



NX-API CLI

- [NX-API CLI について \(1 ページ\)](#)
- [NX-API CLI の使用 \(3 ページ\)](#)
- [カーネル スタック ACL \(28 ページ\)](#)
- [NX-API 応答コードの表 \(29 ページ\)](#)
- [JSON および XML 構造化出力 \(31 ページ\)](#)
- [サンプル NX-API スクリプト \(34 ページ\)](#)

NX-API CLI について

NX-API CLI は、XML 出力をサポートする Cisco NX-OS CLI システムの拡張機能です。NX-API CLI は、特定のコマンドの JSON 出力フォーマットもサポートしています。

Cisco Nexus スイッチでは、コマンドラインインターフェイス (CLI) はスイッチ上でのみ実行されます。NX-API CLI は HTTP / HTTPS を使ってスイッチの外部で CLI を使用できるようにすることで、これらの CLI のユーザー補助を改善します。この拡張機能をスイッチの既存の Cisco NX-OS CLI システムに使用できます。NX-API CLI は **show** コマンド、構成と Linux Bash をサポートします。

NX-API CLI は JSON-RPC をサポートしています。

注意事項と制約事項

NX-API CLI は、スイッチで Cisco NX-OS CLI を実行するために VSH を生成します。VSH のタイムアウトは 5 分です。Cisco NX-OS CLI の実行に 5 分以上かかると、コマンドは失敗し、「Back-end processing error.」というメッセージが表示されます。これは、NX-API コマンドのタイムアウトによって制御されます。これは、NX-API を介して要求されたコマンドを実行できる時間を制御します。この値は 300 秒に固定されており、変更できません。

転送

NX-API は、転送のように HTTP または HTTPS を使用します。CLI は、HTTP / HTTPS POST 本文にエンコードされます。

Cisco NX-OS リリース 9.2(1) 以降、NX-API 機能は HTTPS ポート 443 でデフォルトで有効になっています。HTTP ポート 80 は無効です。

NX-API は、ホスト上でネイティブに、またはゲストシェル内で実行されるアプリケーションの、UNIX ドメインソケットを介してサポートされます。

NX-API バックエンドは Nginx HTTP サーバを使用します。Nginx プロセスとそのすべての子プロセスは、CPU とメモリの使用量が制限されている Linux cgroup 保護下にあります。Nginx のメモリ使用量が cgroup の制限を超えると、Nginx プロセスは再起動されて、NX-API 構成（VRF、ポート、証明書構成）が復元されます。

メッセージ形式



- (注)
- NX-API XML 出力は、情報を使いやすいフォーマットで表示します。
 - NX-API XML は、Cisco NX-OS NETCONF 導入に直接マッピングされません。
 - NX-API XML 出力は、JSON に変換できます。

セキュリティ

- NX-API は HTTPS をサポートします。HTTPS を使用すると、デバイスへのすべての通信が暗号化されます。
- NX-API は、デフォルトでは非セキュア HTTP をサポートしていません。
- NX-API は、デフォルトでは弱い TLSv1 プロトコルをサポートしていません。

NX-API は、デバイスの認証システムに統合されています。ユーザーは、NX-API を介してデバイスにアクセスするための適切なアカウントを持っている必要があります。NX-API では HTTP basic 認証が使用されます。すべてのリクエストには、HTTP ヘッダーにユーザー名とパスワードが含まれている必要があります。



- (注) ユーザーのログイン資格情報を保護するには、HTTPS の使用を検討する必要があります。

[機能 (feature)] マネージャ CLI コマンドを使用して、NX-API を有効にすることができます。NX-API はデフォルトで無効になっています。

NX-API は、ユーザーが最初に認証に成功したときに、セッションベースの Cookie、`nxapi_auth` を提供します。セッション Cookie を使用すると、デバイスに送信される後続のすべての NX-API 要求にユーザー名とパスワードが含まれます。ユーザー名とパスワードは、完全な認証プロセスの再実行をバイパスするために、セッション Cookie で使用されます。セッション Cookie が後続の要求に含まれていない場合は、別のセッション Cookie が必要であり、認証プロセスに

よって提供されます。認証プロセスの不必要な使用を避けることで、デバイスのワークロードを軽減できます。



(注) **nxapi_auth** cookie は 600 秒（10 分）で期限切れになります。この値は固定されており、調整できません。



(注) NX-API は、スイッチ上の Programmable Authentication Module（PAM）を使用して認証を行います。**cookie** を使用して PAM の認証数を減らし、PAM の負荷を減らします。

NX-API CLI の使用

Cisco Nexus 9000 シリーズ スイッチのコマンド、コマンドタイプ、および出力タイプは、CLI を HTTP/HTTPS POST の本文にエンコードすることにより、NX-API を使用して入力されます。要求に対する応答は、XML または JSON 出力形式で返されます。



(注) NX-API 応答コードの詳細については、[NX-API 応答コードの表（29 ページ）](#) を参照してください。

NX-API CLI は、ローカルアクセスに対してはデフォルトで有効になっています。リモート HTTP アクセスに対してはデフォルトで無効になっています。

次の例は、NX-API CLI を構成して起動する方法を示しています。

- 管理インターフェイスを有効にします。

```
switch# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# interface mgmt 0
switch(config-if)# ip address 10.126.67.53/25
switch(config-if)# vrf context managment
switch(config-vrf)# ip route 0.0.0.0/0 10.126.67.1
switch(config-vrf)# end
switch#
```

- NX-API **nxapi** 機能を有効にします。

```
switch# conf t
switch(config)# feature nxapi
```

次の例は、リクエストとそのレスポンスを XML 形式で示しています。

要求:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ins_api>
```

```

<version>0.1</version>
<type>cli_show</type>
<chunk>0</chunk>
<sid>session1</sid>
<input>show switchname</input>
<output_format>xml</output_format>
</ins_api>

```

応答 :

```

<?xml version="1.0"?>
<ins_api>
  <type>cli_show</type>
  <version>0.1</version>
  <sid>eoc</sid>
  <outputs>
    <output>
      <body>
        <hostname>switch</hostname>
      </body>
      <input>show switchname</input>
      <msg>Success</msg>
      <code>200</code>
    </output>
  </outputs>
</ins_api>

```

次の例は、JSON 形式の要求とその応答を示しています。

要求:

```

{
  "ins_api": {
    "version": "0.1",
    "type": "cli_show",
    "chunk": "0",
    "sid": "session1",
    "input": "show switchname",
    "output_format": "json"
  }
}

```

応答 :

```

{
  "ins_api": {
    "type": "cli_show",
    "version": "0.1",
    "sid": "eoc",
    "outputs": {
      "output": {
        "body": {
          "hostname": "switch"
        },
        "input": "show switchname",
        "msg": "Success",
        "code": "200"
      }
    }
  }
}

```



- (注) ユーザーを削除しようとするとう失敗し、次のようなエラーメッセージが約 12 時間ごとに表示されるといふ既知の問題があります。

```
user delete failed for username:userdel: user username is currently logged in - securityd
```

この問題は、NX-API を介してスイッチにログインしているユーザーを削除しようとした場合に発生する可能性があります。この場合、次のコマンドを入力して、最初にユーザーのログアウトを試行します。

```
switch(config)# clear user username
```

その後、ユーザーの削除を再試行します。回避策を試みても問題が解決しない場合は、Cisco TAC へお問い合わせください。

NX-API で権限を root にエスカレーションする

NX-API では、管理者ユーザーの権限を root アクセスの権限にエスカレーションできます。

以下は、権限をエスカレーションするためのガイドラインです：

- 特権を root にエスカレーションできるのは管理者ユーザーのみです。
- root へのエスカレーションはパスワードで保護されています。

次の例は、管理者の権限を root にエスカレーションする方法と、エスカレーションを確認する方法を示しています。root になっても、**whoami** コマンドを実行すると **admin** として表示されることに注意してください。ただし、**admin** アカウントにはすべての root 権限があります。

最初の例：

```
<?xml version="1.0"?>
<ins_api>
  <version>1.0</version>
  <type>bash</type>
  <chunk>0</chunk>
  <sid>sid</sid>
  <input>sudo su root ; whoami</input>
  <output_format>xml</output_format>
</ins_api>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ins_api>
  <type>bash</type>
  <version>1.0</version>
  <sid>eoc</sid>
  <outputs>
    <output>
      <body>admin </body>
      <code>200</code>
      <msg>Success</msg>
    </output>
  </outputs>
</ins_api>
```

2 番目の例 :

```
<?xml version="1.0"?>
<ins_api>
  <version>1.0</version>
  <type>bash</type>
  <chunk>0</chunk>
  <sid>sid</sid>
  <input>sudo cat path_to_file </input>
  <output_format>xml</output_format>
</ins_api>

<?xml version="1.0" encoding="UTF-8"?>
<ins_api>
  <type>bash</type>
  <version>1.0</version>
  <sid>eoc</sid>
  <outputs>
    <output>
      <body>[Contents of file]</body>
      <code>200</code>
      <msg>Success</msg>
    </output>
  </outputs>
</ins_api>
```

NX-API 管理コマンド

次の表にリストされている CLI コマンドを使用して、NX-API を有効にして管理できます。

表 1: NX-API 管理コマンド

NX-API 管理コマンド	説明
feature nxapi	NX-API を有効化します。
no feature nxapi	NX-API を無効化します。
nxapi {http https} port port	ポートを指定します。
no nxapi {http https}	HTTP / HTTPS を無効化します。
show nxapi	ポートと証明書情報を表示します。

NX-API 管理コマンド	説明
nxapi certificate { httpsrct certfile httpskey keyfile } <i>filename</i>	次のアップロードを指定します： <ul style="list-style-type: none">• httpsrct が指定されている場合の HTTPS 証明書。• httpskey が指定されている場合の HTTPS キー。 HTTPS 証明書の例： <code>nxapi certificate httpsrct certfile bootflash:cert.crt</code> HTTPS キーの例： <code>nxapi certificate httpskey keyfile bootflash:privkey.key</code>
nxapi certificate enable	証明書を有効化します。

NX-API 管理コマンド	説明
nxapi certificate trustpoint <trustpoint label>	<p>Cisco NX-OS リリース 10.2(3)F 以降では、トラストポイントインフラを使用して NX-API の証明書をインポートするかまたは CA 証明書を使用できるようになりました。</p> <p>(注) 最初に証明書をインポートするように crypto ca import トラストポイントを設定するには、<i>Cisco Nexus 9000</i> セキュリティ構成ガイドを参照してください。</p> <p>(注) 現在、この形式では pkcs12 証明書のインポートのみがサポートされています。NX-API 証明書の有効化/NX-API 証明書のトラストポイントと NX-API 証明書の SUDI は相互に排他的であり、それぞれの構成は証明書/キーを上書きします。</p> <p>(注) NX-API 証明書の有効化でサポートされる証明書/キーの最大サイズは 8k です。サイズが 8k を超える場合は、NX-API 証明書トラストポイントを使用して証明書をインポートしてください。</p> <p>(注) トラストポイントインフラを使用して NX-API でカスタム証明書を構成した場合、reload ascii コマンドを入力すると、構成は失われます。デフォルトの day-1 NX-API 証明書が復元されます。reload ascii コマンドを入力すると、スイッチがリロードされます。スイッチが再び起動したら、NX-API 証明書トラストポイントの構成を再構成する必要があります。</p> <p>(注) 現在の実行構成にトラストポイントとインポートされた証明書が含まれていないが、ターゲット構成にトラストポイント「crypto ca trustpoint <trustpoint name>」の作成と「nxapi certificate trustpoint <trustpoint-name>」 CLI が含まれている場合、構成置換は失敗します。トラストポイントが存在しない場合は、「nxapi certificate trustpoint <trustpoint-label>」を試行する前に、トラストポイントを作成して証明書をインポートする必要があります。</p>

NX-API 管理コマンド	説明
nxapi certificate sudi	<p>この CLI は、Secure Unique Device Identifier (SUDI) を使用してデバイスを安全に認証する方法を提供します。</p> <p>nginx の SUDI ベースの認証は、CISCO SUDI 準拠のコントローラによって使用されます。</p> <p>SUDI は、X.509v3 証明書に含まれる IEEE 802.1AR 準拠のセキュアデバイス識別子で、Cisco デバイスの製品識別子とシリアル番号を維持します。ID は製造時に実装され、公的に識別可能なルート認証局につながれます。</p> <p>(注) NX-API が SUDI 証明書を使用している場合、ブラウザ、curl などのサードパーティアプリケーションからはアクセスできません。</p> <p>(注) 「nxapi certificate sudi」は、構成されるとカスタム証明書/キーを上書きします。カスタム証明書/キーを元に戻す方法はありません。</p> <p>(注) 「nxapi certificate sudi」と「nxapi certificate trustpoint」と「nxapi certificate enable」は排他的であり、いずれかを構成すると他の構成は削除されます。</p> <p>(注) NX-API は、SUDI 証明書ベースのクライアント証明書認証をサポートしていません。クライアント証明書認証が必要な場合は、アイデンティティ証明書を使用する必要があります。</p> <p>(注) NX-API 証明書 CLI は show run の出力に存在しないため、現在の CR/ロールバックでは、「nxapi certificate sudi」オプションで上書きした場合、カスタム証明書に戻せません。</p>
no nxapi certificate sudi	これにより、SUDI は無効になります。NX-API にはデフォルトの自己署名証明書が付属しています。

NX-API 管理コマンド	説明
nxapi ssl-ciphers weak	Cisco NX-OS リリース 9.2(1) 以降、弱い暗号はデフォルトで無効になっています。このコマンドを実行すると、デフォルトの動作が変更され、NGINX の弱い暗号が有効になります。このコマンドの no 形式を使用すると、デフォルトに戻ります（デフォルトでは弱い暗号は無効です）。
nxapi ssl-protocols {TLSv1.0 TLSv1.1 TLSv1.2 TLSv1.3}	<p>Cisco NX-OS リリース 10.2(4)M 以降、TLSv1.3 が Cisco Nexus 9000 シリーズプラットフォームスイッチでサポートされています。このコマンドを実行すると、文字列で指定された TLS バージョンが有効になります。Cisco NX-OS リリース 9.3(2) 以降では、TLSv1.2 のみがデフォルトで有効になっています。</p> <p>このコマンドの no 形式を使用すると、TLS バージョンがデフォルトのバージョンに戻ります。</p> <p>(注)</p> <ul style="list-style-type: none"> • 下位互換性のために、TLSv1.2 および TLSv1.3 を使用することをお勧めします。 <p>次に例を示します。</p> <pre>switch(config)# nxapi ssl protocols TLSv1.2 TLSv1.3</pre> <ul style="list-style-type: none"> • TLSv1.3 を構成する前に、TLSv1.3 をサポートするためのサーバーとクライアントの証明書を検証します。 • NX-API サーバー側の SUDI 証明書は、TLSv1.3 ではサポートされていません。
nxapi use-vrf vrf	デフォルト VRF、管理 VRF、または名前付き VRF を指定します。
system server session cmd-timeout <timeout>	Cisco NX-OS リリース 10.2(3)F 以降、NGINX サーバーでは、コマンドを実行するためのデフォルトのタイムアウトは 5 分です。ユーザーは、必要に応じ、およびコマンドの実行にかかる時間に応じて、タイムアウトを 60 秒（1 分）から 3600 秒（1 時間）の間の任意の値に増やすことができます。

NX-API 管理コマンド	説明
ip netns exec management iptables	<p>アクセス制限を実装したうえで、管理 VRF で実行できます。</p> <p>(注) feature bash-shell を有効にしてから、Bash シェルからコマンドを実行する必要があります。Bash シェルの詳細については、Bash の章を参照してください。</p> <p><i>Iptables</i> は、ポリシーチェーンを使用してトラフィックを許可または阻止するコマンドラインファイアウォールユーティリティであり、ほとんどのLinuxディストリビューションにプリインストールされています。</p> <p>(注) iptables を bash シェルで変更した後、リロード後も iptables を永続化する方法の詳細については、リロード間で Iptable を永続化する (27 ページ) を参照してください。</p>
nxapi idle-timeout <timeout>	<p>リリース 9.3(5) 以降では、アイドル状態の NX-API セッションが無効になるまでの時間を設定できます。指定できる時間は 1 ~ 1440 分です。デフォルトの時間は 10 分です。デフォルト値に戻すには、no nxapi idle-timeout <timeout> コマンドの no 形式を使用します。</p>

次に、SUDI の NX-API 出力の例を示します。

```
switch(config)# nxapi certificate sudi
switch# show nxapi
nxapi enabled
NXAPI timeout 10
NXAPI cmd timeout 300
HTTP Listen on port 80
HTTPS Listen on port 443
Certificate Information:
  Issuer:   issuer=CN = High Assurance SUDI CA, O = Cisco
  Expires: Aug  9 20:58:26 2099 GMT
switch#
switch#
switch# show run | sec nxapi
feature nxapi
nxapi http port 80
nxapi certificate sudi
switch#
```

次に、トラストポイントの構成例を示します。

```
switch(config)# crypto ca trustpoint ngx
switch(config-trustpoint)# crypto ca import ngx pkcs12 bootflash:server.pfx cisco123
switch(config)# nxapi certificate trustpoint ngx
switch(config)# show nxapi
nxapi enabled
NXAPI timeout 10
NXAPI cmd timeout 300
HTTP Listen on port 80
Trustpoint label ngx
```

```

HTTPS Listen on port 443
Certificate Information:
Issuer: issuer=C = IN, ST = KA, L = bang, O = cisco, OU = nxpi, CN = suprss@cisco.com,
emailAddress = suprss@cisco.com
Expires: Jan 13 06:13:50 2023 GMT
switch(config)#
switch(config)# show run | sec nxapi
feature nxapi
nxapi http port 80
nxapi certificate trustpoint ngx

```

以下は、HTTPS 証明書の正常なアップロードの例です：

```

switch(config)# nxapi certificate httpsrct certfile certificate.crt
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
switch(config)#

```



(注) 証明書を有効にする前に、証明書とキーを構成する必要があります。

以下は、HTTPS キーの正常なアップロードの例です：

```

switch(config)# nxapi certificate httpskey keyfile bootflash:privkey.key
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
switch(config)#

```

NX-API を使用したインタラクティブコマンドの操作

対話型コマンドの確認プロンプトを無効にし、エラーコード 500 によるタイムアウトを回避するには、対話型コマンドの前に[端末の **dont-ask** (**terminal dont-ask**)]を追加します。 **を使用**。複数の対話型コマンドを区切るには、それぞれが。は単一の空白文字で囲まれています。

エラー コード 500 でのタイムアウトを回避するために**端末の dont-ask** を使用する対話型コマンドの例をいくつか次に示します：

```

terminal dont-ask ; reload module 21
terminal dont-ask ; system mode maintenance

```

NX-API クライアント認証

NX-API Client Basic Authentication

NX-API clients can authenticate with the NGINX server on the switch through basic authentication over SSL/TLS. This authentication method is supported by configuring a username and password that is saved to a database on the switch. When the NX-API client initiates a connection request, it sends the Hello message which contains the username and password. Assuming the username and password exist in the database, the switch responds by sending the Hello response, which contains a cookie. After this initial

handshake is complete, the communication session is open, and the client can begin sending API calls to the switch. For additional information, see [セキュリティ](#), on page 2.

For additional information about basic authentication, including how to configure the username and password on the switch, refer to the [Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#).

NX-API のクライアント証明書認証

NX-OS 9.3(3) 以降、NX-API はクライアントが開始する証明書ベースの認証をサポートしています。証明書ベースの認証では、TLS ハンドシェイク時に信頼できる関係者、つまり認証局 (CA) を使用してクライアントとサーバーの両方を相互に認証することで、セキュリティを強化します。証明書ベースの認証では、NX-OS スイッチにアクセスするためのマシン認証だけでなく、人間による認証も可能です。

クライアント証明書認証は、有効な CA (認証局) を介して割り当てられ、NX-API クライアントに保存されている X509 SSL 証明書を使用してサポートされます。証明書は、各 NX-API ユーザー名に割り当てられます。

NX-API クライアントが Hello メッセージを使用して接続要求を開始すると、サーバーの Hello 応答に有効な CA のリストが含まれます。クライアントの応答には、NX-API クライアントが使用している特定のユーザー名の証明書など、追加の情報要素が含まれます。

NX-API クライアントは基本認証、証明書認証のいずれかを使用するように構成することができます。または証明書を優先するものの、証明書認証方式が使用できない場合は基本認証にフォールバックするように構成することもできます。

注意事項と制約事項

証明書認証には次の注意事項と制約事項があります。

- NX-API クライアントには、ユーザー名とパスワードを設定する必要があります。
- NX-API クライアントとスイッチは、デフォルトでウェルノウンポートで HTTP を介して通信します。柔軟性を高めるために、HTTP はウェルノウンポートでもサポートされます。ただし、追加のポートを設定することもできます。
- クライアント証明書認証の Python スクリプティングがサポートされています。クライアント証明書がパスフレーズで暗号化されている場合、python はパスフレーズの入力を通常どおり要求します。ただし、Python 要求ライブラリの現在の制限により、パスフレーズをスクリプトに渡すことはできません。
- NX-API クライアントとスイッチは、同じトラストポイントを使用する必要があります。
- サポートされるトラストポイントの最大数は、スイッチごとに 26 です。
- 信頼できる CA のリストは、すべての NX-API クライアントとスイッチで同じである必要があります。信頼できる CA の個別のリストはサポートされていません。
- 証明書認証は、NX-API サンドボックスではサポートされていません。
- 次の条件によって、NX-API サンドボックスがスイッチにロードされるかどうかが決まります。

- NX-API サンドボックスは、**nxapi client certificate authentication optional** または **no nxapi client certificate authentication** が構成されている場合にのみロードされます。
- NX-API サンドボックスは、接続の確立時に有効なクライアント証明書がブラウザに提示されない限り、**strict** および **two-step** 認証モードをロードしません。
- スイッチには NGINX サーバーが組み込まれています。複数のトラストポイントが設定されていても、証明書失効リスト (CRL) が1つのトラストポイントだけにインストールされている場合、NGINX の制限により NX-API クライアント証明書認証は失敗します。この制限を回避するには、すべてのトラストポイントに CRL を構成します。
- 証明書は期限切れになったり、期限切れになったりする可能性があり、CA (トラストポイント) によって設定された CRL の有効性に影響を与える可能性があります。スイッチが有効な CRL を使用できるように、設定されているすべてのトラストポイントに必ず CRL をインストールしてください。トラストポイントによって失効した証明書が存在しない場合は、空の CRL を生成、インストールし、更新する必要があります。これはたとえば週に1回行います。

暗号化 CLI を使用して CRL を更新した後、**nxapi client cert authentication** を発行して、新しく更新された CRL を再適用します。
- NX-API クライアント証明書認証が有効になっているときに ASCII リロードを使用する場合は、リロードの完了後に **nxapi client certificate authentication** を発行する必要があります。
- 証明書パスは信頼済み CA 証明書で終了している必要があります。
- TLS 用に提示されるサーバー証明書には、**extendedKeyUsage** フィールドにサーバー認証目的 (OID 1.3.6.1.5.5.7.3.1 の **id-kp 1**) が必要です。
- TLS 用に提示されるクライアント証明書には、**extendedKeyUsage** フィールドにサーバー認証目的 (OID 1.3.6.1.5.5.7.3.2 の **id-kp 1**) が必要です。
- この機能は CRL (証明書失効リスト) をサポートします。オンライン証明書ステータスプロトコル (OCSP) はサポートされていません。
- 『NX-OS セキュリティ ガイド』の追加の注意事項と制約事項に従ってください。
 - 証明書と基本認証の両方を使用します。そうすることで、証明書が何らかの理由で侵害された場合でも、正しいユーザーとパスワードが要求されます。
 - 秘密キーは秘密にしておきます。サーバーの公開キーには接続を試みるすべてのユーザーがアクセスできるからです。
 - CRL は中央 CA からダウンロードし、最新の状態に保つ必要があります。古い CRL はセキュリティリスクにつながる可能性があります。
 - トラストポイントは最新の状態に保ちます。トラストポイントまたは構成の変更が証明書認証機能に加えられた場合は、更新された情報をリロードするために、この機能を明示的に無効にしてから再度有効にします。

- **nxapi certificate https-cert certfile bootflash:** <> 「CLI」でNX-APIに関連付けられるクライアント証明書アイデンティティファイルには、最大8Kというファイルサイズの制限があります。これはDay-1の制限です。
- NX-API管理コマンドの表1において、コマンド `nxapi certificate {https-cert certfile | https-key keyfile} filename` に関連付けられる行で、サポートされる証明書ファイルの最大サイズは8K未満です。

NX-API Client Certificate Authentication Prerequisites

Before configuring certificate authentication, make sure the following are present on the switch:

1. Configure the client with a username and password. For information see [Configuring User Accounts and RBAC](#).
2. Configure the CA(s) (trustpoint) and CRL(s) (if any).

If no certificates were revoked by a trustpoint, create a blank CRL for each trustpoint.

For information, see the [Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#).

NX-API クライアント証明書認証の構成

nxapi client certificate authentication コマンドを使用して、NX-API 証明書認証を設定できます。コマンドは、認証方法を制御する制限オプションをサポートします。

この機能は、**no nxapi client certificate authentication** を使用して無効にすることができます。

NX-API クライアントの証明書認証を構成するには、次の手順を実行します。

手順の概要

1. この機能の前提条件が満たされていることを確認します。
2. **config terminal**
3. **nxapi client certificate authentication** [{optional | strict | two-step}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	この機能の前提条件が満たされていることを確認します。	「NX-API Client Certificate Authentication Prerequisites (15 ページ)」 を参照してください。
ステップ 2	config terminal 例： <pre>switch-1# config terminal Enter configuration commands, one per line. End with CNTL/Z. switch-1(config)#</pre>	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 3	<p>nxapi client certificate authentication [{optional strict two-step}]</p> <p>例 :</p> <pre>switch-1# nxapi client certificate authentication strict switch-1(config)#</pre>	<p>次のいずれかのモードで証明書認証を有効にします。</p> <ul style="list-style-type: none"> • optional はクライアント証明書を要求します。 <ul style="list-style-type: none"> • クライアントが証明書を提供すると、クライアントとサーバーの間で相互検証が行われます。 • クライアントが無効な証明書を提供した場合、認証は失敗し、基本認証へのフォールバックは行われません。 • クライアントが証明書を提供しなかった場合、認証は基本認証（ユーザー名とパスワード）にフォールバックします。 • strict は、クライアント証明書の検証を有効にし、認証のために有効なクライアント証明書の提示を要求します。 • two-step は、基本認証方式と証明書認証方式の両方が必要な 2 段階検証を有効にします。 <p>(注) スイッチにトラストポイントが構成されていない場合は、この機能を有効にすることはできず、スイッチの画面にエラーメッセージが表示されます。</p> <pre>No trustpoints configured! Please configure trustpoint using 'crypto ca trustpoint <trustpoint-label>' and associated commands, and then enable this feature.</pre>

証明書認証用の Python スクリプトの例

次の例は、認証用のクライアント証明書を使用した Python スクリプトを示しています。

```
import requests
import json

"""
Modify these please
"""
switchuser='USERID'
switchpassword='PASSWORD'
mgmtip='NXOS MANAGEMENT IP/DOMAIN NAME'

client_cert_file='PATH_TO_CLIENT_CERTIFICATE'
client_key_file='PATH_TO_CLIENT_KEY_FILE'
ca_cert='PATH_TO_CA_CERT_THAT_SIGNED_NXAPI_SERVER_CERT'
```



```

url='https://' + mgmtip + '/ins'
myheaders={'content-type':'application/json-rpc'}
payload=[
  {
    "jsonrpc": "2.0",
    "method": "cli",
    "params": {
      "cmd": "show clock",
      "version": 1
    },
    "id": 1
  }
]
response = requests.post(url,data=json.dumps(payload),
headers=myheaders,auth=(switchuser,switchpassword),cert=(client_cert_file_path,client_key_file),verify=ca_cert).json()

```

必要に応じて、スクリプトを変更できます。

- クライアント証明書認証モードによっては、スイッチパスワードをヌル値に設定することで (switchpassword=)、スイッチパスワードを省略できます。
 - **optional** および **strict** モードの場合、switchpassword= は空白のままにできます。この場合、NX-API はユーザー名とクライアント証明書のみに基づいてクライアントを認証します。
 - **two-step** モードの場合、パスワードが必要なため、switchpassword= の値を指定する必要があります。
- **POST** コマンドで verify=False を設定することで、NX-API サーバの証明書が有効であることの確認をバイパスできます。

cURL 証明書要求の例

次に、NX-API クライアント認証用の正しく構造化された cURL 証明書要求の例を示します。

```

/usr/bin/curl --user admin: --tlsv1.2 --cacert ./ca.pem --cert ./user.crt:pass123! --key ./user.key -v -X POST -H "Accept: application/json" -H "Content-type: application/json" --data '{"ins_api":{"version": "1.0", "type": "cli_show", "chunk": "0", "sid": "1", "input": "show clock","output_format": "json"}}' https://<device-management-ip>:443/ins

```

構文要素

次の表は、この要求で使用されるパラメータを示しています。

パラメータ	説明
--user	<p>ユーザーがログインするユーザー名を取得します。これは、user.crt の共通名と同じである必要があります。</p> <p>ユーザーのパスワードを指定するには、コロンの後にパスワードを指定します。例： --user username:password</p>

パラメータ	説明
--cacert	NX-API サーバー証明書に署名した CA へのパスを使用します。 サーバー証明書を検証する必要がない場合は、 -k (insecure) オプションを使用して cURL を指定します。例： <code>/usr/bin/curl -k</code>
--cert	クライアント証明書へのパスを指定します。 クライアント証明書が暗号化されている場合は、コロンの上にパスワードを指定します。例： <code>--cert user.crt:pass123!</code>
--key	クライアント証明書の秘密キーへのパスを指定します。

証明書認証の検証

正しく構成されている場合、証明書認証が行われ、NX-API クライアントはスイッチにアクセスできます。

NX-API クライアントがスイッチにアクセスできない場合は、次のガイドラインに従ってトラブルシューティングを行うことができます。

手順の概要

1. ユーザーまたはクッキーのエラーを確認します。
2. 証明書に誤りがないか確認してください。
3. エラーが発生した場合は、**no nxapi client certificate authentication**、それから **nxapi client certificate authentication** を発行して、トラストポイント、CA、CRL、または NX-OS 証明書機能に対する変更をリロードするように機能をフラッシュします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザーまたはクッキーのエラーを確認します。	次のいずれかのエラーが発生していないか、確認します： <ul style="list-style-type: none"> • 認証ヘッダーにユーザー名が指定されておらず、有効なクッキーが指定されていない • 認証ヘッダーで指定されたユーザーが正しくない • 無効なクッキーが提供された

	コマンドまたはアクション	目的
		<p>• 認証ヘッダーのユーザー名とクライアント証明書の CN フィールドのユーザー名が一致しない</p> <p>使用されている NX-API 方式に応じて、特定のエラーが表示されます：</p> <ul style="list-style-type: none"> • JSON/XML の場合、401 認証エラー：ユーザーが見つからないエラーが発生します。次に例を示します。 <pre> {{{ "code": "400", "msg": "Authentication failure - user not found." }}}</pre> • JSON RPC 2.0 の場合、-32004 無効なユーザー名またはパスワードエラーが発生します。次に例を示します。 <pre> {{ "code": -32004, "message": "Invalid username or password" }}</pre>
ステップ 2	証明書に誤りがないか確認してください。	<p>次の内容を示す HTTPs 400 エラーを探します。</p> <ul style="list-style-type: none"> • 無効または失効したクライアント証明書が提供された場合。 • スイッチに構成されている CRL の有効期限が切れている場合。 <p>次に例を示します。</p> <pre> <html> <head><title>400 The SSL certificate error</title></head> <body bgcolor="white"> <center><h1>400 Bad Request</h1></center> <center>The SSL certificate error</center> <hr><center>nginx/1.7.10</center> </body> </html></pre>
ステップ 3	エラーが発生した場合は、 no nxapi client certificate authentication 、それから nxapi client certificate authentication を発行して、トラストポイント、CA、CRL、または NX-OS 証明書機能に対する変更をリロードするように機能をフラッシュします。	証明書認証を無効にしてから、再度有効にします。

NX-API リクエスト要素

NX-API リクエスト要素は、XML フォーマットまたは JSON フォーマットでデバイスに送信されます。リクエストの HTTP ヘッダーは、リクエストのコンテンツタイプを識別する必要があります。

次の表にリストされている NX-API 要素を使用して、CLI コマンドを指定します。



- (注) ユーザーには、「`configure terminal`」コマンドを実行する権限が必要です。JSON-RPC が入力リクエストフォーマットの場合、「`configure terminal`」コマンドは、常に、ペイロード内のコマンドが実行される前に実行されます。

表 2: XML または JSON フォーマットの NX-API リクエスト要素

NX-API リクエスト要素	説明
version	NX-API バージョンを指定します。

NX-API リクエスト要素	説明
<p><i>type</i></p>	<p>実行するコマンドのタイプを指定します。</p> <p>次のタイプのコマンドがサポートされています。</p> <ul style="list-style-type: none"> • cli_show 構造化された出力が必要な CLI show コマンド。コマンドが XML 出力をサポートしていない場合は、エラーメッセージが返されます。 • cli_show_ascii ASCII 出力が必要な CLI show コマンド。これは、ASCII 出力を解析する既存のスクリプトと一致します。ユーザーは、最小限の変更で既存のスクリプトを使用できます。 • cli_conf CLI 構成コマンド • bash Bash コマンド。ほとんどの非対話型 Bash コマンドは、NX-API でサポートされています。 <p>(注)</p> <ul style="list-style-type: none"> • 各コマンドは、現在のユーザーの権限でのみ実行可能です。 • メッセージタイプが ASCII の場合、出力でパイプ操作がサポートされます。出力が XML 形式の場合、パイプ操作はサポートされていません。 • 最大 10 の連続する show コマンドがサポートされています。show コマンドの数が 10 を超える場合、11 番目以降のコマンドは無視されます。 • 対話型コマンドはサポートされていません。

NX-API リクエスト要素	説明						
チャンク	<p>一部の show コマンドは、大量の出力を返す場合があります。コマンド全体が完了する前に NX-API クライアントが出力の処理を開始するために、NX-API は show コマンドの出力チャンクをサポートしています。</p> <p>次の設定を有効または無効にできます。</p> <table border="1" data-bbox="943 510 1482 632"> <tr> <td data-bbox="943 510 1029 569">(注)</td> <td data-bbox="1029 510 1482 569">0</td> <td data-bbox="1029 510 1482 569">チャンク出力しません。</td> </tr> <tr> <td data-bbox="943 569 1029 632"></td> <td data-bbox="1029 569 1482 632">1</td> <td data-bbox="1029 569 1482 632">チャンク出力。</td> </tr> </table> <p>(注)</p> <ul style="list-style-type: none"> • チャンクをサポートするのは show コマンドだけです。一連の show コマンドが入力されると、最初のコマンドだけがチャンクされて返されます。 • XML 出力メッセージ形式の場合（XML がデフォルトです。）<または>などの特殊文字は、有効な XML メッセージを形成するために変換されます（<は<に変換されます>は &gt;に変換されます）。 <p>XML SAX を使用して、チャンクされた出力を解析できます。</p> <p>(注) チャンクが有効な場合、メッセージ形式は XML に制限されます。チャンクが有効な場合、JSON 出力形式はサポートされません。</p>	(注)	0	チャンク出力しません。		1	チャンク出力。
(注)	0	チャンク出力しません。					
	1	チャンク出力。					
<i>sid</i>	<p>セッションID要素は、応答メッセージがチャンクされている場合にのみ有効です。メッセージの次のチャンクを取得するには、前の応答メッセージの <i>sid</i> と一致する <i>sid</i> を指定する必要があります。</p>						

NX-API リクエスト要素	説明						
input	<p>入力は1つのコマンドまたは複数のコマンドです。ただし、異なるメッセージタイプに属するコマンドを混在させてはなりません。たとえば、show コマンドは cli_show メッセージタイプであり、cli_conf モードではサポートされません。</p> <p>(注) bash を除き、複数のコマンドは「;」で区切ります。(;は、単一の空白文字で囲む必要があります。)</p> <p>エラーコード 500 でタイムアウトしないように、コマンドの前に <code>terminal dont-ask</code> を付加します。次に例を示します。</p> <pre>terminal dont-ask ; cli_conf ; interface Eth4/1 ; no shut ; switchport</pre> <p>bash の場合、複数のコマンドは「;」で区切ります。(;は単一の空白文字で囲まれていません。)</p> <p>以下は、複数のコマンドの例です。</p> <p>(注)</p> <table border="1" data-bbox="980 1024 1523 1276"> <tbody> <tr> <td data-bbox="980 1024 1075 1104">cli_show</td> <td data-bbox="1075 1024 1523 1104">show version ; show interface brief ; show vlan</td> </tr> <tr> <td data-bbox="980 1104 1075 1205">cli_conf</td> <td data-bbox="1075 1104 1523 1205">interface Eth4/1 ; no shut ; switchport</td> </tr> <tr> <td data-bbox="980 1205 1075 1276">bash</td> <td data-bbox="1075 1205 1523 1276">cd /bootflash;mkdir new_dir</td> </tr> </tbody> </table>	cli_show	show version ; show interface brief ; show vlan	cli_conf	interface Eth4/1 ; no shut ; switchport	bash	cd /bootflash;mkdir new_dir
cli_show	show version ; show interface brief ; show vlan						
cli_conf	interface Eth4/1 ; no shut ; switchport						
bash	cd /bootflash;mkdir new_dir						

NX-API リクエスト要素	説明				
<i>output_format</i>	<p>使用可能な出力メッセージ形式は次のとおりです。</p> <p>(注)</p> <table border="1" data-bbox="943 348 1481 506"> <tr> <td data-bbox="943 348 1125 407">xml</td> <td data-bbox="1125 348 1481 407">XML 形式を指定します。</td> </tr> <tr> <td data-bbox="943 407 1125 506">json</td> <td data-bbox="1125 407 1481 506">JSON 形式で出力を指定します。</td> </tr> </table> <p>(注)</p> <p>Cisco NX-OS CLI は XML 出力をサポートしています。つまり、JSON 出力は XML から変換されます。変換はスイッチで処理されます。</p> <p>計算のオーバーヘッドを管理するために、JSON 出力は出力の量によって決定されます。出力が 1 MB を超える場合、出力は XML 形式で返されます。出力がチャンクされている場合、XML 出力のみがサポートされます。</p> <p>HTTP/HTTPS ヘッダーの content-type ヘッダーは、応答形式 (XML または JSON) のタイプを示します。</p>	xml	XML 形式を指定します。	json	JSON 形式で出力を指定します。
xml	XML 形式を指定します。				
json	JSON 形式で出力を指定します。				

NX-API 応答要素

CLI コマンドに回答する NX-API 要素を次の表に示します。

表 3: NX-API 応答要素

NX-API 応答要素	説明
version	NX-API バージョン。
type	実行するコマンドのタイプ。
sid	応答のセッション識別子。この要素は、応答メッセージがチャンクされている場合にのみ有効です。
outputs	<p>すべてのコマンド出力を囲むタグ。</p> <p>複数のコマンドが <code>cli_show</code> または <code>cli_show_ascii</code> にある場合、各コマンド出力は単一の出力タグで囲まれます。</p> <p>メッセージタイプが <code>cli_conf</code> または <code>bash</code> の場合、<code>cli_conf</code> および <code>bash</code> コマンドにはコンテキストが必要なため、すべてのコマンドに単一の出力タグがあります。</p>

NX-API 応答要素	説明
出力	単一のコマンド出力の出力を囲むタグ。 cli_conf と bash メッセージタイプの場合、この要素にはすべてのコマンドの出力が含まれます。
input	リクエストで指定された 1 つのコマンドを囲むタグ。この要素は、要求入力要素を適切な応答出力要素に関連付けるのに役立ちます。
本文	コマンド応答の本文。
コード	コマンドの実行から返された原因コード。 NX-API は、ハイパーテキスト転送プロトコル (HTTP) ステータスコードレジストリ (http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml) で説明されている標準規格の HTTP 原因コードを使用します。
msg	返された原因コードに関連付けられたエラーメッセージ。

NX-API へのアクセスの制限

デバイスへの HTTP および HTTPS アクセスを制限するには、ACL と iptable の 2 つの方法があります。使用する方法は、`nxapi use-vrf<vrf-name> CLI` コマンドを使用して、NX-API 通信の VRF を構成していたかどうかに応じて決まります。

特定の VRF を使用するように NX-API を構成していない場合にのみ、ACL を使用してデバイスへの HTTP または HTTPS アクセスを制限します。ACL の構成の詳細については、使用しているスイッチファミリの *Cisco Nexus* シリーズ NX-OS セキュリティ構成ガイドを参照してください。

ただし、NX-API 通信用に VRF を設定した場合、ACL は HTTP または HTTPS アクセスを制限しません。代わりに、iptables のルールを作成します。ルールの作成の詳細については、[iptables の更新 \(25 ページ\)](#) を参照してください。

iptables の更新

iptables を使用すると、VRF が NX-API 通信用に構成されている場合に、デバイスへの HTTP または HTTPS アクセスを制限できます。このセクションでは、既存の iptable に HTTP および HTTPS アクセスをブロックするルールを追加、確認、削除する方法を示します。

ステップ 1 HTTP アクセスをブロックするルールを作成するには、次の手順を実行します。

```
bash-4.3# ip netns exec management iptables -A INPUT -p tcp --dport 80 -j DROP
```

ステップ 2 HTTPS アクセスをブロックするルールを作成するには、次の手順を実行します。

```
bash-4.3# ip netns exec management iptables -A INPUT -p tcp --dport 443 -j DROP
```

ステップ3 適用されたルールを確認するには、次の手順を実行します。

```
bash-4.3# ip netns exec management iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  anywhere              anywhere        tcp dpt:http
DROP      tcp  --  anywhere              anywhere        tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

ステップ4 10.155.0.0/24 サブネットのポート 80 へのすべてのトラフィックをブロックするルールを作成して確認するには、次の手順を実行します。

```
bash-4.3# ip netns exec management iptables -A INPUT -s 10.155.0.0/24 -p tcp --dport 80 -j DROP
bash-4.3# ip netns exec management iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  10.155.0.0/24        anywhere        tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

ステップ5 以前に適用したルールを削除して確認するには、次の手順を実行します。

この例では、最初のルールを INPUT から削除します。

```
bash-4.3# ip netns exec management iptables -D INPUT 1
bash-4.3# ip netns exec management iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

次のタスク

iptables のルールを bash シェルで変更した場合、リロード後は保持されません。ルールを永続的にするには、[リロード間で Iptable を永続化する \(27 ページ\)](#) を参照してください。

リロード間で iptable を永続化する

iptables のルールを bash シェルで変更した場合、リロード後は保持されません。このセクションでは、リロード後も変更された iptable を永続化する方法について説明します。

始める前に

iptables を変更したとします。

ステップ 1 iptables_init.log という名前のファイルを /etc ディレクトリに作成します。

```
bash-4.3# touch /etc/iptables_init.log; chmod 777 /etc/iptables_init.log
```

ステップ 2 iptable の変更を保存する /etc/sysconfig/iptables ファイルを作成します。

```
bash-4.3# ip netns exec management iptables-save > /etc/sysconfig/iptables
```

ステップ 3 次の一連のコマンドを使用して、/etc/init.d ディレクトリに「iptables_init」という起動スクリプトを作成します。

```
#!/bin/sh

### BEGIN INIT INFO

# Provides:          iptables_init
# Required-Start:
# Required-Stop:
# Default-Start:    2 3 4 5
# Default-Stop:
# Short-Description: init for iptables
# Description:       sets config for iptables
#
#                   during boot time

### END INIT INFO

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
start_script() {
    ip netns exec management iptables-restore < /etc/sysconfig/iptables
    ip netns exec management iptables
    echo "iptables init script executed" > /etc/iptables_init.log
}
case "$1" in
    start)
        start_script
        ;;
    stop)
        ;;
    restart)
        sleep 1
        $0 start
```

```
;;
*)
  echo "Usage: $0 {start|stop|status|restart}"
  exit 1
esac
exit 0
```

ステップ 4 起動スクリプトに適切な権限を設定します。

```
bash-4.3# chmod 777 /etc/init.d/iptables_init
```

ステップ 5 `chkconfig` ユーティリティを使用して、「`iptables_init`」起動スクリプトを「オン」に設定します。

```
bash-4.3# chkconfig iptables_init on
```

「`iptables_init`」起動スクリプトは、リロードを実行するたびに実行されます。これで `iptables` ルールを永続的にすることができました。

カーネルスタック ACL

カーネルスタック ACL は、インバンドコンポーネントとアウトバンドコンポーネントを管理するための ACL を構成するための一般的な CLI インフラストラクチャです。

カーネルスタック ACL は、NX-OS ACL CLI を使用して、管理およびフロントパネルポート上の管理アプリケーションを保護します。単一の ACL を設定することで、NX-OS 上のすべての管理アプリケーションを保護できる必要があります。

カーネルスタック ACL は、ユーザーの手動介入を修正し、ACL が `mgmt0` インターフェイスに適用されるときに `iptables` エントリを自動的にプログラムするコンポーネントです。

以下は、カーネルスタック ACL を構成する例です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list kacl1
switch(config-acl)# statistics per-entry
switch(config-acl)# 10 deny tcp any any eq 443
switch(config-acl)# 20 permit ip any any
switch(config-acl)# end
switch#

switch(config-if)# interface mgmt0
switch(config-if)# ip access-group kacl1 in
switch(config-if)# ipv6 traffic-filter acl6 in
switch(config-if)#

switch# sh ip access-lists kacl1
IP access list kacl1
statistics per-entry
10 deny tcp any any eq 443 [match=136]
20 permit ip any any [match=44952]
switch(config)#
```

以下は、構成に基づいた `iptables` エントリのカーネルスタックフィルタリングです。

```
bash-4.4# ip netns exec management iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
```

```

num pkts bytes target prot opt in out source destination
1 9 576 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
2 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
3 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

```

```

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination

```

```

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination
bash-4.4#

```

カーネルスタック ACL サポートの制限は次のとおりです。

- この機能は、`mgmt0` インターフェイスでのみサポートされ、他のインバンドインターフェイスではサポートされません。
- ACL エントリの 5 つのタプル (`protocol`、`source-ip`、`destination-ip`、`source-port`、および `destination-port`) は、`iptables` にプログラムされています。ACL エントリで提供される残りのオプションは `iptables` でプログラムされておらず、そのような場合に警告の `syslog` をスローします。
たとえば、「警告: 一部の ACL オプションは `kstack` ではサポートされていません。部分的なルールのみがインストールされます。」
- デバイス ユーザーがホスト `bash` アクセス権を持っている場合、ユーザーは手動で `iptables` を更新できます。この更新により、プログラムされている `iptables` ルールが破損する可能性があります。
- 検証される ACE の最大数は、IPv4 トラフィックの場合は 100、IPv6 トラフィックの場合は加えてさらに 100 です。このスケール以上を適用すると、スループットに影響を与える可能性があります。

NX-API 応答コードの表



(注) 標準の HTTP エラー コードは、ハイパーテキスト転送プロトコル (HTTP) ステータス コード レジストリ (<http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>) にあります。

表 4: NX-API 応答コード

[NX-API 応答 (NX-API Response)]	コード	メッセージ
成功	200	成功。
CUST_OUTPUT_PIPED	204	要求により、出力は別の場所にパイプされます。
BASH_CMD_ERR	400	Bash コマンドエラー

CHUNK_ALLOW_ONE_CMD_ERR	400	チャンクは、1つのコマンドだけを受け入れます。
CLI_CLIENT_ERR	400	CLI の実行エラー
CLI_CMD_ERR	400	CLI コマンドエラーの入力。
IN_MSG_ERR	400	着信メッセージが無効です。
INVALID_REMOTE_IP_ERR	400	要求のリモートIPを取得できません。
NO_INPUT_CMD_ERR	400	入力コマンドがありません。
PERM_DENY_ERR	401	権限が拒否されました。
CONF_NOT_ALLOW_SHOW_ERR	405	構成モードは [表示 (show)] を許可しません。
SHOW_NOT_ALLOW_CONF_ERR	405	表示モードでは構成できません。
EXCEED_MAX_SHOW_ERR	413	連続する show コマンドの最大数を超過しました。最大値は 10 です。
MSG_SIZE_LARGE_ERR	413	応答サイズが大きすぎます。
MAX_SESSIONS_ERR	429	最大セッション数に到達しました。新しいユーザー/クライアントの場合は、しばらくしてからもう一度お試しください。
BACKEND_ERR	500	バックエンド処理エラー。
CREATE_CHECKPOINT_ERR	500	チェックポイントの作成をするエラー。
FILE_OPER_ERR	500	システム内部ファイル操作エラー。
LIBXML_NS_ERR	500	システムの内部 LIBXML NS エラー。これは要求フォーマットのエラーです。
LIBXML_PARSE_ERR	500	システムの内部 LIBXML 解析エラー。これは要求フォーマットのエラーです。
LIBXML_PATH_CTX_ERR	500	システムの内部 LIBXML パス コンテキストエラー。これは要求フォーマットのエラーです。
MEM_ALLOC_ERR	500	システムの内部メモリ割り当てエラー。
SERVER_BUSY_ERR	500	サーバーがビジー状態のため、リクエストは拒否されました。

USER_NOT_FOUND_ERR	500	入力またはキャッシュからユーザーが見つかりません。
XML_TO_JSON_CONVERT_ERR	500	XML から JSON への変換エラー。
BASH_CMD_NOT_SUPPORTED_ERR	501	Bash コマンドはサポートされていません。
CHUNK_ALLOW_XML_ONLY_ERR	501	チャンクは XML 出力のみを許可します。
JSON_NOT_SUPPORTED_ERR	501	大量の出力の可能性があるため、JSON はサポートされていません。
MSG_TYPE_UNSUPPORTED_ERR	501	メッセージタイプはサポートされていません
PIPE_XML_NOT_ALLOWED_IN_INPUT	501	このコマンドへのパイプ XML は入力では許可されていません。
STRUCT_NOT_SUPPORTED_ERR	501	構造化出力はサポートされていません。
ERR_UNDEFINED	600	不明なエラー。

JSON および XML 構造化出力

NX-OS は、次の構造化された出力フォーマットで、さまざまな **show** コマンドの標準規格出力のリダイレクトをサポートしています。

- XML
- JSON。JSON 出力の上限は 60 MB です。
- JSON フォーマット出力の標準規格ブロックを読みやすくした JSON Pretty もあります。JSON 出力の上限は 60 MB です。

NX-OS CLI で、標準の NX-OS 出力を JSON または XML インタープリターに「パイプ接続」すると、これらのフォーマットへの変換が行われます。たとえば、**show ip access** コマンドを発行する際、論理パイプ (|) を続けて、その後に出力形式を指定できます。こうすると、NX-OS コマンドの出力が適切に構造化され、その形式でエンコードされます。この機能により、プログラムによるデータの解析が可能になり、ソフトウェア ストリーミング テレメトリを介したスイッチからのストリーミングデータがサポートされます。Cisco NX-OS のほとんどのコマンドは、JSON、JSON Pretty、および XML 出力をサポートしています。整合性チェッカー コマンドなど、一部のコマンドは、すべての形式をサポートしていません。整合性チェッカー コマンドは XML をサポートしていますが、JSON のバリエーションはどれもサポートしていません。



(注) 検証エラーを回避するには、ファイルリダイレクトを使用して JSON 出力をファイルにリダイレクトし、そのファイル出力を使用します。

例:

```
Switch#show version | json > json_output ; run bash cat /bootflash/json_output
```

この機能の選択された例を以下に表示します。

JSON の概要 (JavaScript オブジェクト表記)

JSON は、判読可能なデータのために設計された軽量テキストベースのオープンスタンダードで、XML の代替になります。JSON はもともと JavaScript から設計されましたが、言語に依存しないデータ形式です。コマンド出力では、JSON および JSON プリティフォーマットがサポートされています。

ほぼすべての最新のプログラミング言語で何らかの方法でサポートされている 2 つの主要なデータ構造は次のとおりです。

- 順序付きリスト :: 配列
- 順序付けられていないリスト (名前/値のペア) :: オブジェクト

show コマンドの JSON または XML 出力には、NX-API サンドボックスからもアクセスできます。

CLI の実行

```
switch-1-vxlan-1# show cdp neighbors | json
{"TABLE_cdp_neighbor_brief_info": {"ROW_cdp_neighbor_brief_info": [{"ifindex": "83886080", "device_id": "SW-SWITCH-1", "intf_id": "mgmt0", "ttl": "148", "capability": ["switch", "IGMP_cnd_filtering"], "platform_id": "cisco AA-C0000 S-29-L", "port_id": "GigabitEthernet1/0/24"}, {"ifindex": "436207616", "device_id": "SWITCH-1-VXLAN-1 (FOC1234A01B)", "intf_id": "Ethernet1/1", "ttl": "166", "capability": ["router", "switch", "IGMP_cnd_filtering", "Supports-STP-Dispute"], "platform_id": "N3K-C3132Q-40G", "port_id": "Ethernet1/1"}]}}
BLR-VXLAN-NPT-CR-179#
```

XML および JSON 出力の例

このセクションでは、XML および JSON 出力として表示される NX-OS コマンドの例について説明します。

次の例は、ハードウェア テーブルのユニキャストおよびマルチキャストルーティング エントリを JSON 形式で表示する方法を示しています。

```
switch(config)# show hardware profile status | json
{"total_lpm": ["8191", "1024"], "total_host": "8192", "max_host4_limit": "4096", "max_host6_limit": "2048", "max_mcast_limit": "2048", "used_lpm_total": "9", "used_v4_lpm": "6", "used_v6_lpm": "3", "used_v6_lpm_128": "1", "used_host_lpm_total": "0", "used_host_v4_lpm": "0", "used_host_v6_lpm": "0", "used_mcast": "0", "used_mcast_oif1": "2", "used_host_in_host_total": "13", "used_host4_in_host": "12", "used_host6_in_host": "1", "max_ecmp_table_limit": "64", "used_ecmp_table":
```



```
"0", "mfib_fd_status": "Disabled", "mfib_fd_maxroute": "0", "mfib_fd_count": "0"
}
switch(config)#
```

次に、ハードウェア テーブルのユニキャストおよびマルチキャスト ルーティング エントリを XML 形式で表示する例を示します。

```
switch(config)# show hardware profile status | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0:fib">
  <nf:data>
    <show>
      <hardware>
        <profile>
          <status>
            <__XML__OPT_Cmd_dynamic_tcam_status>
              <__XML__OPT_Cmd_dynamic_tcam_status__readonly__>
                <__readonly__>
                  <total_lpm>8191</total_lpm>
                  <total_host>8192</total_host>
                  <total_lpm>1024</total_lpm>
                  <max_host4_limit>4096</max_host4_limit>
                  <max_host6_limit>2048</max_host6_limit>
                  <max_mcast_limit>2048</max_mcast_limit>
                  <used_lpm_total>9</used_lpm_total>
                  <used_v4_lpm>6</used_v4_lpm>
                  <used_v6_lpm>3</used_v6_lpm>
                  <used_v6_lpm_128>1</used_v6_lpm_128>
                  <used_host_lpm_total>0</used_host_lpm_total>
                  <used_host_v4_lpm>0</used_host_v4_lpm>
                  <used_host_v6_lpm>0</used_host_v6_lpm>
                  <used_mcast>0</used_mcast>
                  <used_mcast_oif1>2</used_mcast_oif1>
                  <used_host_in_host_total>13</used_host_in_host_total>
                  <used_host4_in_host>12</used_host4_in_host>
                  <used_host6_in_host>1</used_host6_in_host>
                  <max_ecmp_table_limit>64</max_ecmp_table_limit>
                  <used_ecmp_table>0</used_ecmp_table>
                  <mfib_fd_status>Disabled</mfib_fd_status>
                  <mfib_fd_maxroute>0</mfib_fd_maxroute>
                  <mfib_fd_count>0</mfib_fd_count>
                </__readonly__>
              </__XML__OPT_Cmd_dynamic_tcam_status__readonly__>
            </__XML__OPT_Cmd_dynamic_tcam_status>
          </status>
        </profile>
      </hardware>
    </show>
  </nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

この例では、JSON 形式でスイッチ上に LLDP タイマーを表示する方法を示します。

```
switch(config)# show lldp timers | json
{"ttl": "120", "reinit": "2", "tx_interval": "30", "tx_delay": "2", "hold_mplier
": "4", "notification_interval": "5"}
switch(config)#
```

この例では、XML 形式でスイッチ上に LLDP タイマーを表示する方法を示します。

```
switch(config)# show lldp timers | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:lldp">
  <nf:data>
    <show>
      <lldp>
        <timers>
          <__XML__OPT_Cmd_lldp_show_timers__readonly__>
            <__readonly__>
              <t1>120</t1>
              <reinit>2</reinit>
              <tx_interval>30</tx_interval>
              <tx_delay>2</tx_delay>
              <hold_mplier>4</hold_mplier>
              <notification_interval>5</notification_interval>
            </__readonly__>
          </__XML__OPT_Cmd_lldp_show_timers__readonly__>
        </timers>
      </lldp>
    </show>
  </nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

サンプル NX-API スクリプト

ユーザーはNX-APIでスクリプトを使用する方法を示すサンプルスクリプトにアクセスできます。サンプルスクリプトにアクセスするには、次のリンクをクリックして、必要なソフトウェアリリースに対応するディレクトリを選択します：[Cisco Nexus 9000 NX-OS NX-API](#)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。