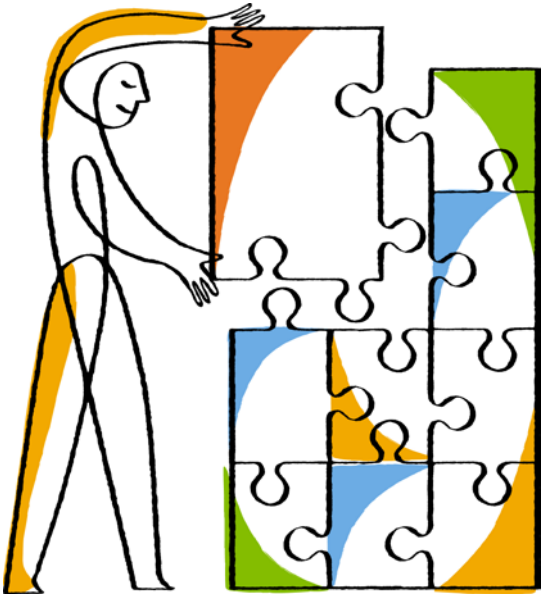
NDMP Cloud Extension Software 1.0

Installation and Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-09775_C0
June 2015

Contents

Introduction to NDMP Cloud Extension Software 4

Setting up NDMP Cloud Extension Software 5

System requirements for NCE 5

Linux host requirements 5

Storage system requirements 6

Licensing requirements 6

Installing NCE 6

Privilege levels for NCE operations 7

Configuring NCE to communicate to Amazon S3 7

Creating the ndmpcopy metaconfiguration file 10

Transferring data between storage systems and Amazon S3 12

What a backup set is 12

Transferring data to Amazon S3 13

Retrieving data from Amazon S3 14

Viewing backup set summary 16

Deleting a backup set 16

How NCE verifies data integrity 16

Parameters for the ndmpcopy command 17

What the ndmpcopy metadata file contains 19

NCE log files 19

Known problems and limitations 20

Where to find additional information 21

Copyright information 22

Trademark information 23

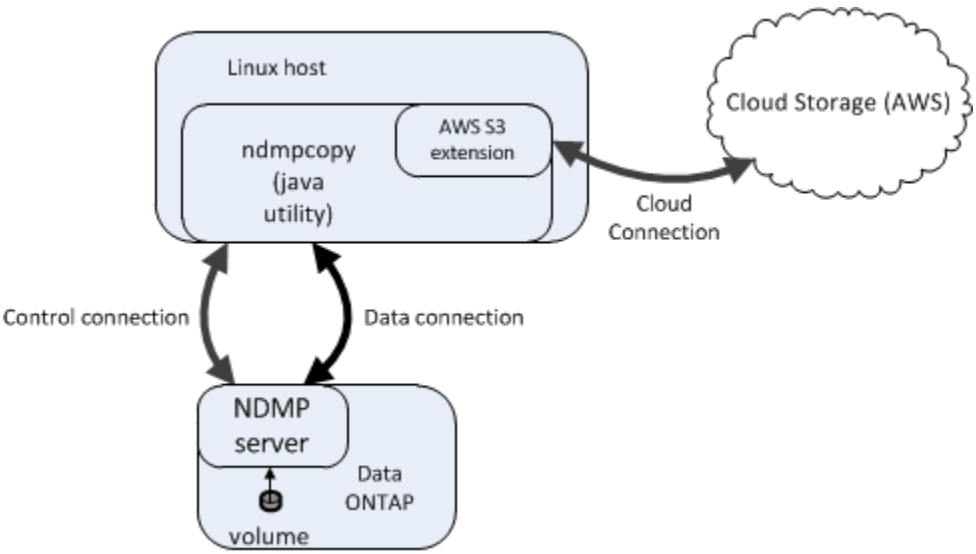
How to send your comments 24

Introduction to NDMP Cloud Extension Software

NDMP Cloud Extension Software (NCE) is a host-based utility that transfers data between Data ONTAP storage systems and object storage in the Amazon Simple Storage Service (Amazon S3) cloud. You can transfer data to Amazon S3 by executing the `ndmpcopy` command. Data transfer is supported at the volume, qtree, directory, or file level.

Note: NCE supports data transfer from both 7-Mode and clustered Data ONTAP systems.

The NCE architecture uses Network Data Management Protocol (NDMP) to communicate with a Data ONTAP system and an Amazon Web Service (AWS) extension to communicate with Amazon S3.



During data transfer, the ndmpcopy utility, running on the Linux host, establishes a data connection with the Data ONTAP system. The ndmpcopy utility reads the data stream generated by Data ONTAP and streams it to Amazon S3 through the cloud connection. Data transfer from Amazon S3 to a Data ONTAP system works in a similar way.

When using NCE, be aware of the following considerations:

- NCE does not work on multi-homed Linux hosts.
- NCE does not support client-side encryption of the data stored on Amazon S3.

Setting up NDMP Cloud Extension Software

You must ensure that you meet certain system requirements and then install and configure NCE to communicate to Amazon S3.

Note: NCE 1.0 supports data transfer only between NetApp storage systems and Amazon Simple Storage Service.

System requirements for NCE

Before you install NCE, you must ensure that your storage system meets the system requirements.

Linux host requirements

The Linux host must meet the specific software, hardware, CPU, and memory requirements.

Software requirements

Any 64-bit Linux system installed with Oracle Java Runtime Environment (JRE) version 1.7 update 61 or later is supported.

Note: The default trust store file `cacerts`, whichis available in the `lib/security` directory of the JRE install directory. must not be deleted or be empty. If the file is deleted or is empty, communication with Amazon Web Service cannot be established.

Hardware requirements

- 2.1 GHz quad-core processor or faster
- 15-GB RAM or more (based on the memory required to run 16 concurrent data transfers to or from Amazon S3)

Storage system requirements

- Data ONTAP 8.1.4 or later
- NDMP v4 must be enabled
- NDMP service must be enabled

  On clustered Data ONTAP systems, data transfer is supported for both SVM-scoped and node-scoped NDMP modes.

Licensing requirements

NDMP Cloud Extension Software does not require any license.

Installing NCE

You can install NCE by downloading the `ndmpcopy-1.0.0.tar.gz` from the *NetApp Support Site*. You do not require any specific privilege to install this product. Any non-root user can also install this product.

1. Extract the `ndmpcopy-1.0.0.tar.gz` file to a directory in the Linux host:
   `$ tar zxvf ndmpcopy-1.0.0.tar.gz`
   An `ndmpcopy` directory is created while extracting the `tar.gz` file.
2. Go to the `ndmpcopy` directory:
   `$ cd ndmpcopy-1.0.0`
3. View the files in the `ndmpcopy` directory:
   `$ ls -l`

   The following files are displayed:

   ```
   -drwxr-xr-x 4 user engr   4096 Jan 14 05:52 aws-java-sdk-1.9.3
   -rwxr-xr-x 1 user engr    737 Jan 15 00:30 ndmpcopy
   -rwxr-xr-x 1 user engr 203124 Jan 14 05:52 ndmpcopy.jar
   -rwxr-xr-x 1 user engr   1289 Jan 14 05:52 ndmpcopysupport
   -rw-r--r-- 1 user engr    299 Jan 14 05:52 sdklog.properties
   ```
4. Edit the `ndmpcopy` script file to set the JAVA environment variable to the correct Java binary that is installed in the system.

a) View the location of the Java binary on the Linux host:

```
$ which java
```

The location of the Java binary on the Linux host is displayed:

```
/usr/bin/java
```

Note: If the Java binary location is not displayed, then the Java binary is not installed or is incorrectly installed. In this case, you must install Java. For details, see *Java for Linux Platforms.* While installing the Java binary, you must ensure that the installed version is 1.7_61 or above.

b) Verify the installed Java binary version:

```
$ java -version
```

c) After installing the Java binary, copy the Java binary location path to set the `JAVA` environment variable in the `ndmpcopy` script file.

5. Provide access permission to the `ndmpcopy` file:
   `$ chmod +x ndmpcopy`

Privilege levels for NCE operations

NCE supports two privilege levels of operations, the `admin` mode and the `advanced` mode.

The `admin` mode is the default mode and you can perform all the operations using this mode. However, `advanced` mode commands must be performed only when directed by NetApp personnel.

Configuring NCE to communicate to Amazon S3

You must create a configuration file to transfer data between storage systems and Amazon S3 by using the `-cloudconf <config file>` option with the `ndmpcopy` command. NCE deletes the configuration file after every transfer. However, you can retain the configuration file by using the `nodeleteconf` option.

1. Create a configuration file using a text editor of your choice.
   `vi <config_file.conf>`

   For example, `aws.conf`

2. Enter the following mandatory parameters in the configuration file.

```
SECRET_KEY=<value>
ACCESS_KEY=<value>
REGION_NAME=<value>
```

The following table lists the details of the NCE configuration file parameters.

"*" indicates mandatory parameters.

Parameter	Valid values	Description
ACCESS_KEY*		This parameter is supplied by Amazon for S3
SECRET_KEY*		This parameter is supplied by Amazon for S3.
REGION_NAME*	• US_EAST_1 (US Standard) • US_WEST_2 (US West - Oregon) • US_WEST_1 (US West -N. California) • EU_WEST_1 (EU Ireland) • EU_CENTRAL_1 (EU Frankfurt) • AP_SOUTHEAST_1 (Asia Pacific -Singapore) • AP_SOUTHEAST_2 (Asia Pacific -Sydney) • AP_NORTHEAST_1 (Asia Pacific -Tokyo) • SA_EAST_1 (South America -Sao Paulo)	Regions that are supported by NCE
PROTOCOL	HTTP or HTTPS The default value is HTTPS.	Allows you to choose either HTTP or HTTPS while connecting to Amazon S3

CONNECTION_TIMEOUT_MSECS	Default value: 300000 milliseconds (ms)	Overrides the default timeout value while establishing a new connection to Amazon S3
SOCKET_TIMEOUT_MSECS	Default value: 300000 milliseconds (ms)	Overrides the default timeout value for reading from a connected socket
MAX_RETRIES	Default value: 3	Overrides the default retry count for retry-able errors
ABORT_RESTORE_ON_CHECKSUM_ERROR	YES or `NO` Default value: `NO`	Aborts data transfer from Amazon S3 to the storage system if there is a checksum mismatch
DISABLE_RESTORE_CHECKSUM	YES or `NO` Default value: `NO`	Disables the checksum upload during data transfer to Amazon S3
BKP_SEG_SIZE_IN_MB	64 MB to 65536 MB Default value: 16384 MB (16 GB)	Specifies the image segmentation size
TCP_WINDOW_SIZE_IN_KB	Default value: 1024	Specifies the TCP window size setting for the data connection between the storage system and NCE. However, the effective window size is dependent on the maximum window size supported by the host platform. **Note**: The TCP window size can impact the system performance.
PROXY_HOST	For example: `192.0.2.1`	IP address of the proxy server
PROXY_PORT	For example: `88`	Port number of the proxy server
PROXY_USER	For example: `user1`	User name for the proxy server.
PROXY_PASSWORD		Password of the proxy server user

Example of an NCE configuration file:

```
$ cat aws.conf
ACCESS_KEY=xxxxxxxxxxxx
SECRET_KEY=xxxxxxxxxxxxxxxx
REGION_NAME=US_EAST_1
PROTOCOL=HTTPS
CONNECTION_TIMEOUT_MSECS=500000
SOCKET_TIMEOUT_MSECS=500000
MAX_RETRIES=4
ABORT_RESTORE_ON_CHECKSUM_ERROR=YES
BKP_SEG_SIZE_IN_MB=1024
TCP_WINDOW_SIZE_IN_KB=2048
PROXY_HOST=192.0.2.1
PROXY_PORT=88
PROXY_USER=user
PROXY_PASSWORD=xxxxxxx
```

Creating the ndmpcopy metaconfiguration file

You can create a metaconfiguration file named `ndmpcopy.cfg` if you want to change the default behavior of NCE. You must create the file in the `.ndmpcopy` directory of the user's home directory.

1. Create a metaconfiguration file using a text editor of your choice.
   ```
   vi ndmpcopy.cfg
   ```

   You can override the default behavior by setting the parameters listed in the following table:

Parameter	Description
METADATA_PATH	Directory path for the metadata file (`ndmpcopy.dat`) location. The metadata file stores information such as data transfer between a particular source and a destination, the time stamp, and the level of transfers. The default location is the user's home directory.
METADATA_FILE_SIZE_LIMIT	Metadata file size limit in bytes. The default file

Parameter	Description
	size limit is 10 MB.
LOG_DIR	Directory path for the log file created for every NCE operation. The default location is the `ndmpcopylog` directory in the user's home directory.
DATA_PORT_RANGE *<startport>-<endport>*	Specifies the local data port that is used when establishing a data connection between the NDMP server and NCE. The startport value must be less than the endport value. By default, any available port is used.
DATA_CONNECT_IP *<ip address string>*	Specifies the local IP address that is used when establishing a data connection between the NDMP server and NCE. By default, any available IP address is used.

Example of a metaconfiguration file:

```
myhost>cat ~/.ndmpcopy/ndmpcopy.cfg
LOG_DIR=/user/logpath/
METADATA_FILE_SIZE_LIMIT=15 MB
METADATA_PATH=/home1
DATA_PORT_RANGE=5080-5989
```

Transferring data between storage systems and Amazon S3

You can transfer data between Data ONTAP storage systems and the Amazon Simple Storage Service (Amazon S3) by using the `ndmpcopy` command. Data transfer is supported at the volume, qtree, directory, and file levels.

You can transfer data from the storage system to Amazon S3 using baseline, incremental, and incremental forever transfer methods:

- Baseline transfer: Transfers all the data from the source to the destination.
- Incremental transfer: Transfers only the data that has changed since the previous transfer. You must specify a level for the transfer that is higher than the previous level of transfer.
- Incremental forever transfer: Transfers only the data that has changed since the previous transfer. Each incremental forever transfer uses the previous incremental as the baseline for the current data transfer. The transfer is not limited to any specific level.

If data transfer to Amazon S3 is terminated due to an automatic or manual abort, the objects that are created in Amazon S3 until that time are also automatically deleted.

What a backup set is

A baseline and subsequent incremental data transfer of a volume from storage systems to Amazon S3 storage is collectively termed as a backup set. You must choose a unique string referred to as a backup set identifier for a given backup set. The backup set identifier, along with the level of transfer, is used to uniquely identify and store backup objects on Amazon S3.

You must specify a Data ONTAP system as the source, and Amazon Web Service (AWS) S3 and the backup set identifier string as the destination for data transfer to Amazon S3.

AWS S3 is specified by using the keyword `awss3` as the address. The address must be followed by the bucket name and the backup set identifier. The bucket name and the backup set identifier must be separated by `#`. The AWS S3 bucket must be created by the administrator before it is provided as an endpoint to NCE.

Each successful data transfer from the storage system to Amazon S3 creates data and metadata objects on the Amazon S3 storage. The backup stream is stored on the Amazon S3 storage as one or more data backup objects. Each data object represents a segment of the backup image. The default size of each segment object is 16 GB. You can override the default size by setting the `BKP_SEG_SIZE_IN_MB` property in the NCE configuration file.

Transferring data to Amazon S3

You can transfer data from the storage system to AWS S3 using baseline, incremental, and incremental forever transfer. You must specify the path of a volume, qtree, file, or directory on the Data ONTAP system as the source for the data transfer, and the Amazon S3 bucket and backup set identifier as the destination.

- **Performing a baseline transfer to Amazon S3 (admin mode)**

  Command syntax:

  ```
  ndmpcopy -l <level> -sa <username>:<password> -cloudconf
  <conffile> <host_name>:/<vol_path>
  awss3:<bucketname>#<backupsetid>
  ```

  Example:

  ```
  myhost>ndmpcopy -l 0 -sa admin1:***** -cloudconf ./aws.conf
  remotehost1:/vserver1/mybackupvol awss3:ndmpbucket#mybackup
  ```

- **Performing an incremental transfer to Amazon S3 (admin mode)**

  Command syntax:

  ```
  ndmpcopy –l <level> -sa <username>:<password> -cloudconf
  <conffile> <host_name>:/<vol_path>
  awss3:<bucketname>#<backupsetid>
  ```

  Example:

  ```
  myhost>ndmpcopy -l 1 -sa admin1:***** -cloudconf ./aws.conf
  remotehost1:/vserver1/mybackupvol awss3:ndmpbucket#mybackup
  ```

- **Performing an incremental forever transfer to Amazon S3 (advanced mode)**

  You must set the system property, `ndmpcopy.mode` to `advanced` in the `ndmpcopy` script file. For more details, see *Privilege levels for NCE operations*.

  Note: A baseline transfer using the "-l 0" is necessary before invoking incremental-forever transfers.

  Command syntax:

  ```
  ndmpcopy -i -sa <username>:<password> -cloudconf <conffile>
  <host_name>:/<vol_path> awss3:<bucketname>#<backupsetid>
  ```

  Example:

  ```
  myhost>ndmpcopy -i -sa admin1:***** -cloudconf ./aws.conf
  remotehost1:/vserver1/mybackupvol awss3:ndmpbucket#mybackup
  ```

- **Transferring data using Snapshot copies to Amazon S3 (admin mode)**

  Command syntax:

  ```
  ndmpcopy -l <level> -sa <username>:<password> -cloudconf
  <conffile>host:/<vol_path>/.snapshot/<snapname>
  awss3:<bucketname>#<backupsetid>
  ```

  Example:

  ```
  myhost>ndmpcopy -l 0 -sa admin1:****- cloudconf ./aws.conf
  remotehost1:/vserver1/mybackupvol/.snapshot/snapshotname1
  awss3:ndmpbucket#mybackup
  ```

At the end of a data transfer operation, the `ndmpcopy` command displays the approximate number of HTTP requests, such as GET, PUT, POST, HEAD, which are sent during the transfer.

Retrieving data from Amazon S3

You can retrieve data from the baseline or incremental data backup sets. You must specify the path of a volume, qtree, file, or directory on the Data ONTAP system as the destination, and the Amazon S3 bucket and backup set identifier as the source for retrieving data from the cloud.

- **Performing a baseline transfer from Amazon S3 (admin mode)**

  Command syntax:

  ```
  ndmpcopy –l <level> -da <username>:<password> -cloudconf
  <conffile> awss3:<bucketname>#<backupsetid>
  <host_name>:/<vol_path>
  ```

  Example:

  ```
  myhost> ndmpcopy –l 0 –da admin1:***** -cloudconf ./aws.conf
  awss3:ndmpbucket#mybackup remotehost1:/vserver1/myrestore
  ```

- **Performing an incremental transfer from Amazon S3 (admin mode)**

  Command syntax:

  ```
  ndmpcopy –l <level> -da <username>:<password> -cloudconf
  <conffile> awss3:<bucketname>#<backupsetid>
  <host_name>:/<vol_path>
  ```

  Example:

  ```
  myhost> ndmpcopy –l 1 –da admin1:***** -cloudconf ./aws.conf
  awss3:ndmpbucket#mybackup remotehost1:/vserver1/myrestore
  ```

- **Performing an incremental forever transfer from Amazon S3 (advanced mode)**

  You must set the system property, `ndmpcopy.mode` to `advanced` in the `ndmpcopy` script file. For more details, see *Privilege levels for NCE operations*.

  Note: A baseline transfer using the "-l 0" is necessary before invoking incremental-forever transfers.

  Command syntax:

  ```
  ndmpcopy -i -da <username>:<password> -cloudconf <conffile>
  awss3:<bucketname>#<backupsetid> <host_name>:/<vol_path>
  ```

  Example:

  ```
  myhost>ndmpcopy -i -da admin1:***** -cloudconf ./aws.conf
  awss3:ndmpbucket#mybackup remotehost1:/vserver1/myrestore
  ```

Viewing backup set summary

You can view the backup set summary information such as the backup engine, IP address, level of the backup, host name, and backup path, by using the `-describe` option.

Command syntax:

```
ndmpcopy –describe -cloudconf  <conffile>
awss3:<bucketname>#<backupsetid>
```

Example:

```
myhost> ndmpcopy –describe -cloudconf ./aws.conf
awss3:ndmpbucket#mybackup
```

Deleting a backup set

You can delete an Amazon S3 backup set identifier from an Amazon S3 bucket if you no longer want to retain it.

During a backup set deletion, only the backup objects are deleted. The Amazon S3 bucket and the bucket properties are not deleted.

Command syntax:

```
ndmpcopy –delete all -cloudconf <conffile>
awss3:<bucketname>#<backupsetid>
```

Example:

```
myhost> ndmpcopy –delete all -cloudconf ./aws.conf
awss3:ndmpbucket#mybackup
```

How NCE verifies data integrity

During data transfer from the storage system to Amazon S3, NCE uses MD5 checksum-based verification to verify whether the data that is transferred from the storage system and received by the Amazon S3 network is the same. The integrity of the data is also verified while retrieving the data from the Amazon S3 network.

- Integrity check during data transfer to Amazon S3:

If data transfer to Amazon S3 fails due to a checksum error, NCE retries to transfer the data. The default retry count is 3, after which the transfer is terminated. You can override the default retry limit by setting the MAX_RETRIES parameter in the NCE configuration file.

- Integrity check during data transfer from Amazon S3:
  While transferring data to Amazon S3, NCE associates a checksum to each of the data objects. The data object size is determined by setting the parameter BKP_SEG_SIZE_IN_MB in the NCE configuration file. These checksums are used to validate the integrity of the data received from Amazon S3. If there is a mismatch in the checksum value between the data that is transferred and received, a warning message is displayed and the data is transferred. You can also abort data transfer on a checksum mismatch by setting the parameter ABORT_RESTORE_ON_CHECKSUM_ERROR to YES in the NCE configuration file.

Parameters for the ndmpcopy command

Option	Description
`-sa username:password`	Authenticates the ndmpcopy connections to the source node of the storage system. If the option is used, the user name must be followed by a colon (:) even if the password is not included. Password should be left blank if the password is not configured for the user name on the source node.
`-da username:password`	Authenticates the `ndmpcopy` connections to the destination node of the storage system. If the option is used, the user name must be followed by a colon (:) even if the password is not included. Password should be left blank if the password is not configured for the user name on the destination node.
`-st { text | md5 }`	The source node authentication type is used to identify the authentication mechanism. MD5 is the default authentication type used. The MD5 authentication exchanges the user name and password in encrypted form. The text authentication exchanges the user name and password in clear text.
`-dt { text | md5 }`	The destination node authentication type is used to identify the authentication mechanism. MD5 is the default authentication type used. The MD5

Option	Description
	authentication exchanges the user name and password in encrypted form. The text authentication exchanges the user name and password in clear text.
`-l { 0 - 9 }`	The incremental level used for the transfer is in the range from 0 through 9. The default level used is 0. You can perform a level 0 transfer at any time, after which you can sequentially perform one incremental level, from level 1 through level 9 transfer.
`-d`	The debug mode option allows NCE to generate diagnostic or debugging information while it runs. For more details, see *NCE log files*.
`-df <filename>`	The debug to file option allows NCE to generate diagnostic or debugging information that is sent only to the specified log file. For more details, see *NCE log files*.
`<vol_path>`	Volume path used during data transfer The <vol_path> should be in either of the following formats: • For a 7-Mode volume: `/vol/<volume_name>` • For a clustered Data ONTAP volume: `/<vserver>/<volume_name>`
`-p`	Prompts for passwords so that they are not displayed on the screen
`-h`	Displays the usage and help message
`-v`	Displays the version of ndmpcopy
`-cloudconf <path>`	Used if the source or destination is cloud storage
`-describe` `<cloud storage path>`	Provides the summary of the backups for a given backup set identifier
`-delete all` `<cloud storage path>`	Deletes all the backup images for a given backup set identifier
`-delete-force all` `<cloud storage path>`	Deletes all the backup images for a given backup set identifier. This option does not prompt you for confirmation.
`-i` `<Incremental forever>`	This advance mode option cannot be used along with –l level option (1 through 9). A baseline transfer must be performed before using this option.
`-e` `<var=value>[,<var=value>[...]]`	This advance mode option sends the specified environment variables to the NDMP server.

What the ndmpcopy metadata file contains

A metadata file `ndmpcopy.dat` is created under the `.ndmpcopy` directory in the user's home directory. The `.ndmpcopy` directory is created if it does not already exist. The ndmpcopy metadata file is created whenever there is data transfer between the source and the destination. The metadata file stores information such as data transfer between a particular source and a destination, time stamp, and the level of transfer. This information is required to enable incremental ndmpcopy data transfer from storage systems to Amazon S3.

The size limit of the metadata file is 10 MB. If the size of the file exceeds the limit, new additions cannot be made to the file.

NCE log files

All data transfer operations are logged by default, including the console log messages. You can enable detailed logging using the options `–d` or `–df.`

The ndmpcopy logs are available in the `ndmpcopylog` directory in the user's home directory. The default log directory can be changed by setting the appropriate property in the ndmpcopy metaconfig file named `ndmpcopy.cfg.`

NCE uses AWS SDK. The SDK logging is controlled by modifying the appropriate properties in the `sdklog.properties` file available in the install directory.

The properties such as `com.amazonaws.request.level` and `com.amazonaws.level` are available in the `sdklog.properties` file that controls the SDK log levels.

The following values can be set for the SDK log levels:

```
SEVERE
WARNING
INFO
FINE
FINER
FINEST
```

The properties are set to `WARNING` by default. When a severity level is specified, all log messages of that severity level and higher are logged. For example, specifying the level `FINE` enables `INFO`, `WARNING`, and `SEVERE` log messages.

Known problems and limitations

You must be aware of the known issues in NDMP Cloud Extension Software (NCE) and workarounds for each of the issues, so that you can use it more effectively.

- NCE is not supported on multi-homed hosts.
  When the host has multiple IP addresses on different subnets (for example, only a few of the IP addresses are configured to access Amazon S3), it is not possible to instruct NCE to choose a local IP address that allows access to Amazon S3. As a result, NCE is not supported on such multi-homed hosts.
- NCE does not support client side encryption.
  Data that is stored on Amazon S3is not encrypted by NCE. The data stream generated by the storage system is stored as it is on Amazon S3.

For more information about the bugs in this release of NCE, see Bugs Online on the NetApp Support Site at *mysupport.netapp.com/NOW/cgi-bin/bol*.

Where to find additional information

Additional documentation is available for setting up NDMP when using the NDMP Cloud Extension Software and also for using the NDMP Cloud Extension Software with Amazon Web Services.

NDMP Configuration Express Guide: Describes how to quickly configure a Data ONTAP 8.3 cluster to use the Network Data Management Protocol (NDMP) to back up data using a third-party backup application.

Technical Report TR-4388: NDMP Cloud Extension Software Best Practices Guide: Describes best practices when using the NDMP Cloud Extension Software with Amazon Web Services.

Copyright information

Copyright © 1994–2015 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, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277