

Cisco Evolved Programmable Network Manager 6.0.2 デバイス パックおよびポイントパッチ

2022 年 5 月 24 日

このドキュメントでは、Cisco EPN Manager 6.0 デバイスパックおよびポイントパッチ 2 (Cisco EPN Manager 6.0.2) の情報とインストール手順について説明します。デバイスパックとポイントパッチは、Cisco EPN Manager 6.0/6.0.x にインストールする必要があります。

目次

特記事項.....	3
Cisco EPN Manager 6.0.2 の新機能.....	4
Cisco EPN Manager 6.0.2 の既知の問題.....	6
Cisco EPN Manager 6.0.2 で修正された問題.....	8
Cisco EPN Manager 6.0.2 デバイスパックおよびポイントパッチの入手とインストール.....	11
前提条件.....	11
非 HA 展開.....	11
アップデートのダウンロードとインストール.....	11
すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）.....	12
HA の導入.....	12
サーバのセッション タイムアウトを増やす.....	12
HA 設定の削除.....	13
プライマリサーバーとセカンダリサーバー（HA 展開）にデバイスパックとポイントパッチをインストールします。.....	13
プライマリサーバーへのデバイスパックとポイントパッチのインストール.....	14
セカンダリサーバーへの Cisco EPN Manager 6.0.x のインストール.....	14
セカンダリサーバーでのインストールの検証.....	15
高可用性を有効にして HA ステータスを確認.....	15
すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）.....	16
ハードウェアと NTP クロックの同期.....	16
マニュアルの入手方法、テクニカルサポート、およびセキュリティガイドライン.....	18

特記事項

- Cisco EPNM 3.1.3 リリース以降、Linux CLI のルートユーザーログインは無効になります。
ルートユーザーログインを再度有効にする場合は、次のファイルを手動で編集する必要があります。

```
/etc/ssh/sshd_config
```

PermitRootLogin の値 no を yes に変更します。

sshd をリロードします。

```
#systemctl reload sshd.service
```

Cisco EPN Manager 6.0.2 の新機能

- 6.0.x から 6.0.2 へのアップグレード
- NCS2K 11.1.2.3 OS の検証
- NCS4K 6.5.32 の検証
- ASR9K 64 ビットでの IOS-XR 7.5.2 のサポート
- IOS XR 7.6.1 および NCS540 のサポート
- NCS5500/NCS5700 での IOS-XR 7.5.2 のサポート
- NCS560 での IOS-XR 7.5.2 のサポート
- Cisco 8000 での IOS-XR 7.5.2 のサポート
- XRv9000 での IOS-XR 7.5.2 のサポート
- NCS560 での IOS-XR 7.6.1 のサポート
- NCS5500/NCS5700 での IOS-XR 7.6.1 のサポート
- Cisco ASR9K デバイスでの IOS-XR 7.6.1 のサポート
- IOS-XR 7.6.1 および XRv9000 のサポート
- NCS540 での IOS-XR 7.5.2 のサポート
- IOS-XR 7.5.2 での Cisco N540-6Z14S-SYS-D のサポート
- NCS5700 での IOS-XR 7.5.2 を使用した Cisco NCS-57C1-48Q6-SYS のサポート
- NCS5700 での IOS-XR 7.5.2 を使用した Cisco NCS-57C1-48Q6-SYS のシャーシビューのサポート
- Cisco N540-6Z14S-SYS-D のシャーシビューのサポート
- IOS-XR 7.5.2 での Cisco 8202-32FH-M のサポート
- Cisco 8202-32FH-M のシャーシビューのサポート
- CRS および IOS-XR 6.7.4 の検証
- NCS4200/ASR900 での IOS XE 17.7.1 の検証
- EPNM に NCS1004 OTN-XPL のサポートを追加
- NCS4200/ASR900 での IOS XE 17.6.2/3 の検証
- NCS4200/ASR900 での IOS XE 17.8.1 の検証
- NCS2K SVO 回線のソーク時間は復元に適用せず、均等に元に戻す必要があります
- NCS2K デバイス用の Netconf リプレイ機能の実装
- NCS2K SVO は SWITCH DOWN Clear イベントに基づいて Netconf ストリームを再確立します
- 不完全 (Partial) 状態からの NCS2K SVO の回線自動リカバリ

- NCS2K SVO は同期完了イベントを受信した後に NE の完全同期を実行します
- NCS2K SVO には、復元の再試行全体での指数関数的な復元時間ではなく、一定の復元時間 (WSON では 5 分) があります。

Cisco EPN Manager 6.0.2 の既知の問題

ID	見出し
CSCwb57844	サテライトデバイスが、iccpgroupsettings が原因で CF 状態になる
CSCwb59989	6.0.2 GA : ncs4k デバイスの l2vpn 作成でオプティカル制御ポート (表示不可) が表示される
CSCwb60776	BGP ネイバーの詳細が欠落している
CSCwb75340	6.0.2 GA : ブラウンフィールド evp ツリーの変更により、XE デバイスでエラーがスローされる
CSCwb76010	上位 N CE/L3VPN パフォーマンスタブの切断ページのサービス名ハイパーリンクが機能していない
CSCwb81793	CEM サービスのプロビジョニング中にホップエンptyエラーが発生する
CSCwb82974	EPNM_6_0_2_NCS5500 : アクティブ化でコミットが失敗し、コミットジョブにエラー「CPU ノードがダウンしています (CPU Nodes are down)」が表示される
CSCwb84451	チームインターフェイスまたはセカンダリ管理インターフェイスの IPv6 アドレスにアクセスできない
CSCwb85811	モニタリングポリシーのカスタム MIB ポーリングで、個々のデバイスをテストするためのルータ型デバイスのみが表示される
CSCwb86147	TACACS/Radius 対応 2K ノードの EPNM で、ログイン情報とノード同期の検証が失敗する
CSCwb87022	モニタリングポリシーのエクスポートファイル出力の詳細が GUI の詳細と異なる
CSCwb68437	ソフトウェアアップデートのタイプとドロップダウン フィルタ オプションに Prime アドオンが表示される
CSCwb72654	SONET の上位および下位パスの復元クロック ID は必須パラメータである
CSCwb73935	SONET および SDH の下位パスを誤って設定しても、意味のあるエラーが表示されない
CSCwb74846	ASR9k XRv は MEF オプションをサポートしていないため、CE の展開が失敗する
CSCwb77184	BERT UI を起動した後、システム設定オプションにアクセスできなくなる
CSCwb82168	[デバイス (Device)] > [インベントリ (Inventory)] の行の高さが一部の行で高い
CSCwb82214	SVO の有線デバイスインベントリ詳細レポートにモジュール ポート インターフェイスと IP インターフェイスがない
CSCwb84514	EVPL プロビジョニングの「パフォーマンス測定プローブ (Performance Measurement Probes) 」テーブルのフィールド幅を広くする必要がある
CSCwb86270	QoS イーグレスポリシーに、すべてのポリサー アクション オプションの展開が含まれていない
CSCwb86458	QoS イーグレスポリシーが 903 デバイスによって拒否されるが、プロビジョニングウィザードでは検出されない
CSCwb87191	モニタリングポリシーがフォルダ内にあると、最終アクティブ化時刻の詳細が正しく表示されない
CSCwb81066	シリアルサービスフローのエラーメッセージとヘルプヒントの変更

ID	見出し
CSCwb86834	モニタリングポリシーのデバイス選択の詳細ページで、[すべて選択 (Select all)] チェックボックスがデフォルトで有効になっていない

Cisco EPN Manager 6.0.2 で修正された問題

ID	見出し
CSCwa68748	CIAM : Expat - 2.1.0
CSCwa77560	アラーム通知ポリシーですべてを選択した後、個々のアラームを選択解除すると、正しくないポリシーが作成される
CSCwa86907	CIAM : xstream 1.4.18 CVE-2021-43859
CSCwb11653	EPNM HA フェールオーバーと同時ファイバ切断により復元が失敗する
CSCwb23668	リプレイ機能の開始時刻が間違っている。そのため、収集エラーが発生する
CSCwb30946	ルータ NC560 回線を使用した TIM-B セットアップが削除されると、古いエントリが原因で再作成できない
CSCwb35978	SVO HA スイッチオーバーとファイバ切断により、デバイスで収集エラーが発生する
CSCwb36916	EPNM_6_0_2_CRSDDevice : EPNM からのイメージ (.tar) のインポートジョブで、CRS デバイスの場合、部分的に失敗したと表示される
CSCwb36966	EPNM_6_0_2_CRSDDevice : CRS デバイスのダウングレードで、配布場所に「該当なし (Not Applicable)」と表示される
CSCwb38007	TIM-B セットアップの実際のファイバ切断により、回線が復元中状態でのみスタックする
CSCwb38101	EPNM メモリリークで、NMS メモリリークにより EPNM がダウンする
CSCwb45266	電源オフによる実際の NE 切断で、PCE エラーが発生し、回線の復元が失敗する
CSCwb84434	EPNM6.0.2 : Nessus で脆弱性が検出される
CSCvz97671	NCS2K : EPNM で特定の OCHCC WSON 回線が不完全 (Partial) 状態であり、証跡の関連する cc 情報が欠落している
CSCwa56226	移行後に一部の回線が不完全 (Partial) 状態になる
CSCwa57168	見出しがマークされない
CSCwa57197	あるユーザーグループの回線が別のユーザーグループに表示される
CSCwa70523	MCH グループサービスの終了 (Terminate) は失敗するが、UI からは正常に動作する
CSCwa71912	回線の作成中にエンドポイントが SVO デバイスに表示されない
CSCwa74076	NCS1004 : 実際の周波数/波長に少し問題がある
CSCwa85013	log4j 2.17.1 へのアップグレード
CSCwa87330	ルートユーザーおよびスーパーユーザー以外のユーザーがオンラインヘルプページにアクセスできない
CSCwa94989	POST トリガー型 OTDR スキャンファイルに対する GET API は、GUI OTDR スキャンデータのダウンロード後にのみ部分的に機能する
CSCwa95775	NBI から OTDR スキャンが実行された場合、NBI と UI からダウンロードしたレポートファイルのサイズに違いがある
CSCwb00635	NCS5504 のカード NC55-24H12F-SE では、ブレイクアウトポートが TenGigx/x/x/x ではなく Opticsx/x/x/x と表示される
CSCwb02929	EPNM 5.1.4 - エクスプレスプロファイルのインベントリで corePoolSize と maxPoolSize の値が正しくない

ID	見出し
CSCwb06849	インストールガイド 6.0 の変更
CSCwb07385	通信の送信エラーによるスマート ソフトウェア ライセンスの登録失敗
CSCwb14130	回線設定が結合されている場合、running-config の回線設定が正しく解析されない (RS232)
CSCwb16379	LDAP SSL 認証が機能しない
CSCwb16840	EPNM データベースに古いエントリが残っている
CSCwb17991	自動復帰により、回線が不完全 (Partial) 状態になる
CSCwb22508	ファイバ切断、NE 切断などの複数の操作の後に偽の損失が生成される
CSCwb22532	NE-DISCONNECT がクリアされた後に、回線が不完全 (Partial) 状態のままになる
CSCwb23759	EPNM 6.1 および 6.0.1 - 物理リンク/LAG ダウンステータスが正常に 60 秒以内に更新されない
CSCwb23975	クリアされたアラームタブヘッダー数が 0 と表示され、アラームタブヘッダー名を変更する必要がある
CSCwb26389	SVO コンテナを切断すると、EPNM で偽の NETCONF アラームが生成される
CSCwb33245	最大ホップ数の値を変更し、ノードを含めるまたは除外すると、「使用可能なデータがありません (No data Available)」が表示される
CSCwb33882	XR デバイスのポートベースの設定で MPLSTE BGP L3Link 修正が失敗する
CSCwb36536	IOS-XR を使用する CRS デバイスの [インベントリ (Inventory)] > [デバイスの詳細 (Device Details)] に PSU およびファンモジュールが表示されない
CSCwb36769	MPLS リンク遅延 - XR 7.3.1 デバイスでのサポートを追加
CSCwb46469	EPNM HA スイッチオーバーとファイバ切断 SIP が回線からクリアされない
CSCwb48219	メインパス上のデバイスでの NE 切断時に EPNM が自動復帰を試行する
CSCwb49339	SVO がダウンした状態で自動復帰すると、回線が不完全 (Partial) 状態になる - 修復と再同期がトリガーされない
CSCwb53536	EPNM_6_0_2_CRSDDevice : デバイスでコミットの準備ができていないため、アクティブ化およびコミットジョブでコミットが失敗する
CSCwb54887	WAE 応答後に BFD テンプレートの関連付けが行われない
CSCwb55162	誤ったアーティファクトがリリースされるため (xmp_snmp_sessionmgr-3.855.0.jar)、CSCvz98965 は 6.0 では解決されない
CSCwb60327	復元後の復帰可能な回線の復元に失敗する。回線が復元中状態でスタックする
CSCwb60417	EPNM の警告メッセージは、WAE 応答に合わせる必要がある
CSCwb60744	デバイスがメンテナンス状態でスタックする
CSCwb65764	ActiveMQ での OOM
CSCwb68491	INCLUDE/EXCLUDE テーブルでインターフェイスが選択されていない場合、文字列「noInterfaceSelected」を含める
CSCwb71148	EPNM 6.0 インストールガイド - CSCvy23276 の参照を削除
CSCwb80321	6.0.2 : elib_11123 : リアルタイムサービス PM で空白の画面が表示されるため、リアルタイムサービス PM を確認できない

ID	見出し
CSCvz95522	NCS2K : 一部の ochtrail/ochcc WSON 回線の波長に 2 つのエントリが表示される
CSCvz95559	NCS2K : 復元設定は、回線内テーブルで「なし (None) 」と表示されるが、回線 360 では正しい
CSCwa74971	NCS4k : TCM : Performance Monitor の有効化が機能せず、常に無効になる
CSCwa91691	アラーム概要ページの注釈に、サーバーまたはローカル UI クライアント時間ではなく、UTC 時間が表示される
CSCwa94994	GET API でダウンロードした OTDR (POST によってトリガー) SOR ファイル名が GUI エクスポートファイル名と異なる
CSCwa95404	OTDR : 2 行が選択されている場合、OTDR で Geo マップと X 軸プロットの問題が発生する
CSCwb14977	保存とテストがスマートライセンス設定で無効になる
CSCwb16177	削除がサポートされていないアラームが他のアラームとともに削除される
CSCwb16487	インストールガイドに次の認定アップグレードパスを追加するリクエストが行われている
CSCwb17982	詳細ページに手動復帰の予定復帰時間と予定時間が表示される
CSCwb23007	[ライセンス (License)] ダッシュボードにスマートライセンスが表示される
CSCwb30615	[SVO デバイスのアラームとイベントの再生時間 (Duration for the Alarms & Events Replay for SVO devices)] フィールドに検証が必要である
CSCwb33872	トポロジマップでテクノロジーとして ISIS をフィルタリングすると、すべてのリンクが表示される
CSCwb38228	アラーム概要ページのアラームが、24 時間形式ではなく 12 時間形式の時刻を表示する
CSCwb42909	6.0.2 で XFT Failure マルチスレッド実行が失敗すると、ビルドが不安定になる
CSCwb49508	収集失敗アラームの場合、失敗ソースが表示されない
CSCwb71220	アラーム ID ハイパーリンクページの注釈の更新時刻が、ローカルタイムゾーンの UTC 時間として表示される
CSCwa35291	SVO : EPNM 回線復元設定で復元可能な回線が復元済みステータスになる
CSCwb03047	復帰設定を手動または自動にして NE-DISCONNECT CLEAR イベントが発生すると、回線が不完全 (Partial) 状態になる
CSCwb04517	オプティカルコンテンツ cepnm6.0PI_DPP2 の Pom の変更
CSCwa95404	OTDR : 2 行が選択されている場合、OTDR で Geo マップと X 軸プロットの問題が発生する

Cisco EPN Manager 6.0.2 デバイスパックおよびポイントパッチの入手とインストール

この手順では、Cisco EPN Manager 6.0.2 をダウンロードして、既存の Cisco EPN Manager 6.0/6.0.1 インストール上にインストールする方法について説明します。

前提条件

Cisco EPNM 6.0/6.0.1。

非 HA 展開

アップデートのダウンロードとインストール

1. 左側のサイドバーから、[管理 (Administration)] > [ライセンスとソフトウェアアップデート (Licenses and Software Update)] > [ソフトウェアアップデート (Software Update)] を選択します。
2. EPNM GUI から [Cisco.com からのダウンロード (Download from Cisco.com)] オプションを使用するか、ブラウザから Cisco.com に直接ログインして、最新のアップデートをダウンロードします。
ファイルには、プレフィックス **cepnm6.0-dppX-buildxxx.ubf** が付きます。
3. ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード (Upload from local computer)] または [サーバーのローカルディスクからコピー (Copy from server's local disk)] を選択します。
4. ファイルがロードされたら、EPN Manager アップデートに関連付けられている [インストール (Install)] ボタンをクリックします。
5. インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい (Yes)] をクリックします。
注：インストールが完了すると、サーバーが再起動します。
6. 既存のファイルを上書きするかどうかを確認するメッセージが表示された場合は、[はい (Yes)] をクリックします。
インストールが成功すると、ステータスが [インストール済み (Installed)] に変わります。Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります (最大 1 時間)。
7. Cisco EPN Manager サービスのステータスを確認します。
 1. Cisco EPN Manager サーバーとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。
 2. 「**ncs status**」コマンドを実行して、少なくともヘルスマニター、データベース、NMS、SAM デーモン、DA デーモン、コンプライアンスエンジンのサービスが稼働していることを確認します。
注：最適な Cisco EPN Manager 機能を使用するには、すべてのサービスが稼働している必要があります。
8. Cisco EPN Manager の Web GUI にアクセスできる場合は、ログインして、[ソフトウェアアップデート (Software Update)] ページでパッチのステータスが [インストール済み (Installed)] になっていることを確認します。
 - 左側のサイドバーから、[管理 (Administration)] > [ライセンスとソフトウェアアップデート (Licenses and Software Update)] > [ソフトウェアアップデート (Software Update)] を選択します。

すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）

以前のバージョンの Cisco EPN Manager をすでに使用している場合（つまり、新規インストールではない場合）、デバイスで同期操作を実行する必要があります。同期操作では、デバイスの物理インベントリと論理インベントリを収集し、その情報をデータベースに保存するように Cisco EPN Manager に指示します。

1. [モニター (Monitor)] > [ネットワークデバイス (Network Devices)] の順に選択します。
2. すべてのデバイスを選択し、[同期 (Sync)] をクリックします。

HA の導入

高可用性環境に Cisco EPN Manager 6.0.2 をインストールします。

注：外部の認証および承認を使用している場合は、インストール後に、最新のアップデートを取得するために、ユーザータスク情報を AAA サーバーにエクスポートする必要があります。詳細については、『[Cisco Evolved Programmable Network Manager 6.0.0 ユーザーおよび管理者ガイド](#)』を参照してください。

サーバのセッションタイムアウトを増やす

はじめる前に

- プライマリおよびセカンダリ HA サーバーへのパッチ適用中、両方のサーバーがダウン状態になります。
- HA を有効にしたときに作成したパスワード（認証キー）があることを確認します。セカンダリ サーバーにパッチをインストールするときに必要です。
- データをバックアップします（データをバックアップする手順については、『[Cisco Evolved Programmable Network Manager 6.0.0 ユーザーおよび管理者ガイド](#)』を参照してください）。

次のように、プライマリ サーバとセカンダリ サーバのタイムアウトを 30 分から 90 分に増やします。

1. Linux CLI ルート ユーザーとしてログインします。
2. 次のコマンド（1 行）を実行して、/opt/CSColumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/ にある web.xml ファイルのバックアップを保存します。

```
cp /opt/CSColumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml/opt/CSColumos/tomcatSWUpdate/webapps /ROOT/WEB-INF/web.xml.orig
```
3. web.xml ファイル (/opt/CSColumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml) で、**<session-timeout>30</session-timeout>** を検索します。
4. セッションタイムアウトを 90 分に変更します (**<session-timeout>90</session-timeout>**)

5. Cisco EPN Manager CLI 管理者ユーザーとして、手動でサーバーを停止し、再起動します。

```
ncs stop

ncs start
```

6. 次のコマンドを実行して、すべてのサービスが起動していて実行されていることを確認します。

```
ncs status
```

HA 設定の削除

1. Cisco EPN Manager Web GUI に管理者権限を持つユーザーとしてログインします。
2. 左側のサイドバーから、[管理 (Administration)] > [設定 (Settings)] > [高可用性 (High Availability)] の順に選択します。
3. [HA 設定 (HA Configuration)] タブをクリックします。
4. [削除] をクリックします。
5. プライマリサーバーで、[管理 (Administration)] > [設定 (Settings)] > [高可用性 (High Availability)] に移動し、[コンフィギュレーションモード (Configuration Mode)] フィールドに「HA 未構成 (HA Not Configured)」と表示されていることを確認します。
6. セカンダリサーバーのヘルスマニターページ (<https://serverIP:8082>) にログインし、[状態 (State)] 列に「HA 未構成 (HA Not Configured)」と表示されていることを確認します。

プライマリサーバーとセカンダリサーバー (HA 展開) にデバイスパックとポイントパッチをインストールします。

はじめる前に

- HA を有効にしたときに作成したパスワード (認証キー) があることを確認します。セカンダリサーバーにメンテナンスパックをインストールする必要があります。
- 進行中のバックアップがないことを確認します。
- セカンダリ サーバで、ソフト リンクを使用してタイム ゾーンを更新します (次のコマンドは 1 行です)。

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d
" " -f 3) /etc/localtime
```

これにより、フェールオーバー後に EPNM サーバーがセカンダリサーバー上で稼働するようになります。

プライマリサーバーへのデバイスパックとポイントパッチのインストール

1. 左側のサイドバーから、[管理 (Administration)] > [ライセンスとソフトウェアアップデート (Licenses and Software Update)] > [ソフトウェアアップデート (Software Update)] を選択します。
2. EPNM GUI から [Cisco.com からのダウンロード (Download from Cisco.com)] オプションを使用するか、ブラウザから **Cisco.com** に直接ログインして、最新のアップデートをダウンロードします。
ファイルには、プレフィックス **cepnm6.0-dppX-buildxxx.ubf** が付きます
3. ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード (Upload from local computer)] または [サーバーのローカルディスクからコピー (Copy from server's local disk)] を選択します。
4. ファイルがロードされたら、EPN Manager アップデートに関連付けられている [インストール (Install)] ボタンをクリックします。
5. インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい (Yes)] をクリックします。
Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります (最大 1 時間) 。
6. 「ハードウェアと NTP クロックの同期」で説明されているように、プライマリサーバーとセカンダリサーバーの両方でハードウェアクロックと NTP クロックを同期し、各サーバーのクロックが相互に同期されていることを確認します。
注：デバイスパックおよびポイントパッチをインストールすると Cisco EPN Manager が再起動されるため、同期クロック操作でのサービスの再起動は無視できます。

セカンダリサーバーへの Cisco EPN Manager 6.0.x のインストール

1. ブラウザに次の URL を入力することにより、セカンダリ サーバーの HM Web ページにログインします。
`https://serverIP:8082`
ここで、serverIP はセカンダリ サーバーの IP アドレスまたはホスト名です。
2. 認証キーを入力して、[ログイン (Login)] をクリックします。
3. [ソフトウェアアップデート (Software Update)] ボタンをクリックします。
4. ログインページが表示されます。管理者として EPNM にログインします。
5. EPNM GUI から [Cisco.com からのダウンロード (Download from Cisco.com)] オプションを使用するか、ブラウザから **Cisco.com** に直接ログインして、最新のアップデートをダウンロードします。
ファイルには、プレフィックス **cepnm6.0-dppX-buildxxx.ubf** が付きます
6. ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード (Upload from local computer)] または [サーバーのローカルディスクからコピー (Copy from server's local disk)] を選択します。
7. インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい (Yes)] をクリックします。
Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります (最大 1 時間) 。

セカンダリサーバーでのインストールの検証

1. Cisco EPN Manager サーバーとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。
2. `ncs status` コマンドを実行して、少なくともヘルスマニター、データベース、NMS、SAM デーモン、DA デーモン、コンプライアンスエンジンのサービスが稼働していることを確認します。最適な Cisco EPN Manager 機能を使用するには、すべてのサービスが稼働している必要があることに注意してください。
3. Web GUI にアクセスできたら、セカンダリ サーバーの [HM Web] ページでインストールとバージョンを確認します。ブラウザに URL (`https://serverIP:8087`) を入力します。

ここで、`serverIP` はセカンダリ サーバーの IP アドレスまたはホスト名です。

4. 認証キーを入力して、[ログイン (Login)] をクリックします。
5. [アップロード済みのアップデートファイル (Uploaded Update Files)] タブで、MPx ubf ファイル (`cepnm.6.0-dpX-buildxxx.ubf` の形式) が表示されており、[使用中 (In Use)] ステータスが [はい (Yes)] になっていることを確認します。
6. 次のコマンドを実行して、すべてのサービスが起動していて実行されていることを確認します。

```
ncs status
```

高可用性を有効にして HA ステータスを確認

1. 高可用性を有効にします。
 1. Cisco EPN Manager Web GUI に管理者権限を持つユーザーとしてログインします。
 2. 左側のサイドバーメニューから、[管理 (Administration)] > [設定 (Settings)] > [高可用性 (High Availability)] の順に選択します。
 3. [HA 設定 (HA Configuration)] タブをクリックして、セカンダリサーバーの IP アドレス、セカンダリサーバーの認証キー、および Cisco EPN Manager が HA の状態変更通知を送信する電子メールアドレスを入力します。
 4. HA セットアップで仮想 IP アドレッシングを使用している場合 (プライマリ サーバとセカンダリ サーバが同じサブネットにある場合) は、[仮想 IP の有効化 (Enable Virtual IP)] チェックボックスをオンにして、仮想 IP アドレスを入力します。
 5. [保存 (Save)] をクリックして、サーバーが同期されるまで待ちます。
 6. 設定モードが [HA 対応 (HA Enabled)] になっていることを確認します。
2. プライマリ サーバーの HA ステータスを確認します。
 1. [HA 設定 (HA Configuration)] タブをクリックします。
 2. サーバーのステータスが [HA コンフィギュレーションモード (HA Configuration mode)] で「プライマリアクティブ (Primary Active)」であることを確認します。

3. セカンダリサーバーの HA ステータスを確認します。

1. ブラウザに次の URL を入力することにより、セカンダリ サーバーの HM Web ページにログインします。

https://serverIP:8082

ここで、serverIP はセカンダリ サーバーの IP アドレスまたはホスト名です。

2. 認証キーを入力して、[ログイン (Login)] をクリックします。
3. ステータスが緑のチェックマークで、状態が「セカンダリ同期中 (Secondary Synching)」であることを確認します。

すべてのデバイスのインベントリとデータベースの同期 (既存の展開のみ)

以前のバージョンの Cisco EPN Manager をすでに使用している場合 (つまり、新規インストールではない場合)、デバイスで同期操作を実行する必要があります。同期操作では、デバイスの物理インベントリと論理インベントリを収集し、その情報をデータベースに保存するように Cisco EPN Manager に指示します。

1. [モニター (Monitor)] > [ネットワークデバイス (Network Devices)] の順に選択します。
2. すべてのデバイスを選択し、[同期 (Sync)] をクリックします。

ハードウェアと NTP クロックの同期

この手順では、hwclock コマンドを使用してハードウェアのクロックを NTP クロックと同期します。

1. Linux CLI ルート ユーザーとしてログインします。
2. NTP サービスのステータスを確認し、NTP が次のコマンドを使用して安定した時刻参照を取得していることを確認します。次に、表示される出力の例を示します。

- ntpd が実行されていることを確認します。

```
service ntpd status
```

```
ntpd (pid 3290) is running...
```

- ntpd (pid 3290) が実行されていない場合は、次のコマンドを使用して開始します。

```
service ntpd start
```

(ntpd のステータスを再確認して、実行されていることを確認します)。

- NTP が NTP サーバから時間を受信していることを確認します。

```
ntpstat
```

```
synchronised to NTP server (10.116.134.075) at stratum 3 time correct to within 62 ms polling server every 1024 s
```

このような出力が表示されない場合、NTP の同期はまだ行われていません。数分間待ってから、ntpstat を再度実行します。10 分以内に同期が行われない場合は、システム管理者またはシスコ サポートに連絡してください。

3. 次のコマンドを使用して、ハードウェアのクロックを NTP と同期します。

```
hwclock --systohc --debug
```

以下のような出力が表示されます。

```
hwclock from util-linux-ng 2.17.2
Using /dev interface to clock.
Last drift adjustment done at 1470117750 seconds after 1969
Last calibration done at 1470117750 seconds after 1969
Hardware clock is on local time
Assuming hardware clock is kept in local time.
Waiting for clock tick...
...got clock tick
Time read from Hardware Clock: 2021/08/02 16:03:30
Hw clock time: 2021/08/02 16:03:30 = 1470117810 seconds since 1969
1470117810.500000 is close enough to 1470117810.500000 (0.000000 < 0.001000)
Set RTC to 1470117810 (1470117810 + 0; refsystime = 1470117810.000000)
Setting Hardware Clock to 16:03:30 = 1470117810 seconds since 1969
ioctl(RTC_SET_TIME) was successful.
Not adjusting drift factor because it has been less than a day since the last calibration.
root$
```

4. ハードウェアのクロックが NTP と同期されていることを確認します。

```
echo "hwclock is: $(hwclock --show)" ; echo "linux clock is: $(date)";
```

出力を確認し、2つのクロックが（少なくとも数秒以内に）同期していることを確認します。

```
Hwclock is: Tue 26 Jul 2021 06:11:40 PM AEST -0.391028 secondslinux clock is: Tue Jul 26
18:11:40
AEST 2021
```

5. Linux CLI 管理者ユーザーとして、Cisco EPN Manager サービスを再起動します。

- Linux CLI ルート ユーザーとしてログインしている場合は、Linux CLI 管理者ユーザーに切り替えます。

```
exit
```

- Cisco EPN Manager CLI 管理者ユーザーに切り替えます。
- Cisco EPN Manager サービスを停止して再起動します。

```
nscs stop
```

```
nscs start
```

マニュアルの入手方法、テクニカルサポート、およびセキュリティガイドライン

マニュアルの入手方法、テクニカルサポート、マニュアルに関するフィードバックの提供、セキュリティガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、毎月更新される『[What's New in Cisco Product Documentation](#)』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback



©2022 Cisco Systems, Inc. All rights reserved.
Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間の
パートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は2022年8月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp