



# **NetApp XCP documentation**

**XCP**

NetApp  
March 14, 2024

This PDF was generated from <https://docs.netapp.com/us-en/xcp/index.html> on March 14, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

NetApp XCP documentation .....	1
XCP v1.9.3 Release Notes .....	2
Get started with XCP .....	3
Learn about XCP .....	3
XCP NFS add-on features .....	4
Unsupported features .....	5
Supported configurations .....	6
Ports used by XCP .....	7
Install XCP .....	8
Prepare for XCP installation .....	8
Prepare Linux for XCP NFS .....	10
Prepare Windows for XCP SMB .....	11
Prepare File Analytics .....	13
Install XCP NFS .....	14
Install XCP SMB .....	17
Install File Analytics for NFS .....	19
Install File Analytics for SMB .....	20
Configure XCP .....	23
Configure the INI file .....	23
Performance tuning .....	24
Environment variable .....	24
Configure the POSIX connector .....	25
Configure the HDFS connector .....	27
Configure multinode scale-out .....	28
Configure the S3 connector .....	30
Plan data migration .....	32
Plan NFS data migration .....	32
Plan SMB data migration .....	33
Plan HDFS data migration .....	33
Plan using File Analytics .....	34
Filters .....	47
Logging for NFS and SMB (optional) .....	47
Migrate data .....	51
Migrate NFS data .....	51
Migrate SMB data .....	53
Migrate HDFS data .....	54
Run multiple XCP jobs on the same XCP host .....	56
Additional NFS features .....	57
Troubleshoot .....	60
Troubleshoot XCP NFS errors .....	60
Troubleshoot XCP SMB errors .....	63
Troubleshoot XCP File Analytics errors .....	65
Legal notices .....	69

Copyright .....	69
Trademarks .....	69
Patents .....	69
Privacy policy .....	69
Open source .....	69

# NetApp XCP documentation

# XCP v1.9.3 Release Notes

The [XCP v1.9.3 Release Notes](#) describe new features, upgrade notes, fixed issues, known limitations, and known issues.

You are required to sign on to the NetApp Support Site to access the Release Notes.

# Get started with XCP

## Learn about XCP

NetApp XCP is a client-based software that allows for scalable and high-performance data migrations for any-to-NetApp and NetApp-to-NetApp data migrations and file analytics. XCP is designed to scale and achieve greater performance by utilizing all the available system resources to manage high-volume datasets and high-performance data migrations. XCP helps you get complete visibility into the file system with the option to generate customer reports. Thanks to the matching and formatting capabilities, you can customize the reports to match any reporting needs.

Use XCP for NFS or SMB systems as one of the following solutions:

- Migration solution
- File Analytics solution

XCP is command-line software available in a single package supporting NFS and SMB protocols. XCP is available as a Linux binary for NFS datasets and is available as a Windows executable for SMB datasets.

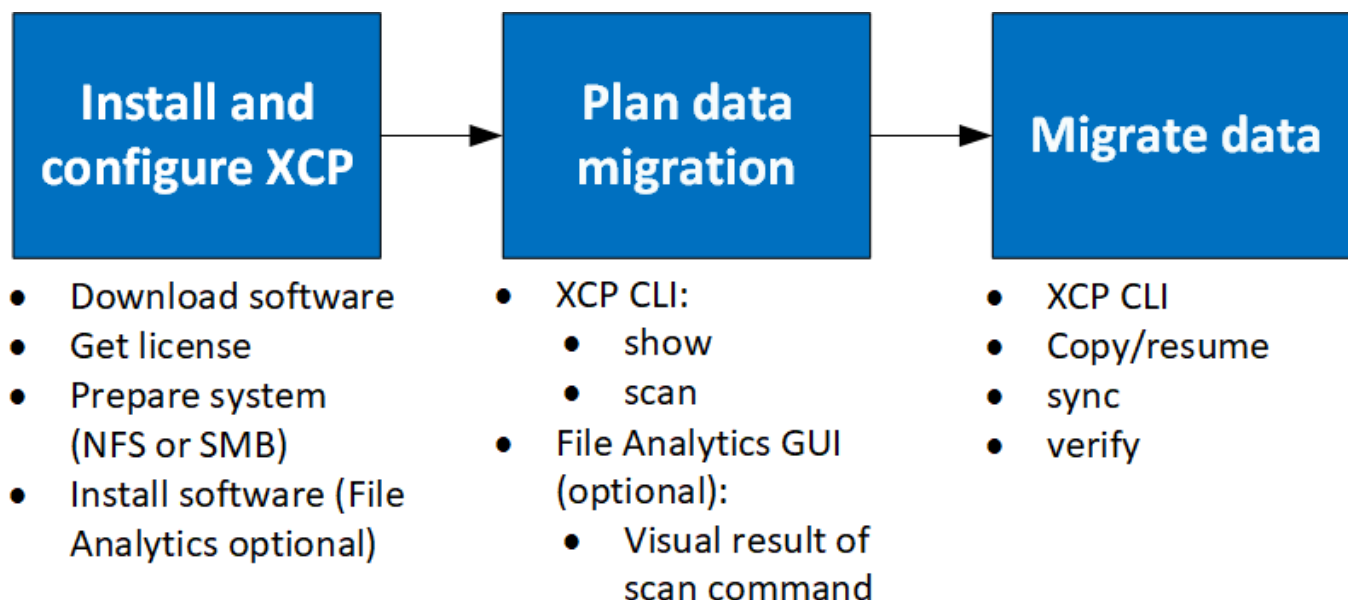
XCP File Analytics is host-based software that detects file shares, runs scans on the file system, and provides a dashboard for file analytics. XCP File Analytics works for both NetApp and third-party systems and runs on Linux or Windows hosts to provide analytics for NFS and SMB exported file systems. The binary for the file analytics GUI is included in the single package supporting NFS and SMB protocols.



The XCP binary is code signed. For more details, please refer to the README in `NETAPP_XCP_<version>.tgz`.

The XCP CLI is robust. For more information, download *XCP Reference* on the [XCP site](#).

### XCP workflow



# XCP NFS add-on features

The XCP NFS add-on features support the use of POSIX and HDFS connectors, enhance security, and support the use of scale-out architecture to speed up data migrations.

## NFSv4 support

When you only enable NFSv4 on the source, destination, and catalog volumes in the data center, you can use the POSIX path instead of the export path to migrate your data. To use the POSIX path, you must first mount the source, destination, and catalog volumes on the host system running XCP and then use the POSIX file path to provide the source and destination to XCP. See [Configure the POSIX connector](#).



- NFSv4 support is limited to the POSIX path and the `copy` operation, the `sync` operation is not supported.
- The POSIX connector might be slower when compared to the XCP NFSv3 TCP socket client engine.

## POSIX connectors

XCP 1.8 supports the use of POSIX connectors to provide source, destination, and catalog paths for data migration. The POSIX connector (`file://`) gives XCP the capability to access any Linux-mounted file system, such as NFSv4, XFS, and Veritas. For non-root users, the system administrator can mount the file system to give any non-root user the capability to access the file system by using a POSIX connector with the `file://` prefix.

You can benefit from using POSIX connectors when you do not have enough permissions to mount the file or when the support available in the data centers is limited to NFSv4. In such cases, any root user can mount the source and destination and then access the path by using a POSIX connector. When you are using POSIX connectors, you can only run the `xcp copy` operation.

## XCP security

The XCP security feature gives you the capability to perform a migration as a non-root user on a Linux host machine. In earlier XCP versions, as a root user on the Linux machine, you perform a migration with all the permissions for the source, destination, and catalog volumes, and the mount is completed by the XCP operations.

When you are performing data migrations, it is common to turn off security and let an administrator copy everything as fast as possible. For ongoing transitions in production environments where XCP has been in use for several years, it is not secure to run as an administrator (or root). Therefore, removing the requirement to run XCP as the root user gives you the capability to use XCP in secure environments. When a regular non-root user runs XCP operations, the non-root user has the same access rights and limits as the user.

In this secure environment, a root user can mount the source, destination, and catalog volume on the host machine and provide the necessary permissions for the destination and catalog volumes for a non-root user to write the data. This gives the non-root user the capability to perform a migration by using the XCP POSIX connector feature.

## XCP scale-out

Until now, data migration using XCP was limited to a single host with higher RAM and CPU. To speed up the migration, memory and cores on the single host were increased, but it could still take a significant time to copy petabytes of data. XCP scaled-out architecture gives you the capability to use multiple hosts to perform a data migration. With this feature, you can use multiple Linux hosts to distribute your workload and decrease the migration time.

You can benefit from multinode scale-out in any environment where the performance of a single system is not sufficient. To overcome the performance limits of a single node, you can use a single `copy` (or `scan -md5`) command to run workers on multiple Linux systems or Hadoop cluster nodes. Currently, XCP scale-out is only supported for `copy` command operations.

## Hadoop Distributed File System connectors

XCP supports migrating data from a Hadoop Distributed File System (HDFS) file system to a NetApp file system and vice versa. In a Hadoop environment with security enabled, a non-root user on a Hadoop cluster can perform the migration to a NetApp NFSv4 exported file system. The HDFS connector (`hdfs://`) gives XCP the capability to access any HDFS file system that is available with different vendors. A non-root user can use XCP to perform migrations by using HDFS or POSIX connectors.

You can include HDFS clusters in an XCP scale-out configuration because they use multiple high end Linux machines. This minimizes the requirement for additional XCP worker nodes. For the data migration, you have the choice to reuse the HDFS cluster nodes or to go with separate hosts.



HDFS connectors are qualified and supported for MapR and Cloudera clusters but can only perform a baseline `copy` operation.

## Unsupported features

The following features are not supported on XCP NFS:

Feature Name	Description
IPv6	Does not support IP version 6 (IPv6)
NFSv4 access control lists (ACLs) (third-party)	Does not support third-party to NetApp NFSv4 ACLs
POSIX connector	<ul style="list-style-type: none"><li>• The <code>sync</code> command does not support the POSIX connector</li><li>• You should not use the <code>copy</code> command when the source is active</li></ul>
Linux	XCP is no longer supported on earlier distributions of Linux that were supported by XCP 1.6.3.
Active source support	XCP does not support combining baseline or incremental Snapshot copy operations with live source migrations.
NFS to S3 migration	XCP does not support NFS to S3 migration.

The following features are not supported on XCP SMB:



Feature Name	Description
NFS symbolic link (symlink)	NFS symlink is not supported in XCP SMB
ACL option for scan	ACLs not supported for scan option
IPv6	Does not support IP version 6 (IPv6)
XCP Filters	The XCP SMB exclude option currently excludes directories based on their pattern in the filter and traverses the filesystem of those directories.
Live source migration	XCP does not support modifying data on the source volume during migration.
Multiple instances of XCP on the same host	When running multiple instances of XCP on the same host you might get unpredictable results.

The following common features are not available for XCP NFS and SMB:

- **Time to complete migration:** XCP upfront does not provide the time to complete the migration or the time to complete any command used for migration. If you are doing final cutover confirm that data churn on the source volume is low.
- **Running copy again on an uncleaned target:** XCP baseline copy will fail when there is partial data on the destination target. For a successful XCP baseline copy and XCP verify, the destination must be clean.
- **Live destination:** XCP does not support modifying data on the destination volume during a migration or during an incremental sync.
- **Non-root user for File Analytics:** XCP does not support installations and configurations performed by a non-root user or a sudo user.

The following features are not available for Hadoop Distributed File System (HDFS) connectors:

Feature Name	Description
Support for the <code>sync</code> command	The HDFS connector does not support the <code>sync</code> command.
Symbolic link (symlink) and hard link support	The HDFS file system does not support symlinks, hard links, or special files.
Live source HDFS migration	XCP does not support modifying data on the HDFS file system at the source during migration

The following features are not available for Simple Storage Service (S3) connectors:

- **Migration with S3 bucket as the source:** XCP does not support migration with an S3 bucket as the source.

## Supported configurations

All the XCP supported configurations such as hosts, ONTAP versions, and supported browsers, are listed in the [Interoperability Matrix Tool \(IMT\)](#).

## Ports used by XCP

The following ports are used by XCP.

Service	Port
CIFS	445 TCP/UDP
HTTP (httpd)	80
HTTPS	443
NFS	111 TCP/UDP and 2049 TCP/UDP
Postgresql	5432
XCP (as a service for File Analytics)	5030
HDFS	7222

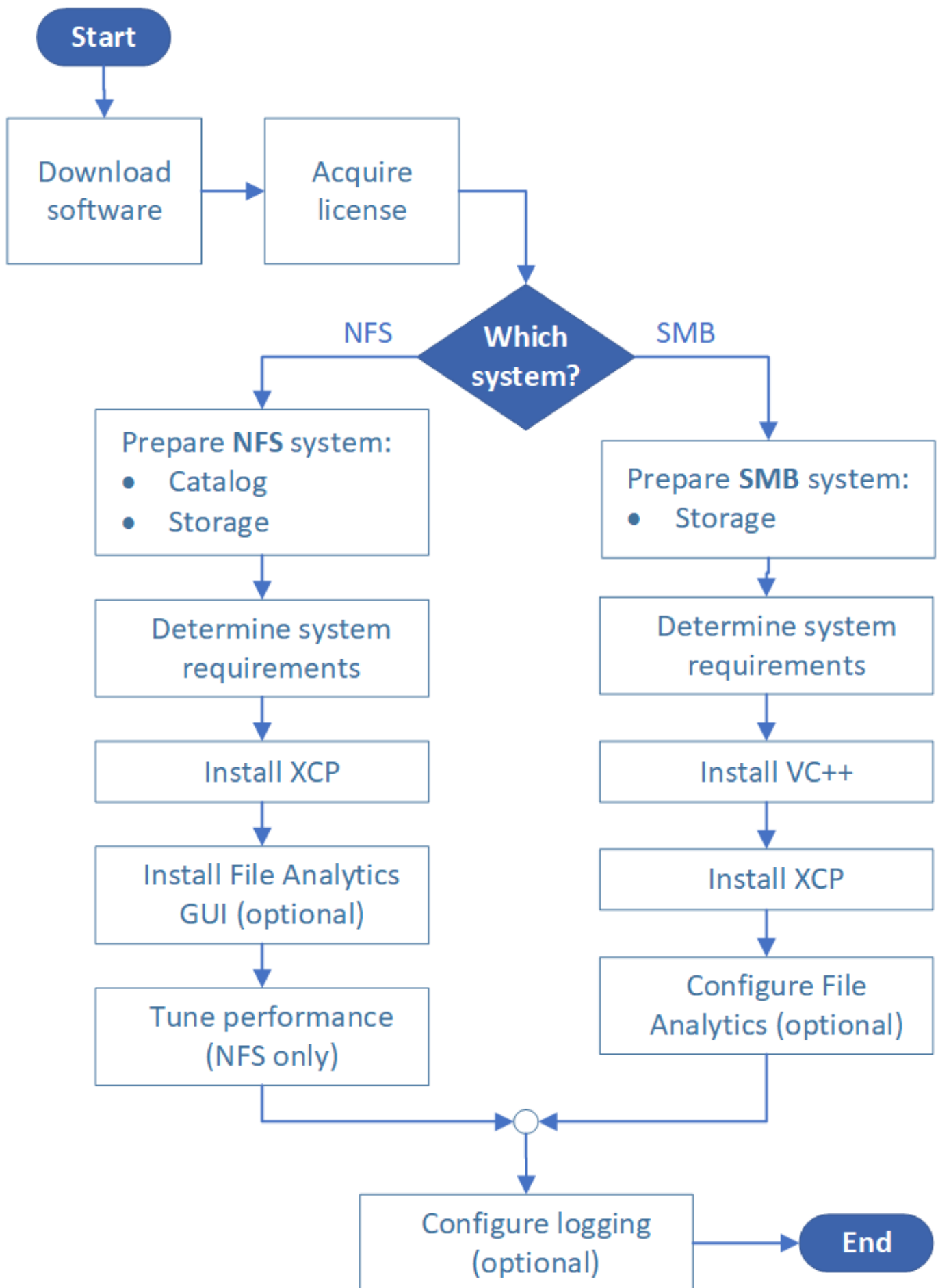
# Install XCP

## Prepare for XCP installation

In preparation for installation, you download XCP, obtain a license, and prepare your system.

## Install and configure workflow

This document provides an easy workflow for installing and setting up XCP on NFS and SMB systems.



## Download XCP

Download XCP from the NetApp support site and obtain a license from the XCP site.

You can download XCP from the [NetApp Support site](#).

## License XCP

NetApp offers a free one year XCP license. You can obtain the license file from the [XCP site](#). The licensing portal offers different licensing options. After one year, you can renew the license for another year using the same portal.

The XCP license is available as an offline or online license. If you want to send migration statistics use an online license. The online license requires an internet connection. The offline license does not require an internet connection.

To run XCP 1.9.3 and later, you must obtain a new XCP license from the [XCP site](#).



Licenses used with XCP 1.9.2 and earlier are not supported in XCP 1.9.3 and later. Similarly, licenses used with XCP 1.9.3 and later are not supported in XCP 1.9.2 and earlier.

## Prepare your system

If you are using [XCP NFS on a Linux system](#), you must prepare catalog and storage.

If you are using [XCP SMB on a Microsoft Windows system](#), you must prepare storage.

## Prepare Linux for XCP NFS

XCP NFS uses Linux client host systems to generate parallel I/O streams and fully use available network and storage performance.

You can configure your setup for a root and a non-root user and then, depending on your setup, you can select either user.

## Configure catalog

XCP saves operation reports and metadata in an NFSv3-accessible catalog directory or on any POSIX path with the required permissions.

- Provisioning the catalog is a one-time pre-installation activity.
- Approximately 1 GB of space is indexed for every 10 million objects (directories plus files and hard links); each copy that can be resumed or synched and each offline-searchable scan requires an index.
- To support performance, at least ten disks or SSDs are required in the aggregate containing the export directory.



You must store XCP catalogs separately. They must not be located on either the source or the destination NFS export directory. XCP maintains the metadata, which are the reports in the catalog location specified during the initial setup. Before you run any operation using XCP, you must specify and update the location for storing the reports.

## Configure storage

XCP NFS transitions and migrations have the following source and target storage requirements:

- Source and target servers must have the NFSv3 or NFS v4.0 protocol service enabled
  - For NFSv4 ACL migration, you must enable NFSv4 protocol service and NFSv4 ACL on the destination server
- Source and target volumes must be exported with `root` access to the XCP Linux client host
- For NFSv4 ACL migration, NFSv4 requires that you use the encoding language UTF-8 for volumes that require ACL migration.



- To prevent administrators accidentally modifying the source volume, you should configure the source volume for the NFSv3 and NFSv4 export directories as read-only.
- In ONTAP, you can use the diagnostic `-atime-update` option to preserve atime on source objects. This feature is only available in ONTAP and is helpful if you want to preserve atime in source objects while running XCP.
- In XCP, you can use the `-preserve-atime` option to preserve atime on source objects. This option is available to use with all commands that access source objects.

## Root user

A root user on a Linux machine has the permissions to mount the source, destination, and catalog volumes.

## Non-root user

A non-root user is required to have the following permissions on a mounted volume:

- Read permission access to the source volume
- Read/write permission access to the mounted destination volume
- Read/write permission access to the catalog volume

## Prepare Windows for XCP SMB

XCP SMB uses Windows client host systems to generate parallel I/O streams and fully use available network and storage performance.

## Configure storage

XCP SMB transitions and migrations have the following user login requirements:

- XCP host system: An XCP host user must have administrator privilege (the user must be part of the "BUILTIN\Administrators" group on the target SMB server).
- Add the migration or XCP host user to the audit and security log policy for Active Directory. To locate the 'Manage Auditing and Security Log' Policy on Windows 10, follow these steps:

### Steps

1. Open the **Group Policy Editor** dialog box.
2. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User**

### Rights Assignment.

3. Select **Mange auditing and security log**.
4. To add an XCP host user, select **Add User or Group**.

For more information, see: [Manage auditing and security log](#).

- Target storage system: XCP host user must have read and write access.
- Source storage system:
  - If the user is part of the “Backup Operators” group in the source storage system, the members of this group can read files while bypassing the security rules, regardless of any permissions that protect those files.
  - If the user is not part of “Backup Operators” group in source system, the user must have read access.



Write permission is required in the source storage system for supporting the XCP option – `preserve-atime`.

## Configure a Windows client

- Add the destination storage box and the source storage box to the host file:
  1. Navigate to the following location: (C:\Windows\System32\drivers\etc\hosts)
  2. Insert the following host entries to the file in the following format:

```
<Source data vservers data interface ip> <Source cifs server name>  
<Destination data vservers data interface ip> <Destination cifs server name>
```

### Example

```

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       XXX.XX.XX.XX      rhino.acme.com      # source server
#       XX.XX.XX          x.acme.com          # x client host


# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
xx.xxx.xxx.xxx          00906A52DFE247F
xx.xxx.xxx.xxx          42D1BBE1219CE63

```

## Prepare File Analytics

Prepare for your data migration using File Analytics.

File Analytics has the following two parts:

- File Analytics server running on Linux
- XCP SMB service running on Windows

File Analytics installation has the following requirements:

- Supported OS and system requirements are the same as given for NFS and SMB installation. Because the database will reside on a Linux box, you must make sure you have a minimum of 10 GB free space.
- The Linux machine where you install the File Analytics server must be connected to the internet or the yum repository. The installation script talks to the yum repository to download the required packages, such as PostgreSQL, HTTP and SSL.
- The File Analytics GUI can only be hosted on a Linux machine along with XCP services for Linux running on same box.
- For running SMB services, complete the following steps:
  - Verify that your Windows box can ping the Linux machine where the File Analytics server is running.
  - If you are inside a firewall, verify that ports 5030 and 5432 are open. Port 5030 is used to make the REST call to Windows. Port 5432 port is used for the PostgreSQL connection.





The XCP File Analytics server always runs on a Linux machine. There is no separate installation available for SMB File Analytics. If you are a Windows user and want to run File Analytics for SMB share, then you must install File Analytics for Linux and connect the Windows box to a Linux database.

If you only use XCP File Analytics, you do not need to configure the XCP Catalog for NFS.

## Install XCP NFS

If you want to upgrade XCP, delete the current installation and replace it with a new installation of the latest version.

This section details the system requirements and the procedures for the initial setup of XCP on a Linux client and the INI file configuration.

### System Requirements

Item	Requirement
System	64-bit Intel or AMD server, minimum 8 cores and 64 GB RAM
Operating System & Software	See the <a href="#">IMT</a> for supported operating systems
Special Requirements	Network connectivity and root level access to source and destination NFSv3 exports  No other active applications
Storage	20 MB of disk space for the XCP binary and at least 50 MB of disk space for the logs that are stored in the /opt/NetApp/xFiles/xcp/ directory
Supported Protocol Version	NFSv3 and NFSv4 (POSIX and ACL)
Supported browser (File Analytics only)	Refer to the <a href="#">IMT</a> matrix for all supported browser versions for XCP File Analytics.



The recommended configuration for live source migration is 8 cores and 64 GB RAM.

### Install XCP NFS for a root user

You can use the following procedure to install XCP for a root user.

#### Steps

1. Log in to the Linux machine as the root user and download and install the license:

```
[root@scspr1980872003 ~]# ls -l
total 36188
-rw-r--r--  1 root root 37043983 Oct  5 09:36 NETAPP_XCP_<version>.tgz
-rw-----  1 root root      1994 Sep  4 2019 license
```

2. To extract the tool, untar XCP:

```
[root@scspr1980872003 ~]# tar -xvf NETAPP_XCP_<version>.tgz
[root@scspr1980872003 ~]# ls
NETAPP_XCP_<version>.tgz license xcp
[root@scspr1980872003 ~]# cd xcp/linux/
[root@scspr1980872003 linux]# ls
xcp
```

3. Verify that the `/opt/NetApp/xFiles/xcp` path is available on the system from a previous version of XCP.

If `/opt/NetApp/xFiles/xcp` is available, activate the license by using the `xcp activate` command and proceed with data migration.

If `/opt/NetApp/xFiles/xcp` is not available, when you run the `xcp activate` command is run for the first time, the system creates the XCP host configuration directory in `/opt/NetApp/xFiles/xcp`.

The `xcp activate` command fails because the license is not installed:

```
[root@scspr1980872003 linux]# ./xcp activate
(c) yyyy NetApp, Inc.
xcp: Host config file not found. Creating sample at
'/opt/NetApp/xFiles/xcp/xcp.ini'

xcp: ERROR: License file /opt/NetApp/xFiles/xcp/license not found.
Register for a license at https://xcp.netapp.com
```

4. Copy the license to `/opt/NetApp/xFiles/xcp/`:

```
[root@scspr1980872003 linux]# cp ~/license /opt/NetApp/xFiles/xcp/
```

5. Verify that the license file was copied to `/opt/NetApp/xFiles/xcp/`:

```
[root@scspr1980872003 ~]# ls -altr /opt/NetApp/xFiles/xcp/
total 44
drwxr-xr-x 3 root root    17 Oct  1 06:07 ..
-rw-r--r-- 1 root root   304 Oct  1 06:07 license
drwxr-xr-x 2 root root     6 Oct  1 10:16 xcpfalog
drwxr-xr-x 2 root root    21 Oct  1 10:16 xcplogs
-rw-r--r-- 1 root root   110 Oct  5 00:48 xcp.ini
drwxr-xr-x 4 root root    83 Oct  5 00:48 .
[root@scspr1978802001 ~]#
```

6. Activate XCP:

```
[root@scspr1980872003 linux]# ./xcp activate
XCP <version>; (c) yyyy NetApp, Inc.;
XCP activated
```

## Install XCP for a non-root user

You can use the following procedure to install XCP for a non-root user.

### Steps

1. Log in to the Linux machine as the non-root user and download and install the license:

```
[user1@scspr2474004001 ~]$ ls -l
total 36640
-rwxr-xr-x 1 user1 user1      352 Sep 20 01:56 license
-rw-r--r-- 1 user1 user1 37512339 Sep 20 01:56
NETAPP_XCP_Nightly_dev.tgz
[user1@scspr2474004001 ~]$
```

2. To extract the tool, untar XCP:

```
[user1@scspr2474004001 ~]$ tar -xvf NETAPP_XCP_Nightly_dev.tar
[user1@scspr2474004001 ~]$ cd xcp/linux/
[user1@scspr2474004001 linux]$ ls
xcp
[user1@scspr2474004001 linux]$
```

3. Verify that the `/home/user1/NetApp/xFiles/xcp` path is available on the system from a previous version of XCP.

If the `/home/user1/NetApp/xFiles/xcp` path is available, activate the license by using the `xcp activate` command and proceeding with data migration.

If `/home/user1/NetApp/xFiles/xcp` is not available, when you run the `xcp activate` command for the first time, the system creates the XCP host configuration directory in `/home/user1/NetApp/xFiles/xcp`.

The `xcp activate` command fails because the license is not installed:

```
[user1@scspr2474004001 linux]$ /home/user1/xcp/linux/xcp activate
(c) yyyy NetApp, Inc.
xcp: Host config file not found. Creating sample at
'/home/user1/NetApp/xFiles/xcp/xcp.ini'

xcp: ERROR: License file /home/user1/NetApp/xFiles/xcp/license not
found.
Register for a license at https://xcp.netapp.com
[user1@scspr2474004001 linux]$
```

4. Copy the license to /home/user1/NetApp/xFiles/xcp/:

```
[user1@scspr2474004001 linux]$ cp ~/license
/home/user1/NetApp/xFiles/xcp/
[user1@scspr2474004001 linux]$
```

5. Verify that the license file was copied to /home/user1/NetApp/xFiles/xcp/:

```
[user1@scspr2474004001 xcp]$ ls -ltr
total 8
drwxrwxr-x 2 user1 user1 21 Sep 20 02:04 xcplogs
-rw-rw-r-- 1 user1 user1 71 Sep 20 02:04 xcp.ini
-rwxr-xr-x 1 user1 user1 352 Sep 20 02:10 license
[user1@scspr2474004001 xcp]$
```

6. Activate XCP:

```
[user1@scspr2474004001 linux]$ ./xcp activate
(c) yyyy NetApp, Inc.

XCP activated

[user1@scspr2474004001 linux]$
```

## Install XCP SMB

This section details the system requirements and the procedure for VC++ redistributable installation and the initial setup of XCP on a Windows client.



There is no option to upgrade; reinstall XCP to replace any existing version.

## System Requirements

Item	Requirement
System	64-bit Intel or AMD server, minimum 4 cores and 32 GB RAM
Operating System & Software	Windows 2012 R2 or above. For supported Microsoft OS versions, see the <a href="#">Interoperability Matrix Tool</a> .  Visual C++ 2017 redistributable must be installed on the XCP host.
Special Requirements	The source storage system, XCP host, and the target ONTAP system must be part of same Active Directory domain
Storage	20 MB of disk space for the XCP binary and at least 50 MB of disk space for the logs that are stored in the C:\NetApp\XCP directory
Supported Protocol Version	All SMB protocol versions
Supported browser (File Analytics only)	Refer to the <a href="#">IMT</a> matrix for all supported browser versions for XCP File Analytics.

## XCP SMB Microsoft VC++ Redistributable installation

Follow these steps for the VC++ redistributable installation.

### Steps

1. Click [VC++ 2017 redistributable](#) to download the executable to your default downloads folder.
2. To start the installation, double click the installer. Accept the terms and conditions and select **Install**.
3. When the installation is complete, restart the Windows client.

## XCP SMB Initial Setup Procedure

Follow these steps to perform the initial setup of XCP SMB.

### Steps

1. Download the license and the XCP SMB binary `NETAPP_XCP_<version>.tgz` on a Windows client.
2. Extract the `NETAPP_XCP_<version>.tgz` file.
3. Copy the `xcp.exe` file to your Windows C: drive, this binary is available inside `NETAPP_XCP_<version>\xcp\windows` after you extract the `tgz` file.
4. Verify that the `C:\NetApp\XCP` path is available on the system from a previous version of XCP.  
If `C:\NetApp\XCP` is available, activate XCP by using the `xcp.exe activate` command and proceed with data migration.

If `C:\NetApp\XCP` is not available, the system creates the XCP host configuration directory and files it at `C:\NetApp\XCP` when you run the `xcp.exe activate` command for the first time. The `xcp.exe activate` command fails and creates an error message asking for a new license.

```
C:\>xcp.exe activate
(c) yyyy NetApp, Inc.

License file C:\NetApp\XCP\license not found.
Register for a license at https://xcp.netapp.com
```

5. Copy the license to the newly created folder C:\NetApp\XCP:

```
C:\>copy license c:\NetApp\XCP
1 file(s) copied.
```

6. Activate XCP:

```
C:\>xcp.exe activate
XCP SMB; (c) yyyy NetApp, Inc.;

XCP activated

C:\>
```

## Install File Analytics for NFS

Install or upgrade File Analytics for NFS.

### About this task

For system requirements for NFS, see [Install XCP NFS](#).

The `configure.sh` script installs XCP File Analytics on a Red Hat Enterprise Linux (RHEL) host machine. As part of the installation, the script installs Postgres Database, Apache HTTPD server, and other required packages on the host Linux machine. For information on specific supported RHEL versions, refer to the [IMT](#). You can change or update to a more recent version as needed and to adhere to security guidelines. To learn more about the `configure.sh` script, run `./configure.sh -h` on the command line.

### Before you begin

- If any XCP operations are running, NetApp recommends that you complete the operations before you start the configuration.
- Your Linux machine must be connected to the Yum repository server or the internet.
- If a firewall is configured on the Linux machine, you must change the firewall settings to enable port 5030, which is used by the XCP service.

### Steps

1. Install or upgrade File Analytics for NFS.

### Install File Analytics

- a. Navigate to the `xcp` folder and run the `./configure.sh` script.

If installation is successful, the following message is displayed:

```
You can now access XCP file analytics using
(<username>:<password>)
https://<ip_address>/xcp
```



You can use this username and password to log in to the File Analytics GUI.

### Upgrade File Analytics

- a. Navigate to the `xcp` folder and run `./configure.sh -f`.
- b. At the prompt, enter `y` to clean up and reconfigure the system.

After the script is approved, it cleans up the existing configuration and reconfigures the system.

If successful, the following message is displayed:

```
You can now access XCP file analytics using
(<username>:<password>)
https://<ip_address>/xcp
```

2. Launch File Analytics in a supported browser: **`https://<ip address of linux>/xcp`**.

Refer to [Install XCP NFS](#) for information on supported browsers.

## Install File Analytics for SMB

Install or upgrade File Analytics for SMB.

### About this task

For system requirements for SMB, see [Install XCP SMB](#).

### Before you begin

- You must configure XCP File Analytics for NFS on a Linux machine to use the XCP SMB service.
- Make sure the XCP service is running on your Linux machine, before you begin configuring XCP File Analytics on a Windows machine.

### Fresh install of File Analytics for SMB

To perform a fresh install of File Analytics for SMB, complete the following steps.

## Steps

1. Copy the `xcp.exe` file to your Windows C: drive, this binary is available inside `/xcp/windows` after you untar the `tgz` file.
2. Download the XCP license file from the [XCP site](#).
3. Create the folder `C:\NetApp\XCP` and copy the XCP license to this location.
4. Activate the XCP license using the following command at the command prompt: `xcp.exe activate`
5. In the Windows CLI command prompt, run `xcp configure`.
6. When prompted, provide the IP address of the Linux machine where the XCP File Analytics server is configured.
7. Copy the `server.key` and `server.crt` files from `/opt/NetApp/xFiles/xcp/` (in the Linux box where XCP File Analytics is already configured) to `C:\NetApp\XCP`.

Optionally, if you have a CA certificate, place the certificate in `C:\NetApp\XCP` with the same name and extensions.

8. Go to your Windows machine and run `xcp listen`, now XCP File Analytics for SMB is configured. Keep the window open to continuously run the service.
9. Launch File Analytics on a supported browser: `https://<ip address of linux>/xcp`

Refer to [Install XCP SMB](#) for information on supported browsers.

10. Select **OK** when the dialog box displays.



A new tab opens. Enable pop-ups on the browser if they are blocked.

11. Accept the privacy policy for the URL. The following message displays: `SMB agent is ready to use. Please refresh the analytics page`
12. Display the SMB agent under the Agents card by returning to the original tab hosting the XCP File Analytics GUI and refreshing the page.

## Upgrade of File Analytics for SMB

To upgrade the existing File Analytics for SMB, complete the following steps.

1. Before you run File Analytics, verify that the Linux server that File Analytics is running on is also upgraded and that the service is running.
2. In Windows, stop the existing XCP service by entering `CTRL-C` on the command line.
3. Replace `xcp.exe` with the latest binary.
4. Go to your Windows machine and run `xcp listen` to configure XCP File Analytics for SMB. Keep the window open to continuously run the service.
5. Launch File Analytics on a supported browser: `https://<ip address of linux>/xcp`

Refer to [Install XCP SMB](#) for information on supported browsers.

6. Select **OK** when the dialog box displays.





A new tab opens. Enable pop-ups on the browser if they are blocked.

7. Accept the privacy policy for the URL. The following message displays: SMB agent is ready to use. Please refresh the analytics page
8. Display the SMB agent under the Agents card by returning to the original tab hosting the XCP File Analytics GUI and refreshing the page.

# Configure XCP

## Configure the INI file

Steps to configure the INI file for XCP.

### Configure the INI file for a root user

You can use the following procedure to configure the INI file for an XCP NFS root user.

#### Steps

1. Add the catalog location for the XCP server in the host configuration file by using the `vi` editor:



Catalog location should be exported before modifying the details in the `xcp.ini` XCP configuration file. Catalog location (NFSv3) should be mountable by the XCP Linux host but not necessarily be mounted.

```
[root@localhost ~]# vi /opt/NetApp/xFiles/xcp/xcp.ini
```

2. Verify that the XCP Linux client host configuration file entries for the catalog were modified:

```
[root@localhost ~]# cat /opt/NetApp/xFiles/xcp/xcp.ini
# Sample xcp config
[xcp]
catalog = 10.61.82.210:/vol/xcpvol/
```

### Configure the INI file for a non-root user

As a non-root user, you do not have permission to mount the NFS file system. A root user is required to first mount the catalog volume and then, as a non-root user running XCP, if you have read/write permission to the catalog volume, you can access the mounted catalog volume by using a POSIX connector. After the volume is mounted, you can add catalog the path:

(t/10.237.170.53\_catalog\_vol - This is the path where catalog volume is mounted) as follows.

```
[user1@scspr2474004001 xcp]$ ls -ltr
total 8
drwxrwxr-x 2 user1 user1  21 Sep 20 02:04 xcplogs
-rw-rw-r-- 1 user1 user1  71 Sep 20 02:04 xcp.ini
-rwxr-xr-x 1 user1 user1 352 Sep 20 02:10 license
[user1@scspr2474004001 xcp]$ cat /home/user1/NetApp/xFiles/xcp/xcp.ini

Sample xcp config [xcp]
catalog = file:///t/10.237.170.53_catalog_vol
```

## Performance tuning

For XCP NFS, after planning the migration by using the `show` and `scan` commands, you can migrate data.



When you are performing data migration as a non-root user, a root user can perform the following step.

For the optimal performance and reliability, NetApp recommends setting the following Linux kernel TCP performance parameters in `/etc/sysctl.conf` on the XCP Linux client host. Run `sysctl -p` or the `reboot` command to commit the changes:

```
net.core.rmem_default = 1342177
net.core.rmem_max = 16777216
net.core.rmem_max = 16777216
net.core.wmem_default = 1342177
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 1342177 16777216
net.ipv4.tcp_wmem = 4096 1342177 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_fin_timeout = 10
```



For a non-root user, the setting must be performed by a root user.

## Environment variable

Optional environment variable configuration for XCP NFS systems.



A non-root user can also use the following variables.

The environment variable `XCP_CONFIG_DIR` overrides the default location, `/opt/NetApp/xFiles/xcp`. If set, the value should be an OS filesystem path, possibly to a mounted NFS directory. When the `XCP_CONFIG_DIR` variable is set, a new directory with the same name as the host name is created inside the custom configuration directory path, new logs are stored at this location.

```
[root@localhost /]# export XCP_CONFIG_DIR='/tmp/xcp_config_dir_path'
```

The environment variable `XCP_LOG_DIR` overrides the default location that stores the XCP log in the configuration directory. If set, the value should be an OS filesystem path, possibly to a mounted NFS directory. When the `XCP_LOG_DIR` variable is set, a new directory with the same name as the host name is created inside the custom log directory path, new logs are stored at this location.

```
[root@localhost /]# export XCP_LOG_DIR='/tmp/xcp_log_dir_path'
```

The environment variable `XCP_CATALOG_PATH` overrides the setting in `xcp.ini`. If set, the value should be in the xcp path format, `server:export[:subdirectory]`.

```
[root@localhost /]# export XCP_CATALOG_PATH='10.61.82.210:/vol/xcpvol/'
```



For a non-root user, you must replace `XCP_CATALOG_PATH` from the exported path with the POSIX path.

## Configure the POSIX connector

XCP NFS now supports the use of POSIX connectors to provide source and destination paths for data migration.

### Supported features

The following features are supported for POSIX connectors:

- For POSIX file systems that support nanosecond `atime`, `mtime`, and `ctime`, the `scan` command gets the full values (seconds and nanoseconds) and the `copy` command sets them
- POSIX connectors are more secure than XCP with NFSv3 TCP sockets.

### Path Syntax

The path syntax for a POSIX connector is `file://<mounted path on linux>`.

### Set up a POSIX connector

To set up a POSIX connector, you must perform the following tasks:

- Mount a source and a destination volume
- Verify that the destination path has the necessary permission to write the data

A destination and a catalog are mounted in the following example:

```
root@scspr2395903001 ~]# findmnt -t nfs4
TARGET SOURCE FSTYPE OPTIONS
/t/10.237.170.39_src_vol 10.237.170.39:/source_vol nfs4
rw,relatime,vers=4.0,rsize=65536,wsiz=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
/t/10.237.170.53_dest_vol 10.237.170.53:/dest_vol nfs4
rw,relatime,vers=4.0,rsize=65536,wsiz=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
/t/10.237.170.53_catalog_vol 10.237.170.53:/xcp_catalog nfs4
rw,relatime,vers=4.0,rsize=65536,wsiz=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
[root@scspr2395903001 ~]#
```

POSIX connectors access a source and destination volume by using the POSIX syntax `file://`. In the above example, the source path is `file:///t/10.237.170.39_src_vol` and the destination path is `file:///t/10.237.170.53_dest_vol`.

You can manage the sample configuration of an XCP catalog shared by non-root users by creating a Linux group for XCP users. For non-root users, the following permissions are required for Linux group users to perform migrations.

In the following sample output, `demo` is the non-root user and `/mnt/xcp-catalog` is the path where catalog volume is mounted:

```
sudo groupadd -g 7711 xcp_users
sudo usermod -G xcp_users -a demo
sudo chown -R :xcp_users /mnt/xcp-catalog
sudo chmod -R g+w /mnt/xcp-catalog
```

The XCP catalog does not store data but it does store scan and copy file names, directory names, and other metadata. Therefore, it is recommended that you configure the catalog file system permissions for allowed users to give them the capability to secure the stored metadata.

## Ownership (UID and GID)

When you are set up as a regular user, by default, a `copy` command to a POSIX or NFS3 destination does not attempt to set the ownership (user ID (UID) and group ID (GID)). Setting the ownership is typically performed by an administrator. When user A copies files from user B, user A expects to own the destination. However, this is not the case when a root user copies the files. When a root user copies the files, the `-chown` option changes the behavior so that a non-root `copy` command with `-chown` attempts to set the UID and GID.

## Increase the maximum number of open file descriptors

For optimal performance and reliability, you can increase the maximum number of open file descriptors for the XCP user on all nodes.

## Steps

1. Open the file by using the following command:  
`vi /etc/security/limits.conf`
2. Add the following line to the file:  
`<username> - nofile 999999`

## Example

```
root - nofile 999999
```

See [Red Hat solutions](#) for more information.

# Configure the HDFS connector

For XCP NFS, the Hadoop Distributed File System (HDFS) connector (`hdfs://`) gives XCP the capability to access any HDFS file system that is available with different vendors.

## Supported features

The `copy` command operation from HDFS to NFS is supported for HDFS connectors.

## Path Syntax

The path syntax for a HDFS connector is `hdfs://[user@host:port]/full-path`.



If you do not specify a user, host, and port, XCP calls `hdfsConnect` with the host set to `default` and the port set to 0.

## Set up a HDFS connector

To run the HDFS `copy` command, you must set the HDFS client on the Linux system, and based on the Hadoop vendor, follow the setup configuration available on the internet. For example, you can set the client for a MapR cluster by using <https://docs.datafabric.hpe.com/60/AdvancedInstallation/SettingUptheClient-redhat.html>.

After you complete the HDFS client setup, you must complete the configuration on the client. To use the HDFS paths with XCP commands, you must have the following environment variables:

- `NHDFS_LIBHDFS_PATH`
- `NHDFS_LIBJVM_PATH`

In the following examples, the settings work with MapR and `java-1.8.0-openjdk-devel` on CentOS:

```
export JAVA_HOME=$(dirname $(dirname $(readlink $(readlink $(which javac))))
export NHDFS_LIBJVM_PATH=`find $JAVA_HOME -name "libjvm.so"` export
NHDFS_LIBHDFS_PATH=/opt/mapr/lib/libMapRClient.so
```

```
[demo@mapr0 ~]$ hadoop fs -ls Found 3 items
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d1
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d2
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d3
```

## Configure multinode scale-out

For XCP NFS, you can overcome the performance limits of a single node by using a single `copy` (or `scan -md5`) command to run workers on multiple Linux systems or cluster nodes.

### Supported features

Multinode scale-out is helpful in any environment where the performance of a single system is not sufficient, for example, in the following scenarios:

- When it takes months for a single node to copy petabytes of data
- When high latency connections to cloud object stores slows down an individual node
- In large HDFS cluster farms where you run a very large number of I/O operations

### Path syntax

The path syntax for multinode scale-out is `--nodes worker1,worker2,worker3`.

### Set up multinode scale-out

Consider a setup with four Linux hosts with similar CPU and RAM configurations. You can use all four hosts for migration because XCP can coordinate the copy operations across all the host nodes. To make use of these nodes in a scale-out environment, you must identify one of the four nodes as the master node and other nodes as worker nodes. For example, for a Linux four-node setup, name the nodes as "master", "worker1", "worker2", and "worker3" and then set up the configuration on the master node:

1. Copy XCP in the home directory.
2. Install and activate the XCP license.
3. Modify the `xcp.ini` file and add the catalog path.
4. Set passwordless Secure Shell (SSH) from the master node to the worker nodes:
  - a. Generate the key on the master node:

```
ssh-keygen -b 2048 -t rsa -f /root/.ssh/id_rsa -q -N ''
```

- b. Copy the key to all the worker nodes:

```
ssh-copy-id -i /root/.ssh/id_rsa.pub root@worker1
```

The XCP master node uses SSH to run workers on other nodes. You must configure the worker nodes to enable passwordless SSH access for the user running XCP on the master node. For example, to enable a user demonstration on a master node to use node "worker1" as an XCP worker node, you must copy XCP binary from the master node to all the worker nodes in the home directory.

### MaxStartups

When you start up multiple XCP workers simultaneously, to avoid errors, you should increase the `sshd` `MaxStartups` parameter on each worker node as shown in the following example:

```
echo "MaxStartups 100" | sudo tee -a /etc/ssh/sshd_config
sudo systemctl restart sshd
```

### The "nodes.ini" file

When XCP runs a worker on a cluster node, the worker process inherits the environment variables from the main XCP process on the master node. To customize a particular node environment, you must set the variables in the `nodes.ini` file in the configuration directory only on the master node (worker nodes do not have a configuration directory or catalog). For example, for an ubuntu server mars that has its `libjvm.so` in a different location to the master node, such as wave (which is CentOS), it requires a configuration directory to allow a worker on mars to use the HDFS connector. This setup is shown in the following example:

```
[schay@wave ~]$ cat /opt/NetApp/xFiles/xcp/nodes.ini [mars]
NHDFS_LIBJVM_PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/
amd64/server/libjvm.so
```

If you are using a multisession with POSIX and HDFS file paths, you must mount the file system and the source and destination exported file system on the master node and all worker nodes.

When XCP runs on a worker node, the worker node has no local configuration (no license, log files, or catalog). XCP binary only is required on the system in your home directory. For example, to run the `copy` command, the master node and all worker nodes need access to the source and destination. For `xcp copy --nodes linux1,linux2 hdfs:///user/demo/test file:///mnt/ontap`, the `linux1` and `linux2` hosts must have the HDFS client software configured and the NFS export mounted on `/mnt/ontap`, and, as mentioned previously, a copy of the XCP binary in the home directory.

### Combine POSIX and HDFS connectors, multinode scale-out, and security features

You can use the POSIX and HDFS connectors, multinode scale-out, and security features in combination. For example, the following `copy` and `verify` commands combine POSIX and HDFS connectors with the security and scale-out features:

- `copy` command example:

```
./xcp copy hdfs:///user/demo/d1 file:///mnt/nfs-server0/d3
./xcp copy -match "'USER1 in name'" file:///mnt/nfs-server0/d3
hdfs:///user/demo/d1
./xcp copy -node worker1,worker2,worker3 hdfs:///user/demo/d1
file:///mnt/nfs-server0/d3
```

- `verify` command example:

```
./xcp verify hdfs:///user/demo/d2 file:///mnt/nfs-server0/d3
```



# Configure the S3 connector

Beginning with XCP 1.9.2, the Simple Storage Service (S3) connector enhances the scope of XCP data migration by enabling data migration from Hadoop Distributed File System (HDFS) file systems to S3 object storage.

## Supported migration use cases

The following migration use cases are supported for the S3 connectors:

- Migration from HDFS to NetApp StorageGRID
- Migration from HDFS to Amazon S3
- Migration from HDFS to NetApp ONTAP S3



Currently MapR is only qualified and supported for HDFS.

## Supported features

Support for the `scan`, `copy`, `verify`, `resume` and `delete` commands is available for the S3 connectors.

## Unsupported Features

Support for the `sync` command is not available for the S3 connectors.

## Path Syntax

The path syntax for the S3 connector is `s3://<bucket in S3>`.

- You can provide a specific S3 profile for the XCP commands using the `-s3.profile` option.
- You can use the `s3.endpoint` option to modify the endpoint value to communicate with S3



Endpoint usage is mandatory for StorageGRID and ONTAP S3.

# Set up an S3 connector

## Steps

1. To run the XCP command with the S3 connector, create a bucket in S3 by following the online documentation for the respective platforms:

- [ONTAP S3 object storage management](#)
- [StorageGRID: Use a tenant account overview](#)



Before continuing, you must have the `access key`, `secret key`, `certificate authority (CA) certificate bundle`, and `endpoint url` information. XCP identifies and connects to the S3 bucket using these parameters before initiating an operation.

2. Install the Amazon Web Services (AWS) CLI packages and run the AWS CLI commands to configure the keys and Secure Sockets Layer (SSL) certificates for S3 accounts:
  - See [Installing or updating the latest version of the AWS CLI](#) to install the AWS packages.
  - See the [AWS CLI Command Reference](#) for more information.
3. Use the `aws configure` command to configure your credentials file. By default, the file's location is

/root/.aws/credentials. The credentials file should specify the access key and secret access key.

4. Use the `aws configure set` command to specify a CA certificate bundle, which is a file with the `.pem` extension that is used when verifying SSL certificates. By default, the file's location is `/root/.aws/config`.

**Example:**

```
[root@client1 ~]# aws configure
AWS Access Key ID [None]: <access_key>
AWS Secret Access Key [None]: <secret_key>
Default region name [None]:
Default output format [None]:
[root@client1 ~]# cat /root/.aws/credentials
[default]
aws_access_key_id = <access_key>
aws_secret_access_key = <secret_key>
[root@client1 ~]#
[root@client1 ~]# aws configure set default.ca_bundle
/u/xxxx/s3/ca/aws_cacert.pem
[root@client1 ~]# cat /root/.aws/config
[default]
ca_bundle = /u/xxxx/s3/ca/aws_cacert.pem
```

5. After the required setup configuration is completed, confirm that the AWS CLI commands can access the S3 buckets from the Linux client before running the XCP commands:

```
aws s3 ls --endpoint-url <endpoint_url> s3://bucket-name/
```

```
aws s3 ls --profile <profile> --endpoint-url <endpoint_url> s3://bucket-name
```

**Example:**

```
[root@client1 linux]# aws s3 ls --profile <profile> --endpoint
<endpoint_url> s3://<bucket-name>
PRE 1G/
PRE aws_files/
PRE copied_folders/
PRE d1/
PRE d2/
PRE giant_size_dirs/
PRE medium_size_dirs/
PRE small_size_dirs/

[root@client1 l
```

# Plan data migration

You can plan your migration using the CLI or the File Analytics GUI.

Use the following commands to plan your migration:

- Show
- Scan

Use File Analytics to visualize the statistics for exports and shares.

## Plan NFS data migration

Plan your NFS data migrations.

### Show

The `show` command queries the RPC services and NFS exports of one or more storage servers. The command lists the available services and exports with the used and free capacity of each export, followed by the root attributes of each export.

#### Example:

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

Run `xcp help show` for more details.

### Scan

The `scan` command recursively scans the entire source NFSv3 exported paths and prints the statistics of file structure at the end of the scan. NetApp recommends putting the source NFS export mounts in read-only mode during the scan operation.



If a file or directory name contains non-UTF-8 characters, these characters are converted to the UTF-8 format and displayed when you run the `xcp-scan` command. Depending on the translation from the source encoding to UTF-8, the characters might not display as expected.

#### Example:

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

Run `xcp help scan` for more details.

Optionally, use File Analytics to view the results graphically.

# Plan SMB data migration

Plan your SMB data migrations.

## Show

The `show` command shows all SMB shares available on the server with the permissions and space available.

Example:

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

Run `xcp help show` for more details.

## Scan

The `scan` command recursively scans the entire SMB share and lists all the files at the end of the scan.



During the scan operation, you can use the `-preserve-atime` flag with the `scan` command to preserve access time at the source .

**Example:**

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

Run `xcp help scan` for more details.

Optionally, use File Analytics to view the results graphically.

# Plan HDFS data migration

Plan your HDFS data migrations.

## Scan

The `scan` command recursively scans the entire source paths and prints the statistics for the file structure at the end of the scan.

- `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`

Run `xcp help scan` for more details.

# Plan using File Analytics

## Plan your data migration

Plan your data migration using File Analytics.



XCP is a CLI, whereas File Analytics has a GUI.

### Overview

XCP File Analytics uses the XCP scan API to collect data from NFS or SMB hosts. This data is then displayed on XCP File Analytics GUI. There are three main components involved in XCP File Analytics:

- XCP service
- File Analytics database
- File Analytics GUI to manage and view data

The deployment method for XCP File Analytics components depends on the solution required:

- Deploying XCP File Analytics solutions for NFS file systems:
  - You can deploy the File Analytics GUI, database, and XCP service in the same Linux host.
- Deploying XCP File Analytics solutions for SMB file systems:  
You must deploy the File Analytics GUI and database in a Linux host and deploy the XCP service on a Windows host.

## Access File Analytics

File Analytics provides a graphical view of scan results.

### Log in to the File Analytics GUI

The XCP File Analytics GUI provides a dashboard with graphs for visualizing File Analytics. The XCP File Analytics GUI is enabled when you configure XCP on a Linux machine.



To check the supported browsers for accessing File Analytics, see the [NetApp IMT](#).

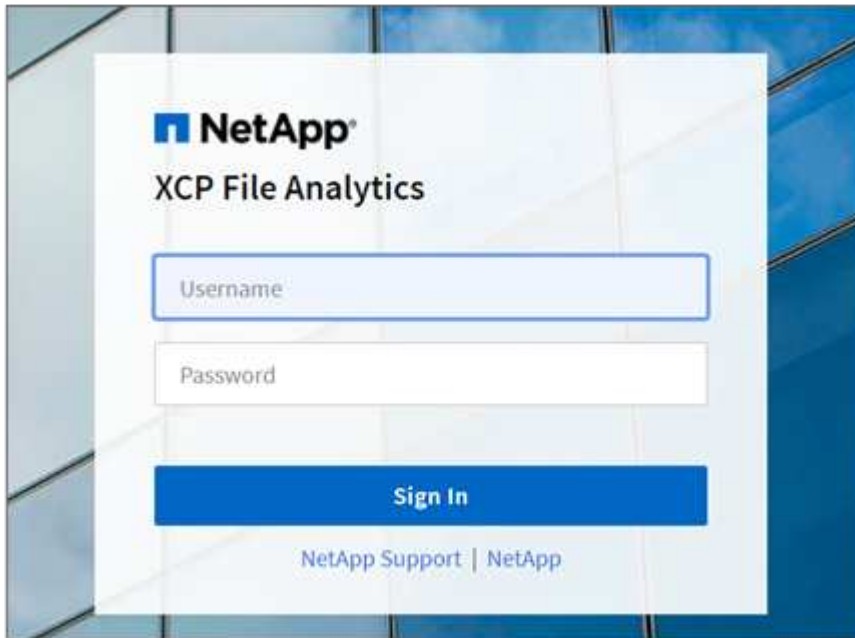
### Steps

1. Use the link `https://<IP address of linux machine>/xcp` to access the File Analytics GUI. When prompted, accept the security certificate:
  - a. Select **Advanced** below the privacy statement.
  - b. Select the **Proceed to <IP address of linux machine>** link.
2. Log in to the File Analytics GUI.

There are two ways to log in to the File Analytics GUI:

### Log in using user credentials

- a. Log in to the GUI using the user credentials obtained when you installed File Analytics.



- b. Optionally, change the password to your own password.

If you want to change the password obtained during installation to your own password, select the user icon and select **Change password**.

Your new password must be at least eight characters in length and contain at least one number, one upper case letter, one lower case letter, and one special character (! @ # \$ % ^ & \* - \_).



After changing the password, you are automatically logged out of the GUI and you must sign in again using the new password that you created.

### Configure and enable SSO capability

You can use this login capability to set up XCP File Analytics on a particular machine and share the web UI URL enterprise-wide, allowing users to log in to the UI using their single sign-on (SSO) credentials.



SSO login is optional and can be configured and enabled permanently. To set up Security Assertion Markup Language (SAML) based SSO login, see [Configure SSO credentials](#).

3. After logging in, you can see the NFS agent; a green tick is present showing minimal system configuration of the Linux system and XCP version.
4. If you have configured an SMB agent, you can see the SMB agent added in the same agent card.

### Configure SSO credentials

The SSO login functionality is implemented in XCP File Analytics using SAML and is supported with the Active

Directory Federation Services (ADFS) identity provider. SAML offloads the authentication task to the third-party identity provider (IdP) for your enterprise which can utilize any number of approaches for MFA (multifactor authentication).

## Steps

1. Register the XCP File Analytics application with your enterprise identity provider.

File Analytics now runs as a service provider and therefore must be registered with your enterprise identity provider. Generally, there is a team in the enterprise that handles this SSO integration process. The first step is to find and reach out to the relevant team and share the File Analytics application metadata details with them.

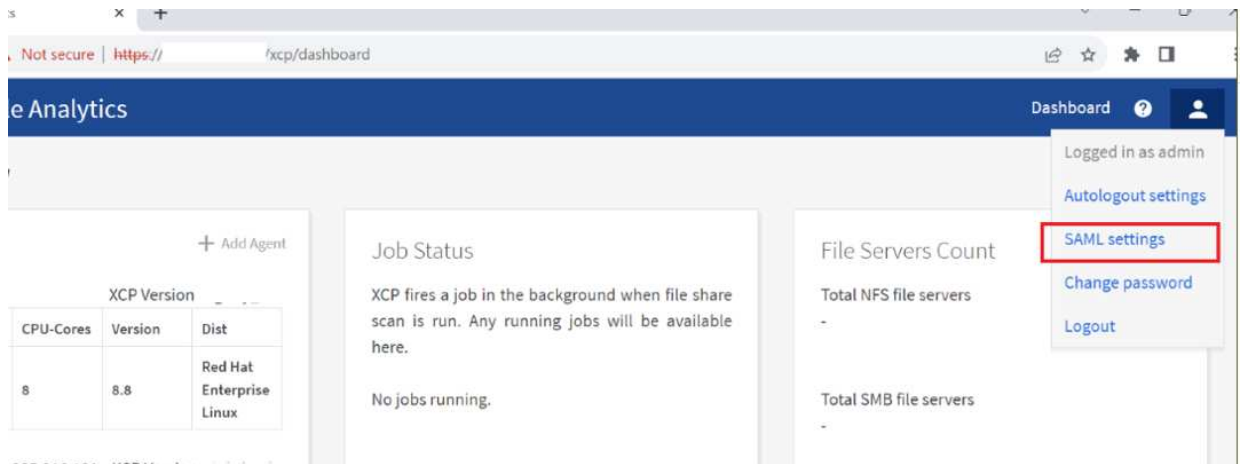
The following are the mandatory details that you must share to register with your identity provider:

- **Service provider entity ID:** `https://<IP address of linux machine>/xcp`
- **Service provider Assertion Consumer Service (ACS) URL:** `https://<IP address of linux machine>:5030/api/xcp/SAML/sp`

You can also verify these details by logging in to the File Analytics UI:

- a. Log in to the GUI using the steps described in [Log in to the File Analytics GUI](#).
- b. Select the **User** icon on the top right corner of the page, then select **SAML settings**.

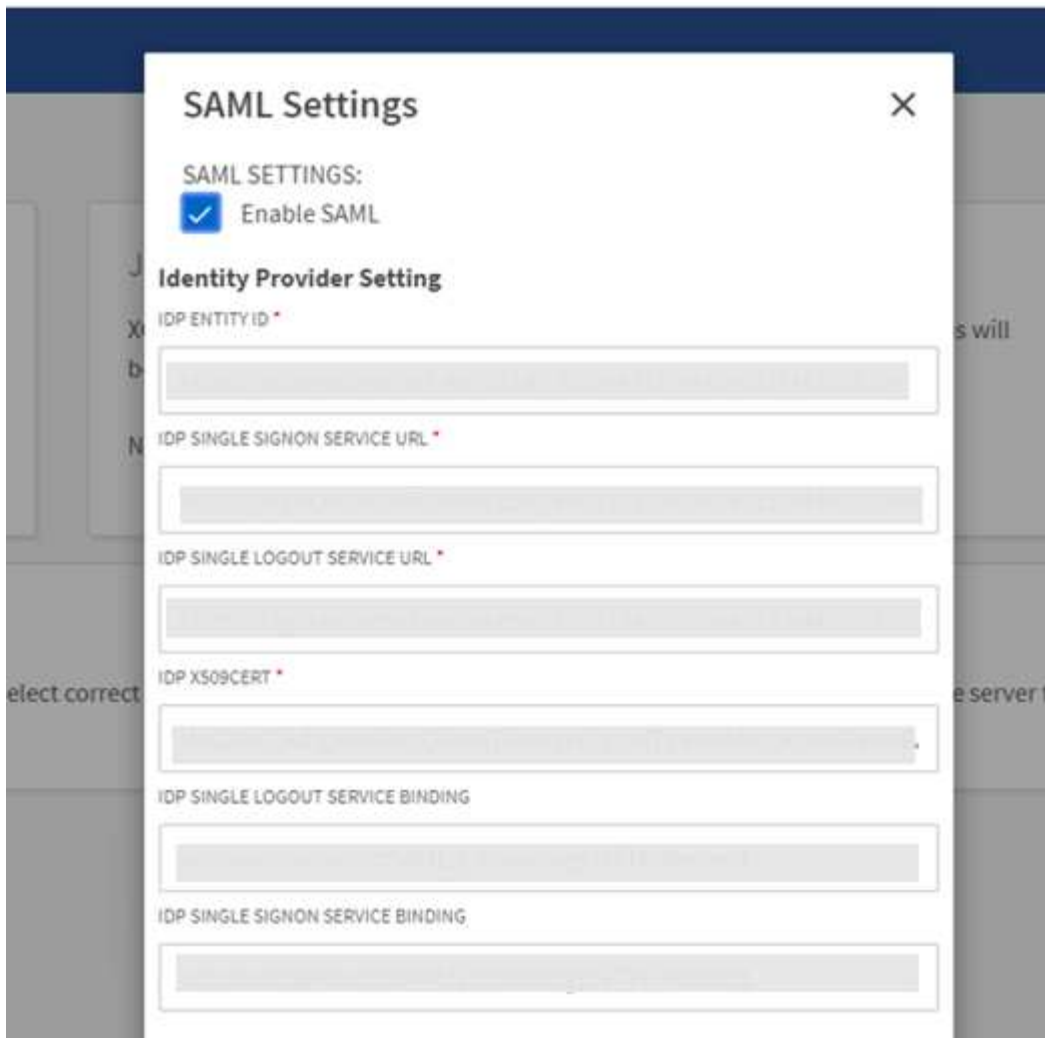
Check **Service provider settings** in the drop down menu that appears.



After registration, you receive the IdP endpoint details for your enterprise. You are required to provide this IdP endpoint metadata to the File Analytics UI.

2. Provide the IdP details:
  - a. Go to **Dashboard**. Select the **User** icon at the top right corner of the page and select **SAML settings**.
  - b. Input the IdP details that you obtained after registration.

## Example



- c. Select the **Enable SAML** checkbox to permanently enable SAML-based SSO.
- d. Select **Save**.
- e. Log out of File Analytics and log back in again.

You are redirected to your enterprise SSO page.

## Add file servers

You can configure NFS and SMB exported file systems in the XCP File Analytics GUI.

This enables XCP File Analytics to scan and analyze data on the file system. Use the following steps to add NFS or SMB file servers.

### Step

1. To add file servers, select **Add File Server**.



Add the file server IP address, select the NFS or SMB option and click **Add**.



If an SMB agent is not visible in the GUI, you will not be able to add SMB server.

After adding the file server, XCP displays:

- Total file shares available
- File shares with analytics data  
(The initial count is “0”, this updates when you run a successful scan)
- Total space utilization – the sum of space utilized by all the exports
- The data for file shares and space utilization is real-time data direct from the NFS/SMB server. Collecting and processing the data takes several seconds.



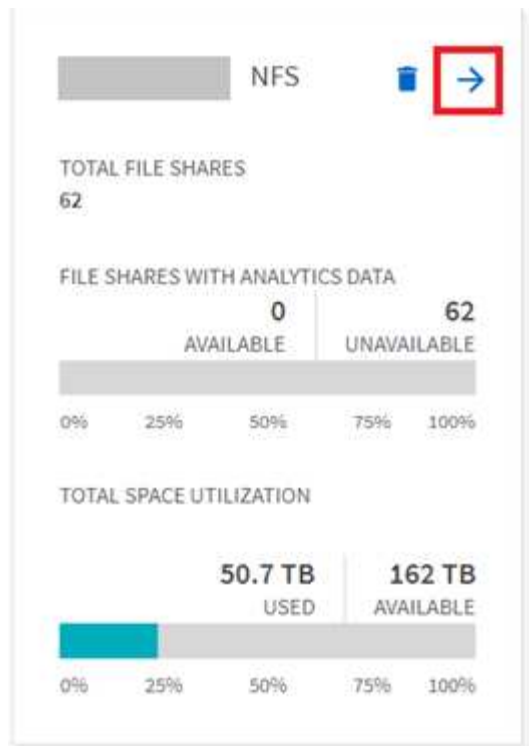
Space available versus space used in File Analytics is calculated from each exported file system available over NFS. For example, if the volumes consist of qtrees and the exports are created over a qtree, the overall space is the cumulative space of the volume size and the qtree size.

## Run a scan

When the NFS/SMB files system is added to the XCP File Analytics GUI, you can start a file system scan to analyze and represent the data.

### Steps

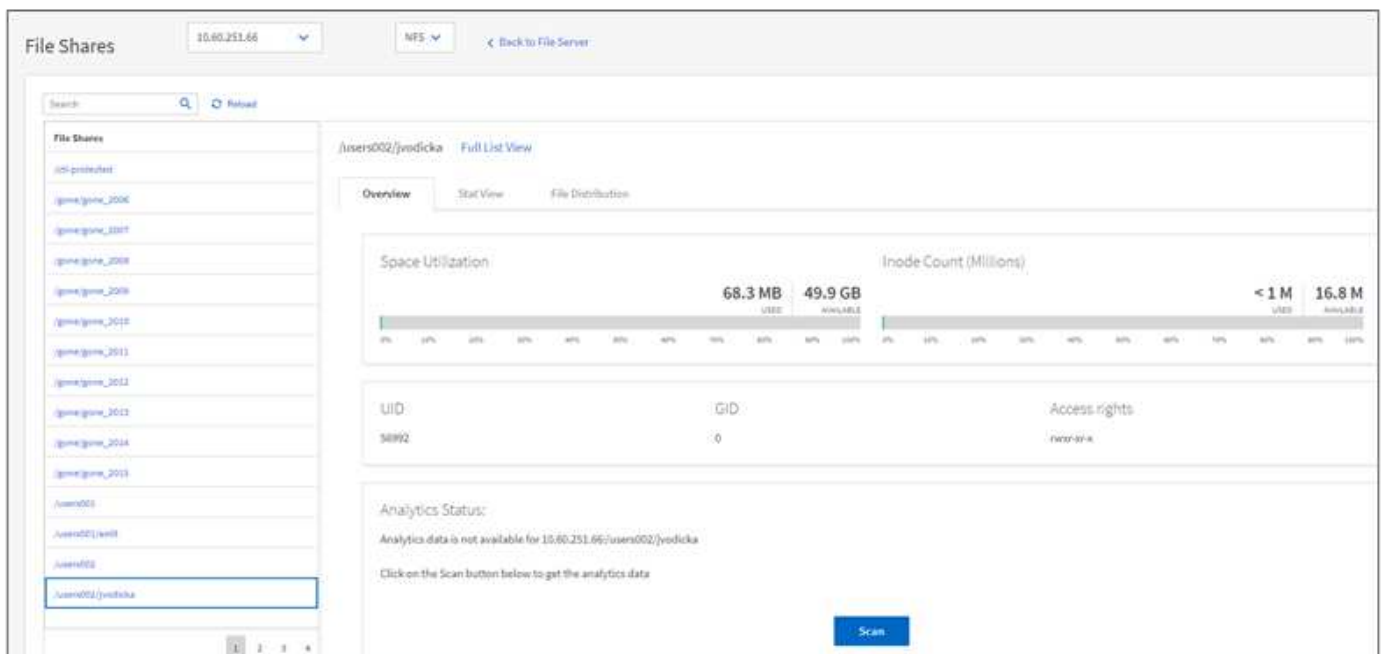
1. Select the arrow on the added file server card to view the file shares on the file server.



- From the list of file shares, select the name of the file share to scan.
- Select **Scan** to start the scan.

XCP displays a progress bar for the scan.

- When the scan is complete the **stat view** and **file distribution** tabs are enabled to allow you to view graphs.

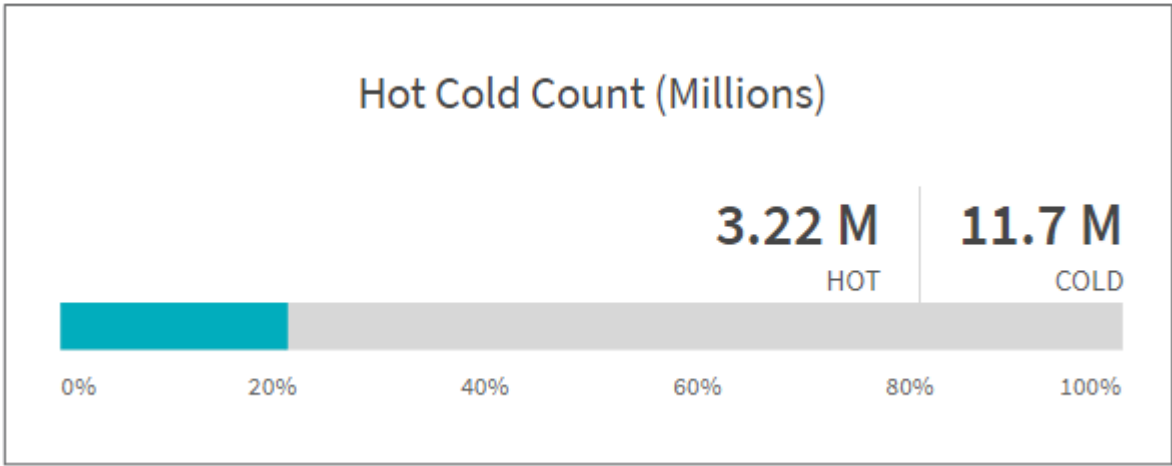


## Learn about graphs

The File Analytics GUI dashboard displays multiple graphs for visualizing File Analytics.

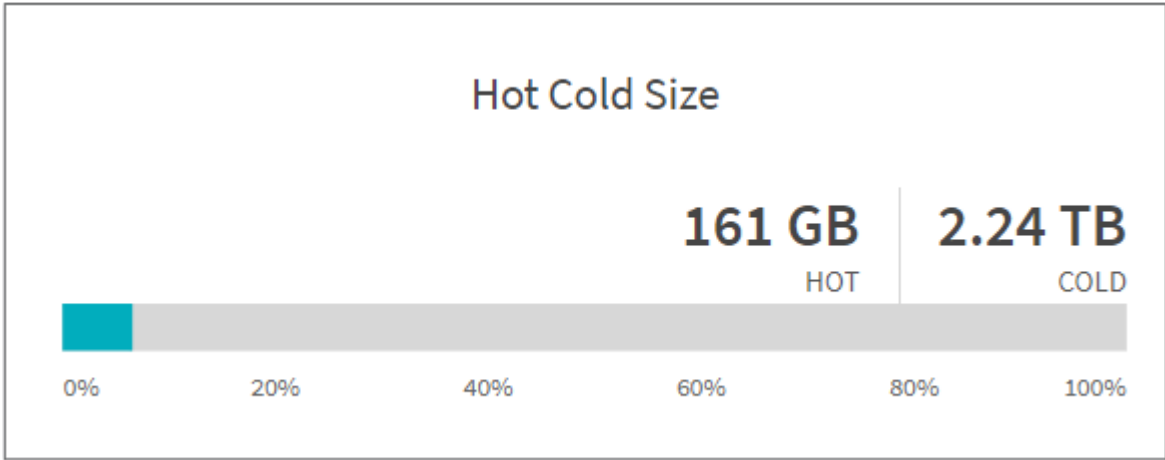
Hot Cold Count Graph

XCP File Analytics categorizes files not accessed for 90 days as cold data. Files accessed in the last 90 days are hot data. Criteria to define hot and cold data is based on access time only.



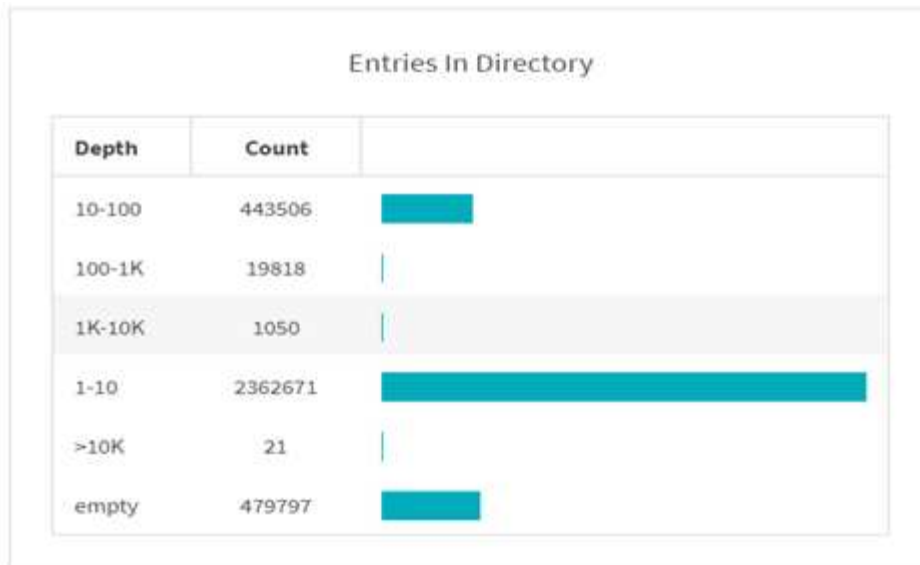
The Hot Cold Count graph displays the number of inodes (in millions) that are hot or cold in XCP NFS. In XCP SMB, this graph denotes the number of files that are hot or cold. The colored bar represents the hot data and shows the percentage of files accessed within 90 days.

Hot Cold Size Graph



The Hot Cold Size graph displays the percentage of files that are hot and cold and the total size of the files in each category. The colored bar represents the hot data and the uncolored part represents the cold data. Criteria to define hot and cold data is based on access time only.

Entries in Directory Graph



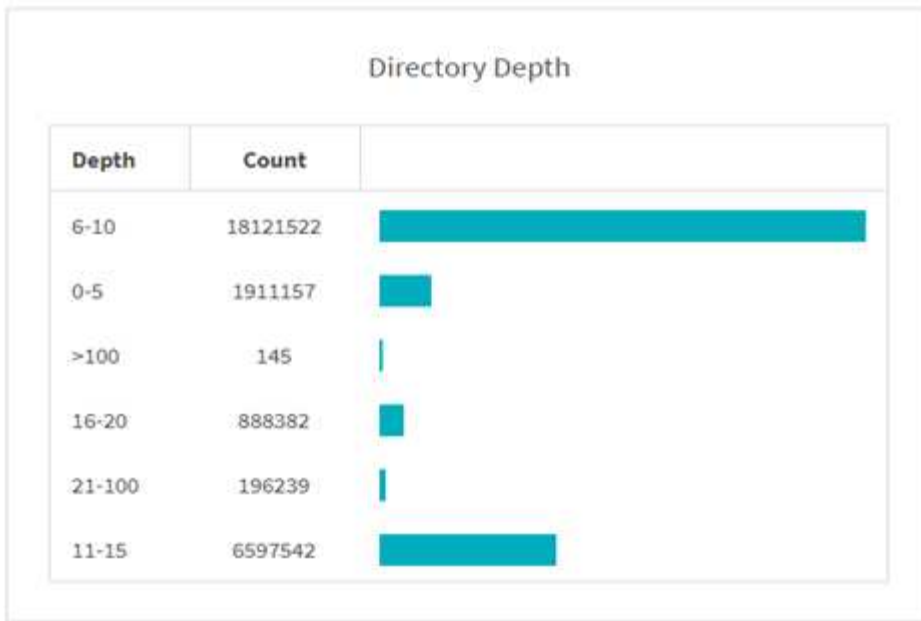
The Entries in Directories graph displays the number of entries in directories. The Depth column contains different directory sizes and the Count column indicates the number of entries in each directory depth.

#### File Distribution by Size Graph



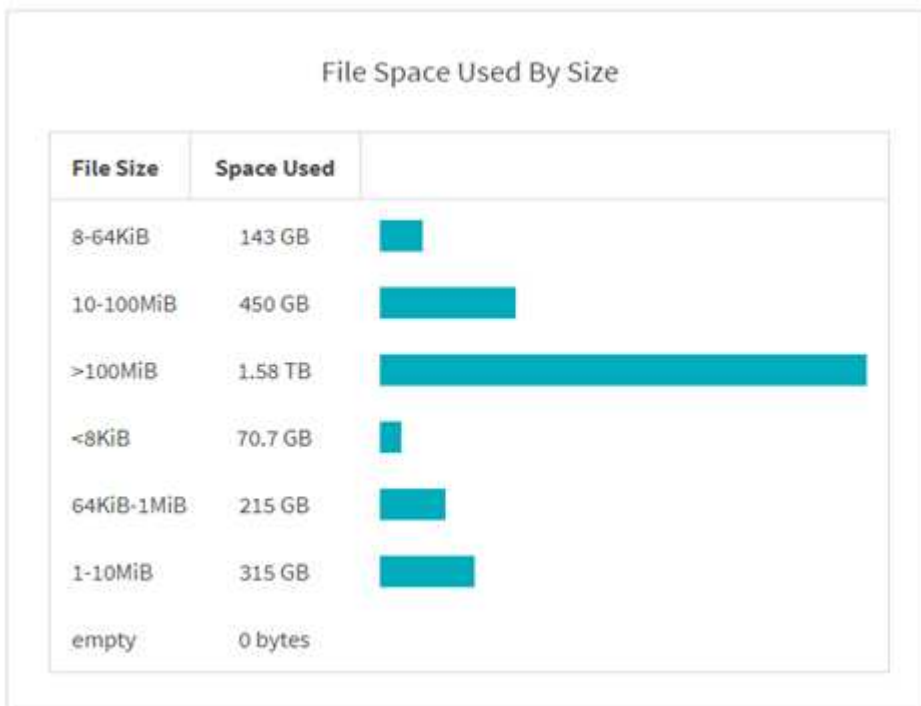
The File Distribution by Size graph displays the number of files that are under the given file sizes. The File Size column contains the categories of file size and the Count column indicates the distribution of the number of files.

#### Directory Depth Graph



The Directory Depth graph represents the distribution of the number of directories in various directory depth ranges. The Depth column contains various directory depths and the Count column contains the count of each directory depth in the file share.






#### File Space Used by Size Graph



The File Space Used by Size graph displays the number of files in different file-size ranges. The File Size column contains different file size ranges and the Space Used column indicates the space used by each file size range.

#### Space Occupied by Users Graph

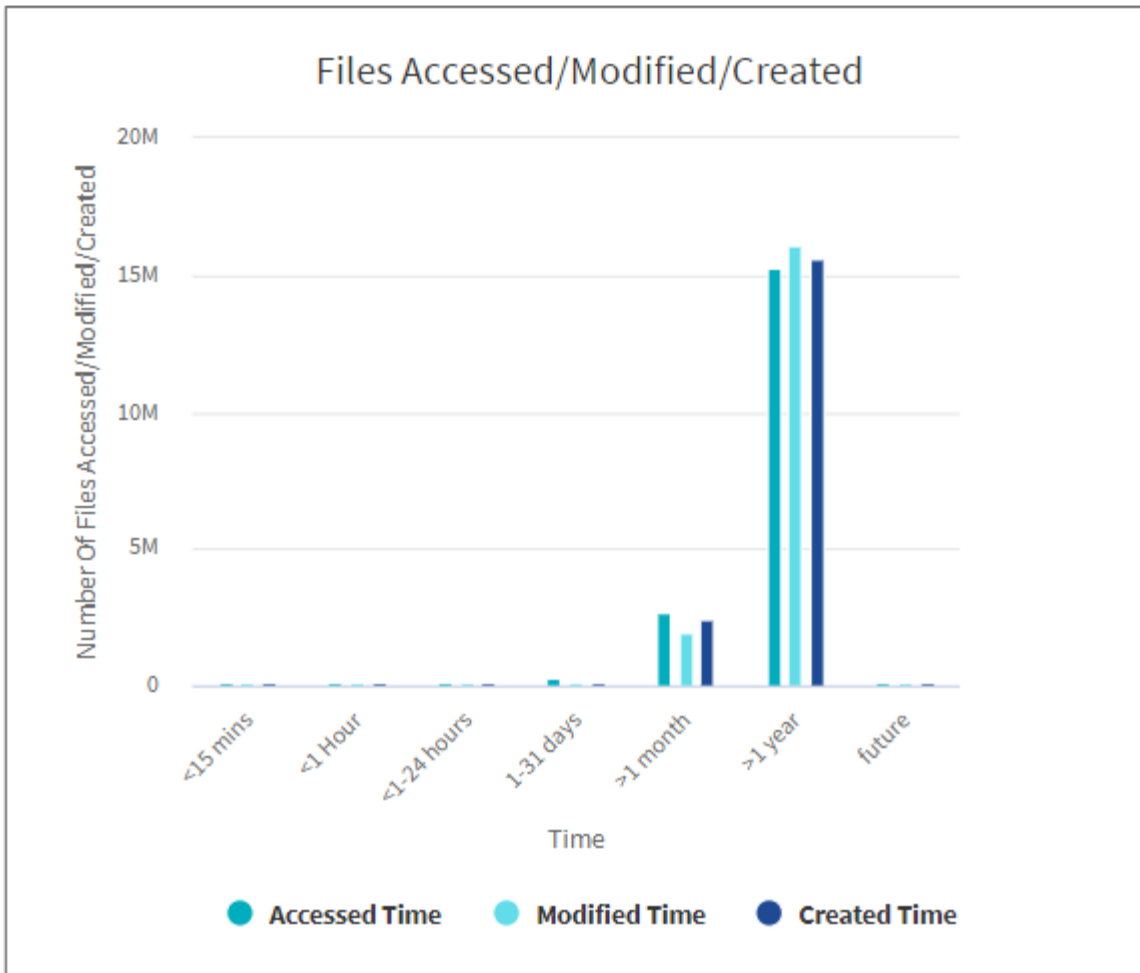
### Space Occupied By Users

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

The Space Occupied by Users graph displays the space used by users. The Username column contains the names of users (UID when usernames cannot be retrieved) and the Space Used column indicates the space used by each username.

#### Files Accessed/Modified/Created Graph

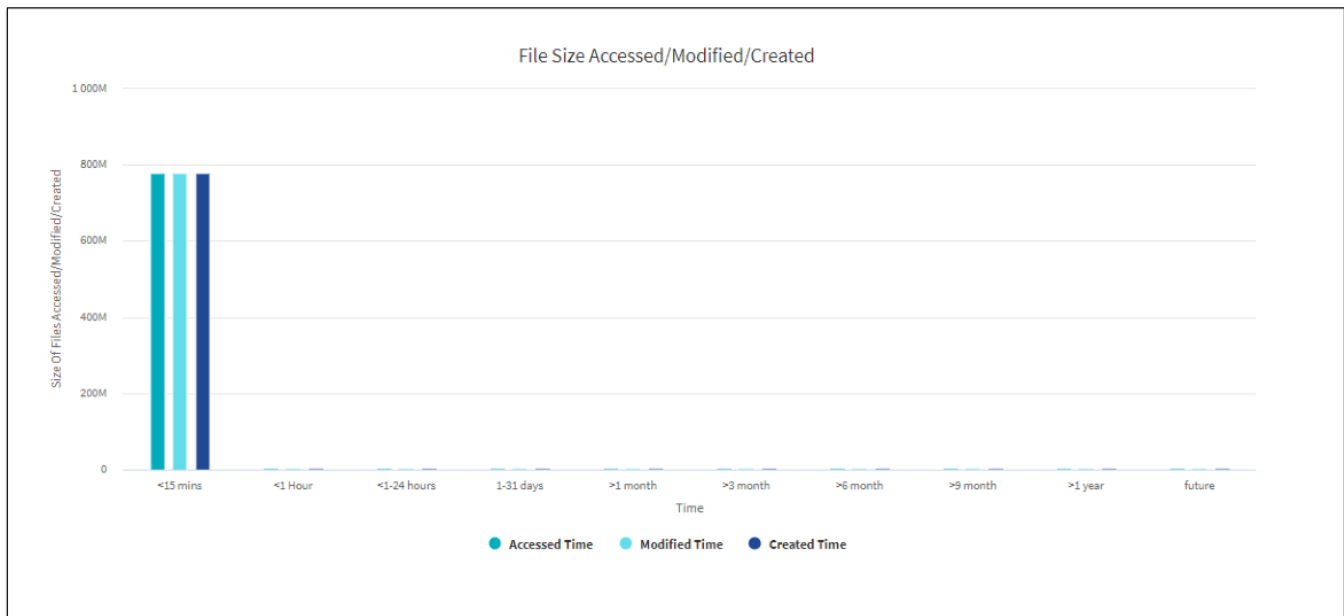


The Files Accessed/Modified/Created graph displays the count of files changed over time. The X-axis represents the period of time within which changes were made and the Y-axis represents the number of files changed.



To get the access time (atime) graph in SMB scans, check the box for preserving atime before running a scan.

#### File Size Accessed/Modified/Created Graph

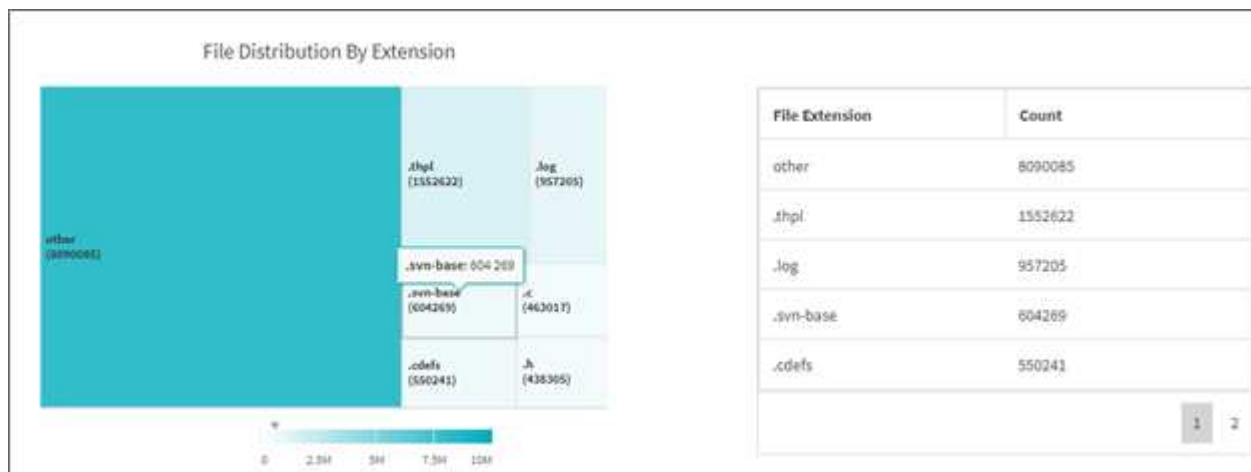


The File Size Accessed/Modified/Created graph displays the size of files changed over time. The X-axis represents the period of time within which changes were made and the Y- axis represents the size of files changed.



To get the access time (atime) graph in SMB scans, check the box for preserving atime before running a scan.

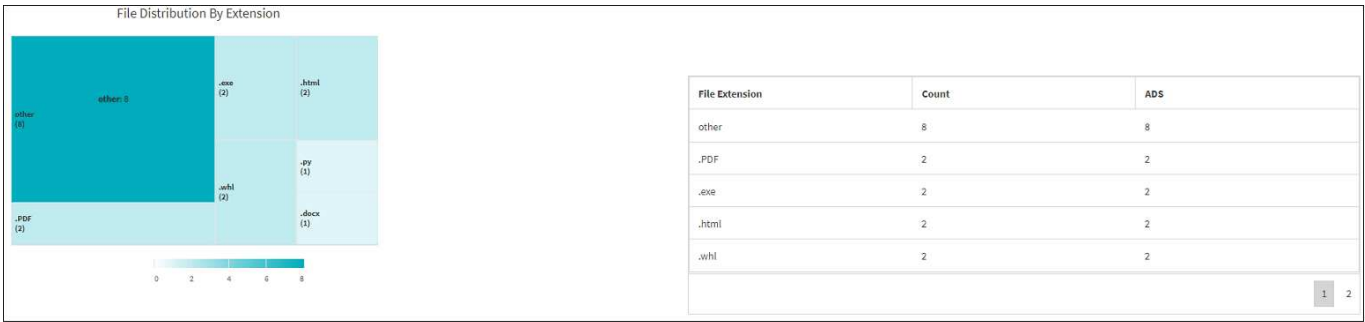
### File Distribution by Extension Graph



The File Distribution by Extension graph represents the count of the different file extensions in a file share. The size of the divisions representing the extensions is based on the number of files with each extension.

Additionally, for SMB shares, you can get the number of Alternate Data Streams (ADS) files for each file extension by checking the box for ADS before running a scan.



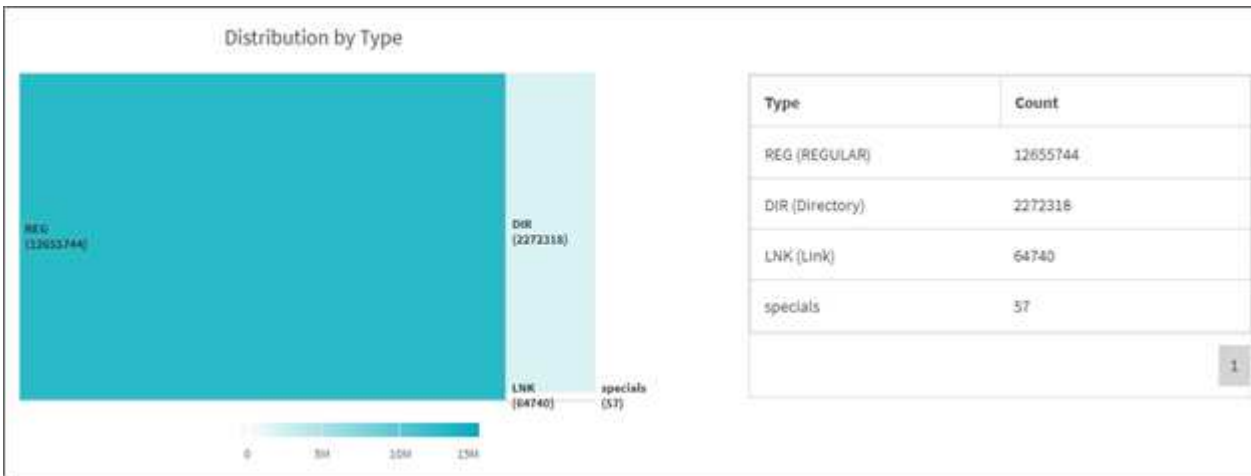


### File Size Distribution by Extension Graph



The File Size Distribution by Extension graph represents the cumulative size of the different file extensions in a file share. The size of the divisions representing the extensions is based on the size of files with each extension.

### File Distribution by Type Graph



The Distribution by Type graph represents the count of the following types of files:

- REG: Regular files
- LNK: Files with links
- Specials: Files with device files and character files.
- DIR: Files with directories

- Junction: Available in SMB only

Additionally, for SMB shares, you can get the number of Alternate Data Streams (ADS) files for different types by checking the box for ADS before running a scan.



## Filters

XCP provides filter options that can be used in XCP operations.

XCP uses filters for `-match` and `-exclude` options for NFS and SMB.

For NFS, run `xcp help info` and refer to the FILTERS section to see how to use `-match` and `-exclude` filters.

For SMB, run `xcp help -match` and `xcp help -exclude` to get more details on match and exclude filters.

If you want to use filters in XCP commands, run `xcp help <command>` to see if they are supported options.

## Logging for NFS and SMB (optional)

Logging for XCP NFS and SMB.

XCP supports configuring multiple optional features by using the `xcpLogConfig.json` JSON configuration file. To enable only specific features, manually create the `xcpLogConfig.json` configuration file. You can use the `xcpLogConfig.json` configuration file to enable:

- event log messages
- syslog client for XCP
- custom XCP logging

Event log messages and the syslog client are disabled in the default configuration. Configuration is common for both NFS and SMB.

Config JSON file location	NFS	SMB
Config file default location	/opt/NetApp/xFiles/xcp/	C:\NetApp\XCP\ConfigFile
Custom location requires the XCP_CONFIG_DIR environment variable	Use the location you have set against the XCP_CONFIG_DIR variable	N/A

The JSON configuration file options are case sensitive. These options are the same for XCP NFS and XCP SMB.

Sub options name	JSON data type	Default	Description
logConfig			Option to customize XCP logging.
"level"	String	INFO	Log message severity filter level. XCP log messages support five severity levels in order of decreasing severity: CRITICAL, ERROR, WARNING, INFO, DEBUG (NetApp strongly recommends using INFO or DEBUG)
"maxBytes"	Integer	52428800	Size of each rotating log file. Max supported rotation files are 10.
"name"	String	xcp.log	Option to set custom log file name.
eventlog			Option to configure event log message.
"isEnabled"	Boolean	true	This boolean option is used to enable event messaging. Setting it to <code>false</code> will not generate any event messages and no event logs will be published to event log file.
"level"	String	INFO	Event message severity filter level. Event messaging support five severity levels in order of decreasing severity: CRITICAL, ERROR, WARNING, INFO, DEBUG
syslog			Option to configure syslog messaging.
"isEnabled"	Boolean	false	This boolean option is used to enable syslog client in XCP.
"level"	String	INFO	Message severity filter level. XCP event log messages support five severity levels in order of decreasing severity: CRITICAL, ERROR, WARNING, INFO, DEBUG
"serverIp"	String	None	Remote syslog server IP addresses or hostname.
"port"	Integer	514	Remote syslog receiver port. Syslog receivers accepting syslog datagrams on a different port can be configured with port option UDP port 514 but you can also configure to the desired port.

Sub options name	JSON data type	Default	Description
"sanitize"	Boolean	false	<p>A common option for XCP support; setting its value to true hides sensitive information (IP and username) in the messages going to support (logging, events, syslog, and so on).</p> <p>For example, with the <code>sanitize</code> option as false:</p> <pre>* 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</pre> <p>With the <code>sanitize</code> option as true:</p> <pre>* 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: * * *</pre>

## Create the JSON configuration file

If you want to enable event log messages, the syslog client, or customer logging, complete the following steps.

### Steps

1. Open any text editor, such as notepad or vi.
2. Create a new file with the following JSON template.

```
{
  "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. For any features that you want to enable, change the `isEnabled` value to `true`.
4. Name the file `xcpLogConfig.json` and save it to the default location: `/opt/NetApp/xFiles/xcp/`

If the `XCP_CONFIG_DIR` environment variable is set, save the `xcpLogConfig.json` file in the same location that is set against the `XCP_CONFIG_DIR` variable.

Default configuration	Example json configuration file
<pre>{   "logConfig": {     "level": "INFO",     "maxBytes": 52428800,     "name": "xcp.log"   },   "sanitize": false }</pre>	<pre>{   "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 }</pre>

# Migrate data

## Migrate NFS data

After planning the migration with the `show` and `scan` commands, you can migrate the NFS data.

### Copy

The `copy` command scans and copies the entire source directory structure to a destination NFSv3 export. The `copy` command requires having source and destination paths as variables. The scanned and copied files, throughput/speed, and elapsed time details are displayed at the end of the copy operation.

#### Example:

```
xcp copy -newid <id> src_server:/src_export dst_server:/dst_export
```

#### POSIX path example:

```
xcp copy -newid <id> file:///mnt/source file:///mnt/dest
```

Run `xcp help copy` for more details.

### Resume

The `resume` command restarts a previously interrupted copy operation by specifying the catalog index name or number. The catalog index name or number of the previous copy operation is stored on the `<catalog path>:/catalog/indexes` directory.

#### Example:

```
xcp resume [options] -id <id used for copy>
```

Run `xcp help resume` for more details.

### Sync

The `sync` command scans for changes and modifications performed on a source NFS directory using a catalog index tag name or the number of a previous copy operation. Source incremental changes are copied and applied to the target directory. The old catalog index numbers are replaced with a new one after the sync operation.

#### Example:

```
xcp sync [options] -id <id used for copy>
```

Run `xcp help sync` for more details.

## Verify

The `verify` command uses a full byte-by-byte data comparison between source and target directories after the copy operation without using a catalog index number. The command checks for modification times and other file or directory attributes, including permissions. The command also reads the files on both sides and compares the data.

### Example:

```
xcp verify src_server:/src_export dst_server:/dst_export
```

### POSIX path example:

```
xcp verify file:///mnt/source file:///mnt/dest
```

Run `xcp help verify` for more details.

## iSync

The `isync` command compares the source and destination and synchronizes the differences on the target without using the catalog index.

### Example

```
xcp isync <source_ip_address>:/src <destination_ip_address>:/dest
```

You can use `isync` with the `estimate` option to estimate the time it takes for the `isync` command to synchronize the incremental changes. The `-id` parameter specifies the catalog name of a previous copy operation.



If you change more than 25% of the data set size used, the `isync estimate` command might not show the expected results.

### Example

```
xcp isync estimate -id <name>
```

Run `xcp help isync` for more details.

# Migrate SMB data

After planning the migration with the `show` and `scan` commands, you can migrate the SMB data.

## Copy

The `copy` command scans and copies the entire source directory structure to a destination SMB share. The `copy` command requires having source and destination paths as variables. The scanned and copied files, throughput/speed, and elapsed time details are printed to the console once every five seconds.



During the copy operation, you can use the `-preserve-atime` flag with the `copy` command to preserve access time at the source.

### Example:

```
C:\xcp>xcp copy \\<source SMB share> \\<destination SMB share>
```

Run `xcp help copy` for more details.

## Sync

The `sync` command scans for changes and modifications in the source and target shares in parallel, and applies the appropriate actions (remove, modify, rename, and so on) to the target to make sure that the target is identical to the source.

The `sync` command compares data content, time stamps, file attributes, ownership, and security information.



During the sync operation, you can use the `-preserve-atime` flag with the `sync` command to preserve access time at the source.

### Example:

```
C:\xcp>xcp sync \\<source SMB share> \\<destination SMB share>
```

Run `xcp help sync` for more details.

## Verify

The `verify` command reads both source and target shares and compares them, providing information about what is different. You can use the command on any source and destination, regardless of the tool used to perform the copy or sync.



During the verify operation, you can use the `-preserve-atime` flag with the `verify` command to preserve access time at the source.

### Example:



```
C:\xcp>xcp verify \\<source SMB share> \\<destination SMB share>
```

Run `xcp help verify` for more details.

## NTFS Alternate Data Streams migration for SMB

Beginning with XCP 1.9.3, XCP SMB supports migration of NTFS Alternate Data Streams (ADS) by using the `-ads` option with the XCP SMB commands.

### Supported use cases

You can use the XCP SMB `copy` and `sync` commands to migrate data that includes ADS, and the XCP SMB `scan` command to scan the SMB share for ADS.

### Supported XCP SMB commands

The following XCP SMB commands support the `-ads` option:

- `scan`
- `copy`
- `verify`
- `sync`

### Command examples

The following example commands show how to use the `-ads` option:

- `xcp scan -ads \\<SMB share>`
- `xcp copy -ads \\<source SMB share> \\<destination SB share>`
- `xcp sync -ads \\<source SMB share> \\<destination SB share>`
- `xcp verify -ads \\<source SMB share> \\<destination SB share>`

## Migrate HDFS data

After planning the migration with the `scan` command, you can migrate the HDFS data.

### Copy

The `copy` command scans and copies the entire source Hadoop Distributed File System (HDFS) data to an NFS or Simple Storage Service (S3) bucket. The `copy` command requires having source and destination paths as variables. The scanned and copied files, throughput, speed, and elapsed time details are displayed at the end of the copy operation.

### NFS path example:

```
xcp copy -newid <id> hdfs:///demo/user dst_server:/dst_export
```

### POSIX path example:

```
xcp copy -newid <id> hdfs:///demo/user file:///mnt/dest
```

### S3 path example:

```
xcp copy -newid <id> hdfs:///demo/user s3://my-bucket  
xcp copy -newid <id> -s3.profile <s3 profile name> -s3.endpoint <endpoint-  
url> hdfs:///demo/user s3://my-bucket
```

Run `xcp help copy` for more details.

## Resume

The `resume` command restarts a previously interrupted copy operation by specifying the catalog index name or number. The catalog index name or number of the previous copy operation is stored in the `<catalog path>:/catalog/indexes` directory.

### Example:

```
xcp resume [options] -id <id used for copy>  
xcp resume [options] -s3.profile <s3 profile name> -s3.endpoint <endpoint-  
url> -id <id used for copy>
```



By default, the XCP `resume` command uses the S3 endpoint and S3 profile from the copy index that was used during the `copy` command. However, if new `-s3.endpoint` and `-s3.profile` values are provided with the `resume` command, the new values for the options are used and the values used with the `copy` command are overridden.

Run `xcp help resume` for more details.

## Verify

The `verify` command uses a full byte-by-byte data comparison between source and target directories after the copy operation without using a catalog index number. The command reads the files on both sides and compares the data.

### Example:

```
xcp verify hdfs:///demo/user dst_server:/dst_export
```

### POSIX path example:

```
xcp verify hdfs:///user/demo1/data file:///user/demo1/dest
```

### S3 path example:

```
xcp verify hdfs:///user/demo1/data s3://my-bucket  
xcp verify -s3.profile <s3 profile name> -s3.endpoint <endpoint-url>  
hdfs:///demo/user s3://my-bucket
```

Run `xcp help verify` for more details.

## Run multiple XCP jobs on the same XCP host

Beginning with XCP 1.9.2, you can run multiple XCP jobs or commands on a single XCP host, provided that the host has sufficient resources for each job. When you run a command that supports multiple jobs, XCP uses minimal host memory to complete the job, which creates the capacity to run additional jobs on the same host configuration.

### Minimum system requirements

For each XCP job, you should allow up to 64GB of host memory and eight cores for medium to large migrations.



Running multiple XCP jobs on the same host is not supported for SMB data migration.

### Logging

By default, each XCP job is logged in a separate log file that is unique to the job ID. This logging mechanism works well when running multiple jobs on the same individual host. NetApp does not recommend changing the `xcpLogConfig.Json` file to use a single `xcp.log` file to log multiple XCP jobs running in parallel on the same host.

### Supported commands

Running multiple XCP jobs on the same host is supported with the following XCP commands:

- scan
- copy
- resume
- verify
- isync
- chmod
- chown

- delete

## Unsupported commands

Running multiple XCP jobs on the same host is not supported with the `sync` command.

## Additional NFS features

XCP includes some additional NFS features.

### Chown and Chmod

You can use the XCP `chown` and `chmod` commands to recursively change all of the files and directories for a given NFS share or POSIX path. This increases the performance of millions of files.



Before changing the ownership of the files, you must configure the new owner. Otherwise, the command will fail. The XCP `chown` and `chmod` commands work similar to the Linux `chown` and `chmod` commands.

### Chmod

The `chmod` command scans and changes the file permission of all files in the chosen directory structure. The `chmod` command requires a mode or reference and an NFS share or POSIX path as variables. XCP `chmod` recursively changes the permissions for a given path. You can use the `chmod` command to display the total files scanned and the permissions that have been changed in the output.

#### Example:

```
xcp chmod -mode 777 NFS [server:/export path | file://<NFS mounted path>]
xcp chmod -mode 707 nfs_server01.netapp.com:/export1
xcp chmod -reference nfs_server01.netapp.com:/export/dir1/file.txt
nfs_server02.netapp.com: export1
xcp chmod -match "fnm('file.txt')" -mode 111 file:///mnt/nfs_mount_point/
xcp chmod -exclude "fnm('file.txt')" -mode 111 file:///demo/user1/
```

Run the `xcp help chmod` command for more information.

### Chown

You can use the XCP `chown` command to recursively change all of the files and directories for a given NFS share or POSIX path. This increases the performance of millions of files.

The `chown` command scans and changes the ownership of all files in the chosen directory structure. The `chown` command requires an NFS share or POSIX path as variables. XCP `chown` recursively changes the ownership for a given path.

#### Example

```
xcp chown -user user1 NFS [server:/export path | file:///<NFS mounted path>
xcp chown -user user1 nfs_server01.netapp.com:/export1
xcp chown -user user1 -group group1 nfs_server01.netapp.com:/export1/dir1/
xcp chown -reference nfs_server01.netapp.com:/export/dir1/file.txt
nfs_server02.netapp.com:/export1
xcp chown -match "fnm('file.txt')" -user user1
file:///mnt/nfs_mount_point/
xcp chown -exclude "fnm('file.txt')" -user user1 -group group1
xcp chown -user-from user1 -user user2 file:///mnt/nfs_mount_point/
xcp chown -group-from group1 -group group2
nfs_server01.netapp.com:/export1/
```

Run the `xcp help chown` command for more information.

## XCP Estimation

The XCP estimation feature estimates the time to complete a baseline `copy` operation from the source to the destination. It calculates the estimated time to complete a baseline `copy` operation by using all the currently available system resources such as CPU, RAM, network, or other parameters. When you use the `-target` option, XCP runs a sample `copy` operation to find the estimation time.

### Example

```
server : NFS server IP
export : NFS exported path for the above IP

xcp static estimation
xcp estimate -id <scan id>

xcp live estimation with default time
xcp estimate -id <scan id> -target server:/export

xcp live estimation with -t option
xcp estimate -id <scan id> -t <time for which estimation should run>
-target server:/export
```

## indexdelete

You can use the `indexdelete` command to delete catalog indexes.

### Example

```
xcp indexdelete
```

Run `xcp help indexdelete` for more details.

# Troubleshoot

## Troubleshoot XCP NFS errors

Review the solutions to troubleshoot your issue.


### XCP issues and solutions

XCP issue	Solution
<code>xcp</code> : ERROR: compare batches: Incompatible index file. Please use the index file generated with the current version of XCP only. Alternatively, you can download an older XCP binary from <a href="http://xcp.netapp.com">xcp.netapp.com</a> .	You are trying to perform operations on an index that was generated using an XCP version older than XCP 1.9. This is not supported. It is recommended to complete any in-progress migrations and then switch to this version of XCP. Alternatively, you can re-run the <code>scan</code> , <code>copy</code> or <code>verify</code> commands to generate a new index with XCP 1.9.
<code>xcp</code> : ERROR: must run as root	Execute XCP commands as root user
<code>xcp</code> : ERROR: License file /opt/NetApp/xFiles/xcp/license not found.	Download the license from the <a href="#">XCP site</a> , copy it to /opt/NetApp/xFiles/xcp/, and activate it by running the <code>xcp activate</code> command.
<code>xcp</code> : ERROR: This license has expired	Renew or obtain the new XCP license from the <a href="#">XCP site</a> .
<code>xcp</code> : ERROR: License unreadable	License file might be corrupted. Obtain the new XCP license from the <a href="#">XCP site</a> .
<code>xcp</code> : ERROR: XCP not activated, run 'activate' first	Run the <code>xcp activate</code> command
This copy is not licensed	Obtain the appropriate XCP license file. Copy the XCP license to the /opt/NetApp/xFiles/xcp/ directory on the XCP server. Run the <code>xcp activate</code> command to activate the license.
<code>xcp</code> : ERROR: Failed to activate license: Server unreachable	You are trying to activate the online license and your host system is not connected to the internet. Make sure your system is connected to the internet.
<code>xcp</code> : ERROR: Failed to activate license: Server <a href="http://xcp.netapp.com">xcp.netapp.com</a> unreachable <code>xcp</code> : HINT: Configure DNS on this host or return to the license page to request a private license Expected error: Failed to activate license: Server <a href="http://xcp.netapp.com">xcp.netapp.com</a> unreachable	Make sure <a href="http://xcp.netapp.com">xcp.netapp.com</a> is reachable from your host or request for the offline license

XCP issue	Solution
xcp: ERROR: Catalog inaccessible: Cannot mount nfs_server:/export[:subdirectory]	Open the editor on the XCP Linux client host and update the configuration file with the proper catalog location. The XCP configuration file is located at /opt/NetApp/xFiles/xcp/xcp.ini. Sample entries of configuration file:  [root@scspr1949387001 ~]# cat /opt/NetApp/xFiles/xcp/xcp.ini [xcp] catalog = 10.235.128.153:/catalog
nfs3 error 2: no such file or directory	Operation did not find the source file(s) on the target NFS export. Run the xcp sync command to copy the incremental updates from source to destination
xcp: ERROR: Empty or invalid index	Previous copy operation was interrupted before the index file was created. Rerun the same command with the new index and when the command is executing, verify that the keyword “indexed” is displayed in the stats.
xcp: ERROR: compare batches: child process failed (exit code -9): recv <type 'exceptions.EOFError'>	Follow the instructions in the following KB article: <a href="#">Cannot allocate memory when synching NFS data</a>
xcp: ERROR: For xcp to process ACLs, please mount <path> using the OS nfs4 client	Mount the source and target on the XCP host using NFSv4, for example, mount -o vers=4.0 10.10.10.10:/source_vol /mnt/source
The XCP verify command fails during a migration. The STATUS shows as FAILED. (Live)	The XCP verify command was run when the source was live. Run the XCP verify command after the final cutover.
The XCP verify command fails after a cutover. (Live)	The XCP cutover sync operation might not have copied all the data. Rerun the XCP sync command followed by the verify command after the final cutover. If the problem persists, contact technical support.
The XCP sync command fails (this applies to all sync failures during migrations). (Live)	XCP is not able to read the data, this might be due to an XCP issue. Check the XCP STATUS message after the command operation completes. Rerun the sync command. If the sync operation fails again, contact technical support.
The XCP copy, resume, and sync commands fail due to insufficient memory. XCP crashes and the XCP status shows as FAILED. (Live)	There is low available memory on the host or there has been a huge incremental change. Follow the instructions in the following KB article: <a href="#">Cannot allocate memory when synching NFS data</a>
mnt3 error 13: permission denied	As a non-root user, you do not have the correct permissions to access the file system. Check if you can access the file system and perform read write operations.



XCP issue	Solution
xcp: batch 1: ERROR: [Errno 13] Permission denied:	As a non-root user, you do not have the correct permissions to access the file system. Check if you can access the file system and perform read write operations.
mxcp: ERROR: OSMounter 'file:///t/10.234.115.215_src_vol/DIR': [Errno 2] No such file or directory	The path /t/10.234.115.215_src_vol/ DIR is not mounted on the Linux file system. Check if the path exists.
ERROR: run sync {-id: 'xcp_index_1624263869.3734858'}: sync not yet available for hdfs/ posix/s3fs sources and targets -workaround is copy with a match filter for recent mods	The sync command is not supported in XCP for the POSIX and HDFS connectors.
The xcp verify command fails with different mod time	You can identify the file and manually copy the file to the destination.
Non dir object copy/sync can not be resumed; try copy again. For more details please refer XCP user guide.	Because you cannot resume a single file, it is recommended to run the xcp copy command again for the file. Any change in the file leads to a complete copy of the file. As a result, performance is not affected.
Non dir object can not be synced; try copy again. For more details please refer XCP user guide.	Because you cannot sync a single file, it is recommended to run the xcp copy command again for the file. Any change in the file leads to a complete copy of the file. As a result, performance is not affected.
xcp: ERROR: batch 4: Could not connect to node:	Verify that the node given in the --nodes parameter is reachable. Try connecting by using Secure Shell (SSH) from the master node
[Error 13] permission denied	Check if you have permission to write on the destination volume.
xcp: ERROR: batch 2: child process failed (exit code -6): recv <type 'exceptions.EOFError'>:	Increase your system memory and rerun the test.
xcp:ERROR: invalid path 'IP:/users009/user1/2022-07-01_04:36:52_1489367	If there is one or more colons in the NFS server share path name, use a double colon (::) instead of a single colon (:) to separate the NFS server IP and NFS server share path.

XCP issue	Solution
<p>The SnapLock volume does not retain the WORM files after an <code>xcp copy</code> operation.</p>	<p>XCP copies the WORM files to the volume successfully but the files are not retained by the SnapLock volume.</p> <ol style="list-style-type: none"> <li>1. Perform the <code>xcp copy</code> operation from the source to the destination volume:  <pre>xcp copy src_server:/src_export dst_server:/dst_export</pre> </li> <li>2. Use the <code>xcp chmod</code> command to change the file permissions on the destination volume to <b>readonly</b>:  <pre>xcp chmod -mode a-w dst_server:/dst_export</pre> </li> </ol> <p>When the above steps are complete, the SnapLock volume starts retaining the copied files.</p> <div data-bbox="850 772 1412 982">  <p>The retention time of a SnapLock volume is governed by the volume's default retention policy. Check the volume retention settings before starting migration: <a href="#">Set the retention time</a></p> </div>

## Logdump

If you encounter an issue with an XCP command or job, the `logdump` command enables you to dump log files related to the issue into a `.zip` file that can be sent to NetApp for debugging. The `logdump` command filters logs based on the migration ID or job ID and dumps those logs into a `.zip` file in the current directory. The `.zip` file has the same name as the migration or job ID that is used with the command.

### Example

```
xcp logdump -j <job id>
xcp logdump -m <migration id>
```



After migration, if you use the `XCP_CONFIG_DIR` or `XCP_LOG_DIR` environment variables to override the default config location or log location, the `logdump` command fails when used with an old migration or job ID. To avoid this, use the same logpath until migration completes.

## Troubleshoot XCP SMB errors

Review the solutions to troubleshoot your issue.

Issue	Solution
XCP commands do not show the expected results when a junction path is used in the source or destination.	Use an SMB share path instead of a junction path when running XCP commands.
<p>A traceback error might occur if the source, destination, or both is a junction with no directories and an online license is used in migration. If this occurs, the XCP command status is <code>PASSED</code> but the following error is returned at the end of the console output:</p> <pre>Error in atexit._run_exitfuncs: Traceback (most recent call last):   File "xcp\stats.py", line 214, in call_home   File "xcp\histograms.py", line 387, in calculate_averages ZeroDivisionError: division by zero</pre>	Use an offline license instead of an online license.
xcp: ERROR: This license has expired	Renew or obtain the new XCP license from the <a href="#">XCP site</a> .
This copy is not licensed	Obtain the appropriate XCP license file. Copy the XCP license to the <code>c:\netapp\xcp</code> folder on the XCP host. Run the <code>xcp activate</code> command to activate the license
xcp: ERROR: XCP not activated, run 'activate' first	Download the XCP license from the <a href="#">XCP site</a> . Copy the file on the XCP Linux client host at <code>c:\netapp\xcp</code> on the XCP host. Run the <code>xcp activate</code> command to activate the license.
xcp: ERROR: License file C:\NetApp\XCP\license not found	Register for the XCP license on the <a href="#">XCP site</a> . Download and copy the license file to <code>C:\NetApp\XCP\</code> on the XCP Windows client host.
xcp scan Error: The network name cannot be found	Rerun the command with correct share name
<p>xcp copy Error: ERROR failed to obtain fallback security principal</p> <p>Error message logged in xcp.log file:</p> <pre>pywintypes.error: (1722, 'LookupAccountName', 'The RPC server is unavailable.')</pre>	<p>Add the destination box in the hosts file (<code>C:\Windows\System32\drivers\etc\hosts</code>). Netapp storage destination box entry must be in the below format:</p> <pre>&lt;data vserver data interface ip&gt; 1 or more white spaces &lt;cifs server name&gt;</pre>

Issue	Solution
<p>xcp copy: ERROR failed to obtain fallback security principal (Post adding destination box entry in the hosts files)</p> <p>Error messaged logged in xcp.log file: 'No mapping between account names and security IDs was done'</p>	<p>The fallback user/group does not exist at the target system (destination box) or active directory.</p> <p>Rerun the command with correct fallback user/group options</p>
<p>xcp copy: ERROR failed to obtain fallback security principal (Post adding destination box entry in the hosts files)</p> <p>Error messaged logged in xcp.log file: pywintypes.error: (87, 'LookupAccountName', 'The parameter is incorrect.')</p>	<p>Incorrect parameter for fallback user/group option. Rerun the command with the correct syntax for fallback user/group options</p>
<p>xcp copy with ACL migration</p> <p>Error message logged in xcp.log file: pywintypes.error: (1314, 'GetNamedSecurityInfo', 'A required privilege is not held by the client.')</p>	<p>An issue related to security descriptors because the migration user account only has the required privileges for XCP to retrieve owner, group, and DACL. It cannot retrieve SACL.</p> <p>Add your migration user account to the "Manage Audit and Security Log" policy in your Active Directory. Reference: <a href="#">Manage auditing and security log</a></p>

## Troubleshoot XCP File Analytics errors

Review the solutions to troubleshoot your issue.

Issue	Solution
PostgreSQL service failed	<p>Run configure again and select the installation option. If the previous installation was successful, you can select the repair option. If you are still getting the error, try manual steps as follows:</p> <ol style="list-style-type: none"> <li>Restart the PostgreSQL service: <pre>sudo systemctl restart postgresql.service</pre> </li> <li>Check the service status: <pre>sudo systemctl status postgresql.service   grep Active</pre> </li> </ol>

Issue	Solution
HTTPD service failed	<p>Run configure again and select the installation option. If the previous installation was successful, you can select the repair option. If you are still getting the error, try manual steps as follows:</p> <ol style="list-style-type: none"> <li>1. Restart the HTTPD services: <pre>sudo systemctl restart httpd</pre> </li> <li>2. Check the HTTPD service status: <pre>sudo systemctl status httpd   grep Active</pre> </li> </ol>
Not able to open login page after successful install	<p>Verify that your system can ping the Linux machine where XCP File Analytics is installed and HTTPD is running. If the services are not running, run <code>configure</code> and choose the repair option.</p> <p>Verify that you are using a supported browser version. See the <a href="#">IMT</a>.</p>
User login failed	<ul style="list-style-type: none"> <li>• Verify that you are using a supported browser version. See the <a href="#">IMT</a>.</li> <li>• Verify that the user is “admin” and the password is correct.</li> <li>• Verify that the XCP service is running by issuing <code>xcp service status</code>.</li> <li>• Verify that port 5030 is open on Linux. Open the application at <b><code>https:// &lt;linux ip&gt; :5030/api/xcp</code></b>, and confirm that the <code>messagereads msg: Missing Authorization Header</code>.</li> <li>• Check whether the <code>xcp.ini</code> file is present in the <code>/opt/NetApp/xFiles/xcp/</code> location. To reset the <code>xcp.ini</code> file, run the configuration script and select the <b>Repair</b> option. Next, select the menu option to <b>rebuild xcp.ini file</b>.</li> <li>• Manually run the <code>xcp --listen</code> command on the CLI and try logging in. If you do not receive a request on the server, re-check the installation and the ports used for communication with the server. After you verify that the installation is correct, run the <code>service xcp start</code> command to restart the service.</li> </ul>
XCP GUI is not showing updated pages	Clear the cache and try again
XCP service is not starting	To run the <code>xcp</code> service, use the <code>sudo systemctl start xcp</code> command. Alternatively, run the configuration script and select the <b>Repair</b> option to start the services that are stopped.

Issue	Solution
Failed to scan file share	<p>File share/volume might not be readable. Check manually whether the file share is accessible/readable by running the <code>xcp show</code> command.</p> <p>Also, check if the <code>xcp.ini</code> file is deleted. If it is deleted, rebuild the <code>xcp.ini</code> file by using the <code>configure.sh</code> script repair option.</p>
Could not load file servers	<p>Try a page refresh. If the problem persists, manually run the <code>xcp show</code> command on the prompt and check whether you can scan the file server. If successful, raise a ticket with NetApp customer support. If unsuccessful, check if the file server is active by performing a manual check.</p> <p>Check whether the <code>xcp.ini</code> file and license files are in the correct location. To reset the <code>xcp.ini</code> file, run the configuration script and select the <b>Repair</b> option. Next, select the menu option to <b>rebuild xcp.ini file</b>.</p> <p>Check the <code>xcpfalogs</code> logs to see if the license needs renewal.</p>
XCP File Analytics page is not displayed after system reboot	<p>XCP services might be down. Run the configuration script and select the option to <b>Repair</b>. This will restart all the services that are stopped.</p>
The total space for an exported file system on a given file server might show more space compared to the allocated physical storage.	<p>This can happen when there are qtree level exports inside the volume.</p> <p>For example, if the volume size that is exported as <code>/vol1</code> is 10 GB and there is a qtree inside the volume <code>/vol1/mtree1</code>, then the <code>xcp show</code> command will show the <code>vol1</code> size as 10 GB and the <code>mtree1</code> size as 10 GB. XCP File Analytics sums the space of both exports and gives the total space, in this case, 20 GB. It does not understand that <code>mtree1</code> is a logical space.</p>

Issue	Solution
<p>The site can't be reached or user login failed after a successful install.</p>	<ol style="list-style-type: none"> <li>1. Check if XCP services are running:  <pre>service xcp status</pre> </li> <li>2. Start the XCP listen operation and confirm that there are no errors:  <pre>xcp -listen</pre> </li> <li>3. If you see the following error, install the CodeReady packages using yum, such as <code>yum install codeready-builder-for-rhel-8-x86_64-rpms</code>:</li> </ol> <div data-bbox="683 562 1477 1871" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Error:</p> <pre>----- Traceback (most recent call last):   File "xcp.py", line 1146, in &lt;module&gt;     File "xcp.py", line 1074, in main       File "&lt;frozen importlib._bootstrap&gt;", line 991, in _find_and_load       File "&lt;frozen importlib._bootstrap&gt;", line 975, in _find_and_load_unlocked       File "&lt;frozen importlib._bootstrap&gt;", line 671, in _load_unlocked       File "PyInstaller/loader/pyimod03_importers.py" , line 495, in exec_module       File "rest/routes.py", line 61, in &lt;module&gt;       File "&lt;frozen importlib._bootstrap&gt;", line 991, in _find_and_load       File "&lt;frozen importlib._bootstrap&gt;", line 975, in _find_and_load_unlocked       File "&lt;frozen importlib._bootstrap&gt;", line 671, in _load_unlocked       File "PyInstaller/loader/pyimod03_importers.py" , line 495, in exec_module       File "onelogin/saml2/auth.py", line 14, in &lt;module&gt; xmlsec.Error: (1, 'cannot load crypto library for xmlsec.') [23891] Failed to execute script 'xcp' due to unhandled exception!</pre> </div>

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<https://www.netapp.com/company/legal/copyright/>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

## Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- [Notice for NetApp XCP 1.9.2](#)
- [Notice for NetApp XCP 1.9.1](#)
- [Notice for NetApp XCP 1.9](#)
- [Notice for NetApp XCP 1.8.1](#)
- [Notice for NetApp XCP 1.8](#)
- [Notice for NetApp XCP 1.7](#)
- [Notice for NetApp XCP 1.6.2](#)
- [Notice for NetApp XCP 1.6.1](#)



## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.