启用NSO日志和垂直度

目录

简介

本文档介绍NSO中可用的各种日志、它们的用途以及如何启用它们。

先决条件

要求

要查看、启用和设置日志，您需要一个有权访问运行NSO服务的主机环境以及有权访问NSO CLI和NSO IPC端口的用户。

使用的组件

思科Crosswork Network Service Orchestrator(NSO)6.4.1版

本文档是为截至NSO 6.4的可用日志记录选项编写的。虽然本文档中的大多数信息适用于不同的版本，但与您使用的版本相比，有些日志可能已被弃用或添加。本文档不包括在NSO系统外部导出日志的配置。

本文档中提供的命令假设使用默认目录设置进行系统安装NSO。在您的环境中，某些文件的位置可能不同。

- 默认情况下，ncs.conf可在$NCS_CONFIG_DIR中找到/etc/ncs/ncs.conf
- 默认情况下可在$NCS_LOG_DIR中找到日志/var/log/ncs/
- 默认情况下，NSO安装在$NCSDIR中/opt/ncs/
- 默认情况下，NSO的运行目录为$NCS_RUN_DIR， /var/opt/ncs/

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

一般日志准则

日志记录影响

以更高的详细程度启用日志可能会增加NSO服务器的负载和磁盘空间要求。对于诸如devel.log之类的高活动日志，这是特别需要考虑的问题。在故障排除期间在较短时间内启用详细数据通常不是问题，但在较长时间启用详细数据时，请确保将资源和磁盘空间考虑在内。

生成技术报告

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

选项:

--install-dir
:指定安装NCS静态文件的目录，如安装程序的 — install-dir选项。

--full :收集系统的ncs备份，以便思科支持人员更轻松地重现任何错误。

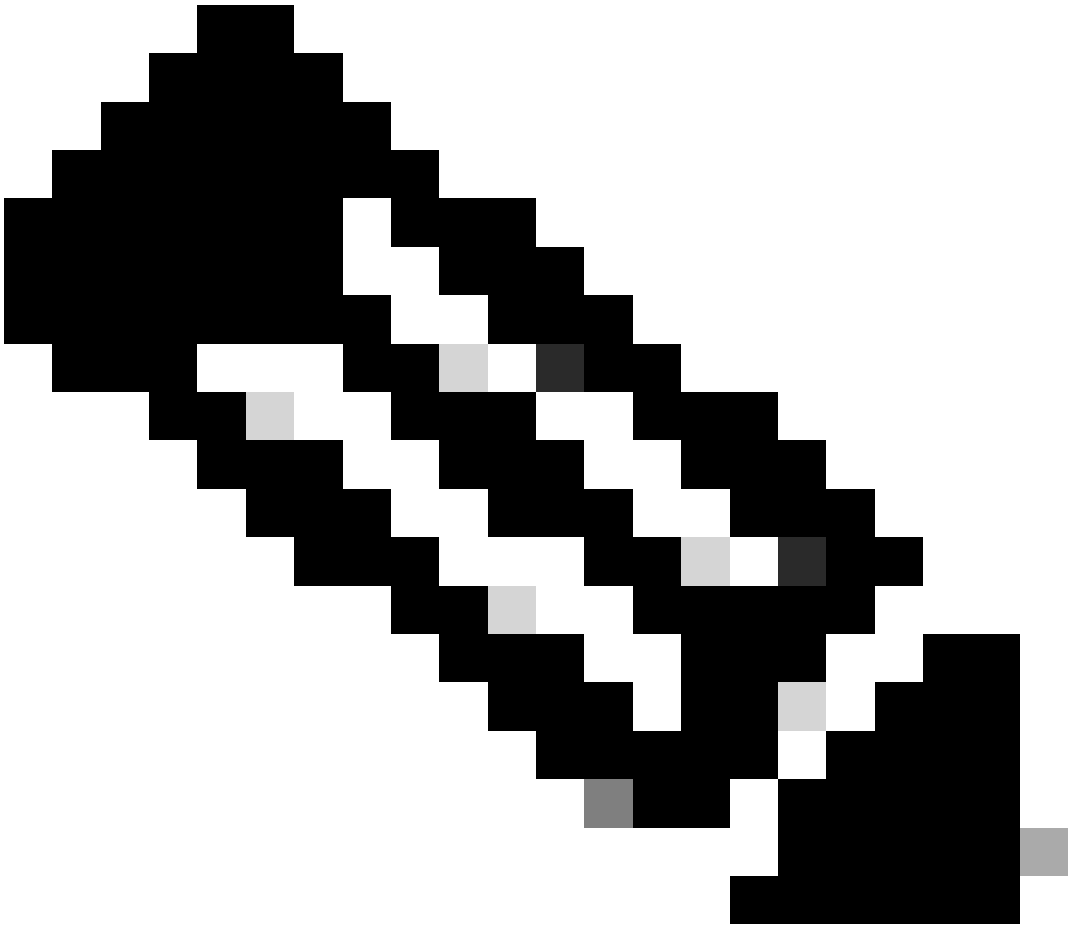
--num-debug-dumps :默认1，生成调试转储快照。对于跟踪资源泄漏的情况（例如内存/文件描述符泄漏），请将此值设置为3。

推荐选项：

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

可以单独收集和提供备份，以限制捆绑包的文件大小，从而更轻松地上传。

在运行脚本的当前目录中生成技术报告。



> 注意：技术报告收集NSO日志目录的内容。在生成新的技术报告之前，请验证此目录不包含任何以前的技术报告或备份。

生成备份

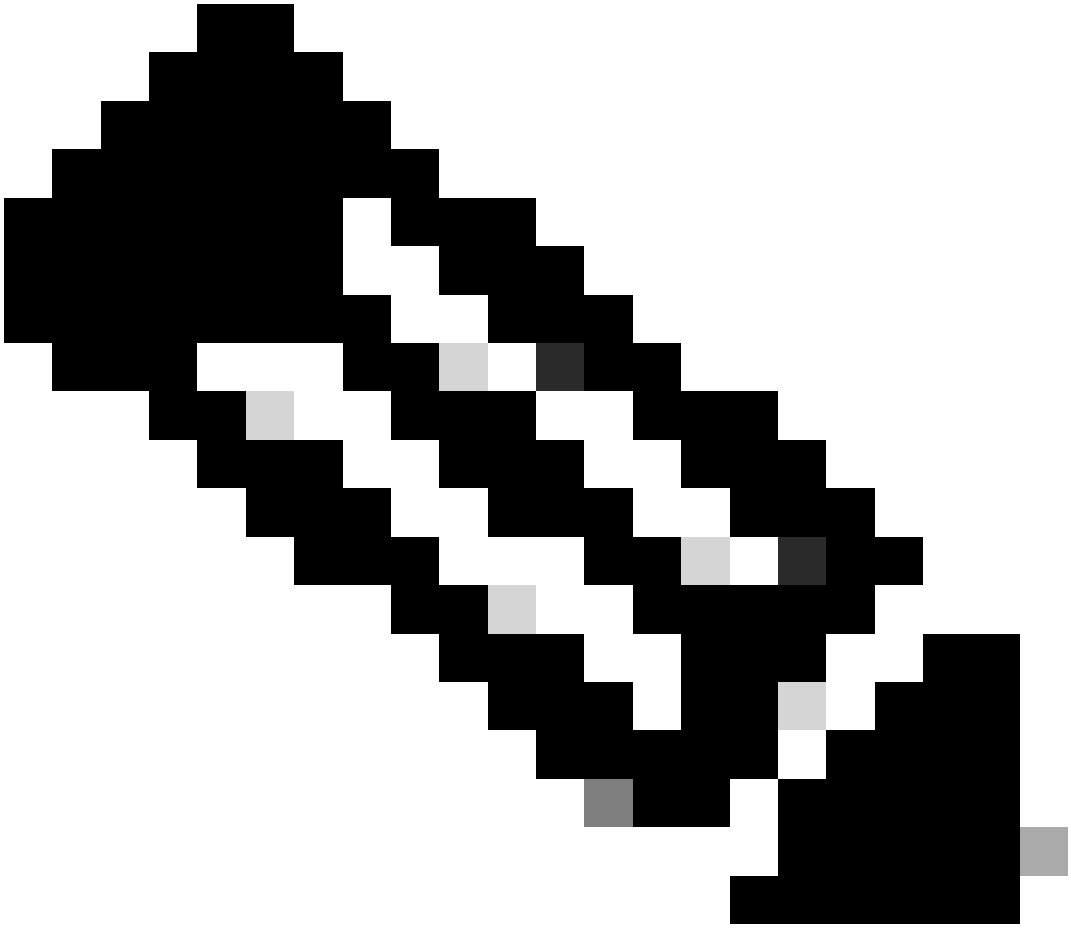
/opt/ncs/current/bin/ncs-backup

备份是在中生成的 /var/opt/ncs/backups/.

未生成日志文件

当日志文件被存档或删除时，NSO需要创建新文件。通常，此情况会自动发生，但如果它没有发生，请使用命令：

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



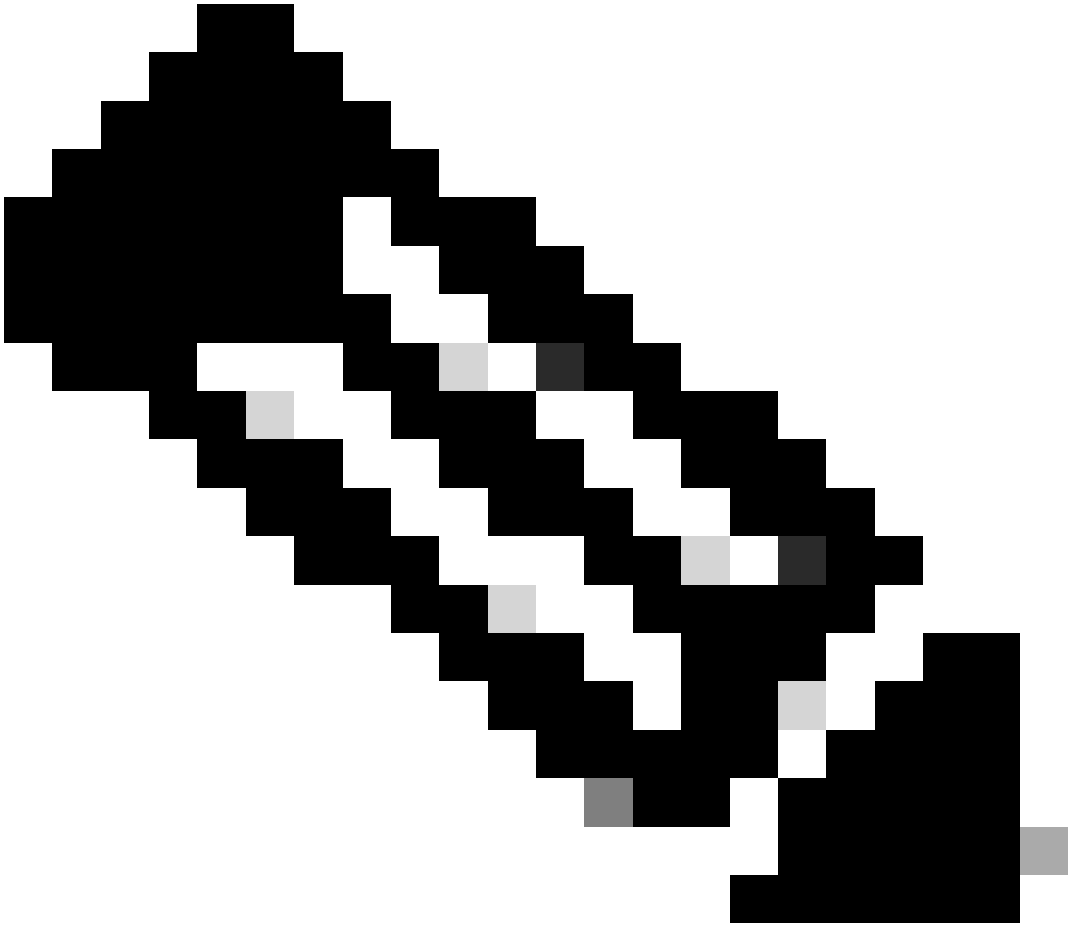
注意：例如，当限制对IPC端口的访问时，使用ncs.conf中的ipc-access设置，请确保将必要的变量定义为cron或anacron的一部分，以便每周日志旋转可以正确重新打开日志。

日志概述

- NSO内部日志
  - ncs.log:ncs日志记录了NSO的主要进程。它提供的深入信息有限，但可用于涉及关机、启动、加载软件包和升级的问题。
  - audit.log:审核日志记录通过任何API在NSO上进行身份验证的所有用户。它还记录NSO CLI和低精度北向接口上的任何活动。
  - audit-log-commit :启用此设置会增强audit.log。它不会创建自己的日志。在提交和同步源操作期间，它会记录对NSO CDB的所有非默认更改。

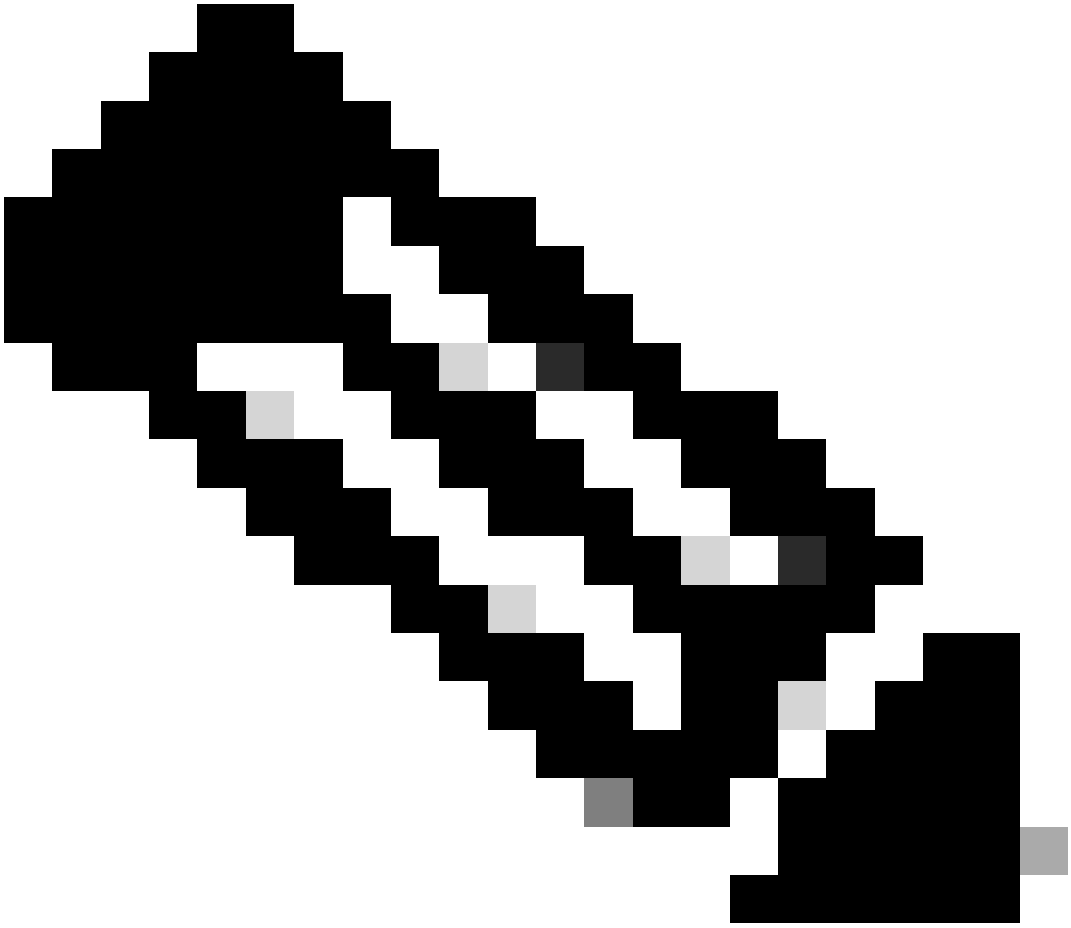
    - audit-log-commit-default :启用此设置会增强audit.log。它不会创建自己的日志。它会在提交和同步源操作期间记录对NSO CDB的所有默认更改。
    - devel.log:日志记录了NSO的一般操作和工作流程。
    - ncs-java-vm.log:Java日志记录所有与Java-VM相关的操作。最值得注意的是所有网络元件驱动程序(NED)和服务包都用Java编写。所有CLI NED都用java编写。
    - ncs-python-vm.log:python日志记录与Python中写入的服务包相关的活动。为以python编写的每个服务包生成单独的python日志。没有使用python编写NED。
    - upgrade.log:升级日志记录在NSO升级期间的NSO型号更改，包括重新加载软件包期间的NSO版本升级和NSO软件包升级。
    - raft.log:专用于利用HA-Raft功能的NSO集群的日志。
    - xpath.trace:xpath跟踪记录NSO执行的所有xpath评估。这对于确定删除操作花费较长时间的原因很有用。
    - ncserr.log:ncserr.log是记录来自NCS守护程序的内部进程的错误的二进制日志。对于几乎任何“内部错误”错误消息和崩溃情况都是强制性的。
    - transerr.log:事务错误日志是收集导致CDB启动错误或运行时事务失败的失败事务信息的日志。
    - progress.trace:progress trace用于跟踪系统中事务和操作所发出的进度事件。在/progress/trace中配置要发射的数据。
    - ncs-smart-licensing.log:NSO内部许可证智能代理的日志。
- 北向：从北向元素到达NSO
    - audit.log:审核日志记录在NSO CLI上执行的命令。
    - localhost:8080.access/localhost:8888.access :这是嵌入式Web服务器的访问日志并收集HTTP活动。此文件遵循Apache定义的通用日志格式
    - traffic.trace:此日志收集非常高详细的HTTP流量。使用它调试Restconf和json-rpc API。
    - netconf.log:Netconf API的日志
    - netconf-trace.log:高详细度netconf API的日志
    - json-rpc.log:json-rpc.log API的日志
- 南行：记录从NSO到网络的通信。
    - 设备NED跟踪：每台设备都会生成自己的跟踪。设备跟踪命名为ned-<ned-id>-<devicename>.trace或netconf-<devicename>.trace
    - audit-network.log:记录NSO发送到南向设备的配置命令。
- 系统日志
    - Linux日志：通常位于/var/log/并包括消息或系统日志等日志。具体取决于主机。
    - ncs_crash.dump:NSO因内存问题终止时生成的NSO系统转储。
    - core dump:当NSO因非内存原因终止时，Linux可以生成一个称为core的核心转储。<PID>

Linux需要满足某些条件才能生成核心转储。ulimit配置是阻止转储的最常见设置。有关要求的完整列表，请参阅Linux手动页



注意：NCS技术报告不收集系统日志，但可能有助于解决性能和崩溃相关问题。

启用日志和设置详细程度



注意：更改ncs.conf文件中的配置设置可以通过执行命令来ncs --reload应用。 ncs --reload, it 从ncs.conf文件中重新加载值并更新正在运行的系统，同时关闭并重新打开所有日志文件，以便应用所有日志记录更改。这不会中断服务。

一般准则

- 当ncs.conf文件中不存在特定配置时，NSO会采用文件中指定的默认行/opt/ncs/current/src/ncs/ncs_config/tailf-ncs-config.yang为。
- 如果日志被指定为默认启用，则意味着即使缺少启用日志的配置，该日志也会启用。
- 默认情况下，某些日志被禁用，但在首次安装NSO时，ncs.conf具有启用日志的特定说明。
- 当ncs.conf文件中不存在特定配置时，可以添加配置，如logs container所示，即在ncs.conf文件中和。

内部

ncs.log

默认情况下启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并更改<ncs-log>的内容。

```
        true

         ${NCS_LOG_DIR}/ncs.log

         true
```

编辑ncs.conf后，执行ncs —reload。

audit.log

默认情况下启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并更改<audit-log>的内容。

```
        true
```

```
        ${NCS_LOG_DIR}/audit.log

        true
```

编辑ncs.conf后，执行ncs —reload。

audit-log-commit和audit-log-commit-defaults

默认情况下未启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并在<audit-log>之后添加内容。

```
      true

        ${NCS_LOG_DIR}/audit.log

        true
```

```
        true
```

```
        true
```

编辑ncs.conf后，执行ncs —reload。

devel.log

此日志默认在INFO详细程度启用。要启用和更改此日志的详细性，请打开/etc/ncs/ncs.conf并更改<developer-log>的内容。

```
         true
```

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

```
          true
```

```
        trace
```

编辑ncs.conf后，执行ncs —reload。

ncs-java-vm.log

此日志默认在INFO详细程度启用。可以设置由java-vm管理的各个元素的详细程度。从NSO CLI(可通过SSH或ncs_cli -C -noaaa访问)更改详细程度

要增加com.tailf下所有java元素的详细程度，请执行以下操作：

config
java-vm java-logging logger com.tailf level level-trace
提交无网络

要增加特定NED包的详细程度，请执行以下操作：

config

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

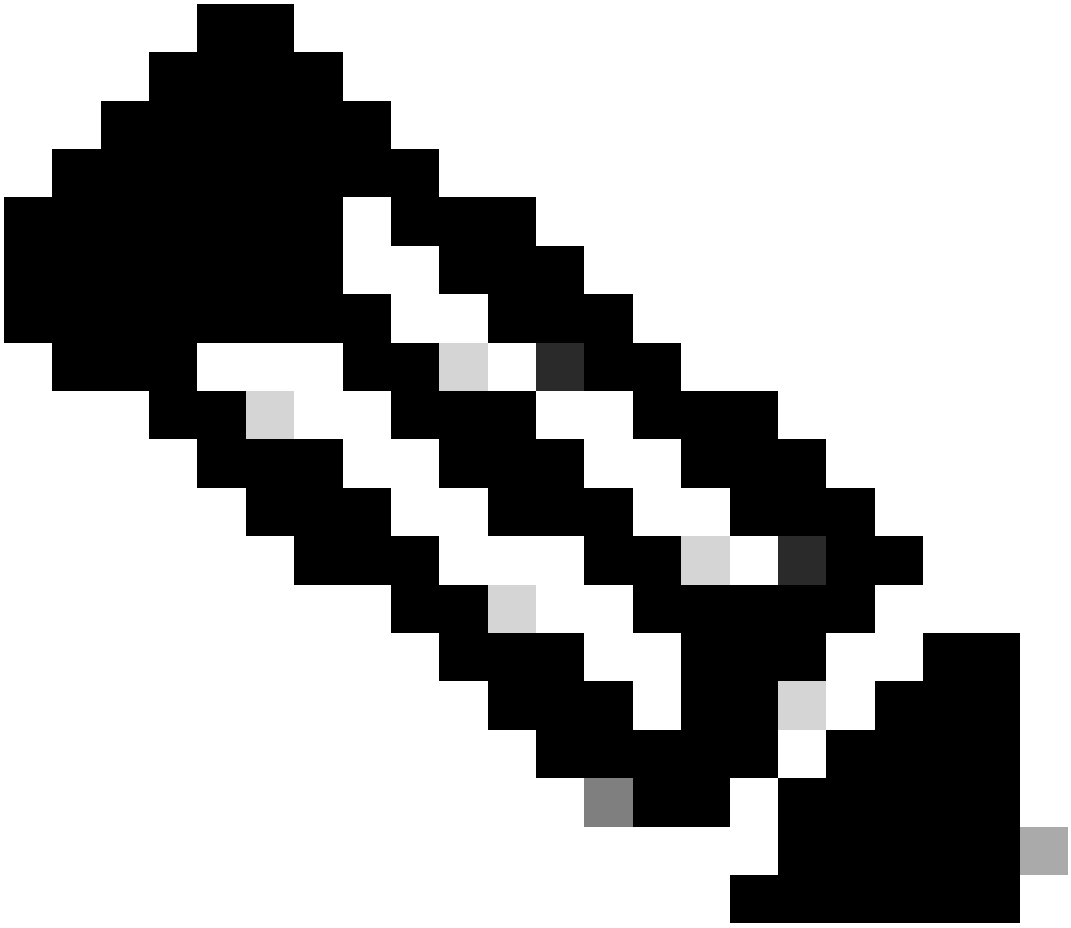
提交无网络

要增加Java NED包中使用的SSHJ客户端的详细程度，请执行以下操作：

config

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

提交无网络



注意：Cisco建议将SSHJ客户端的日志记录设置为level-error。默认情况下禁用该技术。

要恢复特定java元素的日志记录，请执行以下操作：

config

no java-vm java-logging logger com.tailf

提交无网络

要查看当前的java-vm日志记录设置，请执行以下操作：

show running-config java-vm java-logging

ncs-python-vm.log

此日志默认在INFO详细程度启用。从NSO CLI更改详细程度，NSO CLI可通过SSH或ncs_cli -C -noaaa进行访问。

为所有Python VM的日志设置详细程度。

config
python-vm logging level level-debug
提交无网络

要恢复，请执行以下操作：
config
no python-vm logging level-debug
提交无网络

要查看当前的python-vm日志记录设置，请执行以下操作：
show running-config python-vm logging

upgrade.log

默认情况下启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并更改<upgrade-log>的内容。

```
        true

         ${NCS_LOG_DIR}/upgrade.log

         true
```

编辑ncs.conf后，执行ncs —reload。

raft.log

此日志默认在INFO详细程度启用。要启用和设置此日志的详细性，请打开/etc/ncs/ncs.conf并更改<raft-log>的内容。

```
        true

         ${NCS_LOG_DIR}/raft.log

         true

        trace
```

编辑ncs.conf后，执行ncs —reload。

xpath.trace

默认情况下未启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并更改<xpath-trace-log>的内容

。

```
        true

        ${NCS_LOG_DIR}/xpath.trace
```

编辑ncs.conf后，执行ncs —reload。

ncserr.log

此日志记录的信息量有限。NSO维护5个错误文件，每个文件的最大默认大小为1MB。在极少数情况下，当日志数据中发生超过5MB的问题时，您需要增加最大大小。默认情况下启用此日志。要将此日志的最大大小更改为每个文件10MB，请打开/etc/ncs/ncs.conf并更改<error-log>的内容。

```
        true

        ${NCS_LOG_DIR}/ncserr.log

        S10M
```

编辑ncs.conf后，执行ncs —reload。

transerr.log

默认情况下未启用此日志，但在首次安装时在ncs.conf中启用。要启用此日志，请打开/etc/ncs/ncs.conf并更改<transaction-error-log>的内容。

```
        true
```

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

编辑ncs.conf后，执行ncs —reload。

progress.trace

默认情况下未启用此日志，但在首次安装时在ncs.conf中启用。要启用此日志，请打开/etc/ncs/ncs.conf并更改<progress-trace>的内容。

```
        true
```

```
        ${NCS_LOG_DIR}
```

编辑ncs.conf后，执行ncs —reload。

ncs-smart-licensing.log

默认情况下未启用此日志。日志从NSO CLI启用，可通过SSH或ncs_cli -C -noaaa进行访问。要启用此日志，请执行以下操作：

config

支持智能许可证智能代理静态捕获

提交无网络

要恢复日志记录更改，请执行以下操作：

config

未启用智能许可证智能代理stdout捕获

提交无网络

北向

localhost:xxxx.access

默认情况下启用此日志。此日志的名称因HTTP端口而异。默认值为8080和8888。要启用此日志，请打开/etc/ncs/ncs.conf并更改<webui-access-log>的内容。

```
        true
```

```
        ${NCS_LOG_DIR}
```

编辑ncs.conf后，执行ncs —reload。

traffic.trace

默认情况下未启用此日志。traffic.trace日志在目录(例如/var/log/ncs/trace_20240628_010010/中生成。要启用此日志，请打开/etc/ncs/ncs.conf并更改<webui-access-log>的内容。

```
        true

        ${NCS_LOG_DIR}

        true
```

编辑ncs.conf后，执行ncs —reload。

netconf.log

默认情况下启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并在<netconf-log>之后添加内容。

```
        true

        ${NCS_LOG_DIR}/netconf.log

        true
```

编辑ncs.conf后，执行ncs —reload

其他选项：在之

true

后插入，使NSO记录rpc-reply状态“ok”或“error”。

netconf-trace.log

默认情况下未启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并更改<netconf-trace-log>的内容。

```
        true
```

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

编辑ncs.conf后，执行ncs —reload。

json-rpc.log

默认情况下未启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并在<jsonrpc-log>之后添加内容。

```
        true
```

```
         ${NCS_LOG_DIR}/json-rpc.log
```

```
         true
```

编辑ncs.conf后，执行ncs —reload。

南向

设备NED跟踪

默认情况下未启用此日志。日志从NSO CLI启用，可通过SSH或ncs_cli -C -noaaa进行访问。

要为设备启用跟踪，请执行以下操作：

config
devices device <devicename> trace raw
devices device <devicename> ned-setting <ned-id> logger level debug
提交无网络

要查看应用到设备的所有日志设置，请使用show devices device <devicename> active-settings。

要清除device-trace文件的内容，请使用devices device <devicename> clear-trace。

要禁用设备跟踪，请执行以下操作：

config

no devices device <devicename> trace

提交无网络

audit-network.log

默认情况下未启用此日志。要启用此日志，请打开/etc/ncs/ncs.conf并在<audit-network-log>之后添加内容。

```
        true

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

```
        true
```

编辑ncs.conf后，执行ncs —reload。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。