



Cisco Prime Network Registrar 10.1 アドミニストレーションガイド

初版：2019年12月16日

最終更新：2021年10月19日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <http://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 部 :

使用する前に 17

第 1 章

Cisco Prime Network Registrar の概要 1

- 対象ユーザー 1
- リージョンおよびローカル クラスタ 2
- 導入シナリオ 3
 - 中小規模の LAN 3
 - 大企業およびサービス プロバイダ ネットワーク 3
- 設定とパフォーマンスの注意事項 4
 - 関連項目 5
 - 一般的な設定時の注意事項 5
 - 特別な構成事例 6
 - パフォーマンスに関する一般的な注意事項 6
 - 以前のリリースとの相互運用性 7

第 2 章

Cisco Prime Network Registrar ユーザー インターフェイス 9

- 管理コンポーネント 9
- Web ベースのユーザー インターフェイスの概要 11
 - 関連項目 11
 - サポートされる Web ブラウザ 11
 - アクセス セキュリティ 11
 - Web UI へのログイン 12
 - 複数のユーザー 13
 - パスワードの変更 13

Web UI のナビゲート	14
続行する前のページ解決の待機	15
Web UI での変更のコミット	15
ロールと属性の可視性の設定	15
属性の表示と変更	16
属性のグループ化とソート	16
属性の変更	16
属性ヘルプの表示	16
左側のナビゲーション ペイン	16
ヘルプ ページ	17
ログアウト	18
ローカル クラスタ Web UI	18
関連項目	18
ローカルの基本メイン メニュー ページ	18
ローカルの詳細なメイン メニュー ページ	20
ローカル ユーザーの環境設定の設定	21
ローカル Web UI でのクラスタの構成	23
リージョン クラスタ Web UI	23
関連項目	24
コマンドライン インターフェイス	24
Prime Network Registrar でのグローバル検索	26

第 3 章	サーバー ステータス ダッシュボード	27
	ダッシュボードを開く	27
	表示タイプ	28
	一般ステータス インジケータ	29
	アラートレベルのグラフィックインジケータ	29
	グラフの拡大と変換	29
	凡例	29
	テーブル	30
	折れ線グラフ	30

面グラフ	31
その他のチャートタイプ	32
ダッシュボード要素のヘルプの取得	33
表示のカスタマイズ	33
表示の更新	34
ポーリング間隔の設定	34
表としてのグラフの表示	34
CSV形式へのエクスポート	34
含めるダッシュボード要素の選択	35
サーバーチャートタイプの設定	35
ホストメトリック	37
システムメトリック	37
JVMメモリ使用率	38

第 II 部 : **ローカルおよびリージョンの管理** 41

第 4 章	管理者の管理	43
	管理者、グループ、ロール、テナント	43
	関連項目	44
	管理者とグループ、ロール、およびテナントとの関連	44
	管理者タイプ	45
	ロール、サブロール、および制約	45
	グループ	49
	外部認証サーバー	50
	RADIUS 外部認証サーバーの設定	50
	AD 外部認証サーバーの設定	52
	テナントの管理	54
	テナントの追加	55
	テナントの編集	56
	テナントデータの管理	56
	単一テナントへのローカルクラスタの割り当て	58

テナントデータのプッシュとプル	58
外部認証を使用する場合のテナントの割り当て	59
テナントデータでの <code>cnr_exim</code> の使用	59
管理者の管理	60
管理者の追加	61
管理者の編集	62
管理者の削除	62
管理者の一時停止/再開	62
CLI コマンド	62
パスワードの管理	63
グループの管理	63
グループの追加	64
グループの編集	64
グループの削除	64
CLI コマンド	64
ロールの管理	65
ロールの追加	65
ロールの編集	65
ロールの削除	65
CLI コマンド	66
きめ細かい管理	66
ローカル詳細およびリージョン Web UI	66
関連項目	67
スコープレベルの制約	67
プレフィックスレベルの制約	69
リンクレベルの制約	70
管理者の一元管理	71
関連項目	72
管理者のプッシュとプル	72
ローカル クラスタへの管理者のプッシュ	72
ローカル クラスタへの管理者の自動プッシュ	73

レプリカ データベースからの管理者のプル	74
外部認証サーバーのプッシュとプル	75
グループのプッシュとプル	78
ローカル クラスタへのグループのプッシュ	78
レプリカ データベースからのグループのプル	79
ロールのプッシュとプル	80
ローカル クラスタへのロールのプッシュ	81
レプリカ データベースからのロールのプル	82
テナントのプッシュとプル	83
ローカル クラスタへのテナントのプッシュ	83
レプリカ データベースからのテナントのプル	83
セッション管理	84
ユーザーセッション	84
アクティブユーザーセッション	86
セッションイベントのログ	87

 第 5 章

所有者とリージョンの管理 89

所有者の管理	89
ローカル詳細およびリージョン詳細 Web UI	89
CLI コマンド	90
リージョンの管理	90
ローカル詳細およびリージョン詳細 Web UI	90
CLI コマンド	90
所有者とリージョンの一元管理	91
関連項目	91
所有者またはリージョンのプッシュとプル	91
ローカル クラスタへの所有者またはリージョンのプッシュ	91
レプリカ データベースからの所有者とリージョンのプル	92

 第 6 章

中央構成の管理 95

中央構成タスク	95
---------	----

Cisco Prime Network Registrar サービスのデフォルト ポート	96
ファイアウォールの考慮事項	97
DNS パフォーマンスとファイアウォール接続追跡	98
Umbrella を使用するためのキャッシュ DNS の設定	101
ライセンスング	101
ライセンスの追加	102
NAT の背後にあるローカル クラスタの登録	103
ライセンス履歴	105
ライセンス使用率	106
サーバー クラスタの設定	106
関連項目	107
ローカル クラスタの追加	107
ローカル クラスタの編集	109
ローカル クラスタへの接続	109
ローカル クラスタとの同期	110
ローカル クラスタ データの複製	110
レプリカ データの表示	111
レプリカ データのページ	112
クラスタのデータの非アクティブ化、再アクティブ化、およびリカバリ	112
クラスタ レポートの表示	114
中央構成管理サーバー	115
CCM サーバーの管理	115
CCM サーバーのプロパティの編集	116
トリビアルファイル転送	117
関連項目	117
TFTP サーバーの表示と編集	117
TFTP サーバー ネットワーク インターフェイスの管理	118
簡易ネットワーク管理	119
SNMP サーバーのセットアップ	120
通知の仕組み	122
SNMP 通知イベントの処理	126

非アクティブ化されたスコープまたはプレフィックスの処理	127
トラップ設定の編集	128
トラップ設定の削除	128
サーバーのアップ/ダウン トラップ	128
SNMP クエリの処理	129
Cisco Prime Network Registrar SNMP とシステム SNMP の統合	131
個人所有デバイスの Web サーバーの持ち込み	131
BYOD Web サーバーの管理	131
BYOD Web サーバーのプロパティの編集	132
BYOD のテーマとコンテンツのセットアップ	132
BYOD テーマの追加とプレビュー	132
BYOD コンテンツの追加とプレビュー	133
ポーリング プロセス	134
使用率とリース履歴データのポーリング	134
ポーリング間隔の調整	135
リース履歴収集の有効化	136
DHCP スコープ テンプレートの管理	136
関連項目	137
ローカル クラスタへのスコープ テンプレートのプッシュ	137
レプリカ データからのスコープ テンプレートのプル	138
DHCP ポリシーの管理	139
関連項目	139
ローカル クラスタへのポリシーのプッシュ	139
レプリカ データからのポリシーのプル	140
DHCP クライアントクラスの管理	141
関連項目	141
ローカル クラスタへのクライアントクラスのプッシュ	141
レプリカ データからのクライアントクラスのプル	142
仮想プライベート ネットワークの管理	143
関連項目	143
ローカル クラスタへの VPN のプッシュ	143

レプリカ データからの VPN のプル	144
DHCP フェールオーバー ペアの管理	145
リージョン Web UI	145
CLI コマンド	146
リース予約の管理	146
関連項目	146
DHCPv4 予約	146
DHCPv6 予約	147
リソース制限アラームのモニターリング	147
リソース制限アラームしきい値の設定	149
リソース制限アラームのポーリング間隔の設定	150
リソース制限アラームの表示	150
ローカル クラスタ管理チュートリアル	151
関連項目	151
管理者の責任とタスク	152
管理者の作成	152
アドレス インフラストラクチャの作成	153
ゾーン インフラストラクチャの作成	154
転送ゾーンの作成	155
逆引きゾーンの作成	155
最初のホストの作成	156
制約付きのホスト管理者ロールの作成	157
ホスト管理者に割り当てるグループの作成	158
ホスト アドレス範囲のテスト	159
リージョン クラスタ管理チュートリアル	159
関連項目	160
管理者の責任とタスク	160
リージョン クラスタ管理者の作成	161
中央構成管理者の作成	161
ローカル クラスタの作成	162
ルータの追加とインターフェイスの変更	163

構成管理者へのゾーン管理の追加	164
ローカル クラスターのゾーンの作成	164
ゾーン データのプルとゾーン分散の作成	165
サブネットの作成とアドレス空間のプル	166
DHCP ポリシーのプッシュ	166
スコープ テンプレートの作成	167
フェールオーバー ペアの作成と同期	168

第 7 章

ルータおよびルータ インターフェイスの管理	171
ルータの追加	171
ローカル詳細およびリージョン Web UI	171
CLI コマンド	172
ルータの編集	172
ローカル詳細およびリージョン Web UI	172
CLI コマンド	172
ルータ インターフェイスの表示と編集	172
ローカル詳細およびリージョン Web UI	172
CLI コマンド	173
関連項目	173
変更可能ルータ インターフェイス属性	173
インターフェイスのバンドル	173
ルータのサブネットのプッシュと再利用	174

第 8 章

サーバーとデータベースの保守	175
サーバーの管理	175
ローカル基本または詳細とリージョン Web UI	176
CLI コマンド	177
反復タスクのスケジューリング	178
ローカル基本または詳細 Web UI	178
CLI コマンド	179
ログ	179

ログ ファイル	179
サーバー イベントのロギング	182
ロギングの形式と設定	183
ログの検索	184
変更ログの表示	184
サーバー ログ設定の動的更新	185
データ整合性ルールの実行	186
ローカルおよびリージョン Web UI	186
CLI ツール	187
サーバー ステータスのモニターリングと報告	189
関連項目	190
サーバーの状態	190
正常性の表示	190
サーバーの正常性ステータス	191
統計の表示	192
DNS 統計	194
CDNS 統計	196
DHCP 統計	201
TFTP 統計	203
IP アドレスの使用状況の表示	205
関連サーバーの表示	206
永続イベントを使用したリモート サーバーのモニターリング	206
DNS ゾーン分散サーバー	208
DHCP フェールオーバー サーバー	208
リースの表示	209
DHCP および DNS サーバーのトラブルシューティング	209
関連項目	209
即時のトラブルシューティング アクション	210
cnr.conf ファイルの変更	210
サーバー障害のトラブルシューティング	213
Linux トラブルシューティング ツール	214

TAC ツールの使用	215
statscollector ユーティリティの使用	215
TFTP サーバーのトラブルシューティングと最適化	218
関連項目	218
TFTP サーバー アクティビティのトレース	218
TFTP メッセージ ログの最適化	218
TFTP ファイル キャッシングの有効化	219

第 9 章

バックアップとリカバリ	221
データベースのバックアップ	221
推奨	221
関連項目	222
シンタックスと位置	222
バックアップ戦略	223
手動バックアップ (cnr_shadow_backup ユーティリティを使用)	223
自動バックアップ時間の設定	224
手動バックアップの実行	224
cnr_shadow_backup を使用したサードパーティ製バックアッププログラムの使用	224
CNRDB データのバックアップ	225
tar または類似のツールを使用したすべての CNRDB のバックアップ	226
データベース リカバリ戦略	227
バックアップからの CNRDB データのリカバリ	229
tar または類似のツールを使用したすべての CNRDB のリカバリ	230
tar または類似のツールからの単一の CNRDB のリカバリ	230
リージョン クラスタ データベース問題からの回復	231
リース履歴データベース問題の処理	232
サブネット使用率データベース問題の処理	232
レプリカ使用率データベース問題の処理	233
リージョン クラスタの再構築	233
Cisco Prime Network Registrar 実行中のウイルス スキャン	235
データベースのトラブルシューティング	235

関連項目	235
cnr_exim データ インポートおよびエクスポート ツールの使用	236
cnrdb_recover ユーティリティの使用	239
cnrdb_verify ユーティリティの使用	240
cnrdb_checkpoint ユーティリティの使用	240
cnrdb_util ユーティリティの使用	240
フェールオーバー サーバーからの DHCP データの復元	243

第 10 章

レポートの管理 247

ARIN レポートと割り当てレポート	247
ARIN レポートの管理	247
関連項目	248
担当者および組織レポートの管理	248
担当者レポートの作成	249
担当者の登録	249
担当者レポートの編集	250
組織レポートの作成	250
組織の登録	251
組織レポートの編集	251
IPv4 アドレス空間使用率レポートの管理	252
リージョン詳細 Web UI	252
共有 WHOIS プロジェクトの割り振りおよび割り当てレポートの管理	253
BYOD レポートの管理	253
登録済みデバイス	254
登録済みデバイス レポート	254
スコープ/プレフィックス	254
スコープ/プレフィックス レポート	254

第 III 部 :

仮想アプライアンス 257

第 11 章

Cisco Prime Network Registrar 仮想アプライアンスの概要 259

Cisco Prime Network Registrar 仮想アプライアンスの動作	260
仮想アプライアンスでの Cisco Prime Network Registrar の起動	260
VMware でのディスク領域の可用性のモニターリング	260
仮想アプライアンスで使用されているディスク領域の使用状況のモニターリング	260
VMware でのディスクのサイズの増加	261
KVM ハイパーバイザ上のディスク サイズの増加	261
トラブルシューティング	263

用語集	265
-----	-----



第 1 部

使用する前に

- [Cisco Prime Network Registrar の概要 \(1 ページ\)](#)
- [Cisco Prime Network Registrar ユーザー インターフェイス \(9 ページ\)](#)
- [サーバー ステータス ダッシュボード \(27 ページ\)](#)



第 1 章

Cisco Prime Network Registrar の概要

Cisco Prime Network Registrar は、中規模から大規模の IP ネットワークのための、完全な機能を備えたスケーラブルなドメイン ネーム システム (DNS)、Dynamic Host Configuration Protocol (DHCP)、および Trivial File Transfer Protocol (TFTP) の実装です。IP インフラストラクチャを安定化し、クライアントの設定やケーブルモデムのプロビジョニングなどのネットワークサービスを実行を自動化するという主な利点を備えています。これは、ポリシーベースのネットワークの基盤となります。

サービスプロバイダと企業ユーザーは、ネットワークをより適切に管理して、他のネットワーク インフラストラクチャ ソフトウェアやビジネス アプリケーションと統合できます。

- [対象ユーザー \(1 ページ\)](#)
- [リージョンおよびローカル クラスタ \(2 ページ\)](#)
- [導入シナリオ \(3 ページ\)](#)
- [設定とパフォーマンスの注意事項 \(4 ページ\)](#)

対象ユーザー

Cisco Prime Network Registrar は、次のユーザー向けに設計されています。

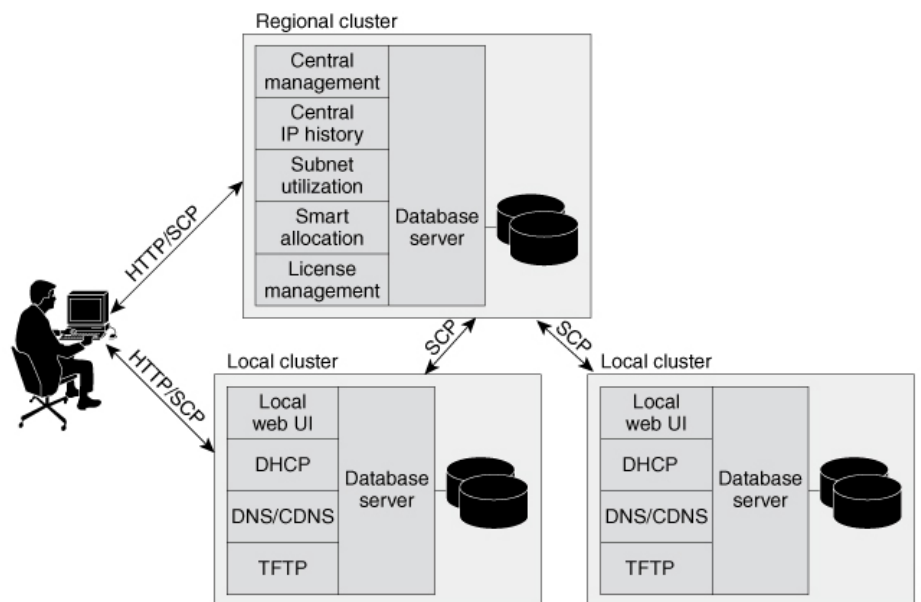
- **Internet service providers (ISPs)** : お客様に専用回線、ダイヤルアップ、および DSL (イーサネットおよび DHCP 経由のポイントツーポイント) アクセスを提供するネットワークの、ISP による運用コストの削減を支援します。
- **Multiple service operators (MSOs)**- ケーブルまたはワイヤレス テクノロジーを使用して加入者にインターネットアクセスを提供する MSO を支援します。MSO は、データオーバークーブルサービスインターフェイス仕様 (DOCSIS) に準拠した信頼性と管理性を備えた DHCP および DNS サービスを提供するサービスとツールからメリットを得ることができます。Cisco Prime Network Registrar は、完全なケーブル モデム プロビジョニング システムの基盤を形成する、ポリシーベースの堅牢でスケーラブルな DNS および DHCP サービスを提供します。
- **Enterprises** : ネットワーク機能を管理および制御する単一およびマルチサイトの企業 (小規模から大規模の企業) のニーズを満たします。Cisco Prime Network Registrar は、個々のネットワーク デバイスに対して IP アドレスを割り当て、Transport Control protocol/Internet protocol (TCP/IP) ソフトウェアを設定するタスクを自動化します。未来志向の企業ユーザー

ザーは、ユーザーの登録など、新規または既存のネットワーク管理アプリケーションとの統合に役立つサービスクラスやその他の機能を活用できます。

リージョンおよびローカル クラスタ

リージョンクラスタは、最大 100 個のローカルクラスタの集約管理システムとして機能します。アドレスおよびサーバー管理者は、リージョンおよびローカルの Web ベースのユーザーインターフェイス (WebUI) を介してリージョンおよびローカルクラスタと対話し、ローカルクラスタ管理者は、ローカルクラスタでコマンドラインインターフェイス (CLI) を引き続き使用できます。リージョンクラスタは、中央構成管理 (CCM) サーバー、Tomcat Web サーバー、サーブレット エンジン、およびサーバー エージェントで構成されます (管理コンポーネント (9 ページ) を参照)。ライセンス管理がリージョンクラスタで実行されるようになるため、必要なサービスを利用するためには、ローカルサーバーをリージョンサーバーに登録する必要があります。詳細については、『Cisco Prime Network Registrar 10.1 インストールガイド』の「概要」の章を参照してください。

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



一般的な導入は、顧客のネットワーク オペレーションセンター (NOC) における 1 つのリージョンクラスタであり、組織のネットワーク運用の中心点です。組織の各部門には、ネットワークの一部の管理を担当するローカルアドレス管理サーバー クラスタが含まれます。システム設定プロトコル (SCP) は、サーバー間の設定変更を伝達します。

導入シナリオ

Cisco Prime Network Registrar リージョン クラスター Web UI は、DNS、CDNS、DHCP、または TFTP サーバーをホストする任意の数のローカルクラスターを管理する単一ポイントを提供します。リージョンおよびローカルクラスターは、管理者ロールをアプリケーションにログインしているユーザーに割り当てることができるように、管理者管理も提供します。

ここでは、2つの基本的な管理シナリオと、2つの異なるタイプのインストール（中小規模のローカルエリアネットワーク（LAN）と、3つの地理的位置を持つ大規模なエンタープライズネットワークまたはサービスプロバイダネットワーク）について、ハードウェアとソフトウェアの導入について説明します。

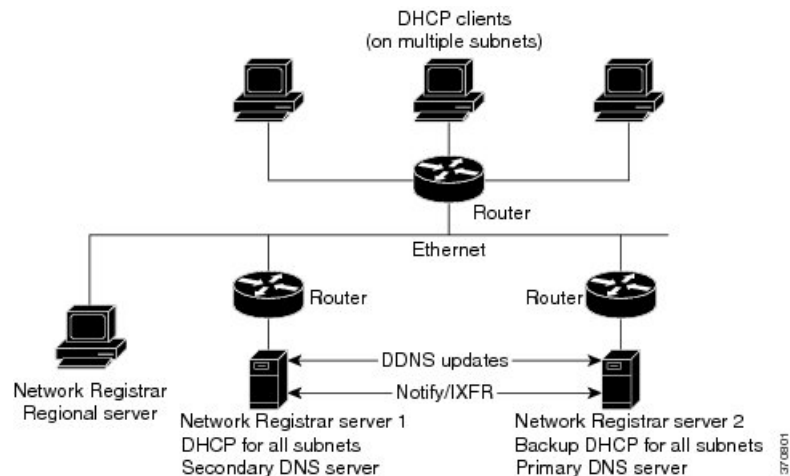
中小規模の LAN

このシナリオでは、ローエンドの Windows または Linux サーバーが使用できます。次の図は、このネットワークに適切な設定を示しています。



(注) リージョン サーバーは、中小規模の LAN の導入に必須です。

図 2: 中小規模の LAN 構成

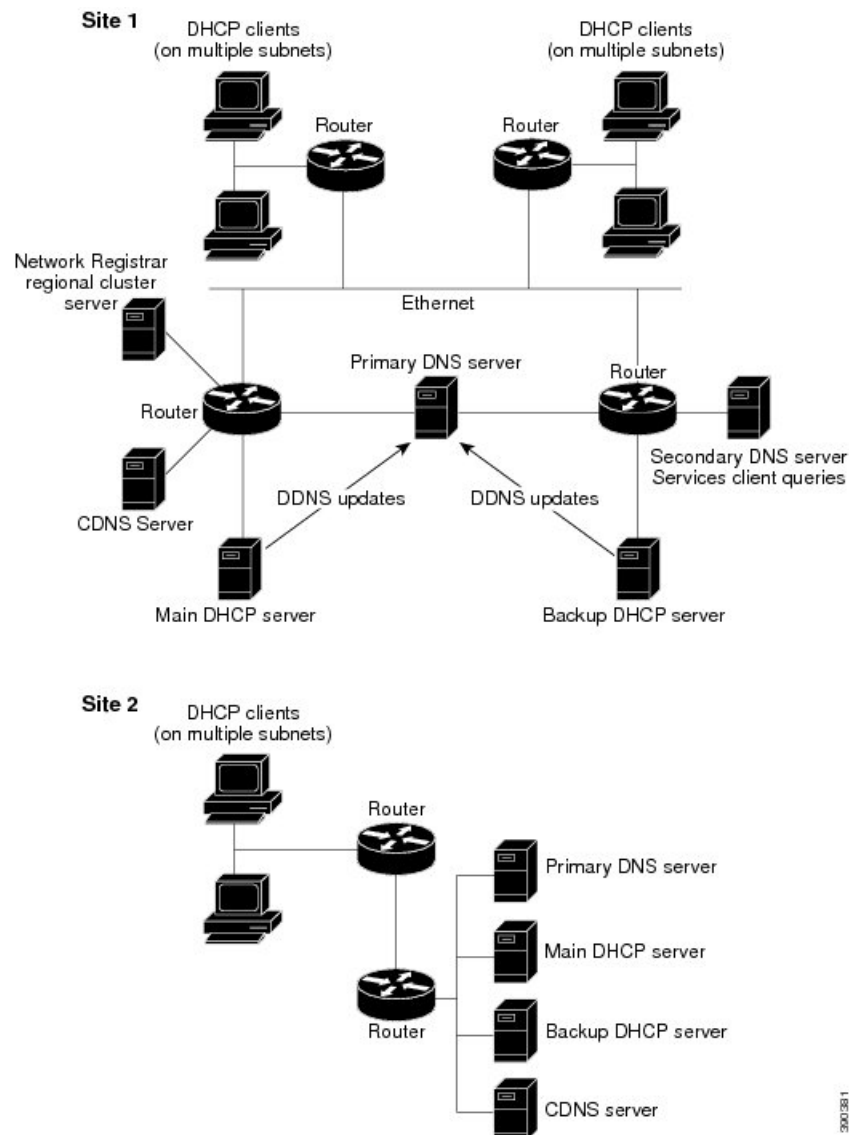


大企業およびサービス プロバイダ ネットワーク

50 万以上の DHCP クライアントにサービスを提供する大企業またはサービスプロバイダのネットワークでは、ミッドレンジの Windows サーバーまたは Linux サーバーを使用します。DNS サーバーと DHCP サーバーを異なるシステムに配置します。次の図は、このネットワークに適したハードウェアを示しています。

地理的に分散したクライアントをサポートする場合、ワイドエリア接続が失敗した場合のローカルサービスの中断を回避するために、DHCP サーバーをリモート位置に配置します。Cisco Prime Network Registrar リージョン クラスタをインストールして、分散クラスタを一元的に管理します。

図 3: 大企業またはサービス プロバイダのネットワーク構成



300281

設定とパフォーマンスの注意事項

Cisco Prime Network Registrar は、Windows または Linux ワークステーションまたはサーバー上で実行可能な、統合された DHCP、DNS、および TFTP サーバークラスタです。

Cisco Prime Network Registrar は幅広いネットワーク トポロジに導入できるため、まず、次の注意事項を考慮する必要があります。これらの注意事項は非常に一般的であり、ほとんどのケースをカバーしています。特定の、または困難な実装では、追加のハードウェアまたはサーバーが必要になる場合があります。

関連項目

[一般的な設定時の注意事項 \(5 ページ\)](#)

[特別な構成事例 \(6 ページ\)](#)

[パフォーマンスに関する一般的な注意事項 \(6 ページ\)](#)

一般的な設定時の注意事項

次の推奨事項は、Cisco Prime Network Registrar のほとんどの導入に適用されます。

- ワイドエリアネットワーク (WAN) のリモートセグメントで実行する別の DHCP サーバーを設定します。

DHCP クライアントが常に 1 秒未満でサーバーにパケットを送信できることを確認します。DHCP プロトコルでは、クライアントは、DHCPDISCOVER または DHCPREQUEST パケットへの応答を送信から 4 秒以内に受信する必要があります。多くのクライアント (特に Microsoft DHCP スタックの最初のリリース) では、実際には 2 秒のタイムアウトが実装されています。

- 大規模な展開では、ダイナミック DNS アップデートに使用されるプライマリ DNS サーバーからセカンダリ DHCP サーバーを分離します。

リース要求とダイナミック DNS アップデートはディスクに保持されるため、共通のディスクシステムを使用すると、サーバーのパフォーマンスが影響を受けます。DNS サーバーが悪影響を受けないようにするには、DHCP サーバーとは別のクラスタで実行します。

- ローカルクラスタとリージョンクラスタ間の時間の違いに対処するためのタイムサーバーを構成に含めて、リージョンサーバーでの集約データが一貫した方法で表示されるようにします。[使用率とリース履歴データのポーリング \(134 ページ\)](#) を参照してください。
- ポリシーの DHCP リース時間を 4 ~ 10 日に設定します。

DHCP クライアントがオフになったときにリースが期限切れにならないようにするには (夜間または長い週末)、DHCP リース時間を、予想されるダウンタイムの最長期間よりも長く設定します (7 日間など)。『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「リースの管理」の項を参照してください。

- バックアップ DNS サーバーを別のネットワーク セグメントに置きます。

DNS サーバーは、本質的に冗長です。ただし、ネットワーク障害時のクライアントへの影響を最小限に抑えるには、プライマリおよびセカンダリ DNS サーバーを別々のネットワーク セグメントに置きます。

- ネットワーク内のダイナミック DNS アップデート レートが高い場合は、転送ゾーンと逆引きゾーン用に個別の DNS サーバーを設定します。

- NOTIFY/IXFR を使用します。

セカンダリ DNS サーバーは、プライマリ DNS サーバーからのデータを2つの方法で受信できます（RFC 1995 および 1996 で説明されているように、フルゾーン転送（AXFR）または増分ゾーン転送（NOTIFY/IXFR））。名前空間が比較的ダイナミックな環境では、NOTIFY/IXFR を使用します。これにより、プライマリ サーバーからセカンダリ サーバーに転送されるレコードの数が減少します。『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「増分ゾーン転送（IXFR）の有効化」の項を参照してください。

特別な構成事例

いくつかの特別な設定には、次の推奨事項が適用されます。

- 大規模な導入または非常にダイナミックなネットワークに対してダイナミック DNS 更新を使用する場合は、プライマリおよびセカンダリ DNS サーバーと DHCP サーバーを複数のクラスタに分割します。

ダイナミック DNS 更新は、すべての Cisco Prime Network Registrar サーバーに対して追加の負荷を生成します。これは、新しい DHCP リース要求によって、ゾーン転送を介してセカンダリ サーバーを更新するプライマリ サーバーへのダイナミック DNS 更新がトリガーされるためです。

- ネットワークの再設定時に、DHCP リースの更新時間を小さい値に設定します。

これは、ネットワーク インフラストラクチャ（ゲートウェイ ルータや DNS サーバーのアドレスなど）を変更する数日前に実行する必要があります。更新時間が8時間の場合、すべての DHCP クライアントが、1 営業日以内に変更された DHCP オプションパラメータを受信します。『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「リースの管理」の項を参照してください。

パフォーマンスに関する一般的な注意事項

Cisco Prime Network Registrar では、一般的な注意事項として、使用可能な最高のパフォーマンスのディスク I/O サブシステム、次にメモリ、最後にプロセッサに投資することです。DHCP および権威 DNS は（特に DNS アップデートを使用する場合）、ディスク遅延、次にメモリとネットワークのパフォーマンス、最後に CPU の影響を受けます（これらのアプリケーションは CPU 集約ではありません）。

- 遅延を削減し、パフォーマンスを向上させる最善の方法は、高性能なディスクを提供することです（従来のハードディスクよりも SSD が推奨されます）。高性能ディスク コントローラも推奨されます。これは、ダイナミック アップデートを処理する DHCP および権威 DNS サーバーで特に重要です。
- ファイル システム キャッシュを使用できる場合は、ディスク読み取り要件が減るため、大量のメモリを提供することも重要です。ここでの推奨事項は、システムに十分な空きメ

メモリがあり、Cisco Prime Network Registrar データベースの 2 倍のサイズであるようにすることです。多くの変数に依存するため、ここで正確な要件を示すことは困難です。

- ネットワーク パフォーマンスも重要な考慮事項であり、1 GB 以上のイーサネット コントローラを推奨します。
- ほとんどの Cisco Prime Network Registrar は CPU 集約的ではないため、CPU のパフォーマンスは重要性が低い傾向があります。

以前のリリースとの相互運用性

次の表に、リージョン CCM サーバーの Cisco Prime Network Registrar の機能とローカル クラスターのバージョンの相互運用性を示します。

表 1: CCM リージョンの機能とサーバーのバージョンとの相互運用性

機能	ローカル クラスターのバージョン				
	8.3	9.0	9.1	10.0	10.1
プッシュとプル:					
アドレス空間	X	X	X	X	X
IPv6 アドレス空間	X	X	X	X	X
スコープ テンプレート、ポリシー、クライアントクラス	X	X	X	X	X
IPv6 プレフィックスおよびリンク テンプレート	X	X	X	X	X
ゾーン データとテンプレート	X	X	X	X	X
グループ、所有者、リージョン	X	X	X	X	X
リソース レコード (RR)	X	X	X	X	X
ローカル クラスターの復元	X	X	X	X	X
ホスト管理	X	X	X	X	X
拡張ホスト管理	X	X	X	X	X

機能	ローカル クラスタのバージョン				
	8.3	9.0	9.1	10.0	10.1
管理者とロール	X	X	X	X	X
ゾーン ビュー	X	X	X	X	X
管理者 :					
シングルサインオン	X	X	X	X	X
パスワードの変更	X	X	X	X	X
IP 履歴レポート :					
リース履歴	X	X	X	X	X
詳細なリース履歴	X	X	X	X	X
使用率レポート :					
DHCP 使用率履歴 (v4 履歴)	X	X	X	X	X
DHCP 使用率履歴 (v6 履歴)			X	X	X
サブネットおよびスコープの使用率	X	X	X	X	X
IPv6 プレフィックス使用率	X	X	X	X	X



第 2 章

Cisco Prime Network Registrar ユーザー インターフェイス

Cisco Prime Network Registrar は、リージョンおよびローカル Web UI とリージョンおよびローカル CLI を提供して、CDNS、DNS、DHCP、TFTP、および CCM サーバーを管理します。

- ローカル クラスタ サーバーにアクセスするためのリージョン クラスタの **WEB UI - リージョン クラスタ Web UI (23 ページ)** を参照してください。
- ローカル クラスタの **WEB UI - ローカル クラスタ Web UI (18 ページ)** を参照してください。
- ローカル クラスタの **CLI - インストール/docs** ディレクトリの **CLIContent.html** ファイルを開きます (**コマンドライン インターフェイス (24 ページ)** を参照)。
- これらのインターフェイスをサポートするインフラストラクチャを提供する **CCM サーバー - 中央構成管理サーバー (115 ページ)** を参照してください。

この章では、Cisco Prime Network Registrar ユーザー インターフェイスと、CCM サーバーが提供するサービスについて説明します。Cisco Prime Network Registrar サーバーの設定を開始する前に、この章を読んで、各ユーザーインターフェイス機能について十分に理解しておいてください。

- **管理コンポーネント (9 ページ)**
- **Web ベースのユーザー インターフェイスの概要 (11 ページ)**
- **ローカル クラスタ Web UI (18 ページ)**
- **リージョン クラスタ Web UI (23 ページ)**
- **コマンドライン インターフェイス (24 ページ)**
- **Prime Network Registrar でのグローバル検索 (26 ページ)**

管理コンポーネント

Cisco Prime Network Registrar には、次の 2 つの管理コンポーネントが含まれています。

- 以下で構成されるリージョン コンポーネント。

- Web UI
 - CLI
 - CCM サーバー
 - 個人所有デバイスの持ち込み (BYOD)
 - 簡易ネットワーク管理プロトコル (SNMP) サーバー
- 次のもので構成されるローカル コンポーネント。
- Web UI
 - CLI
 - CCM サーバー
 - 権威あるドメイン ネーム システム (DNS) サーバー
 - キャッシング/再帰ドメイン ネーム システム (CDNS) サーバー
 - 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) サーバー
 - トリビアル ファイル 転送 プロトコル (TFTP) サーバー
 - SNMP サーバー
 - ローカルアドレス空間、ゾーン、スコープ、DHCPv6プレフィックスとリンク、およびユーザーの管理



(注) Cisco Prime Network Registrar には、ハイブリッド DNS 機能が含まれています。この機能を使用すると、2つの独立した仮想マシンまたは物理マシンを使用せずに、キャッシング DNS サーバーと権威 DNS サーバーの両方を同じオペレーティング システムで実行できます。ただし、小規模な展開の場合にのみ、ハイブリッドモードを推奨します。大規模な展開では、キャッシング DNS と権威 DN を別々の物理マシンまたは VM に分離することを推奨します。

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、リージョン クラスタから実行されます。まず、リージョンサーバーをインストールし、リージョンサーバー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、ライセンスを取得するためにリージョンに登録されます。

リージョン CCM サーバーは、DHCP アドレス空間と DNS ゾーンの集約ビューを使用して、ローカル クラスタの一元管理を提供します。これにより、分散アドレス空間、ゾーン、スコープ、DHCPv6 プレフィックスとリンク、およびユーザーの管理が可能になります。

ローカル CCM サーバーは、ローカルアドレス空間、ゾーン、スコープ、DHCPv6 プレフィックスとリンク、およびユーザーの管理を提供します。

この章の残りの部分では、TFTP および SNMP プロトコルについて説明します。CCM サーバー、Web UI、および CLI については、[Cisco Prime Network Registrar ユーザー インターフェ](#)

[イス \(9 ページ\)](#) で説明しています。DNS、CDNS、および DHCP サーバーについては、それぞれのセクションで説明します。

Web ベースのユーザー インターフェイスの概要

Web UI は、ユーザーのロールと制約により、構成データへのきめ細かいアクセスを提供します。UI を使用すると、一般的な機能に簡単にアクセスできます。Web UI の詳細については、以降の項で説明します。

関連項目

- [サポートされる Web ブラウザ \(11 ページ\)](#)
- [アクセス セキュリティ \(11 ページ\)](#)
- [Web UI へのログイン \(12 ページ\)](#)
- [複数のユーザー \(13 ページ\)](#)
- [パスワードの変更 \(13 ページ\)](#)
- [Web UI のナビゲート \(14 ページ\)](#)
- [続行する前のページ解決の待機 \(15 ページ\)](#)
- [Web UI での変更のコミット \(15 ページ\)](#)
- [ロールと属性の可視性の設定 \(15 ページ\)](#)
- [属性の表示と変更 \(16 ページ\)](#)
- [ヘルプ ページ \(17 ページ\)](#)
- [ログアウト \(18 ページ\)](#)

サポートされる Web ブラウザ

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。

アクセス セキュリティ

Cisco Prime Network Registrar のインストールでは、Web UI へのセキュアなクライアントアクセスをサポートするように HTTPS を設定することができます。HTTPS ポート番号を指定し、その時点でのキーストアを指定する必要があります。HTTPS セキュリティが有効な場合、Web UI ログイン ページには次のように示されます。「ページは SSL です。¹安全です。(Page is SSL Secure.)」

¹ 本製品には OpenSSL Toolkit で使用するために OpenSSL プロジェクトによって開発されたソフトウェアが含まれています (<http://www.openssl.org/>)。



(注) キーストア パスワードの一部としてドル記号 (\$) を使用しないでください。

Web UI へのログイン

Cisco Prime Network Registrar のローカルまたはリージョン クラスタ Web UI にログインするには、HTTPS セキュアまたは HTTP 非セキュアログインのいずれかを使用します。Cisco Prime Network Registrar をインストールした後、サポートされている Web ブラウザの 1 つを開き、ブラウザのアドレス フィールドまたはネットサイト フィールドにログイン位置の URL を指定します。ログインは便利であり、いくつかのメモリ機能を提供して、ログイン速度を高めます。非セキュアログインを使用してログインするには、次の 2 つの方法があります。

- Windows の [スタート (Start)] メニューから、**Start > All Programs > Network Registrar 10.1 > Network Registrar 10.1 {local | regional} Web UI** を選択します。デフォルトの Web ブラウザで、ローカルまたはリージョン クラスタ Web UI が開きます。



注 最初にリージョン Web UI を開き、必要なサービスのライセンスを追加します。

- Web ブラウザを開き、Web サイトに移動します。たとえば、インストール時にデフォルトのポートが使用された場合、URL は、ローカル クラスタ Web UI については **http://ホスト名:8080** になり、リージョン クラスタ Web UI については **http://ホスト名:8090** になります。

インストール時に有効なライセンスが追加されていない場合は、[新しい製品のインストール (New Product Installation)] ページが開きます。有効なライセンスを参照して追加する必要があります。ライセンス キーが受け入れ可能な場合は、Cisco Prime Network Registrar のログイン ページが表示されます。



(注) ライセンスは、リージョン サーバーにのみ追加できます。必要なライセンス サービスを実行するには、インストール時にローカルをリージョンに登録する必要があります。

ローカル サーバーで、リージョン サーバーの IP アドレスとポート番号を確認し、最初のログイン時に実行するサービスも確認します。[登録 (Register)] をクリックして、登録を確認します。必要なライセンスを使用してリージョンサーバーが設定されている場合は、ログイン ページが表示されます。

インストール時に作成されたスーパーユーザーのユーザー名とパスワードを入力して、Web UI にログインします。パスワードは大文字と小文字が区別されます ([パスワードの管理 \(63 ページ\)](#) を参照)。インストール時に有効なライセンスとスーパーユーザーを追加し、パスワードを設定した場合は、そのユーザー名とパスワードを使用して Web UI にログインできます。



(注) ログイン用のデフォルトのユーザー名またはパスワードはありません。



(注) HTTPS で保護されたログインの準備については、*Cisco Prime Network Registrar 10.1* インストール ガイド を参照してください。

ブラウザのセットアップ方法によっては、ユーザー名を設定する際に、アカウント名を省略したり、ドロップダウン リストから選択したりすることができます。

ログインするには、[ログイン (Login)] をクリックします。

デフォルトでは、[設定の要約 (Configuration Summary)] ページが表示され、クラスタの設定の詳細の要約が示されます。リージョンクラスタの [設定の要約 (Configuration Summary)] ページには、設定されているフェールオーバーペアとゾーン分散が表示され、基盤となるクラスタまたはHAのペアも表示できます。ネットワークデータをチャートまたは表形式で表示するには、チャートの [可視化表示 (show Visualization)] アイコン (📊) または [テーブルビューを表示 (show Table View)] アイコン (📄) などのグラフィカルユーティリティを使用します。

複数のユーザー

Cisco Prime Network Registrar ユーザー インターフェイスは、複数の同時ユーザーをサポートします。2人のユーザーが同じオブジェクトレコードまたはデータにアクセスしようとする、2番目のユーザーに対して**変更されたオブジェクト**エラーが発生します。ユーザーデータの編集集中にこのエラーが表示された場合は、次の手順を実行します。

- **In the web UI** - 編集をキャンセルし、リストを更新します。最初のユーザーによって行われた変更がリストに反映されます。必要に応じて、編集をやり直します。
- **In the CLI - session cache refresh** コマンドを使用して、現在の編集をクリアしてから、変更を表示し、さらに編集します。他のユーザーの変更後でも必要と思われる場合は、変更を加えます。

パスワードの変更

Web UI ページでパスワードを編集するときには、8つのドットの文字列として表示されます。実際のパスワードの値は、Web ブラウザには送信されません。したがって、パスワードを変更すると、フィールドは自動的にクリアされます。新しいパスワードの値を、必要に応じて完全に入力する必要があります。



(注) パスワードの長さは 255 文字以下でなければなりません。

ローカルクラスタおよびリージョンクラスタでの管理者パスワードの変更の詳細については、[パスワードの管理 \(63 ページ\)](#) を参照してください。

Web UI のナビゲート

Web UI は、必要な機能と、管理タスクの一部として実行しているスレッドに基づいて、ページの階層を提供します。ページ階層を使用すると、簡単に失われることがなくなります。



注意 ブラウザの[戻る (Back)]ボタンは使用しないでください。前のページに戻るには、必ずナビゲーションメニューを使用するか、ページの[キャンセル (Cancel)]ボタンを使用してください。ブラウザの[戻る (Back)]ボタンを使用すると、異常な動作が発生したり、障害が発生したりする可能性があります。

シングルサインオン機能は、リージョンとローカルクラスタの間で接続するために使用できます。リージョンクラスタ Web UI ページには、[リモートクラスタの一覧表示/追加 (List/Add Remote clusters)] ページに [接続 (Connect)] ボタンがあり、これをクリックすると、アイコンに関連付けられているローカルクラスタに接続できます。ローカルクラスタへのシングルサインオン権限がある場合、接続によって関連するローカルサーバー管理ページ（または関連するサーバー設定の関連ページ）に移動します。これらの権限を持っていない場合、接続によってローカルクラスタのログインページに移動します。リージョンクラスタに戻るために、ローカルクラスタ ページのメイン ツールバーに [戻る (Return)] ボタンがあります。

ナビゲーションメニューの検索バーを使用すると、簡単にメニューを検索することができます。ナビゲーションメニューの右上隅にあるピンアイコンを使用すると、メニューのピン留め/ピン留め解除ができます。

Cisco Prime Network Registrar は頻繁に使用されるページ/メニューをお気に入りとして保存して、簡単にアクセスできる機能を提供します。ページ/メニューをお気に入りとして設定するには、目的のメニューに移動した後、[お気に入り (Favorite)] アイコン（ナビゲーションパスの横にある星形のアイコン (*)）をクリックして、適切な名前を入力し、[OK] をクリックします。お気に入りとして設定されているページ/メニューは、グローバルナビゲーションの [お気に入り (Favorites)] セクションに表示されます。お気に入りリストからメニューを削除するには、その横にある [削除 (Delete)] アイコンをクリックします。[設定の要約 (Configuration Summary)] ページは、デフォルトで [お気に入り (Favorites)] セクションに表示されます。



(注) 任意のページの二重矢印アイコン (⌂) をクリックすると、非表示のオプション/機能が表示されます。



(注) [ナビゲーション (Navigation)] メニュー項目は、IPv4 または IPv6 のロール権限を持っているかどうかによって異なります。たとえば、addrblock-admin ロールの ipv6-management サブロールが割り当てられている場合、[設計 (Design)] メニューは **DHCPv4** と **DHCPv6** です。

続行する前のページ解決の待機

Web UI で実行される操作（サーバー クラスタからのデータの再同期や複製など）は、操作が完了するまで、ブラウザに制御を戻さないという点で同期しています。これらの操作では、確認メッセージが青色のテキストで表示されます。また、操作の進行中は、ブラウザに待機カーソルが表示されます。



ヒント Web UI の各操作が完了するまで待機してから、新しい操作を開始します。ブラウザに障害が発生した場合は、ブラウザを閉じて、再度開き、再度ログインします。ゾーン分散などの一部の操作は長時間かかることがあるため、操作が完了するまで待機する必要がある場合があります。

Web UI での変更のコミット

ページの [保存 (Save)] をクリックするまで、入力したページのエント리는実際にはコミットされません。[削除 (Delete)] アイコンを使用して、項目を削除できます。不要な削除を防ぐため、多くの場合は、[削除の確認 (Confirm Delete)] ダイアログボックスが表示されて、削除を確定またはキャンセルできます。

ロールと属性の可視性の設定

メインページの上にあるツールバーの [設定 (Settings)] ドロップダウンリストをクリックして、ユーザー設定、セッション設定、ユーザー権限、またはデバッグ設定を変更します。

- 管理者のユーザー グループとロールを表示するには、[ユーザー設定 (User Preferences)] オプションを選択します。スーパーユーザーは、特別な種類の管理者です。（これらの管理者ロールを設定する方法の詳細については、[管理者の作成 \(152 ページ\)](#) を参照してください）。
- [セッション設定 (Session Settings)] を選択して [セッション設定 (Session Settings)] ダイアログを開き、[セッション Web UI モード (Session Web UI Mode)] ドロップダウンリストからモードを選択し、[セッション設定の変更 (Modify Session Settings)] をクリックします。モードアイコン (🔽) のドロップダウン矢印をクリックして、モードのリストを表示することもできます。リストから必要なモードを選択します。
 - [基本 (Basic)] - 基本ユーザー モード (プリセットの選択)。
 - [詳細 (Advanced)] - 通常の属性を公開する詳細ユーザー モード。
 - [エキスパート (Expert)] - 設定の微調整またはトラブルシューティングに関連する一連の属性を公開するエキスパートユーザー モード。ほとんどの場合、これらのエキスパート属性のデフォルト値を受け入れてください。Cisco Technical Assistance Center (TAC) のガイダンスなしで変更しないでください。エキスパートモードの各属性には、設定ページに警告アイコンが付いています。各ページは、エキスパートモードとして明確にマークされています。

属性の表示と変更

サーバー、ゾーン、スコープなどの Web UI ページの多くには、CLI を使用して設定できる属性設定が含まれています。（該当する CLI 名は属性名の下に表示されます。）属性は、その機能によってグループに分類され、主要な属性から先に表示され、設定されることが少ない属性はページの下の方に表示されます。

属性のグループ化とソート

多くの詳細モード Web UI ページでは、属性の表示をグループ順とアルファベット順で切り替えることができます。これらのページは、通常、デフォルトではグループビューで開くため、それぞれのカテゴリの属性を確認できます。ただし、属性の数が多い場合、属性をアルファベット順に表示する必要があります。[昇順ビューを表示 (Show A-Z View)] をクリックすると、ページの属性表示をアルファベット順に変更できます。[グループビューを表示 (Show Group View)] をクリックすると、属性の表示をグループ順に変更できます。[すべて展開 (Expand All)] または [すべて折りたたむ (Collapse All)] をクリックして、グループ表示の属性グループを展開または折り畳むこともできます。エキスパートモードでは、エキスパートモードの属性は、ページの下の方の Visibility=3 の見出しの下に個別にアルファベット順で表示され、すべてに警告アイコンが表示されます。

属性の変更

属性値を変更し、オプション属性の設定を解除することができます。多くの場合、これらの属性にはプリセット値があり、ページの [デフォルト (Default)] 列にリストされます。明示的な値はデフォルト値をオーバーライドしますが、デフォルト値は常にフォールバックです。デフォルト値がない場合、明示的な値を解除すると、その属性のすべての値が削除されます。

属性ヘルプの表示

属性のコンテキストヘルプについては、属性の名前をクリックして、別のポップアップ ウィンドウを開きます。

左側のナビゲーションペイン

Web UI には、メインページの左側にナビゲーションペインもあります。このナビゲーションペインから、さまざまなカテゴリの一部として追加されたオブジェクトにアクセスできます。オブジェクトは表形式で表示されます。オブジェクトをクリックすると、メインページでプロパティを編集できます。

ペインのカテゴリの下に表示される各オブジェクトには、そのオブジェクトに関連付けられたクイックビューアイコンがあります。[クイックビュー (Quick View)] アイコンをクリックすると、オブジェクトに関する主要な詳細を示すダイアログボックスが開き、オブジェクトに関連付けられている主要なアクションを実行するためのリンク（存在する場合）が表示されます。

デフォルトでは、オブジェクトのリストは1列形式で表示されます。ただし、左側のペインに列を追加できます。オブジェクトの列を追加するには、左側のペインのオブジェクトテーブル

の上にある歯車アイコン (⚙) をクリックして、目的の列名を選択し、[閉じる (Close)] をクリックします。列形式を保存するには、[列形式の保存 (Save Column format)] ボタンをクリックします。

必要に応じてオブジェクトをフィルタリングするためのクイック フィルタ オプションと詳細フィルタ オプションがあります。オブジェクトのクイック検索を実行するには、[クイック フィルタ (Quick Filter)] オプションを使用できます。[フィルタ (Filter)] アイコン (▼) をクリックするか、オブジェクトテーブルの上にある [表示 (Show)] ドロップダウンリストから [クイック フィルタ (Quick Filter)] を選択して、検索バーに検索文字列を入力します。オブジェクトは、検索条件に従ってリストされます。

また、[詳細フィルタ (Advanced Filter)] を使用してオブジェクトをフィルタリングすることもできます。[表示 (Show)] ドロップダウンリストから [詳細フィルタ (Advanced Filter)] を選択して、[詳細フィルタ (Advanced Filter)] ダイアログ ボックスで適切なフィルタと条件を設定し、[OK] をクリックします。[OK] をクリックすると、左側のペインのオブジェクトリストが、指定されたフィルタに従ってフィルタリングされます。フィルタを保存するには、[詳細フィルタ (Advanced Filter)] ダイアログ ボックスの [名前を付けて保存 (Save As)] をクリックして、[フィルタの保存 (Save Filter)] ダイアログ ボックスに適切な名前を入力し、[保存 (Save)] をクリックします。保存されたフィルタ名が [表示 (Show)] ドロップダウン リストに表示され、その特定のオブジェクトリストに対していつでもこのフィルタを使用できます。[デフォルト フィルタの設定 (Set Default Filter)] ボタンをクリックすると、このフィルタをデフォルトのフィルタとして設定することもできます。


ユーザー定義フィルタは編集または削除できます。これを行うには、[表示 (Show)] ドロップダウンリストから [ユーザー定義フィルタの管理 (Manage User Defined Filters)] を選択し、[ユーザー定義フィルタの管理 (Manage User Defined Filters)] ダイアログ ボックスのフィルタリストから必要なユーザー定義フィルタを選択して、必要に応じて [編集 (Edit)] または [削除 (Remove)] をクリックします。

ヘルプ ページ

Web UI には、各ページのヘルプ テキストを表示する別のウィンドウが用意されています。ヘルプ ページには、次のものが用意されています。

- 開いているアプリケーション ページに応じた状況依存のヘルプ トピック。
- クリック可能な階層型のコンテンツとインデックス、および [お気に入り (Favorites)] 設定は、左側のペインのタブとして表示または非表示にすることができます。
- 検索機能。検索文字列を含むトピックのリストを返します。トピックは、検索文字列の表示頻度の順に並べられます。
- 開いたヘルプ ページの履歴を次へ、および元へ戻ることができます。
- 印刷機能。
- 用語集。


ログアウト

Web UI からログアウトするには、[ログアウト (**Log Out**)] リンクをクリックします。アプリケーションページの右上隅にある歯車アイコン  の下に [ログアウト (**Log Out**)] があります。

ローカル クラスタ Web UI

ローカル クラスタ Web UI は、Cisco Prime Network Registrar ユーザーとプロトコル サーバーの管理および構成への同時アクセスを提供します。これは、各要素または機能ごとに設定できる権限を持つ、サーバー全体でのきめ細かい管理を提供します。ローカル クラスタ Web UI は、次の 3 つのユーザー モードで使用できます。

- **基本モード (Basic Mode)** - DHCP スコープや DNS ゾーンなど、より頻繁に設定されるオブジェクトの設定をより簡単にします ([ローカルの基本メインメニューページ \(18 ページ\)](#) を参照)。
- **詳細モード (Advanced Mode)** - Cisco Prime Network Registrar Web UI の過去のユーザーが慣れている詳細な設定方法と機能強化を提供します ([ローカルの詳細なメインメニューページ \(20 ページ\)](#) を参照)。
- **エキスパートモード (Expert Mode)** (アイコンでマークされている) - エキスパートモードの詳細については、[ロールと属性の可視性の設定 \(15 ページ\)](#) を参照してください。

基本、詳細、またはエキスパート モードに変更するには、ページの右上にあるツールバーの [モード (Mode)] アイコン  のドロップダウン矢印をクリックします ([ローカルユーザーの環境設定の設定 \(21 ページ\)](#) を参照)。




-
- (注) ローカル クラスタ マシンの IP アドレスを変更する場合は、[ローカル Web UI でのクラスタの構成 \(23 ページ\)](#) の注を参照してください。
-

関連項目

[Web ベースのユーザー インターフェイスの概要 \(11 ページ\)](#)

[リージョン クラスタ Web UI \(23 ページ\)](#)

ローカルの基本メインメニューページ

ページの右上隅にあるツールバーで [基本 (Basic)] タブがアクティブになっている場合は、基本ユーザー モードになっていることを意味します。それ以外の場合は、モードアイコン  のドロップダウン矢印をクリックして、モードのリストを表示し、[基本 (Basic)] を選択します。

ページの左上隅にあるグローバルナビゲーションアイコンをクリックすると、ナビゲーションメニューの下にサブメニュー項目が表示されます。ナビゲーションメニューの下にあるサブメニューを選択するには、ナビゲーションメニュー項目にカーソルを置きます。たとえば、カーソルを[操作 (Operate)]に置いて、[サーバーの管理 (Manage Servers)]を選択します。

また、必要なナビゲーションメニューの下にある任意のサブメニューを選択し、左側のペインから必要なサブメニューページに移動することもできます。たとえば、カーソルを[操作 (Operate)]に置いて、[タスクのスケジュール設定 (Schedule Tasks)]を選択します。[サーバーの管理 (Manage Servers)]、[クラスタの管理 (Manage Clusters)]、[タスクのスケジュール設定 (Schedule Tasks)]、および[変更ログの表示 (View Change Log)]へのリンクがある左側のペインとともに、[スケジュール済みタスクの一覧表示/追加 (List/Add Scheduled Tasks)]ページを表示できます。[サーバーの管理 (Manage Servers)]リンクをクリックすると、[サーバーの管理 (Manage Servers)]ページが表示されます。

ローカルの基本メインメニューページには、次のことができる機能があります。

- **ダッシュボードを開いて、システムの正常性をモニターする** - [操作 (Operate)]メニューを開き、[ダッシュボード (Dashboard)]をクリックします。「サーバーステータスダッシュボード」の章を参照してください。
- **Set up a basic configuration by using the Setup interview pages** - 上部にある[セットアップ (Setup)]アイコンをクリックして、[セットアップ (Setup)]ページのさまざまなタブを選択します。詳細については、『Cisco Prime Network Registrar 10.1 クイックスタートガイド』を参照してください。
- **Administer users, tenants, encryption keys** - カーソルを[管理 (Administration)]メニュー (ユーザーアクセスオプションの場合) または[設計 (Design)]メニュー (セキュリティ (Security)]>[キー (Keys)]オプションの場合) に置きます。[管理者の管理 \(43 ページ\)](#) を参照してください。
- **Manage the Cisco Prime Network Registrar protocol servers** - カーソルを[操作 (Operate)]メニューに置き、[サーバーの管理 (Manage Servers)]または[タスクのスケジュール設定 (Schedule Tasks)]オプションを選択します。[サーバーとデータベースの保守 \(175 ページ\)](#) を参照してください。
- **Manage clusters** - カーソルを[操作 (Operate)]メニューに置き、[クラスタの管理 (Manage Clusters)]オプションを選択します。[サーバークラスタの設定 \(106 ページ\)](#) を参照してください。
- **Configure DHCP** - カーソルを[設計 (Design)]メニューに置き、[DHCPの設定DHCP Settings]、[DHCPv4]、[DHCPv6]のオプションを選択します。『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「DHCPサーバーの管理」の章を参照してください。
- **Configure DNS** - カーソルを[設計 (Design)]メニューに置き、[キャッシュDNS (Cache DNS)]と[権威DNS (Auth DNS)]のオプションを選択します。カーソルを[展開 (Deploy)]メニューに置き、[DNS]と[DNSアップデート (DNS Updates)]のオプションを選択します。『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「ゾーンの管理」の項を参照してください。

- **Manage hosts in zones** - [設計 (Design)]メニューから [権威DNS (Auth DNS)]サブメニューの [ホスト (Hosts)]を選択します。『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「ホストの管理」の項を参照してください。
- **Go to Advanced mode** - ページの右上隅にある [詳細 (Advanced)]をクリックします。ローカルの詳細なメインメニューページ (20 ページ) を参照してください。

ローカルの詳細なメインメニューページ

基本ユーザーのメインメニューページから詳細ユーザーモードに切り替えるには、ウィンドウの右上にあるモードアイコン (☰) のドロップダウン矢印をクリックして、モードのリストを表示し、[詳細 (Advanced)]を選択します。これを行うと、もう1つのメインメニューページが開きますが、詳細ユーザーモード機能が表示されます。いつでも基本モードに戻ることができ、そのためには、ウィンドウの右上にあるモードアイコンの横にあるドロップダウン矢印をクリックして、[基本 (Basic)]を選択します。

ローカルの詳細モードメインメニューページには、基本モードのCisco Prime Network Registrar機能に加えて、詳細機能も含まれています。

- **ダッシュボードを開いて、システムの正常性をモニターする** - [操作 (Operate)]メニューを開き、[ダッシュボード (Dashboard)]をクリックします。「サーバーステータスダッシュボード」の章を参照してください。
- **Administer users, tenants, groups, roles, regions, access control lists (ACLs)、および view change logs** - カーソルを [管理 (Administration)]メニュー (ユーザーアクセスオプションの場合)、[設計 (Design)]メニュー (ACLの場合)、または [操作 (Operate)]メニュー (変更ログの場合) に置きます。管理者の管理 (43 ページ) を参照してください。
- **Manage the Cisco Prime Network Registrar protocol servers** - カーソルを [操作 (Operate)]メニューに置き、[サーバーの管理 (Manage Servers)]または [タスクのスケジュール設定 (Schedule Tasks)]オプションを選択します。サーバーとデータベースの保守 (175 ページ) を参照してください。
- **Manage clusters** - カーソルを [操作 (Operate)]メニューに置き、[クラスタの管理 (Manage Clusters)]を選択します。サーバークラスタの設定 (106 ページ) を参照してください。
- **Configure Routers** - カーソルを [展開 (Deploy)]メニューに置き、[ルータの設定 (Router Configuration)]のオプションを選択します。ルータおよびルータ インターフェイスの管理 (171 ページ) を参照してください。
- **Configure DHCPv4** - カーソルを [設計 (Design)]メニューに置き、[DHCPv4] のオプションを選択します。『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「DHCPサーバーの管理」の章を参照してください。
- **Configure DHCPv6** - カーソルを [設計 (Design)]メニューに置き、[DHCPv6] のオプションを選択します。『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「DHCPv6アドレス」の項を参照してください。

- **Configure DNS** - カーソルを [設計 (Design)] メニューに置き、[キャッシュDNS (Cache DNS)] と [権威DNS (Auth DNS)] のオプションを選択します。カーソルを [展開 (Deploy)] メニューに置き、[DNS] と [DNSアップデート (DNSUpdates)] のオプションを選択します。『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「ゾーンの管理」の項を参照してください。
- **Manage hosts in zones** - [設計 (Design)] メニューから [権威DNS (Auth DNS)] サブメニューの [ホスト (Hosts)] を選択します。『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「ホストの管理」の項を参照してください。
- **Manage IPv4 address space** - カーソルを [設計 (Design)] メニューに置き、[DHCPv4] のオプションを選択します。『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「アドレス空間の管理」の項を参照してください。
- **Configure IPv6 address space** - カーソルを [設計 (Design)] メニューに置き、[DHCPv6] のオプションを選択します。『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「DHCPv6 アドレス」の項を参照してください。
- **基本モードに移動** - ページの右上隅にあるモードアイコン (☰) のドロップダウン矢印をクリックし、[基本 (Basic)] を選択します。ローカルの基本メインメニューページ (18 ページ) を参照してください。

詳細ユーザーモードページには、次の追加機能があります。

- **View the user role and group data for the logged-in user** - [ロールと属性の可視性の設定 \(15 ページ\)](#) を参照。
- **Set your preferred session settings** - [ロールと属性の可視性の設定 \(15 ページ\)](#) を参照。
- **Set server debugging** - プロトコルサーバーのデバッグフラグをセットできます。これらの値は、Cisco Technical Assistance Center (TAC) と通信するときに診断条件の下でのみ設定します。
- **Change your login administrator password** - [パスワードの管理 \(63 ページ\)](#) を参照。

ローカルユーザーの環境設定の設定

後続のユーザーセッションを通じて、WebUI設定の短いリストを維持できます。[基本 (Basic)] と [詳細 (Advanced)] または [エキスパート (Expert)] モードのユーザー環境設定ページの唯一の違いは、詳細およびエキスパートモードでは、データ型とデフォルトをリストする追加の列があることです。

[設定 (Settings)] ドロップダウンリストの [ユーザー環境設定 (User Preferences)] に移動して、ユーザー環境設定を編集できます。設定するユーザー環境設定属性は、次のとおりです。

- **ユーザー名 (Username)** - ユーザー名の文字列。事前設定値は **admin** です。このフィールドを変更することはできません。
- **Web UI 一覧表示のページサイズ (Web UI list page size)** - リストに表示される行数によってページサイズを調整します。事前設定値は 10 行です。

- Web UI モード (**Web UI mode**) - 起動時のユーザー モード : 基本 (**Basic**)、詳細 (**Advanced**)、またはエキスパート (**Expert**) ([ロールと属性の可視性の設定 \(15 ページ\)](#)) を参照)。設定されていない場合、モードは、デフォルトで CCM サーバー設定で設定されているものになります ([サーバーの管理 \(175 ページ\)](#)) を参照)。
- Web UI ツリーのページ サイズ (**Web UI tree page size**) - Web UI に ツリー ビューを表示するときのページ サイズを調整します。
- Web UI ログのページ サイズ (**Web UI log page size**) - ログ ページのページ サイズを調整します。
- **Web UI レポート ページ サイズ (Web UI report page size)** - Web UI にレポート ページを表示するとき使用するページ サイズを調整します。
- **ビュー (Views)** - Web UI または CLI でのセッション起動時の DNS ビュー設定を指定します。
- **VPN** - Web UI または CLI でのセッション起動時の VPN 設定を指定します。
- **アラーム ポーリング間隔 (Alarm poll interval)** - アラームのポーリング間隔を調整します。つまり、Network Registrar がサーバーにアラーム データをポーリングする頻度です。
- **ホームページ (Homepage)** - お気に入りリストのページをアプリケーションのホームページとして設定します。デフォルトでは、[設定の概要 (**Configuration Summary**)] ページがホームページとして設定されています。選択したページをアプリケーションのホームページとして設定できます。これを行うには、目的のページを [お気に入り (**Favorites**)] リストに追加し ([Web UI のナビゲート \(14 ページ\)](#)) を参照)、[ホームページ (**Homepage**)] ドロップダウンリストからページ名を選択して、[ユーザー環境設定の変更 (**Modify User Preferences**)] をクリックします。Web UI の左上隅にあるホーム アイコン (🏠) をクリックすると、ホームページに移動できます。
- **日付形式 (Date format)** - Web UI の日時の値の日付と時刻の形式を設定します。形式は、デフォルトのリストから選択するか、テキスト形式で、<日付のパターン><時間のパターン> として入力できます。

サポートされているパターンは、次のとおりです。

- 年 : "yy"、"yyyy"
- 月 : "M"、"MM"、"MMM"、"MMMM"
- 日 : "d"、"dd"
- 時 : "h"、"hh"、"H"、"HH"
- 分 : "mm"
- 秒 : "s"、"ss"
- 区切り文字 : ":", "-", "/"

- **チャート X 軸タイムスタンプパターン (Chart X-Axis Timestamp Pattern)** - チャートを表示するときに X 軸にタイムスタンプを表示するために使用するパターンを指定します。
- **ツリーノード表示 (Tree node display)** - ツリーノードの初期表示オプションを指定します。この設定が [展開 (Expanded)] に設定され、ネストされた子ノードの数が 500 を超える場合、ツリーを表示するまでに数分かかることがあります。

ページサイズと Web UI モードの値を設定解除するには、属性の横にある [設定解除 (Unset?)] 列のチェックボックスをオンにします。ユーザー環境設定を行った後、[ユーザー環境設定の変更 (Modify User Preferences)] をクリックします。

ローカル Web UI でのクラスタの構成

ローカル Web UI で他のローカル Cisco Prime Network Registrar クラスタを定義できます。現在のマシン上のローカルクラスタは、**localhost** クラスタと呼ばれます。他のクラスタをセットアップするには、[操作 (Operate)] メニューから [クラスタの管理 (Manage Clusters)] を選択して、[クラスタのリスト/追加 (List/Add Clusters)] ページを開きます。**localhost** クラスタは、ローカルマシンの IP アドレスと SCP ポートを持つことに注意してください。

左側のペインで [クラスタの追加 (Add Cluster)] アイコンをクリックして、[クラスタの追加 (Add Cluster)] ページを開きます。少なくとも、リモートローカルクラスタの名前とアドレス (IPv4 または IPv6) を入力する必要があります。また、リモートクラスタの SCP ポート (1234 でない場合) とともに、管理者名とパスワードも入力する必要があります。[クラスタの追加 (Add Cluster)] をクリックします。クラスタを編集するには、左側の [クラスタ (Clusters)] ペインでクラスタ名をクリックして、[クラスタの編集 (Edit Cluster)] ページを開きます。セキュアアクセスモードを使用する場合は、[use-ssl as disabled]、[optional]、または [required] を選択します (optional はプリセット値です。required を選択した場合は、セキュリティライブラリがインストールされている必要があります)。変更を行い、[保存 (Save)] をクリックします。



- (注) ローカルクラスタマシンの IP アドレスを変更する場合は、**localhost** クラスタを変更して、[ipaddr] フィールドのアドレスを変更する必要があります。値をループバックアドレス (127.0.0.1) に設定しないでください。そうする場合には、DHCP フェールオーバーおよび高可用性 (HA) DNS 設定のために、メインサーバーとバックアップサーバーの実際の IP アドレスも設定する必要があります。

リージョンクラスタ Web UI

リージョンクラスタ Web UI は、リージョンおよび中央管理タスクへの同時アクセスを提供します。これは、各要素または機能ごとに設定できる権限を持つ、サーバー全体でのきめ細かい管理を提供します。アプリケーションにログインすると、[ホーム (Home)] ページが表示されます。リージョンクラスタ管理については、[中央構成の管理 \(95 ページ\)](#) で説明しています。

関連項目

[Web ベースのユーザー インターフェイスの概要 \(11 ページ\)](#)

[ローカル クラスタ Web UI \(18 ページ\)](#)

コマンドライン インターフェイス

Cisco Prime Network Registrar CLI (**nrcmd** プログラム) を使用して、ローカル クラスタ サーバーの動作を制御できます。設定可能なすべてのオプションを設定し、サーバーを起動および停止することもできます。



(注) CLI は、クラスタごとに最大 14 の同時ユーザーとプロセスによって、同時アクセスを提供します。



ヒント 詳細については、インストールディレクトリの **/docs** サブディレクトリにある **CLIContents.html** ファイルを参照してください。

CLI の **nrcmd** プログラムは、次の場所にあります。

- **Windows** - インストールパス\bin ディレクトリ。
- **Linux** - インストールパス/usrbin ディレクトリ。

ローカルクラスタで、適切なディレクトリにいる場合は、プロンプトで次のコマンドを使用します。

```
nrcmd [-C cluster[:port]] [-N user] [-P password] [-h] [-r] [-v] [-b < script | command]
nrcmd -C clustername:port -N username -P password [-L] -R
```

- **-C**- クラスタ名、プリセット値 **localhost**。別のクラスタに接続するために **nrcmd** を呼び出すときには、クラスタ名とともにポート番号を指定します。前の例を参照してください。
クラスタがデフォルトの SCP ポート (ローカルの場合は 1234、リージョンの場合は 1244) を使用する場合、ポート番号はオプションです。使用されるポートがデフォルトのポートではない場合は、必ずポート番号を含めてください。
- **-N**- ユーザー名。WebUI に初めてログインしたときに作成したユーザー名を入力する必要があります。
- **-P**- ユーザーパスワード。ユーザー名に対して作成したパスワードを入力する必要があります。
- **-L**- ローカル クラスタ CLI にアクセスします。
- **-R**- リージョン クラスタ CLI にアクセスします。

- **-b** < *script* - nrcmd コマンドのスクリプトファイル进行处理します。
- **-h** - このヘルプ テキストを表示します。
- **-r** - 読み取り専用ユーザーとしてログインします。
- **-R** - リージョンに接続します。
- **-v** (または **-vv**) - プログラムのバージョンを報告して終了します。
- **-V** - セッションの可視性を指定します。



(注) クラスタのデフォルトは、指定されていない場合は **localhost** です。



ヒント その他のコマンド オプションについては、/doc の **CLIGuide.html** ファイルを参照してください。



(注) ローカル クラスタ マシンの IP アドレスを変更する場合は、**localhost** クラスタを変更して、*ipaddress* 属性のアドレスを変更する必要があります。値を 127.0.0.1 に設定しないでください。

出力をファイルに送信することもできます。

```
nrcmd> session log filename
```

次に例を示します。

DHCP サーバー上のリースをファイル (*leases.txt*) に送信するには、次のコマンドを使用します。

```
nrcmd> session log leases.txt  
nrcmd> lease list
```



(注) 以前に開いたファイルを閉じるには、**session log** (ファイル名なし) を使用します。これにより、すべてのファイルへの出力の書き込みが停止します。

クラスタから切断するには、**exit** を使用します。

```
nrcmd> exit
```



ヒント CLI は、複数のユーザー ログインと連携して動作します。クラスタ ロック メッセージを受信した場合は、ロックしているユーザーを特定し、その人と問題を話し合います。(複数のユーザー (13 ページ) を参照。)

Prime Network Registrar でのグローバル検索

Prime Network Registrar のローカルおよびリージョン Web UI は、ローカルクラスタで使用可能な IP アドレスまたは DNS 名のグローバル検索機能も提供します。検索インターフェイス要素は、メインページの右上隅にあります。



- (注) 検索インターフェイス要素を表示し、IP アドレスと DNS 名の検索を実行するには、Cisco Prime Network Registrar が DHCP または DNS を使用してライセンスされている必要があります。また、ローカルクラスタに対して DHCP または DNS サービスが有効になっている必要があります（リージョン Web UI の [リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページで）。

次の表に、さまざまなシナリオでの一般的な検索結果を示します。

表 2: 一般的な検索結果

検索対象	アクティブなライセンスとサービス	検索結果
IPv4 アドレス	DHCP のみ	最も近く一致するスコープ、スコープのリース、またはスコープの予約
IPv4 アドレスまたは DNS FQDN	DNS のみ	関連するゾーンまたはリソースレコード
IPv6 アドレス	DHCP のみ	最も近く一致するプレフィックス、プレフィックスのリース、またはプレフィックス予約
IPv6 アドレスまたは DNS FQDN	DNS のみ	関連するゾーンまたはリソースレコード
IPv4 アドレス、IPv6 アドレス、または DNS FQDN	DHCP と DNS の両方	アドレスのタイプに基づいて、上記のすべて



第 3 章

サーバー ステータス ダッシュボード

Web ユーザー インターフェイス(Web UI)の Cisco Prime Network レジストラーサーバー ステータスダッシュボードには、トラッキングと診断に役立つグラフ、チャート、テーブルを使用して、システム ステータスのグラフィカル ビューが表示されます。これらのダッシュボード要素は、システム情報を整理および統合された方法で伝達するように設計されており、次の項目が含まれます。

- 重要なプロトコルサーバーおよびその他のメトリック
- アラームとアラート
- データベース インベントリ
- サーバーの正常性の傾向

ダッシュボードは、ダッシュボードを表示するシステムがその目的専用であり、プロトコルサーバーを実行しているシステムとは異なる場合があるトラブルシューティングのデスクコンテキストで使用するのが最適です。ダッシュボードシステムは、プロトコルサーバーを実行しているシステムをブラウザでポイントする必要があります。

ダッシュボードインジケータは、予想される通常の使用パターンからの逸脱を考慮して解釈する必要があります。異常なスパイクやアクティビティの低下に気付いた場合は、ネットワーク上で通信障害や停電が発生して調査する必要があります。

- [ダッシュボードを開く \(27 ページ\)](#)
- [表示タイプ \(28 ページ\)](#)
- [表示のカスタマイズ \(33 ページ\)](#)
- [含めるダッシュボード要素の選択 \(35 ページ\)](#)
- [ホストメトリック \(37 ページ\)](#)

ダッシュボードを開く

ダッシュボード機能は、地域クラスターでも使用できます。既定では、システムメトリックチャートが提供されます。さまざまなクラスターのサーバー固有の(DHCP、DNS、およびCDNS)

チャートを表示できます。これは、[チャートの選択 (Chart Selections)] ページで構成できます。

Web UI でダッシュボードを開くには、[操作 (Operate)] メニューから [ダッシュボード (Dashboard)] を選択します。

表示タイプ

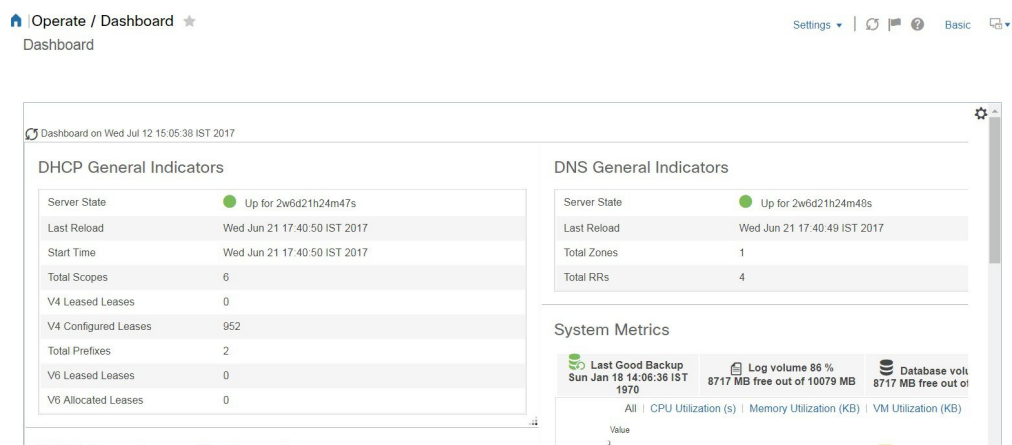
割り当てられた管理者ロールを使用して DHCP および DNS 権限を持っている場合、ダッシュボードのプリセット表示は次の表で構成されます(例については、次の表を参照してください)。

- [システム メトリック - システム メトリック \(37 ページ\)](#) を参照。
- [DHCP 一般インジケータ](#) - 『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「DHCP 一般インジケータ」の項を参照してください。
- [DNS 一般インジケータ](#): の『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「DNS 一般インジケータ」の項を参照してください。



ヒント これらは、プリセットの選択です。選択できる他のダッシュボード要素については、「[含めるダッシュボード要素の選択 \(35 ページ\)](#)」を参照してください。ダッシュボードには、セッション間での選択が保持されます。

図 4: プリセットのダッシュボード要素



各ダッシュボード要素は、最初は、要素に応じて、テーブルまたは特定のパネルチャートとして表示されます。

- [表-テーブル \(30 ページ\)](#) を参照。
- [折れ線グラフ - 折れ線グラフ \(30 ページ\)](#) を参照。
- [面グラフ - 面グラフ \(31 ページ\)](#) を参照。

一般ステータス インジケータ

上の図のサーバー状態の説明の緑色のインジケータに注意してください。これは、情報を提供するサーバーが正常に機能していることを示します。黄色のインジケータは、サーバーの動作が最適でないことを示します。赤いインジケータは、サーバーがダウンしていることを示します。これらのインジケータは、通常の Web UI の [サーバーの管理 (Manage Servers)] ページのサーバーの状態と同じです。

アラートレベルのグラフィックインジケータ

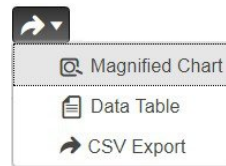
グラフ化された線とグラフの積み上げ領域は、標準の色と視覚的なコーディングに従って、主要な診断インジケータを一目ですぐに判断できます。グラフは、次の色とテキストのインジケータを使用します。

- **High alerts or warnings** — 線または赤の領域(ハッチングされたテクスチャ付き)。
- **All other indicators** — 線や様々な他の色の領域でデータ要素を区別。グラフでは、緑や黄色は使用しません。

グラフの拡大と変換

別のウィンドウでグラフを拡大するには、パネルグラフの下部にある **グラフリンクアイコン** をクリックし、次に「拡大グラフ」オプションをクリックします(下の図を参照)。拡大表示モードでは、最初に表示されるグラフの種類から別のグラフの種類を選択できます([その他のチャートタイプ \(32 ページ\)](#) を参照)。

図 5: 拡大グラフ



(注) 拡大されたグラフの自動更新はオフになっています。最新のデータを取得するには、ページの左上にある [ダッシュボード (Dashboard)] の横にある [更新 (Refresh)] アイコンをクリックします。

グラフを表に変換するには、「表としてグラフを表示する」を参照してください。表をグラフィック・グラフ形式に変換することはできません。

凡例

各グラフには、既定で色分けされた凡例が含まれています。

テーブル

テーブルとして表示されるダッシュボード要素には、行と列にデータが表示されます。以下のダッシュボード要素は、あらかじめ設定されており、テーブルで構成されます(または含める)。

- DHCP DNS の更新
- DHCP アドレスの現在の使用率
- DHCP の一般的なインジケータ
- DNS一般インジケータ
- DNS 一般インジケータのキャッシュ



(注) エキスパートモードでテーブルを表示すると、追加のデータが表示されることがあります。

折れ線グラフ

折れ線グラフとしてレンダリングされるダッシュボード要素には、x 軸と y 軸に対してプロットされた 1 つまたは複数の線を含めることができます。次の表では、3 種類の折れ線グラフについて説明します。

表 3: 折れ線グラフのタイプ

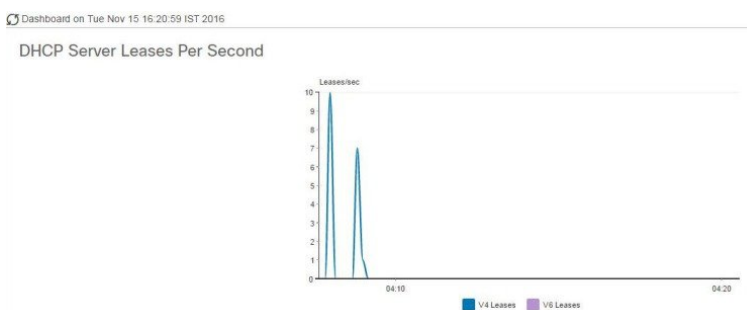
折れ線グラフの種類	説明	表示されるダッシュボード要素
生データ折れ線グラフ	生データに対してプロットされた線。	<ul style="list-style-type: none"> • Java 仮想マシン (JVM) メモリー使用率(エキスパート・モードのみ) • DHCP バッファ容量 • DHCP フェールオーバーステータス(2つのグラフ) • DNS ネットワーク エラー • DNS 関連サーバー のエラー
デルタ折れ線グラフ	2つの連続した生データの差に対してプロットされた線。	<ul style="list-style-type: none"> • DNS インバウンドゾーン転送 • DNS アウトバウンドゾーン転送

折れ線グラフの種類	説明	表示されるダッシュボード要素
レート折れ線グラフ	2つの連続した生データの差に対してプロットされた線は、それらの間のサンプル時間で割った。	<ul style="list-style-type: none"> • DHCP サーバー要求アクティビティ(下の画像を参照) • DHCP サーバー応答アクティビティ • DHCP 応答遅延 • DNS クエリー応答 • DNS 転送エラー



ヒント デルタまたはレートデータを示すグラフの生データを取得するには、エキスパートモードに入り、必要なチャートに移動します。パネルチャートの下にある[**チャートリンク (ChartLink)**] アイコンをクリックしてから[**データテーブル (Data Table)**]をクリックします。生データテーブルは、グラフデータテーブルの下にあります。

図 6: 折れ線グラフの例



面グラフ

面グラフとしてレンダリングされるダッシュボード要素は、複数の関連するメトリックを傾向グラフとしてプロットしますが、一方が積み上げ、最高点が累積値を表すようにします。値は、コントラストの色で個別にシェーディングされます。(面グラフとして図 6: 折れ線グラフの例 (31 ページ) に表示される DHCP サーバー要求アクティビティ チャートの例については、次の図を参照してください)。

図 7: 面グラフの例



これらは、凡例にリストされている順序で積み重ねられ、スタックの下部に左端の凡例項目、スタックの一番上に右端の凡例項目が表示されます。面グラフに事前に設定されているダッシュボード要素は次のとおりです。

- DHCP バッファ容量
- DHCP フェールオーバーステータス
- DHCP 応答遅延
- 1 秒あたりの DHCP サーバーのリース数
- DHCP サーバー要求アクティビティ
- DHCP サーバーの応答アクティビティ
- DNS 受信ゾーン転送
- DNS ネットワーク エラー
- DNS 送信ゾーン転送
- 1 秒あたりの DNS クエリ
- DNS 関連サーバー エラー

その他のチャートタイプ

選択できるその他のグラフの種類は次のとおりです。

- **Line-** [折れ線グラフ \(30 ページ\)](#) で説明した折れ線グラフの 1 つ。
- **Area-** [面グラフ \(31 ページ\)](#) で説明したグラフ。
- **Column-** グラフを横方向に垂直バーで表示し、値軸をグラフの左側に表示します。
- **Scatter-** 散布図は、デカルト座標を使用して、一連のデータの通常 2 つの変数の値を表示するプロットまたは数学図の一種です。



ヒント 各グラフの種類は、異なる方法で、異なる解釈でデータを示しています。どのタイプが最適かを判断できます。

ダッシュボード要素のヘルプの取得

テーブル/グラフウィンドウのヘルプアイコンをクリックすると、各ダッシュボード要素のヘルプウィンドウを開くことができます。

表示のカスタマイズ

ダッシュボードの表示をカスタマイズするには、次の操作を行います。

- データを更新し、自動更新間隔を設定します。
- グラフを展開し、別の形式でレンダリングします。
- グラフィック グラフを表に変換します。
- データをコンマ区切り値 (CSV) 出力にダウンロードします。
- グラフの凡例を表示または非表示にします。
- サーバー グラフの種類を構成します。
- デフォルト表示にリセット

各グラフは次の機能をサポートします。

- サイズ変更
- 新しいセル位置にドラッグ アンド ドロップ
- 最小化
- クローズ

各グラフには、グラフの説明と、説明の下部にあるリンク (詳細..) をクリックすると詳細なヘルプが表示されたヘルプ アイコンが表示されます。



(注) ダッシュボード/グラフに加えられた変更は、[ダッシュボード (Dashboard)]ウィンドウで[保存 (Save)]をクリックした場合にのみ保持されます。

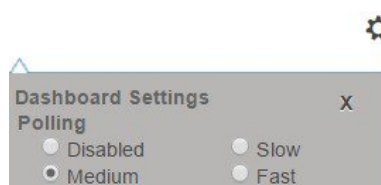
表示の更新

[最新の情報に更新 (Refresh)] アイコンをクリックして、最新のポーリングを選択するように各ディスプレイを更新します。

ポーリング間隔の設定

データのポーリング頻度を設定できます。ダッシュボード表示の右上隅の [ダッシュボード設定 (Dashboard Settings)] アイコンをクリックします。キャッシュされたデータのポーリング間隔を設定するには、4つのオプションがあり、プロトコルサーバーに更新のポーリングを行います (下の図を参照)。

図 8: グラフのポーリング間隔の設定



キャッシュされたデータポーリング (したがって、自動更新) 間隔を次の値に設定できます。

- **Disabled**—ポーリングを行わないため、データは自動的に更新されません。
- **Slow**—30 秒ごとにデータを更新します。
- **Medium**—20 秒ごとにデータを更新します。
- **Fast** (プリセット値) —10 秒ごとにデータを更新します。

表としてのグラフの表示

パネルグラフの下部にある [チャートリンク (Chart Link)] アイコンを使用して、チャートリンクオプションを表示します (下の図を参照)。[データテーブル (Data Table)] オプションをクリックすると、グラフィック チャートを表として表示できます。

図 9: 表形式へのグラフ変換の指定



CSV形式へのエクスポート

グラフデータは、カンマ区切り値 (CSV) ファイル (スプレッドシートなど) にダンプできます。パネルグラフの下部にあるチャートリンクコントロール (上の図を参照) で、[CSV形式でエクスポート (CSV Export)] オプションをクリックします。[名前を付けて保存 (Save As)] ウィンドウが表示され、CSV ファイルの名前と場所を指定できます。

含めるダッシュボード要素の選択

ページに表示するダッシュボードエレメントの数を決定できます。DHCP サーバーなど、1つのサーバーのアクティビティのみに集中し、他のサーバーの他のすべてのメトリックを除外する場合があります。このように、ダッシュボードの混雑が少なくなり、要素が大きくなり、読みやすくなります。それ以外の場合は、すべてのサーバーアクティビティの概要を表示し、結果として小さな要素を表示する場合があります。

[ダッシュボードの設定 (Dashboard Settings)] アイコンをクリックし、[ダッシュボードの設定 (Dashboard Settings)] ダイアログの [チャート選択 (Chart Selection)] をクリックすると、メインの [ダッシュボード (Dashboard)] ページから表示するダッシュボード要素を選択できます。リンクをクリックすると、[チャートの選択 (Chart Selection)] ページが開きます (図 10: [ダッシュボード要素の選択 \(36 ページ\)](#) を参照)。

サーバー チャート タイプの設定

メインダッシュボードビューでデフォルトのグラフタイプを設定できます。ダッシュボードのサーバー・グラフをカスタマイズして、特定のグラフ・タイプのみをデフォルトとして表示できます。

既定のグラフの種類を設定するには、表示するメトリック スグラフに対応するチェックボックスをオンにし、**Type** ドロップダウンリストからグラフの種類を選択します。既定のグラフの種類は、さまざまなユーザーセッション間で一貫性があり、共有されます (下の図を参照)。

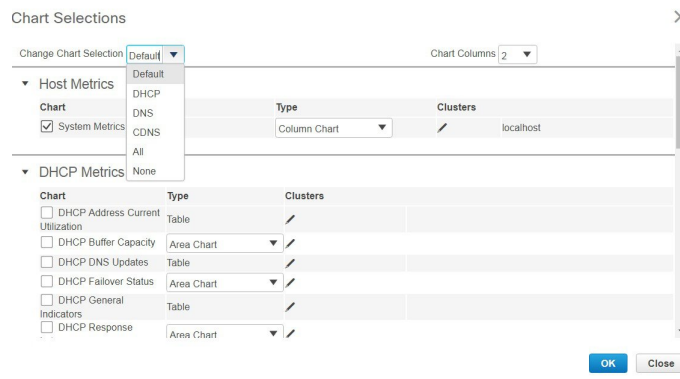


(注) サーバーで構成されたサービスに基づいて、[ダッシュボードの設定 (Dashboard Settings)] > [グラフの選択 (Chart Selection)] ページで CDNS または DNS メトリックを確認できます。



ヒント ダッシュボード要素がグラフの選択リストに表示される順序は、必ずしもページ上での要素の表示順序を決定するものではありません。使用可能な領域を考慮するアルゴリズムによって、グリッドレイアウトの順序とサイズが決まります。ダッシュボード要素の選択を送信するたびにレイアウトが異なる場合があります。選択を変更するには、表示するダッシュボード要素の横にあるチェックボックスをオンにします。

図 10: ダッシュボード要素の選択



上の図は、リージョン Web UI のグラフ選択テーブルを表示します。[クラスター (Clusters)] 列は、リージョンダッシュボードでのみ使用でき、構成されているローカルクラスターの一覧が表示されます。ローカルクラスターを追加するには、[編集 (Edit)] アイコンをクリックし、[ローカルクラスターリスト (Local Cluster List)] ダイアログボックスでローカルクラスター名を選択します。

選択を変更するには、表示するダッシュボード要素の横にあるチェックボックスをオンにします。

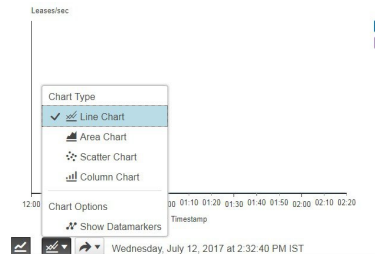
ページの上部にある [チャート選択の変更 (Change Chart Selection)] ドロップダウンリストで特定のグループコントロールを使用できます (上の図を参照)。その内容は:

- すべてのチェックボックスをオフにするには、[なし (None)] を選択します。
- プリセットの選択に戻すには、[デフォルト (Default)] を選択します。DHCP および DNS をサポートする管理者ロール用の事前設定されたダッシュボード要素は次のとおりです。
 - ホストメトリック: システムメトリック
 - DHCP メトリック: 一般的なインジケーター
 - DNS メトリック: 一般的なインジケーター
- DHCP メトリックのみを選択し、**DHCP** を選択します (『Cisco Prime Network Registrar 10.1 DHCP User Guide』の「DHCP Metrics」の項を参照)。
- DNS メトリックのみを選択し、**DNS** を選択します (『Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide』の「Authoritative DNS Metrics」の項を参照)。
- DNS メトリックのみを選択し、**CDNS** を選択します (『Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide』の「Caching DNS Metrics」の項を参照)。
- すべてのダッシュボード要素を選択するには、[すべて (All)] を選択します。

ページの下部にある [OK] をクリックして選択内容を保存するか、または [キャンセル (Cancel)] をクリックして、変更をキャンセルします。

グラフの種類を変更するには、パネルチャートの下部にある [グラフの種類 (Chart Type)] アイコンをクリックし、必要なグラフの種類を選択します (下の図を参照)。使用できるグラフには、折れ線グラフ、棒グラフ、面グラフ、散布図があります。

図 11: グラフの種類の選択



ホストメトリック

ホストメトリックは、次の2つのチャートで構成されます。

- [システムメトリック - システムメトリック \(37 ページ\)](#) を参照。
- [JVM メモリ使用率 \(エキスパートモードでのみ使用可能\) - JVM メモリ使用率 \(38 ページ\)](#) を参照。

システムメトリック

システムメトリックダッシュボード要素は、Cisco Prime Network Registrar のログおよびデータベースディレクトリがあるディスクボリュームの空き領域、最後のサーバーバックアップの日付と時刻、およびさまざまなサーバーの CPU とメモリの使用率を示します。システムメトリックは、[チャート選択 (Chart Selection)] リストで [ホストメトリック: システムメトリック (Host Metrics: System Metrics)] を選択した場合に使用できます。

結果の表には、次のように表示されます。

- ログボリューム (**Logs Volume**) - logs ディレクトリがあるディスクドライブの合計領域のうちの現在の空き領域 (空き領域のパーセンテージ)。
- データベースボリューム (**Database Volume**) - data ディレクトリがあるディスクドライブの合計領域のうちの現在の空き領域 (空き領域のパーセンテージ)。
- 正常な最終バックアップ (**Last Good Backup**) - サーバーエージェントの前の起動後の前の成功したシャドウバックアップが行われた日付と時刻 (または、まだおこなわれていない場合は、[未完了 (Not Done)])。
- 以下についての [CPU 使用率 (**CPU Utilization**)] (秒単位)、[メモリ使用率 (**Memory Utilization**)] (キロバイト単位)、[VM 使用率 (**VM Utilization**)] (キロバイト単位)、およびプロセス ID (**PID**)
 - Cisco Prime Network Registrar サーバーエージェント

- CCM サーバー
- DNS サーバー
- DHCP サーバー
- Web サーバー
- SNMP サーバー
- DNS キャッシュ サーバー

データの解釈方法

システム メトリック データは、Cisco Prime Network Registrar の logs および data ボリュームについて、使用可能な空き領域に基づき、ディスク ボリュームがどの程度いっぱいになっているかを示します。また、データ ファイルが最後に正常にバックアップされたかどうか、および行われた日時も示します。最後に、Cisco Prime Network Registrar サーバーが使用している使用可能な CPU とメモリの量を示します。メモリと VM 使用率の値の違いは、次のとおりです。

- **Memory Utilization** - プロセスが使用している物理メモリ。または、UNIX の **ps** コマンドの出力の常駐セット サイズ (RSS) の値、または Windows のタスクマネージャのメモリ使用率の値にほぼ相当し、プロセスが実メモリに持つページ数から管理使用量を差し引いたものです。この値には、テキスト、データ、またはスタック領域に対してカウントされるページだけが含まれ、デマンドロードまたはスワップアウトされたページは含まれません。
- **VM Utilization** - プロセスが使用している仮想メモリ。または、UNIX の **ps** コマンドの出力の SZ 値、または Windows のタスクマネージャの VM サイズの値にほぼ相当し、メモリ内ページ数にページファイルとデマンドゼロ ページを加えたものですが、通常、メモリマップされたファイルは含まれません。この値は、プロセスの大きさを診断し、それが増加し続けるかどうかを診断するのに役立ちます。

結果に基づくトラブルシューティング

logs または data ディレクトリの空きディスク容量の減少に気づいた場合は、ディスク容量の増加を検討するか、または Cisco Prime Network Registrar と同時に実行しているプログラムを確認してください。

JVM メモリ使用率

Java 仮想マシン (JVM) メモリ使用率ダッシュボード要素は、エキスパート モードの場合にのみ使用できます。これは、JVM メモリの未使用の最大、未使用、および使用バイトをトレースする折れ線トレンドチャートとしてレンダリングされます。このチャートは、エキスパート モードのときに、[チャートの選択 (Chart Selection)] リストで [ホスト メトリック : JVM メモリ使用率 (Host Metrics: JVM Memory Utilization)] を選択した場合に使用できます。

データの解釈方法

JVMメモリ使用率データは、ブラウザでダッシュボードを実行するためにどのくらいのメモリが適用されるかを示しています。使用バイトデータのスパイクが表示される場合は、ダッシュボードの要素がメモリを大量に使用している可能性があります。

結果に基づくトラブルシューティング

使用メモリデータが急増している場合は、ブラウザの設定を確認するか、ポーリング間隔を調整してデータのポーリング頻度を低くします。



第 II 部

ローカルおよびリージョンの管理

- [管理者の管理 \(43 ページ\)](#)
- [所有者とリージョンの管理 \(89 ページ\)](#)
- [中央構成の管理 \(95 ページ\)](#)
- [ルータおよびルータ インターフェイスの管理 \(171 ページ\)](#)
- [サーバーとデータベースの保守 \(175 ページ\)](#)
- [バックアップとリカバリ \(221 ページ\)](#)
- [レポートの管理 \(247 ページ\)](#)



第 4 章

管理者の管理

この章では、ローカルクラスターとリージョンクラスターでネットワーク管理者をセットアップする方法について説明します。この章には、多くの管理機能に関するローカルおよびリージョンクラスターのチュートリアルも含まれています。

- [管理者、グループ、ロール、テナント \(43 ページ\)](#)
- [外部認証サーバー \(50 ページ\)](#)
- [テナントの管理 \(54 ページ\)](#)
- [管理者の管理 \(60 ページ\)](#)
- [パスワードの管理 \(63 ページ\)](#)
- [グループの管理 \(63 ページ\)](#)
- [ロールの管理 \(65 ページ\)](#)
- [きめ細かい管理 \(66 ページ\)](#)
- [管理者の一元管理 \(71 ページ\)](#)
- [セッション管理 \(84 ページ\)](#)

管理者、グループ、ロール、テナント

ネットワーク管理者が Cisco Prime Network Registrar で実行できる機能のタイプは、割り当てられたロールに基づきます。ローカルおよびリージョン管理者は、これらのロールを定義して、ネットワーク管理機能の粒度を提供できます。Cisco Prime Network Registrar では、管理機能をセグメント化する基本ロールのセットが事前定義されています。これらの基本ロールから、特定のアドレス、ゾーン、およびその他のネットワークオブジェクトの管理に限定された、さらに制約されたロールを定義できます。

管理者をロールに関連付けるためのメカニズムは、これらのロールを含むグループに管理者を配置することです。

管理者が表示できるデータと設定は、テナントによっても制限されます。管理者にテナントタグが割り当てられている場合、アクセスはテナントに割り当てられたか、読み取り専用のコア設定オブジェクトとしてテナントでの使用が可能にされた設定オブジェクトにさらに制限されます。

関連項目

[管理者とグループ、ロール、およびテナントとの関連 \(44 ページ\)](#)

[管理者タイプ \(45 ページ\)](#)

[ロール、サブロール、および制約 \(45 ページ\)](#)

[グループ \(49 ページ\)](#)

[管理者の管理 \(60 ページ\)](#)

[パスワードの管理 \(63 ページ\)](#)

[グループの管理 \(63 ページ\)](#)

[ロールの管理 \(65 ページ\)](#)

[テナントの管理 \(54 ページ\)](#)

管理者とグループ、ロール、およびテナントとの関連

Cisco Prime Network Registrarには、管理者、グループ、ロール、およびテナントの4つの管理者オブジェクトがあります。

- **管理者 (Administrator)** - ログインしたアカウントは、1つ以上の管理者グループとの関連付けによって、割り当てられたロールに基づいて特定の機能を実行できます。ローカルクラスタでは、これらの機能は、ローカルの中央構成管理 (CCM) サーバーとデータベース、ホスト、ゾーン、アドレス空間、および DHCP を管理しています。リージョンクラスタでは、これらの機能は、リージョン CCM サーバーとデータベース、中央構成、およびリージョンのアドレス空間を管理しています。有効にするには、管理者を少なくとも1つのグループに割り当てる必要があります。

管理者の追加については、[管理者の管理 \(60 ページ\)](#) を参照してください。

- **グループ (Group)** - ロールのグループ化。1つ以上のグループを管理者に関連付ける必要があります。グループを使用可能にするには、グループに少なくとも1つのロールが割り当てられている必要があります。Cisco Prime Network Registrar の事前定義グループは、各ロールを一意的なグループにマッピングします。

グループの追加については、[グループの管理 \(63 ページ\)](#) を参照してください。

- **ロール (Role)** - 管理者が管理できるネットワーク オブジェクトと、管理者が実行できる機能を定義します。事前定義の一連のロールがインストール時に作成され、追加の制約付きロールを定義できます。一部のロールには、さらに機能的な制約を加えるサブロールが含まれています。

ロールの追加については、[ロールの管理 \(65 ページ\)](#) を参照してください。

- **テナント (Tenant)** - 管理者のセットに関連付けられているテナント組織またはグループを識別します。テナントを作成すると、リージョンとローカルの両方のクラスタに保存されるデータは、テナント別にセグメント化されます。テナントが別のテナントのデータにアクセスすることはできません。

テナントの追加については、[テナントの管理 \(54 ページ\)](#) を参照してください。

管理者タイプ

管理者には、スーパーユーザーと専門管理者の2つの基本タイプがあります。

- **スーパーユーザー (Superuser)** - Web UI、CLI、およびすべての機能への無制限のアクセス権を持つ管理者。この管理者タイプは少数のユーザーに制限する必要があります。管理者のスーパーユーザー権限は、他のすべてのロールをオーバーライドします。



インストール時、または Web UI に初めてログインするときに、スーパーユーザーとパスワードを作成する必要があります。

スーパーユーザーにテナントタグが割り当てられている場合、無制限のアクセスは、対応するテナントデータについてのみ付与されます。他のテナントのデータは表示できず、コアオブジェクトは読み取り専用アクセスに制限されます。

- **専門 (Specialized)** - 管理者が割り当てたロール（および該当する場合はサブロール）に基づいて、特定の DNS 転送またはリバースゾーンを管理するなど、特別な機能を実行するために名前によって作成された管理者。専門管理者は、スーパーユーザーと同様に、パスワードを必要としますが、関連するロールを定義する少なくとも1つの管理者グループに割り当てられる必要もあります。CLI は **admin** コマンドを提供します。

ローカルゾーンまたはホスト管理者を作成する例については、[管理者の作成 \(152 ページ\)](#) を参照してください。

テナントタグが割り当てられている専門ユーザーは、関連するロールにも一致する、対応するテナントまたはコアデータにのみアクセスできます。コアデータは、さらに読み取り専用アクセスに制限されます。

ロール、サブロール、および制約

ライセンスタイプは、各ロールとサブロールの組み合わせに関連付けられます。ロールとサブロールは、そのライセンスがそのクラスターで使用可能な場合にのみ有効になります。

制約を適用することによって、管理者ロールを制限できます。たとえば、**host-admin** 基本ロールを使用して、192.168.50.0 サブネットに制約されている 192.168.50.0-host-admin という名前のホスト管理者を作成できます。管理者は、このロールを含むグループを割り当てた後、この制約を有効にしてログインします。ロールとサブロールの追加については、[ロールの管理 \(65 ページ\)](#) で説明しています。

ロールの制約を読み取り専用アクセスに制限することができます。管理者は、そのロールのデータを読み取ることはできますが、変更することはできません。ただし、制限されたデータが読み取り/書き込みロールにも関連付けられている場合、読み取り/書き込み権限は読み取り専用の制約に優先します。



ヒント ロール制約の追加の例は、[制約付きのホスト管理者ロールの作成 \(157ページ\)](#) にあります。

DNS とホスト管理者ロールの割り当ての間の相互作用により、制約のない `dns-admin` ロールをグループ内の任意の `host-admin` ロールと組み合わせることができます。たとえば、グループ内の `dns-admin-readonly` ロールと `host-admin` ロールを組み合わせる（およびグループに `host-rw-dns-ro` という名前を付ける）と、完全なホストアクセス権と読み取り専用アクセス権がゾーンと RR に与えられます。ただし、制限付きの `dns-admin` ロールを `host-admin` ロールとともにグループに割り当て、次に管理者に割り当てると、制約付き `dns-admin` ロールが優先され、ログイン時の管理者権限によってホスト管理が排除されます。

特定のロールにはサブロールがあり、それによってロール機能をさらに制限できます。たとえば、ローカルの `ccm-admin` または `regional-admin` に `owner-region` サブロールが適用されると、所有者とリージョンのみを管理できます。デフォルトでは、制約付きのロールを作成すると、可能なすべてのサブロールが適用されます。

事前定義されたロールについては、[表 4: ローカル クラスタ管理者の事前定義ロールと基本ロール \(46 ページ\)](#)（ローカル）と [表 5: リージョン クラスタ管理者の事前定義ロールと基本ロール \(48 ページ\)](#)（リージョン）を参照してください。

表 4: ローカル クラスタ管理者の事前定義ロールと基本ロール

ローカル ロール	サブロールとアクティブな機能
<code>addrblock-admin</code>	<p>コア機能：アドレス ブロック、サブネット、およびリバース DNS ゾーンを管理します（<code>dns-admin</code> も必要）。また、スコープ アクティビティを通知します。</p> <ul style="list-style-type: none"> • <code>ric-management</code>：DHCP フェールオーバーペアとルータにサブネットをプッシュし、再利用します。 • <code>ipv6-management</code>：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • <code>lease-history</code>：リース履歴データを照会、ポーリング、およびトリミングします。
<code>ccm-admin</code>	<p>コア機能：アクセス コントロール リスト (ACL) と暗号キーを管理します。</p> <ul style="list-style-type: none"> • <code>authentication</code>：管理者を管理します。 • <code>authorization</code>：ロールとグループを管理します。 • <code>owner-region</code>：所有者とリージョンを管理します。 • <code>database</code>：データベースの変更エントリを表示し、CCM の変更セットをトリミングします。 • <code>security-management</code>：ACL と DNSSEC の設定を管理します。

ローカル ロール	サブロールとアクティブな機能
cdns-admin	<p>コア機能：メモリ内キャッシュを管理します（フラッシュ キャッシュとフラッシュ キャッシュ名）。</p> <ul style="list-style-type: none"> • <i>security-management</i>：ACL と DNSSEC の設定を管理します。 • <i>server-management</i>：DNSSEC 設定、フォワーダー、例外、DNS64、およびスケジュールされたタスクを管理し、サーバーを停止、開始、またはリロードします。
cfg-admin	<p>コア機能：クラスタを管理します。</p> <ul style="list-style-type: none"> • <i>ccm-management</i>：CCM サーバーの設定を管理します。 • <i>dhcp-management</i>：DHCP サーバーの設定を管理します。 • <i>dns-management</i>：DNS サーバーの設定を管理します。 • <i>cdns-management</i>：キャッシング DNS サーバーの設定を管理します。 • <i>ric-management</i>：ルータを管理します。 • <i>snmp-management</i>：SNMP サーバーの設定を管理します。 • <i>tftp-management</i>：TFTP サーバーの設定を管理します。
dhcp-admin	<p>コア機能：DHCP スコープとテンプレート、ポリシー、クライアント、クライアントクラス、オプション、リース、および予約を管理します。</p> <ul style="list-style-type: none"> • <i>lease-history</i>：リース履歴データを照会、ポーリング、およびトリミングします。 • <i>ipv6-management</i>：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • <i>server-management</i>：DHCP サーバーの設定、フェールオーバー ペア、LDAP サーバー、拡張、および統計情報を管理します。
dns-admin	<p>コア機能：DNS ゾーンとテンプレート、リソース レコード、セカンダリ サーバー、およびホストを管理します。</p> <ul style="list-style-type: none"> • <i>security-management</i>：DNS 更新ポリシー、ACL、および暗号キーを管理します。 • <i>server-management</i>：DNS サーバーの設定とゾーン分散を管理し、ゾーンと HA サーバーのペアを同期し、更新マップをプッシュします。 • <i>ipv6-management</i>：IPv6 ゾーンとホストを管理します。 • <i>enum-management</i>：DNS ENUM ドメインと番号を管理します。

ローカル ロール	サブロールとアクティブな機能
host-admin	コア機能：DNS ホストを管理します。（管理者に制約付き dns-admin ロールも割り当てられた場合、これは host-admin の定義をオーバーライドするため、管理者には host-admin ロールが割り当てられないことに注意してください）。

表 5: リージョンクラスタ管理者の事前定義ロールと基本ロール

リージョンのロール	サブロールとアクティブな機能
central-cfg-admin	<p>コア機能：クラスタを管理し、レプリカ データを表示します。</p> <ul style="list-style-type: none"> • <i>dhcp-management</i> : DHCP スコープテンプレート、ポリシー、クライアントクラス、フェールオーバー ペア、バーチャルプライベート ネットワーク (VPN) 、およびオプションを管理します。サブネットを変更します。データを複製します。 • <i>ric-management</i> : ルータとルータ インターフェイスを管理し、レプリカ ルータのデータをプルします。 • <i>ccm-management</i> : CCM サーバーの設定を管理します。 • <i>snmp-management</i> : SNMP サーバーの設定を管理します。 • <i>ipv6-management</i> : IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • <i>cdns-management</i> : CDNS サーバーの設定を管理します。 • <i>byod-management</i> : BYOD サーバーの設定を管理します。
central-dns-admin	<p>コア機能：DNS ゾーンとテンプレート、ホスト、リソース レコード、およびセカンダリ サーバーを管理します。サブゾーンと逆引きゾーンを作成します。</p> <ul style="list-style-type: none"> • <i>security-management</i> : DNS 更新ポリシー、ACL、および暗号キーを管理します。 • <i>server-management</i> : DNS ゾーンと HA サーバー ペアを同期し、ゾーン分散を管理し、レプリカ ゾーンデータをプルし、更新マップをプッシュします。 • <i>ipv6-management</i> : IPv6 ゾーンとホストを管理します。 • <i>enum-management</i> : DNS ENUM ドメインと番号を管理します。

リージョンのロール	サブロールとアクティブな機能
central-host-admin	コア機能：DNS ホストを管理します。（管理者に制約付き central-dns-admin ロールも割り当てられた場合、これは central-host-admin の定義をオーバーライドするため、管理者には central-host-admin ロールが割り当てられないことに注意してください）。
regional-admin	コア機能：ライセンスと暗号キーを管理します。 <ul style="list-style-type: none"> • <i>authentication</i>：管理者を管理します。 • <i>authorization</i>：ロールとグループを管理します。 • <i>owner-region</i>：所有者とリージョンを管理します。 • <i>database</i>：データベースの変更エントリを表示し、CCM の変更セットをトリミングします。 • <i>security-management</i>：ACL と DNSSEC の設定を管理します。
regional-addr-admin	コア機能：アドレスブロック、サブネット、およびアドレス範囲を管理します。割り当てレポートを生成します。レプリカ アドレス空間データをプルします。 <ul style="list-style-type: none"> • <i>dhcp-management</i>：サブネットをプッシュし、再利用します。サブネットを DHCP フェールオーバー ペアに追加し、削除します。 • <i>lease-history</i>：リース履歴データを照会、ポーリング、およびトリミングします。 • <i>subnet-utilization</i>：サブネットとプレフィックス使用率データのクエリ、ポーリング、トリミング、およびコンパクト化を行います。 • <i>ipv6-management</i>：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • <i>byod-management</i>：BYOD サーバーの設定を管理します。

グループ

管理者グループは、管理者にロールを割り当てるために使用されるメカニズムです。したがって、グループは、使用可能な1つ以上の管理者ロールで構成される必要があります。Cisco Prime Network Registrar を初めてインストールすると、事前定義の各ロールに対応する事前定義のグループが作成されます。

同じ基本ロールを持つロールは結合されます。制約のない *dhcp-admin* ロールと制約付きの *dns-admin* ロールを持つグループは、*dns-admin* ロールに割り当てられた権限を変更しません。たとえば、いずれかのロールに制約なしの読み取り/書き込み権限が割り当てられている場合、他のロールには読み取り専用権限が割り当てられていても、そのグループには制約なしの読み

取り/書き込み権限が割り当てられます。したがって、すべてのデータへの読み取り専用アクセスを許可しながら、ユーザーの読み取り/書き込み権限を制限するには、制約付きの読み取り/書き込みロールとともに、制約なしの読み取り専用ロールを含むグループを作成します。
 (グループ内の `host-admin` ロールと `dns-admin` ロールの組み合わせの実装については、[ロール、サブロール、および制約 \(45 ページ\)](#) を参照してください)。

外部認証サーバー

Cisco Prime Network Registrar には、CCM サーバーの認証および承認モジュールと統合された RADIUS クライアント コンポーネントと Active Directory (AD) クライアント コンポーネントが含まれています。外部認証を有効にするには、ローカルおよびリージョン クラスターで外部 RADIUS または AD サーバーのリストを設定し、すべての承認ユーザーがそれぞれのサーバーで適切に設定されていることを確認する必要があります。

外部認証が有効なとき、CCM サーバーは、RADIUS サーバーに対して RADIUS 要求を発行するか、設定済みリストから選択された AD サーバーに対して LDAP 要求を発行することによって、Web UI、SDK、または CLI を介したログインの試みを処理します。対応するサーバーがログイン要求を検証した場合、アクセスが許可され、CCM サーバーは RADIUS または AD サーバーが指定したグループ割り当てを持つ承認済みセッションを作成します。



(注) CCM サーバーのデータベースで定義されている管理者は、外部認証が有効になっている場合は無視されます。これらのユーザー名とパスワードを使用してログインしようとしても失敗します。外部認証を無効にするには、設定されているすべての外部サーバーを削除または無効にするか、`auth-type` 属性値を [ローカル (Local)] に変更する必要があります。



ヒント RADIUS サーバーにアクセスできないか、誤って設定されているために、すべてのログインが失敗する場合は、`local.superusers` ファイルを使用して、一時的なユーザー名とパスワードを作成します。詳細については、[管理者の管理 \(60 ページ\)](#) を参照してください。

RADIUS 外部認証サーバーの設定

RADIUS サーバーを起動して実行し、ユーザーを作成したら、RADIUS ユーザーが Cisco Prime Network Registrar にログインするために必要な特定のグループとベンダー固有の属性 (VSA) がいくつかあります。Cisco ベンダー `id (9)` を使用し、`cnr:groups=group1,group2,group3` の形式を使用して、管理者ごとに Cisco Prime Network Registrar のグループ属性を作成します。

たとえば、管理者を組み込みグループ `dhcp-admin-group` および `dns-admin-group` に割り当てるには、次のように入力します。

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

スーパーユーザーのアクセス権限を割り当てるには、予約済みグループ名 **superusers** が使用されます。管理者にスーパーユーザー権限を与えるには、次のように入力します。

```
cnr:groups=superusers
```

スーパーユーザー権限は、他のすべてのグループよりも優先されます。

Cisco Prime Network Registrar に使用される VSA 名は、**cisco-avpair** です。次に、Cisco Prime Network Registrar 用の FreeRadius サーバーの設定例を示します。

ユーザーの場合：（これには、サーバーからのデフォルト情報が含まれます）

```
ciscoprime Cleartext-Password := "Cisco123" -> CPNR Username/Password
Service-Type = Framed-User,
cisco-avpair += "cnr:groups=superusers", -> CPNR group for CNR. This is the VSA.
Framed-Protocol = PPP,
Framed-IP-Address = 192.168.1.2, -> CPNR IP
Framed-Filter-Id = "std.ppp",
Framed-MTU = 1500,
```

クライアントの場合：

```
client CNR-HOST {
  ipaddr = 192.168.1.2 -> IP of CPNR server
  secret = P@$$W0rd! -> Password for CPNR Radius
```

RADIUS サーバーを保存してリロードすると（すべての設定が正しいことを前提として）、RADIUS で作成されたユーザーを使用して Cisco Prime Network Registrar にログインでき、認証が可能になります。



- (注) Cisco Prime Network Registrar を使用して、外部ユーザー名とそのパスワードまたはグループを追加、削除、または変更することはできません。この設定を実行するには、RADIUS サーバーを使用する必要があります。

RADIUS 外部コンフィギュレーション サーバーの追加

外部コンフィギュレーション サーバーを追加するには、次の手順を実行します。

ローカルの詳細 [Web UI](#) とリージョンの詳細 [Web UI](#)

- ステップ 1** [管理 (Administration)] メニューから、[外部認証 (External Authentication)] サブメニューの [Radius] を選択します。[Radius サーバーの一覧表示/追加 (List/Add Radius Server)] ページが表示されます。
- ステップ 2** [Radius] ペインで [Radius の追加 (Add Radius)] アイコンをクリックして、外部認証サーバーとして設定するサーバーの名前、IPv4 および/または IPv6 アドレスを入力し、[外部認証サーバーの追加 (Add External Authentication Server)] ダイアログボックスで、このサーバーとの通信に使用する *key* 属性を設定し、[外部認証サーバーの追加 (Add External Authentication Server)] をクリックします。CCM サーバーはキーを使用して、クライアントとサーバーによって共有される秘密鍵である *key-secret* 属性を設定します。
- ステップ 3** 外部認証サーバーを有効にするには、[Radius サーバーの編集 (Edit Radius Server)] ページで、*ext-auth* 属性の [有効 (enabled)] チェックボックスをオンにして、[保存 (Save)] をクリックします。
- ステップ 4** [サーバーの管理 (Manage Servers)] ページで *auth-type* 属性を RADIUS に変更し、[保存 (Save)] をクリックしてから、Cisco Prime Network Registrar を再起動します。

- (注) この時点で、ローカル認証が無効になっているために Cisco Prime Network Registrar にログインできない場合は、`/opt/var/nwreg2/local/conf/priv` 下にバックドア アカウントを作成し、ユーザー名とパスワードを使用して `local.superusers` という名前のファイルを作成する必要があります。

CLI コマンド

外部認証サーバーを作成するには、`auth-server name create <address|ip6address> [attribute=value ...]` を使用します（構文と属性の説明については、`/docs` ディレクトリにある `CLIGuide.html` ファイルの `auth-server` コマンドを参照してください）。

RADIUS 外部認証サーバーの削除

RADIUS 外部認証サーバーを削除するには、[Radius] ペインでサーバーを選択し、[Radiusの削除 (Delete Radius)] アイコンをクリックして、削除を確定します。[閉じる (Close)] ボタンをクリックして、削除をキャンセルすることもできます。

AD 外部認証サーバーの設定

Cisco Prime Network Registrar 管理者が管理機能を実行するには、1 つ以上の管理者グループに割り当てられている必要があります。外部認証に AD サーバーを使用する場合、これらはユーザーごとにベンダー固有の属性として設定されます。Cisco ベンダー id (9) を使用し、Cisco Prime Network Registrar グループ属性を各管理者について、`cnr:groups=group1, group2, group3` という形式で作成します。

たとえば、管理者を組み込みグループ `dhcp-admin-group` および `dns-admin-group` に割り当てるには、次のように入力します。

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

スーパーユーザーのアクセス権限を割り当てるには、予約済みのグループ名 `superusers` が使用されます。管理者にスーパーユーザー権限を与えるには、次のように入力します。

```
cnr:groups=superusers
```

スーパーユーザー権限は、他のすべてのグループよりも優先されます。

Cisco Prime Network Registrar にアクセスするにはグループを作成し、ユーザーをそのグループに追加する必要があります。ユーザー属性を選択して、`cnr:group1,group2,..` という形式でグループ情報を指定します。

Active Directory (AD) 外部認証サーバーを設定するには、次のようにします。

- ステップ 1 AD サーバーで、グループ スコープドメイン ローカルを使用して、*CPIPE*などの新しいグループを作成します。
- ステップ 2 ユーザーを選択し、[追加 (Add)] をクリックして、グループに追加します。
- ステップ 3 [オブジェクト名の入力 (Enter the Object Names)] ウィンドウで、[CPNR] を選択し、[OK] をクリックします。

ステップ 4 [AD サーバー オブジェクト (AD Server Object)] ウィンドウで、*ad-group-name* 属性として **CPNR** を選択し、*ad-user-attr-map* 属性として **info** を選択します。

- (注) Cisco Prime Network Registrar を使用して、外部ユーザー名とそのパスワードまたはグループを追加、削除、または変更することはできません。この設定を実行するには、AD サーバーを使用する必要があります。

ケルベロスのレルムと KDC の設定

Cisco Prime Network Registrar が AD サーバーと通信するには、ケルベロスのレルムおよび KDC サーバーが必要です。Windows および Linux プラットフォームでケルベロスのレルムおよび KDC サーバーを設定するには、次の例に従います。

Cisco Prime Network Registrar が Windows プラットフォームで実行されている場合は (ksetup)、次のコマンドを実行して、レルムの KDC エントリを定義します。

```
ksetup /AddKdc <RealmName> [KdcName]
```

たとえば、`ksetup/AddKdc ECNR.COM tm-chn-ecnr-ad.ecnr.com`

確認するには、次のコマンドを実行します。

```
ksetup /dumpstate
```

結果は、次のメッセージのようになります。

```
default realm = partnet.cisco.com (NT Domain)
ECNR.COM:
  kdc = tm-chn-ecnr-ad.ecnr.com
  Realm Flags = 0x0No Realm Flags
No user mappings defined.
```

Prime Network Registrar が Linux プラットフォームで実行している場合は、次に示すように、変更を **krb5.conf** (*/etc/krb5.conf*) ファイルで設定する必要があります。

```
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
  ticket_lifetime = 1d
  default_realm = ECNR.COM
  default_tkt_enctypes = rc4-hmac
  default_tgs_enctypes = rc4-hmac
  dns_lookup_realm = false
  dns_lookup_kdc = false
  forwardable = true
[realms]
  ECNR.COM = {
    kdc = <kdc server host name>
    admin_server = <kdc server host name>
  }
[domain_realm]
  .ecnr.com = ECNR.COM
  ecnr.com = ECNR.COM
```

AD 外部コンフィギュレーション サーバーの追加

外部コンフィギュレーション サーバーを追加するには、次の手順を実行します。

ローカルの詳細 Web UI とリージョンの詳細 Web UI

- ステップ 1** [管理 (Administration)]メニューから、[外部認証 (External Authentication)]サブメニューの[Active Directory]を選択します。[Active Directory サーバーの一覧表示/追加 (List/Add Active Directory Server)]ページが表示されます。
- ステップ 2** [Active Directory] ペインで [Active Directory サーバーの追加 (Add Active Directory Server)]アイコンをクリックし、外部認証サーバーとして設定するサーバーの名前、ホスト名、およびドメインを入力します。[Active Directory サーバーの追加 (Add Active Directory Server)]ダイアログボックスで、このサーバーとの通信に使用されるベースドメイン、LDAP ユーザー属性マップ、および AD グループ名を設定できます。[Active Directory サーバーの追加 (Add Active Directory Server)]をクリックします。
- ステップ 3** [サーバーの管理 (Manage Servers)]ページで、*auth-type* 属性を Active Directory に変更し、[保存 (Save)]をクリックしてから、Cisco Prime Network Registrar を再起動します。

CLI コマンド

外部認証サーバーを作成するには、**auth-server name create** <address | ip6address> [attribute=value ...] を使用します。

AD 外部認証サーバーの削除

AD 外部認証サーバーを削除するには、[Active Directory] ペインでサーバーを選択し、[Active Directory サーバーの削除 (Delete Active Directory Server)]アイコンをクリックして、削除を確定します。[閉じる (Close)]ボタンをクリックして、削除をキャンセルすることもできます。

テナントの管理

Cisco Prime Network Registrar のマルチテナントアーキテクチャは、テナントがリージョンとローカルの両方のクラスタに保存されているデータをセグメント化できる機能を提供します。テナントが定義されると、データは各クラスタの組み込みデータベースでテナント別に分割されます。これは、各テナントにデータセキュリティとプライバシーを提供すると同時に、クラウドまたはマネージドサービスプロバイダが一連のインフラストラクチャサーバーに多くの小規模顧客の設定を統合したり、大規模顧客の設定をいくつかの専用サーバーに分散したりできる柔軟性を提供します。

特定のローカルクラスタを1つ以上のテナントに関連付けることができますが、ローカルクラスタ内では、特定のテナントに割り当てられたアドレスプールとドメイン名が重複しないようにする必要があります。

大規模顧客については、クラスタをテナントに明示的に割り当てることができます。この場合、ローカルクラスタ上のすべてのデータがテナントに関連付けられ、カスタマイズされたサーバー設定を含めることができます。または、インフラストラクチャサーバーから多くのテナントにサービスを提供することもできます。このモデルでは、テナントは独自のアドレス空間とドメイン名を維持できますが、サービスプロバイダによって管理される共通のサーバー設定を共有します。パブリックまたはプライベートネットワークアドレスの使用は、テナント

に重複しないアドレスが割り当てられるようにするために、サービスプロバイダによって管理される必要があります。

テナントを設定する際に知る必要があるキーポイントは、次のとおりです。

- テナント管理者は、テナントのタグと識別子を定義するテナントオブジェクトによってデータにリンクされます。
- テナントオブジェクトは、すべてのクラスタ間で一貫性があり、一意である必要があります。
- タグまたは識別子を別のテナントに再利用しないでください。
- 1つのクラスタに複数のテナントを設定できます。
- テナント管理者は、テナントオブジェクトを作成、変更、または削除することはできません。
- テナント管理者は、別のテナントのデータを表示または変更できません。
- テナントに割り当てられていないオブジェクトは、コアデータとして定義され、全てのテナントに対して読み取り専用モードで表示されます。

テナントの追加

テナントを追加するには、次の操作を行います。

ローカルおよびリージョン Web UI

ステップ 1 [管理 (**Administration**)] メニューから、[ユーザーアクセス (**User Access**)] サブメニューの [テナント (**Tenants**)] を選択します。[テナントの一覧表示/追加 (**List/Add Tenants**)] ページが開きます。

ステップ 2 [テナント (**Tenants**)] ペインの [テナントの追加 (**Add Tenants**)] アイコンをクリックして、テナントタグとテナント ID を入力し、[テナントの追加 (**Add Tenant**)] をクリックします。名前と説明の属性は任意です。

(注) 同じテナント ID またはテナント タグを持つ複数のテナントを作成することはできません。

ステップ 3 [保存 (**Save**)] をクリックします。

ページの上にあるツールバーの [設定 (**Settings**)] ドロップダウンリストには、[テナント (**Tenant**)] サブメニューの下にテナントが表示されます。

テナント固有の設定を行う必要があるときには、このドロップダウンリストを使用してテナントを選択できます。

CLI コマンド

テナントを追加するには、**tenant tag create tenant-id [attribute=value]** を使用します (構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **tenant** コマンドを参照してください)。

テナントの編集

テナントを追加するには、次の操作を行います。

ローカルおよびリージョン Web UI

ステップ 1 [テナントの一覧表示/追加 (List/Add Tenants)] ページで、[テナント (Tenants)] ペインの目的のテナントの名前をクリックすると、選択したテナントの詳細を含む [テナントの編集 (Edit Tenant)] ページが表示されます。

ステップ 2 [テナントの編集 (Edit Tenant)] ページでテナントのテナント タグ、名前、または説明を変更し、[保存 (Save)] をクリックします。テナント ID を変更することはできません。

テナントの削除



警告 テナントを削除すると、テナントのすべてのデータも削除されます。

テナントを削除するには、[テナント (Tenants)] ペインで目的のテナントの名前を選択し、[テナント (Tenants)] ペインで [削除 (Delete)] アイコンをクリックして、削除を確定します。[閉じる (Close)] ボタンをクリックして、削除をキャンセルすることもできます。



(注) 特定のテナントに制限されたユーザーは、テナントを削除できません。

テナント データの管理

テナントに対して、次の 2 種類のデータを作成できます。

- テナントデータ。指定されたテナントに割り当てられ、他のテナントは表示できません。
- コア データは。すべてのテナントに対して読み取り専用モードで表示されます。

ローカルおよびリージョン Web UI

Web UI でテナント データ オブジェクトを作成するには、次の手順を実行します。

ステップ 1 目的のテナントのデータを設定するには、ページの上部にあるツールバーの [設定 (Settings)] ドロップダウンリストをクリックして、[テナント (Tenant)] サブメニューで目的のテナントを選択します。

ステップ 2 オブジェクトを作成します。

テナント データを作成するときには、ほとんどのオブジェクト名は、指定されたテナントに対して一意である必要があります。たとえば、テナント *abc* および *xyz* は両方とも、それぞれの設定に対してプライベートな独自のスコープ *test* を使用します。

(注) 管理者 (Admin)、ゾーン (CCMZone、CCMReverseZone、および CCMSecondaryZone)、キー (Key)、およびクライアント (ClientEntry) は、すべてのテナントで一意である必要があります。

初期ログイン認証を実行し、ユーザーがテナントであるかどうかを確立するには、管理者名が一意である必要があります。ゾーンとキー クラスは、インターネット全体で一意であると予想される DNS ドメイン名を必要とするため、一意である必要があります。クライアント名は、着信した要求を照合するために DHCP サーバーが使用できる一意のクライアント識別子に対応している必要があります。

ローカルおよびリージョン Web UI

Web UI でコア データ オブジェクトを作成するには、次の手順を実行します。

ステップ 1 ページの上部にあるツールバーの [設定 (Settings)] ドロップダウン リストから **[all]** を選択し、[テナント (Tenant)] サブメニューから目的のテナントを選択します。

ステップ 2 オブジェクトを作成し、オブジェクトのテナント割り当てを [なし (none)] に設定したままにします。デフォルトでは、[なし (none)] が [テナント (Tenant)] ドロップダウン リストで選択されます。そのままにしておくと、オブジェクトは特定のテナントに制限されません。

コア データを使用して、テナントに提供するために選択したポリシーやクライアント クラスなどの共通の設定要素を提供できます。テナントは、設定内のこれらのオブジェクトを表示および参照できますが、変更または削除することはできません。コア データはすべてのテナントに対して表示されるため、オブジェクト名はすべてのテナントで一意である必要があります。

CLI コマンド

session set tenant=タグを使用して、選択したテナントを設定します。設定されている場合、テナント選択をクリアするには、**session unset tenant** を使用します (構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **session** コマンドを参照してください)。



(注) 作成後にオブジェクトのテナントまたはコアの指定を変更することはできません。テナントの割り当てを変更するには、オブジェクトを削除してから再作成する必要があります。



ヒント **cnr_exim** ツールを使用して、テナント データのセットを 1 つのテナントから別のテナントに移動することができます。

単一テナントへのローカル クラスタの割り当て

単一のテナントに割り当てられている場合、ローカル クラスタのコア データは読み取り専用アクセスに制限されません。これは、サーバーを停止して起動し、デフォルトを変更し、カスタム拡張機能をインストールする機能がテナントに与えられる可能性があることを意味します。クラスタが特定のテナントに割り当てられると、他のテナントはクラスタにログインできなくなります。



(注) ローカルクラスタとの同期に失敗した場合、クラスタはテナントに割り当てられません。接続の問題を解決し、再同期アイコンを使用してローカル クラスタ テナントを設定します。

リージョン Web UI

1つのテナントにローカル クラスタを割り当てるには、次の手順を実行します。

- ステップ 1** クラスタを新しいテナントに割り当てる場合は、[テナントの一覧表示/追加 (List/Add Tenant)] ページでテナントを追加します ([テナントの追加 \(55 ページ\)](#) を参照)。
- ステップ 2** [操作 (Operate)] メニューから、[サーバー (Servers)] サブメニューの [クラスタの管理 (Manage Clusters)] を選択します。[クラスタの一覧表示/追加 (List/Add Clusters)] ページが表示されます。
- ステップ 3** ページの上部にあるツールバーの [設定 (Settings)] ドロップダウンリストから、**ステップ 1** で追加したテナントを選択し、[テナント (Tenant)] サブメニューで目的のテナントを選択します。
- ステップ 4** [クラスタの管理 (Manage Clusters)] ペインの [クラスタの管理を追加 (Add Manage Clusters)] アイコンをクリックします。[クラスタの追加 (Add Cluster)] ダイアログボックスが表示されます。
- ステップ 5** [クラスタの追加 (Add Cluster)] をクリックしてクラスタを追加します。クラスタの追加の詳細については、[ローカル クラスタの作成 \(162 ページ\)](#) を参照してください。

(注) クラスタが特定のテナントに割り当てられると、変更または設定解除できません。

テナント データのプッシュとプル

リージョン Web UI では、リストページには、オブジェクトをローカル クラスタのリストに配布できるプッシュ オプションと、ローカル クラスタ オブジェクトをレプリカ データから中央の設定にマージできるプル オプションが含まれています。これらの操作はテナントとコアデータの両方で実行できますが、1回の操作でプッシュまたはプルできるデータセットは1つだけです。

ページの上にあるツールバーの [設定 (Settings)] ドロップダウンリストを使用して、[テナント (Tenant)] サブメニューで目的のテナントを選択し、プッシュまたはプルするデータのセットを指定します。



- (注) テナントデータの一貫性のあるビューを維持するには、関連するすべてのクラスタに同じテナントのリストを設定する必要があります。テナントリストの管理に役立つ手順については、[テナントのプッシュとプル \(83 ページ\)](#) を参照してください。

CLI コマンド

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。

- `tenant <tag | all> push <ensure | replace | exact> cluster-list [-report-only | -report]`
- `tenant <tag | all> push <ensure | replace | exact> cluster-list [-report-only | -report]`
- `tenant tag reclaim cluster-list [-report-only | -report]`

外部認証を使用する場合のテナントの割り当て

外部RADIUS認証が設定されている場合、RADIUSサーバー設定に割り当てられているグループは、ユーザーのアクセス権限を確立します。テナントステータスを指定するには、テナントユーザーのグループのリストに、暗黙的なグループ名 `ccm-tenant-tag` または `ccm-tenant-id` を追加する必要があります。その他の割り当てられたグループは、同じテナントに割り当てられたコアグループまたはグループである必要があります。無効なグループは、ログイン時にユーザーのログイン情報を作成するときに無視されます。

たとえば、テナント `abc` のスーパーユーザーアクセスを割り当てるには、グループ属性を次のように指定します。

```
cnr:groups=superusers,ccm-tenant-abc
```

[外部認証サーバー \(50 ページ\)](#) を参照してください。

テナント データでの `cnr_exim` の使用

`cnr_exim` ツールを使用すると、テナントデータをエクスポートしたり、必要に応じてインポート時に別のテナントにデータを再割り当てしたりできます ([cnr_exim データ インポートおよびエクスポート ツールの使用 \(236 ページ\)](#) を参照)。次の機能を使用できます。

- 各テナントの標準オブジェクトセットの作成
- テナント データの新しいテナントへの移動



- (注) 特定のテナントに制限されたユーザーは、そのテナントのデータのみをエクスポートまたはインポートできます。

テナントオブジェクトの標準セットの作成

テナントオブジェクトの標準セットを使用して、スコープ、ゾーンテンプレート、ポリシー、クライアントクラスなどの共通オブジェクトを提供できます。これらの設定をカスタマイズするオプションをテナントに提供するには、コア データ オブジェクトの代わりにこれらを使用できます。

テナント オブジェクトの標準セットを作成するには、次の手順を実行します。

ステップ 1 プレースホルダとして使用するテンプレートテナントユーザーを作成し（`tag=template` および `id=9999`）、各テナントで再利用するオブジェクトのセットを作成します。

ステップ 2 `cnr_exim` ツールを使用して、テンプレート設定をエクスポートします。

```
cnr_exim -f template -x -e template.bin
```

ステップ 3 `cnr_exim` ツールを使用して、テナント `abc` のテンプレート設定をインポートします。

```
cnr_exim -f template -g abc -i template.bin
```

(注) テンプレートテナントユーザーがクラスタに存在しなくても、データをインポートできるため、他のクラスタで `template.bin` エクスポート ファイルを再利用できます。エクスポート ファイルを作成したら、必要に応じて、元のクラスタのプレースホルダテナントを削除して、関連付けられているすべてのテンプレート データを削除することもできます。

テナントデータの移動

テナントの ID は、テナントを削除してから再作成することによってのみ変更できます。これが必要な場合にテナントのデータを保持するには、次の手順を実行します（テナントのテナントタグが `xyz` であることを前提とします）。

ステップ 1 `cnr_exim` ツールを使用して、テナント `xyz` の設定をエクスポートします。

```
cnr_exim -f xyz -x -e xyz.bin
```

ステップ 2 テナント `xyz` を削除します。

ステップ 3 修正されたテナント `id` を使用してテナントを再作成します。

ステップ 4 `cnr_exim` ツールを使用して、設定を再インポートします。

```
cnr_exim -f xyz -g xyz -i xyz.bin
```

管理者の管理

初めてログインすると、Cisco Prime Network Registrarには1人の管理者（スーパーユーザーアカウント）が割り当てられます。このスーパーユーザーは、Web UI のすべての機能を実行でき、通常は他の主要な管理者を追加します。ただし、`ccm-admin` および `regional-admin` 管理者

は、管理者の追加、編集、および削除を行うこともできます。管理者を作成するには、以下が必要です。

- 名前を追加します。
- パスワードを追加します。
- 管理者がスーパーユーザー権限を持っている必要があるかどうかを指定します（通常は非常に限定的な方法で割り当てられます）。
- スーパーユーザーを作成しない場合は、管理者が属するグループを指定します。これらのグループには適切なロール（および場合によってはサブロール）の割り当てが必要であり、それによって適切な制約が設定されます。

Cisco Prime Network Registrar にログインできるすべてのロール（スーパーユーザー、`ccm-admin`、または `regional-admin` 権限を持つユーザー）を誤って削除した場合は、`install-path/conf/priv/local.superusers` ファイルで管理者名とパスワードのペアを作成することによって回復できます。このファイルを作成し、`admin password` という形式の行を含める必要があります。次のログインセッションには、この管理者名とパスワードを使用します。`local.superusers` ファイル内のすべてのユーザーに「`local$`」というプレフィックスを付ける必要があります。これにより、すべてのユーザーの先頭に `local$` が付くので、`local.superusers` ファイルがいつ使用されたのかを特定するために役立ちます。`local$` で始まるユーザーは、`local.superusers` ファイルのエントリに対して検証されます。これらのユーザーは、ローカル CCM ユーザーデータベースのユーザーに対してチェックされることも、外部認証を使用することはありません。



- (注)
- 管理者名は大文字と小文字が区別されないため、`local$` プレフィックスも大文字と小文字が区別されません。
 - `nrcmd -N admin` で `local$` ユーザーを使用する場合は、`$` をエスケープする必要があります（そのため、`local\$` を使用）。代わりに、`nrcmd` でユーザーのプロンプトを表示させることができます（この場合、エスケープは不要）。



重要 `local.superusers` ファイルを使用すると、セキュリティが低下します。したがって、このファイルは、一時的にすべてのログインアクセスを失う場合など、緊急時にのみ使用してください。ログイン後、通常の方法でスーパーユーザーアカウントを作成してから、`local.superusers` ファイルまたはその内容を削除します。管理上の変更を追跡するには、個人ごとに新しい管理者アカウントを作成する必要があります。

このファイルをそのままにしておく場合は、一般的な読み取りアクセスから保護されていることを確認してください（読み取りアクセスは `ccmsrv` でのみ必要）。

管理者の追加

管理者を追加するには、次の手順を実行します。

ローカルおよびリージョン Web UI

- ステップ 1** [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [テナント (Administrators)] を選択します。[管理者の一覧表示/追加 (List/Add Administrators)] ページが開きます (例については、[管理者の作成 \(152 ページ\)](#) を参照してください)。
- ステップ 2** [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックして、[管理者を追加 (Add admin)] ダイアログボックスで、[名前 (Name)] フィールドに名前を入力し、[パスワード (Password)] フィールドにパスワードを入力し、[パスワードの確認 (Confirm Password)] フィールドにパスワードを再入力して、[管理者を追加 (Add admin)] をクリックします。
- ステップ 3** [使用可能なグループ (Groups Available)] リストから 1 つ以上の既存のグループを選択し (または管理者がスーパーユーザーである必要があるかどうか)、[保存 (Save)] をクリックします。

管理者の編集

管理者を編集するには、[管理者 (Administrators)] ペインで管理者を選択し、[管理者の編集 (Edit Administrator)] ページで名前、パスワード、スーパーユーザーのステータス、またはグループメンバーシップを変更し、[保存 (Save)] をクリックします。アクティブなグループは、[選択済み (Selected)] リストに表示されます。

セッション制限が設定されている場合、[セッション数無制限 (Unlimited Sessions?)] チェックボックスをオンにすることで、無制限の数の同時トークンおよびユーザーセッションが管理者に許可されることを示すことができます。詳細については、[セッション管理 \(84 ページ\)](#) を参照してください。

管理者の削除

管理者を削除するには、[管理者 (Administrators)] ペインで管理者を選択し、[管理者の削除 (Delete Administrators)] アイコンをクリックして、削除を確定またはキャンセルします。

管理者の一時停止/再開

管理者のログインアクセスを一時停止するには、[管理者 (Administrators)] ペインでその管理者を選択し、右側のペインで [管理者の編集 (Edit Administrator)] ページの上部にある [一時停止 (Suspend)] ボタンをクリックします。



- (注) 管理者のログインが有効になっている場合は、[一時停止 (Suspend)] アクションのみが使用可能になります。一時停止されている場合は、[再開 (Reinstate)] アクションのみが使用可能になります。

CLI コマンド

管理者を作成するには、**admin name create [attribute=value]** を使用します。

管理者を削除するには、**admin name delete** を使用します。

管理者を一時停止するには、**admin name suspend** を使用します。

管理者を再開するには、**admin name reinstate** を使用します。

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再使用の場合は、クラスターのリストまたは「すべて」を指定できます。push の場合、**-omitrelated** が指定されていない限り、関連付けられたロールとグループも（置換モードを使用して）プッシュされます。

- **admin < name | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]**
- **admin < name | all > push < ensure | replace | exact > cluster-list [-omitrelated] [-report-only | -report]**
- **admin name reclaim cluster-list [-report-only | -report]**

パスワードの管理

パスワードは、Web UI および CLI への管理者アクセスのためのキーです。Web UI では、[ログイン (Login)] ページでパスワードを入力します。CLI では、最初に **nrcmd** プログラムを呼び出すときにパスワードを入力します。ローカルまたはリージョン CCM 管理者またはスーパーユーザーは、管理者パスワードを変更できます。

入力時にパスワードを公開しないようにすることができます。Web UI では、ログインするか、パスワードを追加しても、ページにはアスタリスクしか表示されません。CLI では、管理者を作成し、パスワードを省略し、**admin** 名前 **enterPassword** を使用してパスワードを公開しないようにすることができます。この場合、プロンプトにはパスワードはアスタリスクとして表示されます。この操作は、パスワードをプレーンテキストとして公開する通常の **admin name set password** コマンドの代わりに行うことができます。

管理者は、クラスターで自分のパスワードを変更できます。パスワードの変更をリージョンサーバーからすべてのローカルクラスターに反映させる場合は、リージョンクラスターにログインします。最初に、セッションの **admin-edit-mode** が **synchronous** に設定されていることを確認してから、パスワードを更新します。



(注) パスワードの長さは 255 文字以下でなければなりません。

グループの管理

スーパーユーザー、**ccm-admin**、または **regional-admin** は、管理者グループを作成、編集、および削除できます。管理者グループの作成には、次の作業が含まれます。

- 名前を追加します。
- オプションの説明を追加します。
- 関連ロールを選択します。

グループの追加

グループを追加するには、次の手順を実行します。

ローカル詳細およびリージョン Web UI

- ステップ 1** [管理 (Administration)] メニューから、[ユーザー アクセス (User Access)] サブメニューの [グループ (Groups)] を選択します。[管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページが開きます (例については、[ホスト管理者に割り当てるグループの作成 \(158ページ\)](#) を参照してください)。
- ステップ 2** [グループ (Groups)] ペインの [グループの追加 (Add Groups)] アイコンをクリックして、[CCM 管理者グループの追加 (Add CCMAdminGroup)] ダイアログボックスに名前とオプションの説明を入力し、[CCM 管理者グループの追加 (Add CCMAdminGroup)] をクリックします。
- ステップ 3** [使用可能なロール (Roles Available)] リストから 1 つ以上の既存のロールを選択し、[保存 (Save)] をクリックします。

グループの編集

グループを編集するには、[グループ (Groups)] ペインで編集するグループの名前をクリックして、[管理者グループの編集 (Edit Administrator Group)] ページを開きます。このページでは、名前、説明、またはロール メンバーシップを変更できます。[選択済み (Selected)] リストでアクティブなロールを表示できます。

グループの削除

グループを削除するには、[グループ (Groups)] ペインでグループを選択し、[グループの削除 (Delete Groups)] アイコンをクリックして、削除を確定します。[閉じる (Close)] ボタンをクリックして、削除をキャンセルすることもできます。

CLI コマンド

グループを作成するには、**group name create** [attribute=value] を使用します。

グループを削除するには、**group name delete** を使用します。

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。push 操作では、これを防止するために **-omitrelated** が指定されていない限り、関連するロール (置換モードを使用) および関連する所有者とリージョン (保証モードを使用) もプッシュされます。

- **group** < name | all > pull < ensure | replace > cluster-name [-report-only | -report]
- **group** < name | all > push < ensure | replace | exact > cluster-list [-omitrelated] [-report-only | -report]
- **group name reclaim** cluster-list [-report-only | -report]

ロールの管理

スーパーユーザー、`ccm-admin`、または `regional-admin` 管理者は、管理者ロールを作成、編集、および削除できます。管理者ロールの作成には、次の作業が含まれます。

- 名前を追加します。
- 基本ロールを選択します。
- ロールを制約なしにするか、または読み取り専用にするかを指定する場合があります。
- 場合によっては制約を追加します。
- グループを割り当てる可能性があります。

ロールの追加

ロールを追加するには、次の手順を実行します。

ローカル詳細およびリージョン詳細 Web UI

- ステップ 1** [管理 (Administration)]メニューから、[ユーザーアクセス (User Access)]サブメニューの[**ロール (Roles)**]を選択します。[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)]ページが開きます。
- ステップ 2** [ロール (Roles)]ペインの[**ロールの追加 (Add Role)**]アイコンをクリックして、名前を入力し、テナントと基本ロールを選択して、[**ロールの追加 (Add Roles)**]ダイアログボックスに名前と基本ロールを入力し、[**ロールの追加 (Add Role)**]をクリックします。
- ステップ 3** [管理者ロールの一覧表示/追加 (List/Add Administrator Roles)]ページで、ロールの制約、サブロールの制限、またはグループ選択を指定し、[**保存 (Save)**]をクリックします。

ロールの編集

ロールを編集するには、[**ロール (Roles)**]ペインでロールを選択し、[**管理者ロールの編集 (Edit Administrator Role)**]ページで、名前または制約、サブロールの制限、またはグループ選択を変更します。アクティブなサブロールまたはグループは、[**選択済み (Selected)**]リストに表示されます。[**保存 (Save)**]をクリックします。

ロールの削除

ロールを削除するには、[**ロール (Roles)**]ペインでロールを選択し、[**ロールの削除 (Delete Role)**]アイコンをクリックして、削除を確定します。



(注) デフォルト ロールは削除できません。

CLI コマンド

管理者ロールを追加および編集するには、**role name create base-role [attribute=value]** を使用します（構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **role** コマンドを参照してください）。基本ロールには、デフォルトグループが関連付けられています。他のグループを追加するには、**groups** 属性（カンマ区切りの文字列値）を設定します。

リージョンクラスタに接続されているときには、次の **pull**、**push**、および **reclaim** コマンドを使用できます。**push** および **reclaim** コマンドでは、クラスタのリストまたは「all」を指定できます。**push** 操作では、関連グループ（置換モードを使用）および関連する所有者とリージョン（保証モードを使用）もプッシュされます。**pull** 操作では、関連する所有者とリージョンが（保証モードを使用して）プルされます。どちらの操作についても、これを防止するために **-omitrelated** を指定して、ロールのみをプッシュまたはプルします。

- **role < name | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]**
- **role < name | all > push < ensure | replace | exact > cluster-list [-omitrelated] [-report-only | -report]**
- **role name reclaim cluster-list [-report-only | -report]**

きめ細かい管理

きめ細かい管理により、権限のないユーザーがゾーン、アドレスブロック、サブネット、およびルータインターフェイスを誤って変更するのを防止できます。また、許可されたユーザーのみが、特定のスコープ、プレフィックス、およびリンクを表示または変更することも保証します。きめ細かい管理では、管理者は特定のスコープ、プレフィックス、およびリンクのセットに制限されます。制限付き管理者は、許可されたスコープ、プレフィックス、およびリンクオブジェクトのみを表示または変更できます。CCM サーバーは、所有者およびリージョン制約を使用して、IPv4 アドレス空間オブジェクト、および DNS ゾーン関連オブジェクト（CCMZone、CCMReverseZone、CCMSecondaryZone、CCMRSet、および CCMHost）を承認およびフィルタリングします。ゾーンは、所有者とリージョンによって制約されます。CCMSubnetの所有者またはリージョン属性は、スコープへのアクセスを制御します。また、プレフィックスおよびリンクオブジェクトの所有者またはリージョン属性は、プレフィックスとリンクへのアクセスを制御します。

ローカル詳細およびリージョン Web UI

- ステップ 1 [管理 (Administration)] メニューから [ロール (Roles)] を選択して、[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページを開きます。
- ステップ 2 [ロール (Roles)] ペインの [ロールの追加 (Add role)] アイコンをクリックして、カスタム ロールの名前、たとえば、my-dhcp を入力し、テナント を選択し、[ロール (Role)] ドロップダウン リストから [dhcp-admin] を選択して、[ロールの追加 (Add role)] をクリックします。
- ステップ 3 [DHCP 管理者ロールの追加 (Add DHCP Administrator Role)] ページで、必要に応じて [True] または [False] オプション ボタンをクリックします。

ステップ 4 [使用可能 (Available)] フィールドで必要なサブロールを選択して、[選択済み (Selected)] フィールドに移動します。

ステップ 5 [制約の追加 (Add Constraint)] をクリックします。

- a) [ロール制約の追加 (Add Role Constraint)] ページで、必要に応じてフィールドを変更します。
- b) [制約の追加 (Add Constraint)] をクリックします。制約のインデックス番号は1である必要があります。

ステップ 6 [保存 (Save)] をクリックします。

カスタムロールの名前が、[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページのロールのリストに表示されます。

関連項目

[スコープレベルの制約 \(67 ページ\)](#)

[プレフィックスレベルの制約 \(69 ページ\)](#)

[リンクレベルの制約 \(70 ページ\)](#)

スコープレベルの制約

dhcp-admin ユーザーは、次の条件のいずれかが満たされた場合にスコープを表示または変更できます。

- スコープのサブネットの所有者が、dhcp-admin 所有者に一致します。
- スコープのサブネットのリージョンが、リージョン ロールの制約と一致します。
- 親アドレス ブロックの所有者またはリージョンが、dhcp-admin 所有者またはリージョン ロールの制約と一致します。所有者またはリージョンが定義されている最も直接的な親アドレス ブロックが優先されることに注意してください。

次の条件も有効です。

- 一致する所有者またはリージョンの制約が読み取り専用としてマークされている場合は、スコープの表示だけができます。
- スコープにプライマリ ネットワークが定義されている場合、プライマリ サブネットとその親アドレスブロックの所有者またはリージョンの制約は、セカンダリ サブネットをオーバーライドします。
- 親サブネットまたはアドレスブロックに所有者またはリージョンの制約が定義されていない場合は、スコープにアクセスできます。
- 制約なしの dhcp-admin ユーザーの場合は、すべてのスコープにアクセスできます。



- (注) これらの階層的な承認チェックは、スコープ、サブネット、および親アドレスブロックに適用されます。addrblock-admin 所有者/リージョン制約に関する同一の階層型承認チェックが、アドレスブロックとサブネットに適用されます。dhcp-admin および addrblock-admin 権限がある場合は、いずれかのロールでアクセスが許可されていれば、アドレスブロックとサブネットにアクセスできます。

スコープレベル制約の例：

```
Parent CCMAddrBlock 10.0.0.0/8 has owner 'blue' set.
  Scope 'A' has subnet 10.0.0.0/24 has parent CCMSubnet with owner 'red'.
  Scope 'B' has subnet 10.0.1.0/24 has parent CCMSubnet with no owner set.
  Scope 'C' has subnet 10.10.0.0/24 has parent CCMSubnet with owner 'green' and
primary-subnet 10.0.0.0/24.
  Scope 'D' has subnet 100.10.0.0/24 has parent CCMSubnet with owner unset, and no
parent block.

Scope 'A' owner is 'red'.
Scope 'B' owner is 'blue'.
Scope 'C' owner is 'red'.
Scope 'D' owner is unset. Only unconstrained users can access this scope.
```

ローカル詳細 Web UI

スコープを追加するには、次の手順を実行します。

- ステップ 1 [設計 (Design)] メニューから、[DHCPv4] サブメニューの [スコープ (Scopes)] を選択して、[DHCP スコープの一覧表示/追加 (List/Add DHCP Scopes)] ページを開きます。
- ステップ 2 [スコープ (Scopes)] ペインの [スコープの追加 (Add Scopes)] アイコンをクリックして、[DHCP スコープの追加 (Add DHCP Scope)] ダイアログボックスで名前、サブネット、プライマリ サブネットを入力し、ポリシーを選択し、selection-tag-list を入力し、スコープ テンプレートを選択します。
- ステップ 3 [DHCP スコープの追加 (Add DHCP Scope)] をクリックします。[DHCP スコープの一覧表示/追加 (List/Add DHCP Scopes)] ページが表示されます。
- ステップ 4 必要に応じて、フィールドまたは属性の値を入力します。
- ステップ 5 属性値を設定解除するには、[設定解除 (Unset?)] 列のチェックボックスをオンにしてから、ページの下部にある [フィールドの設定解除 (Unset Fields)] をクリックします。
- ステップ 6 [保存 (Save)] をクリックして、スコープを追加するか、[元に戻す (Revert)] をクリックして変更をキャンセルします。

ヒント 新しいスコープ値を追加するか、既存の値を編集する場合は、[保存 (Save)] をクリックしてスコープ オブジェクトを保存します。

プレフィックスレベルの制約

次のいずれかを持っている場合は、プレフィックスを表示または変更できます。

- dhcp-admin の ipv6-management サブロール、またはローカル クラスタの addrblock-admin ロール。
- central-cfg-admin、またはリージョン クラスタの regional-addr-admin ロール。

次の条件のいずれかが当てはまる場合は、プレフィックスを表示または変更できます。

- 親リンクの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約と一致します。
- このプレフィックスの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約と一致します。
- 親プレフィックスの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約に一致します。

次の条件のいずれかが当てはまる場合は、プレフィックスを表示または変更できます。

- ユーザーについて一致する所有者またはリージョンの制約が読み取り専用としてマークされている場合は、プレフィックスの表示のみができます。
- プレフィックスが親リンクを参照している場合、リンクの所有者またはリージョン制約は、リンクの所有者またはリージョンの制約が設定されている場合に適用されます。
- 親リンクまたはプレフィックスが所有者またはリージョンの制約を定義していない場合は、所有者またはリージョンのロール制約がユーザーに対して定義されていない場合のみ、このプレフィックスにアクセスできます。
- 制約なしのユーザーの場合は、すべてにアクセスできます。

プレフィックスレベルの制約の例 :

```
Link 'BLUE' has owner 'blue' set.
Parent Prefix 'GREEN' has owner 'green' set.
Prefix 'A' has owner 'red' set, no parent prefix, and no parent link.
Prefix 'B' has owner 'yellow' set, parent Prefix 'GREEN' and parent link 'BLUE'.
Prefix 'C' has no owner set, parent prefix 'GREEN', and no parent link.
Prefix 'C' has no owner set, no parent prefix, and no parent link.

Prefix 'A' owner is 'red'.
Prefix 'B' owner is 'blue'.
Prefix 'C' owner is 'green'.
Prefix 'D' owner is unset. Only unconstrained users can access this prefix.
```

ローカル詳細およびリージョン詳細 Web UI

ユニファイド v6 アドレス空間を表示するには、次の手順を実行します。

- ステップ 1** [設計 (Design)]メニューから、[DHCPv6]サブメニューの[アドレスツリー (Address Tree)]を選択して、[DHCPv6 アドレス ツリー (DHCP v6 Address Tree)]ページを開きます。

- ステップ2** プレフィックスを表示するには、名前、アドレス、および範囲を追加してから、DHCP タイプと可能なテンプレートを選択します（『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「IPv6 アドレス空間の表示」の項を参照してください）。
- ステップ3** 所有者ドロップダウンリストから所有者を選択します。
- ステップ4** リージョンドロップダウンリストからリージョンを選択します。
- ステップ5** [プレフィックスの追加 (Add Prefix)] をクリックします。新しく追加されたプレフィックスが [DHCP v6 アドレス ツリー (DHCP v6 Address Tree)] ページに表示されます。

ローカル詳細およびリージョン詳細 Web UI

DHCP プレフィックスを一覧表示または追加するには、次の手順を実行します。

- ステップ1** [設計 (Design)] メニューから、[DHCPv6] サブメニューの [プレフィックス (Prefixes)] を選択して、[DHCPv6 プレフィックスの一覧表示/追加 (List/Add DHCP v6 Prefixes)] ページを開きます。
- ステップ2** [プレフィックス (Prefixes)] ペインの [プレフィックスの追加 (Add Prefixes)] アイコンをクリックして、プレフィックスの名前、アドレス、および範囲を入力し、DHCP タイプと可能なテンプレートを選択します。
- ステップ3** 所有者ドロップダウンリストから所有者を選択します。
- ステップ4** リージョンドロップダウンリストからリージョンを選択します。
- ステップ5** [IPv6 プレフィックスの追加 (Add IPv6 Prefix)] をクリックします。新しく追加されたプレフィックスが [DHCP v6 プレフィックスの一覧表示/追加 (List/Add DHCP v6 Prefixes)] ページに表示され、左側の [プレフィックス (Prefixes)] ペインにも表示されます。

リンクレベルの制約

次の場合、リンクを表示または変更できます。

- ユーザーは、ローカルクラスタの `dhcp-admin` または `addrblock-admin` ロールの `ipv6-management` サブロールとして、またはリージョンクラスタの `central-cfg-admin` または `regional-addr-admin` ロールとして承認されています。
- リンクの所有者またはリージョンは、ユーザーに定義されている所有者またはリージョンロールの制約に一致します。
- リンクに所有者またはリージョンが定義されていず、ユーザーに対して所有者またはリージョンロールの制約が定義されていない場合に限りです。

制約なしのユーザーの場合は、すべてのリンクにアクセスできます。

次に、リンクレベルの制約の例を示します。

```
Link 'BLUE' has owner 'blue' set.
Link 'ORANGE' has owner unset.

Link 'BLUE' owner is 'blue'.
Link 'ORANGE' owner is unset. Only unconstrained users can access this link.
```


ローカルおよびリージョン Web UI

リンクを追加するには、次の手順を実行します。

-
- ステップ 1** [設計 (Design)]メニューから、[DHCPv6]サブメニューの[リンク (Links)]を選択して、[DHCPv6 リンクの一覧表示/追加 (List/Add DHCP v6 Links)]ページを開きます。
- ステップ 2** [リンク (Links)]ペインの[リンクの追加 (Add Links)]アイコンをクリックし、名前を入力してから、リンクタイプを選択し、グループを入力します。
- ステップ 3** [リンクの追加 (Add Link)]をクリックします。新しく追加された DHCPv6 リンクが、[DHCPv6 リンクの一覧表示/追加 (List/Add DHCP v6 Links)]ページに表示されます。
-

管理者の一元管理

リージョンまたはローカル CCM 管理者として、次のことができます。

- ローカルおよびリージョンクラスタ管理者、グループ、およびロールを作成および変更します。
- 管理者、グループ、およびロールをローカルクラスタにプッシュします。
- ローカルクラスタの管理者、グループ、およびロールを中央クラスタにプルします。

これらの各機能には、少なくとも 1 つのリージョン CCM 管理者サブロールが定義されている必要があります。次の表に、これらの操作に必要なサブロールを示します。

表 6: 集中管理者管理に必要なサブロール

集中管理者管理アクション	必要なリージョンサブロール
管理者の作成、変更、プッシュ、プル、または削除	認証
グループまたはロールの作成、変更、プッシュ、プル、または削除	承認
関連付けられた所有者またはリージョンによるグループまたはロールの作成、変更、プッシュ、プル、または削除	承認所有者リージョン
外部認証サーバーの作成、変更、プッシュ、プル、または削除	認証
テナントの作成、変更、プッシュ、プル、または削除	認証

関連項目

- [管理者のプッシュとプル \(72 ページ\)](#)
- [グループのプッシュとプル \(78 ページ\)](#)
- [ロールのプッシュとプル \(80 ページ\)](#)
- [テナントのプッシュとプル \(83 ページ\)](#)

管理者のプッシュとプル

リージョンクラスタ Web UI の [管理者の一覧表示/追加 (List/Add Administrators)] ページで、ローカルクラスタに管理者をプッシュしたり、管理者をプルしたりすることができます。

リージョンクラスタで、ローカルとリージョンの両方のロールを持つ管理者を作成できます。ただし、ローカルクラスタはリージョンのロールを認識しないため、関連付けられているローカルロールのみをプッシュまたはプルできます。

関連項目

- [ローカルクラスタへの管理者のプッシュ \(72 ページ\)](#)
- [ローカルクラスタへの管理者の自動プッシュ \(73 ページ\)](#)
- [レプリカデータベースからの管理者のプル \(74 ページ\)](#)

ローカルクラスタへの管理者のプッシュ

ローカルクラスタに管理者をプッシュするには、1つ以上のクラスタとプッシュモードを選択する必要があります。

リージョン基本および詳細 *Web UI*

-
- ステップ 1** [管理 (Administration)] メニューから [管理者 (Administrators)] を選択します。
- ステップ 2** [管理者の一覧表示/追加 (List/Add Administrators)] ページで、[管理者 (Administrators)] ペインの [すべてプッシュ (Push All)] アイコンをクリックして、ページにリストされているすべての管理者をプッシュします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ダイアログボックスが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオボタンのいずれかをクリックして、プッシュモードを選択します。すべての管理者をプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)] を選択できます。単一の管理者をプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できます。いずれの場合も、[保証 (Ensure)] がデフォルトのモードです。ローカルクラスタの既存の管理者データを置換する場合にのみ、[置換 (Replace)] を選択します。ローカルクラスタで管理者データベースの正確なコピーを作成し、それによって、リージョンクラスタで定義されていないすべての管理者を削除する場合にのみ、[完全 (Exact)] を選択します。
- ステップ 4** デスティネーションクラスタの [使用可能 (Available)] フィールドで1つ以上のローカルクラスタを選択し、それらを [選択済み (Selected)] フィールドに移動します。

ステップ 5 [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。

ステップ 6 [プッシュ データ レポートの表示 (View Push Data Report)] ダイアログボックスで、プッシュの詳細を確認して、[OK] をクリックして、[管理者の一覧表示/追加 (List/Add Administrators)] ページに戻ります。

CLI コマンド

リージョン クラスタに接続されているときには、**admin <name | all> push <ensure | replace | exact> cluster-list [-omitrelated] [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。push の場合、**-omitrelated** が指定されていない限り、関連付けられたロールとグループも（置換モードを使用して）プッシュされます。

ローカル クラスタへの管理者の自動プッシュ

新しいユーザー名とパスワードの変更は、リージョン クラスタからローカル クラスタに自動的にプッシュできます。これを行うには、リージョン クラスタで同期編集モードを有効にする必要があります。編集モードは、現在の Web UI セッションに対して設定されます。または、CCM サーバーの設定で設定されているすべてのユーザーのデフォルトとして設定されます。

同期モードが設定されている場合は、ユーザー名とパスワードに対する後続のすべての変更がローカル クラスタと同期されます。リージョン サーバーでパスワードを変更でき、この変更はローカル クラスタに自動的に反映されます。

管理者ユーザーの場合は、リージョン クラスタのユーザー ログイン情報に対して複数の変更を加えることができます。これらの変更はすべて、自動的にローカル クラスタにプッシュされます。

リージョン 基本および詳細 Web UI

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

ステップ 2 [サーバーの管理 (Manage Servers)] ペインの [ローカル CCM サーバー (Local CCM Server)] リンクをクリックして、[CCM サーバーの編集 (Edit CCM Server)] ページを開きます。

ステップ 3 同期ラジオ ボタンを使用して、admin、dhcp、および dns のリージョン編集モードの値を選択します。

ステップ 4 **webui-mode** ドロップダウンリストから webui モード値を選択します。

ステップ 5 idle-timeout 値を入力します。

ステップ 6 属性値を設定解除するには、[設定解除 (Unset?)] 列のチェックボックスをオンにしてから、ページの下部にある [フィールドの設定解除 (Unset Fields)] をクリックします。属性値を設定解除または変更するには、[保存 (Save)] をクリックするか、[キャンセル (Cancel)] をクリックして変更をキャンセルします。

(注) アスタリスクでマークされている属性の値を入力します。これらは、CCM サーバーの動作に必要なためです。任意の属性の名前をクリックすると、その属性の説明ウィンドウを開くことができます。

リージョンモードでの CLI への接続

CLI にはリージョンモードで接続する必要があります。リージョンモードには、**-R** フラグが必要です。同期編集モードを設定するには、次のようにします。

```
nrcmd-R> session set admin-edit-mode=synchronous
```

レプリカ データベースからの管理者のプル

ローカルクラスタからの管理者のプルは、主に、他のローカルクラスタにプッシュできる管理者の初期リストを作成する場合にのみ役立ちます。ローカル管理者は、リージョンクラスタ自体では有効ではありません。これらの管理者にはリージョンロールが割り当てられていないためです。

管理者をプルするとき、実際にはリージョンクラスタのレプリカ データベースからプルします。ローカルクラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカルクラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン基本および詳細 *Web UI*

- ステップ 1** [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [グループ (Administrators)] を選択します。
- ステップ 2** [管理者の一覧表示/追加 (List/Add Administrators)] ページで、[管理者 (Administrators)] ペインの [データのプル (Pull Data)] をクリックします。[プルするレプリカ管理者データの選択 (Select Replica Admin Data to Pull)] ダイアログボックスが開きます。
- ステップ 3** クラスタの [レプリカデータの更新 (Update Replica Data)] 列で [レプリカ (Replica)] アイコンをクリックします (自動複製間隔については、[ローカルクラスタデータの複製 \(110 ページ\)](#) を参照してください)。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。ほとんどの場合、デフォルトの [置換 (Replace)] モードのままにしておきますが、リージョンクラスタですでに定義されている既存の管理者プロパティを保持するには [保証 (Ensure)] を選択します。または、ローカルクラスタの管理者データベースの正確なコピーを作成するには、[完全 (Exact)] を選択します (非推奨)。
- ステップ 5** クラスタの横にある [コア管理者のプル (Pull Core Administrators)] をクリックするか、クラスタ名を展開して [管理者のプル (Pull Administrator)] をクリックして、クラスタ内の個々の管理者をプルします。
- ステップ 6** [プルするレプリカ管理者データの選択 (Select Replica Admin Data to Pull)] ダイアログボックスで、変更設定データを表示し、[OK] をクリックします。[管理者の一覧表示/追加 (List/Add Administrators)] ページに戻ると、プルした管理者がリストに追加されています。

- (注) リージョンクラスタがなく、1つのローカルクラスタから別のクラスタに管理者、ロール、またはグループをコピーする場合は、それらをエクスポートしてから、`cnr_exim` ツールを使用して、ターゲットクラスタに再インポートすることができます ([cnr_exim データインポートおよびエクスポートツールの使用 \(236ページ\)](#) を参照)。ただし、このツールは管理者パスワードを保持しないため、ターゲットクラスタで手動でリセットする必要があります。パスワードのセキュリティを維持するために、この方法が実装されています。エクスポートコマンドは、次のとおりです。

```
cnr_exim -c admin -x -e outputfile.txt
```

CLI コマンド

リージョンクラスタに接続されているときには、`admin <name | all > pull <ensure | replace | exact > cluster-name [-report-only | -report]` コマンドを使用できます。

外部認証サーバーのプッシュとプル

リージョン Web UI の [RADIUS サーバーの一覧表示/追加 (List/Add RADIUS Server)] ページまたは [Active Directory サーバーの一覧表示/追加 (List/Add Active Directory Server)] ページで、すべての外部認証サーバーをローカルクラスタにプッシュしたり、ローカルクラスタから外部認証サーバーデータをプルしたりできます。

RADIUS 外部認証サーバーのプッシュ

外部認証サーバーをローカルクラスタにプッシュするには、次の手順を実行します。

リージョンの詳細 Web UI

- ステップ 1** [管理 (Administration)] メニューから、[外部認証 (External Authentication)] サブメニューの [Radius] を選択して、リージョン Web UI で [RADIUS サーバーの一覧表示/追加 (List/Add RADIUS Server)] ページを表示します。
- ステップ 2** [Radius] ペインの [すべてプッシュ (Push All)] アイコンをクリックして、ページにリストされているすべての外部認証サーバーをプッシュするか、[プッシュ (Push)] をクリックして、個々の外部認証サーバーをプッシュします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ダイアログボックスが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。
 - すべての外部認証サーバーをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)] を選択できます。
 - 単一の外部認証サーバーをプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できます。

上記のいずれの場合も、[保証 (Ensure)] がデフォルトのモードです。

RADIUS 外部認証サーバーのプル

ローカルクラスタの既存の外部認証サーバーデータを置換する場合のみ、[置換 (Replace)] を選択します。ローカルクラスタに外部認証サーバーデータの正確なコピーを作成し、それによって、リージョンクラスタで定義されていないすべての外部認証サーバーを削除する場合にのみ、[完全 (Exact)] を選択します。

ステップ 4 [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。

RADIUS 外部認証サーバーのプル

外部認証サーバーのデータをローカルクラスタからプルするには、次の手順を実行します。

リージョンの詳細 Web UI

ステップ 1 [管理 (Administration)] メニューから、[外部認証 (External Authentication)] サブメニューの [Radius] を選択して、リージョン Web UI で [Radius サーバーの一覧表示/追加 (List/Add Radius Server)] ページを表示します。

ステップ 2 [Radius サーバーの一覧表示/追加 (List/Add Radius Server)] ページで、[Radius] ペインの [データのプル (Pull Data)] をクリックします。[プルするレプリカ外部認証サーバーデータの選択 (Select Replica External Authentication Server Data to Pull)] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカデータの更新 (Update Replica Data)] 列の [レプリカ (Replica)] アイコンをクリックします。(自動複製間隔については、[ローカルクラスタデータの複製 \(110 ページ\)](#) を参照してください)。

ステップ 4 [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。

ローカルクラスタの既存の認証サーバー プロパティを保持するには、[保証 (Ensure)] を選択しますが、それ以外の場合は、デフォルトの [置換 (Replace)] モードのままにします。

(注) [完全 (Exact)] を選択して、ローカルクラスタで外部認証サーバーデータの正確なコピーを作成することは推奨されません。

ステップ 5 クラスタの横にある [すべての外部認証サーバーのプル (Pull All External Authentication Servers)] をクリックします。

ステップ 6 [レプリカ認証サーバーのプルの報告 (Report Pull Replica Authentication servers)] ページで、プルの詳細を確認し、[実行 (Run)] をクリックします。

[レプリカ認証サーバーのプルの実行 (Run Pull Replica Authentication servers)] ページで、変更設定データを確認し、[OK] をクリックします。[認証サーバーの一覧表示/追加 (List/Add Authentication Server)] ページに戻ると、プルされた外部認証サーバーがリストに追加されています。

AD 外部認証サーバーのプッシュ

外部認証サーバーをローカルクラスタにプッシュするには、次の手順を実行します。

リージョンの詳細 Web UI

- ステップ 1** [管理 (Administration)]メニューから、[外部認証 (External Authentication)]サブメニューの[Active Directory]を選択して、リージョン Web UI で [Active Directoryサーバーの一覧表示/追加 (List/Add Active Directory Server)] ページを表示します。
- ステップ 2** [Active Directory] ペインで [すべてプッシュ (Push All)] をクリックして、外部認証サーバーをプッシュします。 [ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ダイアログボックスが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。
- すべての外部認証サーバーをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)] を選択できます。
 - 単一の外部認証サーバーをプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できます。
- 上記のいずれの場合も、[保証 (Ensure)] がデフォルトのモードです。

ローカル クラスタの既存の外部認証サーバー データを置換する場合のみ、[置換 (Replace)] を選択します。ローカル クラスタに外部認証サーバー データの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべての外部認証サーバーを削除する場合にのみ、[完全 (Exact)] を選択します。

- ステップ 4** [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。
-

CLI コマンド

リージョン クラスタに接続されているときには、**auth-ad-server <name | all > push <ensure | replace | exact > cluster-list [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

AD 外部認証サーバーのプル

ローカル クラスタから AD 外部認証サーバーのデータをプルするには、次の手順を実行します。

リージョンの詳細 Web UI

- ステップ 1** [管理 (Administration)]メニューから、[外部認証 (External Authentication)]サブメニューの[Active Directory]を選択して、リージョン Web UI で [Active Directoryサーバーの一覧表示/追加 (List/Add Active Directory Server)] ページを表示します。
- ステップ 2** [Active Directoryサーバーの一覧表示/追加 (List/Add Active Directory Server)] ページで、[Active Directory] ペインの [データのプル (Pull Data)] をクリックします。 [プルするレプリカ外部認証サーバー データの選択 (Select Replica External Authentication Server Data to Pull)] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカ データの更新 (Update Replica Data)] 列の [レプリカ (Replica)] アイコンをクリックします (自動複製間隔については、[ローカル クラスタ データの複製 \(110 ページ\)](#) を参照してください)。

ステップ 4 [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。

ローカル クラスタの既存の認証サーバー プロパティを保持するには、[保証 (Ensure)] を選択しますが、それ以外の場合は、デフォルトの [置換 (Replace)] モードのままにします。

(注) [完全 (Exact)] を選択して、ローカル クラスタで外部認証サーバーデータの正確なコピーを作成することは推奨されません。

ステップ 5 クラスタの横にある [すべての外部認証サーバーのプル (Pull All External Authentication Servers)] をクリックします。

ステップ 6 [レプリカ認証サーバーのプルの報告 (Report Pull Replica Authentication servers)] ページで、プルの詳細を確認し、[実行 (Run)] をクリックします。

[レプリカ認証サーバーのプルの実行 (Run Pull Replica Authentication servers)] ページで、変更設定データを確認し、[OK] をクリックします。[認証サーバーの一覧表示/追加 (List/Add Authentication Server)] ページに戻ると、プルされた外部認証サーバーがリストに追加されています。

CLI コマンド

リージョン クラスタに接続されているときには、`auth-ad-server <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]` コマンドを使用できます。

グループのプッシュとプル

グループのプッシュとプルは、管理者をローカルクラスタの一貫したロールのセットに関連付ける上で不可欠です。リージョンクラスタ Web UI の [管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページで、グループをローカル クラスタにプッシュしたり、グループをプルしたりできます。

関連項目

[ローカル クラスタへのグループのプッシュ \(78 ページ\)](#)

[レプリカ データベースからのグループのプル \(79 ページ\)](#)

ローカル クラスタへのグループのプッシュ

ローカルクラスタにグループをプッシュするには、1つ以上のクラスタとプッシュモードを選択する必要があります。

リージョン基本および詳細 [Web UI](#)

ステップ 1 [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [グループ (Groups)] を選択します。

- ステップ 2** [管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページで、[グループ (Groups)] ペインの [すべてプッシュ (Push All)] アイコンをクリックして、ページにリストされているすべてのグループをプッシュします。または [プッシュ (Push)] をクリックして、個々のグループをプッシュします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ダイアログボックスが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。すべてのグループをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)] を選択できます。1 つのグループをプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できます。いずれの場合も、[保証 (Ensure)] がデフォルトのモードです。ローカルクラスタの既存のグループデータを置換する場合にのみ、[置換 (Replace)] を選択します。ローカルクラスタにグループデータの正確なコピーを作成し、それによって、リージョンクラスタで定義されていないすべてのグループを削除する場合にのみ、[完全 (Exact)] を選択します。
- ステップ 4** デフォルトでは、関連付けられているロールと所有者がグループとともにプッシュされます。ロールは置換モードでプッシュされ、所有者は保証モードでプッシュされます。関連付けられているロールまたは所有者のプッシュを無効にするには、それぞれのチェックボックスをオフにします。
- ステップ 5** デスティネーションクラスタの [使用可能 (Available)] フィールドで 1 つ以上のローカルクラスタを選択し、それらを [選択済み (Selected)] フィールドに移動します。
- ステップ 6** [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。
- ステップ 7** [プッシュ グループ データ レポートの表示 (View Push Group Data Report)] ダイアログボックスで、プッシュの詳細を確認して、[OK] をクリックし、[管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページに戻ります。

CLI コマンド

リージョン クラスタに接続されているときには、**group <name | all> push <ensure | replace | exact> cluster-list [-omitrelated] [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。この操作では、関連するロール (置換モードを使用) と関連する所有者とリージョン (保証モードを使用) もプッシュされます。これを防止し、グループだけをプッシュする場合は、**-omitrelated** を指定します。

レプリカ データベースからのグループのプル

ローカル クラスタからの管理者グループのプルは、主に、他のローカル クラスタにプッシュできるグループの初期リストを作成する場合にのみ役立ちます。ローカル グループは、リージョン クラスタ自体では有効ではありません。これらのグループには、リージョン ロールが割り当てられていないためです。

グループをプルするときには、実際にはリージョン クラスタのレプリカ データベースからプルします。ローカル クラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカル クラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン基本および詳細 Web UI

-
- ステップ 1** [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [グループ (Groups)] を選択します。
- ステップ 2** [管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページで、[グループ (Groups)] ペインの [データのプル (Pull Data)] アイコンをクリックします。[プルするレプリカ CCMAdminGroup データの選択 (Select Replica CCMAdminGroup Data to Pull)] ダイアログボックスが開きます。
- ステップ 3** クラスタの [レプリカデータの更新 (Update Replica Data)] 列で [レプリカ (Replica)] アイコンをクリックします (自動複製間隔については、[ローカル クラスタ データの複製 \(110 ページ\)](#) を参照してください)。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。ほとんどの場合、デフォルトの [置換 (Replace)] モードのままにしておきますが、ローカル クラスタの既存のグループ プロパティを保持するには [保証 (Ensure)] を選択します。または、ローカル クラスタのグループ データの正確なコピーを作成するには、[完全 (Exact)] を選択します (非推奨)。
- ステップ 5** クラスタの横にある **Pull Core Groups** をクリックするか、クラスタ名を展開して、**Pull Group** をクリックして、クラスタ内の個々のグループをプルします。
- ステップ 6** [レプリカ グループのプルの報告 (Report Pull Replica Groups)] ページで、プルの詳細を確認し、[実行 (Run)] をクリックします。
- ステップ 7** [レプリカ グループのプルの実行 (Run Pull Replica Groups)] ページで、変更設定データを確認し、[OK] をクリックします。[管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページに戻ると、プルしたグループがリストに追加されています。
-

CLI コマンド

リージョン クラスタに接続されているときには、`group <name | all> pull <ensure | replace> cluster-name [-report-only | -report]` コマンドを使用できます。

ロールのプッシュとプル

リージョン クラスタ Web UI の [管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページで、ロールをローカル クラスタにプッシュしたり、ロールをプルしたりすることができます。また、サブロールの権限に応じて、関連付けられたグループと所有者をプッシュしたり、関連付けられた所有者をプルしたりすることもできます ([表 6: 集中管理者管理に必要なサブロール \(71 ページ\)](#) を参照)。

関連項目

- [ローカル クラスタへのロールのプッシュ \(81 ページ\)](#)
- [レプリカ データベースからのロールのプル \(82 ページ\)](#)

ローカル クラスタへのロールのプッシュ

管理者ロールをローカルクラスタにプッシュするには、1つ以上のクラスタとプッシュモードを選択する必要があります。

リージョン詳細 *Web UI*

- ステップ 1** [管理 (Administration)]メニューから、[ユーザーアクセス (User Access)]サブメニューの[ロール (Roles)]を選択します。
- ステップ 2** [管理者ロールの一覧表示/追加 (List/Add Administrator Roles)]ページで、[ロール (Roles)]ペインの **Push All** アイコンをクリックして、ページにリストされているすべてのロールをプッシュするか、または **Push** をクリックして、個々のロールをプッシュします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)]ダイアログボックスが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)]ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。すべてのロールをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)]を選択できます。1つのグループをプッシュする場合は、[保証 (Ensure)]または [置換 (Replace)]を選択できます。いずれの場合も、[保証 (Ensure)]がデフォルトのモードです。ローカルクラスタの既存のロールデータを置き換える場合にのみ、[置換 (Replace)]を選択します。ローカルクラスタにロールデータの正確なコピーを作成し、それによって、リージョンクラスタで定義されていないすべてのロールを削除する場合にのみ、[完全 (Exact)]を選択します。
- ステップ 4** デフォルトでは、関連付けられたグループと所有者がロールとともにプッシュされます。グループは置換モードで、所有者は保証モードでプッシュされます。関連付けられているロールまたは所有者のプッシュを無効にするには、それぞれのチェックボックスをオフにします。
 - 関連付けられたグループのプッシュを無効にし、グループがローカル クラスタに存在しない場合、ロールの名前に基づくグループがローカル クラスタで作成されます。
 - 関連付けられた所有者のプッシュを無効にし、所有者がローカル クラスタに存在しない場合、そのロールは意図した制約を使用して設定されません。グループをローカル クラスタに個別にプッシュするか、または **owner-region** サブロールが割り当てられているリージョン管理者が、ロールをプッシュする前にグループをプッシュしたことを確認する必要があります。
- ステップ 5** デスティネーションクラスタの [使用可能 (Available)]フィールドで1つ以上のローカル クラスタを選択し、それらを [選択済み (Selected)]フィールドに移動します。
- ステップ 6** [クラスタへのデータのプッシュ (Push Data to Clusters)]をクリックします。
- ステップ 7** [ロールデータのプッシュ レポートの表示 (View Push Role Data Report)]ページで、プッシュの詳細を確認してから、**OK** をクリックして、[管理者ロールの一覧表示/追加] ページに戻ります。

CLI コマンド

リージョンクラスタに接続されているときには、**role <name|all> push <ensure|replace|exact> <cluster-list [-omitrelated] [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。この操作では、関連するグループ (置換モードを使用) および

関連する所有者とリージョン（保証モードを使用）もプッシュされます。これを防止し、ロールだけをプッシュするには、**-omitrelated** を指定します。

レプリカ データベースからのロールのプル

ローカル クラスタからの管理者ロールのプルは、主に、他のローカル クラスタにプッシュできるロールの初期リストを作成する場合にのみ役立ちます。ローカル ロールは、リージョン クラスタ自体では有用ではありません。

ロールをプルするときには、実際にはリージョン クラスタのレプリカ データベースからプルします。ローカル クラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカル クラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン詳細 Web UI

-
- ステップ 1** [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [ロール (Roles)] を選択します。
- ステップ 2** [管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページで、[ロール (Roles)] ペインの [データのプル (Pull Data)] アイコンをクリックします。[プルするレプリカ管理者ロールデータの選択 (Select Replica Administrator Role Data to Pull)] ダイアログボックスが開きます。
- ステップ 3** クラスタの [レプリカ データの更新 (Update Replica Data)] 列の [レプリカ (Replica)] アイコンをクリックします。（自動複製間隔については、[ローカル クラスタ データの複製 \(110 ページ\)](#) を参照してください）。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。ほとんどの場合、デフォルトの [置換 (Replace)] モードのままにしておきますが、ローカル クラスタの既存のロール プロパティを保持するには [保証 (Ensure)] を選択します。または、ローカル クラスタのロール データの正確なコピーを作成するには、[完全 (Exact)] を選択します（非推奨）。
- ステップ 5** owner-region サブロール権限を持っている場合は、関連するすべての所有者をロールとともにプルするかどうかを決定できます。これは常に保証モードになります。この選択はデフォルトで有効になっています。
- ステップ 6** クラスタの横にある **Pull Core Roles** をクリックするか、クラスタ名を展開して、**Pull Role** をクリックして、クラスタ内の個々のロールをプルします。
- ステップ 7** [レプリカ ロールのプルの報告 (Report Pull Replica Roles)] ページで、**Run** をクリックします。
- ステップ 8** [レプリカ ロールのプルの実行 (Run Pull Replica Roles)] ページで、変更設定データを確認し、**OK** をクリックします。[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページに戻ると、プルしたロールがリストに追加されています。
-

CLI コマンド

リージョン クラスタに接続されているときには、**role <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]** コマンドを使用できます。この操作によって、関連する所有者とリージョンが（保証モードを使用して）プルされます。これを防止し、ロールだけをプルするには、**-omitrelated** を指定します。

テナントのプッシュとプル

リージョン Web UI の [テナントの一覧表示/追加 (List/Add Tenants)] ページで、すべてのテナントをローカル クラスタにプッシュしたり、ローカル クラスタからテナントデータをプルしたりすることができます。

ローカル クラスタへのテナントのプッシュ

テナントをローカル クラスタにプッシュするには、次の手順を実行します。

リージョン基本および詳細 *Web UI*

スコープを追加するには、次の手順を実行します。

-
- ステップ 1 Administration** メニューから、**Tenants User Access** サブメニューの を選択して、リージョン Web UI で [テナントの一覧表示/追加 (List/Add Tenants)] ページを表示します。
- ステップ 2** [テナント (Tenants)] ペインの **Push All** アイコンをクリックして、ページにリストされているすべてのテナントをプッシュするか、**Push** をクリックして、個々のテナントをプッシュします。[ローカル クラスタへのテナントデータのプッシュ (Push Tenant Data to Local Clusters)] ページが開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。
- すべてのテナントをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)] を選択できます。
 - 1 つのテナントをプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できます。
- いずれの場合も、[保証 (Ensure)] がデフォルトのモードです。
- ローカル クラスタのテナントデータを置換する場合のみ、[置換 (Replace)] を選択します。ローカル クラスタのテナントデータの正確なコピーを作成して、それによって、リージョン クラスタで定義されていないすべてのテナントを削除する場合にのみ、[完全 (Exact)] を選択します。
- ステップ 4 Push Data to Clusters** をクリックします。
-

CLI コマンド

リージョン クラスタに接続されているときには、**tenant <tag | all> push <ensure | replace | exact> cluster-list [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データベースからのテナントのプル

レプリカ データベースからテナントをプルするには、次の手順を実行します。

リージョン基本および詳細 Web UI

- ステップ 1 Administration** メニューから、**Tenants User Access** サブメニューの を選択して、[テナントの一覧表示/追加 (List/Add Tenants)] ページを開きます。
- ステップ 2** [テナントの一覧表示/追加 (List/Add Tenants)] ページで、[テナント (Tenants)] ペインの **Pull Data** アイコンをクリックします。[プルするレプリカ テナント データの選択 (Select Replica Tenant Data to Pull)] ダイアログボックスが開きます。
- ステップ 3** クラスタの [レプリカ データの更新 (Update Replica Data)] 列の [レプリカ (Replica)] アイコンをクリックします。(自動複製間隔については、[ローカルクラスタデータの複製 \(110 ページ\)](#) を参照してください)。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。
- ローカル クラスタの既存のテナント データを保持するには、[保証 (Ensure)] を選択しますが、それ以外の場合は、デフォルトの [置換 (Replace)] モードのままにします。
- (注) [完全 (Exact)] を選択して、ローカル クラスタのテナント データの正確なコピーを作成することは推奨されません。
- ステップ 5 Pull Replica** をクリックします。
- ステップ 6** [プルするレプリカ テナント データの選択 (Select Replica Tenant Data to Pull)] ページで、[すべてのテナントをプル (Pull all Tenants)] をクリックして、プルの詳細を表示し、**Run** をクリックします。
- [レプリカ テナントのプルの実行 (Run Pull Replica Tenants)] ページで、変更設定データを表示し、**OK** をクリックします。[テナントの一覧表示/追加 (List/Add Tenants)] ページに戻ると、プルしたテナントがリストに追加されています。

CLI コマンド

リージョンクラスタに接続されているときには、**tenant <tag | all> pull <ensure | replace | exact > cluster-name [-report-only | -report]** コマンドを使用できます。

セッション管理

Cisco Prime Network Registrar は、ユーザーセッションをモニターし、セッション管理に関するシステム設定を管理し、各ユーザーのログイン情報をレポートする管理者機能を提供します。各ユーザーのログインおよびログアウトの詳細を提供するために、セッションイベントが追加されます。

ユーザー セッション

アプリケーションページの右上隅にある歯車アイコン (⚙️) をクリックすると、アカウントがいつ、どこで使用されたのかを確認できます。最初のログインでは、ユーザー名とホストだけが表示されます。2 回目のログインでは、最後に成功したログインが日時とともに表示されま

す。ログインに失敗すると、次に成功したログインでは、ログイン試行の失敗回数が表示されます。

スーパーユーザー管理者は、1人のユーザーの同時セッション数を制限して、アカウントの共有や過度の使用を防ぐことができます。また、ログイン試行の失敗回数を制限して、自動ログイン攻撃から保護することもできます。再試行制限に達すると、ユーザーアカウントは一時停止されます。

セッション制御属性を設定するには、次の手順を実行します。

ローカルおよびリージョン Web UI

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

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

ステップ 3 次のフィールドに必要な値を入力します。

- **admin-failed-login-limit** : 管理者アカウントが一時停止されるまでに許可されるユーザーまたはトークンログイン試行の失敗の最大回数を指定します。0 に設定すると、制限は適用されません。この値を 1 または 2 にすることは推奨されません。
- **admin-user-session-limit** : 単一管理者の同時ユーザーセッションの最大数を指定します。0 に設定すると、制限は適用されません。
- **admin-token-session-limit** : 単一管理者の同時トークンセッションの最大数を指定します。シングルサインオン接続が、最も一般的なトークンセッションです。Web UI は、リソースモニターリングおよびダッシュボード表示のためにトークンセッションを開くこともあります。0 に設定すると、制限は適用されません。この値を 1 または 2 にすることは、予期しない Web UI 障害が発生する可能性があるため、推奨されません。
- **admin-suspended-timeout** : 一時停止の管理者アカウントが管理上再開されていない場合に、一時停止のままにする時間を指定します。0 に設定すると、アカウントを再開するには管理アクションが必要になります。アカウントが自動的に再開される場合は最大 30 分の追加の遅延が発生する可能性があります。

ステップ 4 [保存 (Save)]をクリックして設定を保存します。

ステップ 5 サーバーを再起動し、変更を確認します。

CLI コマンド

ユーザーアカウントを一時停止するには、**admin name suspend** を使用します。

ユーザーアカウントを再開するには、**admin name reinstate** を使用します。

アクティブユーザーセッション

アクティブユーザーセッションは、[CCM ユーザー接続 (CCM User Connections)] ページに一覧表示されます。このレポートページは、スーパーユーザーだけが使用できます。

CCM ユーザー接続レポートを表示するには、次の手順を実行します。

ローカルおよびリージョン Web UI

[操作 (Operate)] メニューの [レポート (Reports)] サブメニューで [CCM ユーザー接続 (CCM User Connections)] を選択し、[CCM ユーザー接続 (CCM User Connections)] ページを開きます。すべてのアクティブユーザーセッションが、管理者名、接続に関連付けられている認証のタイプ (管理者認証タイプ)、接続開始時間、要求の総数、およびクライアントの送信元の詳細とともに表示されます。

[送信元クライアント (Client Source)] 列には、接続に関する追加情報が表示されます (利用可能な場合)。これらの情報には、次のようなものがあります。

- 着信 HTTP/HTTPS 接続の送信元アドレスとポート (web UI および REST セッションの場合)。
- 受信した CLI、ツール、または SDK セッションの送信元アドレス、ポート、およびユーザー情報。使用可能な場合は、開始側のユーザーの SSH 接続用アドレスとポートも指定できます (これは、ユーザーの SSH_CONNECTION 環境変数に基づいています)。
- ほかにも次のような役に立つインジケータがあります。
 - ローカルクラスタとリージョンクラスタ間の CCM 接続に対する「Regional-to-local management」または「Local-to-regional management」。
 - ローカルクラスタ間のフェールオーバー、HA 同期、またはその他の CCM 間接続に対する「Local-to-local management」。
 - サーバーを識別するサーバー関連の接続 (および場合によっては追加の詳細情報) については、<および> で囲まれたその他の ID。



(注) この情報はクライアントによって CCM に提供されるため、スプーフィングの対象となる可能性があります。情報として扱う必要があるため権限はありません。



(注) [CCM ユーザー接続 (CCM User Connections)] では、2つの認証タイプ (管理者認証タイプ : 1) ユーザーと 2) トークン) をサポートしています。

- Cisco Prime Network Registrar は、アプリケーションレベルの 2～3 個のスレッドを実行して、ダッシュボードとリソースモニターを操作します。これらは、トークンタイプの接続として表示されます。したがって、ログアウトしてもこれらの接続は存続し、バックグラウンドで実行され続けるため、トークンタイプの接続の要求数が増加します。すべての接続 (主にトークンタイプ) をクリアする場合は、Cisco Prime Network Registrar を再起動する必要があります。
- Cisco Prime Network Registrar からログアウトせずにブラウザを閉じると、ユーザータイプの接続は 2 時間 (デフォルトのセッションタイムアウト) 維持されます。

CLI コマンド

アクティブユーザーセッションを表示するには、**ccm listConnections** を使用します。

セッションイベントのログ

スーパーユーザー管理者は、セッションイベントのログエントリを表示するか Web UI の上部にある [アラーム (Alarms)] アイコンをクリックしてセッションイベントを表示することにより、セッションアクティビティをモニターできます。

セッションイベントのログを表示するには、次の手順を実行します。

ローカルおよびリージョン Web UI

- ステップ 1** [操作 (Operate)] メニューから、[サーバー (Servers)] サブメニューの [サーバー管理 (Manage Servers)] を選択して [サーバー管理 (Manage Server)] ページを開きます。
- ステップ 2** 左側の [サーバー管理 (Manage Server)] ペインで、[ローカル CCM サーバー (Local CCM Server)] をクリックします。[ローカル CCM サーバーの編集 (Edit Local CCM Server)] ページが表示されます。
- ステップ 3** [モニターのログ (Monitor Logs)] タブをクリックしてセッションイベントのログを表示します。

CCM は、ユーザーが CCM に認証されるときに、クライアントが提供する追加の送信元情報 (詳細については、[アクティブユーザーセッション \(86 ページ\)](#) を参照) をログに記録します。また、接続が閉じられるときに情報が提供される場合は、その情報をログに記録します。この情報は、ユーザーログイン (ユーザー設定) 情報に関連する変更ログエントリにも示されます。



-
- (注) この情報は、Cisco Prime Network Registrar 10.1 CLI および SDK 以降でのみ提供されます (Cisco Prime Network Registrar 10.0 以前のクライアントでは、この追加情報がレポートされないため、CCM はそれをログに記録しない)。
-



第 5 章

所有者とリージョンの管理

この章では、DHCPアドレスブロック、サブネット、プレフィックス、リンク、およびゾーンに適用できる所有者とリージョンを設定する方法について説明します。

- [所有者の管理 \(89 ページ\)](#)
- [リージョンの管理 \(90 ページ\)](#)
- [所有者とリージョンの一元管理 \(91 ページ\)](#)

所有者の管理

アドレスブロック、サブネット、プレフィックス、リンク、およびゾーンに関連付ける所有者を作成できます。1つのページで所有者を一覧表示したり、追加したりすることができます。所有者を作成するには、タグ名、氏名、および連絡先名を作成する必要があります。

ローカル詳細およびリージョン詳細 Web UI

- ステップ 1** [管理 (**Administration**)]メニューから、[設定 (**Settings**)]サブメニューの[所有者 (**Owners**)]を選択して、[所有者の一覧表示/追加 (**List/Add Owners**)]ページを開きます。リージョンクラスタには、プル機能とプッシュ機能も含まれています。
- ステップ 2** 左側の[所有者 (**Owners**)]ペインで、[所有者の追加 (**Add Owners**)]アイコンをクリックします。[所有者の追加 (**Add Owner**)]ページが開きます。
- ステップ 3** 一意の所有者タグを入力します。
- ステップ 4** 所有者名を入力します。
- ステップ 5** オプションの連絡先名を入力します。
- ステップ 6** **Add Owner** をクリックします。
- ステップ 7** 所有者を編集するには、左側の[所有者 (**Owners**)]ペインで、その所有者の名前をクリックします。

CLI コマンド

所有者を作成するには、**owner tag create name [attribute=value]** を使用します。次に例を示します。

```
nrcmd> owner owner-1 create "First Owner" contact="Contact at owner-1"
```

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再使用の場合は、クラスターのリストまたは「すべて」を指定できます。

- **owner < tag | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]**
- **owner < tag | all > push < ensure | replace | exact > cluster-list [-report-only | -report]**
- **owner tag reclaim cluster-list [-report-only | -report]**

リージョンの管理

アドレスブロック、サブネット、プレフィックス、リンク、およびゾーンに関連付けるリージョンを作成できます。1つのページにリージョンを一覧表示したり、追加したりすることができます。リージョンを作成するには、タグ名、フルネーム、および連絡先名を作成する必要があります。

ローカル詳細およびリージョン詳細 Web UI

- ステップ 1 Administration** メニューから、**Settings**サブメニューの **Regions** を選択して、[リージョンの一覧表示/追加 (List/Add Regions)] ページを開きます。リージョンクラスターには、プル機能とプッシュ機能も含まれています。
- ステップ 2** 左側の [リージョン (Regions)] ペインで、[リージョンの追加 (Add Regions)] アイコンをクリックします。
- ステップ 3** 一意のリージョンタグを入力します。
- ステップ 4** リージョン名を入力します。
- ステップ 5** オプションの連絡先名を入力します。
- ステップ 6 Add Region** をクリックします。
- ステップ 7** リージョンを編集するには、左側の [リージョン (Regions)] ペインでその領域の名前をクリックします。

CLI コマンド

region tag create name [attribute=value] を使用します。次に例を示します。

```
nrcmd> region region-1 create "Boston Region" contact="Contact at region-1"
```

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再使用の場合は、クラスターのリストまたは「すべて」を指定できます。

- **region < tag | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]**

- `region <tag | all> push <ensure | replace | exact> cluster-list [-report-only | -report]`
- `region tag reclaim cluster-list [-report-only | -report]`

所有者とリージョンの一元管理

リージョンまたはローカル CCM 管理者として、次のことができます。

- 所有者とリージョンをローカル クラスタにプッシュします。
- ローカル クラスタの所有者とリージョンを中央クラスタにプルします。

これらの各機能には、少なくとも 1 つのリージョン CCM 管理者サブロールが定義されている必要があります（[ロール、サブロール、および制約（45 ページ）](#)を参照）。

次の表に、これらの操作に必要なサブロールを示します。

表 7: 集中管理者管理に必要なサブロール

集中管理者管理アクション	必要なリージョン サブロール
所有者またはリージョンの作成、変更、プル、プッシュ、または削除	owner-region

関連項目

[所有者またはリージョンのプッシュとプル（91 ページ）](#)

所有者またはリージョンのプッシュとプル

リージョン クラスタ Web UI の [所有者の一覧表示/追加 (List/Add Owners)] ページまたは [リージョンの一覧表示/追加 (List/Add Regions)] ページで、所有者またはリージョンをローカル クラスタにプッシュしたり、プルしたりすることができます。

関連項目

[ローカル クラスタへの所有者またはリージョンのプッシュ（91 ページ）](#)

[レプリカ データベースからの所有者とリージョンのプル（92 ページ）](#)

ローカル クラスタへの所有者またはリージョンのプッシュ

所有者またはリージョンをローカル クラスタにプッシュするには、1 つ以上のクラスタとプッシュモードを選択する必要があります。

リージョン Web UI

ステップ 1 Administration メニューから **Settings** サブメニューの **Owners** または **Regions** を選択します。

ステップ 2 [所有者の一覧表示/追加 (List/add Owners)]または[リージョンの一覧表示/追加 (List/Add Regions)]ページで、左側のペインの **Push All** アイコンをクリックするか、または特定の所有者またはリージョンの [所有者の編集 (Edit Owner)]ページまたは [リージョンの編集 (Edit Region)]ページの上部にある **Push** をクリックします。[所有者のプッシュ (Push Owner)]または [リージョンのプッシュ (Push Region)]ページが開きます。

ステップ 3 [データ同期モード (Data Synchronization Mode)]ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。

- すべての所有者またはリージョンをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [完全 (Exact)]を選択できます。
- 1 つの所有者またはリージョンをプッシュする場合は、[保証 (Ensure)]または [置換 (Replace)]を選択できます。

上記のいずれの場合も、[保証 (Ensure)]がデフォルトのモードです。

ローカルクラスタの既存の所有者またはリージョンデータを置き換える場合のみ、[置換 (Replace)]を選択します。ローカル クラスタで所有者またはリージョン データの正確なコピーを作成し、リージョンクラスタで定義されていないすべての所有者またはリージョンを削除する場合にのみ、[完全 (Exact)]を選択します。

ステップ 4 デスティネーションクラスタの [使用可能 (Available)]フィールドで1つ以上のローカルクラスタを選択し、それらを [選択済み (Selected)]フィールドに移動します。

ステップ 5 [クラスタへのデータのプッシュ (**Push Data to Clusters**)]をクリックします。

ステップ 6 [プッシュ所有者データ レポートの表示 (View Push Owner Data Report)]または [プッシュリージョンデータ レポートの表示 (View Push Region Data Report)]ページでプッシュの詳細を確認し、**OK** をクリックして、[所有者の一覧表示/追加 (List/Add Owners)]または [リージョンの一覧表示/追加 (List/Add Regions)]ページに戻ります。

CLI コマンド

リージョンクラスタに接続されている場合は、次の `push` コマンドを使用できます。push コマンドでは、クラスタのリストまたは「all」を指定できます。

- `owner < tag | all > push < ensure | replace | exact > cluster-list [-report-only | -report]`
- `region < tag | all > push < ensure | replace | exact > cluster-list [-report-only | -report]`

レプリカ データベースからの所有者とリージョンのプル

所有者またはリージョンをプルするとき、実際にはリージョンクラスタのレプリカデータベースからプルします。ローカルクラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカルクラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン Web UI

-
- ステップ 1** リージョン クラスタ Web UI の [管理 (**Administration**)] メニューから、[設定 (**Settings**)] サブメニューの [所有者 (**Owners**)] または [リージョン (**Regions**)] を選択します。
- ステップ 2** [所有者の一覧表示/追加 (List/add Owners)] または [リージョンの一覧表示/追加 (List/Add Regions)] ページで、左側のペインの [データのプル (**Pull Data**)] アイコンをクリックします。[プルするレプリカ所有者データの選択 (Select Replica Owner Data to Pull)] または [プルするレプリカ リージョンデータの選択 (Select Replica Region Data to Pull)] ページが開きます。
- ステップ 3** クラスタの [レプリカデータのアップデート (Update Replica Data)] 列の [複製 (**Replicate**)] アイコンをクリックします。(自動複製間隔については、[ローカルクラスタデータの複製 \(110 ページ\)](#) を参照してください)。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。
- ローカル クラスタの既存の所有者またはリージョンのプロパティを保持するには、[保証 (**Ensure**)] を選択しますが、それ以外の場合は、デフォルトの [置換 (**Replace**)] モードのままにします。
- (注) [完全 (**Exact**)] を選択して、ローカルクラスタの所有者またはリージョンデータの正確なコピーを作成することはお勧めしません。
- ステップ 5** クラスタの横にある **Pull All Owners** または **Pull All Regions** をクリックするか、クラスタ名を展開して、**Pull Owner** または **Pull Region** をクリックして、クラスタ内の個々の所有者またはリージョンをプルします。
- ステップ 6** [レプリカ所有者のプルの報告 (Report Pull Replica Owners)] または [レプリカ リージョンのプルの報告 (Report Pull Replica Regions)] ページで、**Run** をクリックします。
- ステップ 7** [レプリカ所有者のプルの実行 (Run Pull Replica Owners)] または [レプリカ リージョンのプルの実行 (Run Pull Replica Region)] ページで、変更設定データを確認し、**OK** をクリックします。[所有者の一覧表示/追加 (List/Add Owners)] または [リージョンの一覧表示/追加 (List/Add Regions)] ページに戻ると、プルした所有者またはリージョンがリストに追加されています。
-

CLI コマンド

リージョン クラスタに接続されている場合は、次の pull コマンドを使用できます。

- **owner** < tag | all > **pull** < ensure | replace | exact > cluster-name [-report-only | -report]
- **region** < tag | all > **pull** < ensure | replace | exact > cluster-name [-report-only | -report]



第 6 章

中央構成の管理

この章では、Cisco Prime Network Registrar リージョン クラスタで中央構成を管理する方法について説明します。

- [中央構成タスク \(95 ページ\)](#)
- [Cisco Prime Network Registrar サービスのデフォルト ポート \(96 ページ\)](#)
- [ライセンスング \(101 ページ\)](#)
- [サーバー クラスタの設定 \(106 ページ\)](#)
- [中央構成管理サーバー \(115 ページ\)](#)
- [トリビアル ファイル転送 \(117 ページ\)](#)
- [簡易ネットワーク管理 \(119 ページ\)](#)
- [Cisco Prime Network Registrar SNMP とシステム SNMP の統合 \(131 ページ\)](#)
- [個人所有デバイスの Web サーバーの持ち込み \(131 ページ\)](#)
- [ポーリング プロセス \(134 ページ\)](#)
- [DHCP スコープ テンプレートの管理 \(136 ページ\)](#)
- [DHCP ポリシーの管理 \(139 ページ\)](#)
- [DHCP クライアントクラスの管理 \(141 ページ\)](#)
- [仮想プライベート ネットワークの管理 \(143 ページ\)](#)
- [DHCP フェールオーバー ペアの管理 \(145 ページ\)](#)
- [リース予約の管理 \(146 ページ\)](#)
- [リソース制限アラームのモニターリング \(147 ページ\)](#)
- [ローカル クラスタ管理チュートリアル \(151 ページ\)](#)
- [リージョン クラスタ管理チュートリアル \(159 ページ\)](#)

中央構成タスク

リージョン クラスタでの中央構成管理には、次のものが含まれます。

- サーバークラスタのセットアップ、データの複製、および DHCP 使用率とリース履歴データのポーリング。

- ルータのセットアップ ([ルータおよびルータ インターフェイスの管理 \(171 ページ\)](#) を参照)。
- DHCP スコープテンプレート、ポリシー、クライアントクラス、オプション、ネットワーク、バーチャルプライベート ネットワーク (VPN) などのネットワーク オブジェクトの管理。
- DHCP フェールオーバー サーバー ペアの管理。

これらの機能は、central-cfg-admin ロールが割り当てられている管理者のみが使用できます。(central-cfg-admin の機能の完全なリストについては、[表 5: リージョン クラス タ管理者の事前定義ロールと基本ロール \(48 ページ\)](#) を使用してください)。中央構成管理には、管理者のセットアップやリージョンサーバーのステータスの確認は含まれません。これらの機能は、[ライセンスング \(101 ページ\)](#) および [サーバーの管理 \(175 ページ\)](#) で説明されているように、リージョン管理者によって実行されます。

Cisco Prime Network Registrar サービスのデフォルト ポート

次の表に、Cisco Prime Network Registrar サービスに使用されるデフォルトのポートを示します。

表 8: Cisco Prime Network Registrar サービスのデフォルト ポート

ポート番号	プロトコル	サービス
53	TCP/UDP	DNS
53	TCP/UDP	DNS のキャッシング
67	UDP	DHCP クライアントからサーバーへ
68	UDP	DHCP サーバーからクライアントへ
69	UDP	TFTP (オプション) クライアントからサーバーへ
80	HTTP	BYOD Web サーバー クライアントからサーバー Web UI へ
162	TCP	SNMP トラップ サーバーからサーバーへ
389	TCP	DHCP サーバーから LDAP サーバーへ

ポート番号	プロトコル	サービス
443	HTTPS	BYOD Web サーバー セキュアクライアントからサーバー Web UI へ
546	UDP	DHCPv6 サーバーからクライアントへ
547	UDP	DHCPv6 クライアントからサーバーへ
647	TCP	DHCP フェールオーバー サーバーからサーバーへ
653	TCP	高可用性 (HA) DNS サーバーからサーバーへ
1234	TCP	ローカル クラスタ CCM サーバーからサーバーへ
1244	TCP	リージョン クラスタ CCM サーバーからサーバーへ
4444	TCP	SNMP クライアントからサーバーへ
8080	HTTP	ローカル クラスタ クライアントからサーバー Web UI へ
8090	HTTP	リージョン クラスタ クライアントからサーバー Web UI へ
8443	HTTPS	ローカル クラスタ セキュアクライアントからサーバー Web UI へ
8453	HTTPS	リージョン クラスタ セキュアクライアントからサーバー Web UI へ

ファイアウォールの考慮事項

DNS (キャッシングまたは権限) サーバーがステートフルファイアウォールの背後に展開されている場合 (物理ハードウェアまたは `contrack` などのソフトウェア)、次のことを行うことをお勧めします。

- 可能な場合は、少なくとも UDP DNS トラフィックについて、ステートフルサポートを無効にします。
- ステートフルサポートを無効にできない場合は、許可状態テーブルエントリの数を大幅に増加させる必要があります。

通常、DNS クエリは多くの異なるクライアントから着信し、同じクライアントからの要求が異なる送信元ポートを使用する場合があります。毎秒数千のクエリがあると、これらのさまざまなソースの数が大きくなり、ファイアウォールがステートフルトラッキングを使用している場合は、この状態を維持し、一定期間にわたって実行する必要があります。したがって、クエリトラフィックレートと状態時間間隔を指定して、ファイアウォールが十分な状態を維持できるようにする必要があります。

ファイアウォールを使用している場合は、使用しているサービスに応じて、一部のポート ([Cisco Prime Network Registrar サービスのデフォルトポート \(96 ページ\)](#)) に対してファイアウォールを開く必要があります。

DNS パフォーマンスとファイアウォール接続追跡



- (注) Redhat 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。

Cisco Prime Network Registrar のキャッシングおよび権威 DNS サーバーは、毎秒処理クエリ数 (QPS) が非常に大きくなるように設計されており、多くの場合、それを実現するように展開されます。通常、クエリの大部分は、解決時間の短い UDP ベースであり、さまざまな送信元ポートを持つ多数のクライアントから送信されます。DNS トラフィックのファイアウォール接続追跡が使用されている場合、ファイアウォールはこれらの要求を追跡用の新しい接続として扱います。UDP はコネクションレス型プロトコルであるため、ファイアウォールは接続のモニターリングを停止するために接続タイムアウトに依存する必要があります。ファイアウォール接続モニターリングタイムアウトは、通常、DNS 解決時間に比べて非常に長いため、ファイアウォールは、完了した要求をモニターするために引き続きリソースを使用します。これにより、ファイアウォールが設定制限にすぐに達し、最大 90% の要求がドロップされて DNS サーバーに到達しないため、DNS パフォーマンスが大幅に低下します。

シスコでは、DNS サーバー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。ファイアウォールは、DNS サーバーの OS の外部にある個別のアプリケーションで実行してください。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。DNS 接続追跡が無効になっていても、ファイアウォールが同じ場所に配置されていると、システムと DNS のパフォーマンスが 25 - 30 % 低下する可能性があることに注意してください。



- (注) シスコは、DNS トラフィックのファイアウォール接続追跡を使用した展開をサポートしていません。

ファイアウォールの無効化

ファイアウォールの停止および無効化の例を次に示します。Redhat/CentOS 7 では **firewalld** が使用されますが、それ以前のバージョンでは **iptables** と **ip6tables** が使用されます。これらのコマンドはルートとして実行する必要があることに注意してください。

firewalld

```
# systemctl stop firewalld
# systemctl disable firewalld
```

iptables

```
# /etc/init.d/iptables save
# /etc/init.d/iptables stop
# chkconfig iptables off
```

ip6tables

```
# /etc/init.d/ip6tables save
# /etc/init.d/ip6tables stop
# chkconfig ip6tables off
```

DNS トラフィックの接続追跡の無効化

DNS のファイアウォール接続追跡を無効にする例を次に示します。Redhat/CentOS 7 では **firewalld/firewall-cmd** が使用されますが、それ以前のバージョンでは **iptables/ip6tables** が使用されます。これらのコマンドはルートとして実行する必要があり、IPv4 と IPv6 には個別の設定があることに注意してください。

firewall-cmd (IPv4)

```
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --sport 53
-j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --sport 53 -j
ACCEPT
```

```
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --sport 53
-j ACCEPT
```

firewall-cmd (IPv6)

```
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --sport 53
-j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --sport 53
-j ACCEPT
```

iptables (IPv4)

```
# iptables -t raw -I OUTPUT -p udp --dport 53 -j CT --notrack
# iptables -t raw -I OUTPUT -p udp --sport 53 -j CT --notrack
# iptables -t raw -I PREROUTING -p udp --dport 53 -j CT --notrack
# iptables -t raw -I PREROUTING -p udp --sport 53 -j CT --notrack
# iptables -I INPUT -p udp --dport 53 -j ACCEPT
# iptables -I INPUT -p udp --sport 53 -j ACCEPT
# iptables -I OUTPUT -p udp --dport 53 -j ACCEPT
# iptables -I OUTPUT -p udp --sport 53 -j ACCEPT

# iptables -t raw -I OUTPUT -p tcp --dport 53 -j CT --notrack
# iptables -t raw -I OUTPUT -p tcp --sport 53 -j CT --notrack
# iptables -t raw -I PREROUTING -p tcp --dport 53 -j CT --notrack
# iptables -t raw -I PREROUTING -p tcp --sport 53 -j CT --notrack
# iptables -I INPUT -p tcp --dport 53 -j ACCEPT
# iptables -I INPUT -p tcp --sport 53 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 53 -j ACCEPT
# iptables -I OUTPUT -p tcp --sport 53 -j ACCEPT
```

ip6tables (IPv6)

```
# ip6tables -t raw -I OUTPUT -p udp --dport 53 -j CT --notrack
# ip6tables -t raw -I OUTPUT -p udp --sport 53 -j CT --notrack
# ip6tables -t raw -I PREROUTING -p udp --sport 53 -j CT --notrack
# ip6tables -t raw -I PREROUTING -p udp --dport 53 -j CT --notrack
# ip6tables -I INPUT -p udp --dport 53 -j ACCEPT
# ip6tables -I INPUT -p udp --sport 53 -j ACCEPT
# ip6tables -I OUTPUT -p udp --dport 53 -j ACCEPT
# ip6tables -I OUTPUT -p udp --sport 53 -j ACCEPT

# ip6tables -t raw -I OUTPUT -p tcp --dport 53 -j CT --notrack
# ip6tables -t raw -I OUTPUT -p tcp --sport 53 -j CT --notrack
# ip6tables -t raw -I PREROUTING -p tcp --sport 53 -j CT --notrack
# ip6tables -t raw -I PREROUTING -p tcp --dport 53 -j CT --notrack
# ip6tables -I INPUT -p tcp --dport 53 -j ACCEPT
# ip6tables -I INPUT -p tcp --sport 53 -j ACCEPT
# ip6tables -I OUTPUT -p tcp --dport 53 -j ACCEPT
# ip6tables -I OUTPUT -p tcp --sport 53 -j ACCEPT
```

Umbrella を使用するためのキャッシュ DNS の設定

Cisco Umbrella は、フィッシングやマルウェアなどのインターネット上の脅威に対する防御の最前線となります。Umbrella を解決に使用するようにキャッシング DNS を設定することにより、シスコの Umbrella のクラウドサービスで、要求されたドメイン/ホストに関する最新の応答を提供することが可能になります。詳細については、『*Cisco Prime Network Registrar 10.1 Caching and Authoritative DNS User Guide*』の「*Configuring Caching DNS to Use Umbrella*」の項を参照してください。



- (注) Umbrella サービスを最大限に活用するには、Cisco Umbrella とビジネス関係を持つ必要があります。

ライセンスング

Cisco Prime Network Registrar には、CCM、権威 DNS、キャッシング DNS、および DHCP サービス、またはこれらのサービスの組み合わせに対して個別のライセンスが必要です。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。将来のアップグレードにはサブスクリプションライセンスを購入する必要があります。初期サブスクリプションは常に 3 年間で、更新によって 1 年間延長されます。ライセンスの詳細については、『*Cisco Prime Network Registrar 10.1 Installation Guide*』の「*License Files*」を参照してください。

初めてログインを試みる際のライセンスデータの入力については、[Web UI へのログイン \(12 ページ\)](#) を参照してください。

ログイン後に、リージョンサーバーに追加のサービスベースのライセンスを追加できます。ファイルからロードされた個々のライセンスは削除しないでください。アップグレード後には古いバージョンの DNS および DHCP ライセンスを削除できます。サーバー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。

リージョンまたはローカルクラスタにログインするときには、システムの全体的なライセンスステータスがチェックされます。有効なシステムライセンスがない場合、ログインは拒否されます。違反があった場合は、違反と詳細が通知されます。この通知は、ユーザーセッションごとに1回だけ実行されます。また、違反を示すメッセージが各ページに表示されるようにすることもできます。

リージョン Web UI

[製品ライセンスの一覧表示/追加 (List/Add Product Licenses)] ページを開くには、**Administration** > **User Access** から **Licenses** を選択します。**Browse** をクリックしてライセンス ファイルを探し、ファイルをクリックして、**Open** をクリックします。ファイル内のライセンス ID が有効な場合、ライセンス キーがライセンスのリストに表示され、「ライセンス ファイル "filename" が正常に追加されました (Successfully added license file "filename").」というメッセージが表示されます。ID が有効でない場合は、[ライセンス (License)] フィールドにファイルの内容が表示され、「オブジェクトは無効です (Object is invalid)」というメッセージが表示されます。

ページの上部にある [ライセンス使用状況 (License Utilization)] セクションには、ライセンスのタイプ、ライセンスに許可されるノード数、および実際に使用されているノード数が表示されます。プラス記号 (+) をクリックして、セクションを展開します。ライセンスされた各サービスのライセンス使用状況が、このセクションに個別に表示されます。

[使用権 (Right To Use)] と [使用中 (In Use)] の数が、ライセンスされた各サービスについて表示されます。使用権の値は、そのサービスに追加されたすべてのライセンスのカウンターの集約です。[使用合計 (total in use)] の値は、すべてのローカル クラスタから取得された最新の使用率の数値を集約したものです。このセクションには、使用権または使用中カウントがプラスのサービスのみが表示されます。[使用中 (In Use)] の数が [使用権 (Right To Use)] の数を超えると、「License exceed count」というエラーメッセージが表示されます。

以前のバージョンの Cisco Prime Network Registrar のライセンスと使用数は、別のセクション「ip-node」に表示されます。

Expert モード 属性を使用すると、すべてのローカル クラスタからライセンス使用率が収集される頻度を指定できます。この設定を変更したときには、サーバーを再起動して、変更を有効にする必要があります。この属性は、[CCM サーバーの編集 (Edit CCM Server)] ページで設定できます。デフォルトは 4 時間です。

ライセンスの追加

シスコは、製品に付属しているソフトウェア ライセンス請求証明書に従って、Web で Cisco Prime Network Registrar 製品承認キー (PAK) を登録した後、1 つ以上のライセンス ファイルを電子メールでユーザーに送信します。シスコは、FLEXlm システムを通じてライセンスを管理します。



(注) ライセンスファイルのロードに失敗した場合は、ファイルが適切に書式化されたテキストファイルであり、余分な文字が含まれていないことを確認してください。電子メールからファイルを抽出して、システム間で移動すると、このような問題が発生することがあります。

ファイルがある場合は、次のようにします。

リージョン Web UI

- ステップ 1** 見つけやすいディレクトリ（またはデスクトップ）にライセンス ファイルを置きます。
- ステップ 2** [製品ライセンスの一覧表示/追加（List/Add Product Licenses）] ページで、**Choose File** ボタンをクリックして、各ファイルを参照します。
 - (注) [製品ライセンスの一覧表示/追加（List/Add Product Licenses）] オプションは、リージョンでのみ使用できます。
- ステップ 3** [ファイルの選択（Choose file）] ウィンドウで、最初のライセンス ファイルの場所を検索し、**Open** をクリックします。
- ステップ 4** ライセンス キーが受け入れ可能な場合、[スーパーユーザー管理者の追加（Add Superuser Administrator）] ページがすぐに表示されます。
- ステップ 5** さらにライセンスを追加するには、**Administration** メニューから、**Licenses User Access** サブメニューのを選択して、[製品ライセンスの一覧表示/追加（List/Add Product Licenses）] ページを開きます。**Choose File** をクリックして、追加のライセンス ファイルを見つけ、**Open** をクリックします。ファイル内のキーが受け入れ可能な場合は、キー、タイプ、カウント、および有効期限が表示され、評価キーであるかどうかも表示されます。キーが受け入れられない場合、ページには、ライセンステキストとエラーメッセージが表示されます。ライセンス タイプのリストについては、[ライセンスング（101 ページ）](#) を参照してください。

ライセンスのテーブルの上に [ライセンス使用率（License Utilization）] エリアがあります。展開すると、ライセンスのタイプが、使用可能なノードの総数と実際に使用されているノード数とともに表示されます。

Cisco Prime Network Registrar が分散システムとしてインストールされている場合、ライセンス管理はリージョンクラスタから実行されます。ローカルクラスタにライセンスを追加するためのオプションはありません。

CLI コマンド

license ファイルを使用して、**create** ファイルに格納されているライセンスを登録します。参照されるファイルには、コマンドを実行する場所の絶対パスが含まれています。次に例を示します。

```
nrcmd-R> license "C:\licenses\product.licenses" create
```

license list を使用して、作成されたすべてのライセンス（キーによって識別されます）のプロパティを一覧表示し、**license listnames** を使用して、キーだけを一覧表示します。特定のライセンス キーのプロパティを表示するには、**license** キー **show** を使用します。

NAT の背後にあるローカルクラスタの登録

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、リージョンクラスタから実行されます。最初にリージョンクラスタをインストールし、リージョンクラス

タ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 クラスタは、インストール プロセス時にリージョンクラスタに登録することによって、リージョンに登録できます。ただし、ローカルクラスタが NAT インスタンスの背後にある場合、初期要求がリージョンクラスタに到達しないため、登録が失敗する可能性があります。

Cisco Prime Network Registrar 8.3 以降では、ローカルクラスタから登録を開始することによって、NAT インスタンスの背後にあるローカルクラスタに登録できます。NAT インスタンスによってスパンされているローカルクラスタに登録するには、Cisco Prime Network Registrar 8.3 以降がリージョンとローカルの両方のクラスタにインストールされていることを確認する必要があります。また、ローカルクラスタのライセンス使用状況を確認することもできます。



- (注) リージョンクラスタが NAT インスタンスの背後にあるときにローカルクラスタに登録するには、リージョンサーバーからローカルクラスタに登録し、サービスを選択して、データを再同期することによって、リージョンサーバーからローカルクラスタに登録する必要があります。

NAT インスタンスの背後にあるローカルクラスタに登録するには、次の手順を実行します。

ローカル Web UI

ステップ 1 Administration メニューから、**User Access** サブメニューの **Licenses** を選択して [List Licenses] ページを開きます。

[ライセンスの一覧表示 (List Licenses)] ページで、リージョンクラスタの詳細を追加します。

- a) リージョンクラスタの IP アドレス (IPv4 または IPv6) を入力します。
- b) リージョンクラスタの SCP ポートを入力します (1244 がプリセット値です)。
- c) 登録するローカルクラスタの IP アドレス (IPv4 または IPv6) を選択します。
- d) ローカルクラスタに登録するコンポーネント サービスを選択します。

ステップ 2 [登録 (Register)] をクリックします。

- (注) リージョン CCM サーバーは、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のライセンス使用状況履歴を維持します。

ローカルクラスタのライセンス使用状況を表示するには、[ポーリングステータスのチェック (Check Poll Status)] をクリックします。

新しい UUID の生成

新しい UUID を生成して登録するには、次の手順を実行します。

ローカル Web UI

- ステップ 1** [管理 (Administration)]メニューから、[ユーザーアクセス (User Access)]サブメニューの [ライセンス (Licenses)]を選択して [ライセンスの一覧表示 (List Licenses)]ページを開きます。
- ステップ 2** リージョンクラスタの詳細を追加します。
- ステップ 3** [新しいホスト識別子の生成 (Generate new host identifier)]チェックボックスをオンにします。
- ステップ 4** [登録 (Register)]をクリックします。

CLI コマンド

ローカルクラスタを登録または再登録するには、次のコマンドを使用します。

```
nrcmd> license register [cdns|dns|dhcp[,...]] [<regional-ip>|<regional-ipv6>]
[<regional-port>] [-new-uuid]
nrcmd> license register cdns|dns|dhcp[,...] <regional-ip> <regional-ipv6> [<regional-port>]
[-new-uuid]
```

ライセンス履歴

[ライセンス履歴 (License History)]ページでは、指定された時間内に使用されたライセンスを表示できます。ライセンス履歴をチャート形式で表示できます。ここでは、一定期間にわたるさまざまなサービスのライセンス使用状況履歴を1つのビューで確認できます。また、データは時系列の逆順で表示されるため、最新のデータが上部に表示されます。設定された使用とサービスに基づいて、チャートの Y 軸は異なる場合があります。

ライセンス履歴を表示するには、次の手順を実行します。

リージョン Web UI

- ステップ 1** **Administration** メニューから [ユーザーアクセス (User Access)]サブメニューの **License History** を選択して、[ライセンス使用状況履歴の表示 (View License Utilization History)]ページを開きます。
- ステップ 2** [ライセンス履歴フィルタの設定 (Set License History Filter)]属性でフィルタ設定を指定します。指定された数の時間バケットに収まるようにフィルタオプションに一致するデータセットをダウンサンプリングするには、[結果のダウンサンプリング (Down-sample results)]チェックボックスをオンにします。
- ステップ 3** [フィルタの適用 (Apply Filter)]をクリックして、指定した時間枠のライセンス履歴を表示します。
 - 詳細は、[ライセンス履歴チャート (License History Charts)]タブにチャート形式で表示されます。チャートの下にある [チャートタイプ (Chart Type)]アイコンをクリックして、チャートタイプを変更できます。使用可能なチャートのタイプは、縦棒グラフ、折れ線グラフ、面グラフ、および散布図です。チャートの下にある [テーブルビュー (Table View)]アイコンをクリックすると、チャートデータが表形式で表示されます。
 - [ライセンステーブル (License Table)]タブをクリックすると、ライセンス履歴の詳細が表形式で表示されます。

CLI コマンド

license showUtilization を使用して、RTU (Right-to-Use) に対して使用された IP ノードの数を表示します (構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **license** コマンドを参照してください)。

ライセンス使用率

リージョン CCM サーバーは、ローカル クラスタからライセンス使用率情報を定期的に収集し、収集した使用率と登録済みライセンスに基づいて、ライセンスが準拠しているかどうかについてローカル クラスタを更新します。

リージョン サーバーは、ローカル クラスタから次のメトリックを収集して、ライセンス数を求めます。

- **DHCP サービス** - アクティブなリース数は、DHCPv4 と DHCPv6 のリース カウントを合計して求められます。

Cisco Prime Network Registrar 10.1.1 では、DHCPv4 カウントは、次の式で求めます。DHCP サーバーの **サーバー** カテゴリ *active-leases + reserved-leases - reserved-active-leases* 統計。DHCPv6 カウントは、次の式で求めます。DHCP サーバーの **dhcpv6** カテゴリ *active-leases + reserved-leases - reserved-active-leases* 統計。

- **認証 DNS サービス** - このカウントは、DNS サーバーの **サーバー** カテゴリの *total-rrs* 統計からのものです。
- **キャッシュ DNS サービス** - CDNS がクラスタでライセンスされている場合、カウントは 1 です。



- (注)
- フェールオーバー ペアと HA DNS ペアの場合、1 つのクラスタのみに接続されます。通常、到達可能な場合は main です。リージョンに有効なフェールオーバー ペアと HA DNS 情報がない場合、DHCP または DNS のライセンス使用率の計算が誤っている可能性があります。
 - クラスタのレプリカデータが最新であることを確認し ([ローカルクラスタとの同期 \(110 ページ\)](#) を参照)、アドレス空間やゾーンデータをプルします。

サーバー クラスタの設定

サーバー クラスタは、ローカル クラスタの場所にある CCM、DNS、CDNS、DHCP、および TFTP サーバーのグループです。たとえば、組織には、DNS サーバーと DHCP サーバーの Boston および Chicago クラスタが存在する場合があります。中央管理者は、これらのクラスタでのアドレスの割り当て方法に影響を与えるか、または DHCP 使用率またはリース履歴データをポー

リングすることができます。中央管理者は、必要な権限が存在する場合、サーバーの変更の表示または再起動のために、これらのローカル クラスタに接続することもできます。

[クラスタ サーバーのツリーの表示 (View Tree of Cluster Servers)] ページで、作成したクラスタを表示します。これを表示するには、**Clusters** をクリックします。ページにクラスタが入力されると、いくつかの豊富な情報が表示され、いくつかの有用な機能が提供されます。ローカル クラスタに同等の管理者アカウントが存在する場合、[ローカルに移動 (Go Local)] アイコンを使用して、ローカル クラスタ Web UI へのシングルサインオンが可能になります。

[クラスタのツリーの表示 (View Tree of Clusters)] ページは、[リモート クラスタのリスト/追加 (List/Add Remote Clusters)] ページで手動でクラスタを追加することによって、またはサーバー クラスタも作成するルータの追加および同期によって自動的に値が入力されている場合があります。クラスタ名は、クリックしてクラスタ情報を編集できるリンクです。再同期、レプリケーション、およびポーリング機能については、この章で詳しく説明します。

DHCP サーバーには、クラスタの DHCP サーバーの横に [関連サーバー (Related Servers)] アイコンが表示される場合があります。このアイコンをクリックすると、[DHCPサーバーの関連サーバーのリスト (List Related Servers for DHCP Server)] ページが表示されます。これらのサーバーは、DNS、TFTP、または DHCP フェールオーバー サーバーです。

関連項目

- [ローカル クラスタの追加 \(107 ページ\)](#)
- [ローカル クラスタの編集 \(109 ページ\)](#)
- [ローカル クラスタへの接続 \(109 ページ\)](#)
- [ローカル クラスタとの同期 \(110 ページ\)](#)
- [ローカル クラスタ データの複製 \(110 ページ\)](#)
- [レプリカ データの表示 \(111 ページ\)](#)
- [レプリカ データのページ \(112 ページ\)](#)
- [クラスタのデータの非アクティブ化、再アクティブ化、およびリカバリ \(112 ページ\)](#)
- [クラスタ レポートの表示 \(114 ページ\)](#)
- [使用率とリース履歴データのポーリング \(134 ページ\)](#)
- [リース履歴収集の有効化 \(136 ページ\)](#)

ローカル クラスタの追加

リージョン クラスタへのローカル クラスタの追加は、`central-cfg-admin` ロールの中核機能です。

クラスタを追加するために必要な最小限の値は、マシン名、IP アドレス (IPv4 または IPv6)、管理者のユーザー名、およびパスワードです。クラスタ名は一意である必要があり、その IP アドレスは CNRDB データベースが配置されているホストと一致している必要があります。ローカル クラスタ管理者から SCP および HTTP ポート、ユーザー名、およびパスワードを取

得します。Cisco Prime Network Registrar の SCP ポートのインストールのプリセット値は 1234 であり、HTTP ポートは 8080 です。

また、*use-ssl* 属性をオプションまたは必須に設定することで、ローカルサーバーへのアウトバウンド接続をセキュアにするかどうかを設定することもできます。デフォルトでは [オプション (optional)] に設定されており、有効にするには、Cisco Prime Network Registrar Communications Security オプションがインストールされている必要があります。

リージョン Web UI

[操作 (Operate)] メニューから、[サーバー (Servers)] サブメニューの [サーバーの管理 (Manage Servers)] を選択します。[サーバーの管理 (Manage Servers)] ページが開きます。このページでローカルクラスタを確認します。[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページでサーバー クラスタを追加することもできます。[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページには、次の機能があります。

- ローカル管理用のローカル クラスタ Web UI に接続します。
- ローカル クラスタと再同期して、そこで更新を調整します。
- データをリージョン クラスタのレプリカ データベースにプルします。
- レプリカをパージして、クラスタを削除/再追加することなく、不良なレプリカ データをクリアします。レプリカのパージを実行するときには、手動でレプリケーションを実行して、レプリカ データを再度取得する必要があります。



注 このオプションは、エキスパートモードでのみ表示されます。

- ローカルクラスタに DHCP 使用率データを照会します。この機能は、少なくともサブネット使用率のサブロールを持つ `regional-addr-admin` ロールが割り当てられているユーザーに対してのみ表示されます。
- ローカルクラスタにリース履歴データを照会します。この機能は、少なくともリース履歴サブロールを持つ `regional-addr-admin` ロールが割り当てられているユーザーに対してのみ表示されます。

クラスタを追加するには、[クラスタの管理 (Manage Clusters)] ペインの [クラスタの追加 (Add Cluster)] アイコンをクリックします。[クラスタの追加 (Add Cluster)] ダイアログボックスが開きます。ローカルクラスタの追加例については、[ローカルクラスタの作成 \(162 ページ\)](#) を参照してください。Add Cluster をクリックして、[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページに戻ります。

ローカル Web UI

ローカル Web UI でクラスタを管理することもできます。詳細については、[ローカル Web UI でのクラスタの構成 \(23 ページ\)](#) を参照してください。

CLI コマンド

クラスタを追加するには、**cluster name create** <address | ipv6-address> [attribute=value ...] を使用して、クラスタに名前を付けて、アドレスを指定し、重要な属性を設定します。次に例を示します。

```
nrcmd> cluster example-cluster create 192.168.100.101 admin=admin password=changeme
```

ローカルクラスタで完全に同期するには、管理者がスーパーユーザーである必要があることに注意してください。

ローカルクラスタの編集

リージョンクラスタでのローカルクラスタの編集は、central-cfg-admin ロールのコア機能です。

リージョン Web UI

ローカルクラスタを編集するには、[クラスタの管理 (Manage Clusters)] ペインで名前をクリックして、[リモートクラスタの編集 (Edit Remote Cluster)] ページを開きます。このページは、基本的には[リモートクラスタのリスト/追加 (List/Add Remote Clusters)] ページと同じですが、追加の属性設定解除機能があります。ローカルで実行するサービス (dhcp、dns、cdns、または none) を選択するには、**Local Services** エリアにあるチェックボックスをオンまたはオフにします。変更を行ってから、**Save** をクリックします。

ローカル Web UI

ローカル Web UI でクラスタを編集することもできます。詳細については、[ローカル Web UI でのクラスタの構成 \(23 ページ\)](#) を参照してください。

CLI コマンド

ローカルクラスタを編集するには、**cluster name set attribute=value** [attribute=value ...] を使用して、属性を設定またはリセットします。次に例を示します。

```
nrcmd> cluster Example-cluster set poll-replica-interval=8h
```

ローカルクラスタへの接続

Web UI で、ローカルクラスタに同等の管理者アカウントがある場合は、[リモートクラスタのリスト/追加 (List/Add Remote Clusters)] ページの[接続 (Connect)] アイコンをクリックして、ローカルクラスタの[サーバーの管理 (Manage Servers)] ページにシングルサインオンできます。リージョンクラスタの Web UI に戻るには、ローカルクラスタ ページの右上隅にある[戻る (Return)] アイコンをクリックします。ローカルクラスタで同等のアカウントを持っていない場合、[接続 (Connect)] アイコンをクリックすると、ローカルクラスタのログイン ページが開きます。

ローカル クラスタとの同期

同期は、統一された方法で連携できるように、リージョンとローカルのクラスタを設定します。同期するタイミング：

1. ローカル サーバーのリストが、リージョン クラスタにコピーされます。
2. シングルサインオンのために、リージョンとローカルのクラスタ間で共有秘密が確立されます。

同期は、リージョン クラスタにローカル クラスタを作成するときに 1 回実行されます。ただし、変更はローカルクラスタで定期的に行われることもあり、その場合は同期を再実行する必要があります。たとえば、ローカル接続を行うために使用されるユーザー名とパスワードを変更する場合があります。再同期は自動的に行われません。[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページの [再同期 (Resync)] アイコンをクリックする必要があります。結果として、成功の場合は肯定確認、失敗の場合はエラー メッセージが表示されます。

ローカルクラスタをアップグレードするときには、クラスタも再同期する必要があります。同期を有効にするには、ローカルクラスタに指定されたユーザーアカウントがスーパーユーザーである必要があります。同期エラー メッセージが表示された場合は、ローカル クラスタをチェックして、正常に動作していることを確認します。



- (注) リージョン クラスタでクラスタを再同期すると、レプリカ データの自動再初期化が行われます。その結果、大規模なサーバー構成の場合、再同期に数分かかることがあります。ただし、レプリカ データを更新するための個別のアクションが不要であるという利点があります。

ローカル クラスタ データの複製

レプリケーションは、ローカル サーバーからリージョン クラスタのレプリカ データベースに設定データをコピーします。レプリケーションは、DHCP オブジェクト データをリージョン サーバー データベースにプルする前に実行する必要があります。レプリケーション時：

1. ローカル データベースの現在のデータがリージョン クラスタにコピーされます。これは通常、一度だけ行われます。
2. 最後のレプリケーション後にプライマリデータベースに加えられた変更がすべてコピーされます。

レプリケーションは所定の時間間隔で行われます。[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページの [複製 (Replicate)] アイコンをクリックして、即時レプリケーションを強制することもできます。

[サーバー クラスタの追加 (Add Server Cluster)] ページで自動レプリケーション間隔を設定するか、または [サーバー クラスタの編集 (Edit Server Cluster)] ページで、*poll-replica-interval* 属性を使用して調整できます。この間隔は 4 時間に事前設定されています。また、

poll-replica-offset 属性を使用して、レプリカ データをポーリングする固定の時間帯を設定することもできます。デフォルト値は 0 時間（オフセットなし）です。*Poll-replica-rrs* 属性は、他のデータレプリケーションを無効にせずに RR データの複製を制御します。この属性は、[サーバーの管理 (Manage Servers)] ページと [クラスタの管理 (Manage Cluster s)] ページに表示され、値は none、all、および protected です。*poll-replica-rr* が none に設定されている場合、このクラスタの RR データは複製されません。設定を解除すると、CCM サーバーの設定が適用されます。



注意 レプリカデータベースが何らかの方法で破損している場合、リージョン CCM サーバーは起動しません。この問題が発生した場合は、リージョンサービスを停止し、*install-path/regional/data/replica* ディレクトリにあるレプリカ データベース ファイル（および /logs サブディレクトリのログファイル）を削除（または移動）してから、リージョンサーバーを再起動します。これを行うと、データ損失なしでレプリカデータベースが再作成されます。

レプリカ データの表示

Web UI では、[操作 (Operate)] メニューの [サーバー (Servers)] サブメニューから [レプリカデータの表示 (View Replica Data)] を選択することによって、リージョンクラスタのレプリカデータベースにキャッシュされているレプリカデータを表示できます。[レプリカクラスリストの表示 (View Replica Class List)] ページが開きます。

リージョン Web UI

次のものを選択します。

1. [クラスタの選択 (Select Cluster)] リストのクラスタ。
2. [クラスの選択 (Select Class)] リストのオブジェクトクラス。
3. 選択したクラスタとクラスのデータを複製します。[クラスタのデータの複製 (Replicate Data For Cluster)] ボタンをクリックします。
4. レプリカデータを表示します。[レプリカクラスリストの表示 (View Replica Class List)] をクリックします。選択したオブジェクトのクラスタと特定のクラスの [クラスタのレプリカデータの一覧表示 (List Replica Data for Cluster)] ページが開きます。このページでは、次の操作を実行できます。
 - オブジェクトの名前をクリックすると、リージョンクラスタのビューページが開きます。[レプリカの一覧表示 (List Replica)] ページに戻るには、**Return to object List** をクリックします。



注 [レプリカ アドレス ブロックの一覧表示 (List Replica Address Blocks)] および [レプリカ サブネットの一覧表示 (List Replica Subnets)] ページでは、この機能は提供されません。ローカルクラスタのアドレスブロックまたはサブネットを表示するには、[ローカルに移動 (Go local)] アイコンを使用します。

- [接続 (Connect)] アイコンをクリックして、ローカル クラスタにあるオブジェクトのリスト ページに移動します。[レプリカ *object* の一覧表示] ページに戻るには、[戻る (Return)] アイコンをクリックします。

[クラスタのレプリカ データの一覧表示 (List Replica Data for Cluster)] ページの [戻る (Return)] をクリックして、[レプリカ クラス リストの表示 (View Replica Class List)] ページに戻ります。

レプリカ データのページ

リージョン Web UI (エキスパート モードのみ) では、[リモート クラスタの一覧表示/追加 (List/Add Remote Clusters)] ページの [レプリカのページ (Purge Replica)] アイコンをクリックすることによって、クラスタを削除/再追加することなく、不良なレプリカ データをクリアできます。レプリカのページを実行するたびに、手動で複製を実行して、レプリカ データを再度取得する必要があります。

クラスタのデータの非アクティブ化、再アクティブ化、およびリカバリ

ハードディスク エラーが発生して、構成データが失われたと思われる場合は、クラスタの非アクティブ化が必要になることがあります。クラスタを非アクティブ化し、問題を解決し、レプリカ データベースからクラスタ データを回復してから、クラスタを再アクティブ化することができます。これにより、クラスタを削除してから、プロセスで失われたすべてのデータでクラスタを再作成する必要がなくなります。

クラスタのデータを非アクティブ化、再アクティブ化、および回復するには、`central-config-admin` ロールが必要です。

回復されない (手動で復元する必要がある) データには、次のものが含まれます。

- `cnr.conf` ファイルの内容 ([cnr.conf ファイルの変更 \(210 ページ\)](#) を参照)
- Web UI 構成ファイル
- 保護されていない DNS リソース レコード
- 管理者アカウント



注 ローカルシークレット db が失われた場合、古い参照は復元されても無効です。パスワードを回復するには、管理者の中央管理を使用してから、それらをローカルクラスタにプッシュする必要があります。ローカルクラスタ パートナー オブジェクトの場合、[リージョンから同期 (sync from regional)] を実行すると、有効なオブジェクトが作成されますが、古いクラスタ オブジェクトを削除しておかなければならない場合があります。

- リース履歴
- 拡張スクリプト



(注) データを別の IP アドレスに復元するには、DHCP フェールオーバー サーバー ペアや高可用性 (HA) DNS サーバー ペア アドレスなど、手動での再設定が必要です。

リージョン Web UI

クラスタの [非アクティブ化 (Deactivate)] ボタンをクリックして、クラスタを非アクティブします。これにより、ボタンはすぐに [再アクティブ化 (Reactivate)] に変わり、クラスタのステータスが表示されます。クラスタを非アクティブ化すると、データの削除、同期、複製、および DHCP 使用率とリース履歴のポーリングが無効化されます。これらの操作は、クラスタが非アクティブになっている間は使用できません。

クラスタを非アクティブにすると、クラスタの [データの回復 (Recover Data)] 列に [回復 (Recover)] アイコンが表示されます。レプリカ データを回復するには、このアイコンをクリックします。これにより、個別の進行中ステータスウィンドウが開き、リカバリの進行中は Web UI ページでの操作ができなくなります。リカバリが成功するとすぐに、無効になっていた機能が再び有効になり、使用可能になります。

クラスタを再アクティブ化するには、[再アクティブ化 (Reactivate)] ボタンをクリックします。ボタンが [非アクティブ化 (Deactivate)] に戻り、ステータスがアクティブとして表示されます。

CLI コマンド

次のクラスタ コマンドは、リージョン クラスタに接続されている場合にのみ使用できます。

表 9: クラスタ コマンド

操作	コマンド
アクティブ化	<code>cluster name activate</code>

操作	コマンド
非アクティブ化	cluster name deactivate
再同期	cluster name resynchronize
同期	cluster name sync
レプリカ データの更新	cluster name updateReplicaData
レプリカ データの削除	cluster name removeReplicaData
データの回復	cluster name recoverData
リース履歴のポーリング	cluster name pollLeaseHistory
リース履歴状態の取得	cluster name getLeaseHistoryState
サブネット使用率のポーリング	cluster name pollSubnetUtilization
レプリカ データの表示	cluster name viewReplicaData < class-name cli-command > [-listbrief -listcsv]

クラスタ レポートの表示

リージョン Web UI の [クラスタ レポート (Cluster Report)] ページには、選択したクラスタの関連情報がグラフィカル/チャートベースで表示されます。これにより、クラスタ固有のデータをリージョン クラスタから簡単にモニターおよび視覚化できます。このレポート ページには、クラスタ接続のステータス (接続済み、未接続など) が表示されます。また、クラスタでライセンス付与されているサービスのステータス (DHCP がアップ、DNS がダウンなど)、サーバーの概要、システム メトリック、DNS/CDNS のトップ名、およびリソースの概要も表示されます。

クラスタ レポートを表示するには、次の手順を実行します。

リージョン Web UI

- ステップ 1** [操作 (Operate)] メニューから [サーバー (Servers)] サブメニューの [クラスタの管理 (Manage Clusters)] を選択して、[リモート クラスタの一覧表示/追加 (List/Add Remote Clusters)] ページを開きます。
- ステップ 2** 左のペインのクラスタの名前をクリックします。
- ステップ 3** [リモート クラスタの編集 (Edit Remote Cluster)] ページの [クラスタ レポート (Cluster Report)] タブをクリックします。選択したクラスタに関連する情報が表示されます。クラスタの現在のシステムおよびリソース メトリックは、チャート/表の形式で表示されます。チャートの下にある [表示 (Show)] アイコン

(Show ▼) を使用すると、データがチャートまたは表形式で表示されます。また、[チャートタイプ (Chart Type)] アイコン () を使用すると、チャートのタイプを変更できます。使用可能なチャートのタイプは、縦棒グラフ、折れ線グラフ、面グラフ、および散布図です。

中央構成管理サーバー

ローカルクラスタとリージョンクラスタの CCM サーバーは、Cisco Prime Network Registrar の動作とユーザー インターフェイスのインフラストラクチャを提供します。CCM サーバーは、Cisco PrimeNetwork Registrarデータベース (CCMDB) の読み取り、書き込み、および変更を行います。CCM サーバーの主な目的は、ユーザーからプロトコルサーバー、およびサーバーからユーザーにデータを保存して伝搬することです。

変更セットは、データストアに対する変更の基本単位です。これは、複製サーバーに差分変更を送信し、データストアに対する変更の監査ログを提供します。変更セットは、単一のネットワークオブジェクトに対する1つ以上の変更のグループである変更エントリのリストで構成されます。Web UI には、各データストアの変更セットのビューが表示されます。

CCM サーバーの管理

ログと起動ログを表示できます。サーバー属性を編集できます。

ログと起動ログを表示するには、ローカルクラスタ Web UI の **Operate** メニューから、[サーバー (Servers)] サブメニューの [サーバーの管理 (Manage Servers)] を選択して、[サーバーの管理 (Manage Servers)] ページを開きます。次の表で説明するように、CCM サーバーの *log-settings* 属性を使用して、必要なログカテゴリを有効または無効にします。ログカテゴリは、情報メッセージにのみ適用されます。エラーおよび警告レベルのログメッセージは、常にログファイルに書き込まれます。

表 10: CCM ログ設定

ログ設定 (数値同等)	説明
all (0)	サーバーに、すべてのカテゴリのメッセージをログに記録させます。この設定はデフォルトでイネーブルになっています。
authentication (2)	サーバーに、ユーザーまたはトークンセッション認証中のメッセージをログに記録させます。
database (1)	サーバーに、シャドウバックアップなどのデータベース操作に関するメッセージをログに記録させます。

ログ設定 (数値同等)	説明
dnssec (9)	サーバーに、DNSSEC 処理関連のメッセージをログに記録させます。DNSSEC キーが CCM サーバーによって作成、削除、有効化、無効化、またはロールオーバーされると、メッセージがログに記録されます。また、サーバーに、ゾーンで DNSSEC が無効になったときやゾーンに署名または再署名するタスクがスケジュールされたときにメッセージをログに記録させます。
lease-history (10)	サーバーに、リース履歴ポーリングが開始されたときや終了したときにメッセージをログを記録させます。
licensing (5)	サーバーに、ローカルクラスタ登録に関するメッセージや、リージョンおよびローカルクラスタのライセンス使用状況が収集またはレポートされたときにメッセージをログに記録させます。
replica (7)	サーバーに、レプリカポーリングが開始されたときやローカルクラスタが正常に復元されたときにメッセージをログに記録させます。
scheduled-tasks (4)	サーバーに、CCM サーバーがタスクをスケジュールしたときやスケジュールされたタスクが完了したときにメッセージをログに記録させます。
scp-details (3)	サーバーに、SCP メッセージ応答や CCM と他のサーバーの間の内部 SCP 通信をログに記録させます。CLI や Web UI からの通信などの外部 SCP 要求は、常にログに記録されます。
server-events (6)	サーバーに、プロトコルサーバーから CCM サーバーに送信されたすべてのサーバーイベント (SNMP トラップに関するイベントなど) をログに記録させます。
utilization (8)	サーバーに、使用率ポーリングが開始されたときや終了したときにメッセージをログに記録させます。

CCM サーバーのプロパティの編集

[CCM サーバーの編集 (Edit CCM Server)] ページを使用して、CCM サーバーのプロパティを編集できます。

ローカルおよびリージョン Web UI

ステップ 1 CCM サーバーのプロパティにアクセスするには、**Operate** メニューから [管理 (Manage) Servers] を選択して、[サーバーの管理 (Manage Servers)] ページを開きます。

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

ステップ3 必要に応じて設定を変更します。

ステップ4 **Save** をクリックして、CCM サーバー属性の変更を保存します。

トリビアル ファイル転送

Trivial File Transfer Protocol (TFTP) は、コネクションレス型トランスポート層プロトコルであるユーザー データグラム プロトコル (UDP) を使用して、ネットワーク経由でファイルを転送する方法です。Cisco Prime Network Registrar は TFTP サーバーを保持しているため、システムは Data Over Cable Service Interface Specification (DOCSIS) 規格に準拠したケーブル モデムにデバイスプロビジョニングファイルを提供できます。TFTP サーバーは、ファイルをモデムに送信する際に、DOCSIS ファイルをローカルメモリにバッファします。TFTP 転送の後、サーバーはローカルメモリからファイルをフラッシュします。TFTP は、非 DOCSIS コンフィギュレーション ファイルもサポートしています。

Cisco Prime Network Registrar TFTP サーバーの機能の一部を次に示します。

- RFC 1123、1350、1782、および 1783 に準拠
- 高性能なマルチスレッドアーキテクチャを含む
- IPv6 をサポートします。
- パフォーマンス強化のためにデータをキャッシュ
- 設定および制御可能
- 柔軟なパスとファイルアクセス制御を含む
- TFTP 接続とファイル転送の監査ロギングを含む
- Cisco Prime Network Registrar の *install-path/data/tftp* にデフォルトのルートディレクトリがある

関連項目

[TFTP サーバーの表示と編集 \(117 ページ\)](#)

[TFTP サーバー ネットワーク インターフェ이스の管理 \(118 ページ\)](#)

TFTP サーバーの表示と編集

ローカル クラスタで、TFTP サーバーを編集して属性を変更できます。ccm-admin ロールの server-management サブロールが割り当てられている必要があります。

ローカル基本または詳細 Web UI

- ステップ 1 Operate** メニューから、**Servers** サブメニューの **Manage Servers** を選択して、[サーバーの管理 (Manage Servers)] ページを開きます ([サーバーの管理 \(175 ページ\)](#) を参照)。
- ステップ 2** 左側のペインの [ローカル TFTP サーバー (Local TFTP Server)] リンクをクリックして、[ローカル TFTP サーバーの編集 (Edit Local TFTP Server)] ページを開きます。
- 任意の属性の名前をクリックすると、その属性の説明ウィンドウを開くことができます。
- ステップ 3** 属性値を設定解除するには、[Unset?] 列のチェックボックスをオンにします。
- ステップ 4** 変更内容を保存するには **Save** をクリックし、変更をキャンセルには **Revert** をクリックします。

CLI コマンド

属性値を表示するには、**tftp show** を使用します。属性を設定または有効にするには、**tftp set attribute=value [attribute=value ...]** または **tftp enable attribute** を使用します。また、**tftp serverLogs show** および **tftp serverLogs nlogs=number logsize=size** を使用することもできます。

TFTP サーバー ネットワーク インターフェイスの管理

TFTP サーバーのネットワーク インターフェイスを管理できます。

ローカル詳細 Web UI

TFTP サーバーに関連付けられているネットワーク インターフェイスを管理するには、[サーバーの管理 (Manage Servers)] ページで、選択したローカル TFTP サーバーの **Network Interfaces** タブをクリックします。デフォルトで設定されているネットワーク インターフェイスを表示し、追加のネットワーク インターフェイス作成して編集することができます。作成して編集するには、**ccm-admin** ロールの **server-management** サブロールが割り当てられている必要があります。

[ネットワーク インターフェイス (Network Interfaces)] ページの列は、次のとおりです。

- **Name-** LAN アダプタ、ループバック、ファストイーサネット インターフェイスなど、ネットワーク インターフェイスの名前。名前が [Configured Interfaces] 列にある場合、そのインターフェイスを編集および削除できます。名前をクリックすると、[TFTP サーバー ネットワーク インターフェイスの編集 (Edit TFTP Server Network Interface)] ページが開き、インターフェイスの名前とアドレスを編集できます。変更を加えてから、このページの **Save** をクリックします。
- **IP Address-** ネットワーク インターフェイスの IP アドレス。
- **IPv6 Address-** ネットワーク インターフェイスの IPv6 アドレス (該当する場合)。
- **Flags-** インターフェイスがゼロブロードキャスト、仮想、v4、v6、非マルチキャスト、または受信専用のいずれであるかを示すフラグ。

- **Configure** - 新しいネットワーク インターフェイスを設定するには、インターフェイス名の横にある [設定 (Configure)] アイコンをクリックします。これにより、選択したインターフェイスに基づきますが、より一般的な IP アドレスを持つ別のインターフェイスが作成され、この TFTP サーバーの設定済みインターフェイスに追加されます。
- **List of available interfaces for this TFTP server** - ユーザー設定のネットワーク インターフェイス。それぞれの名前と関連付けられたアドレスが表示されます。インターフェイス名をクリックして編集するか、[削除 (Delete)] アイコンをクリックして削除します。

サーバーの管理に戻るには、**Revert** をクリックします。

CLI コマンド

tftp-interface コマンドを使用します。

簡易ネットワーク管理

Cisco Prime Network Registrar Simple Network Management Protocol (SNMP) 通知サポートを使用すると、DHCP および DNS カウンタを照会し、エラー条件と DNS および DHCP サーバーに関する問題の警告を受け、障害または差し迫った障害の条件を示す可能性のあるしきい値条件をモニターすることができます。

Cisco Prime Network Registrar は、SNMPv2c 標準に従って SNMP トラッププロトコルデータユニット (PDU) を実装します。各トラップ PDU には、次のものが含まれます。

- 汎用通知コード (企業固有の場合)。
- 発生したイベントまたはしきい値の超過を示すコードを含む特定通知フィールド。
- 特定のイベントに関する追加情報を含む変数バインディング フィールド。

詳細については、管理情報ベース (MIB) を参照してください。SNMP サーバーは、MIB 属性の読み取りのみをサポートしています。属性への書き込みはサポートされていません。

次の MIB ファイルが必要です。

- **Traps** - CISCO-NETWORK-REGISTRAR-MIB.my および CISCO-EPM-NOTIFICATION-MIB.my
- **DNS server** - CISCO-DNS-SERVER-MIB.my



注 キャッシング DNS サーバーは、動作するときに DNS MIB のサブセットのみを必要とします。キャッシング DNS サーバーは、*server-start* および *server-stop* 通知イベントのみをサポートします。

- **DHCPv4 server** - CISCO-IETF-DHCP-SERVER-MIB.my
- **DHCPv4 server capability** - CISCO-IETF-DHCP-SERVER-CAPABILITY.my

- **DHCPv4 server extensions** - CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- **DHCPv4 server extensions capability** - CISCO-IETF-DHCP-SERVER-EXT-CAPABILITY.my
- **DHCPv6 server** - CISCO-NETREG-DHCPV6-MIB.my (試験的)



(注) この MIB、CISCO-NETREG-DHCPV6-MIB は、新しい DHCP v6 関連の統計および新しい DHCP v6 トラップのクエリをサポートするために定義されています。

これらの MIB ファイルは、Cisco Prime Network Registrar インストールパスの /misc ディレクトリにあります。

次の URL には、試験的な CISCO-NETREG-DHCPV6-MIB.my ファイルを除くすべてのファイルが含まれています。

<ftp://ftp.cisco.com/pub/mibs/supportlists/cnr/cnr-supportlist.html>

次の依存関係ファイルも必要です。

- **Dependency for DHCPv4 and DHCPv6**- CISCO-SMI.my
- **Additional dependencies for DHCPv6**- INET-ADDRESS-MIB.my

これらの依存関係ファイルは、次の URL にあるすべての MIB ファイルとともに使用できます。

<ftp://ftp.cisco.com/pub/mibs/v2/>

MIB 属性のオブジェクト識別子 (OID) を取得するには、次の URL にある同等の名前の .OID ファイルに移動します。

<ftp://ftp.cisco.com/pub/mibs/oid/>

SNMP サーバーのセットアップ

SNMP サーバーへのクエリを実行するには、サーバーのプロパティをセットアップする必要があります。

ローカルおよびリージョン Web UI

- ステップ 1** [操作 (Operate)] メニューから **Servers** サブメニューの **Manage Servers** を選択して、[サーバーの管理 (Manage Servers)] ページを開きます ([サーバーの管理 \(175 ページ\)](#) を参照)。
- ステップ 2** [ローカル SNMP サーバー (Local SNMP Server)] リンクをクリックして、[ローカル SNMP サーバーの編集 (Edit Local SNMP Server)] ページを開きます。
- ステップ 3** *Community string* 属性は、サーバーにアクセスするためのパスワードです。(コミュニティ文字列は、読み取り専用のコミュニティ文字列です)。プリセット値は **public** です。
- ステップ 4** [ログ設定 (Log Settings)]、[その他のオプションと設定 (Miscellaneous Options and Settings)]、および [詳細オプションと設定 (Advanced Options and Settings)] を指定できます。

- **trap-source-addr**- 発信トラップに使用するオプションの送信者アドレス。
- **trap-source-ip6address**- 発信トラップに使用するオプションの送信元 IPv6 アドレス。
- **server-active**- SNMP サーバーがクエリーに対してアクティブであるかどうかを決定します。デフォルト値は `true` です。 `false` に設定すると、サーバーは実行されますが、クエリーにはアクセスできず、トラップは送信されません。
- **cache-ttl**- SNMP キャッシュがクエリーに応答する時間を決めます。デフォルトは 60 秒です。

ステップ 5 SNMP サーバー インターフェイスを管理するには、詳細モードで、**Network Interfaces** タブをクリックします。デフォルトで設定されているネットワーク インターフェイスを表示し、追加のネットワーク インターフェイス作成して編集することができます。作成して編集するには、`ccm-admin` ロールの `server-management` サブロールが割り当てられている必要があります。インターフェイスのプロパティは、TFTP サーバーのプロパティと同様です ([TFTP サーバー ネットワーク インターフェイスの管理 \(118 ページ\)](#) を参照)。

ステップ 6 サーバーのトラップ受信者を管理するには、次のようにします。

- a) **Trap Recipients** タブをクリックします。
- b) トラップ受信者の名前を入力します。
- c) トラップ受信者の IPv4 アドレスまたは IPv6 アドレスを入力します。
- d) **Add Trap Recipient** をクリックします。
- e) 追加のトラップ受信者ごとに繰り返します。
- f) トラップ受信者のポート、コミュニティ文字列、およびエージェントアドレスを設定するには、[トラップ受信者 (Trap Recipients)] タブで名前をクリックして、[トラップ受信者の編集 (Edit Trap Recipient)] ページを開き、値を設定します。

ステップ 7 SNMP サーバーの設定を完了するには、**Save** をクリックします。

CLI コマンド

SNMP サーバーにアクセスできるように CLI でコミュニティ文字列を設定するには、`snmp set community=name` を使用します。トラップ送信元 IPv4 アドレスを設定するには、`snmp set trap-source-addr=value` を使用します。トラップ送信元 IPv6 アドレスを設定するには、`snmp set trap-source-ip6address=value` を使用します。SNMP サーバーを非アクティブにするには `snmp disable server-active` を使用し、キャッシュの存続可能時間を設定するには `snmp set cache-ttl=time` を使用します。

トラップ受信者を設定するには、`trap-recipient name set attribute=value [attribute=value ...]` を使用します。次に例を示します。

```
nrcmd> trap-recipient example-recipient set ip-addr=192.168.0.34
nrcmd> trap-recipient example-recipient set ip6address=2001:4f8:ffff:0:8125:ef1b:bdcb:4b4e
```

トラップ受信者の `agent-address`、`community`、および `port-number` の値を追加することもできます。

その他の SNMP 関連のコマンドとしては、起動時にサーバーを実行しないようにする **snmp disable server-active** と、インターフェイスを設定する **snmp-interface** コマンドがあります。**addr-trap** コマンドについては、[TFTP サーバー ネットワーク インターフェイスの管理 \(118 ページ\)](#) で説明しています。

通知の仕組み

Cisco Prime Network Registrar SNMP 通知サポートにより、標準の SNMP 管理ステーションは DHCP サーバーと DNS サーバーから通知メッセージを受信できます。これらのメッセージには、SNMP トラップをトリガーしたイベントの詳細が含まれています。

Cisco Prime Network Registrar は、アプリケーションコードが検出して信号を送信した事前定義イベントに応じて通知を生成します。各イベントは、特定のパラメータのセットまたは現在の値のセットとともに伝送することもできます。たとえば、*free-address-low-threshold* イベントは、10%未使用の値の範囲内で発生する可能性があります。そのようなイベントでは、他の範囲と値も可能であり、各タイプのイベントには異なるパラメータが関連付けられています。

次の表では、通知を生成するイベントについて説明します。

表 11: SNMP 通知イベント

イベント	通知
別の DHCP サーバーとのアドレス競合が検出された (<i>address-conflict</i>)	アドレスが別の DHCP サーバーと競合しています。
DNS キューが満杯 (<i>dns-queue-size</i>)	DHCP サーバーの DNS キューがいっぱいになり、DHCP サーバーが要求の処理を停止します。(これは、通常、まれな内部条件です)。
重複する IP アドレスが検出された (<i>duplicate-address</i> と <i>duplicate-address6</i>)	重複する IPv4 または IPv6 アドレスが発生しています。
重複する IPv6 プレフィックスが検出された (<i>duplicate-prefix6</i>)	重複する IPv6 プレフィックスが発生しています。
フェールオーバー設定の不一致 (<i>failover-config-error</i>)	DHCP フェールオーバー設定がパートナー間で一致しません。
未使用アドレスしきい値 (<i>free-address-low</i> と <i>free-address-high</i> 、または <i>free-address6-low</i> と <i>free-address6-high</i>)	IPv4 または IPv6 の空きアドレスの数が上限しきい値を超えたときには high トラップ。または、以前に high トラップをトリガーした後に、空きアドレスの数が下限しきい値を下回ったときには low トラップ。
高可用性 (HA) DNS 設定の不一致 (<i>ha-dns-config-error</i>)	HA DNS 設定がパートナー間で一致しません。

イベント	通知
HA DNS パートナーが応答していない (<i>ha-dns-partner-down</i>)	HA DNS パートナーが DNS サーバーへの応答を停止しています。
HA DNS パートナーが応答 (<i>ha-dns-partner-up</i>)	HA DNS パートナーが、無応答の後、応答しています。
DNS マスターが応答しない (<i>masters-not-responding</i>)	マスター DNS サーバーが DNS サーバーへの応答を停止しています。
DNS マスターが応答 (<i>masters-responding</i>)	マスター DNS サーバーが、無応答の後、応答しています。
他のサーバーが応答していない (<i>other-server-down</i>)	DHCP フェールオーバー パートナー、または DNS または LDAP サーバーが、DHCP サーバーへの応答を停止しています。
他のサーバーが応答 (<i>other-server-up</i>)	DHCP フェールオーバー パートナー、または DNS または LDAP サーバーが、無応答の後、応答しています。
DNS セカンダリ ゾーン期限切れ (<i>secondary-zone-expired</i>)	DNS セカンダリ サーバーは、ゾーン転送中にクエリに応答するときに、ゾーンデータの権限を要求できなくなります。
サーバーの起動 (<i>server-start</i>)	DHCP または DNS サーバーが起動または再初期化されました。
サーバー停止 (<i>server-stop</i>)	DHCP または DNS サーバーが停止しています。

リソース モニターリング SNMP 通知

SNMP トラップがリソース制限アラームに対して有効になっている場合、Cisco Prime Network Registrar は、モニター対象のリソースがクリティカルレベルまたは警告レベルを超えたときに SNMP トラップを生成します。SNMP トラップは、次のリソース制限について生成されます。

- リソースの値が警告またはクリティカル限界を超えたとき（これらは、値がいずれかのしきい値を超えている限り、定期的送信されます）。
- リソースの値が警告限界より下のレベルに戻ったとき。

SNMP サーバーは、CISCO-EPM-NOTIFICATION MIB を使用してトラップを生成します。マッピングは、次のとおりです。

表 12: CISCO-EPM-NOTIFICATION-MIB トラップ属性のマッピング

トラップ属性名	オブジェクト ID	タイプ	リソースイベントの値
cenAlarmVersion	1.3.6.1.4.1.99.311.1.1.2.1.2	SnmpAdminString (SIZE(1..16))	"1.2"
cenAlarmTimestamp	1.3.6.1.4.1.99.311.1.1.2.1.3	タイムスタンプ	リソースイベント状態の最終変更時刻
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.99.311.1.1.2.1.4	タイムスタンプ	現在の時刻
cenAlarmInstanceID	1.3.6.1.4.1.99.311.1.1.2.1.5	SnmpAdminString (SIZE(1..20))	イベントの一意 ID - 16 進数のみ
cenAlarmStatus	1.3.6.1.4.1.99.311.1.1.2.1.6	Integer32 (1..250)	1 (確認応答されなかった場合)
cenAlarmStatusDefinition	1.3.6.1.4.1.99.311.1.1.2.1.7	SnmpAdminString (SIZE(1..255))	"1,Not acknowledged"
cenAlarmType	1.3.6.1.4.1.99.311.1.1.2.1.8	整数	未使用
cenAlarmCategory	1.3.6.1.4.1.99.311.1.1.2.1.9	Integer32 (1..250)	100 (Raw アラームの場合)
cenAlarmCategoryDefinition	1.3.6.1.4.1.99.311.1.1.2.1.10	SnmpAdminString (SIZE(1..255))	"100,Raw alarm"
cenAlarmServerAddressType	1.3.6.1.4.1.99.311.1.1.2.1.11	InetAddressType	クラスタサーバーアドレスタイプ - IPv4 (1) または IPv6 (2)
cenAlarmServerAddress	1.3.6.1.4.1.99.311.1.1.2.1.12	InetAddress	クラスタアドレス (ローカルクラスタのオブジェクトに基づく)
cenAlarmManagedObjectClass	1.3.6.1.4.1.99.311.1.1.2.1.13	SnmpAdminString (SIZE(1..255))	アプリケーション
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.99.311.1.1.2.1.14	InetAddressType	未使用
cenAlarmManagedObjectAddress	1.3.6.1.4.1.99.311.1.1.2.1.15	InetAddress	未使用
cenAlarmDescription	1.3.6.1.4.1.99.311.1.1.2.1.16	OctetString (SIZE(1..1024))	","と書式化された説明

トラップ属性名	オブジェクト ID	タイプ	リソースイベントの値
cenAlarmSeverity	1.3.6.1.4.1.99311.1.1.2.1.17	Integer32	クリアの場合は 0、警告の場合は 2、クリティカルの場合は 5
cenAlarmSeverityDefinition	1.3.6.1.4.1.99311.1.1.2.1.18	SnmpAdminString (SIZE(1..255))	文字列アラームの重大度、"0,Clear"、"2,Warning"、または "5,Critical" のいずれか
cenAlarmTriageValue	1.3.6.1.4.1.99311.1.1.2.1.19	Integer32 (0..100)	未使用
cenEventIDList	1.3.6.1.4.1.99311.1.1.2.1.20	OctetString (SIZE(1..1024))	未使用
cenUserMessage1	1.3.6.1.4.1.99311.1.1.2.1.21	SnmpAdminString (SIZE(1..255))	モニター対象リソースの名前
cenUserMessage2	1.3.6.1.4.1.99311.1.1.2.1.22	SnmpAdminString (SIZE(1..255))	サーバー名 (dhcp、dns、cdns、...)
cenUserMessage3	1.3.6.1.4.1.99311.1.1.2.1.23	SnmpAdminString (SIZE(1..255))	"Network Registrar"
cenAlarmMode	1.3.6.1.4.1.99311.1.1.2.1.24	整数	3 (イベント)
cenPartitionNumber	1.3.6.1.4.1.99311.1.1.2.1.25	Gauge (0..100)	未使用
cenPartitionName	1.3.6.1.4.1.99311.1.1.2.1.26	SnmpAdminString (SIZE(1..255))	未使用
cenCustomerIdentification	1.3.6.1.4.1.99311.1.1.2.1.27	SnmpAdminString (SIZE(1..255))	未使用
cenCustomerRevision	1.3.6.1.4.1.99311.1.1.2.1.28	SnmpAdminString (SIZE(1..255))	未使用
cenAlertID	1.3.6.1.4.1.99311.1.1.2.1.29	SnmpAdminString (SIZE(1..255))	cenAlarmInstanceID

リソース制限アラームの詳細については、[リソース制限アラームのモニターリング \(147 ページ\)](#) を参照してください。

SNMP 通知イベントの処理

Cisco Prime Network Registrar が通知を生成すると、通知の 1 つのコピーを各受信者に SNMP トラップ PDU として送信します。すべてのイベント（およびスコープまたはプレフィックス）は、受信者とその他の通知設定データのリストを共有し、通知を初期化すると、サーバーはそれらを読み取ります。

SNMP 属性は、次の 3 つの方法で設定できます。

- DHCP サーバーの場合、スコープまたはプレフィックス（またはそれらのテンプレート）のトラップを特に設定していない場合、デフォルトの未使用アドレストラップ設定を有効にするトラップを含みます。
- *free-address-config* 属性を設定することによって、スコープまたはプレフィックス（またはそのテンプレート）レベルで。
- DNS サーバーの場合、*traps-enabled* 設定が含まれます。

SNMP 通知を使用するには、トラップ通知を送信する場所を示すトラップ受信者を指定する必要があります。デフォルトでは、すべての通知が有効になっていますが、明示的に受信者を定義する必要があります。そうでない場合、通知は送信されません。使用する IP アドレスは、多くの場合、**localhost** です。

DHCP サーバーは特別なトラップ設定を提供します。これにより、特に DHCPv4 および DHCPv6 の空きアドレスに関する通知を送信できるようになります。トラップ設定名、モード、低しきい値および高しきい値のパーセンテージを設定できます。モードによって、スコープが空きアドレス レベルを集約する方法が決まります。

DHCP v4 通知

DHCPv4 のモードとしきい値は、次のとおりです（[非アクティブ化されたスコープまたはプレフィックスの処理 \(127 ページ\)](#) も参照）。

- **scopemode**—各スコープが独自の空きアドレス レベルを個別に追跡します（デフォルト）。
- **network mode** - このトラップ設定で設定されたすべてのスコープが（スコープまたはスコープテンプレートの *free-address-config* 属性を通じて）、同じ *primary-subnet* を共有する場合、空きアドレス レベルを集約します。
- **selection-tags mode** - スコープがプライマリ サブネットを共有し、一致する選択タグ値のリストを持つ場合、空きアドレス レベルを集約します。
- **low-threshold**- DHCP サーバーが低しきい値トラップを生成し、高しきい値を再度有効にする空きアドレスのパーセンテージ。スコープの空きアドレス レベルは、次の計算です。

```
100 * available-nonreserved-leases
total-configured-leases
```

- **high-threshold**- DHCP サーバーが高しきい値トラップを生成し、低しきい値を再度有効にする空きアドレスのパーセンテージ。

DHCP v6 通知

DHCPv6のモードとしきい値は、次のとおりです（[非アクティブ化されたスコープまたはプレフィックスの処理](#)（127 ページ）も参照）。

- **prefix mode** - 各プレフィックスが独自の空きアドレス レベルを個別に追跡します。
- **link mode** - すべてのプレフィックスが同じリンクを共有している場合、リンクに設定されているすべてのプレフィックスが独自の空きアドレス レベルを集約します。
- **v6-selection-tags mode** - プレフィックスがリンクを共有し、一致する選択タグ値のリストを持つ場合、プレフィックスは空きアドレス レベルを集約します。
- **low-threshold** - DHCP サーバーが低しきい値トラップを生成し、高しきい値を再度有効にする空きアドレスのパーセンテージ。プレフィックスの空きアドレスレベルは、次の計算になります。

```
100 * max-leases - dynamic-leases  
max-leases
```
- **high-threshold** - DHCP サーバーが高しきい値トラップを生成し、低しきい値を再度有効にする空きアドレスのパーセンテージ。

非アクティブ化されたスコープまたはプレフィックスの処理

非アクティブ化されたスコープまたはプレフィックスは、そのカウンタを他のスコープまたはプレフィックスと集約しません。たとえば、プレフィックスを **link** または **v6-selection-tags** トラップモードで設定し、その後、プレフィックスを非アクティブにすると、そのカウンタは集約の合計カウントから消えます。非アクティブ化されたプレフィックスのリースに対する変更は、集約合計には適用されません。

したがって、非アクティブ化されたスコープまたはプレフィックスのクライアントを検出するには、イベント モードを **scope** または **prefix** に設定する必要があり、いずれかの集約モード（**network**、**selection-tags**、**link**、または **v6-selection-tags**）には設定しないでください。

たとえば、非アクティブ化されたプレフィックスに対してトラップを設定する使用事例は、ネットワーク番号の再設定です。この場合、新しいプレフィックス（集約として、すべてのクライアントに十分な領域があることを確認します）と古いプレフィックスの両方をモニターして、リースが解放されるようにする必要があります場合があります。また、古いプレフィックスの上限しきい値を 90% または 95% に設定して、ほとんどのアドレスが解放されたときにトラップが発生するようにすることもできます。

ローカルの基本または詳細 *Web UI*

DHCP サーバーの SNMP 属性にアクセスするには、**Operate** メニューから **Manage Servers** を選択し、左側のペインの **Local DHCP Server** をクリックします。[DHCP サーバーの編集 (Edit DHCP Server)] ページの [SNMP 設定]（基本モード）または [SNMP 設定]（詳細モード）で、SNMP 属性を確認できます。

4 つの *lease-enabled* 値（`free-address6-low`、`free-address6-high`、`duplicate-address6`、`duplicate-prefix6`）は DHCPv6 のみに関係します。トラップをイネーブルにするとともに、デ

フォルトの free-address トラップ設定を名前で指定でき、明示的に設定されていないすべてのスコープとプレフィックスまたはリンクに影響します。

トラップ設定を追加するには、次の手順を実行します。

-
- ステップ 1 詳細モードで、**Deploy** メニューから **[DHCP]** サブメニューの **Traps** を選択して、DHCP トラップ設定にアクセスします。[トラップ設定の一覧表示/追加 (List/Add Trap Configurations)] ページが表示されます。
 - ステップ 2 左側のペインの **[トラップの追加 (Add Trap)]** アイコンをクリックして、[AddrTrapConfig の追加 (Add AddrTrapConfig)] ページを開きます。
 - ステップ 3 名前、モード、およびしきい値のパーセンテージを入力して、**Add AddrTrapConfig** をクリックします。
-

トラップ設定の編集

トラップ設定を編集するには、次の手順を実行します。

-
- ステップ 1 [トラップ (Traps)] ペインで目的のトラップ名をクリックして、[トラップ設定の編集 (Edit Trap Configuration)] ページを開きます。
 - ステップ 2 名前、モード、またはしきい値の割合を変更します。
 - ステップ 3 [enabled] 属性の **on** オプションをクリックして、トラップ設定を有効にします。
 - ステップ 4 **Save** をクリックして、変更を有効にします。
-

トラップ設定の削除

トラップ構成を削除するには、[トラップ (Traps)] ペインでトラップを選択し、[削除 (Delete)] アイコンをクリックして、削除を確定またはキャンセルします。

リージョンの基本または詳細 *Web UI*

リージョン Web UI では、ローカル Web UI と同様にトラップ構成を追加および編集できます。また、[トラップ構成のリスト/追加 (List/Add Trap Configurations)] ページで、レプリカトラップ構成をプルしたり、トラップ構成をローカルクラスタにプッシュしたりすることもできます。

サーバーのアップ/ダウン トラップ

すべてのダウン トラップには、対応するアップ トラップが続く必要があります。ただし、このルールは、次のシナリオでは厳密には適用されません。

1. フェールオーバー パートナーまたは LDAP サーバーまたは DNS サーバーまたは HA DNS パートナーが長時間ダウンしている場合は、ダウン トラップが定期的に発行されます。アップ トラップは、そのサーバーまたはパートナーがサービスに戻るときにのみ生成されます。

2. DHCPまたはDNSサーバーがリロードまたは再起動されると、パートナーまたは関連するサーバーの以前の状態は保持されず、重複するダウンまたはアップトラップが発生する可能性があります。



(注) 他のフェールオーバー パートナーまたは LDAP サーバーまたは DNS サーバーまたは HA DNS パートナーのアップまたはダウントラップは、そのパートナーまたはサーバーと通信するためにのみ発生します。そのため、他のパートナーまたはサーバーがダウンしたり、サービスに戻ったりしたときには、発生しない可能性があります。

CLI コマンド

ローカルクラスタでDHCPサーバーのトラップ値を設定するには、`dhcp set traps-enabled=value`を使用します。また、`default-free-address-config` 属性をトラップ設定に設定することもできます。次に例を示します。

```
nrcmd> dhcp set traps-enabled=server-start,server-stop,free-address-low,free-address-high
```

```
nrcmd> dhcp set default-free-address-config=v4-trap-config
```



(注) `default-free-address-config` (または IPv6 の場合は `v6-default-free-address-config`) を定義しなかった場合、Cisco Prime Network Registrar は、`default-aggregation-addr-trap-config` という名前の内部の非リストトラップ設定を作成します。このため、作成したトラップ設定にその名前を使用しないようにしてください。

DHCPv4 および DHCPv6 のトラップ設定を定義するには、設定の `addr-trap` 名前 `create` の後に属性=値のペアを続けて使用します。次に例を示します。

```
nrcmd> addr-trap v4-trap-conf create mode=scope low-threshold=25% high-threshold=30%
```

```
nrcmd> addr-trap v6-trap-conf create mode=prefix low-threshold=20% high-threshold=25%
```

地域クラスタに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再利用の場合は、クラスタのリストまたは「すべて」を指定できます。

- アドルトラップ<名前|すべて>プル<確認する |置き換える|正確な>クラスタ名[-レポートのみ|-レポート]
- アドルトラップ<名前|すべて>プッシュ<確認する |置き換える|正確な>クラスタリスト[-レポートのみ|-レポート]
- 追加トラップ名再利用クラスタリスト[-レポートのみ|-レポート]

SNMP クエリの処理

SNMP クライアントアプリケーションを使用して、次の MIB を照会できます。

- CISCO-DNS-SERVER-MIB.my
- CISCO-IETF-DHCP-SERVER-MIB.my
- CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- CISCO-NETREG-DHCPV6-MIB.my (試験的)

SNMP サーバーは、これらの MIB のいずれかで定義されている属性のクエリを受信すると、その属性値を含む応答 PDU を返します。たとえば、(インターネット経由で使用可能な) NET-SNMP クライアントアプリケーションを使用して、次のいずれかのコマンドを使用して、特定のアドレスの DHCPDISCOVER パケットの数を取得できます。

```
C:\net-snm5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39:4444.iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.
ciscoIetfDhcpSrvMIB.ciscoIetfDhcpv4SrvMIBObjects.cDhcpv4Counters.cDhcpv4CountDiscovers
```

```
CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
C:\net-snm5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39:4444
1.3.6.1.4.1.9.10.102.1.3.1
```

```
CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
```

どちらのコマンドも同じ結果を返します。最初のコマンドは完全な MIB 属性名を照会し、2 番目は OID に相当するものを照会します (エラーが発生する可能性が低いです)。前述したように、OID に相当する MIB 属性は、次の URL にある関連ファイルにあります。

<ftp://ftp.cisco.com/pub/mibs/oid/>

たとえば、CISCO-IETF-DHCP-SERVER-MIB.oid ファイルには、前のクエリの例に対応する次の OID 定義が含まれています。

```
"cDhcpv4CountDiscovers" "1.3.6.1.4.1.9.10.102.1.3.1"
```

SNMP クエリのエラー状態には、次のようなものがあります。

- 要求 PDU で送信されたコミュニティ文字列が、設定した内容と一致しません。
- 要求 PDU のバージョンが、サポートされているバージョン (SNMPv2) と同じではありません。
- クエリ対象のオブジェクトのインスタンスがサーバー内にない場合、対応する [変数バインディングタイプ (variable binding type)] フィールドが SNMP_NOSUCHINSTANCE に設定されます。GetNext を使用すると、次の属性がない場合、対応する [変数バインディングタイプ (variable binding type)] フィールドが SNMP_ENDOFMIBVIEW に設定されます。
- OID に一致するものがない場合、対応する [変数バインディングタイプ (variable binding type)] フィールドが SNMP_NOSUCHOBJECT に設定されます。GetNext を使用すると、SNMP_ENDOFMIBVIEW に設定されます。
- 属性のクエリによって返された不正な値がある場合、応答 PDU のエラー ステータスは SNMP_ERR_BAD_VALUE に設定されます。

Cisco Prime Network Registrar SNMP とシステム SNMP の統合

Cisco Prime Network Registrar SNMP サーバーを、それが実行しているシステムの SNMP サーバーに統合できます。統合は、システムが Cisco Prime Network Registrar MIB エントリのクエリに応答する方法で実行できます。NET-SNMP（および互換性のあるサーバー）を使用しているシステムでは、次のエントリを `/etc/snmp/snmpd.conf` コンフィギュレーション ファイルに追加することによって実行されます。

- IPv4 の場合 :

```
view systemview included .1.3.6.1.4.1.9.9
view systemview included .1.3.6.1.4.1.9.10

proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.9
proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.10
```

- IPv6 の場合 :

```
view systemview included .1.3.6.1.4.1.9.9
view systemview included .1.3.6.1.4.1.9.10

proxy -v 2c -c public [::1]:4444 .1.3.6.1.4.1.9.9
proxy -v 2c -c public [::1]:4444 .1.3.6.1.4.1.9.10
```

Cisco Prime Network Registrar SNMP サーバーがこれらの設定について異なる値で構成されている場合は、コミュニティ文字列 **public** とポート番号 **4444** を置き換えなければならない場合があります。

NET-SNMP は、Linux やその他の Unix ライクなシステムで一般に使用可能です。他のシステムでも同様のメカニズムを使用できることがあります。

個人所有デバイスの Web サーバーの持ち込み

リージョン クラスターの BYOD Web サーバーは、Cisco Prime Network Registrar に BYOD 動作のインフラストラクチャを提供します。BYOD Web サーバーの主な目的は、ユーザー所有のデバイスを Cisco Prime Network Registrar に登録することによって、AD に対してユーザーを認証し、デバイスのメタデータを収集することです。

BYOD Web サーバーの管理

ログと起動ログを表示できます。サーバー属性を編集できます。

ログと起動ログを表示するには、リージョン クラスター Web UI の [操作 (Operate)] メニューから [サーバー (Server)] サブメニューの [サーバーの管理 (Manage Servers)] を選択し、[サーバーの管理 (Manage Servers)] ページを開きます。

BYOD Web サーバーのプロパティの編集

BYOD Web サーバーのプロパティを編集するには、[ローカルBYOD Web サーバーの編集 (Edit Local BYOD Web Server)] ページを使用します。

地域の Web UI

ステップ 1 BYOD Web サーバーのプロパティにアクセスするには、[操作 (Operate)] メニューの [サーバーの管理] を選択し、[サーバーの管理 (Manage Servers)] ページを開きます。

ステップ 2 左側の [サーバーの管理 (Manage Servers)] ペインで、**BYOD Web** サーバーをクリックします。[ローカル BYOD Web サーバー (Local BYOD Web Server)] ページが表示されます。このページには、BYOD Web サーバーの属性が表示されます。

- **キーストアの設定** : BYOD Web サーバーの「http コール」を、キーストアファイルとキーストアパスワードの組み合わせを使用して、セキュアな「https」にリダイレクトします。
- **LDAP の設定** : クライアント登録に使用されるリモート LDAP サーバーを指定します。
- **追加属性 (自動起動)** : サーバーエージェントの再起動ごとに BYOD サーバーを自動的に起動するかどうかを示します。

ステップ 3 必要に応じて設定を変更します。

ステップ 4 BYOD Web サーバー属性の変更を保存するには、[保存 (Save)] をクリックします。

ステップ 5 変更を BYOD Web サーバーに適用するには、[サーバーの起動 (Start Server)] または [サーバーの再起動 (Restart Server)] をクリックします。

BYOD のテーマとコンテンツのセットアップ

リージョン クラスターで、BYOD Web サーバー インターフェイスで適用できるコンテンツと複数の BYOD テーマを作成できます。

BYOD テーマの追加とプレビュー

[BYOD テーマ (BYOD Theme)] ページを使用して、リージョン クラスターに独自のテーマを作成し、作成したテーマを BYOD Web サーバーに適用できます。これにより、BYOD インターフェイスのロゴ、背景、フォント、およびその他のプロパティがカスタマイズに従って表示されます。作成したテーマは、BYOD Web サーバーにパブリッシュする前にプレビューできます。

テーマを追加してプレビューするには、次のようにします。

地域の高度な Web UI

ステップ 1 [展開 (Deploy)] メニューから、[BYOD] サブメニューの [テーマ (Theme)] を選択して、[カスタムテーマの一覧表示/追加 (List/Add Custom Theme)] ページを開きます。

- ステップ 2** [テーマ (Theme)] ペインで [テーマの追加 (Add Theme)] アイコンをクリックします。
[カスタム テーマの追加 (Add Custom Theme)] ウィンドウが表示されます。
- ステップ 3** [カスタム テーマの追加 (Add Custom Theme)] ウィンドウでテーマの名前を入力します。
- ステップ 4** [カスタム テーマの追加 (Add Custom Theme)] をクリックして、新しい BYOD テーマを作成します。
- ステップ 5** 必要なテーマ属性を使用して [カスタム テーマの編集 (Edit Custom Theme)] ページを更新します。
- ステップ 6** [カスタム テーマの一覧表示/追加 (List/Add Custom Theme)] ページの右上隅にある [テーマのレビュー (Review Theme)] アイコンをクリックします。
[テーマのプレビュー (Theme Preview)] ウィンドウが表示され、新しく追加されたテーマで BYOD ページが表示されます。
- (注) [登録 (Register)] と [再起動 (Reboot)] で BYOD ページ間を移動して、テーマが BYOD ページにどのように適用されているかを確認できます。デフォルトでは、[テーマのプレビュー (Theme preview)] ウィンドウには [BYOD デバイス登録 (BYOD Device Registration)] ページがロードされます。
- ステップ 7** [再起動 (Reboot)] をクリックして、[デバイス アクティベーション (Device Activation)] ページでテーマをプレビューします。
- (注) プレビュー後は、[テーマのプレビュー (Theme Preview)] ウィンドウを閉じて、リージョンサーバーの [カスタム テーマの一覧表示/追加 (List/Add Custom Theme)] ページに戻る必要があります。
- ステップ 8** リージョンサーバーの [カスタム テーマの一覧表示/追加 (List/Add Custom Theme)] ページの [保存 (Save)] をクリックして、テーマを BYOD Web サーバーに適用するか、[元に戻す (Revert)] をクリックして、カスタム テーマを保存する前の属性値に変更します。
- (注) テーマの変更とプレビューは、何度でも行うことができます。最近保存されたテーマのみが BYOD Web サーバーに適用されます。

BYOD コンテンツの追加とプレビュー

ログイン ページメッセージ、説明、サービス条件、連絡先の詳細、ヘルプ メッセージなど、BYOD Web サーバーの内容をリージョン クラスターの BYOD コンテンツ ページで作成して、プレビューしてから、BYOD Web サーバーに公開できます。これらのコンテンツは、デバイス登録およびログイン ページの BYOD Web サーバー インターフェイスで公開できます。

コンテンツを追加およびレビューするには、次のようにします。

地域の高度な Web UI

- ステップ 1** [展開 (Deploy)] メニューから、[BYOD] サブメニューの [コンテンツ (Content)] を選択して、[BYOD コンテンツの編集 (Edit BYOD content)] ページを開きます。
- ステップ 2** ファイルをアップロードするか、[BYOD コンテンツの編集 (Edit BYOD content)] ページに該当するテキストを入力します。

(注) .html、.htm、または .txt ファイルのみをアップロードする必要があります。

- ステップ 3** 保存する前に [BYOD コンテンツの編集 (Edit BYOD content)] ページでコンテンツをプレビューするには、[レビュー (Review)] をクリックします。コンテンツを含む [コンテンツのレビュー (Content Review)] ウィンドウが表示されます。
- ステップ 4** コンテンツ レビュー ページの [バージョン情報 (About) / サービス条件/連絡先/ヘルプ (Terms Of Service/Contact/Help)] をクリックして、リージョン サーバーの [BYOD コンテンツの編集 (Edit BYOD content)] ページに追加されたコンテンツをプレビューします。
- ステップ 5** 追加された BYOD コンテンツを BYOD Web サーバーに公開するには、[保存 (Save)] をクリックします。

ポーリング プロセス

リージョン クラスタが DHCP 使用率またはリース履歴をローカル クラスタにポーリングするときには、まず、現在時刻までに使用可能なすべてのデータを要求します。この時刻は履歴データベースに記録され、後続のポーリングでは、この時刻より新しいデータのみを要求します。すべての時刻は、各ローカル クラスタの時刻に対して相対的に保存され、その時刻は、そのクラスタのタイムゾーンに合わせて調整されます。

各サーバーの時刻が同期されていない場合、奇妙なクエリ結果が表示されることがあります。たとえば、リージョン クラスタの時刻がローカル クラスタの時刻より遅れていた場合、収集された履歴は、リージョン クラスタでの時間範囲クエリに対して未来のものになる可能性があります。その場合、クエリの結果は空のリストになります。複数のクラスタからマージされたデータも、ローカル クラスタ間の時差により、順序が正しくない場合があります。このタイプの不整合があると、トレンドの解釈が困難になります。これらの問題を回避するには、すべてのクラスタでネットワーク タイム サービスを使用することを強く推奨します。

使用率とリース履歴データのポーリング

ローカルがリージョンまたはデフォルトのポーリング(1時間ごと)または手動ポーリングで登録されている場合、DHCP 使用率データが収集されます。使用可能なすべてのスコープとプレフィックスの情報がリージョンサーバーによって収集されます。リージョンデータベースを更新するためのデフォルトのポーリング間隔は1時間です。サーバーにポーリングするには、[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページの [リース履歴 (Lease History)] アイコンをクリックします。この手動ポーリングでは、サーバーがフェールオーバー関係にある場合、データはサーバーがメインであるサブネットについてのみ取得されます。

アドレス空間の権限を持っている場合 (regional-addr-admin ロールを割り当てられ、少なくとも、subnet-utilization および lease-history サブロールが割り当てられている場合)、DHCP 使用率またはリース履歴データを照会することができます。そのためには、**Operate** メニューから [使用率 (Utilization)] または [リース履歴 (Lease History)] オプションを選択します (Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイドの「使用率履歴レポートの生成」の項、また

は *Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド* の「IP リース履歴の実行」の項を参照)。

関連項目

[ポーリング プロセス \(134 ページ\)](#)

[ポーリング間隔の調整 \(135 ページ\)](#)

ポーリング間隔の調整

DHCP 使用率およびリース履歴の自動ポーリング間隔は、その他の属性とともに調整できます。これらの属性は、次の優先順位を使用して、リージョンクラスタの3つの場所で設定されます。

1. **Cluster** これらの値はサーバー全体の設定を上書きしますが、これらの値が設定解除されている場合はサーバー値が使用されます。クラスタの値は、クラスタを追加または編集するときに設定されます。CLI で、**cluster** コマンドを使用して、次の表に示す属性を設定します。
2. **Regional CCM server** (プリセットのポーリング間隔は 1 時間です) - これは **Servers** をクリックした後、ローカル CCM サーバー リンクをクリックしてアクセスできる [CCM サーバーの編集 (Edit CCM Server)] ページで設定されます。CLI で、**ccm** コマンドを使用して、次の表に示す属性を設定します。



(注) リース履歴収集がローカルクラスタ DHCP サーバーで明示的に有効になっていない場合 ([リース履歴収集の有効化 \(136 ページ\)](#) を参照)、ポーリングがデフォルトでオンになっている場合でも、データは収集されません。DHCP サーバーでの DHCP 使用率の収集は、リージョンクラスタでのポーリングとは異なり、ポーリングによって自動的に収集がトリガーされることはありません。新しいポーリングで新しいデータをピックアップする前に、DHCP 使用率の収集が行われる必要があります。この収集は 15 分ごとに事前設定されているため、ポーリング間隔はこの間隔よりも大きい値に設定する必要があります (自動ポーリング間隔は 1 時間ごとに事前設定されています)。

表 13: DHCP 使用率およびリース履歴のポーリングのリージョン属性

属性タイプ	DHCP 使用率	リース履歴
ポーリング間隔-データをポーリングする頻度	<code>addrutil-poll-interval 0</code> (ポーリングなし) ~ 1 年、CCM サーバーの場合は 1 時間に事前設定	<code>lease-hist-poll-interval 0</code> (ポーリングなし) ~ 1 年、CCM サーバーの場合は 4 時間に事前設定
再試行間隔-ポーリングが失敗した後の再試行回数	<code>addrutil-poll-retry 0</code> ~ 4 回再試行	<code>lease-hist-poll-retry 0</code> ~ 4 回再試行

属性タイプ	DHCP 使用率	リース履歴
オフセット-ポーリングを保証する時間帯	<i>addrutil-poll-offset</i> 0 ~ 24h (0h = 深夜)	<i>lease-hist-poll-offset</i> 0 ~ 24h (0h = 深夜)

ポーリングオフセット属性は、ポーリング間隔に関連して、ポーリングが1日の特定の時間帯(24時間制で設定)に行われることを保証します。たとえば、間隔を4hに、オフセットを6h(午前6時)に設定した場合、ポーリングは毎日午前2時、午前6時、午前10時、午後2時、午後6時、午後10時に行われます。

リース履歴収集の有効化

ステップ 1 クライアントが要求したリースを得られるように、スコープとアドレス範囲を使用してローカルクラスタ DHCP サーバーを設定します。

ステップ 2 リース履歴データの収集を明示的に有効にします。設定する DHCP サーバー属性は、次のとおりです。

- *ip-history* - リース履歴データベースを有効または無効にします。v4-only (DHCPv4)、v6-only (DHCPv6)、または both。
- *ip-history-max-age* - 履歴レコードの有効期間を制限します (4 週間に事前設定)。

CLI で、**dhcp set ip-history=<value> (v4-only, v6-only, both, or disable)** コマンドを使用して属性を設定します。

ステップ 3 ステージング DHCP 編集モードで、ローカルクラスタ DHCP サーバーをリロードします。

ステップ 4 リージョンクラスタで、この DHCP サーバーを含むクラスタを作成します。

ステップ 5 リージョン Web UI で、[リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページの [リース履歴設定 (Lease History Settings)] セクションに移動します。

ステップ 6 [表 13: DHCP 使用率およびリース履歴のポーリングのリージョン属性 \(135 ページ\)](#) で属性を設定します。

ステップ 7 **Save** をクリックします。

ステップ 8 [リモートクラスタの一覧表示/追加 (List/Add Remote Clusters)] ページで、クラスタ名の横にある [レプリカ (Replica)] アイコンをクリックします。

ステップ 9 リース履歴データの初期セットの取得に関連するクラスタの [リース履歴 (Lease History)] アイコンをクリックします。このデータはポーリング間隔ごとに自動的に更新されます。

DHCP スコープ テンプレートの管理

スコープテンプレートは、特定の共通属性を複数のスコープに適用します。これらの共通属性には、式に基づくスコープ名、ポリシー、アドレス範囲、式に基づく組み込みポリシー オプションが含まれます。ローカルクラスタから追加またはプルしたスコープテンプレートは、

[DHCP スコープ テンプレートの一覧表示/追加 (List/Add DHCP Scope Templates)] ページに表示されます (**Design > DHCPv4** メニューから **Scope Templates** を選択します)。

スコープ テンプレートの作成と編集、およびスコープへの適用の詳細については、『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「スコープテンプレートの作成と適用」の項を参照してください。リージョンクラスタ Web UI には、スコープテンプレートをローカルクラスタにプッシュし、ローカルクラスタからプルする機能が追加されています。

関連項目

[ローカルクラスタへのスコープテンプレートのプッシュ \(137 ページ\)](#)

[レプリカデータからのスコープテンプレートのプル \(138 ページ\)](#)

ローカルクラスタへのスコープテンプレートのプッシュ

作成したスコープテンプレートをリージョンクラスタから任意のローカルクラスタにプッシュできます。Web UI で、[DHCP スコープ テンプレートの一覧表示/追加 (List/Add DHCP Scope Templates)] ページに移動し、次のいずれかを実行します。

- 特定のテンプレートをクラスタにプッシュする場合は、左側の [スコープ テンプレート (Scope Templates)] ペインからスコープテンプレートを選択して、**Push** (ページの上部にある) をクリックします。[DHCP スコープテンプレートのプッシュ (Push DHCP Scope Template)] ページが開きます。
- 使用可能なすべてのスコープテンプレートをプッシュする場合は、[スコープテンプレート (Scope Templates)] ペインの上部にある [すべてプッシュ (**Push All**)] アイコンをクリックします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ページが開きます。

リージョン Web UI

[DHCP スコープ テンプレートのプッシュ (Push DHCP Scope Template)] ページと [ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ページでは、プッシュするデータ、ローカルクラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- **保証 (Ensure)** (プリセット値): 既存のデータに影響を与えずに、ローカルクラスタに新しいデータが含まれるようになります。
- **Replace**- ローカルクラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスタに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能 (Available)] フィールドで宛先クラスタを選択し、[選択済み (Available)] フィールドに移動します。



ヒント 同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であるため、変更しない限り、このページにアクセスするたびに有効になります。

これらの選択を行った後 **Push Data to Clusters**、をクリックします。[スコープテンプレートデータのプッシュ レポートの表示 (View Push Scope Template Data Report)] ページが開きます。

CLI コマンド

リージョン クラスタに接続されているときには、**scope-template <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのスコープ テンプレートのプル

明示的に作成するのではなく、ローカルクラスタのレプリカ データからスコープ テンプレートをプルすることもできます。(クラスタ名の横にある[複製 (Replicate)] アイコンをクリックして、ポリシーのレプリカ データを更新しておいてください)。リージョン Web UI でスコープ テンプレートをプルするには、[スコープ テンプレート (Scope Templates)] ペインの上部にある[データのプル (Pull Data)] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP スコープ テンプレート データの選択 (Select Replica DHCP Scope Template Data to Pull)] ページには、ローカルクラスタのスコープテンプレートのリージョンサーバーのレプリカデータのツリービューが表示されます。ツリーには2つのレベルがあり、1つはローカルクラスタ、もう1つは各クラスタのスコープテンプレートです。クラスタから個々のスコープテンプレートをプルすることも、すべてのスコープテンプレートをプルすることもできます。個々のスコープテンプレートをプルするには、クラスタのツリーを展開して、名前横にある **Pull Scope Template** をクリックします。クラスタからすべてのスコープテンプレートをプルするには、**Pull All Scope Templates** をクリックします。

スコープテンプレートをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョンクラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値)-地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

リージョン クラスタに接続されているときには、**scope-template <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]** コマンドを使用できます。

DHCP ポリシーの管理

すべての DHCP サーバーには、1 つ以上のポリシーが定義されている必要があります。ポリシーは、リース期間、ゲートウェイ ルータ、およびその他の設定パラメータを、DHCP オプションと呼ばれるものとして定義します。ポリシーは 1 回だけ定義し、複数のスコープに適用する必要があるため、複数のスコープがある場合は特に役立ちます。

DHCP ポリシーの作成と編集、およびスコープへの適用の詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド*』の「DHCP ポリシーの設定」の項を参照してください。リージョン クラスタ Web UI には、ローカル クラスタにポリシーをプッシュし、ローカル クラスタからプルする機能が追加されています。また、ポリシーを再利用する機能も提供されます。

関連項目

[ローカル クラスタへのポリシーのプッシュ \(139 ページ\)](#)

[レプリカ データからのポリシーのプル \(140 ページ\)](#)

ローカル クラスタへのポリシーのプッシュ

また、作成したポリシーをリージョン クラスタから任意のローカル クラスタにプッシュすることもできます。リージョン Web UI で、[DHCP ポリシーの一覧表示/追加 (List/Add DHCP Policies)] ページに移動し、次のいずれかを実行します。

- 特定のポリシーをクラスタにプッシュする場合は、左側の [ポリシー (Policies)] ペインからポリシーを選択して、**Push** (ページの上部にある) をクリックします。
- すべてのポリシーをプッシュする場合は、[ポリシー (Policies)] ペインの上部にある [すべてプッシュ (Push all)] アイコンをクリックします。

リージョン Web UI

[ローカル クラスタへの DHCP ポリシー データのプッシュ (Push DHCP Policy Data to Local Clusters)] ページでは、プッシュするデータ、ローカル クラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- **保証 (Ensure)** (プリセット値): 既存のデータに影響を与えずに、ローカル クラスタに新しいデータが含まれるようになります。
- **Replace**- ローカル クラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプッシュ」操作のみに使用できます。データを上書きし、ローカル クラスタに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能 (Available)]フィールドで宛先クラスタを選択し、[選択済み (Available)]フィールドに移動します。次に **Push Data to Clusters** をクリックして、[ポリシー データのプッシュ レポートの表示 (View Push Policy Data Report)] ページを開きます。



ヒント 同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョン クラスタに接続されているときには、**policy <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのポリシーのプル

明示的に作成する代わりに、ローカルクラスタのレプリカデータからポリシーをプルすることもできます。(リージョン Web UI では、クラスタ名の横にある [複製 (Replicate)] アイコンをクリックして、ポリシーのレプリカデータを更新しておいてください)。ポリシーをプルするには、[ポリシー (Policies)] ペインの上部にある [データのプル (Pull Data)] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP ポリシー データの選択 (Select Replica DHCP Policy Data to Pull)] ページには、ローカル クラスタのポリシーのリージョン サーバーのレプリカ データのツリービューが表示されます。ツリーには2つのレベルがあり、1つはローカルクラスタ、もう1つは各クラスタのポリシーです。個々のポリシーをクラスタからプルすることも、すべてのポリシーをプルすることもできます。個々のポリシーをプルするには、クラスタのツリーを展開して、名前横にある [ポリシーのプル (Pull Policy)] をクリックします。クラスタからすべてのポリシーをプルするには、[すべてのポリシーをプル (Pull All Policies)] をクリックします。

すべてのポリシーをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値)- 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

リージョン クラスタに接続されているときには、**policy <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]** コマンドを使用できます。

DHCP クライアントクラスの管理

クライアントクラスは、共通のネットワークに接続したユーザーに差別化されたサービスを提供します。管理基準に基づいてユーザー・コミュニティをグループ化し、各ユーザーが適切なサービス・クラスを受け取れるようにすることができます。Cisco Prime Network レジストラークライアントクラス機能を使用して、設定パラメータを制御できますが、最も一般的な用途は次のとおりです。

- **Address leases** - 一連のクライアントがアドレスを保持する期間。
- **IP address ranges** : クライアントアドレスを割り当てるリースプールの元。
- **DNS server addresses** : クライアントが DNS クエリを送信する場所。
- **DNS hostnames** : クライアントを割り当てる名前。
- **Denial of service** : 許可されていないクライアントにリースを提供するかどうか。

クライアントクラスの作成および編集の詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザガイド*』の「クライアントクラスとクライアントの管理」の章を参照してください。リージョンクラスタ Web UI には、クライアントクラスをローカルクラスタにプッシュし、ローカルクラスタからプルする機能が追加されています。また、クライアントクラスを再利用する機能も提供されます。

関連項目

[ローカルクラスタへのクライアントクラスのプッシュ \(141 ページ\)](#)

[ローカルクラスタへのクライアントクラスのプッシュ \(141 ページ\)](#)

ローカルクラスタへのクライアントクラスのプッシュ

また、ユーザーが作成したクライアントクラスをリージョンクラスタから任意のローカルクラスタにプッシュすることもできます。リージョン Web UI で、[DHCP クライアントクラスの一覧表示/追加 (List/Add DHCP Client Classes)] ページに移動し、次のいずれかを実行します。

- Web UI で特定のクライアントクラスをクラスタにプッシュする場合は、左側の [クライアントクラス (Client Classes)] ペインからクライアントクラスを選択し、**Push** (ページの上部にある) をクリックします。[DHCP クライアントクラスのプッシュ (Push DHCP Client Class)] ページが開きます。
- すべてのクライアントクラスをプッシュする場合は、[クライアントクラス (Client Classes)] ペインの上部にある [すべてプッシュ (**Push All**)] アイコンをクリックします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] ページが開きます。

リージョン Web UI

[DGCP クライアント クラスのプッシュ (Push DHCP Client Class)] ページと [ローカル クラスタへのデータのプッシュ (Push Data to Local Clusters)] ページには、プッシュするデータ、ローカルクラスタとの同期方法、およびプッシュ先のクラスタが示されます。データ同期モードは次のとおりです。

- 保証 (**Ensure**) (プリセット値): 既存のデータに影響を与えずに、ローカル クラスタに新しいデータが含まれるようになります。
- **Replace**- ローカルクラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスタに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能 (Available)] フィールドで宛先クラスタを選択し、[選択済み (Available)] フィールドに移動します。次に **Push Data to Clusters** をクリックして、[クライアントクラスデータプッシュ レポートの表示 (View Push Client-Class Data Report)] ページを開きます。



ヒント

同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョンクラスタに接続されているときには、**client-class <name | all> push <ensure | replace | exact > cluster-list [-report-only | -report]** コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのクライアントクラスのプル

明示的に作成する代わりに、ローカル クラスタのレプリカ データからクライアントクラスをプルすることもできます。(Web UI では、クラスタ名の横にある [複製 (**Replicate**)] アイコンをクリックして、クライアントクラスのレプリカデータを更新しておいてください)。クライアントクラスをプルするには、[クライアント クラス (Client Classes)] ペインの上部にある [データのプル (**Pull Data**)] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP クライアントクラス データの選択 (Select Replica DHCP Client-Class Data to Pull)] ページには、ローカル クラスタのクライアントクラスのリージョン サーバーのレプリカデータのツリービューが表示されます。ツリーには2つのレベルがあり、1つはローカルクラスタ、もう1つは各クラスタ内のクライアントクラスです。クラスタから個々のクライアントクラスをプルすることも、すべてのクライアントクラスをプルすることもできます。個々のクライアントクラスをプルするには、クラスタのツリーを展開して、名前の横にある

Pull Client-Class をクリックします。クラスタからすべてのクライアントクラスをプルするには、**Pull All Client-Classes** をクリックします。

クライアントクラスをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値)- 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

リージョン クラスタに接続したら、**client-class <name | all > pull <ensure | replace | exact > cluster-name [-report-only | -report]** コマンドを使用できます。

仮想プライベート ネットワークの管理

バーチャルプライベート ネットワーク (VPN) は、キーによって識別される特殊なアドレス空間です。VPN では、アドレスが個別のキーによって区別されるため、ネットワーク内でのアドレスの重複が許されます。ほとんどの IP アドレスは、VPN 外のグローバル アドレス空間に存在します。管理者が **central-cfg-admin** ロールの **dhcp-management** サブロールを割り当てられている場合にのみ、リージョン VPN を作成できます。

VPN の作成と編集、およびさまざまなネットワーク オブジェクトへの適用の詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド*』の「DHCP を使用したバーチャルプライベート ネットワークの設定」の項を参照してください。リージョン Web UI には、VPN をローカルクラスタにプッシュし、ローカルクラスタからプルする機能が追加されています。また、VPN を再利用する機能も提供されます。

関連項目

[ローカルクラスタへの VPN のプッシュ \(143 ページ\)](#)

[レプリカデータからの VPN のプル \(144 ページ\)](#)

ローカルクラスタへの VPN のプッシュ

作成した VPN をリージョンクラスタから任意のローカルクラスタにプッシュできます。リージョン Web UI で、[VPN の一覧表示/追加 (List/Add VPNs)] ページに移動し、次のいずれかを実行します。

- Web UI で特定の VPN をクラスタにプッシュする場合は、左側の [VPN] ペインから VPN を選択して、**Push** (ページの上部にある) をクリックします。[VPN のプッシュ (Push VPN)] ページが開きます。

- すべての VPN をプッシュする場合は、[VPN] ペインの上部にある [すべてプッシュ (Push All)] アイコンをクリックします。[ローカル クラスタへのデータのプッシュ (Push Data to Local Clusters)] ページが開きます。

リージョン Web UI

[VPN のプッシュ (Push VPN)] ページと [ローカル クラスタへのデータのプッシュ (Push Data to Local Clusters)] ページでは、プッシュするデータ、ローカル クラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- **保証 (Ensure)** (プリセット値): 既存のデータに影響を与えずに、ローカル クラスタに新しいデータが含まれるようになります。
- **Replace**- ローカル クラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカル クラスタに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能 (Available)] フィールドで宛先クラスタを選択し、[選択済み (Available)] フィールドに移動します。次に **Push Data to Clusters** をクリックして、[VPN データのプッシュ レポートの表示 (View Push VPN Data Report)] ページを開きます。



ヒント 同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョン クラスタに接続されているときには、`vpn <name> | all > push <ensure | replace | exact > cluster-list [-report-only] | -report` コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからの VPN のプル

VPN を明示的に作成するのではなく、ローカル クラスタからプルすることができます。(リージョン Web UI では、クラスタ名の横にある [レプリカ (Replica)] アイコンをクリックして、VPN レプリカ データを更新しておいてください)。レプリカ データをプルするには、左側の [VPN] ペインの上部にある [データのプル (Pull Data)] アイコンをクリックして、[プルするレプリカ VPN データの選択 (Select Replica VPN Data to Pull)] ページを開きます。

このページには、ローカル クラスタの VPN のリージョンサーバーのレプリカデータのツリービューが表示されます。このツリーには2つのレベルがあり、1つはローカル クラスタ、もう1つは各クラスタ内の VPN です。個々の VPN をプルすることも、すべてをプルすることもできます。個々の VPN をプルするには、クラスタのツリーを展開して、名前横にある **Pull VPN** をクリックします。すべての VPN をプルするには、**Pull All VPNs** をクリックします。

VPN をプルするには、同期モードを選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値)- 地域クラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスタに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

リージョン クラスタに接続されているときには、`vpn <name> | all > pull <ensure | replace | exact > cluster-name [-report-only | -report]` コマンドを使用できます。

DHCP フェールオーバー ペアの管理

DHCP フェールオーバーでは、バックアップ DHCP サーバーは、メイン サーバーが何らかの理由でネットワークから切断された場合、メインサーバーを引き継ぐことができます。フェールオーバーを使用して、冗長ペアとして動作するように2つのサーバーを設定できます。1つのサーバーがダウンした場合、もう1つのサーバーがシームレスに引き継ぐため、新しいDHCP クライアントはアドレスを取得でき、既存のクライアントはアドレスを更新することができます。新しいリースを要求するクライアントは、どちらのサーバーがリース要求に応答するかを知る必要はありません。これらのクライアントは、メインサーバーがダウンしている場合でもリースを取得できます。

リージョン Web UI では、[DHCP フェールオーバー ペアの一覧表示/追加 (List/Add DHCP Failover Pairs)] ページで、作成されたフェールオーバー ペアを表示できます。このページにアクセスするには、**DHCP** をクリックしてから、**Failover** をクリックします。この機能は、`centra-cfg-admin` ロールの `dhcp-management` サブロールが割り当てられている管理者のみが使用できます。

フェールオーバー ペアの作成と編集の詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド*』の「フェールオーバー サーバー ペアのセットアップ」の項を参照してください。リージョンクラスタ Web UI には、ローカルクラスタからアドレスをプルしてフェールオーバー ペアを作成する機能が追加されています。

フェールオーバー ペアのアドレス空間をプルするには、`regional-addr-admin` 権限が必要です。

リージョン Web UI

ステップ 1 [DHCPフェールオーバーペアの一覧表示/追加 (List/Add DHCP Failover Pairs)] ページまたは [ユニファイドアドレス空間の表示 (View Unified Address Space)] ページで、[フェールオーバーペア (Failover Pairs)] ペインの [プルv4データ (Pull v4 Data)] または [プルv6データ (Pull v6 Data)] アイコンをクリックします。

- ステップ 2** [プルレプリカアドレス空間の選択 (Select Pull Replica Address Space)] ページで、データ同期モード (**Update**、**Complete**、または **Exact**) を選択します。これらのモードを選択した結果については、ページの表を参照してください。
- ステップ 3** [フェールオーバー ペアの同期 (Synchronize Failover Pair)] タブの **Report** ボタンをクリックし、[戻る (**Return**)] をクリックします。
- ステップ 4** [プルレプリカアドレス空間の報告 (Report Pull Replica Address Space)] ページの **Run** をクリックします。
- ステップ 5** [プルレプリカアドレス空間の実行 (Run Pull Replica Address Space)] ページの **OK** をクリックします。

CLI コマンド

リージョンクラスタに接続されている場合は、次のコマンドを使用して、アドレス空間（および予約）をプルできます。

- `ccm pullAddressSpace < update | complete | exact > [-omitreservations] [-report-only | -report]`
- `ccm pullIPv6AddressSpace < update | complete | exact > [-report-only | -report]`

リース予約の管理

リージョンクラスタから作成したリース予約をローカル クラスタのいずれかにプッシュできます。リージョンクラスタ Web UI で、[DHCPv4 予約の一覧表示/追加 (List/Add DHCPv4 Reservations)] ページまたは [DHCPv6 予約の一覧表示/追加 (List/Add DHCPv6 Reservations)] ページに移動し、左側の予約ペインの [すべてプッシュ (**Push All**)] アイコンをクリックします。個々の予約をプッシュすることはできないことに注意してください。プッシュ先のクラスタが DHCP フェールオーバー設定の一部である場合、予約をプッシュすると、パートナーサーバーにもプッシュされます。

関連項目

[DHCPv4 予約 \(146 ページ\)](#)

[DHCPv6 予約 \(147 ページ\)](#)

DHCPv4 予約

DHCPv4 予約を作成するには、親サブネット オブジェクトがリージョンサーバーに存在している必要があります。リージョンで保留中の予約の編集がある場合は、それらをサブネットのローカル クラスタまたはフェールオーバー ペアにプッシュできます。サブネットがプッシュされていない場合は、親スコープがローカル クラスタまたはペアに追加されます。

サブネットがローカルクラスタまたはペアにプッシュされると、予約がそのクラスタまたはペアにプッシュされます。スコープとサブネットを別のローカル クラスタまたはフェールオーバー ペアに移動するには、最初にサブネットを回収する必要があります。

DHCPv6 予約

DHCPv6 予約を作成するには、親プレフィックスがリージョンサーバーに存在している必要があります。保留中の予約またはプレフィックスの変更がある場合は、ローカルクラスタに更新をプッシュできます。

プレフィックスがローカルクラスタにプッシュされると、そのローカルクラスタのみを更新できます。プレフィックスを別のローカルクラスタに移動するには、最初に再利用する必要があります。

リージョン Web UI

表示されるページで、プッシュするデータ、ローカルクラスタと同期する方法、およびプッシュ先のクラスタを識別できます。データ同期モードは、次のとおりです。

- **保証 (Ensure)** - 既存のデータに影響を与えずに、ローカルクラスタに新しいデータがあることを確認します。
- **Replace** (プリセット値) - ローカルクラスタに固有の他のオブジェクトに影響を与えずに、データを置き換えます。
- **Exact** - 「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能 (Available)] フィールドで宛先クラスタを選択し、[選択済み (Available)] フィールドに移動します。



ヒント

同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であるため、変更しない限り、このページにアクセスするたびに有効になります。

これらの選択を行った後 **Push Data to Clusters**、をクリックします。[プッシュ予約データ レポートの表示 (View Push Reservations Data Report)] ページが開きます。このページの **OK** をクリックします。

また、[DHCP v6 予約のリスト/追加 (List/Add DHCP v6 Reservations)] ページでレプリカアドレス空間をプルし、そのときに予約を省略するかどうかを選択することもできます。このオプションは、マージする予約に保留中の変更がないことが確認された場合にのみ、処理時間を短縮するために使用してください。プルの予約を省略するには、[予約を省略? (Omit Reservations?)] チェックボックスをオンにして、**Pull Data** をクリックします。

『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「DHCPv6 アドレス」の項を参照してください。

リソース制限アラームのモニターリング

リソース制限アラームを使用すると、Cisco Prime Network Registrar システム リソースをモニターして、1 つ以上の製品リソースが潜在的に危険なレベルに入り、注意が必要なときに通知

を受けることができます。リソース制限アラームは、リソース制限情報を整理して統合して伝達するように設計されています。



- (注) リソース制限に関連するログメッセージは、`ccm_monitor_log` ファイルに記録されます。ログファイルの詳細については、[ログファイル \(179 ページ\)](#) を参照してください。

モニター対象の各リソースの重要レベルと警告レベルの両方について、事前定義されたしきい値レベルをリセットできます。

Cisco Prime Network Registrar は、Web UI および CLI で、モニター対象リソースの現在のステータス、現在の値、およびピーク値を報告します。ピーク値は、設定されたリソース制限アラームの警告または危機的な限界と比較され、リソース制限アラームのステータスが [OK]、[Warning]、または [Critical] と表示されます。Cisco Prime Network Registrar では、結果の条件が発生しなくなり、ピーク値がリセットされるまで、Web UI と CLI にアラームが表示されます。

リソース制限アラームは、設定したポーリング間隔に基づいて定期的に更新されます。ポーリング間隔の設定の詳細については、[リソース制限アラームのポーリング間隔の設定 \(150 ページ\)](#) を参照してください。

SNMP トラップがリソース制限アラームに対して有効になっている場合、Cisco Prime Network Registrar は、モニター対象のリソースがクリティカルレベルまたは警告レベルを超えたときに SNMP トラップを生成します。SNMP トラップは、現在の値が設定された警告または危機的レベルを超えたときに生成されます。

リソース制限アラームは、リージョンとローカルクラスタの両方で設定できます。リソース制限アラームデータは、個々のローカルクラスタレベルで統合されます。リージョンクラスタレベルで使用可能なリソース制限アラームは、リージョンクラスタにのみ関係します。次の表に、リージョンまたはローカルクラスタで使用可能なリソース制限アラームのタイプを示します。

表 14: リソース制限アラーム

	リージョンクラスタ	ローカルクラスタ
データの空き領域/データパーティション	✓	✓
シャドウバックアップ時間	✓	✓
CCM メモリ	✓	✓
CNR サーバー エージェント メモリ	✓	✓
Tomcat メモリ	✓	✓
DHCP メモリ	x	✓
CDNS メモリ	x	✓

DNS メモリ	X	✓
SNMP メモリ	✓	✓
TFTP メモリ	X	✓
リース数	X	✓
ゾーン数	X	✓
リソース レコード数	X	✓

リソース制限アラームしきい値の設定

[CCM サーバーの編集 (Edit CCM Server)] ページを使用して、リソース制限アラームの警告および重大制限を設定できます。

ローカルおよびリージョン Web UI

ステップ 1 CCM サーバーのプロパティにアクセスするには、[操作 (Operate)] メニューの [サーバーの管理 (Manage Servers)] を選択して、[サーバーの管理 (Manage Servers)] ページを開きます。

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

ステップ 3 [リソース制限の設定 (Configure Resource Limits)] タブをクリックします。

ステップ 4 必要に応じて設定を変更します。

(注) リソース制限アラームの SNMP トラップを有効にするには、[トラップ設定 (Trap Configuration)] グループの [トラップの有効化 (Enable Traps)] オプションを選択します。

ステップ 5 [保存 (Save)] をクリックして、CCM サーバー属性の変更を保存します。

CLI コマンド

ローカルまたはリージョン クラスタでリソース制限アラームを設定するには、**resource set attribute = value [attribute = value ...]** を使用します。現在の設定をレビューするには、**resource show** を使用し、リソースに関するレポートを生成するには、**resource report [all | full | levels]** コマンドを使用します。

定義された警告および重大レベルを表示するには、**resource report levels** コマンドを使用します。

次のシナリオでは、109 ステータス メッセージが報告されます (少なくとも 1 つのリソースが重大または警告状態になっている場合)。

- **resource report** コマンドを実行します。

- CLI を使用してクラスタに接続します。
- CLI を終了します。

リソース制限アラームのポーリング間隔の設定

Cisco Prime Network Registrar がサーバーからアラームデータをポーリングして、Web UI データを更新する頻度を設定できます。 *stats-history-sample-interval* は、CCM サーバー システムのポーリング レートを制御します。

- ステップ 1** アラーム ポーリング間隔を編集するには、[設定 (Settings)] ドロップダウンリスト (メインページの上) で [ユーザー環境設定 (User Preferences)] に移動して、ユーザー環境設定を編集する必要があります。
- ステップ 2** ユーザー環境設定を行った後、[ユーザー環境設定の変更 (Modify User Preferences)] をクリックします。

リソース制限アラームの表示

リソース制限アラームは [アラーム (Alarms)] ページに表示されます。アラームの概要を表示するには、Cisco Prime Network Registrar Web UI で、Web UI の上部にある [アラーム (Alarms)] アイコンをクリックします。 [アラーム (Alarms)] ページが開き、各リソース制限アラームのリソース、タイプ、ステータス、リソース使用率、および現在の値が表示されます。各リソース制限のピーク値に基づいて、リソース制限のステータスは、Web UI および CLI に [OK]、[Warning]、または [Critical] と表示されます。アラームは、設定したポーリング間隔に基づいて定期的に更新されます。ポーリング間隔の設定の詳細については、[リソース制限アラームのポーリング間隔の設定 \(150 ページ\)](#) を参照してください。



- (注) リソースが警告または重大な状態にある場合、リソース制限アラームは [設定の概要 (Configuration Summary)] ページにも表示されます。

リソース制限アラームのピーク値のリセット

Cisco Prime Network Registrar は、各リソース制限のピーク値を維持します。ピーク値は、現在の値がピーク値を超えた場合にのみ更新されます。ピーク値は、設定されたリソース制限アラームの警告または危機的な限界と比較され、リソース制限アラームのステータスが [OK]、[Warning]、または [Critical] と表示されます。

ピーク値が設定された警告または重大な制限を超えると、ピーク値が明示的にリセットされるまで、リソース制限アラームのステータスがそれぞれ [警告 (Warning)] または [クリティカル (Critical)] (Web UI および CLI で) として表示されます。ピーク値をリセットするには、次の手順を実行します。

-
- ステップ 1** Web UI の上部にある [アラーム (Alarms)] アイコンをクリックして、[アラーム (Alarms)] ページを開きます。
- ステップ 2** ピーク値をリセットするアラームを選択します。
- ステップ 3** [アラームのリセット (**Reset Alarm**)] ボタンをクリックして、ピーク値をクリアします。
-

CLI コマンド

ローカルまたはリージョンクラスタでピーク値をリセットするには、**resource reset** [name [,name [...]]] を使用します。



(注) リソース名が指定されていない場合、すべてがリセットされます。

リソース制限アラーム データのエクスポート

リソース制限アラーム データを CSV ファイルにエクスポートできます。リソース制限アラームをエクスポートするには、次の手順を実行します。

-
- ステップ 1** Web UI の上部にある [アラーム (Alarms)] アイコンをクリックして、[アラーム (Alarms)] ページを開きます。
- ステップ 2** [CSV にエクスポート (**Export to CSV**)] をクリックします。
- ステップ 3** [ファイルのダウンロード (File Download)] ポップアップ ウィンドウが表示されます。[保存 (**Save**)] をクリックします。
- ステップ 4** [名前を付けて保存 (Save As)] ポップアップ ウィンドウで、ファイルの保存場所を選択して、[保存 (**Save**)] をクリックします。
-

ローカル クラスタ管理チュートリアル

このチュートリアルでは、Example Company のローカルクラスタの基本的なシナリオについて説明します。クラスタの管理者は、ユーザー、ゾーンデータ、DHCP データ、アドレス空間データ、およびサーバーについて一般に責任を負います。タスクは、2つのゾーン (example.com と boston.example.com) 、ゾーン内のホスト、およびサブネットをセットアップすることです。また、ローカルクラスタは、[リージョンクラスタ管理チュートリアル \(159 ページ\)](#) に述べられているように、サンノゼのリージョンクラスタが中央構成を実行し、別のクラスタのローカルクラスタ管理者とアドレス空間を複製できるように、特別な管理者アカウントも作成する必要があります。

関連項目

[管理者の責任とタスク \(152 ページ\)](#)

- [管理者の作成 \(152 ページ\)](#)
- [アドレス インフラストラクチャの作成 \(153 ページ\)](#)
- [ゾーン インフラストラクチャの作成 \(154 ページ\)](#)
- [制約付きのホスト管理者ロールの作成 \(157 ページ\)](#)
- [ホスト管理者に割り当てるグループの作成 \(158 ページ\)](#)
- [ホストアドレス範囲のテスト \(159 ページ\)](#)

管理者の責任とタスク

ローカル クラスタ管理者には、次の責任とタスクがあります。

- **example-cluster-admin**- スーパーユーザーによって作成されます。
 - Boston クラスタでは、他のローカル管理者を作成します (**example-zone-admin** と **example-host-admin**) 。
 - ローカル クラスタの基本的なネットワーク インフラストラクチャを作成します。
 - **example-host-role** を **boston.example.com** ゾーン内のアドレス範囲に制限します。
 - **example-zone-admin** が **example-host-admin** に割り当てる **example-host-group** (**example-host-role** で定義) を作成します。
- **example-zone-admin** :
 - **example.com** ゾーンと **boston.example.com** ゾーンを作成し、後者のゾーンを保守します。
 - **example-host-group** を **example-host-admin** に割り当てます。
- **example-host-admin**- ローカル ホスト リストと IP アドレスの割り当てを保守します。

管理者の作成

この例では、ボストンのスーパーユーザーが、[管理者の責任とタスク \(152 ページ\)](#) に説明されているように、ローカル クラスタ、ゾーン、およびホスト管理者を作成します。

ローカル基本 Web UI

- ステップ 1** ボストンのローカル クラスタで、スーパーユーザー (通常は **admin**) としてログインします。
- ステップ 2** 基本モードで、[管理 (**Administration**)] メニューから [管理者 (**Administrators**)] を選択します。
- ステップ 3** ローカル クラスタ管理者 (スーパーユーザーアクセス権を持つ) を追加します。[管理者の一覧表示/追加 (List/Add Administrators)] ページで。

- a) [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックし、[名前 (Name)] フィールドに **example-cluster-admin** と入力します。
- b) [パスワード (Password)] フィールドと [パスワードの再入力 (Confirm password)] フィールドに **exampleadmin** と入力し、[管理者の追加 (Add Admin)] をクリックします。
- c) [スーパーユーザー (Superuser)] チェックボックスをオンにします。
- d) [グループ (Groups)] リストからグループを選択しないでください。
- e) [保存 (Save)] をクリックします。

ステップ 4 同じページでローカルゾーン管理者を追加します。

- a) [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックし、[名前 (Name)] フィールドに **example-zone-admin** と入力し、[パスワード (Password)] フィールドと [パスワードの再入力 (Confirm Password)] フィールドに **examplezone** と入力して、[管理者の追加 (Add Admin)] をクリックします。
- b) [管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションにある [追加 (Add)] をクリックして、[グループ (Groups)] ウィンドウを開きます。 **ccm-admin-group**、**dns-admin-group**、および **host-admin-group** を選択して、[選択 (Select)] をクリックします。選択されたグループが、[管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションに表示されます。
dns-admin-group は、DNS ゾーンおよびサーバーを管理する **dns-admin** ロールです。すでに事前定義されています。**ccm-admin-group** では、**example-zone-admin** は後で制約付きロールで **example-host-admin** をセットアップできます。**host-admin-group** は、主に、ゾーン内のホスト作成をテストします。
- c) [保存 (Save)] をクリックします。

ステップ 5 同じページでローカルホスト管理者を追加します。

- a) [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックし、[名前 (Name)] フィールドに **example-host-admin** と入力し、[パスワード (Password)] フィールドに **examplehost** と入力して、[管理者の追加 (Add Admin)] をクリックします。
- b) この時点ではグループを選択しないでください。(**example-zone-admin** は、後で、**example-host-admin** を制約付きロールを持つグループに割り当てます) 。
- c) [保存 (Save)] をクリックします。

(注) 管理者に制約を適用する方法の詳細については、[制約付きのホスト管理者ロールの作成 \(157 ページ\)](#) を参照してください。

アドレスインフラストラクチャの作成

クラスターでゾーンとホストを管理するための前提条件は、基盤となるネットワークインフラストラクチャを作成することです。ネットワーク設定は、多くの場合、すでに存在し、インポートされています。ただし、このチュートリアルでは、白紙の状態から始めることを前提としています。

ローカルの **example-cluster-admin** は次に、静的 IP アドレスが割り当てられる **boston.example.com** ゾーン内のホストに対して許可されるアドレス範囲を作成します。これらのアドレスは、100 ~ 200 の範囲のホストを持つ **192.168.50.0/24** サブネット内にあります。

ローカル詳細 Web UI

- ステップ 1** ローカルクラスタで、スーパーユーザーとしてログアウトし、**example-cluster-admin** ユーザーとしてパスワード **exampleadmin** を使用してログインします。管理者はスーパーユーザーであるため、すべての機能を使用できます。
- ステップ 2** **Advanced** をクリックして、詳細モードに入ります。
- ステップ 3** [設計 (**Design**)] メニューから、[DHCPv4] サブメニューの [サブネット (**Subnets**)] を選択して、[サブネットの一覧表示/追加 (List/Add Subnets)] ページを開きます。
- ステップ 4** [サブネットの一覧表示/追加 (List/Add Subnets)] ページで、**boston.example.com** サブネットアドレスを入力します。
- [サブネット (**Subnets**)] ペインの [サブネットの追加 (**Add Subnets**)] アイコンをクリックし、[アドレス (**Address**)] フィールドに **192.168.50** と入力します。
 - [マスク (**mask**)] ドロップダウンリストで **24** を選択します。このサブネットは、通常のクラス C ネットワークになります。
 - [所有者 (**Owner**)]、[リージョン (**Region**)]、および [アドレス タイプ (**Address Type**)] フィールドはそのままにしておきます。必要な場合は説明を追加します。
 - Add Subnet** をクリックします。
- ステップ 5** **192.168.50.0/24** アドレスをクリックして、[サブネットの編集 (**Edit Subnet**)] ページを開きます。
- ステップ 6** [IP 範囲 (**IP Ranges**)] フィールドに、静的アドレスの範囲を入力します。
- [開始 (**Start**)] フィールドに **100** と入力します。次のフィールドにタブ移動します。
 - [終了 (**End**)] フィールドに **200** と入力します。
 - Add IP Range** をクリックします。アドレスの範囲がフィールドの下に表示されます。
- ステップ 7** **Save** をクリックします。
- ステップ 8** **Address Space** をクリックすると、[ユニファイドアドレス空間の表示 (**View Unified Address Space**)] ページが開きます。**192.168.50.0/24** サブネットがリストに表示されます。[更新 (**Refresh**)] アイコンをクリックします。
-

ゾーンインフラストラクチャの作成

このシナリオでは、**example-cluster-admin** は、**example.com** ゾーンとそのサブゾーンを含めて、**Example Company** のゾーンをローカルに作成する必要があります。**example-cluster-admin** は、いくつかの初期ホストレコードも **boston.example.com** ゾーンに追加します。

関連項目

[転送ゾーンの作成 \(155 ページ\)](#)

[逆引きゾーンの作成 \(155 ページ\)](#)

[最初のホストの作成 \(156 ページ\)](#)

転送ゾーンの作成

まず、example.com と boston.example.com の転送ゾーンを作成します。

ローカル基本 Web UI

- ステップ 1 ローカル クラスタで、**example-zone-admin** ユーザーとしてパスワード **examplezone** でログインします。
- ステップ 2 **Design** メニューから、**Auth DNS** サブメニューの**Forward Zones** を選択します。[ゾーンの一覧表示/追加 (List/Add Zones)] ページが開きます。
- ステップ 3 example.com ゾーンを作成します (フィールド間移動にはタブを使用します)。
 - a) [転送ゾーン (Forward Zones)] ペインの [転送ゾーンの追加 (Add Forward Zone)] アイコンをクリックし、[名前 (Name)] フィールドに **example.com** と入力します。
 - b) [ネームサーバー FQDN (Nameserver FQDN)] フィールドに、**ns1** と入力します。
 - c) [連絡先の電子メール (Contact E-Mmail)] フィールドに、**hostadmin** と入力します。
 - d) [シリアル番号 (Serial Number)] フィールドに、シリアル番号を入力します。
 - e) **Add Zone** をクリックします。
- ステップ 4 前の手順と同じ値を使用して、同じ方法で **boston.example.com** ゾーンを作成します。
 - a) 既存のゾーンにプレフィックスが追加されたゾーンを作成すると、[親ゾーンにサブゾーンを作成 (Create Subzone in Parent Zone)] ページが開きます。これは、ゾーンが潜在的なサブゾーンである可能性があるためです。このゾーンを example.com のサブゾーンとして作成するには、[親ゾーンにサブゾーンを作成 (Create Subzone in Parent Zone)] ページの **Create as Subzone** をクリックします。
 - b) ネームサーバーはゾーンごとに異なるため、複数のゾーンを関連付けるには、グルー アドレス (A) レコードを作成する必要があります。[A レコード (A record)] フィールドに 192.168.50.1 と入力して、**Specify Glue Records** をクリックします。次に、**Report**、**Run**、および **Return** をクリックします。
 - c) [ゾーンの一覧表示/追加 (List/Add Zones)] ページに example.com と boston.example.com が表示されません。
- ステップ 5 **Advanced** をクリックしてから **Show Forward Zone Tree** をクリックして、ゾーンの階層を表示します。リスト モードに戻るには、**Show Forward Zone List** をクリックします。

逆引きゾーンの作成

次に、example.com と boston.example.com の逆引きゾーンを作成します。これにより、追加された各ホストの逆引きアドレス ポインタ (PTR) レコードを追加できます。Example.com の逆引きゾーンは、192.168.50.0 サブネットに基づきます。boston.example.com の逆引きゾーンは、192.168.60.0 サブネットに基づきます。

ローカル基本 Web UI

- ステップ 1 ローカルクラスタで、前のセクションと同じように、example-zone-admin ユーザーとしてログインします。
- ステップ 2 [設計 (Design)] メニューから、**Reverse Zones** サブメニューの **Auth DNS** を選択します。

- ステップ 3** [逆引きゾーンの一覧表示/追加 (List/Add Reverse Zones)] ページで、[逆引きゾーン (Reverse Zones)] ページの [逆引きゾーンの追加 (Add Reverse Zone)] アイコンをクリックし、[名前 (Name)] フィールドに **50.168.192.in-addr.arpa** と入力します。(ループバック アドレス 127.in-addr.arpa の逆引きゾーンは既に存在します)。
- ステップ 4** 転送ゾーンの値を使用し、必要なフィールドに入力して、逆引きゾーンを作成します。
- Nameserver - ns1.example.com.** を入力します (必ず末尾のドットを含めてください)。
 - Contact E-Mail - hostadmin.example.com.** を入力します (必ず末尾のドットを含めてください)。
 - [シリアル番号 (Serial number)] - シリアル番号を入力します。
- ステップ 5** **Add Reverse Zone** クリックして、ゾーンを追加し、[逆引きゾーンの一覧表示/追加 (List/Add Reverse Zones)] ページに戻ります。
- ステップ 6** boston.example.com ゾーンについて同じことをしますが、ゾーン名として **60.168.192.in-addr.arpa** を使用し、**ステップ 4** と同じネームサーバーと連絡先電子メール値を使用します。(テーブルから値をカットアンドペーストすることができます)。

最初のホストの作成

ボストン クラスタでホストを作成できることを確認するために、example-zone-admin は example.com ゾーンで 2 つのホストの作成を試みます。

ローカル詳細 Web UI

- ステップ 1** example-zone-admin ユーザーとして、**Advanced** をクリックして詳細モードに入ります。
- ステップ 2** [設計 (Design)] メニューから、**Hosts** サブメニューの **Auth DNS** を選択します。[ゾーンのホストの一覧表示/追加 (List/Add Hosts for Zones)] ページが開きます。ウィンドウの左側にある [ゾーンの選択 (Select Zones)] ボックスに、boston.example.com と example.com が表示されます。
- ステップ 3** ゾーンのリストの example.com をクリックします。
- ステップ 4** アドレス 192.168.50.101 を持つ最初の静的ホストを追加します。
- [名前 (Name)] フィールドに **userhost101** と入力します。
 - [IP アドレス (IP Address(es))] フィールドに完全なアドレス **192.168.50.101** を入力します。[IPv6 アドレス (IPv6 Address(es))] フィールドと [エイリアス (Alias(es))] フィールドは空白のままにします。
 - [PTR レコードの作成 (Create PTR Records?)] チェックボックスがオンになっていることを確認します。
 - Add Host** をクリックします。
- ステップ 5** 同じ方法で、2 番目のホスト **userhost102** をアドレス **192.168.50.102** で追加します。2 つのホストが、[ゾーンのホストの一覧表示/追加 (List/Add Hosts for Zone)] ページにネームサーバー ホストとともに表示されます。

制約付きのホスト管理者ロールの作成

チュートリアルはこの部分では、ボストンの `example-cluster-admin` は `boston.example.com` ゾーンにアドレス制約付きの `example-host-role` を作成します。

ローカル詳細 Web UI

- ステップ 1** `example-zone-admin` ユーザとしてログアウトし、**example-cluster-admin** ユーザー（パスワード `exampleadmin`）としてログインします。
- ステップ 2** [詳細 (**Advanced**)] をクリックして、詳細モードに入ります。
- ステップ 3** [管理 (**Administration**)] メニューから、[ユーザー アクセス (User Access)] サブメニューの [ロール (**Roles**)] を選択して、[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページを開きます。
- ステップ 4** `example-host-role` を追加します。
- [ロール (Roles)] ペインの [ロールの追加 (Add Role)] アイコンをクリックして、[ロールの追加 (Add Roles)] ダイアログボックスを開きます。
 - [名前 (Name)] フィールドに **example-host-role** と入力します。
 - [ロールの追加 (Add Role)] をクリックします。 `example-host-role` が、[管理者ロールの一覧表示/追加 (List/Add Administrator Roles)] ページのロールのリストに表示されます。
- ステップ 5** ロールの制約を追加します。
- [制約の追加 (**Add Constraint**)] をクリックします。
 - [ロールの制約の追加 (Add Role Constraint)] ページで、[ホスト制限 (Host Restrictions)] まで下にスクロールします。
 - `all-forward-zones` 属性について、**false** ラジオ ボタンをクリックします。
 - `zones` 属性として、**boston.example.com** と入力します。
 - `ipranges` 属性として、範囲 **192.168.50.101–192.168.50.200** を入力します。
 - `zone-regexp` および `host-regexp` 属性フィールドには、正規表現を入力して、それぞれゾーンとホストを正規表現構文で照合します。（よく使用される正規表現の値については、次の表を参照してください）。

表 15: 一般的な正規表現の値

値	一致
.	任意の文字 (ワイルドカード)。ドット文字そのもの (ドメイン名など) に一致させるには、バックスラッシュ (\) を使用してエスケープする必要があります (\.com は .com に一致します)。
\char	続くりテラル文字 (<i>char</i>)、または <i>char</i> には特別な意味があります。特にドット (.) やもう1つのバックスラッシュなどのメタ文字をエスケープするために使用されます。特別な意味としては、10進数に一致させる \d、非数字に一致させる \D、英数字に一致させる \w、および空白に一致させる \s があります。
char?	先行する1個または0個の <i>char</i> は、その文字が任意であることを意味します。たとえば、 example\?.com は <code>example.com</code> または <code>examplecom</code> に一致します。

値	一致
<i>char*</i>	先行する 0 個以上の <i>char</i> 。たとえば、 ca*t は ct 、 cat 、および caaat に一致します。この反復メタキャラクターは、文字セットで反復処理を行います ([文字セット]を参照)。
<i>char+</i>	先行する 1 個以上の <i>char</i> 。たとえば、 ca+t は cat と caaat に一致します (ct には一致しません)。
[<i>charset</i>]	ブラケットで囲まれた任意の文字 (文字セット)。[a-z] (任意の小文字と一致する) など、文字範囲を含めることができます。* 繰り返しメタ文字が適用されている場合、検索エンジンは、一致に影響を与えるために必要な回数だけセットを繰り返します。たとえば、 a[bcd]*b は、 abcdb を見つけます (2 回目のセットを繰り返ることによって)。メタ文字の多く (ドットなど) は非アクティブであり、文字セット内ではリテラルと見なされることに注意してください。
[^charset]	<i>charset</i> 以外の任意の文字。たとえば、[^a-zA-Z0-9] は非英数字に一致します (\W を使用することと同じ)。文字セットの外側のキャレットは異なる意味を持つことに注意してください。
^	行頭。
\$	行末。

g) **Add Constraint** をクリックします。制約のインデックス番号は 1 になります。

ステップ 6 **Save** をクリックします。

ホスト管理者に割り当てるグループの作成

ボストンの **example-cluster-admin** は、**example-host-role** を含む **example-host-group** を作成して、**example-zone-admin** がこのグループを **example-host-admin** に割り当てるようにします。

ローカル詳細 Web UI

ステップ 1 **example-cluster-admin** として、詳細もノードのままで、[管理 (Administration)] メニューから **Groups** サブメニューを選択して、[管理者グループの一覧表示/追加 (List/Add Administrator Groups)] ページを開きます。

ステップ 2 **example-host-group** を作成して、それに **example-host-role** を割り当てます。

- [グループ (Groups)] ペインの [グループの追加 (Add Groups)] アイコンをクリックし、[名前 (Name)] フィールドに **example-host-group** と入力します。
- [ベース ロール (Base Role)] ドロップダウン リストから、**example-host-role** を選択します。
- Add Group** をクリックします。

d) **Group for the example-host-role** のような説明を追加して、[保存 (Save)] をクリックします。

ステップ 3 example-cluster-admin としてログアウトしてから、**example-zone-admin** ユーザー (パスワード **examplezone**) としてログインします。

ステップ 4 example-zone-admin として、example-host-group を example-host-admin に割り当てます。

- a) 基本モードで、**Administration** メニューから **Administrators** を選択します。
- b) [管理者の一覧表示/追加 (List/Add Administrators)] ページで、example-host-admin をクリックして管理者を編集します。
- c) [管理者の編集 (Edit Administrator)] ページで、[使用可能 (Available)] リストの **example-host-group** を選択し、<< をクリックして、[選択済み (Selected)] リストに移動します。
- d) **Save** をクリックします。example-host-admin は [List/Add Administrators] ページの [Groups] 列に example-host-group が表示されているのを確認できます。

ホストアドレス範囲のテスト

example-host-admin は次に、範囲外のアドレスをテストし、受け入れ可能なアドレスを追加します。

ローカル詳細 Web UI

ステップ 1 ローカル クラスタで、example-zone-admin としてログアウトしてから、**example-host-admin** として (パスワード **examplehost** を使用して) ログインします。

ステップ 2 **Advanced** をクリックして、詳細モードに入ります。

ステップ 3 **Design** メニューから、**Auth DNS** サブメニューの **Hosts** を選択します。

ステップ 4 [ゾーンのホストの一覧表示/追加] ページで、範囲外のアドレスを入力してみてください ([有効な IP 範囲 (Valid IP Ranges)] フィールドの有効なアドレスの範囲に注意してください)。

- a) [名前 (Name)] フィールドに **userhost3** と入力します。
- b) [IP アドレス (IP Address(es)) **192.168.50.3**] フィールドに、故意に範囲外のアドレスを入力します。
- c) **Add Host** をクリックします。エラー メッセージが表示されます。

ステップ 5 有効な IP アドレスを入力します。

- a) **userhost103** を入力します。
- b) [IP アドレス (IP Address(es))] フィールドに **192.168.50.103** を入力します。
- c) **Add Host** をクリックします。ホストがアドレスとともにリストに表示されます。

リージョンクラスタ管理チュートリアル

このチュートリアルは、[ローカルクラスタ管理チュートリアル \(151 ページ\)](#) で説明されているシナリオの拡張です。リージョンクラスタのチュートリアルでは、サンノゼに2名の管理者 (リージョンクラスタ管理者と中央設定管理者) がいます。彼らの目的は、これらのクラスタ

のサーバーを使用して、DNS ゾーン配布、ルータ設定、および DHCP フェールオーバー設定を作成するために、ボストンおよびシカゴのローカルクラスタとアクティビティを調整することです。構成は、次のとおりです。

- サンノゼの 1 つのリージョン クラスタ マシン。
- 2 つのローカル クラスタ マシン (ボストンに 1 つ、シカゴに 1 つ)。
- シカゴに 1 つの Cisco uBR7200 ルータ。

関連項目

- [管理者の責任とタスク \(160 ページ\)](#)
- [リージョン クラスタ管理者の作成 \(161 ページ\)](#)
- [中央構成管理者の作成 \(161 ページ\)](#)
- [ローカル クラスタの作成 \(162 ページ\)](#)
- [ルータの追加とインターフェイスの変更 \(163 ページ\)](#)
- [構成管理者へのゾーン管理の追加 \(164 ページ\)](#)
- [ローカル クラスタのゾーンの作成 \(164 ページ\)](#)
- [ゾーン データのプルとゾーン分散の作成 \(165 ページ\)](#)
- [サブネットの作成とアドレス空間のプル \(166 ページ\)](#)
- [DHCP ポリシーのプッシュ \(166 ページ\)](#)
- [スコープ テンプレートの作成 \(167 ページ\)](#)
- [フェールオーバー ペアの作成と同期 \(168 ページ\)](#)
- [リージョンクラスタの再構築 \(233 ページ\)](#)

管理者の責任とタスク

リージョン管理者には、次の責任とタスクがあります。

- **example-regional-admin**- サンノゼのリージョン クラスタで、**example-cfg-admin** を作成するスーパーユーザーによって作成されます。
- **example-cfg-admin** :
 - ボストンおよびシカゴのクラスタを定義し、それらとの接続を確認します。
 - ルータおよびルータ インターフェイスを追加します。
 - ローカル クラスタからゾーン データをプルして、ゾーン配布を作成します。
 - サブネットとポリシーを作成し、アドレス空間をプルして、ボストンとシカゴの DHCP フェールオーバー ペアを設定します。

リージョン クラスタ管理者の作成

リージョンのスーパーユーザーは、まず、クラスタとユーザーの管理を実行するために、グループとともに定義された `example-regional-administrator` を作成します。

リージョン Web UI

- ステップ 1** スーパーユーザーとしてリージョン クラスタにログインします。
- ステップ 2** [管理 (Administration)] メニューから [ユーザーアクセス (User Access)] サブメニューの [管理者 (Administrators)] を選択して、このページのローカル クラスタ バージョンの [管理者の一覧表示/追加 (Add Administrators)] ページを開きます。これは基本的に同じです。
- ステップ 3** [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックし、[名前 (Name)] フィールドに `example-regional-admin` と入力し、[パスワード (Password)] フィールドと [パスワードの再入力 (Confirm Password)] フィールドに `examplereg` と入力して、[管理者の追加 (Add Admin)] をクリックします。
- ステップ 4** [管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションにある [追加 (Add)] をクリックして、[グループ (Groups)] ウィンドウを開きます。 `central-cfg-admin-group` (クラスタ管理のため) および `regional-admin-group` (ユーザー管理のため) を選択し、[選択 (Select)] をクリックします。選択されたグループが、[管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションに表示されます。
- ステップ 5** **Save** をクリックします。

中央構成管理者の作成

このチュートリアルの一部として、`example-regional-admin` は次に、ログインして、`example-cfg-admin` を作成します。これは、リージョンの設定およびアドレス管理能力を持つ必要があります。

リージョン Web UI

- ステップ 1** スーパーユーザーとしてログアウトし、`example-regional-admin` としてパスワード `examplereg` でログインします。管理者には、ホストとアドレス空間のすべての管理権限があることに注意してください。
- ステップ 2** [管理 (Administration)] メニューから、[ユーザーアクセス (User Access)] サブメニューの [管理者 (Administrators)] を選択して、[管理者の一覧表示/追加 (List/Add Administrators)] ページを開きます。
- ステップ 3** [管理者 (Administrators)] ペインの [管理者の追加 (Add Administrators)] アイコンをクリックし、[名前 (Name)] フィールドに `example-cfg-admin` と入力し、[パスワード (Password)] フィールドと [パスワードの再入力 (Confirm Password)] フィールドに `cfgadmin` と入力して、[管理者の追加 (Add Admin)] をクリックします。
- ステップ 4** [管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションにある [追加 (Add)] をクリックして、[グループ (Groups)] ウィンドウを開きます。 `central-cfg-admin-group` および

regional-addr-admin-group を選択して、[選択 (Select)] をクリックします。選択されたグループが、[管理者の編集 (Edit Administrator)] ページの [グループ (Groups)] セクションに表示されます。

ステップ 5 [保存 (Save)] をクリックします。example-cfg-admin に割り当てられた 2 つのグループが表示されます。

管理者の制約を追加することもできます。[制約の追加 (Add Constraint)] をクリックし、[ロールのローカル制約の追加 (Add Role Constraint for Role)] ページで、読み取り専用、所有者、またはリージョン制約を選択し、[制約の追加 (Add Constraint)] をクリックします。

ローカルクラスタの作成

example-cfg-admin は次に、ボストンとシカゴの 2 つのローカルクラスタを作成します。

リージョン Web UI

ステップ 1 example-regional-admin としてログアウトし、**example-cfg-admin** としてパスワード **cfgadmin** でログインします。

ステップ 2 **Operate** メニューから、**Manage Clusters** サブメニューの **Servers** を選択して、[リモートクラスの一覧表示/追加 (List/Add Remote Clusters)] ページを開きます。

ステップ 3 [Add Manage Clusters クラスタの管理 (Manage Clusters)] ペインの アイコンをクリックします。

ステップ 4 [クラスタの追加 (Add Cluster)] ダイアログボックスで、管理者から提供されたデータに基づいてボストンクラスタを作成します。

- a) [名前 (Name)] フィールドに **Boston-cluster** と入力します。
- b) [IPv4 アドレス (IPv4 Address)] フィールドにボストンサーバーの IPv4 アドレスを入力します。
- c) [IPv6 アドレス (IPv6 Address)] フィールドにボストンサーバーの IPv6 アドレスを入力します。
- d) [管理者名 (Admin Name)] フィールドに **example-cluster-admin** と入力し、[管理者パスワード (Admin Password)] フィールドに **exampleadmin** と入力します。
- e) [SCP ポート (SCP Port)] フィールドに、インストール時に設定された、クラスタにアクセスする SCP ポートを入力します (**1234** はプリセット値です)。
- f) **Add Cluster** をクリックします。

ステップ 5 同じ方法でシカゴクラスタを作成しますが、[名前 (name)] フィールドに **Chicago-cluster** を使用し、残りの値はシカゴ管理者から提供されたデータに基づいて入力し、**Add Cluster** をクリックします。2 つのクラスタが [リモートクラスの一覧表示/追加 (List/Add Remote Clusters)] ページに表示されます。

ステップ 6 ボストンクラスタに接続します。Boston-cluster の横にある [ローカルに移動 (Go Local)] アイコンをクリックします。ローカルクラスタの [サーバーの管理 (Manage Servers)] ページが開いた場合、クラスタへの管理者の接続が確定されます。リージョンクラスタ Web UI に戻るには、[リージョンに移動 (Go Regional)] アイコンをクリックします。

ステップ 7 シカゴのクラスタに接続して、同じ方法で接続を確認します。

ステップ 8 ボストンのクラスタ同期から 2 つの転送ゾーンのデータを複製できることを確認します。

- a) **Operate** メニューから、**Servers** サブメニューの **View Replica Data** を選択します。

- b) [レプリカクラスリストの表示 (View Replica Class List)] ページで、[クラスタの選択 (Select Cluster)] リストの **Boston-cluster** をクリックします。
- c) [クラスの選択 (Select Class)] リストの **Forward Zones** をクリックします。
- d) [データの複製 (Replicate Data)] をクリックします。
- e) **View Replica Class List** をクリックします。[クラスタのレプリカ転送ゾーンの一覧表示 (List Replica Forward Zones for Cluster)] ページに、**boston.example.com** ゾーンと **example.com** ゾーンが表示されます。

ルータの追加とインターフェイスの変更

次の **example-cfg-admin** は、リージョンクラスタを引き継ぎ、ルータを追加し、インターフェイスの1つを変更して DHCP リレー エージェントを設定します。サブネットを手動で追加します。

リージョン詳細 Web UI

- ステップ 1** **example-cfg-admin** として、[展開 (Deploy)] メニューから、**Router Configuration** サブメニューの **Router List** を選択します。
- ステップ 2** [ルータの一覧表示/追加 (List/Add Routers)] ページで、[ルータ リスト (Router List)] ペインの [ルータの追加 (Add router)] アイコンをクリックします。
- ステップ 3** [ルータの追加 (Add Router)] ダイアログボックスで、管理者からのデータに基づいてルータを追加します。
 - a) [名前 (name)] フィールドにルータの識別名を指定します。この例では、**router-1** と入力します。
 - b) [説明 (description)] フィールドにルータの説明を入力します。
 - c) アドレス フィールドに、ルータの管理インターフェイス アドレスを入力します。
 - d) **ip6address** フィールドに、ルータの IPv6 管理インターフェイスのアドレスを入力します。
 - e) 所有者とリージョンを選択します。
 - f) **Add Router** をクリックします。これで、ルータが [ルータの一覧表示/追加 (List/Add Routers)] ページに表示されます。
- ステップ 4** ルータが作成されたことを確認します。**Router Tree** をクリックすると、[ルータのツリーの表示 (View Tree of Routers)] ページに、**router-1** のルータ インターフェイスの階層が表示されます。
- ステップ 5** ルータの DHCP リレー エージェントを設定します。
 - a) ルータの新しいインターフェイスを作成します。
 - b) [ルータのツリーの表示 (View Tree of Routers)] ページのインターフェイス名をクリックして、[ルータ インターフェイスの編集 (Edit Router Interface)] ページを開きます。(または、[ルータの一覧表示/追加 (List/Add Routers)] ページから、ルータに関連付けられている [インターフェイス (Interfaces)] アイコンをクリックし、[ルータのルータ インターフェイスの一覧表示 (List Router Interfaces for Router)] ページのインターフェイス名をクリックします)。
 - c) [ルータ インターフェイスの編集 (Edit Router Interface)] ページで、[ip-helper] フィールドに DHCP サーバーの IP アドレスを入力します。

d) ページ下部の **Save** をクリックします。

ステップ 6 ルータ管理者とともに、DHCP リレー エージェントが正常に追加されたことを確認します。

構成管理者へのゾーン管理の追加

Chicago クラスタにはゾーンがセットアップされていないため、**example-cfg-admin** はリージョン クラスタでゾーンを作成して、ゾーン分散の一部にすることができます。ただし、**example-regional-admin** は、まず、**example-cfg-admin** を変更して、ゾーンを作成できるようにする必要があります。

リージョン Web UI

ステップ 1 **example-cfg-admin** としてログアウトし、**example-regional-admin** としてログインします。

ステップ 2 [管理 (Administration)] メニューから、[ユーザー アクセス (User Access)] サブメニューの [グループ (Administrators)] を選択します。

ステップ 3 [管理者の一覧表示/追加 (List/Add Administrators)] ページで、[管理者 (Administrators)] ペインから **example-cfg-admin** をクリックします。

ステップ 4 [管理者の編集 (Edit Administrator)] ページで、[使用可能なグループ (Groups Available)] リストの **central-dns-admin-group** をクリックし、(<< を使用して) [選択済み (Selected)] リストに移動します。[選択済み (Selected)] リストに **central-cfg-admin-group**、**regional-admin-group**、および **central-dns-admin-group** が表示されます。

ステップ 5 **Save** をクリックします。変更が [管理者の一覧表示/追加 (List/Add Administrators)] ページに反映されます。

ローカル クラスタのゾーンの作成

example-cfg-admin は次に、ボストンおよびシカゴ ゾーンとのゾーン分散のための **chicago.example.com** ゾーンを作成します。

リージョン Web UI

ステップ 1 **example-regional-admin** としてログアウトし、**example-cfg-admin** としてログインします。

ステップ 2 [設計 (Design)] メニューから、[Auth DNS] サブメニューの **Forward Zones** を選択します。

ステップ 3 [転送ゾーン (Forward Zones)] ペインの **Add Forward Zone** アイコンをクリックします。

ステップ 4 [ゾーンの追加 (Add Zone)] ダイアログボックスで、次のように入力します。

- a) **Name - chicago.example.com**。
- b) **Nameserver FQDN - ns1**。
- c) **Contact E-mail - hostadmin**。
- d) **Nameservers - ns1 (Add Nameserver をクリック)**。

e) **Add DNS Zone** をクリックします。

ステップ 5 Reverse Zones サブメニューをクリックします。

ステップ 6 [逆引きゾーンの一覧表示/追加 (List/Add Reverse Zones)] ページで、適切な属性が設定された Chicago ゾーンの **60.168.192.in-addr.arpa** 逆引きゾーンを作成します。

ゾーンデータのプルとゾーン分散の作成

example-cfg-admin は次に、ボストンとシカゴからゾーンデータをプルして、ゾーン分散を作成します。

リージョン Web UI

ステップ 1 example-cfg-admin として、**Design** メニューから **Auth DNS** サブメニューの **Views** を選択して、[ゾーンビューの一覧表示/追加 (List/Add Zone Views)] ページを表示します。

ステップ 2 [ゾーンビューの一覧表示/追加 (List/Add Zone Views)] ページで、レプリカデータベースからゾーンをプルします。

- [Views] ペインの **Pull Data** アイコンをクリックします。
- [プルするレプリカ DNS ビューデータの選択 (Select Replica DNS View Data to Pull)] ダイアログボックスで、データ同期モードをデフォルトの [Update] のままにして、**Report** をクリックして、[プルレプリカゾーンデータの報告 (Report Pull Replica Zone Data)] ページを開きます。
- プルするデータの変更セットに注目してから、**Run** をクリックします。
- [プルレプリカゾーンデータの実行 (Run Pull Replica Zone Data)] ページで、**OK** をクリックします。

ステップ 3 [ゾーンビューの一覧表示/追加 (List/Add Zone Views)] ページで、ボストンクラスターゾーン分散に、[名前 (Name)] 列でインデックス番号 (**1**) が割り当てられていることに注意してください。番号をクリックします。

ステップ 4 [ゾーンビューの編集 (Edit Zone Views)] ページの [プライマリ サーバー (Primary Server)] フィールドで、Boston-cluster をクリックします。(Boston-cluster の IP アドレスは、[マスター サーバー (Master Servers)] リストの最初のマスターサーバーになります)。

ステップ 5 Chicago-cluster の DNS サーバーを Boston-cluster のセカンダリサーバーにするには、次のようにします。

- [セカンダリ サーバー (Secondary Servers)] エリアの **Add Server** をクリックします。
- [ゾーン分散セカンダリサーバーの追加 (Add Zone Distribution Secondary Server)] ページで、[セカンダリ サーバー (Secondary Server)] ドロップダウンリストから **Chicago-cluster** を選択します。
- Add Secondary Server** をクリックします。

ステップ 6 [ゾーン分散の編集 (Edit Zone Distribution)] ページの [転送ゾーン (Forward Zones)] エリアで、**chicago.example.com** を [選択済み (Selected)] リストに移動します。

ステップ 7 [逆引きゾーン (Reverse Zones)] エリアで、**60.168.192.in-addr.arpa** を [選択済み (Selected)] リストに移動します。

ステップ 8 **Modify Zone Distribution** をクリックします。

サブネットの作成とアドレス空間のプル

example-cfg-admin は次に、リージョン クラスタにサブネットを作成します。このサブネットは、ローカル クラスタからプルされた他の 2 つのサブネットと結合されて、DHCP フェールオーバー サーバー構成を作成します。

リージョン Web UI

-
- ステップ 1** example-cfg-admin として、**Design** メニューから **DHCPv4** サブメニューの **Subnets** を選択して、[サブネットの一覧表示/追加 (List/Add Subnets)] ページを開きます。ルータを追加することによって作成されたサブネットが表示されます (**ルータの追加とインターフェイスの変更 (163 ページ)** に)。
- ステップ 2** [サブネット (Subnets)] ペインの [サブネットの追加 (Add Subnets)] アイコンをクリックして、追加のサブネット 192.168.70.0/24 を作成します。
- [アドレス/マスク (Address/Mask)] フィールドにサブネット ネットワーク アドレスとして **192.168.70** (省略形) を入力します。
 - ネットワーク マスクとして **24** (255.255.255.0) を選択したままにします。
 - Add Subnet** をクリックします。
- ステップ 3** **Address Space** をクリックして、作成したサブネットを確認します。
- ステップ 4** [ユニファイドアドレス空間の表示 (View Unified Address Space)] ページで、**Pull Replica Address Space** をクリックします。
- ステップ 5** [プルレプリカアドレス空間の選択 (Select Pull Replica Address Space)] ページで、すべての項目をデフォルトのままにして、**Report** をクリックします。
- ステップ 6** [プルレプリカアドレス空間の報告 (Report Pull Replica Address Space)] ページに、クラスタからの 2 つのサブネットの変更セットが表示されます。**Run** をクリックします。
- ステップ 7** **OK** をクリックします。プルされた 2 つのサブネットが、[サブネットの一覧表示/追加 (List/Add Subnets)] ページに表示されます。
-

DHCP ポリシーのプッシュ

example-cfg-admin は次に、DHCP ポリシーを作成し、ローカル クラスタにプッシュします。

リージョン Web UI

-
- ステップ 1** example-cfg-admin として、**Design** メニューから **DHCP Settings** サブメニューの **Policies** を選択します。
- ステップ 2** [DHCP ポリシーの一覧表示/追加 (List/Add DHCP Policies)] ページで、[ポリシー (Policies)] ペインの **Add Policies** アイコンをクリックします。
- ステップ 3** [DHCP ポリシーの追加 (Add DHCP Policy)] ダイアログボックスで、すべてのローカルクラスタの中央ポリシーを作成します。
- [名前 (Name)] フィールドに **central-policy-1** と入力します。[オファーのタイムアウト (Offer Timeout)] 値と [猶予期間 (Grace Period)] の値はそのままにしておきます。

- b) [DHCP ポリシーの追加 (Add DHCP Policy)] をクリックします。
- c) [DHCP ポリシーの編集 (Edit DHCP Policy)] ページの [DHCPv4 オプション (DHCPv4 Options)] セクションで、[名前 (Name)] ドロップダウンリストから **dhcp-lease-time [51] (unsigned time)** を選択し、[値 (Value)] フィールドに、リース期間として **2w** (2 週間) と入力します。
- d) **Add Option** をクリックします。
- e) [保存 (Save)] をクリックします。

ステップ 4 ローカル クラスタにポリシーをプッシュします。

- a) ポリシー **central-policy-1** を選択して、**Push** ボタンをクリックします。
- b) [DHCP ポリシーデータをローカルクラスタにプッシュ (Push DHCP Policy Data to Local Clusters)] ページで、[データ同期モード (Data Synchronization Mode)] を **Ensure** のままにします。これにより、ポリシーがローカルクラスタで複製されますが、その名前のポリシーがすでに存在する場合は、その属性は置き換えられません。
- c) ページの [デスティネーションクラスタ (Destination Clusters)] セクションの **Select All** をクリックします。
- d) << をクリックして、両方のクラスタを [選択済み (Selected)] フィールドに移動します。
- e) **Push Data to Clusters** をクリックします。
- f) プッシュ操作の結果を表示するには、[DHCP ポリシーデータのプッシュ レポートの表示 (View Push DHCP Policy Data Report)] ページを表示します。

スコープテンプレートの作成

example-cfg-admin は、次に、フェールオーバー サーバー ペアの作成を処理する DHCP スコープテンプレートを作成します。

リージョン Web UI

- ステップ 1** example-cfg-admin ユーザーとして、[設計 (Design)] メニューから **DHCPv4** サブメニューの **Scope Templates** を選択します。
- ステップ 2** [DHCP スコープテンプレートの一覧表示/追加 (List/Add DHCP Scope Templates)] ページで、[スコープテンプレート (Scope Templates)] ペインの **Add Scope Templates** アイコンをクリックします。[名前 (Name)] フィールドに **scope-template-1** と入力して、[DHCP スコープテンプレートの追加 (Add DHCP Scope Template)] をクリックします。
- ステップ 3** テンプレートが [DHCP スコープテンプレートの一覧表示/追加 (List/Add DHCP Scope Templates)] ページに表示されます。スコープテンプレートの基本プロパティを設定します。フィールドに次の値を入力するか選択します。
 - a) **Scope Name Expression** - 派生スコープの名前を自動生成するには、example-scope 文字列と、スコープに対して定義されたサブネットを連結します。これを行うには、フィールドに (**concat “example-scope-” subnet**) と入力します (カッコも含めて)。
 - b) **Policy** - ドロップダウンリストの **central-policy-1** を選択します。

- c) **Range Expression - (create-range 2 100)** と入力することによって、サブネットの残り（2番目のアドレスから最後のアドレスまで）に基づいてアドレス範囲を作成します。
- d) **Embedded Policy Option Expression - (create-option “routers” (create-ipaddr subnet 1))** と入力することによって、組み込みポリシーでスコープのルータを定義し、サブネット内の最初のアドレスを割り当てます。

ステップ4 **Save** をクリックします。

フェールオーバー ペアの作成と同期

example-cfg-admin は次に、フェールオーバー サーバー ペア関係を作成し、フェールオーバー ペアを同期します。ボストンの DHCP サーバーがメインになり、シカゴのサーバーがバックアップになります。

リージョン Web UI

ステップ1 example-cfg-admin ユーザーとして、**[展開 (Deploy)]** メニューから、**DHCP** サブメニューの **Failover Pairs** を選択します。

ステップ2 [DHCPフェールオーバーペアの一覧表示/追加 (List/Add DHCP Failover Pairs)] ページで、[フェールオーバーペア (Failover Pairs)] ペインの **Add Failover Pair** アイコンをクリックします。

ステップ3 [DHCP フェールオーバー ペアの追加 (Add DHCP Failover Pair)] ダイアログボックスで、次の値を入力または選択します。

- a) **Failover Pair Name - central-fo-pair** を入力します。
- b) **Main Server - Boston-cluster** をクリックします。
- c) **Backup Server - Chicago-cluster** をクリックします。
- d) **Scope Template - scopetemplate-1** をクリックします。
- e) **Add Failover Pair** をクリックします。

ステップ4 フェールオーバー ペアをローカル クラスタと同期します。

- a) [DHCPフェールオーバーペアの一覧表示/追加 (List/Add DHCP Failover Pairs)] ページで、[同期 (Synchronize)] 列の [レポート (Report)] アイコンをクリックします。
- b) [フェールオーバー ペアの同期の報告 (Report Synchronize Failover Pair)] ページで、ネットワーク データのソースとして **Local Server** を受け入れます。
- c) 同期の方向として **Main to Backup** を受け入れます。
- d) 操作 **Update** を受け入れます。
- e) ページ下部の **Report** をクリックします。
- f) [フェールオーバー ペア同期レポートの表示 (View Failover Pair Sync Report)] ページで、**Run Update** をクリックします。
- g) **Return** をクリックします。

ステップ5 フェールオーバー設定を確認し、ボストン クラスタでサーバーをリロードします。

- a) [DHCP フェールオーバー ペアの一覧表示/追加 (List/Add DHCP Failover Pairs)] ページで、Boston-cluster の横にある [ローカルへ移動 (Go Local)] アイコンをクリックします。
- b) [DHCP サーバーの管理 (Manage DHCP Server)] ページの [リロード (Reload)] アイコンをクリックします。
- c) ページの上部にある [リージョンへ移動 (Go Regional)] アイコンをクリックして、リージョンクラスタに戻ります。

ステップ 6 フェールオーバー設定を確認し、同じ方法でシカゴクラスタにサーバーをリロードします。

CLI コマンド

フェールオーバー ペアを作成するには、**failover-pair name create main-cluster/address backup-cluster/address [attribute=value ...]** を使用します。次に例を示します。

```
nrcmd> failover-pair example-fo-pair create Example-cluster Boston-cluster
```

フェールオーバー ペア設定を同期するには、**failover-pair name sync {update | complete | exact} [{main-to-backup | backup-to-main}] [-report-only | -report]** を使用します。次に例を示します。

```
nrcmd> failover-pair example-fo-pair sync exact main-to-backup -report
```




第 7 章

ルータおよびルータ インターフェイスの管理

この章では、Cisco Prime Network Registrar でルータおよびルータ インターフェイスを追加および編集する方法について説明します。

- [ルータの追加 \(171 ページ\)](#)
- [ルータの編集 \(172 ページ\)](#)
- [ルータ インターフェイスの表示と編集 \(172 ページ\)](#)
- [ルータのサブネットのプッシュと再利用 \(174 ページ\)](#)

ルータの追加

ローカル詳細およびリージョン Web UI

ステップ 1 Deploy メニューから、**Router List Router Configuration** サブメニューの (リージョン Web UI で) または **Routers** (ローカル Web UI で) を選択します。[ルータの一覧表示/追加 (List/Add Routers)] ページが開きます。

ステップ 2 Add Routers アイコンをクリックします。[ルータの追加 (Add Router)] ページが開きます。

ステップ 3 [ルータの追加 (Add Router)] ダイアログボックスで、管理者からのデータに基づいてルータを追加します。

- a) [名前 (name)] フィールドにルータの識別名を指定します。
- b) [説明 (description)] フィールドにルータの説明を入力します。
- c) [アドレス (address)] フィールドにルータの IP アドレスを入力します。
- d) アドレス フィールドに、ルータの管理インターフェイス アドレスを入力します。
- e) ip6address フィールドに、ルータの IPv6 管理インターフェイスのアドレスを入力します。
- f) 所有者とリージョンを選択します。

ステップ 4 Add Router をクリックします。

CLI コマンド

router name create address [attribute=value] を使用してルータを追加します。アドレスは IPv4 または IPv6 を使用できます。

次に例を示します。

```
nrcmd> router router-1 create 192.168.121.121
```

ルータの編集

ルータの編集には、一部のルータ属性の変更が含まれます。

ローカル詳細およびリージョン Web UI

左側の [ルータ ツリー (Router Tree)] ペインまたは [ルータ リスト (Router List)] ペインで、ルータ名をクリックします。[ルータの編集 (Edit Router)] ページで、さまざまな属性の値を入力できます。さらに、**Unset** チェックボックスを使用して属性を無効にすることもできます。変更を行ってから、**Save** をクリックします。

CLI コマンド

router name set attribute=value [attribute=value ...] を使用して、ルータ属性を編集します。次に例を示します。

```
nrcmd> router router-1 set owner=owner-1
```

ルータ インターフェイスの表示と編集

ルータ インターフェイスを編集するには、その属性の一部を変更する必要があります。

ローカル詳細およびリージョン Web UI

[ルータの一覧表示/追加 (List/Add Routers)] ページでルータに関連付けられている **Interfaces** タブをクリックすると、関連するケーブルまたはイーサネットインターフェイスのリストが表示されます。このページと左側の [ルータ ツリー (Router Tree)] ペインの両方から、インターフェイス名をクリックして編集できます。[インターフェイス (Interfaces)] タブには、インターフェイスを削除するオプションも含まれています (インターフェイスに対応する [削除 (Delete)] アイコンをクリックします)。インターフェイスの編集には、追加属性 **Unset** 機能も含まれます。仮想ルータのインターフェイスの追加、編集、または削除を無制限に行うことができます。ルータ インターフェイスのアドレス、サブネット、およびプレフィックスを修飾する **vpn-id** も、[ルータ インターフェイスの編集 (Edit Router Interface)] ページで選択できます。



(注) ルータ インターフェイスの変更は、ルータ インターフェイスの削除とその後の追加として実行されます。

CLI コマンド

ルータ インターフェイスの属性を編集するには、**router-interface name set attribute=value** を使用します。次に例を示します。

```
nrcmd> router-interface Ethernet1/0 set ip-helper=192.168.121.122
```

関連項目

[変更可能ルータ インターフェイス属性 \(173 ページ\)](#)

[インターフェイスのバンドル \(173 ページ\)](#)

変更可能ルータ インターフェイス属性

ルータ インターフェイスの属性を編集する場合、次の属性を変更できます。

- 名前
- MAC アドレス
- 説明
- インターフェイス上のプライマリ サブネット アドレスのアドレス
- インターフェイス上のセカンダリ サブネットのアドレス
- インターフェイスの任意の IP ヘルパー (DHCP リレー エージェント) のアドレス
- インターフェイスのユニキャスト パケットを受け入れる DHCP サーバーのケーブル ヘルパーのアドレス
- ルータ インターフェイスに関連付けられているリンク
- ルータ インターフェイスの IPv6 アドレス
- インターフェイス用に設定された IPv6 DHCP リレー宛先アドレス

インターフェイスのバンドル

インターフェイス バンドルは、ルータ インターフェイス間のロード バランシングを提供します。バンドルを定義するときには、バンドル内のすべての参加インターフェイスが同じバンドル識別子 (ID) を持つ必要があります。これは、マスターとして指定されたインターフェイスの名前です。

バンドルを使用する場合は、[Edit Router Interface] ページの [インターフェイスのバンドル設定] セクションに次の属性があるか、または CLI で **router-interface** コマンドを使用して設定しません。

- *bundle-id* - インターフェイスバンドル識別子。マスターインターフェイスの名前。バンドル内の参加しているすべてのインターフェイスは、同じバンドル ID を持つ必要があります。
- *is-master* - このインターフェイスは、バンドル内のマスターインターフェイスです。

ルータのサブネットのプッシュと再利用

サブネットをルータインターフェイスにプッシュしたり、サブネットを再利用したりすることができます（『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「サブネットの再利用」の項を参照）。仮想ルータを使用してサブネットをプッシュまたは再利用すると、ルータインターフェイスに設定されているすべてのプライマリおよびセカンダリ関係は、関連するサブネットとスコープについても設定されます。



第 8 章

サーバーとデータベースの保守

この章では、ローカルおよびリージョンサーバーの運用を管理および制御する方法について説明します。

- [サーバーの管理 \(175 ページ\)](#)
- [反復タスクのスケジューリング \(178 ページ\)](#)
- [ログ \(179 ページ\)](#)
- [データ整合性ルールの実行 \(186 ページ\)](#)
- [サーバー ステータスのモニターリングと報告 \(189 ページ\)](#)
- [DHCP および DNS サーバーのトラブルシューティング \(209 ページ\)](#)
- [TAC ツールの使用 \(215 ページ\)](#)
- [TFTP サーバーのトラブルシューティングと最適化 \(218 ページ\)](#)

サーバーの管理

ccm-admin ロールの `server-management` サブロールが割り当てられている場合、Cisco Prime Network Registrar サーバーを次のように管理できます。

- **Start-** データベースをロードし、サーバーを起動します。
- **Stop-** サーバーを停止します。
- **Reload-** サーバーを停止し、再起動します。(保護された RR の更新であっても、すべての RR 更新に対してサーバーをリロードする必要はありません。詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド*』の「DNS アップデートの管理」の章を参照してください)。
- **Check statistics - 統計の表示 (192 ページ)** を参照してください。
- **View logs - ログの検索 (184 ページ)** を参照してください。
- **Manage interfaces - サーバー インターフェイスを管理する方法については、特定のプロトコルのページを参照してください。**

サーバーの起動と停止は説明不要です。サーバーをリロードすると、Cisco Prime Network Registrar は、3つの手順を実行します。つまり、サーバーを停止し、設定データをロードし、サーバーを再起動します。サーバーをリロードした後にのみ、設定の変更が使用されます。



- (注) CDNS、DNS、DHCP、および SNMP サーバーはデフォルトで有効になっており、リブート時に開始されます。TFTP サーバーは、デフォルトでは有効になっていない、リブート時に起動しません。これを変更するには、CLI で `[server] type enable` または `disable start-on-reboot` を使用します。



- (注) DHCP、DNS、または TFTP サーバーの `exit-on-stop` 属性が有効になっている場合、属性が無効になっている間は、最後の起動（リロード）からの統計情報とスコープ使用率のデータのみが報告され、リロード全体の情報が表示されます。

ローカル基本または詳細とリージョン Web UI

ユーザーのロールに応じて、次の方法でプロトコル サーバーを管理できます。

- **Local or regional cluster administrator - [Operate]** メニューから **[サーバーの管理 (Manage Servers)]** を選択して、**[サーバーの管理 (Manage Servers)]** ページを開きます。

サーバー管理へのローカルおよびリージョン クラスタ Web UI アクセスは同じですが、使用可能な機能が異なります。リージョン管理者として、リージョン CCM サーバーとサーバーエージェントの状態と正常性を確認できます。ただし、統計、ログ、またはインターフェイスを停止、開始、リロード、または表示することはできません。

ローカルクラスタで、DHCP、DNS、CDNS、TFTP、または SNMP サーバーを管理するには、**[サーバーの管理 (Manage Servers)]** ペインでサーバーを選択し、次のいずれかを実行します。

- **[統計 (Statistics)]** タブをクリックして、サーバーの統計を表示します。[\(統計の表示 \(192 ページ\)\)](#) を参照してください。
- **[View Log]** 列の **[Logs]** タブをクリックして、サーバーのログメッセージを表示します。[\(ログの検索 \(184 ページ\)\)](#) を参照してください。
- **[サーバーの起動 (Start Server)]** ボタンをクリックして、サーバーを起動します。
- **[サーバーの停止 (Stop Server)]** ボタンをクリックして、サーバーを停止します。
- **[サーバーの再起動 (Restart Server)]** ボタンをクリックして、サーバーを再起動します。

- **Local cluster DNS administrator - [Deploy]** メニューから **[DNS Server]** を選択して、**[DNS 権威サーバーの管理 (Manage DNS Authoritative Server)]** ページを開きます。

統計、起動ログ、ログ、HA DNS サーバー ステータス、サーバーの起動、サーバーの停止、およびサーバーの再起動機能のほかに、**[コマンド (Commands)]** ボタンをクリックして **[DNS コマンド (DNS Commands)]** ダイアログ ボックスを開くと、その他の機能を実行することもできます。

サーバー コマンドの機能は、次のとおりです。

- **すべてのゾーン転送の強制**（『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「ゾーン転送の有効化」の項を参照） - [実行 (Run)] アイコンをクリックします。これは、CLI の **dns forceXfer secondary** と同じです。
- **すべてのゾーンのスカベンジング**（『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「動的レコードのスカベンジング」の項を参照） - [実行 (Run)] アイコンをクリックします。これは、CLI での **dns scavenge** と同じです。
- **Local cluster Caching DNS server— [Deploy] メニューから [CDNS Server] を選択して、[DNS キャッシングサーバーの管理 (Manage DNS Caching Server)] ページを開きます。**

統計、起動ログ、ログ、サーバーの起動、サーバーの停止、およびサーバーの再起動機能のほかに、[コマンド (Commands)] ボタンをクリックして [DNS コマンド (DNS Commands)] ダイアログ ボックスを開くと、その他の機能を実行することもできます。

詳細およびエキスパート モードでは、キャッシング CDNS キャッシュをフラッシュし、リソース レコードをフラッシュできます。コマンドを実行するには、[コマンド (Commands)] ボタンをクリックします。
- **Local cluster DHCP administrator - [Deploy] メニュー の [DHCP サーバー (Server)] をクリックして、[DHCP サーバーの管理 (Manage DHCP Server)] ページを開きます。**

統計、起動ログ、ログ、サーバーの起動、サーバーの停止、およびサーバーの再起動機能のほかに、[コマンド (Commands)] ボタンをクリックして [DHCP サーバー コマンド (DHCP Server Commands)] ダイアログ ボックスを開くと、その他の機能を実行することもできます。

このページには、制限 ID を使用したリース取得機能が用意されています。これにより、共通の制限識別子を使用して関連付けられているクライアントを検索できます（『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「管理オプション 82 の制限」を参照）。[IP アドレス (IP Address)] フィールドに、現在アクティブなリースの IP アドレスを少なくとも 1 つ入力して、[実行 (Run)] アイコンをクリックします。また、制限 ID 自体を *nn:nn:nn* の形式で入力するか、文字列 ("*nnnn*") として入力することもできます。その場合は、IP アドレスが検索対象のネットワークになります。この機能は、CLI の **dhcp limitationList ipaddress [limitation-id] show** と同じです。

CLI コマンド

CLI では、リージョン クラスタは CCM サーバー管理のみを許可します。

- サーバーを起動するには、**server type start** を使用します（または単に **type start**、たとえば、**dhcp start**）。
- サーバーを停止するには、**server type stop** を使用します（または単に **type stop**、たとえば、**dhcp stop**）。サーバーを停止する場合は、まず、**save** コマンドを使用して保存することをお勧めします。
- サーバーをリロードするには、**server type reload** を使用します（または単に **type reload**、たとえば、**dhcp reload**）。Cisco Prime Network Registrar は、選択したサーバーを停止し、設定データをロードしてから、サーバーを再起動します。

- サーバーの属性を設定または表示するには、`[server] type set` 属性=値または `[server]type show` を使用します。次に例を示します。

```
nrcmd> ccm set ipaddr=192.168.50.10
```

反復タスクのスケジューリング

ローカルクラスタ Web UI の基本および詳細ユーザー モードでは、多数の反復タスクをスケジュールできます。タスクは、次のとおりです。

- DHCP サーバーをリロードします。
- DNS サーバーをリロードします。
- DHCP フェールオーバー サーバー ペアの同期：
 - ステージング dhcp 編集モードで、メイン DHCP サーバーをリロードします。
 - フェールオーバー設定をバックアップ DHCP サーバーに同期させます。
 - ステージング dhcp 編集モードで、バックアップ DHCP サーバーをリロードします。
- 高可用性 (HA) DNS サーバー ペアの同期：
 - ステージング dhcp 編集モードで、メイン DNS サーバーをリロードします。
 - HA DNS 設定をバックアップ DNS サーバーに同期させます。
 - ステージング dhcp 編集モードで、バックアップ DNS サーバーをリロードします。
- ゾーン分散マップの同期：
 - ステージング dhcp 編集モードで、メイン DNS サーバーをリロードします。
 - ステージング dhcp 編集モードで、バックアップ HA DNS サーバーをリロードします。
 - ゾーン分散マップを同期します。
 - ステージング dhcp 編集モードで、セカンダリ DNS サーバーをリロードします。

ローカル基本または詳細 Web UI

これらの反復サーバー タスクを 1 つ以上セットアップするには、次の手順を実行します。

ステップ 1 Operate メニューから、[サーバー (Servers)] サブメニューの **Schedule Tasks** を選択して、[スケジュールされたタスクの一覧表示/追加 (List/Add Scheduled Tasks)] ページを開きます。

ステップ 2 左側の [スケジュールされたタスク (Scheduled Tasks)] ペインの [スケジュールされたタスクの追加 (Add Scheduled Task)] アイコンをクリックして、[スケジュールされたタスクの追加 (Add Scheduled Task)] ページを開きます。

ステップ 3 適切なフィールドに値を入力します。

- スケジュールされたタスクの名前。これは、任意の識別テキスト文字列にすることができます。
- 次のように、使用可能なタスク タイプのリストからプルダウンします。

- **dhcp-reload-** DHCP サーバーをリロードします。

- **dns-reload**- DNS サーバーをリロードします。
- **cdns-reload**- キャッシング DNS サーバーをリロードします。
- **sync-dhcp-pair**- DHCP フェールオーバー サーバー ペアを同期します。
- **sync-dns-pair**- HA DNS フェールオーバー サーバー ペアを同期します。
- **sync-zd-map**- ゾーン分散マップを同期します。
- **sync-dns-update-map**- DNS 更新マップを同期します。

c) [Schedule Interval] フィールドに、15m や 4w2d など、スケジュールされたタスクの時間間隔を入力します。

ステップ 4 Add Scheduled Task をクリックします。

ステップ 5 [スケジュールされたタスクの一覧表示/追加 (List/Add Scheduled Tasks)] ページのタスクの名前をクリックした場合、[スケジュール済みタスクの編集 (Edit Scheduled Task)] ページで、タスクの実行中に発生した最後のステータスまたは最後のエラー (存在する場合) のリストを ([タスクステータス (Task Status)] セクションで) 確認できます。 **Run Now** をクリックして、タスクを今すぐ実行します。

(注) HA DNS サーバーがパートナーと通信する前に HA が有効になっている場合、DNS サーバーの起動とバックグラウンドのロードが遅くなります。DNS サーバーをリロードまたは再起動する前に、HA DNS サーバーがパートナーと通信できるようにする必要があります。

CLI コマンド

task コマンドにより、スケジュール済みタスクオブジェクトを設定できます。これらのオブジェクトにより、定期的な操作を自動的に実行できます。

スケジュール済みタスクを作成するには、**task name create task-type interval [sync-obj] [attribute=value]** を使用します。 **task-type** により、スケジュールするタスクのタイプを制御できます。使用可能なタスクタイプは、dhcp-reload、dns-reload、cdns-reload、sync-dhcp-pair、sync-dns-pair、sync-zd-map、および sync-dns-update-map です。

スケジュール済みタスクを削除するには、**task name delete** を使用します。

スケジュール済みタスクを編集するには、**task name set attribute=value [attribute=value ...]** を使用します。

ログ

ログ ファイル

次の表では、install path/logs ディレクトリ内の Cisco Prime IP Express ログファイルについて説明します。

表 16: .../logs ディレクトリ内のログファイル

コンポーネント	/logs ディレクトリ内のファイル	ローカル/リージョン	ログ
インストール	install_cnr_log	両方	インストールプロセス
アップグレード	ccm_upgrade_status_log	両方	アップグレードプロセス
	dns_upgrade_status_log	ローカル	アップグレードプロセス
	dhcp_upgrade_status_log	ローカル	アップグレードプロセス
サーバーエージェント	agent_server_1_log	両方	サーバーエージェントの起動と停止
ポート チェック	checkports_log	両方	ネットワーク ポート
DNS サーバー	name_dns_1_log	ローカル	DNS アクティビティ
	dns_startup_log	ローカル	DNS の起動アクティビティ
	dns_packet_log	ローカル (Local)	DNS パケットロギングメッセージ ²
CDNS サーバー	cdns_log	ローカル	CDNS アクティビティ
	cdns_startup_log	ローカル	CDNS の起動アクティビティ
	cdns_query_log	ローカル (Local)	CDNS クエリログエントリ ³
DHCP サーバー	name_dhcp_1_log	ローカル	DHCP アクティビティ
	dhcp_startup_log	ローカル	DHCP の起動アクティビティ
TFTP サーバー	file_tftp_1_log file_tftp_1_trace	ローカル	TFTP アクティビティ
	tftp_startup_log	ローカル	TFTP の起動アクティビティ
SNMP サーバー	cnrsnmp_log	両方	SNMP アクティビティ

コンポーネント	/logs ディレクトリ内のファイル	ローカル/リージョン	ログ
CCM データベース	config_ccm_1_log	両方	CCM の設定、開始、停止
	ccm_startup_log	両方	CCM の起動アクティビティ
Web UI	cnrwebui_log	両方	Web UI の状態
Tomcat/Web UI (cnrwebui サブディレクトリ内)	catalina.date.log.txt jsui_log.date.txt cnrwebui_access_log.date.txt	両方	Tomcat サーバーおよび Web UI の CCM データベース (新しいファイルが毎日作成されるため、定期的に古いログファイルをアーカイブします)。
リソース制限	ccm_monitor_log	両方	リソース制限アクティビティ。

- ² packet-logging が有効になっており、「packet」が packet-logging-file として設定されている場合は、パケットロギングメッセージが dns_packet_log ファイルにログ記録されます。このログファイルを表示するには、サーバーを再起動します。
- ³ クエリログ設定を有効になっている場合、クエリログエントリが cdns_query_log ファイルにログ記録されます。

DNS、DHCP、CDNS、CCM、および TFTP サーバーは、それぞれ事前設定された最大サイズの 10 MB を持つ多数のログ ファイルを生成できます。この事前設定値は、新規インストールにのみ適用されます。



- (注) 10.1 より前のバージョンからのアップグレードでは、ログファイルについては、古い事前設定済み (または明示的に設定された) 値の 100 万バイトが使用されます。

最初のログ ファイル名には _log サフィックスが付きます。このファイルの最大サイズに達すると、その名前に .01 バージョン拡張子が付加され、バージョン拡張子なしで新しいログファイルが作成されます。各バージョン拡張子は、作成された新しいファイルごとに1ずつ増分されます。ファイルが設定された最大数に達すると、最も古いファイルが削除され、次に古いファイルがその名前を引き継ぎます。DNS、DHCP、CDNS、CCM、および TFTP サーバーの場合、通常の最大数は 10 です。

Cisco Prime Network Registrar には server_startup_log ファイルもあります。これは、CCM、DHCP、DNS、および TFTP サーバーに適用されます。これらのファイルは、サーバーの起動フェーズとシャットダウンフェーズをログに記録します (情報は通常のログ ファイル情報と

同様です)。サーバーのスタートアップ ログ ファイルは、サーバーが最後に起動したときに報告された問題の診断に役立ちます。

これらの起動ログの数はサーバーに対して 4 で固定されており、サイズはサーバーあたり 10 MB に固定されています。



(注) 一部のユーザー コマンドでは、クラスタへの個別の接続が原因で、サーバー エージェント ログにユーザー認証エントリを作成できます。これらを別のユーザーによるシステム セキュリティ違反として解釈しないでください。

ロギングは、Syslog に転送することもできます。[cnr.conf ファイルの変更 \(210 ページ\)](#) を参照してください。

CLI コマンド

CLI で `[server] type serverLogs show` を使用して、DNS、DHCP、および TFTP サーバーの設定済み最大値を確認できます。これらのプロトコルのサーバー ログ ファイルの最大数 (`nlogs`) と最大サイズ (`logsize`) が表示されます。これらのパラメータは、`[server] type serverLogs set nlogs=nlogs logsize=logsize` を使用して調整できます。その他のログ ファイルについては、これらの最大値を調整することはできません。



(注) Cisco Prime Network Registrar を再起動するまで、サーバー ログへの変更は有効になりません。

サーバー イベントのロギング

Cisco Prime Network Registrar を起動すると、Cisco Prime Network Registrar システム アクティビティのロギングが自動的に開始されます。Cisco Prime Network Registrar では、すべてのログがデフォルトで次の位置に維持されます。

- Windows - `install-path\logs`
- Linux - `install-path/logs` (これらのログを表示するには、`tail -f` コマンドを使用します)



ヒント Windows イベントビューアがいっぱいになり、Cisco Prime Network Registrar が実行されなくなるのを避けるには、[イベント ログ設定 (Event Log Settings)] で **Overwrite Events as Needed** チェックボックスをオンにします。イベントがいっぱいになった場合は、イベントをファイルに保存してから、イベント ログのイベントをクリアします。

ローカル基本または詳細とリージョン Web UI

サーバーのロギングを Web UI で使用するには、サーバーの [サーバーの管理 (Manage Servers)] ページを開き ([サーバーの管理 \(175 ページ\)](#) を参照)、[ログ (Logs)] タブをクリックします。サーバーのログ ページが開きます。ログは時間順に表示され、最新のエントリを含むペー

ジから順に表示されます。以前のエントリを確認する必要がある場合は、ページの上部または下部にある左矢印をクリックします。

関連項目

[ログの検索 \(184 ページ\)](#)

[ロギングの形式と設定 \(183 ページ\)](#)

ロギングの形式と設定

サーバー ログ エントリには、次のカテゴリが含まれます。

- **Activity**- サーバーのアクティビティをログに記録します。
- **Info**- 起動やシャットダウンなど、サーバーの標準動作をログに記録します。
- **Warning**- 要求の処理中に、無効なパケット、ユーザーのミスコミュニケーション、またはスクリプトのエラーなどの警告をログに記録します。
- **Error**- メモリ不足、リソースの取得ができない、または設定のエラーなど、サーバーが正常に動作しないイベントをログに記録します。



(注) 警告とエラーは、Windows のイベントビューアに表示されます ([サーバー イベントのロギング \(182 ページ\)](#) のヒントを参照)。各サーバー モジュールのログ メッセージの説明については、[install-path/docs/msgid/MessageIdIndex.html](#) ファイルを参照してください。

ローカル基本または詳細とリージョン Web UI

ログに記録するイベントに影響を与えることができます。たとえば、ローカルクラスタの DNS および DHCP サーバーのロギングを設定するには、次のようにします。

- **DNS** - [導入 (Deploy)] メニューから、[DNS] サブメニューで [DNS サーバー (DNS Server)] を選択して、[DNS サーバーの管理 (Manage DNS Server)] ページを開きます。サーバーの名前をクリックして、[DNS サーバーの編集 (Edit DNS Server)] ページを開きます。[ログ設定 (Log Settings)] セクションを展開して、ログ設定を表示します。必要に応じて属性を変更し、[保存 (Save)] をクリックして、サーバーをリロードします。(DNS サーバーのパフォーマンスを最大化するためのログ設定については、『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「DNS サーバーのトラブルシューティング」の項の表を参照してください)。
- **DHCP** - [導入 (Deploy)] メニューから、[DHCP] サブメニューの [DHCP サーバー (DHCP Server)] を選択して、[DHCP サーバーの管理 (Manage DHCP Server)] ページを開きます。サーバーの名前をクリックして、[DHCP サーバーの編集 (Edit DHCP Server)] ページを開きます。[Logging] セクションを展開して、ログ設定を表示します。必要に応じて属性を変更し、[保存 (Save)] をクリックして、サーバーをリロードします。(DHCP サーバーのパフォーマンスを最大化するためのログ設定については、『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「DHCP サーバーの調整」の項の表を参照してください)。

- **CCM - [Operate]** メニューで、**[Servers]** サブメニューから **[Manage Servers]** を選択し、**[Manage Servers]** ページを開きます。サーバーの名前をクリックして、**[Edit Local CCM Server]** ページを開きます。**[Logging]** セクションを展開して、ログ設定を表示します。属性に必要な変更を加え、**[Save]** をクリックします（必要なログカテゴリを有効または無効にするには、[CCM サーバーの管理 \(115 ページ\)](#) の表を参照してください）。

CLI コマンド

それぞれのサーバーについて、**dns set log-settings=value**、**dhcp set log-settings=value**、**ccm set log-settings=value**、および **tftp set log-settings=value** を使用します。

ログの検索

Web UI は、アクティビティおよび起動ログ ファイル内のエントリを検索する便利な方法を提供します。正規表現文字列エントリを使用して、特定のメッセージテキスト、ログメッセージ ID、およびメッセージのタイムスタンプを検索できます。ページの上部または下部にある **[検索 (Search)]** アイコンの横にあるテキストフィールドに、正規表現構文で検索文字列を入力します。（たとえば、**name?** と入力すると、ログファイル内の文字列 **name** の出現が検索されます）。**[検索 (Search)]** アイコンをクリックすると、ログ検索の結果が表示されます。テーブルビューとテキストビューを切り替えるには、ページの上部と下部で使用可能な **[ページ (Page)]** アイコンをクリックします。

メッセージの全文を表示するには、ログメッセージの名前をクリックします。**[ログ検索結果 (Log Search Result)]** ページの **Close** をクリックすると、ブラウザ ウィンドウが閉じます。

変更ログの表示

Web UI で、設定に関連付けられている変更ログとタスクを表示できます。

ローカルおよびリージョン Web UI

Operate メニューから **Change Log** を選択します。変更ログを表示するには、**ccm-admin** または **regional-admin** ロールのデータベース サブロールが割り当てられている必要があります。

- **[変更ログの表示 (View Change Log)]** ページには、すべての変更ログが **DBSN** 名でソートされて表示されます。リストの下部を表示するには、ページの左下にある右矢印をクリックします。変更ログエントリの **DBSN** 番号をクリックして、**[変更セットの表示 (View Change Set)]** ページを開きます。

[変更ログの表示 (View Change Log)] ページでは、リストをフィルタリングして、手動でトリミングし、ファイルに保存することができます。次によって、リストをフィルタリングできます。

- 開始日と終了日
- 変更を開始した管理者
- 設定オブジェクト クラス

- 特定のオブジェクト
- OID-00:00:00:00:00:00:00:00 の形式のオブジェクト識別子 (ID)
- サーバー
- データベース

Filter List または **Clear Filter** をクリックします (セッション中に保持されるフィルタをクリアします)。[より古い (older than)] フィールドに日数の値を設定し、[削除 (Delete)] アイコンをクリックすることによって、レコードをトリミングするまでの日数を設定することで、変更ログのトリミングを開始できます。

変更ログエントリをカンマ区切り値 (CSV) ファイルに保存するには、[CSV 形式で保存 (Save to CSV Format)] アイコンをクリックします。

タスクが変更ログに関連付けられている場合は、[変更セットの表示 (View Change Set)] ページに表示されます。タスク名をクリックして、[CCM タスクの表示 (View CCM Task)] タスクページを開くことができます。

CLI コマンド

変更ログレコード (CSV 形式) をエクスポートするには、**export changeLog filename [attribute=value ...] [-all]** を使用します。

サーバー ログ設定の動的更新

DHCP および DNS サーバーは、サーバーの設定中のみ、サーバーのログに変更を登録します。これは、リロード時に発生します。サーバーのリロードには時間がかかります。Cisco Prime Network Registrar では、DHCP および DNS サーバーは、リロードせずに、ログ設定に変更を登録できます。

ローカル基本または詳細 Web UI

DHCP サーバーのログ設定を動的に更新するには、次の手順を実行します。

- ステップ 1** [展開 (Deploy)] メニューから、[DHCP] サブメニューの [DHCP サーバー (DHCP Server)] を選択します。[DHCP サーバーの管理 (Manage DHCP Server)] ページが表示されます。
- ステップ 2** 左側のペインで DHCP サーバーの名前をクリックして、[DHCP サーバーの編集 (Edit DHCP Server)] ページを開きます。
- ステップ 3** 必要に応じて設定を変更します。
- ステップ 4** ページ下部の [保存 (Save)] をクリックします。新しいログ設定が DHCP サーバーに適用されます。[DHCP サーバーの管理 (Manage DHCP Server)] ページに、更新されたページ更新時間が表示されます。

ローカル基本または詳細 Web UI

DNS サーバーのログ設定を動的に更新するには、次の手順を実行します。

- ステップ 1** [展開 (Deploy)] メニューから、[DNS] サブメニューの [DNS サーバー (DNS Server)] を選択します。
[DNS サーバーの管理 (Manage DNS Server)] ページが開きます。
- ステップ 2** 左側のペインで DNS サーバーの名前をクリックして、[DNS サーバーの編集 (Edit DNS Server)] ページを開きます。
- ステップ 3** 必要に応じて設定を変更します。
- ステップ 4** ページ下部の [保存 (Save)] をクリックします。新しいログ設定が DNS サーバーに適用されます。[DNS サーバーの管理 (Manage DNS Server)] ページに、更新されたページ更新時間が表示されます。
- (注) `dhcp-edit-mode` または `dns-edit-mode` が `synchronous` に設定されていて、サーバーが実行中の場合、サーバー ログ設定の変更はサーバーに伝達されます。

CLI コマンド

CLI を使用して DHCP または DNS サーバーのログ設定を動的に更新するには、適切な `edit-mode` が `synchronous` に設定されている必要があります。サーバー ログ設定を変更した後、`save` コマンドを使用して設定を保存します。

次に例を示します。

```
nrcmd> session set dhcp-edit-mode=synchronous
nrcmd> dhcp set log-settings=new-settings
nrcmd> save
```

データ整合性ルールの実行

整合性ルールを使用して、重複するアドレス範囲やサブネットなど、データの不整合をチェックできます。データ整合性ルールは、リージョンおよびローカル クラスタで設定できます。

[整合性ルールの一覧表示 (List Consistency Rules)] ページのテーブルには、これらのルールが記載されています。実行するルールの横にあるチェックボックスをオンにします。



- (注) `cnr_rules` など、Java SDK を使用する Java ツールを実行するときには、UNIX のロケールパラメータを `en_US.UTF-8` に設定する必要があります。

[整合性ルールの一覧表示 (List Consistency Rules)] ページには、すべてのルールを選択する機能と、選択をクリアする機能が含まれています。各ルール違反の詳細を表示したり、出力を表示したりすることができます。ユーザーが行ったルール選択は、ユーザーセッション中は永続的です。

ローカルおよびリージョン Web UI

整合性ルールを実行するには、次の手順を実行します。

ステップ 1 Operate メニューから、レポート (**Reports**)] サブメニューの **Consistency Reports** を選択します。

[整合性ルールの一覧表示 (List Consistency Rules)] ページが表示されます。

ステップ 2 リストされた各整合性ルールのうち、適用するルールのチェックボックスをオンにします。

- すべてのルールを選択するには、**Select All Rules** リンクをクリックします。
- すべての選択をクリアするには、**Clear Selection** リンクをクリックします。

ステップ 3 Run Rules をクリックします。

[整合性ルール違反 (Consistency Rules Violations)] ページが表示されます。ルールは違反タイプによって分類されます。

- 違反の詳細を表示するには、**Show Details** リンクをクリックします。
- 出力を表示するには、ページアイコンをクリックします。
- **[XML の表示 (Display XML)]** をクリックして、出力を XML 形式で表示します。

ステップ 4 Return to Consistency Rules をクリックして、[整合性ルールの一覧表示 (List Consistency Rules)] ページに戻ります。

CLI ツール

コマンドラインから **cnr_rules** 整合性ルール ツールを使用して、データベースの不整合がないかどうかを確認します。このツールを使用して、ルールの結果をテキストファイルまたは XML ファイルでキャプチャすることもできます。

cnr_rules ツールは、次の場所にあります。

- **Windows-** ...\bin\cnr_rules.bat
- **Linux-** .../usrbin/cnr_rules

cnr_rules ツールを実行するには、次のように入力します。

```
> cnr_rules -N username -P password [options]
```

- **-N username** - 指定された **username** を使用して認証します。
- **-P password** - 指定された **password** を使用して認証します。
- **[オプション (options)]** - 次の表に示すように、ツールの修飾オプションについて説明します。オプションを入力しなかった場合は、コマンドの使用法が表示されます。

表 17: `cnr_rules` オプション

オプション	説明
<code>-list</code>	<p>使用可能な整合性ルールを一覧表示します。</p> <p>(注) 使用可能なコマンドのリストは、<code>-N</code> オプションの値で指定された管理者の権限に合わせて調整されます。</p> <pre>> cnr_rules -N admin -P changeme -list</pre>
<code>-run [rule-match]</code>	<p>使用可能なルールを実行します。オプションで、大文字と小文字を区別しない <code>rule-match</code> 文字列を適用することで、使用可能なルールのサブセットを実行できます。</p> <ul style="list-style-type: none"> すべてのルールを実行します。 <pre>> cnr_rules -N admin -P changeme -run</pre> 名前に文字列「<code>dhcp</code>」が含まれているルールのみを実行します。 <pre>> cnr_rules -N admin -P changeme -run dhcp</pre> <p>ヒント スペースを含む文字列と一致させるには、二重引用符 (") で文字列を囲みます。例: <code>> cnr_rules -N admin -P changeme -run "router interface"</code></p>
<code>-details</code>	<p>整合性ルールに違反するデータベースオブジェクトの詳細を結果に含めます。</p> <p>DNSルールを実行し、データベースオブジェクトの詳細を結果に含めます。</p> <pre>> cnr_rules -N admin -P changeme -run DNS -details</pre>
<code>-xml</code>	<p>ルールの結果をXMLファイルで生成します。</p> <p>(注) <code>-xml</code> オプションを使用すると、XMLファイルにすべての詳細情報が含まれているため、<code>-details</code> オプションは無視されます。</p> <pre>> cnr_rules -N admin -P changeme -run -xml</pre>

オプション	説明
<code>-path .classpath</code>	<p>使用可能な整合性ルールを検索する Java のクラスパスを変更します (任意)。</p> <p>新しいカスタム整合性ルールを実行するために、このオプションを使用できます。これを行うには、サポート エンジニアのサポートを受ける必要があります。</p>
<code>-interactive</code>	<p>インタラクティブ セッションでツールを実行します。</p> <pre>> cnr_rules -N admin -P changeme -run -interactive RuleEngine [type ? for help] > ? Commands: load <class> // load the specified rule class run <rule-match> // run rules matching a string, or '*' for all list // list rules by name xml // toggle xml mode detail // toggle detail mode (non-xml only) quit // quit RuleEngine</pre>
<code>-both</code>	Unicode と ASCII の両方でドメイン名を表示します。

上記のコマンドの出力を別のファイルにリダイレクトできます。ルールの結果をキャプチャするには、次の構文を使用します。

- テキスト ファイル :

```
> cnr_rules -N username -P password -run -details > filename.txt
```

- XML ファイル :

```
> cnr_rules -N username -P password -run -xml > filename.xml
```

サーバー ステータスのモニターリングと報告

サーバーのステータスのモニターリングには、次のチェックが含まれます。

- 状態
- 正常性
- 統計
- ログ メッセージ
- アドレス使用状況

- 関連サーバー (DNS および DHCP)
- リース (DHCP)

関連項目

- [サーバーの状態 \(190 ページ\)](#)
- [正常性の表示 \(190 ページ\)](#)
- [統計の表示 \(192 ページ\)](#)
- [IP アドレスの使用状況の表示 \(205 ページ\)](#)
- [関連サーバーの表示 \(206 ページ\)](#)
- [リースの表示 \(209 ページ\)](#)

サーバーの状態

すべての Cisco Prime Network Registrar プロトコル サーバー (DNS、DHCP、SNMP、および TFTP) は、次の状態で構成される状態マシンを通過します。

- **Loaded-** サーバー エージェントがサーバーを起動した後の最初のステップ (過渡的)。
- **Initialized-** サーバーが停止したか、設定に失敗しました。
- **Unconfigured-** サーバーは設定の失敗が原因で動作していません (過渡的)。
- **Stopped-** サーバーは管理上停止しており、動作していません (過渡的)。
- **Running-** サーバーは正常に動作しています。

2つの基本的状態が初期化され、実行されます。これは、サーバーの状態遷移が速すぎて、他の状態は基本的に非表示になるためです。通常、サーバーエージェントがサーバーを起動するときには、サーバーに起動するように通知します。サーバープロセスが起動し、状態をロード済みに設定してから、実行状態に移行します。サーバーを停止すると、状態は初期化済みに戻り、再起動すると、再び実行中まで移行します。何らかの理由で設定に失敗した場合は、停止した場合と同様に、初期化済みに戻ります。

また、プロセスが終了したときにサーバーが非常に短時間だけ遷移する終了中状態もあります。ユーザーインターフェイスは、サーバーの無効化を検討することもあります。これはほとんど発生せず、サーバープロセスがまったく存在しない (サーバープロセスを起動しないようにサーバー エージェントが命令された) 場合に限られます。

正常性の表示

サーバーの正常性の側面、つまりサーバーがどの程度正常に実行されているかを表示できません。次の項目はサーバーの正常性を損なうことがあるため、ステータスを定期的にモニターする必要があります。次について：

- サーバー エージェント (ローカルおよびリージョン クラスター)
- CCM サーバー (ローカルおよびリージョン クラスター)
- DNS サーバー (ローカル クラスター) :

- 設定エラー
- メモリ
- ディスク領域使用率
- ルートサーバーへの接続不可

- キャッシュ DNS サーバー（ローカル クラスタ）
- DHCP サーバー（ローカル クラスタ）：
 - 設定エラー
 - メモリ
 - ディスク領域使用率
 - パケット キャッシングの低下
 - 指定されたパケット制限に適合しないオプション
 - 使用可能なリースがない

- TFTP サーバー（ローカル クラスタ）：
 - メモリ
 - ソケットの読み取りまたは書き込みエラー
 - 過負荷しきい値の超過と要求パケットのドロップ

サーバーの正常性ステータス

サーバーの正常性ステータスは、0~10の値があります。値0は、サーバーが動作していないことを意味し、10はサーバーが稼働していることを意味します。一部のサーバーでは、0または10のみが報告され、その間は何も報告されません。サーバーが1~9の値を報告した場合、問題が発生していることを示す条件が検出されたことを意味します。サーバーの実際のパフォーマンスには関係ありません。そのため、サーバーの正常性が1~9の値である場合、サーバーログファイルを確認して、どのようなエラーが記録されたかを確認する必要があります。



- (注) アクティビティのレベルとログファイルのサイズと数によっては、サーバーの正常性を低下させる条件がログファイルに表示されない場合があります。ログファイルを確認することが重要ですが、サーバーはサーバーの正常性を低下させるすべての条件をログに記録するわけではありません。

次の条件は、DHCP サーバーの正常性を低下させることがあります。

- 設定エラー（サーバーの起動時または再起動時に発生します）
- サーバーがメモリ不足条件を検出したとき
- パケット受信障害が発生したとき
- サーバーの要求または応答バッファ不足のため、パケットがドロップされたとき
- サーバーが応答パケットを構築できないとき

TFTP サーバーにも同様の条件があります。



ヒント 正常性の値の範囲は 0（サーバーが動作していない）から 10（最高レベルの正常性）までです。ゼロはサーバーが動作していないことを意味し、ゼロより大きい値はサーバーが動作していることを意味することを理解したうえで、正常性ステータスの正確な値（1〜10）は無視することを推奨します。Linux では、*install-path/usrbin/* ディレクトリで **cnr_status** コマンドを実行して、ローカルクラスタサーバーが実行しているかどうかを確認できます。ローカルクラスタサーバーが実行しているかどうかを確認する方法の詳細については、*Cisco Prime Network Registrar 10.1* インストールガイドを参照してください。

ローカル基本または詳細とリージョン Web UI

[操作 (Operate)] メニューから、[サーバーの管理 (Manage Servers)] を選択します。[サーバーの管理 (Manage Servers)] ページで、各サーバーの状態と正常性を確認します。

CLI コマンド

[server] タイプ **getHealth** を使用します。数値 10 は、最高レベルの正常性を示し、0 はサーバーが動作していないことを示します。

統計の表示

サーバー統計を表示するには、サーバーが実行している必要があります。

ローカル基本または詳細とリージョン Web UI

[サーバーの管理 (Manage Servers)] ページに移動し、左側のペインでサーバーの名前をクリックしてから、[統計 (Statistics)] タブをクリックします（使用可能な場合）。[サーバー統計 (Server Statistics)] ページで、属性の名前をクリックして、ポップアップヘルプを表示します。

DHCP、DNS、および CDNS 統計は、それぞれ 2 つの統計グループに分かれています。最初のグループは合計統計であり、2 番目のグループはサンプル統計です。合計統計は、時間の経過とともに累積されます。サンプル統計は、設定可能なサンプル間隔の間に発生します。2 つのカテゴリの名前は、サーバーごと、またユーザーインターフェイスごとに異なり、次の表に示されています。

表 18: サーバー統計のカテゴリ

サーバー	ユーザーインターフェイス	合計統計 (コマンド)	サンプル統計 (コマンド)
DHCP	Web UI	合計統計	アクティビティ要約
	CLI	最後の DHCP サーバープロセスの開始以降の合計カウンタ。 (dhcp getStats)	最後のサンプル間隔中に収集されたサンプルカウンタ。これらは、サンプル期間ごとに 1 回更新されます。 (dhcp getStats server sample)
DNS	Web UI	合計統計	サンプル統計
	CLI	最後のサーバープロセスの開始以降の合計カウンタ。 (dns getStats)	現在のサンプル間隔中に収集されているサンプルカウンタ。これらは絶えず更新されます。 (dns getStats performance sample)
CDNS	Web UI	合計統計	サンプル統計
	CLI	最後のサーバープロセスの開始以降の合計カウンタ。 (cdns getStats server total)	最後のサンプル間隔以降にサンプリングされたカウンタ。 (cdns getStats server sample)

サンプルカウンタをセットアップするには、サーバーの *collect-sample-counters* 属性または *activity-summary* と呼ばれる *log-settings* 属性値のいずれかをアクティブにする必要があります。また、各サーバーのサンプル間隔の *log-settings* 値を設定することもでき、5分に事前設定されています。 *collect-sample-counters* 属性は、DNS サーバーの場合は true に事前設定されていますが、DHCP サーバーの場合は false に事前設定されています。たとえば、サンプルカウンタを有効にし、DHCP の間隔を設定するには、DHCP サーバーの次の属性を設定します。

- *collect-sample-counters* を有効化 (**dhcp enable collect-sample-counters**)
- *activity-summary* の *log-settings* を設定 (**dhcp set log-settings=activity-summary**)
- *activity-summary-interval* を 5m に設定 (**dhcp set activity-summary-interval=5m**)

CLI コマンド

CLI では、`[server] type getStats` を使用する場合、DNS については表 19 : DNS 統計、DHCP については表 21 : DHCP 統計、TFTP については表 22 : TFTP 統計、で説明されているように、統計は波カッコで囲まれ、その後の一連のフィールドが続きます。`server type getStats all` コマンドは、より冗長であり、各統計が 1 行ずつ表示されます。追加の `sample` キーワードを使用すると、サンプル統計のみが表示されます。

カウンタと合計統計をリセットするには、`dhcp resetStats`、`dns resetStats`、または `cdns resetStats` を使用します。

DNS 統計

Web UI の DNS サーバー統計が [DNS サーバー統計 (DNS Server Statistics)] ページに表示されたら、統計の名前をクリックして説明を読みます。DNS サーバー統計を更新できます。

DNS サーバー統計の詳細には、サーバー識別子、再帰的なサービス、プロセス稼働時間、リセット以降の時間、サーバーステータス、カウンタリセット時間、サンプル時間、統計間隔、経過時間、合計ゾーン、および合計 RR が含まれ、次に示す合計およびサンプル統計が続きます。

- [Performance Statistics] - DNS サーバーのパフォーマンスの統計が表示されます。
- [Query Statistics] - クエリの統計が表示されます。
- [Update Statistics] - DNS アップデートの統計が表示されます。
- [HA Statistics] - HA DNS サーバーの統計が表示されます。
- [Push Notification Statistics] - DNS プッシュ通知の統計が表示されます。
- [Host Health Check Statistics] - DNS ホスト正常性チェックの統計が表示されます。
- [DB Statistics] - DNS データベースの統計が表示されます。
- [Cache Statistics] - DNS クエリキャッシュの統計が表示されます。
- [Security Statistics] - セキュリティの統計が表示されます。
- [IPv6 Statistics] - 送受信された IPv6 パケットの統計が表示されます。
- [Error Statistics] - エラーの統計が表示されます。
- [Max Counter Statistics] - 同時スレッド、RR、DNS アップデート遅延、同時パケットなどの最大数の統計が表示されます。
- [Top Name Statistics] : トップネームの統計が表示されます。



(注) 最新のデータを取得するには、[統計 (Statistics)] ページの左上にある [サーバー統計の更新 (Refresh Server Statistics)] アイコンをクリックします。

dns getStats コマンドには、次のオプションがあります。

```
dns getStats [<performance [,] query [,] update [,] errors [,] security [,]
maxcounters [,] ha [,] ipv6 [,] dns-pn [,] cache [,] datastore [,] top-names [,]
dns-hhc | all> [total | sample]]
```

dns getStats all コマンドは、最もよく使用されています。 **all** オプションのない **dns getStats** コマンドは、1 行の位置値の統計を次の形式で返します（次の表は、これらの値を読み取る方法を示しています）。

```
nrcmd> dns getStats

100 Ok
{1} 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
```

表 19: DNS 統計

フィールド	統計	説明
{1}	id	実装 ID（リリースおよびビルド情報）。
2	config-recurs	再起サービス - (1) available、(2) restricted、(3) unavailable。
3	config-up-time	最後のサーバーの起動時からの経過時間（秒単位）。
4	config-reset-time	最後のサーバーのリセット（再起動）からの経過時間（秒単位）。
5	config-reset	ネームサーバーの状態を再初期化するステータスまたはアクション - (2) リセットアクションを使用した場合、永続的なネームサーバーの状態が再初期化されます。以下に、読み取り専用ステータスを示します。(1) other - 未知の状態のサーバー、(3) 初期化中、または (4) 実行中。
6	counter-auth-ans	信頼できる応答が返されたクエリの数。
7	counter-auth-no-names	そのような名前がないという信頼できる応答が返されたクエリの数。
8	counter-auth-no-data-resps	そのようなデータはないという信頼できる応答（空の応答）が返されたクエリの数。（廃止された統計）
9	counter-non-auth-datas	信頼できない応答（キャッシュ）が返されたクエリの数。（廃止された統計）

フィールド	統計	説明
10	counter-non-auth-no-datas	データなしで信頼できない応答が返されたクエリの数。
11	counter-referrals	他のサーバーに転送されたクエリの数。
12	counter-errors	エラー（0または3以外の RCODE 値）で応答された応答の数。
13	counter-rel-names	1つのラベル（相対名）のみの名前に対して受信された要求の数。
14	counter-req-refusals	拒否されたクエリの数。
15	counter-req-unparses	解析不能な要求の数。
16	counter-other-errors	他のエラーが原因で中止された要求の数。
17	total-zones	設定済みゾーンの合計数。

CDNS 統計

Web UI の CDNS サーバーの統計情報は、[DNS キャッシング サーバーの統計] ページに表示され、統計の名前をクリックすると、説明が表示されます。CDNS サーバー統計を更新できません。

CDNS サーバー統計情報の詳細には、サーバー識別子、再帰的なサービス、現在の時間、プロセス稼働時間、サーバー再起動時間、カウンタリセット時間、サンプル時間、統計間隔、経過時間などが含まれ、次に示す合計およびサンプル統計が続きます。

- [Query Details] : クエリの統計情報が表示されます。
- [Answer Details] : CDNS クエリ応答に関連する統計情報が表示されます。
- [Performance] : DNS サーバーのパフォーマンスの統計情報が表示されます。
- [DNS64] : DNS64 の統計情報が表示されます。
- [Firewall] : DNS ファイアウォールの統計情報が表示されます。
- [Rate Limiting] : レート制限に関連する統計情報が表示されます。
- [Top Name Statistics] : トップネームの統計が表示されます。



(注) 最新のデータを取得するには、[統計 (Statistics)] ページの左上にある [サーバー統計の更新 (Refresh Server Statistics)] アイコンをクリックします。

cdns getStats コマンドには、次のオプションがあります。

```
cdns getStats [<server | top-names | rate-limit | all> [total | sample]]
```

cdns getStats コマンドと **cdns getStats server** コマンドはどちらも、**cdns getStats server total** と同じです。

cdns getStats top-names コマンドと **cdns getStats rate-limit** コマンドでは常に「サンプル」データがレポートされ、モードパラメータは無視されます（「合計」データはレポートされない）。

cdns getStats コマンドと **cdns getStats all** コマンドは、次の表に示す統計情報を返します。

表 20: CDNS 統計

統計	説明
name	DNS キャッシング サーバーを識別する名前。
restart-time	DNS キャッシュサーバーが最後に再起動またはリロードされた時刻。
config-recurs	このネームサーバーによって提供される再帰サービス。
time-current	CDNS サーバーによって提供される現在時刻。
time-up	サーバーの実行時間。
time-elapsed	前回の統計ポーリングからの経過時間。
reset-time	統計が最後にリセットされた時刻（つまり、CLI の cdns resetStats ）。
sample-time	サーバーがサンプル統計の最後のセットを収集した時刻。
sample-interval	サンプル統計を収集するときに、サーバーによって使用されるサンプル間隔。
queries-total	CDNS サーバーが受信したクエリの合計数。
queries-over-tcp	CDNS サーバーが TCP を介して受信したクエリの合計数。
queries-over-ipv6	CDNS サーバーが TCP を介して受信したクエリの合計数。
queries-with-edns	EDNS OPT RR が存在するクエリの数。
queries-with-edns-do	EDNS OPT RR with DO (DNSSEC OK) ビットがセットされているクエリの数。
queries-type-A	受信されたクエリの数。
queries-type-AAAA	受信された AAAA クエリの数。
queries-type-ANY	受信された ANY クエリの数。

統計	説明
queries-type-CNAME	受信されたクエリの数。
queries-type-PTR	受信されたクエリの数。
queries-type-NS	受信された NS クエリの数。
queries-type-SOA	受信された SOA クエリの数。
queries-type-MX	受信された MX クエリの数。
queries-type-DS	受信された DS クエリの数。
queries-type-DNSKEY	受信された DNSKEY クエリの数。
queries-type-RRSIG	受信された RRSIG クエリの数。
queries-type-NSEC	受信された NSEC クエリの数。
queries-type-NSEC3	受信された NSEC3 クエリの数。
queries-type-other	受信された タイプ 256+ のクエリの数。
queries-with-flag-QR	QR (クエリ応答) フラグがセットされた着信クエリの数。これらのクエリはドロップされます。
queries-with-flag-AA	AA (認証応答) フラグがセットされた着信クエリの数。これらのクエリはドロップされます。
queries-with-flag-TC	TC (切り捨て) フラグがセットされた着信クエリの数。これらのクエリはドロップされます。
queries-with-flag-RD	RD (再帰希望) フラグがセットされた着信クエリの数。
queries-with-flag-RA	RA (再帰利用可能) フラグがセットされた着信クエリの数。
queries-with-flag-Z	Z フラグがセットされた着信クエリの数。
queries-with-flag-AD	AD フラグがセットされた着信クエリの数。
queries-with-flag-CD	CD フラグがセットされた着信クエリの数。
queries-failing-acl	ACL 障害のためにドロップまたは拒否されたクエリの数。
cache-hits	キャッシュから応答されたクエリの合計数。
cache-misses	キャッシュ内で見つからなかったクエリの合計数。
cache-prefetches	実行されたプリフェッチの数。

統計	説明
mem-query-cache-exceeded	メッセージキャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
mem-cache-exceeded	RRSet キャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
remote-ns-cache-exceeded	リモート ネーム サーバー キャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
key-cache-exceeded	キーキャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
smart-cache	スマートキャッシュが有効になっている場合に、CDNS サーバーがスマートキャッシュ応答を使用した合計回数。
requestlist-total	再帰応答を待つキューに入れられた要求の合計数。
requestlist-total-user	再帰応答を待つキューに入れられたユーザー要求の合計数。
requestlist-total-system	再帰応答を待つキューに入れられたシステム要求の合計数。
requestlist-total-average	要求リストの平均要求数。
requestlist-total-max	要求リストの最大要求数。
requestlist-total-overwritten	新しいエントリによって上書きされた要求リスト上の要求の数。
requestlist-total-exceeded	要求リストがいっぱいになったためにドロップされた要求の数。
recursive-replies-total	再帰クエリの応答の合計数。
recursive-time-average	再帰クエリを完了するまでの時間の平均値。
recursive-time-median	再帰クエリを完了するまでの時間の中央値。
mem-process	CDNS プロセスのメモリの推定値 (バイト数)。
mem-cache	RRSet キャッシュのメモリ (バイト数)。
mem-query-cache	着信クエリ メッセージキャッシュのメモリ (バイト数)。

統計	説明
mem-iterator	CDNS イテレータ モジュールによって使用されたメモリ (バイト数)。
mem-validator	CDNS バリデータ モジュールによって使用されたメモリ (バイト数)。
answers-with-NOERROR	NOERROR の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with- NXDOMAIN	NXDOMAIN の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-REFUSED	REFUSED の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-SERVFAIL	SERVFAIL の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-FORMERR	FORMERR の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-NOTAUTH	NOTAUTH の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-NOTIMP	NOTIMP の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
answers-with-NODATA	NODATA の疑似 rcode がクライアントに返される結果となった応答の数。
answers-with-other-errors	NODATA の疑似 rcode がクライアントに返される結果となった応答の数。
answers-secure	正しく検証された応答の数。
answers-unsecure	正しく検証されなかった応答の数。
answers-rrset-unsecure	バリデータによって偽としてマークされた RRSet の数。
answers-unwanted	望ましくない、または未承諾の応答の数。高い値は、スプーフィングの脅威を示している可能性があります。
dns64-a2aaaa-conversions	DNS64 がタイプ A の RR をタイプ AAAA の RR に変換した回数。
dns64-ptr-conversions	DNS64 が IPv4 PTR RR を IPv6 PTR RR に変換した回数。
firewall-dropped	DNS ファイアウォールがクエリをドロップした回数。

統計	説明
firewall-redirected	DNS ファイアウォールがクエリをリダイレクトした回数。
firewall-refused	DNS ファイアウォールがクエリを拒否した回数。
firewall-redirect-nxdomain	DNS ファイアウォールがクエリを NXDOMAIN 応答とともにリダイレクトした回数。
firewall-rpz	DNS ファイアウォール RPZ ルールが着信クエリと一致した回数。
exceeded-max-target-count	許可されるネーム サーバー グループ ルックアップの最大数を越えたクエリの数。
client-rate-limit	<i>client-rate-limiting</i> が有効になっている場合に、クライアントがレート制限された回数。
domain-rate-limit	<i>domain-rate-limiting</i> が有効になっている場合に、ゾーンがレート制限された回数。

DHCP 統計

Web UI の DHCP サーバー統計が [DHCP サーバー統計 (DHCP Server Statistics)] ページに表示されたら、統計の名前をクリックして説明を読みます。

DHCP サーバー統計の詳細情報には、サーバーの開始時刻、サーバーのリロード時間、サーバーの稼働時間、統計リセット時間などが含まれ、次のセクションの統計が続きます。

- [合計統計 (Total Statistics)] - スコープ、要求バッファ、応答バッファ、パケットなどの合計統計が表示されます。
- [リースカウント (Lease Counts) (IPv6)] - アクティブなリース、設定されたリース、予約済みリース、予約済みアクティブリースなど、IPv4 リースカウントの統計が表示されます。
- [受信パケット (Packets Received) (IPv6)] - 受信した IPv4 パケットの統計が表示されます。
- [[送信パケット (Packets Sent) (IPv6)] - 送信した IPv4 パケットの統計が表示されます。
- [失敗パケット (Packets Failed) (IPv4)] - 失敗した IPv4 パケットの統計が表示されます。
- [フェールオーバー統計 (Failover Statistics)] - DHCP フェールオーバー サーバーの統計が表示されます。
- [IPv6統計 (IPv6 Statistics)] - 設定されている IPv6 プレフィックス、タイムアウトになった IPv6 オファー パケットなどの統計が表示されます。

- [リースカウント (Lease Counts) (IPv6)] - アクティブなリース、設定されたリース、予約済みリース、および予約済みアクティブリースの IPv6 リースカウントの統計が表示されます。
- [受信パケット (Packets Received) (IPv6)] - 受信した IPv6 パケットの統計が表示されます。
- [送信パケット (Packets Sent) (IPv6)] - 送信された IPv6 パケットの統計が表示されます。
- [失敗パケット (Packets Failed) (IPv6)] - 失敗した IPv6 パケットの統計が表示されます。

追加の属性には、使用率の高い集約とアクティビティの要約が含まれます。



(注) 最新のデータを取得するには、[統計 (Statistics)] ページの左上にある [サーバー統計の更新 (Refresh Server Statistics)] アイコンをクリックします。

dhcp getStats コマンドには、次のオプションがあります。

```
dhcp getStats [<all | server [, failover [, dhcpv6 [, top-utilized]
[total | sample]]]
```

dhcp getStats all コマンドは、最もよく使用されています。 **all** オプションのない **dhcp getstats** コマンドは、1 行の位置値の統計を次の形式で返します (次の表は、これらの値を読み取る方法を示しています)。

```
nrcmd> dhcp getStats
```

```
100 Ok
{1} 2 3 4 5 6 7 8
```

表 21: DHCP 統計

フィールド	統計	説明
{1}	start-time-str	テキスト文字列としての最後のサーバーのリロードの日付と時刻。
2	total-discovers	受信された DISCOVER パケットの数。
3	total-requests	受信された REQUEST パケットの数。
4	total-releases	受信された RELEASED パケットの数。
5	total-offers	送信された OFFER パケットの数。
6	total-acks	送信された確認応答 (ACK) パケットの数。
7	total-naks	送信された否定応答 (NAK) パケットの数。
8	total-declines	受信された DECLINE パケットの数。

TFTP 統計

Web UI の TFTP サーバー統計は、[TFTP サーバー統計 (TFTP Server Statistics)] ページに表示され、統計の名前をクリックすると、説明を確認できます。次の表に、汎用の `tftp getStats` コマンドの出力としてエンコードされた TFTP 統計を示します。

TFTP サーバーが起動すると、使用するセッション (`tftp-max-sessions`) とパケット (`tftp-max-packets`) が割り当てられます。TFTP セッションは、TFTP クライアントと TFTP サーバー間の通信を表します。

読み取り要求が TFTP サーバーに到達すると、サーバーは要求にパケットを割り当てて、`total-packets-in-use` および `total-read-requests` 値を 1 ずつ増加させ、データ パケットでユーザーに応答します。TFTP サーバーは、必要に応じて、最新の通信パケットをバックアップして再送信します。TFTP サーバーは、データ パケットとして使用するために、プールから別のパケットを選択します。TFTP サーバーは、クライアントに送信されたデータ ブロックの確認応答を受信すると、次のデータ ブロックを送信します。セッションがただちにパケットを処理できない場合、TFTP サーバーはセッションに関連付けられているパケットをキューに入れます。

TFTP サーバー統計の詳細については、次を参照してください。

- 属性 (Attribute) - ポート番号、デフォルトのデバイス、ホーム ディレクトリ、ルートとしてのホーム ディレクトリの使用など、サーバーの統計を表示します。
- ログ設定 (Log Settings) - ログ レベル、ログ設定、およびパケット トレース レベルの統計を表示します。



(注) 最新のデータを取得するには、ページの左上にある [サーバー統計の更新 (Refresh Server Statistics)] アイコンをクリックします。

TFTP 統計は、汎用の `tftp getStats` コマンドの出力として次の形式でエンコードされます。

```
nrcmd> tftp getStats

100 Ok
{1} 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
```

表 22: TFTP 統計

フィールド	属性	説明
{1}	id	実装 ID (リリースおよびビルド情報)。
2	server-state	サーバーの状態 (アップまたはダウン)。
3	server-time-since-start	前回の起動からの実行時間。
4	server-time-since-reset	前回のリセットからの実行時間。
5	total-packets-in-pool	プール内のパケット数。

フィールド	属性	説明
6	total-packets-in-use	サーバーが使用しているパケット数。
7	total-packets-received	前回の起動またはリロード後に受信したパケット数。
8	total-packets-sent	前回の起動またはリロード後に送信されたパケット数。
9	total-packets-drained	前回の起動またはリロード後に読み取られ、破棄されたパケット数。
10	total_packets_dropped	前回の起動またはリロード後にドロップされたパケット数。
11	total-packets-malformed	前回の起動またはリロード後に形式が間違っていた受信パケット数。
12	total-read-requests	前回の起動またはリロード後に読み取られたパケット数。
13	total-read-requests-completed	前回の起動またはリロード後に完了した読み取りパケット数。
14	total-read-requests-refused	前回の起動またはリロード後に拒否された読み取りパケット数。
15	total-read-requests-ignored	前回の起動またはリロード後に無視された読み取りパケット数。
16	total-read-requests-timed-out	前回の起動またはリロード後にタイムアウトした読み取りパケット数。
17	total-write-requests	前回の起動またはリロード後に書き込み要求であった読み取りパケット数。
18	total-write-requests-completed	前回の起動またはリロード後に完了した書き込み要求の数。
19	total-write-requests-refused	前回の起動またはリロード後に拒否された書き込み要求の数。
20	total-write-requests-ignored	前回の起動またはリロード後に無視された書き込み要求の数。
21	total-write-requests-timed-out	前回の起動またはリロード後にタイムアウトした書き込み要求の数。

フィールド	属性	説明
22	total-docsis-requests	前回の起動またはリロード後に受信された DOCSIS 要求の数。
23	total-docsis-requests-completed	前回の起動またはリロード後に完了した DOCSIS 要求の数。
24	total-docsis-requests-refused	前回の起動またはリロード後に拒否された DOCSIS 要求の数。
25	total-docsis-requests-ignored	前回の起動またはリロード後に無視された DOCSIS 要求の数。
26	total-docsis-requests-timed-out	前回の起動またはリロード後にタイムアウトした DOCSIS 要求の数。
27	read-requests-per-second	1 秒あたりの読み取り要求の数。
28	write-requests-per-second	1 秒あたりの書き込み要求の数。
29	docsis-requests-per-second	1 秒あたりの DOCSIS 要求の数。

IP アドレスの使用状況の表示

IP アドレスの使用状況を表示すると、クライアントに現在どのようなアドレスが割り当てられているかの概要が示されます。

ローカル詳細およびリージョン Web UI

ローカルまたはリージョン クラスタのアドレス空間を確認するか、リージョン クラスタの DHCP 使用率またはリース履歴レポートを生成して、IP アドレスの使用状況を確認できます。これらの機能は、ローカルまたはリージョナルクラスタでアドレス空間権限がある場合、**Design > DHCPv4** メニューで使用できます。

ユニファイドアドレス空間、アドレスブロック、およびサブネットの[現在の使用状況 (Current Usage)] タブをクリックすることによって、現在のアドレス空間使用率を確認できます (『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「アドレスブロック、サブネット、およびスコープのアドレス使用状況の表示」の項を参照)。リース履歴を照会することによって、最新の IP アドレス使用状況を取得することもできます (『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「リースの照会」の項を参照)。後者の場合、リージョン CCM サーバーは適切な DHCP サーバーを直接参照します。このサブネットからサーバーへのマッピングを確保するには、関連するローカルクラスタと一致するようにリージョンのアドレス空間ビューを更新する必要があります。これを行うには、レプリカアドレス空間をプルするか、サブネットを回収して DHCP サーバーにプッシュします (『Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド』の「サブネットの回収」の項を参照)。また、特定の DHCP サーバーが実行していることを確認します。

CLI コマンド

report コマンドを使用して、IP アドレス使用状況レポートを生成できます。コマンドの構文は、次のとおりです。

```
report [column-separator=string]
      [dhcp-only]
      [dhcpv4]
      [dhcpv6]
      [file=outputfile]
      [vpn=name]
```

列区切りは、レポートの列を区切る文字列を指定します（プリセット値はスペース文字です）。複数のスペースを含める場合は、その前にバックスラッシュ (\) エスケープ文字を付けます（引用符で囲まれています）。DHCPv4 または DHCPv6 アドレスを指定できます（**dhcp-only** は **dhcpv4** と同じです）。VPN を指定しないと、現在の VPN のアドレスのみが返されます。

関連サーバーの表示

Cisco Prime Network Registrar には、DNS ゾーン分散または DHCP フェールオーバー設定内のサーバー間の関係が表示されます。Web UI では、さまざまなページで **[関連サーバー (Related servers)]** アイコンをクリックすると、関連サーバーのページを表示できます。関連サーバーの表示を使用して、誤って設定されたサーバーや到達不能なサーバーを診断し、モニターすることができます。

関連項目

[永続イベントを使用したリモートサーバーのモニターリング \(206 ページ\)](#)

[DNS ゾーン分散サーバー \(208 ページ\)](#)

[DHCP フェールオーバーサーバー \(208 ページ\)](#)

永続イベントを使用したリモートサーバーのモニターリング

DNS および LDAP 関連サーバーの更新を必要とするクライアントにサービスを提供するために、DHCPサーバーは永続的なイベントアルゴリズムを使用して、関連サーバーが一時的に使用できなくなった場合に、関連サーバーの更新を保証します。さらに、このアルゴリズムにより、設定ミスまたはオフラインの DNS サーバーは、使用可能なすべての更新リソースを使用できなくなります。

DHCPサーバーは、起動時に、永続イベントを必要とする設定内の関連サーバーの数を計算します。事前設定された最大保留イベント属性（4 万に事前設定されているメモリ内イベントの数を指定するエキスパートモード属性）がサーバーの数で除算されて、各リモートサーバーに許可されるイベント数の制限が求められます。この計算では、関連する DNS サーバーと LDAP サーバーをカバーします（DHCP フェールオーバーでは、イベントに永続的なストレージは使用されません）。DHCPサーバーは、この計算を使用してログメッセージを発行し、次の表に記載されているアクションを実行します。次の表は、4つの関連する DNS サーバーがあり、それぞれが 10K イベントの制限を持つ DHCP サーバーの架空のケースを示しています。

表 23: 永続イベント アルゴリズム

イベントに到達	
<p>計算されたサーバごとの制限の 50% (最大保留イベントの値を関連するサーバの合計数で除算したもの)。たとえば、合計 40K の最大保留イベントのうち、関連サーバーのイベントが 5K</p>	<p>制限を超えている限り、2分ごとに INFO ログメッセージを発行します。</p> <p>The queue of events for the <i>name</i> remote server at <i>address</i> has <i>x</i> events, and has reached the info limit of $y/2$ events out of an upper limit of <i>y</i> events per remote server. The remote server may be misconfigured, inoperative, or unreachable.</p>
<p>計算されたサーバーごとの制限の 100%、および最大保留イベント値の 50% 未満。たとえば、関連サーバーのイベントが 10K で、最大保留イベントの合計が 10K 未満</p>	<p>制限を超えている限り、2分ごとに WARNING ログメッセージを発行します。</p> <p>The queue of events for the <i>name</i> remote server at <i>address</i> has <i>x</i> events, has exceeded the limit of <i>y</i> events per remote server, but is below the limit of <i>z</i> total events in memory. The remote server may be misconfigured, inoperative, or unreachable.</p>
<p>計算されたサーバーごとの制限の 100%、および最大保留イベント値の 50% 以上。たとえば、関連サーバーのイベントが 10K で、合計最大保留イベントが 20K</p>	<p>制限を超えている限り、2分ごとに ERROR ログメッセージを発行します。</p> <p>The queue of events for the <i>name</i> remote server at <i>address</i> has <i>x</i> events, and has grown so large that the server cannot continue to queue new events to the remote server. The limit of <i>y</i> events per remote server and $z/2$ total events in memory has been reached. This and future updates to this server will be dropped. The current eventID <i>n</i> is being dropped.</p> <p>サーバーは、現在のトリガー イベントとそのサーバーでの後続のすべてのイベントをドロップします。</p>
<p>最大保留イベント値の 100%。たとえば、すべての関連サーバーのイベントが 40K</p>	<p>ERROR ログメッセージを発行します。</p> <p>The queue of pending events has grown so large that the server cannot continue to queue new events. The queue's size is <i>z</i>, and the limit is <i>z</i>.</p> <p>サーバーは、すべての関連サーバーで後続のすべてのイベントをドロップします。</p>

SNMP トラップおよび DHCP サーバーのログメッセージは、関連サーバーに到達不能であることも通知します。

DNS ゾーン分散サーバー

DNS ゾーン分散により、同じセカンダリ サーバー属性を共有する複数のゾーンを簡単に作成できます。ゾーン分散のプライマリおよびセカンダリ DNS サーバーを表示および設定できます。

ローカル基本または詳細 [Web UI](#)

Deploy メニューから、**[DNS]** サブメニューの **Zone Distribution** をクリックします。[ゾーン分散のリスト/追加 (List/Add Zone Distributions)] ページが開きます。ローカル クラスタでは、デフォルトのゾーン分散が 1 つだけ可能です。このゾーン分散名をクリックして [ゾーン分散の編集 (Edit Zone Distribution)] ページを開くと、ゾーン分散内の権威サーバーとセカンダリサーバーが表示されます。

リージョン [Web UI](#)

Deploy メニューから、**[DNS]** サブメニューの **Zone Distribution** を選択します。[ゾーン分散のリスト/追加 (List/Add Zone Distributions)] ページが開きます。リージョン クラスタでは、複数のゾーン分散を作成できます。ゾーン分散名をクリックして [ゾーン分散の編集 (Edit Zone Distribution)] ページを開くと、ゾーン分散マップ名、ゾーン分散内のプライマリ サーバー、権威サーバ、およびセカンダリ サーバが表示されます。



(注) デフォルトのゾーン分散名は編集できません。ただし、デフォルト以外のゾーン分散名は編集可能であり、保存できます。

CLI コマンド

zone-dist name create primary-cluster [attribute=value] を使用してゾーン分散を作成し、**zone-dist list** を使用して表示します。次に例を示します。

```
nrcmd> zone-dist distr-1 create Boston-cluster

nrcmd> zone-dist list
```

DHCP フェールオーバー サーバー

DHCP フェールオーバー ペア関係の関連サーバーは、次の情報を表示できます。

- **Type-** メインまたはバックアップ DHCP サーバー。
- **Server name-** サーバーの DNS 名。
- **IP address -** ドット付きオクテット形式のサーバー IP アドレス。
- **Requests-** 未処理の要求の数、または該当しない場合は 2 つのダッシュ。
- **Communication status-** OK または INTERRUPTED。
- **Cluster state -** この DHCP サーバーのフェールオーバー状態。
- **Partner state -** パートナー サーバーのフェールオーバー状態。

DHCP フェールオーバーの実装の詳細については、『*Cisco Prime Network Registrar 10.1 DHCP ユーザ ガイド*』の「DHCP フェールオーバーの管理」の項を参照してください。

ローカル基本または詳細 *Web UI*

Deploy メニューから、**[DHCP]** サブメニューの **Failover Pairs** を選択します。[DHCP フェールオーバー ペアのリスト/追加 (List/Add DHCP Failover)] ページに、フェールオーバー関係のメイン サーバーとバックアップ サーバーが表示されます。

CLI コマンド

dhcp getRelatedServers を使用して、メインとパートナーの DHCP サーバー間の接続ステータスを表示します。関連サーバーがない場合、出力は単に 100 Ok です。

リースの表示

スコープを作成した後、リース アクティビティをモニターし、リース属性を表示できます。

ローカル基本または詳細 *Web UI*

Design メニューから **[DHCPv4]** サブメニューの **Scopes** を選択するか、**Design** メニューから **[DHCPv6]** サブメニューの **Prefixes** を選択します。[DHCP スコープのリスト/追加 (List/Add DHCP Scopes)] または [DHCPv6 プレフィックスのリスト/追加 (List/Add DHCPv6 Prefixes)] ページの **[リース (Leases)]** タブをクリックすると、リースが表示されます。

ローカル詳細およびリージョン詳細 *Web UI*

Operate メニューから **Reports** サブメニューの **DHCPv4 Lease History** または **DHCPv6 Lease History** を選択します。クエリパラメータを設定し、リース履歴を照会します。（『Cisco Prime Network Registrar 10.1 DHCP ユーザガイド』の「リースの照会」の項を参照してください）。

DHCP および DNS サーバーのトラブルシューティング

以下のセクションでは、設定と DNS、DHCP、および TFTP サーバーのトラブルシューティングについて説明します。

関連項目

[即時のトラブルシューティング アクション \(210 ページ\)](#)

[cnr.conf ファイルの変更 \(210 ページ\)](#)

[サーバー障害のトラブルシューティング \(213 ページ\)](#)

[TFTP サーバーのトラブルシューティングと最適化 \(218 ページ\)](#)

[Linux トラブルシューティング ツール \(214 ページ\)](#)

[TAC ツールの使用 \(215 ページ\)](#)

即時のトラブルシューティングアクション

問題が発生したときには、最初の問題を分離して修正する際、損害を拡大しないようにすることが重要です。特に、次のことを実行する（または実行しない）ことが重要です。

- 512 MB 以上のメモリと 2.5 GB 以上のデータパーティションがあること。
- ケーブルモデム終端システム（CMTS）を再起動しないでください。
- DHCP フェールオーバーを有効にします。
- フェールオーバーの再同期が進行中は、Cisco Prime Network Registrar をリロード、再起動、または中断しないでください。

cnr.conf ファイルの変更

Cisco Prime Network Registrar は、基本設定パラメータに **cnr.conf** ファイルを使用します。このファイルは通常、*install-path/conf* ディレクトリにあります。Cisco Prime Network Registrar は、インストール時にファイルを作成し、1 行ずつ処理します。

設定パラメータを変更する場合は、このファイルを編集します。通常の場合は、値を変更する必要はありません。ただし、特定の条件では、ディスク領域の理由でデータファイルを移動する場合など、特定の値を変更する必要がある場合があります。

cnr.conf ファイルの形式は、パラメータ名と値のペア（1 行に 1 つ）で構成されます。たとえば、Windows ローカルクラスタのインストールの場合は、次のようになります。

```
cnr.rootdir=C:\\Program Files\\Network Registrar\\Local
cnr.ccm-port=1234
cnr.cisco-gss-appliance-integration=n
cnr.datadir=C:\\NetworkRegistrar\\Local\\data
cnr.java-home=C:\\Program Files\\Java\\jre1.5.0_12
cnr.logdir=C:\\NetworkRegistrar\\Local\\logs
cnr.https-port=8443
cnr.tempdir=C:\\NetworkRegistrar\\Local\\temp
cnr.http-port=8080
cnr.ccm-mode=local
cnr.ccm-type=cnr
cnr.http-enabled=y
cnr.https-enabled=n
cnr.keystore-file=C:
cnr.keystore-password=unset
cnr.backup-time=23:45
```

ディレクトリパスは、オペレーティングシステムのネイティブ構文である必要があります。この形式では、ディレクトリパスにコロン（:）を使用できますが、名前と値のペアの区切り文字として使用することはできません。行の継続や unicode 文字の埋め込みはできません。ファイルに対するその他の変更には、ログディレクトリの場所（[ログファイル \(179 ページ\)](#)）を参照、または **cnr_shadow_backup** バックアップの実行時間（[自動バックアップ時間の設定 \(224 ページ\)](#)）を参照）などがあります。

まれに、ファイルを変更したい場合があります。たとえば、キャパシティの問題により、毎日のバックアップから特定のデータを除外します。これを行うには、適切な設定を手動で追加する必要があります。



注意 このファイルのデフォルト設定を使用することを推奨します。これらの設定を変更する必要がある場合は、Cisco Technical Assistance Center (TAC) または Cisco Prime Network Registrar 開発チームと相談してください。

次の設定がサポートされています。

- **cnr.backup-dest** - バックアップされたデータベースを配置する宛先を指定します。指定されなかった場合のデフォルトは、**cnr.datadir** です。
- **cnr.backup-dbs** - バックアップするデータベースのカンマ区切りのリストを指定します。ローカルクラスタの場合、デフォルトは **cdns,ccm,dhcp,dns,mcd,cnrsnmp** です。リージョンクラスタの場合は、**ccm,dns,leasehist,lease6hist,subnetutil,replica** です。
- **cnr.backup-files** - バックアップの一部としてコピーするファイルのカンマ区切りリスト、ファイルへの完全なパスを指定します。ファイルは **cnr.backup-dest** にコピーされます。
- **cnr.dbrecover-backup** - バックアップされた Oracle Berkeley データベースに対して **db recover** と **db verify wo** 実行するかどうかを指定します。デフォルトは **true** です。この設定は、毎日のバックアップにのみ使用されます。手動バックアップは、この設定を無視します。自動動作を無効にするということは、手動で操作を実行する必要があることを意味します。これは、別のマシンで、または Cisco Prime Network Registrar サーバーが比較的アイドル状態のときに実行する必要があることを意味します。
- **cnr.daily-backup** - 毎日バックアップを実行するかどうかを指定します。デフォルトは **true** です。

Syslog のサポート

Cisco Prime Network Registrar は、(Linux での) Syslog サーバーへのロギングをサポートしています。Syslog サポートは、デフォルトでは有効になっていません。ロギングレベルに基づいて、ログに記録する必要があるメッセージを設定するには、**cnr.conf** ファイルを更新する必要があります。

さらに、Windows では、警告とエラーのイベントロギングはデフォルトで有効になっていません (Windows イベントログの場合)。このリリースでは、ログ設定を変更することにより、より多くの (またはより少ない) イベントをイベントログに記録することができます。

次の **cnr.conf** 設定パラメータがサポートされています。

- **cnr.syslog.enable** - Syslog サーバーまたは Windows イベントログへのロギングが Prime Network Registrar サーバーについて有効かどうかを指定します。
 - すべてのロギングを無効にするには、値を 0、off、または **disabled** にします。
 - すべてのロギングを有効にするには、値を 1、on、または **enabled** にします。
 - デフォルトでは、このパラメータは Linux では無効になっており、Windows では有効になっています。
- **cnr.syslog.levels** - Syslog または Windows イベントログに記録する重大°Cレベルを指定します。Syslog が有効な場合、デフォルトは **warning** と **error** です。値は、大文字と小文字が区

別されず、カンマで区切られたキーワード (error、warning、activity、info、debug) のリストです。このパラメータは、Syslog が無効な場合は無視されます。



注意 すべての重大度レベルを有効にすることは可能ですが、すべてのメッセージがサーバーログファイルに書き込まれ、Syslog にも記録されるため、これは推奨されません。Syslog とサーバーのパフォーマンスに与える影響は、ロギングの設定方法によって大きく異なる場合があります。Syslog はメッセージのレート制限を行うことができるため、有用なメッセージも失われる可能性があります。

書き込まれるメッセージの数を最小限に抑えるために、Syslog 設定とメッセージを確認することを強くお勧めします。Syslog に書き込まれるメッセージが多すぎると、Cisco Prime Network Registrar サーバーと Syslog のパフォーマンスに影響を与えます。

- `cnr.syslog.facility` - Syslog ログがあるファシリティを指定します (Linux OS)。このパラメータは、Windows では無視されます。有効なファシリティ キーワードは、`daemon` (デフォルト)、`local0`、`local1`、`local2`、`local3`、`local4`、`local5`、`local6`、`local7` です。
- `cnr.syslog.ids` - ログに記録する (またはログに記録しない) 個別のメッセージを、メッセージ ID のカンマ区切りリストまたはメッセージ ID 範囲 ($x-y$) として指定します。メッセージ ID または範囲の前にマイナス記号 (ハイフン) または ! (感嘆符) がある場合、そのメッセージ ID または ID 範囲は明示的にログに記録されません。明示的に参照されるメッセージ ID は、他の Syslog 設定 (.enable 設定を含む) に関係なくログに記録されたり記録されなかったりします。

メッセージ ID を確認するには、`/opt/nwreg2/local/docs/msgid/*.html` ファイル (または実際のサーバーログファイル) を参照してください。

次に例を示します。

```
cnr.syslog.ids=4000-4100,-4101-4200,4300
```

これにより、メッセージ 4000 ~ 4100 および 4300 が Syslog (または Windows イベントロギング) に記録され、メッセージ 4101 ~ 4200 がログに記録されません (他の Syslog 設定に関係なく)。



- (注)
- これらのパラメータは、すべての Cisco Prime Network Registrar サーバー (`cnrservagt`、`ccm`、`cdns`、`cnrsnmp`、`dns`、`dhcp`、および `tftp`) に適用されます。
 - `cnr.conf` パラメータに変更を適用するには、Cisco Prime Network Registrar を再起動する必要があります。

次の `cnr.conf` 設定パラメータによって、上記のパラメータのサーバー固有のオーバーライドが可能です。server は、`cnrservagt`、`ccm`、`cdns`、`cnrsnmp`、`dns`、`dhcp`、および `tftp` のいずれかです。

- `cnr.syslog.server.enable` - 指定されたサーバーについて、Syslog または Windows イベントロギングが有効かどうかを指定します (`cnr.syslog.enable` は、そのサーバーについては無視されます)。
- `cnr.syslog.server.levels` - 指定されたサーバーの重大度レベルを指定します (`cnr.syslog.levels` は、そのサーバーについては無視されます)。
- `cnr.syslog.server.facility` - 指定されたサーバーの Syslog ファシリティを指定します (`cnr.syslog.facility` は、そのサーバーについては無視されます)。

指定されている場合は、サーバー固有の設定値が使用されます。それ以外の場合は、サーバーのすべてのパラメータが使用されます。たとえば、DHCP についてのみ Syslog を有効にするには、`cnr.conf` ファイルに次のように追加します。

```
cnr.syslog.dhcp.enable=1
```

すべてのサーバーの Syslog 設定を設定する例：

```
cnr.syslog.enable=1
cnr.syslog.levels=error,warning,activity
```

権威 DNS サーバーについてのみ Syslog を有効にするには、次のようにします。

```
cnr.syslog.dns.enable=1
cnr.syslog.dns.levels=error,warning,activity
```



ヒント

`cnr.conf` パラメータの構文またはその他のエラーは報告されず、無視されます (つまり、レベルキーワードがタイプミスされた場合、そのキーワードは無視されます)。したがって、設定変更が機能しない場合は、パラメータが正しく指定されているかどうかを確認してください。



- (注) 多くの Syslog 実装ではレート制限が実装されており、Cisco Prime Network Registrar サーバーのロギングによってこれが容易にトリガーされ、ログデータの Syslog への喪失が発生します。これが発生している場合は通常、`/var/log/messages` の「Suppressed *number* messages from」メッセージが表示されます。多くの Syslog 実装には、これをトリガーするレートを制御したり、アクションを無効にしたりする設定があります (ただし無効にすることは推奨されません)。これらの調整を行うか、Syslog に記録する内容を減らすことを検討する必要があります (特に高レベルのアクティビティの場合は、すべてを記録することは推奨されません)。通常、これは `/etc/systemd/journald.conf` の `RateLimitInterval` および `RateLimitBurst` 設定を調整することを意味します。

サーバー障害のトラブルシューティング

サーバー エージェント プロセス (`nwreglocal` および `nwreglocal`) は、通常、サーバー障害を検出して、サーバーを再起動します。通常、障害から回復でき、サーバーが再起動後すぐに再び

障害を起こすことはありません。まれに、サーバー障害の原因によってサーバーの正常な再起動が妨げられ、再起動するとすぐにサーバーが再び障害を起こすことがあります。このような場合は、次の手順を実行します。

ステップ 1 サーバーの再起動にかなり時間がかかる場合は、サーバーエージェントを停止して再起動します。次の場合、

- Windows :

```
net stop nwreglocal or nwregregion
net start nwreglocal or nwregregion
```

- Linux :

```
/etc/rc.d/init.d/nwreglocal stop or nwregregion stop
/etc/rc.d/init.d/nwreglocal stop or nwregregion start
```

ステップ 2 すべてのログ ファイルのコピーを保存します。ログ ファイルは、Linux では *install-path/logs* ディレクトリに、Windows では *install-path/logs* フォルダにあります。ログ ファイルには、サーバー障害の原因を特定するのに役立つ有用な情報が含まれていることがよくあります。

ステップ 3 **TAC ツールの使用 (215 ページ)** の説明に従って TAC ツールを使用するか、オペレーティング システムに応じて、コアまたは *user.dmp* ファイル (存在する場合) を保存します。

- **Windows-** *user.dmp* ファイルはシステム ディレクトリにあり、これは Windows システムによって異なります。このファイルを検索して、名前を変更したコピーを保存します。
- **Linux -** コア ファイルは *install-path* にあります。Cisco Prime Network Registrar が上書きしないように、このファイルのコピーを名前を変更して保存します。

ステップ 4 Windows では、ネイティブ イベント ログिंग アプリケーションを使用して、システムおよびアプリケーション イベント ログをファイルに保存します。これは、イベントビューアから行うことができます。これらのイベント ログには、Cisco Prime Network Registrar サーバー問題のデバッグに役立つデータが含まれていることがよくあります。各サーバー モジュールのログ メッセージの説明については、*install-path/docs/msgid/MessageIdIndex.html* ファイルを参照してください。

Linux トラブルシューティング ツール

Linux システムで次のコマンドを使用して、Cisco Prime Network Registrar のトラブルシューティングを行うこともできます。目的 :

- すべての Cisco Prime Network Registrar プロセスを表示します。

```
ps -leaf | grep nwr
```

- システムの使用状況とパフォーマンスをモニターします。

```
top
vmstat
```


- ログインまたはブートアップ エラーを表示します。

```
grep /var/log/messages*
```

- 設定されているインターフェイスおよびその他のネットワーク データを表示します。

```
ifconfig -a
```

TAC ツールの使用

多くのトラブルシューティング手順でも問題を解決できないときには、最後の手段として、Cisco Technical Assistance Center (TAC) に連絡して支援を受ける必要がある場合があります。Cisco Prime Network Registrar は、サーバーまたはシステム エラー情報を簡単に収集して、このデータを TAC サポート エンジニアのためにパッケージ化するためのツールを提供します。これにより、TAC の支援によってこの情報を手動で収集する必要がなくなります。このツールによって生成されたパッケージは、エンジニアが問題を迅速かつ簡単に診断し、解決策を提供できるだけの十分なデータを提供します。

cnr_tactool ユーティリティは、Windows の bin ディレクトリと、UNIX または Linux のインストール ディレクトリの usrbin ディレクトリにあります。**cnr_tactool** ユーティリティを実行します。

```
> cnr_tactool -N username -P password [-d output-directory] [-n]
```

出力ディレクトリはオプションであり、通常はインストール ディレクトリの temp ディレクトリです (Linux の /var パスにあります)。**-n** オプションを指定すると、**cnr_exim** ツールが実行されるときに、リソース レコードをエクスポートせずに実行することを指定できます (これは、**cnr_exim** に対して **-a none** オプションを指定します)。コマンドラインでユーザー名とパスワードを指定しなかった場合は、次のプロンプトが表示されます。

```
> cnr_tactool
user:
password:
[processing messages....]
```

このツールは、名前に日付とバージョンを含むパッケージ化された tar ファイルを生成します。tar ファイルには、すべての診断ファイルが含まれています。

statscollector ユーティリティの使用

Cisco Prime Network Registrar には、ローカルクラスタの CCM サーバーによって収集された統計情報を読み取る **statscollector** ユーティリティが含まれています。これには、次のようなオプションがあります。

- クラスタから CCM サーバーの履歴を取得します。現在利用可能な履歴を取得し、必要に応じて新しい履歴が利用可能になったときに引き続き収集し、それをファイルに書き込むことができます。このファイルは、後で処理したり追加することができます。デフォルトでは statscollector は「恒久的」に動作しつづけて履歴を収集することに注意してください。**-i 0** を指定することにより、現在の履歴を取得し、そこで終了するように要求することが

できます。ファイルが存在する場合は、その履歴データを読み取って、収集された「最後の」サンプルを判別し、そこから追加のデータを収集し始めます（そのため、**-i 0**を指定して実行することにより、多くの場合、「新しい」履歴だけを取得できます）。1つのファイルを別のクラスタにも使用すると、2つのクラスタデータが混在し、役に立たなくなる可能性があることに注意してください。

例：

```
statscollector -C cluster -N user -P password stats.bin
```

- 以前にファイルに収集された統計データまたはクラスタから取得された統計データのXML（Excelなどのツールへのインポート用）を生成します。

- 例（既存のファイルを使用）：

```
statscollector -e stats.xml stats.bin
```

- 例（クラスタからの収集）：

```
statscollector -C cluster -N user -P password -e stats.xml
```

- 以前にファイルに収集された統計データまたはクラスタから取得された統計データのHTML（Google Charts APIを使用）を生成します。組み込みグラフを使用するか独自のグラフを定義し、それらをプロットできます。

- 例（既存のファイルを使用）：

```
statscollector -h stats.html stats.bin
```

- 例（クラスタからの収集）：

```
statscollector -C cluster -N user -P password -h stats.html
```

Linux では、次の場所から statscollector を実行できます。

/opt/nwreg2/local/usrbin

次のオプションを使用できます。

表 24: statscollector のオプション

オプション	説明
-C <i>cluster</i> :[port]	接続するローカルクラスタ（デフォルト：localhost）。
-N <i>admin</i>	管理者アカウント名。
-P <i>password</i>	管理者パスワード。
-i <i>interval</i>	新しい統計をポーリングする間隔（デフォルト：60秒）。これを0に設定すると、1回読み取った後に終了します。

オプション	説明
-e <i>file.xml</i>	バイナリデータファイルをXML形式でエクスポートします。 注 ： -i により、使用するデータのサンプリングの最小間隔が制御されます（デフォルト：1秒）。
-h <i>file.html</i>	統計グラフを含むHTMLファイルを作成します。 注 ： -i により、使用するデータのサンプリングの最小間隔が制御されます（デフォルト：1秒）。
-c <i>charts.txt</i>	-h の場合は、オプションのチャート定義ファイルが作成されます。
-s <i>date time</i>	指定した日時より前の統計サンプルを無視します。
-f <i>date time</i>	指定した日時より後の統計サンプルを無視します。
-w <i>width X height</i>	グラフの幅と高さをピクセル単位で指定します（デフォルト：800 X 400）。
-j <i>name,value</i>	Google 注釈グラフオプションを指定します。
-t " <i>title</i> "	グラフのタイトル（デフォルトを上書きする）。
-u <i>infile.html</i>	ソースHTMLファイル内のグラフを更新します。 -h オプションが必要です。
<i>file</i>	バイナリデータファイル（ -e または -h が指定されていない場合に必要）。ファイルが存在する場合、データはファイルに追加されます。



(注) XML または HTML にエクスポートする場合、収集される統計情報によっては、生成されるファイルが非常に大きくなる可能性があります。**-i**、**-s**、および**-f** オプションを使用することにより、データを制限できます。たとえば、**-i 300** は、エクスポートされたデータが5分ごとにのみレポートされることを意味します。ただし、特定の（より短い）時間間隔のデータを表示するには、**-s** と **-f** の方が効果的である場合があります。

TFTP サーバーのトラブルシューティングと最適化

特定の属性を設定して、TFTP サーバーのパフォーマンスをトラブルシューティングし、最適化することができます。

関連項目

[TFTP サーバー アクティビティのトレース \(218 ページ\)](#)

[TFTP メッセージ ロギングの最適化 \(218 ページ\)](#)

[TFTP ファイル キャッシングの有効化 \(219 ページ\)](#)

TFTP サーバー アクティビティのトレース

TFTP サーバーのアクティビティをトレースするには、TFTP サーバーでトレース ファイルへのメッセージの書き込みに使用する冗長性のレベルに応じて、`packet-trace-level` 属性を 1~4 の値に設定します。トレース ファイルは、インストールディレクトリの `/logs` サブディレクトリにあります。Windows のトレースは、`file_tftp_1_log` ファイルに送られます。Linux のトレースは、`/var/nwreg2/{local | regional}/logs/file_tftp_1_log` および `file_tftp_1_trace` ファイルに送られます。

次にトレース レベルを示します。レベルが高いほど累積的です。

- **0-** すべてのサーバー トレースを無効にします (デフォルト)。
- **1-** トレース ファイル内のすべてのログ メッセージを表示します。
- **2-** すべてのパケットのクライアント IP アドレスとポート番号を表示します。
- **3-** パケットのヘッダー情報を表示します。
- **4-** パケットの最初の 32 バイトを表示します。



(注) トレース レベルの設定と取得は、TFTP サーバーが起動している場合にのみ機能します。パフォーマンス上の理由から、パケットトレースはデバッグ目的でのみ有効にして、その後は長時間使用しないようにします。

TFTP メッセージ ロギングの最適化

ロギングとトレースを制限することによって、TFTP サーバー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、サーバーはエラー、警告、および情報メッセージを `file_tftp_1_log` ファイルに記録します。次のいくつかの TFTP サーバーパラメータを使用して、ログ レベルを設定できます。

- **Log level** (`log-level` 属性を使用) : サーバーロギングのプライマリコントローラであり、レベル 3 (エラー、警告、および情報メッセージのすべてをログに記録) に事前設定され

ており、そのままにしておくことをお勧めします。パケットトレースと同様に、ロギングレベルが高いほど累積的です。0 に設定すると、サーバー ロギングは行われません。

- **Log settings** (*log-settings* 属性を使用) - これはロギング制御の第 2 レベルであり、*default* または *no-success-messages* の 2 つの値のいずれかを取ります。*default* ログ設定では、ログレベル 3 のデフォルト値は変更されません (エラー、警告、および情報メッセージ)。ただし、ログ設定を *no-success-messages* に変更することによって、成功情報メッセージの書き込みを無効にして、サーバーのパフォーマンスを向上させることができます。
- **Log file count and size** (*log-file-count* 属性を使用) - /logs ディレクトリに維持するログファイルの数と、最大許容サイズを設定します。デフォルト値では、それぞれ 10 MB のファイルを最大 10 個まで維持します。



(注) これらの値を変更した後は、TFTP サーバーをリロードしてください。

TFTP ファイル キャッシングの有効化

サーバーのファイル キャッシングを有効にすることで、TFTP サーバーのパフォーマンスを大幅に向上させることができます。これは、無効に事前設定されているため、明示的に行う必要があります。また、ファイル キャッシュ ディレクトリを作成してポイントする必要があります。また、このディレクトリの最大サイズを設定することができます。次に、手順を示します。

- ステップ 1** TFTP キャッシュ ファイルの移動先を決定します。これは TFTP ホーム ディレクトリのサブディレクトリになります。これは、*install-path/data/tftp* に事前設定されています (Linux では、*/var/nwreg2/{local|regional}/data/tftp*)。別の場所を使用する場合は、*home-directory* 属性を設定します。
- ステップ 2** TFTP ホームディレクトリに移動し、**mkdir Cachedir** コマンドを使用して、ホームディレクトリに *CacheDir* などのキャッシュ ディレクトリを作成します。Cisco Prime Network Registrar は、このキャッシュ ディレクトリのサブディレクトリにあるすべてのファイルが無視することに注意してください。
- ステップ 3** *file-cache-directory* 属性を使用して、キャッシュ ディレクトリを指すように TFTP サーバーを設定します。ディレクトリ名に絶対パスまたは相対パスを使用することはできません。*file-cache-directory* 名は、*home-directory* またはデフォルトのホーム ディレクトリ パスで指定されたパスに付加されます (いずれかを指定しなかった場合)。
- ステップ 4** *file-cache-max-memory-size* 属性を使用して、キャッシュの最大メモリ サイズをバイト単位で設定します。プリセット値は 32 KB です。Cisco Prime Network Registrar は、このメモリ サイズに累積的に適合するすべてのファイルをキャッシュにロードします。値を 0 に設定した場合、ファイル キャッシングを有効にした場合でも、Cisco Prime Network Registrar はデータをキャッシュしません。
- ステップ 5** キャッシュしたいすべてのファイルを、サブディレクトリではなく、キャッシュディレクトリにコピーします。このディレクトリ内のすべてのファイルはキャッシュにロードされるため、大きなファイルを含めないでください。

- ステップ 6** *file-cache* 属性を有効にして、ファイルキャッシングを有効にし、サーバーをリロードします。Cisco Prime Network Registrar は、キャッシュされた各ファイルの名前を記録し、ロードできないものをすべてスキップします。すべてのファイルをバイナリデータとして読み取り、TFTPクライアント要求として変換します。たとえば、クライアントが NetASCII としてファイルを要求した場合、クライアントはその形式でキャッシュされたデータを受信します。
- ステップ 7** キャッシュへの書き込みは許可されていません。キャッシュファイルを更新する必要がある場合は、キャッシュディレクトリで上書きしてから、サーバーをリロードします。
-



第 9 章

バックアップとリカバリ

この章では、Cisco Prime Network Registrar データベースを維持する方法について説明します。

- [データベースのバックアップ \(221 ページ\)](#)
- [シンタックスと位置 \(222 ページ\)](#)
- [バックアップ戦略 \(223 ページ\)](#)
- [CNRDB データのバックアップ \(225 ページ\)](#)
- [tar または類似のツールを使用したすべての CNRDB のバックアップ \(226 ページ\)](#)
- [データベース リカバリ戦略 \(227 ページ\)](#)
- [リージョン クラスタ データベース問題からの回復 \(231 ページ\)](#)
- [Cisco Prime Network Registrar 実行中のウイルス スキャン \(235 ページ\)](#)
- [データベースのトラブルシューティング \(235 ページ\)](#)

データベースのバックアップ

Cisco Prime Network Registrar データベースはさまざまなメモリ キャッシングを実行し、いつでもアクティブにすることができるため、サードパーティのシステム バックアップを使用してデータベースを保護することはできません。これらでは、バックアップデータの不整合や、使用できない交換データベースが発生することがあります。

この目的のために、Cisco Prime Network Registrar はシャドウ バックアップ ユーティリティ、**cnr_shadow_backup** を提供します。1 日に 1 回、Cisco Prime Network Registrar は重要なファイルのスナップショットを取ります。このスナップショットは、データベースの一貫性のあるビューであることが保証されています。

推奨

Cisco Prime Network Registrar の 10.1 よりも前のバージョンから 10.1 (以上) にアップグレードする場合、および DHCPv6 リース (または DHCPv6 リース履歴レコード) の数が多い場合、アップグレード後に DHCPv4 データベースのサイズを減らすために、DHCP データベースのダンプとロード ([cnrdb_util ユーティリティの使用 \(240 ページ\)](#) を参照) をスケジュールする必要があります。DHCPv6 リース (アクティブ+履歴) が新しい dhcp6.ndb に移動される時、アップグレードによって元の dhcp.ndb データベースのサイズが縮小されることはなく、元の

データベースのサイズを減らす唯一の方法は、ダンプとロードを実行することです。dhcp6.ndb ファイルのサイズを表示すると (ls (Unix) または dir (Windows) コマンドを使用)、減らすことができるデータベースのサイズを推計できます。

関連項目

[シンタックスと位置 \(222 ページ\)](#)

[バックアップ戦略 \(223 ページ\)](#)

[データベース リカバリ戦略 \(227 ページ\)](#)

[CNRDB データのバックアップ \(225 ページ\)](#)

[tar または類似のツールを使用したすべての CNRDB のバックアップ \(226 ページ\)](#)

[バックアップからの CNRDB データのリカバリ \(229 ページ\)](#)

[tar または類似のツールを使用したすべての CNRDB のリカバリ \(230 ページ\)](#)

[tar または類似のツールからの単一の CNRDB のリカバリ \(230 ページ\)](#)

[Cisco Prime Network Registrar 実行中のウイルス スキャン \(235 ページ\)](#)

シンタックスと位置

以下の項の「`.../data/db`」という表記は、オペレーティング システムに応じて、Cisco Prime Network Registrar 製品のデータ ロケーションパスのディレクトリを指しています。

- **Windows** - 「`.../data`」はデータ ディレクトリを意味し、デフォルトでは **C:\NetworkRegistrar\{Local | Regional}\data** です。
- **Linux** - 「`.../data`」はデータ ディレクトリを意味し、デフォルトでは **/var/nwreg2/{local | regional}/data** です。

以下の項で説明する Cisco Prime Network Registrar データベース ユーティリティプログラムは「`.../bin`」ディレクトリにあり、フルパス名で実行します。

- **Windows** - 「`.../bin/program`」は、bin ディレクトリ内のプログラム ファイルを意味し、デフォルトでは、32 ビット OS の場合は **C:\Program Files\Network Registrar\{Local | Regional}\bin\program**、64 ビット OS の場合は **C:\Program Files (x86)\Network Registrar\{Local | Regional}\bin\program** です。
- **Linux** - 「`.../bin/program`」は、bin ディレクトリ内のプログラム ファイルを意味し、デフォルトでは、**/opt/nwreg2/local/usrbin/program** または **/opt/nwreg2/regional/usrbin/program** です。



- (注) データベースのタイプごとに、承認済みのユーティリティのみを使用してください。Windows では、インストールパスの外部からユーティリティを実行する場合は、CNR_HOME 環境変数を設定する必要があります。

バックアップ戦略

バックアップ戦略には、次のいずれかが含まれます。

CCM を使用して夜間のシャドウバックアップを実行し（[自動バックアップ時間の設定（224 ページ）](#) を参照）、パーマネントバックアップ用にシャドウバックアップを使用してから、明示的なバックアップを実行します。**cnr_shadow_backup** ユーティリティを使用して、バックアップファイル (*.bak DB) をバックアップします。

または

Cisco Prime Network Registrar をシャットダウンし、TAR またはその他同様のツールを使用してバックアップを実行します。

手動バックアップ (cnr_shadow_backup ユーティリティを使用)

cnr_shadow_backup ユーティリティを使用して、次のデータベースをバックアップします。

- **CNRDB databases -**

`./data/dhcp`、`./data/dns/cstdb`、`./data/dns/ndb`、`./data/cchs`、`./data/leasehist`、`./data/leasehist`、`./data/subnetutil`、`./data/mod`、`./data/replica`、
および ...data/ccm/ndb



(注) データ ディレクトリの場所を変更した場合は、`.../conf` にある **cnr.conf** ファイルを編集する必要があります（[cnr.conf ファイルの変更（210 ページ）](#) を参照）。**cnr.datadir** 変数をデータ ディレクトリへのフルパスに変更します。たとえば、Windows のデフォルト値は、次のとおりです。

```
cnr.datadir=C:\\NetworkRegistrar\\{Local|Regional}\\data
```

バックアップ戦略の最も基本的なコンポーネントは、毎日のシャドウバックアップです。運用データベースで問題が発生した場合は、前日のシャドウバックアップに基づいて回復を試みる必要がある場合があります。したがって、バックアップの成功を妨げる問題を認識し、修正する必要があります。

最も一般的な問題は、ディスク領域の枯渇です。必要なディスク領域を大まかに見積もるには、`.../data` ディレクトリのサイズを取得し、10 倍します。使用パターン、アプリケーションミックス、Cisco Prime Network Registrar 自体の負荷などのシステム負荷によって、より大きな容量の予約が使用可能であることが示される場合があります。

将来のリカバリのために、既存のシャドウバックアップを定期的に（テープ、他のディスク、または他のシステムなどに）アーカイブしておく必要があります。



注意 推奨されるタイプとは異なるタイプのデータベースでユーティリティを使用すると、データベースが破損する可能性があります。示されているユーティリティのみを使用してください。また、運用データベースではデータベースユーティリティを使用せず、コピーでのみ使用してください。

関連項目

[自動バックアップ時間の設定 \(224 ページ\)](#)

[手動バックアップの実行 \(224 ページ\)](#)

[cnr_shadow_backup を使用したサードパーティ製バックアッププログラムの使用 \(224 ページ\)](#)

自動バックアップ時間の設定

cnr.conf ファイル (.../conf 内) を編集することによって、自動バックアップを実行する時間を設定できます。**cnr.backup-time** 変数を自動シャドウ バックアップの時間と分に24 時間の *HH:MM* 形式で変更して、サーバーエージェントを再起動します。たとえば、次のようなプリセット値があります。

```
cnr.backup-time=23:45
```



(注) **cnr.backup-time** に加えた変更を有効にするには、Cisco Prime Network Registrar を再起動する必要があります。

手動バックアップの実行

cnr_shadow_backup ユーティリティを使用して手動バックアップを開始することもできますが、これにはルート権限が必要です。バックアップを実行するには、プロンプトで **cnr_shadow_backup** コマンドを入力します。



(注) バックアップよりも最新のフェールオーバー パートナーから DHCP データを復元するには、[フェールオーバー サーバーからの DHCP データの復元 \(243 ページ\)](#) を参照してください。

cnr_shadow_backup を使用したサードパーティ製バックアッププログラムの使用

cnr_shadow_backup が動作している間は、サードパーティのバックアッププログラムをスケジュールしないようにする必要があります。サードパーティのバックアッププログラムは、**cnr_shadow_backup** 操作よりも前または後のいずれかの時刻に実行する必要があります。自動

[バックアップ時間の設定 \(224 ページ\)](#) で説明されているように、デフォルトのシャドウバックアップ時間は毎日 23:45 です。

Cisco Prime Network Registrar の運用データベースのディレクトリとファイルをスキップし、シャドウ コピーのみをバックアップするように、サードパーティのバックアッププログラムを設定します。

運用ファイルは、[バックアップ戦略 \(223 ページ\)](#) に記載されています。Linux では、Cisco Prime Network Registrar は、次のディレクトリのロックファイルも保持します。

- Cisco Prime Network Registrar サーバー プロセス - /var/nwreg2/local/temp/np_destiny_trampoline または /var/nwreg2/regional/temp/np_destiny_trampoline

ロックファイルは再起動時に再作成されます。これらのファイルは、システムの実行中は重要です。メンテナンス プロセス（ウイルススキャンやアーカイブなど）では、一時ディレクトリ、運用データベース ディレクトリ、およびファイルを除外する必要があります。

Windows はロック ファイルを維持せず、代わりに名前付きパイプを使用します。

CNRDB データのバックアップ

CNRDB データベースの場合、**cnr_shadow_backup** ユーティリティは、データベースとすべてのログファイルを、インストールされている Cisco Prime Network Registrar 製品のディレクトリツリー内のセカンダリディレクトリにコピーします。手順は次のとおりです。

- **DHCP** : 運用データベースは .../data/dhcp/ndb、.../data/dhcp/ndb6、および .../data/dhcp/clientdb ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは、.../data.bak/dhcp/ndb、.../data.bak/dhcp/ndb6、および.../data.bak/dhcp/clientdb ディレクトリにあります。
- **DNS** : 運用データベースは .../data/dns/rrdb ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。重要な運用コンポーネントは、.../data/dns/hadb ディレクトリにある高可用性 (HA) DNS であり、ログファイルは.../data/dns/hadb/logs ディレクトリにあります。シャドウコピーは .../data.bak/dns ディレクトリにあります。
- **CCM** : 運用データベースは .../data/ccm/ndb、.../data/ccm/rrdb、および .../data/ccm/clientdb ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは .../data.bak/ccm ディレクトリにあります。
- **MCD change log** : 運用データベースとログファイルは .../data/mcd/ndb ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。シャドウ コピーは .../data.bak/mcd ディレクトリにあります。変更ログのエントリがない場合、MCD 変更ログデータベースは存在しない可能性があります。また、MCD 変更ログの履歴が除去されたとき、または開始する MCD 変更ログデータがないときにも、データベースは削除されません。
- **Lease history** : 運用データベースとログファイルは .../data/leasehist および .../data/lease6hist ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは .../data.bak/leasehist および .../data.bak/lease6hist ディレクトリにあります。

- **DHCP utilization** : 運用データベースとログファイルは `.../data/subnetutil` ディレクトリにあり、データベースログファイルは `logs` サブディレクトリにあります。シャドウ コピーは `.../data.bak/subnetutil` ディレクトリにあります。
- **Replica** : 運用データベースとログファイルは `.../data/replica` ディレクトリにあり、データベースログファイルは `logs` サブディレクトリにあります。

次の表に、Cisco Prime Network Registrar のデータベースファイルを示します。

表 25: データベース ファイル

ディレクトリ	サブディレクトリ	ファイル名
dhcp	<code>.../data/dhcp/ndb</code>	<code>dhcp.ndb</code>
	<code>.../data/dhcp/ndb6</code>	<code>dhcp6.ndb</code>
	<code>.../data/dhcp/clientdb</code>	<code>*.db</code>
dns	<code>.../data/dns/csetdb</code>	<code>dnscset.db</code>
	<code>.../data/dns/hadb</code>	<code>dnsha.db</code>
	<code>.../data/dns/rrdb</code>	<code>*.db</code>
ccm	<code>.../data/ccm/clientdb</code>	<code>changelog.db</code> <code>config.db</code>
	<code>.../data/ccm/ndb</code>	<code>*.db</code>
	<code>.../data/ccm/rrdb</code>	<code>changelog.db</code> <code>config.db</code>

ログファイルは、`log.0000000001` ~ `log.9999999999` として示されます。ファイルの番号は、サーバーに対する変更の頻度によって異なります。通常は、少数の番号しかありません。サイトの特定のファイル名拡張子は、データベースが使用される時間の経過とともに変化します。これらのログ ファイルは人間に読める形式ではありません。

tar または類似のツールを使用したすべての CNRDB のバックアップ

ここでは、tar または類似のツールを使用して、すべての Cisco Prime Network Registrar データベースをバックアップする手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。

Cisco Prime Network Registrar が実行している場合、tar または類似のツールを使用してバックアップを実行することはできません。

ステップ2 data ディレクトリとサブディレクトリ全体をバックアップします。

```
> /var/nwreg2/local/data or /var/nwreg2/regional/data
> /opt/nwreg2/*/conf
```

ステップ3 バックアップが完了したら、Cisco Prime Network Registrarを再起動します。

(注) 技術的には、バックアップには、夜間のシャドウ バックアップが含まれているため、*.bak ディレクトリ（およびそれらのディレクトリのサブディレクトリ）を含める必要はありません。ただし、使用可能なストレージ領域が非常に制限されている場合を除き、シャドウバックアップを含め、data ディレクトリ（およびサブディレクトリ）全体の完全バックアップを推奨します。

データベース リカバリ戦略

Cisco Prime Network Registrar は CNRDB データベースを使用します。次の表に、バックアップとリカバリが必要な CNRDB データベースのタイプを示します。

表 26: リカバリのための Cisco Prime Network Registrar データベース

サブディレクトリ	クラスタ	タイプ	説明
mcd	ローカル	CNRDB	MCD 変更ログ データ。除去されていない MCD 変更ログ履歴がある限り、8.0 以前のデータベースからのアップグレードのためにのみ存在します。
ccm	ローカル、リージョン	CNRDB	中央構成管理データベース。ローカルの一元管理対象のクラスタと SNMP サーバーデータを格納します。
dns	ローカル	CNRDB	DNS データベース。ゾーンの状態情報、保護された RR の名前、および DNS サーバーのゾーン設定データを格納します。

サブディレクトリ	クラスタ	タイプ	説明
cdns	ローカル		DNS データベースをキャッシュしています。最初の DNSSEC ルートトラストアンカーおよびルートヒントを格納します。
dhcp ⁴	ローカル	CNRDB	DHCP データベース。DHCP サーバーのリース状態データを格納します。
dhcpeventstore	ローカル		Cisco Prime Network Registrar が、LDAP および DHCPv4 DNS アップデートの相互作用など、外部サーバーと対話するために維持するキュー。リカバリは必要ありません。
tftp	ローカル		TFTP サーバーのデフォルトのデータディレクトリ。リカバリは必要ありません。
レプリカ	リージョン	CNRDB	ローカルクラスタのレプリカデータを格納します。
lease6hist	リージョン	CNRDB	DHCPv6 リース履歴データベース。
leasehist	リージョン	CNRDB	DHCPv4 リース履歴データベース。
subnetutil	リージョン	CNRDB	DHCP 使用率データベース。サブネットとプレフィックスのデータベースが個別に含まれます。

⁴ DHCP データベース (.../data/dhcp/ndb および .../data/dhcp/ndb6) をバックアップから復元することは推奨されません。このデータは、DHCP サーバーの実行中は常に変化するためです（このサーバーまたはパートナーのいずれかでクライアントアクティビティとリー

スの期限が切れているため)。したがって、バックアップから DHCP ndb/ndb6 データベースを復元すると、サーバーのクロックが元に戻りますが、クライアントのクロックは元に戻りません。そのため、DHCP サーバーのデータベースはバックアップからリカバリするよりも保持する方が望ましく、または、リカバリが必要な場合は、データベースを削除して、フェールオーバーを介してパートナーから現在のリースをリカバリする方が望ましいです（[フェールオーバー サーバーからの DHCP データの復元 \(243 ページ\)](#) を参照）。

Cisco Prime Network Registrar のインストールをリカバリする一般的なアプローチは、次のとおりです。

1. Cisco Prime Network Registrar サーバー エージェントを停止します。
2. データを復元または修復します。
3. サーバー エージェントを再起動します。
4. サーバーでエラーがないかモニターします。

データベースリカバリが正常に実行されたことが確認できたら、常に手動で `cnr_shadow_backup` ユーティリティを実行して、現在の設定と状態のバックアップを作成します。

バックアップからの CNRDB データのリカバリ

サーバー ログ メッセージや欠落しているデータなど、何らかの理由でデータベースの回復に失敗した場合は、現在のシャドウ バックアップ（Cisco Prime Network Registrar のインストール ツリー）でリカバリの試行が必要になることがあります。手順は、次のとおりです。

ステップ 1 Cisco Prime Network Registrar サーバー エージェントを停止します。

ステップ 2 運用データベース ファイルを別の一時的な場所に移動します。

ステップ 3 各 `.../data/name.bak` ディレクトリを `.../data/name` にコピーします。たとえば、`.../data/ccm.bak` を `.../data/ccm` にコピーします。

(注) `cnr.conf` ファイル `cnr.dbrecover` 変数を `false` に設定して、`cnr_shadow_backup` の夜間のバックアップ時のリカバリを無効にした場合は、次の手順の一部として、リカバリも実行する必要があります。

ステップ 4 ファイルの名前を変更します。

CNRDB データベースは一元管理される設定データを維持し、これはサーバー設定データベースと同期されます。

ステップ 5 新しいデータ ディレクトリを作成し、バックアップされたディレクトリを解凍または回復します。

DB ディレクトリとリカバリ ツールを実行して、データベースが正常であることを確認することをお勧めします。

(注) `logs` サブディレクトリが同じディレクトリに存在するか、または `logs` パスが `DB_CONFIG` ファイルに記載されていることを確認します。

ステップ 6 サーバー エージェントを再起動します。

tar または類似のツールを使用したすべての CNRDB のリカバリ

(注) リカバリが失敗した場合は、現在のシャドウバックアップが単に破損したファイルのコピーである可能性があるため、以前の最新のシャドウバックアップを使用します。これは、シャドウバックアップを定期的にアーカイブする必要があることを示しています。以前のシャドウバックアップファイルに動作ログ ファイルを追加することはできません。シャドウバックアップの作成後にデータベースに追加されたすべてのデータが失われます。

データベースのリカバリが成功したら、**cnr_shadow_backup** ユーティリティを使用して即時バックアップを開始し、ファイルをアーカイブします ([手動バックアップの実行 \(224 ページ\)](#) を参照)。

tar または類似のツールを使用したすべての CNRDB のリカバリ

ここでは、**tar** または類似のツールを使用して、すべての Cisco Prime Network Registrar データベースを回復する手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。**/etc/init.d/nwreglocal stop** (RHEL/CentOS 6.x の場合) または **systemctl stop nwreglocal** (RHEL/CentOS 7.x の場合) を実行して、Cisco Prime Network Registrar がダウンしていることを確認します。

ステップ 2 アクティブなデータ ディレクトリの名前を変更します (**mv data old-data** など)。

(注) データ ディレクトリ (およびそのサブディレクトリ内のすべてのファイル) の 2 倍のサイズに対応できる十分なディスク領域が必要です。十分なディスク領域がない場合は、アクティブなデータ ディレクトリを別のドライブに移動します。

ステップ 3 新しいデータ ディレクトリを作成し、バックアップされたディレクトリを解凍または回復します。

CNRDB ディレクトリとリカバリ ツールを実行して、データベースが正常であることを確認することをお勧めします。

ステップ 4 Cisco Prime Network Registrar を起動します。

(注) 技術的には、復元には、夜間のシャドウバックアップが含まれているため、***.bak** ディレクトリ (およびそれらのディレクトリのサブディレクトリ) を含める必要はありません。ただし、使用可能なストレージ領域が非常に制限されている場合を除き、シャドウバックアップを含むデータ ディレクトリ (およびサブディレクトリ) 全体を完全に復元することをお勧めします。

tar または類似のツールからの単一の CNRDB のリカバリ

このセクションでは、**tar** または類似のツールを使用して単一のデータベースを回復する手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。`/etc/init.d/nwreglocal stop` (RHEL/CentOS 6.x の場合) または `systemctl stop nwreglocal` (RHEL/CentOS 7.x の場合) を実行して、Cisco Prime Network Registrar がダウンしていることを確認します。

ステップ 2 アクティブなデータ ディレクトリの名前を変更します (`mv data old-data` など)。

(注) データ ディレクトリ (およびそのサブディレクトリ内のすべてのファイル) の 2 倍のサイズに対応できる十分なディスク領域が必要です。十分なディスク領域がない場合は、アクティブなデータ ディレクトリを別のドライブに移動します。

ステップ 3 新しいデータディレクトリを作成し、そのディレクトリ (およびそのサブディレクトリ) 内のファイルのみをバックアップから解凍または回復します。

CNRDB 整合性およびリカバリ ツールを実行して、CNRDB が正常であることを確認することをお勧めします。

ステップ 4 回復する必要があるその他の DB について、**ステップ 2**~**ステップ 3**を繰り返します。

ステップ 5 Cisco Prime Network Registrar を起動します。

リージョンクラスタ データベース問題からの回復

リージョンクラスタには高可用性ソリューションはありません。リージョンクラスタは、ローカルクラスタの動作にとって重要ではありません (ライセンスを除く)。最悪の事態が発生し、バックアップ (夜間のシャドウ バックアップなど) からの復元が失敗した場合は、リージョンクラスタを再構築できます。

リージョンクラスタ データベースは非常に信頼性が高くなっていますが (トランザクションベースであるため)、いくつかの状況では (たとえば、ディスク領域の不足や、不良ブロックなどの物理ディスク問題)、データベースの問題が発生する可能性があり、CCM が起動できなかったり、特定の機能を実行できないことがあります。

リージョンクラスタでは、主に 4 つのデータベースが使用されます。

- 設定オブジェクトを含む CCM データベース (ccm ディレクトリ)。
- ローカルクラスタから収集されたリース履歴 (有効な場合) を含むリース履歴データベース (lease6hist および leasehist)。
- 時間の経過とともに収集されたスコープとプレフィックス使用率の履歴 (有効な場合) を含むサブネット使用率データベース (subnetutil)。
- ローカルクラスタから定期的にプルされた設定を含むレプリカデータベース (replica)。

次の項では、これらのデータベースの 1 つ以上で問題が発生した場合に使用する手順について説明します (これは、`config_ccm_1_log` ファイルとこのファイルで報告されているエラーから判断でき、リージョンの開始不能が含まれている場合もあります)。



- (注) これらの手順を実行する前に、[データベースのトラブルシューティング \(235 ページ\)](#) セクションがデータベースの修正に役立つかどうかを最初に確認してください。修正に役立たない場合は、復元できる可能性がある最新のバックアップが使用可能かどうかを確認してください。

リース履歴データベース問題の処理

リース履歴データベースは、データが保存される期間とクライアントアクティビティのレートによっては、非常に大きくなる可能性があります。このデータベースが破損し、復元できない場合、リージョンクラスタ操作を回復する方法の1つは、このデータベースを削除することです（これにより、リース履歴が失われます）。

次のステップを実行します。

ステップ 1 リージョンクラスタを停止します。

ステップ 2 Lease6hist および/または leasehist データベース ディレクトリを削除（または名前を変更）します。問題が発生したデータベースのみを削除（または名前変更）します。

- (注) これらのデータベースの1つまたは両方を最近のバックアップから復元できた場合は、バックアップ lease6hist および/または leasehist ディレクトリ（およびその下にあるすべてのファイルとディレクトリ）をコピーして、削除された（または名前が変更された）データベースを置き換えることができます。

ステップ 3 リージョンクラスタを起動します。



- (注) これらの手順は、リース履歴を収集する必要がなく、すべての履歴を削除したい場合にも使用できます。ステップ 1 を実行する前に、すべてのリース履歴収集を無効にしてください。

サブネット使用率データベース問題の処理

サブネット/プレフィックス使用率のデータベースは、データが保存される期間、ポーリングの頻度、サブネット/プレフィックスの数に応じて非常に大きくなる可能性があります。このデータベースが破損し、復元できない場合、リージョンクラスタ操作を回復する方法の1つは、このデータベースを削除することです（これにより、使用率の履歴が失われます）。

次のステップを実行します。

ステップ 1 リージョンクラスタを停止します。

ステップ2 subnetutil データベース ディレクトリを削除（または名前変更）します。

(注) 最近のバックアップから subnetutil データベースを復元できる場合は、バックアップ subnetutil ディレクトリ（およびその下にあるすべてのファイルとディレクトリ）をコピーして、削除された（または名前が変更された）データベースディレクトリを置き換えることができます。

ステップ3 リージョン クラスタを起動します。



(注) これらの手順は、使用率データを収集する必要がなくなり、収集したすべてのデータを削除したい場合にも使用できます。ステップ1を実行する前に、すべての使用率履歴収集を無効にしてください。

レプリカ使用率データベース問題の処理

レプリカ データベースは、ローカル クラスタから簡単に再作成できます（各ローカル クラスタの設定のコピーを保存するため）。このデータベースが破損している場合は、このデータベースを削除するのが最善の方法です。

次のステップを実行します。

ステップ1 リージョン クラスタを停止します。

ステップ2 レプリカ データベース ディレクトリを削除（または名前を変更）します。

(注) このデータベースは、ローカルクラスタから簡単に再構築できるため、バックアップから復元しないことをお勧めします。

ステップ3 リージョン クラスタを起動します。

ステップ4 各ローカル クラスタからレプリカ データのプルを開始します（これは数時間以内にローカル クラスタごと自動的に行われるため、発生するまで待機することもできます）。

リージョン クラスタがローカル クラスタと一致することを保証するために、通常、レプリカ データベースが更新されたら、（DHCP を使用している場合は）（IPv4 および IPv6）アドレス空間とゾーン データをプルすることをお勧めします。

リージョンクラスタの再構築

ccm データベースが破損しており、バックアップからのリカバリが不可能である場合や、インデックスの再構築（rebuild_indexes ツールの詳細については、Cisco Technical Assistance Center（TAC）に連絡してください）では問題を解決できない場合は、リージョンを完全に再構築しなければならぬことがあります。場合によっては、新しいシステムにリージョンクラスタを再構築する必要がある場合があります。

既存のリージョンクラスタが動作している場合は、設定データを抽出できる可能性があります。ただし、これは、古いデータや破損したデータを抽出する可能性もあるため、問題です（データベースの破損によっては、同じデータのエクスポートが繰り返される場合もあります）。これを行うには、`cnr_exim` ツールを実行して、バイナリ モードで設定をエクスポートします（`-x` オプションを使用します）。成功した場合は、後でインポートすることができます。ただし、すべてのデータがインポートされるわけではないため、次の手順に従うことが重要です。

新しいシステムの場合は、次のようになります。

-
- ステップ 1 Cisco Prime Network Registrar リージョンクラスタをインストールします。
 - ステップ 2 管理者アカウントをセットアップし、ライセンスを追加します。
 - ステップ 3 すべてのローカルクラスタをリージョンに登録します。このためには、`license register` コマンドを発行する必要があります。リージョンのアドレスとポートが変更されていない場合は、リージョンサーバーのアドレスとポートを指定する必要はありません。
 - ステップ 4 古いリージョンクラスタからデータをエクスポートするために `cnr_exim` を使用した場合は、`cnr_exim` を使用してこれをインポートできます。
 - ステップ 5 「既存のリージョンクラスタ」の手順をスキップして、以下の「共通の手順」に進みます。
-

既存のリージョンクラスタの場合は、次のようになります。

-
- ステップ 1 リージョンクラスタが実行している場合は、停止します。
 - ステップ 2 `/var/nwreg2/regional/data` ディレクトリ（その下のすべてのファイルとディレクトリ）を削除します。
 - (注) `lease6hist`、`leasehist`、および/または `subnetutil` ディレクトリ（およびこれらのディレクトリのすべてのファイル）が破損していず、この履歴情報を保持する場合は、これらのデータベースを保持できます。削除すると、この履歴データは失われます。
 - (注) `ccm` データベースが削除された場合、そのデータは使用できないため、レプリカデータベースを保持しておかないでください。レプリカデータベースを削除しないと、重大な問題が発生する可能性があります。
 - ステップ 3 空の `/var/nwreg2/regional/data` ディレクトリを作成します（完全に削除または移動した場合）。
 - ステップ 4 リージョンクラスタを起動します。
 - ステップ 5 管理者アカウントをセットアップし、ライセンスを追加します。
 - ステップ 6 古いリージョンクラスタからデータをエクスポートするために `cnr_exim` を使用した場合は、`cnr_exim` を使用してこれをインポートできます。
 - ステップ 7 リージョンクラスタを再起動します（すべてのサービスが実行されていることを保証するために必要です）。

- ステップ 8** すべてのローカル クラスタをリージョンに再登録します。このためには、**license register** コマンドを発行する必要があります（これは、ローカルサーバー、IP アドレス、およびポートの既存のリージョン情報に再登録されるため、追加のパラメータは必要ありません）。
- ステップ 9** 次の共通の手順に進みます。

共通の手順（新規または既存のリージョン クラスタの場合）：

- ステップ 1** すべてのレプリカ データが最新であることを確認します。このためには、ローカル クラスタごとに（Web UI で、または **cluster name updateReplicaData** コマンドを使用して）レプリカをプルします。
- ステップ 2** DHCP を使用している場合は、v4 および v6 アドレス空間をプルします（Web UI で、または **ccm pullAddressSpace** および **ccm pullIPv6AddressSpace** コマンドを使用して）。
- ステップ 3** DNS を使用している場合は、ゾーン データをプルします（Web UI で、または **ccm pullZoneData** コマンドを使用して）。
- ステップ 4** この情報を持つローカル クラスタの 1 つから、適切な管理者またはその他のオブジェクト（ポリシー、テンプレートなど）をプルします（Web UI で、または **pull** サブコマンドを使用して）。
-

Cisco Prime Network Registrar 実行中のウイルス スキャン

システムでウイルス スキャンが有効になっている場合は、特定の Cisco Prime Network Registrar ディレクトリをスキャン対象から除外するように設定することをお勧めします。これらのディレクトリを含めると、Cisco Prime Network Registrar の動作が妨げられる可能性があります。除外できるのは、`.../data`、`.../logs`、および `.../temp` ディレクトリとそのサブディレクトリです。

データベースのトラブルシューティング

以下のセクションでは、Cisco Prime Network Registrar データベースのトラブルシューティングについて説明します。

関連項目

- [cnr_exim データ インポートおよびエクスポート ツールの使用](#)（236 ページ）
- [cnrdb_recover ユーティリティの使用](#)（239 ページ）
- [cnrdb_verify ユーティリティの使用](#)（240 ページ）
- [cnrdb_checkpoint ユーティリティの使用](#)（240 ページ）
- [cnrdb_util ユーティリティの使用](#)（240 ページ）
- [フェールオーバー サーバーからの DHCP データの復元](#)（243 ページ）

cnr_exim データ インポートおよびエクスポート ツールの使用

cnr_exim データ インポートおよびエクスポート ツールは、特定のテナントに制限されていないユーザーについて、次のことをサポートするようになりました。

- すべてのデータのエクスポート
- コア データがあるかどうかにかかわらず、テナントに固有のデータのエクスポート
- ライセンス関連データのエクスポートとインポート
- すべてのデータのインポート
- テナントに固有のデータのインポートと、オプションで、コア データの有無にかかわらず、新しいテナントへのマッピング。これにより、新しいテナントの基本設定を作成できます。テナント タグを指定すると、インポートしたデータを使用して古いテナント ID が検索され、現在の設定が新しいテナント ID の検索に使用されます。

マルチテナントアーキテクチャの使用には、テナントの設定を別のクラスタに移動して、テナント テンプレート データをエクスポートし、そのデータを別のテナントとしてインポートできるという利点があります。



- (注) 特定のテナントに制限されたユーザーは、そのテナントのデータのみをエクスポートまたはインポートできます。

cnr_exim ツールは、保護されていないリソース レコードの情報をエクスポートするためにも機能します。ただし、cnr_exim は単に既存のデータに上書きするだけで、競合の解決を試みません。



- (注) Cisco Prime Network Registrar の別のバージョンにデータをインポートまたはエクスポートするために cnr_exim ツールを使用することはできません。これは、Cisco Prime Network Registrar の同じバージョンからのデータのインポートまたはエクスポートにのみ使用できます。

cnr_exim ツールを使用する前に、CLI から終了して、次の場所でツールを見つけます。

- **Windows-** ...\bin\cnr_exim.exe
- **Linux-** .../usrbin/cnr_exim

インポートされたデータをアクティブにするには、サーバーをリロードする必要があります。

テキストのエクスポートは読み取り専用であることに注意してください。再インポートすることはできません。

テキストのエクスポートでは、ユーザー名とパスワードの入力が求められます（クラスタはデフォルトでローカルクラスタになります）。構文は、次のとおりです。

```
> cnr_exim -e exportfile [-N username -P password -C cluster]
```

(インポート可能な) raw データをエクスポートするには、**-x** オプションを使用します。

```
> cnr_exim -e exportfile -x
```

DNS サーバーおよびゾーン コンポーネントをバイナリ データとして raw 形式でエクスポートするには、**-x** および **-c** オプションを使用します。

```
> cnr_exim -e exportfile -x -c "dnserver,zone"
```

データ インポートの構文は、次のとおりです（インポート ファイルは raw 形式である必要があります）。

```
> cnr_exim -i importfile [-N username -P password -C cluster]
```

また、**-o** オプションを使用して、既存のデータに書き替えることもできます。

```
> cnr_exim -i importfile -o
```

次の表では、cnr_exim ツールのすべての修飾オプションについて説明します。

表 27: cnr_exim オプション

オプション	説明
-a	<p>保護された、または保護されていない RR のエクスポートとインポートを許可します。有効な値は、次のとおりです。</p> <p>protectedRR、 unprotectedRR、 および none</p> <p>Export :</p> <p>デフォルトではすべての RR がエクスポートされるため、オプション「-a protectedRR」、「-a unprotectedRR」、または「-a none」を使用して、保護された RR または保護されていない RR のエクスポートを明示的に指定する必要があります。このオプションが指定されなかった場合は、すべての RR がエクスポートされます。</p> <p>Import:</p> <p>デフォルトではすべての RR がインポートされるため、オプション「-a protectedRR」または「-a unprotectedRR」を使用して、保護された RR または保護されていない RR のインポートを明示的に指定する必要があります。このオプションが指定されなかった場合は、すべての RR がインポートされます。</p>
-c	<p>Cisco Prime Network Registrar コンポーネントを、引用符で囲まれたカンマ区切りの文字列としてインポートまたはエクスポートします。-c helpを使用して、サポートされているコンポーネントを表示します。デフォルトでは、ユーザーはエクスポートされません。このオプションを使用して明示的にエクスポートする必要があります。ユーザーは、定義されたグループとロールで常にグループ化されます。秘密はエクスポートされません。</p> <p>(注) 管理者名をインポートした後は、新しいパスワードを設定する必要があります。グループとロールをユーザー名（デフォルトではエクスポートされない）とは別にエクスポートすると、ユーザー名との関係が失われます。</p>

オプション	説明
-C クラスタ	指定されたクラスタからインポートまたはエクスポートします。 localhost に事前設定されています。
-e <i>exportfile</i>	指定されたファイルに設定をエクスポートします。
-h	サポートされているオプションのヘルプ テキストを表示します。
-i <i>importfile</i>	指定されたファイルに設定をインポートします。インポートファイルはraw形式である必要があります。
-N <i>username</i>	指定されたユーザー名を使用してインポートまたはエクスポートします。
-o	-i (インポート) オプションとともに使用すると、既存のデータに上書きします。
-p <i>port</i>	SCP サーバーへの接続に使用されるポート。
-P <i>password</i>	指定されたパスワードを使用してインポートまたはエクスポートします。
-t <i>exportfile</i>	エクスポート先のファイル名を指定し、データを s 式形式でエクスポートします。
-v	バージョン情報を表示します。
-x	-e (エクスポート) オプションとともに使用すると、バイナリデータを (インポート可能な) raw 形式でエクスポートします。
-d	cnr_exim ログ ファイルのディレクトリ パスを指定します。
-f	ソーステナントを指定します。エクスポートおよびインポートについて有効です。
-g	デスティネーション テナントを指定します。インポートの場合のみ有効です。 <i>tenant-id</i> は、データをエクスポートするときに変更することはできず、データがインポートされる時にのみ変更できます。
-b	コア (基本) オブジェクトをインポート/エクスポートに含めることを指定します。これには、明示的な <i>tenant-id</i> が 0 であるすべてのオブジェクトと、 <i>tenant-id</i> 属性を持たないすべてのオブジェクトが含まれます。
-w	エクスポートするビュータグを指定します。このオプションを使用すると、ユーザーは、「w」オプションで説明されているように、同じビュータグを持つゾーンおよび RR データをエクスポートできます。他のすべてのオブジェクトでは、このオプションは考慮されず、使用されている場合も以前と同じようにエクスポートされます。

cnrdb_recover ユーティリティの使用

cnrdb_recover ユーティリティは、システム障害後に Cisco Prime Network Registrar データベースを一貫した状態に復元するのに役立ちます。通常、このコマンドとともに **-c** および **-v** オプションを使用します（次の表では、すべての修飾オプションについて説明しています）。このユーティリティは、インストール先の **bin** ディレクトリにあります。

表 28: **cnrdb_recover** オプション

オプション	説明
-c	通常のリカバリではなく、致命的なリカバリを実行します。存在するすべてのログファイルを検査するだけでなく、ファイルが欠落している場合は現在または指定されたディレクトリに .ndb （または .db ）ファイルを再作成し、存在する場合は更新します。
-e	リカバリの実行後に環境を維持します。ホーム ディレクトリに DB_CONFIG ファイルがない場合は、ほとんど使用されません。
-h dir	データベース環境のホーム ディレクトリを指定します。デフォルトでは、現在の作業ディレクトリが使用されます。
-t	可能な最新の日付ではなく、指定された時刻に回復します。時刻の形式は [[CC]YY]MMDDhhmm[.ss] です（角カッコは省略可能なエントリを示し、年を省略した場合は、デフォルトで現在の年に設定されます）。
-v	冗長モードで実行します。
-V	標準出力にライブラリのバージョン番号を書き込み、終了します。

致命的な障害が発生した場合は、すべてのデータベース ファイルのスナップショットを、スナップショット後に書き込まれたすべてのログファイルとともに復元します。致命的でない場合は、障害発生時のシステム ファイルだけがが必要です。ログ ファイルが欠落している場合、**cnrdb_recover -c** は欠落しているものを特定して失敗します。その場合は、復元して、リカバ리를再度実行する必要があります。

致命的なリカバリ オプションを使用することを強く推奨します。このようにして、リカバリユーティリティは使用可能なすべてのデータベース ログ ファイルを順に再生します。何らかの理由でログ ファイルが欠落している場合は、リカバリ ユーティリティはエラーを報告します。たとえば、次のログ ファイルのギャップが表示されます。

```
log.0000000001
log.0000000053
```

次のエラーが発生し、TAC ケースを開くことが必要になる場合があります。

```
db_recover: Finding last valid log LSN:file:1 offset 2411756
db_recover: log_get: log.0000000002: No such file or directory
db_recover: DBENV->open: No such for or directory
```

cnrdb_verify ユーティリティの使用

cnrdb_verify ユーティリティは、Cisco Prime Network Registrar データベースの構造を確認するのに役立ちます。このコマンドは、ファイルパラメータを必要とします。このユーティリティは、ファイルを変更しているプログラムが実行していないことがわかっている場合にのみ使用してください。次の表では、すべての修飾オプションについて説明します。このユーティリティは、インストール先の **bin** ディレクトリにあります。構文については、コマンドを実行するときの使用方法で説明します。

```
C:\Program Files\Network Registrar\Local\bin>cnrdb_verify
```

```
usage: cnrdb_verify [-NoqV] [-h dir] [-P password] file
```

表 29: **cnrdb_verify** オプション

オプション	説明
-h dir	データベース環境のホーム ディレクトリを指定します。デフォルトでは、現在の作業ディレクトリが使用されます。
-N	実行中の共有リージョンロックの取得を防止します。これは、エラーのデバッグのみを目的としているため、他の状況では使用しないでください。
-o	データベースのソートまたはハッシュの順序を無視して、デフォルト以外の比較またはハッシュ設定で cnrdb_verify を使用できるようにします。
-P password	ユーザーパスワード（ファイルが保護されている場合）。
-q	終了の成功または失敗以外のエラー説明の表示を抑制します。
-V	標準出力にライブラリのバージョン番号を書き込み、終了します。

cnrdb_checkpoint ユーティリティの使用

cnrdb_checkpoint ユーティリティは、データベースファイルのチェックポイントを設定して、最新の状態に保つのに役立ちます。このユーティリティは、インストール先の **bin** ディレクトリにあります。構文については、コマンドを実行するときの使用方法で説明します。

```
C:\Program Files\Network Registrar\Local\bin>cnrdb_checkpoint ?
```

```
usage: cnrdb_checkpoint [-lVv] [-h home] [-k kbytes] [-L file] [-P password] [-p min]
```

cnrdb_util ユーティリティの使用

cnrdb_util ユーティリティは、Cisco Prime Network Registrar データベースのダンプとロードに役立ちます。さらに、このユーティリティを使用して、Cisco Prime Network Registrar データ

ベースのシャドウバックアップとリカバリを実行したり、ログファイルをクリアしたり、データベースのページサイズを変更したりすることができます。

このユーティリティは、次のディレクトリにあります。

- **Windows** : `install-path\bin\cnrdb_util.bat`
- **Linux** : `install-path/usrbin/cnrdb_util`



重要 Cisco Prime Network Registrar データベースで操作を実行する前に、バックアップを実行することを強くお勧めします。既存のバックアップファイルが保持される場合は、それらもバックアップする必要があります。

cnrdb_util ユーティリティは、次の 2 つのモードで動作します。

- **インタラクティブモード** - ユーザーに操作とオプションを求めるプロンプトを表示します。
- **バッチモード** - このユーティリティの実行中に、引数として情報（操作とオプションの両方）が必要です。

構文については、コマンドを実行するときの使用方法で説明します。

```
./cnrdb_util -h
```

次の表では、すべての修飾操作とオプションについて説明します。

表 30: **cnrdb_util** の操作

操作	説明
-d	1 つまたはすべての Cisco Prime Network Registrar データベースをダンプします。
-l	1 つまたはすべての Cisco Prime Network Registrar データベースをロードします。
-b	すべての Cisco Prime Network Registrar データベースのシャドウバックアップを作成します。
-r	シャドウバックアップから 1 つまたはすべての Cisco Prime Network Registrar データベースを復元します。
-c	1 つまたはすべての Cisco Prime Network Registrar データベース内の sleepycat ログファイルをクリーンアップします。
-h	サポートされているオプションのヘルプテキストを表示します。



重要 一度に実行できる操作は 1 つだけです。

表 31: cnrdb_util のオプション

オプション	説明
-m { local regional }	Cisco Prime Network Registrar のインストールモードを指定します。指定されていない場合、この情報は <code>cnr.conf</code> ファイルから読み取られます。ファイルが見つからない場合は、デフォルトでローカルモードが使用されます。
-prog path	ダンプ、ロード、またはシャドウバックアップ実行可能ファイルのパスを指定します。指定しない場合は、Cisco Prime Network Registrar のインストールパスから取得されます。
-db_pagesize number	新しいデータベースを作成するとき使用するデータベース ページのサイズ (バイト数) を指定します。 最小ページサイズは 512 バイトであり、最大ページサイズは 64K バイトであり、2 の累乗にする必要があります。ページサイズが指定されていない場合、ページサイズは、基盤となるファイルシステムの I/O ブロック サイズに基づいて選択されます。(この方法で選択されるページサイズは、512 バイトを下限とし、16K バイトを上限とします)。 通常、デフォルトは適切です。ただし、大きなページサイズはパフォーマンスが良好でない可能性があります。通常、4096 と 8192 は良好なサイズです。 <code>cnrdb_stat</code> ユーティリティを使用して、データベースのページサイズを決定できます。
-n { ccm dhcp dns mcd leasehist lease6hist replica subnetutil all }	「-d」ダンプ、「-l」ロード、または「-r」リカバリ操作のソースデータベースの名前を指定します。指定しない場合、操作はデータベースパスに存在するすべてのデータベースに対して実行されます。このオプションは、「-b」バックアップ操作には適用されません。 <ul style="list-style-type: none"> ローカルモードの有効なデータベース名は { ccm dhcp dns mcd all } です。 リージョンモードの有効なデータベース名は { ccm dns leasehist lease6hist replica subnetutil all } です。

オプション	説明
-s	実行している場合、Cisco Prime Network Registrar サーバーエージェントの停止を試みることを指定します。
-out path	出力ファイルのデスティネーションパスを指定します。指定しない場合は、ソース db パスを使用されます。このオプションは、「-b」バックアップおよび「-c」クリーンアップ操作には適用されません。



重要

ソースとターゲットのディレクトリが同じ場合、ダンプおよびロード操作は、ターゲットファイルが作成されると、ソース ファイルを削除します。これは、ダンプ/ロード操作が実行されて、大きなデータベースファイルの未使用領域を再キャプチャする際のディスク領域の要件を最小限に抑えるために行われます。



(注) ダンプ操作は、「.dbdump」を付加したデータベース ファイル名を使用して、各データベースを指定された場所のファイルにダンプします。ロード操作は、*.dbdump ファイルが見つかった場合にのみデータベース ファイルをロードします。データベース ファイルの名前は、「.dbdump」のない名前です。

フェールオーバー サーバーからの DHCP データの復元

フェールオーバー サーバーから、シャドウ バックアップの結果よりも新しい DHCP データを復元できます。フェールオーバー パートナーの設定が同期されていることを確認します。また、不正なフェールオーバーパートナー（つまり、データベースが不良なパートナー）で次の手順が実行され、復元する必要があることを確認します。

Windows の場合

1. デフォルトのパスを設定します。たとえば、次のとおりです。

```
SET PATH=%PATH%;.;C:\PROGRA~1\NETWOR~1\LOCAL\BIN
```

2. サーバー エージェントを停止します。

```
net stop "Network Registrar Local Server Agent"
```

3. eventstore、ndb、および logs ディレクトリを削除します。

```
del C:\NetworkRegistrar\Local\data\dhcpeventstore\*.*
del C:\NetworkRegistrar\Local\data\dhcp\ndb\dhcp.ndb
del C:\NetworkRegistrar\Local\data\dhcp\ndb\logs\*.*
```

```
del C:\NetworkRegistrar\Local\data\dhcp\ndb6\dhcp6.ndb
del C:\NetworkRegistrar\Local\data\dhcp\ndb6\logs\*.*
```



警告 いずれかの DHCP データベースを削除する場合は、両方を削除する必要があります。DHCPv4 (data/dhcp/ndb) または DHCPv6 (data/dhcp/ndb6) リースデータベース。1つだけ削除して、もう1つをそのままにしておくことはサポートされず、予期しない結果が生じる可能性があります。

4. サーバー エージェントを再起動します。

```
net start "Network Registrar Local Server Agent"
```

Linux の場合

1. サーバー エージェントを停止します。

- RHEL/CentOS 6.x :

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

- RHEL/セントロス 7.x:

```
systemctl stop nwreglocal
```

2. 実行中のプロセスを確認します。

```
/opt/nwreg2/local/usrbin/cnr_status
```

3. 残りのプロセスをキルします。

```
kill -9 pid
```

4. eventstore、ndb、および logs ディレクトリを削除します。

```
rm /var/nwreg2/data/dhcpeventstore/*.*
```

```
rm -r /var/nwreg2/data/dhcp/ndb/
```

```
rm -r /var/nwreg2/data/dhcp/ndb6/
```



警告 いずれかの DHCP データベースを削除する場合は、両方を削除する必要があります。DHCPv4 (data/dhcp/ndb) または DHCPv6 (data/dhcp/ndb6) リースデータベース。1つだけ削除して、もう1つをそのままにしておくことはサポートされず、予期しない結果が生じる可能性があります。

5. サーバー エージェントを再起動します。

- RHEL/CentOS 6.x :

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

- RHEL/セントロス 7.x:

```
systemctl start nwreglocal
```




第 10 章

レポートの管理

この章では、WebUIを使用してリージョンクラスタから入手可能な Cisco Prime Network Registrar アドレス空間レポートツールを管理する方法について説明します。この章を読み進める前に、ユーザーガイドのこの部分の前の章の概念をよく理解しておいてください。

- [ARIN レポートと割り当てレポート \(247 ページ\)](#)
- [ARIN レポートの管理 \(247 ページ\)](#)
- [IPv4 アドレス空間使用率レポートの管理 \(252 ページ\)](#)
- [共有 WHOIS プロジェクトの割り振りおよび割り当てレポートの管理 \(253 ページ\)](#)
- [BYOD レポートの管理 \(253 ページ\)](#)
- [登録済みデバイス \(254 ページ\)](#)
- [スコープ/プレフィックス \(254 ページ\)](#)

ARIN レポートと割り当てレポート

Cisco Prime Network Registrar Web UI を使用して、次のものを生成できます。

- 次のような、American Registry of Internet Numbers (ARIN) レポート。
 - 組織および担当者 (POC) レポート
 - IPv4 アドレス空間使用状況レポート
 - 共有 WHOIS プロジェクト (SWIP) の配分および割り当てレポート
- ネットワークのルータとルータインターフェイスの間でアドレスがどのように展開されているかを示す配分レポート。これには、次のものが含まれます。
 - 所有者別配分レポート
 - ルータ インターフェイス別またはネットワーク別配分レポート

ARIN レポートの管理

ARIN は、5つのリージョンインターネットレジストリ (RIR) の1つであり、カナダ、アメリカ合衆国、およびカリブ海および北大西洋諸島の IP リソースを管理します。

ARIN は、IP アドレスのブロックをインターネット サービス プロバイダ (ISP) に割り振り、ISP がアドレス空間のブロックを顧客に割り当てます。ARIN では、IP アドレス空間の割り振り (*allocate*) と IP アドレス空間の割り当て (*assign*) が区別されます。ARIN は、後で IR のメンバーと顧客に分配されるように、アドレス空間をより小さな IR に割り振ります。ARIN は、アドレス空間を ISP またはその他の組織に割り当て、その組織のネットワーク内だけで使用され、また、ARIN への要求とレポートに記載されている目的のためにのみ使用されます。



- (注) ARIN は、Internet Corporation for Assigned Names and Numbers (ICANN) の保護下で IP アドレス リソースを管理します。他のリージョンでは、ICANN は IP リソースに関する権限をさまざまなリージョン インターネット レジストリに委任しています。Cisco Prime Network Registrar は現在、これらのレジストリに必要なレポートをサポートしていません。IPv6 レポートまたは自律システム (AS) 番号もサポートしていません。

ARIN のポリシーと注意事項に関する詳細なドキュメントは、ARIN の Web サイトにあります。

<http://www.arin.net>

ARIN レポートに進む前に、これらのポリシーと注意事項に精通していることを確認してください。

ARIN レポートに指定できる 3 つのオプションは、次のとおりです。

- **New-** 新しく追加された POC または組織の場合。
- **Modify-** 電話番号と住所など、変更された POC または組織のデータを含みます。
- **Remove-** POC または組織を ARIN データベースから削除したい旨を通知します。

関連項目

[担当者および組織レポートの管理 \(248 ページ\)](#)

[IPv4 アドレス空間使用率レポートの管理 \(252 ページ\)](#)

[共有 WHOIS プロジェクトの割り振りおよび割り当てレポートの管理 \(253 ページ\)](#)

担当者および組織レポートの管理

Cisco Prime Network Registrar には、担当者 (POC) および組織情報を ARIN に送信できるレポートが用意されています。これらのレポートに入力した後、情報を電子メールで ARIN に送信する必要があります。他のレポートを準備する前に、POC レポート (テンプレートとも呼ばれます) を ARIN に送信します。

各 POC は、POC ハンドルと呼ばれる名前によって一意に識別され、1 つ以上の組織識別子 (組織 ID) またはリソース委任 (IP アドレス空間の割り振りや割り当てなど) に関連付けられます。ARIN によって割り当てられる POC ハンドルは、個人またはロールのいずれかを表すことができます。

組織レポートによって組織 ID が作成され、POC レコードがそれに関連付けられます。POC レポートを作成した後、組織レポートを作成します。

POC および組織レポートを管理するには、Cisco Prime Network Registrar リージョン Web UI に、`regional-addr-admin` ロールに割り当てられた管理者グループのメンバーとしてログインします。

関連項目

[担当者レポートの作成 \(249 ページ\)](#)

[担当者の登録 \(249 ページ\)](#)

[担当者レポートの編集 \(250 ページ\)](#)

[組織レポートの作成 \(250 ページ\)](#)

[組織の登録 \(251 ページ\)](#)

[組織レポートの編集 \(251 ページ\)](#)

担当者レポートの作成

マネージャが ARIN と対話して IP リソースを要求して管理できるように POC を作成します。これにより、ネットワークの専門家はネットワークの運用上の問題を管理できるようになります。

リージョン詳細 *Web UI*

ステップ 1 Administration メニューから **Settings** サブメニューの **Contacts** を選択して、[ARIN 連絡先の一覧表示/追加 (List/Add ARIN Points of Contact)] ページを開きます。

ステップ 2 左側の [連絡先 (Contacts)] ペインの [連絡先の追加 (Add Contact)] アイコンをクリックして、[連絡先の追加 (Add Point of Contact)] ページを開きます。

ステップ 3 ページのフィールドにデータを入力します。

- **Name**- POC の一意識別子 (必須)。
- **First Name** - 連絡先の名 (必須)。
- **Last Name** - 連絡先の姓 (必須)。
- **Type**- ドロップダウンリストから、[ユーザー (Person)] または [ロール (Role)] を選択します (オプションで、事前設定された値 Person)。

ステップ 4 Add Point of Contact をクリックします。

担当者の登録

POC のハンドルを受信するには、POC を ARIN に登録する必要があります。

リージョン詳細 Web UI

-
- ステップ 1 Administration** メニューから **Settings** サブメニューの **Contacts** を選択して、[ARIN 連絡先の一覧表示/追加 (List/Add ARIN Points of Contact)] ページを開きます。
- ステップ 2** 左側の [連絡先 (Contacts)] ペインで、必要な連絡先をクリックします。
- ステップ 3 Register Report** タブをクリックして、ARIN テンプレート ファイルを表示します。
- ステップ 4** テンプレート ファイルをコピーして、電子メールに貼り付け、ARIN にファイルを送信します。
-

担当者レポートの編集

ARIN が POC ハンドルを組織に返した後、または POC が変更された場合は、POC レポートを編集します。

リージョン詳細 Web UI

-
- ステップ 1 Administration** メニューから **Settings** サブメニューの **Contacts** を選択して、[ARIN 連絡先の一覧表示/追加 (List/Add ARIN Points of Contact)] ページを開きます。
- ステップ 2** 左側の [連絡先 (Contacts)] ペインで必要な連絡先をクリックすると、.[連絡先の編集 (Edit Point of contact)] ページが開きます。
- ステップ 3** ミドルネーム、ハンドル、および説明の値を入力します (任意)。
- ステップ 4** [電子メール (Email)] セクションで、次のようにします。
- Add** をクリックして、[電子メールアドレスの追加 (Add Email Address)] ウィンドウを開きます。
 - 電子メールアドレスを入力し、[追加 (Add)] をクリックします。
- ステップ 5** [電話 (Phone)] セクションで、次の手順を実行します。
- [追加 (Add)] をクリックして、[電話の追加 (Add Phone)] ウィンドウを開きます。
 - 電話番号と内線番号 (該当する場合) を入力してから、ドロップダウンリストからタイプ ([オフィス (Office)]、[携帯 (Mobile)]、[Fax]、または [ポケットベル (Pager)]) を選択します。
 - Add** をクリックします。
- ステップ 6** [その他の設定 (Miscellaneous Settings)] セクションで、追加の属性を文字列またはテキストのリストとして入力します。
- ステップ 7** 変更を行った後、**Save** をクリックします。
-

組織レポートの作成

各組織は、ARIN WHOIS データベースでは一意な組織 ID によって表され、これは組織名、住所、および POC で構成されます。組織は複数の組織 ID を持つことができますが、ARIN では単一の組織 ID で IP アドレス リソースを統合することを推奨しています。

ARIN に組織 ID がない場合、または追加の組織 ID を確立する場合は、まず、POC レポートを作成して送信する必要があります。ARIN が POC 情報を受信したことを確認したら、Cisco Prime Network Registrar を使用して、組織フォームを完成させ、その情報を送信します。

リージョン詳細 Web UI

- ステップ 1 Administration** メニューから、**Settings** サブメニューの **Organizations** を選択して、[ARIN 組織の一覧表示/追加 (List/Add ARIN Organizations)] ページを開きます。
- ステップ 2** 左側の [組織 (Organizations)] ペインの [組織の追加 (Add Organization)] アイコンをクリックして、[組織の追加 (Add Organization)] ページを開きます。
- ステップ 3** ページのフィールドにデータを入力します。
- **Organization Name** - ARIN に登録する組織の名前。
 - **Description**- 組織のテキスト説明。
 - **Organization Admin POC** - ドロップダウンリストから、IP リソースを管理する POC を選択します。
 - **Organization Technical Points Of Contact** - ドロップダウンリストから、ネットワーク操作を管理する 1 つ以上の POC を選択するか、**Add Point of Contact** をクリックして、新しい連絡先情報を追加します。
- ステップ 4 Add Organization** をクリックします。[組織の編集 (Edit Organization)] ページが開き、詳細を追加できます。
-

組織の登録

組織 ID を受信するには、組織を ARIN に登録する必要があります。

リージョン詳細 Web UI

- ステップ 1** [管理 (Administration)] メニューから、[設定 (Settings)] サブメニューの [組織 (Organizations)] を選択して、[ARIN 組織の一覧表示/追加 (List/Add ARIN Organizations)] ページを開きます。
- ステップ 2** 左側の [組織 (Organizations)] ペインで必要な組織をクリックします。
- ステップ 3** [登録レポート (Register Report)] タブをクリックして、ARIN テンプレート ファイルを表示します。
- ステップ 4** テンプレート ファイルをコピーして、電子メールに貼り付け、ARIN にファイルを送信します。
-

組織レポートの編集

ARIN に登録した組織情報を変更する必要がある場合があります。

リージョン詳細 Web UI

ステップ 1 Administration メニューから、**Settings** サブメニューの **Organizations** を選択して、[ARIN 組織の一覧表示/追加 (List/Add ARIN Organizations)] ページを開きます。

ステップ 2 左側の [組織 (Organizations)] ペインで必要な組織をクリックします。

ステップ 3 フィールドの値を入力または変更します。

- **Miscellaneous Settings** - これらの追加属性を文字列またはテキストのリストとして追加します。
- **Organization Abuse Points of Contact** - ドロップダウンリストから、ネットワークの不正利用に関する苦情を処理する 1 つ以上の POC を選択するか、**Add Point of Contact** をクリックして、新しい連絡先情報を追加します。
- **Organization NOC Points of Contact** - ドロップダウンリストから、ネットワーク オペレーションセンターの 1 つ以上の POC を選択するか、**Add Point of Contact** をクリックして、新しい連絡先情報を追加します。

ステップ 4 Save をクリックします。

ステップ 5 組織の登録 (251 ページ) の説明に従って、更新されたレポートを ARIN に送信します。

IPv4 アドレス空間使用率レポートの管理

アドレス空間使用率レポートには、次の 2 つの目的があります。

- POC ハンドルと組織 ID を受信した後、IPv4 アドレス空間の最初の要求を作成するため。
- ビジネス予測で IP アドレスの不足が示されたときに、IPv4 アドレスの追加割り振りの要求をサポートするため。



(注) ARIN Web サイトには、最初にアドレス空間を割り振る方法と、追加のアドレス空間を要求するためのしきい値基準に関する詳細情報が含まれています。一般に、シングルホーム構成の組織では、ARIN からの最小割り振りは /20 のアドレスブロックです。マルチホーム組織の場合、最小割り振りは /22 アドレスブロックです。ARIN では、必要なアドレスブロックが少ない組織は、アップストリームの ISP に連絡してアドレスを取得することを推奨しています。

Cisco Prime Network Registrar の使用率レポートは、ARIN ISP ネットワーク要求テンプレート (ARIN-NET-ISP-3.2.2) に対応しています。

リージョン詳細 Web UI

ステップ 1 Operate メニューから、**Reports** サブメニューの **ARIN Address Space Usage** を選択して、アドレス空間レポートの選択 ([Select Address Space Report)] ページを開きます。

- ステップ 2** [レポートタイプの選択 (Select the Report Type)] フィールドで、ドロップダウンリストから **Utilization** を選択します。[フィルタタイプの選択 (Select the Filter Type)] フィールドは、値 *by-owner* で更新されます。ブラウザに [アドレス空間レポートの選択 (Select Address Space Report)] ページが再表示され、[ネットワーク名 (Network Name)] と [ネットワークプレフィックス長 (Network Prefix Length)] の 2 つの新しいフィールドが表示されます。
- ステップ 3** [所有者の選択 (Select Owner)] フィールドで、ドロップダウンリストから、このアドレスブロックの所有者を選択します。
- ステップ 4** ネットワーク名とネットワークプレフィックス長の値を入力します。
- ステップ 5** **Generate Report** をクリックします。ブラウザに ARIN テンプレート ファイル (ARIN-NET-ISP-3.2.2) が表示されます。
- Cisco Prime Network Registrar アプリケーションの外部で情報が生成されて維持されるため、レポートのいくつかのセクションは、手動でデータを入力する必要があります。
- ステップ 6** **Save Report** をクリックします。ブラウザには、アドレス空間使用率レポートが、書式化されていないテキスト ファイルとして表示されます。
- ステップ 7** アドレス空間使用率レポートをテキスト エディタにコピーして、Cisco Prime Network Registrar が生成しないデータを手動で入力します。
- ステップ 8** 編集したレポートをコピーして電子メールに貼り付け、ARIN にファイルを送信します。

共有 WHOIS プロジェクトの割り振りおよび割り当てレポートの管理

ARIN 共有 WHOIS プロジェクト (SWIP) は、ARIN に登録されているリソースの連絡先および登録情報を検索するためのメカニズムを提供します。ARIN データベースには、IP アドレス、自律システム番号、これらのリソースに関連付けられている組織または顧客、および関連する POC が含まれています。

ARIN WHOIS は、ドメインまたは軍事関連の情報を特定しません。ドメイン情報を特定するには、`whois.internic.net` を使用し、軍事ネットワーク情報を特定するには、`whois.nic.mil` を使用します。

リージョン Web UI には、次の 2 つの割り振りおよび割り当てレポート ページもあります。

- ARIN SWIP 再割り振りレポートの表示
- ARIN SWIP 再割り当てレポートの表示

BYOD レポートの管理

BYOD レポートには、次の 2 つのタイプがあります。

- 登録済みデバイス

- スコープ/プレフィックス

登録済みデバイス

登録済みデバイス レポートには、BYOD Web サーバーによって登録されたデバイスのリストが表示されます。レポートは csv 形式でエクスポートできます。管理者ユーザーのみが、[登録済みデバイス レポート (Registered Device Report)] ページを使用してデバイスを削除できます。

登録済みデバイス レポート

登録済みデバイス レポートにアクセスするには、次のようにします。

リージョン詳細 Web UI

[操作 (Operate)] メニューから、[レポート (Reports)] サブメニューの [BYOD 登録済みデバイス (BYOD Registered Devices)] を選択して、[BYOD 登録済みデバイスの一覧表示 (List BYOD Registered Devices)] ページのレポートにアクセスします。

[クラスタ (clusters)] ペインには、BYOD Web サーバーまたはローカル DHCP サーバーまたはフェールオーバー ペアに設定された LDAP サーバーが、リージョン サーバーに関連付けられたものとして表示されます。LDAP サーバーのすべての登録済みデバイス、または BYOD Web サーバーを介してローカル DHCP サーバーまたはフェールオーバー ペアに登録されているデバイスが、[BYOD 登録済みデバイスの一覧表示 (List BYOD Registered Devices)] ページに表示されます。



- (注) [クラスタ (cluster)] ペインから目的のサーバーを選択して、対応する登録済みデバイス レポートを [BYOD 登録済みデバイスの一覧表示 (List BYOD Registered Devices)] ページに表示する必要があります。

スコープ/プレフィックス

スコープ/プレフィックス レポートには、BYOD に使用されるスコープとプレフィックスのリストが表示されます。レポートは csv 形式でエクスポートできます。

スコープ/プレフィックス レポート

スコープ/プレフィックス レポートを表示するには、次のようにします。

リージョン詳細 Web UI

[操作] メニューから、[レポート (Reports)] サブメニューの [BYOD スコープ/プレフィックス (BYOD Scope/prefix)] を選択して、[BYOD スコープ/プレフィックス (BYOD Scope/prefix)] ページでレポートを表示します。

リージョン サーバーに関連付けられているローカル DHCP サーバーまたはフェールオーバー ペアは、[クラスタ (clusters)] ペインに表示されます。BYOD Web サーバーのローカル DHCP サーバーまたはフェールオーバー ペアで作成されたすべてのスコープとプレフィックスは、[BYOD スコープ/プレフィックスの一覧表示 (List BYOD Scope/Prefix)] ページに表示されます。



-
- (注) [クラスタ (cluster)] ペインから目的のサーバーを選択して、BYOD のセットアップ中に作成された対応するスコープとプレフィックスを、[BYOD スコープ/プレフィックスの一覧表示 (List BYOD Scope/Prefix)] ページに表示する必要があります。
-



第 III 部

仮想プライアンス

- [Cisco Prime Network Registrar 仮想プライアンスの概要 \(259 ページ\)](#)



第 11 章

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

Cisco Prime Network Registrar 仮想アプライアンスは、ローカルシステムでの Cisco Prime Network Registrar の実行に関連するインストール、設定、およびメンテナンスのコストを削減することを目的としています。また、相互運用性が保証されるため、あるマシンから別のマシンに Cisco Prime Network Registrar を移動する際のリスクが軽減されます。

Cisco Prime Network Registrar のライセンスを取得し、Cisco.com から仮想アプライアンスをダウンロードする必要があります。すべての Cisco Prime Network Registrar ローカルクラスタは、ローカルクラスタによって提供される DHCP または DNS サービスのライセンスを含んでいるリージョンクラスタに接続されている必要があります。すべてのライセンスがリージョンクラスタにロードされ、最初のインストール時にローカルクラスタがリージョンクラスタに登録されます。その後、Cisco Prime Network Registrar は起動して、設定に使用できるようになります。

これは、Cisco Prime Network Registrar のコピーをダウンロードして、お客様が用意したサーバーまたは仮想マシンにインストールするだけでなく、Cisco Prime Network Registrar が実行されるオペレーティングシステムも仮想アプライアンスで提供されます。

Cisco Prime Network Registrar 仮想アプライアンスは、VMware ESXi 6.x プラットフォーム、KVM ハイパーバイザ、および OpenStack でサポートされます。

vApp と仮想アプライアンスの違いについては、vApp および仮想アプライアンスの導入ユーザーガイドを参照してください。

- [Cisco Prime Network Registrar 仮想アプライアンスの動作 \(260 ページ\)](#)
- [仮想アプライアンスでの Cisco Prime Network Registrar の起動 \(260 ページ\)](#)
- [VMware でのディスク領域の可用性のモニターリング \(260 ページ\)](#)
- [VMware でのディスクのサイズの増加 \(261 ページ\)](#)
- [KVM ハイパーバイザ上のディスクサイズの増加 \(261 ページ\)](#)
- [トラブルシューティング \(263 ページ\)](#)

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

仮想アプライアンスは、実行可能なゲスト OS (CentOS 7.7) とその OS にインストールされている Cisco Prime Network Registrar を含む仮想マシンで構成されます。仮想アプライアンスがインストールされている場合、Cisco Prime Network Registrar はすでにインストールされており、仮想マシンの電源投入によって開始されます。

仮想アプライアンスでの Cisco Prime Network Registrar の起動

Cisco Prime Network Registrar アプリケーションを直接起動するには、URL `http://hostname:8080` を使用します。URL `https://hostname:8443` を介したセキュアな `https` 接続も可能です。

VMware でのディスク領域の可用性のモニターリング

仮想アプライアンスのディスク サイズを増やすために使用できるスペースの量を確認するには、次の手順を実行します。

ステップ 1 [vSphere クライアント (vSphere Client)] ウィンドウで、仮想 Cisco Prime Network Registrar アプライアンスが存在するホスト/サーバーを選択します。

ステップ 2 **Storage Views** をクリックすると、サーバーによってホストされているマシンのリストと、各マシンによって現在使用されているスペースの詳細が表示されます。

また、[仮想マシン (Virtual Machines)] タブに移動して、マシン別に **Provisioned Space** と **Used Space** の両方を表示することもできます。

ステップ 3 **Summary** をクリックします。

[概要 (Summary)] タブの **Resources** エリアには、ディスクの容量と使用されている CPU およびメモリが表示されます。

ステップ 4 仮想マシンを選択して、**Summary** タブをクリックします。

[概要 (Summary)] タブの **Resources** エリアに、マシンのディスク領域の詳細が表示されます。

仮想アプライアンスで使用されているディスク領域の使用状況のモニターリング

仮想アプライアンスのディスクのサイズを増やす必要があるかどうかを判断するための参考として、仮想アプライアンスで使用されているディスクの空き容量を確認するには、次の手順を実行します。

ステップ 1 [vSphere クライアント (vSphere Client)] ウィンドウで仮想マシンを選択し、右側のペインの **Console** タブをクリックするか、仮想マシン名を右クリックして、**Open Console** を選択します。

ステップ 2 root としてログインし、**df -k** と入力します。ディスク領域の詳細が表示されます。

ディスクのディスク領域が不足している場合は、ディスクのサイズを増やす必要があります ([VMware でのディスクのサイズの増加 \(261 ページ\)](#) を参照)。

VMware でのディスクのサイズの増加

より大きなディスクが必要な場合は、次の手順を実行します。

ステップ 1 VM を停止します。

ステップ 2 [仮想マシンのプロパティ (Virtual Machine Properties)] ウィンドウでサイズを変更することによって、ディスクのサイズを大きくします。[仮想マシンのプロパティ (Virtual Machine Properties)] ウィンドウを開くには、VM 名を使用して VM を選択し、右クリックして、[設定の編集 (Edit Settings)] を選択する必要があります。

ステップ 3 VM を再起動します。

ブートプロセス時に、ファイルシステムを含んでいるパーティションが、ディスク全体を包含するように拡張され、ファイルシステムがパーティション全体に拡張されます。

KVM ハイパーバイザ上のディスク サイズの増加

初期ディスク サイズは 14 GB であり、6 GB がスワップ パーティションに割り当てられ、約 5.4 GB は Cisco Prime Network Registrar が実行するパーティションである /dev/sda3 に残されません。これは、どのようなインストール環境にとっても、確かに小さすぎます。したがって、ディスクのサイズを増やす必要がある場合があります。このプロセスには2つの手順があります。

- ファイルを保持するディスクを大きくする
- ディスクを再パーティション化して、パーティション内の使用可能なすべての領域を使用するようにファイル システムに指示します。

ディスク サイズの増加は、VM が動作していないときに行う必要があります。VM をインストールする前、VM が実行していないことが確実なとき、または VM を起動した後、すでに実行しているときに行うことができます。VM が実行している場合は、ディスクのサイズを増やす前に VM をシャットダウンする必要があります。VM が実行していない場合は、**truncate** および **virt-install** コマンドを使用して、より大きなディスクを作成し、ここにデータをコピーし


ます。さらに、パーティションテーブルを変更し、ファイルシステムのサイズを変更して、追加のスペースを使用することができます。

次に、これらのコマンドを使用して、ディスクのサイズをデフォルトサイズの 14 GB から 16 GB に増やす例を示します。実際には、16 GB よりも大きなサイズを使用します。ディスクの新しいサイズは、**truncate** コマンドで指定します。

例

```
root:tsegi$ truncate -s 16G @BUILDNAME-disk1.big.raw

root:tsegi$ virt-resize --expand /dev/sda3 @BUILDNAME-disk1.raw @BUILDNAME-disk1.big.raw

Examining @BUILDNAME-disk1.raw ...
 100%
[[]] --:--

*****

Summary of changes:


/dev/sda1: This partition will be left alone.


/dev/sda2: This partition will be left alone.


/dev/sda3: This partition will be resized from 7.5G to 9.5G.

*****

Setting up initial partition table on @BUILDNAME-disk1.big.raw ...

Copying /dev/sda1 ...
 100%
[[]] 00:00

Copying /dev/sda2 ...
 100%
[[]] 00:00

Copying /dev/sda3 ...
 100%
[[]] 00:00

Resize operation completed with no errors. Before deleting the old disk, carefully check
that the resized disk boots and works correctly.
```

上記の例の操作には、比較的強力なマシンで約5~6分かかりました。実際のマシンでの所要時間は、さまざまな要因によって異なります。

truncate コマンドは、指定されたサイズの新しいディスクファイルを作成し、**virt-install** コマンドは、入力ディスクのパーティションを出力ディスクに再作成し、元のディスクファイルのデータを新しいディスクファイルにコピーし、指定されたパーティション内のファイルシステムを拡張して、パーティション内のすべてを包含します。この操作が完了したら、仮想マシンマネージャを使用して、VM のディスクを新しいディスクに置き換えます。



- (注) 新しいディスクを使用すると、元のディスクのデータは古くなるため、使用すべきではありませんが、やはり作業ディスクであり、バックアップとして保存することもできます。元のディスクを再び使用する場合、新しい、より大きなディスクの稼働中に実行された処理のすべてのメモリが失われ、新しいディスクの使用中に DHCP に付与された IP アドレスと、古いディスクを使用するときの DHCP サーバーの将来のアクティビティの間に重大な競合が発生します。

VM をインストールする前にディスクのサイズを増やす場合は、新しいディスク ファイルの名前を元のディスク ファイルと同じ @BUILDNAME-disk1.raw に変更する必要があります。これは、installonkvm スクリプトがディスク ファイルの名前として予期している名前です。

トラブルシューティング

Cisco Prime Network Registrar 仮想アプライアンスの使用中に問題が発生した場合は、次の手順を実行することをお勧めします。

/var/nwreg2/{local|regional}/logs のログ ファイルを確認します。特に、ログ ファイルに、これらの信号例外的条件としてのエラーがないか探します。問題を解決できず、シスコサポートを購入した場合は、問題について Cisco Technical Assistance Center (TAC) に事例を送信してください。

用語集

A	
A レコード	DNS アドレス リソース レコード (RR)。ホスト名をアドレスにマッピングし、ホストのインターネットプロトコルアドレス (ドット付き 10 進形式) を指定します。ホストアドレスごとに1つのレコードが存在する必要があります。
アクセス コントロール リスト (ACL)	DHCP メカニズム。これにより、サーバーは、パケットで定義された要求またはアクションを許可または禁止できます。 トランザクションシグニチャ (TSIG) も参照してください。
アドレス ブロック	オンデマンド アドレス プールを使用する DHCP サブネット割り当てで使用する IP アドレスのブロック。
admin	スーパーユーザーまたはグローバル管理者のデフォルト名。
管理者	特定の機能を採用するユーザー アカウント。ロール、制約付きロール、またはグループによって定義されます。
エイリアス	1つのドメイン名から正式な (正規の) ドメイン名へのポインタ。
割り当てプライオリティ	デフォルトのラウンドロビン方式以外の、スコープ間でのアドレスの割り振りを制御する代替方法。
ARIN	American Registry of Internet Numbers 。いくつかのリージョンインターネットレジストリ (IR) の 1 つ。北米、カリブ海諸国、赤道直下アフリカの IP リソースを管理します。 Cisco Prime Network Registrar は、このレジストリのアドレス空間レポートを提供します。
非同期転送モード (ATM)	複数のサービス タイプ (音声、ビデオ、またはデータ) が固定長 (53 バイト) セルで伝送されるセルリレーに関する国際標準。
権威ネーム サーバー	ゾーンに関する完全な情報を所有する DNS ネーム サーバー。
AXFR	完全な DNS ゾーン転送。 ゾーン転送 と IXFR も参照。

B	
Berkeley Internet Name Domain (BIND)	ドメインネームシステム (DNS) プロトコルの実装。DNS も参照。
バインド	メインおよびバックアップ DHCP サーバーによって管理される、DHCP クライアントオプションとリース情報の集合。バインドデータベースは、すべての DHCP クライアントに関連付けられている設定パラメータの集合です。このデータベースには、すべてのデータセットに関する設定情報が格納されています。
BOOTP	ブートストラッププロトコル。ネットワークノードがネットワークブートに影響を与えることができるように、イーサネットインターフェイスの IP アドレスを決定するために使用されます。
C	
ケーブル モデム終端システム (CMTS)	ケーブル モデム終端システム。通常、ケーブルヘッドエンドのルータまたはブリッジ。
キャッシュ	物理メモリの量を削減するためにインデックス化されたディスクファイルに保存されるデータ。
キャッシング ネーム サーバー	トランザクションごとに他のサーバーに照会しなくても、要求にすばやく応答できるように、他のネームサーバーから学習した情報をキャッシュする DNS サーバーのタイプ。
正規名	CNAME リソースレコード (RR) に固有のエイリアス DNS ホストの別の名前。
大文字と小文字の区別	Cisco Prime Network Registrarの値は、パスワードを除き、大文字と小文字が区別されません。
中央構成管理 (CCM) データベース	Cisco Prime Network Registrar Web ベースのユーザーインターフェイス (Web UI) のメインデータベース。
chaddr	DHCP クライアントハードウェア (MAC) アドレス。クライアントとサーバー間で RFC 2131 パケットで送信されます。

変更ログ、チェンジセット	変更ログは、Web UI での追加、変更、または削除により、Cisco Prime Network Registrar データベースに対して行われたチェンジセットのグループです。チェンジセットは、データベース内の 1 つのオブジェクトに対して行われた一連の変更です。
ciaddr	DHCP クライアントの IP アドレス。クライアントとサーバー間で RFC 2131 パケットで送信されます。
アドレスのクラス	ネットワーク プレフィックスとホスト サフィックスの間の境界の位置を決定する IP アドレスのカテゴリ。インターネット アドレスには、A、B、C、D、または E レベルのアドレスがあります。クラス D アドレスはマルチキャストに使用され、ホストでは使用されません。クラス E アドレスは、実験専用です。
クライアントクラス	Cisco Prime Network Registrar の機能。共通のネットワークに接続するユーザーに差別化されたサービスを提供します。これにより、管理基準に基づいてユーザー コミュニティをグループ化し、各ユーザーが適切なクラスのサービスを受けられるようにできます。
クラスタ	Cisco Prime Network Registrar において、同じデータベースを共有する DNS、DHCP、および TFTP サーバーのグループ。
CNAME レコード	DNS 正規名リソース レコード (RR)。ニックネームまたはエイリアスに使用されます。リソース レコードに関連付けられている名前は、ニックネームです。データ部分は正式名称または正規名です。
CNRDB	Cisco Prime Network Registrar の内部データベースの 1 つの名前。もう 1 つは、チェンジセット データベースです。
制約	管理者のロールまたは許可された機能に割り当てられた制限。
D	

Data Over Cable Service Interface Specification (DOCSIS)	データ オーバー ケーブル サービス インターフェイス仕様。オープンなケーブル システム 標準規格をめざして、1995 年にケーブル会社 によって作成され、インターフェイスと呼ば れる接続ポイントの仕様をもたらした標準規 格。
委任	DNS サブゾーンの管理責任を別のサーバーに 割り当てる行為、または DHCP アドレス ブ ロックをローカルクラスに割り当てる行為。
DHCP	Dynamic Host Configuration Protocol (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)。インターネット技術特別調査委員会 によって指定 (IETF) TCP/IP の使用時に必要 な設定の数を削減します。DHCP はホストに IP アドレスを割り当てます。また、接続して いるインターネット ネットワークの情報をホ ストが操作および交換するために必要なすべ てのパラメータを提供します。
DHCP 使用率	サブネットまたはプレフィックスに割り当て られたアドレスの数と、どのくらいの空きア ドレス空間があるかを判断するために生成で きるレポート。
デジタル加入者線 (DSL)	従来の銅線ケーブル配線を介して限られた距 離で高い帯域幅を提供するパブリック ネット ワーク テクノロジー。
DNS	ドメイン ネーム システム。インターネット ユーザー数の増加を処理します。DNS は www.cisco.com などの名前を 192.168.40.0 など のインターネット プロトコル (IP) アドレス に変換して、コンピュータが互いに通信でき るようにします。
DNS アップデート	プロトコル (RFC2136) を使用して、DNS を DHCP と統合します。
ドメイン	DNC 命名階層ツリーの一部。組織の種類や地 理情報に基づいてネットワークの全般的な分 類を指します。階層は、ルート、トップまた はファーストレベル、セカンドレベルドメイ ンです。

ドメイン名	絶対または相対のいずれかの DNS 名。絶対名は完全修飾ドメイン名 (FQDN) であり、ピリオドで終わります。相対名は、現在のドメインに対して相対的であり、ピリオドで終わりません。
ドット付き 10 進表記	32 ビットの整数の構文表現。ベース 10 で記述され、ドットで区切られた 48 ビットの数値で構成される IP アドレスの表現です。多くの TCP/IP アプリケーションプログラムは、宛先マシン名の代わりにドット付き 10 進表記を受け入れます。
E	
式	クライアント ID を作成したり、クライアントを検索したりするために、Cisco Prime Network Registrar DHCP 実装で一般的に使用される構造体。たとえば、式を使用して、テンプレートからスコープを構築することができます。
拡張および拡張ポイント	Cisco Prime Network Registrar では、TCP、C、または C++ で記述されたスクリプトの要素。サーバーが処理する DHCP パケットの処理をカスタマイズし、さらに DHCP クライアントをカスタマイズするための追加のレベルをサポートします。
F	
フェールオーバー	Cisco Prime Network Registrar の機能。(RFC 2131 で述べられているように) 複数の冗長 DHCP サーバーを提供して、障害発生時に 1 台のサーバーが引き継ぐことができます。DHCP クライアントは、どのサーバーが要求に応答しているかを認識することなく、リースを継続的に維持し、更新することができます。
フォワーダ	すべてのオフサイトクエリを処理するように指定された DNS サーバー。フォワーダを使用すると、他の DNS サーバーは、オフサイトにパケットを送信する必要がなくなります。
転送、DHCP	DHCP パケットをクライアント単位で別の DHCP サーバーに転送するメカニズム。これは、拡張スクリプトを使用することによって、Cisco Prime Network Registrar で達成できます。

FQDN	完全修飾ドメイン名。DNS 階層内のホストの位置を明確に指定する絶対ドメイン名。
G	
giaddr	DHCP ゲートウェイ (リレー エージェント) IP アドレス。クライアントとサーバー間で RFC 2131 パケットで送信されます。
グルー レコード	サブドメインの権威ネーム サーバーのアドレスを指定する DNS アドレス リソース レコード。ドメイン自体ではなく、ドメインを委任しているサーバー内のグルー レコードのみが必要です。
グループ	ロールと制限付きロールを割り当てることができるように管理者を結合する連想エンティティ。
H	
高可用性 (HA) DNS	2 つ目のプライマリ サーバーがメインプライマリサーバーをシャドウイングするホットスタンバイにできる DNS 構成。
HINFO レコード	DNS ホスト情報リソース レコード (RR)。ホストマシンのハードウェアおよびソフトウェアに関する情報を提供します。
ヒント サーバー	ルート ヒント サーバー を参照。
ホスト	TCP/IP ネットワーク アドレスを持つ任意のネットワーク デバイス。
I	
IEEE	電気電子学会。通信やネットワークなどの標準化を行う米国の専門機関。
in-addr.arpa	ホストアドレスと名前のインデックスを作成できる DNS アドレス マッピング ドメイン。これにより、インターネットは IP アドレスをホスト名に変換し直すことができます。 逆引きゾーン も参照。
IP アドレス	インターネットプロトコルアドレス。たとえば、192.168.40.123 です。

IP 履歴	Cisco Prime Network Registrar ツール。IP アドレスのリース履歴をデータベースに記録します。
IPv6	128 ビットのアドレスを含む新しい IP 標準。Cisco Prime Network Registrar は DHCPv6 実装を提供します。
ISP	Internet Service Provider (インターネット サービス プロバイダ)。お客様に専用回線、ダイヤルアップ、および DSL (イーサネットおよび DHCP 経由のポイントツーポイント) アクセスを提供する会社。
反復クエリ	ネームサーバーが最も近い応答をクエリサーバーに返す DNS クエリのタイプ。
IXFR	増分ゾーン転送。変更されたデータのみをプライマリサーバーから転送することによって、Cisco Prime Network Registrar がセカンダリサーバーの更新を許可する標準規格。
L	
不完全委任	ゾーンにリストされている DNS サーバーがゾーンの権威として設定されていない場合の条件。
LDAP	Lightweight Directory Access Protocol。Cisco Prime Network Registrar クライアントおよびリース情報を統合するためのディレクトリサービスを提供する方法。
リース	DHCP クライアントへの IP アドレスの割り当て。これにより、クライアントがアドレスを使用できる期間も指定されます。リースが期限切れになると、クライアントは DHCP サーバーと新しいリースをネゴシエートする必要があります。
リース猶予期間	リースが期限切れになった後、DHCP サーバーデータベースに保持される時間の長さ。これにより、クライアントとサーバーが異なるタイムゾーンにあり、クロックが同期されていない場合、またはリースが期限切れになったときにクライアントがネットワーク上にない場合に、クライアントリースが保護されます。

リンクのグループ化	CMTS プレフィックスの安定性に対応するようにリンクをグループ化します。 <i>group-name</i> 属性は、リンクが属するグループの名前を指定するために使用されます。
リース履歴	クライアントがリースを発行された日時、クライアントまたはサーバーが期限切れになる前にリースを解放した時間、サーバーがリースを更新した時間、サーバーがリースを更新した日時と時間の長さについての履歴ビューを提供するために生成できるレポート。
リース クエリ	リレーエージェントがクライアント/サーバートランザクションからの収集に加えて、DHCP サーバーに直接、リース（および予約）データを要求できるプロセス。
リンク タイプ	トポロジ、ロケーション独立、およびユニバーサルな 3 種類のリンクがあります。トポロジリンクとは、接続されているネットワークセグメントに基づいてクライアントにリースが割り当てられることを意味します。ロケーション独立リンクタイプを使用すると、中央オフィス内の 1 つの CMTS から別の CMTS に移動されたサブスクリイバは、委任されたプレフィックスを保持することができますが、ユニバーサルリンクタイプでは、サブスクリイバが中央オフィスから別の中央オフィスに移動されても、委任されたプレフィックスを保持できます。
ローカル クラスタ	ローカルの Cisco PrimeNetwork Registrar サーバーの場所。 リージョン クラスタ も参照。
localhost	現在のマシンの名前を参照する識別名。 Localhostは、ホスト名を必要とするアプリケーションに役立ちます。
ループバック ゾーン	サーバーがトラフィックを自身に転送できる DNS ゾーン。ホスト番号はほぼ常に 127.0.0.1 です。
M	

MAC アドレス	標準化されたデータリンク層アドレス。LANに接続するすべてのポートまたはデバイスに必要です。ネットワーク内の他のデバイスは、これらのアドレスを使用してネットワーク内の特定のポートを探し、ルーティングテーブルやデータ構造の作成と更新を行います。MACアドレスは6バイト長であり、IEEEによって管理されます。ハードウェアアドレス、MAC層アドレス、物理アドレスとも呼ばれます。一般的なMACアドレスは、1,6,00:d0:ba:d3:bd:3bです。
メール エクスチェンジャ	電子メールを受け入れるホスト。その一部はメールフォワーダとして機能します。MXレコードも参照。
マスター ネーム サーバー	ゾーン転送を介してセカンダリサーバーにゾーンデータを転送する権威DNSネームサーバー。
最大クライアント リードタイム (MCLT)	DHCPフェールオーバーにおいて、クライアントリースの有効期限が切れてからバックアップサーバーのリースの有効期限が切れるまでの時間を制御するリース保険のタイプ。
マルチネットティング	1つのサブネットまたは複数のLANセグメントに複数のDHCPスコープがある状態。
マルチプル サービス オペレータ (MSO)	ケーブルまたはワイヤレステクノロジーを使用して加入者にインターネットアクセスを提供します。
マルチスレッディング	複数のサーバータスクを実行するプロセス。
MX レコード	DNSメールエクスチェンジャリソースレコード (RR)。ドメイン名のメールを配信する場所を指定します。1つのドメイン名に対して複数のMXレコードを設定し、優先順位を指定することができます。
N	
ネームサーバー	ドメインのデータとRRを保存するDNSホスト。

NAPTR	DNS 命名機関ポインタ リソース レコード (RR) . 特定の名前空間の名前解決に役立つとともに、解決サービスに到達するために処理されます。提案された標準RFC 2915に基づいています。
ネガティブ キャッシュ時間	「そのような名前はない」や「そのようなデータはない」などのネガティブ情報に対する繰り返し要求に迅速に応答するために、DNS サーバーが保持するメモリキャッシュ。Cisco Prime Network Registrar は、この情報を一定間隔で破棄します。
ネットワーク ID	32 ビット IP アドレスの一部。特定のシステムがあるネットワークを識別します。これは、サブネット マスクと IP アドレスの AND 演算によって決定されます。
NOTIFY	DNS マスターサーバーがゾーンに対して行われた変更をスレーブに通知し、ゾーン転送を開始する標準規格 (RFC 1996)。
nrcmd	Cisco Prime Network Registrar コマンドライン インターフェイス (CLI)。
O	
オンデマンド アドレス プール	クライアント (通常はVPN ルータまたはその他のプロビジョニング デバイス) に発行されたホールセール IP アドレスプール。このプールからリース割り当て用に引き出すことができます。DHCP サブネット割り当てとも呼ばれます。
オプション、DHCP	DHCP メッセージの options フィールドに保存された DHCP 設定パラメータとその他の制御情報。DHCP クライアントは、どのオプションが要求され、DHCP パケットで送信されたかを決定します。Cisco Prime Network Registrar では、オプション定義とそれらが属するオプションセットを作成することができます。
組織レポート	ARIN に送信されるレポートの 1 つであり、POC は他のレポートになります。 ARIN と POC レポート も参照。

組織固有識別子 (OUI)	VPN の所有者または ISP を識別するために IEEE によって割り当てられます。IEEE とバーチャルプライベートネットワーク (VPN) も参照。
所有者	所有者は、アドレスブロック、サブネット、およびゾーンの区別要因として作成できます。コンテキストまたは DNS RR では、所有者は RR の名前です。
P	
ping	Packet Internet Groper。デバイスのアクセシビリティをトラブルシューティングするための一般的な方法。一連の Internet Control Message Protocol (ICMP) Echo メッセージを使用して、リモートホストがアクティブか非アクティブか、およびホストとの通信のラウンドトリップ遅延を判断します。
POC レポート	担当者レポート。ARIN に送信されるレポートの 1 つ。組織はその他のレポートです。ARIN と組織レポートも参照。
ポリシー	単一のスコープまたはスコープのグループに適用される DHCP 属性またはオプションのグループ。埋め込みポリシーは、スコープおよびその他の DHCP オブジェクトに対して作成できます。
ポーリング	特定の一定期間における DHCP 使用率またはリース履歴データの収集。
プレフィックス割り当てグループ	プレフィックス割り当ての優先順位付けを容易にするために、プレフィックスをグループ化します。
プレフィックスの安定性	クライアントは、自身の場所を変更するとき、つまり、ある CMTS から別の CMTS に移動するとき (CMTS プレフィックスの安定性)、またはアドレス空間内で移動するとき (ユニバーサルプレフィックスの安定性)、委任されたプレフィックスを保持できます。
プライマリ マスター	セカンダリ サーバーがゾーン転送要求を介してデータを受信する DNS サーバー。

暫定アドレス	短時間、つまりワンショットベースで DHCP サーバーによって未知のクライアントに割り当てられるアドレス。
PTR レコード	DNS ポインタ リソース レコード。ドメイン ツリー内の他の場所を指す特別な名前を有効にするために使用されます。エイリアスではなく、正式な（正規の）名前を参照する必要があります。In-addr.arpa も参照。
オブジェクトのプルとプッシュ	Cisco Prime Network Registrar リージョン クラスタは、ローカルクラスタデータのレプリカ データベースからネットワーク オブジェクトをプルし、ローカルクラスタにオブジェクトを直接プッシュする機能を提供します。
R	
再帰クエリ	ネーム サーバーが自身のキャッシュに含まれていない非権威データを他の DNS サーバーに要求する DNS クエリ。再帰クエリは、応答またはエラーを受信するまで、すべてのネーム サーバーにクエリを続けます。
更新間隔	セカンダリ DNS サーバーが AXFR パケットをプライマリ サーバーに送信することによってデータの精度をチェックする時間間隔。
リージョン	リージョンは、アドレス ブロック、サブネット、およびゾーンの区別要因として作成できます。リージョンは、リージョン クラスタとは異なります。
リージョン クラスタ	リージョンの Cisco Prime Network Registrar CCM サーバーの場所。ローカルクラスタも参照。
リレー エージェント	2つ以上のネットワーク、またはネットワーク システムを接続するデバイス。DHCP では、DHCP サーバーの IP ヘルパーであるバーチャルプライベート ネットワーク上のルータ。
レプリカ データベース	リージョン クラスタでローカルクラスタ構成のコピーをキャプチャする CCM データベース。これらの構成は、リージョン クラスタにプルして、他のローカル クラスタにプッシュできます。
Request For Comments (RFC)	TCP/IP の標準セット。

予約	特定の DHCP クライアント用に予約されている IP アドレスまたはリース。
解決例外	インターネットのルート名と外部サーバーを再帰的にクエリするのではなく、指定されたドメインの DNS クエリを内部サーバーに選択的に転送すること。
リゾルバ	DNS クライアント/サーバー メカニズムのクライアント部分。リゾルバは、ネットワークを介してネーム サーバーに送信されるクエリを作成し、応答を解釈して、要求プログラムに情報を返します。
リソース レコード (RR)	DNS 構成レコード (SOA、NS、A、CNAME、HINFO、WKS、MX、および DNS ゾーン内のデータを構成する PTR など)。ほとんどの場合、RR と略記されます。 『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「リソース レコード」の項を参照。
逆引きゾーン	名前をアドレスとして使用して、アドレス クエリをサポートする DNS ゾーン。 In-addr.arpa も参照。
ロール、制約付きロール	アプリケーションで使用できる機能を決定するために、1つ以上のロールを管理者に割り当てることができます。制約付きロールは、さらに制限によって制約されるロールです。 DNS、ホスト、アドレス ブロック、DHCP、および CCM データベースの管理のための一般的なロールがあります。特定のホストとゾーンのロールをさらに制約することができます。一部のロールには、データベース サブロールなど、区別用のサブロールがあります。
ルート ヒント サーバー	すべてのルート名クエリの階層の最上位にある DNS ネーム サーバー。ルート ネーム サーバーは、すべてのトップレベル ドメインの権威ネーム サーバーのアドレスを認識しています。非権威データまたはキャッシュされていないデータの解決は、ルート サーバーから開始する必要があります。ヒント サーバーと呼ばれることもあります。

ラウンドロビン	クエリのたびに、DNS サーバーが複数の同じタイプのレコードの順序を再配置するアクション。
ルーテッドブリッジカプセル化 (RBE)	スタブブリッジセグメントがポイントツーポイントルーテッドインターフェイスで終端されるプロセス。具体的には、ルータは、PPP、RFC 1483 ATM、RFC 1490 フレームリレーなどのポイントツーポイントプロトコルを介して伝送される IEEE 802.3 またはイーサネットヘッダーでルーティングしています。
S	
スカベンジング	DNS サーバーへのダイナミックアップデートを定期的にスキャンして古いリソースレコードを検索し、これらのレコードをパージするアクション。
スコープ	DHCP サーバー上の TCP/IP アドレスの管理グループ。リースの割り当てに必要です。
セカンダリマスター	ゾーンに対して権威のある別のネームサーバーからゾーンデータを取得する DNS ネームサーバー。セカンダリマスターサーバーが起動すると、プライマリマスターに接続して、そこから更新を受信します。
セカンダリサブネット	1 つの LAN が同じ LAN に適用される複数のサブネット番号を持つ場合があります。またはルータ内のネットワークセグメント。一般に、1 つのサブネットがプライマリに指定され、その他はセカンダリに指定されます。サイトは、1 つのインターフェイスに関連付けられた複数のサブネット番号のアドレスをサポートしている場合があります。セカンダリサブネットに関する必要な情報で DHCP サーバーを設定する必要があります。
選択タグ	クライアントとクライアントクラスの DHCPv4 スコープと DHCPv6 プレフィックスを選択するためのメカニズム。
siaddr	DHCP ブートプロセスの次のステップで使用するサーバーの IP アドレス。クライアントとサーバー間で RFC 2131 パケットで送信されず。

スレーブ フォワーダ	スタブリゾルバのように動作し、ほとんどのクエリを解決のために他のネーム サーバーに渡す DNS サーバー。 スタブリゾルバ も参照。
スレーブ サーバー	キャッシュから応答できないクエリを、応答用のルート名サーバーに照会する代わりに、転送サーバーの固定リストに常に転送する DNS サーバー。
SNMP 通知	サーバーのエラー状態と問題を警告する Simple Network Management Protocol メッセージ。 トラップ も参照。
SOA レコード	DNS 機関開始リソースレコード (RR) 。ゾーンの開始を指定します。
SRV レコード	DNS リソースレコード (RR) のタイプ。管理者は単一のホストドメインについて複数のサーバーを使用して、少々の困難はあるものの、ホスト間でサービスを移動でき、一部のホストをサービスのプライマリサーバーとして指定し、他のホストをバックアップとして指定することができます。
ステージング編集モード	データはCCMサーバーに保存されるが、プロトコルサーバーでライブではない dhcp または dns 編集モード。 同期編集モード も参照。
スタブリゾルバ	完全な解決を自分で実行する代わりに、別のサーバーにクエリを手渡す DNS サーバー。
サブネット割り当て、DHCP	サブネット全体について、プロビジョニングデバイスへの IP アドレスの割り当てを目的とした、Cisco Prime Network Registrar によるオンデマンドアドレスプールの使用。
サブネットマスク	ホストアドレスサブネットを決定する個別の IP アドレス、またはホスト IP アドレスの一部。たとえば、192.168.40.0 255.255.255.0 (または 192.168.40.0/24) は、IP アドレスの最初の 24 ビットがサブネット 192.168.40 であることを示します。このように、アドレスをネットワーククラスラインに沿って厳密に分割する必要はありません。
サブネットプール	セカンダリサブネットを含め、ネットワーク番号とサブネットマスクに関連付けられている IP アドレスのセット。

サブネットティング	ネットワーク クラスを複数のサブネットワークに分割するアクション。
サブスクリバの制限	DHCP オプション 82 定義によって Cisco Prime Network Registrar で処理される顧客宅内のデバイスに DHCP サーバーが与えるようにサービスプロバイダが決定できるアドレス数の制限。
サブゾーン	親ノードの子として表される、委任されたドメインのパーティション。サブゾーンは常に親の名前で終わります。たとえば、 <code>boston.example.com</code> は <code>example.com</code> のサブゾーンです。
サブゾーン委任	ゾーンをサブゾーンに分割します。これらのサブゾーンの管理権限を委任して、それらのサブゾーン内のユーザーによって管理されるようにしたり、別のサーバーによってサービスが提供されるようにすることができます。
スーパーネット	単一のクラスレスネットワークアドレスとしてアドバタイズされた IP ネットワークアドレスの集約。
同期	同期は、リージョンクラスタとローカルクラスタ、CCM とその他のプロトコルサーバー、フェールオーバー サーバー、HA DNS サーバー、およびルータの間で発生する可能性があります。
同期編集モード	データがプロトコルサーバーにある <code>dhcp</code> または <code>dns</code> 編集モード。 ステージング編集モード も参照。
T	
TAC	Cisco Technical Assistance Center。 Cisco Prime Network Registrar は、問題を TAC に報告するときに使用する <code>cnr_tactool</code> ユーティリティを提供します。
TCP/IP	データ通信プロトコルのスイート。この名前は、伝送制御プロトコル (TCP) とインターネットプロトコル (IP) という、スイート内のより重要な2つのプロトコルに由来します。インターネットトラフィックの基礎を形成します。

テンプレート	DNS ゾーンと DHCP スコープには、類似したプロパティを持つ複数のオブジェクトを作成するためのテンプレートを設定できます。
トランザクション シグニチャ (TSIG)	DNS メッセージが信頼できる送信元から送信され、改ざんされていないことを保証する DHCP メカニズム。 アクセスコントロールリスト (ACL) も参照。
トラップ	ネットワーク上の空きアドレスを決定するなど、特定の SNMP イベントを検出するように設定された基準。 SNMP 通知 も参照。
トリミングと圧縮	トリミングは、ログやその他のファイルのサイズを調整するために古い履歴データを定期的に削除することです。圧縮は、特定の期間よりも古いデータをレコードのサブセットに削減します。
トリビアルファイル転送プロトコル (TFTP)	UDP を使用してネットワーク経由でファイルを転送するために使用されるプロトコル。 ユーザー データグラム プロトコル (UDP) も参照。
U	
万国標準時 (UT)	以前はグリニッジ標準時 (GMT) と呼ばれていた国際標準時間基準。協定世界時 (UCT) とも呼ばれます。
更新設定、DNS	DNS アップデートのために、ゾーンとメインおよびバックアップ DNS サーバーとの関係を定義します。
更新マップ、DNS	DHCP ポリシーと DNS ゾーンのリスト間の更新関係を定義します。
更新ポリシー、DNS	DNS RR レベルで更新承認を管理するための DHCP のメカニズムを提供します。
ユーザー データグラム プロトコル (UDP)	コネクションレス型の TCP/IP トランスポート層プロトコル。
V	

仮想チャネル識別子 (VCI) と仮想パス識別子 (VPI)	ATM セルのヘッダー内の 16 ビットフィールド。セルが一連の ATM スイッチを経由して宛先に送られるとき、VCI は、VPI とともに、セルの次の宛先を識別します。ATM スイッチは VPI/VCI フィールドを使用して、最終宛先への途中でセルが中継を必要とする次のネットワーク VCL を識別します。VCI の機能は、フレームリレーにおける DLCI の機能に似ています。
バーチャルプライベートネットワーク (VPN)	プライベートアドレス空間の IP トラフィックがパブリック TCP/IP ネットワークを介して安全に移動できるプロトコル。VPN は、トンネリングを使用して、すべての情報を IP レベルで暗号化します。VRF も参照。
VRF	VPN ルーティングおよび転送インスタンス。ルーティングプロトコルコンテキストによって入力されたルーティングテーブルおよび転送情報ベーステーブル。バーチャルプライベートネットワーク (VPN) も参照。
W	
ウェルノウンポート	トランスポートレベルプロトコル (たとえば、TCP や UDP) によって特定の用途のために事前割り当てられた IP プロトコルポート番号の任意のセット。各サーバーはウェルノウンポートでリッスンし、クライアントがそれを見つけることができますようにします。
WKS レコード	DNS ウェルノウンサービスリソースレコード (RR)。ゾーン内のホストによって提供されるサービスを一覧表示するために使用されます。一般的なプロトコルは TCP と UDP です。
Y	
yiaddr	クライアントの IP アドレス、または DHCP サーバーがクライアントに提供する (最終的に割り当てる) アドレス。クライアントとサーバー間で RFC2131 パケットで送信されます。
Z	

ゾーン	他のゾーンに委任された名前を除き、特定のポイント以下のすべての名前を含む DNS ツリー階層内の委任ポイント。ゾーンは、通常は管理境界によって区切られるドメイン空間の連続セクションの内容を定義します。各ゾーンには、リソースレコードと呼ばれるエンタリで構成される構成データがあります。ゾーンは、1つのドメインに正確にマッピングできますが、ドメインの一部だけを含み、残りは別のサブゾーンに委任することもできます。
ゾーン分散	同じセカンダリゾーン属性を共有する複数のゾーンの作成を簡素化する構成。ゾーン分散では、1つ以上の定義済みセカンダリサーバーを追加する必要があります。
権限のゾーン	特定のネームサーバーが権限を持つDNSドメインのグループ。
ゾーン転送	セカンダリDNSサーバーが起動し、プライマリサーバーから自身を更新するときに発生するアクション。セカンダリDNSサーバーは、プライマリネームサーバーに対して、AXFR（すべて転送）またはIXFR（増分転送）と呼ばれる特定の packets タイプで照会し、データベースのコピーの転送を開始します。



索引

A

- A レコード 265
- AD 外部認証サーバー 76–77
 - プッシュ 76
 - 引っ張って 77
- addrblock-admin ロール 45
 - ipv6-management サブロール 45
 - ric-management サブロール 45
 - コア機能 45
- addrtrapconfig-list 126
- admin コマンド (CLI) 62–63, 73, 75
 - enterPassword 63
 - pull 62, 75
 - push 62, 73
 - set password 63
 - 再利用 62
 - delete 62
 - create 62
- admin ロール 265
- agent_server_log ファイル 179
- auth-ad-server コマンド (CLI) 77–78
 - pull 78
 - push 77

C

- catalina.date.log ファイル 179
- ccm コマンド (CLI) 135, 177, 184
 - set 177, 184
 - log-settings 184
 - ポーリング属性、設定 135
- CCM サーバー 9, 135
 - ポーリング属性 135
- CCM サーバーのプロパティ 116
 - 編集 116
- CCM データベース 179, 266
 - ファイル 179
- ccm_startup_log ファイル 179
- ccm_upgrade_status_log ファイル 179

- CCM 179
 - データベース 179
 - ロギング 179
- ccm-admin ロール 45
 - owner-region サブロール 45
 - server-management サブロール 45
 - 許可サブロール 45
 - コア機能 45
 - データベース サブロール 45
 - 認証サブロール 45
- cdns コマンド (CLI) 194
 - resetStats 194
- cdns_log ファイル 179
- cdns_startup_log ファイル 179
- CDNS 196
 - 統計情報 196
- central-cfg-admin ロール 45
 - dhcp-management サブロール 45
 - ric-management サブロール 45
 - コア機能 45
- central-dns-admin ロール 45
 - security-management サブロール 45
 - server-management サブロール 45
 - コア機能 45
- central-host-admin ロール 45
 - コア機能 45
- cfg-admin ロール 45
 - ccm-management サブロール 45
 - cdns-management サブロール 45
 - dhcp-management サブロール 45
 - dns-management サブロール 45
 - ric-management サブロール 45
 - snmp-management サブロール 45
 - tftp-management サブロール 45
 - コア機能 45
- chaddr 266
 - DHCP フィールド 266
- checkports_log ファイル 179
- CLI 9, 24
 - コマンドシンタックス 24

cluster コマンド (CLI) **109, 135**

set **109**

create **109**

ポーリング属性、設定 **135**

CMTS **2**

ケーブル モデム終端システムを参照 **2**

CNAME レコード **267**

cnr_exim ユーティリティ **236**

CNRDB データベース **225, 229, 267**

バックアップ **225**

ファイル **225**

リカバリ **229**

ログファイル **225**

cnrdb_checkpoint ユーティリティ **240**

cnrdb_recover ユーティリティ **239**

cnrdb_verify ユーティリティ **240**

cnrsnmp_log ファイル **179**

cnrwebui_access_log.date.txt ファイル **179**

cnrwebui_log ファイル **179**

config_ccm_log ファイル **179**

D

DHCP **4, 136, 179, 206, 266, 278**

関連サーバー、表示 **206**

クライアント **266**

MAC アドレス **266**

サーバ **179, 278**

次の DHCP の IP アドレス **278**

ロギング **179**

設定時の注意事項 **4**

リース履歴収集 **136**

dhcp コマンド (CLI) **129, 136, 176–177, 184, 192, 194, 201, 209**

getRelatedServers **209**

getStats **201**

制限リスト **176**

resetStats **194**

set **129, 184, 192**

traps-enabled **129**

v6-default-free-address-config **129**

アクティビティの概要 - 間隔 **192**

デフォルトフリーアドレス-コンフィグ **129**

log-settings **184**

start **177**

stop **177**

イネーブル化 **192**

collect-sample-counters **192**

リース履歴収集属性 **136**

DHCP 使用率 **134–135**

ポーリング **134–135**

オフセット **135**

再試行間隔 **135**

DHCP 使用率 (続き)

ポーリング (続き)

データ **134**

dhcp_startup_log ファイル **179**

dhcp-admin ロール **45**

ipv6-management サブロール **45**

コア機能 **45**

dns コマンド (CLI) **184, 194**

getStats **194**

resetStats **194**

set **184**

log-settings **184**

dns_startup_log ファイル **179**

dns_upgrade_status_log ファイル **179**

DNS **179, 265, 270**

グルー レコード **270**

権威サーバ **265**

サーバ **179**

ロギング **179**

dns-admin ロール **45**

ipv6-management サブロール **45**

security-management サブロール **45**

server-management サブロール **45**

コア機能 **45**

DOCSIS **1, 268**

F

file_tftp_1_log ファイル **179, 218**

file_tftp_1_trace ファイル **179**

FQDN **270**

free-address-low-threshold イベント、SNMP **122**

G

giaddr **270**

DHCP フィールド **270**

grep ツール (UNIX) **214**

group コマンド (CLI) **64, 79–80**

pull **64, 80**

push **64, 79**

再利用 **64**

delete **64**

create **64**

H

HINFO レコード **270**

host-admin ロール **45**

コア機能 **45**

HTTPS ログイン **12**

- I**
- IETF 268
 - ifconfig ツール (UNIX) 214
 - in-addr.arpa ドメイン 270
 - install_cnr_log ファイル 179
 - IP ヘルパー 163
 - ルータへの追加 163
 - ISP 1
 - インターネット サービス プロバイダを参照 1
- J**
- jsui_log.date.txt ファイル 179
- L**
- LAN セグメント 278
 - Linux 24
 - CLI 位置 24
 - lock files/temp directory [temp directory] 224
 - log.xxx ファイル、CNRDB 225
- M**
- MSO 1
 - MX レコード 273
- N**
- name_dhcp_1_log ファイル 179
 - name_dns_1_log ファイル 179
 - NOTIFY 274
- O**
- OUI 275
 - VPN 275
 - owner コマンド (CLI) 90, 92–93
 - pull 90, 93
 - push 90, 92
 - 再利用 90
 - create 90
- P**
- PTR レコード 276
- R**
- RADIUS 外部認証サーバー 75–76
 - プッシュ 75
 - RADIUS 外部認証サーバー (続き)
 - 引っ張って 76
 - region コマンド (CLI) 90, 92–93
 - pull 90, 93
 - push 90, 92
 - 再利用 90
 - create 90
 - regional-addr-admin ロール 45
 - dhcp-management サブロール 45
 - lease-history サブロール 45
 - subnet-utilization サブロール 45
 - コア機能 45
 - regional-admin ロール 45
 - owner-region サブロール 45
 - 許可サブロール 45
 - コア機能 45
 - データベース サブロール 45
 - 認証サブロール 45
 - RFC 5–6, 117, 268
 - 1123 117
 - 1350 117
 - 1782 117
 - 1783 117
 - 1995 5–6
 - 1996 5–6
 - 2316 268
 - RIC サーバー 2
 - 「ルータ インターフェイス設定サーバー」を参照 2
 - role コマンド (CLI) 66, 81–82
 - pull 66, 82
 - push 66, 81
 - 再利用 66
 - create 66
 - router コマンド (CLI) 172
 - set 172
 - router-interface コマンド (CLI) 173
 - set 173
- S**
- SCP 2
 - システム設定プロトコルを参照 2
 - server コマンド (CLI) 175, 177, 182, 192, 194
 - enable/disable start-on-reboot 175
 - getHealth 192
 - getStats 194
 - reload 177
 - serverLogs 182
 - set logsize 182
 - show 182
 - set 177
 - start 177
 - stop 177

siaddr **278**
 DHCP フィールド **278**

SNMP **119, 122, 126, 179**
 free-address-low-threshold **122**
 v2c 標準 **119**
 通知 **119**
 通知イベント **126**
 traps **119, 122**
 PDU **119**
 ロギングとトレース **179**

snmp コマンド (CLI) **121**
 server-active の無効化 **121**
 server-active の有効化 **121**
 set **121**
 cache-ttl **121**
 trap-source-addr **121**
 コミュニティ **121**

SNMP サーバー **120**
 セットアップ **120**

snmp-interface コマンド (CLI) **121**

SOA レコード **279**

SSL **107**
 クラスタ接続 **107**

T

TAC ツール **215**
 cnr_tactool ユーティリティ **215**

tenant コマンド (CLI) **55, 59, 83–84**
 pull **59, 84**
 push **59, 83**
 再利用 **59**
 create **55**

tftp コマンド (CLI) **184, 203, 218–219**
 enable file-cache **219**
 getStats **203**
 set **184, 218–219**
 file-cache-directory **219**
 file-cache-max-memory-size **219**
 home-directory **219**
 log-file-count **218**
 log-level **218**
 log-settings **184, 218**

TFTP サーバー **117–118**
 ネットワーク インターフェイス **118**
 管理 **118**
 表示 **117**
 編集 **117**

TFTP **117, 218–219**
 DOCSIS **117**
 トラブルシューティング **218**
 パケット、トレース **218**

TFTP (続き)
 ファイル キャッシング **219**
 ロギングとトレース **218**

tftp-interface コマンド (CLI) **119**

Tomcat **2, 179**
 サーバー **2**
 データベース ログ ファイル **179**

top ツール (UNIX) **214**
 vmstat ツール (UNIX) **214**

trap コマンド (CLI) **122**
 set **122**
 free-address-low-threshold **122**

trap-recipient コマンド (CLI) **121**
 create **121**

TTL プロパティ **274**
 negative cache **274**

U

uBR 10000 ルータ **171**
 uBR 7200 ルータ **163, 171**
 UNIX トラブルシューティング ツール **214**

V

vpn コマンド (CLI) **144–145**
 pull **145**
 push **144**

VPNs **143–144**
 リージョン **143**
 ローカル (local) **143–144**
 プッシュ **143**
 引っ張って **144**

W

Web UI **3, 9, 12, 14–17, 84, 179**
 セッション管理 **84**
 セッション設定 **15**
 属性 **16**
 表示 **16**
 変更 **16**
 導入シナリオ **3**
 ナビゲーション **14**
 ヘルプ **16–17**
 属性 **16**
 トピック **17**
 変更、コミット **15**
 ユーザー設定 **15**
 ロギング **179**
 ログイン **12**

Windows 24, 182–183

CLI 位置 24

イベントビューア 183

ロギング 182

WKS レコード 282

Y

yiaddr 282

DHCP フィールド 282

Z

zone-dist コマンド (CLI) 208

create 208

リスト 208

あ

アドレス 205, 270

IP 形式 270

使用状況、表示 205

アドレス範囲 154

追加 154

address space 166

ローカル、サブネットからのプル 166

アドレス インフラストラクチャ、作成 153

アドレス制限、ゾーン 157

アドレス使用状況レポート 205

表示 205

い

イベントビューア、Windows 183

イベント ロギング 183

インターネット技術特別調査委員会 268

インターネット サービス プロバイダ 1

う

ウイルス スキャン、ディレクトリの除外 235

え

面グラフ 32

お

折れ線グラフ 32

か

ガイドラインに準拠 4

設定: 4

パフォーマンス 4

外部認証サーバー 50, 52, 75

追加 52

プッシュ 75

引っ張って 75

仮想パス識別子 282

管理コンポーネント 9

管理者 43–45, 60, 63, 71–72, 74, 152, 161, 265

一元管理 71

グループとの関係 44

タイプ 45

追加 60

パスワード 60, 63

管理 63

追加 60

変更 63

編集 60

リージョン 161

レプリカのプル 74

ローカル クラスタ 152

ローカルへのプッシュ 72

き

企業ユーザー 1

きめ細かい管理 66

キャッシュ、セッションの更新 13

く

クライアント 266, 282

ハードウェア アドレス 266

IP アドレス 282

クライアント クラス コマンド (CLI) 142–143

pull 143

push 142

クライアント クラス 141–142

リージョン 141

ローカル、プッシュ 141

ローカル、プル 142

クラスタ 2, 107, 110, 112, 135

poll-replica-interval 110

poll-replica-offset 110

poll-replica-rrs 110

アクティブ化 112

セキュア接続 107

データ、リカバリ 112

クラスタ (続き)

- 非アクティブ化 112
- ポーリング属性 135
- ローカル、リージョン 2

グループ 44, 49, 63, 78–79

- 削除 63
- 追加 63
- プッシュ 78
- 引っ張って 79
- 編集 63
- ロールとの相互作用 44

け

ゲートウェイアドレス 270

ケーブル モデム 終端システム (CMTS) 2

権限 43–45, 49, 65, 81–82, 157, 277

- addrblock-admin 45
- ccm-admin 45
- central-cfg-admin 45
- central-dns-admin 45
- central-host-admin 45
- cfg-admin 45
- dhcp-admin 45
- dns-admin 45
- host-admin 45
- regional-addr-admin 45
- regional-admin 45
- グループ 49
- グループとの相互作用 44
- サブロール 45
- 制約 45
- 制約付き 157, 277
 - 作成 157
- 追加 65
- プッシュ 81
- 引っ張って 82

さ

サーバ 175, 182, 190, 192, 213, 278

- IP アドレス 278
- イベント、ロギング 182
- 管理 175
- 障害、トラブルシューティング 213
- 状態、表示 190
- 正常性、表示 190
- 統計、表示 192

サーバー クラスタ、追加 106

再帰クエリ 276

サブゾーン 268, 280

- 委任 268, 280

subnets 154

- 追加 154

サブロール 71, 91

- 集中管理 71, 91

散布図 32

し

システム設定プロトコル (SCP) 2

シャドウ バックアップ 221, 224

- cnr_shadow_backup ユーティリティ 224
- サードパーティ バックアップ プログラム 224
- 時間、設定 224
- 手動 224

所有者 89, 91–92

- 管理 89
- 設定 89
- プッシュ 91
- 引っ張って 92

シングルサインオン 106

す

スコープ 279–280

- ステーjing編集モード 279
- 同期編集モード 280

スコープ・テンプレート・コマンド (CLI) 138

- pull 138
- push 138

スコープ テンプレート 136–138, 167

- 名前式 167
- 範囲式 167
- リージョン 136
- リージョン クラスタでの作成 167
- ローカル クラスタへのプッシュ 137
- ローカル クラスタからのプル 138
- 埋め込みポリシー式 167

staged 279

- 編集モード 279

せ

整合性ルール 186

- 表示 186
- リスト 186

制約付きロール 277

- secondary 278
- subnets 278

secondary (続き)

ネーム サーバー **278**
DNS **278**

セキュア **107**

クラスタ接続 **107**

セッション・コマンド (CLI) **13**

cache refresh **13**

設定 **274**

ネガティブ キャッシュ時間 **274**

設定: **5-6**

ガイドラインに準拠 **5-6**
特別な事例 **6**

そ

増分ゾーン転送 **5-6, 271**

有効化 **5-6**

zones **154-155, 157, 279-280**

アドレス制限 **157**

インフラストラクチャ **154**

サブゾーン **280**

委任 **280**

ステージング編集モード **279**

同期編集モード **280**

ホストの制限 **157**

リスト **155**

ゾーンツリー、表示 **155**ゾーンデータ **165**

引っ張って **165**

ゾーン分散 **208**

作成 **208**

リスト **208**

属性 **16**

表示 **16**

ヘルプ ウィンドウ **16**

変更 **16**

組織、登録 **251**

た

大企業での導入 **3**タスク、スケジューリング **178**ダッシュボード **37**

システム メトリック **37**

担当者、登録 **249**

ち

値の大文字と小文字の区別 **266**中央構成 **95**中央構成管理 (CCM) サーバー **2**

CCM サーバーを参照 **2**

チュートリアル **151, 159**

リージョン クラスタ **159**

ローカル クラスタ **151**

て

データ オーバー ケーブル サービス インターフェイス仕様 **1**

DOCSIS を参照 **1**

データ ディレクトリ、変更 **223**データベース **110, 175, 179, 221, 223, 236, 266-267**

CNRDB **223, 267**

インポート **236**

エクスポート **236**

起動、ロード **175**

binding **266**

バックアップ **221, 223**

戦略 **223**

レプリカ **110**

ログ ファイル **179**

デジタル加入者線 (DSL) **268**テナント **43, 54-56, 58-59, 83**

外部認証の使用 **59**

管理 **54**

クラスタの割り当て **58**

削除 **56**

追加 **55**

編集 **56**

レプリカ データベースからのプル **83**

ローカルへのプッシュ **83**

テナント データ **56, 58-59**

cnr_exim の使用 **59**

管理 **56**

プッシュとプル **58**

と

同期 **280**

編集モード **280**

統計情報 **192**

サーバー **192**

トラップ、SNMP **119, 121-122**

free-address-high **122**

free-address-low **122**

受信者、作成 **121**

トリビアル ファイル転送プロトコル **117**

TFTP を参照 **117**

ね

ネガティブ キャッシュ時間 274

は

パスワード 13, 63
 管理者 63
 変更 63
 非表示 63
 変更 13

ひ

非セキュア ログイン 12
 非同期転送モード (ATM) 265

ふ

フェールオーバー, DHCP 168
 サーバー ペアの作成 168
 ペアの同期 168
 不完全委任 271
 複数のユーザー 13
 プロトコル データ ユニット, SNMP 126
 「PDUSNMP」を参照 126
 PDUPDU, SNMP 126

へ

ヘルプ ページ 17
 変更ログ 184
 表示 184
 編集モード 279-280
 staged 279
 同期 280

ほ

棒グラフ 32
 ホーム 18
 設定の要約 18
 ポーリング 134-135, 275
 オフセット 135
 間隔 135
 再試行間隔 135
 時間誤差の影響 134
 使用率データ 134
 リース履歴データ 134

ホスト 156-157, 159
 アドレス範囲のテスト 159
 作成 156
 ゾーン制限 157
 ポリシー 139-140, 275
 定義済みの 275
 リージョンの作成 139
 ローカル (local) 139-140
 プッシュ 139
 引っ張って 140
 ポリシー コマンド (CLI) 140
 pull 140
 push 140
 ポリシー, DHCP 166
 ローカル クラスターへのプッシュ 166

ま

マルチスレッド サーバー 117
 マルチネット化 273
 マルチプル サービス オペレータ 1
 MSO を参照 1

め

メイン メニュー 18

ゆ

ユーザ 183
 イベント警告 183
 ユーザー インターフェイス 9
 ユーザー環境設定、設定 21
 ユーティリティ プログラム 224
 サードパーティ バックアップ 224

ら

ライセンス 12, 101-102
 追加 12, 102
 ライセンス使用率 106
 ライセンス履歴 105
 round-robin 278

り

リージョン 89-92
 管理 90
 設定 89
 プッシュ 91

リージョン (続き)
 引っ張って 92

リージョン クラスタ 9, 43, 106–107, 136–137, 139–143, 145–146, 159, 162

VPNs 143

管理 43

クライアント クラス 141–142
 プッシュ 141
 引っ張って 142

スコープ テンプレート 136–137
 プッシュ 137

チュートリアル 159

追加 106–107, 162
 サーバー クラスタ 106
 ローカル クラスタ 107, 162

フェールオーバー ペア 145

ポリシー 139–140
 プッシュ 139
 引っ張って 140

予約 146
 プッシュ 146

リージョンのメイン メニュー 23

leases 6, 179, 209
 アクティビティ 209
 推奨される更新時間 6
 データベース 179
 表示 209

リリース履歴 134–136
 収集の最大有効期間 136
 ポーリング 134–135
 オフセット 135
 間隔 135
 再試行間隔 135
 データ 134

有効化 136

リソース レコード 265, 267, 270, 273, 276, 279, 282

A 265

CNAME 267

HINFO 270

MX 273

PTR 276

SOA 279

WKS 282

リリースの相互運用性 7

る

ルータ 163, 171–173, 270

IP ヘルパー 163

uBR7200 163

ゲートウェイ アドレス 270

ルータ (続き)
 属性の編集 172
 追加 163, 171
 バンドル 173
 編集 172
 リスト 171

ルータ インターフェイス 163, 172–173
 属性の編集 173
 追加 163
 表示 172
 編集 172

ルータ インターフェイス設定 (RIC) サーバー 2

ルーテッドブリッジカプセル化 (RBE) 278

ルート ネーム サーバー 277

loopback 272
 アドレス 272
 zones 272

れ

レプリカ データ 110–111
 表示 111

レポート 205, 247–253
 ARIN 247
 IPv4 使用率 252
 WHOIS/SWIP 253
 アドレスの使用法 205
 組織 250–251
 作成 250
 編集 251
 担当者 248–250
 作成 249
 編集 250
 割り当て 247

レポート・コマンド (CLI) 206

ろ

ローカル クラスタ 2, 9, 43, 106, 109–110, 151
 管理 43
 接続 109
 チュートリアル 151
 ツリー表示 106
 データの複製 110
 同期 110
 編集 109

ローカル クラスタへの管理者の自動プッシュ 73

ログアウト 18

ログイン、Web UI 12

わ

サブネット割り当て (続き)
DHCP [279](#)

サブネット割り当て [279](#)