



# **Planificación de la migración de datos**

## **XCP**

NetApp  
January 22, 2026

# Tabla de contenidos

Planificación de la migración de datos .....	1
Planificación de la migración de datos .....	1
Planifique la migración de datos NFS .....	1
mostrar .....	1
escanee .....	1
Planifique la migración de datos de SMB .....	2
Mostrar .....	2
Exploración .....	2
Planifique la migración de datos HDFS .....	2
Exploración .....	2
Planificar mediante Análisis de archivos .....	3
Planificar la migración de los datos .....	3
Acceda a File Analytics .....	3
Aregar servidores de archivos .....	6
Ejecute una exploración .....	7
Filtros .....	16
Registro para NFS y SMB (opcional) .....	16
Cree el archivo de configuración JSON .....	18

# Planificación de la migración de datos

## Planificación de la migración de datos

Puede planificar la migración mediante la CLI o la GUI de análisis de archivos.

Utilice los siguientes comandos para planificar la migración:

- Mostrar
- Exploración

Utilice File Analytics para visualizar las estadísticas de exportaciones y recursos compartidos.

## Planifique la migración de datos NFS

Planifique las migraciones de datos NFS.

### mostrar

La `show` Command consulta los servicios RPC y las exportaciones NFS de uno o varios servidores de almacenamiento. El comando enumera los servicios y exportaciones disponibles con la capacidad libre y usada de cada exportación, seguidos por los atributos raíz de cada exportación.

#### Ejemplo:

- `xcp show <NFS file server IP/FQDN>`
- `xcp show nfs_server01.netapp.com`

Ejecución `xcp help show` para obtener más detalles.

### escanee

La `scan` El comando explora de forma recursiva todas las rutas exportadas de NFSv3 de origen e imprime las estadísticas de la estructura de archivos al final del análisis. NetApp recomienda poner los montajes de exportación NFS de origen en modo de solo lectura durante la operación de exploración.



Si un nombre de archivo o directorio contiene caracteres que no sean UTF-8, estos caracteres se convierten al formato UTF-8 y se muestran al ejecutar el `xcp-scan` comando. Dependiendo de la traducción de la codificación de origen a UTF-8, es posible que los caracteres no se muestren como se esperaba.

#### Ejemplo:

- `xcp scan NFS [server:/export path | file:// ]`
- `xcp scan nfs_server01.netapp.com:/export1`
- `xcp scan file:///mnt/nfs-source`

Ejecución `xcp help scan` para obtener más detalles.

De forma opcional, utilice Análisis de archivos para ver los resultados gráficamente.

## Planifique la migración de datos de SMB

Planifique las migraciones de datos de SMB.

### Mostrar

La `show` El comando muestra todos los recursos compartidos de SMB disponibles en el servidor con los permisos y el espacio disponibles. Ejemplo:

- `xcp show \\<SMB file server IP/FQDN>`
- `xcp show smb_server01.netapp.com`

Ejecución `xcp help show` para obtener más detalles.

### Exploración

La `scan` Comando escanea de forma recursiva todo el recurso compartido SMB y enumera todos los archivos al final del análisis.



Durante la operación de exploración, puede utilizar `-preserve-atime` marcar con la `scan` comando para conservar el tiempo de acceso en el origen .

### Ejemplo:

- `xcp scan \\SMB server\share1`
- `xcp scan smb_server01.netapp.com:/share1`

Ejecución `xcp help scan` para obtener más detalles.

De forma opcional, utilice Análisis de archivos para ver los resultados gráficamente.

## Planifique la migración de datos HDFS

Planifique las migraciones de datos HDFS.

### Exploración

La `scan` command explora recursivamente todas las rutas de origen e imprime las estadísticas de la estructura de archivos al final de la exploración.

- `xcp scan HDFS [hdfs://<hdfs mounted path> ]`
- `xcp scan hdfs:///demo/user1`
- `xcp scan s3://my-bucket`
- `xcp scan -s3.profile <s3 profile name> -s3.endpoint <endpoint-url> s3://my-bucket`

Ejecución `xcp help scan` para obtener más detalles.

## Planificar mediante Análisis de archivos

### Planificar la migración de los datos

Planifique la migración de datos con File Analytics.



XCP es una interfaz de línea de comandos, mientras que File Analytics tiene una interfaz gráfica de usuario.

#### Descripción general

XCP File Analytics utiliza la API de exploración XCP para recopilar datos de hosts NFS o SMB. A continuación, estos datos se muestran en la GUI de análisis de archivos XCP. El análisis de archivos XCP incluye tres componentes principales:

- Servicio XCP
- Base de datos de análisis de archivos
- GUI de análisis de archivos para gestionar y ver datos

El método de implementación de los componentes de XCP File Analytics depende de la solución necesaria:

- Implementación de soluciones de análisis de archivos XCP para sistemas de archivos NFS:
  - Puede implementar la GUI de File Analytics, la base de datos y el servicio XCP en el mismo host Linux.
- Implementación de soluciones de análisis de archivos XCP para sistemas de archivos SMB: Debe implementar la GUI y la base de datos de análisis de archivos en un host Linux e implementar el servicio XCP en un host de Windows.

### Acceda a File Analytics

Análisis de archivos proporciona una vista gráfica de los resultados del análisis.

#### Inicie sesión en la GUI de File Analytics

La GUI de XCP File Analytics proporciona un panel de control con gráficos para visualizar el análisis de archivos. La GUI de análisis de archivos XCP se activa al configurar XCP en una máquina Linux.



Para consultar los exploradores admitidos para acceder a File Analytics, consulte "[IMT de NetApp](#)".

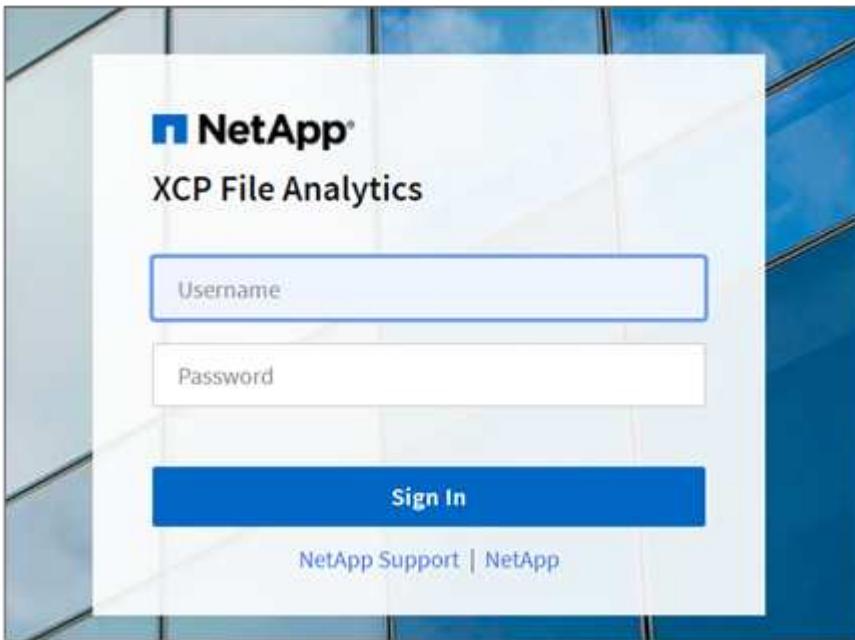
#### Pasos

1. Utilice el enlace `https://<IP address of linux machine>/xcp` Para acceder a la GUI de análisis de archivos. Cuando se le solicite, acepte el certificado de seguridad:
  - a. Seleccione **Avanzado** debajo de la declaración de privacidad.
  - b. Seleccione el **Proceder To <IP address of linux machine>** enlace.
2. Inicie sesión en la GUI de análisis de archivos.

Hay dos formas de iniciar sesión en la GUI de File Analytics:

#### **Inicie sesión con las credenciales de usuario**

- Inicie sesión en la GUI con las credenciales de usuario obtenidas al instalar File Analytics.



- De manera opcional, cambie la contraseña por su propia contraseña.

Si desea cambiar la contraseña obtenida durante la instalación a su propia contraseña, seleccione el ícono de usuario y seleccione **Cambiar contraseña**.

La nueva contraseña debe tener al menos ocho caracteres de longitud y contener al menos un número, una letra mayúscula, una letra minúscula y un carácter especial (! @ # \$ % ^ & \* - \_).



Después de cambiar la contraseña, se cerrará automáticamente la sesión en la GUI y deberá volver a iniciar sesión con la nueva contraseña que creó.

#### **Configure y habilite la funcionalidad SSO**

Puede utilizar esta función de inicio de sesión para configurar XCP File Analytics en un equipo en particular y compartir la URL de la interfaz de usuario web en toda la empresa, lo que permite a los usuarios iniciar sesión en la interfaz de usuario con sus credenciales de inicio de sesión único (SSO).



El inicio de sesión SSO es opcional y se puede configurar y habilitar de forma permanente. Para configurar el inicio de sesión SSO basado en el lenguaje de marcado de aserción de seguridad (SAML), consulte [Configure las credenciales de SSO](#).

- Después de iniciar sesión, puede ver el agente NFS; una marca verde está presente que muestra una configuración mínima del sistema del sistema Linux y la versión XCP.
- Si ha configurado un agente SMB, puede ver el agente SMB agregado en la misma tarjeta de agente.

## Configure las credenciales de SSO

La funcionalidad de inicio de sesión SSO se implementa en XCP File Analytics con SAML y es compatible con el proveedor de identidades de Active Directory Federation Services (ADFS). SAML descarga la tarea de autenticación en el proveedor de identidades (IDP) de terceros de la empresa, que puede utilizar cualquier número de métodos para la MFA (autenticación multifactor).

### Pasos

1. Registre la aplicación XCP File Analytics con su proveedor de identidades empresarial.

El análisis de archivos se ejecuta ahora como proveedor de servicios y, por lo tanto, debe registrarse en el proveedor de identidades de su empresa. En general, existe un equipo en la empresa que se encarga de este proceso de integración SSO. El primer paso es buscar y contactar con el equipo pertinente y compartir con ellos los detalles de metadatos de la aplicación File Analytics.

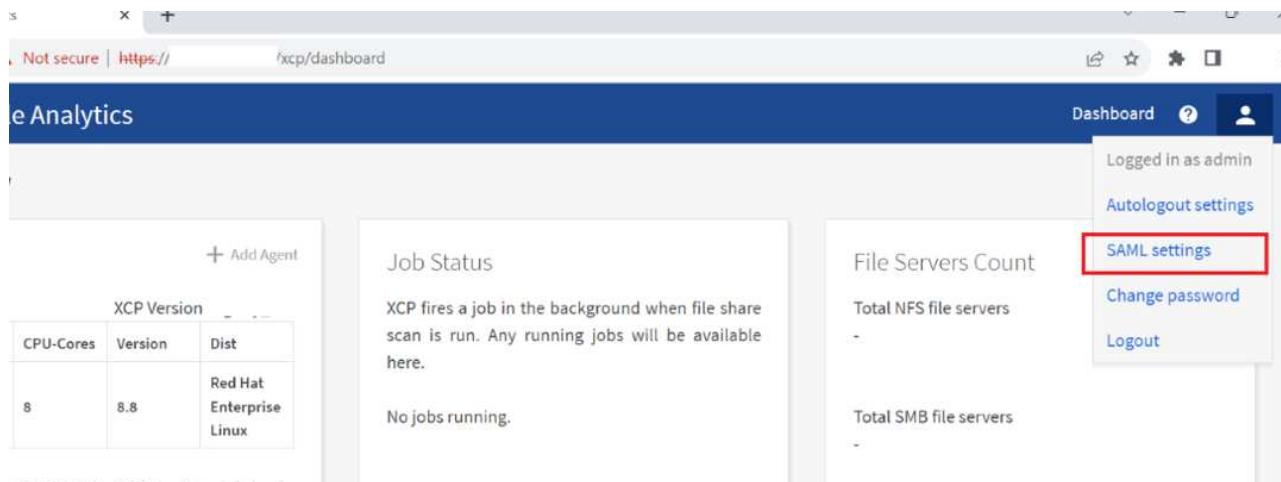
A continuación se muestran los detalles obligatorios que debe compartir para registrarse en su proveedor de identidades:

- **ID de entidad de proveedor de servicios:** `https://<IP address of linux machine>/xcp`
- **URL del Servicio de consumidores de aserción del proveedor de servicios (ACS):** `https://<IP address of linux machine>:5030/api/xcp/SAML/sp`

También puede verificar estos detalles iniciando sesión en la interfaz de usuario de File Analytics:

- i. Inicie sesión en la GUI mediante los pasos descritos en [Inicie sesión en la GUI de File Analytics](#).
- ii. Seleccione el ícono **Usuario** en la esquina superior derecha de la página y, a continuación, seleccione **Configuración de SAML**.

Compruebe **Ajustes del proveedor de servicios** en el menú desplegable que aparece.

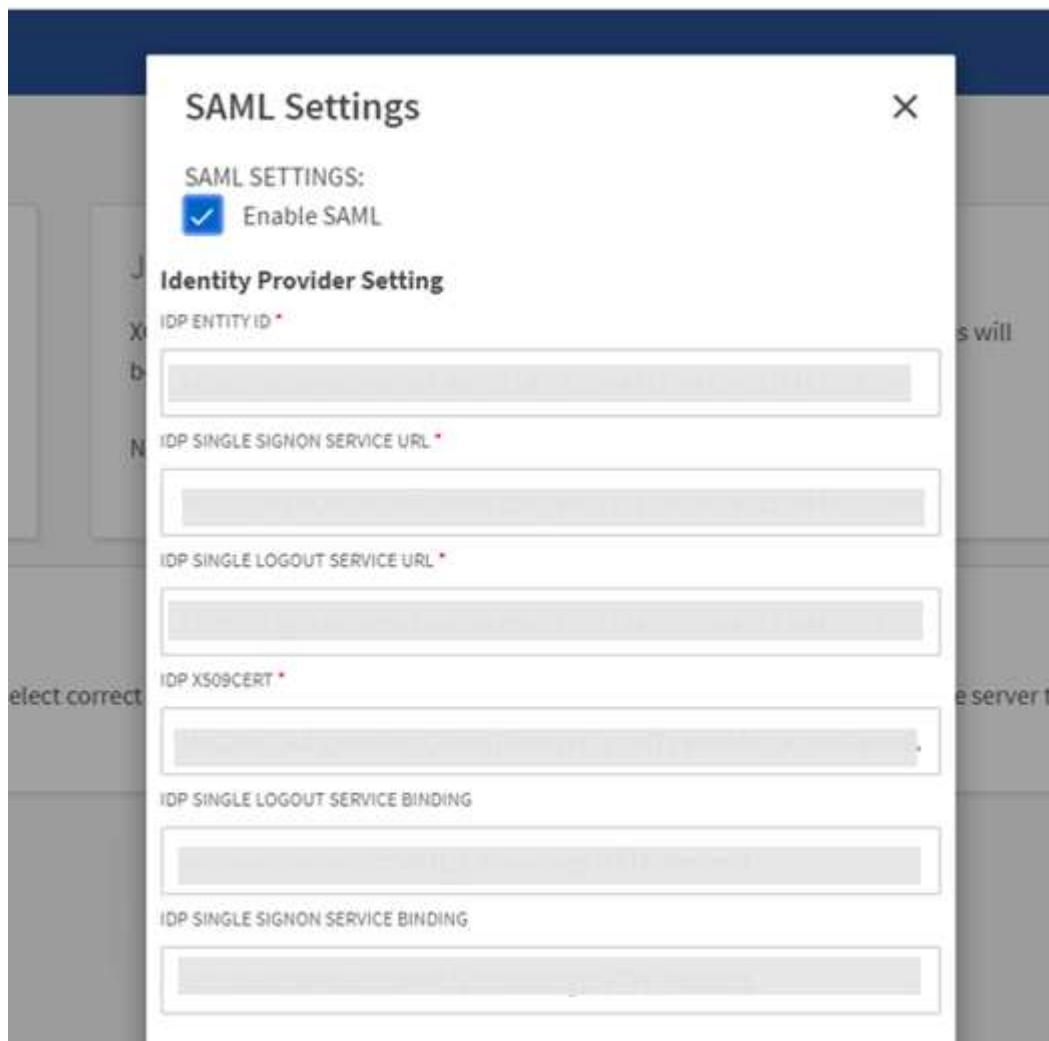


Después del registro, recibirá los detalles de los extremos de IDP de su empresa. Debe proporcionar estos metadatos de extremo de IDP a la interfaz de usuario de análisis de archivos.

2. Proporcione los detalles del IDP:

- a. Vaya a **Panel**. Seleccione el ícono **Usuario** en la esquina superior derecha de la página y seleccione **Configuración de SAML**.
- b. Introduzca los detalles de IDP que obtuvo después del registro.

## ejemplo



- a. Active la casilla de verificación **Habilitar SAML** para habilitar de forma permanente SSO basado en SAML.
- b. Seleccione **Guardar**.
- c. Cierre la sesión en File Analytics y vuelva a iniciarla.

Se le redirigirá a su página SSO de empresa.

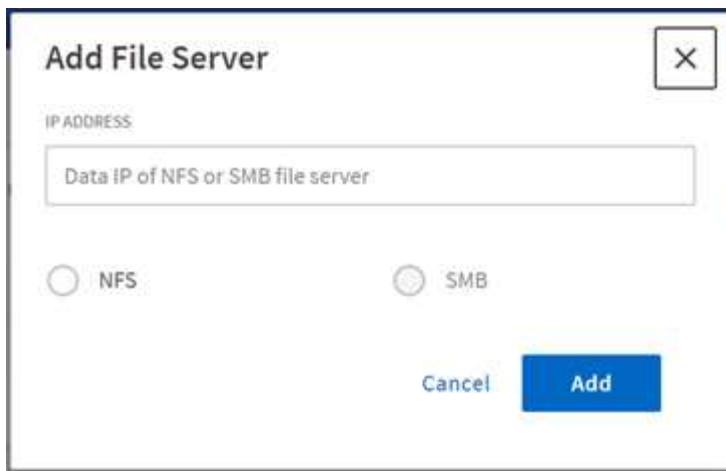
## Agregar servidores de archivos

Puede configurar sistemas de archivos exportados NFS y SMB en la GUI de análisis de archivos XCP.

Esto permite a XCP File Analytics analizar y analizar datos en el sistema de archivos. Siga estos pasos para añadir servidores de archivos NFS o SMB.

### Paso

1. Para agregar servidores de archivos, seleccione **Agregar servidor de archivos**.



Agregue la dirección IP del servidor de archivos, seleccione la opción NFS o SMB y haga clic en **Agregar**.



Si no puede ver un agente SMB en la GUI, no podrá agregar un servidor SMB.

Después de agregar el servidor de archivos, XCP muestra:

- Total de recursos compartidos de archivos disponibles
- Archivos compartidos con datos de análisis (el recuento inicial es “0”, se actualiza cuando se ejecuta un análisis correcto)
- Uso total del espacio: La suma del espacio utilizado por todas las exportaciones
- Los datos para recursos compartidos de archivos y aprovechamiento del espacio son datos en tiempo real directamente desde el servidor NFS/SMB. La recogida y el procesamiento de los datos tarda varios segundos.



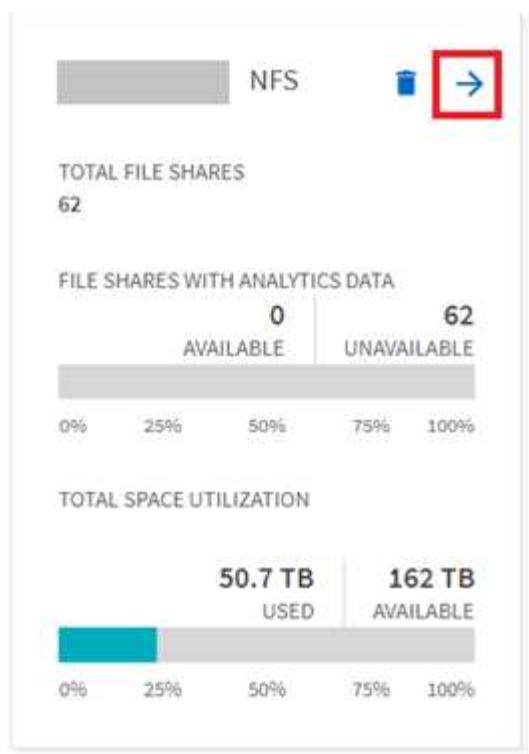
El espacio disponible frente al espacio utilizado en Análisis de archivos se calcula a partir de cada sistema de archivos exportado disponible a través de NFS. Por ejemplo, si los volúmenes constan de qtrees y las exportaciones se crean a través de un qtree, el espacio general es el espacio acumulativo del tamaño del volumen y del tamaño del qtree.

## Ejecute una exploración

Cuando el sistema de archivos NFS/SMB se agrega a la GUI de análisis de archivos XCP, puede iniciar un análisis del sistema de archivos para analizar y representar los datos.

### Pasos

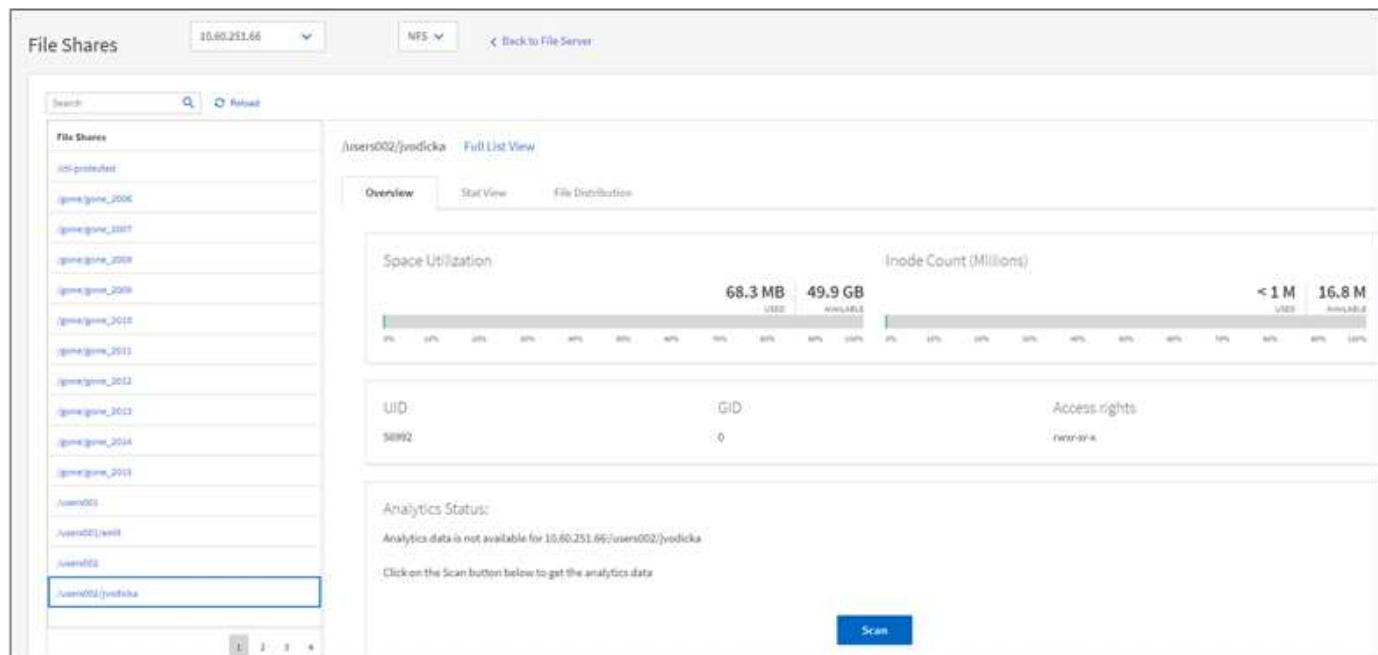
1. Seleccione la flecha de la tarjeta del servidor de archivos agregada para ver los recursos compartidos de archivos en el servidor de archivos.



2. En la lista de archivos compartidos, seleccione el nombre del recurso compartido de archivos que desea analizar.
3. Seleccione **Escanear** para iniciar la exploración.

XCP muestra una barra de progreso para la exploración.

4. Una vez finalizada la exploración, se activan las fichas **stat View** y **distribución de archivos** para que pueda ver los gráficos.

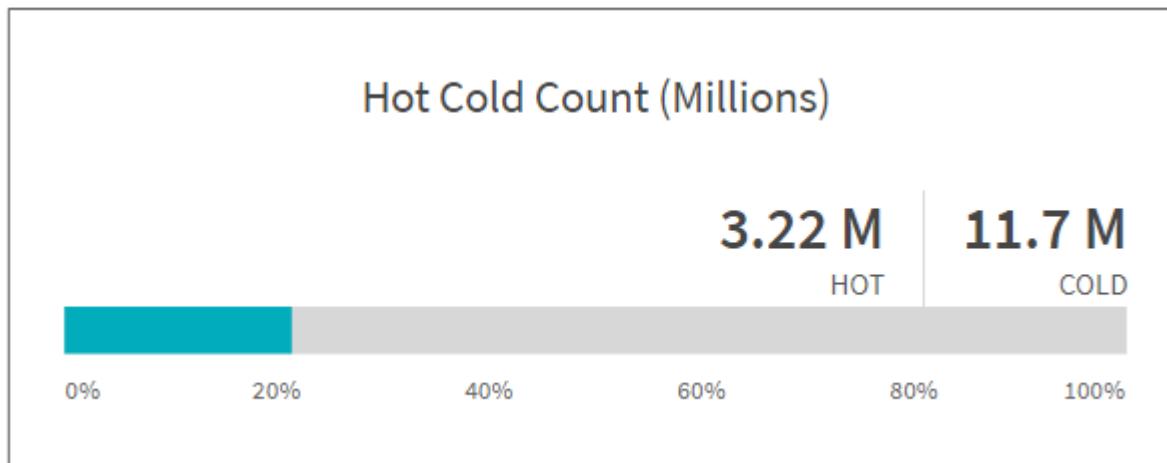


## Más información acerca de los gráficos

El panel GUI de File Analytics muestra varios gráficos para visualizar el análisis de archivos.

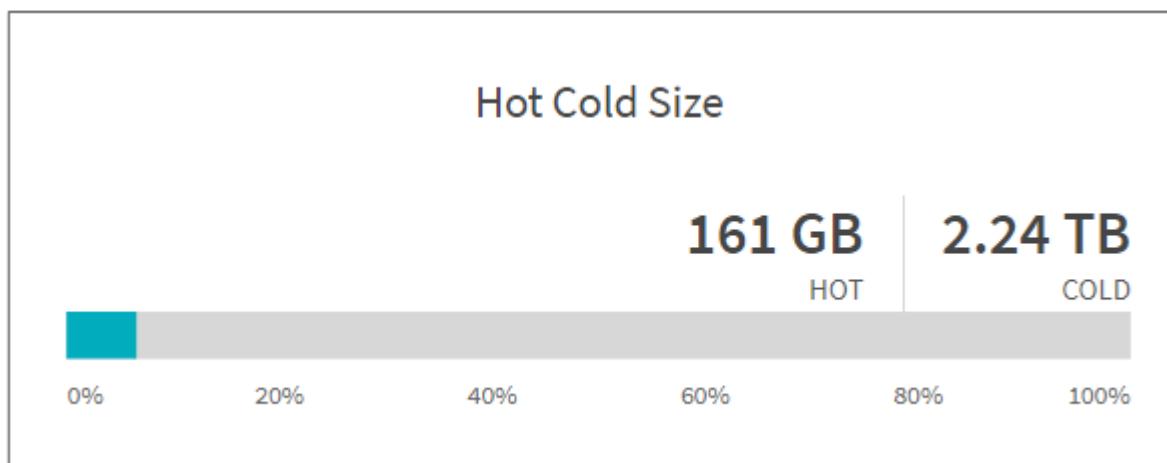
### Gráfico de recuento en frío caliente

XCP File Analytics categoriza los archivos a los que no se acceda durante 90 días como datos inactivos. Los archivos a los que se accede en los últimos 90 días son datos activos. Los criterios para definir los datos activos e inactivos se basan únicamente en el tiempo de acceso.



El gráfico Hot Cold Count muestra el número de inodos (en millones) que están activos o inactivos en XCP NFS. En XCP SMB, este gráfico indica el número de archivos activos o inactivos. La barra de colores representa los datos activos y muestra el porcentaje de archivos a los que se accede en un plazo de 90 días.

### Gráfico de tamaño frío caliente



El gráfico Hot Cold Size muestra el porcentaje de archivos activos e inactivos y el tamaño total de los archivos de cada categoría. La barra de colores representa los datos activos y la parte sin color representa los datos fríos. Los criterios para definir los datos activos e inactivos se basan únicamente en el tiempo de acceso.

### Entradas en Gráfico de directorios

Entries In Directory

Depth	Count	
10-100	443506	
100-1K	19818	
1K-10K	1050	
1-10	2362671	
>10K	21	
empty	479797	

El gráfico Entradas en directorios muestra el número de entradas en los directorios. La columna Depth contiene diferentes tamaños de directorio y la columna Count indica el número de entradas en cada profundidad de directorio.

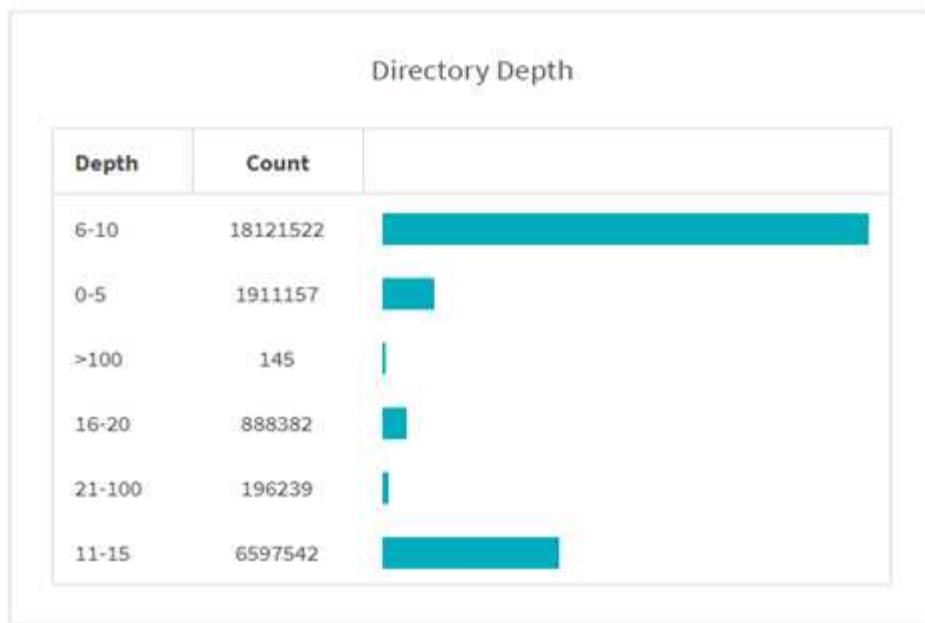
Distribución de archivos por gráfico de tamaño

File Distribution By Size

File Size	Count	
8-64KiB	5998834	
10-100MiB	17069	
>100MiB	3589	
<8KiB	16046580	
64KiB-1MiB	1034391	
1-10MiB	109732	
empty	467594	

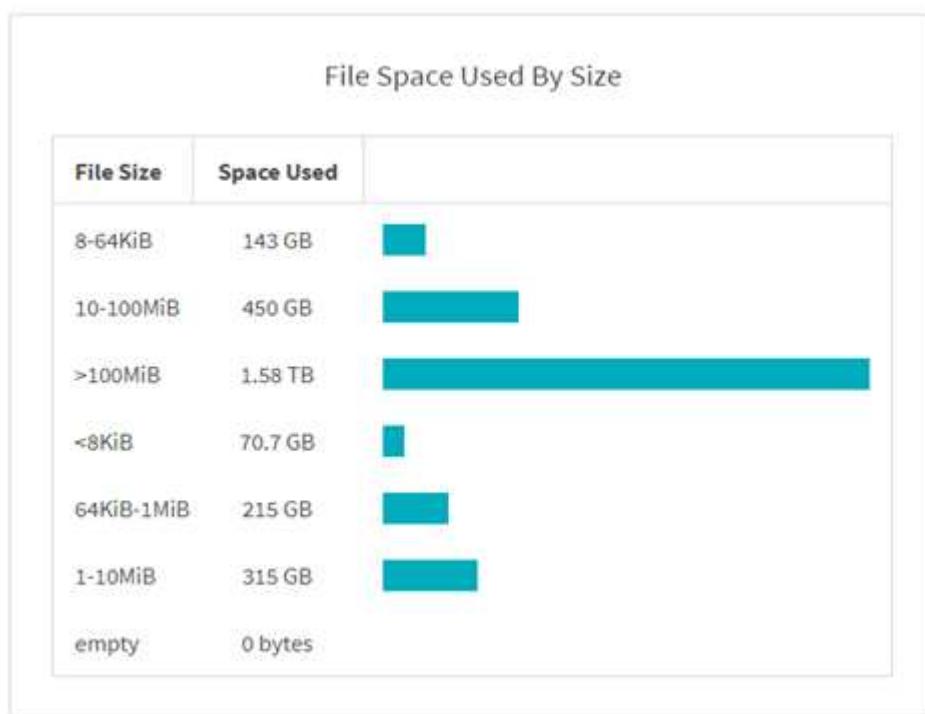
El gráfico distribución de archivos por tamaño muestra el número de archivos que están debajo de los tamaños de archivo especificados. La columna Tamaño de archivo contiene las categorías de tamaño de archivo y la columna número indica la distribución del número de archivos.

Gráfico de profundidad del directorio



El gráfico profundidad de directorios representa la distribución del número de directorios en varios rangos de profundidad de directorios. La columna Depth contiene varias profundidades de directorio y la columna Count contiene el recuento de cada profundidad de directorio en el recurso compartido de archivos.

#### Espacio de archivos utilizado por gráfico de tamaño



El gráfico espacio de archivos utilizado por Tamaño muestra el número de archivos en diferentes rangos de tamaño de archivo. La columna Tamaño de archivo contiene distintos rangos de tamaño de archivo y la columna espacio utilizado indica el espacio utilizado por cada intervalo de tamaño de archivo.

#### Gráfico espacio ocupado por usuarios

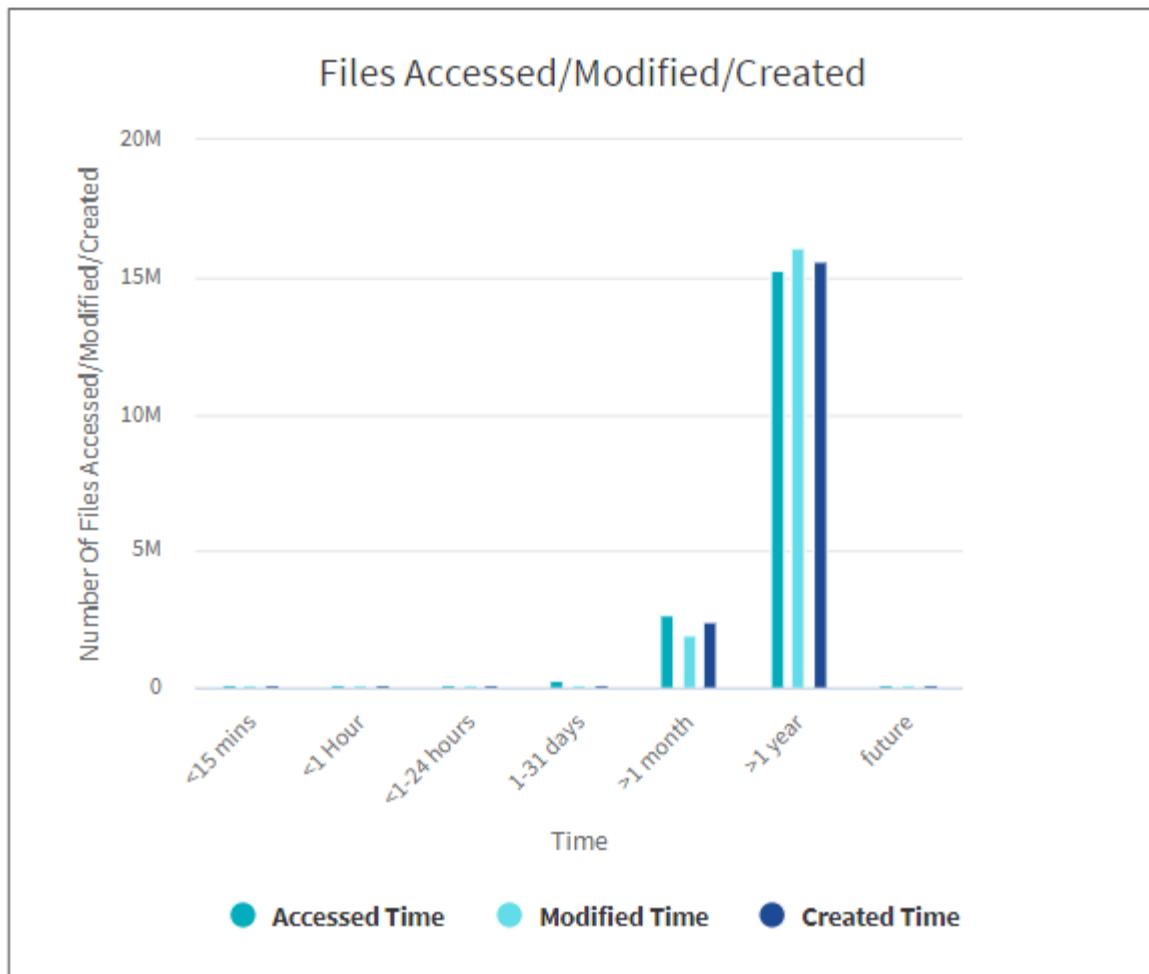
### Space Occupied By Users

Username	Space Used	
4568	47.8 GB	
14952	67.1 GB	
19592	48.2 GB	
48973	54.5 GB	
50900	47.3 GB	

1 2

El gráfico espacio ocupado por los usuarios muestra el espacio utilizado por los usuarios. La columna Nombre de usuario contiene los nombres de los usuarios (UID cuando no se pueden recuperar los nombres de usuario) y la columna espacio utilizado indica el espacio utilizado por cada nombre de usuario.

### Gráfico de archivos accedidos, modificados o creados

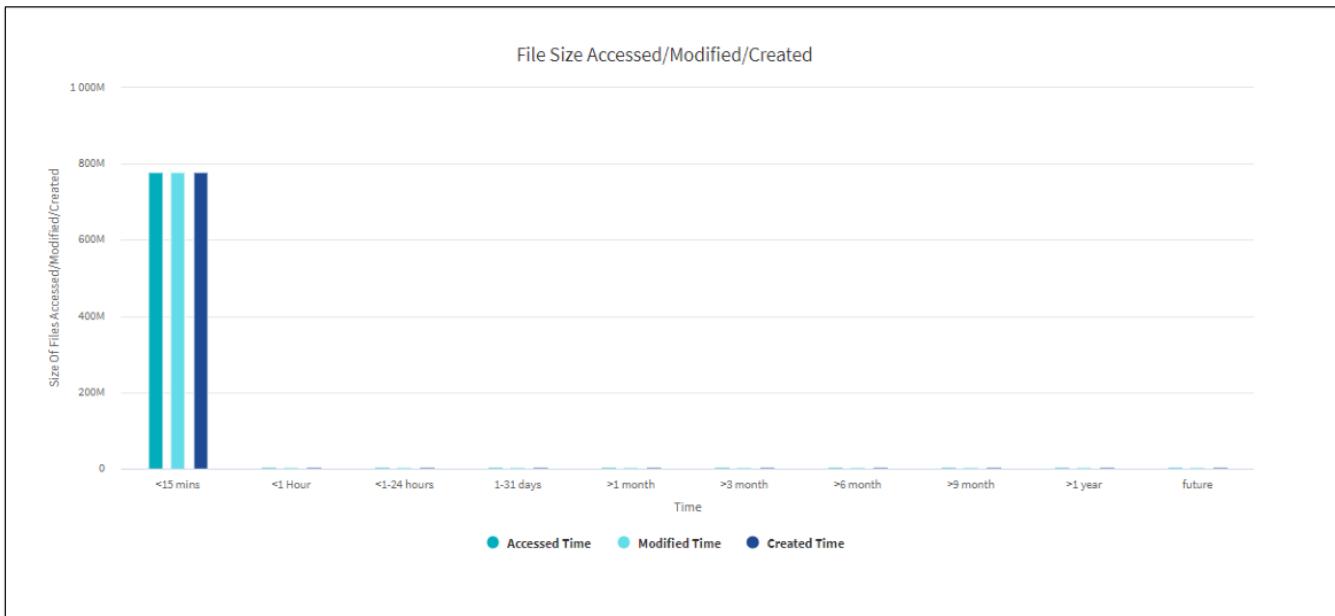


El gráfico Archivos accedidos/modificados/creados muestra el recuento de archivos modificados a lo largo del tiempo. El eje X representa el período de tiempo en el que se realizaron los cambios y el eje Y representa el número de archivos modificados.



Para obtener el gráfico de tiempo de acceso (atime) en los análisis de SMB, marque la casilla de verificación conservar atime antes de ejecutar un análisis.

#### Gráfico de tamaño de archivo accedido/modificado/creado



El gráfico Tamaño de archivo al que se ha accedido/modificado/creado muestra el tamaño de los archivos modificados con el tiempo. El eje X representa el período de tiempo en el que se realizaron los cambios y el eje Y representa el tamaño de los archivos modificados.



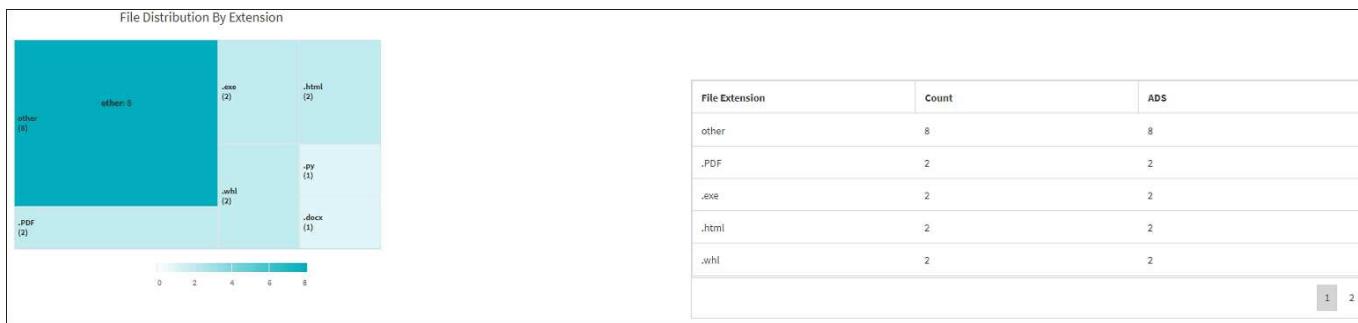
Para obtener el gráfico de tiempo de acceso (atime) en los análisis de SMB, marque la casilla de verificación conservar atime antes de ejecutar un análisis.

#### Distribución de archivos por gráfico de extensión



El gráfico distribución de archivos por extensión representa el recuento de las diferentes extensiones de archivo de un recurso compartido de archivos. El tamaño de las divisiones que representan las extensiones se basa en el número de archivos con cada extensión.

Además, para los recursos compartidos SMB, puede obtener el número de archivos de flujos de datos alternativos para cada extensión de archivo activando la casilla para los flujos de datos alternativos antes de ejecutar un análisis.

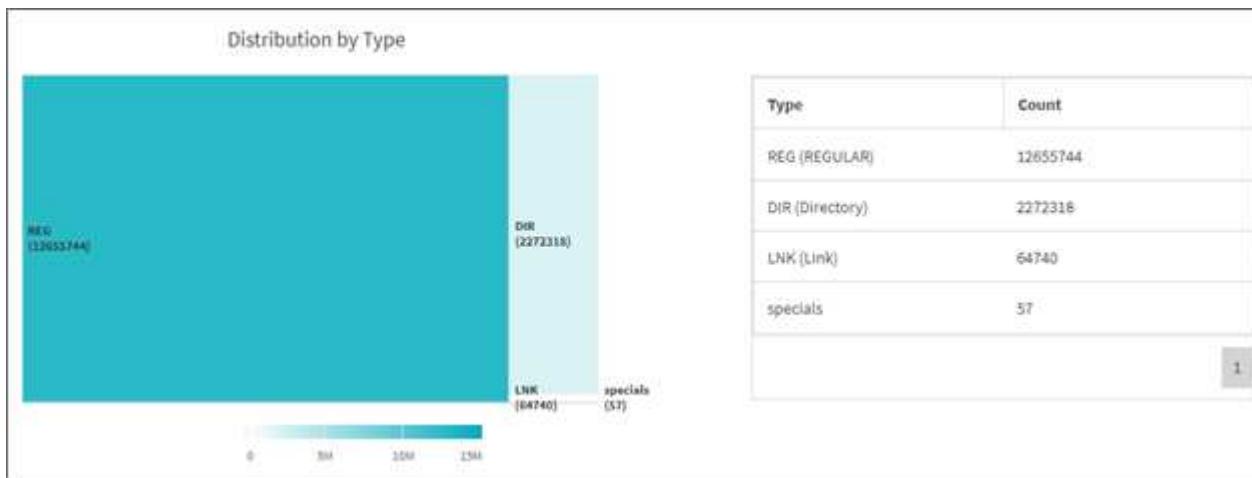


## Distribución de tamaño de archivo por gráfico de extensión



El gráfico Distribución de tamaño de archivo por extensión representa el tamaño acumulativo de las diferentes extensiones de archivo en un recurso compartido de archivos. El tamaño de las divisiones que representan las extensiones se basa en el tamaño de los archivos con cada extensión.

## Distribución de archivos por gráfico de tipo



El gráfico distribución por tipo representa el recuento de los siguientes tipos de archivos:

- REG: Archivos regulares
- LNK: Archivos con vínculos
- Especiales: Archivos con archivos de dispositivos y archivos de caracteres.
- DIR: Archivos con directorios

- Junction: Disponible únicamente en SMB

Además, para recursos compartidos SMB, puede obtener el número de archivos de flujos de datos alternativos para diferentes tipos activando la casilla para flujos de datos alternativos antes de ejecutar una exploración.



## Filtros

XCP proporciona opciones de filtro que se pueden utilizar en operaciones XCP.

XCP utiliza filtros para `-match` y `-exclude`. Opciones para NFS y SMB.

Para NFS, ejecute `xcp help info` Y consulte la sección DE FILTROS para ver cómo usar `-match` y `-exclude` filtros.

Para SMB, ejecute `xcp help -match` y `xcp help -exclude` para obtener más información acerca de `match` y `exclude` filtros.

Si desea utilizar filtros en los comandos XCP, ejecute `xcp help <command>` para ver si son opciones compatibles.

## Registro para NFS y SMB (opcional)

Registro para XCP NFS y SMB.

XCP admite la configuración de varias funciones opcionales mediante el `xcpLogConfig.json` Archivo de configuración JSON. Para habilitar sólo funciones específicas, cree manualmente la `xcpLogConfig.json` archivo de configuración. Puede utilizar el `xcpLogConfig.json` archivo de configuración para habilitar:

- mensajes del registro de eventos
- Cliente syslog para XCP
- Registro XCP personalizado

Los mensajes del registro de eventos y el cliente de syslog están deshabilitados en la configuración predeterminada. La configuración es común para NFS y SMB.

Configurar la ubicación del archivo JSON	NFS	SMB
Ubicación predeterminada del archivo de configuración	/Opt/NetApp/xFiles/xcp/	C:\NetApp\XCP\ConfigFile
La ubicación personalizada requiere la <code>XCP_CONFIG_DIR</code> variable de entorno	Utilice la ubicación que ha establecido en <code>XCP_CONFIG_DIR</code> variable	N.A.

Las opciones del archivo de configuración JSON distinguen mayúsculas de minúsculas. Estas opciones son las mismas para XCP NFS y XCP SMB.

Nombre de las subopciones	Tipo de datos JSON	Predeterminado	Descripción
LogConfig			Opción para personalizar el registro XCP.
"nivel"	Cadena	INFORMACIÓN	Nivel de filtro de gravedad de los mensajes de registro. Los mensajes de registro XCP admiten cinco niveles de gravedad por orden de disminución de gravedad: CRÍTICO, ERROR, ADVERTENCIA, INFORMACIÓN, DEPURACIÓN (NetApp recomienda encarecidamente utilizar INFO o DEBUG).
"Maxbytes"	Entero	52428800	Tamaño de cada archivo de registro giratorio. El número máximo de archivos de rotación admitidos es 10.
"nombre"	Cadena	xcp.log	Opción para establecer el nombre del archivo de registro personalizado.
eventlog			Opción para configurar el mensaje de registro de eventos.
".IsEnabled"	Booleano	verdadero	Esta opción booleana se utiliza para habilitar la mensajería de eventos. Configuración en <code>false</code> no generará ningún mensaje de evento y no se publicará ningún registro de eventos en el archivo de registro de eventos.
"nivel"	Cadena	INFORMACIÓN	Nivel de filtro de gravedad de mensajes de eventos. La mensajería de eventos admite cinco niveles de gravedad en orden decreciente: CRÍTICO, ERROR, ADVERTENCIA, INFORMACIÓN, DEPURACIÓN
syslog			Opción para configurar la mensajería de syslog.
".IsEnabled"	Booleano	falso	Esta opción booleana se utiliza para habilitar el cliente de syslog en XCP.
"nivel"	Cadena	INFORMACIÓN	Nivel del filtro de gravedad del mensaje. Los mensajes de registro de sucesos XCP admiten cinco niveles de gravedad en orden de disminución de gravedad: CRÍTICO, ERROR, ADVERTENCIA, INFORMACIÓN, DEPURACIÓN
"ServerIP"	Cadena	Ninguno	Nombre de host o direcciones IP del servidor de syslog remoto.

Nombre de las subopciones	Tipo de datos JSON	Predeterminado	Descripción
“puerto”	Entero	514	Puerto del receptor de syslog remoto. Los receptores de syslog que aceptan datagramas de syslog en un puerto diferente se pueden configurar con la opción de puerto UDP puerto 514, pero también se puede configurar para el puerto deseado.
“higienizar”	Booleano	falso	Una opción común para la compatibilidad con XCP; al establecer su valor en true, se oculta la información confidencial (IP y nombre de usuario) en los mensajes que se van a admitir (registro, eventos, syslog, etc.). Por ejemplo, con el sanitize opción como false: * 2020-07-17 03:10:23,779 - INFO - 12806 xcp xcp Paths: ['10.234.104.251:/cat_vol'] * 2020-07-17 03:10:23,778 - INFO - 12806 xcp xcp User Name: root`Con la `sanitize opción como true: * 2020-07-17 03:13:51,596 - INFO - 12859 xcp xcp Paths: ['IP: XX.XX.XX.XX:/cat_vol'] * 2020-07-17 03:13:51,595 - INFO - 12859 xcp xcp User Name: * * *

## Cree el archivo de configuración JSON

Si desea habilitar los mensajes del registro de eventos, el cliente syslog o el registro de clientes, complete los siguientes pasos.

### Pasos

1. Abra cualquier editor de texto, como bloc de notas o vi.
2. Cree un archivo nuevo con la siguiente plantilla JSON.

```
{  
  "logConfig": {  
    "level": "INFO",  
    "maxBytes": 52428800,  
    "name": "xcp.log"  
  },  
  "eventlog": {  
    "isEnabled": false,  
    "level": "INFO"  
  },  
  "syslog": {  
    "isEnabled": false,  
    "level": "INFO",  
    "serverIp": "10.234.219.87",  
    "port": 514  
  },  
  "sanitize": false  
}
```

3. Para las funciones que desee activar, cambie la `isEnabled` valor a. `true`.
4. Asigne un nombre al archivo `xcpLogConfig.json` Y guárdelo en la ubicación predeterminada:  
`/Opt/NetApp/xFiles/xcp/`

Si la `XCP_CONFIG_DIR` se establece la variable de entorno, guarde la `xcpLogConfig.json` archivo en la misma ubicación que se establece en la `XCP_CONFIG_DIR` variable.

## Configuración predeterminada

```
{  
  "logConfig": {  
    "level": "INFO",  
    "maxBytes": 52428800,  
    "name": "xcp.log"  
  },  
  "sanitize": false  
}
```

## Archivo de configuración del json de ejemplo

```
{  
  "logConfig": {  
    "level": "INFO",  
    "maxBytes": 52428800,  
    "name": "xcp.log"  
  },  
  "eventlog": {  
    "isEnabled": false,  
    "level": "INFO"  
  },  
  "syslog": {  
    "isEnabled": false,  
    "level": "INFO",  
    "serverIp": "10.234.219.87",  
    "port": 514  
  },  
  "sanitize": false  
}
```

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

## Información de la marca comercial

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