



# Cisco Prime Network Registrarのインストールおよびアップグレード

この章は、次の項で構成されています。

- [Cisco Prime Network Registrar のインストール](#) (1 ページ)
- [アップグレードの考慮事項](#) (4 ページ)
- [Cisco Prime Network Registrar のアップグレード](#) (6 ページ)
- [以前の製品バージョンへの復元](#) (8 ページ)
- [新しいマシンへのローカルクラスタの移動](#) (9 ページ)
- [リージョナルクラスタの新しいマシンへの移動](#) (10 ページ)
- [独自の Web UI アクセス用証明書のインストール](#) (11 ページ)
- [インストールに関するトラブルシューティングを実行](#) (13 ページ)
- [ローカルクラスタのライセンスの問題のトラブルシューティング](#) (14 ページ)

## Cisco Prime Network Registrar のインストール

11.0 以降のリリースでは、インストール時に設定について質問されることはありません。Cisco Prime Network Registrar また、管理者のログイン情報とライセンスの詳細を要求されることはなくなりました。Cisco Prime Network Registrar に初めて接続するときに、これらの詳細を入力する必要があります ([Cisco Prime Network Registrar の使用](#)を参照)。

次のパスが使用されます。

- プログラムファイル : `/opt/nwreg2/{local | regional}`



**警告** `/opt/nwreg2/*` ディレクトリ内のファイルは、アップグレードまたはインストール中に上書きされるため、追加または変更しないでください。`/var` 領域でのみファイルを追加または変更することができます。たとえば、`/var/nwreg2/local/extensions` 領域で拡張を追加するようにし、`/opt` 領域では追加しないようにしてください。

- データファイル : /var/nwreg2/{local | regional}/data
- ログファイル : /var/nwreg2/{local | regional}/logs
- cnr.conf ファイル : /var/nwreg2/{local | regional}/conf

また、Cisco Prime Network Registrar 11.0 のインストールはデフォルトで次のように設定されます。

- Web セキュリティのタイプ : HTTPS のみ (ローカルの場合は 8443、リージョナルの場合は 8453)
- Web サービス : REST API が有効 (HTTPS ポート、個別のポートはなし)
- セキュリティモード : 必須
- SCP ポート番号 : デフォルトポートの CCM (ローカルの場合は 1234、リージョナルの場合は 1244)
- ルートとして実行 : 常にルートとして実行します。最初のログイン時にスーパーユーザー管理者を作成する必要があります ([Cisco Prime Network Registrar の使用](#) を参照)。
- インストールのタイプ (ローカル、リージョナル、クライアントのみ) : 使用する RPM キットによって異なります。Cisco Prime Network Registrar 11.0 では、次の RPM キットが使用可能です。

表 1: RPM キット

	RHEL/CentOS 7.x	RHEL/CentOS 8.x
リージョナルクラスタ	cpnr-regional-11.0-1.el7*.x86_64.rpm	cpnr-regional-11.0-1.el8*.x86_64.rpm
ローカルクラスタ	cpnr-local-11.0-1.el7*.x86_64.rpm	cpnr-local-11.0-1.el8*.x86_64.rpm
クライアントのみ	cpnr-client-11.0-1.el7*.x86_64.rpm	cpnr-client-11.0-1.el8*.x86_64.rpm
キット名の * は、パッケージの分岐元の RHEL マイナーバージョンを示します。		

次の手順は、新規インストールに適用されます。Cisco Prime Network Registrar の以前のバージョンから 11.0 にアップグレードするには、[Cisco Prime Network Registrar のアップグレード \(6 ページ\)](#) を参照してください。

Cisco Prime Network Registrar をインストールするには、次の手順を実行します。

**ステップ 1** ターゲットマシンにログインします。

**注意** Red Hat および CentOS Linux の多くのディストリビューションでは、デフォルトで、ファイアウォールと接続追跡がインストールされ、有効になります。DNS サーバーのオペレーティングシステムでステートフルファイアウォールを実行すると、サーバーのパフォーマンスが大幅に低下します。シスコでは、DNS サーバのオペレーティングシステム上でファイアウォールを使用しないことを強くお勧めします。ファイアウォールを無効にできない場合は、DNS トラフィックの接続追跡を無効にする必要があります。詳細については、*Cisco Prime Network Registrar 11.0* アドミニストレーションガイドの「DNS パフォーマンスとファイアウォールの接続追跡 (*DNS Performance and Firewall Connection Tracking*)」の項を参照してください。

**ステップ 2** OpenJDK 1.8 以降をまだインストールしていない場合は、インストールします。次のコマンドを使用します。

```
# yum install java-1.8.0-openjdk
```

一部のシステムでは、**dnf install** コマンドを使用する必要があります。

**ステップ 3** 必要に応じて、Cisco.com からディストリビューションファイル (RPMキット) をダウンロードします。Cisco Prime Network Registrar 11.0 で使用可能な RPM キットのリストについては、上記の表 1: RPM キットを参照してください。

Cisco Prime Network Registrar 11.0 は、デフォルトでクライアントとサーバーの両方をインストールします。クライアントのみのインストールの場合は、上記の表 1: RPM キット一覧に記載されている適切なキットを使用します。

(注) クライアントソフトウェアをプロトコルサーバーとは異なるマシンで実行する場合には、クライアントのみのインストールを選択します。次に、クライアントからプロトコルサーバーへの接続を設定する必要があります。

**ステップ 4** ダウンロードしたディストリビューションファイルを保存したディレクトリに移動します。

**ステップ 5** 次のコマンドを入力して、Cisco Prime Network Registrar をインストールします。

```
# yum install filename
```

または

```
# rpm -i filename
```

または

```
# dnf install filename
```

*filename* は、表 1: RPM キット (2 ページ) に記載されている RPM キット名です。

RHEL/CentOS 7.x キットの名前には「el7 \*」が、RHEL/CentOS 8.x キットの名前には「el8 \*」が含まれていることに注意してください。\* は、パッケージの分岐元の RHEL マイナーバージョンであることを示しています。

たとえば、RHEL/CentOS 7.x にリージョナルクラスタをインストールするには、次のいずれかのコマンドを使用します。

```
# yum install cpnr-regional-11.0-1.el7_9.x86_64.rpm
```

または

```
# rpm -i cpnr-regional-11.0-1.e17_9.x86_64.rpm
```

または

```
# dnf install cpnr-regional-11.0-1.e17_9.x86_64.rpm
```

(注) ライセンス管理にはリージョナルサーバーが必要であるため、最初にリージョナルサーバーをインストールして、ローカルをリージョナルに登録できるようにします。

**ステップ 6** 次のコマンドを使用して Cisco Prime Network Registrar サーバーエージェントを起動します（または、Cisco Prime Network Registrar が自動的に起動するように設定されているので、システムを再起動します）。

ローカルクラスタの場合

```
# systemctl start nwreglocal
```

リージョナルクラスタの場合

```
# systemctl start nwregregional
```

起動時に、`/var/nwreg2/{local|regional}` フォルダが作成されます。キーストアファイルは `/var/nwreg2/{local|regional}/conf/priv` フォルダに作成され、キーストアの詳細が `cnr-priv.conf` ファイルで更新されます。

独自の証明書を使用する場合は、[独自の Web UI アクセス用証明書のインストール \(11 ページ\)](#) を参照してください。

**ステップ 7** Cisco Prime Network Registrar サーバーのステータスを確認します。次のコマンドのいずれかを実行します。

```
# ./cnr_status (install-path/usrbin ディレクトリで使用可能)
```

または

```
# systemctl status nwreglocal (ローカルクラスタの場合)
```

```
# systemctl status nwregregional (リージョナルクラスタの場合)
```

---

インストールが完了したら、[Cisco Prime Network Registrar の使用の手順](#)に従って Cisco Prime Network Registrar の使用を開始します。これらのファイルは、今後のアップグレードで上書きされる可能性があるため、`/opt` フォルダに変更や追加を行わないようにしてください。`/var` フォルダは変更可能です。

## アップグレードの考慮事項

Cisco Prime Network Registrar 11.0 は、8.3 以降からの直接アップグレードをサポートしています。

Cisco Prime Network Registrar 11.0 は Red Hat/CentOS 7.x および 8.x で実行できます。以前のバージョンのオペレーティングシステムを使用している場合は、まずシステムを、サポートされているバージョンにアップグレードする必要があります。

ソフトウェアをインストールすると、インストールプログラムによって既存のバージョンが自動的に検出され、ソフトウェアが最新リリースにアップグレードされます。既存の Cisco Prime

Network Registrar データをアーカイブします。アップグレードが失敗し、開始できない場合は、作成したバックアップから回復する必要があります（古い Cisco Prime Network Registrar バージョンをインストールする場合があります）。データのバックアップは、`/var/nwreg2/{local|regional}` ディレクトリ (`upgrade-backup-date.tar.gz`) にも保存されています。独自のバックアップを作成しなかった場合は、このバックアップを使用してデータベースを復元できます。

イベントストアは、保留中の DNS 更新を追跡するために使用されなくなりました。リースを使用する DHCPv6 DNS 更新と同様に、DHCPv4 リースオブジェクトがこの目的で使用されません。したがって、Cisco Prime Network Registrar 10.x 以前からアップグレードする場合は、保留中の DHCPv4 DNS 更新が失われるため、DNS 更新のバックログが少ないときにアップグレードするのが最適です。DHCP サーバーは、ログメッセージ 19669 を使用して、ドロップした DNS 更新イベントをログに記録します。これにより、各保留中のイベントに関連するリース、保留中のアクション、FQDN、および DNS 更新設定オブジェクトが報告されます。これらは、サーバーがイベントストアからイベントを削除するときに 1 度だけ記録されます。DNS 更新のバックログは、`dhcp getRelatedServers` コマンドを使用し、DNS サーバーの「要求」数を調べることで確認できます。

## スマートライセンシングの使用

Cisco Prime Network Registrar 11.x リージョナルは、スマートライセンスモードで動作し、11.0 より前のローカルクラスタをサポートしません。ただし、スマートライセンスに移行するには、次の手順を実行する必要があります。

**ステップ 1** Cisco Prime Network Registrar リージョナルクラスタを 11.x にアップグレードし、スマートライセンスを無効にします（アップグレード後）。スマートライセンスを無効にする方法については、*Cisco Prime Network Registrar 11.0* アドミニストレーションガイドの「スマートライセンスの無効化 (*Disabling Smart Licensing*)」の項を参照してください。

**ステップ 2** Cisco Prime Network Registrar 11.x リージョナルクラスタに必要な従来のライセンスをロードします。

**ステップ 3** ローカルクラスタをアップグレードしたリージョナルクラスタに再登録または再同期します。

**警告** 10.x ローカルクラスタを 11.x リージョナルクラスタに登録する前に、10.x ローカルクラスタを 10.1.1（またはそれ以降のバージョン）にアップグレードする必要があります。Cisco Prime Network Registrar バージョン 10.1.1 より前の 10.x ローカルクラスタでは、11.x リージョナルクラスタに登録する際に問題が発生します。

**ステップ 4** スケジュールに従って、すべてのローカルクラスタを 11.x にアップグレードしてください。

**ステップ 5** すべてのクラスタが 11.x にアップグレードされると、スマートライセンスに移行する場合は、リージョナルでスマートライセンスを有効にすることができます。この手順は、CSSM またはサテライトのスマートアカウントに必要なライセンスがある場合にのみ実行してください。スマートライセンスを有効にするには、*Cisco Prime Network Registrar 11.0* アドミニストレーションガイドの「スマートライセンスの有効化 (*Enabling Smart Licensing*)」の項を参照してください。

# Cisco Prime Network Registrar のアップグレード

Cisco Prime Network Registrar 11.0 で導入された主な変更点の 1 つは、配布されたファイル（つまり、RPM によってインストールされたファイル）を、インストールに固有のデータや設定ファイルと区別することです。基本的に、`//opt/nwreg2` の領域には、インストールの一部として提供されないファイルを含めないようにします。インストールに固有のすべてのデータや設定ファイルが `/var/nwreg2` の領域にあるはずですが。

Cisco Prime Network Registrar の以前のバージョンをインストールしたときにデフォルトのパスを使用した場合、Cisco Prime Network Registrar 11.0 のインストール後に初めて Cisco Prime Network Registrar を起動すると、次のファイルが自動的に再配置されます。

- `/opt/nwreg2/{local | regional}/conf/cnr.conf` は `/var/nwreg2/{local | regional}/conf` に移動されます
- `/opt/nwreg2/{local | regional}/conf/priv`（およびその内容）は `/var/nwreg2/{local | regional}/conf/priv` に移動されます
- `/opt/nwreg2/{local | regional}/conf/cert`（およびその内容）は `/var/nwreg2/{local | regional}/conf/cert` に移動されます
- `cnr.conf` および `cnr-priv.conf` 内のすべてのパスは、この移動を反映して更新されます。

Cisco Prime Network Registrar データ領域が `/var/nwreg2/{local | regional}/data` にない場合も同様の移動が行われますが、結果のパスはデータディレクトリの親ディレクトリにある新しい `conf` ディレクトリを使用します。または、ファイルをそのままにしておくこともできます。

以前のバージョンから Cisco Prime Network Registrar 11.0 にアップグレードすると、上記の他にも、次のような変更が発生します。

- `/opt/nwreg2/{local | regional}/bin/cnr.env` ファイルの代わりに、`/usr/lib/systemd/system` ディレクトリにある、`nwreglocal.env`（ローカル用）ファイルまたは `nwregregional.env`（リージョン用）ファイルが使用されます。したがって、インストール後（Cisco Prime Network Registrar の起動前）に、`cnr.env` の変更（拡張機能の `LD_LIBRARY_PATH` など）を新しい `new.env` ファイルに適用する必要があるかどうかを確認する必要があります。
- Web UI キーストアは、既存のものがある場合、または新規に生成される場合に使用されます。既存の `priv/cnr-priv.conf` が使用され、`/var/nwreg2/{local | regional}` に再配置されます。
- Web UI および REST では、HTTP の代わりに HTTPS が使用されます。HTTPS 用に設定されたポートがない場合は、デフォルト（リージョン|ローカル）のポートが使用されます。
- 以前のインストールで REST が無効になっている場合は、アップグレード後に有効になります。REST API を無効にする場合は、アップグレード後に **REST API の無効化** の手順に従います。以前に REST が HTTPS とは異なるポートを使用していた場合、それはサポートされなくなり、HTTPS（Web UI）および REST に同じポートが使用されます。



- (注) Cisco Prime Network Registrar 10.1 以降では、キーストアパスワードはデフォルトで暗号化されます。したがって、10.1 から 11.0 にアップグレードする場合は、キーストアパスワードを暗号化する必要はありません。ただし、10.1 より前のバージョンから 11.0 にアップグレードする場合は、キーストアパスワードを手動で暗号化する必要があります。

暗号化されたパスワードを生成するには、*install-path/usrbin* ディレクトリにある暗号化スクリプト (**encrypt -s <plain-text password>**) を使用します。server.xml でこの暗号化されたパスワードを更新し、変更後に Cisco Prime Network Registrar を再起動する必要があります。

Cisco Prime Network Registrar 11.0 にアップグレードするには、次の手順を実行します。

- ステップ 1** ご使用の環境が現在のシステム要件を満たしていることを確認します ([システム要件](#)を参照)。
- ステップ 2** [Cisco Prime Network Registrar のアンインストール](#) に記載されている手順を使用して、既存のインストールを削除します。最後に記載されているクリーンアップ操作は行わないようにします (つまり、データ、cnr.conf など保持します)。
- ステップ 3** 古い cnr.conf が *install-path/conf* にある場合は、何もせずにアップグレードできます。古い cnr.conf が別の場所にある場合は、次の行を含む *install-path/conf* ディレクトリに cnr.conf ファイルを作成します。
- ```
cnr.confdir=古い cnr.conf ファイルのディレクション
```
- ステップ 4** Java のアップグレードに関連する問題を軽減するため、cnr.conf ファイルを編集して cnr.java-home のエントリパスを /usr/bin/java に置き換えることを強く推奨します (cnr.conf で指定された Java のバージョンを持つパスの場合)。これをテストするには、次の手順を実行します。
- ```
/usr/bin/java -version
```
- および
- ```
cnr.java-home-path/bin/java -version
```
- 2つの結果が同じである場合は、cnr.java-home のパスを変更して /usr/bin/java を指定します。これをテストすることで、Java を更新するときに cnr.java-home パスを更新する必要がなくなります。
- ステップ 5** Cisco Prime Network Registrar 11.0 をインストールします。インストール手順については、[Cisco Prime Network Registrar のインストール \(1 ページ\)](#) を参照してください。
- ステップ 6** 次のコマンドを使用して、Cisco Prime Network Registrar サーバーエージェントを起動します。

- ローカルクラスタの場合

```
# systemctl start nwreglocal
```
- リージョナルクラスタの場合

```
# systemctl start nwregregional
```

設定やリース/リソースレコードデータのサイズ、およびアップグレード前のバージョンによっては、アップグレードプロセスに時間がかかる場合があります。ステータスは、**systemctl status nwreglocal** (ローカルクラスタの場合) または **systemctl status nwregregional** (リージョナルクラスタの場合) コマンドを使用し

て表示できます。これが「trampolic startup、local mode」（ローカルクラスタの場合）または「trampoline startup、regional mode」（リージョナルクラスタの場合）になっている場合は、サービスが起動していることを示しています。[Cisco Prime Network Registrar の使用](#) の手順に従って Cisco Prime Network Registrar の使用を開始します。

アップグレードが失敗した場合は、Cisco Prime Network Registrar の以前のバージョンに戻すことができます。以前のバージョンに戻す方法の詳細については、[以前の製品バージョンへの復元（8 ページ）](#) を参照してください。

## 以前の製品バージョンへの復元

Cisco Prime Network Registrar インストールプログラムは、新しいバージョンにアップグレードすると、既存の製品構成とデータをアーカイブします。アップグレードプロセスが失敗した場合は、次の手順を使用して以前の製品バージョンと構成に戻します。



**注意** このプロセスを完了するには、以前の Cisco Prime Network Registrar バージョンの製品インストーラとライセンスキーまたはライセンスファイルにアクセスする必要があります。それ以外の方法で進めようとする、製品が不安定になる可能性があります。

インストーラがアップグレードを正常に実行したが、後で以前のバージョンにロールバックする場合、この手順によりネットワークが不安定になり、データが失われる可能性があります。たとえば、アップグレード後に Cisco Prime Network Registrar データベースに加えられた更新（DHCP リースデータや DNS 動的更新など）は失われます。

**ステップ 1** アーカイブファイル `upgrade-backup- date.tar.gz` が `/var/nwreg2/{local | regional}` ディレクトリ内で使用可能であることを確認します。

**ステップ 2** [Cisco Prime Network Registrar のアンインストール](#) に記載されている手順を使用して、Cisco Prime Network Registrar をアンインストールします。

**ステップ 3** アーカイブファイルの内容以外に、Cisco Prime Network Registrar インストールパスの残りのファイルとディレクトリを削除します。

**ステップ 4** バックアップ（ステップ 7 で作成したアーカイブファイル）を復元します。

**ステップ 5** Cisco Prime Network Registrar の元のバージョンを再インストールします。元の製品バージョンに固有の『*Cisco Prime Network Registrar* インストールガイド』に記載されている再インストール手順に従ってください。

**ステップ 6** インストールが正常に終了したら、Cisco Prime Network Registrar サーバエージェントを停止します。

- ローカルクラスタの場合
  - # `systemctl stop nwreglocal`
- リージョナルクラスタの場合

```
# systemctl stop nwregregional
```

**ステップ 7** Cisco Prime Network Registrar の再インストールされたバージョンにバックアップファイルの内容を展開します。

- a) ファイルシステムのルートディレクトリ (*/*) に移動します。
- b) アーカイブディレクトリへの完全修飾パスを使用して、アーカイブを展開します。

- **cd /** を使用して、ファイルシステムのルートディレクトリに移動します。

- **upgrade-backup-date.tar.gz** ファイルを含むアーカイブディレクトリへの完全修飾パスを使用して、アーカイブを展開します。

```
tar xzf /var/nwreg2/{local | regional}/upgrade-backup-date.tar.gz
```

上記のコマンドは、**opt** および **var** フォルダを作成します。**opt** フォルダには **conf** ディレクトリのみが含まれます。

**ステップ 8** 範囲とゾーンを含む以前の構成が変更されていないことを確認します。

## 新しいマシンへのローカルクラスタの移動

開始する前に、新しいマシンが現在のシステム要件を満たしていることを確認します ([システム要件](#)を参照)。

次のステップを使用して、クラスタを Cisco Prime Network Registrar の最新バージョンにアップグレードできます (つまり、ステップ 5 で同じバージョンの Cisco Prime Network Registrar をインストールする必要はありません。以前のバージョンからのアップグレードをサポートする新しいバージョンをインストールできます)。

既存の Cisco Prime Network Registrar インストールを同じプラットフォーム上の新しいマシンに移動するには、次の手順を実行します。

**ステップ 1** 古いローカルサーバのサーバエージェントを停止します。

```
# systemctl stop nwreglocal
```

**ステップ 2** /var/nwreg2/local/tomcat を除いて、/var/nwreg2/local を tar ファイルにします。最新のバックアップをコピーしない場合は、/var/nwreg2/local/data.bak をスキップすることもできます。

**ステップ 3** 新しいサーバに tar ファイルをコピーし、ファイルを同じ場所 (/var/nwreg2/local) に展開します。/var/nwreg2/local/tomcat ディレクトリがないことを確認します (存在する場合は削除します)。

(注) ステップ 2 とステップ 3 は、Cisco Prime Network Registrar 11.0 以降に適用されます。以前のリリースについては、そのバージョンのマニュアルを参照してください。

**ステップ 4** /usr/lib/systemd/system/nwreglocal.env ファイルを新しいシステムに移動します。

**ステップ 5** 新しいサーバに Cisco Prime Network Registrar（ローカルクラスタ）をインストールします。インストールにより、コピーされたデータに基づいてアップグレードが検出されます。

この手順では、元のデータが古いマシンに保存されます。

インストール後にカスタム構成の変更（Web UIのセキュリティ強化で説明されている変更など）を再適用します。

**ステップ 6** Web UIにログインし、[管理（Administration）]メニューの[ライセンス（Licenses）]ページに移動して[ライセンスの一覧（List Licenses）]ページを開きます。

**ステップ 7** 必要に応じて、リージョナルサーバ情報を編集します。提供されたリージョナルサーバ情報が、新しいマシンを登録する場所にあることを確認します。

**ステップ 8** [登録（Register）] ボタンをクリックして、リージョナルサーバに登録します。

**ステップ 9** マシンのIPアドレスが変更された場合は、フェールオーバー/HADNS パートナーも更新して、サーバの新しいアドレスも確保する必要があります。DHCPでは、リレーエージェントヘルパーアドレスとDNSサーバアドレスを更新する必要がある場合があります。

(注) アドレスを変更すると、DHCP クライアントはすぐに更新できなくなり（再バインド時間に達するまで更新できなくなる可能性があります）、クライアントまたは他のDNSサーバが更新された情報を受信するまで、DNS クエリが解決されないことがあります。

## リージョナルクラスタの新しいマシンへの移動

ライセンス管理は、Cisco Prime Network Registrar がインストールされるときに、リージョナルクラスタから実行されます。まず、リージョナルサーバがインストールされ、リージョナルサーバにすべてのライセンスをロードされます。ローカルクラスタがインストールされると、ライセンスを取得するためにリージョナルサーバに登録されます。

リージョナルクラスタを新しいマシンに移動する場合は、古いリージョナルクラスタのデータをバックアップし、新しいマシンの同じ場所にデータをコピーする必要があります。



(注) リージョナルサーバがダウンした場合、またはサービスを停止した場合、ローカルクラスタはこのアクションを認識しません。停止時間が 24 時間未満の場合、ローカルクラスタの機能に影響はありません。ただし、リージョナルクラスタが 24 時間を超える期間にわたって復元されない場合、ローカルクラスタは（Web UI、CLI、または SDK で）適切にライセンスされていないという警告メッセージをレポートすることがあります。これはローカルクラスタの操作には影響せず、ローカルクラスタは引き続き動作して要求に対応します。

次のステップを使用して、クラスタを Cisco Prime Network Registrar の最新バージョンにアップグレードできます（つまり、ステップ 5 で同じバージョンの Cisco Prime Network Registrar をインストールする必要はありません。以前のバージョンからのアップグレードをサポートする新しいバージョンをインストールできます）。

既存の Cisco Prime Network Registrar インストールを新しいマシンに移動するには、次の手順を実行します。

**ステップ 1** 古いリージョナルサーバでサーバエージェントを停止します。

```
# systemctl stop nwregregional
```

**ステップ 2** /var/nwreg2/regional/tomcat を除いて、/var/nwreg2/regional/tomcat を tar ファイルにします。最新のバックアップに対してコピーしない場合は、/var/nwreg2/regional/data.bak をスキップすることもできます。

**ステップ 3** tar ファイルを新しいサーバにコピーし、ファイルを同じ場所 (/var/nwreg2/regional) に展開します。/var/nwreg2/regional/tomcat ディレクトリがないことを確認します（存在する場合は削除します）。

(注) ステップ 2 とステップ 3 は、Cisco Prime Network Registrar 11.0 以降に適用されます。以前のリリースについては、そのバージョンのマニュアルを参照してください。

**ステップ 4** /usr/lib/systemd/system/nwregregional.env ファイルを新しいシステムに移動します。

**ステップ 5** 新しいサーバに Cisco Prime Network Registrar（リージョナルクラスタ）をインストールします。詳細については、[Cisco Prime Network Registrar のインストール（1 ページ）](#) を参照してください。

インストールにより、コピーされたデータに基づいてアップグレードが検出されます。この手順では、古いリージョナルサーバからの元のデータが保持されます。

インストール後にカスタム構成の変更（[Web UI のセキュリティ強化](#)で説明されている変更など）を再適用します。

(注) 新しいマシンに Cisco Prime Network Registrar をインストールする場合は、古いリージョンサーバからデータをコピーしたデータディレクトリを選択する必要があります。

**ステップ 6** Cisco Prime Network Registrar の Web UI または CLI を起動します。詳細については、[Cisco Prime Network Registrar の使用](#)を参照してください。

**ステップ 7** スーパーユーザとして新しいリージョナルクラスタの CLI にログインします。

**ステップ 8** ローカルクラスタを一覧表示するには、次のコマンドを使用します。

```
nrcmd-R> cluster listnames
```

**ステップ 9** データとライセンス情報を同期するには、次のコマンドを使用します。

```
nrcmd-R> cluster cluster-name sync
```

## 独自の Web UI アクセス用証明書のインストール

Web UI アクセスに独自の証明書を使用する場合は、次の手順を実行します。

**ステップ 1** **openssl** または **keytool** を使用して、自己署名証明書を含むキーストアファイルを作成します。ユーティリティを使用して、自己署名証明書を定義するか、または外部署名機関から証明書を要求して後でインポートします。

- 自己署名証明書を含むキーストアファイルを作成するには、次のコマンドを実行し、プロンプトに回答します。

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
```

```
Enter keystore password: password
```

```
What is your first and last name? [Unknown]: name
```

```
What is the name of your organizational unit? [Unknown]: org-unit
```

```
What is the name of your organization? [Unknown]: org-name
```

```
What is the name of your City or Locality? [Unknown]: local
```

```
What is the name of your State or Province? [Unknown]: state
```

```
What is the two-letter country code for this unit? [Unknown]: cc
```

```
Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
```

```
Enter key password for <tomcat> (RETURN if same as keystore password):
```

(注) Web UI で弱い暗号を無効にするには、128 ビット SSL を使用する必要があります。詳細については、[Web UI のセキュリティ強化](#)を参照してください。

- 証明書を要求するときに認証局 (CA) に送信する証明書署名要求 (CSR) を作成するには、前のステップのとおりキーストアファイルを作成し、次のコマンドを実行します。

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
```

結果の **certreq.cer** ファイルを CA に送信します。CA から証明書を受信したら、まず CA からチェーン証明書をダウンロードし、次にチェーン証明書と新しい証明書を次のようにキーストアファイルにインポートします。

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
```

```
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

**keytool** ユーティリティの詳細については、Oracle の Java Web サイトにある資料を参照してください。キーストアファイルと **tomcat** の詳細については、Apache Software Foundation の Web サイトにある資料を参照してください。

- openssl** を使用して自己署名証明書を作成するには、次のコマンドを使用します。

```
> openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

Cisco Prime Network Registrar での証明書管理の詳細については、*Cisco Prime Network Registrar 11.0* アドミニストレーションガイドの「証明書の管理 (Certificate Management)」の章を参照してください。

**ステップ 2** 必要に応じて `cnr-priv.conf` ファイル (`/var/nwreg2/{local|regional}/conf/priv`) を編集し、新しいキーストアを指定して、暗号化されたパスワードを指定します。暗号化されたパスワードを生成するには、`install-path/usrbin` ディレクトリにある暗号化スクリプト (`encrypt -s <plain-text password>`) を使用します。

**ステップ 3** Cisco Prime Network Registrar を再起動します。

Cisco Prime Network Registrar を再起動するたびに、キーストアの詳細が Tomcat の設定に適用されます。

## インストールに関するトラブルシューティングを実行

ログディレクトリは、デフォルトで次の場所に設定されます。

- ローカルクラスタ : `/var/nwreg2/local/logs`
- リージョナルクラスタ : `/var/nwreg2/regional/logs`

インストールまたはアップグレードが正常に完了しない場合 :

- 上記のログファイルの内容を確認して、何が失敗したのかを判断します。考えられる失敗の原因の例を次に示します。
  - Java の間違っただバージョンがインストールされている。
  - 使用可能なディスク容量が不足している。
  - アップグレードに一貫性のないデータが存在する。

- 次のコマンドを使用して、サービスのステータスをチェックします。

- ローカルクラスタの場合

```
# systemctl status -l nwreglocal.service
```

- リージョナルクラスタの場合

```
# systemctl status -l nwregregional.service
```

- 次のコマンドを使用して systemd ジャーナルを確認します。

- ローカルクラスタの場合

```
# journalctl -u nwreglocal --since=today
```

- リージョナルクラスタの場合

```
# journalctl -u nwregregional --since=today
```

それ以降で使用される時間間隔を変更できます。詳細については、`man journalctl` コマンドを使用してください。

## ローカルクラスタのライセンスの問題のトラブルシューティング

リージョナルクラスタとローカルクラスタが隔離されたネットワークに配置されている場合、またはファイアウォールによって分離されている場合、またはリージョナルクラスタとローカルクラスタの間の時間のずれが5分を超える場合、ローカルクラスタはリージョナルサーバに登録できない可能性があります。ファイアウォールは、ローカルクラスタからリージョナルクラスタに送信されるローカルクラスタの管理者ログイン情報を検証するために、使用されるリターン接続をブロックすることがあります。

ローカルクラスタをリージョナルクラスタに登録するには、次の手順を実行します。

---

**ステップ 1** サーバに Cisco Prime Network Registrar (ローカルクラスタ) をインストールし、ローカルクラスタの管理ユーザを作成します。詳細については、[Cisco Prime Network Registrarのインストールおよびアップグレード \(1 ページ\)](#) を参照してください。

ローカルクラスタに Cisco Prime Network Registrar をインストールした後に (Web UI または CLI で) 初めてログインしようとする、スーパーユーザーを作成してリージョナルクラスタに登録するように求められます。

**ステップ 2** リージョナルクラスタにログインし、管理者ログイン情報を使用して新しいローカルクラスタをリージョナルクラスタに追加します。詳細については、『*Cisco Prime Network Registrar 11.0* アドミニストレーションガイド』の「ローカルの追加 (Adding Local Clusters)」の項を参照してください。

**ステップ 3** データとライセンス情報を同期するには、[再同期 (Resynchronize)] アイコンをクリックします。

---