Obtenga información sobre la privacidad de sus datos

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

Obtenga información sobre la privacidad de sus datos

Más información sobre Cloud Compliance

Cloud Compliance es un servicio de cumplimiento de normativas y privacidad de datos para Cloud Manager que analiza sus volúmenes, bloques de Amazon S3 y bases de datos para identificar los datos personales y confidenciales que se encuentran en esos archivos. Con la tecnología impulsada por la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales.

"Obtenga información sobre los casos de uso de Cloud Compliance".

Funciones

Cloud Compliance proporciona varias herramientas que le ayudan en sus tareas de cumplimiento de normativas. Puede usar Cloud Compliance para:

- Identificación de la Información personal de identificación (PII).
- Identificar un amplio abanico de información confidencial que requieran las normativas de privacidad del RGPD, la CCPA, el PCI y la HIPAA
- Responder a solicitudes de acceso de sujetos de datos (DSAR)

Entornos de trabajo y fuentes de datos compatibles

Cloud Compliance puede analizar datos de los siguientes tipos de orígenes de datos:

- Cloud Volumes ONTAP en AWS
- Cloud Volumes ONTAP en Azure
- Azure NetApp Files
- Amazon S3
- Bases de datos que residen en cualquier ubicación (no hay ningún requisito de que la base de datos resida en un entorno de trabajo)

Nota: para Azure NetApp Files, Cloud Compliance puede analizar cualquier volumen que se encuentre en la misma región que Cloud Manager.

Coste

- El coste de utilizar Cloud Compliance depende de la cantidad de datos que se escanee. A partir del 7 de octubre de 2020, el primer TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager es gratuito. Esto incluye datos de Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, bloques de Amazon S3 y esquemas de base de datos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto. Consulte "precios" para obtener más detalles.

  "Aprenda a suscribirse".

- La instalación de Cloud Compliance requiere la puesta en marcha de una instancia de cloud, que resulta en cobros al proveedor de cloud en el que se ha puesto en marcha. Consulte el tipo de instancia que se pone en marcha en cada cloud proveedor
- Cloud Compliance requiere que haya implementado un conector. En muchos casos ya tiene un conector debido a otro almacenamiento y servicios que utiliza en Cloud Manager. La instancia de Connector representa cargos del proveedor de cloud en el que se ha puesto en marcha. Consulte "tipo de instancia que se pone en marcha para cada proveedor de cloud".

Costes de transferencia de datos

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

- "AWS: Precios de Amazon EC2"
- "Microsoft Azure: Detalles de precios del ancho de banda"

Cómo funciona Cloud Compliance

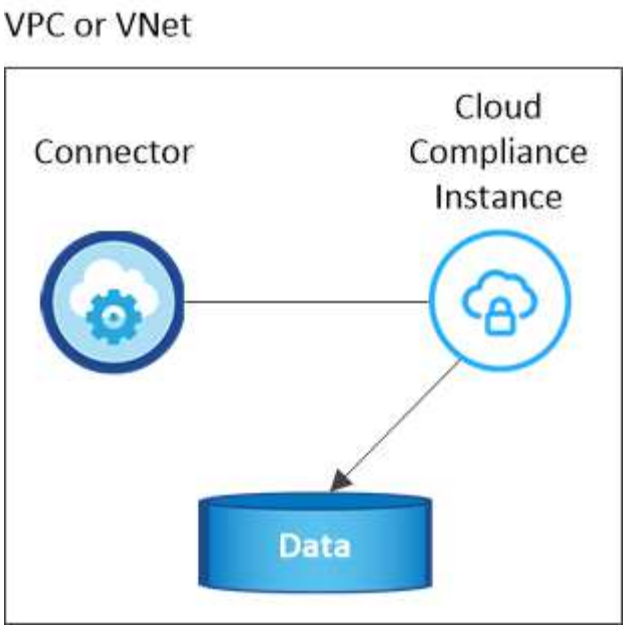
En un nivel superior, Cloud Compliance funciona como esta:

1. Se implementa una instancia de Cloud Compliance en Cloud Manager.
2. Se habilita en uno o más entornos de trabajo o bases de datos.
3. Cloud Compliance analiza los datos mediante un proceso de aprendizaje de IA.
4. En Cloud Manager, haga clic en **conformidad** y utilice el panel y las herramientas de informes proporcionados para ayudarle en sus esfuerzos de cumplimiento.

La instancia de Cloud Compliance

Al habilitar Cloud Compliance, Cloud Manager implementa una instancia de Cloud Compliance en la misma subred que Connector. "Más información sobre conectores."

Si el conector está instalado en las instalaciones, pone en marcha la instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema Cloud Volumes ONTAP de la solicitud.



Tenga en cuenta lo siguiente acerca de la instancia:

- En Azure, Cloud Compliance se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 512 GB.
- En AWS, Cloud Compliance se ejecuta en una instancia de 5,4 x grande con un disco GP2 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

  No se admite el cambio o cambio de tamaño del tipo de máquina virtual/instancia. Debe utilizar el tamaño que se proporciona.

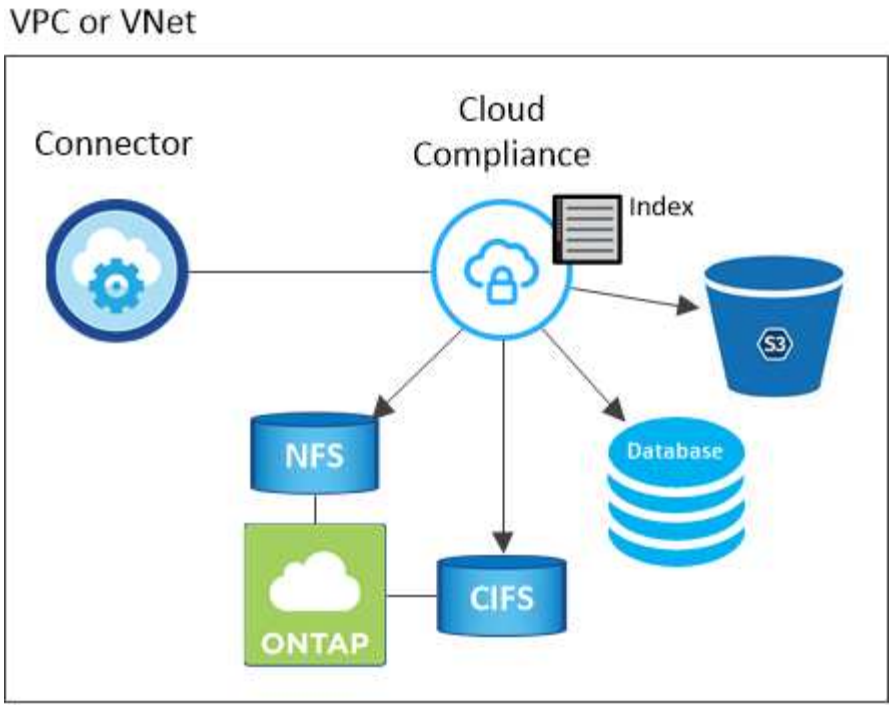
- La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Solo se implementa una instancia de Cloud Compliance por conector.
- Las actualizaciones del software de Cloud Compliance se automatizan, ya que no tiene que preocuparse por ello.

La instancia debe permanecer en ejecución en todo momento debido a que Cloud Compliance analiza los datos de forma continua.

Cómo funcionan las exploraciones

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

Cloud Compliance se conecta a los datos como cualquier otro cliente al montar volúmenes NFS y CIFS. Se accede automáticamente a los volúmenes NFS como de solo lectura, mientras que se necesitan proporcionar credenciales de Active Directory para analizar volúmenes CIFS.



Después del análisis inicial, Cloud Compliance analiza continuamente cada volumen para detectar cambios incrementales (por eso es importante mantener la instancia en ejecución).

Puede activar y desactivar los análisis en el "nivel de volumen", en la "nivel de cucharón", y en el "nivel de esquema de base de datos".

Información que indexa Cloud Compliance

Cloud Compliance recopila, indexa y asigna categorías a datos no estructurados (archivos). Los datos que indexa Cloud Compliance incluyen los siguientes:

Metadatos estándar

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

Datos personales

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

Datos personales confidenciales

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

Categorías

Cloud Compliance toma los datos que ha analizado y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. "Más información sobre categorías".

Reconocimiento de entidad de nombre

Cloud Compliance utiliza la IA para extraer los nombres de las personas naturales de los documentos. "Obtenga información sobre cómo responder a las solicitudes de acceso a sujetos de datos".

Información general sobre redes

Cloud Manager implementa la instancia de Cloud Compliance con un grupo de seguridad que permite conexiones HTTP entrantes desde la instancia de Connector.

Cuando se utiliza Cloud Manager en modo SaaS, la conexión a Cloud Manager se ofrece mediante HTTPS y los datos privados enviados entre el explorador y la instancia de Cloud Compliance se protegen con cifrado integral, lo que significa que NetApp y terceros no pueden leerlo.

Si necesita utilizar la interfaz de usuario local en lugar de la interfaz de usuario SaaS por cualquier motivo, puede seguir siendo así "Acceda a la interfaz de usuario local".

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

Si tiene requisitos estrictos de red, "Obtenga información sobre los extremos con los que se contacta Cloud Compliance".

Acceso de los usuarios a la información de cumplimiento

La función a la que se ha asignado cada usuario proporciona distintas funcionalidades dentro de Cloud Manager y dentro de Cloud Compliance:

- **los administradores de cuentas** pueden administrar la configuración de cumplimiento y ver la información de cumplimiento de todos los entornos de trabajo.
- **los administradores de espacio de trabajo** pueden administrar la configuración de cumplimiento y ver la información de cumplimiento sólo para los sistemas a los que tienen permisos de acceso. Si un administrador de área de trabajo no puede tener acceso a un entorno de trabajo en Cloud Manager, no podrá ver ninguna información de cumplimiento para el entorno de trabajo en la ficha cumplimiento.
- Los usuarios con la función **Cloud Compliance Viewer** sólo pueden ver información de cumplimiento y generar informes para los sistemas a los que tienen permiso de acceso. Estos usuarios no pueden habilitar o deshabilitar el análisis de volúmenes, bloques o esquemas de base de datos.

"Más información acerca de los roles de Cloud Manager" y cómo "añadir usuarios con roles específicos".

Manos a la obra

Ponga en marcha el cumplimiento normativo del cloud

Complete algunos pasos para implementar la instancia de Cloud Compliance en el espacio de trabajo de Cloud Manager.

Inicio rápido

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

Cree un conector

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

Revise los requisitos previos

Asegúrese de que su entorno de nube pueda cumplir con los requisitos previos, que incluyen 16 vCPU para la instancia de Cloud Compliance, acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Compliance a través del puerto 80, etc. Vea la lista completa.

Ponga en marcha el cumplimiento normativo del cloud

Inicie el asistente de instalación para implementar la instancia de Cloud Compliance en Cloud Manager.

Suscríbase al servicio Cloud Compliance

Los primeros 1 TB de datos que analiza Cloud Compliance en Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto.

Creación de un conector

Si aún no tiene un conector, cree un conector en Azure o AWS. Consulte "Creación de un conector en AWS" o. "Creación de un conector en Azure". En la mayoría de los casos probablemente tendrá un juego de conectores Realice el primero antes de intentar activar Cloud Compliance porque la mayoría "Las funciones de Cloud Manager requieren un conector", pero hay casos en los que necesita configurar uno ahora.

Hay algunas situaciones en las que debe utilizar un conector en AWS o Azure para Cloud Compliance.

- Cuando se escanea datos en Cloud Volumes ONTAP en AWS o en bloques de AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.
- Las bases de datos se pueden escanear con cualquiera de los conectores.

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

Si está planeando el análisis de Azure NetApp Files, debe asegurarse de que está implementando en la misma región que los volúmenes que desea analizar.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de implementar Cloud Compliance.

Habilite el acceso saliente a Internet

Cloud Compliance requiere acceso a Internet de salida. Si la red virtual utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de Cloud Compliance tiene acceso saliente a Internet para ponerse en contacto con los siguientes extremos. Tenga en cuenta que Cloud Manager implementa la instancia de Cloud Compliance en la misma subred que Connector.

Puntos finales	Específico
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite a Cloud Compliance acceder y descargar manifiestos y plantillas, así como enviar registros y métricas.

Compruebe que Cloud Manager tenga los permisos necesarios

Asegúrese de que Cloud Manager tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Compliance. Puede encontrar los permisos más recientes de Cloud Manager en "Las políticas proporcionadas por NetApp".

Compruebe sus límites de vCPU

Compruebe que el límite de vCPU de su proveedor de cloud permita poner en marcha una instancia con 16 núcleos. Deberá comprobar el límite de vCPU para la familia de instancias relevante en la región donde se ejecuta Cloud Manager.

En AWS, la familia de instancias es *On-Demand Standard Instances*. En Azure, la familia de instancias es *Standard DSv3 Family*.

Para obtener más información sobre los límites de vCPU, consulte lo siguiente:

- "Documentación de AWS: Límites del servicio de Amazon EC2"
- "Documentación de Azure: Cuotas de vCPU de máquina virtual"

Compruebe que Cloud Manager pueda acceder a Cloud Compliance

Garantice la conectividad entre el conector y la instancia de Cloud Compliance. El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.

Esta conexión permite la implementación de la instancia de Cloud Compliance y permite ver información en la ficha cumplimiento.

Configurar el descubrimiento de Azure NetApp Files

Antes de poder analizar volúmenes para Azure NetApp Files, "Cloud Manager debe configurarse para detectar la configuración".

Asegúrese de poder mantener Cloud Compliance en funcionamiento

La instancia de Cloud Compliance debe permanecer activa para analizar sus datos de forma continua.

Asegúrese de que la conectividad del navegador web es compatible con Cloud Compliance

Después de habilitar Cloud Compliance, asegúrese de que los usuarios acceden a la interfaz de Cloud Manager desde un host que tiene una conexión con la instancia de Cloud Compliance.

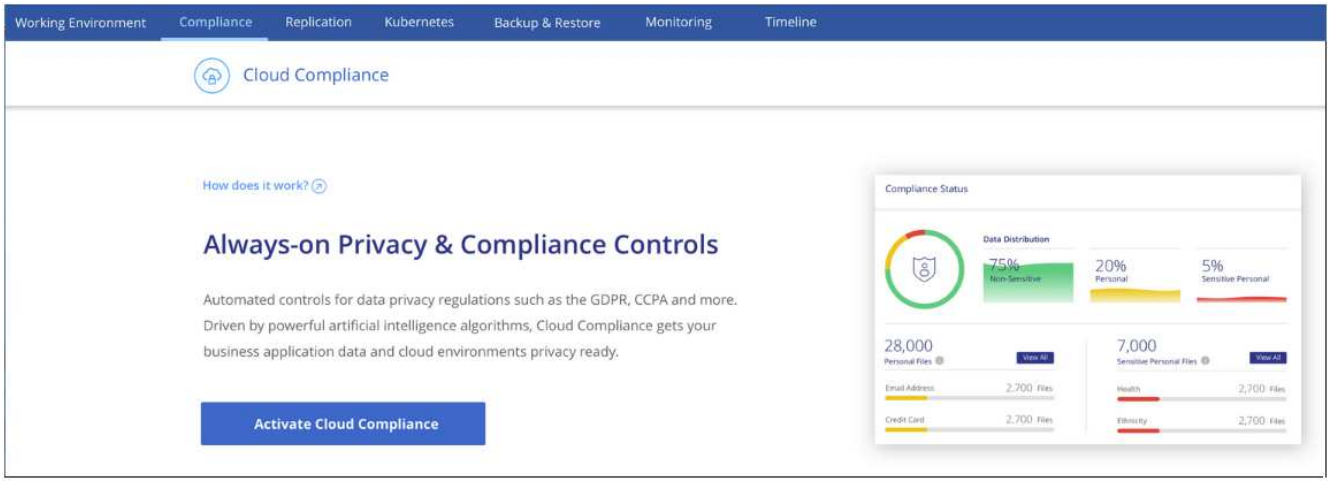
La instancia de Cloud Compliance utiliza una dirección IP privada para garantizar que no se pueda acceder a Internet a los datos indexados. Como resultado, el explorador web que utiliza para acceder a Cloud Manager debe tener una conexión con esa dirección IP privada. Esta conexión puede provenir de una conexión directa a AWS o Azure (por ejemplo, una VPN) o de un host que está dentro de la misma red que la instancia de Cloud Compliance.

Implementación de la instancia de Cloud Compliance

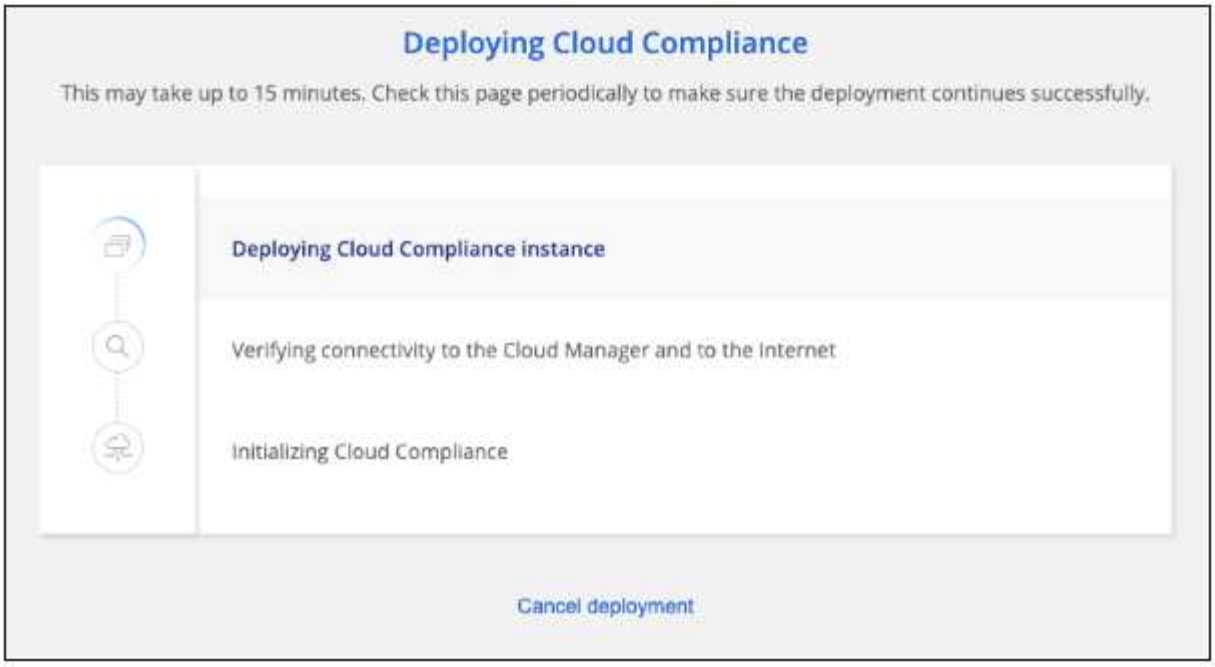
Se implementa una instancia de Cloud Compliance para cada instancia de Cloud Manager.

Pasos

1. En Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en **Activar Cloud Compliance** para iniciar el asistente de implementación.



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



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

Resultado

Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud.

El futuro

En la página Scan Configuration (Configuración de exploración), puede seleccionar los entornos de trabajo, los volúmenes y los bloques que desea analizar para el cumplimiento normativo. También puede conectarse a un servidor de base de datos para analizar esquemas de base de datos específicos. Active Cloud Compliance en cualquiera de estos orígenes de datos.

Suscripción al servicio Cloud Compliance

Los primeros 1 TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto.

Puede suscribirse en cualquier momento y no se le cobrará hasta que la cantidad de datos supere 1 TB. Siempre puede ver la cantidad total de datos que se analizan en la consola de cumplimiento de normativas del cloud. Y el botón *Subscribe Now* facilita la suscripción cuando esté listo.

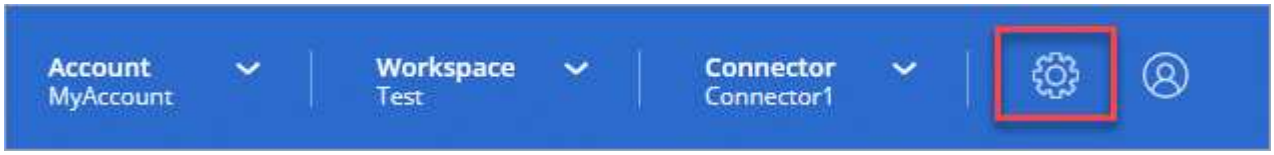
Nota: Si se le solicita la suscripción a Cloud Compliance, pero ya tiene una suscripción a Azure, probablemente utilice la antigua suscripción **Cloud Manager** y tendrá que cambiar a la nueva suscripción **NetApp Cloud Manager**. ConsulteCambiar al nuevo plan Cloud Manager de NetApp en Azure para obtener

más detalles.

Pasos

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

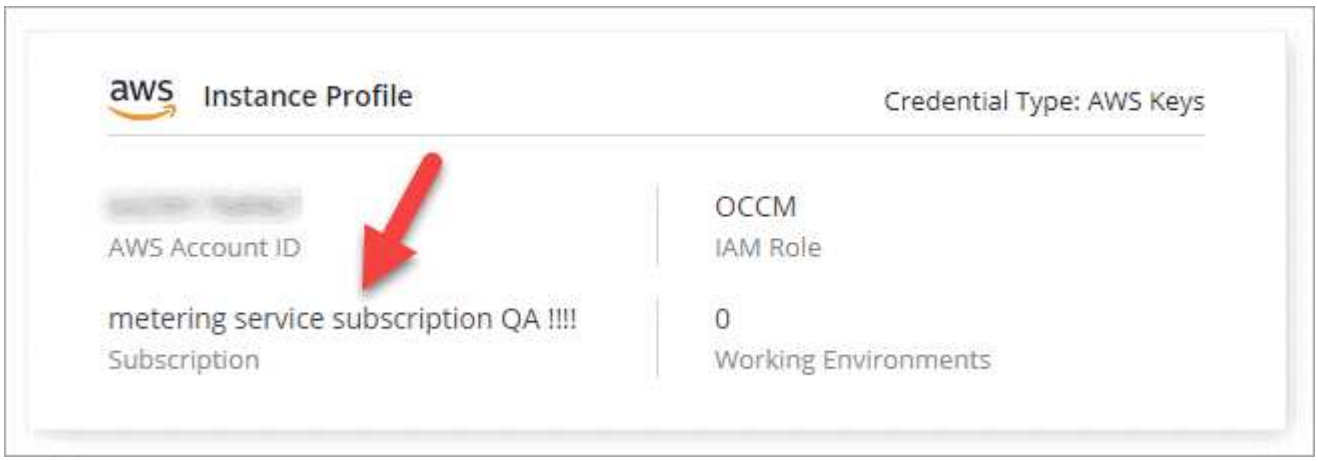
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



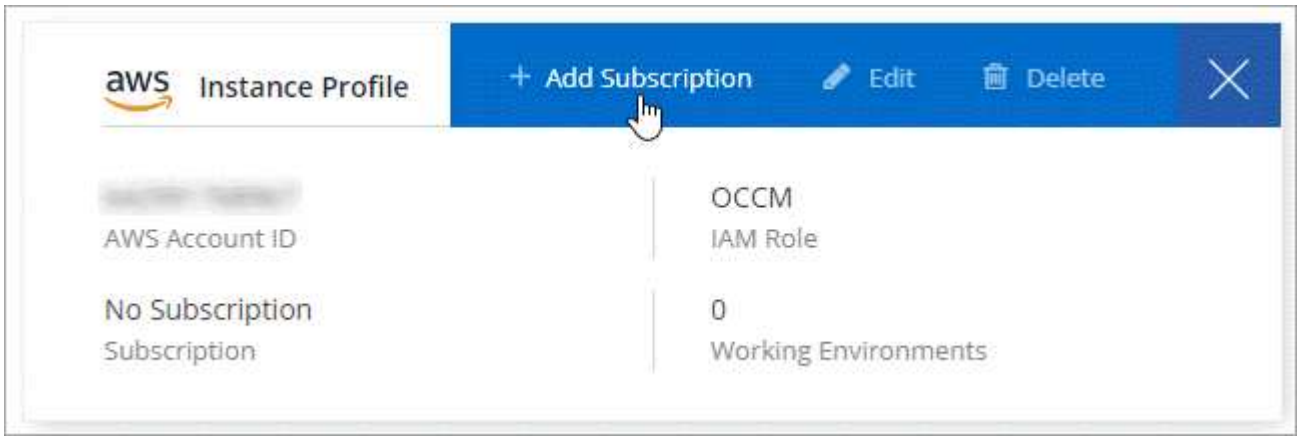
2. Busque las credenciales para el perfil de instancia de AWS o la identidad del servicio gestionado de Azure.

   La suscripción debe agregarse al perfil de instancia o a la identidad del servicio gestionado. La carga no funcionará de otro modo.

   Si ya tienes una suscripción, entonces estás todo establecido, no hay nada más que hacer.



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



5. Haga clic en **Agregar suscripción**, haga clic en **continuar** y siga los pasos.

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de AWS:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de Azure:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

Cambie al nuevo plan de Cloud Manager en Azure

Cloud Compliance se ha añadido a la suscripción a Azure Marketplace llamada * NetApp Cloud Manager* a partir del 7 de octubre de 2020. Si ya tiene la suscripción original de Azure **Cloud Manager**, no le permitirá utilizar Cloud Compliance.

Debe seguir estos pasos, seleccionar la nueva suscripción **NetApp Cloud Manager** y, a continuación, eliminar la antigua suscripción **Cloud Manager**.

> Si su suscripción existente se emitió con una oferta especial privada, debe ponerse en contacto con NetApp para que podamos emitir una nueva oferta especial privada con el cumplimiento incluido.

Pasos

Estos pasos son similares a añadir una nueva suscripción como se describe anteriormente, pero varían en algunos lugares.

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Busque las credenciales de la identidad de servicio gestionado de Azure para las que desea cambiar la suscripción y pase el ratón sobre las credenciales y haga clic en **Suscripción asociada**.

   Se muestran los detalles de su suscripción de Marketplace actual.

3. Haga clic en **Agregar suscripción**, haga clic en **continuar** y siga los pasos. Se le redirigirá al portal de Azure para crear la nueva suscripción.
4. Asegúrese de seleccionar el plan **NetApp Cloud Manager** que proporciona acceso a Cloud Compliance y no a Cloud Manager*.
5. Siga los pasos del vídeo para asociar una suscripción de Marketplace a una suscripción de Azure:

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

6. Vuelva a Cloud Manager, seleccione la nueva suscripción y haga clic en **asociado**.
7. Para verificar que ha cambiado su suscripción, pase el cursor sobre la suscripción “i” anterior en la tarjeta Credentials.

   Ahora puede cancelar la suscripción antigua en el portal de Azure.

8. En el portal de Azure, vaya a Software como servicio (SaaS), seleccione la suscripción y haga clic en **Anular la suscripción**.

Active el análisis en sus orígenes de datos

Primeros pasos con el cumplimiento de normativas cloud para Cloud Volumes ONTAP y Azure NetApp Files

Complete unos pasos para comenzar a utilizar el cumplimiento de normativas cloud para Cloud Volumes ONTAP o Azure NetApp Files.

Inicio rápido

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

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Habilite el cumplimiento de normativas del cloud en sus entornos de trabajo

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

Garantice el acceso a los volúmenes

Ahora que Cloud Compliance está habilitado, asegúrese de que pueda acceder a los volúmenes.

- La instancia de Cloud Compliance necesita una conexión de red para cada subred de Cloud Volumes ONTAP o subred de Azure NetApp Files.
- Los grupos de seguridad para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de Cloud Compliance.
- Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de Cloud Compliance.
- Cloud Compliance necesita credenciales de Active Directory para analizar volúmenes CIFS.

  Haga clic en **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** y proporcione las credenciales. Las credenciales pueden ser de sólo lectura, pero al proporcionar credenciales de administrador se garantiza que Cloud Compliance pueda leer datos que requieran permisos elevados.

Configure los volúmenes que desea analizar

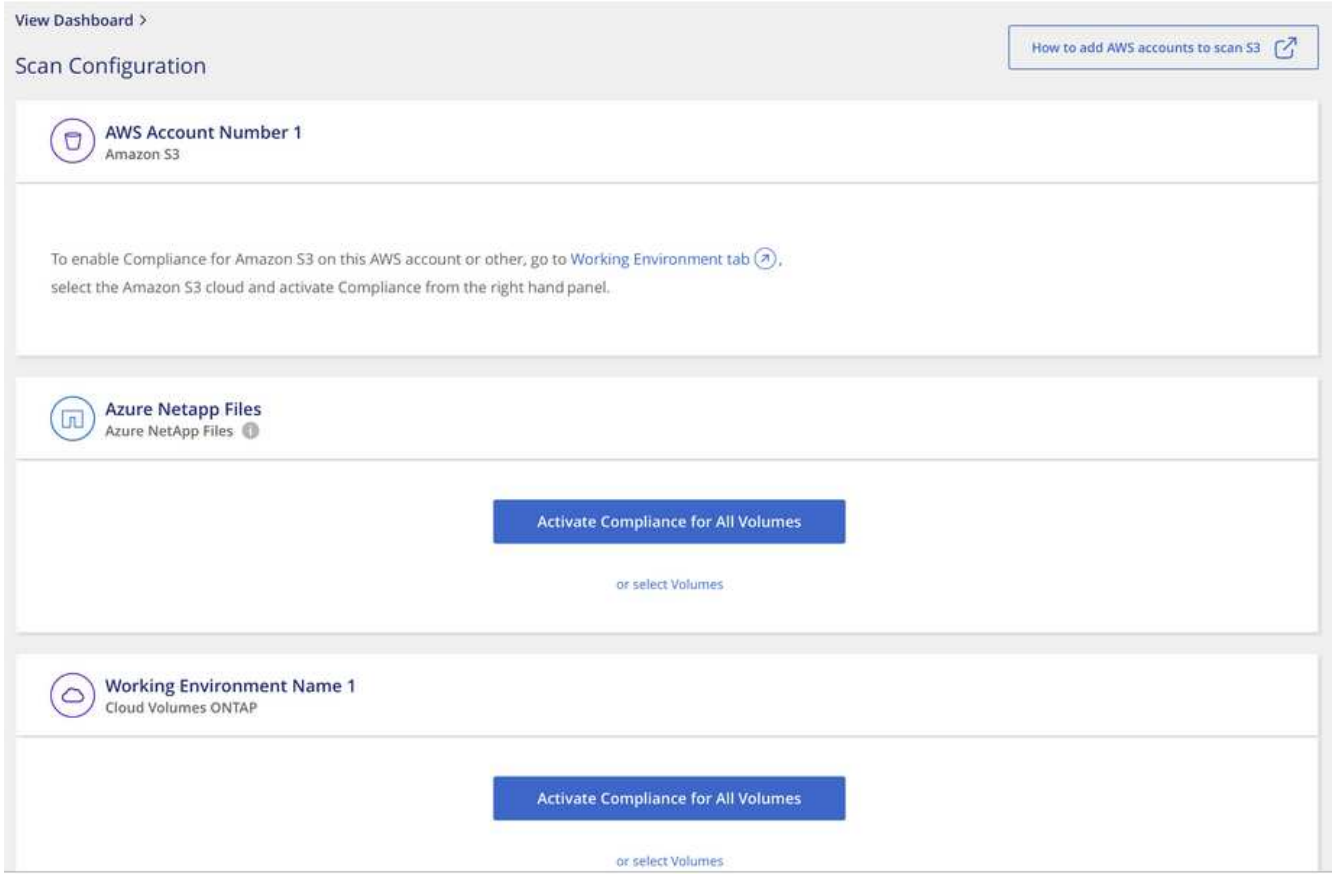
Seleccione los volúmenes que desea analizar y Cloud Compliance empezará a analizarlos.

Implementación de la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Habilitar Cloud Compliance en sus entornos de trabajo

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento de la nube** y, a continuación, seleccione la ficha **Configuración**.



2. Para analizar todos los volúmenes de un entorno de trabajo, haga clic en **Activar conformidad para todos los volúmenes**.

   Para analizar sólo ciertos volúmenes en un entorno de trabajo, haga clic en **o seleccione volúmenes** y, a continuación, elija los volúmenes que desea analizar.

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

Resultado

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

Comprobación de que Cloud Compliance tiene acceso a los volúmenes

Para asegurarse de que Cloud Compliance pueda acceder a los volúmenes, compruebe su red, los grupos de seguridad y las políticas de exportación. Necesitará proporcionar cumplimiento normativo del cloud con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que haya una conexión de red entre la instancia de Cloud Compliance y cada red que incluya los volúmenes para Cloud Volumes ONTAP o Azure NetApp Files.

Para Azure NetApp Files, Cloud Compliance solo puede analizar volúmenes que se encuentren en la misma región que Cloud Manager.

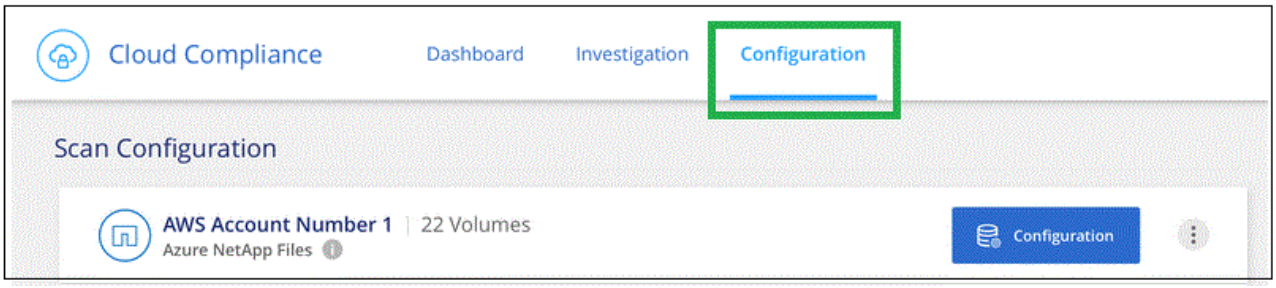
2. Asegúrese de que el grupo de seguridad para Cloud Volumes ONTAP permite el tráfico entrante desde la instancia de Cloud Compliance.

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

3. Compruebe que las políticas de exportación de volúmenes NFS incluyan la dirección IP de la instancia de Cloud Compliance para poder acceder a los datos de cada volumen.
4. Si utiliza CIFS, proporcione Cloud Compliance con credenciales de Active Directory para que pueda analizar volúmenes CIFS.

   a. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.

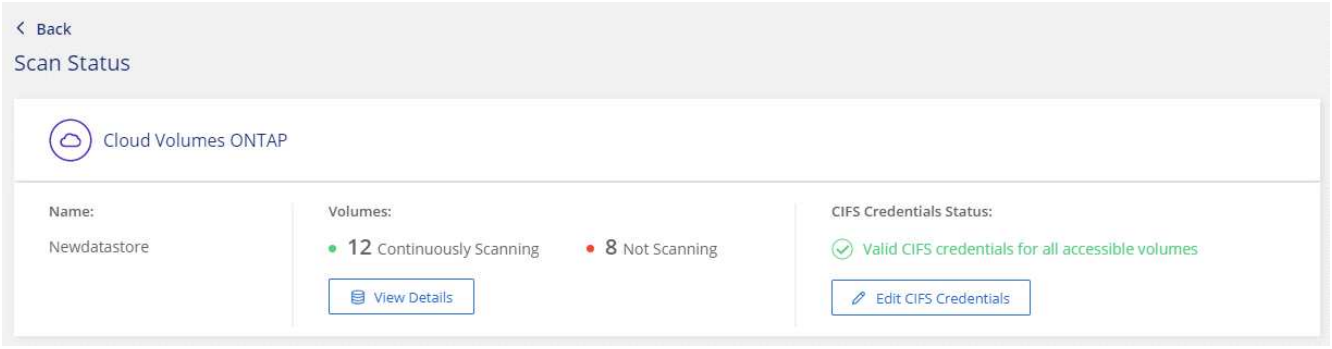
   b. Haga clic en la ficha **Configuración**.



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

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

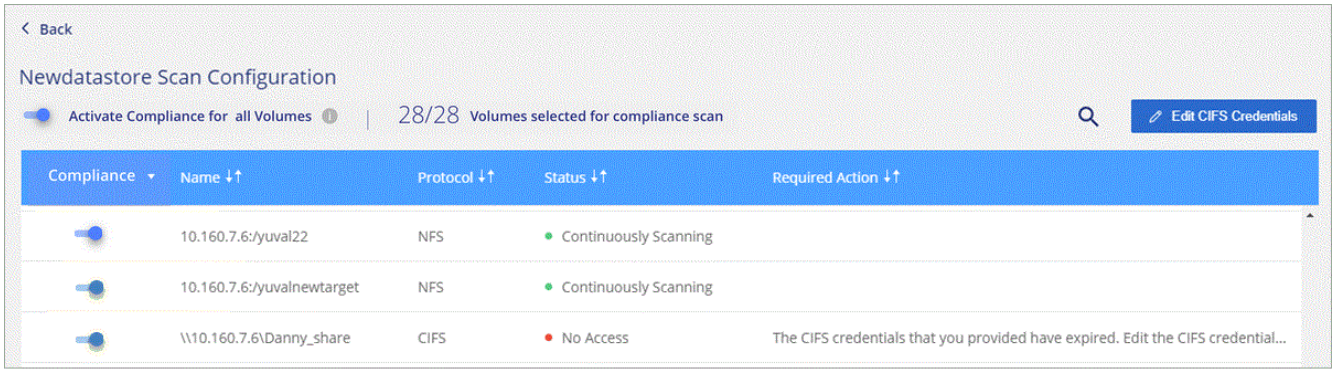
      Después de introducir las credenciales, debe ver un mensaje que indica que todos los volúmenes CIFS se autenticaron correctamente.



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

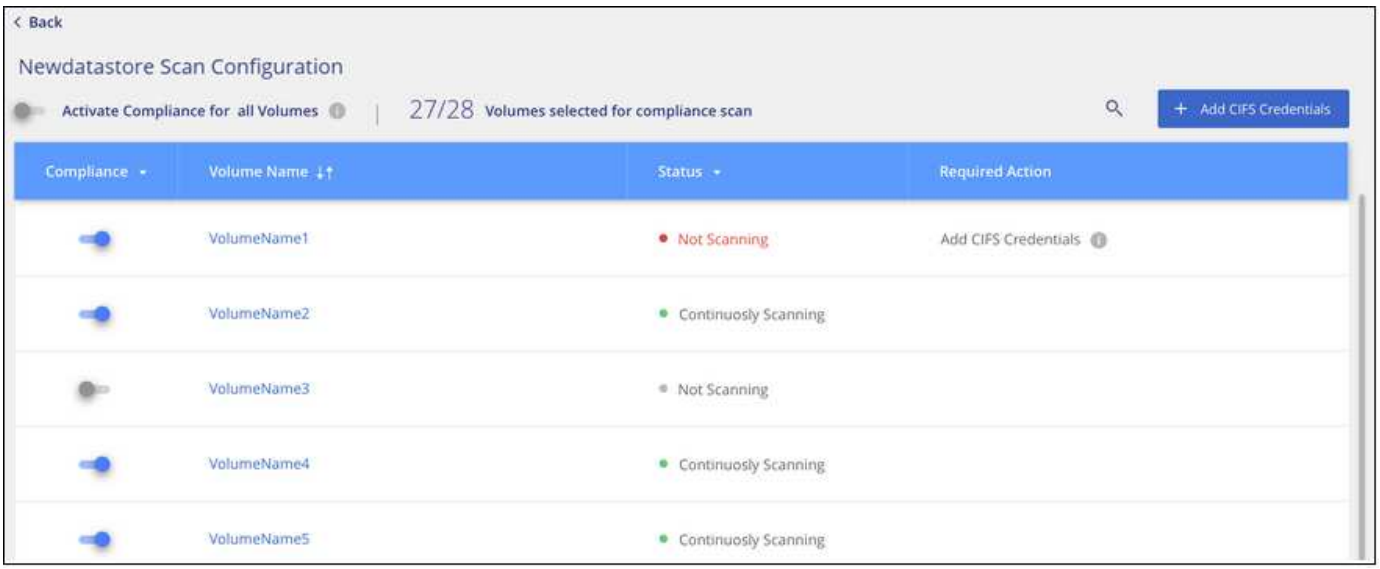
   Por ejemplo, la siguiente imagen muestra tres volúmenes; uno de los cuales no puede analizar Cloud Compliance debido a problemas de conectividad de red entre la instancia de Cloud Compliance y el

volumen.



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

Puede detener o iniciar el análisis de volúmenes en un entorno de trabajo en cualquier momento desde la página Configuración de análisis. Le recomendamos que analice todos los volúmenes.



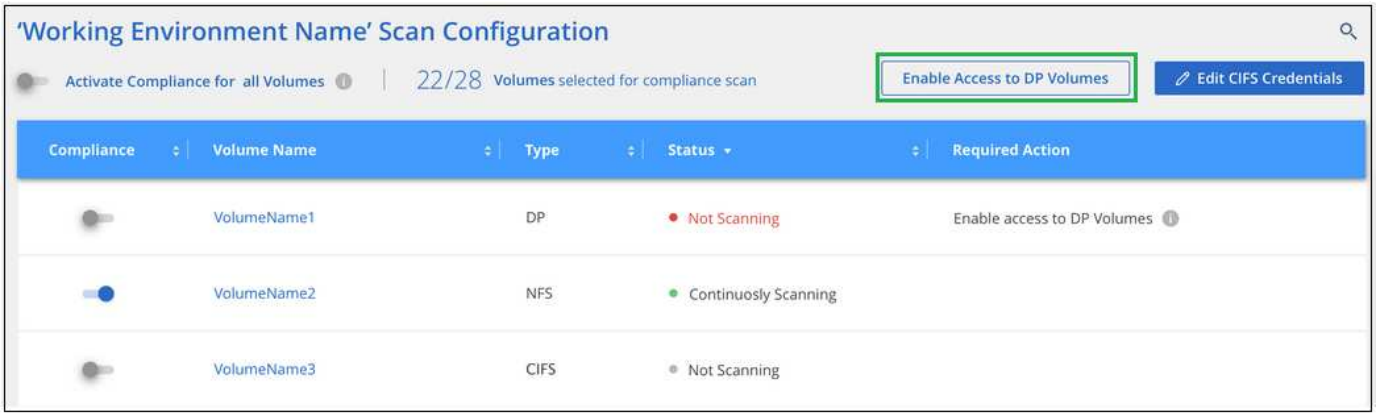
Para:	Haga lo siguiente:
Desactivar el análisis de un volumen	Mueva el control deslizante de volumen hacia la izquierda
Desactive el análisis en todos los volúmenes	Mueva el control deslizante **Activar cumplimiento para todos los volúmenes** a la izquierda
Active la búsqueda de un volumen	Mueva el control deslizante de volumen a la derecha
Active el análisis de todos los volúmenes	Mueva el control deslizante **Activar cumplimiento para todos los volúmenes** a la cierto

Los nuevos volúmenes agregados al entorno de trabajo se analizan automáticamente sólo cuando está activada la opción **Activar cumplimiento para todos los volúmenes**. Cuando este ajuste está desactivado, deberá activar el análisis en cada volumen nuevo que cree 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 que Cloud Compliance no puede acceder a ellos. Estos volúmenes suelen ser los volúmenes de destino de las operaciones de SnapMirror de un clúster ONTAP en las instalaciones.

Inicialmente, la lista de volúmenes de Cloud Compliance 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 el botón **Activar acceso a volúmenes DP** situado en la parte superior de la página.
2. Active cada volumen DP que desee analizar o utilice el control **Activar cumplimiento para todos los volúmenes** para activar todos los volúmenes, incluidos todos los volúmenes DP.

Una vez habilitada, Cloud Compliance crea un recurso compartido NFS de cada volumen DP que se activó para la opción de cumplimiento de normativas de manera que se pueda analizar. Las políticas de exportación compartidas solo permiten el acceso desde la instancia de Cloud Compliance.

Solo se muestran en la lista de volúmenes los volúmenes que se crearon inicialmente como volúmenes NFS en el sistema ONTAP de origen. Los volúmenes de origen creados inicialmente como CIFS no aparecen actualmente en Cloud Compliance.

Introducción a Cloud Compliance para Amazon S3

Cloud Compliance puede analizar sus buckets de Amazon S3 para identificar los datos personales y confidenciales que se encuentran en el almacenamiento de objetos S3. Cloud Compliance 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.

Configure los requisitos de S3 en su entorno de cloud

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

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Active Compliance en su entorno de trabajo de S3

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

Seleccione los cucharones que desea escanear

Seleccione los cubos que desea analizar y Cloud Compliance empezará a analizarlos.

Revisión de los requisitos previos de S3

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

Configurar un rol de IAM para la instancia de Cloud Compliance

Cloud Compliance 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. Cloud Manager le solicita que seleccione un rol de IAM cuando se habilita Cloud Compliance en el entorno de trabajo de Amazon S3.

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

Proporcione conectividad desde Cloud Compliance a Amazon S3

Cloud Compliance 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 VPC, asegúrese de seleccionar la región, VPC y tabla de rutas que correspondan a la instancia de Cloud Compliance. 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, Cloud Compliance no se puede conectar con el servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de 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.

Implementación de la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Debe implementar la instancia en un conector de AWS para que Cloud Manager detecte automáticamente los bloques S3 en esta cuenta de AWS y los muestre en un entorno de trabajo Amazon S3.

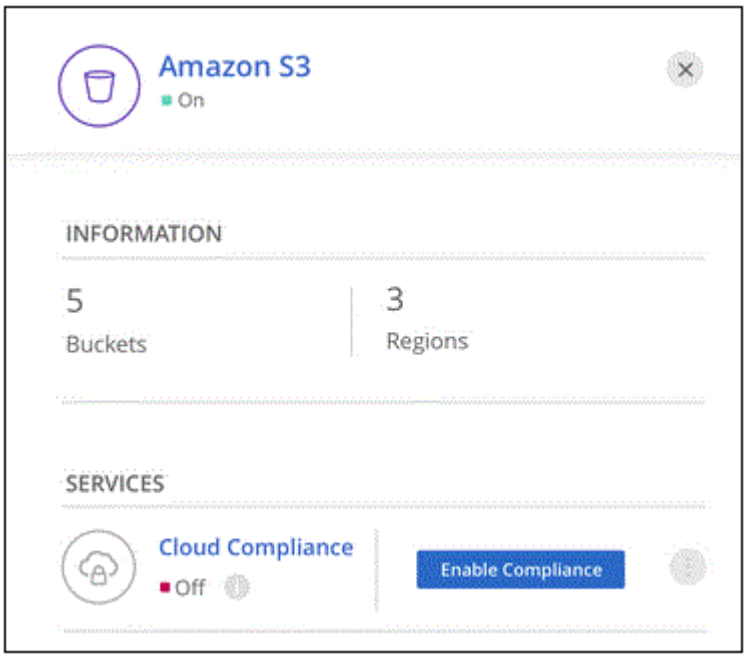
Activar el cumplimiento de normativas en el entorno de trabajo de S3

Habilite Cloud Compliance en Amazon S3 después de comprobar los requisitos previos.

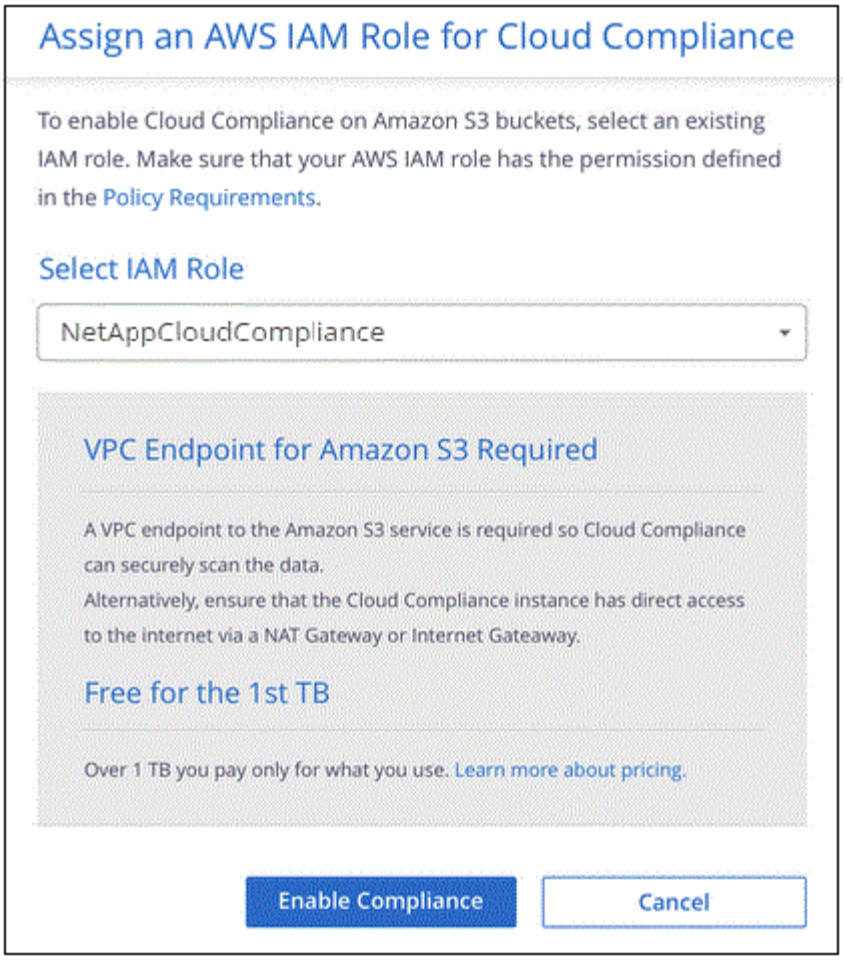
Pasos

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione el entorno de trabajo de Amazon S3.

3. En el panel de la derecha, haga clic en **Activar cumplimiento**.



4. Cuando se le solicite, asigne una función IAM a la instancia de Cloud Compliance que tiene los permisos necesarios.



5. Haga clic en **Activar cumplimiento**.

> También puede habilitar análisis de cumplimiento para un entorno de trabajo En la página Scan Configuration (Configuración de exploración), haga clic en Y seleccione **Activar cumplimiento**.

Resultado

Cloud Manager asigna el rol IAM a la instancia.

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

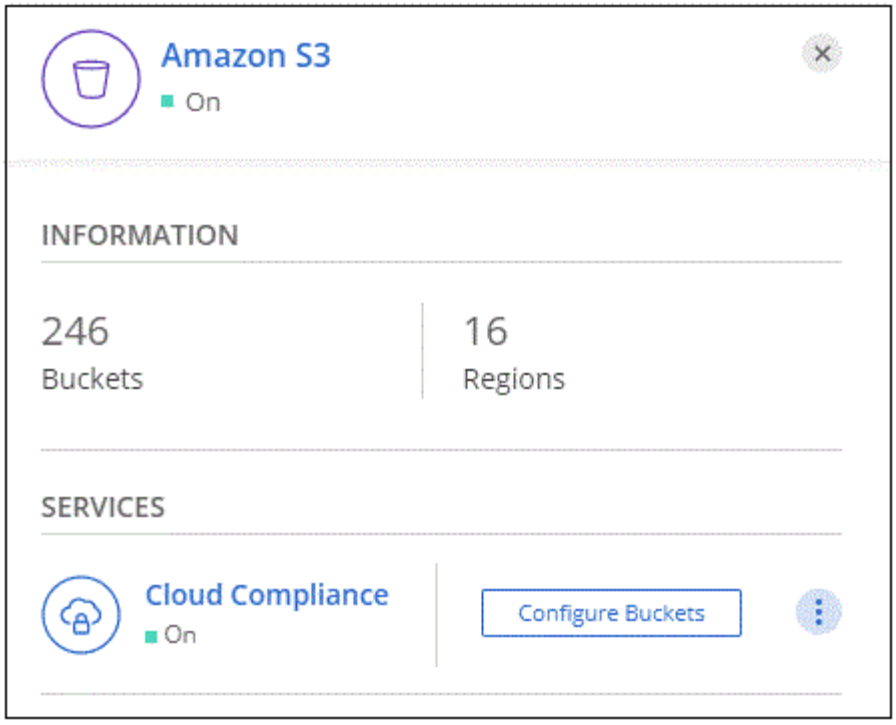
Después de que Cloud Manager habilita Cloud Compliance en Amazon S3, el paso siguiente es configurar los bloques que desea analizar.

Cuando Cloud Manager 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.

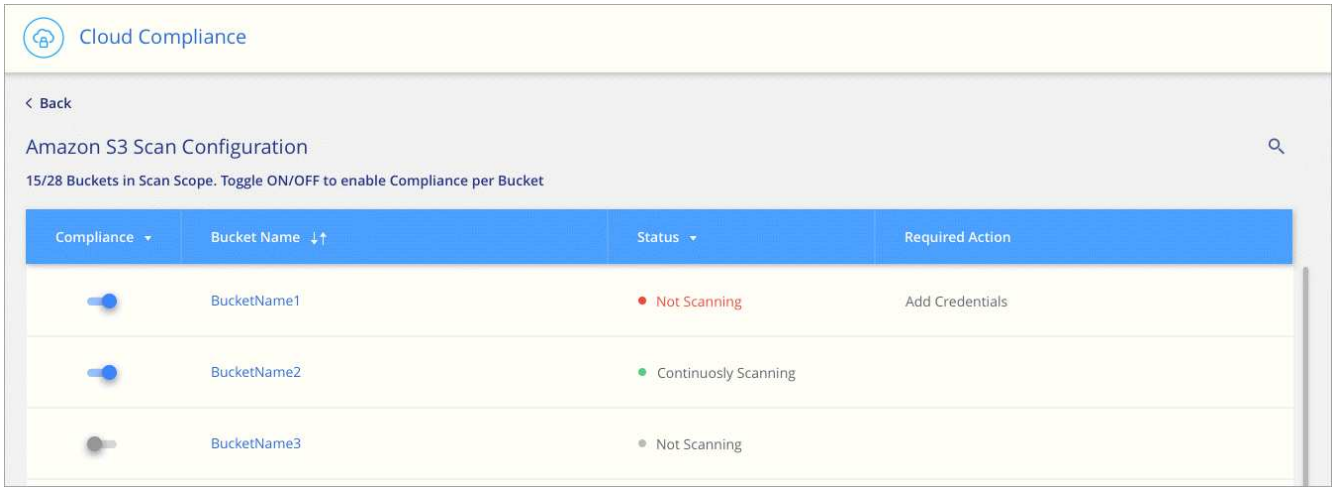
Cloud Compliance también puede Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS.

Pasos

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



3. Habilite el cumplimiento de normativas en los cucharones que desee analizar.



Resultado

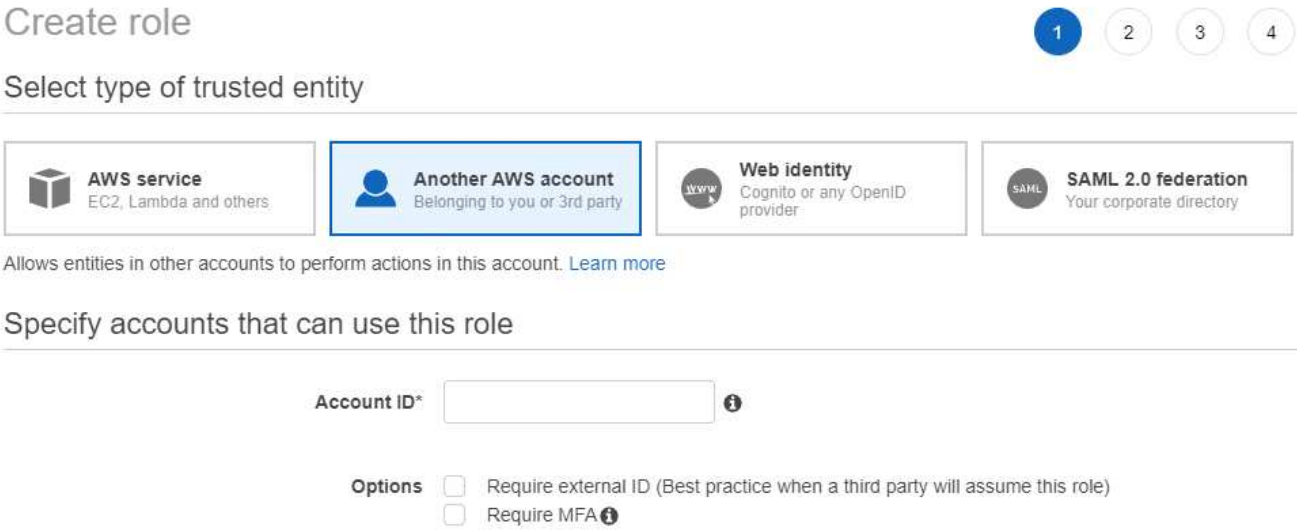
Cloud Compliance comienza a analizar los bloques de S3 que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

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 poder acceder a la instancia existente de Cloud Compliance.

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 Compliance.
- Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
- Asociar la política de IAM de cumplimiento de normativas de cloud. Asegúrese de que tiene los permisos necesarios.

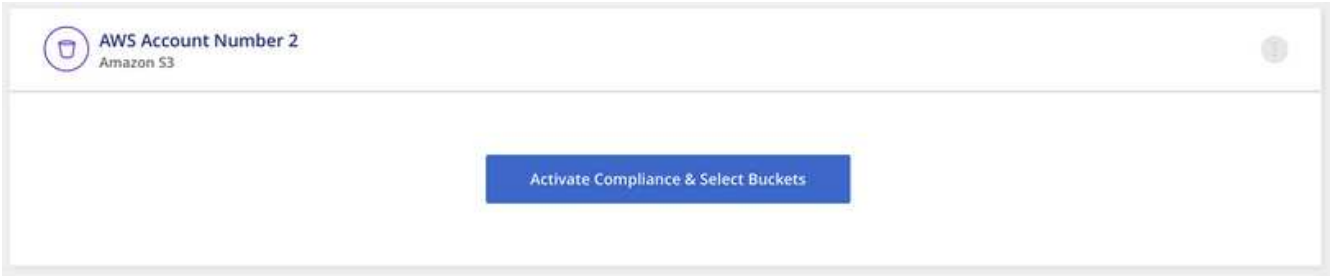
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Vaya a la cuenta de AWS de origen donde reside la instancia de Cloud Compliance y seleccione la función IAM que se adjunta 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 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 Compliance ahora tiene acceso a la cuenta de AWS adicional.

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



4. Haga clic en **Activar cumplimiento y Seleccionar cucharones** y seleccione los cucharones que desea escanear.

Resultado

Cloud Compliance 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 Compliance.

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.

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" 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 Compliance.

Bases de datos compatibles

Cloud Compliance puede analizar esquemas de las siguientes bases de datos:

- MongoDB
- 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 Compliance, independientemente de dónde se encuentre. 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 elegir un nombre de usuario y 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 Compliance con todos los permisos necesarios.

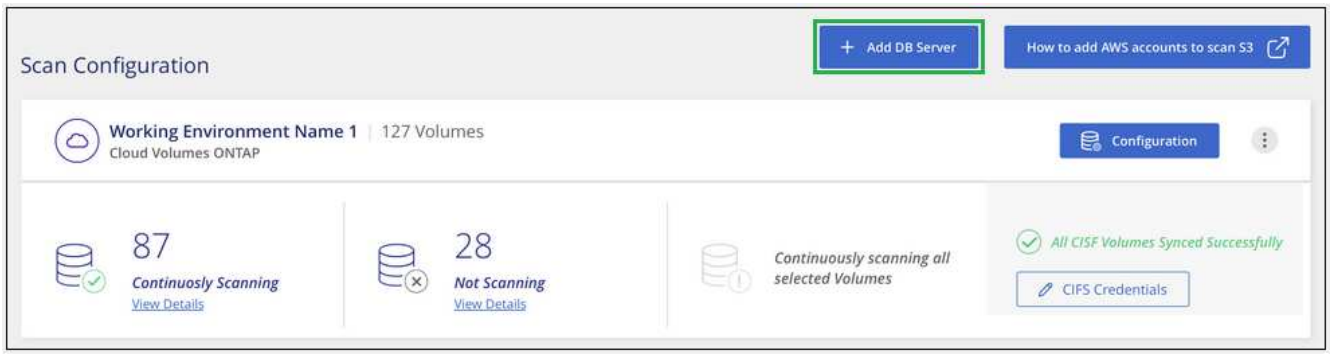
Nota: para MongoDB, se requiere una función de administrador de sólo lectura.

Agregando el servidor de la base de datos

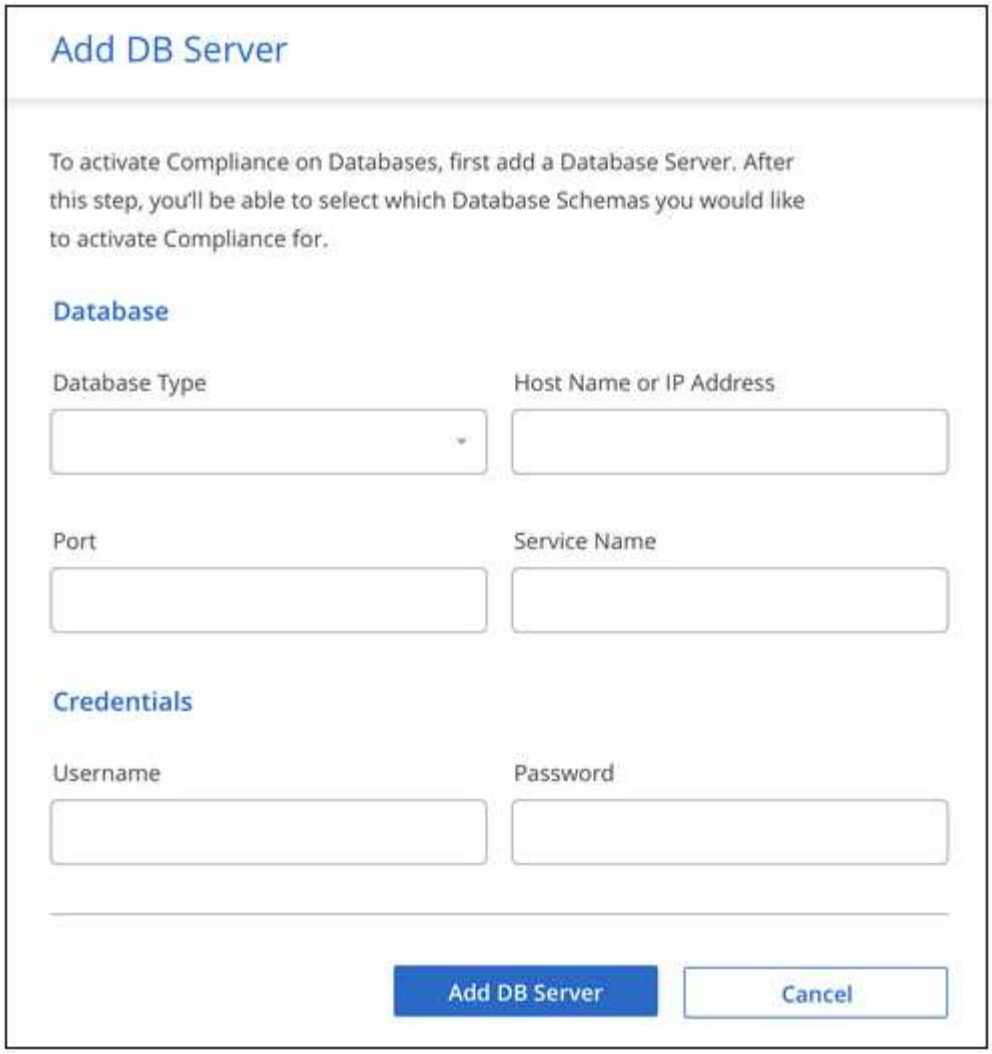
Debe tener "Ya se puso en marcha una instancia de Cloud Compliance en Cloud Manager".

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

1. En la página *Scan Configuration*, haga clic en el botón **Add DB Server**.



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 Compliance pueda acceder al servidor.
   e. Haga clic en **Agregar servidor de base de datos**.



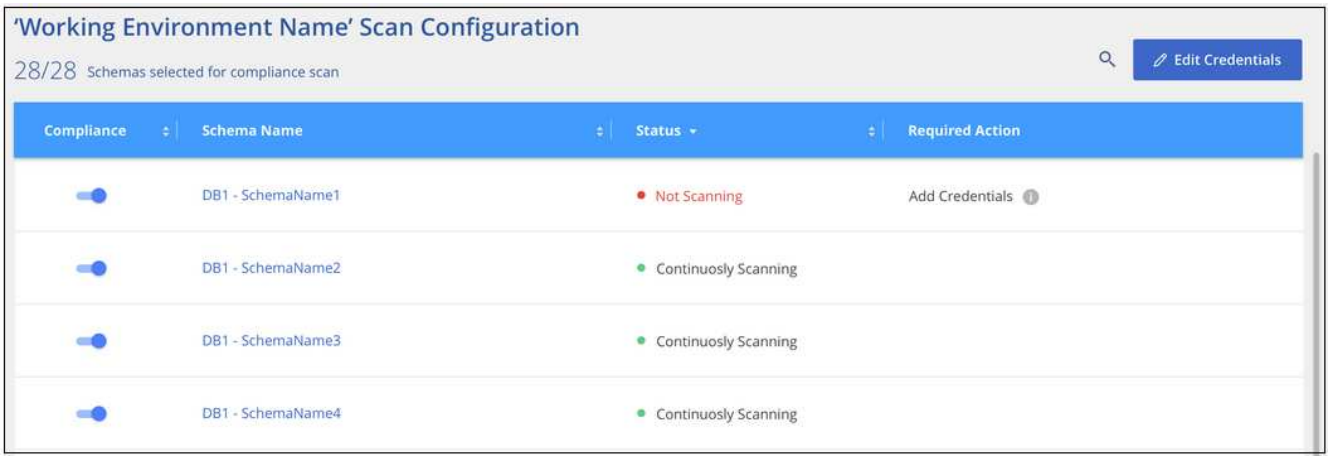
La base de datos se agrega a la lista de directorios de trabajo.

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

Puede detener o iniciar esquemas de análisis en cualquier momento.

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

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



Resultado

Cloud Compliance 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.

Quitar una base de datos de Cloud Manager

Si ya no desea analizar una determinada base de datos, puede eliminarla de la interfaz de Cloud Manager y detener todos los análisis.

En la página *Scan Configuration*, haga clic en En la fila de la base de datos y, a continuación, haga clic en **Quitar servidor de base de datos**.

Análisis de datos de ONTAP en las instalaciones con Cloud Compliance mediante SnapMirror

Puede analizar sus datos de ONTAP en las instalaciones con Cloud Compliance replicando los datos de NFS o CIFS en las instalaciones en un entorno de trabajo de Cloud Volumes ONTAP para después habilitar el cumplimiento de normativas. El análisis de los datos directamente desde un entorno de trabajo ONTAP en las instalaciones no es compatible.

Debe tener "Ya se puso en marcha una instancia de Cloud Compliance en Cloud Manager".

Pasos

1. En Cloud Manager, cree una relación de SnapMirror entre el clúster de ONTAP en las instalaciones y Cloud Volumes ONTAP.
   a. "Descubra el clúster en las instalaciones en Cloud Manager".

b. "Cree una replicación de SnapMirror entre el clúster de ONTAP en las instalaciones y. Cloud Volumes ONTAP de Cloud Manager".

2. Para los volúmenes DP creados a partir de volúmenes de origen SMB, desde la interfaz de línea de comandos de ONTAP, configure los volúmenes de destino SMB para el acceso a los datos. (Esto no es necesario en los volúmenes NFS porque el acceso a los datos se habilita de forma automática mediante Cloud Compliance).
   a. "Cree un recurso compartido de SMB en el volumen de destino".
   b. "Aplique las ACL adecuadas para el recurso compartido de SMB en el volumen de destino".
3. En Cloud Manager, active Cloud Compliance en el entorno de trabajo de Cloud Volumes ONTAP que contiene los datos de SnapMirror:
   a. Haga clic en **entornos de trabajo**.
   b. Seleccione el entorno de trabajo que contiene los datos de SnapMirror y haga clic en **Activar cumplimiento**.

      "Haga clic aquí si necesita ayuda para habilitar Cloud Compliance En un sistema Cloud Volumes ONTAP".

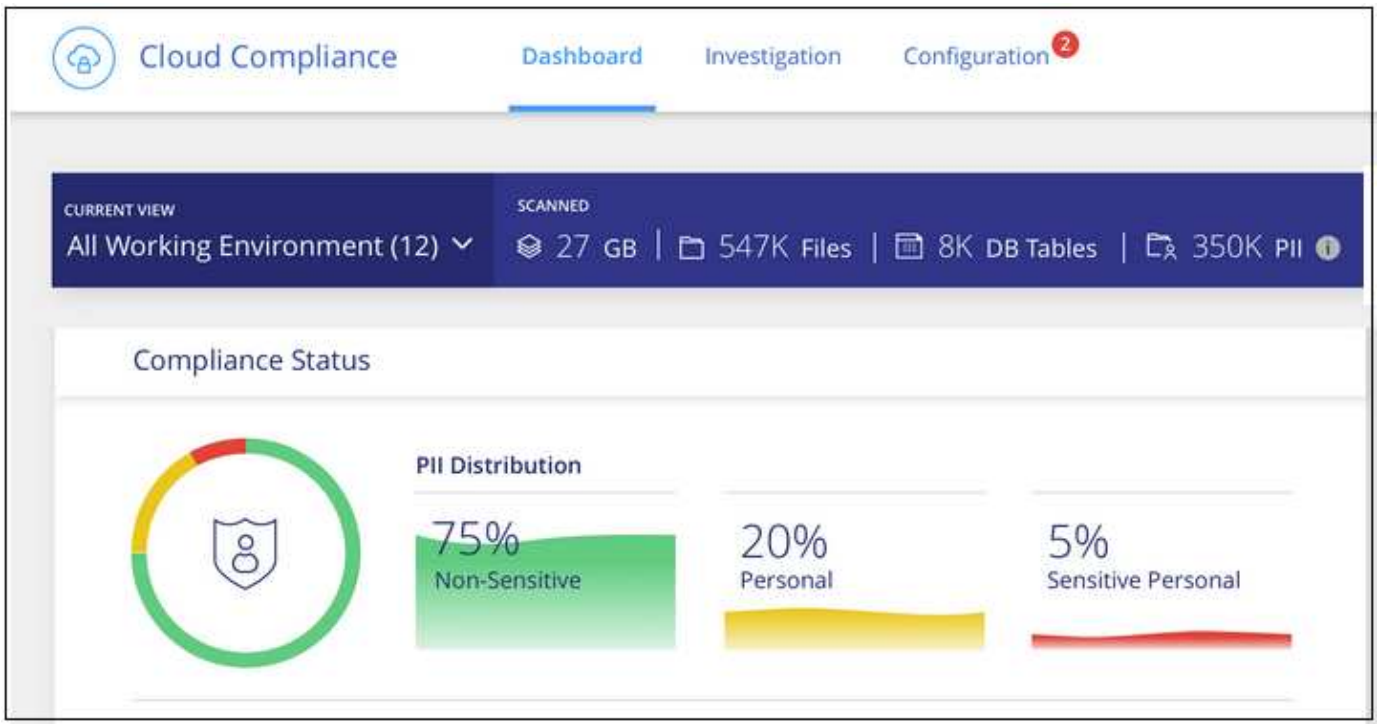
   c. Haga clic en el botón **Activar acceso a volúmenes DP** situado en la parte superior de la página *Scan Configuration*.
   d. Active cada volumen DP que desee analizar o utilice el control **Activar cumplimiento para todos los volúmenes** para activar todos los volúmenes, incluidos todos los volúmenes DP.

Consulte "Análisis de volúmenes de protección de datos" Para obtener más información sobre el análisis de volúmenes DP.

Obtener visibilidad y control de los datos privados

Controle sus datos privados al ver los detalles sobre los datos personales y los datos personales confidenciales de su empresa. También puede ver las categorías y los tipos de archivos que cumple con las normativas del cloud de los datos.

De forma predeterminada, la consola de Cloud Compliance muestra los datos de cumplimiento de normativas de todas las bases de datos y entornos de trabajo.



Si sólo desea ver datos para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

Datos personales

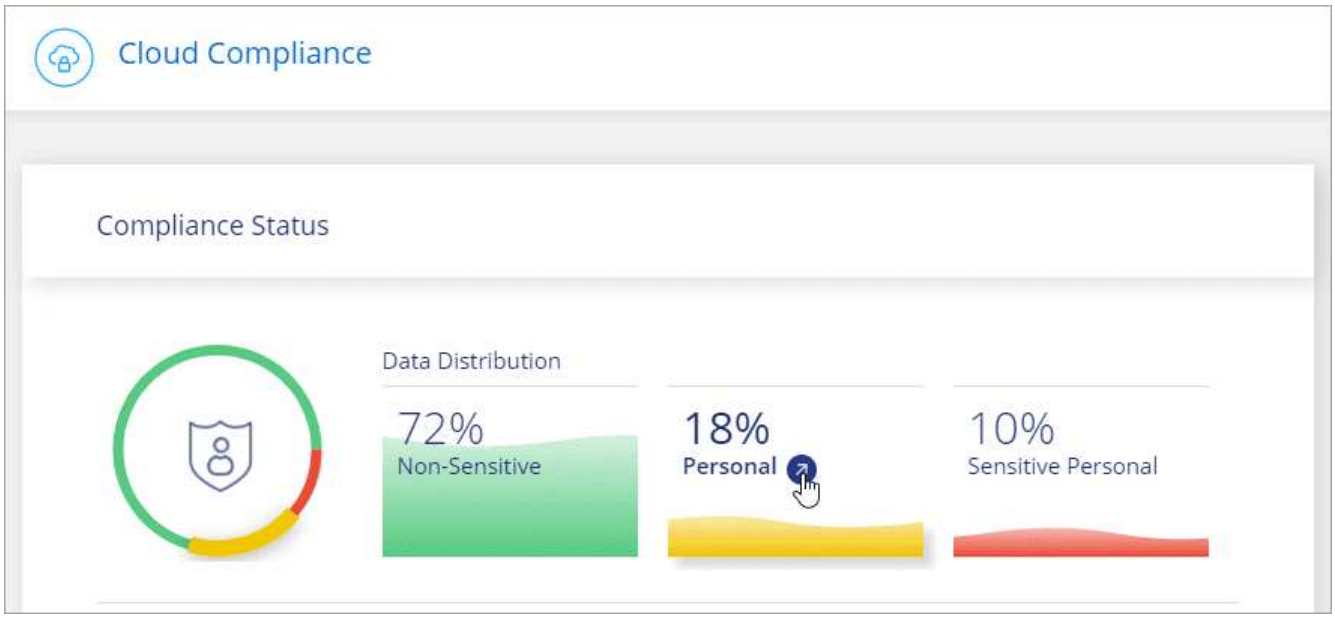
Cloud Compliance identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria y mucho más. Consulte la lista completa.

Para algunos tipos de datos personales, Cloud Compliance utiliza *proximity validation* para validar sus hallazgos. La validación se produce buscando una o más palabras clave predefinidas cerca de los datos personales encontrados. Por ejemplo, Cloud Compliance identifica una normativa estadounidense Número de seguridad social (SSN) como un SSN si ve una palabra de proximidad junto a ella (por ejemplo, *SSN* o *seguridad social*). La siguiente lista Muestra cuándo Cloud Compliance utiliza la validación de proximidad.

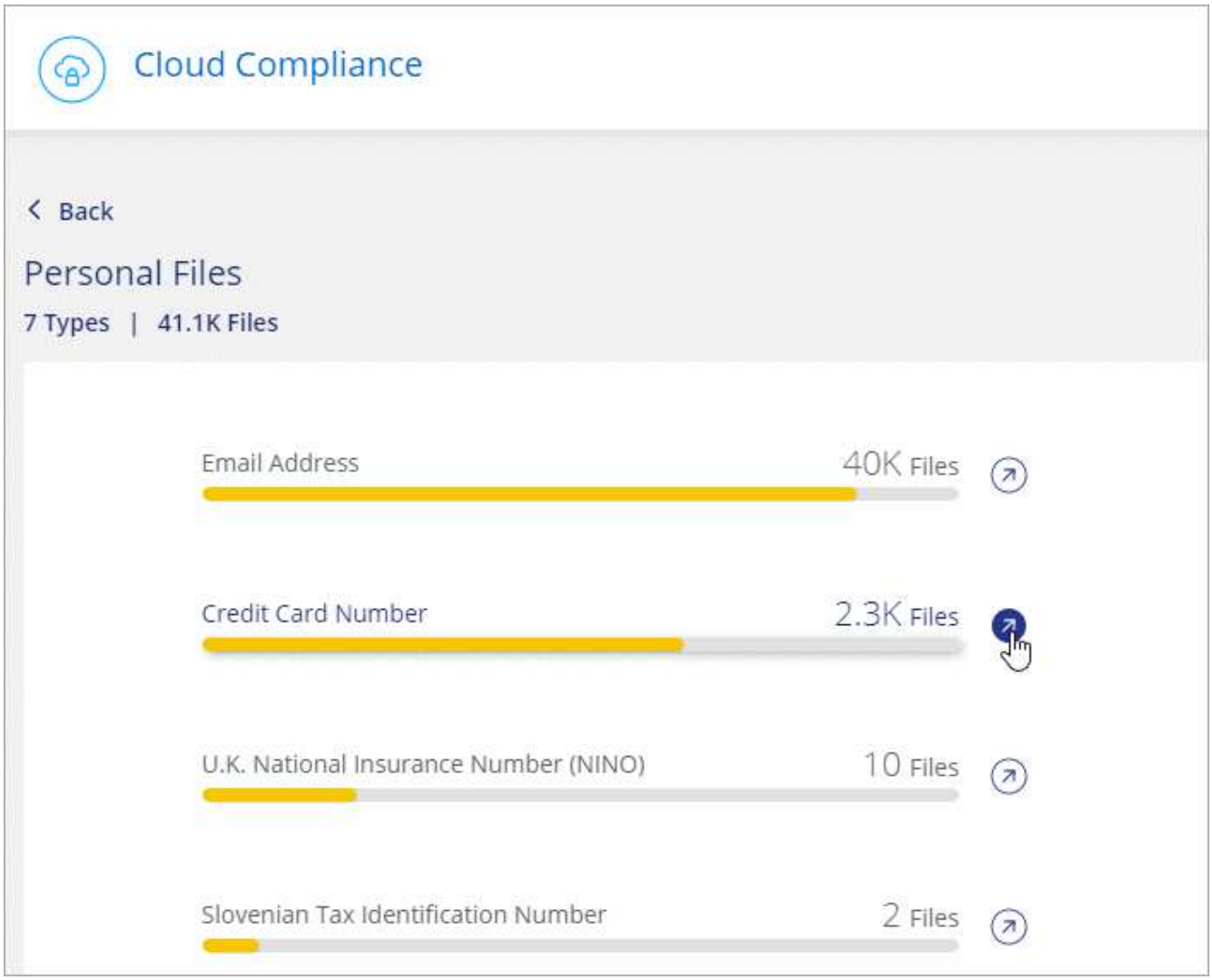
Visualización de archivos que contienen datos personales

Pasos

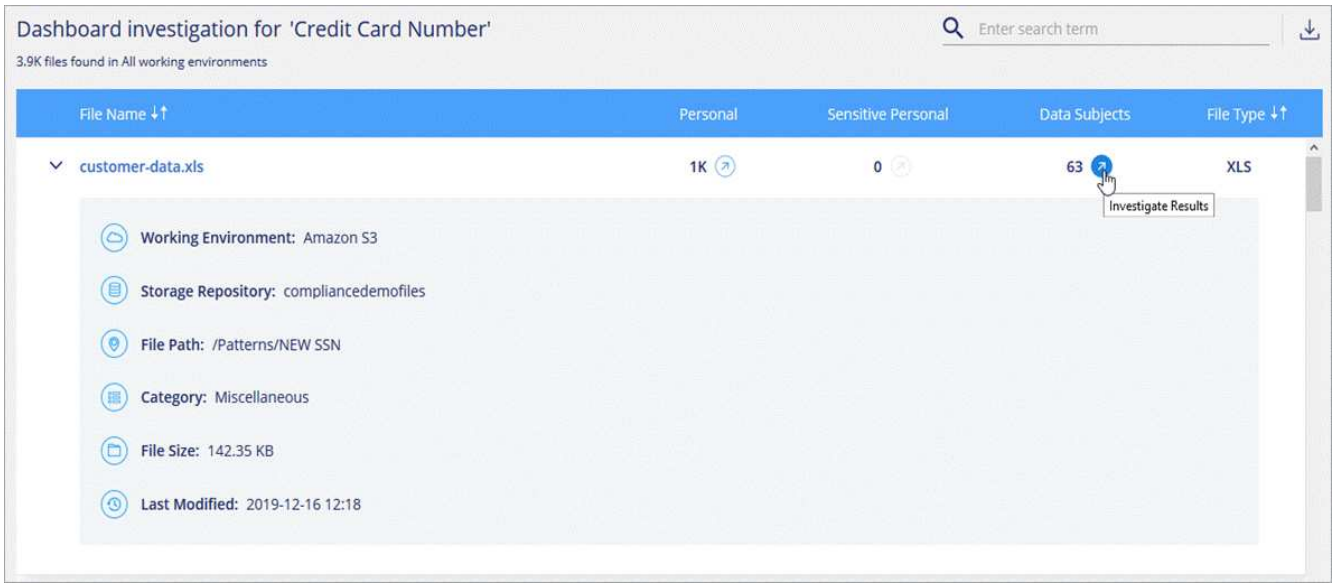
1. En la parte superior de Cloud Manager, haga clic en **cumplimiento de la nube** y haga clic en la ficha **Panel**.
2. Para investigar los detalles de todos los datos personales, haga clic en el icono situado junto al porcentaje de datos personales.



3. Para investigar los detalles de un tipo específico de datos personales, haga clic en **Ver todos** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales.

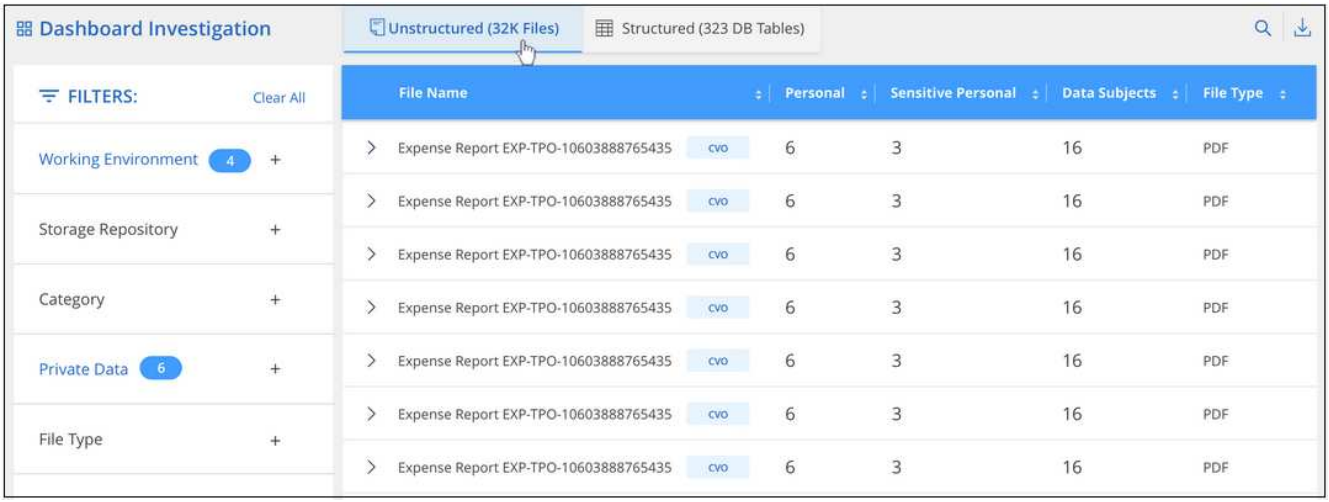


4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.



5. También puede filtrar el contenido de la página Investigación para que muestre solo los resultados que desea ver. Las pestañas de nivel superior le permiten ver datos de archivos (datos no estructurados) o de bases de datos (datos estructurados).

   A continuación, dispone de filtros para entorno de trabajo, repositorio de almacenamiento, categoría, datos privados, tipo de archivo, Fecha de la última modificación, y si los permisos del objeto S3 están abiertos al acceso público.



Tipos de datos personales

Los datos personales encontrados en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna identifica si Cloud Compliance utiliza validación de proximidad validar los resultados del identificador.

Tipo	Identificador	¿validación de proximidad?
Generales	Dirección de correo electrónico	No
	Número de tarjeta de crédito	No
	Número de iban (número de cuenta bancaria internacional)	No

Tipo	Identificador	¿validación de proximidad?
Identificadores nacionales	ID belga (Numero Nacional)	Sí
	ID brasileño (CPF)	Sí
	ID búlgaro (UCN)	Sí
	Licencia de conducir de California	Sí
	Croata ID (OIB)	Sí
	Número de identificación fiscal de Chipre (TIC)	Sí
	ID checo/eslovaco	Sí
	ID danés (CPR)	Sí
	Dutch ID (BSN)	Sí
	Identificación Estonia	Sí
	Finlandés ID (HETU)	Sí
	Número de identificación fiscal francés (SPI)	Sí
	Número de identificación fiscal alemán (Steuerliche Identifikationsnummer)	Sí
	ID griego	Sí
	Número de identificación fiscal húngaro	Sí
	Irish ID (PPS)	Sí
	Documento de identidad israelí	Sí
	Número de identificación fiscal italiana	Sí
	ID letón	Sí
	ID lituano	Sí
	ID de Luxemburgo	Sí
	Identificación maltesa	Sí
	Identificación polaca (PESEL)	Sí
	Número de identificación fiscal (NIF) en portugués	Sí
	Rumano ID (CNP)	Sí
	ID esloveno (EMSO)	Sí
	ID sudafricano	Sí
	Número de identificación fiscal en español	Sí
	ID sueco	Sí
	REINO UNIDO ID (NINO)	Sí
	Número de Seguro Social de Estados Unidos (SSN)	Sí

Datos personales confidenciales

Cloud Compliance identifica automáticamente los tipos especiales de información personal confidencial, tal como se definen en normativas de privacidad como "Artículos 9 y 10 del RGPD". Por ejemplo, información sobre la salud, origen étnico o orientación sexual de una persona. Consulte la lista completa.

Cloud Compliance utiliza la inteligencia artificial (IA), el procesamiento de lenguaje natural (NLP), el aprendizaje automático (ML) y la computación cognitiva (CC) para comprender el significado del contenido que analiza con el fin de extraer entidades y categorizar según sea necesario.

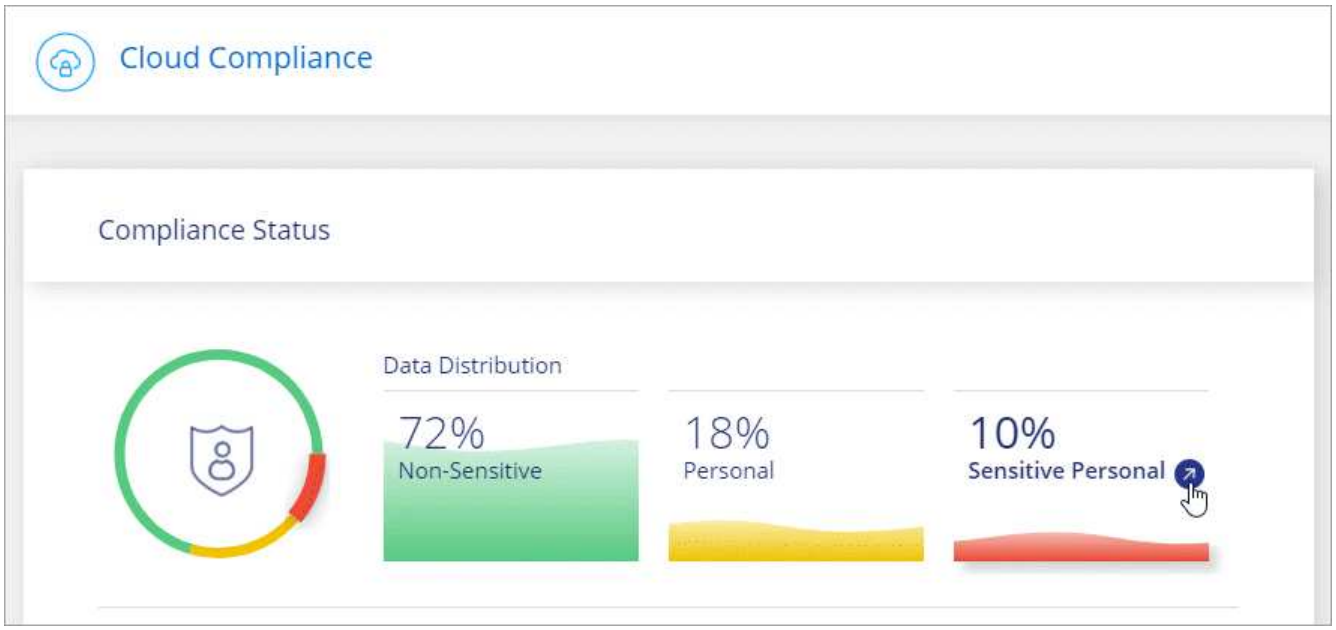
Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Debido a sus habilidades para NLP, Cloud Compliance puede distinguir la diferencia entre una frase que dice "George es mexicano" (que indica datos confidenciales como se especifica en el artículo 9 del RGPD), frente a "George está comiendo comida mexicana".

Sólo se admite inglés cuando se escanea datos personales confidenciales. Más adelante se añadirá compatibilidad con más idiomas.

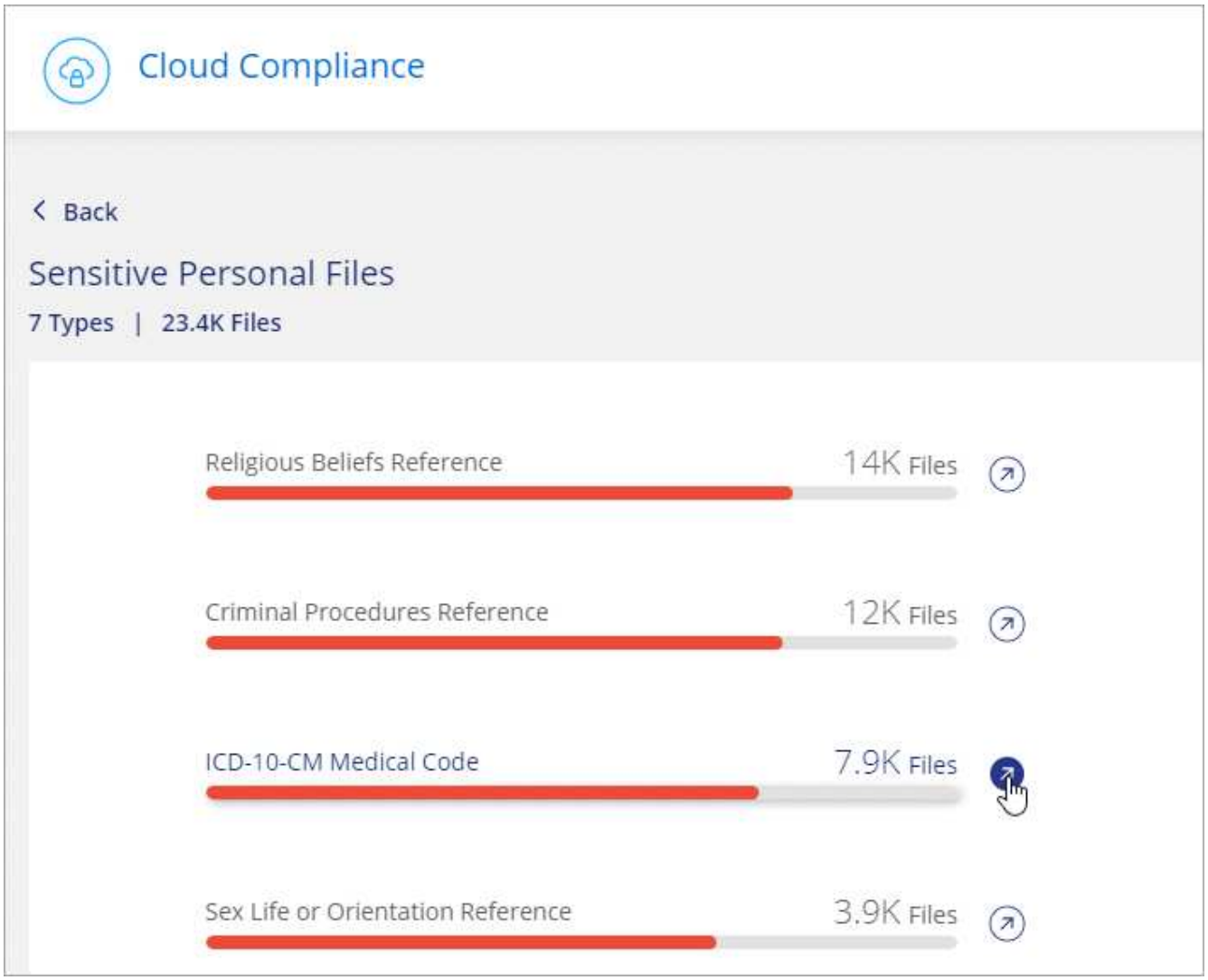
Visualización de archivos que contienen datos personales confidenciales

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Para investigar los detalles de todos los datos personales confidenciales, haga clic en el icono situado junto al porcentaje de datos personales confidenciales.



3. Para investigar los detalles de un tipo específico de datos personales confidenciales, haga clic en **Ver todo** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales confidenciales.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de datos personales confidenciales

Los datos personales confidenciales que Cloud Compliance puede encontrar en los archivos incluyen los siguientes:

Procedimientos penales referencia
Datos relativos a las condenas y delitos penales de una persona natural.

Referencia étnica
Datos relativos al origen racial o étnico de una persona natural.

Referencia de Salud
Datos relativos a la salud de una persona física.

Códigos médicos ICD-9-cm
Códigos utilizados en la industria médica y de la salud.

Códigos médicos ICD-10-cm

Códigos utilizados en la industria médica y de la salud.

Creencias filosóficas referencia

Datos relativos a las creencias filosóficas de una persona natural.

Referencia de creencias religiosas

Datos relativos a las creencias religiosas de una persona natural.

Referencia de vida sexual o orientación

Datos relativos a la vida sexual o la orientación sexual de una persona natural.

Categorías

Cloud Compliance toma los datos que ha analizado y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. Vea la lista de categorías.

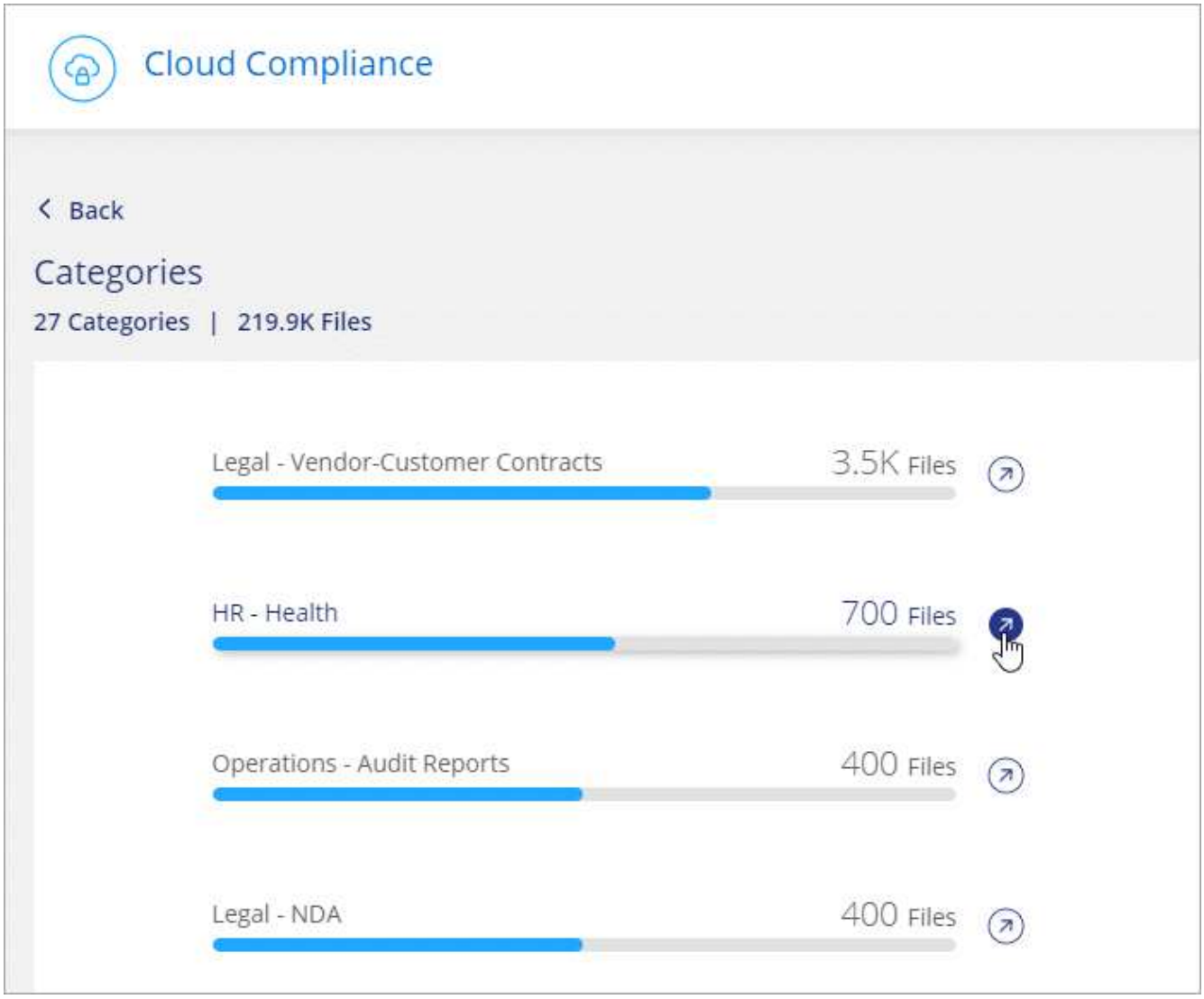
Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

Solo se admite inglés para categorías. Más adelante se añadirá compatibilidad con más idiomas.

Ver archivos por categorías

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en el icono **investigar resultados** de una de las 4 categorías principales directamente desde la pantalla principal, o haga clic en **Ver todos** y luego haga clic en el icono de cualquiera de las categorías.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de categorías

Cloud Compliance categoriza sus datos de la siguiente manera:

Finanzas

- Hojas de balance
- Órdenes de compra
- Facturas
- Informes trimestrales

RR. HH

- Comprobaciones de fondo
- Planes de compensación
- Contratos de empleados
- Revisiones de empleados

- Salud
- Se reanudará

Legal
- NDAS
- Contratos con el proveedor y el cliente

Marketing
- Campañas
- Conferencias

Operaciones
- Informes de auditoría

Ventas
- Pedidos de ventas

Servicios
- RFI
- RFP
- CERDA
- Entrenamiento

Soporte técnico
- Quejas y boletos

Categorías de metadatos
- Datos de aplicaciones
- Archivos de archivo
- Audio
- Datos de aplicaciones de negocio
- Archivos CAD
- Codificación
- Archivos de base de datos e índice
- Archivos de diseño
- Datos de aplicación de correo electrónico
- Ejecutables
- Datos de aplicaciones financieras
- Datos de aplicación de salud
- Imágenes
- Registros
- Documentos varios
- Presentaciones diversas

- Hojas de cálculo varias
- Vídeos

Tipos de archivo

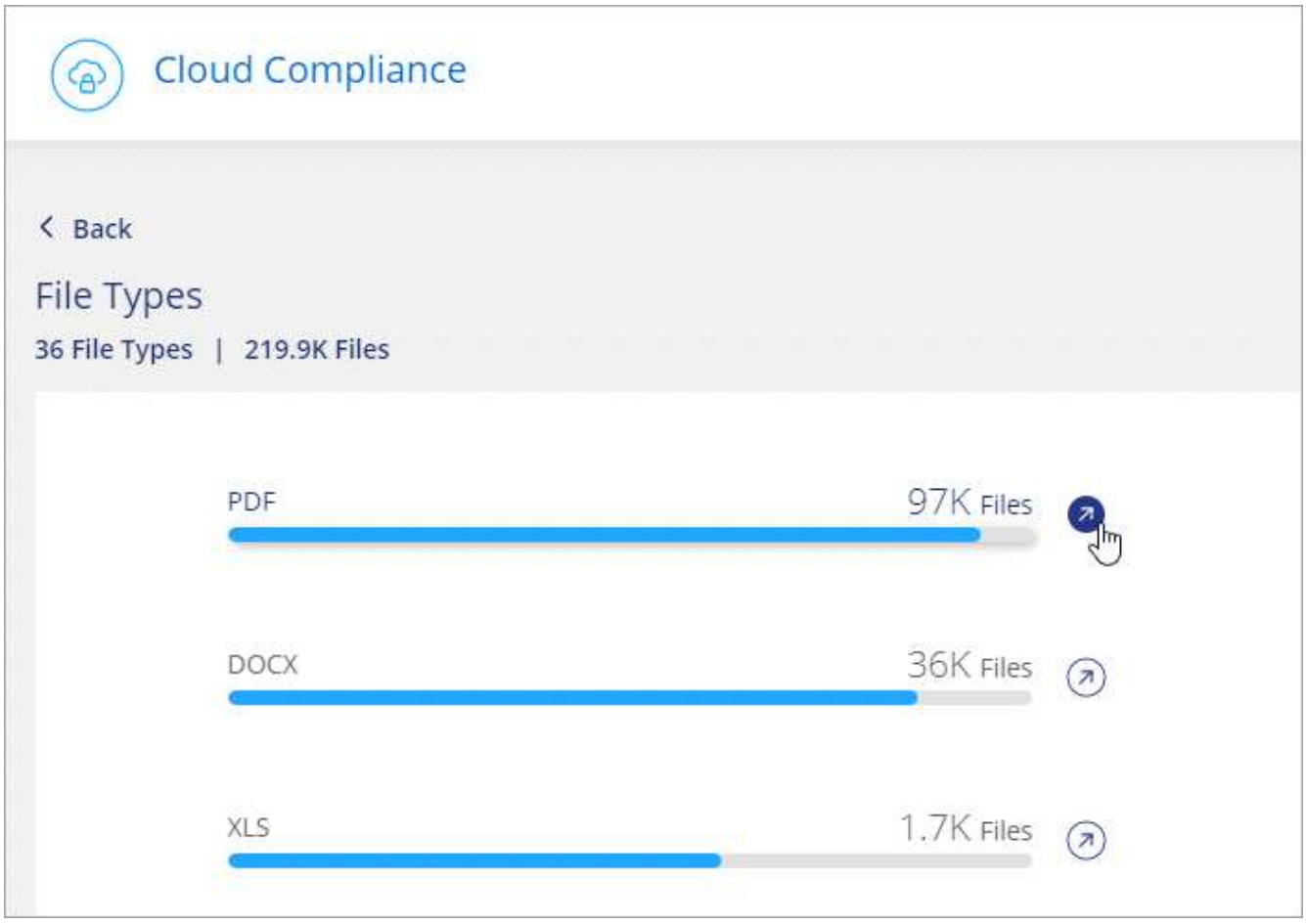
Cloud Compliance toma los datos que ha analizado y los divide por tipo de archivo. La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente. Consulte la lista de tipos de archivo.

Por ejemplo, puede almacenar archivos CAD que incluyan información muy confidencial sobre su organización. Si no está seguro, puede tomar el control de los datos confidenciales restringiendo permisos o moviendo los archivos a otra ubicación.

Visualización de tipos de archivo

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en el icono **investigar resultados** de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y, a continuación, haga clic en el icono de cualquiera de los tipos de archivo.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de archivos

Cloud Compliance analiza todos los archivos para obtener información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Pero cuando Cloud Compliance detecta la información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo: .PDF, .DOCX, .DOC, .PPTX, .XLS, .CSV, .TXT, .RTF y .JSON.

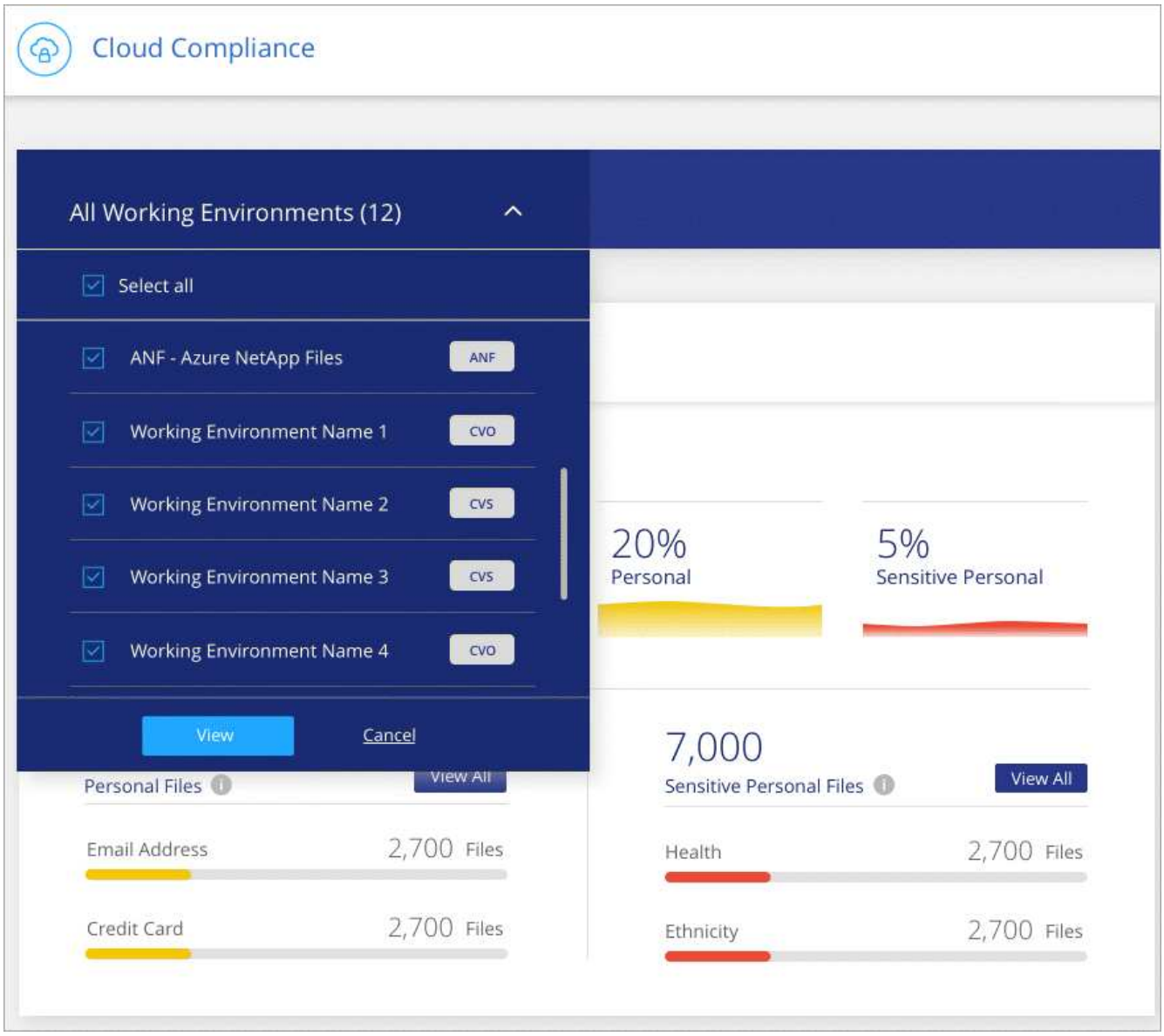
Visualización de datos de entornos de trabajo específicos

Puede filtrar el contenido del panel de Cloud Compliance para ver los datos de cumplimiento de normativas de todos los entornos de trabajo y bases de datos, o solo en entornos de trabajo específicos.

Al filtrar la consola, Cloud Compliance determina los datos de cumplimiento de normativas e informa solo a los entornos de trabajo que haya seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Precisión de la información encontrada

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

La siguiente tabla, basada en nuestras pruebas, muestra la precisión de la información que encuentra Cloud Compliance. La dividiremos por *precision* y *RECALL*:

Precisión

La probabilidad de que lo que encontró el cumplimiento de cloud se haya identificado correctamente. Por ejemplo, una tasa de precisión del 90% para los datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal contienen realmente información personal. 1 de cada 10 archivos sería un falso positivo.

Recuperar

La probabilidad de que el cumplimiento de normativas en el cloud encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70 % para los datos personales significa que Cloud Compliance puede identificar 7 de cada 10 archivos que contienen información personal en su organización. Cloud

Compliance faltaría el 30 % de los datos y no aparecerá en el panel.

Cloud Compliance se encuentra en un lanzamiento de disponibilidad controlado y constantemente mejoramos la precisión de los resultados. Dichas mejoras estarán disponibles automáticamente en los próximos lanzamientos de Cloud Compliance.

Tipo	Precisión	Recuperar
Datos personales - General	90%-95%	60%-80%
Datos personales: Identificadores de país	30%-60%	40%-60%
Datos personales confidenciales	80%-95%	20%-30%
Categorías	90%-97%	60%-80%

Qué se incluye en cada informe de lista de archivos (archivo CSV)

Desde cada página de investigación puede descargar listas de archivos (en formato CSV) que incluyen detalles sobre los archivos identificados. Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista.

Cada lista de archivos incluye la siguiente información:

- Nombre de archivo
- Tipo de ubicación
- Entorno de trabajo
- Repositorio de almacenamiento
- Protocolo
- Ruta del archivo
- Tipo de archivo
- Categoría
- Información personal
- Información personal confidencial
- Fecha de detección de eliminación

  Una fecha de detección de eliminación identifica la fecha en la que se eliminó o movió el archivo. Esto le permite identificar cuándo se han movido los archivos confidenciales. Los archivos eliminados no forman parte del recuento de números de archivo que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

Ver informes de cumplimiento

Cloud Compliance proporciona informes que puede usar para comprender mejor el estado del programa de privacidad de datos de su organización.

De forma predeterminada, la consola de Cloud Compliance muestra los datos de cumplimiento de normativas de todas las bases de datos y entornos de trabajo. Si desea ver informes que contengan datos sólo para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

Informe de evaluación del riesgo de privacidad

El informe de evaluación de riesgos de privacidad proporciona una descripción general del estado de riesgo de privacidad de su organización, tal y como lo exigen las normativas de privacidad como RGPD y CCPA. El informe incluye la siguiente información:

Estado de cumplimiento

A. puntuación de gravedad y la distribución de los datos, ya sean personales, confidenciales o no confidenciales.

Descripción general de la evaluación

Desglose de los tipos de datos personales encontrados, así como de las categorías de datos.

Datos sujetos en esta evaluación

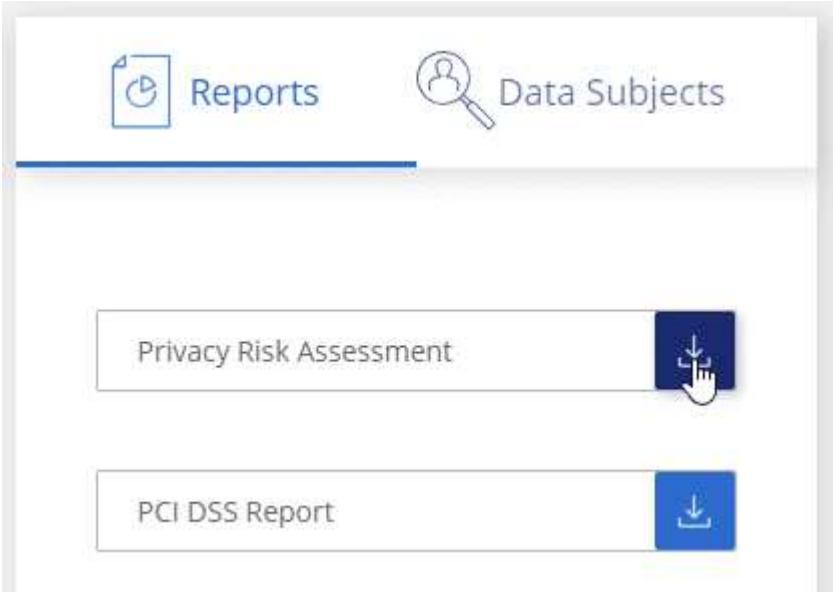
El número de personas, por ubicación, para las cuales se encontraron identificadores nacionales.

Generación del Informe de Evaluación de riesgo de Privacidad

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **Evaluación de riesgo de privacidad**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Puntuación de gravedad

Cloud Compliance calcula la puntuación de gravedad del informe de evaluación del riesgo de privacidad sobre la base de tres variables:

- El porcentaje de datos personales de todos los datos.
- El porcentaje de datos personales confidenciales de todos los datos.
- El porcentaje de archivos que incluyen temas de datos, determinado por identificadores nacionales como ID nacionales, números de Seguro Social y números de identificación fiscal.

La lógica utilizada para determinar la puntuación es la siguiente:

Puntuación de gravedad	Lógica
0	Las tres variables son exactamente 0 %
1	Una de las variables es mayor que 0 %
2	Una de las variables es mayor que el 3 %
3	Dos de las variables son mayores que el 3%
4	Tres de las variables son mayores que el 3%
5	Una de las variables es mayor que el 6 %
6	Dos de las variables son mayores que el 6%
7	Tres de las variables son mayores que el 6%
8	Una de las variables es mayor que el 15 %
9	Dos de las variables son mayores que el 15%
10	Tres de las variables son mayores que el 15%

Informe PCI DSS

El Informe de estándares de seguridad de datos del sector de la tarjeta de pago (PCI DSS) puede ayudarle a identificar la distribución de información de la tarjeta de crédito a través de sus archivos. El informe incluye la siguiente información:

Descripción general
: Cuántos archivos contienen información de tarjeta de crédito y en qué entornos de trabajo.

Cifrado
: Porcentaje de archivos que contienen información de la tarjeta de crédito en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware
: Porcentaje de archivos que contienen información de tarjetas de crédito en entornos de trabajo que tienen o no la protección contra ransomware habilitada. Esta información es específica de Cloud Volumes ONTAP.

Retención
: El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de la tarjeta de crédito por más tiempo de lo que necesita para procesarla.

Distribución de la información de la tarjeta de crédito

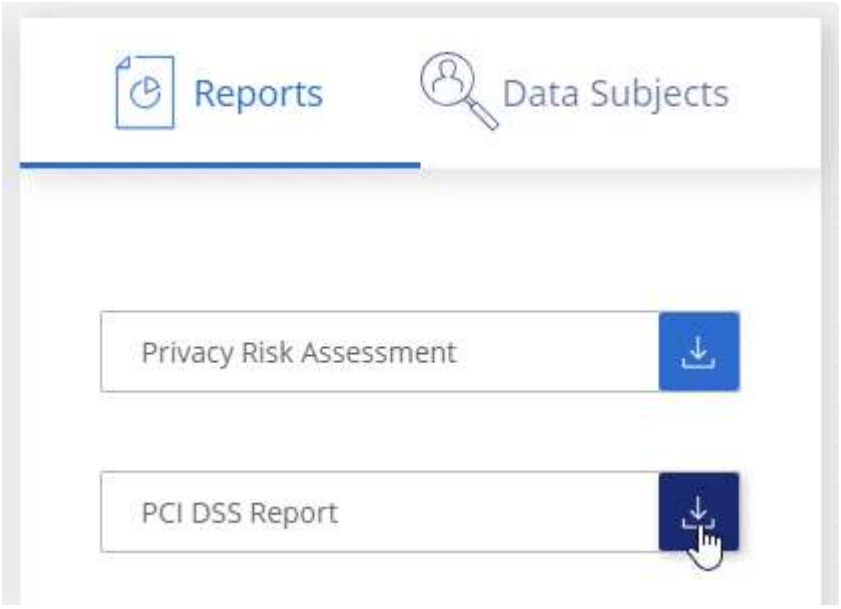
Entornos en los que se encontró la información de la tarjeta de crédito y si la protección mediante cifrado y ransomware están habilitadas.

Generación del informe PCI DSS

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **PCI DSS Report**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Informe HIPAA

El Informe de la Ley de Portabilidad y responsabilidad de los Seguros médicos (HIPAA) puede ayudarle a identificar archivos que contengan información médica. Está diseñado para ayudar en el requisito de su organización de cumplir con las leyes de privacidad de datos HIPAA. El Cloud Compliance de información incluye:

- Patrón de referencia de salud
- Código médico ICD-10-cm
- Código médico ICD-9-cm
- HR – Categoría de salud
- Datos de aplicación de Salud

El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información médica y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información médica en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información médica en entornos de trabajo que tienen o no la protección contra ransomware activada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de salud por más tiempo de lo que necesita para procesarla.

Distribución de la información de salud

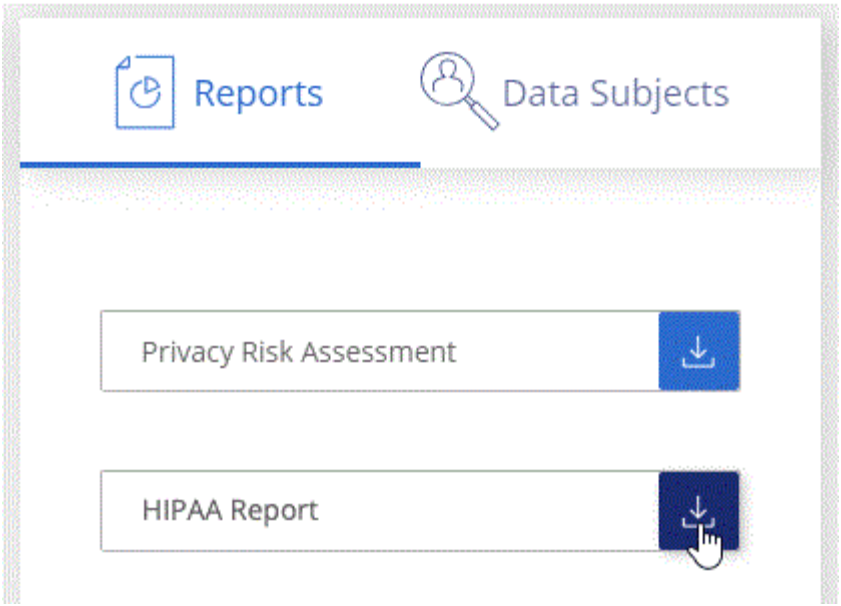
Entornos en los que se encontró la información médica y si está habilitada el cifrado y la protección contra ransomware.

Generación del informe HIPAA

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **Informe HIPAA**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Selección de los entornos de trabajo para los informes

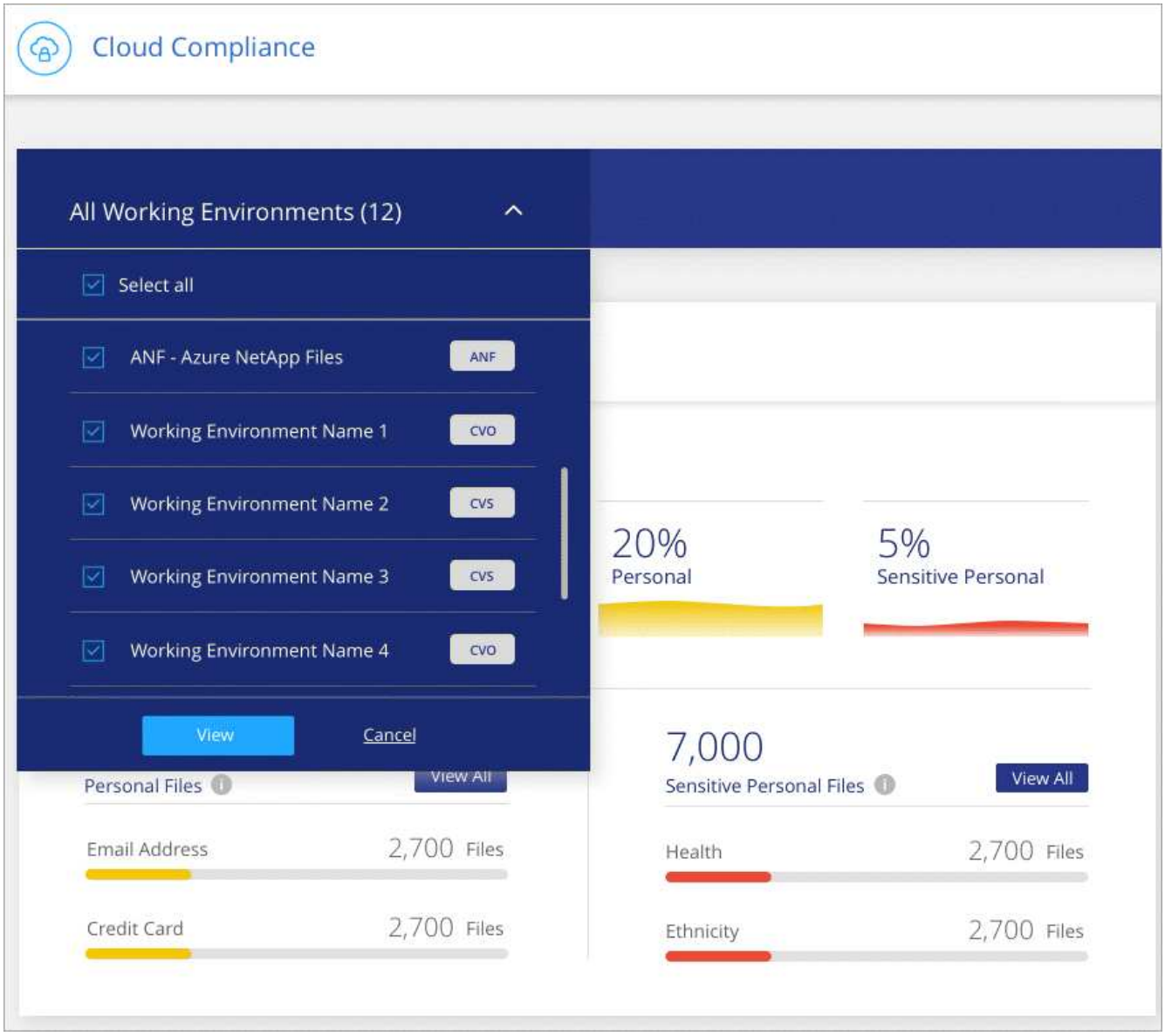
Puede filtrar el contenido del panel de Cloud Compliance para ver los datos de cumplimiento de normativas de

todos los entornos de trabajo y bases de datos, o solo en entornos de trabajo específicos.

Al filtrar la consola, Cloud Compliance determina los datos de cumplimiento de normativas e informa solo a los entornos de trabajo que haya seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Respuesta a una solicitud de acceso de un sujeto de datos

Responda a una solicitud de acceso a un sujeto de datos (DSAR) buscando el nombre completo o el identificador conocido de un sujeto (como una dirección de correo electrónico) y, a continuación, descargando un informe. El informe está diseñado para ayudar en el requisito de su organización a cumplir con el RGPD o con leyes de privacidad de datos similares.

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

¿Qué es una solicitud de acceso de asunto de datos?

Las normas de privacidad, como el GDPR europeo, otorgan a sujetos de datos (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un sujeto de datos solicita esta información, se le conoce como DSAR (solicitud de acceso a sujetos de datos). Las organizaciones deben responder a estas solicitudes "sin demora indebida" y, a más tardar, en el plazo de un mes a partir de su recepción.

¿Cómo puede ayudarle Cloud Compliance a responder a un DSAR?

Cuando realiza una búsqueda de asunto de datos, Cloud Compliance encuentra todos los archivos que contienen el nombre o identificador de esa persona. Cloud Compliance comprueba si existen los datos preindexados más recientes en cuanto a nombre o identificador. No inicia una nueva exploración.

Una vez finalizada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso a un sujeto de datos. El informe agrega información procedente de los datos y los coloca en términos legales de los que se puede enviar a la persona.

Búsqueda de sujetos de datos y descarga de informes

Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "cualquier tipo de información personal".

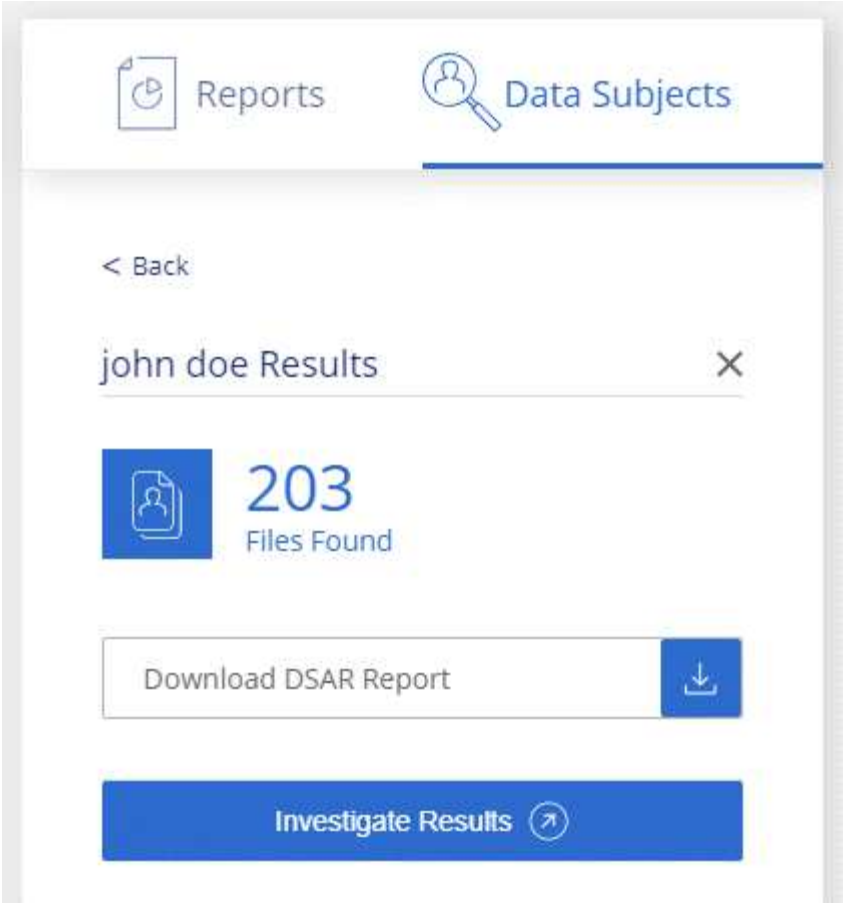
Sólo se admite inglés al buscar los nombres de los sujetos de datos. Más adelante se añadirá compatibilidad con más idiomas.

La búsqueda de sujetos de datos no es compatible en las bases de datos en este momento.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en **Temas de datos**.
3. Busque el nombre completo o el identificador conocido del sujeto de datos.

   A continuación se muestra un ejemplo que muestra una búsqueda del nombre *john doe*:



4. Elija una de las opciones disponibles:
   - **Descargar informe DSAR**: Respuesta formal a la solicitud de acceso que se puede enviar al sujeto de datos. Este informe contiene información generada automáticamente en función de los datos de que Cloud Compliance se encuentra en el asunto de los datos y se ha diseñado para su uso como plantilla. Debe completar el formulario y revisarlo internamente antes de enviarlo al sujeto de datos.
   - **investigar resultados**: Página que permite investigar los datos mediante la búsqueda, clasificación, ampliación de los detalles de un archivo específico y descarga de la lista de archivos.

     Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista de archivos.

Desactivación de Cloud Compliance

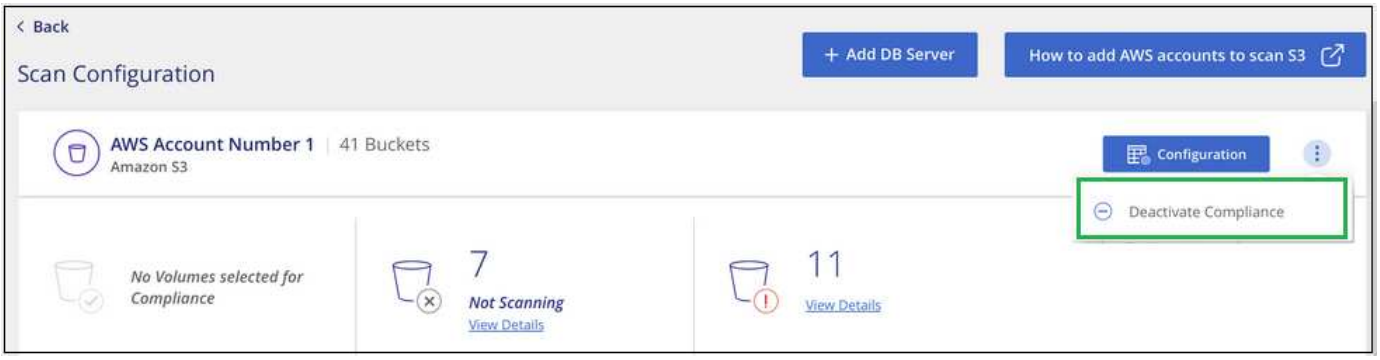
Si lo necesita, puede detener Cloud Compliance de analizar uno o más entornos de trabajo o bases de datos. También puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con sus entornos de trabajo.

Desactivar los análisis de cumplimiento de normativas en un entorno de trabajo

Al desactivar los análisis, Cloud Compliance ya no analiza los datos del sistema y elimina la información de cumplimiento indexada de la instancia de Cloud Compliance (los datos del entorno de trabajo o de la base de datos en sí no se eliminan).

Pasos

En la página *Scan Configuration*, haga clic en En la fila del entorno de trabajo y, a continuación, haga clic en **Desactivar conformidad**.



También puede desactivar los análisis de cumplimiento de un entorno de trabajo desde el panel Servicios cuando seleccione el entorno de trabajo.

Eliminación de la instancia de Cloud Compliance

Puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance. Al eliminar la instancia también se eliminan los discos asociados en los que residen los datos indexados.

Paso

1. Vaya a la consola de su proveedor de cloud y elimine la instancia de Cloud Compliance.

   La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Preguntas frecuentes sobre Cloud Compliance

Estas preguntas frecuentes pueden ayudar si sólo está buscando una respuesta rápida a una pregunta.

¿Qué es el cumplimiento de normativas en el cloud?

Cloud Compliance es una oferta de cloud que utiliza la tecnología impulsada por inteligencia artificial (IA) para ayudar a las organizaciones a comprender el contexto de los datos e identificar datos confidenciales en sus configuraciones de Azure NetApp Files, sistemas Cloud Volumes ONTAP alojados en AWS o Azure, bloques de Amazon S3 y bases de datos.

Cloud Compliance ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para hacer frente a nuevas normativas de cumplimiento de normativas de datos para privacidad y sensibilidad de los datos, como RGPD, CCPA, HIPAA, etc.

¿por qué debo usar Cloud Compliance?

El cumplimiento normativo del cloud puede poner a su disposición todos los datos que le ayudarán a:

- Cumpla con las normativas sobre privacidad y cumplimiento de normativas de datos.
- Cumpla con las políticas de retención de datos.

- Localice con facilidad y cree informes sobre datos específicos en respuesta a sujetos de datos, según lo requiera el RGPD, la CCPA, la HIPAA y otras normativas de privacidad de los datos.

¿Cuáles son los casos de uso comunes de Cloud Compliance?

- Identificación de la Información personal de identificación (PII).
- Identificar un amplio abanico de información confidencial que requieran las normativas de privacidad del RGPD y de la CCPA.
- Cumpla con las normativas de privacidad de datos nuevas y futuras.

"Obtenga más información sobre los casos de uso de cumplimiento de normativas para el cloud".

¿Qué tipos de datos se pueden analizar con Cloud Compliance?

Cloud Compliance admite el análisis de datos no estructurados sobre protocolos NFS y CIFS gestionados por Cloud Volumes ONTAP y Azure NetApp Files. Cloud Compliance también puede analizar datos almacenados en bloques de Amazon S3.

Además, Cloud Compliance puede analizar las bases de datos que se encuentran en cualquier lugar; no es necesario que Cloud Manager las gestione.

"Descubra cómo funcionan las exploraciones".

¿Qué proveedores de cloud son compatibles?

Cloud Compliance funciona como parte de Cloud Manager y actualmente admite AWS y Azure. Esto proporciona a su organización una visibilidad de privacidad unificada a través de distintos proveedores de cloud. Pronto se añadirá la compatibilidad con Google Cloud Platform (GCP).

¿Cómo puedo acceder a Cloud Compliance?

Cloud Compliance se opera y gestiona a través de Cloud Manager. Puede acceder a las funciones de Cloud Compliance desde la ficha **cumplimiento** de Cloud Manager.

¿Cómo funciona Cloud Compliance?

Cloud Compliance pone en marcha otra capa de inteligencia artificial junto con su sistema Cloud Manager y sus sistemas de almacenamiento. A continuación, analiza los datos en volúmenes, bloques y bases de datos e indexa la información que se encuentra.

"Más información sobre el funcionamiento de Cloud Compliance".

¿Cuánto cuesta el cumplimiento de las normativas cloud?

El coste de utilizar Cloud Compliance depende de la cantidad de datos que se escanee. Los primeros 1 TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto. Consulte "precios" para obtener más detalles.

¿con qué frecuencia el Cloud Compliance analiza mis datos?

Los datos cambian con frecuencia, por lo que Cloud Compliance analiza los datos de forma continua y sin

impacto en los datos. Aunque el análisis inicial de los datos puede tardar más tiempo, los análisis posteriores sólo analizan los cambios incrementales, lo que reduce los tiempos de análisis del sistema.

"Descubra cómo funcionan las exploraciones".

¿ofrece informes Cloud Compliance?

Sí. La información que ofrece Cloud Compliance puede ser relevante para otras partes interesadas de sus organizaciones. De esta forma, le permitimos generar informes para compartir la información.

Los siguientes informes están disponibles para Cloud Compliance:

Informe de evaluación de riesgos de privacidad

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

Informe de solicitud de acceso de asunto de datos

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

Informe PCI DSS

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

Informe HIPAA

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

Informa sobre un tipo de información específico

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

¿Qué tipo de instancia o máquina virtual se requiere para Cloud Compliance?

- En Azure, Cloud Compliance se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 512 GB.
- En AWS, Cloud Compliance se ejecuta en una instancia de 5,4 x grande con un disco GP2 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

No se admite el cambio o cambio de tamaño del tipo de máquina virtual/instancia. Debe utilizar el tamaño predeterminado que se proporciona.

"Más información sobre el funcionamiento de Cloud Compliance".

¿el rendimiento del análisis varía?

El rendimiento de análisis puede variar en función del ancho de banda de la red y del tamaño medio de los archivos del entorno de cloud.

¿Qué tipos de archivo son compatibles?

Cloud Compliance analiza todos los archivos para obtener información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Cuando Cloud Compliance detecta información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF y .JSON.

¿Cómo hago posible el cumplimiento de normativas para el cloud?

En primer lugar, tiene que implementar una instancia de Cloud Compliance en Cloud Manager. Una vez que la instancia se esté ejecutando, puede habilitarla en entornos de trabajo y bases de datos existentes desde la ficha **cumplimiento** o seleccionando un entorno de trabajo específico.

"Aprenda cómo empezar".

> La activación de Cloud Compliance da como resultado un análisis inicial inmediato. Los resultados de cumplimiento se muestran poco después.

¿Cómo se deshabilita Cloud Compliance?

Puede deshabilitar Cloud Compliance desde la página entornos de trabajo después de seleccionar un entorno de trabajo individual.

"Leer más".

> Para eliminar por completo la instancia de Cloud Compliance, puede eliminar manualmente la instancia de Cloud Compliance del portal de su proveedor de cloud.

¿Qué sucede si la organización en niveles de datos está habilitada en Cloud Volumes ONTAP?

Es posible que desee habilitar Cloud Compliance en un sistema Cloud Volumes ONTAP que organiza los datos inactivos en almacenamiento de objetos. Si la organización en niveles de los datos está habilitada, Cloud Compliance analiza todos los datos, ya sea en discos o datos inactivos organizados en niveles para el almacenamiento de objetos.

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

¿Puedo utilizar Cloud Compliance para analizar almacenamiento ONTAP en las instalaciones?

No se admite el análisis de los datos directamente desde un entorno de trabajo local de ONTAP. Pero puede analizar sus datos de ONTAP en las instalaciones replicando los datos NFS o CIFS en las instalaciones en un entorno de trabajo de Cloud Volumes ONTAP para después activar el cumplimiento de normativas en dichos volúmenes. Tenemos pensado admitir el cumplimiento de normativas cloud con ofertas de cloud adicionales como Cloud Volumes Service.

"Leer más".

¿Cloud Compliance puede enviar notificaciones a mi organización?

No, pero puede descargar informes de estado que puede compartir internamente en su organización.

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

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

¿Puedo limitar la información de Cloud Compliance a usuarios específicos?

Sí, Cloud Compliance se integra totalmente con Cloud Manager. Los usuarios de Cloud Manager solo pueden ver información de los entornos de trabajo que pueden ver de acuerdo con los privilegios de su espacio de trabajo.

Además, si desea permitir a determinados usuarios ver los resultados del análisis de Cloud Compliance sin tener la capacidad de administrar la configuración de Cloud Compliance, puede asignar a esos usuarios la función *Cloud Compliance Viewer*.

"Leer más".