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

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 （18 ページ） を参照してください。
- **View logs** - ログの検索 （10 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ず、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 （18 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 （10 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。

a) 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。

b) 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 *1 : .../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[1]
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[2]
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。

[1] 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。

[2] 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 （36 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 （1 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 （10 ページ）

ロギングの形式と設定 （9 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 （8 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、サーバーの設定中にのみ、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 *2 : cnr_rules* オプション

オプション	説明
–list	使用可能な整合性ルールを一覧表示します。 （注） 使用可能なコマンドのリストは、**-N** 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。 `> cnr_rules -N admin -P changeme -list`
–run [**rule-match**]	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 rule-match 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。

	• すべてのルールを実行します。
	`> cnr_rules -N admin -P changeme -run`
	• 名前に文字列「dhcp」が含まれているルールのみを実行します。
	`> cnr_rules -N admin -P changeme -run dhcp`
	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：> **cnr_rules -N admin -P changeme -run "router interface"**

–details	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。
	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。 `> cnr_rules -N admin -P changeme -run DNS -details`

オプション	説明
–xml	ルールの結果をXMLファイルで生成します。 （注） **–xml** 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、**–details** オプションは無視されます。 `> cnr_rules -N admin -P changeme -run -xml`
–path *.classpath*	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）。 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。

–interactive	インタラクティブ セッションでツールを実行します。
	`> 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`

–both	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 （16 ページ）
正常性の表示 （17 ページ）
統計の表示 （18 ページ）
IP アドレスの使用状況の表示 （31 ページ）
関連サーバーの表示 （32 ページ）
リースの表示 （35 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が、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す。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）
- CCM サーバー（ローカルおよびリージョン クラスタ）
- DNS 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
  - 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ー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 *3:* 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 4 : DNS 統計 、DHCP については表 6 : DHCP 統計 、TFTP については表 7 : 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、その後に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 *4 : 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）

フィールド	統計	説明
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）
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す。

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 *5 : 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。

統計	説明
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。
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。

統計	説明
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。
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	再帰応答を待ってキューに入れられた要求の合計数。
requestlist-total-user	再帰応答を待ってキューに入れられたユーザー要求の合計数。
requestlist-total-system	再帰応答を待って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）。

統計	説明
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）。
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。

統計	説明
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。
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 ルックアップの最大数を超えたクエリの数。
client-rate-limit	*client-rate-limiting* 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	*domain-rate-limiting* 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 *6 : 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。

フィールド	統計	説明
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 *7 : 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）。

フィールド	属性	説明
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。
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。

フィールド	属性	説明
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。
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 （32 ページ）

DNS ゾーン分散サーバー （34 ページ）

DHCP フェールオーバー サーバー （35 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 *8*:永続イベント アルゴリズム

イベントに到達	
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	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。 `The queue of events for the name remote server at address has x events, and has reached the info limit of y/2 events out of an upper limit of y events per remote server. The remote server may be misconfigured, inoperative, or unreachable.`
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	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。 `The queue of events for the name remote server at address has x events, has exceeded the limit of y events per remote server, but is below the limit of z total events in memory. The remote server may be misconfigured, inoperative, or unreachable.`
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	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。 `The queue of events for the name remote server at address has x events, and has grown so large that the server cannot continue to queue new events to the remote server. The limit of y 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 n is being dropped.` 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。

イベントに到達	
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	ERROR ログ メッセージを発行します。 `The queue of pending events has grown so large that the server cannot continue to queue new events. The queue's size is z, and the limit is z.` 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。

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

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。通常の操作では、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 （5 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 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す（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℃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* ー *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 （41 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 ロギング 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 *9 : statscollector* のオプション

オプション	説明
-C *cluster*:[*port*]	接続するローカルクラスタ（デフォルト：localhost）。
-N *admin*	管理者アカウント名。
-P ***password***	管理者パスワード。
-i *interval*	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。
-e *file.xml*	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 *file.html*	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 *charts.txt*	**-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 *date time*	指定した日時より前の統計サンプルを無視します。
-f *date time*	指定した日時より後の統計サンプルを無視します。
-w *width* X *height*	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 *name,value*	Google 注釈グラフオプションを指定します。
-t "*title*"	グラフのタイトル（デフォルトを上書きする）。
-u *infile.html*	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。

オプション	説明
file	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 （44 ページ）
TFTP メッセージ ロギングの最適化 （45 ページ）
TFTP ファイル キャッシングの有効化 （45 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を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。