Ativar registros e verbosidades NSO

Contents

Introdução

Este documento descreve os vários registros disponíveis no NSO, para que eles são usados e como ativá-los.

Pré-requisitos

Requisitos

Para exibir, ativar e definir logs, você precisa de um usuário com acesso ao ambiente de host que executa o serviço NSO, bem como acesso à CLI do NSO e à porta IPC do NSO.

Componentes Utilizados

Cisco Crosswork Network Service Orchestrator (NSO) versão 6.4.1

Este documento foi escrito para as opções de log disponíveis a partir do NSO 6.4. Embora a maioria das informações neste documento se aplique a várias versões, alguns logs podem ter sido preteridos ou adicionados em comparação com a versão que você está usando. Este documento não aborda a configuração para exportar logs fora do sistema NSO.

Os comandos fornecidos neste documento supõem um NSO de instalação do sistema usando a configuração de diretório padrão. Em seu ambiente, os locais de determinados arquivos podem ser diferentes.

- O ncs.conf pode ser encontrado em $NCS_CONFIG_DIR, por padrão /etc/ncs/ncs.conf
- Os logs podem ser encontrados em $NCS_LOG_DIR, por padrão /var/log/ncs/
- O NSO é instalado em $NCSDIR, por padrão /opt/ncs/
- O diretório de execução do NSO é $NCS_RUN_DIR, por padrão /var/opt/ncs/

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diretrizes gerais de log

Impacto de registro

A habilitação de logs com maior detalhamento pode causar o aumento dos requisitos de carga e espaço em disco do servidor NSO. Isso é especialmente uma consideração para logs altamente ativos, como devel.log. Ativar o detalhamento por curtos períodos de tempo durante a solução de problemas geralmente não é uma preocupação, mas ao ativá-los por períodos de tempo mais longos, não se esqueça de levar em conta os recursos e o espaço em disco.

Geração de um relatório técnico

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

Opções:

--install-dir
: Especifica o diretório para instalação de arquivos estáticos NCS, como a opção —install-dir para o instalador.

--full : Coleta um ncs-backup do sistema, facilitando para o suporte da Cisco a reprodução de erros.

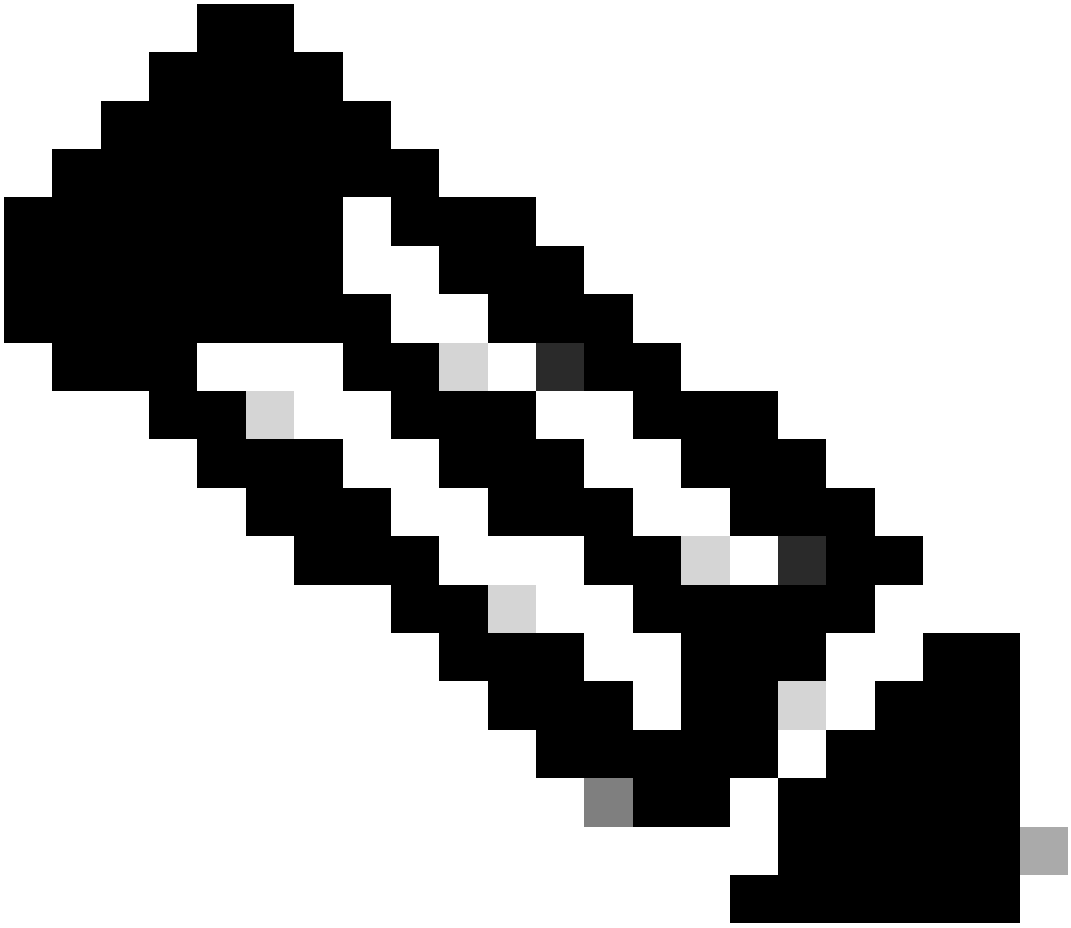
--num-debug-dumps : Padrão 1, gera um instantâneo de despejo de depuração. Para casos que controlam vazamentos de recursos, como vazamentos de descritor de memória/arquivo, defina como 3.

Opções recomendadas:

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

Um backup pode ser coletado e fornecido separadamente para limitar o tamanho do arquivo do pacote para facilitar os uploads.

O relatório técnico é gerado no diretório atual a partir do qual o script é executado.



Note: Um relatório técnico coleta o conteúdo do diretório de log do NSO. Verifique se esse diretório não contém nenhum relatório técnico ou backup anterior antes de gerar o novo relatório técnico.

Gerando um backup

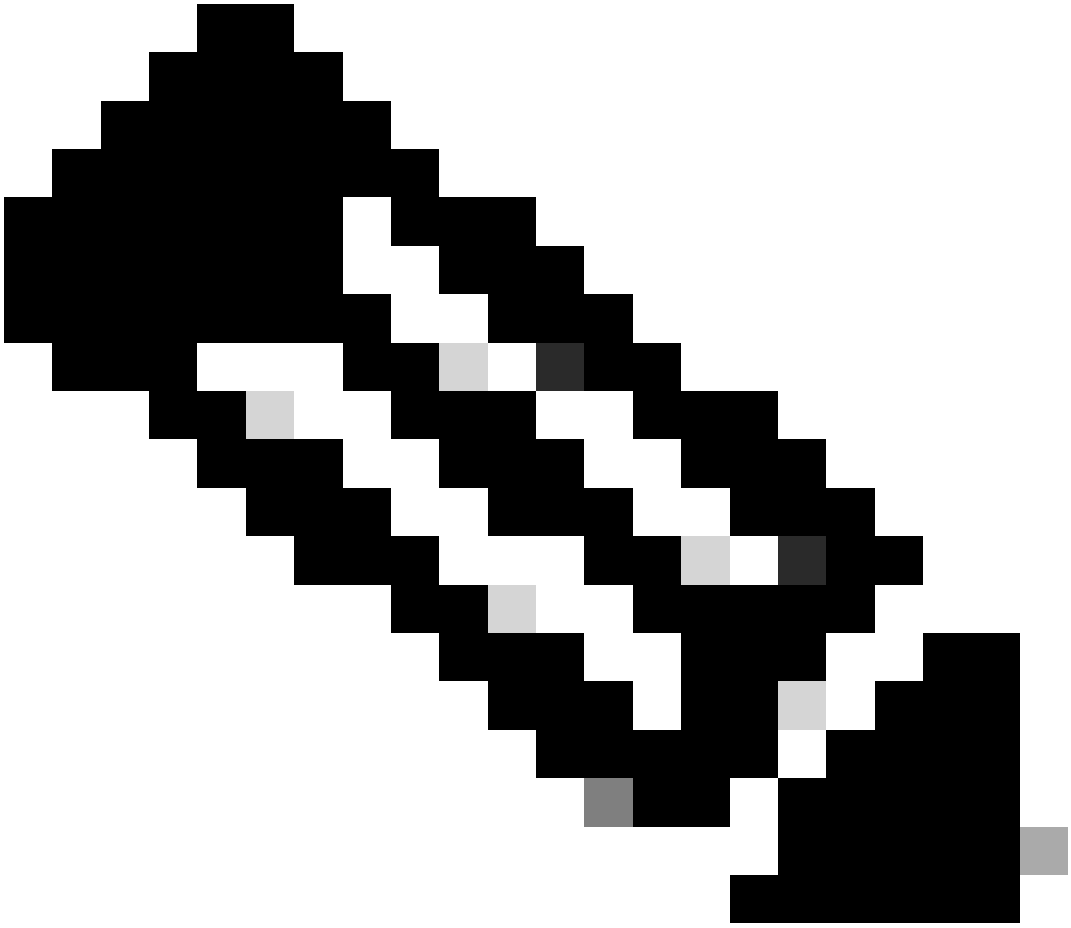
/opt/ncs/current/bin/ncs-backup

Os backups são gerados em /var/opt/ncs/backups/.

Arquivos de log que não estão sendo gerados

Quando um arquivo de registro é arquivado ou excluído, o NSO precisa criar um novo arquivo. Normalmente isso acontece automaticamente, mas caso não aconteça, use o comando:

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



Note: Ao restringir o acesso à porta IPC, por exemplo, usando a configuração ipc-access em ncs.conf, certifique-se de definir as variáveis necessárias como parte de cron ou anacron para que a rotação de log semanal possa reabrir logs adequadamente.

Visão geral dos registros

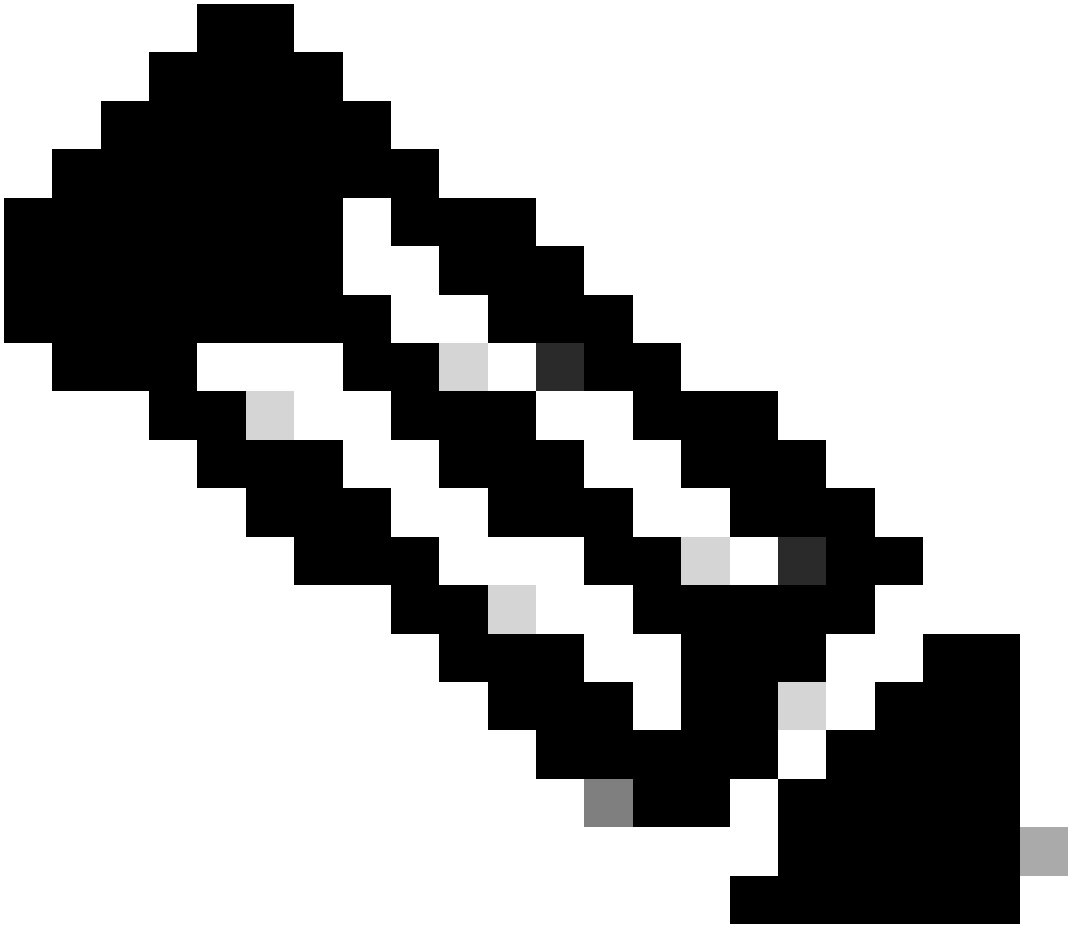
- Logs internos NSO
  - ncs.log: O registro ncs registra o processo principal de NSO. Ele tem informações detalhadas limitadas, mas pode ser usado para problemas que envolvem desligamento, inicialização, carregamento de pacotes e atualizações.
  - audit.log: O registro de auditoria registra todos os usuários que se autenticam no NSO através de qualquer API. Ele também registra qualquer atividade na CLI do NSO e interfaces ascendentes de baixa verbosidade.
  - audit-log-commit: Habilitar essa configuração aprimora o audit.log. Ele não cria seu próprio log. Registra todas as alterações não padrão no NSO CDB durante as operações de confirmação e de sincronização.

    - audit-log-commit-defaults : Habilitar essa configuração aprimora o audit.log. Ele não cria seu próprio log. Registra todas as alterações padrão no NSO CDB durante as operações de confirmação e de sincronização.
    - devel.log: O registro de desenvolvimento registra as operações gerais e os fluxos de trabalho do NSO.
    - ncs-java-vm.log: O log de java registra todas as operações relacionadas a java-vm. Mais notavelmente qualquer NED (Network Element Driver) e pacotes de serviço escritos em Java. Todos os NEDs CLI são escritos em java.
    - ncs-python-vm.log: O python registra a atividade relacionada aos pacotes de serviço escritos em Python. Um log Python separado é gerado para cada pacote de serviço escrito em Python. Nenhum NED é escrito em Python.
    - upgrade.log: O registro de atualização registra as alterações nos modelos NSO durante as atualizações NSO, incluindo as atualizações de versão NSO e as atualizações de pacote NSO durante o recarregamento de pacotes.
    - jangada.log: Um log especificamente para clusters NSO que aproveita os recursos de HA-Raft.
    - xpath.trace: O rastreamento xpath registra todas as avaliações de xpath que o NSO executa. Isso pode ser útil para descobrir por que uma operação de exclusão está demorando.
    - ncserr.log: Os ncserr.log são registros binários que registram erros para processos internos do daemon do NCS. Obrigatório para quase todas as mensagens de erro 'interno' e cenários de travamento.
    - trans.log: O log de erros de transações é um log para coletar informações sobre transações com falha que levam a erro de inicialização de CDB ou falha de transação em tempo de execução.
    - progress.trace: O rastreamento de progresso é usado para rastrear eventos de progresso emitidos por transações e ações no sistema. Quais dados serão emitidos são configurados em /progress/trace.
    - ncs-smart-licensing.log: Logs para o agente inteligente de licença dentro do NSO.
- Direção norte: Chegando ao NSO a partir de elementos ascendentes
    - audit.log: Os comandos de log de auditoria são executados na CLI do NSO.
    - localhost:8080.access/localhost:8888.access : Este é um log de acesso para o servidor Web incorporado e coleta a atividade HTTP. Este arquivo adere ao Common Log Format, conforme definido pelo Apache
    - traffic.trace: Esse log coleta tráfego HTTP de verbosidade muito alta. Use-o para depurar a API Restconf e json-rpc.
    - netconf.log: Log para API netconf
    - netconf-trace.log: Log para API netconf de alta verbosidade
    - json-rpc.log: Log para a API json-rpc.log
- Descendente: Registrando a comunicação indo do NSO para a rede.
    - Rastreamentos NED do dispositivo: Cada dispositivo gera seu próprio rastreamento. Os rastreamentos de dispositivo são nomeados como ned-<ned-id>-<devicename>.trace ou netconf-<devicename>.trace
    - audit-network.log: Registra os comandos de configuração enviados pelo NSO aos dispositivos de destino.
- Registros de sistema

- Registros do Linux: Geralmente encontrado em /var/log/ e inclui logs como mensagens ou syslog. Eles variam dependendo do host.
- ncs_crash.dump: Um despejo de sistema NSO gerado quando o NSO termina devido a problemas de memória.
- Dump central: Quando o NSO é encerrado por razões que não sejam de memória, o Linux pode gerar um dump central chamado core.<PID>

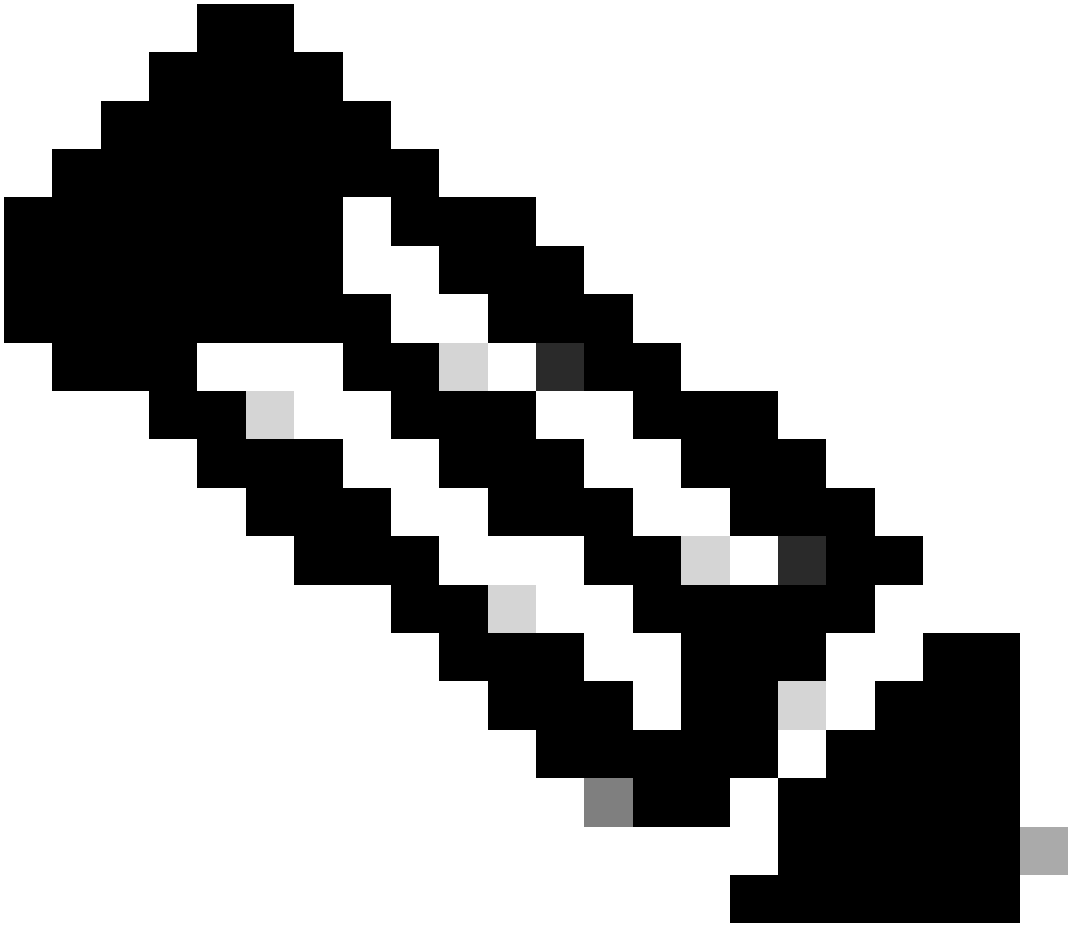
Certas condições precisam ser atendidas para que o Linux gere um dump central. A configuração ulimit é a configuração mais comum que impede um despejo. Consulte a página de manual do Linux para obter uma lista completa de requisitos

---



Note: Os logs do sistema não são coletados pelo relatório técnico do NCS, mas podem ser úteis para problemas relacionados a desempenho e falhas.

Ativando registros e definindo detalhamento



Note: A alteração das definições de configuração no arquivo ncs.conf é aplicada com a execução do `ncs --reload` comando. `ncs --reload, it` recarrega os valores do arquivo ncs.conf e atualiza o sistema em execução, bem como fecha e reabre todos os arquivos de registro para que as alterações de registro sejam aplicadas. Isso não interrompe os serviços.

Diretrizes gerais

- Quando uma configuração específica não está presente no arquivo ncs.conf, o NSO adota o comportamento padrão conforme especificado no `/opt/ncs/current/src/ncs/ncs_config/tailf-ncs-config.yang` arquivo.
- Quando um log é especificado como habilitado por padrão, isso significa que o log está habilitado mesmo que a configuração para habilitá-lo esteja ausente.
- Alguns logs são desativados por padrão, mas durante a primeira instalação do NSO, o ncs.conf tem instruções específicas para ativar o log.
- Quando uma configuração específica não está presente no arquivo ncs.conf, você pode adicionar a configuração conforme mostrado na `logs container`, o que significa entre

e no arquivo ncs.conf.

Interno

ncs.log

Esse log é habilitado por padrão. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de **<ncs-log>**.

```
        true

         ${NCS_LOG_DIR}/ncs.log

         true
```

Depois de editar o ncs.conf, execute ncs —reload.

audit.log

Esse log é habilitado por padrão. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de **<audit-log>**.

```
        true

        ${NCS_LOG_DIR}/audit.log

        true
```

Depois de editar o ncs.conf, execute ncs —reload.

audit-log-commit e audit-log-commit-defaults

Esse log não é habilitado por padrão. Para habilitar este log, abra /etc/ncs/ncs.conf e Adicione o conteúdo após **<**audit-log**>**.

```
        true
```

```
    ${NCS_LOG_DIR}/audit.log

    true

  true

  true
```

Depois de editar o ncs.conf, execute ncs —reload.

devel.log

Esse log é habilitado por padrão no detalhamento INFO. Para habilitar e alterar o detalhamento deste log, abra /etc/ncs/ncs.conf e altere o conteúdo de <developer-log>.

```
    true
```

```
        ${NCS_LOG_DIR}/devel.log

        true

      trace
```

Depois de editar o ncs.conf, execute ncs —reload.

ncs-java-vm.log

Esse log é habilitado por padrão no detalhamento INFO. É possível definir o detalhamento de elementos individuais gerenciados pelo java-vm. O detalhamento é alterado a partir da CLI do NSO, que pode ser acessada por meio de SSH ou ncs_cli -C -noaaa

Para aumentar o detalhamento em todos os elementos java em com.tailf:

config
java-vm java-logging logger com.tailf level level-trace
commit no-networking

Para aumentar o detalhamento de um pacote NED específico:

config

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

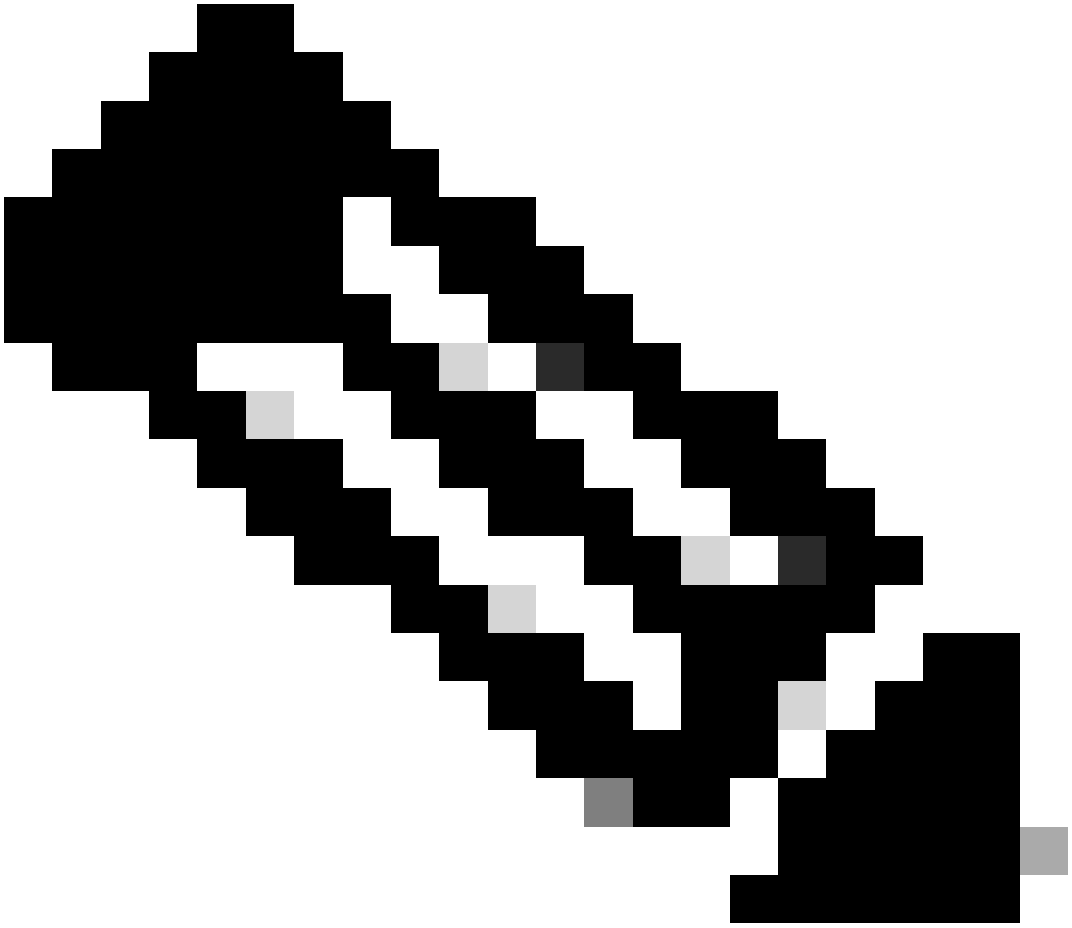
commit no-networking

Para aumentar o detalhamento do cliente SSHJ usado em pacotes NED java:

config

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

commit no-networking



Note: A Cisco recomenda definir o registro do cliente SSHJ como level-error. Por padrão, ela está desativada.

Para reverter o registro de um elemento java específico:

config

no java-vm java-logging logger com.tailf

commit no-networking

Para exibir as configurações atuais de log do java-vm:

show running-config java-vm java-logging

ncs-python-vm.log

Esse log é habilitado por padrão no detalhamento INFO. O detalhamento é alterado a partir da

CLI do NSO, que pode ser acessada por meio de SSH ou ncs_cli -C -noaaa.

Para definir o detalhamento de logs de todas as VMs Python.

config
python-vm logging level-debug
commit no-networking

Para reverter:
config
no python-vm logging level-debug
commit no-networking

Para exibir as configurações atuais de log do python-vm:
show running-config python-vm logging

upgrade.log

Esse log é habilitado por padrão. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de **<upgrade-log>**.

```
        true

         ${NCS_LOG_DIR}/upgrade.log

         true
```

Depois de editar o ncs.conf, execute ncs —reload.

jangada.log

Esse log é habilitado por padrão no detalhamento INFO. Para habilitar e definir o detalhamento desse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <draft-log>.

```
        true

         ${NCS_LOG_DIR}/raft.log

         true

        trace
```

Depois de editar o ncs.conf, execute ncs —reload.

xpath.trace

Esse log não é habilitado por padrão. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <xpath-trace-log>.

```
        true

        ${NCS_LOG_DIR}/xpath.trace
```

Depois de editar o ncs.conf, execute ncs —reload.

ncserr.log

Esse registro registra uma quantidade limitada de informações. O NSO mantém 5 arquivos de erro, cada um com um tamanho máximo de 1 MB por padrão. Na rara situação em que ocorre um problema que cria mais de 5 MB em dados de registro, você precisa aumentar o tamanho máximo. Esse log é habilitado por padrão. Para alterar o tamanho máximo desse log para 10 MB por arquivo, abra /etc/ncs/ncs.conf e altere o conteúdo de <error-log>.

```
        true

        ${NCS_LOG_DIR}/ncserr.log
```

```
        S10M
```

Depois de editar o ncs.conf, execute ncs —reload.

trans.log

Esse registro não é habilitado por padrão, mas habilitado no ncs.conf na primeira instalação. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <transaction-error-log>.

```
        true

        ${NCS_LOG_DIR}/transerr.log
```

Depois de editar o ncs.conf, execute ncs —reload.

progress.trace

Esse registro não é habilitado por padrão, mas habilitado no ncs.conf na primeira instalação. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <progress-trace>.

```
        true




        ${NCS_LOG_DIR}
```

Depois de editar o ncs.conf, execute ncs —reload.

ncs-smart-licensing.log

Esse log não é habilitado por padrão. O registro é ativado a partir da CLI do NSO que pode ser acessada através de SSH ou ncs_cli -C -noaaa. Para habilitar este log:

config

smart-license smart-agent stdout-capture enabled

commit no-networking

Para reverter a alteração de registro:

config

no smart-license smart-agent stdout-capture enabled

commit no-networking

Direção norte

localhost:xxxx.access

Esse log é habilitado por padrão. O nome desse log varia de acordo com a porta HTTP. Por padrão, 8080 e 8888. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <webui-access-log>.

```
        true




        ${NCS_LOG_DIR}
```

Depois de editar o ncs.conf, execute ncs —reload.

traffic.trace

Esse log não é habilitado por padrão. os logs traffic.trace são gerados em um diretório como /var/log/ncs/trace_20240628_010010/. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de **<**webui-access-log**>**.

```
        true




        ${NCS_LOG_DIR}




        true
```

Depois de editar o ncs.conf, execute ncs —reload.

netconf.log

Esse log é habilitado por padrão. Para habilitar este log, abra /etc/ncs/ncs.conf e Adicione o conteúdo após <netconf-log>.

```
        true

         ${NCS_LOG_DIR}/netconf.log

         true
```

Depois de editar o ncs.conf, execute o ncs — reload

Opção adicional: Insira

```
true
```

depois para que o NSO registre o status de rpc-reply "ok" ou "error".

netconf-trace.log

Esse log não é habilitado por padrão. Para habilitar esse log, abra /etc/ncs/ncs.conf e altere o conteúdo de <netconf-trace-log>.

```
true

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

Depois de editar o ncs.conf, execute ncs —reload.

json-rpc.log

Esse log não é habilitado por padrão. Para habilitar este log, abra /etc/ncs/ncs.conf e Adicione o conteúdo após <jsonrpc-log>.

```
true

 ${NCS_LOG_DIR}/json-rpc.log

 true
```

Depois de editar o ncs.conf, execute ncs —reload.

Para baixo

Rastreamento NED do Dispositivo

Esse log não é habilitado por padrão. O registro é ativado a partir da CLI do NSO que pode ser acessada através de SSH ou ncs_cli -C -noaaa.

Para ativar um rastreamento para um dispositivo:

config
device device <nome do dispositivo> trace raw
device device <nome do dispositivo> end-setting <id-end> logger level debug
commit no-networking

Para exibir todas as configurações de log aplicadas a um dispositivo, use show devices <nome do dispositivo> ative-settings.

Para limpar o conteúdo de um arquivo de rastreamento de dispositivo, use devices <nome do dispositivo> clear-trace.

Para desativar o rastreamento do dispositivo:

config

no devices device <nome do dispositivo> trace

commit no-networking

audit-network.log

Esse log não é habilitado por padrão. Para habilitar este log, abra /etc/ncs/ncs.conf e Adicione o conteúdo após <audit-network-log>.

```
        true
```

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




        true
```

Depois de editar o ncs.conf, execute ncs —reload.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.