NSO-Protokolle und -ausführlichkeiten aktivieren

Inhalt

Einleitung

In diesem Dokument werden die verschiedenen Protokolle beschrieben, die im NSO verfügbar sind, wofür sie verwendet werden und wie sie aktiviert werden.

Voraussetzungen

Anforderungen

Zum Anzeigen, Aktivieren und Festlegen von Protokollen benötigen Sie einen Benutzer mit Zugriff auf die Hostumgebung, in der der NSO-Service ausgeführt wird, sowie Zugriff auf die CLI des NSO und den IPC-Port des NSO.

Verwendete Komponenten

Cisco Crosswork Network Service Orchestrator (NSO) Version 6.4.1

Dieses Dokument wurde für die Protokollierungsoptionen geschrieben, die ab NSO 6.4 verfügbar sind. Die meisten Informationen in diesem Dokument gelten versionsübergreifend, aber einige Protokolle können im Vergleich zu der von Ihnen verwendeten Version veraltet oder hinzugefügt worden sein. In diesem Dokument wird nicht auf die Konfiguration zum Exportieren von Protokollen außerhalb des NSO-Systems eingegangen.

Bei den in diesem Dokument angegebenen Befehlen wird von einem NSO ausgegangen, der das Standardverzeichnis verwendet. In Ihrer Umgebung können sich die Speicherorte bestimmter Dateien unterscheiden.

- ncs.conf befindet sich in $NCS_CONFIG_DIR, standardmäßig unter /etc/ncs/ncs.conf
- Protokolle finden Sie in $NCS_LOG_DIR, standardmäßig /var/log/ncs/
- Der NSO wird standardmäßig in $NCSDIR installiert: /opt/ncs/
- Das NSO-Verzeichnis ist $NCS_RUN_DIR, standardmäßig /var/opt/ncs/

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Allgemeine Protokollrichtlinien

Auswirkungen der Protokollierung

Die Aktivierung von Protokollen mit höherer Ausführlichkeit kann zu erhöhten Lade- und Speicherplatzanforderungen für den NSO-Server führen. Dies ist besonders bei hochaktiven Protokollen wie devel.log von Bedeutung. Die Aktivierung der Ausführlichkeit für kurze Zeiträume während der Fehlerbehebung ist im Allgemeinen kein Problem, aber wenn Sie sie für längere Zeiträume aktivieren, stellen Sie sicher, dass Ressourcen und Festplattenspeicher berücksichtigt werden.

Erstellen eines Technologieberichts

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

Optionen:

--install-dir

: Gibt das Verzeichnis für die Installation von statischen NCS-Dateien an, wie die Option —install-dir für das Installationsprogramm.

--full : Erfasst ein ncs-Backup des Systems, wodurch der Cisco Support Fehler leichter reproduzieren kann.

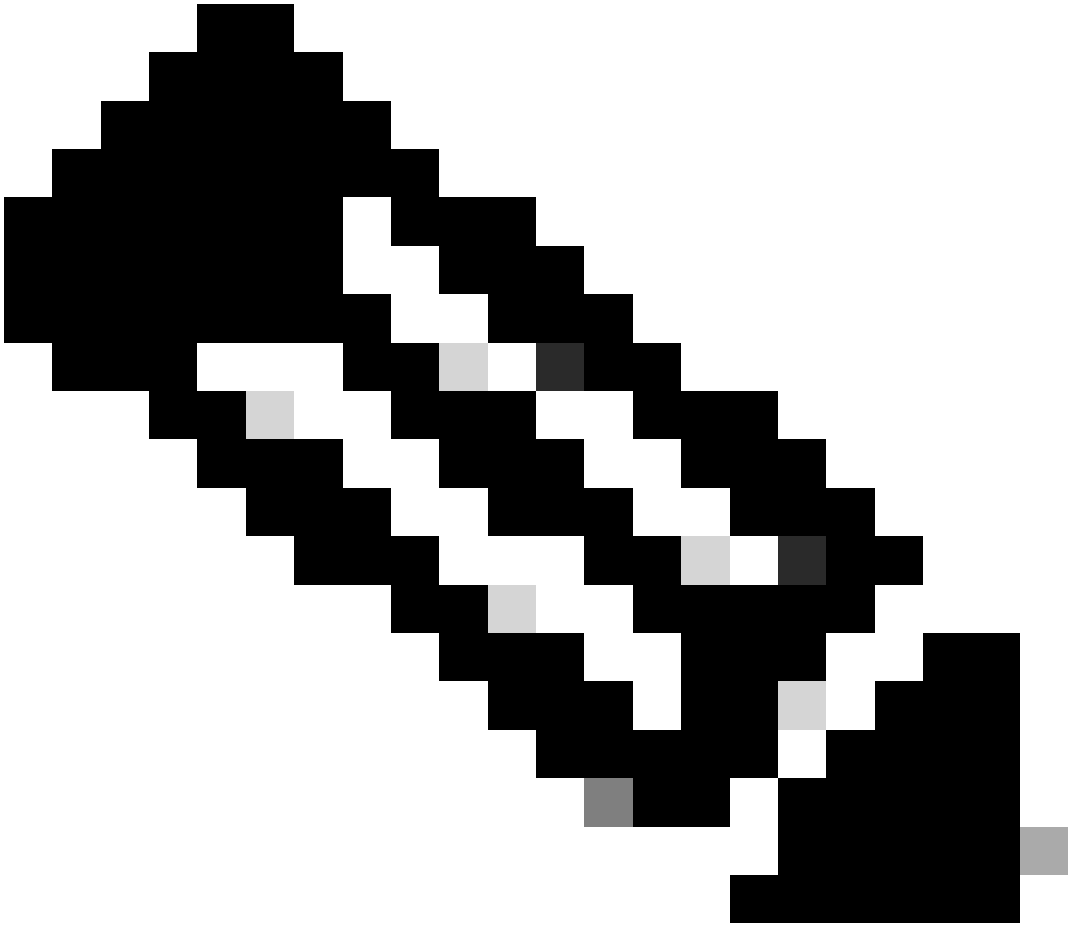
--num-debug-dumps : Standard 1, Generiert einen Snapshot für das Debugdump. Bei Fällen, in denen Ressourcenlecks, wie z. B. Speicher-/Dateideskriptor-Lecks, verfolgt werden, setzen Sie diese Einstellung auf 3.

Empfohlene Optionen

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

Ein Backup kann separat gesammelt und bereitgestellt werden, um die Dateigröße des Pakets für einfachere Uploads zu begrenzen.

Der technische Bericht wird im aktuellen Verzeichnis generiert, aus dem das Skript ausgeführt wird.



Anmerkung: Ein Technologiebericht erfasst den Inhalt des NSO-Protokollverzeichnisses. Vergewissern Sie sich, dass dieses Verzeichnis keine vorherigen technischen Berichte oder Sicherungen enthält, bevor Sie Ihren neuen technischen Bericht erstellen.

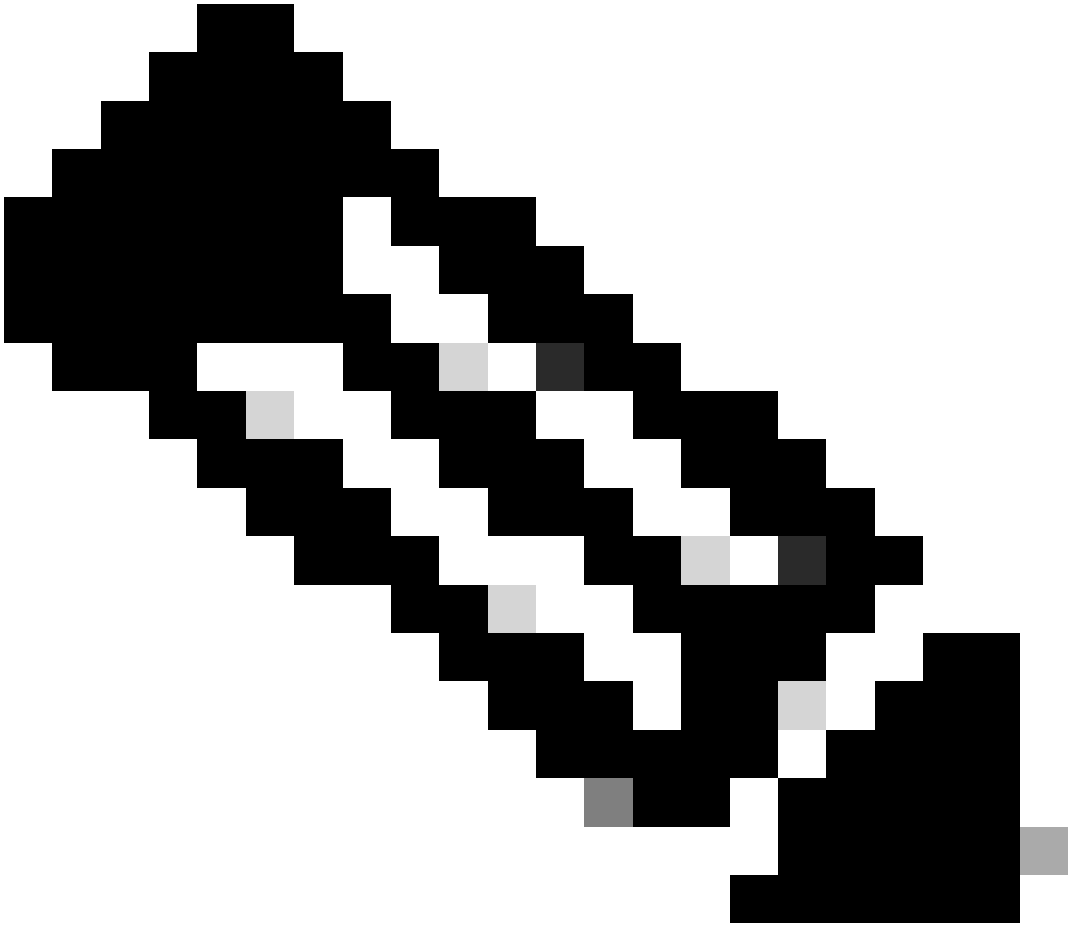
Erstellen eines Backups

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

Sicherungen werden generiert in /var/opt/ncs/backups/.

Protokolldateien werden nicht erstellt

Wenn eine Protokolldatei archiviert oder gelöscht wird, muss der NSO eine neue Datei erstellen. In der Regel geschieht dies automatisch. Falls dies nicht der Fall ist, verwenden Sie den Befehl:
/opt/ncs/current/bin/ncs_cmd -c reopen_logs.



Anmerkung: Wenn Sie den Zugriff auf den IPC-Port einschränken, z. B. mit der Einstellung ipc-access in ncs.conf, stellen Sie sicher, dass Sie die erforderlichen Variablen als Teil von cron oder anacron definieren, damit die wöchentliche Protokollrotation Protokolle ordnungsgemäß öffnen kann.

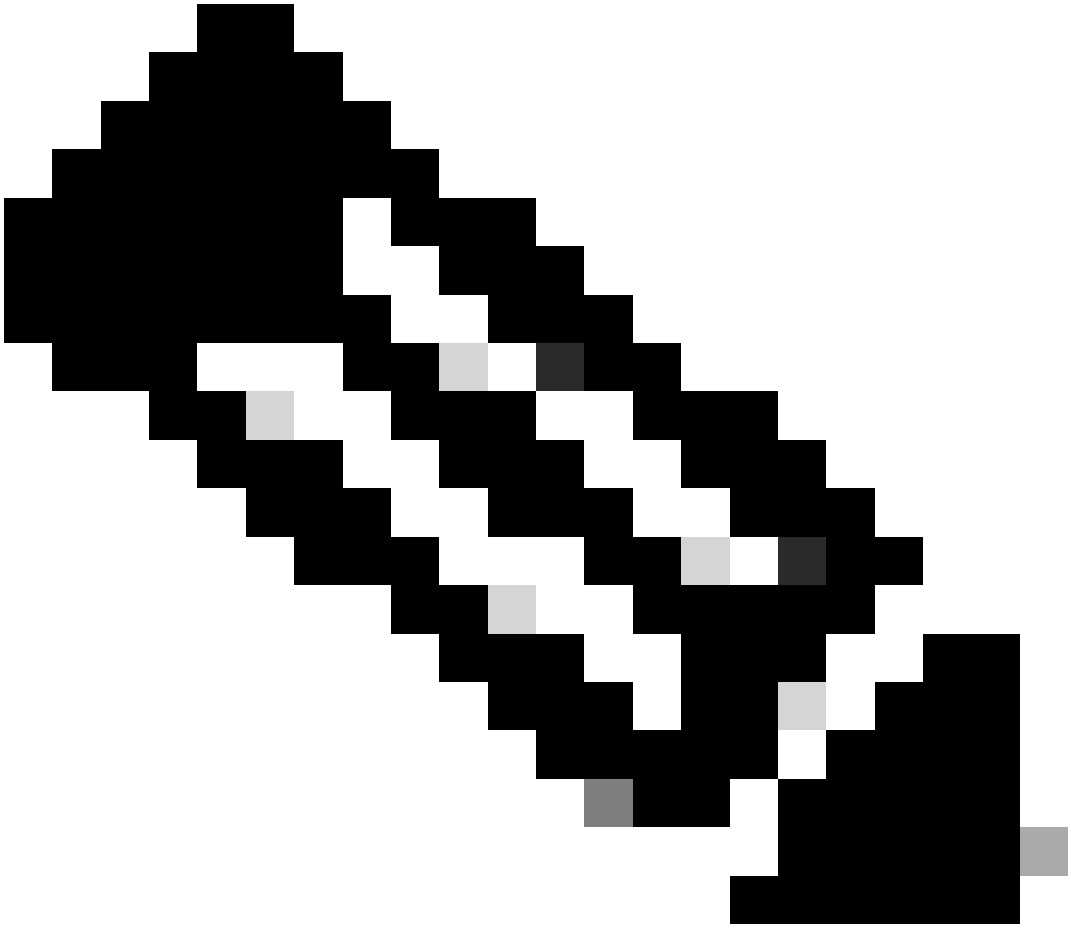
Übersicht über Protokolle

- Interne NSO-Protokolle
  - ncs.log: Das NCS-Protokoll protokolliert den Hauptprozess des NSO. Es verfügt über begrenzte detaillierte Informationen, kann aber für Probleme wie Herunterfahren, Starten, Laden von Paketen und Upgrades verwendet werden.
  - audit.log: Das Prüfprotokoll protokolliert alle Benutzer, die sich auf dem NSO über eine beliebige API authentifizieren. Außerdem werden alle Aktivitäten in der NSO-CLI und an Northbound-Schnittstellen mit niedriger Ausführlichkeit protokolliert.
  - audit-log-commit: Wenn Sie diese Einstellung aktivieren, wird die Datei audit.log erweitert. Es erstellt kein eigenes Protokoll. Es protokolliert alle nicht standardmäßigen

Änderungen an der NSO-CDB während des Commit- und Sync-From-Vorgangs.
    - audit-log-commit-defaults: Wenn Sie diese Einstellung aktivieren, wird die Datei audit.log erweitert. Es erstellt kein eigenes Protokoll. Es protokolliert alle Standardänderungen an NSO-CDB während der Übertragungs- und Synchronisierungsvorgänge.
    - devel.log: Im Entwicklerprotokoll werden die allgemeinen Vorgänge und Workflows des NSO protokolliert.
    - ncs-java-vm.log Das Java-Protokoll protokolliert alle Java-VM-bezogenen Vorgänge. Insbesondere alle Netzwerkelementtreiber (NED) und Servicepakete, die in Java geschrieben wurden. Alle CLI-NEDs werden in Java geschrieben.
    - ncs-python-vm.log: Die Python-Protokolle protokollieren die Aktivitäten im Zusammenhang mit in Python geschriebenen Service-Paketen. Für jedes in Python geschriebene Service-Paket wird ein separates Python-Protokoll generiert. Es werden keine NEDs in Python geschrieben.
    - upgrade.log: Im Upgrade-Protokoll werden die Änderungen der NSO-Modelle während der NSO-Upgrades protokolliert, einschließlich der Upgrades der NSO-Version und der NSO-Paket-Upgrades während des erneuten Ladens der Pakete.
    - raft.log: Ein Protokoll speziell für NSO-Cluster, die die HA-Raft-Funktionen nutzen.
    - xpath.trace: Der xpath-Trace protokolliert alle xpath-Evaluierungen, die der NSO durchführt. Dies kann nützlich sein, um herauszufinden, warum ein Löschvorgang lange dauert.
    - ncserr.log: Bei "ncserr.log" handelt es sich um binäre Protokollaufzeichnungsfehler für interne Prozesse vom NCS-Daemon. Obligatorisch für fast alle 'internen Fehler' Fehlermeldungen und Absturzszenarien.
    - transerr.log: Das Transaktionsfehlerprotokoll ist ein Protokoll zum Sammeln von Informationen über fehlgeschlagene Transaktionen, die zu einem CDB-Startfehler oder Laufzeittransaktionsfehler führen.
    - progress.trace: Die Fortschrittsüberwachung wird zum Verfolgen von Fortschrittereignissen verwendet, die von Transaktionen und Aktionen im System ausgegeben werden. Welche Daten ausgegeben werden sollen, wird in /progress/trace konfiguriert.
    - ncs-smart-license.log: Protokolle für den Lizenz-Smart-Agent im NSO.
- Northbound: Ankunft beim NSO von Northbound-Elementen
    - audit.log: Die in der NSO-CLI ausgeführten Befehle werden im Prüfprotokoll protokolliert.
    - localhost:8080.access/localhost:8888.access: Hierbei handelt es sich um ein Zugriffsprotokoll für den integrierten Webserver, in dem die HTTP-Aktivität erfasst wird. Diese Datei entspricht dem von Apache definierten Common Log Format
    - traffic.trace: Dieses Protokoll sammelt HTTP-Datenverkehr mit sehr hohem Ausführlichkeitsgrad. Verwenden Sie es, um Restconf und json-rpc API zu debuggen.
    - netconf.log: Protokoll für Netconf-API
    - netconf-trace.log: Protokoll für Netconf-API mit hohem Detailgrad
    - json-rpc.log: Protokoll für json-rpc.log API
- Southbound: Protokollierung der Kommunikation zwischen dem NSO und dem Netzwerk
    - Nachverfolgung von Geräte-NEDs: Jedes Gerät generiert seine eigene Ablaufverfolgung. Device Traces werden entweder als end-<end-id>-

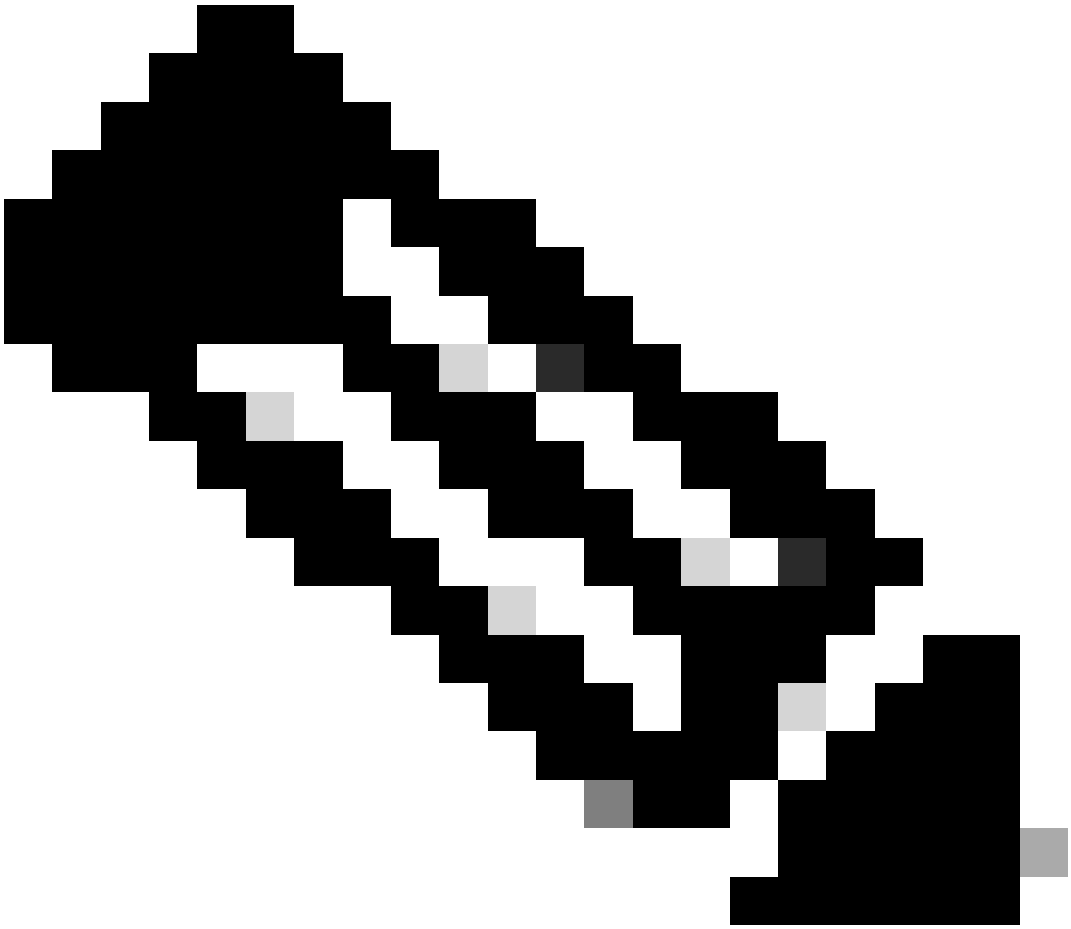
<Gerätename>.trace oder als netconf-<Gerätename>.trace bezeichnet.
    - audit-network.log: Zeichnet Konfigurationsbefehle auf, die vom NSO an die Southbound-Geräte gesendet werden.
- Systemprotokolle
    - Linux-Protokolle: Wird in der Regel unter /var/log/ gefunden und umfasst Protokolle wie Nachrichten oder Syslog. Diese variieren je nach Host.
    - ncs_crash.dump: Ein NSO-Systemabbild, das beim Beenden des NSO aufgrund von Speicherproblemen generiert wird.
    - Core Dump: Wenn der NSO aus Gründen beendet wird, die nicht im Arbeitsspeicher liegen, kann Linux einen Core Dump mit der Bezeichnung "Core" generieren.<PID>

Linux muss bestimmte Bedingungen erfüllen, damit ein Core Dump generiert werden kann. Die ulimit-Konfiguration ist die häufigste Einstellung, die einen Dump verhindert. Eine vollständige Liste der Anforderungen finden Sie im Linux Manual Page.



Anmerkung: Systemprotokolle werden nicht vom technischen Bericht des NCS erfasst, können jedoch für leistungs- und absturzbedingte Probleme nützlich sein.

Aktivieren von Protokollen und Festlegen von Ausführlichkeiten



Anmerkung: Das Ändern der Konfigurationseinstellungen in der Datei ncs.conf wird durch Ausführen des `ncs --reload` Befehls angewendet. `ncs --reload, it` lädt die Werte aus der Datei "ncs.conf" neu und aktualisiert das aktuelle System sowie schließt und öffnet alle Protokolldateien, sodass alle Protokolländerungen angewendet werden. Dies unterbricht keine Dienste.

Allgemeine Richtlinien

- Wenn in der Datei "ncs.conf" keine spezifische Konfiguration vorhanden ist, übernimmt der NSO das Standardverhalten, das in der `/opt/ncs/current/src/ncs/ncs_config/tailf-ncs-config.yang` Datei angegeben ist.
- Wenn ein Protokoll als standardmäßig aktiviert angegeben wird, bedeutet dies, dass das Protokoll aktiviert ist, auch wenn die Konfiguration zum Aktivieren fehlt.
- Einige Protokolle sind standardmäßig deaktiviert, aber bei der ersten Installation des NSO

enthält ncs.conf spezifische Anweisungen zum Aktivieren des Protokolls.
- Wenn in der Datei ncs.conf keine spezifische Konfiguration vorhanden ist, können Sie die Konfiguration hinzufügen, wie unter logs container, d. h. zwischen
  und in der Datei ncs.conf dargestellt.

Intern

NCS.LOG

Dieses Protokoll ist standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <ncs-log>.

```
        true

         ${NCS_LOG_DIR}/ncs.log

         true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

audit.log

Dieses Protokoll ist standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <audit-log>.

```
        true

         ${NCS_LOG_DIR}/audit.log

         true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

audit-log-commit und audit-log-commit-defaults

Dieses Protokoll ist nicht standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und fügen Sie den Inhalt nach <audit-log> hinzu.

```
        true
```

```
        ${NCS_LOG_DIR}/audit.log

        true

      true

      true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

devel.log

Dieses Protokoll ist standardmäßig im INFO-Ausführlichkeitsbereich aktiviert. Um den Ausführlichkeitsgrad für dieses Protokoll zu aktivieren und zu ändern, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <developer-log>.

```
        true
```

```
        ${NCS_LOG_DIR}/devel.log

        true

      trace
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

ncs-java-vm.log

Dieses Protokoll ist standardmäßig im INFO-Ausführlichkeitsbereich aktiviert. Es ist möglich, die Ausführlichkeit einzelner Elemente festzulegen, die von java-vm verwaltet werden. Die Ausführlichkeit wird von der NSO-CLI abgewandelt, auf die über SSH oder ncs_cli -C -noaa zugegriffen werden kann.

So erhöhen Sie die Ausführlichkeit aller Java-Elemente unter com.tailf:

konfig.
java-vm java-logging logger com.tailf level-trace
keine Netzwerkverbindung herstellen

So erhöhen Sie die Ausführlichkeit für ein bestimmtes NED-Paket:

konfig.

java-vm java-logging logger.com.tailf.packages.ned.<NED-Name> Ebene Ebene-Nachverfolgung

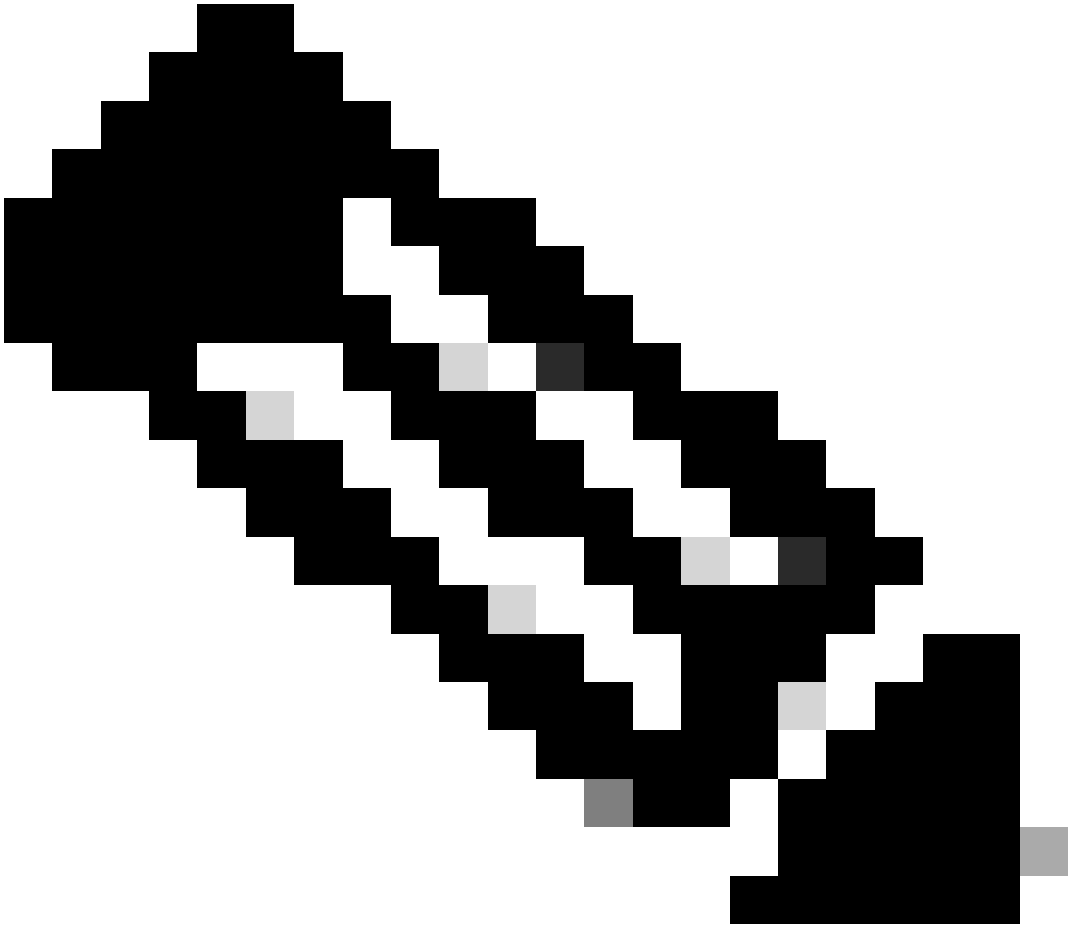
keine Netzwerkverbindung herstellen

So erhöhen Sie die Ausführlichkeit für den SSHJ-Client, der in Java NED-Paketen verwendet wird:

konfig.

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

keine Netzwerkverbindung herstellen



> Anmerkung: Cisco empfiehlt, die Protokollierung für den SSHJ-Client auf "level-error" einzustellen. Es ist standardmäßig deaktiviert.

So setzen Sie die Protokollierung für ein bestimmtes Java-Element zurück:

konfig.

kein java-vm java-logging logger com.tailf

keine Netzwerkverbindung herstellen

So zeigen Sie die aktuellen Java-VM-Protokollierungseinstellungen an:

show running-config java-vm java-logging

ncs-python-vm.log

Dieses Protokoll ist standardmäßig im INFO-Ausführlichkeitsbereich aktiviert. Die Ausführlichkeit wird von der CLI des NSO abgeändert, auf die über SSH oder ncs_cli -C -noaa zugegriffen werden kann.

Zur Einstellung der Ausführlichkeit für Protokolle aller virtuellen Python-Rechner.

konfig.
python-vm, Protokollierungsebene, Debugging
keine Netzwerkverbindung herstellen

So kehren Sie zurück:
konfig.
kein python-vm, Protokollierungsebene, Debugging
keine Netzwerkverbindung herstellen

So zeigen Sie die aktuellen python-vm-Protokollierungseinstellungen an:
show running-config python-vm logging

Upgrade.log

Dieses Protokoll ist standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von **<**upgrade-log**>**.

```
        true

         ${NCS_LOG_DIR}/upgrade.log

         true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

Floß.log

Dieses Protokoll ist standardmäßig im INFO-Ausführlichkeitsbereich aktiviert. Um die Ausführlichkeit dieses Protokolls zu aktivieren und festzulegen, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von **<**raft-log**>**.

```
        true

         ${NCS_LOG_DIR}/raft.log

         true

        trace
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

xpath.trace

Dieses Protokoll ist nicht standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <xpath-trace-log>.

```
        true

        ${NCS_LOG_DIR}/xpath.trace
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

ncserr.log

Dieses Protokoll zeichnet eine begrenzte Menge an Informationen auf. Der NSO verwaltet fünf Fehlerdateien mit einer Standardgröße von jeweils maximal 1 MB. In den seltenen Fällen, in denen ein Problem auftritt, das mehr als 5 MB an Protokolldaten erzeugt, müssen Sie die maximale Größe erhöhen. Dieses Protokoll ist standardmäßig aktiviert. Um die maximale Größe dieses Protokolls auf 10 MB pro Datei zu ändern, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <error-log>.

```
        true
```

```
${NCS_LOG_DIR}/ncserr.log

S10M
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

transerr.log

Dieses Protokoll ist nicht standardmäßig aktiviert, wird jedoch bei der ersten Installation in ncs.conf aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <transaction-error-log>.

```
true

${NCS_LOG_DIR}/transerr.log
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

progress.trace

Dieses Protokoll ist nicht standardmäßig aktiviert, wird jedoch bei der ersten Installation in

ncs.conf aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <progress-trace>.

```
        true


        ${NCS_LOG_DIR}
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

ncs-smart-license.log

Dieses Protokoll ist nicht standardmäßig aktiviert. Das Protokoll wird über die NSO-CLI aktiviert, auf die über SSH oder ncs_cli -C -noaa zugegriffen werden kann. So aktivieren Sie dieses Protokoll:

konfig.

Smart-License Smart-Agent StdOut-Erfassung aktiviert

keine Netzwerkverbindung herstellen

So stellen Sie die Protokollierungsänderung wieder her:

konfig.

Smart-Agent Standout-Erfassung ohne Smart-Lizenz aktiviert

keine Netzwerkverbindung herstellen

Northbound

localhost:xxxx.access

Dieses Protokoll ist standardmäßig aktiviert. Der Name dieses Protokolls hängt vom HTTP-Port ab. Standardmäßig 8080 und 8888. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <webui-access-log>.

```
        true

        ${NCS_LOG_DIR}
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

traffic.trace

Dieses Protokoll ist nicht standardmäßig aktiviert. traffic.trace-Protokolle werden in einem Verzeichnis wie /var/log/ncs/trace_20240628_010010/ generiert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <webui-access-log>.

```
        true

        ${NCS_LOG_DIR}
```

```
        true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

netconf.log

Dieses Protokoll ist standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und fügen Sie den Inhalt nach <netconf-log> hinzu.

```
        true

         ${NCS_LOG_DIR}/netconf.log

         true
```

Nach dem Bearbeiten von ncs.conf führen Sie ncs —reload aus.

Zusätzliche Option: Fügen Sie

true

nach dem RPC-Antwortstatus "ok" oder "error" ein, um das NSO-Protokoll zu erstellen.

netconf-trace.log

Dieses Protokoll ist nicht standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und ändern Sie den Inhalt von <netconf-trace-log>.

```
        true

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

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

json-rpc.log

Dieses Protokoll ist nicht standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und fügen Sie den Inhalt nach <jsonrpc-log> hinzu.

```
        true
```

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




        true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

Southbound

Geräte-NED-Verfolgung

Dieses Protokoll ist nicht standardmäßig aktiviert. Das Protokoll wird über die NSO-CLI aktiviert, auf die über SSH oder ncs_cli -C -noaa zugegriffen werden kann.

So aktivieren Sie die Ablaufverfolgung für ein Gerät:

konfig.
devices device <Gerätename> trace raw
devices device <Gerätename> end-setting <end-id> logger level debug
devices device <Gerätename> trace raw
keine Netzwerkverbindung herstellen

Um alle auf ein Gerät angewendeten Protokolleinstellungen anzuzeigen, verwenden Sie show devices device <Gerätename> active-settings.

Um den Inhalt einer Device-Ablaufverfolgungsdatei zu löschen, verwenden Sie devices device <Gerätename> clear-trace.

audit-network.log

Dieses Protokoll ist nicht standardmäßig aktiviert. Um dieses Protokoll zu aktivieren, öffnen Sie /etc/ncs/ncs.conf, und fügen Sie den Inhalt nach <audit-network-log> hinzu.

```
        true

        ${NCS_LOG_DIR}/audit-network.log

        true
```

Nachdem Sie ncs.conf bearbeitet haben, führen Sie ncs —reload aus.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.