



Active el análisis en sus orígenes de datos

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

- Active el análisis en sus orígenes de datos 1
 - Primeros pasos con el cumplimiento de normativas cloud para Cloud Volumes ONTAP y Azure NetApp Files 1
 - Introducción a Cloud Compliance para Amazon S3 5
 - Analizando esquemas de base de datos 13
 - Análisis de datos de ONTAP en las instalaciones con Cloud Compliance mediante SnapMirror 16

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.



1 Implemente la instancia de Cloud Compliance

"Ponga en marcha [Cloud Compliance en Cloud Manager](#)" si aún no hay una instancia implementada.



2 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.



3 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.



4 Configure los volúmenes que desea analizar

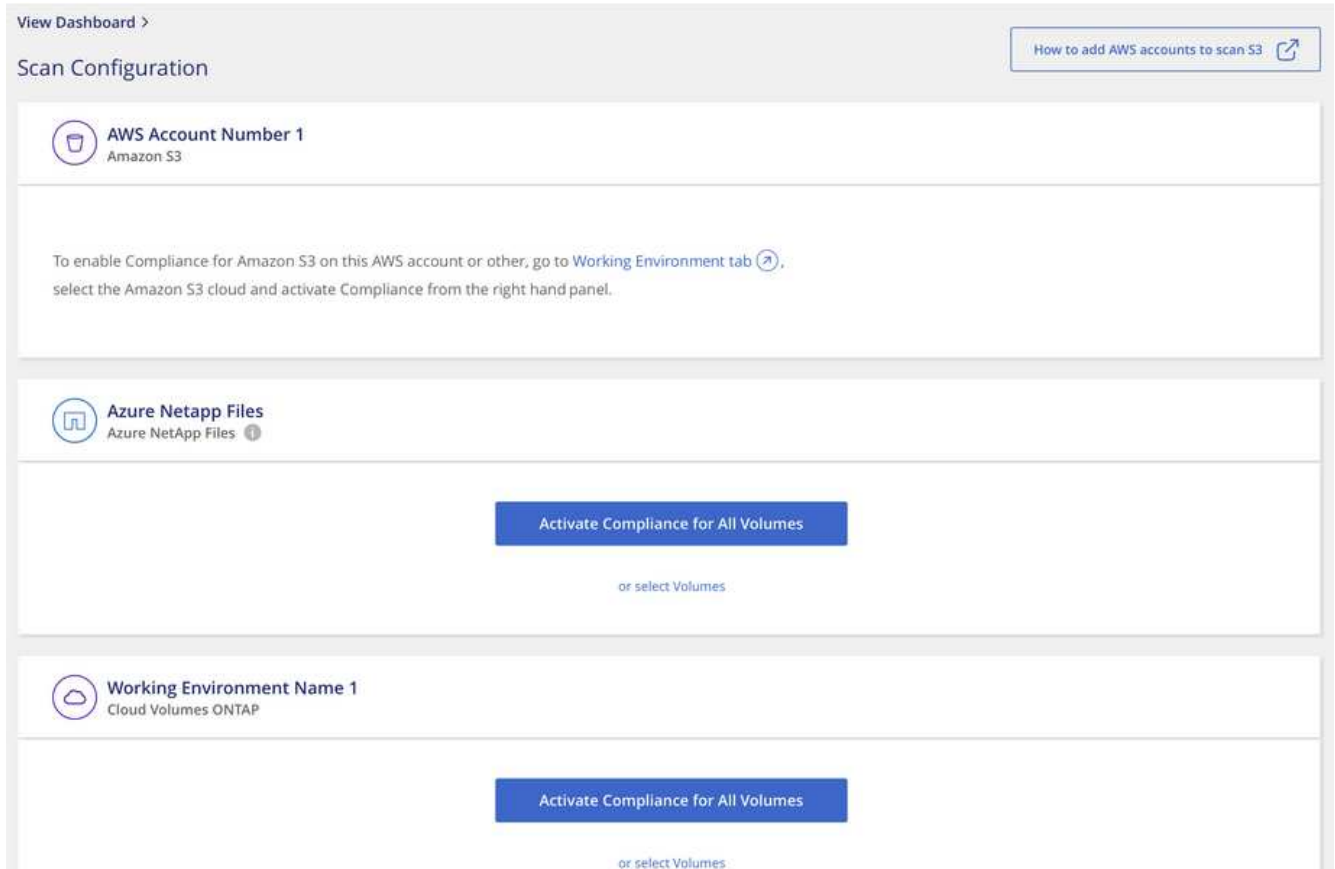
Seleccione los volúmenes que desea analizar y Cloud Compliance empezará a analizarlos.

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.



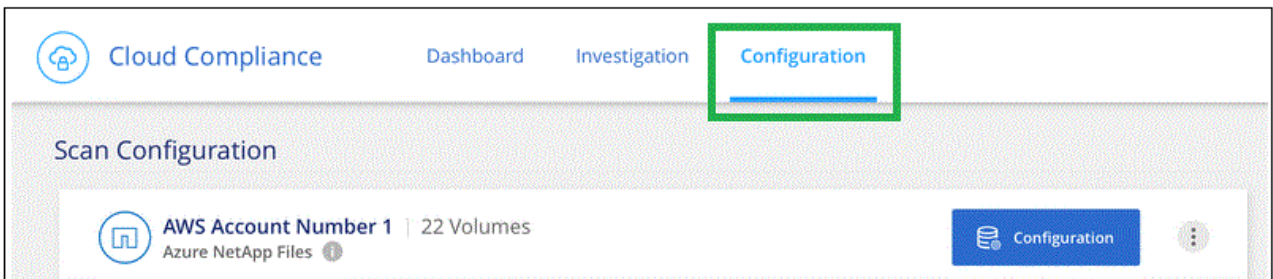
Para Azure NetApp Files, Cloud Compliance solo puede analizar volúmenes que se encuentren en la misma región que Cloud Manager.

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.

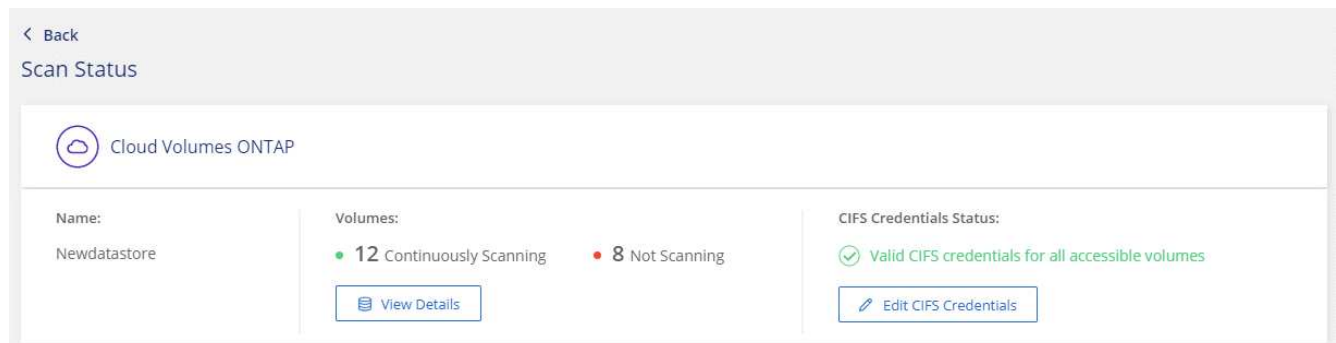
- a. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
- b. Haga clic en la ficha **Configuración**.



- 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.

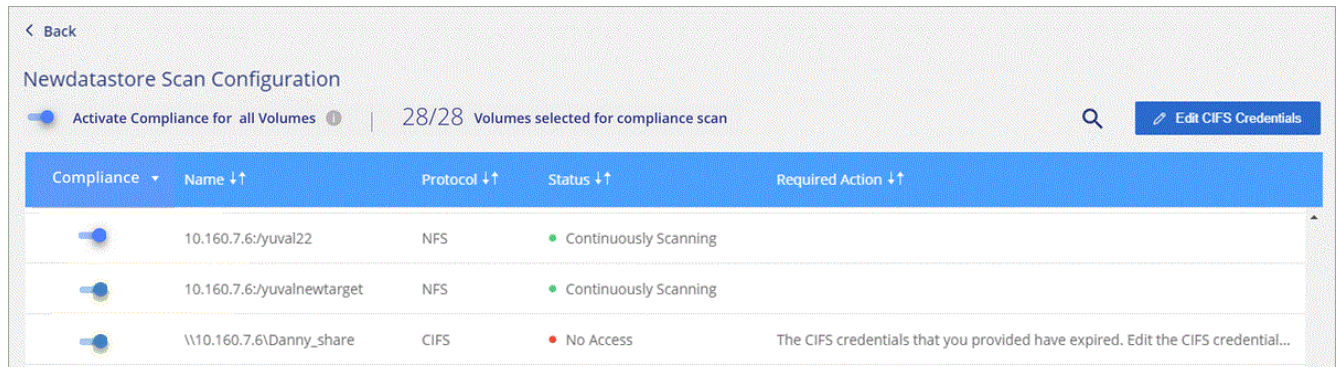
Las credenciales pueden ser de sólo lectura, pero al proporcionar credenciales de administrador se garantiza que Cloud Compliance pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de Cloud Compliance.

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



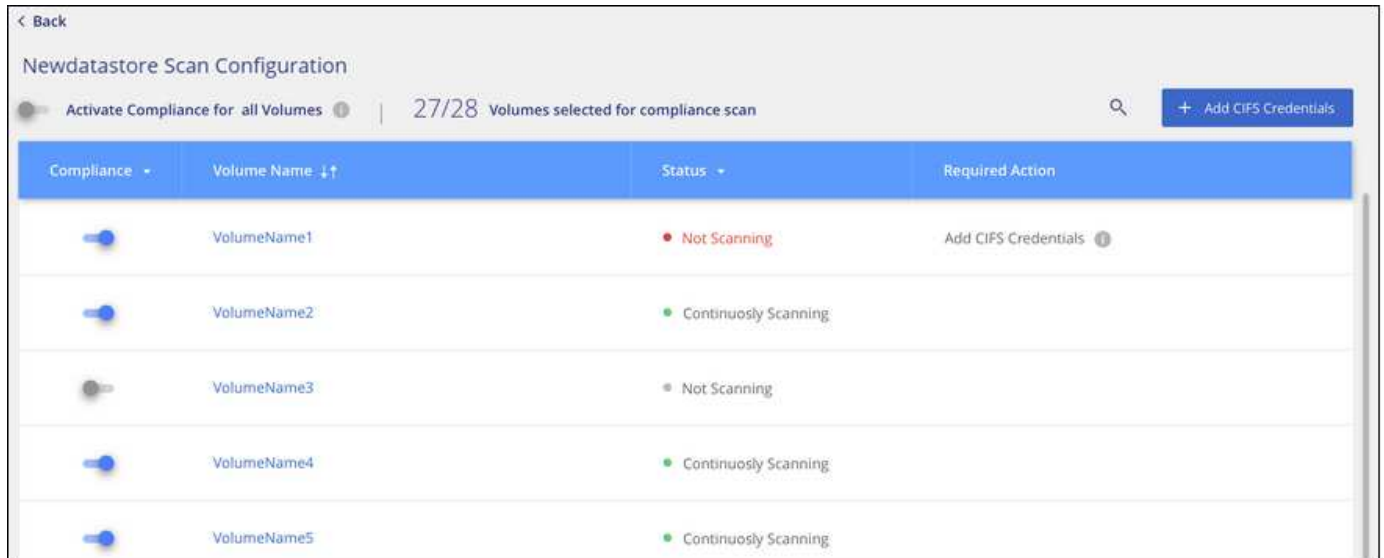
- En la página *Scan Configuration*, haga clic en **View Details** para revisar el estado de cada volumen CIFS y NFS y corregir los errores.

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*.

The screenshot shows the 'Working Environment Name' Scan Configuration interface. At the top, there is a toggle for 'Activate Compliance for all Volumes' and a counter '22/28 Volumes selected for compliance scan'. A button 'Enable Access to DP Volumes' is highlighted with a green box. Below this is a table with the following data:

Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

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

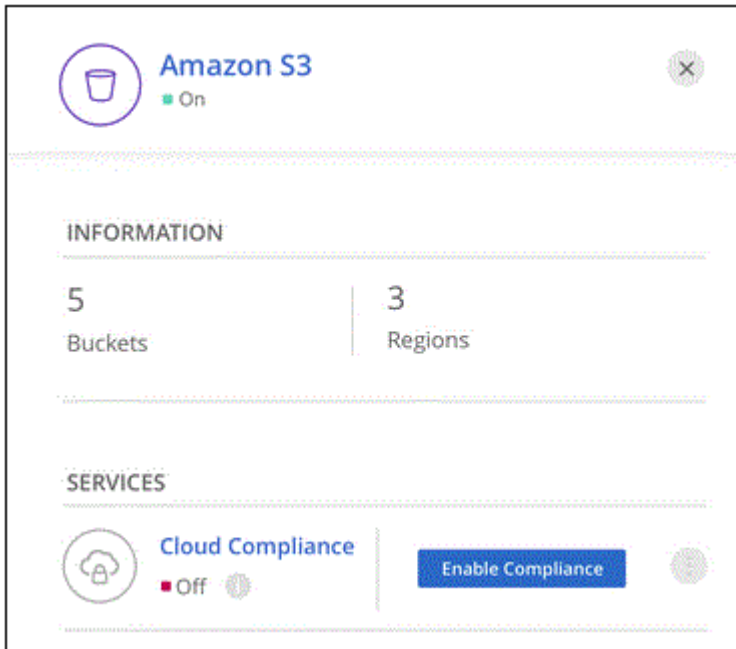
Habilite Cloud Compliance en Amazon S3 después de comprobar los requisitos previos.

Pasos

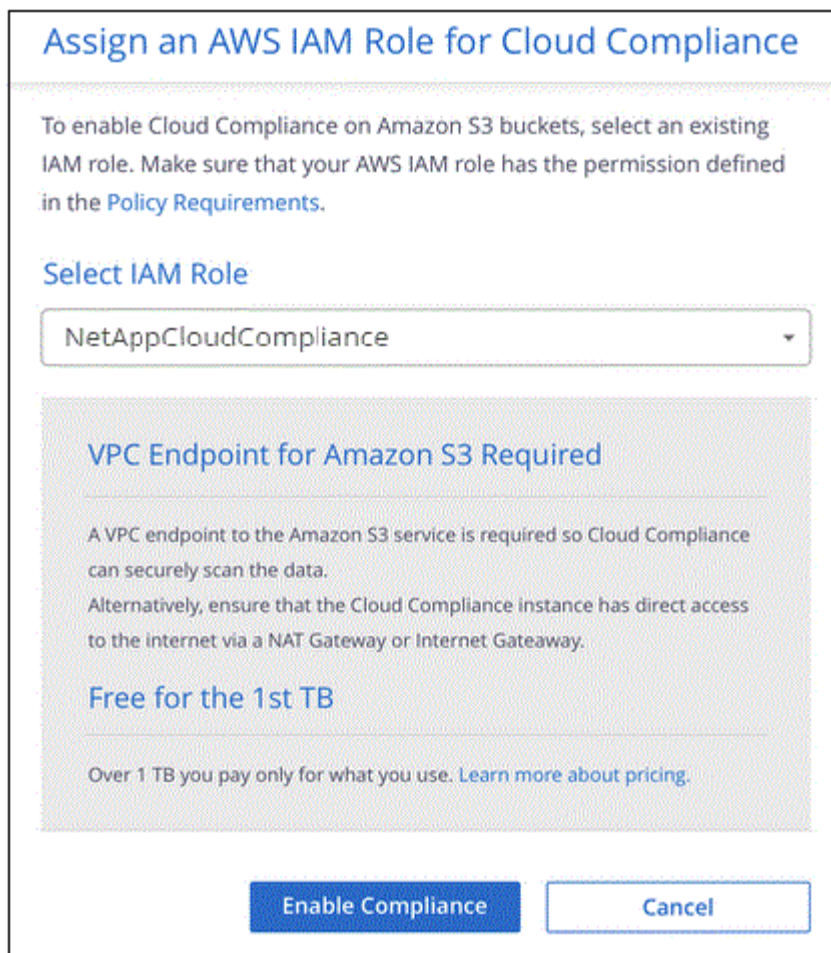
1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione el entorno de trabajo de Amazon S3.



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

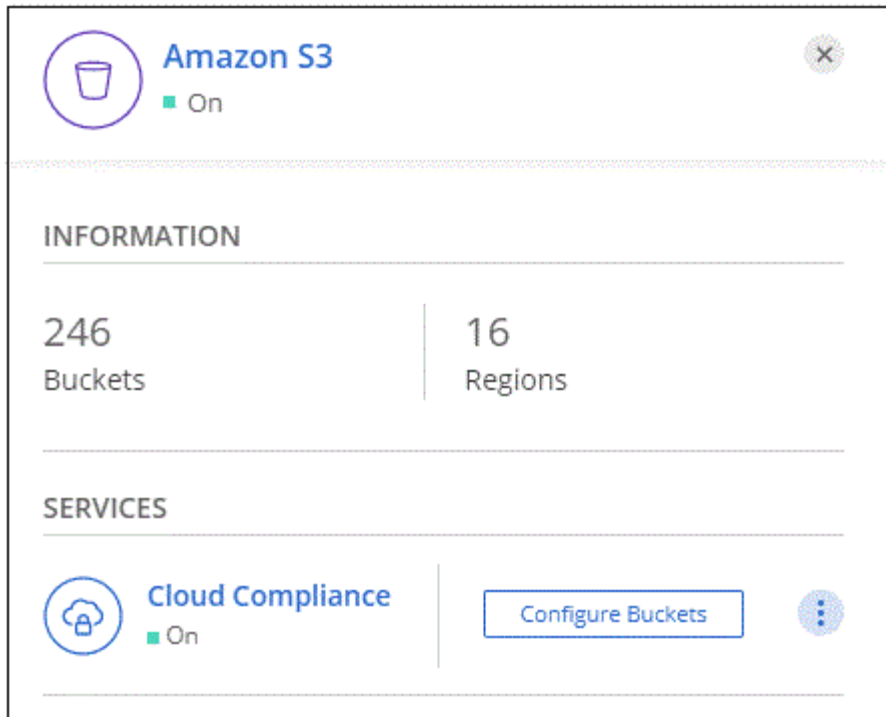
Después de que Cloud Manager habilita Cloud Compliance en Amazon S3, el paso siguiente es configurar los bloques que desea analizar.

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.

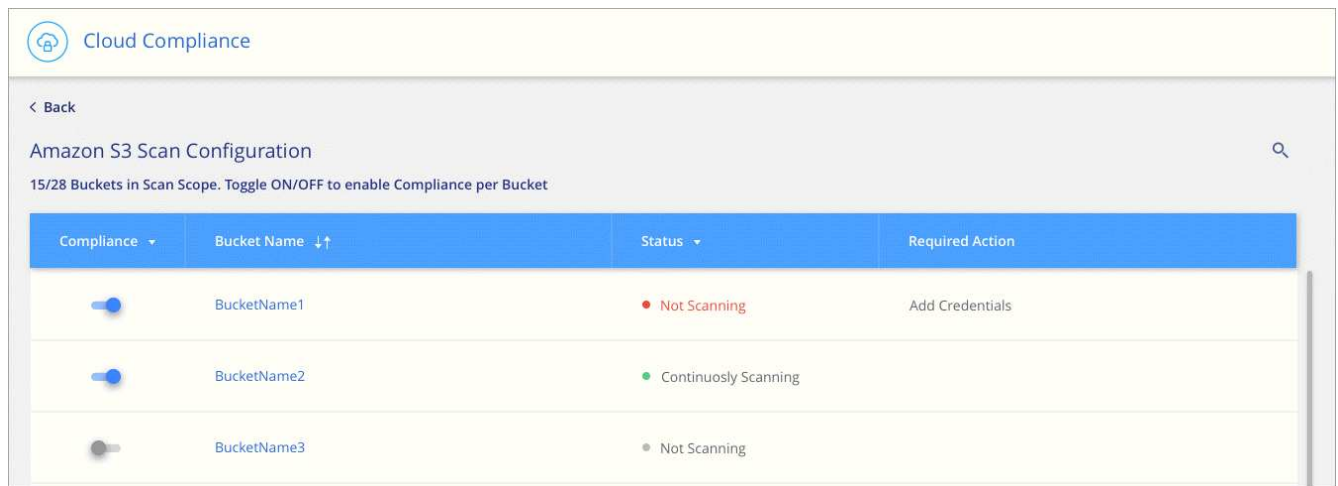
Cloud Compliance también puede [Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS](#).

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**.

Create role



Select type of trusted entity

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

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

Specify accounts that can use this role

Account ID* ⓘ

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

No olvide hacer lo siguiente:

- Introduzca el ID de la cuenta en la que reside la instancia de 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.

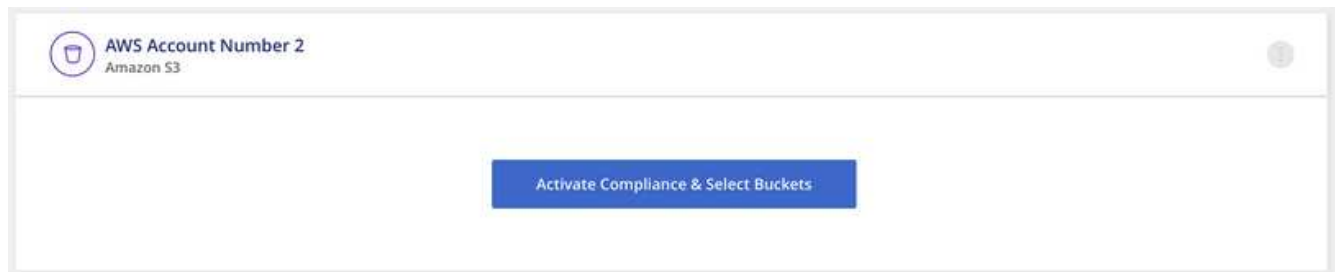
```

{
  "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.

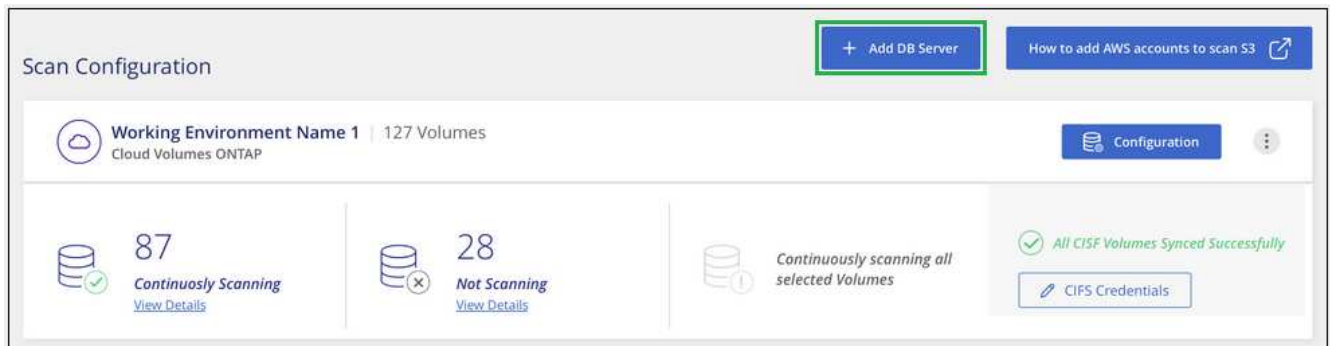
Nota: para MongoDB, se requiere una función de administrador de sólo lectura.

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**.

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

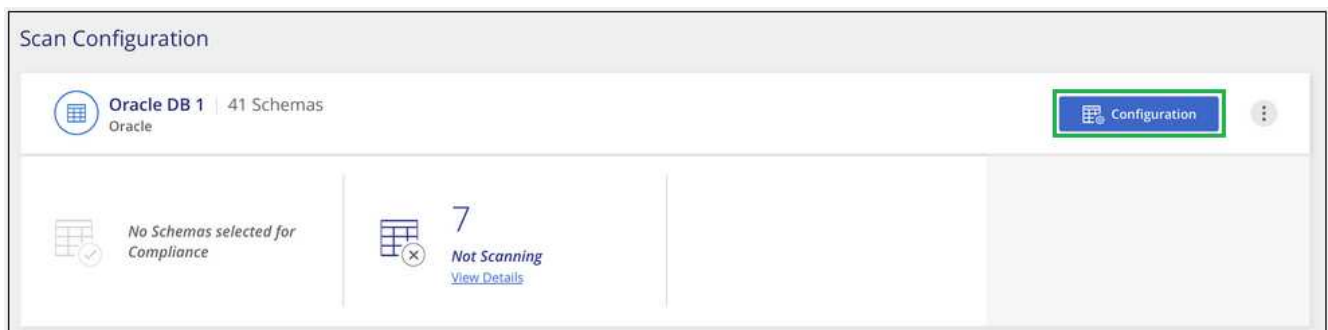
Password

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.


'Working Environment Name' Scan Configuration			
Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

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.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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