google Drive

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

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

Restricciones actuales

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

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

Implementa la clasificación de BlueXP

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

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

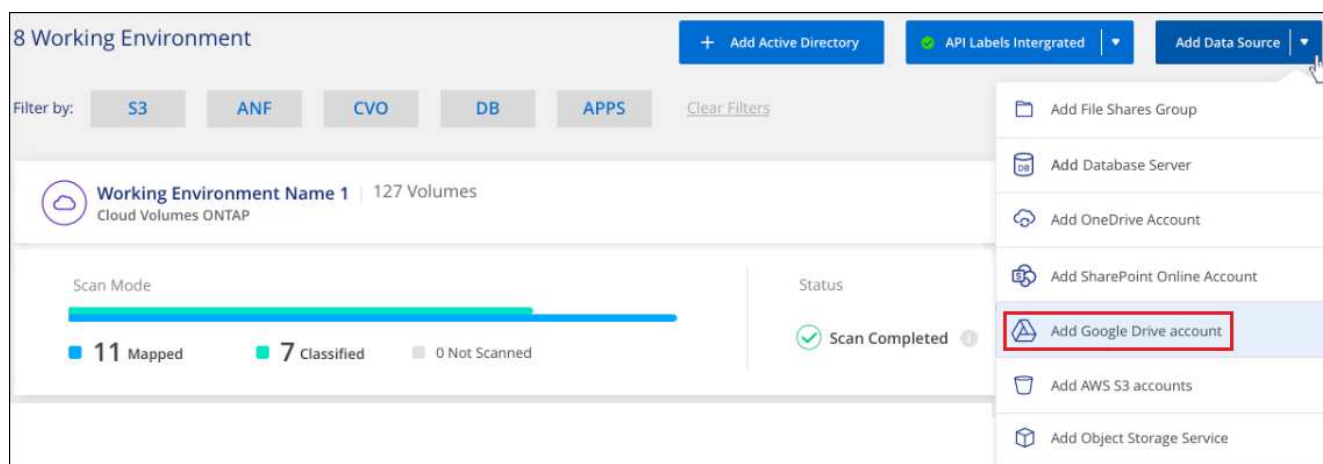
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Agregue la cuenta de Google Drive

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

Pasos

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



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

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

Seleccione el tipo de escaneo de datos de usuario

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

Pasos

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



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



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

Resultado

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

Eliminar una cuenta de Google Drive de los análisis de cumplimiento

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

Analice el almacenamiento de objetos que utiliza el protocolo S3

Completa unos pasos para empezar a analizar datos en el almacenamiento de objetos directamente con la clasificación de BlueXP. La clasificación de BlueXP puede analizar datos de cualquier servicio de almacenamiento de objetos que use el protocolo Simple Storage Service (S3). Entre ellas se incluyen NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3, etc.

NOTA Esta información solo es relevante para las versiones heredadas de clasificación de BlueXP 1,30 y anteriores.

Inicio rápido

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

1

Revise los requisitos previos de almacenamiento del objeto

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

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

2

Implementa la instancia de clasificación de BlueXP

"[Implementa la clasificación de BlueXP](#)" si aún no hay una instancia implementada.

3

Añada el servicio de almacenamiento de objetos

Añade el servicio de almacenamiento de objetos a la clasificación de BlueXP.

4

Seleccione los cucharones que desea escanear

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

Revisión de requisitos de almacenamiento de objetos

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

- Debe tener la URL del extremo para conectarse con el servicio de almacenamiento de objetos.
- Debe tener la clave de acceso y la clave secreta del proveedor de almacenamiento de objetos para que la clasificación de BlueXP pueda acceder a los bloques.

Implementar la instancia de clasificación de BlueXP

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

Si va a analizar datos de un almacenamiento de objetos S3 al que se puede acceder a través de Internet, puede hacerlo "[Pon en marcha la clasificación de BlueXP en el cloud](#)" o "[Pon en marcha la clasificación de BlueXP en una ubicación on-premises que tenga acceso a Internet](#)".

Si va a analizar datos del almacenamiento de objetos S3 que se ha instalado en un sitio oscuro que no tiene acceso a Internet, deberá hacerlo "[Pon en marcha la clasificación de BlueXP en la misma ubicación on-premises que no tiene acceso a Internet](#)". Esto también requiere que el conector BlueXP se despliegue en esa misma ubicación en las instalaciones.

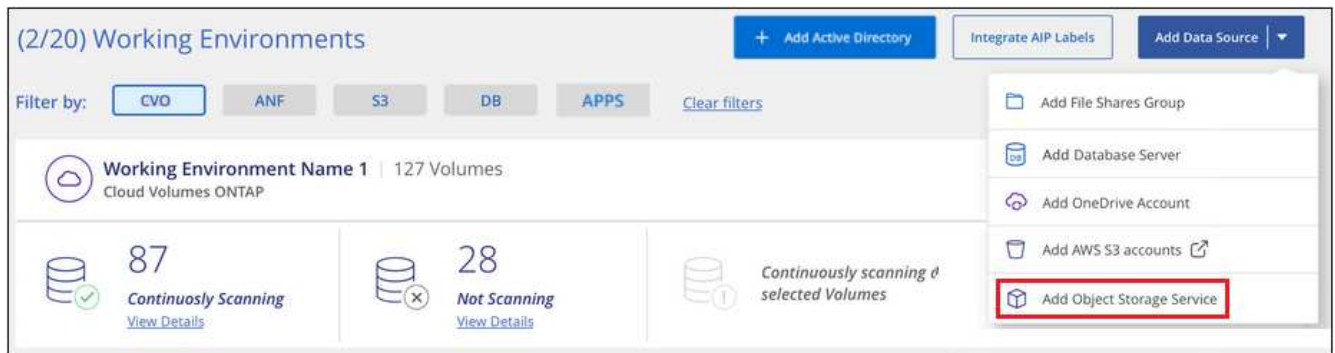
Las actualizaciones del software de clasificación de BlueXP se automatizan siempre que la instancia tenga conectividad a Internet.

Agregar el servicio de almacenamiento de objetos a la clasificación de BlueXP

Añada el servicio de almacenamiento de objetos.

Pasos

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



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

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKDO574NDJG86795"/>	<input type="password" value="....."/>

Resultado

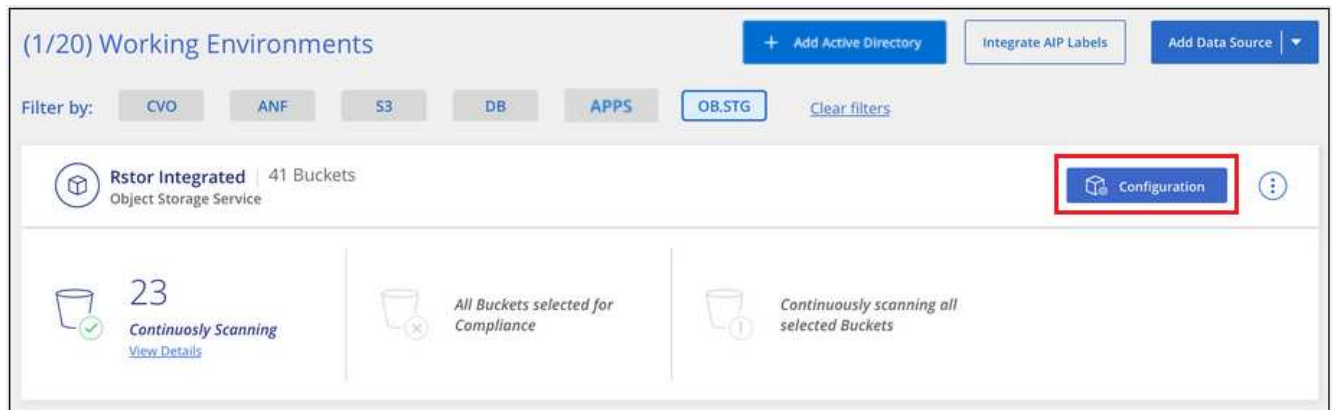
El nuevo Servicio de almacenamiento de objetos se añade a la lista de entornos de trabajo.

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

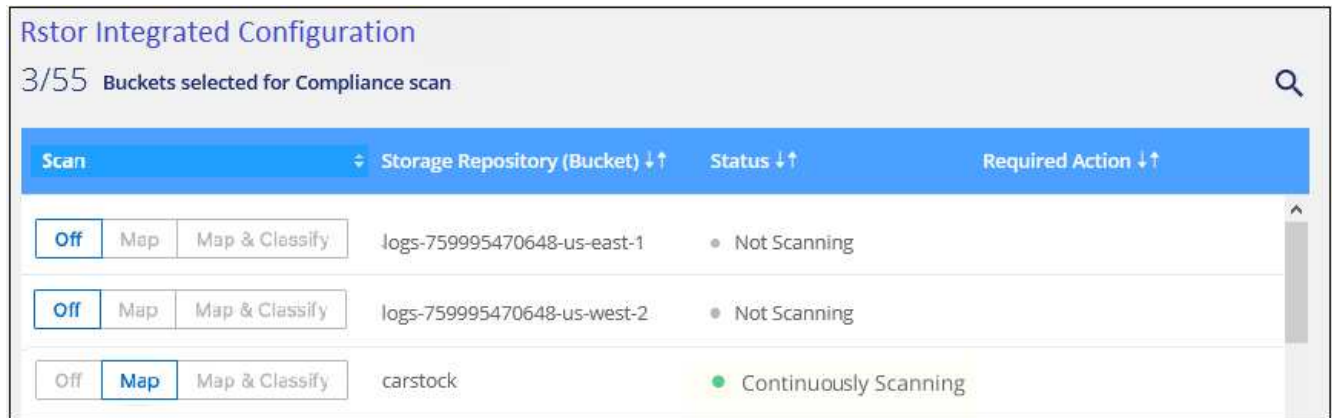
Después de habilitar la clasificación de BlueXP en tu servicio de almacenamiento de objetos, el paso siguiente es configurar los bloques que quieres analizar. La clasificación de BlueXP descubre esos buckets y los muestra en el entorno de trabajo que has creado.

Pasos

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



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



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

Resultado

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

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.