



ゼロタッチプロビジョニング

ネットワークプロビジョニングの課題に対応するため、シスコは、ゼロタッチプロビジョニングモデルを導入しました。このモジュールでは、ゼロタッチプロビジョニング機能について説明します。



(注) ゼロタッチプロビジョニング機能は自動的に有効になり、設定は不要です。

- [ゼロタッチプロビジョニングの制約事項 \(1 ページ\)](#)
- [ゼロタッチプロビジョニングについて \(2 ページ\)](#)
- [ゼロタッチプロビジョニングの構成例 \(11 ページ\)](#)
- [ゼロタッチプロビジョニングに関する追加情報 \(40 ページ\)](#)
- [ゼロタッチプロビジョニングの機能情報 \(41 ページ\)](#)

ゼロタッチプロビジョニングの制約事項

- ゼロタッチプロビジョニングは、Cisco Catalyst 9200L SKU ではサポートされていません。
- Cisco Catalyst 9800-L ワイヤレスコントローラでは、サービスポートといずれかのデータポートが有効化され、接続されている場合、AutoInstall 機能はデフォルトでサービスポートに到達します。
- Cisco Catalyst 9800-L ワイヤレスコントローラは、仮想ポートグループ (VPG) およびネットワークアドレス変換 (NAT) をサポートしていません。したがって、アプリケーションやスクリプトは、データポートを介してゲストシェルからネットワークに通信できません。Cisco Catalyst 9800-L ワイヤレスコントローラでは、データポートまたはサービスポートを介してダウンロードされた ZTP スクリプトは、外部と通信できません。

ゲストシェルは仮想化された Linux ベースの環境で、Python などのカスタム Linux アプリケーションを実行して Cisco デバイスを自動で制御および管理するために設計されています。システムの自動プロビジョニング (デイゼロプロビジョニング) も含まれます。

ゼロタッチプロビジョニングについて

ここでは、DHCP サーバーの設定、DHCPv6 サポート、セキュア ZTP、ブートストラップ情報などについて説明します。

ゼロタッチプロビジョニングの概要

ゼロタッチプロビジョニング (ZTP) は、異機種混在ネットワーク環境でのネットワークデバイスプロビジョニングを自動化する、オープンブートストラップインターフェイスを提供します。

ZTP をサポートするデバイスが起動し、スタートアップコンフィギュレーションが見つからない場合 (初期インストール時)、デバイスはゼロタッチプロビジョニングモードに入ります。デバイスは DHCP サーバーを検索し、インターフェイスの IP アドレス、ゲートウェイ、ドメインネームシステム (DNS) サーバーの IP アドレスを使用してブートストラッププロセスを実行し、ゲストシェルを有効にします。次にデバイスは HTTP/TFTP サーバーの IP アドレスまたは URL を取得し、HTTP/TFTP サーバーからデバイスを構成する Python スクリプトをダウンロードします。

ゲストシェルは、Python スクリプトを実行するための環境を提供します。ゲストシェルは、ダウンロードした Python スクリプトを実行して、初期構成をデバイスに適用します。

初期プロビジョニングが完了したら、ゲストシェルは有効化されたままになります。詳細については、「[ゲストシェル](#)」の章を参照してください。



(注) デバイスが ZTP に失敗すると、自動インストールにフォールバックして構成ファイルを読み込みます。詳細については、「[Using AutoInstall and Setup](#)」[英語] を参照してください。

ゼロタッチプロビジョニングのための DHCP サーバの設定

ZTP では、プロビジョニングされる新しいデバイスと同じネットワークで DHCP サーバーを実行する必要があります。ZTP は、管理用ポートとインバンドポートの両方でサポートされます。

新しいデバイスをオンにすると、そのデバイスは、Python スクリプトが存在する HTTP または TFTP サーバーの IP アドレス情報と Python スクリプトのフォルダパスを DHCP サーバーから取得します。Python スクリプトの詳細については、「[Python API](#)」および「[Python CLI モジュール](#)」の各章を参照してください。

DHCP サーバは、次のオプションで DHCP 検出イベントに応答します。

- オプション 150 : (任意) 管理ネットワークにおいて、実行される Python スクリプトをホストしている HTTP または TFTP サーバーを指す IP アドレスの一覧が含まれます。

- オプション 67 : HTTP/TFTP サーバーに保存された Python スクリプトのファイルパスが含まれます。

これらの DHCP オプションを受信すると、デバイスは、HTTP または TFTP サーバーに接続して Python スクリプトをダウンロードします。この時点で、デバイスは HTTP または TFTP サーバーに到達するルートを持たないため、DHCP サーバーによって提供されるデフォルトのルートを使用します。

DHCPv6 のサポート

Cisco IOS XE Fuji 16.9.1 では、DHCP バージョン 6 のサポートがゼロタッチプロビジョニング機能に追加されました。DHCPv6 はデフォルトで有効になっており、スタートアップコンフィギュレーションなしでブートするすべてのデバイスで機能します。



(注) DHCPv6 は Catalyst 9300 および 9500 シリーズ スイッチでのみサポートされます。

DHCPv6 は、Python スクリプトの TFTP と HTTP の両方のダウンロードによってサポートされています。このダウンロードが失敗した場合、デバイスは初期設定または工場出荷時の設定（設定なし）に戻ります。DHCPv4 と DHCPv6 の両方が機能するためには、正しい HTTP または TFTP ファイルパスが DHCP 設定で指定されている必要があります。

同じインターフェイスに IPv4 と IPv6 の両方のアドレスがあるか、またはネットワーク内に 2 つの異なるインターフェイスがあることが考えられます。つまり、一方は IPv4 トラフィックを受信でき、他方は IPv6 トラフィックを受信できます。導入環境では DHCPv4 または DHCPv6 オプションのいずれかを使用することをお勧めします。

次に、DHCPv4 (/etc/dhcp/dhcpd.conf) の例を示します。

```
host <hostname> {
    hardware ethernet xx:xx:xx:xx:xx:xx;
    option dhcp-client-identifier "xxxxxxxxxxxxxxxx";
    option host-name "<hostname>".
    option log-servers x.x.x.x;
    fixed-address x.x.x.x;
    if option vendor-class-identifier = ".." {
        option vendor-class-identifier "..";
        if exists user-class and option user-class = "iPXE" {
            filename "http://x.x.x.x/.../<image>";
        } else {
            filename "http://x.x.x.x/.../<script-name>";
        }
    }
}
```

次に、ISC DHCPv6 サーバの設定例を示します。

```
option dhcp6.bootfile-url "http://[2001:DB8::21]/sample_day0_script.py";
```

セキュア ZTP

RFC 8572 に記載されているように、セキュア ZTP は、工場出荷時のデフォルト状態での起動中にデバイスを安全にプロビジョニングする技術です。プロビジョニングにより、ブートイメージが更新され、初期設定がコミットされ、ユーザー固有のスクリプトが実行されます。

既存の ZTP は、HTTP または TFTP サーバーから設定スクリプトをダウンロードしてデバイスで実行できますが、デバイスを安全にプロビジョニングすることはできません。

デバイスを安全にプロビジョニングするには、次の要件を満たす必要があります。

- 管理システムは、有効なデバイスをプロビジョニングしていることを検証する必要があります。
- デバイスは、正しいネットワークに展開されていることを検証する必要があります。
- デバイスは、プロビジョニングデータが改ざんされていないことを検証する必要があります。
- プロビジョニングでは、データ通信にセキュアなトランスポートプロトコルを使用する必要があります。

セキュア ZTP 機能はデフォルトで有効になっており、無効にすることはできません。この機能は、従来の ZTP と共存させることができます。DHCP サーバーからの応答に基づいて、ZTP またはセキュア ZTP が有効になります。オプション 67 は ZTP をトリガーし、オプション 143 または 136 はセキュア ZTP をトリガーします。

セキュア ZTP を使用するには、Cisco Manufacturer Authorized Signing Authority (MASA) サーバーから所有権バウチャーを取得する必要があります。



(注) セキュア ZTP は Python スクリプトのみをサポートします。

セキュア ZTP ワークフロー

ここでは、セキュア ZTP ワークフローについて説明します。

1. セキュア ZTP 対応のデバイスが起動し、スタートアップコンフィギュレーションが見つからない場合、デバイスは ZTP モードを開始してプラグアンドプレイ (PnP) エージェントをトリガーします。
2. PnP エージェントは DHCP サーバーを特定して、サーバーから IP アドレスを取得し、オプション 143 (DHCPv4) または 136 (DHCPv6) の応答を確認します。これらのオプションのいずれかが使用可能な場合、セキュア ZTP が開始されます。



(注) DHCP サーバーがすでに設定されている必要があります。

3. デバイスは、ブートストラップサーバーを反復処理する再帰アルゴリズムを開始し、有効なブートストラップデータの取得を試みます。

ブートストラップサーバーはリダイレクトデータを返せるため、アルゴリズムは再帰的な構造をしています。この場合、新しいブートストラップサーバーがリストの先頭に追加されます。ブートストラップデータが受信されて正常に適用されるか、またはブートストラップデータを受信しなかった後にサーバーのリストが使い果たされると、アルゴリズムは停止します。



- (注) ブートストラップサーバーは、HTTPS データ トランスポート プロトコルを使用する RESTCONF サーバーです。

4. サーバーはデバイスを検証し、プロビジョニングします。デバイスは、TLS ハンドシェイク中に Cisco Secure Unique Device Identifier (SUDI) 証明書をブートストラップサーバーに提示します。

デバイスは、以前に学習したサーバートラストアンカーと照合するか、または検証なしで、サーバー証明書を受け入れることができます。

5. デバイスは、`ietf-sztp-bootstrap-server:get-bootstrapping-data` RPC を使用し、RESTCONF POST 要求を介してサーバーからのブートストラップデータを要求します。

ブートストラップサーバーは、応答メッセージでリダイレクトデータやオンボーディングデータを提供できます。ブートストラップサーバーから受信したオンボーディング情報は、署名されたデータになります。

6. デバイスは、ブートストラップアーティファクトを含む CMS 構造のヘッダーをチェックして、復号が必要かどうか、および使用されているデータの形式 (JSON または XML) を判断します。必要に応じて、デバイスの SUDI 秘密キーを使用して復号が実行されます。

7. デバイスは、トラストアンカー (シスコのルート証明書) を使用して所有権バウチャーを検証します。所有権バウチャーは、IOSXE_SZTP 秘密キーで署名する必要があります。IOSXE_SZTP 証明書は Cisco ルートによって署名されますが、バウチャーの信頼チェーンでは IOSXE_SZTP キーを使用する必要があります。Cisco ルートによって署名された他の証明書ではエラーが発生します。

所有権バウチャーのみがデバイスのトラストアンカーに対して検証されることに注意してください。他のすべてのブートストラップアーティファクトは、所有権バウチャー内にあるユーザーの固定ドメイン証明書を使用して検証されます。

8. オンボーディング情報に特定の OS バージョンの要件が含まれている場合、デバイスは実行中の OS バージョンを確認します。要件に一致しない場合、デバイスは特定のバージョンをダウンロードしてインストールします。

OS のインストールが完了すると、デバイスが再起動し、セキュア ZTP プロセスが再開されます。

9. オンボーディング情報がブートストラップサーバーからダウンロードされた後、デバイスはゲストシェルを開始します。

ゲストシェルは、ユーザー固有のスクリプトを実行し、ダウンロードした設定を適用するために使用されます。この設定は、Cisco IOS CLI の形式または NETCONF edit-config 要求の形式で行うことができます。ゲストシェルは、ブートストラップの完了後にシャットダウンされます。

10. サーバーが信頼できる場合、デバイスは進捗メッセージをサーバーに送信します。

セキュア ZTP トランスポートプロトコル

セキュア ZTP は、RESTCONF ブートストラップサーバーと通信するときに、トランスポートプロトコルとして HTTPS を使用します。

デバイスは接続を確立すると、TLS ハンドシェイク中に Cisco Secure Unique Device Identifier (SUDI) 証明書を提示します。この証明書は認証トークンとして機能します。他の認証はサポートされていません。SUDI 証明書は、サーバー側のデバイスを検証します。

ブートストラップサーバーは、デバイスへの TLS ハンドシェイク中に独自の証明書を提示します。デバイスにこのサーバーに対応するサーバートラストアンカーがある場合、デバイスはそのサーバートラストアンカーに対してサーバー証明書の X.509 証明書検証を実行します（デバイスは、リダイレクトサーバーからサーバートラストアンカーを取得できます）。

デバイスにサーバートラストアンカーがあるが、X.509 証明書が正常に検証されない場合、デバイスはサーバートラストアンカーを破棄し、接続を受け入れ、サーバーを信頼できないものとしてマークする必要があります。

デバイスにサーバートラストアンカーがない場合、デバイスはサーバー証明書を受け入れますが、信頼できないものとしてマークします。

デバイスは RESTCONF プロトコルに従って、RPC 要求を続行する前に、ルートリソース検出を開始する必要があります。ルート検出要求の例を以下に示します。

```
GET /.well-known/host-meta HTTP/1.1
Host: example.com
Accept: application/xrd+xml
```

ルート検出応答の例を以下に示します。

```
HTTP/1.1 200 OK
Content-Type: application/xrd+xml
Content-Length: nnn
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>
  <Link rel='restconf' href='/restconf_root'/>
</XRD>
```

HREF 属性の値が RESTCONF サーバーへのフォローアップ要求で使用されるのは、次の場合です。

```
href='/restconf_root'
```

上記の要求が受信されると、`get-bootstrapping-data` RPC のヘッダーは以下のようになります。

```
POST /restconf_root/operations/ietf-sztp-bootstrap-server:  
get-bootstrapping-data HTTP/1.1
```

デバイスはプレーン XML ファイルを受信し、ファイル内のフィールドは Base64 でエンコードされます。デバイスは、情報を抽出してその構造を認識しようとする前に、Base64 デコードを実行します。デコードされた構造形式は、JSON または XML のいずれかです。

セキュア ZTP の DHCP オプション

セキュア ZTP では、DHCP リダイレクトオプション 136 (DHCPv6) および 143 (DHCPv4) がサポートされています。これらのオプションは、ブートストラップサーバーの 1 つ以上の Uniform Resource Identifier (URI) を使用してクライアントをプロビジョニングするために使用されます。

ゼロタッチプロビジョニングモードのデバイスは、DHCP ディスカバリを実行して DHCP サーバーを検出し、IP アドレスやその他の情報を受信します。DHCP クライアントがオプション 136 や 143 を受信すると、セキュア ZTP 手順が開始され、セキュア ZTP 処理機能が呼び出されます。セキュア ZTP 処理機能で障害が発生した場合、処理手順は完了するまで、またはユーザーによって中断されるまで、無期限に繰り返されます。

ブートストラップサーバー

ブートストラップサーバーは、HTTPS データ トランスポート プロトコルを使用する RESTCONF サーバーです。ブートストラップサーバーは、リダイレクトサーバーまたはオンボーディングサーバーにすることができます。

リダイレクトサーバーは、ブートストラップサーバーのリストをデバイスに送信します。デバイスは、リスト内の任意のサーバーからブートストラップを試行できます。各サーバーエントリには、サーバーアドレス、サーバーポート、および TLS ハンドシェイク中に提示されたサーバーの証明書を検証するトラストアンカー (X.509 証明書) が含まれます。トラストアンカーは、リダイレクト情報が署名されている場合、または現在のリダイレクトサーバーが信頼できる場合にのみ受け入れられます。そうでない場合は、リダイレクトサーバーから受信したすべてのトラストアンカーが廃棄されます。

オンボーディングサーバーは、実際のブートストラップデータを送信するサーバーです。ブートストラップデータには、次のタイプの情報が含まれています。

- デバイスで実行する必要がある必須の最新イメージ：バージョン要件、イメージのダウンロード URL、およびダウンロードしたイメージの検証方法に関する情報。
- 事前設定スクリプト：初期デバイス設定を適用する前に実行する必要がある Python スクリプト。
- 設定：デバイスの初期設定この設定は、Cisco IOS CLI の形式または NETCONF edit-config の形式で行うことができます。
- 設定後スクリプト：初期デバイス設定が適用された後に実行する必要がある Python スクリプト。

ブートストラップサーバーは、信頼できるサーバーまたは信頼できないサーバーに設定できます。信頼できるサーバーが送信するブートストラップデータは、必ずしも署名されてる必要はありません。信頼できるサーバーは、TLSハンドシェイク中に送信したサーバー証明書がデバイスのサーバートラストアンカーの検証に失敗した場合、信頼できないサーバーに降格されません。

ブートストラップデータ

ブートストラップデータとは、デバイスがブートストラッププロセス中に取得するデータの集合を指します。

ブートストラップデータ（リダイレクトとオンボーディング情報の両方）には、署名付きまたは署名なしがあります。署名されたブートストラップデータには、所有権バウチャー、所有者証明書、および伝達される情報が存在する必要があります。

署名されたデータは信頼されます。署名されたデータがリダイレクト情報である場合、リダイレクトされるブートストラップサーバーのトラストアンカーは、今後の TLS ハンドシェイクのために保存されます。署名されたオンボーディング情報は信頼され、デバイスに適用されます。

ブートストラップサーバーが署名付きデータを提供する場合、そのデータは信頼できると見なされます。ただし、これにより、サーバーが信頼されるわけではありません。データを受信する前にサーバーが信頼できないと見なされた場合、そのサーバーは信頼できないままになり、進捗レポートを受信しません。

署名されていないデータは、所有権バウチャーと所有者証明書アーティファクトを提示する必要はありません。実際には、これらは破棄されます（存在する場合）。署名されていないデータは、リダイレクトデータであるか、または信頼できるサーバーから受信された場合にのみ受け入れられます。信頼できないオンボーディングサーバーから署名されていないデータを受信するとエラーと見なされ、デバイスはリスト上の次のサーバーに進みます。

所有権バウチャー

所有権の割り当ては、ブートストラップメカニズムにとって重要です。所有権バウチャーは、RFC 8366 のセクション 5.3 で定義されています。バウチャーの主な目的は、所有者にプレッジを安全に割り当てることです。バウチャーは、プレッジが所有者と見なす必要があるエンティティの詳細をプレッジに提供します。

所有権バウチャーは暗号化メッセージ構文（CMS）構造を持ち、識別符号化規則でエンコード（DER エンコード）され、YANG モデルのデータが含まれています。

所有権バウチャーの例を以下に示します。

```
yang-data voucher-artifact:
+---- voucher
+---- created-on                yang:date-and-time
+---- expires-on?              yang:date-and-time
+---- assertion                 enumeration
+---- serial-number             string
+---- idevid-issuer?           binary
+---- pinned-domain-cert       binary
+---- domain-cert-revocation-checks? boolean
+---- nonce?                   binary
```

```
+---- last-renewal-date?                yang:date-and-time
```

CMS 構造は、デバイスのトラストアンカーに対応する秘密キーを使用して署名されます。デバイスは、バウチャーの署名を検証するために必要な唯一の公開キー（トラストアンカー）を伝送します。秘密キーは、バウチャーを作成するときに Cisco MASA サーバーによって使用されます。秘密キーは、Cisco Software Image Management (SWIM) サーバーに安全に保存されません。

デバイスは、トラストアンカーを使用して、CMS 構造から実際の所有権バウチャーを抽出します。所有権バウチャーの署名は、デバイスのトラストアンカーに含まれている公開キーを使用して検証されます。この検証では、追加の中間 X.509 証明書が必要になる場合があります。その場合は、所有権バウチャーに添付する必要があります。

所有権バウチャーの署名が検証されると、YANG モデルのデータフィールドが抽出されます。*created-on* フィールドが存在する場合、デバイスはバウチャーが過去に作成されたかどうかを確認します。*expires-on* フィールドが存在する場合、デバイスはバウチャーの有効期限が切れているかどうかを確認します。これらのフィールドが存在しない場合、バウチャーは拒否されます。

デバイスは、必須フィールドの *serial-number* を確認します。デバイスのシリアル番号は、TLS ハンドシェイク中にサーバーに送信されたデバイスの SUDI 証明書からサーバーによって学習されます。シリアル番号は、サーバーが適切なデバイスに適切な設定データを送信するのに役立ちます。

すべてのチェックが成功すると、デバイスはデータフィールド *pinned-domain-cert* を抽出します。これは、所有権バウチャーのメインペイロードです。固定ドメイン証明書は、Base64 でエンコードされている必要があります。デバイスは、証明書を処理する前に Base64 デコードを実行します。デコードされた証明書は、DER 形式の X509 証明書である必要があります。

検証中にエラーが発生した場合、所有権バウチャーは検証されず、ブートストラップデータは無効と見なされます。

所有者証明書

所有者証明書は、所有者のアイデンティティを公開キーにバインドする X.509 証明書です。デバイスは、このキーを使用して、伝達された情報の署名を検証できます。

デバイスは所有権バウチャーを確認した後、所有権バウチャーから抽出された固定メイン証明書を使用して、所有者証明書を検証します。

所有者証明書を表すブートストラップデータのデータフィールドは、Base64 でエンコードされます。その後、デバイスは Base64 デコードを実行します。このデコードの出力は、縮退 CMS 構造であり、DER でエンコードされ、コンテンツタイプは *signedData* です（縮退構造は、X.509 証明書を配布するために一般的に使用される形式です。この構造には署名が含まれていませんが、中間証明書を添付できます）。所有者証明書は x509 証明書であり、所有者証明書アーティファクトは、x509 証明書を伝達する縮退 CMS 構造です。

伝達される情報

伝達される情報アーティファクトは、デバイスに不可欠なブートストラップデータをエンコードします。このアーティファクトは、リダイレクトおよびオンボーディング情報のタイプをエンコードするために使用されます。

署名された情報の最後の検証ステップは、伝達された情報を含む署名付き CMS 構造の検証です。伝達される情報のデータフィールドは、Base64 でエンコードされます。デバイスは最初に Base64 デコードを実行します。

次に、所有者証明書の CMS 構造から取得した証明書と、トラストアンカーとして固定されたドメイン証明書を使用して署名を検証します。

イメージ更新サポート

ブートストラップデータに特定の OS バージョンが必要な場合、デバイスは現在実行されているソフトウェアのバージョンを確認します。一致しない場合、実行中のバージョンの方が新しい場合でも、デバイスはブートストラップデータで提供された URL を使用し、指定されたイメージをダウンロードします。URL は変更されず、デバイスによって認証情報が追加されることもありません。ブートストラップデータで複数の URL が指定されている場合、デバイスはダウンロードが成功するか、リストを使い果たすまで、URL のリストをループします。

イメージのダウンロード後、*image-verification* データがブートストラップ情報に含まれている場合、デバイスは指定されたアルゴリズムを使用してイメージのハッシュを計算し、その結果をブートストラップデータに含まれるハッシュ文字列と比較します。ブートストラップデータで複数のアルゴリズムやハッシュが指定されている場合、デバイスはリスト内で最初に見つけたサポート対象アルゴリズムを選択して、ハッシュを計算して比較します。

イメージが検証されると、イメージがインストールされ、デバイスが再起動します。ステート情報は、再起動前には保存されません。デバイスが起動すると、セキュア ZTP プロセスが再開され、イメージが更新されるまですべての手順が繰り返されます。デバイスは正しいイメージを実行しているため、イメージを更新する必要はなく、デバイスはオンボーディング情報の適用を続行します。

進捗レポート

デバイスは、ブートストラップサーバーに進捗レポートを送信します。RFC 8572 には、進捗レポートの詳細が定められています。

ブートストラップサーバーが信頼できる場合、*ietf-sztp-bootstrap-server:report-progress* RPC を使用して適切な POST 要求メッセージを受信します。

進捗レポートメッセージには、必須と任意の2種類があります。必須レポートでは、ブートストラッププロセスの開始または終了が示され、次のタイプの報告が含まれます。

- bootstrap-initiated
- bootstrap-error
- bootstrap-complete
- boot-image-installed-rebooting

- config-error
- parsing-error
- pre-script-error
- post-script-error

残りの進捗レポートメッセージは任意です。任意の進捗レポートメッセージは、ブートストラップデータで *reporting-level* パラメータが *verbose* に設定されている場合にのみサーバーに送信されます。

デバイスからサーバーへの *report-progress* 要求の例を示します。

```
POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress/HTTP/1.1
HOST: example.com
Content-Type: application/yang.data+xml

<input xmlns="urn:ietf:params:xml:ns:yang:ietf-sztp-bootstrap-server">
<progress-type>bootstrap-error</progress-type>
<message>Failed to decode data</message>
</input>
```

サーバーからの *No content* 応答の例を以下に示します。

```
HTTP/1.1 204 No Content
Date: Sat, 31 May 2021 17:02:40 GMT
Server: example-server
```

ゼロタッチプロビジョニングの構成例

TFTP コピーを使用する管理ポートにおける DHCP サーバ設定の例

DHCP サーバーがデバイスの管理ポート経由で接続されている場合に、TFTP のコピーを使用して DHCP サーバーを設定する例を以下に示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp excluded-address vrf Mgmt-vrf 10.1.1.1 10.1.1.10
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# vrf Mgmt-vrf
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 150 ip 203.0.113.254
Device(config-dhcp)# option 67 ascii /sample_python_dir/python_script.py
Device(config-dhcp)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# no ip dhcp client request tftp-server-address
Device(config-if)# end
```

HTTP コピーを使用しての管理ポートにおける DHCP サーバ設定の例

DHCP サーバがデバイスの管理ポート経由で接続されている場合に、HTTP のコピーを使用して DHCP サーバを設定する例を以下に示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# vrf Mgmt-vrf
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii http://198.51.100.1:8000/sample_python_2.py
Device(config-dhcp)# end
```

TFTP コピーを使用したインバンドポートでのサンプル DHCP サーバ構成

DHCP サーバがデバイスのインバンドポート経由で接続されている場合に、TFTP のコピーを使用して DHCP サーバを設定する例を以下に示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 150 ip 203.0.113.254
Device(config-dhcp)# option 67 ascii /sample_python_dir/python_script.py
Device(config-dhcp)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# no ip dhcp client request tftp-server-address
Device(config-if)# end
```

HTTP コピーを使用したインバンドポートでのサンプル DHCP サーバ構成

DHCP サーバがデバイスのインバンドポート経由で接続されている場合に、HTTP のコピーを使用して DHCP サーバを設定する例を以下に示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii http://192.0.2.1:8000/sample_python_2.py
Device(config-dhcp)# end
```

Linux Ubuntu デバイス上でのサンプル DHCP サーバの構成

次の DHCP サーバ構成例は、サーバがデバイスの管理ポートまたはインバンドポートに接続されており、Python スクリプトが TFTP サーバからコピーされることを示しています。

```
root@ubuntu-server:/etc/dhcp# more dhcpd.conf
subnet 10.1.1.0 netmask 255.255.255.0 {
  range 10.1.1.2 10.1.1.255;
  host 3850 {
    fixed-address 10.1.1.246 ;
    hardware ethernet CC:D8:C1:85:6F:00;
    option bootfile-name !<opt 67> "/python_dir/python_script.py";
    option tftp-server-name !<opt 150> "203.0.113.254";
  }
}
```

次のサンプル DHCP 構成は、Python スクリプトが HTTP サーバからデバイスにコピーされることを示しています。

```
Day0_with_mgmt_port_http
-----
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.2 192.168.1.255;
  host C2-3850 {
    fixed-address 192.168.1.246 ;
    hardware ethernet CC:D8:C1:85:6F:00;
    option bootfile-name "http://192.168.1.46/sample_python_2.py";
  }
}
```

DHCP サーバの稼働が開始されたら、ネットワークに接続された管理デバイスを起動する必要があります。他は自動的に設定されます。

TFTP コピーを使用する管理ポートでの DHCPv6 サーバ設定の例

DHCPv6 サーバがデバイスの管理ポート経由で接続されている場合に、TFTP コピーを使用して設定する例を以下に示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool ztp
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# domain-name cisco.com
Device(config-dhcpv6)# bootfile-url tftp://[2001:db8::46]/sample_day0_script.py
Device(config-dhcpv6)# exit
Device(config)# interface vlan 20
Device(config-if)# ipv6 dhcp server ztp
Device(config-if)# end
```

サンプルの Python プロビジョニングスクリプト

HTTP サーバーまたは TFTP サーバーのいずれかから使用できる Python スクリプト例を以下に示します。

```
print "\n\n *** Sample ZTP Day0 Python Script *** \n\n"

# Importing cli module
import cli

print "\n\n *** Executing show platform *** \n\n"
cli_command = "show platform"
cli.execute(cli_command)

print "\n\n *** Executing show version *** \n\n"
cli_command = "show version"
cli.execute(cli_command)

print "\n\n *** Configuring a Loopback Interface *** \n\n"
cli.configure(["interface loop 100", "ip address 10.10.10.10 255.255.255.255", "end"])

print "\n\n *** Executing show ip interface brief *** \n\n"
cli_command = "sh ip int brief"
cli.execute(cli_command)

print "\n\n *** ZTP Day0 Python Script Execution Complete *** \n\n"
```

Cisco 4000 シリーズ サービス統合型ルータの起動ログ

次のゼロタッチプロビジョニングの起動ログでは、ゲストシェルが正常に有効にされ、Python スクリプトがゲストシェルにダウンロードされ、ゲストシェルがダウンロードした Python スクリプトを実行してデバイスをデイズロに設定していることが示されています。

```
% failed to initialize nvram
! <This message indicates that the startup configuration
is absent on the device. This is the first indication that the Day Zero work flow is
going to start.>
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco ISR4451-X/K9 (2RU) processor with 7941237K/6147K bytes of memory.
Processor board ID FJC1950D091
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
7341807K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.

%INIT: waited 0 seconds for NVRAM to be available

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: %

!!<DO NOT TOUCH. This is Zero-Touch Provisioning>>

Generating 2048 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable

Guestshell enabled successfully

*** Sample ZTP Day0 Python Script ***

*** Configuring a Loopback Interface ***

Line 1 SUCCESS: interface loop 100

Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255

Line 3 SUCCESS: end

*** Executing show ip interface brief ***

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	unset	down	down
GigabitEthernet0/0/1	unassigned	YES	unset	down	down
GigabitEthernet0/0/2	unassigned	YES	unset	down	down
GigabitEthernet0/0/3	192.168.1.246	YES	DHCP	up	up
GigabitEthernet0	192.168.1.246	YES	DHCP	up	up
Loopback100	10.10.10.10	YES	TFTP	up	up

*** ZTP Day0 Python Script Execution Complete ***

Press RETURN to get started!

デイゼロプロビジョニングが完了すると、IOS プロンプトを利用できるようになります。

Cisco Catalyst 9000 シリーズスイッチの起動ログ

次の項では、ゼロタッチプロビジョニングの起動ログの例を示します。このようなログでは、ゲストシェルが正常に有効にされ、Python スクリプトがゲストシェルにダウンロードされ、ゲストシェルがダウンロードした Python スクリプトを実行してデバイスをデイゼロに設定していることが示されています。

=

```
% Checking backup nvram
% No config present. Using default config

FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled

! <This message indicates that the startup configuration
is absent on the device. This is the first indication that the Day Zero work flow is
going to start.>
```

Cisco IOS XE Everest 16.6.x から Cisco IOS XE Fuji 16.8.x へ

.py スクリプトを実行する前の起動ログの例を以下に示します。

```
Press RETURN to get started!

The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable

*** Sample ZTP Day0 Python Script ***

...

*** ZTP Day0 Python Script Execution Complete ***
```

デバイスでの Day-0 プロビジョニングの設定例を以下に示します。

```
Initializing Hardware...

System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)
Compiled Thu 02/20/2020 23:47:51.50 by rel

Current ROMMON image : Primary
Last reset cause      : SoftwareReload
C9300-48UXM platform with 8388608 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0
```

```
boot: attempting to boot from [flash:cat9k_iosxe.16.06.05.SPA.bin]
boot: reading file cat9k_iosxe.16.06.05.SPA.bin
#####
```

```
Both links down, not waiting for other switches
Switch number is 1
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.6.5, RELEASE SOFTWARE (fc3)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 10-Dec-18 12:52 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

```
% Checking backup nvram
% No config present. Using default config
```

```
FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```

cisco C9300-48UXM (X86) processor with 1392780K/6147K bytes of memory.
Processor board ID FCW2144L045
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address       : ec:1d:8b:0a:68:00
Motherboard Assembly Number     : 73-17959-06
Motherboard Serial Number       : FOC21418FPQ
Model Revision Number           : B0
Motherboard Revision Number     : A0
Model Number                    : C9300-48UXM
System Serial Number            : FCW2144L045

%INIT: waited 0 seconds for NVRAM to be available

SETUP: new interface Vlan1 placed in "shutdown" state

Press RETURN to get started!

*Sep  4 20:35:07.330: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized
*Sep  4 20:35:07.493: %IOSXE_RP_NV-3-NV_ACCESS_FAIL: Initial read of NVRAM contents
failed
*Sep  4 20:35:07.551: %IOSXE_RP_NV-3-BACKUP_NV_ACCESS_FAIL: Initial read of backup NVRAM
contents failed
*Sep  4 20:35:10.932: dev_pluggable_optics_selftest attribute table internally inconsistent
@ 0x1D4

*Sep  4 20:35:13.406: %CRYPTO-4-AUDITWARN: Encryption audit check could not be performed
*Sep  4 20:35:13.480: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Sep  4 20:35:13.715: %LINK-3-UPDOWN: Interface Lsmpi18/3, changed state to up
*Sep  4 20:35:13.724: %LINK-3-UPDOWN: Interface EOBC18/1, changed state to up
*Sep  4 20:35:13.724: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Sep  4 20:35:13.724: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
down
*Sep  4 20:35:13.725: %LINK-3-UPDOWN: Interface LIIN18/2, changed state to up
*Sep  4 20:35:13.749: WCM-PKI-SHIM: buffer allocation failed for SUDI support check
*Sep  4 20:35:13.749: PKI/SSL unable to send Sudi support to WCM
*Sep  4 20:35:14.622: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-vrf
created with ID 1,
    ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*Sep  4 20:34:42.022: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack
port 1 on Switch 1 is nocable
*Sep  4 20:34:42.022: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack
port 2 on Switch 1 is down
*Sep  4 20:34:42.022: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack
port 2 on Switch 1 is nocable
*Sep  4 20:34:42.022: %STACKMGR-6-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 1 has
been added to the stack.
*Sep  4 20:34:42.022: %STACKMGR-6-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 1 has
been added to the stack.
*Sep  4 20:34:42.022: %STACKMGR-6-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 1 has
been added to the stack.
*Sep  4 20:34:42.022: %STACKMGR-6-ACTIVE_ELECTED: Switch 1 R0/0: stack_mgr: Switch 1
has been elected ACTIVE.
*Sep  4 20:35:14.728: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi18/3, changed
state to up
*Sep  4 20:35:14.728: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC18/1, changed

```

```
state to up
*Sep 4 20:35:15.506: %HMANRP-6-HMAN_IOS_CHANNEL_INFO: HMAN-IOS channel event for switch
1: EMP_RELAY: Channel UP!
*Sep 4 20:35:15.510: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Sep 4 20:35:34.501: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively
down
*Sep 4 20:35:34.717: %SYS-5-RESTART: System restarted --
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.5,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 10-Dec-18 12:52 by mcpre
*Sep 4 20:35:34.796: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Sep 4 20:35:35.266: %SYS-6-BOOTTIME: Time taken to reboot after reload = 283 seconds
*Sep 4 20:35:35.796: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
*Sep 4 20:35:36.607: %LINK-3-UPDOWN: Interface GigabitEthernet1/1/1, changed state to
down
*Sep 4 20:35:36.607: %LINK-3-UPDOWN: Interface GigabitEthernet1/1/2, changed state to
down
*Sep 4 20:35:36.607: %LINK-3-UPDOWN: Interface GigabitEthernet1/1/3, changed state to
down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface GigabitEthernet1/1/4, changed state to
down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/1, changed state
to down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/2, changed state
to down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/3, changed state
to down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/4, changed state
to down
*Sep 4 20:35:36.608: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/5, changed state
to down
*Sep 4 20:35:36.609: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/6, changed state
to down
*Sep 4 20:35:36.609: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/7, changed state
to down
*Sep 4 20:35:36.609: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/8, changed state
to down
*Sep 4 20:35:36.609: %LINK-3-UPDOWN: Interface FortyGigabitEthernet1/1/1, changed state
to down
*Sep 4 20:35:36.609: %LINK-3-UPDOWN: Interface FortyGigabitEthernet1/1/2, changed state
to down
*Sep 4 20:35:37.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/1,
changed state to down
*Sep 4 20:35:37.608: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/2,
changed state to down
*Sep 4 20:35:37.608: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/3,
changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/4,
changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/1/1, changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/1/2, changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/1/3, changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/1/4, changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/1/5, changed state to down
*Sep 4 20:35:37.609: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

```
TenGigabitEthernet1/1/6, changed state to down
*Sep  4 20:35:43.511: AUTOINSTALL: Obtain tftp server address (opt 150) 159.14.27.2
*Sep  4 20:35:43.511: PNPA: Setting autoinstall complete to true for 159.14.27.2
*Sep  4 20:35:57.673: %PLATFORM_PM-6-FRULINK_INSERTED: 8x10G uplink module inserted in
the switch 1 slot 1
*Sep  4 20:36:19.562: [IOX DEBUG] Guestshell start API is being invoked

*Sep  4 20:36:19.562: [IOX DEBUG] provided idb is mgmt interface

*Sep  4 20:36:19.562: [IOX DEBUG] Setting up guestshell to use mgmt-intf

*Sep  4 20:36:19.562: [IOX DEBUG] Setting up chasfs for iox related activity

*Sep  4 20:36:19.562: [IOX DEBUG] Setting up for iox pre-clean activity if needed

*Sep  4 20:36:19.562: [IOX DEBUG] Waiting for iox pre-clean setup to take affect

*Sep  4 20:36:19.562: [IOX DEBUG] Waited for 1 sec(s) for iox pre-clean setup to take
affect

*Sep  4 20:36:19.562: [IOX DEBUG] Auto-configuring iox feature

*Sep  4 20:36:19.563: [IOX DEBUG] Waiting for CAF and ioxman to be up, in that order

*Sep  4 20:36:20.076: %UICFGEXP-6-SERVER_NOTIFIED_START: Switch 1 R0/0: psd: Server iox
has been notified to start
*Sep  4 20:36:23.564: [IOX DEBUG] Waiting for another 5 secs

*Sep  4 20:36:28.564: [IOX DEBUG] Waiting for another 5 secs
The process for the command is not responding or is otherwise unavailable

*Sep  4 20:36:33.564: [IOX DEBUG] Waiting for another 5 secs
The process for the command is not responding or is otherwise unavailable

*Sep  4 20:36:34.564: [IOX DEBUG] Waited for 16 sec(s) for CAF and ioxman to come up

*Sep  4 20:36:34.564: [IOX DEBUG] Validating if CAF and ioxman are running

*Sep  4 20:36:34.564: [IOX DEBUG] CAF and ioxman are up and running

*Sep  4 20:36:34.564: [IOX DEBUG] Building the simple mgmt-intf enable command string

*Sep  4 20:36:34.564: [IOX DEBUG] Enable command is: request platform software iox-manager
app-hosting guestshell enable

*Sep  4 20:36:34.564: [IOX DEBUG] Issuing guestshell enable command and waiting for it
to be up
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable

*Sep  4 20:36:38.578: [IOX DEBUG] Waiting for another 5 secs
The process for the command is not responding or is otherwise unavailable

*Sep  4 20:36:39.416: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/48, changed state
to up
*Sep  4 20:36:40.416: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/48,
changed state to upThe process for the command is not responding or is otherwise
unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
```

```

*Sep  4 20:36:43.586: [IOX DEBUG] Waiting for another 5 secs
Guestshell enabled successfully

*Sep  4 20:37:45.321: [IOX DEBUG] Checking for guestshell mount path

*Sep  4 20:37:45.321: [IOX DEBUG] Validating if guestshell is ready for use

*Sep  4 20:37:45.321: [IOX DEBUG] Guestshell enabled successfully

*** Sample ZTP Day0 Python Script ***

*** Executing show platform ***

Switch  Ports   Model                Serial No.   MAC address   Hw Ver.     Sw Ver.
-----  -
1       62      C9300-48UXM          FCW2144L045  ec1d.8b0a.6800 V01         16.6.5

Switch/Stack Mac Address : ec1d.8b0a.6800 - Local Mac Address
Mac persistency wait time: Indefinite
Current
Switch#  Role      Priority   State
-----  -
*1       Active    1         Ready

*** Executing show version ***

Cisco IOS XE Software, Version 16.06.05
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.5,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 10-Dec-18 12:52 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)
Switch uptime is 2 minutes
Uptime for this control processor is 4 minutes
System returned to ROM by Reload Command
System image file is "flash:cat9k_iosxe.16.06.05.SPA.bin"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you

```

agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>
If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

```

-----
Technology-package      Technology-package
Current                 Type                 Next reboot
-----
network-advantage     Permanent           network-advantage
cisco C9300-48UXM (X86) processor with 1392780K/6147K bytes of memory.
Processor board ID FCW2144L045
36 Ethernet interfaces
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
20 Ten Gigabit Ethernet interfaces
2 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
Base Ethernet MAC Address      : ec:1d:8b:0a:68:00
Motherboard Assembly Number    : 73-17959-06
Motherboard Serial Number      : FOC21418FPQ
Model Revision Number          : B0
Motherboard Revision Number    : A0
Model Number                   : C9300-48UXM
System Serial Number           : FCW2144L045
Switch Ports Model             SW Version           SW Image              Mode
-----
* 1 62 C9300-48UXM 16.6.5 CAT9K_IOSXE BUNDLE
Configuration register is 0x102

```

*** Configuring a Loopback Interface ***

```

Line 1 SUCCESS: interface loop 100
Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255
Line 3 SUCCESS: end

```

*** Executing show ip interface brief ***

```

Interface      IP-Address      OK? Method Status        Protocol
Vlan1          unassigned     YES unset  administratively down  down
GigabitEthernet0/0  10.127.128.3  YES DHCP    up            up
Tw1/0/1        unassigned     YES unset  down          down
Tw1/0/2        unassigned     YES unset  down          down
Tw1/0/3        unassigned     YES unset  down          down
Tw1/0/4        unassigned     YES unset  down          down
Tw1/0/5        unassigned     YES unset  down          down
Tw1/0/6        unassigned     YES unset  down          down
Tw1/0/7        unassigned     YES unset  down          down
Tw1/0/8        unassigned     YES unset  down          down
Tw1/0/9        unassigned     YES unset  down          down
Tw1/0/10       unassigned     YES unset  down          down
Tw1/0/11       unassigned     YES unset  down          down
Tw1/0/12       unassigned     YES unset  down          down
Tw1/0/13       unassigned     YES unset  down          down

```

```

Tw1/0/14          unassigned      YES unset   down      down
Tw1/0/15          unassigned      YES unset   down      down
Tw1/0/16          unassigned      YES unset   down      down
Tw1/0/17          unassigned      YES unset   down      down
Tw1/0/18          unassigned      YES unset   down      down
Tw1/0/19          unassigned      YES unset   down      down
Tw1/0/20          unassigned      YES unset   down      down
Tw1/0/21          unassigned      YES unset   down      down
Tw1/0/22          unassigned      YES unset   down      down
Tw1/0/23          unassigned      YES unset   down      down
Tw1/0/24          unassigned      YES unset   down      down
Tw1/0/25          unassigned      YES unset   down      down
Tw1/0/26          unassigned      YES unset   down      down
Tw1/0/27          unassigned      YES unset   down      down
Tw1/0/28          unassigned      YES unset   down      down
Tw1/0/29          unassigned      YES unset   down      down
Tw1/0/30          unassigned      YES unset   down      down
Tw1/0/31          unassigned      YES unset   down      down
Tw1/0/32          unassigned      YES unset   down      down
Tw1/0/33          unassigned      YES unset   down      down
Tw1/0/34          unassigned      YES unset   down      down
Tw1/0/35          unassigned      YES unset   down      down
Tw1/0/36          unassigned      YES unset   down      down
Tw1/0/37          unassigned      YES unset   down      down
Tel1/0/38         unassigned      YES unset   down      down
Tel1/0/39         unassigned      YES unset   down      down
Tel1/0/40         unassigned      YES unset   down      down
Tel1/0/41         unassigned      YES unset   down      down
Tel1/0/42         unassigned      YES unset   down      down
Tel1/0/43         unassigned      YES unset   down      down
Tel1/0/44         unassigned      YES unset   down      down
Tel1/0/45         unassigned      YES unset   down      down
Tel1/0/46         unassigned      YES unset   down      down
Tel1/0/47         unassigned      YES unset   down      down
Tel1/0/48         unassigned      YES unset   up        up
GigabitEthernet1/1/1 unassigned      YES unset   down      down
GigabitEthernet1/1/2 unassigned      YES unset   down      down
GigabitEthernet1/1/3 unassigned      YES unset   down      down
GigabitEthernet1/1/4 unassigned      YES unset   down      down
Tel1/1/1          unassigned      YES unset   down      down
Tel1/1/2          unassigned      YES unset   down      down
Tel1/1/3          unassigned      YES unset   down      down
Tel1/1/4          unassigned      YES unset   down      down
Tel1/1/5          unassigned      YES unset   down      down
Tel1/1/6          unassigned      YES unset   down      down
Tel1/1/7          unassigned      YES unset   down      down
Tel1/1/8          unassigned      YES unset   down      down
Fo1/1/1          unassigned      YES unset   down      down
Fo1/1/2          unassigned      YES unset   down      down
Loopback100      10.10.10.10    YES TFTP    up        up

```

*** Configuring username, password, SSH ***

```

Line 1 SUCCESS: username cisco privilege 15 password cisco
Line 2 SUCCESS: ip domain name domain
Line 3 SUCCESS: line vty 0 15
Line 4 SUCCESS: login local
Line 5 SUCCESS: transport input all
Line 6 SUCCESS: end

```


Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at <http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration of the applicable license term (e.g., 90-day trial period). Cisco reserves the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

```
% Checking backup nvram
% No config present. Using default config
```

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco C9300-48UXM (X86) processor with 1419044K/6147K bytes of memory.
Processor board ID FCW2144L045
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
```

```
Base Ethernet MAC Address       : ec:1d:8b:0a:68:00
Motherboard Assembly Number     : 73-17959-06
Motherboard Serial Number       : FOC21418FPQ
Model Revision Number           : B0
Motherboard Revision Number     : A0
Model Number                     : C9300-48UXM
System Serial Number            : FCW2144L045
```

```
%INIT: waited 0 seconds for NVRAM to be available
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: The process for the
command is not
```

```
responding or is otherwise unavailable
```

```
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
The process for the command is not responding or is otherwise unavailable
```



```

Switch#      Role      Priority    Current
-----
*1           Active      1           Ready
    
```

*** Executing show version ***

```

Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:14 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)
Switch uptime is 4 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "flash:cat9k_iosxe.16.09.04.SPA.bin"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
    
```

Technology Package License Information:

Technology-package Current	Type	Technology-package Next reboot
network-advantage	Smart License	network-advantage
None	Subscription Smart License	None
Smart Licensing Status: UNREGISTERED/EVAL EXPIRED		
cisco C9300-48UXM (X86) processor with 1419044K/6147K bytes of memory.		
Processor board ID FCW2144L045		
36 Ethernet interfaces		
1 Virtual Ethernet interface		
4 Gigabit Ethernet interfaces		
20 Ten Gigabit Ethernet interfaces		
2 TwentyFive Gigabit Ethernet interfaces		
2 Forty Gigabit Ethernet interfaces		
2048K bytes of non-volatile configuration memory.		
8388608K bytes of physical memory.		
1638400K bytes of Crash Files at crashinfo:.		
11264000K bytes of Flash at flash:.		
0K bytes of WebUI ODM Files at webui:.		

```

Base Ethernet MAC Address      : ec:1d:8b:0a:68:00
Motherboard Assembly Number    : 73-17959-06
Motherboard Serial Number      : FOC21418FPQ
Model Revision Number          : B0
Motherboard Revision Number    : A0
Model Number                   : C9300-48UXM
System Serial Number           : FCW21444L045
Switch Ports Model              SW Version      SW Image        Mode
-----
* 1 64 C9300-48UXM 16.9.4         CAT9K_IOSXE    BUNDLE
Configuration register is 0x102

```

*** Configuring a Loopback Interface ***

```

Line 1 SUCCESS: interface loop 100
Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255
Line 3 SUCCESS: end

```

*** Executing show ip interface brief ***

```

Any interface listed with OK? value "NO" does not have a valid configuration
Interface          IP-Address      OK? Method Status        Protocol
Vlan1              unassigned     NO  unset  up            up
GigabitEthernet0/0 10.127.128.5   YES DHCP  up          up
Tw1/0/1            unassigned     YES unset  down         down
Tw1/0/2            unassigned     YES unset  down         down
Tw1/0/3            unassigned     YES unset  down         down
Tw1/0/4            unassigned     YES unset  down         down
Tw1/0/5            unassigned     YES unset  down         down
Tw1/0/6            unassigned     YES unset  down         down
Tw1/0/7            unassigned     YES unset  down         down
Tw1/0/8            unassigned     YES unset  down         down
Tw1/0/9            unassigned     YES unset  down         down
Tw1/0/10           unassigned     YES unset  down         down
Tw1/0/11           unassigned     YES unset  down         down
Tw1/0/12           unassigned     YES unset  down         down
Tw1/0/13           unassigned     YES unset  down         down
Tw1/0/14           unassigned     YES unset  down         down
Tw1/0/15           unassigned     YES unset  down         down
Tw1/0/16           unassigned     YES unset  down         down
Tw1/0/17           unassigned     YES unset  down         down
Tw1/0/18           unassigned     YES unset  down         down
Tw1/0/19           unassigned     YES unset  down         down
Tw1/0/20           unassigned     YES unset  down         down
Tw1/0/21           unassigned     YES unset  down         down
Tw1/0/22           unassigned     YES unset  down         down
Tw1/0/23           unassigned     YES unset  down         down
Tw1/0/24           unassigned     YES unset  down         down
Tw1/0/25           unassigned     YES unset  down         down
Tw1/0/26           unassigned     YES unset  down         down
Tw1/0/27           unassigned     YES unset  down         down
Tw1/0/28           unassigned     YES unset  down         down
Tw1/0/29           unassigned     YES unset  down         down
Tw1/0/30           unassigned     YES unset  down         down
Tw1/0/31           unassigned     YES unset  down         down
Tw1/0/32           unassigned     YES unset  down         down
Tw1/0/33           unassigned     YES unset  down         down
Tw1/0/34           unassigned     YES unset  down         down
Tw1/0/35           unassigned     YES unset  down         down
Tw1/0/36           unassigned     YES unset  down         down

```

```

Te1/0/37          unassigned      YES unset   down      down
Te1/0/38          unassigned      YES unset   down      down
Te1/0/39          unassigned      YES unset   down      down
Te1/0/40          unassigned      YES unset   down      down
Te1/0/41          unassigned      YES unset   down      down
Te1/0/42          unassigned      YES unset   down      down
Te1/0/43          unassigned      YES unset   down      down
Te1/0/44          unassigned      YES unset   down      down
Te1/0/45          unassigned      YES unset   down      down
Te1/0/46          unassigned      YES unset   down      down
Te1/0/47          unassigned      YES unset   down      down
Te1/0/48          unassigned      YES unset   up        up
GigabitEthernet1/1/1 unassigned      YES unset   down      down
GigabitEthernet1/1/2 unassigned      YES unset   down      down
GigabitEthernet1/1/3 unassigned      YES unset   down      down
GigabitEthernet1/1/4 unassigned      YES unset   down      down
Te1/1/1           unassigned      YES unset   down      down
Te1/1/2           unassigned      YES unset   down      down
Te1/1/3           unassigned      YES unset   down      down
Te1/1/4           unassigned      YES unset   down      down
Te1/1/5           unassigned      YES unset   down      down
Te1/1/6           unassigned      YES unset   down      down
Te1/1/7           unassigned      YES unset   down      down
Te1/1/8           unassigned      YES unset   down      down
Fo1/1/1          unassigned      YES unset   down      down
Fo1/1/2          unassigned      YES unset   down      down
TwentyFiveGigE1/1/1 unassigned      YES unset   down      down
TwentyFiveGigE1/1/2 unassigned      YES unset   down      down
Loopback100      10.10.10.10    YES TFTP   up        up

```

*** Configuring username, password, SSH ***

```

Line 1 SUCCESS: username cisco privilege 15 password cisco
**CLI Line # 1: WARNING: Command has been added to the configuration using a type 0
password.
    However, type 0 passwords will soon be deprecated. Migrate to a supported password
type
Line 2 SUCCESS: ip domain name domain
Line 3 SUCCESS: line vty 0 15
Line 4 SUCCESS: login local
Line 5 SUCCESS: transport input all
Line 6 SUCCESS: end

```

*** ZTP Day0 Python Script Execution Complete ***

Press RETURN to get started!

Cisco IOS XE Gibraltar 16.12.x から Cisco IOS XE Amsterdam 17.1.x へ

.py スクリプトを実行する前の起動ログの例を以下に示します。

--- System Configuration Dialog ---

```
Would you like to enter the initial configuration dialog? [yes/no]: day0guestshell
installed successfully
Current state is: DEPLOYED
day0guestshell activated successfully
Current state is: ACTIVATED
day0guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully
```

```
*** Sample ZTP Day0 Python Script ***
```

```
...
```

```
*** ZTP Day0 Python Script Execution Complete ***
```

```
Guestshell destroyed successfully
```

デバイスでの Day-0 プロビジョニングの設定例を以下に示します。

```
Both links down, not waiting for other switches
Switch number is 1
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

```
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.3a,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 28-Apr-20 09:37 by mcpre
```

This software version supports only Smart Licensing as the software licensing mechanism.

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE "SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at <http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or

features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration of the applicable license term (e.g., 90-day trial period). Cisco reserves the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

```
% Checking backup nvram
% No config present. Using default config
```

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
```

```
All TCP AO KDF Tests Pass
cisco C9300-48UXM (X86) processor with 1343703K/6147K bytes of memory.
Processor board ID FCW2144L045
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
```

```
Base Ethernet MAC Address      : ec:1d:8b:0a:68:00
Motherboard Assembly Number    : 73-17959-06
Motherboard Serial Number      : FOC21418FPQ
Model Revision Number          : B0
Motherboard Revision Number    : A0
Model Number                   : C9300-48UXM
System Serial Number           : FCW2144L045
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: day0guestshell
installed successfully
Current state is: DEPLOYED
day0guestshell activated successfully
Current state is: ACTIVATED
day0guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully
```

```
HTTP server statistics:
Accepted connections total: 0
```

```
*** Sample ZTP Day0 Python Script ***
```

```
*** Executing show platform ***
```

Switch	Ports	Model	Serial No.	MAC address	Hw Ver.	Sw Ver.
1	65	C9300-48UXM	FCW2144L045	ec1d.8b0a.6800	V01	16.12.3a

```
Switch/Stack Mac Address : ec1d.8b0a.6800 - Local Mac Address
```

```

Mac persistency wait time: Indefinite
Current
Switch#   Role       Priority   State
-----
*1        Active    1         Ready

```

*** Executing show version ***

```

Cisco IOS XE Software, Version 16.12.03a
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.3a,

```

RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2020 by Cisco Systems, Inc.

Compiled Tue 28-Apr-20 09:37 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.

All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON

BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)

Switch uptime is 4 minutes

Uptime for this control processor is 9 minutes

System returned to ROM by Reload Command

System image file is "flash:cat9k_iosxe.16.12.03a.SPA.bin"

Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

```

-----
Technology-package                               Technology-package
Current                                           Next reboot
-----
network-advantage      Smart License      network-advantage
None                    Subscription Smart License      None

```

AIR License Level: AIR DNA Advantage

Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco C9300-48UXM (X86) processor with 1343703K/6147K bytes of memory.

Processor board ID FCW2144L045

1 Virtual Ethernet interface

4 Gigabit Ethernet interfaces

36 2.5 Gigabit Ethernet interfaces

20 Ten Gigabit Ethernet interfaces

2 TwentyFive Gigabit Ethernet interfaces

2 Forty Gigabit Ethernet interfaces

2048K bytes of non-volatile configuration memory.

```

8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
Base Ethernet MAC Address       : ec:1d:8b:0a:68:00
Motherboard Assembly Number     : 73-17959-06
Motherboard Serial Number       : FOC21418FPQ
Model Revision Number           : B0
Motherboard Revision Number     : A0
Model Number                     : C9300-48UXM
System Serial Number            : FCW2144L045
Switch Ports Model              SW Version      SW Image        Mode
-----
* 1 65 C9300-48UXM 16.12.3a      CAT9K_IOSXE    BUNDLE
Configuration register is 0x102

```

*** Configuring a Loopback Interface ***

```

Line 1 SUCCESS: interface loop 100
Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255
Line 3 SUCCESS: end

```

*** Executing show ip interface brief ***

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
GigabitEthernet0/0	10.127.128.10	YES	DHCP	up	up
Tw1/0/1	unassigned	YES	unset	down	down
Tw1/0/2	unassigned	YES	unset	down	down
Tw1/0/3	unassigned	YES	unset	down	down
Tw1/0/4	unassigned	YES	unset	down	down
Tw1/0/5	unassigned	YES	unset	down	down
Tw1/0/6	unassigned	YES	unset	down	down
Tw1/0/7	unassigned	YES	unset	down	down
Tw1/0/8	unassigned	YES	unset	down	down
Tw1/0/9	unassigned	YES	unset	down	down
Tw1/0/10	unassigned	YES	unset	down	down
Tw1/0/11	unassigned	YES	unset	down	down
Tw1/0/12	unassigned	YES	unset	down	down
Tw1/0/13	unassigned	YES	unset	down	down
Tw1/0/14	unassigned	YES	unset	down	down
Tw1/0/15	unassigned	YES	unset	down	down
Tw1/0/16	unassigned	YES	unset	down	down
Tw1/0/17	unassigned	YES	unset	down	down
Tw1/0/18	unassigned	YES	unset	down	down
Tw1/0/19	unassigned	YES	unset	down	down
Tw1/0/20	unassigned	YES	unset	down	down
Tw1/0/21	unassigned	YES	unset	down	down
Tw1/0/22	unassigned	YES	unset	down	down
Tw1/0/23	unassigned	YES	unset	down	down
Tw1/0/24	unassigned	YES	unset	down	down
Tw1/0/25	unassigned	YES	unset	down	down
Tw1/0/26	unassigned	YES	unset	down	down
Tw1/0/27	unassigned	YES	unset	down	down
Tw1/0/28	unassigned	YES	unset	down	down
Tw1/0/29	unassigned	YES	unset	down	down
Tw1/0/30	unassigned	YES	unset	down	down
Tw1/0/31	unassigned	YES	unset	down	down
Tw1/0/32	unassigned	YES	unset	down	down
Tw1/0/33	unassigned	YES	unset	down	down

```

Tw1/0/34          unassigned      YES unset  down      down
Tw1/0/35          unassigned      YES unset  down      down
Tw1/0/36          unassigned      YES unset  down      down
Tel/0/37          unassigned      YES unset  down      down
Tel/0/38          unassigned      YES unset  down      down
Tel/0/39          unassigned      YES unset  down      down
Tel/0/40          unassigned      YES unset  down      down
Tel/0/41          unassigned      YES unset  down      down
Tel/0/42          unassigned      YES unset  down      down
Tel/0/43          unassigned      YES unset  down      down
Tel/0/44          unassigned      YES unset  down      down
Tel/0/45          unassigned      YES unset  down      down
Tel/0/46          unassigned      YES unset  down      down
Tel/0/47          unassigned      YES unset  down      down
Tel/0/48          unassigned      YES unset  up        up
GigabitEthernet1/1/1 unassigned      YES unset  down      down
GigabitEthernet1/1/2 unassigned      YES unset  down      down
GigabitEthernet1/1/3 unassigned      YES unset  down      down
GigabitEthernet1/1/4 unassigned      YES unset  down      down
Tel/1/1          unassigned      YES unset  down      down
Tel/1/2          unassigned      YES unset  down      down
Tel/1/3          unassigned      YES unset  down      down
Tel/1/4          unassigned      YES unset  down      down
Tel/1/5          unassigned      YES unset  down      down
Tel/1/6          unassigned      YES unset  down      down
Tel/1/7          unassigned      YES unset  down      down
Tel/1/8          unassigned      YES unset  down      down
Fol/1/1         unassigned      YES unset  down      down
Fol/1/2         unassigned      YES unset  down      down
TwentyFiveGigE1/1/1 unassigned      YES unset  down      down
TwentyFiveGigE1/1/2 unassigned      YES unset  down      down
Apl/0/1         unassigned      YES unset  up        up
Loopback100     10.10.10.10    YES TFTP  up        up

```

*** Configuring username, password, SSH ***

```

Line 1 SUCCESS: username cisco privilege 15 password cisco
**CLI Line # 1:  WARNING: Command has been added to the configuration using a type 0
password.
However, type 0 passwords will soon be deprecated. Migrate to a supported password type
Line 2 SUCCESS: ip domain name domain
Line 3 SUCCESS: line vty 0 15
Line 4 SUCCESS: login local
Line 5 SUCCESS: transport input all
Line 6 SUCCESS: end

```

*** ZTP Day0 Python Script Execution Complete ***

Guestshell destroyed successfully

Press RETURN to get started!

Cisco IOS XE Amsterdam 17.2.x 以降のリリース

.py スクリプトを実行する前の起動ログの例を以下に示します。

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Acquired IPv4 address 10.127.128.8 on Interface GigabitEthernet0/0
Received following DHCPv4 options:
    bootfile      : test.py
    tftp-server-ip : 159.14.27.2

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

Attempting bootfile tftp://159.14.27.2/test.py
day0guestshell activated successfully
Current state is: ACTIVATED
day0guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully

*** Sample ZTP Day0 Python Script ***

...

*** ZTP Day0 Python Script Execution Complete ***

Guestshell destroyed successfully
```

デバイスでの Day-0 プロビジョニングの設定例を以下に示します。

```
Both links down, not waiting for other switches
Switch number is 1
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.2.1, RELEASE SOFTWARE (fc4)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 26-Mar-20 03:29 by mcpre

This software version supports only Smart Licensing as the software licensing mechanism.

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR

LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE "SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at <http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration of the applicable license term (e.g., 90-day trial period). Cisco reserves the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

% Checking backup nvram
% No config present. Using default config

FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled

All TCP AO KDF Tests Pass
cisco C9300-48UXM (X86) processor with 1338934K/6147K bytes of memory.
Processor board ID FCW2144L045
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.

Base Ethernet MAC Address	: ec:1d:8b:0a:68:00
Motherboard Assembly Number	: 73-17959-06
Motherboard Serial Number	: FOC21418FPQ
Model Revision Number	: B0
Motherboard Revision Number	: A0
Model Number	: C9300-48UXM
System Serial Number	: FCW2144L045
CLEI Code Number	:

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

Autoinstall trying DHCPv4 on GigabitEthernet0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Acquired IPv4 address 10.127.128.8 on Interface GigabitEthernet0/0
Received following DHCPv4 options:
 bootfile : test.py
 tftp-server-ip : 159.14.27.2

OK to enter CLI now...

```

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

Attempting bootfile tftp://159.14.27.2/test.py
day0guestshell activated successfully
Current state is: ACTIVATED
day0guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully

*** Sample ZTP Day0 Python Script ***

*** Executing show platform ***

Switch  Ports   Model                Serial No.   MAC address   Hw Ver.     Sw Ver.
-----  -----  -
1        65       C9300-48UXM         FCW2144L045  ec1d.8b0a.6800 V01         17.02.01

Switch/Stack Mac Address : ec1d.8b0a.6800 - Local Mac Address
Mac persistency wait time: Indefinite

Switch#  Role      Priority   Current
-----  -
*1       Active   1         Ready

*** Executing show version ***

Cisco IOS XE Software, Version 17.02.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.2.1,
  RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 26-Mar-20 03:29 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)
Switch uptime is 2 minutes
Uptime for this control processor is 8 minutes
System returned to ROM by Reload Command
System image file is "flash:cat9k_iosxe.17.02.01.SPA.bin"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use.  Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
```

compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>
If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

```

-----
Technology-package                               Technology-package
Current                                           Next reboot
-----
network-advantage                               network-advantage
None                                             None
Subscription Smart License
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage
Smart Licensing Status: UNREGISTERED/EVAL EXPIRED
cisco C9300-48UXM (X86) processor with 1338934K/6147K bytes of memory.
Processor board ID FCW2144L045
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
36 2.5 Gigabit Ethernet interfaces
20 Ten Gigabit Ethernet interfaces
2 TwentyFive Gigabit Ethernet interfaces
2 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
Base Ethernet MAC Address      : ec:1d:8b:0a:68:00
Motherboard Assembly Number    : 73-17959-06
Motherboard Serial Number      : FOC21418FPQ
Model Revision Number          : B0
Motherboard Revision Number    : A0
Model Number                   : C9300-48UXM
System Serial Number           : FCW2144L045
CLEI Code Number               :
Switch Ports Model             SW Version   SW Image     Mode
-----
* 1 65 C9300-48UXM 17.02.01    CAT9K_IOSXE BUNDLE
Configuration register is 0x102

```

*** Configuring a Loopback Interface ***

```

Line 1 SUCCESS: interface loop 100
Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255
Line 3 SUCCESS: end

```

*** Executing show ip interface brief ***

```

Interface          IP-Address      OK? Method Status        Protocol
Vlan1              unassigned      YES unset  up            up
GigabitEthernet0/0 10.127.128.8   YES DHCP    up            up
Tw1/0/1            unassigned      YES unset  down          down
Tw1/0/2            unassigned      YES unset  down          down
Tw1/0/3            unassigned      YES unset  down          down
Tw1/0/4            unassigned      YES unset  down          down
Tw1/0/5            unassigned      YES unset  down          down
Tw1/0/6            unassigned      YES unset  down          down
Tw1/0/7            unassigned      YES unset  down          down

```

```

Tw1/0/8          unassigned      YES unset  down      down
Tw1/0/9          unassigned      YES unset  down      down
Tw1/0/10         unassigned      YES unset  down      down
Tw1/0/11         unassigned      YES unset  down      down
Tw1/0/12         unassigned      YES unset  down      down
Tw1/0/13         unassigned      YES unset  down      down
Tw1/0/14         unassigned      YES unset  down      down
Tw1/0/15         unassigned      YES unset  down      down
Tw1/0/16         unassigned      YES unset  down      down
Tw1/0/17         unassigned      YES unset  down      down
Tw1/0/18         unassigned      YES unset  down      down
Tw1/0/19         unassigned      YES unset  down      down
Tw1/0/20         unassigned      YES unset  down      down
Tw1/0/21         unassigned      YES unset  down      down
Tw1/0/22         unassigned      YES unset  down      down
Tw1/0/23         unassigned      YES unset  down      down
Tw1/0/24         unassigned      YES unset  down      down
Tw1/0/25         unassigned      YES unset  down      down
Tw1/0/26         unassigned      YES unset  down      down
Tw1/0/27         unassigned      YES unset  down      down
Tw1/0/28         unassigned      YES unset  down      down
Tw1/0/29         unassigned      YES unset  down      down
Tw1/0/30         unassigned      YES unset  down      down
Tw1/0/31         unassigned      YES unset  down      down
Tw1/0/32         unassigned      YES unset  down      down
Tw1/0/33         unassigned      YES unset  down      down
Tw1/0/34         unassigned      YES unset  down      down
Tw1/0/35         unassigned      YES unset  down      down
Tw1/0/36         unassigned      YES unset  down      down
Te1/0/37         unassigned      YES unset  down      down
Te1/0/38         unassigned      YES unset  down      down
Te1/0/39         unassigned      YES unset  down      down
Te1/0/40         unassigned      YES unset  down      down
Te1/0/41         unassigned      YES unset  down      down
Te1/0/42         unassigned      YES unset  down      down
Te1/0/43         unassigned      YES unset  down      down
Te1/0/44         unassigned      YES unset  down      down
Te1/0/45         unassigned      YES unset  down      down
Te1/0/46         unassigned      YES unset  down      down
Te1/0/47         unassigned      YES unset  down      down
Te1/0/48         unassigned      YES unset  up        up
GigabitEthernet1/1/1 unassigned      YES unset  down      down
GigabitEthernet1/1/2 unassigned      YES unset  down      down
GigabitEthernet1/1/3 unassigned      YES unset  down      down
GigabitEthernet1/1/4 unassigned      YES unset  down      down
Te1/1/1          unassigned      YES unset  down      down
Te1/1/2          unassigned      YES unset  down      down
Te1/1/3          unassigned      YES unset  down      down
Te1/1/4          unassigned      YES unset  down      down
Te1/1/5          unassigned      YES unset  down      down
Te1/1/6          unassigned      YES unset  down      down
Te1/1/7          unassigned      YES unset  down      down
Te1/1/8          unassigned      YES unset  down      down
Fo1/1/1          unassigned      YES unset  down      down
Fo1/1/2          unassigned      YES unset  down      down
TwentyFiveGigE1/1/1 unassigned      YES unset  down      down
TwentyFiveGigE1/1/2 unassigned      YES unset  down      down
Ap1/0/1          unassigned      YES unset  up        up
Loopback100     10.10.10.10    YES TFTP   up        up

```

*** Configuring username, password, SSH ***

```

Line 1 SUCCESS: username cisco privilege 15 password cisco
**CLI Line # 1: WARNING: Command has been added to the configuration using a type 0
password.
However, type 0 passwords will soon be deprecated. Migrate to a supported password type
Line 2 SUCCESS: ip domain name domain
Line 3 SUCCESS: line vty 0 15
Line 4 SUCCESS: login local
Line 5 SUCCESS: transport input all
Line 6 SUCCESS: end

```

```

*** ZTP Day0 Python Script Execution Complete ***

```

```

Guestshell destroyed successfully
Script execution success!

```

```

Press RETURN to get started!

```

ゼロタッチプロビジョニングに関する追加情報

標準および RFC

標準/RFC	タイトル
RFC 5652	<i>Cryptographic Message Syntax (CMS)</i> [英語]
RFC 8040	<i>RESTCONF Protocol</i> [英語]
RFC 8366	<i>A Voucher Artifact for Bootstrapping Protocols</i> [英語]
RFC 8572	<i>Secure Zero Touch Provisioning (SZTP)</i> [英語]

シスコのテクニカルサポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>https://www.cisco.com/c/en/us/support/index.html</p>

ゼロタッチプロビジョニングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: ゼロタッチプロビジョニングの機能情報

機能名	リリース	機能情報
ゼロタッチプロビジョニング	Cisco IOS XE Everest 16.5.1a Cisco IOS XE Everest 16.5.1b Cisco IOS XE Fuji 16.7.1 Cisco IOS XE Fuji 16.8.2 Cisco IOS XE Gibraltar 16.12.1 Cisco IOS XE Amsterdam 17.2.1 Cisco IOS XE Amsterdam 17.3.1 Cisco IOS XE Cupertino 17.8.1	

機能名	リリース	機能情報
		<p>ネットワークプロビジョニングの課題に対応するため、シスコは、ゼロタッチプロビジョニングモデルを導入しました。</p> <p>Cisco IOS XE Everest 16.5.1a では、この機能は次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ <p>Cisco IOS XE Everest 16.5.1b では、この機能は次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • ゲストシェルをサポートするための、最低 8 GB の RAM を搭載した Cisco 4000 シリーズ サービス統合型ルータ モデル。 <p>Cisco IOS XE Fuji 16.7.1 では、この機能は次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco ASR 1000 アグリゲーションサービスルータ (ASR1001-X、ASR1001-HX、ASR1002-X、ASR1002-HX) <p>Cisco IOS XE Fuji 16.8.2 では、この機能は次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco ASR 1000 シリーズ アグリゲーションサービスルータ (ASR1004、ASR1006、ASR1006-X、ASR1009-X、ASR1013)

機能名	リリース	機能情報
		<p>この機能は、Cisco IOS XE Gibraltar 16.12.1 で次のプラットフォームに実装されました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9200 シリーズ スイッチ <p>(注) この機能は C9200L SKU ではサポートされていません。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9300L SKU • Cisco Catalyst 9600 シリーズ スイッチ • Cisco Catalyst 9800-40 ワイヤレスコントローラ • Cisco Catalyst 9800-80 ワイヤレスコントローラ <p>この機能は、Cisco IOS XE Amsterdam 17.2.1で次のプラットフォームに実装されました。</p> <ul style="list-style-type: none"> • Cisco Cloud Services Router 1000V シリーズ • Cisco C1100 ターミナル サービス ゲートウェイ (C1100TGX-1N24P32A でのみサポート) <p>この機能は、Cisco IOS XE Amsterdam 17.3.1で次のプラットフォームに実装されました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 8200 シリーズ エッジ プラットフォーム • Cisco Catalyst 8300 シリーズ エッジ プラットフォーム • Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォーム

機能名	リリース	機能情報
		<p>この機能は、Cisco IOS XE Bengaluru 17.4.1で次のプラットフォームに実装されました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 8000V Edge ソフトウェア <p>Cisco IOS XE Cupertino 17.8.1 では、この機能が次のプラットフォームに実装されました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9800-L ワイヤレスコントローラ
<p>ゼロタッチプロビジョニング：HTTPダウンロード</p>	<p>Cisco IOS XE Fuji 16.8.1 Cisco IOS XE Fuji 16.8.1a</p>	<p>ゼロタッチプロビジョニングは、HTTPおよびTFTPのファイルダウンロードをサポートします。</p> <p>Cisco IOS XE Everest 16.8.1では、この機能は次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco 4000 シリーズ サービス統合型ルータ • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ <p>Cisco IOS XE Fuji 16.8.1aでは、この機能はCisco Catalyst 9500ハイパフォーマンスシリーズスイッチに実装されました。</p>

機能名	リリース	機能情報
ゼロタッチプロビジョニングのための DHCPv6 のサポート	Cisco IOS XE Fuji 16.9.1 Cisco IOS XE Amsterdam 17.3.2a	Cisco IOS XE Fuji 16.9.1 では、この機能は次のプラットフォームに実装されていました。 <ul style="list-style-type: none">• Cisco Catalyst 9300 シリーズ スイッチ• Cisco Catalyst 9500 シリーズ スイッチ Cisco IOS XE Amsterdam 17.3.2a では、この機能は次のプラットフォームに導入されました。 <ul style="list-style-type: none">• Cisco Catalyst 9800-40 ワイヤレスコントローラ• Cisco Catalyst 9800-80 ワイヤレスコントローラ

機能名	リリース	機能情報
<p>コンフィギュレーションデータベースの副次的同期</p>	<p>Cisco IOS XE Bengaluru 17.4.1</p>	<p>DMI の設定変更中に、変更の部分的な同期が行われます。これは、コマンドまたは RPC の設定時にトリガーされます。これは副次的同期と呼ばれ、同期時間と NETCONF のダウンタイムを短縮します。</p> <p>この機能は、次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco ASR 1000 アグリゲーションサービスルータ • Cisco Catalyst 8500 および 8500L シリーズ エッジプラットフォーム • Cisco Catalyst 9200 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9400 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ • Cisco Catalyst 9600 シリーズ スイッチ
<p>YANG モデルによるゼロタッチプロビジョニング</p>	<p>Cisco IOS XE Cupertino 17.7.1</p>	<p>ZTP は、NETCONF が有効であれば、YANG モデルを介して有効化されます。</p> <p>この機能は、NETCONF-YANG をサポートするすべてのプラットフォームでサポートされています。</p>
<p>データポートでのゼロタッチプロビジョニングのサポート</p>	<p>Cisco IOS XE Cupertino 17.7.1</p>	<p>ZTP は、IPv4 と IPv6 の両方のデータポートでサポートされています。</p> <p>この機能は、次のプラットフォームに実装されています。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9800-L ワイヤレスコントローラ

機能名	リリース	機能情報
セキュアなゼロタッチプロビジョニング	Cisco IOS XE Dublin 17.11.1	<p>セキュア ZTP は、工場出荷時のデフォルト状態での起動時にデバイスを安全にプロビジョニングします。</p> <p>この機能は、次のプラットフォームに実装されています。</p> <ul style="list-style-type: none">• Cisco Catalyst 9300 および 9300L シリーズ スイッチ• Cisco Catalyst 9400 シリーズ スイッチ• Cisco Catalyst 9500 および 9500 ハイパフォーマンス シリーズ スイッチ• Cisco Catalyst 9600 シリーズ スイッチ

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。