



XCP 로깅

XCP

NetApp
May 21, 2024

목차

XCP 로깅	1
logConfig 옵션을 설정합니다	1
EventLog 옵션을 설정합니다	1
syslog 클라이언트를 활성화합니다	3

XCP 로깅

logConfig 옵션을 설정합니다

의 logConfig 옵션에 대해 알아봅니다 xcpLogConfig.json XCP NFS 및 SMB용 JSON 구성 파일입니다.

다음 예제는 "logConfig" 옵션이 포함된 JSON 구성 파일 세트를 보여줍니다.

- 예 *

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

- 이 구성을 사용하면 에서 유효한 수준 값을 선택하여 심각도에 따라 메시지를 필터링할 수 있습니다 CRITICAL, ERROR, WARNING, INFO, 및 Debug.
- 를 클릭합니다 maxBytes 설정을 사용하면 회전 로그 파일의 파일 크기를 변경할 수 있습니다. 기본값은 50MB입니다. 값을 0으로 설정하면 회전이 중지되고 모든 로그에 대해 단일 파일이 생성됩니다.
- 를 클릭합니다 name 옵션은 로그 파일의 이름을 구성합니다.
- 키 값 쌍이 누락된 경우 시스템은 기본값을 사용합니다. 기존 키의 이름을 잘못 지정하는 경우 새 키로 처리되며 새 키는 시스템 작동 방법이나 시스템 기능에 영향을 주지 않습니다.

EventLog 옵션을 설정합니다

XCP는 를 사용하여 활성화할 수 있는 이벤트 메시징을 지원합니다 eventlog 의 옵션 xcpLogConfig.json JSON 구성 파일.

NFS의 경우 모든 이벤트 메시지가 에 기록됩니다 xcp_event.log 파일이 기본 위치에 있습니다 /opt/NetApp/xFiles/xcp/ 또는 다음 환경 변수를 사용하여 구성된 사용자 지정 위치:

XCP_CONFIG_DIR



두 위치를 모두 설정하면 XCP_LOG_DIR 사용됩니다.

SMB의 경우 모든 이벤트 메시지가 파일에 기록됩니다 xcp_event.log 기본 위치에 있습니다 C:\NetApp\XCP\.

NFS 및 SMB용 이벤트 메시징을 위한 JSON 구성

다음 예에서는 JSON 구성 파일을 통해 NFS 및 SMB에 대한 이벤트 메시징을 지원합니다.

EventLog 옵션이 활성화된 JSON 구성 파일 예

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

EventLog 및 기타 옵션이 설정된 JSON 구성 파일 예

```
{
  "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
}
```

다음 표에서는 EventLog 하위 옵션과 해당 설명을 보여 줍니다.

하위 옵션	JSON 데이터 유형	기본값	설명
isEnabled	부울	거짓	이 부울 옵션은 이벤트 메시징을 설정하는 데 사용됩니다. false 로 설정하면 이벤트 메시지가 생성되지 않고 이벤트 로그 파일에 이벤트 로그가 게시되지 않습니다.
level	문자열	정보	이벤트 메시지 심각도 필터 수준입니다. 이벤트 메시징은 심각도가 낮은 5가지 심각도 수준(위험, 오류, 경고, 정보 및 디버그)을 지원합니다

NFS 이벤트 로그 메시지의 템플릿입니다

다음 표에서는 템플릿과 NFS 이벤트 로그 메시지의 예를 보여 줍니다.

템플릿	예
<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>	<pre>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"}</pre>

EventLog 메시지 옵션

EventLog 메시지에 사용할 수 있는 옵션은 다음과 같습니다.

- Event ID: 각 이벤트 로그 메시지의 고유 식별자입니다.
- Event Category: 이벤트 유형 및 이벤트 로그 메시지의 범주에 대해 설명합니다.
- Event Type: 이벤트 메시지를 설명하는 짧은 문자열입니다. 여러 이벤트 유형이 하나의 범주에 속할 수 있습니다.
- `Description` 설명 필드에는 XCP에서 생성한 이벤트 로그 메시지가 포함됩니다.
- ExecutionId: 실행된 각 XCP 명령에 대한 고유 식별자입니다.

syslog 클라이언트를 활성화합니다

XCP는 syslog 클라이언트를 지원하여 NFS 및 SMB용 원격 syslog 수신기로 XCP 이벤트 로그 메시지를 전송합니다. 기본 포트 514를 사용하여 UDP 프로토콜을 지원합니다.

NFS 및 SMB에 대해 syslog 클라이언트를 구성합니다

syslog 클라이언트를 활성화하려면 을 구성해야 합니다 syslog 옵션을 선택합니다 xcpLogConfig.json NFS 및 SMB에 대한 구성 파일

NFS 및 SMB용 syslog 클라이언트에 대한 다음 구성 예:

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

Syslog 옵션

다음 표에는 syslog 하위 옵션 및 설명이 나와 있습니다.

하위 옵션	JSON 데이터 유형	기본값	설명
isEnabled	부울	거짓	이 부울 옵션은 XCP에서 syslog 클라이언트를 활성화합니다. 를 로 설정합니다 false는 syslog 구성을 무시합니다.
level	문자열	정보	이벤트 메시지 심각도 필터 수준입니다. 이벤트 메시징은 심각도가 낮은 5가지 심각도 수준(위험, 오류, 경고, 정보 및 디버그)을 지원합니다
serverIp	문자열	없음	이 옵션은 원격 syslog 서버 IP 주소 또는 호스트 이름을 나열합니다.
port	인티저	514	이 옵션은 원격 syslog 수신기 포트입니다. 이 옵션을 사용하여 다른 포트에 syslog 데이터그램을 허용하도록 syslog 수신기를 구성할 수 있습니다. 기본 UDP 포트는 514입니다.



를 클릭합니다 sanitize "syslog" 구성에서 옵션을 지정하면 안 됩니다. 이 옵션은 전역 범위를 가지며 JSON config 내의 로깅, 이벤트 로그 및 syslog에 공통적으로 사용됩니다. 이 값을 "true"로 설정하면 syslog 서버에 게시된 syslog 메시지에 중요한 정보가 숨겨집니다.

Syslog 메시지 형식입니다

UDP를 통해 원격 syslog 서버로 전송되는 모든 syslog 메시지는 NFS 및 SMB에 대한 RFC 5424 형식에 따라 포맷됩니다.

다음 표는 XCP에 대한 syslog 메시지에 대해 지원되는 RFC 5424에 따른 심각도 수준을 보여 줍니다.

심각도 값	심각도 수준
3	오류: 오류 상태입니다
4	경고: 경고 상태
6	정보: 정보 메시지입니다
7	디버그: 디버그 수준 메시지

NFS 및 SMB에 대한 syslog 헤더에서 버전 값은 1이고 XCP에 대한 모든 메시지의 기능 값은 1로 설정됩니다(사용자 수준 메시지).

<PRI> = syslog facility * 8 + severity value

NFS용 syslog 헤더가 있는 **XCP** 애플리케이션 **syslog** 메시지 형식:

다음 표에는 NFS용 syslog 헤더가 있는 syslog 메시지 형식의 템플릿과 예가 나와 있습니다.

템플릿	예
<pre><PRI><version> <Time stamp> <hostname> xcp_nfs - - - <XCP message></pre>	<pre><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"}</pre>

NFS에 대한 syslog 헤더가 없는 XCP 애플리케이션 메시지입니다

다음 표에는 NFS에 대한 syslog 헤더가 없는 syslog 메시지 형식의 템플릿과 예가 나와 있습니다.

템플릿	예
<pre><message severity level i.e CRITICAL, ERROR, WARNING, INFO, DEBUG> <XCP event log message></pre>	<pre>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"}</pre>

SMB용 syslog 헤더를 사용하는 XCP 애플리케이션 syslog 메시지 형식입니다

다음 표에는 SMB용 syslog 헤더가 있는 syslog 메시지 형식의 템플릿과 예가 나와 있습니다.

템플릿	예
<pre><PRI><version> <Time stamp> <hostname> xcp_smb - - - <XCP message></pre>	<pre><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"}</pre>

SMB용 syslog 헤더가 없는 XCP 애플리케이션 메시지

다음 표에는 SMB에 대한 syslog 헤더가 없는 syslog 메시지 형식의 템플릿과 예가 나와 있습니다.

템플릿	예
<pre><message severity level i.e CRITICAL, ERROR, WARNING, INFO, DEBUG> <XCP event log message></pre>	<pre>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"}</pre>

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.