



XCPロギング

XCP

NetApp
January 22, 2026

目次

XCPロギング	1
logconfigオプションを設定します。	1
eventlogオプションを設定する	1
NFSおよびSMBのイベントメッセージ用のJSONの設定	2
syslogクライアントを有効にする	3
NFSおよびSMB用のsyslogクライアントの設定	3
syslogオプション	4
syslogメッセージの形式	4

XCPロギング

logconfigオプションを設定します。

のlogconfigオプションの詳細については、 `xcpLogConfig.json` XCP NFSおよびSMB用のJSON構成ファイル。

次の例は、「logconfig」オプションを使用して設定されたJSON構成ファイルを示しています。

• 例 *

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

- この設定では、有効なレベル値を選択することで、重大度に基づいてメッセージをフィルタリングできます。CRITICAL、ERROR、WARNING、INFO`および`Debug。
- 。 maxBytes を設定すると、ローテーションログファイルのファイルサイズを変更できます。デフォルトは50MBです。値を0に設定するとローテーションが停止し、すべてのログに対して1つのファイルが作成されます。
- 。 name オプションは、ログファイルの名前を設定します。
- キーと値のペアが見つからない場合は、デフォルト値が使用されます。既存のキーの名前を誤って指定した場合、そのキーは新しいキーとして扱われ、システムの動作やシステムの機能には影響しません。

eventlogオプションを設定する

XCPはイベントメッセージングをサポートしています。イベントメッセージングは、eventlog のオプションを選択します `xcpLogConfig.json` JSON構成ファイル。

NFSの場合、すべてのイベントメッセージがに書き込まれます。 `xcp_event.log` デフォルトの場所のいずれかにあるファイル `/opt/NetApp/xFiles/xcp/` または、次の環境変数を使用して設定されたカスタムの場所。

`XCP_CONFIG_DIR`



両方のロケーションが設定されている場合、 `XCP_LOG_DIR` を使用します。

SMBの場合は、すべてのイベントメッセージがファイルに書き込まれます。 `xcp_event.log` デフォルトの場所にあります。 `C:\NetApp\XCP\`。

NFSおよびSMBのイベントメッセージ用のJSONの設定

次の例では、JSON構成ファイルを使用してNFSおよびSMBのイベントメッセージを有効にしています。

eventlog オプションを有効にしたJSON構成ファイルの例

```
{
  "eventlog": {
    "isEnabled": true,
    "level": "INFO"
  },
  "sanitize": false
}
```

eventlog およびその他のオプションを有効にしたJSON構成ファイルの例

```
{
  "logConfig": {
    "level": "INFO",
    "maxBytes": 52428800,
    "name": "xcp.log"
  },
  "eventlog": {
    "isEnabled": true,
    "level": "INFO"
  },
  "syslog": {
    "isEnabled": true,
    "level": "info",
    "serverIp": "10.101.101.10",
    "port": 514
  },
  "sanitize": false
}
```

次の表に、eventlogサブオプションとその概要を示します。

サブオプション	JSON データ型	デフォルト値	説明
isEnabled	ブール値	いいえ	このブーリアンオプションは、イベントメッセージングを有効にするために使用されます。falseに設定すると、イベントメッセージは生成されず、イベントログファイルには公開されません。
level	文字列	情報	イベントメッセージの重大度フィルタレベル。イベントメッセージングでは、重大度の低い順に5つの重大度レベル（CRITICAL、ERROR、WARNING、INFO、DEBUG）がサポートされます。

NFSイベントログメッセージのテンプレート

次の表に、NFSイベントログメッセージのテンプレートと例を示します。

テンプレート	例
<code><Time stamp> - <Severity level> {"Event ID": <ID>, "Event Category":<category of xcp event log>, "Event Type": <type of event log>, "ExecutionId": < unique ID for each xcp command execution >, "Event Source": <host name>, "Description": <XCP event log message>}</code>	<code>2020-07-14 07:07:07,286 - ERROR {"Event ID": 51, "Event Category": "Application failure", "Event Type": "No space left on destination error", " ExecutionId ": 408252316712, "Event Source": "NETAPP-01", "Description": "Target volume is left with no free space while executing : copy {}. Please increase the size of target volume 10.101.101.101:/cat_vol"}</code>

EventLogメッセージのオプション

イベントログメッセージには、次のオプションを使用できます。

- Event ID:各イベントログメッセージの一意の識別子。
- Event Category: イベントタイプとイベントログメッセージのカテゴリについて説明します。
- Event Type: イベントメッセージを説明する短い文字列です。1つのカテゴリに複数のイベントタイプを含めることができます。
- Description: 概要フィールドには、XCPによって生成されたイベントログメッセージが含まれます。
- ExecutionId:実行される各XCPコマンドの一意の識別子。

syslogクライアントを有効にする

XCPは、Syslogクライアントをサポートして、NFSおよびSMBのリモートSyslogレシーバにXCPイベントログメッセージを送信します。デフォルトポート514を使用するUDPプロトコルをサポートします。

NFSおよびSMB用のsyslogクライアントの設定

syslogクライアントを有効にするには、syslog オプション xcpLogConfig.json NFSおよびSMBの構成ファイル。

次に、NFSおよびSMB用のsyslogクライアントの設定例を示します。

```
{
  "syslog":{
    "isEnabled":true,
    "level":"INFO",
    "serverIp":"10.101.101.d",
    "port":514
  },
  "sanitize":false
}
```

syslogオプション

次の表に、syslogのサブオプションとその概要を示します。

サブオプション	JSON データ型	デフォルト値	説明
isEnabled	ブール値	いいえ	このブーリアンオプションは、XCPでSyslogクライアントをイネーブルにします。に設定します falseを指定すると、syslog設定は無視されます。
level	文字列	情報	イベントメッセージの重大度フィルタレベル。イベントメッセージングでは、重大度の低い順に5つの重大度レベル（CRITICAL、ERROR、WARNING、INFO、DEBUG）がサポートされます。
serverIp	文字列	なし	このオプションは、リモートsyslogサーバのIPアドレスまたはホスト名をリストします。
port	インテガー	514	このオプションは、リモートsyslogレシーバポートです。このオプションを使用すると、別のポートでsyslogデータグラムを受け入れるようにsyslogレシーバを設定できます。 デフォルトのUDPポートは514です。



。 sanitize 「syslog」 設定でオプションを指定しないでください。このオプションはグローバルに適用され、JSON構成内のロギング、イベントログ、syslogに共通です。この値を「true」に設定すると、syslogサーバに送信されるsyslogメッセージの機密情報が非表示になります。

syslogメッセージの形式

UDP経由でリモートsyslogサーバに送信されるすべてのsyslogメッセージは、NFSおよびSMBのRFC 5424形式に従ってフォーマットされます。

次の表に、XCPのsyslogメッセージでサポートされるRFC 5424に従って重大度を示します。

シユウタイトチ	重大度レベル
3.	ERROR：エラー状態
4.	WARNING：警告状態

シユウタイトチ	重大度レベル
6.	INFORMATIONAL：情報メッセージ
7.	DEBUG：デバッグレベルのメッセージ

NFSおよびSMBのsyslogヘッダーでは、versionの値は1で、XCPのすべてのメッセージのファシリティの値は1（ユーザレベルのメッセージ）に設定されています。

<PRI> = syslog facility * 8 + severity value

NFSのsyslogヘッダーを含むXCPアプリケーションsyslogメッセージ形式：

次の表に、NFSのsyslogヘッダーを含むsyslogメッセージ形式のテンプレートと例を示します。

テンプレート	例
<PRI><version> <Time stamp> <hostname> xcp_nfs - - - <XCP message>	<14>1 2020-07-08T06:30:34.341Z netapp xcp_nfs - - - INFO {"Event ID": 14, "Event Category": "XCP job status", "Event Type": "XCP scan completion", "Event Source": "netapp", "Description": "XCP scan is completed by scanning 8 items"}

NFSのsyslogヘッダーなしのXCPアプリケーションメッセージ

次の表に、NFSのsyslogヘッダーなしのsyslogメッセージ形式のテンプレートと例を示します。

テンプレート	例
<message severity level i.e CRITICAL, ERROR, WARNING, INFO, DEBUG> <XCP event log message>	INFO {"Event ID": 14, "Event Category": "XCP job status", "Event Type": "XCP scan completion", "Event Source": "netapp", "Description": "XCP scan is completed by scanning 8 items"}

SMBのsyslogヘッダーを含むXCPアプリケーションsyslogメッセージ形式

次の表に、SMBのsyslogヘッダーを含むsyslogメッセージ形式のテンプレートと例を示します。

テンプレート	例
<PRI><version> <Time stamp> <hostname> xcp_smb - - - <XCP message>	<14>1 2020-07-10T10:37:18.452Z bansala01 xcp_smb - - - INFO {"Event ID": 14, "Event Category": "XCP job status", "Event Type": "XCP scan completion", "Event Source": "NETAPP- 01", "Description": "XCP scan is completed by scanning 17 items"}

SMBのsyslogヘッダーなしのXCPアプリケーションメッセージ

次の表に、SMBのsyslogヘッダーがないsyslogメッセージの形式のテンプレートと例を示します。

テンプレート	例
<code><message severity level i.e CRITICAL, ERROR, WARNING, INFO, DEBUG> <XCP event log message></code>	<code>NFO {"Event ID": 14, "Event Category": "XCP job status", "Event Type": "XCP scan completion", "Event Source": "NETAPP-01", "Description": "XCP scan is completed by scanning 17items"}</code>

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。