



## **Cisco Prime Network Registrar 10.1 インストールガイド**

初版：2019年12月16日

最終更新：2021年11月22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/](http://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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019-2021 Cisco Systems, Inc. All rights reserved.



## 目次

---

### 第 1 章

#### インストールの概要 1

##### 概要 1

##### Cisco Prime Network Registrar について 1

##### センシティブデータの露出 3

---

### 第 2 章

#### 設定オプション 5

##### DHCP と DNS の混合シナリオ 5

##### 1 台のマシンの混合コンフィギュレーション 5

##### 2 台のマシンの混合コンフィギュレーション 5

##### 3 台のマシンの混合コンフィギュレーション 6

##### 4 台のマシンの混合コンフィギュレーション 6

##### DHCP のみのシナリオ 7

##### 1 台のマシンの DHCP 設定 7

##### 2 台のマシンの DHCP 設定 7

##### DNS のみのシナリオ 7

##### 1 台のマシンの DNS 設定 7

##### 2 台のマシンの DNS 設定 7

##### 3 台のマシンの DNS 設定 8

---

### 第 3 章

#### インストール要件 9

##### システム要件 9

##### 推奨事項 11

##### インストールモード 12

##### ライセンスファイル 12

---

第 4 章	<b>インストールの準備</b>	<b>15</b>
	インストールチェックリスト	15
	はじめる前に	16
	Cisco Prime Network Registrar ライセンスファイルの取得	17
	他のプロトコルサーバの実行	17
	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	18

---

第 5 章	<b>Cisco Prime Network Registrarのインストールおよびアップグレード</b>	<b>19</b>
	Cisco Prime Network Registrar のインストール	19
	アップグレードの考慮事項	27
	Windows でのアップグレード	28
	Linux でのアップグレード	28
	以前の製品バージョンへの復元	29
	新しいマシンへのローカルクラスタの移動	31
	リージョナルクラスタの新しいマシンへの移動	33
	インストールに関するトラブルシューティングを実行	35
	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	36

---

第 6 章	<b>次のステップ</b>	<b>37</b>
	Cisco Prime Network Registrar の設定	37
	Cisco Prime Network Registrar の起動	38
	サーバの起動と停止	39
	Windows でのサーバの起動と停止	39
	Linux でのサーバの起動と停止	40
	ローカル Web UI を使用したサーバの起動または停止	41
	リージョナル Web UI を使用したサーバの起動と停止	41
	サーバのイベントロギング	42
	Windows インストールでの ACL の変更	42

---

第 7 章	<b>Cisco Prime Network Registrar のアンインストール</b>	<b>45</b>
-------	--	-----------

Windows でのアンインストール	45
Linux でのアンインストール	46
Windows でのパフォーマンス モニタリング ソフトウェアの実行	46

---

**第 8 章**
**Cisco Prime Network Registrar 仮想アプライアンス 49**

システム要件	49
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	50
Cisco Prime Network Registrar 仮想アプライアンスの展開準備	50
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	51
Cisco Prime Network Registrar 仮想アプライアンスの起動と設定	53
KVM ハイパーバイザ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	54
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	55
Cisco Prime Network Registrar 仮想アプライアンスのアップグレード	58
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	58
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	59
Cisco Prime Network Registrar アプリケーションのアップグレード	60
次のステップ : Cisco Prime Network Registrar 仮想アプライアンス	60
仮想アプライアンスの CLI を使用した Cisco Prime Network Registrar の設定	60
自動的に起動するための仮想アプライアンスの設定	61
Cisco Prime Network Registrar 仮想アプライアンスの管理	61
OVA のインストール後	62

---

付録 A :	<b>サイレントインストールの実行 63</b>
	サイレントインストールの実行 63

---

付録 B :	<b>ラボ評価のためのインストール 69</b>
	ラボ評価のためのインストール 69
	ラボでの Cisco Prime Network Registrar のインストール 69
	ラボインストールのテスト 70
	ラボ環境でのアンインストール 70

---

付録 C :	<b>Cisco Prime Network Registrar SDK のインストール</b> 71
	Linux へのインストール 71
	Windows へのインストール 72
	インストールのテスト 72
	互換性に関する考慮事項 72

---

付録 D :	<b>Web UI のセキュリティ強化</b> 75
	Web UI のセキュリティ強化 75

---

付録 E :	<b>セキュリティ強化のガイドライン</b> 77
	セキュリティ強化のガイドライン 77

---

付録 F :	<b>VM パフォーマンスの最適化</b> 81
	推奨される UCS 設定 81
	NUMA の最適化 81
	ハイパースレッディングの考慮事項 82

---

付録 G :	<b>nmcli を使用した RHEL/CentOS 7.x でのネットワークアクセスの設定</b> 83
	nmcli を使用した RHEL/CentOS 7.x でのネットワークアクセスの設定 83

---

付録 H :	<b>nmcli を使用した IP アドレスの変更</b> 87
	nmcli を使用した IP アドレスの変更 87

---

付録 I :	<b>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</b> 89
	DNS システムのデプロイメント上の制限 89
	DNS データベースアーキテクチャ 90
	DNS システムのサイジング 91

---

付録 J :	<b>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</b> 95
	DNS システムのデプロイメント上の制限 95
	キャッシング DNS システムのサイジング 96

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 97

---

付録 K :

**DHCP のキャパシティとパフォーマンスのガイドライン 99**

ローカルクラスタの DHCP の考慮事項 99

単一サーバで許可されるリースの数 100

サーバに関する考慮事項 104

リージョナルクラスタの DHCP の考慮事項 105







# 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 \(1 ページ\)](#)
- [Cisco Prime Network Registrar について \(1 ページ\)](#)
- [センシティブデータの露出 \(3 ページ\)](#)

### 概要

このマニュアルでは、Windows オペレーティングシステムと Linux オペレーティングシステムに Cisco Prime Network Registrar リリース 10.1 をインストールする方法、および Cisco Prime Network Registrar 仮想アプライアンス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 Cisco Prime Network Registrar 仮想アプライアンスの構成と管理の手順については、『*Cisco Prime Network Registrar 10.1 アドミニストレーションガイド*』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 10.1 CLI リファレンス ガイド*』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ビスです。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。

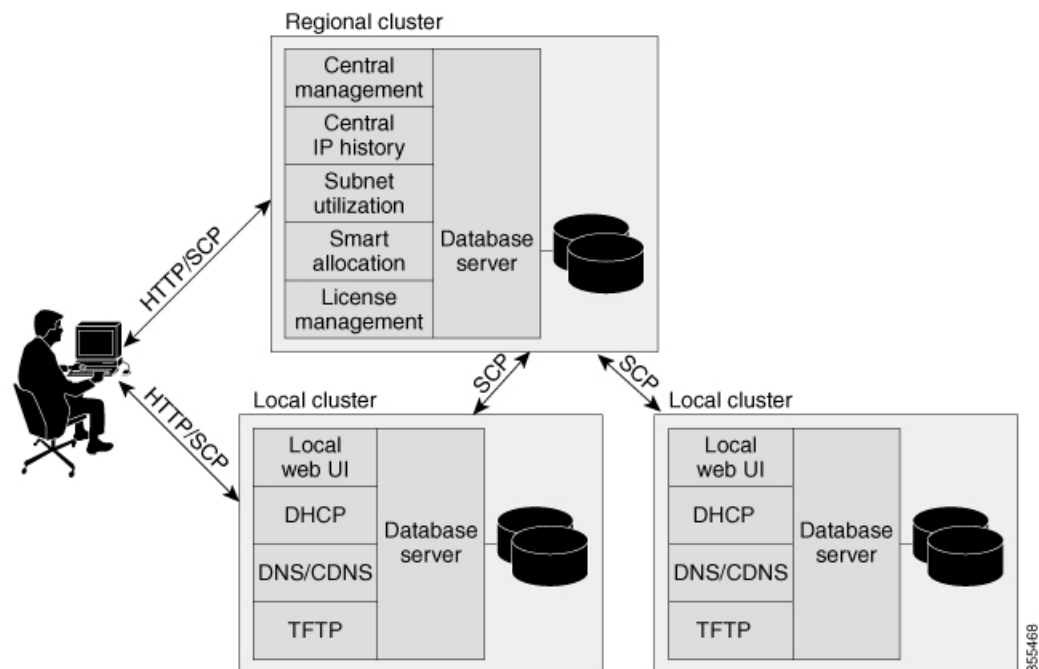
Cisco Prime Network Registrar は、ローカルモードまたはリージョナルモードでインストールできます。

- 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 または Windows 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 \(5 ページ\)](#)
- [DHCP のみのシナリオ \(7 ページ\)](#)
- [DNS のみのシナリオ \(7 ページ\)](#)

## 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、最初の実機でゾーン配信と 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、一方の実機に DNS 更新を設定してから構成をもう一方の実機にプッシュします。
- DHCP サーバおよび権威 DNS サーバを持つ1 台の実機を設定し、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実機のプライマリ権威 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。最初の実機を 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 (9 ページ)
- インストールモード (12 ページ)
- ライセンスファイル (12 ページ)

## システム要件

Cisco Prime Network Registrar 10.1 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ます。

- Java : Java ランタイム環境 (JRE) 1.8 または同等の Java 開発キット (JDK) がシステムにインストールされている必要があります。(JRE は Oracle Web サイトで入手できます)



**注** 64-ビット JRE/JDK が必要です。

- オペレーティングシステム : Cisco Prime Network Registrar マシンを Windows オペレーティングシステムまたは Linux オペレーティングシステムで実行することを推奨します (以下の「サーバの最小要件」の表を参照)。Cisco Prime Network Registrar には、64 ビットオペレーティングシステムが必要です。

Cisco Prime Network Registrar は、VMware ESXi 6.x 環境での実行をサポートしています。

- 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 Internet Explorer 11 と Edge、Mozilla Firefox 69、および Google Chrome 77 でテストされています。Internet Explorer 8 はサポートされていません。
  - CLI は、Windows または 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 の最小要件

コンポーネント	オペレーティングシステム	
	Linux	Windows
OS バージョン <sup>1</sup>	Red Hat Enterprise Linux ES 6.5 64 ビットおよび CentOS 6.5 64 ビット。	Windows Server 2012 R2 <sup>2</sup>
ディスク容量 <sup>3</sup>	基本的な DHCP と最適なハードウェア構成： <ul style="list-style-type: none"> <li>• 予想されるピーク負荷が 500 ～ 1000 DHCP リース/秒の場合は、7500 RPM SATA<sup>4</sup>ドライブが推奨されます。</li> <li>• 予想されるピーク負荷が 1000 DHCP リース/秒を超える場合は、SSD または 15000 RPM ドライブを推奨します。推奨ハードドライブ：146 GB。</li> </ul>	
メモリ <sup>5</sup>	小規模ネットワーク：8 GB、平均ネットワーク：16 GB、または大規模ネットワーク：32 GB。	

<sup>1</sup> Cisco Prime Network Registrar 10.1 は、64 ビットオペレーティングシステムでのみサポートされます。

<sup>2</sup> Cisco Prime Network Registrar 10.1 は、スタンドアロンで動作する Windows Server 2012 R2、または Cisco Unified Computing System (CUCS) 上の VMware (ESXi Server 6.x) で動作する Windows Server 2012 R2、および VMware がサポートするその他のハードウェアをサポートしています。

<sup>3</sup> I/O 帯域幅が大きいほど、通常は 1 秒あたりの平均リース数が多くなります。

<sup>4</sup> Serial Advanced Technology Attachment (シリアル ATA)。

<sup>5</sup> CPU が高速でメモリが多いほど、一般的にピーク時の 1 秒あたりのリース数が多くなります。



(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。

## Linux OS のシステム要件

Red Hat Enterprise Linux または CentOS に Cisco Prime Network Registrar をインストールするには、Java ランタイムの他に次の 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。

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
OpenLDAP	2.4
OpenSSL	1.0
libstdc++	4.x
libgcc	4.x
zlib	1.x
krb5-libs	1.x

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 (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) 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、の「自動バックアップ時間の設定 (Setting Automatic Backup Time)」の項を参照してください。Cisco Prime Network Registrar 10.1 アドミニストレーションガイド



(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またはアップグレードは、オペレーティングシステム固有のソフトウェアインストールメカニズムを使用して実行されます。

- Windows : **InstallShield** 設定プログラム
- Linux : Red Hat Package Manager を使用する **install\_cnr** スクリプト

## ライセンスファイル

Cisco Prime Network Registrar 10.1 の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 および9.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 10.1 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 8.3 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。

- **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 10.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。

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

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
- DHCP サービス : base-dhcp および count-dhcp
- 権威 DNS サービス : base-dns および count-dns
- キャッシング DNS サービス : base-cdns および count-cdns



- (注) Cisco Prime Network Registrar 9.x 以前のライセンスは Cisco Prime Network Registrar 10.x では無効です。Cisco Prime Network Registrar 10.x 用の新しいライセンスが必要です。10.x のリージョナルに 9.x の CDNS クラスタが含まれている場合は、9.x の CDNS ライセンスをリージョナルサーバに追加する必要があります (9.x の CDNS クラスタが 9.x のライセンスを使用し、10.x の CDNS クラスタが 10.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せん。

- **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 (の「*DHCP* フェールオーバーの設定 (*Configuring DHCP Failover*)」の章の「フェールオーバーのシナリオ (*Failover Scenarios*)」*Cisco Prime Network Registrar 10.1 DHCP* ユーザガイドを参照)。

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 \(17 ページ\)](#) 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 \(15 ページ\)](#)
- [はじめる前に \(16 ページ\)](#)
- [Cisco Prime Network Registrar ライセンスファイルの取得 \(17 ページ\)](#)
- [他のプロトコルサーバの実行 \(17 ページ\)](#)
- [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 \(18 ページ\)](#)

## 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 10.1 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。 ( <a href="#">システム要件 (9 ページ)</a> を参照)	<input type="checkbox"/>
ハードウェアが最小要件を満たしていますか。 ( <a href="#">システム要件 (9 ページ)</a> を参照)	<input type="checkbox"/>
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。 ( <a href="#">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 (18 ページ)</a> を参照)	<input type="checkbox"/>

タスク	チェック
Windows では、ウイルススキャンや自動バックアップソフトウェアプログラムなど、他のアプリケーションは閉じていますか。デバッガーユーザグループはローカルユーザとローカルグループに含まれていますか。	<input type="checkbox"/>
適切なソフトウェアライセンスがありますか。 ( <a href="#">ライセンスファイル (12 ページ)</a> を参照)	<input type="checkbox"/>
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。	<input type="checkbox"/>
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。	<input type="checkbox"/>
これは新規インストールですか、アップグレードですか。	<input type="checkbox"/>
クラスタの動作モードはリージョナルですか、ローカルですか。	<input type="checkbox"/>
これはフルインストールですか、クライアント専用インストールですか。	<input type="checkbox"/>
64 ビット JRE/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。	<input type="checkbox"/>
Web UI は HTTP 接続、HTTPS 接続のどちらかですか、それとも両方ですか。	<input type="checkbox"/>
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。	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>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。</li> </ul>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>データベースはバックアップされていますか。</li> </ul>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>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。</li> </ul>	<input type="checkbox"/>
Linux に必要なパッケージがインストールされていますか。 ( <a href="#">Linux OS のシステム要件 (11 ページ)</a> を参照)	<input type="checkbox"/>

## 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。

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

Cisco Prime Network Registrar 10.1 を購入すると、ソフトウェアを登録した後、シスコから電子メールの添付で 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 10.1 permanent uncounted \  
  
VENDOR_STRING=<Count>1</Count> HOSTID=ANY \  
  
NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \  
  
<PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

## 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。Cisco Prime Network Registrar インストールプロセスで競合が検出されると、警告メッセージが表示されます。

Windows システムでは、次のいずれかのメソッドを使用して、サービス コントロール マネージャから構成を変更します。

- いずれかのユーザインターフェイスで停止機能を使用して、Microsoft プロトコルサーバと競合する Cisco Prime Network Registrar プロトコルサーバを停止します。

- Microsoft サーバの [スタートアップの種類 (Startup Type)] を [自動 (Automatic)] から [手動 (Manual)] または [無効 (Disabled)] に変更します。

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、次のディレクトリとそのサブディレクトリを除外します。



(注) このマニュアルでは、*install-path* を使用する場合、Cisco Prime Network Registrar インストール時に指定されたインストールパスのすべてまたは一部を参照します。Linux のデフォルトのローカルクラスパスである `/opt/nwreg2/local` および `/var/nwreg2/local` を使用する例として、*install-path* はこれらのパスを表します。

- Windows :

*install-path*\data (たとえば、C:\NetworkRegistrar\Local\data および C:\NetworkRegistrar\Regional\data)

*install-path*\logs (たとえば、C:\NetworkRegistrar\Local\logs および C:\NetworkRegistrar\Regional\logs)

- Linux :

*install-path*/data (たとえば、/var/nwreg2/local/data および /var/nwreg2/regional/data)

*install-path*/logs (たとえば、/var/nwreg2/local/logs および /var/nwreg2/regional/logs)



## 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](#) (19 ページ)
- [アップグレードの考慮事項](#) (27 ページ)
- [以前の製品バージョンへの復元](#) (29 ページ)
- [新しいマシンへのローカルクラスタの移動](#) (31 ページ)
- [リージョナルクラスタの新しいマシンへの移動](#) (33 ページ)
- [インストールに関するトラブルシューティングを実行](#) (35 ページ)
- [ローカルクラスタのライセンスの問題のトラブルシューティング](#) (36 ページ)

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

**ステップ 1** 管理者権限を持つアカウントを使用してターゲットマシンにログインします。

- Windows : 管理者グループのアカウント
- Linux : **su** (スーパーユーザ) または **root** アカウント

Windows : ウイルス対策ソフトウェアを含む、開いているすべてのアプリケーションを閉じます。

(注) Cisco Prime Network Registrar 9.1 以降、Linux インストーラと Windows インストーラには、Web UI ポートと同じデフォルトで Web サービスポートを要求するオプションがあります。これは、Web サービス機能が有効な場合にのみ表示されます。新規インストールの場合、Web サービスポートのデフォルト値は、Web UI ポートまたは新しく入力された Web UI ポートのデフォルト値と同じになります。それ以降のインストールでは、ポート値が **conf** ファイルから選択されません。

**注意** Red Hat および CentOS Linux の多くのディストリビューションでは、デフォルトで、ファイアウォールと接続追跡がインストールされ、有効になります。同じ OS と DNS でステータスフルファイアウォールを実行すると、サーバ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 10.1* アドミニストレーションガイドの「DNS パフォーマンスとファイアウォールの接続追跡 (*DNS Performance and Firewall Connection Tracking*)」の項を参照してください。

**ステップ 2** JRE 1.8 または同等の JDK をダウンロードしてインストールします（まだ行っていない場合）。これらは、Oracle の Web サイトで入手できます。

(注) Windows では、Java インストールフォルダの bin サブディレクトリのフルパスを PATH 環境変数に追加します。たとえば、C:\Program Files (x86)\Java\jdk1.8\bin です。

**ステップ 3** Web UI への安全なログインを設定しない場合は、**ステップ 4**に進みます。安全なログインを設定する場合は、Java インストールの bin サブディレクトリにある Java **keytool** ユーティリティを使用してキーストアファイルを作成する必要があります（**ステップ 2**を参照）。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。

a) 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):
```

キーストアファイル名 (k-file) は、完全修飾パスです。**ステップ 17**でキーストアのパスとパスワードを入力します。

(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 \(75 ページ\)](#) を参照してください。

b) 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、前のサブステップで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。

**注意** Windows の Cisco Prime Network Registrar インストールプログラムは、インストールされたファイルとディレクトリへのアクセスを制限するために ACL を変更しようとしません。これらのファイルとディレクトリへのアクセスを制限する場合は、ネイティブの Microsoft ユーティリティを使用して、ファイルとディレクトリの権限を手動で変更します。[Windows インストールでの ACL の変更 \(42 ページ\)](#) を参照してください。

**ステップ 4** 必要に応じて、ディストリビューションファイルを Cisco.com からダウンロードします。次のアクションを実行します。

- **Windows** : `cpnr_version-windows.exe` ファイルは、設定ファイルとその他のファイルを実行するディレクトリに配置する自己解凍型の実行可能ファイルです。(自動起動用に設定されていない場合は、そのディレクトリで `setup.exe` ファイルを実行します)。`[Welcome to Cisco Prime Network Registrar]` ウィンドウが表示されます。

[次へ (Next) ] をクリックします。2 番目の `Welcome` ウィンドウに設定プログラムが表示され、ウイルススキャンソフトウェアを含む現在のすべてのプログラムを終了するように通知されます。実行中のプログラムがある場合は、`[キャンセル (Cancel) ]` をクリックしてプログラムを閉じ、**ステップ 4** の最初に戻ります。すべてのプログラムをすでに終了している場合は、[次へ (Next) ] をクリックします。

- **Linux** : Cisco Prime Network Registrar インストールファイルを圧縮解除および展開するために、**gzip** ユーティリティと **gtar** ユーティリティが使用可能であることを確認します。これらのユーティリティの詳細については、GNU 組織の Web サイトを参照してください。次の手順を実行します。

1. 必要に応じて、ディストリビューションファイルを Cisco.com からダウンロードします。
2. インストールファイルを圧縮解除して展開するディレクトリに移動します。ディストリビューションがダウンロードされたのと同じディレクトリを指定できます。
3. `.gtar.gz` ファイルを圧縮解除および展開します。`-z` オプションを指定して **gtar** を使用します。

```
gtar -zxpf cpnr_10_1-linux-x86_64.gtar.gz
```

コマンドは、Cisco Prime Network Registrar インストールファイルが展開される `cpnr_10_1` ディレクトリを作成します。

4. 以下のように `install_cnr` スクリプトを実行します。

```
# ./cpnr_10_1/Linux/install_cnr
```

インストールスクリプトは、サポートされているオペレーティングシステムのバージョンを使用していること、および必要なパッケージがインストールされていることを確認するためのいくつかのチェックを行い、問題がある場合はレポートしてインストールを停止します。

**ステップ 5** ローカルクラスタモードとリージョナルクラスタモードのどちらで Cisco Prime Network Registrar をインストールするかを指定します。

(注) ライセンス管理にはリージョナルサーバが必要であるため、最初にリージョナルサーバ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。登録後にリージョナルクラスタをローカルクラスタに同期する際に問題が発生した場合は、リージョナルクラスタのパスワードを設定解除してから設定し、再度同期してください。

**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。

- **Windows** : デフォルトの [Cisco Prime Network Registrar ローカル (Cisco Prime Network Registrar Local) ] のままにするか、[Cisco Prime Network Registrar リージョナル (Cisco Prime Network Registrar Regional) ] を選択します。[次へ (Next) ] をクリックします。[プログラムフォルダの選択 (Select Program Folder) ] が表示されます。[スタート (Start) ] メニューでプログラムのショートカットを保存するプログラムフォルダを決定します。デフォルトを受け入れるか、別の名前を入力するか、[既存のフォルダ (Existing Folders) ] リストから名前を選択します。[次へ (Next) ] をクリックします。
- **Linux** : ローカルの場合は **1**、リージョナルの場合は **2** を入力します。新規インストールの場合、デフォルトは **1** です。アップグレードの場合、デフォルトは以前にインストールされたものによって異なります。

**ステップ 6** Linux では、非ルート *nradmin* ユーザとして Cisco Prime Network Registrar ローカルサーバエージェントを実行するかどうかを指定します。非ルートユーザに対して Cisco Prime Network Registrar を実行する場合、Cisco Prime Network Registrar サービスを実行するために必要な権限を持つユーザ *nradmin* が作成されません。非ルートユーザ (*nradmin*) として Cisco Prime Network Registrar を実行している場合、製品の CLI 操作にいくつかの変更が発生します。ルートとして実行することも可能ですが、推奨されません。代わりに、通常の Linux ユーザを作成し、*nradmin* グループに追加します。このグループのユーザは、Cisco Prime Network Registrar ファイルにフルアクセスできます。Cisco Prime Network Registrar を起動および停止するために、これらのユーザは、*install-path/bin/cnr\_service* にある新しい **cnr\_service** プログラムを使用できます。

(注) ルートユーザは、インストールとアンインストールにのみ必要です。

**ステップ 7** これらの Cisco Prime Network Registrar インストールのデフォルトディレクトリに注意し、必要に応じて適切な変更を行います。

(注) Windows では、スペースを含むインストールディレクトリパスはサポートされていません (「Program Files」などのシステムディレクトリを除く)。

- (注) アップグレードする場合、アップグレードプロセスは以前のリリースからのインストールディレクトリを自動検出します。

### Windows のデフォルトの場所

**注意** Cisco Prime Network Registrar のデータ、ログ、および一時ファイルの場所として、`\Program Files (x86)` または `\Program Files` または `\ProgramData` を指定しないでください。そうすると、Windows のセキュリティの関係で Cisco Prime Network Registrar の動作が予測不能になる可能性があります。

- ローカルクラスタ
  - プログラムファイル : `C:\Program Files (x86)\Network Registrar\Local`
  - データファイル : `C:\NetworkRegistrar\Local\data`
  - ログファイル : `C:\NetworkRegistrar\Local\logs`
  - 一時ファイル : `C:\NetworkRegistrar\Local\temp`
- リージョナルクラスタ
  - プログラムファイル : `C:\Program Files (x86)\Network Registrar\Regional`
  - データファイル : `C:\NetworkRegistrar\Regional\data`
  - ログファイル : `C:\NetworkRegistrar\Regional\logs`
  - 一時ファイル : `C:\NetworkRegistrar\Regional\temp`

### Linux のデフォルトの場所 :

- ローカルクラスタ
  - プログラムファイル : `/opt/nwreg2/local`
  - データファイル : `/var/nwreg2/local/data`
  - ログファイル : `/var/nwreg2/local/logs`
  - 一時ファイル : `/var/nwreg2/local/temp`
- リージョナルクラスタ
  - プログラムファイル : `/opt/nwreg2/regional`
  - データファイル : `/var/nwreg2/regional/data`
  - ログファイル : `/var/nwreg2/regional/logs`
  - 一時ファイル : `/var/nwreg2/regional/temp`

**ステップ 8** 管理者が定義されていない場合は、ユーザ名とパスワードを指定して管理者を作成します。入力したパスワードを確認する必要があります。

リージョナルをインストールしている場合は、続行します。それ以外の場合は、**ステップ 10**に進みます。

**ステップ 9** 基本ライセンスのファイル名を絶対パスとして入力します ([ライセンスファイル \(12 ページ\)](#) を参照)。

(注) 基本ライセンスの相対パスではなく絶対パスを使用します。これは、インストールを開始した時点からデフォルトパスが変更される可能性があるためです。

インストール時にファイル名を入力するかどうかは任意です。ただし、ここでファイル名を入力しない場合は、Web UI または CLI に最初にログインするときに入力する必要があります。

(注) Windows サーバへのリモートデスクトップ接続を使用して Cisco Prime Network Registrar をインストールする場合、インストール中にライセンス情報を入力することはできません。Cisco Prime Network Registrar はライセンスを無効として拒否します。したがって、Web UI または CLI を使用して、ライセンス情報のステップをスキップし、インストールの完了後にライセンスを追加する必要があります。詳細については、[Cisco Prime Network Registrar の起動 \(38 ページ\)](#) を参照してください。

**ステップ 10** リージョナルの IPv4 アドレスまたはリージョナルの IPv6 アドレスおよび SCP ポートを指定して、ローカルをリージョナルに登録します。

ローカルがリージョナルに登録されると、そのリージョナルにライセンスが存在するサービスを提供できます。

(注) 登録後にリージョナルクラスタをローカルクラスタに同期する際に問題が発生した場合は、リージョナルクラスタのパスワードを設定解除してから設定し、再度同期してください。これは、ローカルクラスタとリージョナルクラスタの間の時間のずれが 5 分を超えているために発生する可能性があります。

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。

**ステップ 11** ローカルにリージョナルを登録した後、ライセンスサービスから必要なサービスを選択できます。

(注) サービスが選択されていない場合、アップグレードプロセスでは既存の構成が使用されます。サービスを削除するには、アップグレードプロセスが完了するまで待ちます。

**ステップ 12** このインストールが成功しない場合に備えて、既存のバイナリとデータベースをアーカイブするかどうかを選択します。デフォルトの推奨される選択肢は [はい (Yes)] または [y (y)] です。

ファイルをアーカイブする場合は、アーカイブディレクトリを指定します。デフォルトのディレクトリは次のとおりです。



- Windows : ローカルクラスタ (`C:\NetworkRegistrar\Local.sav`)。リージョナルクラスタ (`C:\NetworkRegistrar\Regional.sav`)。[次へ (Next) ]をクリックします。
- Linux : ローカルクラスタ (`/opt/nwreg2/local.sav`)。リージョナルクラスタ (`/opt/nwreg2/regional.sav`)。

**ステップ 13** 適切なインストールタイプ：サーバとクライアント（デフォルト）、またはクライアントのみを選択します。

- Windows : [サーバとクライアントの両方 (Both server and client) ]（デフォルト）または[クライアントのみ (Client only) ]を選択します。[次へ (Next) ]をクリックします。[ポートの選択 (Select Port) ]ウィンドウが表示されます。
- Linux : **1**を入力するとサーバとクライアントがインストールされ（デフォルト）、**2**を入力するとクライアントのみがインストールされます。

(注) クライアントソフトウェアをプロトコルサーバ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 (Client only) ]を選択します。クライアントからプロトコルサーバへの接続を設定する必要があることに注意してください。

**ステップ 14** サーバエージェントがサーバ間の内部通信に使用する CCM 管理 SCP ポート番号を入力します。デフォルト値は、ローカルクラスタの場合は 1234、リージョンクラスタの場合は 1244 です。

**ステップ 15** ステップ 2 で選択した JRE 1.8 または JDK の場所を入力します。（インストールまたはアップグレードプロセスでロケーションを検出しようとしています）。

- Windows : Java の要件を示すダイアログボックスが表示されます。[OK] をクリックし、デフォルトの Java ディレクトリまたは別のディレクトリを選択します。[OK] をクリックします。[接続タイプの選択 (Select Connection Type) ]ウィンドウが表示されます。
- Linux : Java のインストール場所を入力します。

(注) パスに bin サブディレクトリを含めないでください。新しい Java バージョンをインストールするか、その場所を変更する場合は、Cisco Prime Network Registrar インストーラを再実行してから、このステップで新しい場所を指定します。

**ステップ 16** Web UI が Web UI ログインに非セキュア (HTTP) 接続またはセキュア (HTTPS) 接続を使用できるようにするかどうかを選択します。

- Windows : **非セキュア (HTTP) のみ**、**セキュア (HTTPS) のみ**（デフォルト）、または **HTTP と HTTPS の両方**を選択します。
- Linux : **非セキュア (HTTP) のみ**の場合は**1**、**セキュア (HTTPS) のみ**の場合は**2**（デフォルト）、**HTTP と HTTPS の両方**の場合は**3**を入力します。

セキュア HTTPS ポートを有効にすると、Apache Tomcat Web サーバに接続するためのセキュリティが設定されます（構成については、**ステップ 3**を参照）。（接続タイプを変更するには、インストーラを再実行し、このステップで別の選択を行います）。

- HTTPS または HTTP と HTTPS を選択した場合は、[次へ (Next) ]をクリックして**ステップ 17**に進みます。

- HTTP 接続を選択した場合は、[次へ (Next)] をクリックし、**ステップ 18**に進みます。

**ステップ 17** HTTPS Web UI 接続を有効にした場合は、必要なキーストアとキーストアファイルの場所を指定するように求められます。

- キーストアの場所には、Apache Tomcat Web サーバへのセキュアな接続に使用する証明書を含むキーストアファイルへの完全修飾パスを指定します。これは、**ステップ 3** で作成したキーストアファイルです。
- キーストアパスワードには、キーストアファイルの作成時に付与されたパスワードを指定します。Windows では、[次へ (Next)] をクリックします。

**注意** キーストアのパスワードにドル記号 (\$) を含めないでください。ドル記号 (\$) を使用すると、Apache Tomcat Web サーバの構成が無効になります。

(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。後でキーストアのパスワードを変更する場合は、プレーンテキストのパスワードを使用できます。ただし、セキュリティを強化するために、*install-path/usrbin* ディレクトリにある暗号化スクリプトを使用して暗号化されたパスワードを生成する必要があります。この暗号化されたパスワードは、*server.xml* で更新する必要があります。変更後、Cisco Prime Network Registrar を再起動する必要があります。

**ステップ 18** Web UI 接続のポート番号を入力します。デフォルトは、次のとおりです。

- HTTP ローカルクラスタ : 8080
- HTTP リージョナルクラスタ : 8090
- HTTPS ローカルクラスタ : 8443
- HTTPS リージョナルクラスタ : 8453

Windows では、[次へ (Next)] をクリックします。

**ステップ 19** Cisco Prime Network Registrar Web サービスを有効にする場合は、[はい (Yes)] を選択します。

**ステップ 20** Web サービス接続のポート番号を入力します。デフォルトは、次のとおりです。

- HTTP ローカルクラスタ : 8080
- HTTP リージョナルクラスタ : 8090
- HTTPS ローカルクラスタ : 8443
- HTTPS リージョナルクラスタ : 8453

(注) Web サービスのユーザには、別のポート番号を入力するオプションがあります。

**ステップ 21** 設定するセキュリティモードを選択します。**[必須。接続を保護できない場合は失敗します。(Required. Fail if the connection cannot be secured.)]** がデフォルトで選択されています。[次へ (Next)] をクリックします。

**ステップ 22** リージョナルをインストールする場合は、[はい (Yes)] を選択して BYOD サービスを有効にします。

Cisco Prime Network Registrar インストールプロセスが開始されます。ステータスメッセージは、インストーラがファイルを転送し、スクリプトを実行していることをレポートします。このプロセスに数分かかることがあります。

- Windows : [設定の完了 (Setup Complete)] ウィンドウが表示されます。[はい、今すぐコンピュータを再起動します (Yes, I want to restart my computer now)] または [いいえ、後でコンピュータを再起動します (No, I will restart my computer late)] を選択し、[終了 (Finish)] をクリックします。
- Linux : 正常終了のメッセージが表示されます。

(注) Cisco Prime Network Registrar をアップグレードすると、インストール中にアップグレードプロセスが実行されます。したがって、インストールプロセスおよびアップグレードプロセスには、設定した範囲、プレフィックス、および予約の数に応じて時間がかかります。

**ステップ 23** Cisco Prime Network Registrar サーバのステータスを確認します。

- Windows : [サービス (Services)] コントロールパネルで、インストールが正常に完了したら、システムをリブートした後に Cisco Prime Network Registrar ローカルサーバエージェントまたは Cisco Prime Network Registrar リージョンサーバエージェントが実行されていることを確認します。
- Linux : ステータスを確認するには、`install-path/usrbin/cnr_status` コマンドを使用します。[サーバの起動と停止 \(39 ページ\)](#) を参照してください。

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 \(29 ページ\)](#) を参照してください。

## アップグレードの考慮事項

Cisco Prime Network Registrar 10.1 は、同じプラットフォーム上で 8.3 (Linux および Windows) 以降からの直接アップグレードをサポートしています。

Cisco Prime Network Registrar は、Red Hat 3.x、4.x、および 5.x をサポートしていません。この最新リリースをインストールする前に、Cisco Prime Network Registrar のデータをバックアップし、オペレーティングシステムをアップグレードします。(現在サポートしているオペレーティングシステムについては[システム要件 \(9 ページ\)](#) を参照してください)

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。プログラムは、最初に既存の Cisco Prime Network Registrar データをアーカイブするように要求します。アップグレード中にプログラムでエラーが発生すると、ソフトウェアは以前のリリースに復元されません。

アップグレード中に、Cisco Prime Network Registrar では、キースタアのファイル名とパスワードの既存の HTTPS 構成のデフォルトが表示され、Web UI ログインのセキュアな接続が可能に

なります。HTTPS を有効にし、アップグレード時にキーストアのファイル名とパスワードを認識しない場合は、アップグレード中に HTTPS 接続を維持し、プロンプトが表示されたらデフォルトを再入力できます。

## Windows でのアップグレード

Cisco Prime Network Registrar 10.1 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** 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リリースを使用して、進行中の構成変更を完了します。
- ステップ 3** 以前のバージョンの Cisco Prime Network Registrar をアンインストールします。アンインストール後も、既存の構成データはそのまま残ります。
- ステップ 4** 別のマシンまたは共有ネットワークデバイスで Cisco Prime Network Registrar データをバックアップし、オペレーティングシステムを Windows Server 2012 R2 にアップグレードします。Windows サーバのインストールとアップグレードの方法については、Microsoft が提供するマニュアルを参照してください。
- (注) アップグレードではなく Windows Server 2012 R2 をインストールし、ディスクを再フォーマットする場合は、Cisco Prime Network Registrar データを C:\NetworkRegistrar\{Local | Regional}\data フォルダに復元する必要があります。

- ステップ 5** Windows Server 2012 R2 マシンに Cisco Prime Network Registrar 10.1 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 \(19 ページ\)](#) を参照してください。既存のデータが見つかるパスを指定していることを確認します。たとえば、C:\NetworkRegistrar\{Local | Regional} を指定して、アップグレードを実行します。
- (注) Cisco Prime Network Registrar インストール中にこの情報を再入力する必要がある場合があるため、古い Cisco Prime Network Registrar の構成とライセンス情報を手元に保管しておいてください。
- (注) Cisco Prime Network Registrar 10.1 へのアップグレード中に、Web サービス専用の別のポート番号を入力するオプションがあります。

リージョナルクラスタの古いバージョンは新しいローカルクラスタに接続できないため、ローカルクラスタをアップグレードする前に、リージョナルクラスタをアップグレードすることを推奨します。

---

## Linux でのアップグレード

Cisco Prime Network Registrar 10.1 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** 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リリースを使用して、進行中の構成変更を完了します。

**ステップ3** Cisco Prime Network Registrar のサーバエージェントを停止し、現在のシステム（または少なくとも Cisco Network Registrar\Program Files\Network Registrar\ ディレクトリと格納ファイル）をバックアップします。Cisco Prime Network Registrar のローカルサーバエージェントまたはリージョナルサーバエージェントを停止するには、次の手順を実行します。

- ローカルの場合：
  - RHEL/CentOS 6.x : `/etc/init.d/nwreglocal stop`
  - RHEL/CentOS 7.x : `systemctl stop nwreglocal`
- リージョナルの場合：
  - RHEL/CentOS 6.x : `/etc/init.d/nwregregion stop`
  - RHEL/CentOS 7.x : `systemctl stop nwregregion`

**ステップ4** Cisco Prime Network Registrar 10.1 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 \(19 ページ\)](#) 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きに既存の製品構成とデータをアーカイブし、製品の以前のバージョンに戻す機能を提供します。このオプションを選択し、アップグレードプロセスが失敗した場合は、次の手順を使用して以前の製品バージョンと構成に戻します。



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

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

**ステップ1** アップグレードプロセス中に指定したアーカイブディレクトリが存在し、有効であることを確認します。これらの例では、インストール時に提供されるデフォルトのアーカイブの場所を想定しています。`cnr_data_archive` ディレクトリへのパスが、インストール時に指定したアーカイブディレクトリの値を反映していることを確認します。使用方法に応じて以下ようになります。

- Windows : C:\NetworkRegistrar\{Local.sav | Regional.sav}
- Linux : /opt/nwreg2/{local.sav | regional.sav}

**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** 指定したアーカイブディレクトリの内容以外に、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** Cisco Prime Network Registrar の元のバージョンを再インストールします。元の製品バージョンに固有の『Cisco Prime Network Registrar インストールガイド』に記載されている再インストール手順に従ってください。

**ステップ 5** 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。

- Windows :
  - ローカル : **net stop nwreglocal**
  - リージョナル : **net stop nwregregion**
- Linux : ローカル :
  - RHEL/CentOS 6.x : **/etc/init.d/nwreglocal stop**
  - RHEL/CentOS 7.x : **systemctl stop nwreglocal**
- Linux : リージョナル :
  - RHEL/CentOS 6.x : **/etc/init.d/nwregregion stop**
  - RHEL/CentOS 7.x : **systemctl stop nwregregion**

**ステップ 6** Cisco Prime Network Registrar *install-path/data* サブディレクトリの内容を削除します。

**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。Windows では、このディレクトリはベースドライブ (C:\ など) です。Linux では / になります。
- 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。これらの例では、インストール時に提供されるデフォルトのアーカイブの場所を想定しています。

- Windows : C:\NetworkRegistrar\{Local.sav|Regional.sav}\cnr\_data\_archive\ の内容を Cisco Prime Network Registrar データディレクトリにコピーします。次に、ローカルクラスタのデフォルトのインストール場所を想定します。

```
xcopy/s C:\NetworkRegistrar\Local.sav\cnr_data_archive C:\NetworkRegistrar\Local\data\
```

(注) また、インストールされたファイルが含まれている *cnr\_file\_archive* ディレクトリもあります。通常、これは再インストールでは回復されません。

- Linux :

- `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。
- `cnr_data_archive.tar` 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。これらの例では、インストール時に提供されるデフォルトのアーカイブの場所を想定しています。tar 実行可能ファイルと `cnr_data_archive.tar` ファイルへのパスが、インストール時に指定したアーカイブディレクトリの値を反映していることを確認します。

```
/opt/nwreg2/{local.sav | regional.sav}/tar -xf /opt/nwreg2/{local.sav | regional.sav}/cnr_data_archive.tar
```

(注) また、インストールされたファイルが含まれている `cnr_file_archive.tar` もあります。通常、これは再インストールでは回復されません。

**ステップ 8** Cisco Prime Network Registrar サーバエージェントを起動します。

- Windows :
  - ローカル : `net start nwreglocal`
  - リージョナル : `net start nwregregion`
- Linux : ローカル :
  - RHEL/CentOS 6.x : `/etc/init.d/nwreglocal start`
  - RHEL/CentOS 7.x : `systemctl start nwreglocal`
- Linux : リージョナル :
  - RHEL/CentOS 6.x : `/etc/init.d/nwregregion start`
  - RHEL/CentOS 7.x : `systemctl start nwregregion`

**ステップ 9** 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 4 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)。この手順は、Linux から Linux または Windows のリリースに移行する場合にのみ使用してください。別のサーバオペレーティングシステムのプラットフォームに移行する場合、これらの手順は無効です。

次の手順ではデフォルトのインストールディレクトリを使用するため、インストールに使用するパスに基づいて調整する必要があります。

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。

• Windows :

ローカル : **net stop nwreglocal**

• Linux : ローカル :

• RHEL/CentOS 6.x : **/etc/init.d/nwreglocal stop**

• RHEL/CentOS 7.x : **systemctl stop nwreglocal**

**ステップ 2** /var/nwreg2/local/data ディレクトリとその下のすべてを tar 圧縮または zip 圧縮します。また、古いローカルサーバで次のファイルを tar 圧縮または zip 圧縮します。これらは Linux のデフォルトのインストールパスを使用していることに注意してください。

• /opt/nwreg2/local/conf/cnr.conf

• /opt/nwreg2/local/conf/cert ディレクトリとその内容

• /opt/nwreg2/local/conf/cnr\_cert\_config

• /opt/nwreg2/local/conf/public.der

• /opt/nwreg2/local/conf/priv/\*

• /opt/nwreg2/local/extensions/dhcp/dex ディレクトリ (libdextension.so を除く) および  
/opt/nwreg2/local/extensions/dhcp/tcl ディレクトリにある DHCP に対するカスタマー拡張

(注) 製品のインストール時に選択したオプションによっては、これらのファイルがすべては存在しない場合があります。

**ステップ 3** tar ファイルと zip ファイルを新しいサーバのそれぞれの場所にコピーし、解凍します。

**ステップ 4** 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 \(75 ページ\)](#)) で説明されている変更などを再適用します。

**ステップ 5** Web UI にログインし、[管理 (Administration) ] メニューの [ライセンスの一覧表示 (List Licenses) ] ページに移動します。

**ステップ 6** 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7** [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8** 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4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）。この手順は、LinuxからLinuxまたはWindowsのリリースに移行する場合にのみ使用してください。別のサーバオペレーティングシステムのプラットフォームに移行する場合、これらの手順は無効です。

次の手順ではデフォルトのインストールディレクトリを使用するため、インストールに使用するパスに基づいて調整する必要があります。

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。

- Windows :

**net stop nwregregion**

- Linux :
  - RHEL/CentOS 6.x : **/etc/init.d/ nwregregion stop**
  - RHEL/CentOS 7.x : **systemctl stop nwregregion**

**ステップ 2** /var/nwreg2/regional/data ディレクトリとその下のすべてを tar 圧縮または zip 圧縮します。また、古いリージョナルサーバ上で次のファイルを tar 形式または zip 形式で圧縮します。これらは Linux のデフォルトのインストールパスを使用していることに注意してください。

- /opt/nwreg2/regional/conf/cnr.conf
- /opt/nwreg2/regional/conf/cert ディレクトリとその内容
- /opt/nwreg2/regional/conf/cnr\_cert\_config
- /opt/nwreg2/regional/conf/public.der
- /opt/nwreg2/regional/conf/priv/\*

(注) 製品のインストール時に選択したオプションによっては、これらのファイルがすべては存在しない場合があります。

**ステップ 3** tar ファイルと zip ファイルを新しいサーバのそれぞれの場所にコピーし、解凍します。

**ステップ 4** 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 \(19 ページ\)](#) 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 \(75 ページ\)](#)) 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 5** 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 の起動 \(38 ページ\)](#) を参照してください。

**ステップ 6** 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 7** 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 8** 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
```

# インストールに関するトラブルシューティングを実行

Cisco Prime Network Registrar のインストールプロセスにより、Cisco Prime Network Registrar のログファイルディレクトリにログファイル `install_cnr_log` が作成されます。アップグレードの場合、`lease_upgrade_log` という 1 つの追加のログファイルが作成されます。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。

- Windows :
  - ローカルクラスタ : `C:\NetworkRegistrar\Local\logs`
  - リージョナルクラスタ : `C:\NetworkRegistrar\Regional\logs`
- Linux :
  - 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は、まずこれらのログファイルの内容を確認して、何が失敗したかを判断します。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。

ログメッセージに失敗が明確に示されていない場合は、**debug\_install** ユーティリティスクリプトを使用して追加のデバッグ情報を収集できます。このスクリプトは、インストールが失敗した場合にのみ表示され、デフォルトでは Cisco Prime Network Registrar のプログラムファイルディレクトリにあります。

- Windows :
  - ローカルクラスタ : `C:\Program Files(x86)\Network Registrar\Local\debug_install.cmd`
  - リージョナルクラスタ : `C:\Program Files\Network Registrar\Regional\debug_install.cmd`
- Linux :
  - ローカルクラスタ : `/opt/nwreg2/local/debug_install.sh`
  - リージョナルクラスタ : `/opt/nwreg2/regional/debug_install.sh`

失敗の原因または解決策の特定についてサポートが必要な場合は、このスクリプトの出力を Cisco Systems に転送して詳細な分析を依頼してください。シスコの連絡先については、次のシスコの Web サイトを参照してください。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

## 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 \(19 ページ\)](#) を参照してください。

ローカルクラスタに Cisco Prime Network Registrar をインストールする場合、リージョナルクラスタへのローカルクラスタの登録をスキップできます。

**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 10.1* アドミニストレーションガイド』の「ローカルの追加 (Adding Local Clusters)」の項を参照してください。

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

---



## 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 \(37 ページ\)](#)
- [Cisco Prime Network Registrar の起動 \(38 ページ\)](#)
- [サーバの起動と停止 \(39 ページ\)](#)
- [サーバのイベントロギング \(42 ページ\)](#)
- [Windows インストールでの ACL の変更 \(42 ページ\)](#)

## 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 10.1 クイックスタートガイド \(Cisco Prime Network Registrar 10.1 Quick Start Guide\)](#)』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 10.1 DHCP ユーザガイド \(Cisco Prime Network Registrar 10.1 DHCP User Guide\)](#)』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 10.1 キャッシュおよび権威 DNS ユーザガイド \(Cisco Prime Network Registrar 10.1 Caching and Authoritative DNS User Guide\)](#)』を参照してください。
- ローカルとリージョナルの管理、Cisco Prime Network Registrar 仮想アプライアンスのセットアップなどの管理タスクを実行します。『[Cisco Prime Network Registrar 10.1 アドミニストレーションガイド \(Cisco Prime Network Registrar 10.1 Administration Guide\)](#)』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 10.1 CLI リファレンスガイド \(Cisco Prime Network Registrar 10.1 CLI Reference Guide\)](#)』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 10.1 REST APIs リファレンスガイド \(Cisco Prime Network Registrar 10.1 REST APIs Reference Guide\)](#)』を参照してください。

# Cisco Prime Network Registrar の起動

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、適切なライセンスファイル（Web UI）またはファイル名（CLI）を入力する必要があります。

Web UI または CLI でライセンス情報を入力するには、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、HTTP（非セキュアログイン）または HTTPS（セキュアログイン）の Web サイトを使用します。

```
http://hostname:http-port
```

```
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。
- *http-port* および *https-port* は、インストール時に指定されるデフォルトの HTTP または HTTPS ポートです。（[Cisco Prime Network Registrar のインストールおよびアップグレード（19 ページ）](#) を参照）。

Windows では、ローカルホストの [スタート (Start)] メニューから Web UI にアクセスできます。

- ローカルクラスタの場合：[スタート (Start)] > [プログラム (Programs)] > [Network Registrar IP Express 10.1] > [Network Registrar IP Express 10.1 ローカル Web UI (Network Registrar IP Express 10.1 local Web UI)]（またはセキュリティログインを有効にした場合は [Network Registrar IP Express 10.1 ローカル Web UI (セキュア) (Network Registrar IP Express 10.1 local Web UI (secure))] を選択します。
- リージョナルクラスタの場合：[スタート (Start)] > [プログラム (Programs)] > [Network Registrar IP Express 10.1] > [Network Registrar IP Express 10.1 リージョナル Web UI (Network Registrar IP Express 10.1 regional Web UI)]（またはセキュリティログインを有効にした場合は [Network Registrar IP Express 10.1 リージョナル Web UI (セキュア) (Network Registrar IP Express 10.1 regional Web UI (secure))] を選択します。
- CLI を起動するには、次の手順を実行します。

- Windows : *install-path*\bin ディレクトリに移動し、次のコマンドを入力します。

```
nrcmd -C cluster-ipaddress -N username -P password
```

- Linux : Navigate to the *install-path*\usrbin ディレクトリに移動し、次のコマンドを入力します。

```
install-path/usrbin/nrcmd -C clustername -N username -P password
```

**ステップ 2** インストール手順中にライセンス情報を入力しなかった場合は、ここで入力する必要があります。

(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、インストール時また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、cdns) を選択できます。

- 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
```

**ステップ3** インストール手順中に作成したユーザ名とパスワードを入力します。

## サーバの起動と停止

Windows では、Windows の [コントロールパネル (Control Panel) ] の [サービス (Services) ] 機能から Cisco Prime Network Registrar サーバエージェントを停止および起動できます。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 10.1 アドミニストレーションガイド』を参照してください。

## Windows でのサーバの起動と停止

Windows でサーバ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** [スタート (Start) ]>[設定 (Settings) ]>[コントロールパネル (Control Panel) ]>[管理ツール (Administrative Tools) ]>[サービス (Services) ] の順に選択します。
- ステップ2** [サービス (Service) ] リストから、[Network Registrar IP Express ローカルサーバエージェント (Network Registrar IP Express Local Server Agent) ] または [Network Registrar IP Express リージョナルサーバエージェント (Network Registrar IP Express Regional Server Agent) ] を選択します。
- ステップ3** 必要に応じて [再起動 (Restart) ] または [停止 (Stop) ] をクリックし、次に [閉じる (Close) ] をクリックします。

## Linux でのサーバーの起動と停止

Linux では、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。



(注) **nradmin** として実行しているときに Cisco Prime Network Registrar を起動および停止するには、**nradmin** グループ (またはルート) のユーザとしてサーバにログインする必要があります。**nradmin** としてログインすることはできません。

```
# /opt/nwreg2/local/bin/cnr_service start  
# /opt/nwreg2/local/bin/cnr_service stop
```

Linux でサーバ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 *nwregregion* スクリプトを実行し、サーバエージェントを起動します。

RHEL/CentOS 6.x ローカルクラスタの場合 :

```
# /etc/init.d/nwreglocal start
```

RHEL/CentOS 7.x ローカルクラスタの場合 :

```
# systemctl start nwreglocal
```

RHEL/CentOS 6.x リージョナルクラスタの場合 :

```
# /etc/init.d/nwregregion start
```

RHEL/CentOS 7.x リージョナルクラスタの場合 :

```
# systemctl start nwregregion
```

**ステップ 3** *cnr\_status* コマンドを入力して、サーバが実行されていることを確認します。

```
# install-path/usrbin/cnr_status
```

**ステップ 4** *stop* 引数を指定して *nwreglocal* スクリプトまたは *nwregregion* スクリプトを実行し、サーバエージェントを停止します。

RHEL/CentOS 6.x ローカルクラスタの場合 :

```
# /etc/init.d/nwreglocal stop
```

RHEL/CentOS 7.x ローカルクラスタの場合 :

```
# systemctl stop nwreglocal
```

RHEL/CentOS 6.x リージョナルクラスタの場合 :



```
# /etc/init.d/nwregregion stop
```

RHEL/CentOS 7.x リージョナルクラスタの場合：

```
# systemctl stop nwregregion
```

---

## 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** 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。
- (注) リージョンクラスタの BYOD Web サーバはデフォルトで停止するため、手動で再起動する必要があります。BYOD サーバを自動的に再起動するには、autostart を true に設定する必要があります。
- 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。

- Windows :
  - ローカルクラスタ : C:\NetworkRegistrar\Local\logs
  - リージョナルクラスタ : C:\NetworkRegistrar\Regional\logs
- Linux :
  - 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。



**注意** Windows では、イベントログがいっぱいになった場合に最新システムのアプリケーション イベント ログ エントリが失われないようにするには、イベント ビューア システム アプリケーションを使用し、アプリケーションログの [ イベントログ設定 (Event Log Settings) ] で [ 必要に応じてイベントを上書きする (Overwrite Events as Needed) ] チェックボックスをオンにします。このオプションが適切に設定されていないことがインストールプロセスによって検出された場合は、修正アクションを通知する警告メッセージが表示されます。

## Windows インストールでの ACL の変更

Windows の Cisco Prime Network Registrar インストールプログラムは、インストールされたファイルとディレクトリへのアクセスを制限するために ACL を変更しようとしません。これらのファイルとディレクトリへのアクセスを制限する場合は、ネイティブの Microsoft ユーティリティ (**cacls** および **icacls**) を使用して、ファイルとディレクトリの権限を手動で変更します。

ACL を手動で変更する場合は、インストールエリア全体の内容が管理者システムグループ以外のすべてのユーザに対して読み取り専用になるように設定を制御することを推奨します。

次のファイルとサブディレクトリには、管理者システムグループのみがアクセスできるデータが含まれています。

- *install-path*\conf\cnr.conf
- *install-path*\tomcat\conf\server.xml
- *install-path*\conf\priv\
- *install-path*\data\

ACL の変更は厳密にオプションであり、Cisco Prime Network Registrar は変更を加えなくても正常に機能します。**cacls** と **icacls** のユーティリティの使用方法については、Microsoft 提供のマニュアルを参照してください。





## 第 7 章

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

アンインストール手順は、ご使用のオペレーティングシステムによって異なります。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 10.1 アドミニストレーションガイド』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 \(39 ページ\)](#) を参照してください。

- [Windows でのアンインストール \(45 ページ\)](#)
- [Linux でのアンインストール \(46 ページ\)](#)
- [Windows でのパフォーマンス モニタリング ソフトウェアの実行 \(46 ページ\)](#)

## Windows でのアンインストール

Windows で Cisco Prime Network Registrar をアンインストールするには、以下を行います。

**ステップ 1** Windows のコントロールパネルから [プログラムの追加と削除 (Add/Remove Programs)] 機能を選択します。

または

Windows の [スタート (Start)] メニューから [Network Registrar 10.1 のアンインストール (Uninstall Network Registrar IP Express 10.1)] を選択します。アンインストールプログラムは、サーバおよびユーザインターフェイス コンポーネントを削除しますが、ユーザデータファイルは削除しません。オプションで、Cisco Prime Network Registrar フォルダを削除して、すべての Cisco Prime Network Registrar データを削除します。

- (注) Cisco Prime Network Registrar フォルダ内の共有ライブラリの削除を妨げる可能性があるパフォーマンスモニタリングと統合するソフトウェアに関連するサービスを、一時的に停止します。

ステップ 2 アンインストールが完了したら再起動します。

## Linux でのアンインストール

Linux で Cisco Prime Network Registrar をアンインストールするには、*install-path*/usrbin ディレクトリから、**uninstall\_cnr** プログラムを実行します。

```
./uninstall_cnr

Stopping Server Agent...

Deleting startup files...

Removing Network Registrar...

cannot remove /opt/nwreg2/usrbin - directory not empty

cannot remove /opt/nwreg2/conf - directory not empty

package optnwreg2 not found in file index

Note that any files that have been changed (including your database) have not been
uninstalled. You should delete these files by hand when you are done with them, before
you
reinstall the package.
```

**checkinstall** 警告は、アンインストールプログラムがサーバおよびユーザ インターフェイス コンポーネントを削除しても、空でないディレクトリを削除できないことを意味します。インストール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、**uninstall\_cnr** スクリプトの実行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ベースとログファイルを削除します。



- (注) Cisco Prime Network Registrar が nradmin としてインストールされると、アンインストールプロセスによって残りのすべてのファイルの所有権がスーパーユーザ（ルート）にリセットされます。

## Windows でのパフォーマンス モニタリング ソフトウェアの実行

Windows システムで、Windows パフォーマンスモニタと統合するソフトウェアがインストールされている状態で、Cisco Prime Network Registrar をアンインストールして関連するデータディレクトリを削除しようとする、競合するソフトウェアが特定の共有ライブラリを保持してい

る場合があります。このアクションにより、Cisco Prime Network Registrar フォルダおよびディレクトリ自体からこれらのファイルを削除できなくなります。これを防ぐには、次の手順を実行します。

1. パフォーマンス モニタリングソフトウェアに関連付けられているサービスを停止します。
2. Network Registrar フォルダを削除します。
3. サービスを再起動します。







## 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 10.1 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 \(49 ページ\)](#)
- [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 \(50 ページ\)](#)
- [Cisco Prime Network Registrar 仮想アプライアンスのアップグレード \(58 ページ\)](#)
- [次のステップ : Cisco Prime Network Registrar 仮想アプライアンス \(60 ページ\)](#)

## 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3つあります。

- VMware ESXi 6.x で実行される OVA
- KVM ハイパーバイザで実行される KVM キット
- 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3つのキットすべてに適用されます。

これらの各キットは、1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 5.4 GB の空き容量がある 7.5 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 14 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タ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 : 35 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 6.x、KVM ハイパーバイザ、または OpenStack の3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 10.1 アドミニストレーションガイド

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 6.x 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\_10\_1\_local.ova*
- リージョナル仮想アプライアンスでは、*cpnr\_10\_1\_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。

ESXi 6.5 より前のバージョンでは [ディスクフォーマット (Disk Format)] ウィンドウが表示され、ESXi 6.5 以降のバージョンでは [展開オプション (Deployment Options)] ウィンドウが表示されます。

ESXi 6.5 より前のバージョンでは、[シックプロビジョニング形式 (Thick provisioned format)] がデフォルトで選択され、ESXi 6.5 以降のバージョンでは、[シンプロビジョニング形式 (Thin provisioned format)] がデフォルトで選択されます。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 10.1 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/CentOS 7.x でのネットワークアクセスの設定 (83 ページ) を参照してください。

## KVMハイパーバイザ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、.bz2 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\_10\_1\_local.kvm.tar.bz2*
- リージョナル仮想アプライアンスでは、*cpnr\_10\_1\_regional.kvm.tar.bz2*

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。

KVM ハイパーバイザに Cisco Prime Network Registrar をインストールするには、次のコマンドを使用してディストリビューション tar アーカイブ (*cpnr\_10\_1\_local.kvm.tar.bz2* or *cpnr\_10\_1\_regional.kvm.tar.bz2*) を展開します。

```
root$ tar xvjf cpnr_10_1_local.kvm.tar.bz2
```

または

```
root$ tar xvjf cpnr_10_1_regional.kvm.tar.bz2
```

ローカル KVM キットとリージョナル KVM キットの両方を展開する場合は、ファイル名の競合を避けるために別々のディレクトリで解凍する必要があります。

展開には数分かかり、14 GB 以上の空きディスク容量が必要です。次のファイルが表示されます。

- cpnr\_10\_1\_local-disk1.raw* : 仮想マシンのディスクが含まれます。
- installonkvm* : 仮想マシンをインストールします。
- readme.kvm.txt* : インストール手順が含まれています。

`cpnr_10_1_local-disk1.raw` ファイルは、実装される Cisco Prime Network Registrar KVM 仮想マシンのディスクファイルとして使用される実際のファイルです。このファイルは、Cisco Prime Network Registrar KVM 仮想マシンの仮想ディスクの「ソースパス」として長期間存在するディレクトリに配置する必要があります。仮想マシンをインストールした後も移動できますが、正しい場所で開始する方が簡単です。`installonkvm` スクリプトも一緒に移動する必要があります。`installonkvm` スクリプトは、正常に動作するために実行可能である必要があります。

インストールを続行するには、`readme.kvm.txt` file ファイルで指定されている手順に従います。

インストールが完了したら、`nmcli` を使用した RHEL/CentOS 7.x でのネットワークアクセスの設定 (83 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、`.ova` 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_10_1_local.qcow2`
- リージョナル仮想アプライアンスでは、`cpnr_10_1_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 1 つの VCPU、8 GB の RAM、および少なくとも 14 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 14 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 \(49 ページ\)](#) 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。

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、または KVM キットを使用する場合は、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 サーバを検出できる 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、リージョナル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ー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 7 GB 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、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 CentOS 7.7 にアップグレードする手順について説明します。

## 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 \(19 ページ\)](#) 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 `install-path/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4** 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** VMware vSphere を使用して Cisco Prime Network Registrar 仮想アプライアンスを再起動します。

## 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 \(58 ページ\)](#) 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 `ncmd` 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。`ncmd` 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 `ncmd` 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。



(注) KVM キットは、自動起動を有効にしてインストールされます。

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

ルートユーザとしてログインすることで、CentOS 7.7 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、ルートとしてログインしないように構成し、別のユーザとしてログイン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 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。

## 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** 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** 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** 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。



## 付録 **A**

# サイレントインストールの実行

この付録では、次の項について説明します。

- [サイレントインストールの実行](#) (63 ページ)

## サイレントインストールの実行

この付録では、Cisco Prime Network Registrar 製品のサイレントインストール、アップグレード、またはアンインストールを実行する方法について説明します。サイレントインストールまたはサイレントアップグレードでは、サイレントインストール応答ファイルの作成時に指定された構成値に基づいて、無人で製品をインストールできます。



**注意** サイレントインストールを実行しているシステムの正しい設定が含まれていないサイレント応答ファイルを使用しようとすると、予測不可能な結果が生じる可能性があります。

サイレント応答ファイルを生成または作成するには、次の手順を実行します。

**ステップ 1** サイレントインストールまたはサイレントアップグレードごとに、次のコマンドを使用して個別の応答ファイルを作成します。

- Windows :

```
setup.exe -r
```

通常どおり、インストールまたはアップグレードのステップを完了します。このコマンドは、指定したパラメータに従って Cisco Prime Network Registrar をインストールまたはアップグレードします。

(注) Cisco Prime Network Registrar がすでにインストールされている場合は、**setup.exe** によって既存のバージョンがアンインストールされ、Cisco Prime Network Registrar がインストールされていない場合はインストールが実行されます。

また、これらのパラメータに基づいて **setup.iss** サイレント応答ファイルを生成します。Windows のインストールディレクトリ (C:\WINDOWS など) でこのファイルを探します。コマンドを使用するたびに、ファイルは上書きされます。

このファイルの名前を変更するか配置場所を変更したうえで、**ステップ 2** のサイレントプロセスを実行することを推奨します。ファイルを **local-nr-https-install** などの識別しやすい名前に変更して、一時フォルダに移動してください。

• Linux :

次の表に示すエントリを含むテキストサイレント応答ファイルを作成します。

表 4: Linux のサイレント応答ファイルのエントリ

サイレント応答ファイルのエントリ	説明
BACKUPDIR=	現在の Cisco Prime Network Registrar インストールファイルを保存するパス (ただし、PERFORM_BACKUP=y の場合のみ)
CCM_LOCAL_SERVICES=	有効にするサービス (dhcp、dns、または cdns)
CCM_PORT=	中央構成管理 (CCM) ポート。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> <li>• CNR_CCM_MODE=local の場合は <b>1234</b></li> <li>• CNR_CCM_MODE = regional の場合は <b>1244</b></li> </ul>
CCM_REGIONAL_IP_ADDR=	リージョンサーバの IPv4 アドレス
CCM_REGIONAL_IPV6_ADDR=	リージョンサーバの IPv6 アドレス
CCM_REGIONAL_SCP_PORT	リージョンサーバの SCP ポート番号
CNR_ADMIN=	スーパーユーザ名。スーパーユーザ名の設定をスキップするには、値を CNR_ADMIN=unset にする必要があります。
NRADMIN=	非ルートユーザ。非ルートユーザとして Cisco Prime Network Registrar をインストールするには、値は NRADMIN=y である必要があります。
CNR_PASSWORD=	スーパーユーザのパスワード。スーパーユーザのパスワードの設定をスキップするには、値を CNR_PASSWORD=unset にする必要があります。



サイレント応答ファイルのエントリ	説明
CNR_CCM_MODE=	CCM モード。 <b>local</b> または <b>regional</b> に設定します。
CNR_CCM_TYPE=	GSS のインストール用に予約されています。常に <b>cnr</b> に設定します。
CNR_EXISTS=	<b>y</b> (推奨) に設定すると、インストール時またはアップグレード時に、開いている CLI 接続を強制終了します。それ以外の場合は、基本的に廃止です。
CNR_LICENSE_FILE=	ライセンスファイルへの完全修飾パス。 CNR_CCM_MODE=local の場合、 CNR_LICENSE_FILE=unset を設定します。
CNR_SECURITY_MODE=	セキュリティモードの設定： <ul style="list-style-type: none"> <li>• 必須。接続を保護できない場合は失敗します。</li> <li>• これはオプションです。セキュアでない接続へのフォールバックを許可します。</li> <li>• ディセーブル。スタートアップ時にセキュリティモジュールをロードしないでください。</li> </ul>
DATADIR=	データディレクトリへの完全修飾パス。
JAVADIR=	Java インストールへの完全修飾パス (JRE 1.8)。
KEYSTORE_FILE=	USE_HTTPS=y の場合、キーストアファイルへの完全修飾パス。
KEYSTORE_PASSWORD=	USE_HTTPS=y の場合、キーストアファイルの生成時に使用されるパスワード。
LOGDIR=	ログファイルディレクトリへの完全修飾パス。
PERFORM_BACKUP=	現在のインストールファイル (存在する場合) をバックアップするかどうかを指定します。クリーンインストールでも <b>y</b> に設定できます (BACKUPDIR も参照)。
ROOTDIR=	製品ファイルの完全修飾インストールパス。 bin、classes、cnrwebui、conf、docs、examples、extensions、lib、misc、schema、tomcat、usrbin サブディレクトリが含まれます。

サイレント応答ファイルのエントリ	説明
START_SERVERS=	完全インストール（プロトコルサーバを使用）の場合は、 <b>y</b> に設定して、インストールまたはアップグレードを完了させる必要があります。また、インストール/アップグレード後に <b>Cisco Prime Network Registrar</b> 製品が起動されます。クライアント専用インストールの場合は、 <b>n</b> に設定する必要があります。
TEMPDIR=	一時ディレクトリへの完全修飾パス。
USE_HTTP=	Web UI サーバが HTTP 接続をリッスンするかどうかを設定します。USE_HTTP または USE_HTTPS の一方または両方を <b>y</b> に設定する必要があります。
USE_HTTPS=	Web UI サーバが HTTPS 接続をリッスンするかどうかを設定します。USE_HTTP または USE_HTTPS の一方または両方を <b>y</b> に設定する必要があります（KEYSTORE_FILE と KEYSTORE_PASSWOR も参照）。
WEBUI_PORT =	Web UI が HTTP トラフィックに使用するポート番号。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> <li>• CNR_CCM_MODE=local の場合は <b>8080</b></li> <li>• CNR_CCM_MODE = regional の場合は <b>8090</b></li> </ul>
WEBUI_SEC_PORT=	Web UI が HTTPS トラフィックに使用するポート番号。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> <li>• CNR_CCM_MODE=local の場合は <b>8443</b></li> <li>• CNR_CCM_MODE = regional の場合は <b>8453</b></li> </ul>
WS_PORT=	Web サービスが HTTP トラフィックに使用するポート番号。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> <li>• CNR_CCM_MODE=local の場合は <b>8080</b></li> <li>• CNR_CCM_MODE = regional の場合は <b>8090</b></li> </ul>
WS_SEC_PORT=	Web サービスが HTTPS トラフィックに使用するポート番号。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> <li>• CNR_CCM_MODE=local の場合は <b>8443</b></li> <li>• CNR_CCM_MODE = regional の場合は <b>8453</b></li> </ul>

サイレント応答ファイルのエントリ	説明
WEB_SERVICES=	Web サービス (DNS ENUM および REST API) を有効にするには <b>y</b> 、無効にするには <b>n</b> に設定します。
CNR_BYOD_ENABLE=	BYOD サービスを有効にするには <b>y</b> 、無効にするには <b>n</b> に設定します。

**ステップ 2** 各インスタンスにサイレントインストールまたはサイレントアップグレードを起動するには、次のコマンドを使用します。

- Windows :

```
setup.exe -s -flpath+response-file
```

(注) 応答ファイルが i386 ディレクトリに格納されていて、`setup.exe` がそのディレクトリから実行されなければ、`-fl` 引数に応答ファイルの完全修飾パスを指定しないとサイレントインストールは失敗します。

- Linux :

```
install_cnr -r response-file
```

**ステップ 3** 製品をアンインストール場合 :

- Windows : アンインストール応答ファイルを生成し、次を実行します。

```
setup.exe -s -fluninstall_response_file
```

- Linux : サイレントアンインストールを起動します (このコマンドは、エラー時以外は非インタラクティブです)。

```
uninstall_cnr
```





## 付録 **B**

# 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](#) (69 ページ)
- [ラボでの Cisco Prime Network Registrar のインストール](#) (69 ページ)
- [ラボインストールのテスト](#) (70 ページ)
- [ラボ環境でのアンインストール](#) (70 ページ)

## 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 Linux 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) 単一の Windows マシンにローカルクラスタとリージョナルクラスタの両方をインストールすることはできません。



**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 (19 ページ) の手順に従って、Linux マシンに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。ローカルクラスタのインストールを指定します。
- 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。リージョナルクラスタのインストールを指定します。
- 

## 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** ポート番号に適した URL を使用して、ローカルクラスタの Web UI を起動し、ログインします。デフォルトでは、ローカルポート番号は HTTP 接続の場合は **8080**、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** ポート番号に適した URL を使用して、リージョナルクラスタの Web UI を起動し、ログインします。デフォルトでは、リージョナルのポート番号は HTTP 接続の場合は **8090**、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

Cisco Prime Network Registrar をアンインストールする必要がある場合は、[Linux でのアンインストール \(46 ページ\)](#) の手順に従います。

デュアルモードのインストール環境でリージョナルクラスタのみまたはローカルクラスタのみをアンインストールするオプションはありません。



## 付録 C

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

この項では、Linux および Windows プラットフォームに Cisco Prime Network Registrar SDK をインストールする方法について説明します。5510 SDK をインストールする前に、JRE 1.8 または同等の JDK 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。

- [Linux へのインストール \(71 ページ\)](#)
- [Windows へのインストール \(72 ページ\)](#)
- [インストールのテスト \(72 ページ\)](#)
- [互換性に関する考慮事項 \(72 ページ\)](#)

## Linux へのインストール

Linux プラットフォームに 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/cnr-sdk.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:.
```

---

## Windows へのインストール

Windows プラットフォームに 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。

```
> md c:\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。

```
> c:
> cd \cnr-sdk
> tar xvf sdk_tar_file_location\cnrsdk.tar
```

オプションで、Winzip を使用して cnrsdk.tar を C:\cnr-sdk ディレクトリに展開することもできます。

**ステップ 2** PATH 変数および CLASSPATH 変数を設定します。

```
> set PATH=%PATH%;c:\cnr-sdk\lib
> set CLASSPATH=c:\cnr-sdk\classes\cnrsdk.jar;.
```

---

## インストールのテスト

Linux では、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
```

Windows では、次のテストプログラムで CLASSPATH が正しく設定されていることを確認します。

```
> java -jar c:\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 10.1* リリースノート』の「*SDK* の互換性に関する考慮事項 (*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 **D**

# 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 \(75 ページ\)](#)

## 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 10.1 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せん。

**ステップ 1** Cisco Prime Network Registrar インストールフォルダの *install-path/tomcat/conf* フォルダにある **server.xml** ファイルを開きます。

**ステップ 2** 次の例に示すように、HTTPS コネクタ文に暗号文を追加し、許可される暗号をリストします。

- (注) **port**, **keystoreFile**, and **keystorePass** の値は、システムで設定した値と一致する必要があります。

```
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
maxHttpHeaderSize="8192"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false"
```

```
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,  
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"  
  
keystoreFile="conf/.keystore"  
  
sslProtocol="TLSv1.2"  
  
sslEnabledProtocols="TLSv1.2"/>
```

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

---



## 付録 E

# 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](#) (77 ページ)

## 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。
  - Red Hat 6 :  
[https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/pdf/Security\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-6-Security\\_Guide-en-US.pdf](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf)
  - RHEL/CentOS 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](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)  
[https://www.cisecurity.org/benchmark/red\\_hat\\_linux/](https://www.cisecurity.org/benchmark/red_hat_linux/)  
[https://www.cisecurity.org/benchmark/centos\\_linux/](https://www.cisecurity.org/benchmark/centos_linux/)
  - Windows Server 2012 :  
[https://www.cisecurity.org/wp-content/uploads/2017/04/CIS\\_Microsoft\\_Windows\\_Server\\_2012\\_R2\\_Benchmark\\_v2.2.0.pdf](https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf)
  - 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](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 10.1* アドミニストレーションガイド』の「*Cisco Prime Network Registrar* サービスのデフォルトポート (*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 10.1* アドミニストレーションガイド』の「*DNS* パフォーマンスとファイアウォールの接続追跡 (*DNS Performance and Firewall Connection Tracking*)」の項を参照してください。
- 非 root アカウントを使用して Cisco Prime Network Registrar をインストールし、セキュリティ機能を使用します（つまり、https で、セキュアな SCP セッションが必要です）。
- 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 10.1* 権威およびキャッシング DNS ユーザガイド』の「権威 DNSSEC の管理 (*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（の「トランザクションセキュリティ (Transaction Security)」の項または「GSS-TSIG」の項 *Cisco Prime Network Registrar 10.1 DHCP ユーザガイド* を参照）をマスターサーバアドレスに追加することができます。それには、形式 *addresskey* を使用して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 10.1 権威およびキャッシング DNS ユーザガイド*』の「ゾーン分散の作成 (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 10.1 権威およびキャッシング DNS ユーザガイド*』の「キャッシングレート制限の管理 (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](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](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 10.1 DHCP ユーザガイド*』の「拡張機能を使用したおしゃべりクライアントの防止 (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 10.1* アドミニストレーションガイド』の「外部認証サーバ (*External Authentication Servers*)」の項を参照してください。





## 付録 F

# 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 \(81 ページ\)](#)
- [NUMA の最適化 \(81 ページ\)](#)
- [ハイパースレッディングの考慮事項 \(82 ページ\)](#)

## 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、バッテリー 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 G

# nmcli を使用した RHEL/CentOS 7.x 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/CentOS 7.x でのネットワークアクセスの設定](#) (83 ページ)

## nmcli を使用した RHEL/CentOS 7.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。これは、CentOS Linux でネットワークアクセスを構成する従来の方法からの重要な変更です。

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** を使用できるようになるにしたいが、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。

**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 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。

- Local RHEL/CentOS 6.x : `/etc/init.d/nwreglocal restart`
- Local RHEL/CentOS 7.x : `systemctl restart nwreglocal`
- リージョン RHEL/CentOS 6.x : `/etc/init.d/nwregregion restart`
- リージョン RHEL/CentOS 7.x : `systemctl restart nwregregion`

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 CentOS 7.7 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 H

# nmcli を使用した IP アドレスの変更

この付録では、次の項について説明します。

- [nmcli を使用した IP アドレスの変更 \(87 ページ\)](#)

## nmcli を使用した IP アドレスの変更

ローカルクラスタまたはリージョナルクラスタの IP アドレスを変更する必要がある場合は、nmcli を使用して非常に簡単に変更できます。

**ステップ 1** 変更するインターフェイスに関連付けられている接続を確認します。nmcli d を使用してデバイスを検索し、nmcli c を使用して IP アドレスを変更するデバイスに関連付けられている接続を確認できます。

**ステップ 2** 新しい IP アドレスを使用して接続を設定します。

```
nmcli con mod connection ip4 new-ip-address
```

**ステップ 3** 変更された接続を、関連付けられているインターフェイスに適用します。これにより、実際に IP アドレスが変更されます。

```
nmcli con up connection
```

**ステップ 4** Cisco Prime Network Registrar を実行しているシステム（仮想アプライアンスなど）の IP アドレスを変更した後、システムの新しい IP アドレスを管理サーバに認識させるために再起動する必要があります。ローカルクラスタの場合は `systemctl restart nwreglocal` コマンドを使用し、リージョナルクラスタの場合は `systemctl restart nwregregion` コマンドを使用します。







付録

## 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、64 ビットの Cisco Prime Network Registrar 8.3.5.4 以降のシステムサイジングに役立つ、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について説明します。

- [DNS システムのデプロイメント上の制限 \(89 ページ\)](#)
- [DNS データベースアーキテクチャ \(90 ページ\)](#)
- [DNS システムのサイジング \(91 ページ\)](#)

### DNS システムのデプロイメント上の制限

Cisco Prime Network Registrar では、権威 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。

- 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 ～ 1000 の RR と 1 ～ 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 ～ 100,000 の RR および 100 ～ 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 ～ 5000 の範囲で指定する必要があります。

## 大規模な展開

- 100,000 ～ 25,000,000 の RR と 1000 ～ 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 ～ 10,000 の範囲で指定する必要があります。





## 付録 J

# 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、システムサイジングに役立つキャッシング DNS のキャパシティとパフォーマンスのガイドラインについて説明します。推奨事項は、64 ビットの Cisco Prime Network Registrar 8.3.5.4 以降に基づいています。

- [DNS システムのデプロイメント上の制限 \(95 ページ\)](#)
- [キャッシング DNS システムのサイジング \(96 ページ\)](#)
- [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 \(97 ページ\)](#)

## 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

# 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～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～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 ～ 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。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)。
- 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 **K**

# DHCP のキャパシティとパフォーマンスのガイドライン

この項では、Cisco Prime Network Registrar 9.0 以降、および 64 ビットバージョンの Cisco Prime Network Registrar 8.3.2 以降のキャパシティとパフォーマンスに関するガイドラインを示します。

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。これらの推奨事項は、主に Linux リリースに適用されます。

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

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、単に拡張機能呼び出しの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する必要があります。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、

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、非常にビジネス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せん。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想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黙化すると、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 10.1 DHCP ユーザガイド』の「拡張機能を使用したおしゃべりクライアントの防止 (Preventing Chatty Clients by Using an Extension)」の項を参照してください。

- 識別レトリミッタ

識別レトリミッタは、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 10.1 DHCP ユーザガイド』の「DHCP サーバの詳細属性の設定 (Setting Advanced DHCP Server Attributes)」の項を参照してください。

### サーバに必要なリースの数

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。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、SSD、または 15K RPM HDD 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。非常に大規模なサービスプロバイダネットワークでは、これが 100 GB 以上になることがあります。



---

**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

[ライセンスの追加 (Add License) ] ページ [38](#)

### C

ciphers [75](#)  
    調節 [75](#)  
CLI [2, 9, 38](#)  
    ライセンスセットキー [38](#)  
    起動 [38](#)  
    要件 [9](#)  
cnr\_status [27, 40](#)  
cnr\_status ユーティリティ [27, 40](#)

### D

debug\_install スクリプト [35](#)  
DHCP サーバ [2](#)  
DNS サーバ [2](#)

### G

gtar [21](#)  
gtar ユーティリティ [21](#)  
gzip [21](#)  
gzip ユーティリティ [21](#)

### I

install\_cnr ユーティリティ [21, 67](#)

### J

Java [9, 25](#)  
    ディレクトリ [25](#)  
    要件 [9](#)  
Java Development Kit (JDK) [20](#)  
Java Runtime Environment (JRE) [20](#)  
JAVA\_HOME 設定 [20](#)

### K

keytool ユーティリティ [20](#)

### L

Linux [10, 19, 21, 27, 40, 46, 64, 67](#)  
    cnr\_status [27, 40](#)  
    gtar [21](#)  
    gzip [21](#)  
    install\_cnr [21, 67](#)  
    uninstall\_cnr [46](#)  
    アンインストールする [46](#)  
    スーパーユーザアカウントと root アカウント [19](#)  
    変数宣言ファイル [64](#)  
    要件 [10](#)

### N

Network Registrar [1](#)  
    概要 [1](#)  
nwreglocal および nwregregion [40](#)  
nwreglocal ユーティリティ [40](#)  
nwregregion ユーティリティ [40](#)

### O

OVA [49](#)

### R

RAM の要件 [10](#)  
root アカウント [19](#)

### S

SDK [71-72](#)  
    互換性に関する考慮事項 [72](#)  
    設置 [71](#)  
Setup.exe ファイル [21](#)

## T

tail コマンド 42

## U

uninst.exe ユーティリティ 67  
uninstall\_cnr ユーティリティ 46

## V

VMWare vCenter 52  
VMWare vSphere 52

## W

Web UI 2, 9, 26, 38, 75  
    ciphers 75  
    ポート 26  
    起動 38  
    要件 9  
Web ベースのユーザインターフェイス 2  
Windows 10, 21–22, 38, 42, 45, 67  
    Setup.exe ファイル 21  
    uninst.exe 67  
    アンインストールプログラム 45  
    プログラムの実行場所 22  
    ロギング 42  
    自己解凍実行可能ファイル 21  
    要件 10

## あ

アーカイブ 24  
アーカイブディレクトリ 24  
    Local.sav ディレクトリ 24  
    Regional.sav ディレクトリ 24  
アクセス 38  
アップグレード 1, 19–22, 24–27, 63, 69  
    Java ディレクトリ 25  
    JAVA\_HOME 設定 20  
    JRE と JDK の要件 20  
    silent 63  
    Web UI ポート 26  
    アーカイブ 24  
    クラスタ モード 22  
    システム権限 19  
    データベースステータス 24  
    ネットワーク ディストリビューション 21  
    メッセージの処理 27  
    ラボ評価 69

アップグレード (続き)  
    安全なログイン 20  
    概要 1  
    接続タイプ 25  
アンインストールする 45–46, 70  
    Linux 46  
    Windows 45  
    ラボ評価 70

## い

インストール 1, 12, 15, 19–20, 22–23, 25–27, 35, 63, 69  
    Java ディレクトリ 25  
    JAVA\_HOME 設定 20  
    JRE と JDK の要件 20  
    silent 63  
    Web UI ポート 26  
    アップグレード 15  
        ライセンスキー 15  
    アップグレードプロセス 19  
    クラスタ モード 22  
    システム権限 19  
    タイプ 25  
    チェックリスト 15  
    ディレクトリ 23  
    トラブルシューティング 35  
    メッセージの処理 27  
    モード 12  
        new 12  
        データ移行なしのアップグレード 12  
        データ移行を伴うアップグレード 12  
    ラボ評価 69  
    リージョナルディレクトリ 23  
    ローカルディレクトリ 23  
    ログ ファイル 35  
        install\_cnr\_log 35  
        lease\_upgrade\_log 35  
    安全なログイン 20  
    概要 1  
    接続タイプ 25

## う

ウイルススキャン 18  
    ディレクトリの除外 18  
ウイルススキャンのディレクトリの除外 18

## え

エラーロギング 42

## お

- オペレーティング システム 9-10
  - バージョン 10
  - 要件 9

## き

- キーストアファイル 20

## く

- クライアントのみのインストール 25
- クラスタ 22
  - モード 22
  - リージョン 22
  - ローカル (local) 22

## こ

- コマンドラインインターフェイス 2

## さ

- サーバ 2, 17, 39, 42
  - DHCP 2
  - DNS 2
  - ロギングイベント 42
  - 起動 39
  - 起動と停止 39
  - 他との実行 17
  - 停止 39
- サーバエージェント 27
- サーバエージェントのステータス 27
- サーバとクライアントのインストール 25
- サーバログの表示 42
- サイレントインストール 63

## す

- スーパーユーザアカウント 19

- ステータスのチェック 27

## せ

- セットアップ 22

## て

- ディスク領域の要件 10
- データベースステータス 24

## ね

- ネットワーク ディストリビューション 21

## め

- メッセージの処理 27
- メディアの圧縮解除 21
- メディアの展開 21

## ら

- ライセンスキー 12, 38
- ライセンスセットキーコマンド (CLI) 38
- ラボ評価のためのインストール 69

## り

- リージョナルモード 22

## ろ

- ローカルモード 22
- ロギング 42
  - Windows 42
    - サーバイベント 42
    - スタートアップ 42
- ログ ファイル 35
  - install\_cnr\_log ファイル 35
  - lease\_upgrade\_log ファイル 35

