XCP 로깅

XCP

NetApp
May 21, 2024

목차

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
`<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>}`	`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"}`

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`	인티거	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
`<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"}`

NFS에 대한 **syslog** 헤더가 없는 **XCP** 애플리케이션 메시지입니다

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

템플릿	예
`<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"}`

SMB용 **syslog** 헤더를 사용하는 **XCP** 애플리케이션 **syslog** 메시지 형식입니다

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

템플릿	예
`<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"}`

SMB용 **syslog** 헤더가 없는 **XCP** 애플리케이션 메시지

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

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