XCP logging

XCP

NetApp
June 11, 2024

Table of Contents

XCP logging

Set the logConfig option

Learn about the logConfig option in the `xcpLogConfig.json` JSON configuration file for XCP NFS and SMB.

The following example shows the JSON configuration file set with the “logConfig” option:

Example

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

- With this configuration you can filter messages according to their severity by selecting a valid level value from `CRITICAL`, `ERROR`, `WARNING`, `INFO`, and `Debug`.
- The `maxBytes` setting enables you to change the file size of the rotating log files. The default is 50MB. Setting the value to 0 stops rotation and a single file is created for all logs.
- The `name` option configures the name of the log file.
- If any key value pair is missing, the system uses the default value. If you make a mistake specifying the name of an existing key, it is treated as a new key, and the new key does not affect how the systems works or system functionality.

Set the eventlog option

XCP supports event messaging, which you can enable using the `eventlog` option in the `xcpLogConfig.json` JSON config file.

For NFS, all event messages are written to the `xcp_event.log` file located in either the default location `/opt/NetApp/xFiles/xcp/` or a custom location configured using the following environment variable:

`XCP_CONFIG_DIR`

When both locations are set, `XCP_LOG_DIR` is used.

For SMB, all event messages are written to the file `xcp_event.log` located in the default location `C:\NetApp\XCP\`.

JSON configuration for event messaging for NFS and SMB

In the following examples, the JSON configuration files enable event messaging for NFS and SMB.

Example JSON configuration file with the eventlog option enabled

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

Example JSON configuration file with eventlog and other options enabled

```
{
"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
}
```

The following table shows the eventlog sub options and their description:

Sub option	JSON data type	Default value	Description
`isEnabled`	Boolean	False	This boolean option is used to enable event messaging. If set to false, it does not generate any event messages and no event logs are published to the event log file.
`level`	String	INFO	Event message severity filter level. Event messaging support five severity levels in order of decreasing severity: CRITICAL, ERROR, WARNING, INFO, and DEBUG

Template for an NFS event log message

The following table shows a template and an example for an NFS event log message:

Template	Example
`<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 message options

The following options are available for an eventlog message:

- `Event ID`: The unique identifier for each event log message.
- `Event Category`: Explains the category of event type and event log message.
- `Event Type`: This is a short string that describes the event message. Multiple event types can belong to one category.
- `Description`: The description field contains the event log message generated by XCP.
- `ExecutionId`: A unique identifier for each XCP command executed.

Enable the syslog client

XCP supports a syslog client to send XCP event log messages to a remote syslog receiver for NFS and SMB. It supports the UDP protocol using the default port 514.

Configure the syslog client for NFS and SMB

Enabling the syslog client requires configuring the `syslog` option in the the `xcpLogConfig.json` configuration file for NFS and SMB.

The following example configuration for the syslog client for NFS and SMB:

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

Syslog options

The following table shows the syslog sub options and their description:

Sub option	JSON data type	Default value	Description
`isEnabled`	Boolean	False	This Boolean option enables the syslog client in XCP. Setting it to false will ignore the syslog configuration.
`level`	String	INFO	Event message severity filter level. Event messaging support five severity levels in order of decreasing severity: CRITICAL, ERROR, WARNING, INFO, and DEBUG
`serverIp`	String	None	This option lists the remote syslog server IP addresses or hostnames.
`port`	Integar	514	This option is the remote syslog receiver port. You can configure syslog receivers to accept syslog datagrams on a different port with this option.The default UDP port is 514.

The `sanitize` option should not be specified within “syslog” configuration. This option has a global scope and is common to logging, event log, and syslog within JSON config. Setting this value to “true” will hide sensitive information in syslog messages posted to the syslog server.

Syslog message format

Every syslog messages sent to the remote syslog server over UDP is formatted as per the RFC 5424 format for NFS and SMB.

The following table shows the severity level as per RFC 5424 supported for syslog messages for XCP:

Severity values	Severity level
3	Error: error conditions
4	Warning: warning conditions
6	Informational: informational messages
7	Debug: debug-level messages

In the syslog header for NFS and SMB, version has a value of 1 and the facility value for all messages for XCP is set to 1 (user-level messages):

```
<PRI> = syslog facility * 8 + severity value
```

XCP application syslog message format with a syslog header for NFS:

The following table shows a template and example of the syslog message format with a syslog header for NFS:

Template	Example
`<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"}`

XCP application message without syslog header for NFS

The following table shows a template and example of the syslog message format without a syslog header for NFS:

Template	Example
`<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"}`

XCP application syslog message format with syslog header for SMB

The following table shows a template and example of the syslog message format with a syslog header for SMB:

Template	Example
`<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"}`

XCP application message without syslog header for SMB

The following table shows a template and example of the syslog message format without a syslog header for SMB:

Template	Example
`<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"}`

Copyright information

Trademark information