



ディザスタ リカバリ

この章で説明する内容は次のとおりです。

- [USB ドライブを使用した起動 \(1 ページ\)](#)
- [iPXE を使用した起動 \(2 ページ\)](#)

USB ドライブを使用した起動

ブート可能な USB ドライブを使用して、システム アップグレードの目的でルータのイメージを再適用したり、起動に失敗した場合にルータを起動したりします。ブート可能な USB ドライブは圧縮ブート ファイルを使用して作成できます。

圧縮ブート ファイルを使用したブート可能な USB ドライブの作成

圧縮ブート ファイルを USB ドライブにコピーすると、ブート可能な USB ドライブが作成されます。圧縮ファイルの内容が展開されると、USB ドライブがブート可能になります。



- (注) USB ドライブからの読み込みまたはブートに失敗した場合は、ドライブが正しく挿入されていることを確認してください。ドライブが正しく挿入されていても USB ドライブから読み込めない場合は、別のシステムで USB の内容を確認してください。

このタスクは、ローカル マシンで利用できる Windows、Linux、または MAC オペレーティングシステムを使用して実行できます。ここで説明する一般的な手順をそれぞれ実行するための操作は、使用中のオペレーティングシステムによって異なります。

始める前に

- ストレージ容量が 8 GB (最小) ~ 32 GB (最大) の USB ドライブにアクセスできるようにします。USB 2.0 および USB 3.0 がサポートされています。

- 圧縮ブート ファイルを cisco.com のソフトウェア ダウンロード ページからローカル マシンにコピーします。圧縮ブート ファイルのファイル名の形式は、`ncs560-usb-boot-<release_number_zip>` です。

手順

- ステップ 1** USB ドライブをローカル マシンに接続し、Windows オペレーティング システムまたは Apple MAC ディスク ユーティリティを使用して FAT32 または MS-DOS ファイル システムでフォーマットします。
- ステップ 2** 圧縮ブート ファイルを USB ドライブにコピーします。
- ステップ 3** コピー処理が正常に行われたことを確認します。確認するには、コピー元とコピー先でファイル サイズを比較します。さらに、MD5 チェックサム値を確認します。
- ステップ 4** 圧縮ブート ファイルを USB ドライブ内で解凍して内容を展開します。これにより、USB ドライブがブート可能なドライブに変換されます。

(注) 圧縮ファイルの内容 (「EFI」および「boot」ディレクトリ) は、USB ドライブのルートに直接展開する必要があります。解凍アプリケーションによって展開ファイルが新しいフォルダに配置された場合は、「EFI」および「boot」ディレクトリを USB ドライブのルートに移動してください。

- ステップ 5** ローカル マシンから USB ドライブを取り出します。

次のタスク

ブート可能な USB ドライブを使用して、ルータの起動またはイメージのアップグレードを実行します。

iPXE を使用した起動

iPXE は、管理インターフェイスのネットワーク カードに含まれ、ルータのシステム ファームウェア (UEFI) レベルで動作するプリブート実行環境です。iPXE は、システムを再イメージするために使用され、ブートに失敗した場合や有効なブート可能なパーティションがない場合にルータを起動します。iPXE は ISO イメージをダウンロードして、イメージのインストールを進行させ、最後に新しいインストール内でブートストラップを行います。

iPXE はブート ロダとして機能し、システムを起動するイメージをプラットフォーム ID (PID)、シリアル番号、または管理 MAC アドレスに基づいて柔軟に選択できるようにします。iPXE は DHCP サーバのコンフィギュレーション ファイルで定義する必要があります。

ゼロタッチプロビジョニング

ゼロタッチプロビジョニング (ZTP) は、iPXEを使用してルータでソフトウェアをインストールした後の自動プロビジョニングに役立ちます。

ZTP の自動プロビジョニングでは以下の手順を実行します。

- **設定**：コンフィギュレーション ファイルをダウンロードおよび実行します。ZTP でコンフィギュレーションとして処理されるように、ファイルの最初の行に `!! IOS XR` が含まれている必要があります。
- **スクリプト**：スクリプト ファイルをダウンロードおよび実行します。スクリプト ファイルには、タスクを完了するためのプログラムによるアプローチが含まれています。たとえば IOS XR コマンドを使用して作成されたスクリプトは、パッチアップグレードを実行します。ZTP でコンフィギュレーションとして処理されるように、ファイルの最初の行に `#!/bin/bash` または `#!/bin/sh` が含まれている必要があります。

DHCP サーバの設定

DHCP サーバは、IPv4 か IPv6、またはその両方の通信プロトコルに対して設定する必要があります。次に、Linux システムで実行されている ISC-DHCP サーバの例を示します。

始める前に

- ネットワーク管理者またはシステムの設計担当者に問い合わせて、管理インターフェイスの IP アドレスおよびサブネット マスクを入手します。
- RP の物理ポート `イーサネット 0` は管理ポートです。ポートが管理ネットワークに接続されていることを確認します。
- サーバが DHCP パケットを処理できるようにファイアウォールを有効にします。
- DHCPv6 の場合、IPv6 アドレスの取得方法を示すルーティングアドバタイズメント (RA) メッセージをネットワーク内のすべてのノードに送信する必要があります。クライアントが DHCP 要求を送信できるようにルータ アドバタイズデーモン (radvd。yum install radvd を使用してインストールします) を設定します。次に例を示します。

```
interface eth3
{
    AdvSendAdvert on;
    MinRtrAdvInterval 60;
    MaxRtrAdvInterval 180;
    AdvManagedFlag on;
    AdvOtherConfigFlag on;
    prefix 2001:1851:c622:1::/64
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr off;
    }
};
```

- HTTP サーバは DHCP サーバと同じサーバにも、別のサーバにも設定できます。IP アドレスが DHCP サーバから割り当てられた後、ルータは HTTP サーバに接続してイメージをダウンロードします。

手順

ステップ 1 dhcpd.conf ファイル (IPv4、IPv6、または両方の通信プロトコル用)、dhcpv6.conf ファイル (IPv6 用)、またはその両方のファイルを /etc/ または /etc/dhcp ディレクトリに作成します。このコンフィギュレーションファイルには、スクリプトへのパス、ISO インストールファイルの場所、プロビジョニング設定ファイルの場所、ルータのシリアル番号、MAC アドレスなどのネットワーク情報が保存されます。

ステップ 2 DHCP サーバが稼働したら、サーバをテストします。たとえば、IPv4 の場合は次のようになります。

- ルータの MAC アドレスを使用した場合：

(注) host ステートメントを使用すると、DNS に使用される固定アドレスが提供されますが、要求内でオプション 77 が iPXE に設定されていることを確認します。このオプションは、必要に応じてブートファイルをシステムに提供するために使用されます。

上記の設定が正常に行われていることを確認します。

- ルータのシリアル番号を使用した場合：ルータのシリアル番号は BIOS から取得され、ID として使用されます。

ステップ 3 DHCP を再起動します。

```
killall dhcpd
/usr/sbin/dhcpd -f -q -4 -pf /run/dhcp-server/dhcpd.pid
-cf /etc/dhcp/dhcpd.conf ztp-mgmt &
```

例

次に、dhcpd.conf ファイルの例を示します。

```
allow bootp;
allow booting;
ddns-update-style interim;
option domain-name "cisco.com";
option time-offset -8;
ignore client-updates;
default-lease-time 21600;
max-lease-time 43200;
option domain-name-servers <ip-address-server1>, <ip-address-server2>;
log-facility local0;
:
subnet <subnet> netmask <netmask> {
    option routers <ip-address>;
    option subnet-mask <subnet-mask>;
```

```
    next-server <server-addr>;
  }
  :
host <hostname> {
  hardware ethernet e4:c7:22:be:10:ba;
  fixed-address <address>;
  filename "http://<address>/<path>/<image.bin>";
}
```

次に、dhcpd6.conf ファイルの例を示します。

```
option dhcp6.name-servers <ip-address-server>;
option dhcp6.domain-search "cisco.com";
dhcpv6-lease-file-name "/var/db/dhcpd6.leases";
option dhcp6.info-refresh-time 21600;
option dhcp6.bootfile-url code 59 = string;
subnet6 <subnet> netmask <netmask> {
  range6 2001:1851:c622:1::2 2001:1851:c622:1::9;
  option dhcp6.bootfile-url "http://<address>/<path>/<image.bin>";
}
```

次のタスク

ZTP を呼び出します。

ZTP の呼び出し

ZTP は XR 名前空間内と、管理インターフェイスおよびラインカードインターフェイスの場合はグローバル VPN ルーティング/転送 (VRF) 名前空間内で実行されます。

始める前に

DHCP サーバが設定されていることを確認します。詳細については、[DHCP サーバの設定 \(3 ページ\)](#) を参照してください。

手順

dhcpd.conf ファイルを編集して、ZTP の機能を利用します。

次に、iPXE と ZTP を含む DHCP サーバの設定例を示します。

```
host <host-name>
{
  hardware ethernet <router-serial-number or mac-id>;
  fixed-address <ip-address>;
  if exists user-class and option user-class = "iPXE" {
    # Image request, so provide ISO image
    filename "http://<ip-address>/<directory>";
  } else
  {
    # Auto-provision request, so provide ZTP script or configuration
    filename "http://<ip-address>/<script-directory-path>";
    #filename "http://<ip-address>/<script-directory-path>";
  }
}
```

(注) 自動プロビジョニング用に一度に提供できるのは、ZTP .script ファイルまたは .cfg ファイルのいずれかのみです。

この設定では、インストール時にを使用してシステムを起動し、その後 XR VM が起動した時点でダウンロードして実行します。

手動による ZTP の呼び出し

ZTP は、変更されたワンタッチプロビジョニング手法を使用して手動で呼び出すこともできます。このプロセスでは、次の手順を実行する必要があります。

始める前に

設定ファイルを使用して、XR で起動され、DHCP が呼び出されるインターフェイスのリストを指定することができます。/pkg/etc/ztp.config はプラットフォーム固有のファイルで、追加のインターフェイスを使用するかどうかをプラットフォームが指定できます。

```
#
# List all the interfaces that ZTP will consider running on. ZTP will attempt
# to bring these interfaces. At which point dhclient will be able to use them.
#
# Platforms may add dynamically to this list.
#
#ZTP_DHCLIENT_INTERFACES=" \
#   Gi0_0_0_0 \
#"
...
```

手順

- ステップ1 ルータを起動します。
- ステップ2 手動でログインします。
- ステップ3 インターフェイスを有効にします。
- ステップ4 **ztp initiate** コマンドを使用して新しい ZTP DHCP セッションを手動で呼び出します。

```
Router#ztp initiate
```

たとえば、GigabitEthernet インターフェイス 0/0/0/0 で DHCP 要求を送信するには、次のコマンドを実行します。

```
Router#ztp initiate debug verbose interface GigabitEthernet0/0/0/0
```

プラットフォームが別の方法で設定していない限り、ZTP はデフォルトで管理ポート上で実行されます。ログは /disk0:/ztp/ztp/log の場所に記録されます。

(注) 40G インターフェイスを 4 つの個別の 10G インターフェイスに設定するには、**ztp breakout nosignal-stay-in-breakout-mode** コマンドを使用します。

(注) データポートブレイクアウトを有効にし、検出されたすべてのデータポートインターフェイスおよびラインカードインターフェイスでDHCPセッションを呼び出すには、**ztp breakout** コマンドを使用します。

```
Router#ztp breakout debug verbose
Router#ztp initiate dataport debug verbose
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:
```

プロンプトを上書きするには：

```
Router#ztp initiate noprompt
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:

ZTP will now run in the background.
Please use "show logging" or look at /disk0:/ztp/ztp/log to check progress.
```

ZTP はデフォルトで起動している管理インターフェイス上で動作します。

ステップ 5 ZTP セッションを終了するには、**ztp terminate** コマンドを使用します。

次のタスク

iPXE を使用してルータを起動します。

iPXE を使用したルータの起動

iPXE ブートを使用する前に、次のことを確認してください。

- DHCP サーバが設定され、動作している。
- **admin** コマンドを使用してシステム管理コンソールにログインしている。

ルータのイメージを再作成するために、次のコマンドを実行して iPXE ブートプロセスを呼び出します。

```
hw-module location all bootmedia network reload
```

例：

```
sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
Wed Dec 23 15:29:57.376 UTC
Reload hardware module ? [no,yes]
```

次の例は、コマンドの出力を示しています。

```
iPXE 1.0.0+ (3e573) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
Trying net0...
net0: c4:72:95:a6:14:e1 using dh8900cc on PCI01:00.1 (open)
[Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 c4:72:95:a6:14:e1)..... Ok << Talking to DHCP/PXE server
to obtain network information
net0: 10.37.1.101/255.255.0.0 gw 10.37.1.0
net0: fe80::c672:95ff:fea6:14e1/64
net0: 2001:1800:5000:1:c672:95ff:fea6:14e1/64 gw fe80::20c:29ff:fefb:b9fe
```

```
net1: fe80::c672:95ff:fea6:14e3/64 (inaccessible)
Next server: 10.37.1.235
Filename: http://10.37.1.235/
```

```
http://10.37.1.235/ ... 58% << Downloading file as indicated by DHCP/PXE server to boot
install image
```