Obtenga información sobre la privacidad de sus datos

Cloud Manager 3.7

NetApp
March 25, 2024

Tabla de contenidos

Obtenga información sobre la privacidad de sus datos . . . 1
- Más información sobre Cloud Compliance . . . 1
- Primeros pasos con Cloud Compliance para Cloud Volumes ONTAP . . . 4
- Obtener visibilidad y control de los datos privados . . . 10
- Ver el Informe de evaluación de riesgo de privacidad . . . 17
- Respuesta a una solicitud de acceso de un sujeto de datos . . . 19
- Desactivación de Cloud Compliance . . . 21
- Preguntas frecuentes sobre Cloud Compliance . . . 22

Obtenga información sobre la privacidad de sus datos

Más información sobre Cloud Compliance

Cloud Compliance es un servicio de privacidad y cumplimiento de normativas de datos para Cloud Volumes ONTAP en AWS y Azure. Mediante la tecnología basada en la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales en los sistemas de Cloud Volumes ONTAP.

Cloud Compliance está actualmente disponible como versión de disponibilidad controlada.

"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)

Coste

Cloud Compliance es un servicio complementario para Cloud Volumes ONTAP que proporciona NetApp sin coste adicional. La activación de Cloud Compliance requiere la puesta en marcha de una instancia cloud que su proveedor de cloud le cobrará. La entrada o salida de datos no supone ningún coste porque los datos no fluyen fuera de la red.

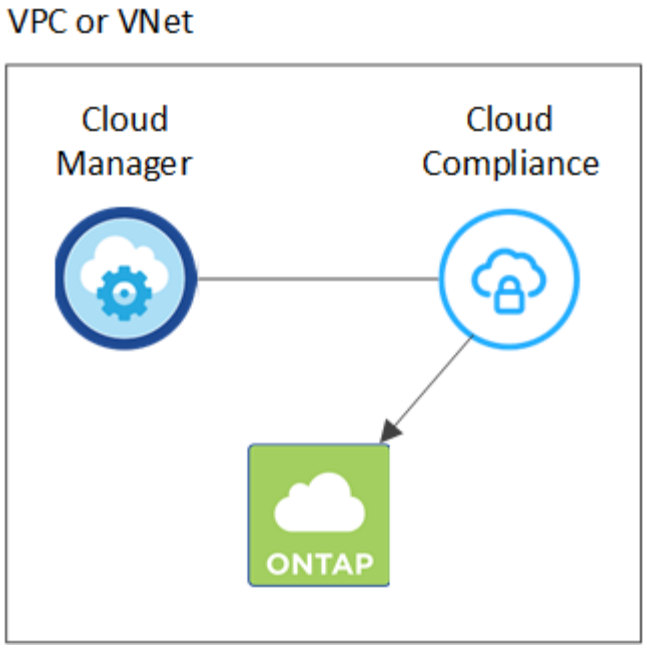
Cómo funciona Cloud Compliance

En un nivel superior, Cloud Compliance funciona como esta:

1. Habilite el cumplimiento de normativas cloud en uno o más sistemas de Cloud Volumes ONTAP.
2. Cloud Compliance analiza los datos mediante un proceso de aprendizaje de IA.
3. 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 en uno o más sistemas de Cloud Volumes ONTAP, Cloud Manager pone en marcha una instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema de 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 io1 de 500 GB.

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

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

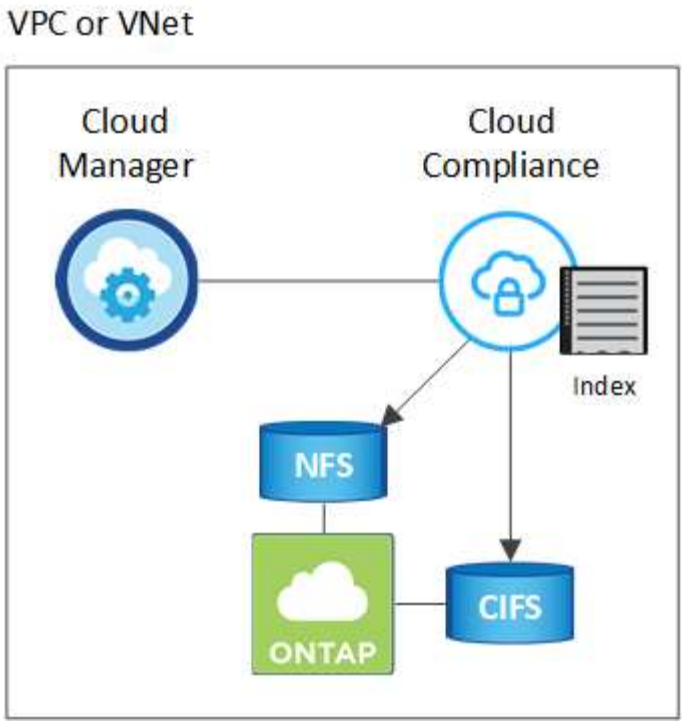
La instancia debe permanecer en ejecución en todo momento debido a que Cloud Compliance analiza continuamente los datos en sistemas Cloud Volumes ONTAP.

Cómo funcionan las exploraciones

Después de activar Cloud Compliance, comienza inmediatamente a analizar sus datos para identificar datos personales y confidenciales.

Cloud Compliance se conecta a Cloud Volumes ONTAP 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.

Cloud Compliance analiza los datos no estructurados en cada volumen para obtener una amplia información personal. 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.



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 entorno de trabajo, pero no en el nivel de volumen. "Vea cómo".

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 una dirección IP privada y un grupo de seguridad que permite conexiones HTTP entrantes desde Cloud Manager. Esta conexión le permite acceder a la consola de Cloud Compliance desde la interfaz de Cloud Manager.

Las reglas salientes están completamente abiertas. La instancia se conecta a los sistemas Cloud Volumes ONTAP y a Internet a través de un proxy desde Cloud Manager. Se necesita acceso a Internet para actualizar el software Cloud Compliance y enviar métricas de uso.

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

Los datos indexados nunca salen de la instancia de cumplimiento en nube. Los datos no se transmiten fuera de su red virtual y no se envían a Cloud Manager.

Acceso de los usuarios a la información de cumplimiento

Los administradores de Cloud Manager pueden ver información de cumplimiento de normativas para todos los entornos de trabajo.

Los administradores de área de trabajo pueden 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.

"Más información acerca de los roles de Cloud Manager".

Primeros pasos con Cloud Compliance para Cloud Volumes ONTAP

Complete unos pasos para comenzar a usar Cloud Compliance para Cloud Volumes ONTAP en AWS o Azure.

Inicio rápido

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

Compruebe que la configuración cumple los requisitos

- Asegúrese de que la instancia de Cloud Compliance tenga acceso saliente a Internet.

  Cloud Manager pone en marcha la instancia en el mismo VPC o vnet que el primer sistema de Cloud Volumes ONTAP de la solicitud.

- Asegúrese de que los usuarios puedan acceder a la interfaz de Cloud Manager desde un host que tenga una conexión directa con AWS o Azure, o desde un host que esté dentro de la misma red que la instancia de Cloud Compliance (la instancia tendrá una dirección IP privada).
- Asegúrese de mantener en funcionamiento la instancia de Cloud Compliance.

Habilite Cloud Compliance en Cloud Volumes ONTAP

- Nuevos entornos de trabajo: Asegúrese de mantener la conformidad con la nube habilitada al crear el entorno de trabajo (está activada de forma predeterminada).
- Entornos de trabajo existentes: Haga clic en **conformidad**, edite opcionalmente la lista de entornos de trabajo y haga clic en **Mostrar panel de cumplimiento**.

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.
- 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 **cumplimiento** > **Estado de exploración CIFS** > **Editar credenciales CIFS** 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.

Garantice la conectividad entre Cloud Manager y Cloud Compliance

- El grupo de seguridad para Cloud Manager debe permitir el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.
- Si la red AWS no utiliza NAT o proxy para el acceso a Internet, el grupo de seguridad para Cloud Manager debe permitir el tráfico entrante a través del puerto TCP 3128 desde la instancia de Cloud Compliance.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Compliance. Deberá garantizar la conectividad entre los componentes después de habilitar Cloud Compliance. Esto se trata a continuación.

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:

Puntos finales	Específico
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.

Puntos finales	Específico
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.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 la conectividad del explorador web con 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.

Si accede a Cloud Manager desde una dirección IP pública, es probable que su navegador web no se ejecute en un host dentro de la red.

Mantenga Cloud Compliance en ejecución

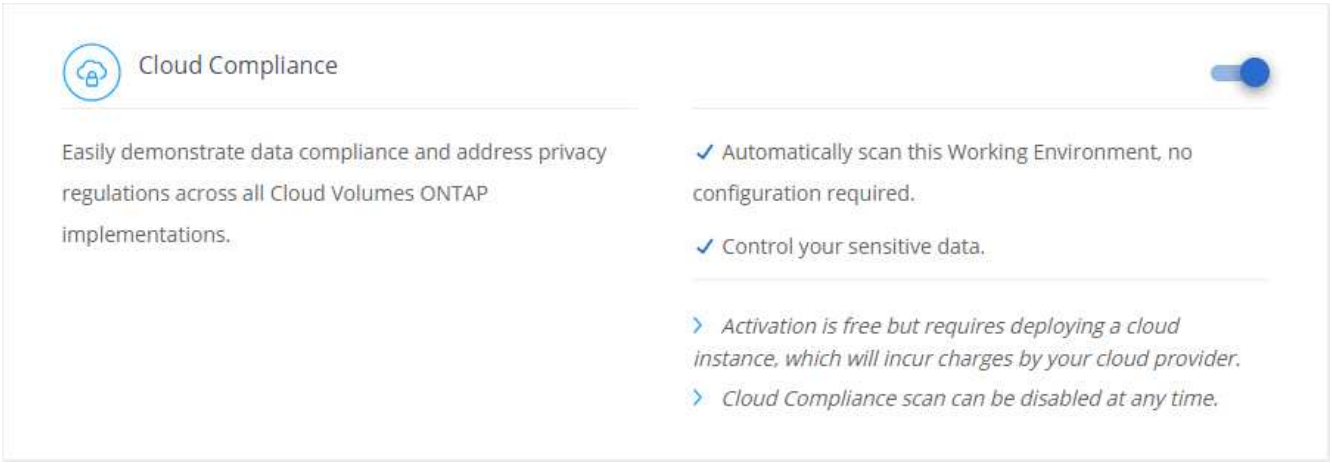
La instancia de Cloud Compliance debe permanecer activa para analizar sus datos de forma continua.

Habilitar Cloud Compliance en un nuevo entorno de trabajo

Cloud Compliance se habilita de forma predeterminada en el asistente de entorno de trabajo. Asegúrese de mantener la opción habilitada.

Pasos

1. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Amazon Web Services o Microsoft Azure como proveedor de cloud y, a continuación, elija un sistema de alta disponibilidad o nodo único.
3. Rellene la página Details & Credentials.
4. En la página Servicios, deje Cloud Compliance activado y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

   Para obtener ayuda, consulte "Inicio de Cloud Volumes ONTAP en AWS" y.. "Inicio de Cloud Volumes ONTAP en Azure".

Resultado

Cloud Compliance se habilita en el sistema Cloud Volumes ONTAP. Si es la primera vez que habilita Cloud Compliance, Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud. En cuanto la instancia esté disponible, comienza a analizar los datos a medida que se escriben en cada volumen que cree.

Habilitar Cloud Compliance en entornos de trabajo existentes

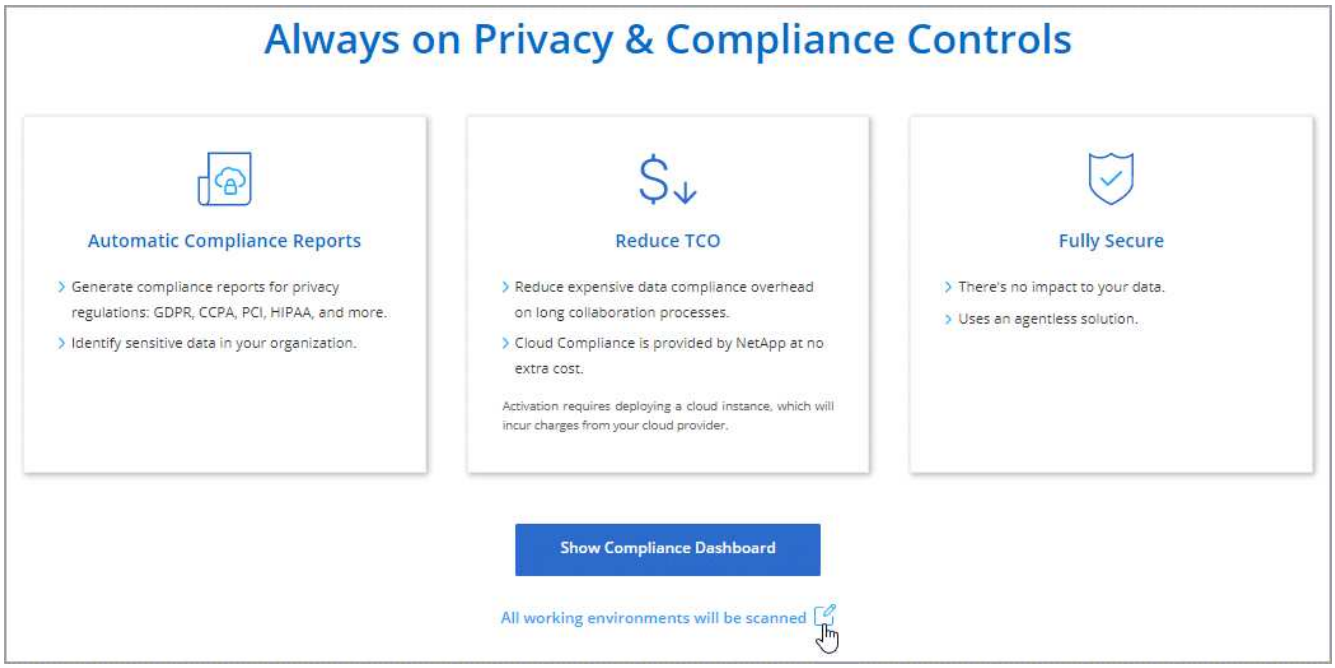
Habilite el cumplimiento de la nube en sus sistemas Cloud Volumes ONTAP existentes desde la pestaña **conformidad** de Cloud Manager.

Otra opción es habilitar Cloud Compliance desde la ficha **entornos de trabajo** seleccionando cada entorno de trabajo individualmente. Tardará más en completarse, a menos que solo tenga un sistema.

Pasos para múltiples entornos de trabajo

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento**.
2. Si desea habilitar Cloud Compliance en entornos de trabajo específicos, haga clic en el icono de edición.

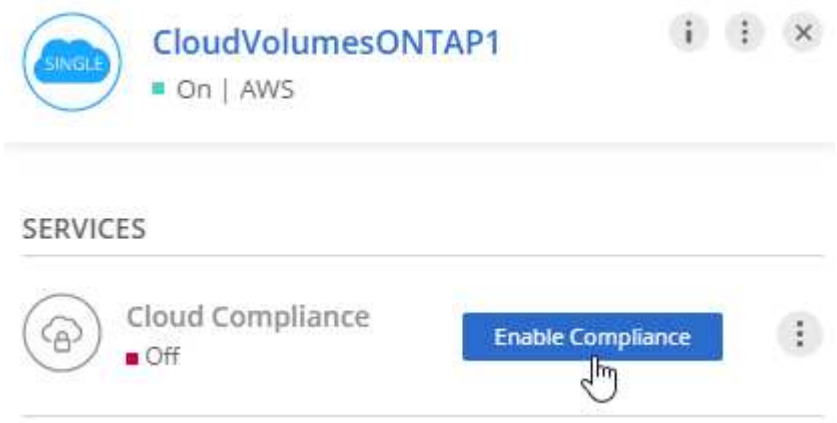
   De lo contrario, Cloud Manager se establece para habilitar Cloud Compliance en todos los entornos de trabajo a los que tenga acceso.



3. Haga clic en **Mostrar panel de cumplimiento**.

Pasos para un único entorno de trabajo

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione un entorno de trabajo.
3. En el panel de la derecha, haga clic en **Activar cumplimiento**.



Resultado

Si es la primera vez que habilita Cloud Compliance, Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud.

Cloud Compliance comienza a analizar los datos en cada entorno de trabajo. Los datos estarán disponibles en la consola de cumplimiento de normativas tan pronto como Cloud Compliance finalice 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 garantizar que Cloud Compliance pueda acceder a los volúmenes en Cloud Volumes ONTAP, compruebe sus redes, grupos de seguridad y políticas de exportación. Necesitará proporcionar cumplimiento normativo

del cloud con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que hay una conexión de red entre la instancia de Cloud Compliance y cada subred de Cloud Volumes ONTAP.

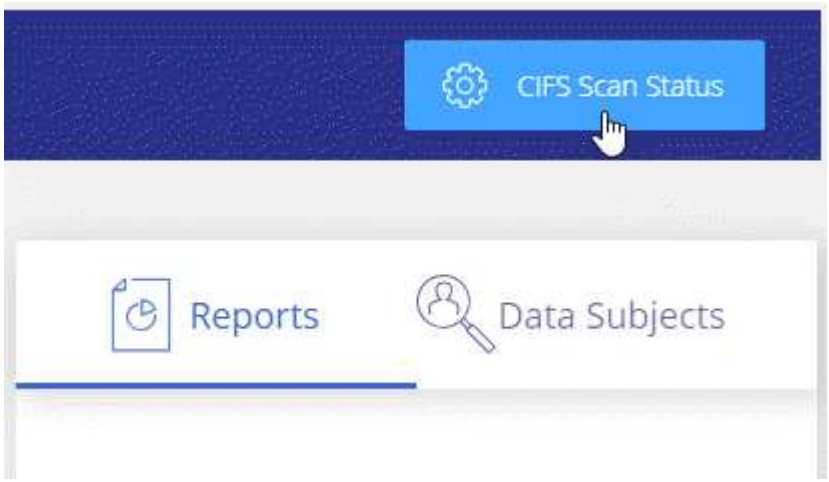
   Cloud Manager pone en marcha la instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema de Cloud Volumes ONTAP de la solicitud. Por lo tanto, este paso es importante si algunos sistemas Cloud Volumes ONTAP están en subredes o redes virtuales diferentes.

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 **cumplimiento**.
   b. En la parte superior derecha, haga clic en **Estado de exploración CIFS**.



   c. Para cada sistema Cloud Volumes ONTAP, 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.

Verificar que Cloud Manager puede acceder a Cloud Compliance

Garantice la conectividad entre Cloud Manager y Cloud Compliance para poder ver los datos sobre el cumplimiento de normativas que encontró Cloud Compliance.

Pasos

1. Asegúrese de que el grupo de seguridad de Cloud Manager permite el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.

   Esta conexión le permite ver información en la ficha cumplimiento.

2. Si la red AWS no utiliza NAT o proxy para el acceso a Internet, modifique el grupo de seguridad para Cloud Manager para permitir el tráfico entrante a través del puerto TCP 3128 desde la instancia de Cloud Compliance.

   Esto es necesario porque la instancia de Cloud Compliance utiliza Cloud Manager como proxy para acceder a Internet.

   Este puerto está abierto de forma predeterminada en todas las nuevas instancias de Cloud Manager, a partir de la versión 3.7.5. No está abierto en las instancias de Cloud Manager creadas antes de esa versión.

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.

Datos personales

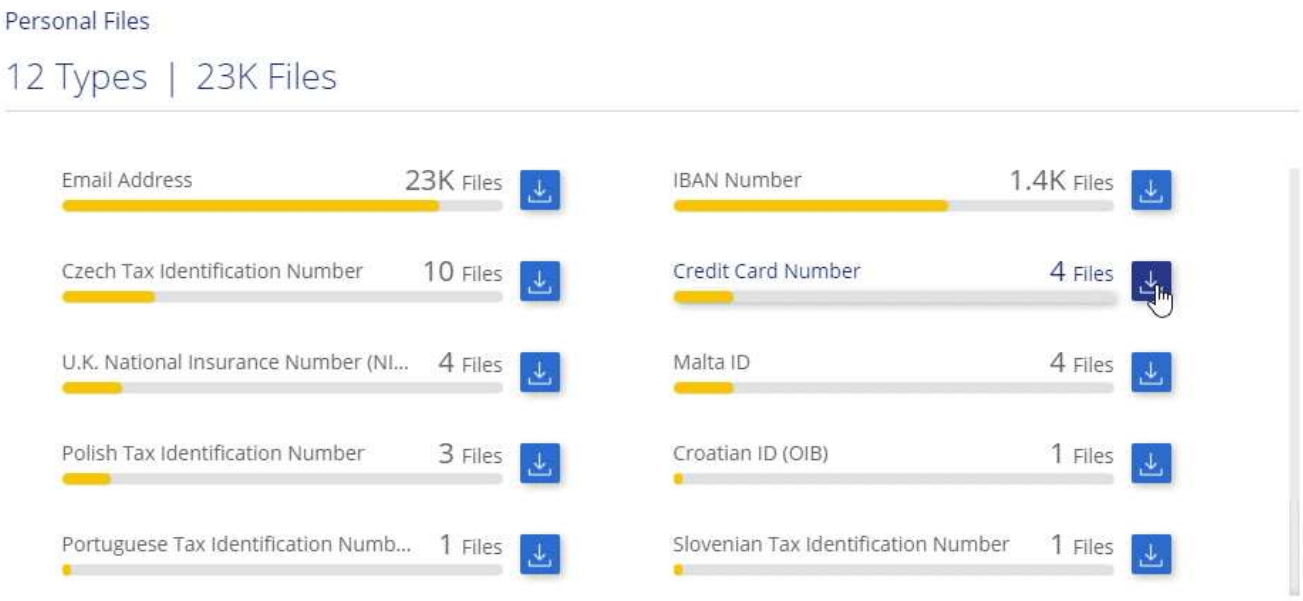
Cloud Compliance identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria y mucho más. Consulte la lista completa.

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**.
2. Descargue los detalles de uno de los dos tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y descargue la lista para cualquiera de los tipos de datos personales encontrados.



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
	Dirección IP	Sí

Tipo	Identificador	¿validación de proximidad?
Identificadores nacionales	ID belga (Numero Nacional)	Sí
	ID búlgaro (número civil unificado)	Sí
	Número de identificación fiscal de Chipre (TIC)	Sí
	Número de identificación fiscal danés (CPR)	Sí
	ID de Estonia (Isikukood)	Sí
	Finlandés ID (henkilötunnu)	Sí
	Número de identificación fiscal francés (SPI)	Sí
	Número de identificación fiscal alemán (Steuerliche Identifikationsnummer)	Sí
	Número de identificación fiscal húngara (Adóazonosísó jel)	Sí
	Irish ID (PPS)	Sí
	Documento de identidad israelí	Sí
	Italiano ID (Codice Fiscale)	Sí
	Número de identificación fiscal letón	Sí
	Lituano ID (Asmens kodas)	Sí
	ID de Luxemburgo	Sí
	Malta ID	Sí
	Netherlands ID (BSN)	Sí
	Número de identificación fiscal polaco	Sí
	Número de identificación fiscal (NIF) en portugués	Sí
	Número de identificación fiscal rumano	Sí
	Número de identificación fiscal eslovaca	Sí
	Número de identificación fiscal esloveno	Sí
	ID sudafricano	Sí
	Número de identificación fiscal en español	Sí
	Número de identificación fiscal sueco	Sí
	REINO UNIDO Número de Seguro Nacional (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.

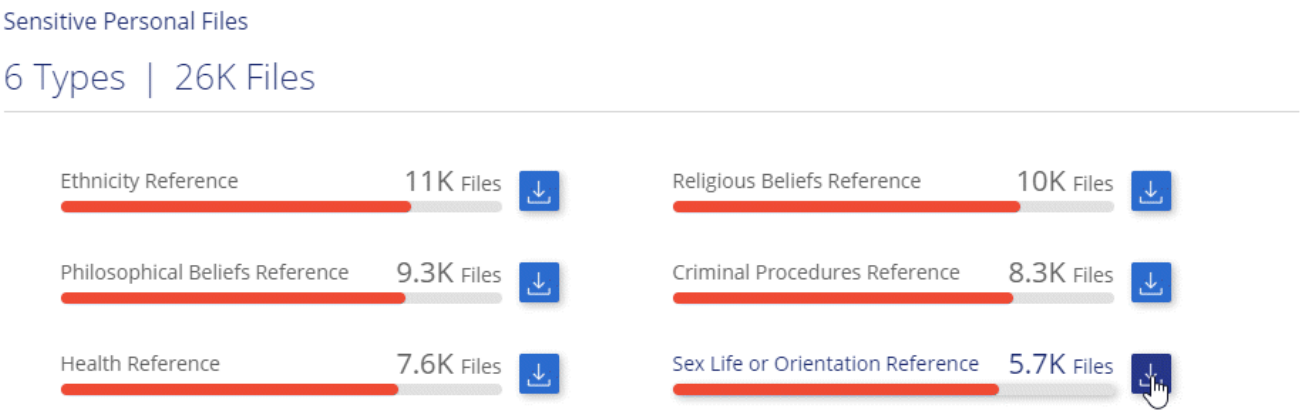
Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Debido a sus habilidades para NLP, Cloud Compliance puede distinguir la diferencia entre una frase que dice "George es mexicano" (que indica datos confidenciales como se especifica en el artículo 9 del RGPD), frente 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 **cumplimiento**.
2. Descargue los detalles de uno de los dos tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y, a continuación, descargue la lista para cualquiera de los tipos de datos personales confidenciales que se hayan encontrado.



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.

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.

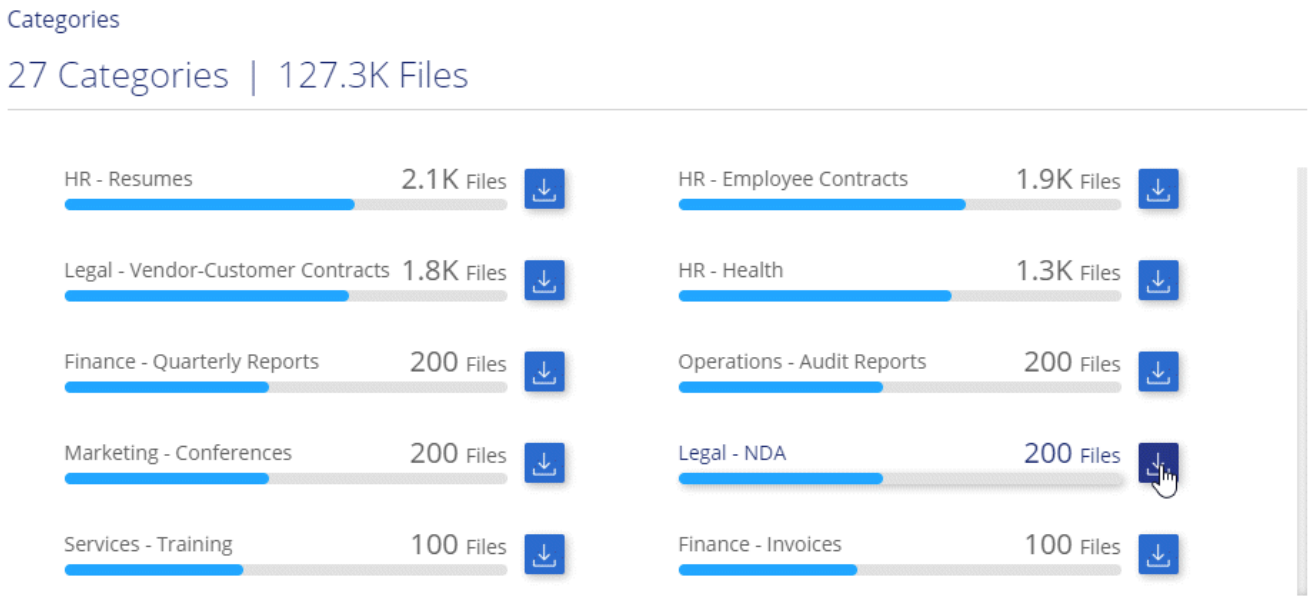
Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole el tipo de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Al descargar el informe CSV, es posible que encuentre que los contratos de empleados se almacenan en una ubicación no segura. 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 **cumplimiento**.
2. Descargue los detalles de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y descargue la lista para cualquiera de las categorías.



Tipos de categorías

Cloud Compliance categoriza sus datos de la siguiente manera:

Finanzas

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

RR. HH

- Comprobación de fondo
- Planes de compensación
- Contratos de empleados
- Revisión de empleados
- Salud
- Se reanudará

Legal

- NDA
- Contratos con el proveedor y el cliente

Marketing

- Campañas
- Conferencias

Operaciones

- Informes de auditoría

Ventas

- Pedidos de ventas

Servicios

- RFI
- RFP
- Entrenamiento

Soporte técnico

- Quejas y boletos

Otros

- Archivos de archivo
- Audio
- Archivos CAD
- Codificación
- Ejecutables
- Imágenes

Tipos de archivo

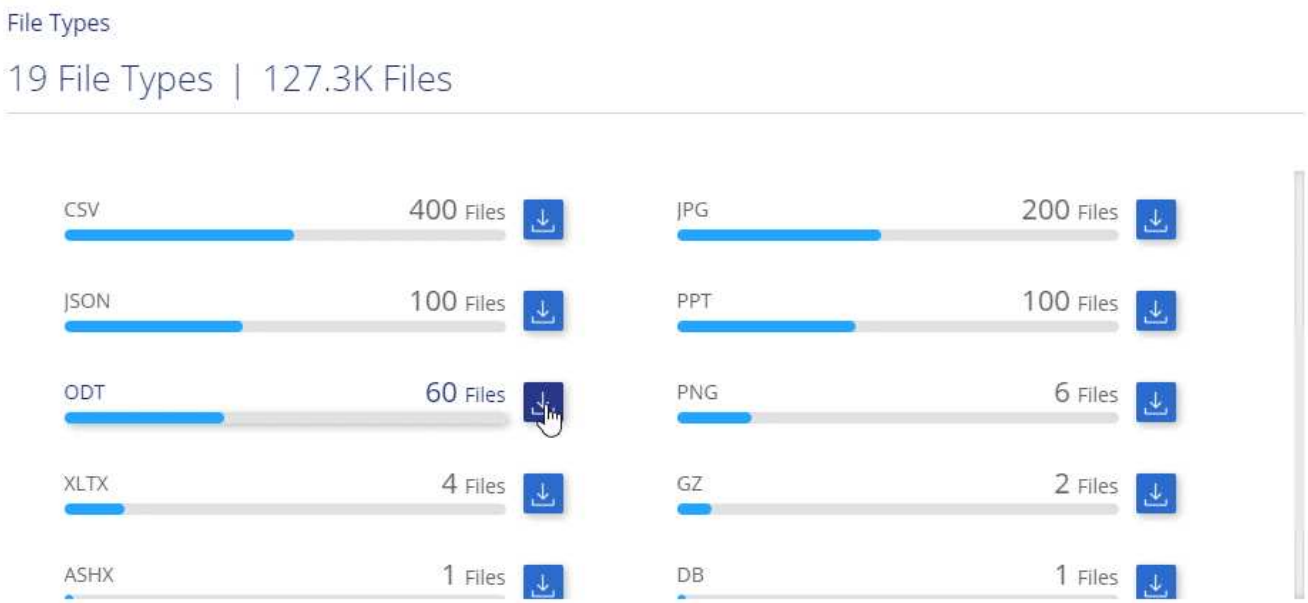
Cloud Compliance toma los datos que ha analizado y los divide por tipo de archivo. Cloud Compliance puede mostrar todos los tipos de archivo que se encuentran en los análisis.

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. 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 **cumplimiento**.
2. Descargue los detalles de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y descargue la lista para cualquiera de los tipos de archivo.



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)

La consola permite 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 (se añadirá más adelante la compatibilidad con más).

Cada lista de archivos incluye la siguiente información:

- Nombre de archivo
- Tipo de ubicación
- Ubicación
- 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. Los archivos solo aparecen en los informes CSV.

Ver el Informe de evaluación de 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.

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.

El informe incluye la siguiente información:

Estado de cumplimiento
: Una puntuación de gravedad (consulte a continuación para obtener más información) 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.

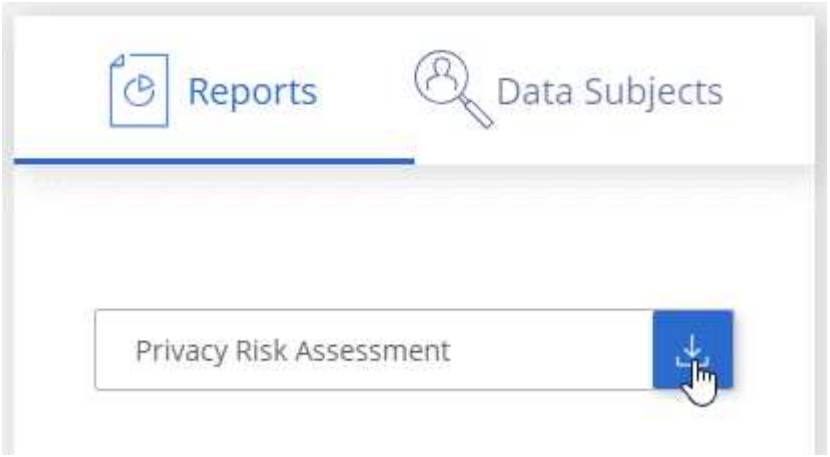
Datos sujetos en esta evaluación
: El número de personas por ubicación para las cuales se encontraron identificadores nacionales.

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 **cumplimiento**.
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 más grande el 6 %
6	Dos de las variables son mayores del 6%
7	Tres de las variables son mayores del 6%
8	Una de las variables es más grande el 15 %
9	Dos de las variables son mayores del 15%
10	Tres de las variables son mayores del 15%

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 o un informe de solicitud de acceso de asunto 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

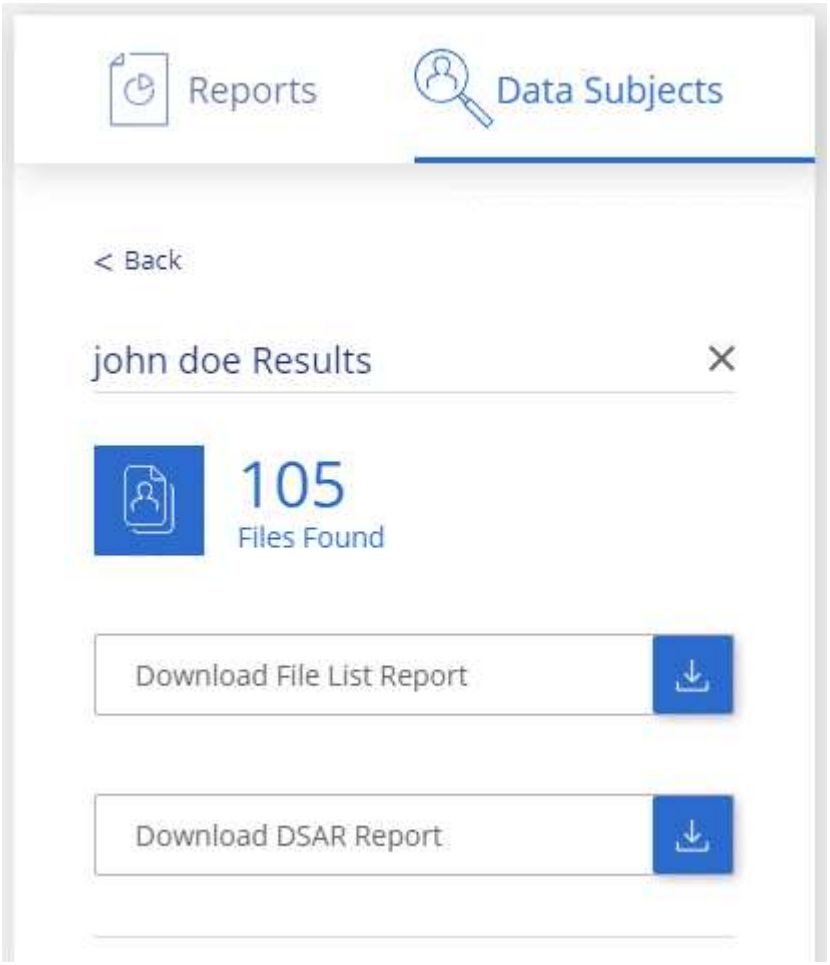
Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "cualquier tipo de información personal".

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

Pasos

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento**.
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 de la lista de archivos**: Una lista de los archivos que contienen información sobre el asunto de los datos.

     Si hay más de 10,000 resultados, sólo aparecen los 10,000 primeros en el informe (más adelante se añadirá compatibilidad con más).

   - **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.

Desactivación de Cloud Compliance

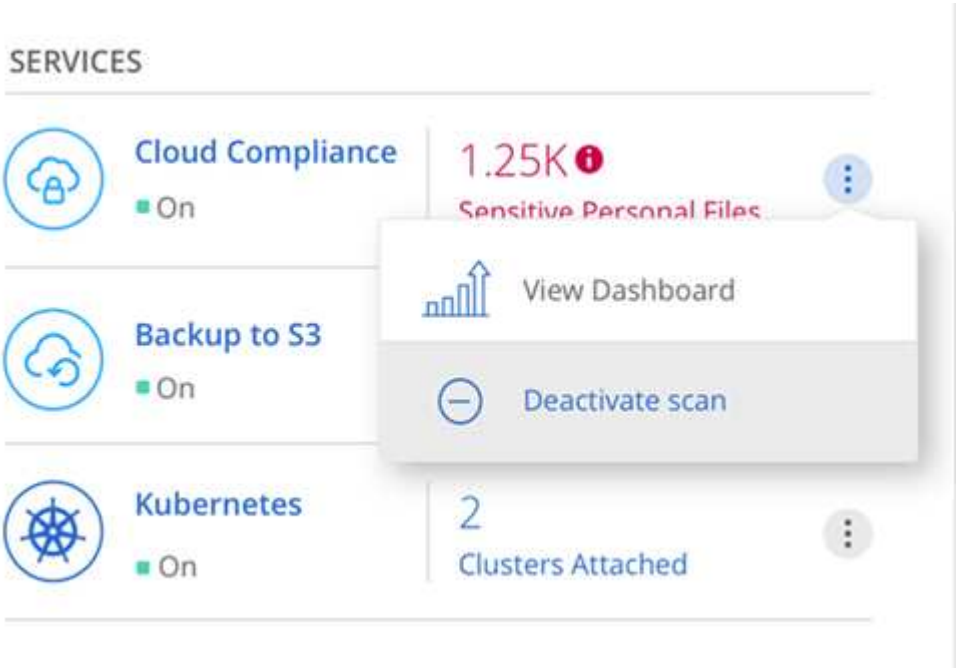
Si lo necesita, puede detener Cloud Compliance de analizar uno o más entornos de trabajo. También puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con sus sistemas Cloud Volumes ONTAP.

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 en sí no se eliminan).

Pasos

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione el entorno de trabajo.
3. En el panel derecho, haga clic en el icono de acción del servicio Cloud Compliance y seleccione **Desactivar análisis**.



Eliminación de la instancia de Cloud Compliance

Puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con Cloud Volumes ONTAP. 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 nueva oferta de cloud de NetApp. Mediante la tecnología basada en la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales en sus sistemas de Cloud Volumes ONTAP alojados en AWS o Azure.

Cloud Compliance ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para abordar nuevas normativas de cumplimiento de normativas de datos en cuanto a privacidad y sensibilidad de los datos, como GDPR, CCPA, 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 y otras normativas de privacidad de 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 permite realizar análisis de datos no estructurados mediante protocolos NFS y CIFS. Actualmente, Cloud Compliance analiza datos gestionados por Cloud Volumes ONTAP.

"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 e instancias de Cloud Volumes ONTAP. A continuación, escanea los datos en Cloud Volumes ONTAP e indexa la información de datos encontrada.

"Más información sobre el funcionamiento de Cloud Compliance".

¿Cuánto cuesta el cumplimiento de las normativas cloud?

Cloud Compliance se ofrece como parte de Cloud Volumes ONTAP y no requiere ningún coste adicional. Es posible que se necesiten costes adicionales en el futuro para lograr funcionalidades personalizadas.

Cloud Compliance requiere la puesta en marcha de una instancia en su proveedor de cloud, para la que su proveedor de cloud le cobrará.

¿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".

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 io1 de 500 GB.

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

"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.

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

Puede habilitar Cloud Compliance al crear un nuevo entorno de trabajo. Puede activarlo en entornos de trabajo existentes desde la ficha **cumplimiento** (sólo en la primera activación) 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 Cloud Compliance se encuentra actualmente disponible como parte de Cloud Manager y es compatible con Cloud Volumes ONTAP. Tenemos pensado admitir el cumplimiento de normativas cloud con ofertas cloud adicionales como Cloud Volumes Service y Azure NetApp Files.

¿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.

"Leer más".

Información de copyright

Información de la marca comercial