NSO 로그 및 세부사항 활성화

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

일반 로그 지침

- 로깅 영향
- 기술 보고서 생성
- 백업 생성
- 로그 파일이 생성되지 않음

로그 개요

로그 활성화 및 세부 정보 설정

- 일반 지침
- 내부
  - ncs.log
  - audit.log
  - audit-log-commit 및 audit-log-commit-defaults
  - devel.log
  - ncs-java-vm.log
  - ncs-python-vm.log
  - upgrade.log
  - raft.log
  - xpath.trace
  - ncserr.log
  - transerr.log
  - 진행률
  - ncs-smart-licensing.log
- 북행
  - localhost:xxxx.access
  - 트래픽.추적
  - netconf.log
  - netconf-trace.log
  - json-rpc.log
- 남행
  - 디바이스 NED 추적
  - audit-network.log

소개

이 문서에서는 NSO에서 사용할 수 있는 다양한 로그, 로그 사용 용도 및 로그 사용 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

로그를 보고, 활성화하고, 설정하려면 사용자가 NSO 서비스를 실행하는 호스트 환경에 대한 액세스 권한과 NSO CLI 및 NSO IPC 포트에 대한 액세스 권한이 있어야 합니다.

사용되는 구성 요소

Cisco Crosswork Network Service Orchestrator(NSO) 버전 6.4.1

이 문서는 NSO 6.4부터 제공되는 로깅 옵션을 위해 작성되었습니다. 이 문서의 대부분의 정보는 여러 버전에 적용되지만, 사용 중인 버전에 비해 일부 로그의 사용이 중단되거나 추가될 수 있습니다. 이 문서에서는 NSO 시스템 외부에서 로그를 내보내는 컨피그레이션을 다루지 않습니다.

이 문서에서 제공하는 명령은 기본 디렉토리 설정을 사용하는 시스템 설치 NSO로 가정합니다. 사용자 환경에서 특정 파일의 위치는 다를 수 있습니다.

- ncs.conf는 기본적으로 $NCS_CONFIG_DIR에서 찾을 수 있습니다. /etc/ncs/ncs.conf
- 로그는 기본적으로 $NCS_LOG_DIR에서 찾을 수 있습니다. /var/log/ncs/
- NSO는 기본적으로 $NCSDIR에 설치됩니다. /opt/ncs/
- NSO의 실행 디렉토리는 $NCS_RUN_DIR입니다. 기본적으로 /var/opt/ncs/

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

일반 로그 지침

로깅 영향

더 높은 세밀도에서 로그를 활성화하면 NSO 서버의 로드 및 디스크 공간 요구 사항이 증가할 수 있습니다. 이는 특히 devel.log와 같이 매우 활성화된 로그를 고려합니다. 트러블슈팅 중에 짧은 시간 동안 자세한 정보를 활성화하는 것은 일반적으로 문제가 되지 않지만, 더 긴 시간 동안 활성화할 때는 리소스와 디스크 공간을 고려해야 합니다.

기술 보고서 생성

To generate a tech report for NSO, run the script at **/opt/ncs/current/bin/ncs-collect-tech-report**.

옵션:

--install-dir

: 설치 프로그램에 대한 —install-dir 옵션과 같은 NCS 고정 파일의 설치 디렉토리를 지정합니다.

--full : 시스템의 ncs-backup을 수집하여 Cisco 지원에서 더 쉽게 오류를 재현할 수 있도록 합니다.

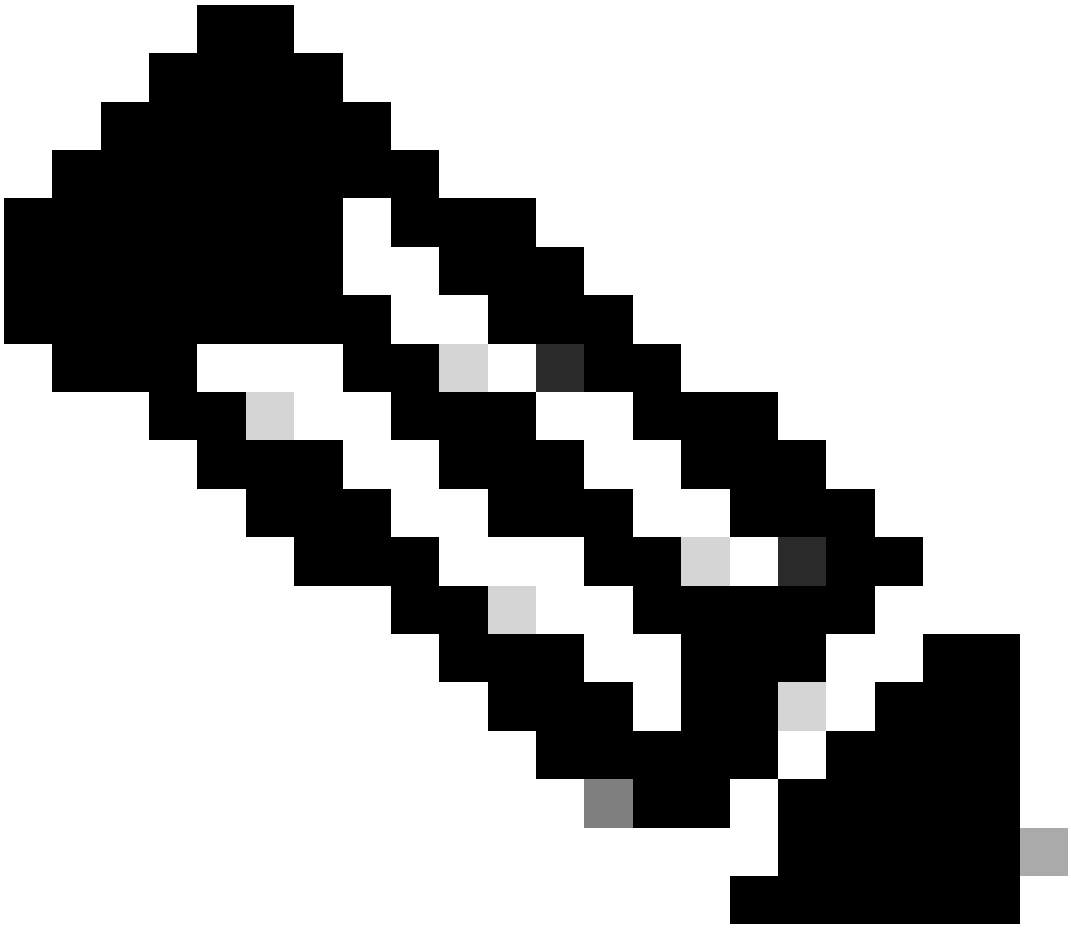
--num-debug-dumps : 기본값 1, debug-dump 스냅샷을 생성합니다. 메모리/파일 설명자 누수와 같은 리소스 누수를 추적하는 케이스의 경우 이 값을 3으로 설정합니다.

권장 옵션:

/opt/ncs/current/bin/ncs-collect-tech-report --num-debug-dumps 3

백업은 번들의 파일 크기를 제한하여 더 쉽게 업로드할 수 있도록 별도로 수집 및 제공할 수 있습니다.

기술 보고서는 스크립트가 실행되는 현재 디렉토리에 생성됩니다.



참고: 기술 보고서는 NSO 로그 디렉토리의 내용을 수집합니다. 새 기술 보고서를 생성하기 전에 이 디렉터리에 이전 기술 보고서 또는 백업이 포함되어 있지 않은지 확인하십시오.

백업 생성

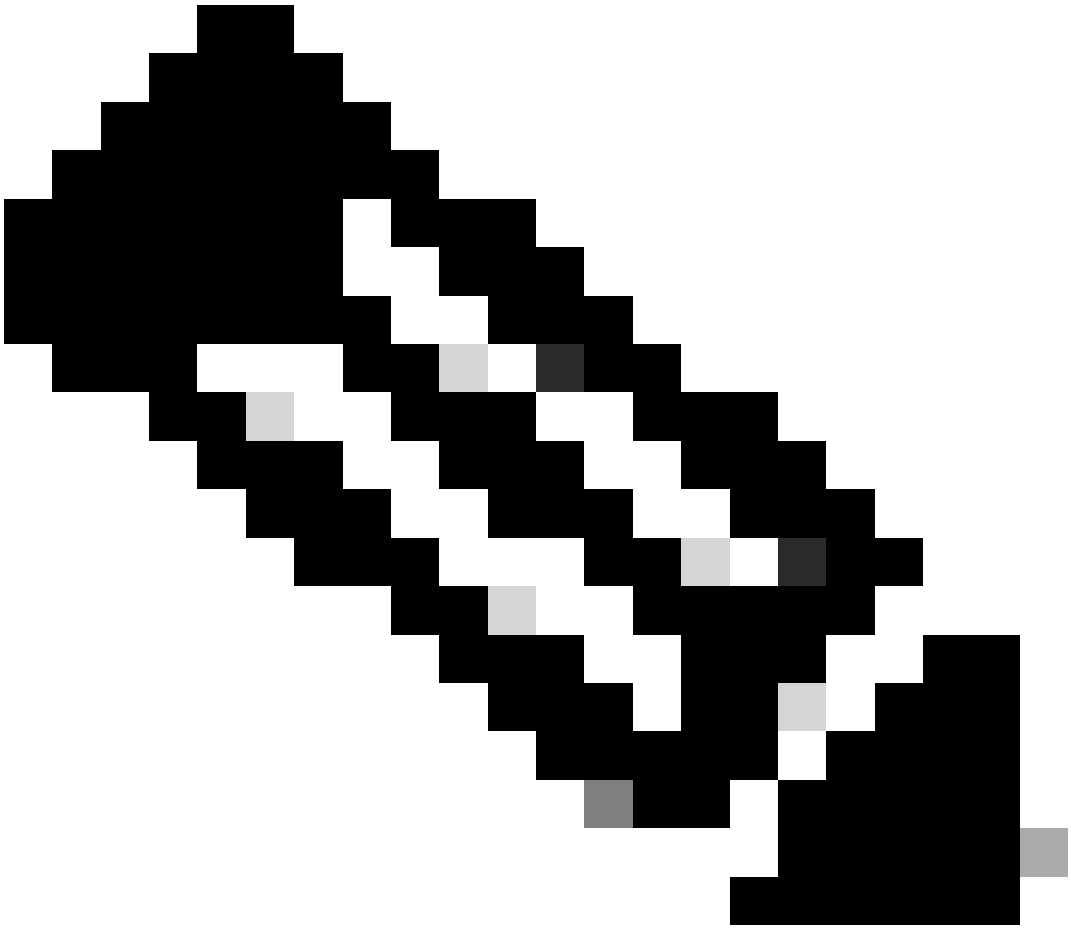
/opt/ncs/current/bin/ncs-backup

백업은 /var/opt/ncs/backups/.

로그 파일이 생성되지 않음

로그 파일이 아카이브되거나 삭제되면 NSO는 새 파일을 생성해야 합니다. 일반적으로 이 작업은 자동으로 수행되지만 그렇지 않은 경우 다음 명령을 사용합니다.

/opt/ncs/current/bin/ncs_cmd -c reopen_logs.



참고: 예를 들어 ncs.conf의 ipc-access 설정을 사용하여 IPC 포트에 대한 액세스를 제한할 때 필요한 변수를 cron 또는 anacron의 일부로 정의해야 매주 로그 순환이 로그를 제대로 다시 열 수 있습니다.

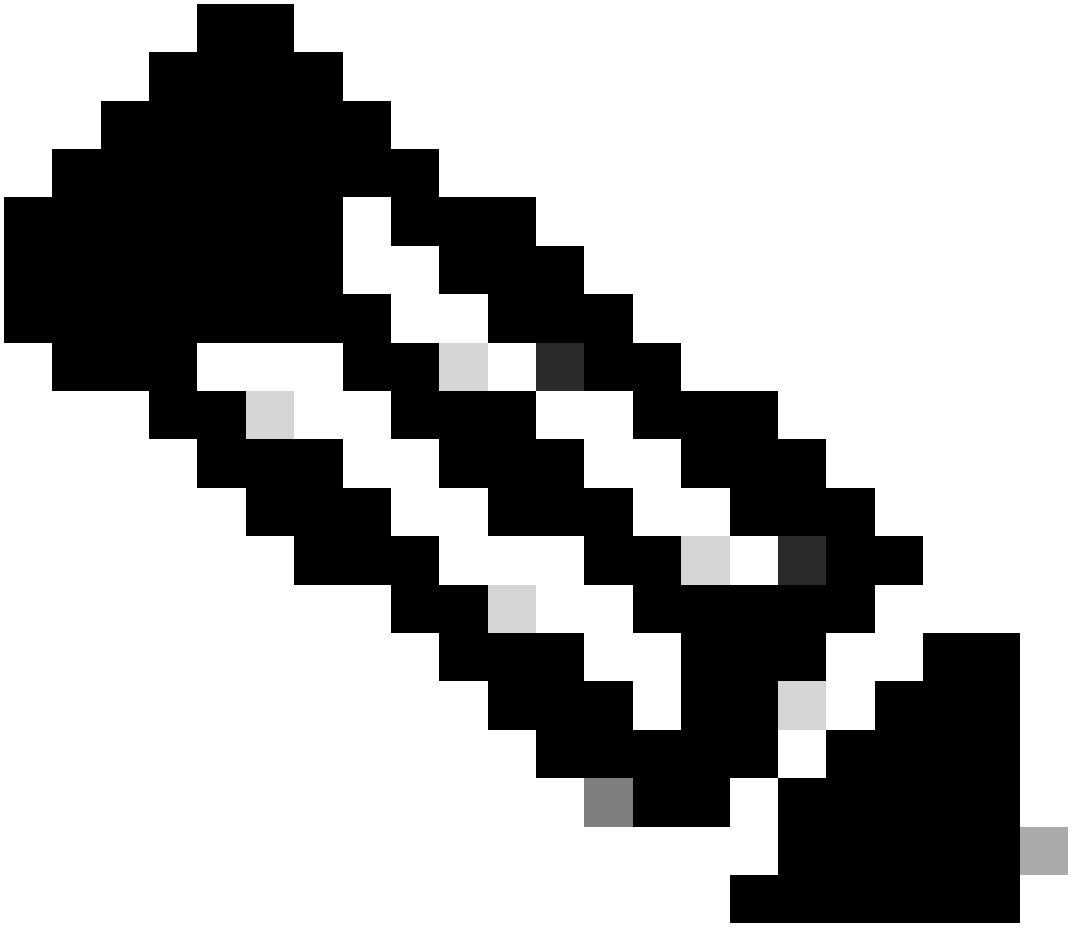
로그 개요

- NSO 내부 로그
  - ncs.log: ncs 로그는 NSO의 주요 프로세스를 기록합니다. 심층적인 정보가 제한적이지

만 종료, 시작, 패키지 로드 및 업그레이드와 관련된 문제에 사용할 수 있습니다.
    - audit.log: 감사 로그는 API를 통해 NSO에서 인증하는 모든 사용자를 기록합니다. 또한 NSO CLI 및 낮은 세밀도의 노스바운드(northbound) 인터페이스에서 모든 활동을 기록합니다.
    - audit-log-commit: 이 설정을 사용하면 audit.log가 향상됩니다. 자체 로그는 생성하지 않습니다. 커밋 및 동기화 시작 작업 중에 기본이 아닌 모든 변경 사항을 NSO CDB에 기록합니다.
    - audit-log-commit-default: 이 설정을 사용하면 audit.log가 향상됩니다. 자체 로그는 생성하지 않습니다. 커밋 및 동기화 시작 작업 중에 모든 기본 변경 사항을 NSO CDB에 기록합니다.
    - devel.log: 개발 로그는 NSO의 일반 작업 및 워크플로를 기록합니다.
    - ncs-java-vm.log: java 로그는 모든 java-vm 관련 작업을 기록합니다. 특히 Java로 작성된 NED(Network Element Driver) 및 서비스 패키지가 있습니다. 모든 CLI NED는 java로 작성됩니다.
    - ncs-python-vm.log: python 로그는 Python에 기록된 서비스 패키지와 관련된 활동을 기록합니다. python으로 작성된 각 서비스 패키지에 대해 별도의 python 로그가 생성됩니다. NED는 python으로 작성되지 않습니다.
    - upgrade.log: 업그레이드 로그는 패키지를 다시 로드하는 동안 NSO 버전 업그레이드 및 NSO 패키지 업그레이드를 포함하여 NSO 업그레이드 과정에서 NSO 모델의 변경 사항을 기록합니다.
    - raft.log: HA-Raft 기능을 활용하는 NSO 클러스터에 대한 로그
    - xpath.trace: xpath 추적은 NSO가 수행하는 모든 xpath-evaluations를 기록합니다. 이 기능은 삭제 작업에 시간이 오래 걸리는 이유를 파악하는 데 유용합니다.
    - ncserr.log: ncserr.log는 NCS 데몬의 내부 프로세스에 대한 오류를 기록하는 이진 로그입니다. 거의 모든 '내부 오류' 오류 메시지 및 충돌 시나리오에 대해 필수입니다.
    - transerr.log: transaction-error log는 CDB 부팅 오류 또는 런타임 트랜잭션 실패로 이어지는 실패한 트랜잭션에 대한 정보를 수집하기 위한 로그입니다.
    - progress.trace: 진행률 추적은 시스템의 트랜잭션 및 작업에서 내보낸 진행률 이벤트를 추적하는 데 사용됩니다. 내보낼 데이터가 /progress/trace에 구성되어 있습니다.
    - ncs-smart-licensing.log: NSO 내의 라이센스 smart-agent에 대한 로그입니다.
- 노스바운드: 노스바운드 요소에서 NSO에 도착
    - audit.log: audit log logs 명령은 NSO CLI에서 실행됩니다.
    - localhost:8080.access/localhost:8888.access : 포함된 웹 서버에 대한 액세스 로그이며 HTTP 활동을 수집합니다. 이 파일은 Apache에서 정의한 일반 로그 형식을 준수합니다
    - traffic.trace: 이 로그는 매우 높은 심각도 HTTP 트래픽을 수집합니다. Restconf 및 json-rpc API를 디버깅하는 데 사용합니다.
    - netconf.log: netconf API 로그
    - netconf-trace.log: 고밀도 netconf API에 대한 로그
    - json-rpc.log: json-rpc.log API용 로그
- 사우스바운드: NSO에서 네트워크로 이동하는 통신을 로깅하는 중입니다.
    - 디바이스 NED 추적: 각 디바이스는 자체 추적을 생성합니다. 장치 추적은 ned-<ned-id>-<devicename>.trace 또는 netconf-<devicename>.trace로 명명됩니다.
    - audit-network.log: NSO에서 사우스바운드 디바이스로 전송한 컨피그레이션 명령을 기록합니다.
- 시스템 로그
    - Linux 로그: 일반적으로 /var/log/에 있으며 메시지 또는 syslog와 같은 로그를 포함합니

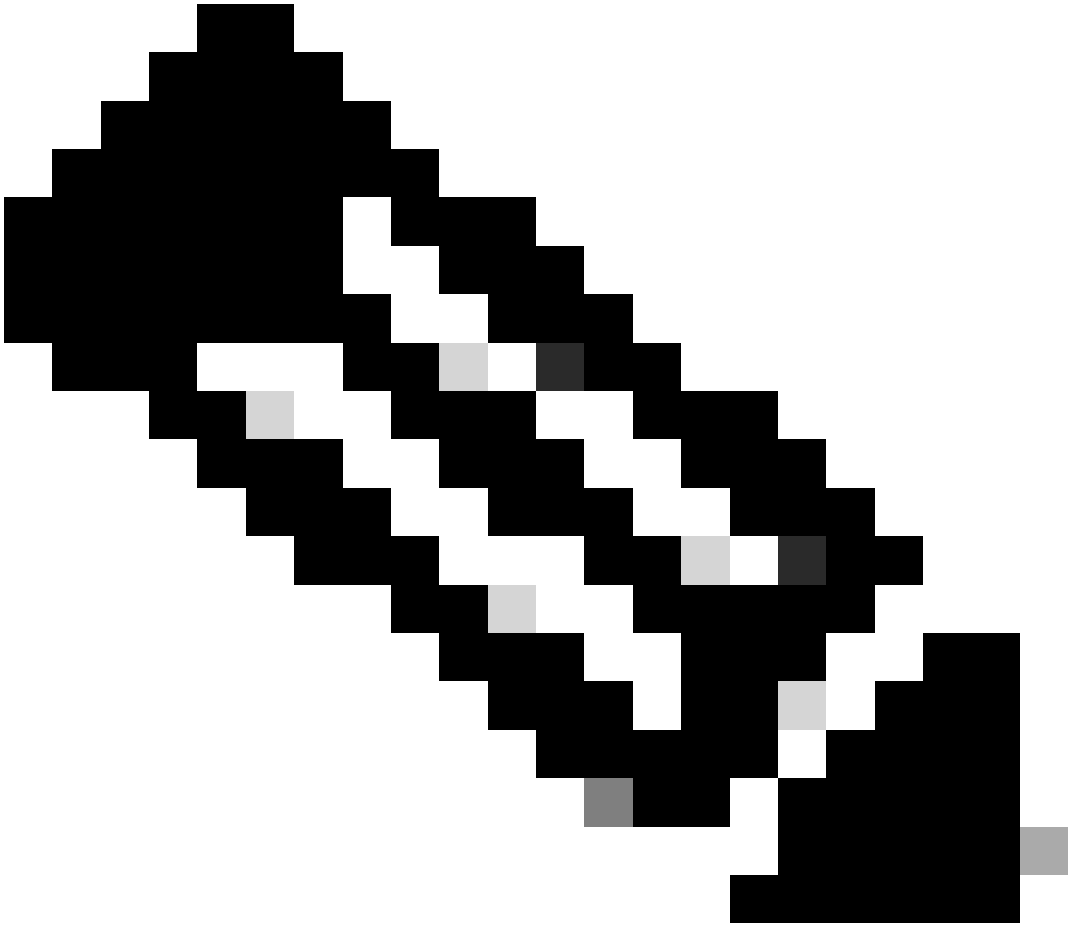
다. 호스트에 따라 다릅니다.
- ncs_crash.dump: 메모리 문제로 인해 NSO가 종료될 때 생성되는 NSO 시스템 덤프.
- 코어 덤프: 비메모리 이유로 NSO가 종료되면 Linux는 core.<PID>라는 코어 덤프를 생성할 수 있습니다.

Linux에서 코어 덤프를 생성하려면 특정 조건을 충족해야 합니다. ulimit 컨피그레이션은 덤프를 방지하는 가장 일반적인 설정입니다. 요구 사항의 전체 목록은 Linux Manual Page를 참조하십시오.



참고: 시스템 로그는 NCS 기술 보고서에서 수집되지 않지만 성능 및 충돌 관련 문제에 유용할 수 있습니다.

로그 활성화 및 세부 정보 설정



참고: ncs.conf 파일의 컨피그레이션 설정 변경은 명령을 실행하여 ncs --reload 적용합니다. ncs --reload, it ncs.conf 파일에서 값을 다시 로드하고 실행 중인 시스템을 업데이트하는 것은 물론 모든 로깅 변경 사항이 적용되도록 모든 로그 파일을 닫았다가 다시 엽니다. 서비스를 중단하지 않습니다.

일반 지침

- ncs.conf 파일에 특정 컨피그레이션이 없는 경우 NSO는 파일에 지정된 대로 기본 동작을 /opt/ncs/current/src/ncs/ncs_config/tailf-ncs-config.yang 적용합니다.
- 로그를 기본적으로 enabled로 지정하면 로그를 활성화할 컨피그레이션이 없어도 로그가 활성화됩니다.
- 일부 로그는 기본적으로 비활성화되어 있지만, NSO를 처음 설치하는 동안 ncs.conf에는 로그를 활성화하는 특정 지침이 있습니다.
- ncs.conf 파일에 특정 컨피그레이션이 없는 경우, ncs.conf 파일에 logs container및 사이를 의미하는 아래에 표시된 컨피그레이션을 추가할 수 있습니다.

내부

ncs.log

이 로그는 기본적으로 활성화되어 있습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf을 열고 <ncs-log>의 내용을 변경합니다.

```
        true

         ${NCS_LOG_DIR}/ncs.log

         true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

audit.log

이 로그는 기본적으로 활성화되어 있습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf를 열고 <audit-log>의 내용을 변경하십시오.

```
        true

        ${NCS_LOG_DIR}/audit.log

        true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

audit-log-commit 및 audit-log-commit-defaults

이 로그는 기본적으로 활성화되어 있지 않습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf을 열고 <audit-log> 다음에 내용을 추가하십시오.

```
        true

        ${NCS_LOG_DIR}/audit.log
```

```
      true
```

```
    true
```

```
    true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

devel.log

이 로그는 INFO Verbosity에서 기본적으로 활성화되어 있습니다. 이 로그에 대한 자세한 내용을 활성화 및 변경하려면 /etc/ncs/ncs.conf을 열고 <developer-log>의 내용을 변경하십시오.

```
     true
```

```
      ${NCS_LOG_DIR}/devel.log
```

```
        true
```

```
      trace
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

ncs-java-vm.log

이 로그는 INFO Verbosity에서 기본적으로 활성화되어 있습니다. java-vm으로 관리되는 개별 요소에 대한 자세한 정보를 설정할 수 있습니다. 자세한 내용은 SSH 또는 ncs_cli -C -noaaa를 통해 액세스할 수 있는 NSO CLI에서 변경됩니다.

com.tailf 아래의 모든 java 요소에 대한 자세한 정보를 보려면 다음을 수행합니다.

설정
java-vm java-logging logger com.tailf level-trace
no-networking 확인

특정 NED 패키지에 대한 자세한 내용을 보려면

설정

java-vm java-logging logger com.tailf.packages.ned.<NED-name> level-trace

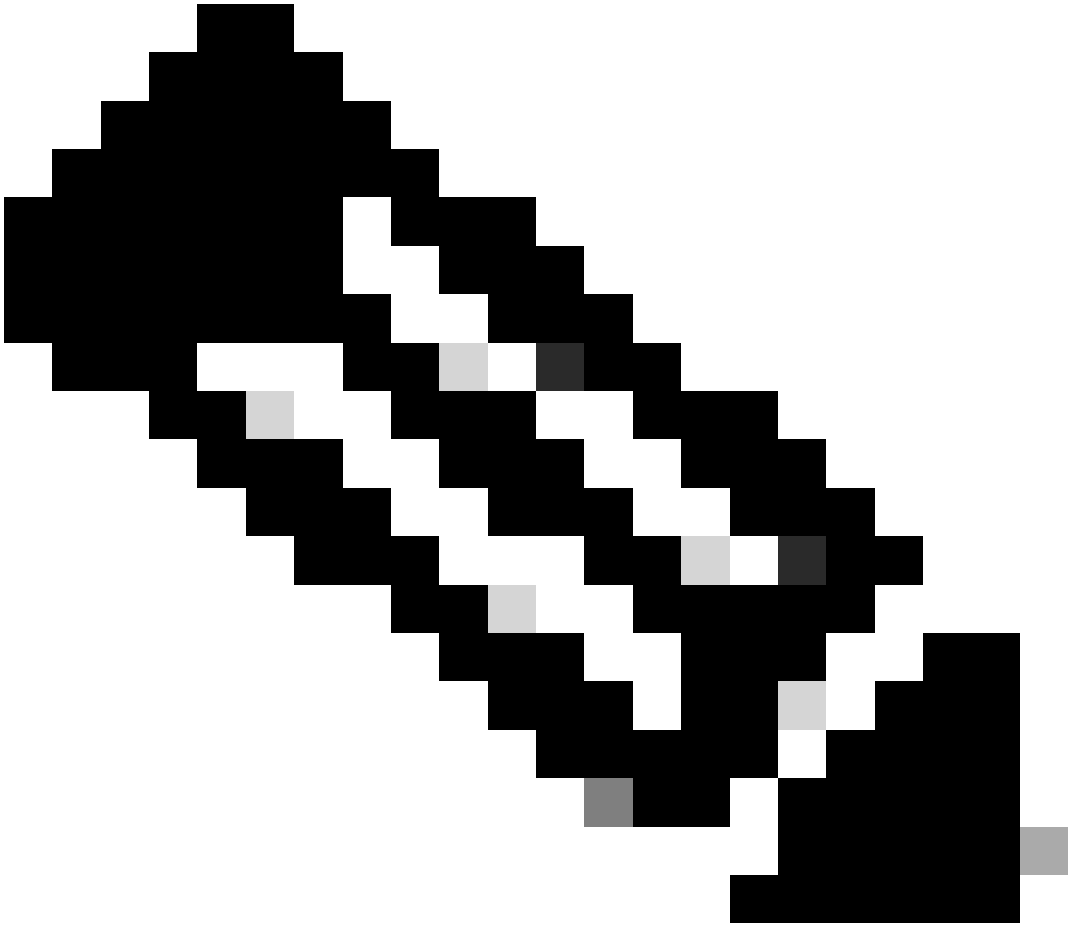
no-networking 확인

Java NED 패키지에 사용되는 SSHJ 클라이언트의 세부 정보를 늘리려면 다음을 수행합니다.

설정

java-vm java-logging logger net.schmizz.sshj level-error

no-networking 확인



참고: SSHJ 클라이언트에 대한 로깅을 level-error로 설정하는 것이 좋습니다. 기본적으로 비활성화되어 있습니다.

특정 Java 요소에 대한 로깅을 되돌리려면

설정

java-vm java-logging logger com.tailf 없음

no-networking 확인

현재 java-vm 로깅 설정을 보려면

show running-config java-vm java-logging

ncs-python-vm.log

이 로그는 INFO Verbosity에서 기본적으로 활성화되어 있습니다. 자세한 내용은 SSH 또는 ncs_cli -

C -noaaa를 통해 액세스할 수 있는 NSO CLI에서 변경됩니다.

모든 Python VM의 로그에 대한 자세한 정보를 설정합니다.

설정
python-vm 로깅 레벨 디버그
no-networking 확인

되돌리려면
설정
python-vm 로깅 레벨 디버그 없음
no-networking 확인

현재 python-vm 로깅 설정을 보려면
show running-config python-vm logging

upgrade.log

이 로그는 기본적으로 활성화되어 있습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf를 열고 <upgrade-log>의 내용을 변경하십시오.

```
        true




         ${NCS_LOG_DIR}/upgrade.log



         true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

raft.log

이 로그는 INFO Verbosity에서 기본적으로 활성화되어 있습니다. 이 로그에 대한 자세한 정보를 활성화하고 설정하려면 /etc/ncs/ncs.conf를 열고 <raft-log>의 내용을 변경하십시오.

```
        true

         ${NCS_LOG_DIR}/raft.log

         true

        trace
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

xpath.trace

이 로그는 기본적으로 활성화되어 있지 않습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf을 열고 <xpath-trace-log>의 내용을 변경하십시오.

```
        true

        ${NCS_LOG_DIR}/xpath.trace
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

ncserr.log

이 로그는 제한된 양의 정보를 기록합니다. NSO는 기본적으로 최대 크기가 1MB인 5개의 오류 파일을 유지 관리합니다. 로그 데이터에 5MB 이상을 생성하는 문제가 발생하는 드문 상황에서는 최대 크기를 늘려야 합니다. 이 로그는 기본적으로 활성화되어 있습니다. 이 로그의 최대 크기를 파일당 10MB로 변경하려면 /etc/ncs/ncs.conf을 열고 <error-log>의 내용을 변경합니다.

```
        true

        ${NCS_LOG_DIR}/ncserr.log
```

```
        S10M
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

transerr.log

이 로그는 기본적으로 활성화되어 있지 않지만 ncs.conf에서 처음 설치할 때 활성화되어 있습니다.
이 로그를 사용하려면 /etc/ncs/ncs.conf를 열고 <transaction-error-log>의 내용을 변경합니다.

```
        true
```

```
        ${NCS_LOG_DIR}/transerr.log
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

진행률

이 로그는 기본적으로 활성화되어 있지 않지만 ncs.conf에서 처음 설치할 때 활성화되어 있습니다.
이 로그를 사용하려면 /etc/ncs/ncs.conf를 열고 <progress-trace>의 내용을 변경하십시오.

```
        true




        ${NCS_LOG_DIR}
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

ncs-smart-licensing.log

이 로그는 기본적으로 활성화되어 있지 않습니다. SSH 또는 ncs_cli -C -noaaa를 통해 액세스할 수 있는 NSO CLI에서 로그가 활성화됩니다. 이 로그를 사용하려면

설정

smart-license smart-agent stdout-capture 사용

no-networking 확인

로깅 변경 사항을 되돌리려면

설정

smart-license smart-agent stdout-capture가 활성화되지 않음

no-networking 확인

북행

localhost:xxxx.access

이 로그는 기본적으로 활성화되어 있습니다. 이 로그의 이름은 HTTP 포트에 따라 다릅니다. 기본적으로 8080 및 8888입니다. 이 로그를 활성화하려면 /etc/ncs/ncs.conf를 열고 <webui-access-log>의 내용을 변경합니다.

```
        true




        ${NCS_LOG_DIR}
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

트래픽.추적

이 로그는 기본적으로 활성화되어 있지 않습니다. traffic.trace 로그는 /var/log/ncs/trace_20240628_010010/와 같은 디렉토리에 생성됩니다. 이 로그를 활성화하려면 /etc/ncs/ncs.conf를 열고 <webui-access-log>의 내용을 변경합니다.

```
        true




        ${NCS_LOG_DIR}




        true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

netconf.log

이 로그는 기본적으로 활성화되어 있습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf을 열고 <netconf-log> 다음에 내용을 추가합니다.

```
        true

         ${NCS_LOG_DIR}/netconf.log

         true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

추가 옵션: NSO

```
    true
```

가 rpc-reply 상태를 "ok" 또는 "error"로 기록하도록 하려면 뒤에 삽입합니다.

netconf-trace.log

이 로그는 기본적으로 활성화되어 있지 않습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf를 열고 <netconf-trace-log>의 내용을 변경합니다.

```
        true

        ${NCS_LOG_DIR}/netconf-trace.log
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

json-rpc.log

이 로그는 기본적으로 활성화되어 있지 않습니다. 이 로그를 활성화하려면 /etc/ncs/ncs.conf을 열고 <jsonrpc-log> 다음에 내용을 추가합니다.

```
        true

         ${NCS_LOG_DIR}/json-rpc.log

         true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

남행

디바이스 NED 추적

이 로그는 기본적으로 활성화되어 있지 않습니다. SSH 또는 ncs_cli -C -noaaa를 통해 액세스할 수 있는 NSO CLI에서 로그가 활성화됩니다.

디바이스에 대한 추적을 활성화하려면

설정
디바이스 디바이스 <devicename> trace raw
device<devicename> ned-setting <ned-id> 로거 수준 디버그
디바이스 디바이스 <devicename> trace raw
no-networking 확인

디바이스에 적용된 모든 로그 설정을 보려면 show devices device <devicename> active-settings를 사용합니다.

device-trace 파일의 내용을 지우려면 device <devicename> clear-trace를 사용합니다.

audit-network.log

이 로그는 기본적으로 활성화되어 있지 않습니다. 이 로그를 사용하려면 /etc/ncs/ncs.conf을 열고 <audit-network-log> 다음에 내용을 추가합니다.

```
        true
```

```
         ${NCS_LOG_DIR}/audit-network.log
```

```
        true
```

ncs.conf를 수정한 후 ncs —reload를 실행합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.