NSOログとバージョンの有効化

内容

- はじめに
- 前提条件
  - 要件
  - 使用するコンポーネント
- 一般的なログガイドライン
  - ロギングの影響
  - テクニカルレポートの生成
  - バックアップの生成
  - ログファイルが生成されない
- ログの概要
- ログの有効化と詳細レベルの設定
  - 一般的なガイドライン
  - 内部
    - ncs.log
    - 監査ログ
    - audit-log-commitおよびaudit-log-commit-defaults
    - デバイス。ログ
    - ncs-java-vm.log（仮想マシンのみ）
    - ncs-python-vm.log（仮想マシンのログ）
    - アップグレード。ログ
    - raft.log（任意）
    - xpath.trace
    - NCSERRログ
    - 転送ログ
    - 進行状況。トレース
    - ncs-smart-licensing.log（登録ユーザ専用）
  - ノースバウンド
    - ローカルホスト：xxxx.access
    - トラフィック.trace
    - netconf.log（オプション）
    - netconf-trace.log（オプション）
    - json-rpc.log
  - サウスバウンド
    - デバイスNEDトレース
    - audit-network.log（監査ネットワークログ）

はじめに

このドキュメントでは、NSOで使用できるさまざまなログ、ログの使用目的、およびログを有効にする方法について説明します。

前提条件

要件

ログを表示、有効化、設定するには、NSOサービスを実行するホスト環境へのアクセス権と、NSO CLIおよびNSO IPCポートへのアクセス権を持つユーザが必要です。

使用するコンポーネント

Cisco Crosswork Network Service Orchestrator(NSO)バージョン6.4.1

このドキュメントは、NSO 6.4の時点で使用可能なログオプションについて記述されています。このドキュメントの情報の大部分は複数のバージョンに適用されますが、一部のログは使用しているバージョンに比べて廃止されたり、追加されたりする可能性があります。このドキュメントでは、NSOシステムの外部にログをエクスポートするための設定については説明していません。

このドキュメントで提供されているコマンドは、デフォルトのディレクトリ設定を使用してシステムインストールNSOを前提としています。環境によっては、特定のファイルの場所が異なる場合があります。

- ncs.confは、デフォルトでは/etc/ncs/ncs.confの$NCS_CONFIG_DIRにあります
- ログは$NCS_LOG_DIRにデフォルトで保存されています。
- NSOはデフォルトで$NCSDIRにインストールされます。
- NSOの実行ディレクトリは、デフォルトでは$NCS_RUN_DIRです。/var/opt/ncs/

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

一般的なログガイドライン

ロギングの影響

より高い冗長性でログを有効にすると、NSOサーバの負荷とディスク容量の要件が増大する可能性があります。これは、特にdevel.logなどの非常にアクティブなログに関する考慮事項です。通常、トラブルシューティングの際に冗長性を短時間だけ有効にしても問題になりませんが、長時間にわたって有効にする場合は、必ずリソースとディスク領域を考慮に入れてください。

テクニカルレポートの生成

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

Options:

--install-dir

：インストーラの – install-dirオプションのように、NCS静的ファイルをインストールするディレクトリを指定します。

--full ：システムのncs-backupを収集します。これにより、シスコのサポートによるエラーの再現が容易になります。

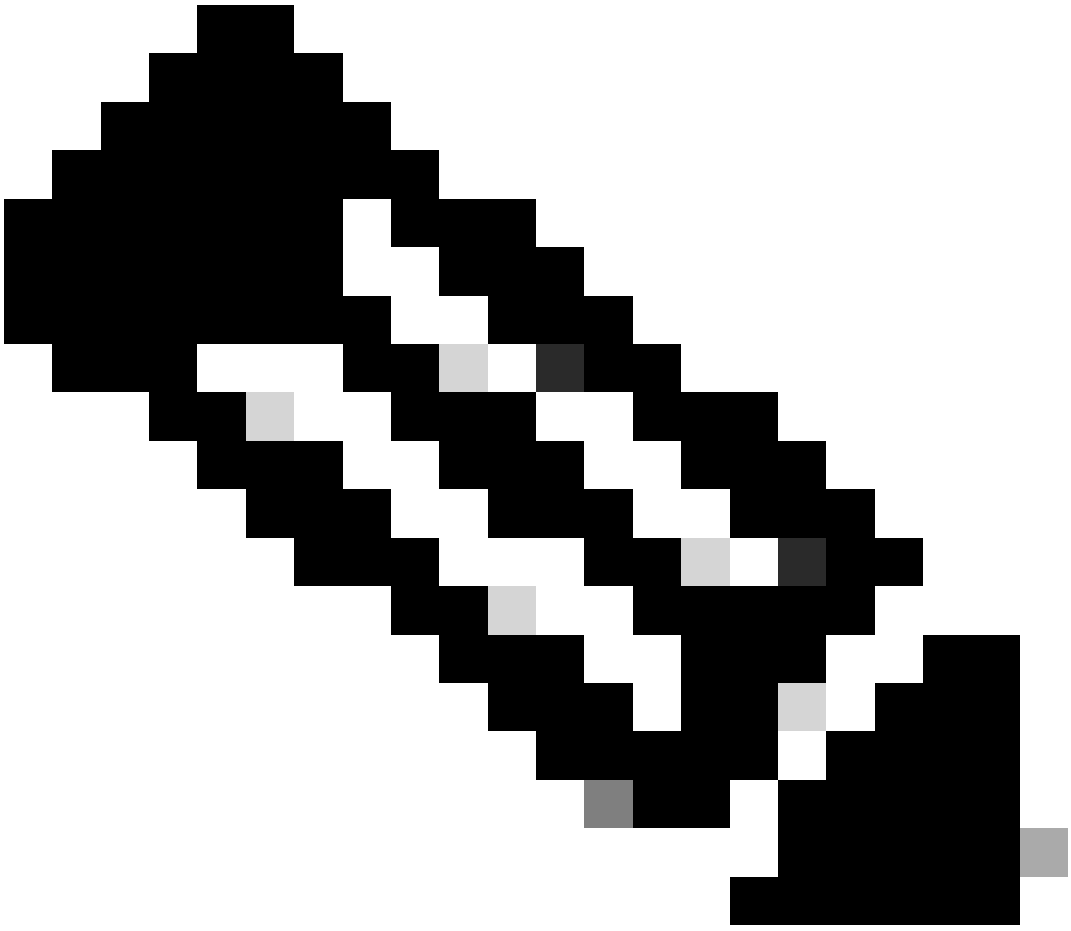
--num-debug-dumps ：デフォルトは1です。デバッグダンプスナップショットを生成します。メモリやファイル記述子のリークなど、リソースリークを追跡する場合は、この値を3に設定します。

推奨オプション：

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

バックアップを個別に収集して提供することで、バンドルのファイルサイズを制限し、アップロードを容易にすることができます。

テクニカルレポートは、スクリプトが実行される現在のディレクトリに生成されます。



注：テクニカルレポートは、NSOログディレクトリの内容を収集します。新しい技術レ

ポートを生成する前に、このディレクトリに以前の技術レポートまたはバックアップが含まれていないことを確認してください。

バックアップの生成

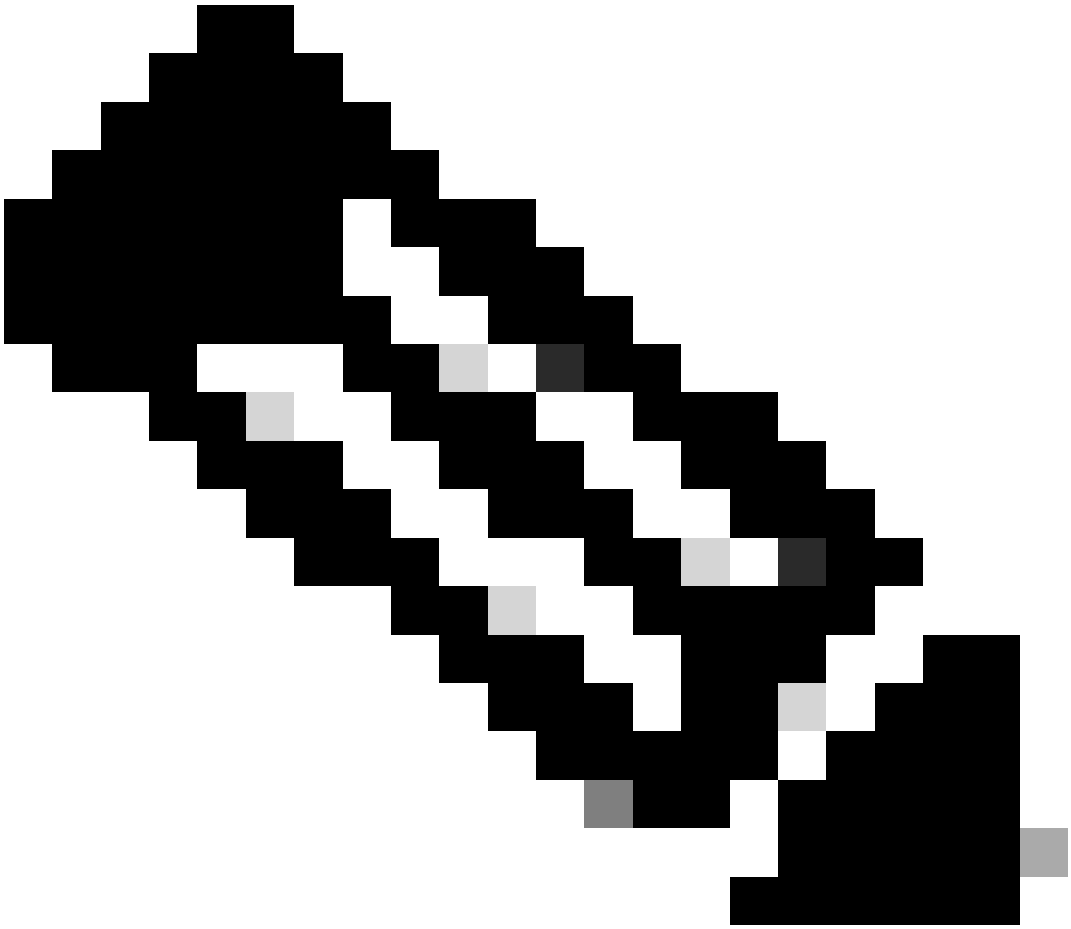
/opt/ncs/current/bin/ncs-backup

バックアップは /var/opt/ncs/backups/.

ログファイルが生成されない

ログファイルがアーカイブまたは削除されると、NSOは新しいファイルを作成する必要があります。通常、これは自動的に発生しますが、発生しなかった場合は次のコマンドを使用します。

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



注:IPCポートへのアクセスを制限する場合、たとえばncs.confでipc-access設定を使用す

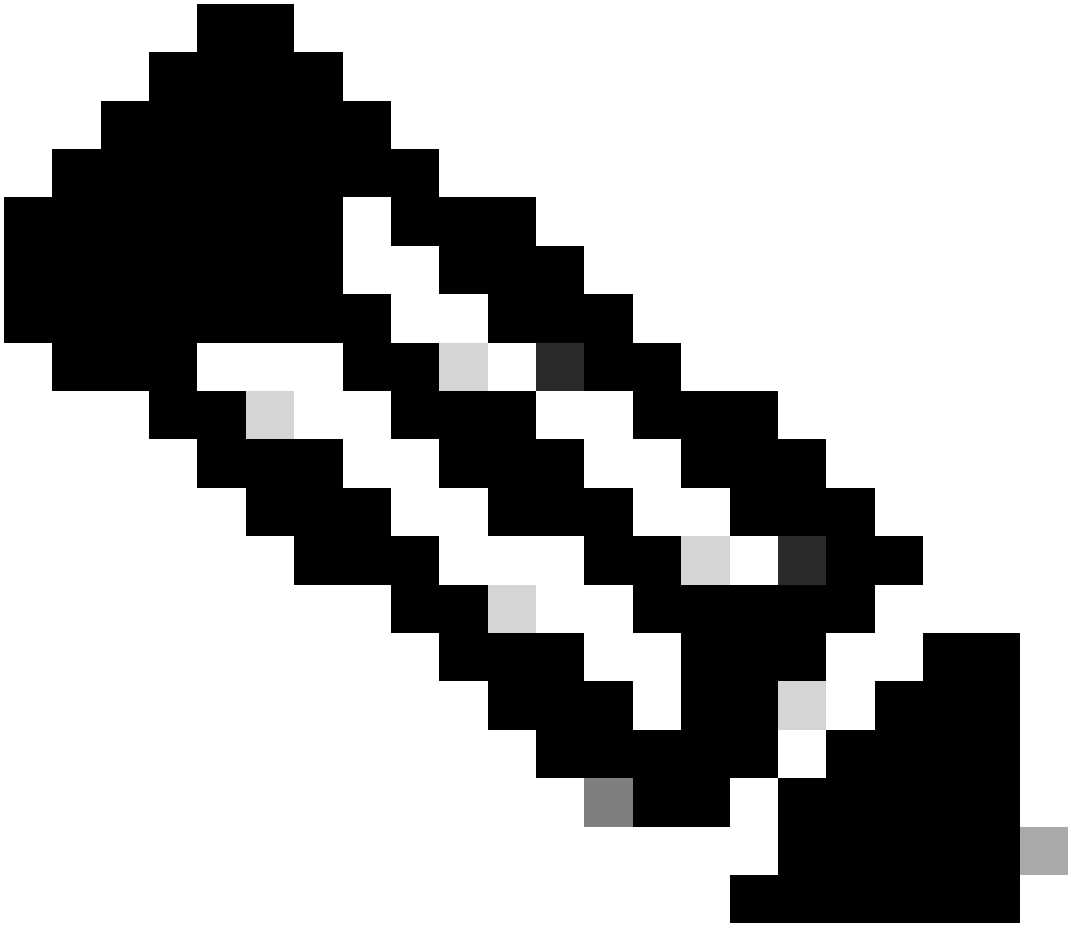
る場合は、週次ログローテーションでログを適切に再オープンできるように、必要な変数をcronまたはanacronの一部として定義していることを確認してください。

ログの概要

- NSO内部ログ
  - ncs.log:ncsログは、NSOのメインプロセスを記録します。詳細な情報は限られていますが、シャットダウン、起動、パッケージのロード、およびアップグレードに関連する問題に使用できます。
  - audit.log：監査ログには、NSOで認証するすべてのユーザがAPIを介して記録されます。また、NSO CLIおよび冗長性の低いノースバウンドインターフェイスのアクティビティもログに記録します。
  - audit-log-commit：この設定を有効にすると、audit.logが拡張されます。それ自体のログは作成されません。コミットおよび同期元の操作中にNSO CDBに対して行われたデフォルト以外のすべての変更をログに記録します。
  - audit-log-commit-defaults：この設定を有効にするとaudit.logが拡張されます。それ自体のログは作成されません。コミットおよび同期元の操作中のNSO CDBに対するデフォルトの変更をすべてログに記録します。
  - devel.log:develログには、NSOの一般的な操作とワークフローが記録されます。
  - ncs-java-vm.log:javaログは、java-vmに関連するすべての操作を記録します。Javaで記述されたNetwork Element Driver(NED)とサービスパッケージが最も重要です。すべてのCLI NEDはJavaで記述されています。
  - ncs-python-vm.log:Pythonログには、Pythonで記述されたサービスパッケージに関連するアクティビティが記録されます。Pythonで書かれたサービスパッケージごとに個別のPythonログが生成されます。NEDはPythonで記述されていません。
  - upgrade.log：アップグレードログには、NSOアップグレード中のNSOモデルの変更が記録されます。これには、NSOバージョンのアップグレード、およびパッケージのリロード中のNSOパッケージのアップグレードが含まれます。
  - raft.log:HA-Raft機能を利用するNSOクラスタ専用のログ。
  - xpath.trace: xpathトレースは、NSOが実行するすべてのxpath評価をログに記録します。これは、削除操作に時間がかかる理由を調べる場合に役立ちます。
  - ncserr.log:ncserr.logは、NCSデーモンからの内部プロセスのエラーを記録するバイナリログです。ほぼすべての「内部エラー」エラーメッセージとクラッシュシナリオに必須です。
  - transerr.log：トランザクションエラーログは、CDBブートエラーまたはランタイムトランザクション障害の原因となる、失敗したトランザクションに関する情報を収集するためのログです。
  - progress.trace：進行状況トレースは、システム内のトランザクションやアクションから発生する進行状況イベントをトレースするために使用されます。生成されるデータは/progress/traceで設定されます。
  - ncs-smart-licensing.log:NSO内のライセンススマートエージェントのログ。
- ノースバウンド：ノースバウンド要素からNSOに到達
  - audit.log：監査ログコマンドはNSO CLIで実行されます。
  - localhost:8080.access/localhost:8888.access：これは組み込みWebサーバのアクセス

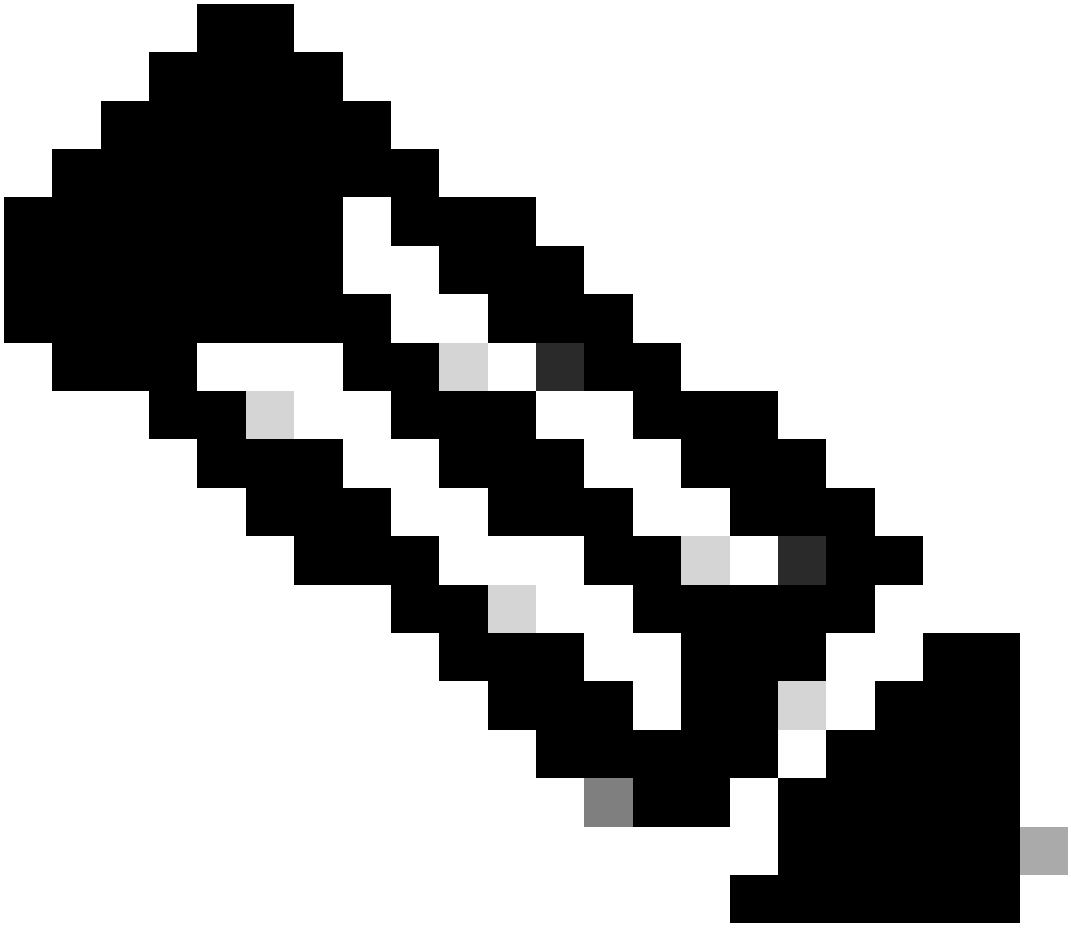
ログで、HTTPアクティビティを収集します。このファイルは、Apacheで定義されているCommon Log Formatに準拠しています
    - traffic.trace：このログは、非常に高い冗長性を持つHTTPトラフィックを収集します。これを使用して、Restconfおよびjson-rpc APIをデバッグします。
    - netconf.log:netconf APIのログ
    - netconf-trace.log：冗長性の高いnetconf APIのログ
    - json-rpc.log: json-rpc.log APIのログ
- サウスバウンド：NSOからネットワークへの通信をロギングします。
    - デバイスNEDトレース：各デバイスが独自のトレースを生成します。デバイストレースの名前はned-<ned-id>-<devicename>.traceまたはnetconf-<devicename>.traceのいずれかです。
    - audit-network.log:NSOからサウスバウンドデバイスに送信された設定コマンドを記録します。
- システム ログ
    - Linuxのログ：通常は/var/log/にあり、メッセージやsyslogなどのログが含まれます。これらはホストによって異なります。
    - ncs_crash.dump：メモリの問題によりNSOが終了したときに生成されるNSOシステムダンプ。
    - コアダンプ：メモリ不足の理由でNSOが終了すると、Linuxはcore.<PID>というコアダンプを生成します。

Linuxがコアダンプを生成するには、特定の条件を満たす必要があります。ulimit設定は、ダンプを防止する最も一般的な設定です。要件の全リストはLinuxのマニュアルページを参照してください



注：システムログはNCSテクニカルレポートによって収集されるのではなく、パフォーマンスやクラッシュに関連する問題の収集に役立つ場合があります。

ログの有効化と詳細レベルの設定



注意: ncs.confファイルの構成設定の変更は、ncs --reloadコマンドを実行して適用されます。ncs --reload, itは、ncs.confファイルの値をリロードし、実行中のシステムを更新します。また、すべてのログファイルを閉じて再度開き、ログの変更が適用されるようにします。これにより、サービスが中断されることはありません。

一般的なガイドライン

- ncs.confファイルに特定の設定がない場合、NSOは「/opt/ncs/current/src/ncs/ncs_config/tailf-ncs-config.yang」ファイルで指定されているデフォルトの動作を採用します。
- デフォルトで有効と指定されているログは、有効にする設定がない場合でも有効であることを意味します。
- 一部のログはデフォルトで無効になっていますが、NSOの最初のインストール時に、ncs.confに口グを有効にする特定の指示が含まれています。
- ncs.confファイルに特定の設定が存在しない場合は、logs containerの下に示されているように設定を追加できます。これは、ncs.confファイルの
との間を意味します。

内部

ncs.log

この口グはデフォルトで有効になっています。この口グを有効にするには、/etc/ncs/ncs.confを開き、<ncs-log> の内容を変更します。

```
        true

         ${NCS_LOG_DIR}/ncs.log

         true
```

ncs.confの編集後、ncs —reloadを実行します。

監査口グ

この口グはデフォルトで有効になっています。この口グを有効にするには、/etc/ncs/ncs.confを開き、<audit-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}/audit.log

        true
```

ncs.confの編集後、ncs —reloadを実行します。

audit-log-commitおよびaudit-log-commit-defaults

このログはデフォルトでは有効になっていません。このログを有効にするには、/etc/ncs/ncs.confを開き、<audit-log>の後にコンテンツを追加します。

```
        true

        ${NCS_LOG_DIR}/audit.log
```

```
  true
```

```
true
```

```
true
```

ncs.confの編集後、ncs —reloadを実行します。

デバイス。ログ

このログは、情報の詳細レベルでデフォルトで有効になっています。このログの冗長性を有効にして変更するには、/etc/ncs/ncs.confを開き、<developer-log>の内容を変更します。

```
 true
```

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

```
        true
```

```
      trace
```

ncs.confの編集後、ncs —reloadを実行します。

ncs-java-vm.log（仮想マシンのみ）

この口グは、情報の詳細レベルでデフォルトで有効になっています。java-vmで管理する個々の要素の冗長性を設定できます。SSHまたはncs_cli -C -noaaaを使用してアクセス可能なNSO CLIから詳細レベルが変更される

com.tailfの下にあるすべてのjava要素の冗長性を高めるには、次の手順を実行します。

config
java-vm java-logging logger com.tailf level level-trace
ネットワークを使用しない

特定のNEDパッケージの詳細レベルを上げるには、次の手順に従います。

config

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

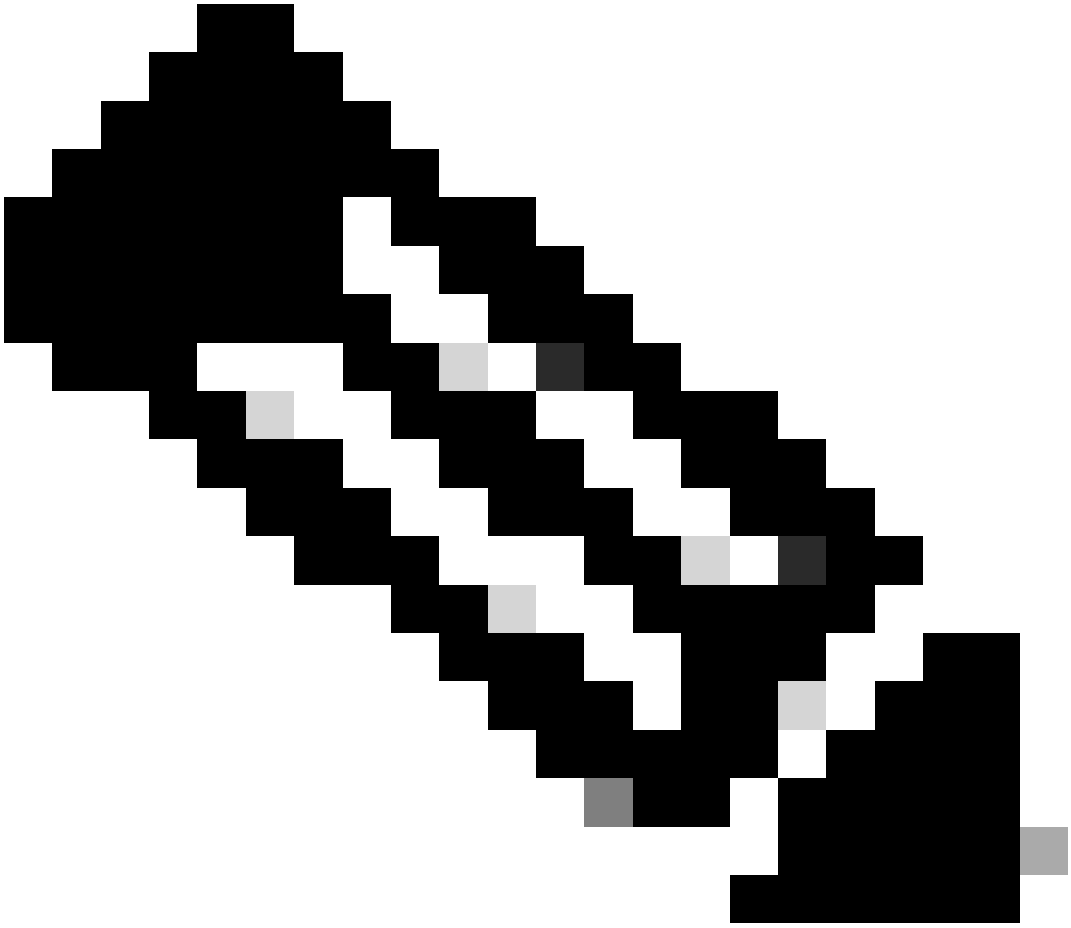
ネットワークを使用しない

Java NEDパッケージで使用されるSSHJクライアントの冗長性を高めるには、次の手順に従います。

config

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

ネットワークを使用しない



注:SSHJクライアントのロギングをlevel-errorに設定することをお勧めします。デフォルトでディセーブルになっている。

特定のJava要素のロギングを元に戻すには、次の手順に従います。

config

no java-vm java-logging logger com.tailf（デフォルト）

ネットワークを使用しない

現在のjava-vmロギング設定を表示するには、次の手順を実行します。

show running-config java-vm java-logging

ncs-python-vm.log（仮想マシンのログ）

このログは、情報の詳細レベルでデフォルトで有効になっています。SSHまたはncs_cli -C -

noaaaを使用してアクセス可能なNSO CLIから詳細レベルが変更される。

すべてのPython VMの口グの詳細レベルを設定します。

config
python-vm口ギングレベルデバッグ
ネットワークを使用しない

元に戻すには、次の手順に従います。
config
no python-vm logging level level-debug
ネットワークを使用しない

現在のpython-vm口ギング設定を表示するには、次の手順を実行します。
show running-config python-vm logging（隠しコマンド）

アップグレード。ログ

この口グはデフォルトで有効になっています。この口グを有効にするには、/etc/ncs/ncs.confを開き、<upgrade-log>の内容を変更します。

```
        true




         ${NCS_LOG_DIR}/upgrade.log



         true
```

ncs.confの編集後、ncs —reloadを実行します。

raft.log（任意）

このログは、情報の詳細レベルでデフォルトで有効になっています。このログの冗長性を有効にして設定するには、/etc/ncs/ncs.confを開き、<raft-log>の内容を変更します。

```
        true

         ${NCS_LOG_DIR}/raft.log

         true

        trace
```

ncs.confの編集後、ncs —reloadを実行します。

xpath.trace

この口グはデフォルトでは有効になっていません。この口グを有効にするには、/etc/ncs/ncs.confを開き、<xpath-trace-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}/xpath.trace
```

ncs.confの編集後、ncs —reloadを実行します。

NCSERR口グ

この口グに記録される情報は限られています。NSOは5つのエラーファイルを保持し、各ファイルの最大サイズはデフォルトで1MBです。まれに、口グデータが5 MBを超えるサイズになる問題が発生する場合は、最大サイズを増やす必要があります。この口グはデフォルトで有効になっています。この口グの最大サイズをファイルあたり10 MBに変更するには、/etc/ncs/ncs.confを開いて<error-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}/ncserr.log
```

```
        S10M
```

ncs.confの編集後、ncs —reloadを実行します。

転送ログ

このログはデフォルトでは有効ではありませんが、最初のインストール時にncs.confで有効になります。このログを有効にするには、/etc/ncs/ncs.confを開き、<transaction-error-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}/transerr.log
```

ncs.confの編集後、ncs —reloadを実行します。

進行状況。トレース

このログはデフォルトでは有効ではありませんが、最初のインストール時にncs.confで有効になります。このログを有効にするには、/etc/ncs/ncs.confを開き、<progress-trace>の内容を変更します。

```
        true




        ${NCS_LOG_DIR}
```

ncs.confの編集後、ncs —reloadを実行します。

ncs-smart-licensing.log（登録ユーザ専用）

このログはデフォルトでは有効になっていません。ログはNSO CLIから有効になります。このCLIには、SSHまたはncs_cli -C -noaaaを使用してアクセスできます。このログを有効にするには、次の手順を実行します。

config

スマートライセンススマートエージェントstdout-capture有効

ネットワークを使用しない

ロギングの変更を元に戻すには、次の手順を実行します。

config

no smart-license smart-agent stdout-capture有効

ネットワークを使用しない

ノースバウンド

ローカルホスト：xxxx.access

このログはデフォルトで有効になっています。このログの名前は、HTTPポートによって異なります。デフォルトでは8080と8888です。このログを有効にするには、/etc/ncs/ncs.confを開き、<webui-access-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}
```

ncs.confの編集後、ncs —reloadを実行します。

トラフィック.trace

この口グはデフォルトでは有効になっていません。traffic.trace口グは、/var/log/ncs/trace_20240628_010010/などのディレクトリに生成されます。この口グを有効にするには、/etc/ncs/ncs.confを開き、<webui-access-log>の内容を変更します。

```
        true

        ${NCS_LOG_DIR}

        true
```

ncs.confの編集後、ncs —reloadを実行します。

netconf.log（オプション）

このログはデフォルトで有効になっています。このログを有効にするには、/etc/ncs/ncs.confを開き、<netconf-log>の後にコンテンツを追加します。

```
        true

         ${NCS_LOG_DIR}/netconf.log

         true
```

ncs.confの編集後、ncs —reloadを実行します。

追加オプション：NSOにrpc-replyステータス「ok」または「error」を記録させるには、

```
    true
```

をの後に挿入します。

netconf-trace.log（オプション）

このログはデフォルトでは有効になっていません。このログを有効にするには、/etc/ncs/ncs.confを開き、<netconf-trace-log>の内容を変更します。

```
        true

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

ncs.confの編集後、ncs —reloadを実行します。

json-rpc.log

この口グはデフォルトでは有効になっていません。この口グを有効にするには、/etc/ncs/ncs.confを開き、<jsonrpc-log>の後にコンテンツを追加します。

```
        true

         ${NCS_LOG_DIR}/json-rpc.log

         true
```

ncs.confの編集後、ncs —reloadを実行します。

サウスバウンド

デバイスNEDトレース

この口グはデフォルトでは有効になっていません。口グはNSO CLIから有効になります。この CLIには、SSHまたはncs_cli -C -noaaaを使用してアクセスできます。

デバイスのトレースを有効にするには、次の手順を実行します。

config
devices device <devicename> trace raw
devices device <devicename> ned-setting <ned-id> logger level debug
ネットワークを使用しない

デバイスに適用されるすべての口グ設定を表示するには、show devices device <devicename> active-settingsを使用します。

デバイストレースファイルの内容をクリアするには、devices device <devicename> clear-traceを使用します。

デバイストレースを無効にするには、次の手順を実行します。

config

no devices device device <devicename> trace

ネットワークを使用しない

audit-network.log（監査ネットワークログ）

この口グはデフォルトでは有効になっていません。この口グを有効にするには、 /etc/ncs/ncs.confを開き、<audit-network-log>の後にコンテンツを追加します。

```
        true

        ${NCS_LOG_DIR}/audit-network.log

        true
```

ncs.confの編集後、ncs —reloadを実行します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。