Cisco Prime Network Registrar 11.1 インストールガイド

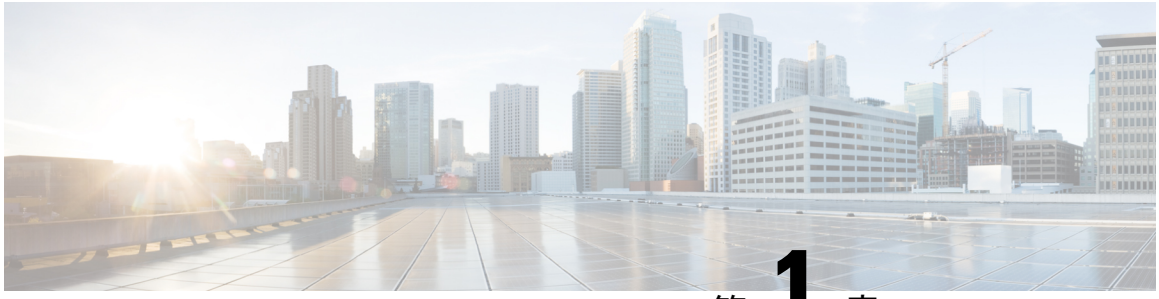
初版：2022 年 7 月 13 日

最終更新：2022 年 11 月 9 日

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
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

インストールの概要

この章は、次の項で構成されています。

概要

このガイドでは、Linux オペレーティングシステムに Cisco Prime Network Registrar 11.1 をインストールする方法について説明します。Cisco Prime Network Registrar の設定と管理に関する重要な情報については、次のマニュアルも参照してください。

- Cisco Prime Network Registrar および の構成と管理の手順については、『Cisco Prime Network Registrar 11.1 Administration Guide』を参照してください。
- CLI（コマンドラインインターフェイス）で使用できるコマンドの詳細については、『Cisco Prime Network Registrar 11.1 CLI Reference Guide』を参照してください。

Cisco Prime Network Registrar について

Cisco Prime Network Registrar は、企業の IP アドレス管理を自動化するネットワークサーバスイートです。アドレス割り当ての信頼性と効率性を向上させる安定したインフラストラクチャを提供します。 次のものが含まれています（下の図を参照）。

- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバ
- ドメイン ネーム システム（DNS）サーバ
- キャッシング ドメイン ネーム システム（CDNS）サーバ
- 簡易ネットワーク管理プロトコル（SNMP）サーバ
- 簡易ファイル転送プロトコル（TFTP）サーバ

これらのサーバは、Cisco Prime Network Registrar の Web ベースのユーザインターフェイス（Web UI）または CLI を使用して制御できます。これらのユーザインターフェイスは、異なるプラットフォームで実行されるサーバクラスタも制御できます。

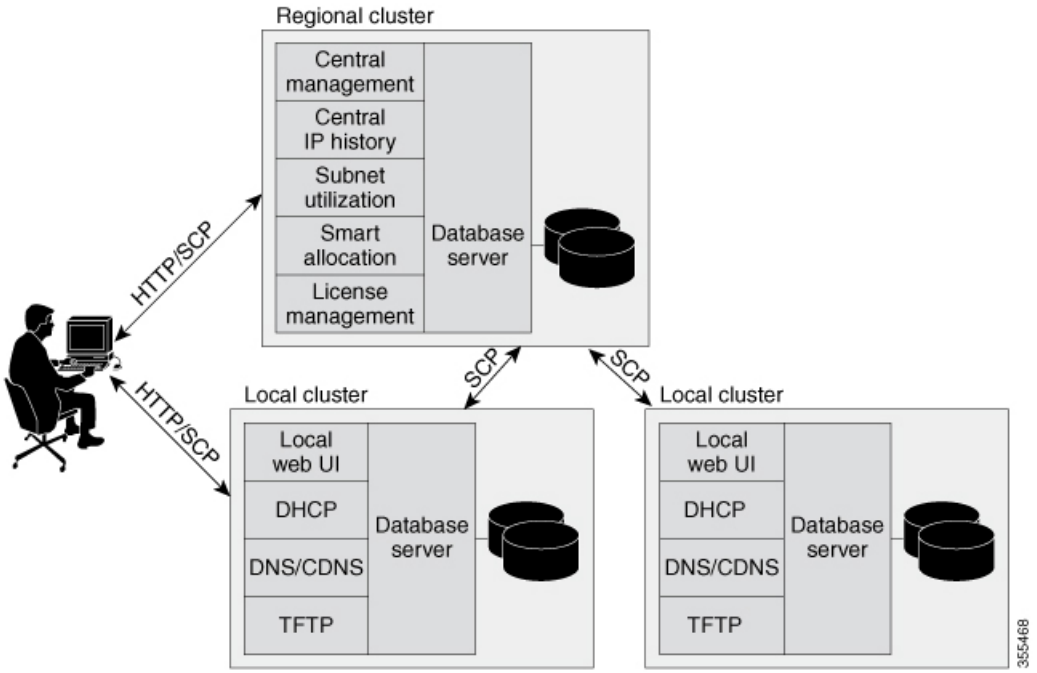
Cisco Prime Network Registrar は、ローカルモードまたはリージョナルモードでインストールできます。

- ローカルモードは、ローカル クラスタ プロトコル サーバの管理に使用されます。
- リージョナルモードは、中央管理モデルを介して複数のローカルクラスタを管理するために使用されます。

リージョナルクラスタはライセンスに必要であり、ローカルクラスタサーバとそのアドレス空間を一元管理するために使用できます。リージョナルの管理者は、次の操作を実行できます。

- Cisco Prime Network Registrar のライセンスを管理します。インストールには、ライセンス管理のために少なくとも 1 つのリージョナルクラスタが必要です。
- ローカル DNS と DHCP サーバとの間で構成データをプッシュおよびプルします。
- ローカルクラスタから DHCP 使用率と IP リース履歴データを取得します。

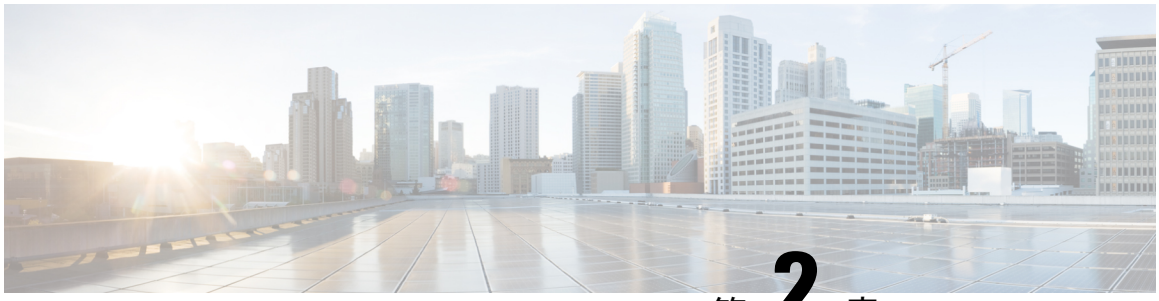
図 *1 : Cisco Prime Network Registrar* ユーザインターフェイスとサーバクラスタ



センシティブデータの露出

Cisco Prime Network Registrar が処理するデータのほとんどは、暗号化されていないネットワーク（特にクライアントデバイスへの最後のホップ）を介して送信され、その性質上、ネットワーク上の他のデバイス（ローカルまたはインターネット経由）で共有および使用できるように設計されています。

Cisco Prime Network Registrar のデータ（またはその一部）は機密性が高いと考えられる場合は、Linux のディスクベースの暗号化サポートを使用してディスクを暗号化することを強く推奨します。これは、制御された領域をディスクが離れた後（つまり、寿命に達したか、適切に消去できないまたは盗まれた場合）、データを保護するのに役立ちます。また、バックアップを保護する方法、またはデータを移動できる他の場所も考慮する必要があります。



第 2 章

設定オプション

Cisco Prime Network Registrar DHCP、権威 DNS、およびキャッシング DNS コンポーネントは、リージョナルサーバからライセンスおよび管理されます。リージョナルサーバが必要で、ローカルクラスタ内のすべてのサービスは、リージョナルクラスタを介してライセンスされます。ライセンスファイルを要求するのはリージョナルのインストールのみで、リージョナルサーバのみが新しいライセンスファイルを受け入れます。次に、リージョナルサーバは、使用可能なライセンスに基づいて個々のローカルクラスタを承認できます。

この章で示す構成例は、次の項で説明する一般的な使用例に基づいています。

DHCP と DNS の混合シナリオ

さまざまな数のマシンで DHCP と DNS の混合構成用に Cisco Prime Network Registrar をセットアップできます。

1 台のマシンの混合コンフィギュレーション

1 台のマシンで DHCP サーバと権威 DNS サーバの両方を設定します。最初にサーバをプライマリとして有効にし、TFTP サーバと SNMP トラップを無効にします。次に、少なくとも 1 つの正引きゾーンおよび対応する逆引きゾーン、および少なくとも 1 つの範囲を設定します。

1 台のマシンで DHCP サーバとキャッシング DNS サーバの両方を設定します。最初にサーバをプライマリとして有効にし、TFTP サーバと SNMP トラップを無効にします。次に、フォワーダと例外リストを設定できます。

2 台のマシンの混合コンフィギュレーション

2 台のマシンの混合 DHCP コンフィギュレーションには、いくつかの選択肢があります。

- 1 台のマシンをプライマリ DHCP サーバおよび権威 DNS サーバとして設定し、2 台目のマシンをセカンダリ権威 DNS サーバとして設定します。次に、最初のマシンでゾーン配信と DNS アクセス コントロールを設定し、オプションで 2 台目のマシンにアクセス コントロールを設定します。
- 1 台のマシンを DHCP および権威 DNS メイン サーバとして設定し、2 台目のマシンを DHCP および権威 DNS バックアップ サーバとして設定します。バックアップ マシンで最小限の設定（パスワードの変更、DHCP および権威 DNS のイネーブル化、およびパートナー バックアップ ロールの選択）を行います。メイン マシンでサーバ ペアを作成し、バックアップ マシンとの同期をスケジュールして、設定を作成します。
- 1 台のマシンを DHCP サーバとして設定し、2 台目のマシンを権威 DNS プライマリとして設定します。そして次に、一方のマシンに DNS 更新を設定してから構成をもう一方のマシンにプッシュします。
- DHCP サーバおよび権威 DNS サーバを持つ 1 台のマシンを設定し、2 台目のマシンをフォワーダとして権威 DNS サーバを持つキャッシング DNS サーバとして設定します。

3 台のマシンの混合コンフィギュレーション

3 台のマシンの混合コンフィギュレーションには、いくつかの選択肢があります。

- 1 台のマシンを DHCP サーバ、2 台目のマシンを権威 DNS プライマリ、3 台目のマシンを権威 DNS セカンダリとして設定します。オプションで、マシンに再度アクセスして、DHCP メインを権威 DNS バックアップ、権威 DNS メインを DHCP バックアップにします。
- 1 台のマシンを DHCP フェールオーバーおよび権威 DNS高可用性（HA）メイン サーバ、2 台目のマシンを DHCP フェールオーバーおよび権威 DNS HA バックアップ サーバ、3 台目のマシンを権威 DNS セカンダリサーバとして設定します。
- 1 台のマシンを DHCP サーバ、2 台目のマシンを権威 DNS サーバ、3 台目のマシンをフォワーダとして権威 DNS を持つキャッシング DNS として設定します。
- 1 台のマシンを DHCP プライマリ サーバおよび権威 DNS プライマリ、2 台目のマシンを DHCP セカンダリおよび権威 DNS セカンダリサーバ、3 台目のマシンをフォワーダとして最初のマシンのプライマリ権威 DNS を持つキャッシング DNS として設定します。

4 台のマシンの混合コンフィギュレーション

4 台のマシンの混合構成は、次のようにすることができます。

- DHCP と権威 DNS のメインとバックアップのペア。最初のマシンを DHCP メイン、2 台目のマシンを DHCP バックアップ、3 台目のマシンを DNS 更新が設定された権威 DNS メイン、4 台目のマシンを権威 DNS バックアップとして設定します。

- 3 台のマシンのシナリオに追加。最初のマシンを DHCP メイン、2 台目のマシンを権威 DNS メイン、3 台目のマシンを DHCP および権威 DNS バックアップ、4 台目のマシンを権威 DNS セカンダリとして設定します。
- 最初のマシンを DHCP メイン、2 台目のマシンを DHCP バックアップ、3 台目のマシンを権威 DNS、4 台目のマシンをフォワーダとして権威 DNS を持つキャッシング DNS として設定します。

DHCP のみのシナリオ

DHCP のみの構成は、1 台または 2 台のマシンで可能です。

1 台のマシンの DHCP 設定

最初は DHCP のみを設定し、サービスクラスとフェールオーバーオプションをスキップします。再度、設定にアクセスして、サービスクラスとポリシーのオプションを有効にします。

2 台のマシンの DHCP 設定

最初のマシンを DHCP メイン、2 台目のマシンを最小限のバックアップ設定（パスワードの変更、DHCP のイネーブル化、およびバックアップ ロールの選択）でバックアップとして設定し、最初のマシンにフェールオーバー ロード バランシングを設定して、オプションでフェールオーバー同期タスクをスケジュールします。

DNS のみのシナリオ

DNS のみの構成は、1 台、2 台、または 3 台のマシンで可能です。

1 台のマシンの DNS 設定

最初に DNS を権威プライマリ、権威セカンダリ、またはキャッシング サーバとして設定します。

2 台のマシンの DNS 設定

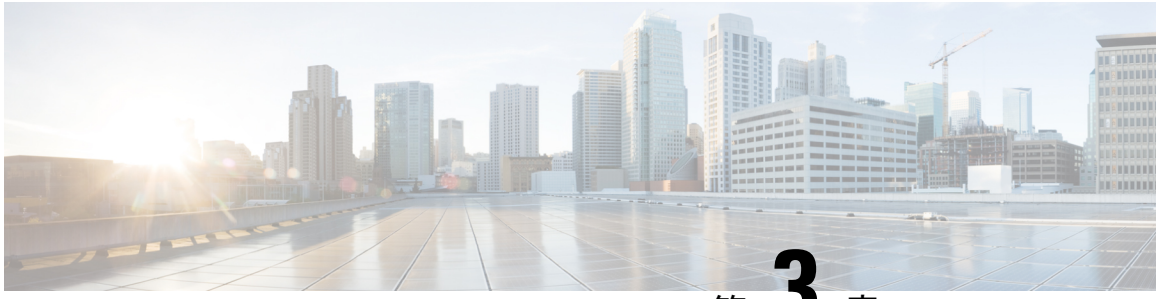
最初のマシンを権威 DNS プライマリ、2 台目のマシンをセカンダリとして設定するか、最初のマシンをメインプライマリ、2 台目のマシンをバックアッププライマリとして設定します。

最初のマシンを権威 DNS、2 台目のマシンをキャッシング DNS として設定します。

3 台のマシンの DNS 設定

最初のマシンを権威 DNS メインプライマリ、2 台目のマシンをバックアッププライマリ、3 台目のマシンをセカンダリサーバとして設定します。

最初のマシンを権威 DNS プライマリ、2 台目のマシンをセカンダリ、3 台目のマシンをキャッシング DNS として設定します。



第 3 章

インストール要件

この章は、次の項で構成されています。

システム要件

Cisco Prime Network Registrar 11.1 ソフトウェアをインストールする前に、システム要件を確認してください。

- Java：システムに Java 開発キット（JDK）11 がインストールされていることを確認します。

（注） すべての 64 ビット Java 11 は Cisco Prime Network Registrar 11.1 でサポートされ、Java 11 OpenJDK パッケージでテストされています。

- オペレーティングシステム：Cisco Prime Network Registrar マシンは、Linux オペレーティングシステムで実行してください（以下の「サーバー要件」の表を参照）。Cisco Prime Network Registrar には 64 ビットのオペレーティング システムが必要です。
- ユーザーインターフェイス：Cisco Prime Network Registrar には現在、Web UI と CLI の 2 つのユーザーインターフェイスが含まれています。
  - Web UI は Microsoft Edge 100、Mozilla Firefox 99、および Google Chrome 100 でテストされています。Internet Explorer はサポートされていません。
  - CLI は Linux のコマンドウィンドウで実行します。

ヒント　ローカルクラスタとリージョナルクラスタの時間差を避けるために、ネットワークタイムサービスを構成に含めます。このメソッドにより、リージョナルサーバの集約データが一貫して表示されます。リージョナルクラスタとローカルクラスタの間の最大許容時間のずれは 5 分です。時間のずれが 5 分を超えると、インストールプロセスでサーバをリージョナルに正しく登録できなくなります。この場合は、リージョナルクラスタでパスワードの設定解除および設定を行い、再度同期します。

表 *1 : Cisco Prime Network Registrar Server* の要件

コンポーネント	要件
OS バージョン[1]	Red Hat Enterprise Linux ES/CentOS 7.3+ または RHEL 8.x/AlmaLinux 8.6 64-bit **注**：このリリースでテストされた最新レベルは RHEL 8.6 です。
最小ディスク領域	200 GB 最適なパフォーマンスを得るために、シスコでは SSD ドライブの使用を推奨しています。
最小メモリ	16 GB
最小 CPU[2]	4 個の CPU

[1] Cisco Prime Network Registrar 11.1 は、64 ビットのオペレーティングシステムでのみサポートされます。
[2] CPU が高速でメモリが多いほど、一般的にピーク時のパフォーマンスが高くなります。

（注）　Cisco Prime Network Registrar 11.1 仮想アプライアンスに使用されるオペレーティングシステムのバージョンは AlmaLinux 8.6 です。

（注）　Cisco Prime Network Registrar 10.1 は、Windows をサポートする最新のリリースです。また、重大度 1 の問題を除き、Windows には 9.x または 10 x リリース（パッチまたはメンテナンスを含む）がありません。

（注）　展開予定のクラスタタイプに応じて、「キャパシティとパフォーマンスに関するガイドライン」の付録を参照してください。

重要 これらのシステム要件を最小限のガイドラインとして扱います。導入をモニターし、実際の使用レベルに基づいて調整することをお勧めします。

Cisco Network Registrar は、Red Hat Enterprise Linux ES 8.6、AlmaLinux 8.6 および CentOS 7.3+ に対してテスト済みです。ただし、エンドユーザーは、OS 関連のバグ修正とセキュリティパッチを使用してOSを最新の状態に保つために、パッチとメンテナンスリリースを適用することが予想されます。シスコでは、同じOSメジャーバージョン内のこれらのパッチ/メンテナンスアップデートが問題を引き起こすことは想定していませんが、実稼働サーバーに適用する前に、すべてのアップデートをラボテストすることを強く推奨します。

Linux OS のシステム要件

Red Hat Enterprise Linux、AlmaLinux または CentOS に Cisco Prime Network Registrar をインストールするには、JDK の他に次の x86_64（64 ビット）パッケージをインストールする必要があります。**yum** または **dnf** コマンドを使用して Cisco Prime Network Registrar をインストールする場合、これらのパッケージは必要に応じてインストールプロセスの一部としてインストールされます。**rpm** コマンドを使用してCisco Prime Network Registrar をインストールする場合は、これらのパッケージを個別にインストールする必要があります。

表 *2:* インストールするパッケージ

パッケージ名	パッケージのバージョン	
	RHEL/CentOS 7.3 以降の場合	**RHEL 8.x/AlmaLinux 8.6 の場合**
glibc	2.17 以降	2.28 以降
krb5-libs	1.15.1 以降	1.17 以降
ldns	（Cisco Prime Network Registrar に含まれる）	1.7.0 以降
libcurl（OpenSSL で構築）	7.29.0 以降	7.61.1 以降
libevent	（Cisco Prime Network Registrar に含まれる）	2.1.8 以降
libgcc	4.8.5 以降	8.3.1 以降
libicu	（Cisco Prime Network Registrar に含まれる）	60.3 以降
libstdc++	4.8.5 以降	8.3.1 以降
libxml2	2.9.1 以降	2.9.7 以降

パッケージ名	パッケージのバージョン	
	RHEL/CentOS 7.3 以降の場合	**RHEL 8.x/AlmaLinux 8.6 の場合**
net-snmp-libs	5.7.2 以降	5.8 以降
openldap	2.4.44 以降	2.4.46 以降
openssl-libs	1.0.2k 以降	1.1.1c 以降
tcl	8.5.13 以降	8.6.8 以降
zlib	1.2.7 以降	1.2.11 以降
libnghttp2	1.33.0 以降	1.33.0 以降

RPM をダウンロードしている場合は、Linux システムで次のコマンドを発行して必要なパッケージを確認することもできます。

rpm -qpR *rpm_package_file*

インストーラによって、インストールプロセスを開始する前に欠落している可能性があるパッケージを報告します。

（注） ご使用の Linux システムの種類を確認するには、次のコマンドを使用します。

```
more /etc/redhat-release
```

推奨事項

Cisco Prime Network Registrar を仮想マシンに展開する場合は、次の推奨事項を確認してください。

- HA DNS または DHCP フェールオーバーパートナーを同じ物理サーバ（別の VM）に展開しないでください。これでは、サーバがダウンしたときに高可用性が得られません。理想的には、高可用性/フェールオーバーパートナーは、一方に障害（ハードウェア、電源、またはネットワーキングの障害が原因）が発生しても、もう一方に障害を起こさないように、十分に「分離」する必要があります。
- 複数の Cisco Prime Network Registrar VM を同じ物理サーバー（またはディスクリソースの共通セットによって提供されるサーバー）に展開する場合は、夜間の自動シャドウバックアップをずらす必要があります（デフォルトでは、サーバーの現地時間で 23 時 45 分に発生します）。この時間を変更する方法については、Cisco Prime Network Registrar 11.1 Administration Guide の「Setting Automatic Backup Time」の項を参照してください。

（注） ラボ環境では、上記の推奨事項に従わなくてもかまいません。ただし、実稼働環境では従う必要があります。

インストールモード

ローカルクラスタおよびリージョナルクラスタに存在するインストールモードは、新規インストールおよび以前のバージョンからのアップグレードです。これらのインストールおよびアップグレードは、**yum install**、**rpm -i**、または **dnf install** コマンドを使用して実行されます。

（注） **rpm -i** コマンドを使用して Cisco Prime Network Registrar をインストールする場合は、状況に応じて依存関係を手動でインストールする必要があります。

ライセンスファイル

Cisco Prime Network Registrar 11.1 は、スマートライセンスと従来のライセンスの両方をサポートしています。

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコ ライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

従来のライセンス（FLEXlm）の場合は、バージョンの永久ライセンスを購入し、Cisco Prime Network Registrar サーバーが新しいメジャーバージョンにアップグレードされるまで使用します。スマートライセンスの場合、ライセンスは個々のシスコ製品にインストールされず、顧客固有のスマートアカウントの Cisco Smart Software Manager（CSSM）または CSSM On-Prem（Satellite）と呼ばれる一元化されたシステムで保持されます。

ライセンスに関する詳細は、『Cisco Prime Network Registrar 11.1 Administration Guide』の「ライセンス」の項を参照してください。

Cisco Prime Network Registrar 11.1 ライセンスファイルには、ライセンスの永続部分およびサブスクリプション部分に対応する2組のライセンスが含まれています。永続ライセンスは、8.x、9.x、および10.xバージョンで発行されたライセンスに似ています。Cisco Prime Network Registrar 11.1の場合、ライセンスは必要なサービスに従って実行されます。ライセンスの永続部分は、Cisco Prime Network Registrar 9.0 以降用に確立されたマッピングを引き続き使用します。

使用可能なライセンスのタイプは次のとおりです。

スマートライセンス

- PNR-System：CCMサービスのライセンス。Cisco Prime Network Registrarを実行する場合、このライセンスは必須。
- PNR-DHCP：DHCP/TFTPサービス、およびリースの初期数（オプション）のライセンス。
- PNR-DNS：権威 DNS サービス、および RR の初期数（オプション）のライセンス。
- PNR-Caching DNS：キャッシング DNS サービス、およびサーバーの初期数（オプション）のライセンス。
- PNR-PLR：すべてのサービスの永続ライセンス予約のライセンス。
- PNR-DHCP Container：コンテナの DHCP サービスのライセンス。
- PNR-DNS Container：コンテナの権威 DNS サービスのライセンス。
- PNR-Caching DNS Container：コンテナのキャッシング DNS サービスのライセンス。

従来のライセンス

- base-system：CCMサービスのライセンス。Cisco Prime Network Registrarを実行する場合、このライセンスは必須。
- base-dhcp：DHCP/TFTP サービスのライセンス、およびリースの初期数（オプション）。
- base-dns：権威 DNS サービス、および RR の初期数（オプション）のライセンス。
- base-cdns：ライセンスキャッシング DNS サービス、およびサーバの初期数（オプション）。
- count-dhcp：アクティブリースの増分数のライセンス。
- count-dns：RR の増分数のライセンス。
- count-cdns：キャッシング サーバ インスタンスの増分数のライセンス。

永続的な Cisco Prime Network Registrar 11.x ライセンスごとに、対応するサブスクリプションライセンスが発行されます。各サブスクリプションライセンスの期限日は、サブスクリプション期間中に設定されます。

使用可能なライセンスのタイプは次のとおりです。

スマートライセンス

- PNR-System SIA：CCM サービスのライセンス。Cisco Prime Network Registrar を実行する場合、このライセンスは必須。
- PNR-DHCP SIA：DHCP/TFTP サービス、およびリースの初期数（オプション）のライセンス。
- PNR-DNS SIA：権威 DNS サービス、および RR の初期数（オプション）のライセンス。
- PNR-Caching DNS SIA：キャッシング DNS サービス、およびサーバーの初期数（オプション）のライセンス。
- PNR-DHCP Container SIA：コンテナの DHCP サービスのライセンス。
- PNR-DNS Container SIA：コンテナの権威 DNS サービスのライセンス。
- PNR-Caching DNS Container SIA：コンテナのキャッシング DNS サービスのライセンス。

従来のライセンス

- sub-system：CCM サービスのライセンス。
- sub-dhcp：DHCP サービスのライセンス。
- sub-count-dhcp：アクティブリースの増分数のライセンス。
- sub-dns—Licenses：権威 DNS サービスのライセンス。
- sub-count-dns：RR の増分数のライセンス。
- sub-cdns：キャッシング DNS サービスのライセンス。

Cisco Prime Network Registrar によって提供されるさまざまなサービスは、次のようにさまざまなライセンスタイプに関連付けられます。

- CCM サービス：基本システム、PNR システム
- DHCP サービス：base-dhcp、count-dhcp、PNR-DHCP
- 権威 DNS サービス：base-dns、count-dns、PNR-DNS
- キャッシング DNS サービス：base-cdns、count-cdns、PNR-Caching DNS

（注） Cisco Prime Network Registrar 10.x 以前のライセンスは Cisco Prime Network Registrar 11.x では無効です。Cisco Prime Network Registrar 11.x 用の新しいライセンスが必要です。11.x のリージョナルに 10.x の CDNS クラスタが含まれている場合は、10.x の CDNS ライセンスをリージョナルサーバーに追加する必要があります（10.x の CDNS クラスタが 10.x のライセンスを使用し、11.x の CDNS クラスタが 11.x のライセンスを使用します）。

（注） ファイルからロードされた個々のライセンスを削除することはできません。必要に応じて、アップグレード後に古いバージョンの DNS および DHCP ライセンスを削除することができます。サーバがアップグレードされていない場合は、古いバージョンの CDNS ライセンスを保持する必要があります。

（注） サブスクリプション ライセンスを提供する場合は、将来のリリースへのアップグレードを保証するためにインストールする必要があります。

（注） このサービスを有効にするには、サーバの基本ライセンスが少なくとも 1 つ必要です。

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、リージョン サーバをインストールしてから、リージョン サーバにすべてのライセンスをロードする必要があります。ローカル クラスタをインストールすると、リージョンを登録してライセンスを取得します。

リージョナルをインストールすると、ライセンスファイルを提供するように求められます。インストール中にアクセスできる場所とファイルであれば、ライセンスファイルを任意の場所に保存できます。

ライセンスの使用率は、カウントされたすべてのサービス（DHCP、DNS、および CDNS）について、Cisco Prime Network Registrar システム内のすべてのローカルクラスタから統計情報を取得することによって計算されます。リージョナル CCM サーバは、所定の期間、ライセンス使用率履歴を保持します。

使用率は、さまざまなサービスについて次のように計算されます。

- **DHCP サービス**：「アクティブな」DHCP リースの合計数（v4 や v6 を含む）

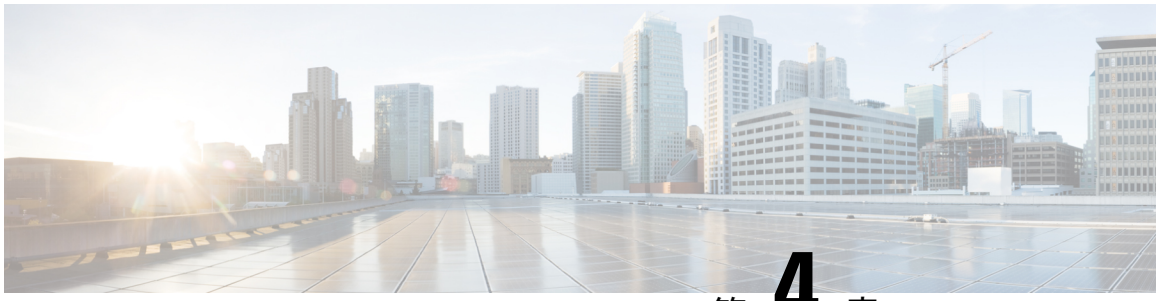
  アクティブなリースには、クライアントが使用中の（したがって、別のクライアントが使用できない）リースの数が含まれます。またこれには、移行中の予約とリースも含まれます。

- **認証 DNS サービス**：DNS リソースレコードの総数（すべての RR タイプ）
- **キャッシング DNS サービス**：Cisco Prime Network Registrar システムで実行されているキャッシング DNS サーバの合計数

各ローカルクラスタのサービスは、ライセンスが存在するサービスに基づいて制限されます。

DHCP フェールオーバーを設定すると、単純なフェールオーバーだけが動作し、サポートされます（『*Cisco Prime Network Registrar 11.1 DHCP* ユーザーガイド』の「Configuring DHCP Failover」の章の「Failover Scenarios」を参照）。

Cisco Prime Network Registrar のライセンスファイルの取得については、Cisco Prime Network Registrar ライセンスファイルの取得 （21 ページ） を参照してください。



第 4 章

インストールの準備

この章では、Cisco Prime Network Registrar をインストールする前に実行する必要があるタスクについて説明します。

インストールチェックリスト

この項では、Cisco Prime Network Registrar をインストールするために従う必要のある手順について説明します。

インストールを開始またはアップグレードする前に、以下のチェックリストを参照して、準備が整っていることを確認します。

表 *3:* インストールチェックリスト

タスク	チェック
Cisco Prime Network Registrar 11.1 をサポートするための最小要件をオペレーティングシステムが満たしていますか。（システム要件 （9 ページ）を参照）	☐
ハードウェアが最小要件を満たしていますか。（システム要件 （9 ページ）を参照）	☐
必要に応じて、Cisco Prime Network Registrar ディレクトリとサブディレクトリをウイルススキャンから除外しましたか。（バックアップソフトウェアとウイルススキャンのガイドライン （23 ページ）を参照）	☐

タスク	チェック
適切なソフトウェアライセンスがありますか。（ライセンスファイル （13 ページ）を参照）	☐
ソフトウェアのインストールに必要な管理権限がありますか。	☐
ターゲットインストールサーバに十分なディスク容量がありますか。	☐
これは新規インストールですか、アップグレードですか。	☐
これは、リージョナルクラスタ、ローカルクラスタ、クライアント専用のうち、どのインストールタイプですか。	☐
64 ビット JDK がシステムにインストールされていますか。その場合、どこにインストールされていますか。	☐
以前のバージョンの Cisco Prime Network Registrar からアップグレードしていますか。その場合は次のことを確認します。	☐
• アクティブなユーザ インターフェイス セッションはありますか。	☐
• データベースはバックアップされていますか。	☐
• サポートされているバージョン（Cisco Prime Network Registrar 8.3 以降）からアップグレードしていますか。	☐
Linux に必要なパッケージがインストールされていますか。（Linux OS のシステム要件 （11 ページ）を参照）	☐
Cisco Prime Network Registrar イメージの署名は検証されていますか。（イメージ署名 （22 ページ） を参照）。	☐

はじめる前に

サポートされているオペレーティングシステムを実行しており、ご使用の環境が他の現行システムの要件をすべて満たしていることを確認します（システム要件 （9 ページ）を参照）。

オペレーティングシステムをアップグレードするには、次の手順を実行します。

1. アップグレードを実行する前に、既存のデータベースの一貫性を保つために、現在インストールされている Cisco Prime Network Registrar リリースを使用して、進行中の構成変更を完了します。
2. データベースをバックアップします。インストールプログラムは、以前のインストールから構成データを検出しようとし、データをアップグレードします。
3. オペレーティングシステムをアップグレードし、前提条件のソフトウェアをインストールします。

（注） このドキュメントでは、*install-path* を使用する場合、Cisco Prime Network Registrar がインストールされているパスを示します（つまり、/opt/nwreg2/{local | regional}）。

Cisco Prime Network Registrar ライセンスファイルの取得

Cisco Prime Network Registrar 11.1 は、スマートライセンスと従来のライセンスの両方をサポートしています。ただし、ハイブリッドモデルはサポートされていません。つまり、一度に使用できるのは、どちらか1つのライセンスタイプです。デフォルトでは、スマートライセンスは Cisco Prime Network Registrarで有効になっています。従来のライセンスを使用する場合は、まずスマートライセンスを無効にする必要があります（Cisco Prime Network Registrar 11.1 Administration Guideの「スマートライセンスの無効化」の項を参照してください）。

スマートライセンス

スマートライセンス付きの Cisco Prime Network Registrar 11.1 を購入すると、ライセンスは CSSM（またはサテライト）のスマートアカウントに登録されます。ライセンスを使用するには、Web UI または CLI を使用して CSSM（またはサテライト）に Cisco Prime Network Registrar を登録する必要があります。Cisco Prime Network Registrar 11.1 Administration Guideの「Registering Cisco Prime Network Registrar with the CSSM」の項を参照してください。

シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

従来のライセンス

Cisco Prime Network Registrar 11.1 を購入すると、ソフトウェアの登録後に、シスコからメールの添付で FLEXlm ライセンスファイルが届きます。

ソフトウェアをインストールする前に、リージョナルクラスタのインストール中にアクセスできる場所にライセンスファイルをコピーする必要があります。インストールプロセスでは、ライセンスファイルの場所を尋ねられます。

ライセンスファイルを取得するには、次の手順を実行します。

1. ソフトウェアに同梱されているソフトウェアライセンス権利証明書のドキュメントをお読みください。
2. 証明書に記載されている製品認証キー（PAK）番号をメモします。
3. 証明書に記載されている Web サイトのいずれかにログインし、登録手順に従います。登録プロセスには PAK 番号が必要です。

   登録後 1 時間以内に、電子メールでライセンスファイルを受け取る必要があります。

一般的なライセンスファイルは次のようになります。

```
INCREMENT base-system cisco 11.1 permanent uncounted \

 VENDOR_STRING=<Count>1</Count> HOSTID=ANY \
```

```
NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \
<PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

イメージ署名

Cisco Prime Network Registrar11.0 以降、すべての Cisco Prime Network Registrar イメージが署名されます。RPM イメージには暗黙的な署名がありますが、非 RPM イメージには個別の対応する署名ファイルがあります。Cisco Prime Network Registrar をインストールする前に署名を確認することをお勧めします。

RPM イメージの署名を確認するには、次の手順を実行します。

1. 次のコマンドを使用して、RPG に GPG 公開キー（**CPNR11-rel.gpg**）をインポートします。GPG 公開キーを RPM にインポートしないと、インストール中に警告メッセージが表示されます。

   ```
   # rpm --import CPNR11-rel.gpg
   ```

2. 次のコマンドを実行します。

   ```
   # rpm -K file.rpm
   file.rpm: rsa sha1 (md5) pgp md5 OK
   ```

   意味：パッケージが署名され、正しい GPG キーがインポートされます

   上記のコマンドの出力は、実際にはパッケージファイルには 3 つの異なる機能があり、-K オプション（詳細レベルでは -Kv オプションを使用）によってチェックされることを示しています。

   - サイズメッセージは、パッケージ化されたファイルサイズが変更されていないことを示します。
   - PGP メッセージは、パッケージファイルに含まれるデジタル署名がパッケージファイルの内容の有効な署名であり、パッケージに最初に署名した組織によって生成されたことを示します。
   - MD5 メッセージは、パッケージの作成時に計算されたチェックサムがパッケージファイルに含まれており、検証時に RPM によって計算されたチェックサムと一致することを示します。2 つのチェックサムが一致しているため、パッケージが変更された可能性は低くなります。

   [OK] は、各テストが成功したことを意味します。

   rpm –K コマンドのその他の出力は次のとおりです。

   - ```
     # rpm -K file.rpm
     file.rpm: size md5 OK
     ```

     意味：パッケージが署名されていません。

   - ```
     # rpm -K file.rpm
     file.rpm: size (PGP) md5 OK (MISSING KEYS)
     ```

     意味：公開キーが間違っています。

- `# rpm -K file.rpm`
  `file.rpm:  size PGP MD5 NOT OK`

  意味：RPM ファイルが変更または改ざんされています。

- `# rpm -K file.rpm`
  `file.rpm:  RSA sha1 ((MD5) PGP) md5 NOT OK (MISSING KEY)`

  意味：パッケージは署名されていますが、GPG キーがインポートされません。

非 RPM イメージの署名検証プログラムを実行するには、次の手順を実行します。

1. イメージと同じ場所から検証ファイル（**cpnr_image_verification.gtar.gz**）をダウンロードします。このファイルには、公開証明書、署名検証スクリプト、および README ファイルが含まれています。
2. 次のコマンドを使用して、署名検証スクリプトを実行します。

   ./cisco_x509_verify_release.py3 -e CNR_REL_KEY-CCO_RELEASE.pem -i *image* **-s** *signature* **-v dgst -sha512**

   次に例を示します。

   ```
   # ./cisco_x509_verify_release.py3 -e CNR_REL_KEY-CCO_RELEASE.pem -i
   cpnr-local-11.1-1.el8.x86_64_rhel_docker.tar.gz -s
   cpnr-local-11.1-1.el8.x86_64_rhel_docker.tar.gz.signature -v dgst -sha512
   ```

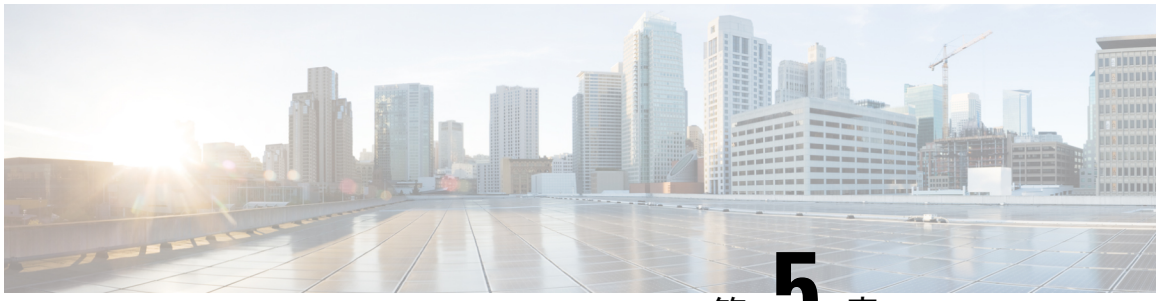
他のプロトコルサーバの実行

Cisco Prime Network Registrar DNS、CDNS、DHCP、または TFTP サーバを、他の DNS、DHCP、または TFTP サーバと同時に実行することはできません。サーバーの起動時にポートの競合がある場合、サーバーは問題をログに記録し、正常に機能しなくなります。

プロトコルサーバを無効にして、システムの再起動後に Cisco Prime Network Registrar サーバが自動的に起動しないようにするには、CLI で **server** {**dns** | **cdns** | **dhcp** | **tftp**} **disable start-on-reboot** コマンドを使用します。

バックアップソフトウェアとウイルススキャンのガイドライン

システムで自動バックアップまたはウイルススキャンソフトウェアを有効にしている場合は、Cisco Prime Network Registrar ディレクトリとそのサブディレクトリをスキャン対象から除外します。除外されていない場合、ファイルロックの問題によってデータベースが破損したり、Cisco Prime Network Registrar プロセスで使用できなくなったりする可能性があります。デフォルトの場所にインストールする場合は、/var/nwreg2 ディレクトリとそのサブディレクトリを除外します。



第 5 章

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

11.0 以降のリリースでは、インストール時に設定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 （40 ページ）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 11.1 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：Cisco Prime Network Registrar は常にルートとして実行されますが、権限は制限されます。
- 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 11.1 では、次の RPM キットが使用可能です。

表 *4 : RPM* キット

	RHEL/CentOS 7.3 以降	**RHEL 8.x/AlmaLinux 8.6**
リージョナルクラスタ	cpnr-regional-11.1.x-1.el7*.x86_64.rpm	cpnr-regional-11.1.x-1.el8*.x86_64.rpm
ローカルクラスタ	cpnr-local-11.1.x-1.el7*.x86_64.rpm	cpnr-local-11.1.x-1.el8*.x86_64.rpm
クライアントのみ	cpnr-client-11.1.x-1.el7*.x86_64.rpm	cpnr-client-11.1.x-1.el8*.x86_64.rpm
キット名の × は、Cisco Prime Network Registrar マイナーバージョンを示します。 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。		

- 最初のログイン時にスーパーユーザー管理者を作成します（Cisco Prime Network Registrar の使用 （40 ページ） を参照）。

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 11.1 にアップグレードするには、Cisco Prime Network Registrar のアップグレード（30 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、AlmaLinux および CentOS 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 11.1 Administration Guide』の「DNS Performance and Firewall Connection Tracking」の項を参照してください。

ステップ 2 OpenJDK 11 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-11-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 11.1 で使用可能な RPM キットのリストについては、上記の 表 4 : RPM キット を参照してください。

Cisco Prime Network Registrar 11.1 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 4 : 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 4 : RPM キット （26 ページ）に記載されている RPM キット名です。

RHEL/CentOS 7.3 以降のキットの名前には「el7*」が、RHEL 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 7.3.x 以降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-11.1-1.el7_9.x86_64.rpm
```

または

```
# rpm -i cpnr-regional-11.1-1.el7_9.x86_64.rpm
```

または

```
# dnf install cpnr-regional-11.1-1.el7_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 （35 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 （40 ページ）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 11.1 は 9.0 以降からの直接アップグレードをサポートします。

Cisco Prime Network Registrar 11.1 は Red Hat/CentOS 7.3 以降、または RHEL 8.x/AlmaLinux 8.6 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もあります）。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す。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 11.1 Administration Guide』の「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 11.1 Administration Guide』の「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 から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。

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 11.1 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/nrweg2/{local | regional}/conf/cert（およびその内容）は /var/nrweg2/{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 11.1 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 （43 ページ） 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 以降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 以降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 11.1 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 （9 ページ）を参照）。

ステップ 2 Cisco Prime Network Registrar のアンインストール （45 ページ） 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 などを保持します）。

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 11.1 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 （25 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 （40 ページ） 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 （32 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できる必要があります。それ以外の方法で進めようとすると、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 （45 ページ）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 Installation Guide』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 （9 ページ）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 新しいサーバーに 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 （77 ページ）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/HA DNS 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ーにコピーし、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 （25 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 （77 ページ）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 （40 ページ）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、プロンプトに応答します。

```
> 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 （77 ページ）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に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 11.1 Administration Guide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。

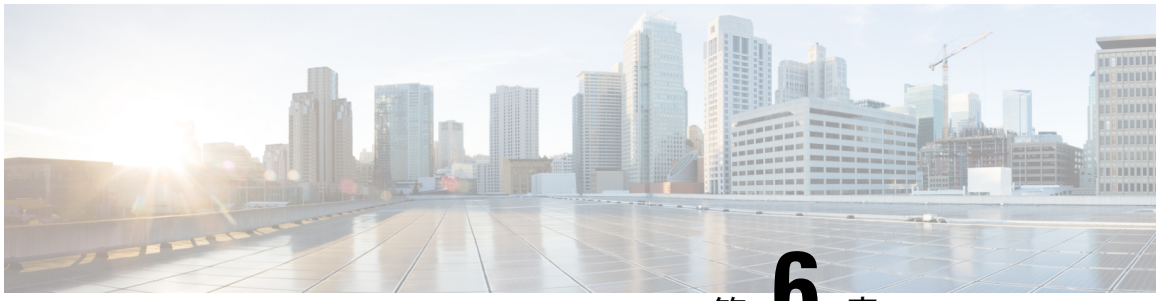
ローカルクラスタをリージョナルクラスタに登録するには、次の手順を実行します。

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（25 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と、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 11.1 Administration Guide』の「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。



第 6 章

次のステップ

この章は、次の項で構成されています。

Cisco Prime Network Registrar の設定

Cisco Prime Network Registrar のインストール後、次のタスクを実行できます。

- Cisco Prime Network Registrar の概要：『Cisco Prime Network Registrar 11.1 Quick Start Guide』を参照してください。
- DHCP アドレス、DHCP フェールオーバー、および DNS 更新のセットアップ：『Cisco Prime Network Registrar 11.1 DHCP User Guide』を参照してください。
- 権威 DNS サービスとキャッシング DNS サービスのセットアップ：『Cisco Prime Network Registrar 11.1 Caching and Authoritative DNS User Guide』を参照してください。
- ローカルとリージョナルの管理、 などの管理タスクの実行：『Cisco Prime Network Registrar 11.1 Administration Guide』を参照してください。
- CLI による Cisco Prime Network Registrar の設定と管理：『Cisco Prime Network Registrar 11.1 CLI Reference Guide』を参照してください。
- REST API による Cisco Prime Network Registrar の設定と管理：『Cisco Prime Network Registrar 11.1 REST APIs Reference Guide』を参照してください。

Cisco Prime Network Registrar の使用

インストールしたローカルクラスタとリージョナルクラスタを管理するには、スーパーユーザー管理者を作成し、適切なライセンス情報を入力する必要があります。これを行うには、Cisco Prime Network Registrar に初めて接続するときに、次の手順を実行します。

ステップ 1 Cisco Prime Network Registrar の Web UI または CLI を起動します。

- Web UI にアクセスするには、Web ブラウザを開き、HTTPS（セキュアログイン）の Web サイトを使用します。

  `https://hostname:https-port`

  値は、次のとおりです。

  - *hostname* はターゲットホストの実際の名前です。
  - *https-port* はデフォルトの HTTPS ポートです（ローカルの場合は8443、リージョナルの場合は8453）。

- CLI を起動するには、次のように入力して nrcmd を起動します。

  install-path`/usrbin/nrcmd -R -N` *username* `-P` *password*

  作成する管理者アカウントのユーザー名とパスワードを指定します。スーパーユーザー管理者アカウントを作成する必要がある場合は、パスワードの確認を求められます（初回ログイン時）。

  （注） -R は、リージョナルクラスタに接続する場合にのみ指定します。

ステップ 2 ユーザー名とパスワードを入力して、スーパーユーザー管理者を作成します。

- Web UI：[管理者（Admin）] フィールドと [パスワード（Password）] フィールドにそれぞれユーザー名とパスワードを入力します。次に、[追加（Add）] ボタンをクリックします。

ステップ 3 デフォルトでは、スマートライセンスは Cisco Prime Network Registrar 11.1 で有効になっています。アラートウィンドウの [スマートライセンスの設定（Configure Smart Licensing）] リンクをクリックして、[スマート ソフトウェア ライセンス（Smart Software Licensing）] ページを開き、スマートライセンスを設定します。詳細については、『Cisco Prime Network Registrar 11.1 Administration Guide』の「*Use Cisco Smart Licensing*」の項を参照してください。

従来のライセンスを使用する場合は、スマートライセンスを無効にする必要があります（『Cisco Prime Network Registrar 11.1 Administration Guide』の「*Disabling Smart Licensing*」の項を参照してください）。次に、[従来のライセンスの使用（Use Traditional Licensing）] をクリックし、次のようにライセンス情報を入力します。

- Web UI：[参照（Browse）] をクリックし、ライセンスファイルを探します。
- CLI：次のように、ライセンスファイル名の絶対パスまたは相対パスを入力します。

  `nrcmd> license create` *filename*

（注） リージョナルクラスタにライセンスを追加する必要があります。つまり、リージョナルを最初にインストールする必要があります。ローカルクラスタは、最初のログイン時にリージョナルクラスタに登録する必要があります。リージョナルクラスタに追加されたライセンスに基づいて、ローカルのサービス（dhcp、dns、および cdns）を選択できます。

ステップ 4 ステップ 2 で作成されたスーパーユーザーのユーザー名とパスワードを入力して、Web UI と CLI にログインします。

他の管理者アカウントを作成して、割り当てられたロールに基づいて特定の機能を実行することができます。詳細については、『Cisco Prime Network Registrar 11.1 Administration Guide』の「*Managing Administrators*」の章を参照してください。

サーバの起動と停止

インストールが正常に完了し、サーバを有効にした場合は、マシンを再起動するたびに Cisco Prime Network Registrar の DNS サーバおよび DHCP サーバが自動的に起動します。

TFTP サーバの場合、次の Cisco Prime Network Registrar CLI コマンドを使用して、ブートアップ時に再起動できるようにする必要があります。

```
nrcmd> tftp enable start-on-reboot
```

クラスタ内のすべてのサーバは、Cisco Prime Network Registrar のリージョナルサーバ エージェントまたはローカルサーバエージェントによって制御されます。サーバを停止または起動するには、サーバエージェントを停止または起動します。

サーバの停止と起動の詳細については、『*Cisco Prime Network Registrar 11.1 Administration Guide*』を参照してください。

インストールまたはアップグレードが成功すると、Cisco Prime Network Registrar サーバーが自動的に起動します。システムを再起動する必要はありません。

サーバーを起動および停止するには、次の手順を実行します。

ステップ 1 SuperUser としてログインします。

ステップ 2 start 引数を指定して nwreglocal スクリプトまたは nwregregional スクリプトを実行し、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
```

ステップ 3 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）

ステップ 4 stop 引数を指定して nwreglocal スクリプトまたは nwregregional スクリプトを実行し、サーバー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
```

ローカル Web UI を使用したサーバの起動または停止

ローカル Web UI でサーバーを起動または停止するには、次の手順を実行します。

ステップ 1 [操作（Operate）] メニューから、[サーバ（Servers）] サブメニューの [サーバの管理（Manage Servers）] を選択して、[サーバの管理（Manage Servers）] ページを開きます。

ステップ 2 DHCP サーバ、DNS サーバ、CDNS サーバ、TFTP サーバ、BYOD サーバまたは SNMP サーバを起動または停止するには、[サーバの管理（Manage Servers）] ペインでサーバを選択し、次のいずれかを実行します。

- [サーバの起動（Start Server）] ボタンをクリックして、サーバを起動します。
- [サーバの停止（Stop Server）] ボタンをクリックして、サーバを停止します。

ステップ 3 サーバをリロードするには、[サーバの再起動（Restart Server）] ボタンをクリックします。

リージョナル Web UI を使用したサーバの起動と停止

リージョナル Web UI でサーバーを起動または停止するには、次の手順を実行します。

ステップ 1 [操作（Operate）] メニューから、[サーバー（Servers）] サブメニューの [サーバーの管理（Manage Servers）] を選択して、[サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 SNMP サーバーを起動または停止するには、[サーバーの管理（Manage Servers）] ペインでサーバーを選択し、次のいずれかを実行します。

- [サーバの起動（Start Server）] ボタンをクリックして、サーバを起動します。
- [サーバの停止（Stop Server）] ボタンをクリックして、サーバを停止します。

ステップ 3 サーバをリロードするには、[サーバの再起動（Restart Server）] ボタンをクリックします。

サーバのイベントロギング

Cisco Prime Network Registrar を起動すると、システムアクティビティのロギングが開始されます。サーバは、デフォルトで次のディレクトリにすべてのログを保持します。

- 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

ログをモニタするには、**tail -f** コマンドを使用します。

REST API の無効化

Cisco Prime Network Registrar 11.1 をインストールするか、以前のバージョンから 11.1 にアップグレードすると、REST API はデフォルトで有効になります。REST API を無効にする場合は、次の手順を実行します。

ローカルおよびリージョンの詳細 Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 左側の [サーバーの管理（Manage Servers）] ペインの [CCM] をクリックします。[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページが表示されます。このページには、すべての CCM サーバー属性が表示されます。

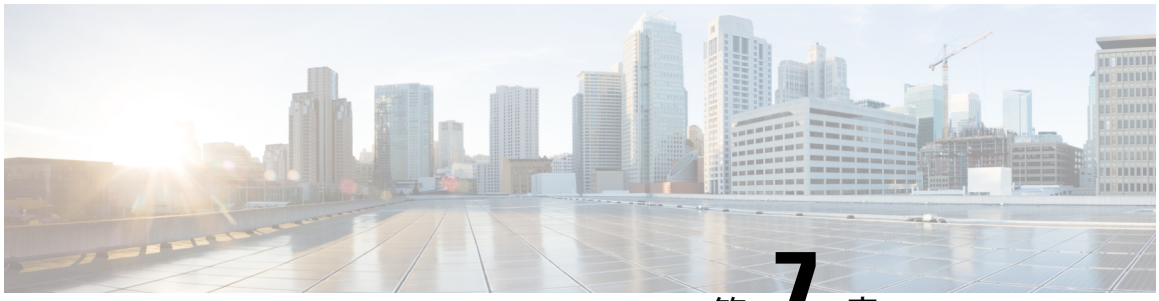
ステップ 3 [制御設定（Control Settings）] セクションで、[is-rest-enabled] 属性値を [false] に設定して REST API を無効にします。

ステップ 4 [**保存（Save**）] をクリックして、変更内容を保存します。

CLI コマンド

REST を無効にするには、**ccm disable is-rest-enabled** を使用します。

REST を有効にするには、**ccm enable is-rest-enabled** を使用します。



第 7 章

Cisco Prime Network Registrar のアンインストール

Cisco Prime Network Registrar をアンインストールするには、管理者権限またはスーパーユーザ権限が必要です。

Cisco Prime Network Registrarをアンインストールする前にデータベースをバックアップするには、『*Cisco Prime Network Registrar 11.1 Administration Guide*』の手順を参照してください。

（注） アンインストールでは、最初に Cisco Prime Network Registrar サーバエージェントが停止します。サーバープロセスがシャットダウンしないことが判明した場合は、サーバの起動と停止 （41 ページ）を参照してください。

Cisco Prime Network Registrar のアンインストール

Cisco Prime Network Registrar をアンインストールするには、次のいずれかのコマンドを実行します。

```
# rpm -e kitname
```

または

```
# yum remove kitname
```

または

```
# dnf remove kitname
```

ここでは、*kitname* は cpnr-local、cpnr-regional、または cpnr-client のいずれかです。

たとえば、リージョナルクラスタをアン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。

```
# rpm -e cpnr-regional
```

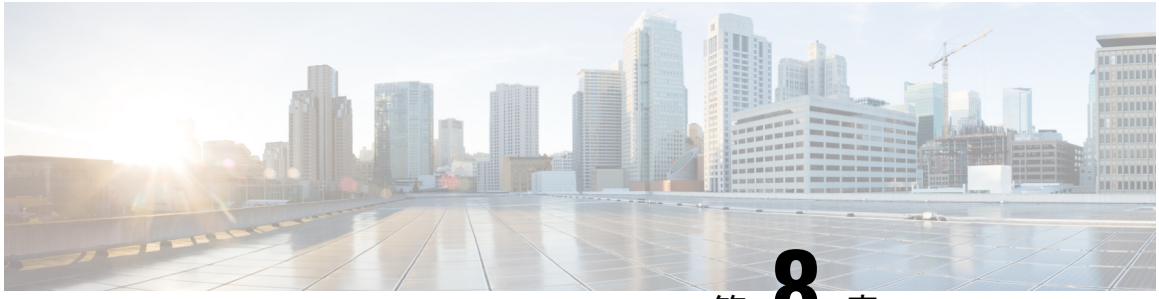
または

```
# yum remove cpnr-regional
```

または

```
# dnf remove cpnr-regional
```

インストール中および操作中に作成された特定の構成とデータファイルは、アンインストール後も意図的に残されます。オプションで、アンインストールのメッセージの最後に示される指示に従って、Cisco Prime Network Registrar に関連付けられているデータファイルを削除します。



第 8 章

Cisco Prime Network Registrar 仮想アプライアンス

Cisco Prime Network Registrar 仮想アプライアンスには、Linux オペレーティングシステムにインストールされた Cisco Prime Network Registrar 11.1 のバージョンで使用可能なすべての機能が含まれています。

この章では、Cisco Prime Network Registrar 仮想アプライアンスのインストール方法について説明します。内容は次のとおりです。

システム要件

仮想アプライアンスのインストールに使用できるキットは 2 つあります。

- VMware ESXi 7.0 で実行される OVA
- OpenStack に展開できるクラウドイメージ

これらのキットは事実上同一のものであり、このマニュアルではOVAについて説明した場合、特に明記しない限りその説明は両方のキットに適用されます。

これらの各キットは、4 つの仮想 CPU、8 GB のメインメモリ、6 GB のスワップパーティション、および 39 GB の空き容量がある 42 GB のシステムパーティションという、限られたリソースを必要とするように作成されています。必要なディスクストレージの合計は 48 GB です。システムディスクのサイズを増やすことはほぼ確実です。仮想アプライアンスに仮想 CPU を追加すると、パフォーマンスが大幅に向上します。これらの要件を満たすために、展開対象のホストで十分なリソースが使用可能であることを確認する必要があります。

仮想 CPU を正しく設定しないと、Non-Uniform Memory Access（NUMA）のパフォーマンスの問題が発生する可能性があることに注意してください。この問題を回避するには、単一の CPU ソケット（1 NUMA ノード内にとどまる）の物理コアの総数以下の量の vCPU を仮想マシンに割り当てます。また、単一の仮想マシンが単一の NUMA ノードよりも多くの vCPU を消費することは避けてください。そうしないと、複数の NUMA ノードにまたがってスケジュールされ、メモリアクセスの低下を引き起こす可能性があります。

仮想アプライアンスで使用されるリソースを増やす必要があります。そうしないと、正常に機能しません。ローカルクラスタの実行、または同じマシン上のリージョナルクラスタとローカルクラスタの実行という 2 つの異なる方式があります。以下の推奨事項は、ジャンプスタートで仮想アプライアンスを実行するためのものですが、これらはローカルクラスまたはリージョナルクラスタの展開の開始点としても役立ちます。ローカルクラスタの場合：

- CPU：1 ソケット、8 CPU
- メモリ：12 GB
- ディスク：100 GB 以上

ローカルクラスタと同じジャンプスタートで動作しているリージョナルクラスタの場合：

- CPU：1 ソケット、7 CPU
- メモリ：8 GB 以上
- ディスク：48 GB

展開のサイズに基づいて、上記よりもかなり多くのディスク容量が必要になる場合があります。割り当てられたディスクのサイズを変更し、アプライアンスを再起動することで、ディスク容量を増やすことができます。

Cisco Prime Network Registrar 仮想アプライアンスのインストールとアップグレード

仮想アプライアンスは、VMware ESXi 7.0 または OpenStack の 2 つの環境のいずれかに展開できます。展開のために決定する必要がある情報について説明した後、個々の環境について詳しく説明します。

Cisco Prime Network Registrar 仮想アプライアンスの展開準備

Cisco Prime Network Registrar 仮想アプライアンスを展開し、そのネットワーク接続を設定するには、いくつかの質問に答える必要があります。質問の中には、仮想アプライアンスが展開されているネットワーキング環境に関するものと、展開されている特定の仮想アプライアンスに固有の値に関するものがあります。

この特定の仮想アプライアンスのインストールに固有の質問を以下に示します。仮想アプライアンスを展開する前に、これらの質問に対する回答を決定する必要があります。

- 展開された仮想アプライアンスの仮想マシン名。
- 基盤となる Linux CentOS オペレーティングシステムのルートパスワード。
- 仮想アプライアンスの IPv4 アドレス。
- 仮想アプライアンスの IPv4 アドレスに関連付けられた DNS 名。
- Cisco Prime Network Registrar アプリケーションの初期管理者アカウントのユーザ名とパスワード。

（注） Cisco Prime Network Registrar 9.1 以降では、既存の VM をコピーして新しいローカルクラスタ（スナップショット）を作成できます。UUID の重複を避けるために、新しい UUID を生成してリージョナルクラスタに再登録する必要があります。の「新しい *UUID* の生成（*Generating new UUID*）」の項を参照してください。 Cisco Prime Network Registrar 11.1 Administration Guide

ネットワーキング環境に関する質問は次のとおりです。これらの質問に対する回答は、仮想アプライアンスに固有のものではなく、仮想アプライアンスを展開する環境によって決定される値です。

- 仮想アプライアンス自体の IP アドレスと関連付けられたネットワークマスク
- 仮想アプライアンスのデフォルト ゲートウェイ アドレス
- 仮想アプライアンスがアクセスできる 1 つ以上の DNS サーバの IP アドレス。ただし、可用性を高めるために、2 つの DNS サーバの IP アドレスを持つことを推奨します。
- 仮想アプライアンスがインターネットにアクセスするために必要なプロキシ値（仮想アプライアンスにインターネットへのアクセスを許可する場合）。
- これがローカルクラスタのインストールの場合、ライセンス情報を受信するために、このローカルクラスタが接続する Cisco Prime Network Registrar リージョナルクラスタの IP アドレスを決定する必要があります。これがリージョナルクラスタインストールの場合、この要件を無視できます。

VMware 上のリージョナルクラスタ OVA またはローカルクラスタ OVA の展開

Cisco Prime Network Registrar 仮想アプライアンスは、VMware ESXi 7.0 での実稼働使用がサポートされており、VMware vSphere クライアントを使用してアクセスまたは管理できます。Cisco Prime Network Registrar 仮想アプライアンスは、オープン仮想アプライアンス（OVA）パッケージで提供されます。

VMware vSphere クライアントは、ESXi に直接接続するか、または vCenter サーバへの接続を介して、vSphere に接続できます。VCenter を介して接続すると、ESXi に直接接続した場合に

は提供されない多くの機能が提供されます。VCenterサーバが使用可能で、ESXiに関連付けられている場合は、VCenter を介した接続を推奨します。

Cisco Prime Network Registrar 仮想アプライアンスをインストールするには、最初に正しいインストールファイルをダウンロードする必要があります。使用可能なファイルは、リージョナル仮想アプライアンスとローカルクラスタ仮想アプライアンスの2つです。これらの各仮想アプライアンスは、.ova ファイルとして提供されます。

名前は次のとおりです。

- ローカル仮想アプライアンスでは、**cpnr_version_local.ova**
- リージョナル仮想アプライアンスでは、**cpnr_version_regional.ova**

選択した仮想アプライアンスをダウンロードします。すべての Cisco Prime Network Registrar ローカルクラスタのインストールでは、操作に必要なライセンス情報を受信するために、Cisco Prime Network Registrar リージョナルクラスタに接続する必要があります。したがって、Cisco Prime Network Registrar ローカル仮想アプライアンスをインストールする前に、ライセンス情報を受信するために接続するリージョナルクラスタのIPアドレスを識別する必要があります。

VSphere を使用して、ESXi のインストールまたは vCenter サーバに直接接続し、OVA の展開先である ESXi のインストールを選択します。

vCenter サーバを使用できる場合は、ESXi ハイパーバイザを既存の vCenter サーバに接続し、その vCenter サーバを介して管理できます。共通の vCenter サーバを介してすべての VMware ハイパーバイザを管理することには、多くの利点があります。

vCenter Server を介して vSphere クライアントで ESXi ハイパーバイザを管理しているときに表示される画面は、vSphere クライアントを ESXi ハイパーバイザに直接接続するときに表示される画面とは異なります。vCenter サーバを介して接続している場合は、追加の画面を表示できます。これらの画面は、実際には Cisco Prime Network Registrar 仮想アプライアンスの展開に関わる操作に利点はありません。vCenter サーバアプローチを使用する利点は、仮想アプライアンスの初期展開後に得られます。

リージョナルクラスタ OVA またはローカルクラスタ OVA を展開するには、次の手順を実行します。

ステップ 1 vSphere のメニューから、[ファイル（File）] > [OVF テンプレートの展開（Deploy OVF Template）] を選択します。

[OVF テンプレートソースの展開（Deploy OVF Template Source）] ウィンドウが表示されます。

ステップ 2 OVA ファイルを展開するには、[参照（Browse）] をクリックし、vSphere が実行されているローカルマシンで使用可能な OVA ファイル（.ova）に移動して選択します。

（注） URL を参照することはできず、ファイルへのフルパスを入力する必要があります。

ステップ 3 [次へ（Next）] をクリックします。

[OVFテンプレートの詳細（OVF Template Details）] ウィンドウが表示されます。製品名、OVA ファイルのサイズ、仮想アプライアンスのために使用可能である必要があるディスク領域が表示されます。

ステップ 4 OVF テンプレートの詳細を確認して、[次へ（Next）] をクリックします。

ステップ 5 新しい仮想アプライアンスの名前を入力して、[次へ（Next）] をクリックします。

（注） 仮想アプライアンスの設定時に同じ名前を入力する必要があるため、この名前を忘れないようにしてください。

[展開オプション（Deployment Nodes）] ウィンドウが表示されます。

デフォルトでは、プロビジョニング フォーマット [シン（Thin）] が選択されています。デフォルト値に関係なく、[シック（Thick）] を選択する必要があります。

ステップ 6 [次へ（Next）] をクリックして続行します。

（注） 仮想アプライアンスは、シックプロビジョニングで展開されている場合にのみサポートされます。

ステップ 7 この OVA テンプレートで使用されるネットワークをインベントリ内のネットワークにマッピングするには、現在の接続先ネットワークを選択し、[接続先ネットワーク（Destination Networks）] ドロップダウンリストから接続先ネットワークを選択します。[次へ（Next）] をクリックします。

[Ready to Complete（終了準備の完了）] ウィンドウが表示されます。

ステップ 8 [終了（Finish）] をクリックして、OVA テンプレートの展開を開始します。

Cisco Prime Network Registrar 仮想アプライアンスの起動と設定

Cisco Prime Network Registrar 仮想アプライアンスを起動して設定するには、次の手順を実行します。

（注） [電源オン（Power On）] ボタン（▶）をクリックする前に、要件に基づいてメモリと CPU を設定する必要があります。VM を起動すると、シャットダウンするまでメモリや CPU の設定を変更できません。

ステップ 1 仮想アプライアンス OVA を展開した後、vSphere で仮想マシン名を選択して右クリックし、[コンソールを開く（Open Console）] を選択します。

ステップ 2 コンソールの [電源オン（Power on）] ボタン（▶）をクリックした後、ウィンドウをクリックします。

新しく展開されたマシンの初回起動時に、ルート（システム）パスワードを入力するように求められます。これは、Cisco Prime Network Registrar アプリケーションのパスワードとは異なります。

（注） これは、Cisco Prime Network Registrar 11.1 アプリケーションを搭載した基盤となる Linux オペレーティングシステムのルートパスワードを指します。このパスワードを 2 回入力するように求められます。今後、さまざまな場面で、基盤となる Linux オペレーティングシステムへのルートアクセスが必要になります。そのため、このパスワードを覚えておいてください。

起動プロセスには、ルートパスワードの入力が求められる前と、ルートパスワードの入力後の両方に時間がかかる場合があります。

[エンドユーザライセンス契約（End User License Agreement）] ウィンドウが初回起動時に表示されます。ライセンス契約を完読し、ライセンス条項を理解して同意した場合にのみ、**y**（Yes）と入力してください。

ステップ 3 ルートユーザとしてサーバにログインします。

ステップ 4 仮想アプライアンスのネットワークを設定するには、nmcli を使用した RHEL/AlmaLinux 8.x でのネットワークアクセスの設定 （85 ページ）を参照してください。

OpenStack 上のリージョナルクラスタまたはローカルクラスタの展開

Cisco Prime Network Registrar 仮想アプライアンスをインストールするには、最初に正しいインストールファイルをダウンロードする必要があります。使用可能なファイルは、リージョナル仮想アプライアンスとローカルクラスタ仮想アプライアンスの 2 つです。これらの各仮想アプライアンスは、.qcow2 ファイルとして提供されます。

その名前は次のとおりです。

- ローカル仮想アプライアンスでは、**cpnr_version_local.qcow2**
- リージョナル仮想アプライアンスでは、**cpnr_version_regional.qcow2**

選択した仮想アプライアンスをダウンロードします。すべての Cisco Prime Network Registrar ローカルクラスタのインストールでは、操作に必要なライセンス情報を受信するために、Cisco Prime Network Registrar リージョナルクラスタに接続する必要があります。したがって、Cisco Prime Network Registrar ローカル仮想アプライアンスをインストールする前に、ライセンス情報を受信するために接続するリージョナルクラスタの IP アドレスを識別する必要があります。

OpenStack でローカルクラスタまたはリージョナルクラスタを実行するには、最初に **.qcow2** 流通キットを使用してローカルイメージまたはリージョナルイメージを作成する必要があります。

このイメージが存在する場合、ローカルクラスタまたはリージョナルクラスタのインスタンスを起動できます。インスタンスに関連付けるフレーバには、少なくとも 4 つの VCPU、8 GB の RAM、および少なくとも 48 GB のルートディスクストレージが必要です。Cisco Prime Network Registrar の動作インスタンスを使用するには、絶対的な最小値として 48 GB を超えるルートディスクストレージを割り当てる必要があります。ローカルクラスタまたはリージョナルクラスタに必要なディスク容量については、システム要件 （47 ページ）を参照してください。

Cisco Prime Network Registrar のインスタンスが固定 IP アドレスで作成されます。Cisco Prime Network Registrar は、起動時に検出できるインターフェイスに関連付けられた IP アドレスを自動的に使用します。Cisco Prime Network Registrar に使用可能なインターフェイスにプロバイダーネットワークから IP アドレスが割り当てられている（つまり、Cisco Prime Network Registrar が提供する DHCP または DNS 機能を必要とするクライアントにアクセスできる）場合、通常どおりに Cisco Prime Network Registrar を設定できます。

（注） OpenStack の最新バージョン（Victoria など）に Cisco Prime Network Registrar qcow2 イメージをインストールすると、Cisco Prime Network Registrar プロセス（DNS、DHCP、および CCM）は正常に実行されますが、Java プロセスと Web UI の実行には数時間または数日かかる場合があります。これは、Java および QEMU ハイパーバイザに固有の問題です。したがって、KVM 仮想化を使用して適切な CPU 設定を行うことをお勧めします。

次のコマンドを使用して、KVM 仮想化のサポートを確認できます。

```
# lscpu | grep -i "Model Name"
Model name: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz

# grep -i -o vmx /proc/cpuinfo | uniq
vmx
```

上記の出力に「vmx」が表示されていることは、必要な CPU 拡張機能が Intel プロセッサ上にあることを示しています。

VMware に Cisco Prime Network Registrar 仮想アプライアンスをインストールする場合は、仮想マシンの初回起動時に、システムコンソールで基盤となる Linux システムのルートパスワードを設定します。ただし、通常、OpenStack インスタンスは、OpenStack インスタンスの一部として設定された SSH キーペアを使用した SSH によるログインのみを許可するように、作成および展開されます。多くの OpenStack インスタンスは、ルートパスワードによるログインをまったく許可せず、SSH キーペアで SSH を使用したログインのみを許可します。

Cisco Prime Network Registrar OpenStack インスタンスは、次の 2 つの状況のいずれかで操作するように設定できます。

オプション 1：ルートパスワードの構成を要求し、パスワードを使用したルートログインを許可します。

オプション 2：ルートパスワードの構成とログインを無効にします。ログインには SSH キーペアが必要です。

オプション 1：

これは、すべての Cisco Prime Network Registrar 仮想アプライアンスキットのデフォルトのアプローチであり、追加のアクションは必要ありません。Cisco Prime Network Registrar 仮想アプライアンスのイメージからインスタンスを起動します。最初の起動時に、Cisco Prime Network Registrar インスタンスのコンソールウィンドウを表示し、Linux システムのルートパスワードを入力し、エンドユーザライセンス契約に同意する必要があります。最初の起動後、コンソールにアクセスする必要はありません。SSH キーペアを使用してこのインスタンスにアクセスすることもできます。

オプション 2：

OpenStack インスタンスの展開における通常の慣行に従った方法で Cisco Prime Network Registrar 仮想アプライアンスインスタンスを展開する場合は、パスワードを使用したルートログインを許可しないように Cisco Prime Network Registrar OpenStack インスタンスを設定し、ログインに SSH キーペアを要求できます。また、ルート権限を持つルート以外のユーザにパスワードベースのログインを許可する場合、設定方法の手順は以下のとおりです。

Web UI から OpenStack インスタンスを起動する場合、ルートパスワードによるログインを防止するには、[インスタンスの起動（Launch instance）] ダイアログの [構成（Configuration）] セクションで特定の構成を実行する必要があります。他のシステムのユーザデータに類似したカスタマイゼーション スクリプトを提供する必要があります。OpenStack インスタンスでルートパスワードベースのログインを無効にするスクリプト（以下に記載）を設定する必要があります。このカスタマイゼーション スクリプトで設定されたインスタンスを展開した後、インスタンス上の Linux オペレーティングシステムにアクセスする唯一の方法は、起動時にインスタンスに関連付けられた **SSH キーペア**を使用して SSH 経由でログインすることです。

たとえば、**ssh -i keypairname.pem root@a.b.c.d** を使用してログインします。キーペアをインスタンスに関連付けなかった場合、またはキーペアへのアクセスを失った場合は、インスタンスにログインできません。この方法でインスタンスを作成すると、デフォルトのルートパスワードはなくなり、ルートパスワードログインは無効になります。

オプション 2 を設定するには、[カスタマイゼーション スクリプト（Customization Script）] テキストボックスに次のように入力します。

```
# cloud-boothook
 # !/bin/bash
 if [ ! -f /etc/cloud/cloud.cfg.orig ]; then
 cp /etc/cloud/cloud.cfg /etc/cloud/cloud.cfg.orig
 cp /etc/cloud/cloud.cfg.norootpasswd /etc/cloud/cloud.cfg
 fi
```

（注） オプション 2 を選択し、**SSH キーペア**を使用してインスタンスにアクセスした後、パスワードを使用してログインする場合は、**useradd** コマンドを使用して新しい Linux ユーザを作成し、そのユーザをグループホイールのメンバーにすることもできます。また、**passwd** コマンドを使用して、そのユーザに安全なパスワードを与える必要があります。これにより、そのユーザとして **SSH** またはコンソールにいつでもログインでき、ルート権限が付与されます。

パスワードログインを許可するユーザを作成するには、次のコマンドを使用します。

```
useradd safeuser -g wheel
passwd safeuser
```

次に、ルートアクセスが必要な場合は、**safeuser** としてログインし、次のコマンドを使用します。

```
sudo su
```

safeuser のパスワードを入力すると、ルートユーザになります。

使用可能なインターフェイスに関連付けられている IP アドレスが固定アドレスである場合（つまり、OpenStack の他のインスタンスにのみアクセス可能）、フローティングアドレスを Cisco Prime Network Registrar インスタンスに関連付ける必要があります。このフローティングアドレスは、Cisco Prime Network Registrar インスタンスによって提供される DHCP サービスまたは DNS サービスのクライアントにアクセスできる必要があります。インスタンスに組み込まれたインターフェイスに関連付けられている Cisco Prime Network Registrar を検出できる固定 IP アドレスではなく、フローティングアドレスの IP アドレスをそのサーバ ID として返すように、Cisco Prime Network Registrar によって提供される DHCP サーバを設定する必要があります。こ

の状況でDHCPを設定するには、エキスパートモードにして、このインスタンスに割り当てられたフローティングアドレスを使用してDHCPポリシー属性 *dhcp-server-identifier-address* を設定する必要があります。そうすれば、DHCPサーバは、クライアントとの通信に使用しているインターフェイスを調べてDHCPサーバが検出できるIPアドレス（固定IPアドレス）ではなく、設定されたIPアドレス（このインスタンスの外部から見えるIPアドレス）を返します。

ローカルクラスタは、リージョナルクラスタに登録する必要があります。この登録後、リージョンクラスタはローカルクラスタに接続できる必要があります。ローカルクラスタは、最初にリージョナルクラスタに登録すると、そのIPアドレスをリージョナルクラスタに送信します。ローカルクラスタがそのネットワーク インターフェイスに設定されていると見なすIPアドレスを使用して、リージョナルクラスタがロクカルクラスタに接続できる場合、アクションは必要ありません。これは、ローカルクラスタに固定IPアドレスがあり、OpenStackクラウド内でのみ表示可能であるが、リージョナルクラスタも同じクラウド内にあった場合です。ローカルクラスタがそのネットワーク インターフェイスのIPアドレスと見なすIPアドレスを、リージョナルクラスタがpingできる場合、追加のステップは必要ありません。ただし、リージョナルクラスタが、ローカルクラスタが実行されているOpenStackクラウドに対してローカルではなく、ローカルクラスタに固定アドレスに加えてフローティングアドレスがある場合、ローカルクラスタに対するリージョナルクラスタの構成では、そのIPアドレスを更新してフローティングアドレスのもの（固定アドレスではなく初期登録時のアドレス）にする必要があります。

ローカルクラスタを割り当てる場合は、4つまたは8つのVCPUと12 GB以上のRAM（大規模システムではさらに多くのRAM）の割り当てを検討する必要があります。ローカルクラスタには、最小インストールに使用可能な7GB以上の空き容量が必ず必要になります。リージョナルクラスタには追加のディスク容量が必要になる可能性がありますが、多くのインストールでは2個から4個のVCPUと8 GBから12 GBのRAMで十分です。

Cisco Prime Network Registrar 仮想アプライアンスのアップグレード

この項では、既存の仮想アプライアンスのデータを使用して、Cisco Prime Network Registrar をCisco Prime Network Registrar 仮想アプライアンスにアップグレードし、オペレーティングシステムをAlmaLinux 8.6にアップグレードする手順について説明します。

（注） Cisco Prime Network Registrar 11.1 仮想アプライアンスに使用される最新のオペレーティングシステムのバージョンはAlmaLinux 8.6です。

Cisco Prime Network Registrar 仮想アプライアンスで実行するための Cisco Prime Network Registrar アップグレードインストール

この項では、Cisco Prime Network Registrar の既存のインストールをアップグレードして、Cisco Prime Network Registrar 仮想アプライアンスにする方法について説明します。

（注） この手順では、Linux オペレーティングシステムで実行中の Cisco Prime Network Registrar の現在のバージョンを、Cisco Prime Network Registrar 仮想アプライアンスの現在のバージョンにアップグレードします。別のプラットフォームから移動する必要がある場合は、仮想アプライアンスにアップグレードする前に、まず Linux プラットフォームに変換する必要があります。別のバージョンの Cisco Prime Network Registrar から現在のバージョンの仮想アプライアンスに移動する必要がある場合、まず外部 Linux システム上で現在のバージョンの Cisco Prime Network Registrar にアップグレードしてから、仮想アプライアンスにアップグレードする必要があります。Cisco Prime Network Registrarのインストールおよびアップグレード （25 ページ）を参照してください。

ステップ 1 Cisco Prime Network Registrar 仮想アプライアンスをインストールします。

ステップ 2 **systemctl stop nwreglocal** コマンドを使用して、アップグレードする Cisco Prime Network Registrar アプリケーションをシャットダウンします。

ステップ 3 次の tar コマンドを使用して、既存の /var/nwreg2/local/data ディレクトリを圧縮します。

```
tar cvf tarfile.tar data
```

ステップ 4 作成した tar ファイルを新しい仮想アプライアンスにコピーします。

ステップ 5 次のコマンドを使用して、新しい仮想アプライアンスの Cisco Prime Network Registrar をシャットダウンします。

```
systemctl stop nwreglocal
```

ステップ 6 次のコマンドを使用して、既存のデータベースの名前を **.orig** に変更します。

```
mv /var/nwreg2/local/data /var/nwreg2/local/data.orig
```

ステップ 7 **tar xvf tarfile.tar** を使用して、ステップ 3 で転送した最新のデータベースを解凍します。

ステップ 8 アップグレードするシステムの既存の拡張機能を、新しい仮想アプライアンスの正しいディレクトリにコピーします。

ステップ 9 次のコマンドを使用して、新しい仮想アプライアンスの Cisco Prime Network Registrar を起動します。

```
systemctl start nwreglocal
```

新しいバージョンの仮想アプライアンス オペレーティング システムへのアップグレード

アップグレードして新しいバージョンの Cisco Prime Network Registrar 仮想アプライアンスを使用するには、新しいバージョンのオペレーティングシステムを含む新しい仮想アプライアンスをインストールし、既存の仮想アプライアンスから新しい仮想アプライアンスにデータと構成を移動します。

これを行うには、Cisco Prime Network Registrar 仮想アプライアンスで実行するための Cisco Prime Network Registrar アップグレードインストール （56 ページ）の手順を実行します。

これで、新しい仮想マシンを起動できます。既存の仮想マシンのデータディレクトリ全体が含まれます。

（注） オペレーティングシステムがアップグレードされた新しい仮想マシンは起動プロセス中に一時停止し、新しい仮想マシン上に存在する Cisco Prime Network Registrar アプリケーションのデータベースのバージョンと一致させるため、Cisco Prime Network Registrar データベースをアップグレードするよう指示します。起動プロセス中にこの一時停止が発生し、メッセージが表示されるたびに、Cisco Prime Network Registrar は、/opt/nwreg2/local/usrbin/upgrade_cnr スクリプト（またはリージョンクラスタの場合は /opt/nwreg2/regional/usrbin/upgrade_cn スクリプト）が実行されるまで起動できません。Cisco Prime Network Registrar は systemctl を使用してマスクされており、**upgrade_cnr** スクリプトはアップグレードを実行する前にマスクを解除します。

ステップ 1 コンソールで [戻る（return）] を押して、起動プロセスを完了します。

ステップ 2 ルートとしてログインし、表示されたコマンドを実行します。
起動が完了すると、新しい仮想マシン上で、新しいバージョンの Cisco Prime Network Registrar で実行されている既存の構成が表示されます。

Cisco Prime Network Registrar アプリケーションのアップグレード

仮想アプライアンスに現在存在する Cisco Prime Network Registrar のインストールを Cisco Prime Network Registrar の新しいバージョンにアップグレードする場合は、このマニュアルの手順に従ってソフトウェア製品の簡単なアップグレードを実行します。仮想アプライアンスでの Cisco Prime Network Registrar のインストールは、Cisco Prime Network Registrar ソフトウェア製品の標準のインストールです。

次のステップ：Cisco Prime Network Registrar 仮想アプライアンス

仮想アプライアンスの CLI を使用した Cisco Prime Network Registrar の設定

Cisco Prime Network Registrar CLI を使用して仮想アプライアンスを設定するには、次の 2 通りの方法があります。

- 最初に SSH を使用して仮想アプライアンスの基盤となる Linux オペレーティングシステムに接続することで、仮想アプライアンスで nrcmd CLI を直接使用できます。SSH ログインには、仮想アプライアンスで作成した任意のユーザ名とパスワードを使用できます。nrcmd CLI を使用して Cisco Prime Network Registrar を設定するには、Cisco Prime Network Registrar の管理者ユーザ名とパスワードを使用する必要があります。

（注） 分散型では、Linux オペレーティングシステムの有効なユーザは root のみです。Cisco Prime Network Registrar CLI を使用するには、ルートとしてログインできますが、システムにユーザを追加することもできます。**useradd** プログラムを使用して、ユーザを追加します。ユーザを追加する方法の詳細については、**man useradd** と入力することもできます。

- あるいは、ネットワーク内の他のシステムで nrcmd CLI を使用して、Cisco Prime Network Registrar のリモートインストールを管理に使用するのと同じ方法で、仮想アプライアンス上の Cisco Prime Network Registrar を設定および管理できます。これには、他のシステムに Cisco Prime Network Registrar をインストールする必要があります（通常はクライアントのみのインストール）。

自動的に起動するための仮想アプライアンスの設定

ESXi ハイパーバイザレイヤに電力が復旧されたときに、Cisco Prime Network Registrar 仮想アプライアンスを自動的に起動するように ESXi ハイパーバイザを設定できます。

自動起動を設定するには、次の手順を実行します。

ステップ 1 VSphere クライアントで、接続先の ESXi マシンを選択します。特定の仮想マシンを選択するのではなく、VM が存在する ESXi ハイパーバイザを選択します。

ステップ 2 [設定（Configuration）] タブを選択します。

ステップ 3 [ソフトウェア（Software）] エリアの下にある [仮想マシンの起動/シャットダウン（Virtual Machine Startup/Shutdown）] リンクをクリックします。ウィンドウ内のリストに仮想マシンが表示されます。

ステップ 4 ページの右上隅にある [プロパティ... （Properties...）] リンクをクリックします。表示されない場合は、表示されるまでウィンドウのサイズを変更します。

[仮想マシンの起動/シャットダウン（Virtual Machine Startup/Shutdown）] ページが表示されます。

ステップ 5 [システムによる仮想マシンの自動起動と自動停止を許可（Allow Virtual machines to start and stop automatically with the system）] チェックボックスをオンにします。

ステップ 6 Cisco Prime Network Registrar 仮想アプライアンスを稼働している仮想マシンを選択し、右側にある [上へ移動（Move up）] ボタンを使用して、[自動起動（Automatic Startup）] というラベル名のグループに移動します。

ステップ 7 [OK] をクリックします。

これにより、電源が復旧されるたびに、確実に ESXi ハイパーバイザが起動します。Cisco Prime Network Registrar アプライアンスが自動的に起動します。

Cisco Prime Network Registrar 仮想アプライアンスの管理

ルートユーザーとしてログインすることで、AlmaLinux 8.6 に基づいて基盤となる Linux オペレーティングシステムを管理できます。SSH を使用して、仮想アプライアンスを最初にブートしたときに指定したユーザ名ルートとルートパスワードで、仮想アプライアンスにログインできます。Openstack では、インスタンスの起動時に作成されたキーペアを使用できます。

ルート以外のユーザ名で Linux システムにアクセスできるように、Linux システムに追加のユーザを作成する必要がある場合があります。

仮想アプライアンスに含まれる Linux システムはかなりの程度まで削減されているため、Windows システムマネージャや関連する GUI ユーザインターフェイスなど、Cisco Prime Network Registrar アプリケーションの実行や管理に不要なものは含まれていません。ただし、Cisco Prime Network Registrar アプリケーションのサポートおよび管理に必要なすべてのツールは、仮想アプライアンス内で使用される Linux オペレーティングシステムに含まれています。

SSH 接続を保護するために追加のステップを実行することもできます。たとえば、ルートとしてロギングしないように構成し、別のユーザとしてロギングした後にルート権限を取得するためにユーザに **su** を要求します。

ご使用の環境に適した方法でロックダウンするために、基盤となる Linux オペレーティングシステムで他の構成変更を実行することもできます。

（注） Cisco Prime Network Registrar 11.1 仮想アプライアンスに使用される最新のオペレーティングシステムのバージョンは AlmaLinux 8.6 です。

（注） Cisco Prime Network Registrar お客様は、適用を希望するパッチに関して OS を最新の状態に維持する責任を単独で負うものとし、シスコはその責任を負いません。

（注） Cisco Prime Network Registrar のオプションのビルド済み VM ダウンロードでパッケージ化された Linux ディストリビューションはオープンソースソフトウェアであり、シスコは所有またはサポートしていません。Linux のサポートが必要なお客様は、サードパーティのソフトウェアプロバイダーにご連絡いただく必要があります。

OVA のインストール後

Cisco Prime Network Registrar を構成する前に、次のステップに従って最新の CentOS アップデート、インストールされているパッケージの最新バージョン、およびセキュリティアップデートを取得します。

（注） **yum update または dnf update** コマンドは、仮想アプライアンスに付属のオペレーティングシステムで Cisco Prime Network Registrar アプリケーションをテストしたときに、ほとんどの場合存在しなかった新規のソフトウェアおよび変更されたソフトウェアで実行中のシステムを更新します。**yum update または dnf update** コマンドの一部としてインストールされる更新は、Cisco Prime Network Registrar アプリケーションに問題を引き起こしません。ただし、シスコは、Cisco Prime Network Registrar のアプリケーションが、テストの実行時に使用できなかったソフトウェアとのインターフェイスで問題なく動作することを保証できません。更新された仮想アプライアンスを実稼働環境に配置する前に、**yum update または dnf update** コマンドを実行した後、ご使用の環境ですべてが正常に動作していることを確認するために、独自のテストを実行する必要があります。

ステップ 1 ルートとしてログインします。

ステップ 2 ネットワーキングを設定します。

ステップ 3 ルートプロンプトに移動し、次のコマンドを入力します。

```
# yum update
```

ステップ 4 システムを再起動し、Cisco Prime Network Registrar を設定します。

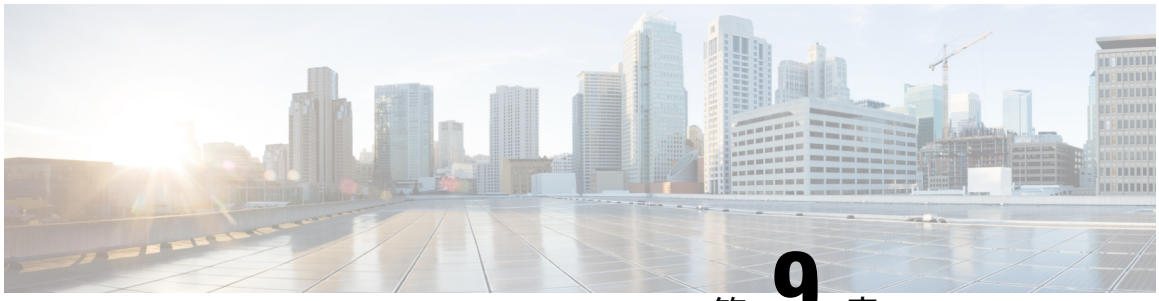
仮想マシンを展開するための独自の基本イメージの構築

dnsmasq と libvirtd の無効化

dnsmasq および libvirtd サービスは、Linux 7 および 8 のディストリビューションに事前にインストールされている場合があります。これらはポート 53 および 67 を使用し、Cisco Prime Network Registrar が適切に動作しなくなる可能性があります。DHCP および DNS サーバーを正しく起動して実行するには、dnsmasq と libvirtd を無効化する必要があります。

dnsmasq および libvirtd サービスを無効化するには、次のコマンドを実行してから仮想マシンを再起動します。

```
# systemctl disable dnsmasq.service
# systemctl disable libvirtd.service
# reboot
```



第 9 章

コンテナでの Cisco Prime Network Registrar

Cisco Prime Network Registrar 11.1 は、独自のインフラストラクチャにインストールできる Docker コンテナとして実行できます。

Cisco Prime Network Registrar 11.1 では、次の Docker イメージが提供されます。

- リージョンコンテナ：**cpnr-regional-11.1-1.el8.x86_64_rhel_docker.tar.gz**
- ローカルコンテナ：**cpnr-local-11.1-1.el8.x86_64_rhel_docker.tar.gz**

この章は、次の項で構成されています。

ホストマシンの要件

- Cisco Prime Network Registrar コンテナが必要とするポートに公開するホストマシン上のポートを特定します。Cisco Prime Network Registrar サービスで使用されるポートの完全なリストについては、Cisco Prime Network Registrar 11.1 Administration Guideの「Cisco Prime Network Registrar サービスのデフォルトポート」の項を参照してください。
- ホストマシン上の Cisco Prime Network Registrar コンテナのデータを保持するオプションを [バインドマウント（Bind mount）]（ホストマシン上のディレクトリが使用されます）または [ボリューム（Volume）]（Docker によって管理されます）のいずれかから選択します。
- IPv4 の場合は、ブリッジネットワークまたは macvlan ネットワークを使用できます。パフォーマンス向上のため、macvlan を推奨します。
- IPv6 の場合は、IPv6 アドレスを持つようにコンテナを設定する必要があります。

Cisco Prime Network Registrar Docker コンテナの実行

Cisco Prime Network Registrar を Docker コンテナとして実行するには、最初に選択した Docker イメージをダウンロードする必要があります。次に、以下の手順を実行します。

ステップ 1 次のコマンドを使用して、Docker イメージを読み込みます。

- リージョナルコンテナの場合：

```
# docker load -i cpnr-regional-11.1-1.el8.x86_64_rhel_docker.tar.gz
```

- ローカルコンテナの場合：

```
# docker load -i cpnr-local-11.1-1.el8.x86_64_rhel_docker.tar.gz
```

ステップ 2 次のコマンドを使用して、イメージが正常に読み込まれていることを確認します。

```
# docker image ls
```

ステップ 3 次のコマンドを使用して Docker コンテナを実行します。

- リージョナルコンテナの場合：

```
# docker run -d --name cpnr_regional_container --privileged=true -p 8453:8453 -p 1244:1244
--mount type=bind,source=/data/cpnr_regional_data,target=/var/nwreg2/regional cpnr-regional:11.1
 /usr/sbin/init
```

上記のコマンドでは、次のようになります。

  - Docker のデフォルトブリッジネットワーキング ドライバが使用されます。コンテナに必要なポートが公開されます。8453 はリージョナルの Web UI 用で、1244 はリージョナルの設定管理用です。
  - Cisco Prime Network Registrar のデータディレクトリは var/nwreg2/regional で、ホストのマウントポイントは /data/cpnr_regional_data です。
  - 実行するコマンドは /usr/sbin/init です。

ホストと Docker コンテナのタイムゾーンを同期する必要がある場合は、上記の Docker run コマンドに **-v /etc/localtime:/etc/localtime** オプションを追加します。

デフォルトでは、コアファイルは Docker ホストマシンの /var/lib/systemd/coredump ディレクトリにあります。**cnr_tactool** ユーティリティを使用してコアファイルを収集するには、Docker ホストマシンで次のコマンドを実行します。

```
# echo '/data/cpnr_regional_data/core.%p' > /proc/sys/kernel/core_pattern'
# ulimit -c unlimited
```

上記のコマンドを実行すると、コアファイルが /data/cpnr_regional_data ディレクトリで使用可能になり、**cnr_tactool** を使用して収集できるようになります。

- ローカルコンテナの場合：

```
# docker run -d --name cpnr_local_container --privileged=true -p 8443:8443 -p 1234:1234 -p
67:67/udp -p 53:53/udp --mount type=bind,source=/data/cpnr_local1_data,target=/var/nwreg2/local
 cpnr-local:11.1 /usr/sbin/init
```

上記のコマンドでは、次のようになります。

- Dockerのデフォルトブリッジネットワーキング ドライバが使用されます。コンテナに必要なポートが公開されます。8443 は Web UI 用、1234 はローカルの設定管理用、67 は DHCP 用、53 は DNS 用です。SNMP や TFTP などの他のサービスについては、『Cisco Prime Network Registrar 11.1 Administration Guide』の「Default Ports for Cisco Prime Network Registrar Services」の項を参照してください。
- Cisco Prime Network Registrar のデータディレクトリは /var/nwreg2/local で、ホストのマウントポイントは /data/cpnr_local1_data です。
- 実行するコマンドは /usr/sbin/init です。

ホストと Docker コンテナのタイムゾーンを同期する必要がある場合は、上記の Docker run コマンドに **-v /etc/localtime:/etc/localtime** オプションを追加します。

デフォルトでは、コアファイルは Docker ホストマシンの /var/lib/systemd/coredump ディレクトリにあります。**cnr_tactool** ユーティリティを使用してコアファイルを収集するには、Docker ホストマシンで次のコマンドを実行します。

```
# echo '/data/cpnr_local1_data/core.%p' > /proc/sys/kernel/core_pattern'
# ulimit -c unlimited
```

上記のコマンドを実行すると、コアファイルが /data/cpnr_local1_data ディレクトリで使用可能になり、**cnr_tactool** を使用して収集できるようになります。

ステップ 4 Cisco Prime Network Registrar の設定を開始します。

- リージョナルコンテナの場合：
  - Web UI を使用して接続するには、https://*hostip*:8453 を使用します。
  - CLI を使用して接続するには、次のコマンドを使用します。

    *install-path***/usrbin/nrcmd -R -C** *hostip***:1244 -N** *username* **-P** *password*

- ローカルコンテナの場合：
  - Web UI を使用して接続するには、https://*hostip*:8443 を使用します。
  - CLI を使用して接続するには、次のコマンドを使用します。

    *install-path***/usrbin/nrcmd -C** *hostip***:1234 -N** *username* **-P** *password*

DHCP フェールオーバーと HA DNS を実行する場合は、2 つ Cisco Prime Network Registrar のコンテナ（メインとバックアップ）を別々のホストで実行することをお勧めします。これにより、シングルポイント障害を回避できます。ブリッジネットワークが単一のホストに制限されている場合は、ネットワークドライバとして macvlan を使用するのが最適な選択です。macvlan では、コンテナは物理ネットワークに直接接続されているように見えます。

Docker デーモンで IPv6 が許可されている場合は、デュアルスタック macvlan ネットワーク、つまり IPv4 と IPv6 の両方を使用できます。

```
# docker network create --driver=macvlan --ipv6 --subnet=2001:db8:1:1::/64
--gateway=2001:db8:1:1::1 --subnet=10.0.0.0/24 --gateway=10.0.0.1 -o macvlan_mode=bridge
 -o parent=eth0 cpnr_macvlan
```

Cisco Prime Network Registrar コンテナを実行し、上記で作成した macvlan ネットワークに接続します。

```
# docker run -d --name cpnr_dhcp_main --network=cpnr_macvlan --ip 10.0.0.20 --ip6
2001:db8:1:1::20 --privileged=true --mount type=bind,source=/data/cpnr_dhcp_main_data,
target=/var/nwreg2/local cpnr-local:11.1 /usr/sbin/init
```

この Cisco Prime Network Registrar コンテナ（ローカル）は、10.0.0.20 および 2001:db8:1:1::20 で到達可能です。

- IPv4 経由の Web UI を使用して接続するには、https://10.0.0.20:8443 を使用します。
- CLI over IPv6 を使用して接続するには、次のコマンドを使用します。

  install-path`/usrbin/nrcmd -C [2001:db8:1:1::20]:1234 -N` *username* `-P` *password*

既存の Cisco Prime Network Registrar クラスタを Docker コンテナに移動

既存の Cisco Prime Network Registrar 9.0 以降のクラスタから Cisco Prime Network Registrar 11.1 Docker コンテナに移動するには、次の手順を実行します。

ステップ 1 Cisco Prime Network Registrar のアンインストール （45 ページ） 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。

ステップ 2 /opt/nwreg2 フォルダを削除します。アンインストール後に /var/nwreg2 フォルダを削除しないでください。

同じマシンで Cisco Prime Network Registrar 11.1 Docker コンテナにアップグレードする場合は、このステップ 3 をスキップして、ステップ 4 に進みます。

ステップ 3 別のマシンで Cisco Prime Network Registrar 11.1 Docker コンテナにアップグレードする場合は、Docker インスタンスを作成するマシン（ターゲットマシン）にソースディレクトリツリー（たとえば、ローカルクラスタの場合は /data/cpnr_local1_data、リージョンクラスタの場合は /data/cpnr_regional_data）を作成します。次に、元のクラスタの /var/nwreg2/{local | region} ディレクトリをこのディレクトリに追加します。次のコマンドを使用します。

- リージョンクラスタの場合：

```
# mkdir  -p  /data/cpnr_regional_data
# mv  /var/nwreg2/regional  /data/cpnr_regional_data
```

- ローカルクラスタの場合：

```
# mkdir  -p  /data/cpnr_local1_data
# mv  /var/nwreg2/local  /data/cpnr_local1_data
```

（注） 11.0 より前のリリースの場合は、cnr.conf ファイルを /opt/nwreg2/{local | regional}/conf ディレクトリからターゲットマシンのソースディレクトリの conf フォルダにコピーしてください。次のコマンドを使用します。

- リージョンクラスタの場合：

```
# mv /opt/nwreg2/regional/conf /data/cpnr_regional_data/conf
```

- ローカルクラスタの場合：

```
# mv /opt/nwreg2/local/conf /data/cpnr_local1_data/conf
```

ステップ 4 次のコマンドを使用して Docker インスタンスを作成します。

- リージョナルコンテナの場合：

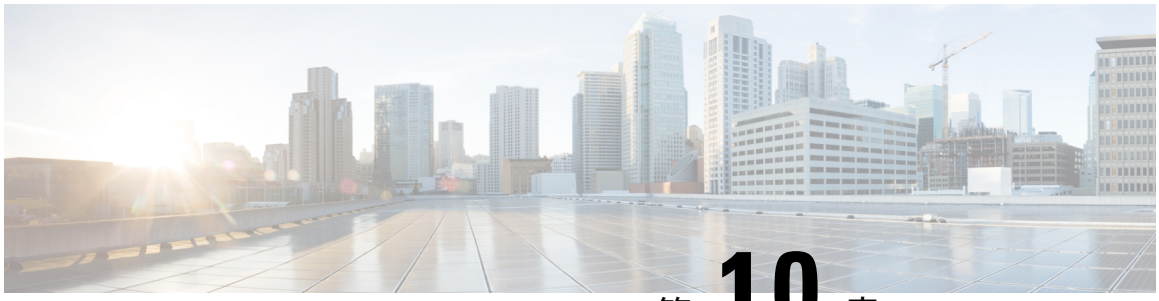
```
$ docker run -d --name cpnr_container -v /etc/localtime:/etc/localtime --network=mymacvlan
--ip hostip --ip6 ipv6address --privileged=true --hostname=hostip --mount type=bind,
source=/data/cpnr_regional_data,target=/var/nwreg2/regional cpnr_regional:11.1 /usr/sbin/init
```

- ローカルコンテナの場合：

```
$ docker run -d --name cpnr_container -v /etc/localtime:/etc/localtime --network=mymacvlan
--ip hostip --ip6 ipv6address --privileged=true --hostname=hostip --mount type=bind,
source=/data/cpnr_local1_data,target=/var/nwreg2/local cpnr_local:11.1 /usr/sbin/init
```

ステップ 5 Cisco Prime Network Registrar 11.1 サーバーで、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。また、アップグレード前のバージョンのデータベースバージョンをバックアップとして含む data.bak フォルダが作成されていることを確認します。

（注） 上記の手順を実行すると、すべての設定がデフォルトに設定され、証明書を再インストールまたはポートを変更するために追加の手順が必要になる場合があります。詳細については、独自の Web UI アクセス用証明書のインストール （35 ページ）を参照してください。



第 10 章

Kubernetes 上の Cisco Prime Network Registrar

Kubernetes は、ソフトウェアの展開、スケーリング、および管理を自動化するためのオープンソースのコンテナ オーケストレーション システムです。Cisco Prime Network Registrar 11.1 以降、次の Docker イメージを使用して Cisco Prime Network Registrar インスタンスを Kubernetes に展開できます。

- リージョンインスタンスの展開の場合：**cpnr-regional-11.1-1.el8.x86_64_rhel_docker.tar.gz**
- ローカルインスタンスの展開の場合：**cpnr-local-11.1-1.el8.x86_64_rhel_docker.tar.gz**

（注） イメージの名前は、今後のリリースで変更されます。

コンテナイメージを読み込むには、Kubernetes にプライベート Docker レジストリが必要です。

この章の内容は、次のとおりです。

Kubernetes 上で Cisco Prime Network Registrar インスタンスを展開

YAML ファイルを使用して、Kubernetes に Cisco Prime Network Registrar インスタンスを展開できます。YAML は、Kubernetes 構成ファイルで使用される標準規格です。Cisco Prime Network Registrar キット **cpnr-11.1-1.el8.x86_64_kubernetes.tar.gz** には、Kubernetes に Cisco Prime Network Registrar を展開する方法の 1 つを示す YAML ファイルの例（cpnr-local-statefulset.yaml および cpnr-regional-statefulset.yaml）が含まれています。

（注） Kubernetes 環境に Cisco Prime Network Registrar を展開するために特別なライセンスは必要ありません。既存のコンテナのライセンスを使用します。

たとえば、Cisco Prime Network Registrar キットの cpnr-local-statefulset.yaml を使用して、Kubernetes に Cisco Prime Network Registrar ローカルインスタンスを作成できます。この設定では、StatefulSet および hostNetwork の展開を使用します。この YAML を使用して作成されたインスタンスは、Cisco Prime Network Registrar ローカルインスタンスを設定済みのワーカーノードにバインドします。このインスタンスは、設定されたワーカーノードでのみ実行され、他のノードでは実行されません。

ポッドが **hostNetwork: true** で設定されている場合、ポッドで実行されているアプリケーションは、ポッドが開始されたホストマシンのネットワーク インターフェイスを直接表示できます。また、すべてのネットワーク インターフェイスでリッスンするように設定されたアプリケーションは、ホストマシンのすべてのネットワーク インターフェイスでアクセスできます。

YAML ファイルは、次の Kubernetes リソースで構成されます。

- サービス

  cpnr-local-statefulset.yaml では cpnr-local がサービス名で、ヘッドレスサービスが使用されているため clusterIp は None に設定されています。

- StatefulSet

  cpnr-local-statefulset.yaml では cpnr-local は StatefulSet 名であり、1 つのレプリカで Cisco Prime Network Registrar 11.1 Docker イメージを実行するために使用されます。

  次の 2 つの理由から、Cisco Prime Network Registrar で StatefulSet が使用されます。

  - 一定のポッド名
  - 展開を使用して作成されたポッドが削除されると、古いポッドが完全に終了する前に新しいポッドが作成されます。ホストノードの古い Cisco Prime Network Registrar プロセスが完全に終了する前に hostNetwork が使用されるため、新しい Cisco Prime Network Registrar ポッドが作成され、古いポッドの Cisco Prime Network Registrar プロセスが完全に終了しないため、新しいポッドの Cisco Prime Network Registrar サービスが停止します。

    これは StatefulSet で古いポッドが完全に終了し、新しいポッドが作成されることで解決されます。

（注） 他のネットワークモードでは HA とフェールオーバーのペアに問題があったため、Cisco Prime Network Registrar は hostNetwork を使用してテストされています。hostNetwork モードでは、ポッドが起動すると、ホストネットワーク名前空間とホスト IP アドレスを使用します。これは基本的に、ポッドがホストのすべてのネットワーク インターフェイスを認識できるということです。hostNetwork モードでは、ノードに展開できる Cisco Prime Network Registrar インスタンスは 1 つだけであるため、YAML のレプリカは 1 に設定されます。hostNetwork モードを使用して複数の Cisco Prime Network Registrar ポッドを同じノードにデプロイする場合は、ポッドごとに、すべての Cisco Prime Network Registrar 関連のポートを変更し、それに応じてレプリカを調整する必要があります。ただし、これが役に立たない場合もあります。

ステップ 1 YAML ファイルで次のパラメータを設定します。

- NODE_NAME：Cisco Prime Network Registrar インスタンスが実行されるワーカーノード名。たとえば、「cnr-k8s-worker2. *server*.com」です。**kubectl get nodes** コマンドを使用してノード名を取得します。
- IMAGE：Docker イメージの場所。たとえば、「cnr-k8s-worker1.server.com/cpnr-local:11.1」の場合、cnr-k8s-worker1. *server*.com はプライベートレジストリで、イメージ名はタグ 11.1 の cpnr-local です。
- HOST_MOUNT_PATH：ホストマシン上のディレクトリパス。このディレクトリは、Cisco Prime Network Registrar インスタンスに構成ファイルとデータを格納するために使用されます。ポッドの /var/nwreg2 は、ホストマシンの HOST_MOUNT_PATH にマッピングされます。これは、ホストマシンで Cisco Prime Network Registrar インスタンスのデータを保持するために必要です。

ステップ 2 次のコマンドを使用して、Kubernetes に Cisco Prime Network Registrar インスタンスを作成します。

- Cisco Prime Network Registrar ローカルインスタンスの展開の場合：

```
# kubectl create -f cpnr-local-statefulset.yaml
```

- Cisco Prime Network Registrar リージョンインスタンスの展開の場合：

```
# kubectl create -f cpnr-regional-statefulset.yaml
```

ステップ 3 次のコマンドを使用して、Kubernetes の Cisco Prime Network Registrar インスタンスの詳細を確認します。

```
# kubectl get all
```

ステップ 4 次のコマンドを使用して、Cisco Prime Network Registrar インスタンスポッドにログインします。

```
# kubectl exec -it <pod name> -- bash
```

次に例を示します。

```
# kubectl exec -it cpnr-dhcp-dns-0 -- bash
# /opt/nwreg2/local/usrbin/nrcmd -s
100 Ok
```

ステップ 5 ユーザー名とパスワードを設定し、ローカルポッドをリージョンポッドに登録します。

Kubernetes の Cisco Prime Network Registrar インスタンスを削除する場合は、次のコマンドを使用します。

- Cisco Prime Network Registrar ローカルインスタンスの場合：

```
# kubectl delete -f cpnr-local-statefulset.yaml
```

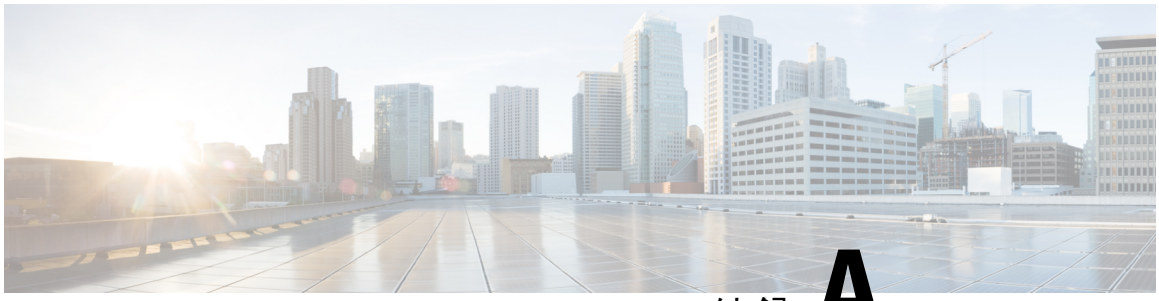
- Cisco Prime Network Registrar リージョンインスタンスの場合：

```
# kubectl delete -f cpnr-regional-statefulset.yaml
```

ポッドの障害をデバッグするには、**kubectl logs** *podname* または **kubectl describe pod** *podname* コマンドを使用します。

（注） Cisco Prime Network Registrar ポッドを別のワーカーノードに展開する場合は、YAML ファイルに変更を加える必要があります（たとえば、service.metadata.name と statefulset.metadata.name を変更する必要があります）。

（注） Cisco Prime Network Registrar 11.1 Docker イメージは、Kubernetes バージョン 1.23.5 でテストされています。使用されている CNI は Calico 3.22.0 です。テスト全体が、例として提供されている YAML ファイルを使用して実行されています。YAML ファイルを変更する場合は、実稼働に移行する前にテストする必要があります。



付録 A

ラボ評価のためのインストール

この付録の構成は、次のとおりです。

ラボ評価のためのインストール

この付録では、評価目的で小規模なテスト構成をサポートするために、単一のマシンで Cisco Prime Network Registrar のリージョナルクラスタとローカルクラスタをインストール、アップグレード、およびアンインストールする方法について説明します。

注意 単一のマシンにリージョナルクラスタとローカルクラスタをインストールするのはラボ評価のみを目的としており、実稼働環境には選択しないでください。集約されたリージョナルクラスタデータベースは、DNS サービスまたは DHCP サービスも実行しているローカルサーバで合理的に配置するには大きすぎると予想されます。空きディスク容量が不足すると、これらのサーバで障害が発生します。

ラボでの Cisco Prime Network Registrar のインストール

評価目的で単一のマシンに 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 Cisco Prime Network Registrar の 2 つの個別のインストールを格納するために十分な空きディスク容量がマシンにあるかどうかを確認します。

ステップ 2 Cisco Prime Network Registrar のインストール （25 ページ）の手順に従って、ローカルクラスタをインストールまたはアップグレードします。cpnr-local キットを使用します。

ステップ 3 同じ手順に従って、同じマシンにリージョナルクラスタをインストールまたはアップグレードします。cpnr-regional キットを使用します。

ラボインストールのテスト

インストールをテストするには、次の手順を実行します。

ステップ 1 ローカルクラスタの Web UI を起動してログインします。デフォルトでは、ローカルポート番号は HTTPS（セキュア）接続の場合は **8443** です。

ステップ 2 データをリージョナルクラスタにプルするためのテストとして、DNS ゾーンと DHCP の範囲、テンプレート、クライアントクラス、または仮想プライベートネットワーク（VPN）を追加します。

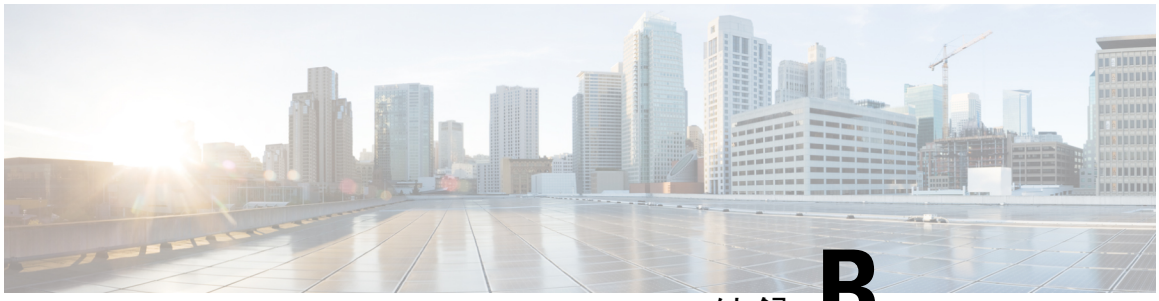
ステップ 3 リージョナルクラスタの Web UI を起動してログインします。デフォルトでは、リージョナルポート番号は HTTPS（セキュア）接続の場合は **8453** です。

ステップ 4 ローカルクラスタへのシングルサインオン接続について、リージョナルクラスタをテストします。DNS ゾーン分散、DHCP の範囲、テンプレート、クライアントクラス、または VPN をローカルクラスタからリージョナルクラスタのレプリカデータベースにプルしようとします。

ラボ環境でのアンインストール

ローカルクラスタを削除するには、Cisco Prime Network Registrar のアンインストール （45 ページ） の手順に従ってキットに cpnr-local を指定します。

リージョナルクラスタを削除するには、Cisco Prime Network Registrar のアンインストール （45 ページ） の手順に従ってキットに cpnr-regional を指定します。



付録 B

Cisco Prime Network Registrar SDK のインストール

このセクションでは、Cisco Prime Network Registrar SDK のインストール方法について説明します。SDK をインストールする前に、JDK 11 がシステムにインストールされていることを確認します。Cisco Prime Network Registrar SDK は別の製品であり、別売りです。

この付録の構成は、次のとおりです。

Cisco Prime Network Registrar SDK のインストール

Cisco Prime Network Registrar SDK 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 配布された .tar ファイルの内容を展開します。

a) SDK ディレクトリを作成します。

```
% mkdir /cnr-sdk
```

b) 作成したディレクトリに移動し、.tar ファイルの内容を展開します。

```
% cd /cnr-sdk
% tar xvf sdk_tar_file_location/cnrsdk.tar
```

ステップ 2 LD_LIBRARY_PATH と CLASSPATH の環境変数をエクスポートします。

```
% export LD_LIBRARY_PATH=/cnr-sdk/lib
% export CLASSPATH=/cnr-sdk/classes/cnrsdk.jar:.
```

（注） システムに Cisco Prime Network Registrar がインストールされている場合は、LD_LIBRARY_PATH/ に /opt/nwreg2/{local | regional}/lib を使用します。Cisco Prime Network Registrar がインストールされていない場合は、ファイルを展開した lib ディレクトリを指定する必要があります。システムがローカルまたはリージョナルクラスタとして実行されていない場合は、cpnr-client キットをインストールすることを検討してください（他のコマンドラインユーティリティにアクセスするため）。次に、LD_LIBRARY_PATH に /opt/nwreg2/client/lib を指定します。

インストールのテスト

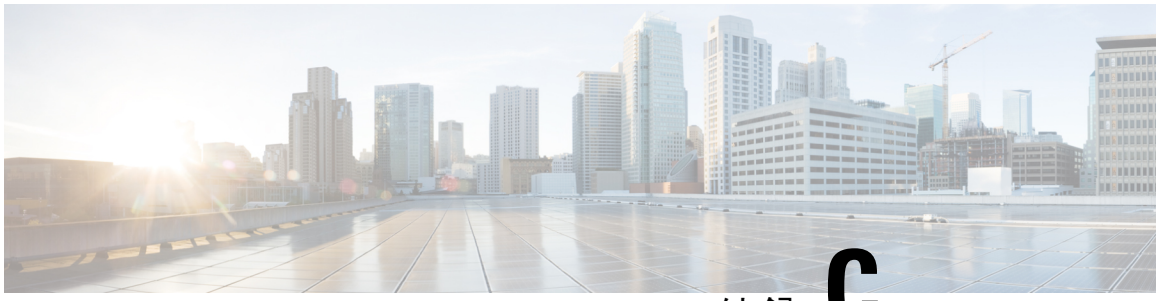
次のテストプログラムで PATH または LD_LIBRARY_PATH が正しく設定されていることを確認します。

```
% java -jar /cnr-sdk/classes/cnrsdk.jar
```

互換性に関する考慮事項

以前のバージョンの SDK で開発された Java SDK クライアントコードの場合、最新の JAR ファイルを使用してほとんどのコードを再コンパイルするだけで、アップグレードされたサーバに接続できます。

介在する Cisco Prime Network Registrar のバージョンの『*Cisco Prime Network Registrar 11.1* リリースノート』の「SDK Compatibility Considerations」の項を確認してください。これらの項は、SDK の互換性に関する重大な考慮事項を強調しています。



付録 C

Web UI のセキュリティ強化

この付録では、次の項について説明します。

Web UI のセキュリティ強化

HTTPS を使用してセキュアソケットレイヤ（SSL）プロトコルで接続すると、Web UI は Java 仮想マシン（JVM）のデフォルトの暗号を使用します。これらの暗号には通常、弱い暗号セッションキーが含まれており、システムセキュリティに影響を与える可能性があります。システムを強化する場合は、次のように暗号を調整します。

（注） Cisco Prime Network Registrar 11.1 のデフォルトのインストールは、Transport Layer Security（TLS）1.2 で動作します。必要に応じて、古い TLS のバージョンで動作するように構成を変更できます。

ステップ 1 /var/nwreg2/{local | regional}/tomcat/con フォルダにある **server.xml** ファイルを開きます。

ステップ 2 以下の推奨される sslEnabledProtocol と暗号を使用するか、セキュリティ要件に従って設定します。詳細については、オンラインで入手可能な tomcat SSL/TLS 設定ドキュメントを参照してください。

```
<Connector port="${cnrui.https.port}" protocol="com.cisco.cnr.webui.tomcat.SecureHTTP"

relaxedQueryChars='[]'

maxConnections="1024" maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false"

keystoreFile="..."

keystorePass="..."

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384,
```

Web UI のセキュリティ強化

```
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA"

compression="on"

compressionMinSize="2048"

noCompressionUserAgents="gozilla, traviata"

URIEncoding="UTF-8"

compressableMimeType="text/html,text/xml,text/plain, text/css,text/javascript,
application/x-javascript,application/javascript"

sslEnabledProtocols="TLSv1.2"/>
```

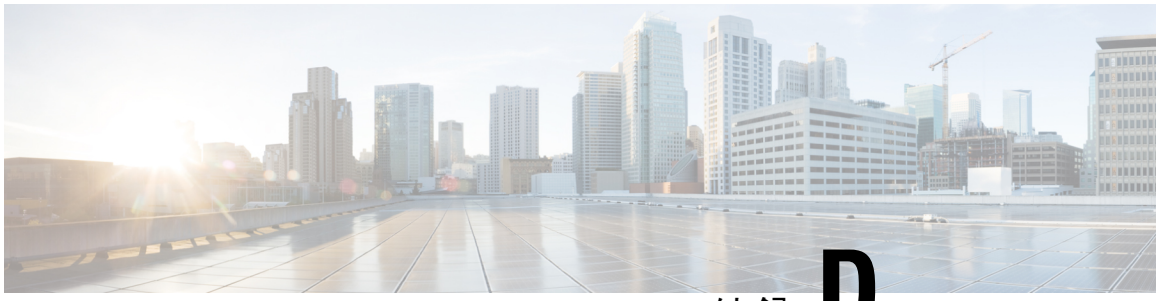
（注） **keystoreFile** および **keystorePass** の値は、インストールに固有です。これらの値は、Cisco Prime Network Registrar が起動されるたびに上書きされるため、変更しないでください。

ステップ 3 Cisco Prime Network Registrar を再起動して、変更を有効にします。

（注） Cisco Prime Network Registrar 11.1 は、以下の暗号で TLS 1.3 をサポートします。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

TLS 1.3 を利用する場合は、server.xml ファイルを適切に更新して Cisco Prime Network Registrar を再起動する必要があります。



付録 D

セキュリティ強化のガイドライン

この付録では、次の項について説明します。

セキュリティ強化のガイドライン

システムのセキュリティ強化を検討する場合は、次のセキュリティ強化ガイドラインを考慮する必要があります。

- ホストプラットフォームのセキュリティ強化ガイドを参照してください。次に例を示します。
  - RHEL/セントロス 7.x:

    https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf
  - RHEL 8.x：

    https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/Red_Hat_Enterprise_Linux-8-Security_hardening-en-US.pdf

    https://www.cisecurity.org/benchmark/red_hat_linux/
  - NSA セキュリティ強化ガイド集：

    https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

（注） 上記のリンクは外部 Web サイトを参照しており、シスコはそれらを最新の状態に保つ責任を負いません。これらは参照のためだけに提供されています。コンテンツが古い場合やリンクにアクセスできない場合は、Web サイトの所有者に連絡して最新情報を入手してください。

- Cisco Prime Network Registrar で使用されていないポートを無効化またはブロックします。Cisco Prime Network Registrar のマニュアルには、ポートの使用法と、接続追跡などのファイアウォール項目の使用に関する問題の概要が記載されています。
  - Cisco Prime Network Registrar で使用されるポートのリストについては、『Cisco Prime Network Registrar 11.1 Administration Guide』の「Default Ports for Cisco Prime Network Registrar Services」の項を参照してください。一部はデフォルトであり、インストール中または構成中に変更されている可能性があることに注意してください。
  - 接続トラッキング関連の問題については、『Cisco Prime Network Registrar 11.1 Administration Guide』の「DNS Performance and Firewall Connection Tracking」の項を参照してください。
- 製品ディレクトリ（主に /opt/nwreg2/* および /var/nwreg2/*）が適切にロックされていることを確認します。必要に応じて保護を調整する必要がある場合があることに注意してください（オフラインバックアップの実行やログの表示など）。
- DNS 固有の考慮事項には、次のようなものがあります。
  - DNS セキュリティ拡張機能（DNSSEC）の使用：

    DNSSECにより、データ出自の認証、データの完全性の確認、および認証による存在否定が可能になります。DNSSEC を使用すると、DNS プロトコルが特定のタイプの攻撃（特に DNS スプーフィング攻撃）の影響を受けにくくなります。DNSSEC は、デジタル署名を DNS データに追加することによって、悪意のある応答や偽造された応答を防ぎ、各 DNS 応答の完全性と真正性を検証できます。

    Cisco Prime Network Registrar 9.0 以前の権威 DNS サーバは、ゾーンの署名をサポートしていません。Cisco Prime Network Registrar 10.0 から権威 DNSSEC のサポートにより、DNS ゾーンに認証と完全性が付加されます。このサポートにより、Cisco Prime Network Registrar DNS サーバはセキュアゾーンと非セキュアゾーンの両方をサポートできます。詳細については、『*Cisco Prime Network Registrar 11.1* 権限のあるキャッシュ *DNS* ユーザーガイド』の「Managing Authoritative DNSSEC」の項を参照してください。
  - ACL を使用したセキュアな DNS サーバアクティビティ：
    - ゾーンクエリの制限：DNS サーバ上の *restrict-query-acl* 属性は、*restrict-query-acl* が明示的に設定されていないゾーンのデフォルト値として機能します。
    - ゾーン転送要求の制限：*restrict-xfer-acl* 属性を使用して、既知のセカンダリサーバへのゾーン転送要求をフィルタリングします。
    - DDNS 更新の制限：*update-acl* 属性を使用して、既知の DHCP サーバからの DDNS パケットをフィルタリングします。
  - TSIG または GSS-TSIG を使用したセキュアゾーン転送および DNS 更新：

    セキュア モードでのゾーン転送は、HMAC MD5 ベースの TSIG と GSS-TSIG の両方をサポートします。オプションの TSIG キーまたは GSS-TSIG キー（『*Cisco Prime Network Registrar 11.1 DHCP* ユーザーガイド』の「Transaction Security」の項または

「GSS-TSIG」の項 を参照）をプライマリサーバーアドレスに追加することができます。それには、*address–key* の形式でエントリをハイフンでつなぎます。エントリごとに、[IP キーの追加（Add IP Key]）] をクリックします。

詳細については、『*Cisco Prime Network Registrar 11.1* 権限のあるキャッシュ *DNS* ユーザーガイド』の「Creating a Zone Distribution」の項を参照してください。

- クエリ ID と送信元ポートをランダム化。
- DNS レートの制限：『*Cisco Prime Network Registrar 11.1* 権限のあるキャッシュ *DNS* ユーザーガイド』の「Managing Caching Rate Limiting」の項を参照してください。
- 再帰サーバと権威サーバの役割分担。

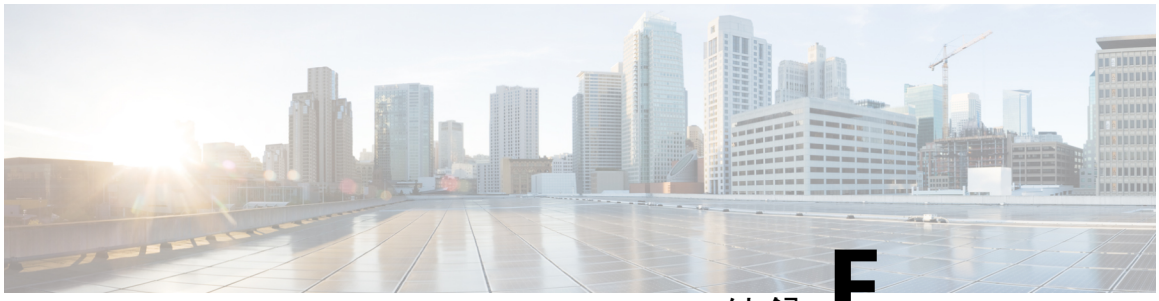
- DHCP 固有の考慮事項には、次のようなものがあります。
  - 「外部」の送信元からの DHCPv4 トラフィックと DHCPv6 トラフィックがルータでブロックされ、有効なリレーエージェントだけが DHCP サーバにパケットを転送できることを確認します。
  - スイッチで DHCP ガードおよび同様のサービスを使用します。

    https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.htmlを参照してください

    https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdfを参照してください
  - おしゃべりクライアントフィルタの使用：『*Cisco Prime Network Registrar 11.1 DHCP* ユーザーガイド』の「Preventing Chatty Clients by Using an Extension」の項を参照してください。

- 通常、Active Directory（LDAP）および RADIUS ユーザに導入できるパスワードのルール（つまり、変更頻度、長さ、および難易度のチェック）として、外部ユーザ認証の使用を検討してください。『Cisco Prime Network Registrar 11.1 Administration Guide』の「External Authentication Servers」の項を参照してください。

セキュリティ強化のガイドライン



付録 E

VM パフォーマンスの最適化

VM のパフォーマンスの最適化については、次の項を参照してください。

推奨される UCS 設定

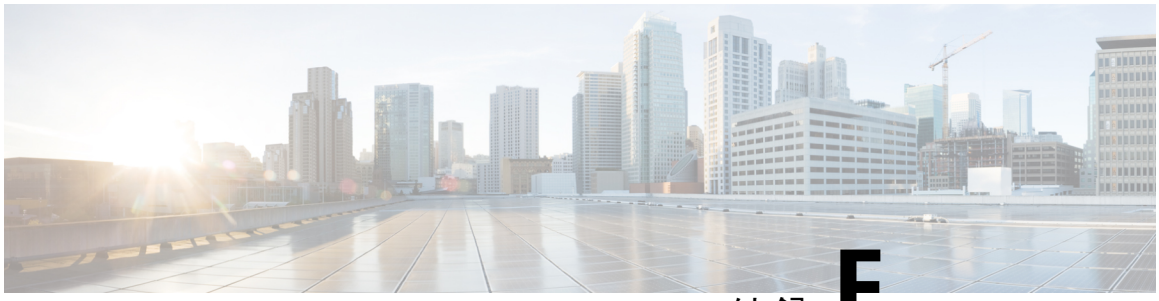
RAID が設定された UCS サーバでは、パフォーマンスを向上させるために、RAID コントローラの [要求された書き込みキャッシュポリシー（Requested Write Cache Policy）] を [ライトスルー（Write Through）] ではなく [ライトバック（Write Back）] に設定することが推奨されます（デフォルト設定）。[ライトバック（Write Back）] オプションを使用する場合の欠点は、キャッシュ内のデータがディスクに書き込まれる前にシステム障害が発生した場合に、一部のデータが失われる可能性があることです。そのため、RAID コントローラの [要求された書き込みキャッシュポリシー（Requested Write Cache Policy）] を [良好なBBUのライトバック（Write Back Good BBU）] に設定することを推奨します。このモードでは、バッテリ バックアップ ユニット（BBU）が取り付けられ、充電されると、コントローラはライトバックキャッシングを有効にします。これにより、データ保護とパフォーマンスのバランスが良くなります。

NUMA の最適化

仮想 CPU を正しく設定しないと、Non-Uniform Memory Access（NUMA）のパフォーマンスの問題が発生する可能性があります。この問題を回避するには、1 つの仮想マシンで使用する仮想 CPU が、1 つの NUMA ノードより多くならないように設定します。そうしないと、複数の NUMA ノードでスケジュールされた場合に、メモリアクセスが低下します。これは一般に、1 つの CPU ソケットの物理コアの総数よりも多くの仮想 CPU を仮想マシンに割り当てないことを意味します。

ハイパースレッディングの考慮事項

ハイパースレッディングの仮想 CPU を使用する場合、一般的な CPU 使用率は 100% ではなく 30% であることに注意してください。これは、メインスレッドが停止し、待機しているときに、他の作業を実行できるようにするためです。実際の数は、ワークロードによって異なります。



付録 F

nmcli を使用した RHEL/CentOS でのネットワークアクセスの設定

この付録では、次の項について説明します。

nmcli を使用した RHEL/AlmaLinux 8.x でのネットワークアクセスの設定

NetworkManager コマンドラインツール（**nmcli**）は、NetworkManager を制御してネットワークを設定するためのコマンドラインの方法を提供します。この項では、nmcli を使用して仮想アプライアンスでネットワークアクセスを設定する方法を学習するのに役立ついくつかの例を挙げて、概要のみを紹介します。

ネットワークインターフェイス構成の従来のアプローチとは異なり、NetworkManager は接続とインターフェイス（デバイスとも呼ばれる）の両方を処理します。接続は IP アドレス、ゲートウェイ、DNS サーバで設定され、インターフェイス（デバイス）に適用されます。

一般的に役立つ 2 つの nmcli コマンドがあります。

- **nmcli d** コマンドは、使用可能なすべてのネットワークインターフェイス（デバイス）を一覧表示します。
- **nmcli c** コマンドは、使用可能なすべての構成を一覧表示します。

nmcli を使用するようになるにしたがい、上記の 2 つのコマンドを頻繁に使用します。

仮想アプライアンスのインターフェイスの IP アドレスを設定するには、次のステップに従います。通常、これらのコマンドは仮想アプライアンスのコンソールに直接入力します。すでにネットワーク経由で接続している場合（たとえば **ssh** を使用）、ネットワークインターフェイスの構成を変更すると、プロセスの任意の時点でネットワーク接続が失われる可能性があるため、問題が発生することがあります。

nmcli を使用した RHEL/CentOS でのネットワークアクセスの設定

ステップ 1 インターフェイスが nmcli をブロックしていないことを確認します。**nmcli d** コマンドは、既存のインターフェイスを一覧表示します。設定するインターフェイスが**管理対象外**としてリストされている場合、NetworkManagerはこのインターフェイスの設定を明示的にブロックされています。このブロックを解除するまで、nmcliコマンドはこのインターフェイスに影響を与えません。インターフェイスが**管理対象外**として記載されている場合を除き、この手順を実行する必要はありません。NetworkManagerで管理できるようにするには、次のステップに従います。

a) ファイル **/etc/sysconfig/network-scripts/ifcfg-***interface* から NM_CONTROLLED-no 行を削除します。ここで、*interface* は **nmcli d** コマンドにリストされているインターフェイス名です。この名前のファイルがない場合は、この手順を実行する必要はありません。

b) 次のコマンドを使用して、構成ファイルを再度読み取るように NetworkManager に指示します。

```
nmcli connection reload
```

（注） **ifcfg** ファイルへの手動変更は、**nmcli connection reload** コマンドが発行されるまで NetworkManager によって通知されません。

ステップ 2 設定するインターフェイスの現在の構成がないことを確認します。作成した構成をインターフェイスのデフォルトにし、インターフェイスに複数の設定が関連付けられている場合は、システムの再起動時に混乱が生じる可能性があります。**nmcli c** コマンドは、既存の構成を一覧表示します。既存の構成がある場合は、それらを調べて、設定するインターフェイスに適用されるかどうかを確認します。これを簡単に行う方法は、次のコマンドを使用することです。

```
nmcli con show config | grep interface
```

出力が表示された場合は、次のコマンドを使用して構成 *config* を削除する必要があります。

```
nmcli con delete config
```

（注） 多くの場合、「Wired connection 1」という構成を削除する必要があります。

ステップ 3 構成を作成し、1 つのコマンドでインターフェイス（デバイス）に関連付けます。このコマンドは、構成を作成してインターフェイスに関連付けるだけで、インターフェイスには適用されません。

```
nmcli con add type ethernet con-name config ifname interface ip4 ip/netmaskwidth gw4 gateway
```

ここで、*config* は構成の名前であり、任意（インターフェイスの名前を含む）です。*interface* はインターフェイス（デバイス）の名前、*ip* は IPv4 アドレス、*netmaskwidth* はネットワークマスクの幅、*gateway* は IPv4 ゲートウェイアドレスです。

例（1 行ですべて入力）：

```
nmcli con add type ethernet con-name my-office ifname ens160 ip4 10.10.24.25/24 gw4 10.10.20.174
```

ステップ 4 インターフェイス（デバイス）の構成に DNS サーバを追加します。

```
nmcli con mod config ipv4.dns dnsip
```

dnsip は DNS サーバの IPv4 アドレスで、*config* は構成の名前です。

次に例を示します。

```
nmcli con mod my-office ipv4.dns 72.63.128.140
```

次の 2 つの DNS アドレスを追加できます。

nmcli を使用した RHEL/CentOS でのネットワークアクセスの設定

```
nmcli con mod my-office ipv4.dns "72.63.128.140 72.63.111.120"
```

（注） これにより、以前に設定された DNS サーバが置き換えられます。以前に設定された DNS エントリに追加するには、次に示すように ipv4.dns の前に + を付加します。

```
nmcli con mod test-lab +ipv4.dns "72.63.128.140 72.63.111.120"
```

ステップ 5 インターフェイスに構成を適用します。インターフェイスがまだ実行されていない場合は、インターフェイスがアップします。

```
nmcli con up config
```

ここで、*config* は構成の名前です。

ステップ 6 接続に関する情報を調べるには、次のコマンドを使用します。

```
nmcli -p con show config
```

これは通常、コンソール画面をスクロールして、最初の部分を読み取れないようにします。前後に移動して出力を簡単に確認できるようにするには、次のコマンドを使用します。

```
nmcli -p con show config | less
```

これから、構成全体を確認できます。次のコマンドを使用して、構成の内容を変更できます。

```
nmcli con mod config something.other new-value
```

次に例を示します。

```
nmcli con mod my-office wifi-min.key-cntl wpa-psk
```

ステップ 7 **set-hostname** コマンドを使用して、システムのホスト名を設定します。

```
hostnamectl set-hostname hostname.domain
```

（注） これは、ローカルをリージョナルに登録する前に行う必要があります。それ以外の場合は、「localhost」がすでに存在するというエラーが発生します。

ここで、*hostname* は使用するホスト名、*domain* はドメイン名で .com や .org などで終わります。これは、DNS ルックアップのデフォルトとして使用されるため、ドメイン名を（.com、.org、または適切な末尾に加えて）含めることが重要です。

次に例を示します。

```
hostnamectl set-hostname my-server.gooddomain.com
```

ステップ 8 ネットワークを設定した後、Cisco Prime Network Registrar を再起動して、インターフェイスが Cisco Prime Network Registrar によって正しく検出されるようにする**必要があります**。再起動するには、次のコマンドを使用します。

- ローカルクラスタの場合：

```
# systemctl restart nwreglocal
```

- リージョンクラスタの場合：

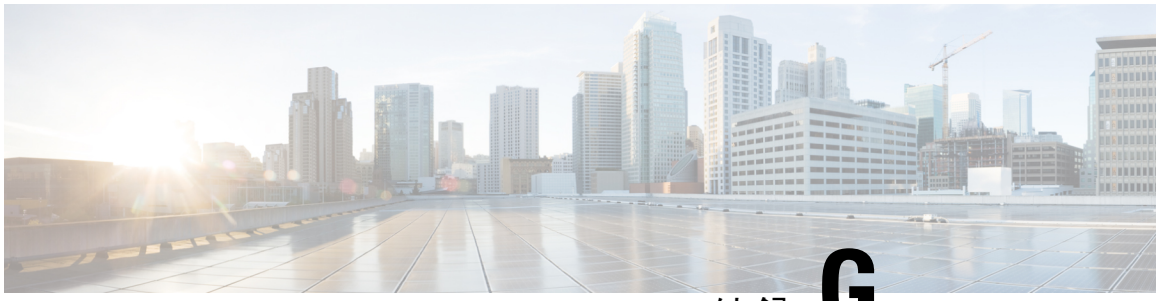
```
# systemctl restart nwregregional
```

nmcli を使用した RHEL/CentOS でのネットワークアクセスの設定

再起動に失敗すると、リージョナルでの登録が誤って設定されます。

---

nmcli の使用方法を完全に理解するには、nmcli と AlmaLinux 8.x のオンラインリソースでインターネットを検索してください。



付録 G

権威 DNS のキャパシティとパフォーマンスのガイドライン

この章では、権威 DNS のキャパシティと Cisco Prime Network Registrar のパフォーマンスのガイドラインに関する情報を提供します。

DNS システムのデプロイメント上の制限

Cisco Prime Network Registrar では、権限 DNS システムの最大構成サイズについて次の推奨事項があります。次の推奨事項は、Cisco Prime Network Registrar の権威 DNS サーバ（プライマリサーバ、プライマリ HA サーバ、またはセカンダリサーバ）に基づいています。冗長 DNS アーキテクチャには、すべて同じデータを処理するこれらのタイプのサーバが複数含まれます。したがって、新しいサーバのセットを導入することで、キャパシティを水平方向に拡張できます。これらの推奨事項は、DNS 展開が適切に機能するためのガイドラインです。

（注） DNSSEC 対応ゾーン（Cisco Prime Network Registrar 9.1 以降のバージョン）には、ゾーン内の RR の数を大幅に増やす自動生成 RR が含まれます。

- 権威 DNS サーバ（プライマリサーバ、HA ペアサーバ、またはセカンダリサーバ）あたり最大 2,500 万 RR、理想的にはゾーンあたり 200 万 RR を超えないようにします。複数の DNS プライマリサーバは、より多くの RR を必要とする展開に使用できます。
- 権威 DNS サーバ（プライマリサーバ、HA ペアサーバ、またはセカンダリサーバ）あたり最大 10000 ゾーン。複数の DNS プライマリサーバは、より多くのゾーンを必要とする展開に使用できます。
- プライマリサーバまたは HA ペアサーバあたり最大 4 台のセカンダリサーバ。

- 最大 2 階層のセカンダリサーバ（第 1 階層のセカンダリサーバと第 2 階層のセカンダリサーバ）。
- 第 1 階層のセカンダリサーバあたり最大 2 台の第 2 階層のセカンダリサーバ。

DNS データベースアーキテクチャ

権威 DNS サーバは、インメモリキャッシュとオンディスクデータベースの組み合わせを使用して、権威 RR データを保存および維持します。サイジングを目的として、各 RR には RR キャッシュ用に 300 バイトのメモリ、RR DB 用に 300 バイトのディスク容量が必要であると想定しています。CSET DB は RR セットへの変更を記録するため、各 RR のディスク容量の要件が高くなりますが、これらの変更はゾーンごとに保持される変更履歴の数に制限されます。

RR DB

- DNS サーバで設定されたゾーンのすべての RR（保護および非保護）を保存するデータベース。
- プライマリ DNS サーバでは、RR データの編集は、管理操作（つまり、RR の追加）、または DNS の更新とゾーンのスカベンジングによって RR DB に書き込まれます。セカンダリでは、RR DB はゾーン転送によって書き込まれます。
- RR DB はすべての ADNS サーバ（プライマリ/セカンダリ）に必要です。

RR キャッシュ

- RR DB データのサブセットを保存する（名前セット全体を保存する）ことで、クエリのパフォーマンスが向上します。
- 最もアクティブな RR データは、DNS クエリ処理によって生成された RR DB ルックアップの一部として、RR キャッシュに動的に保存されます。
- RR キャッシュのメモリフットプリントは、設定可能な DNS サーバ属性（*mem-cache-size*）によって制限されます。最大キャッシュサイズに達すると、DNS サーバは古いエントリをキャッシュから削除して、新しいエントリ用のスペースを確保します。各RR では、約 300 バイトのメモリが必要です。
- DNS サーバのリロードや再起動により、RR キャッシュが削除されます。サーバが再起動すると、クエリトラフィックに基づいて再構築されます。
- RR キャッシュは、すべての ADNS サーバ（プライマリ/セカンダリ）に必要です。

CSET DB

- 増分ゾーン転送要求（IXFR）に応答するために必要な RR 変更（追加、削除、保護の変更、および更新）を保存するデータベース。
- RR 変更は最初に RR DB に保存され、次に CSET DB に保持されます。

- 増分ゾーン転送を処理する必要がない DNS サーバ（つまり、アウトバウンド IXFR を送信しないセカンダリサーバ）の場合は、永続的な変更セット（*csetdb-persist-csets*）を無効にすることで、サーバのパフォーマンスを向上させることができます。デフォルトでは、変更は CSET DB に自動的に保持されます。
- DNS は、制限された設定可能な変更数（*csetdb-htrim-max-cset-kept*）のみを維持し、最大数に達すると自動的にエントリをトリミングします。トリミングは、データベースサイズの制限に役立ちます。DNS アップデートを使用する環境では、フルゾーン転送を回避するために、保持する変更の数を増やすことを推奨します。
- CSET DB が削除されると、DNS サーバは空のデータベースを作成し、新しいゾーンの履歴データがデータベースに入力されるまでフルゾーン転送（AXFR）で応答します。

HA DB

- DNS HA ペアに関するステート情報と、通信中断中またはパートナーダウンイベント時の RR 変更に関するデータを保存するデータベース。
- プライマリ HA DNS サーバ（メインおよびバックアップ）にのみ適用されます。
- HA DB が削除されると、HA 同期によってすべてのゾーンデータが HA メインから HA バックアップにプッシュされます。

DNS システムのサイジング

Cisco Prime Network Registrar の DNS 展開は、RR とゾーンの数、DNS 更新アクティビティ、および停止中または更新中のリカバリ時間に応じて、小規模、中規模、または大規模に分類できます。ゾーンの数は、展開のサイズに影響を与える可能性があります。主に RR の数が決定要因となります。また、DNS 展開に多数の RR やゾーンが必要な場合は、複数の DNS 展開を使用することを推奨します。理想的には、関連するゾーンと RR が一緒に設定されるようにデータを適切に分離します。

（注） 権威 DNS システムを適切に機能させるには、システムのディスク容量とメモリを監視することが重要です。権限のある DNS サーバのメモリが不足すると、クラッシュします。ディスク容量が不足すると、要求を処理できなくなり、データベースが破損して使用できなくなる可能性があります。

DNS 展開のリージョン管理

リージョナルサーバは、すべての Cisco Prime Network Registrar ローカルクラスタのライセンス管理を提供し、Cisco Prime Network Registrar の DNS 展開の集中管理と複製を可能にします。リージョン DNS クラスタ管理を使用する場合は、次の推奨事項に従ってシステムのサイジングと構成を調整します。

権威 DNS のキャパシティとパフォーマンスのガイドライン

- 4 CPU 以上
- 8 GB 以上の RAM
- ディスク容量は、少なくとも、すべての管理対象DNS（メイン）のプライマリクラスタにおけるディスクサイズの合計である必要があります。
- 大規模な DNS 展開では、保護されていない RR の複製を無効にする必要があります（*poll-replica-rrs*）。

小規模な展開

- 1 ー 1000 の RR と 1 ー 100 のゾーン。
- 主に静的データ。ゾーンの編集は、主に管理者が行います。
- 通常、1 つのプライマリサーバとセカンダリサーバで構成されます。
- DNS キャッシングサーバは不要であるか、ハイブリッドモードで処理できます。
- DNSは、実稼働環境にほとんど影響を与えずに、数分以内にシャドウバックアップから復旧できます。
- 2 CPU 以上
- 4 GB 以上の RAM
- 10 GB 以上のディスク容量

中規模な展開

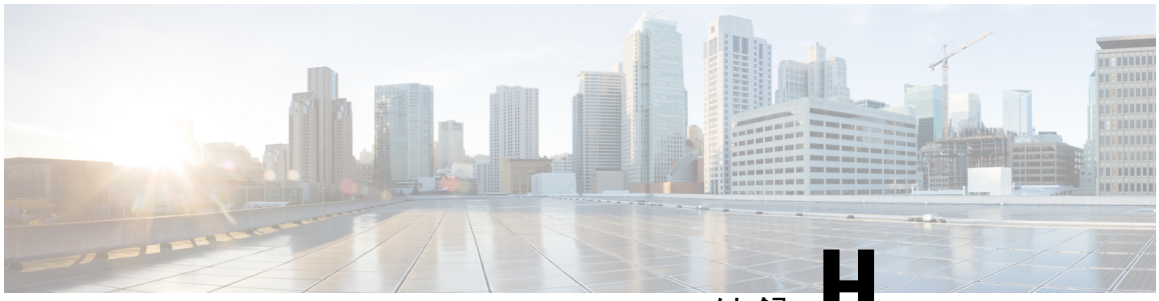
- 1000 ー 100,000 の RR および 100 ー 1000 のゾーン。
- 静的データと動的データがかなり均等に混合しており、1 秒あたり 100 回以下の更新が可能です。
- 通常、1 つのプライマリと 2 つから 4 つのセカンダリで構成されます。
- 通常、2 台から 4 台の DNS キャッシングサーバで構成されます。DNS キャッシングサーバは、別のマシンまたは VM に展開する必要があります。
- DNSは、実稼働環境への影響を最小限に抑えながら、1時間以内にシャドウバックアップから復旧できます。
- 4 CPU 以上
- 8 GB 以上の RAM
- 25 GB 以上のディスク容量。プライマリでは、変更セットの保持数（*csetdb-htrim-max-cset-kept*）を増やす必要があります。この値は、システムで処理されるDNS の更新回数によって異なりますが、1000 ー 5000 の範囲で指定する必要があります。

権威 DNS のキャパシティとパフォーマンスのガイドライン

大規模な展開

- 100,000 ー 25,000,000 の RR と 1000 ー 10,000 のゾーン
- 動的データは、データの大部分を占め、1 秒間に数千回の更新が行われます。
- 通常、2 つのプライマリ（DNS HA ペア）と 4 つのセカンダリで構成されます。
- 通常、4 台以上の DNS キャッシングサーバで構成されます。
- DNS リカバリは複雑で、メンテナンス期間中に行う必要があります。DNS サーバは、シャドウバックアップからの復旧に 1 時間以上かかることがあります。
- 8 CPU 以上
- 16 GB 以上の RAM。DNS RR キャッシュメモリのサイズ（*mem-cache-size*）を増やす必要があります（RR あたり約 300 バイト、ただし 2,000,000 KB を超えないようにする）。
- 100 GB 以上のディスク容量。プライマリでは、変更セットの保持数（*csetdb-htrim-max-cset-kept*）を増やす必要があります。この値は、システムで処理される DNS の更新回数によって異なりますが、5000 ー 10,000 の範囲で指定する必要があります。

権威 DNS のキャパシティとパフォーマンスのガイドライン



付録 H

キャッシング DNS のキャパシティとパフォーマンスのガイドライン

この章では、キャッシュ DNS のキャパシティと Cisco Prime Network Registrar のパフォーマンスのガイドラインに関する情報を提供します。

DNS システムのデプロイメント上の制限

Cisco Prime Network Registrar では、キャッシング DNS システムの最大構成サイズについて次の推奨事項があります。冗長 DNS アーキテクチャには複数のサーバが含まれるため、新しいサーバを追加することでキャパシティを水平方向に拡張できます。Cisco Prime Network Registrar は多くの構成オブジェクトに厳しい制限を設けていませんが、これらの推奨される最大値は、DNS 展開が適切に機能することを保証するためのものです。

- 最大 100 の DNS ビュー
- 最大 500 の例外とフォワーダ
- 最大 3 つの DNS RPZ ファイアウォールオブジェクト。RPZ ゾーンには何千ものエントリが存在する可能性があることに注意してください。
- 各ドメインが 200 以下の最大 12 の DNS ファイアウォールオブジェクト（非 RPZ）
- 最大 30 の DNS64 オブジェクト

（注） メンテナンスまたは停止のために 1 つ以上のサーバーが使用できない状況を考慮して、残りの稼働中のシステムが負担しなければならない追加の負荷に対応するために、展開アーキテクチャに余剰容量を含めることを推奨します。展開する余剰容量またはバックアップシステムの数は、達成したい冗長性のレベルによって異なります。少なくとも n+1 の冗長性が推奨されます。

キャッシング DNS システムのサイジング

Cisco Prime Network Registrar のキャッシング DNS 展開は、サーバの数とクエリの負荷に応じて、小規模、中規模、または大規模に分類できます。次の項では、展開サイズに基づいてキャッシング DNS サーバをプロビジョニングする方法について説明します。

（注） DNS システムを適切に機能させるには、システムのディスク容量とメモリを監視することが重要です。

小規模な展開

- 通常、2 台ー 4 台の DNS キャッシングサーバで構成されます。DNS キャッシングサーバは、ハイブリッドモードを使用して DNS 権威サーバと同じ場所に配置できます。
- 通常、1 秒あたり 1,000 クエリ未満
- 2 CPU 以上
- 4 GB 以上の RAM
- 10 GB 以上のディスク容量

中規模な展開

- 通常、2 台ー 4 台の DNS キャッシングサーバで構成されます。DNS キャッシングサーバは、別のマシンまたは VM に展開する必要があります。
- 通常、1 秒あたり 1,000 ー 50,000 クエリ
- 4 CPU 以上
- 8 GB 以上の RAM
- 25 GB 以上のディスク容量

大規模な展開

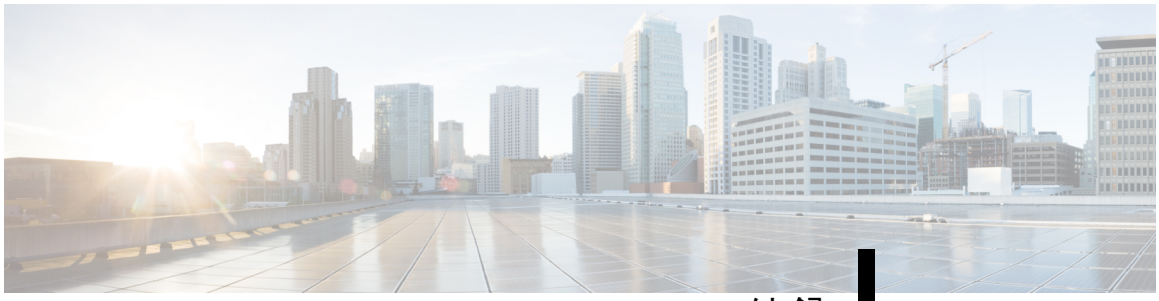
- 通常、4 台以上の DNS キャッシングサーバで構成されます。

- 通常、1 秒あたり 50,000 件を超えるクエリ
- 8 CPU 以上
- 16 GB 以上の RAM。キャッシュ DNS の RR キャッシュ設定は、*msg-cache-size* および *rrset-cache-size* であり、両方とも 4,294,967,295 バイトに増やすことができます。
- 50 GB 以上のディスク容量

キャッシング DNS サーバのパフォーマンスへの影響の可能性

次に、パフォーマンスに影響を与える可能性がある一般的なシステムコンポーネントと、Cisco Prime Network Registrar の構成のリストを示します。

- ファイアウォールおよび接続の追跡は、特にファイアウォールが大量の DNS トラフィックをドロップする可能性がある中規模から大規模の展開で、パフォーマンスに悪影響を及ぼすことがあります。
- 過剰なロギング：有効にするログ設定、パケットロギング、またはデバッグロギングが多すぎると、サーバのパフォーマンスが低下する可能性があります。
- IPv4 も使用するように設定された IPv6 専用ネットワーク。失敗した IPv4 通信でサーバがサイクルを無駄にしないように、IPv6 ネットワークは IPv6 専用モードで設定する必要があります。



付 録

DHCP のキャパシティとパフォーマンスのガイドライン

このセクションでは、DHCP のキャパシティと Cisco Prime Network Registrar のパフォーマンスのガイドラインに関する情報を提供します。

この項の目的は、サーバのキャパシティとパフォーマンスに影響を与える要因を理解し、製品の展開方法や、これらのシステムのハードウェアを購入する際に考慮すべき事項を計画することです。

複数のクラスタが仮想マシンで実行されている場合、基盤となる物理ハードウェアは、個々の仮想マシン要件の合計以上である必要があります。また、高可用性ソリューション（つまり、HA-DNS フェールオーバーまたは DHCP フェールオーバー）では、両方のパートナーを仮想環境の同じ物理マシン上に配置しないことにも注意が必要です。これにより、ハードウェアが単一障害点になります。

（注） 実際のパフォーマンスは実稼働展開の違いによって異なる場合があるため、これらは単なるガイドラインです。

- ローカルクラスタの DHCP の考慮事項 （99 ページ）
- リージョナルクラスタの DHCP の考慮事項 （105 ページ）

ローカルクラスタの DHCP の考慮事項

DHCP のキャパシティに関する 2 つの一般的な質問があります。

1. 1 台のサーバにいくつのリースを設定できますか。
2. サーバに n 個のリースを配置する場合、どのようなサーバを購入する必要がありますか、または仮想マシンを設定する必要がありますか。

単一サーバで許可されるリースの数

サーバのキャパシティについて説明する場合、サーバがサポートできる1秒あたりのDHCP操作の数が最も重要な問題です。サーバがサポートする必要がある1秒あたりの操作に影響する2つの条件があります。

- **安定状態**：リースを更新する既存のDHCPクライアントと、以前はサーバで認識されていなかったDHCPクライアントの到着で構成されます。
- **アバランシェ**：多数の（場合によっては膨大な）既存のDHCPクライアントで構成され、すべてDHCPサーバでアドレスを取得するために競合します。この状況は、障害後の電源復旧や、多くのお客様のデバイスの一括リセットで発生する可能性があります。これは多くの場合、DHCPサーバから同時にIPアドレスを取得しようとする何万ものDHCPクライアントで構成されます。IPアドレスを取得しようとする何十万ものDHCPクライアントが存在することもあります。

安定状態では、DHCPクライアントの数とクライアントに付与されるリースのリース時間が負荷の大半を占めます。

DHCPクライアント群に必要な1秒あたりの操作は、その群に付与されるリース時間（有効期限と更新時間の両方）に加えて、そのクライアント群のサイズによって大きく左右されます。これらの値はすべて設定可能であるため、実際の要件は大幅に異なる場合があります。

次の表に、さまざまなクライアント群と異なるリース時間に必要な1秒あたりの操作数を表すこれらのデータポイントの範囲を示します。

表 *5:* クライアントのリース時間

1秒あたりの操作						
	クライアントのリース時間					
アクティブなリース	30分	1時間	1日	1週間	2週間	30日間
1,000	1	1	-	-	-	-
10,000	11	6	-	-	-	-
100,000	111	72	2	-	-	-
500, 000	556	278	12	2	1	-
1,000,000	1,111	556	23	4	2	1
1,500,000	1,667	833	35	5	2	1
2,000,000	2,222	1,111	46	7	3	2
4,000,000	4,444	2,222	93	13	7	3
6,000,000	6,667	3,333	139	20	10	5

DHCP のキャパシティとパフォーマンスのガイドライン

クライアントに付与されるリース時間は、DHCP サーバで必要な 1 秒あたりの安定状態操作に大きな影響を与えます。既存のリースを持たないクライアントのリース時間はフェールオーバーの最大クライアントリードタイム（MCLT）によって制限され、他の操作（「不良」クライアントやリースクエリ要求など）がある場合もあるため、サーバの操作にはリース時間が混在する可能性があります。

DHCPサーバは、クライアントに負荷がかかるどのような状態でも崩壊しませんが、数万または数十万のクライアントを処理するのに数秒から数分かかることがあります。このため、安定状態でサーバがサポートする必要がある1秒あたりの操作に関する推奨事項は、サーバが最終的なアバランシェを処理するための十分な余裕を持てるように、低い数値になる傾向があります。

1 秒あたりの DHCP 操作

DHCP サーバのパフォーマンスのこの側面には多くの要因が関係しているため、DHCP サーバが DHCP クライアントに提供できる 1 秒あたりの操作に関する具体的な推奨事項を提示することは困難です。

シスコがラボで DHCP サーバのパフォーマンスを測定したところ、1 秒あたりの操作は 20,000 回をはるかに超えています。ただし、これは最大のパフォーマンス（フェールオーバーなし、ロギングなし、リース履歴なし、拡張なし、LDAP なし）のために特別に設定された DHCP サーバでした。DHCPサーバで設定するほとんどすべての機能は、ある程度のパフォーマンスの低下を生じさせます。多くの場合は、以前のパフォーマンスよりも 10% 程度減少します。たとえば、LDAPルックアップやプライム ケーブルプロビジョニング（PCP）製品での実行などの一部の機能は、パフォーマンスに大きく影響する可能性があります。LDAPルックアップまたは DPE との PCP インタラクションには、着信 DHCP 要求を処理する前に、別のサーバとのインターロックとそれに伴うラウンドトリップ遅延を必要とするためです。フェールオーバーには少なくとも 10% のコストがかかります。基本的なロギングには、パフォーマンスの 10% 以上のコストがかかることもあります。拡張には、単に拡張機能を呼び出すための一定のオーバーヘッドに加えて、予測不能なコストがかかります。拡張に費やされる時間も、すべての DHCP 要求の処理にかかる時間に同期して加算されます。

これらすべての結果として、特定のソフトウェア構成で特定のハードウェア構成を実行している場合に、特定の負荷に対してDHCPサーバが提供できる1秒あたりの操作を合理的に予測する方法がなくなります。

また、DHCP クライアントからの DHCP RENEW 要求を処理するための一定の要件（「安定状態」）によって、DHCPサーバにかかる1秒あたりの操作の負荷は、数千から数万までのDHCPクライアントが短時間でDHCPサーバからサービスを取得しようとする、大規模な「アバランシェ」負荷を処理するための要件によって影がうすくなることがよくあります。これらのイベントは、DHCP クライアント間での停電またはネットワーク要素のリセットによって生成され、何千もの DHCP クライアントが IP アドレスの再検出や再送信要求を行うように誘導します。DHCP サーバは、これらの負荷を処理できる必要があります。通常は、安定状態の RENEWAL トラフィックによって生成される負荷を軽減します。

異常な状況でDHCPサーバに提供されるアバランシェ負荷を処理するためのヘッドルームを確保するためにも、シスコはDHCPサーバの安定状態の負荷を1秒あたり数百の操作に制限することを推奨します。高性能のハードウェアと優れた監視体制を備え、1 秒あたり数百の操作、

DHCP のキャパシティとパフォーマンスのガイドライン

場合によっては一定の負荷でそれ以上の操作を実行するお客様もいます。これらは、各サーバのアクティブリースの数を制限することで、アバランシェ負荷のサイズが大きくなりすぎないように注意していることもあり、正常に実行されています。

DHCPサーバには、サーバの負荷を軽減し、特にアバランシェ状態の場合に、可能な限り迅速に要求に対応できるようにするいくつかの機能があります。

- **リース延長の延期**

  デフォルトでは、クライアントが予想される更新時期よりも前にクライアントが「更新」した場合、サーバはクライアントへのリースの延長を保留します。これは、多数のクライアントがディスク書き込み（およびフェールオーバー更新）の必要性を回避するため、通常、それがトリガーされた停止が短かった（リース時間の 1/2 未満）場合に、アバランシェで役立ちます。

- **過負荷時のロギングの削減**

  デフォルトでは、使用中の要求バッファが設定されたバッファの 67% を超えると、サーバはロギングを削減します。ロギングは高コストになる可能性があるため、非常にビジーな場合にサーバが追加のキャパシティを処理できるようにします。この機能は無効にできます。サーバが負荷を軽減できる唯一の方法であり、クライアントが要求を再送信するため、アバランシェ状態でサーバが要求をドロップすることが予期されることに注意してください。安定している状態でサーバが頻繁に要求をドロップする場合は、負荷を処理できないことを示していると考えられます。

- **おしゃべりクライアントフィルタ**

  すべてのサービス プロバイダー ネットワークで、この提供された拡張機能を使用することを強く推奨します。この拡張機能は、クライアントのアクティビティを監視し、「おしゃべり」と見なされるクライアントをブロックします。一旦ブロックされたクライアントが沈静化すると、ブロックが解除されます。多くのサービス プロバイダー ネットワークでは、おしゃべりクライアントフィルタによってサーバへの要求を約 50% 削減できます。ただし、おしゃべりクライアントフィルタは慎重に調整する必要があり、トラフィックパターンが変更されていないことを確認するために定期的に調整を見直す必要があります。詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザーガイド』の「*Preventing Chatty Clients by Using an Extension*」の項を参照してください。

- **識別レートリミッタ**

  識別レートリミッタは、すべての RENEW 要求を受け入れながら、DISCOVER 要求と SOLICIT 要求のレートを制限することで、サービスネットワークの停止後のダウンタイムを短縮します。基本的な概念は、リースを提供されたクライアントがそのリースの取得を完了できることを保証することです。詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザーガイド』の「*Setting Advanced DHCP Server Attributes*」の項を参照してください。

DHCP のキャパシティとパフォーマンスのガイドライン

サーバで必要なリースの数

負荷が 1 秒あたりの安定状態の操作だけである場合は、上記の表を見て、1 週間のリース時間で、1,200 万または 2,400 万のリースで問題が発生しないことを想像できます。ただし、他にも次のような要因があります。

- **アバランシェ負荷**：サーバのリースの合計数に応じて増減する場合があります。
- **リロード時間**：サーバは、リロードされるたびにインメモリキャッシュを更新する必要があります。リロード時間は、サーバ内のアクティブリースの数に比例します。
- **サービス中断の影響**：最初に数百万のリースがある場合は、DHCP クライアントと何らかの顧客との間に関係がある可能性があります。DHCP フェールオーバーペア全体のサービスが数時間停止すると、ビジネスに許容できないリスクが生じる可能性があるため、通常は DHCP サーバに多数のリースが存在しないようにする必要があります。DHCP フェールオーバーはほとんどすべてのサービスの中断を防ぎ、シングルポイント障害がない可能性がありますが、同時に 2 つの障害が発生することもあります。DHCP フェールオーバーペアの両方のサーバでしばらくの間、障害が発生する可能性があります。万が一、これが発生した場合は、1 台のサーバに 200 万台の DHCP クライアントが存在するか、1 台のサーバに 1,000 万台の DHCP クライアントが存在するかの違いが非常に重要になる可能性があります。適度な DHCP リース時間では、フェールオーバーペアがサービスを停止する時間ごとにリースが使用不可になるのは、DHCP クライアントのごくわずかな割合です。

推奨事項

単一の DHCP サーバ（またはサーバフェールオーバーペア）のアクティブリースの合計数を 600 万に制限することを強く推奨します。さらに、アバランシェやその他の例外的な状態を処理するのに十分な帯域幅を確保するために、安定状態における 1 秒あたりの操作の要件を 1 秒あたり 500 操作に制限することを強く推奨します。

ある時点を超えて、スケールアップではなくスケールアウトします。

1 つの DHCP サーバまたはフェールオーバーペアに膨大な数のリースをロードする代わりに、リース数を適度な数（たとえば、300 万から 500 万）に抑えることを検討してください。シスコのリソース制限により、警告レベルは 600 万リースに設定されており、将来の増加に対応するために、サーバあたり 400 万リース以上のように設定することをお勧めします。複数のフェールオーバーペアを管理することは、1 つのフェールオーバーペアを管理するよりも手間がかかりますが、300 万リースから 400 万リースが適度にロードされたサーバの管理が容易なことは、長期的な利益をもたらします。サーバペア全体に数時間障害が発生するという万が一の事態には、当然ながらビジネスに影響を及ぼします。

要求遅延

DHCP サーバの設計は、多数の要求に迅速に応答するように最適化されており、各要求の遅延が最小になるように最適化されているわけではないことに注意してください。これは、いくつかの同時要求によるサーバのパフォーマンスが実際の処理能力を示していない可能性があるため、スケールのテストを複雑にすることがよくあります。

サーバに関する考慮事項

多くの操作を必要とせず、サーバのリース数も少ない場合、どのようなサーバ構成でも可能です。この説明では、可能な限り最大のパフォーマンスを得ることを想定しています。

DHCP の場合、物理サーバまたは仮想サーバに関する一般的な推奨事項は次のとおりです。

1. ディスク書き込みのパフォーマンスは、主な考慮事項です。SAN ストレージまたは SSD ディスクが推奨されます。DHCP サーバは、クライアントに応答する前に、リースの変更（主に新しいクライアントへのリースの割り当てとリース時間の延長）をディスクにコミットする必要があるため、ディスク書き込みパフォーマンスが制限されます。フェールオーバー、リース履歴、DNS 更新などの構成オプションも、追加の書き込み操作を必要とするため、サーバのディスク書き込み負荷が増加します。サーバ上のリースに対して、リースを許可、延長（更新と再バインド）、リリース、または期限切れにする書き込みが最大 4 回あり、さらに次のようにフェールオーバーパートナーで 1 回の書き込みがあります。

   - リース自体（クライアントに応答する前）。一般に、フェールオーバーが使用されている場合は、フェールオーバーバインドも更新されます。
   - 履歴レコード（リース履歴が有効で、リースされていたが、もはやリースが終了した場合にのみ発生）。
   - フェールオーバーバインド更新を受信すると、パートナーはリースを書き込みます（フェールオーバーが使用されている場合）。
   - フェールオーバーバインド更新の確認応答の受信後のリース（フェールオーバーが使用されている場合）。
   - DNS 更新が完了した後のリース（リース用に設定および開始された場合）。

   サーバは、リースのフェールオーバー状態の移行、フェールオーバープールのバランシング時、およびユーザアクションによる影響（たとえば、リースを強制的に使用可能にする場合）など、リースの別の時点で書き込みを開始することもあります。DHCP サーバのリース状態データベースのディスク容量要件は、一般に次のとおりです。

   - 設定済みリースまたはアクティブリースごとに 1 KB。
   - リース履歴が有効な場合、履歴レコードごとに 1 KB。

   リースレコードの圧縮が有効になっている場合、これらの数値は約 30% 削減できます（DHCP サーバの *server-flags* 属性を参照）。

（注） シャドウバックアップに対応するには、これらの数値に 3 を掛ける必要があります。これらの数値は、リース状態データベースを反映するだけで、その他のシステム要件はありません。

2. メモリ（RAM）はセカンダリであり、64 ビットをサポートしているため、システムに十分なメモリがあれば、メモリ制限は一般には問題になりません。ディスクの読み取りの必要性を回避するためには、DHCP リース状態データベース全体をメモリに保持できるように、ファイルシステムには十分な「空き」メモリを確保することが重要です。大まかな経験則では、次のように仮定します。
   - DHCP サーバのメモリ使用量に対して、設定済みリースまたはアクティブリースごとに1KB。DNSアップデート、ホスト名とドメイン名の長さ、オプション82（DHCPv4）またはリレー転送メッセージ（DHCPv6）データの量などの構成オプションは、この経験則に影響を与える可能性があります。
   - 各リース（設定済みまたはアクティブ）のファイルシステムキャッシュ用に 1 KB の「空き」メモリ。
   - リース履歴が有効になっている場合は、各履歴レコードのファイルシステムキャッシュ用に 1 KB の「空き」メモリ（リースの期限切れまたはリリースの頻度に応じて判断が困難になります）。

3. 要求を処理するために必要な処理が全般に低下するため、CPUパフォーマンスへの影響は最も低くなります。一方、アバランシェ処理は、主にCPUサイクルと最小限のディスク書き込みで処理されます。そのため、大規模なアバランシェの可能性がある場合は、優れたCPU能力と高速なネットワークインターフェイスを備えたシステムに投資してください。最新のマルチプロセッサシステムのほとんどは、中程度のアバランシェ負荷に対して十分です。キャパシティとパフォーマンスの高いアプリケーションでは、CPU速度と有効なプロセッサの数の両方を高くする必要があります。DHCP サーバは高度にマルチスレッド化されているため、追加の CPU コアによって DHCP サーバのパフォーマンスがある程度向上します。DHCP サーバ内のロックの最小限の要件により、最大 12 個の CPU コアを追加するとパフォーマンスが向上します。CPU コアが 12 個を超えると、同期の要件によるパフォーマンスの向上はほとんどありません。

リージョナルクラスタの DHCP の考慮事項

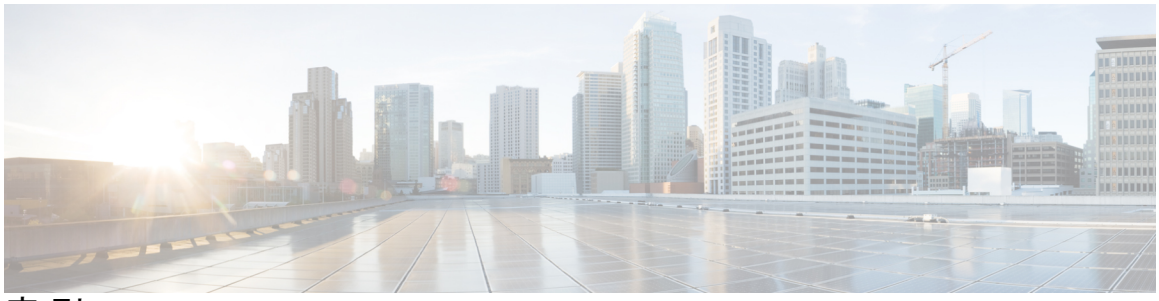
リージョナルクラスタのディスク容量の要件は、DHCP のいくつかの要因によって決まります。

1. **リース履歴**：ローカルクラスタでリース履歴が有効になっている場合、デフォルトでは、リージョナルクラスタはローカルクラスタからこの履歴を収集して長期保存します（デフォルトではこれらのレコードを 24 週間保持します。CCM サーバの *trim-lease-hist-age* 属性を参照してください）。DHCP サーバについて前述したように、各リースレコード（アクティブおよび履歴）は約 1 KB を必要と想定されますが、バックアップ要件に対応するために 3 を掛ける必要があります。つまり、1 リースレコードあたり 3 KB となります。必要なリージョナルクラスタのディスク容量は、リース履歴レコードの合計数に依存します。これは、サーバの数、サーバのリース数とクライアントの活動レベル、および履歴を保持する期間によって異なります。非常に大規模なサービス プロバイダー ネットワークでは、これが 100 GB 以上になることがあります。

DHCP のキャパシティとパフォーマンスのガイドライン

（注） これらのディスク容量の要件は、Cisco Prime Network Registrar 9.0 以降でリースレコード圧縮を有効にすることで、リース履歴データの 30% に減らすことができます（CCM サーバの *lease-hist-compression* 属性を参照）。

2. **ネットワーク使用率**：リージョナルクラスタは、ローカルクラスタからサブネットとプレフィックスの使用率データも収集します（デフォルトでは、1 時間ごとに 24 週間保持されます。CCM サーバの *addrutil-poll-interval* および *addrutil-trim-age* 属性を参照してください）。各レコードは約 1/2 KB（スコープ/プレフィックス名、所有者、リージョン、選択タグ、およびその他のデータによってサイズが異なる）ですが、多くのサブネットとプレフィックスがある場合は、これが加算されることがあります。合計 10,000 スコープ/プレフィックスの展開では、24 週間で 10 GB を使用できます（バックアップ要件を考慮すると、30 GB になります）。



索 引

記号

C

D

J

K

L

N

O

R

S

T

V

W

Y

あ

い

う

え

お

き

こ

さ

す

て

ね

ら

ろ

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。