Get started with XCP

XCP

NetApp
May 25, 2022

This PDF was generated from https://docs.netapp.com/us-en/xcp/xcp-nfs-add-ons.html on May 25, 2022.
Always check docs.netapp.com for the latest.

Table of Contents

Get started with XCP . . . 1
- Learn about XCP . . . 1
- XCP NFS add-on features . . . 1
- Unsupported features . . . 3
- Supported configurations . . . 4
- Ports used by XCP . . . 4

Get started with XCP

NetApp XCP allows for scalable and high-performance data migrations.

Learn about XCP

NetApp XCP is a client-based software 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 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:

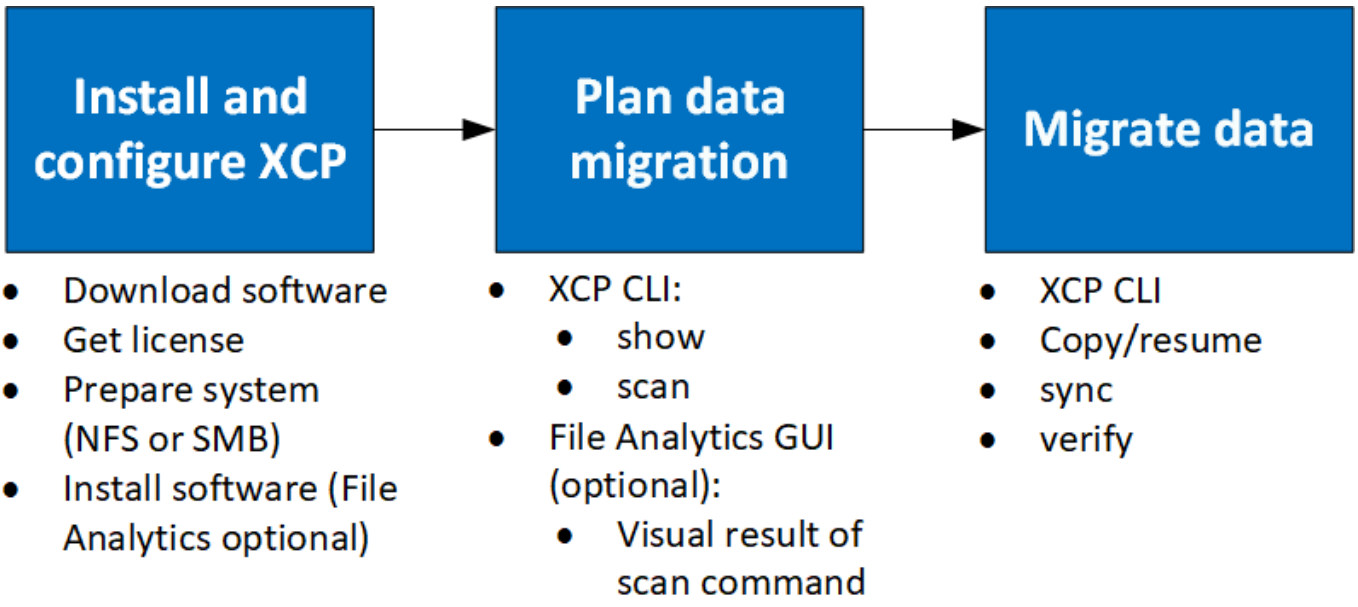
- Migration solution
- File Analytics solution

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 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 preforming 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	• The `sync` command does not support the POSIX connector • You should not use the `copy` command when the source is active
Hadoop Distributed File System (HDFS) connector	• The `sync` command does not support the HDFS connector • The HDFS file system does not support symbolic links (symlinks), hard links, or special files • You should not use the `copy` command when the source is active
ACLs	When the source is a non-NetApp system, XCP does not copy ACLs.
Linux	XCP is no longer supported on earlier distributions of Linux that were supported by XCP 1.6.3.

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)
NTFS Alternate Data Streams	XCP does not currently support Alternate Data Streams
XCP Filters	The XCP SMB exclude option currently excludes directories based on their pattern in the filter and traverses the filesystem of those directories.
Active source support	XCP does not support the use of a baseline or an incremental Snapshot copy followed by live source migration for an incremental sync.

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

- **XCP multiple instances on same host**: When running multiple instances of XCP on the same host you might get unpredictable results.
- **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.

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

Service	Port
XCP (as a service for File Analytics)	5030
HDFS	7222

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.