



## 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 \(1 ページ\)](#)
- [反復タスクのスケジューリング \(4 ページ\)](#)
- [ログ \(6 ページ\)](#)
- [データ整合性ルールの実行 \(13 ページ\)](#)
- [サーバー ステータスのモニターリングと報告 \(16 ページ\)](#)
- [cnr.conf ファイルの変更 \(32 ページ\)](#)
- [DHCP および DNS サーバーのトラブルシューティング \(36 ページ\)](#)
- [TAC ツールの使用 \(37 ページ\)](#)
- [TFTP サーバーのトラブルシューティングと最適化 \(40 ページ\)](#)

## 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 11.1 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 \(19 ページ\)](#) を参照してください。
- **View logs** - [ログの検索 \(11 ページ\)](#) 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。

## ローカルおよびリージョン 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 \(19 ページ\)\)](#) 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 \(11 ページ\)\)](#) 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 11.1 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 11.1 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 11.1 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。
- キャッシング 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：
  - 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。
  - 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：
  - 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。
  - 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：
  - プライマリ DNS サーバーまたは HA メイン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。
  - バックアップ HA DNS サーバーをリロードします (設定されている場合)。
  - セカンダリ DNS サーバーをリロードします。
- DNS 更新マップの同期：
  - DNS 更新マップを DHCP サーバーと DNS サーバーに同期します。
  - ローカルサーバーとリモート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 ペアのスマート同期：
  - サーバーが設定全体を最後に読み取った後に DHCP 設定の更新が行われた場合は、メイン DHCP サーバーをリロードします。

- リロードが完了して失敗した場合は、タスクを中止します。
- 設定をメインからバックアップに同期します。
- 同期が失敗した場合は、タスクを中止します。
- バックアップサーバーが設定全体を最後に読み取った後にバックアップに DHCP 設定の更新がある場合は、バックアップサーバーをリロードします。

## ローカル 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、サーバーをリロードします。
    - **sync-dns-pair** : HA DNS フェールオーバーサーバーペアを同期し、サーバーをリロードします。
    - **sync-zd-map** : ズーン分散マップを同期し、サーバーをリロードします。
    - **sync-dns-update-map** : DNS 更新マップを同期し、サーバーをリロードします。
    - **smart-sync-dhcp-pair** : DHCP フェールオーバーサーバーペアを同期し、必要に応じてサーバーをリロードします。メインとバックアップの両方で設定に変更がない場合、どのサーバーもリロードされません。
  - 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*、*sync-dns-update-map*、and *smart-sync-dhcp-pair* 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、`/var/nwreg2/{local|regional}/logs` ディレクトリ内の Cisco Prime Network Registrar 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	<code>install_cnr_log</code>	両方	インストールプロセス
アップグレード	<code>ccm_upgrade_status_log</code>	両方	アップグレードプロセス
	<code>dns_upgrade_status_log</code>	ローカル	アップグレードプロセス
	<code>dhcp_upgrade_status_log</code>	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	<code>agent_server_1_log</code>	両方	サーバーエージェントの起動と停止

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
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 <sup>1</sup>
	dns_security_log	ローカル (Local)	DNSセキュリティイベント
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 <sup>2</sup>
	cdns_security_log	ローカル (Local)	CDNSセキュリティイベント
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
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

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
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。
スマート ライセンス	ccm_smartagent_log	リージョン	スマートエージェントログ
	ch_dbg.log		Call Home ログ
	SAEvent*.log		スマートエージェントイベントログ

- <sup>1</sup> 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。
- <sup>2</sup> 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) 11.1 より前のバージョンからのアップグレードでは、古い事前設定済み (または明示的に設定された) 値の 100 万バイトがログファイルに使用されます。

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 \(32 ページ\)](#) 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 はデフォルトで `/var/nwreg2/{local|regional}/logs` ディレクトリ内にすべてのログを維持します。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。

## ローカルおよびリージョン 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 \(11 ページ\)](#)

[ロギングの形式と設定 \(10 ページ\)](#)

## ログの形式と設定

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。
- **Packet** : パケットログメッセージを記録します。

## ローカルおよびリージョン 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、ローカルクラスターの DNS および DHCP サーバーのログを設定するには、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 11.1 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 11.1 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、ページの上部和下部で使用可能な [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 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

expert コマンド `ccm trimChangeSets delete-age [db-max-records]` を使用し、指定された引数を使用して変更セット (変更ログ) のトリムを開始します。シンタックスと属性の説明については、/docs ディレクトリの CLIGuide.html ファイルの **expert** コマンドを参照してください。



**警告** 上記の操作は通常必要ではなく、指定された値を使用します。これは、CCM によって実行される定期的なトリムとは異なる場合があります。このコマンドは、保持する必要があるデータを削除する可能性があるため、十分に注意して使用してください。

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 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 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 `.../usrbin/cnr_rules` ディレクトリにあります。

**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
<p><code>-list</code></p>	<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>&gt; cnr_rules -N admin -P changeme -list</pre>
<p><code>-run [rule-match]</code></p>	<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"> <li>すべてのルールを実行します。                     <pre>&gt; cnr_rules -N admin -P changeme -run</pre> </li> <li>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>&gt; cnr_rules -N admin -P changeme -run dhcp</pre> </li> </ul> <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：<pre>&gt; cnr_rules -N admin -P changeme -run "router interface"</pre></p>
<p><code>-details</code></p>	<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>&gt; cnr_rules -N admin -P changeme -run DNS -details</pre>
<p><code>-xml</code></p>	<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>&gt; 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>&gt; cnr_rules -N admin -P changeme -run -interactive RuleEngine [type ? for help] &gt; ? Commands:   load &lt;class&gt;      // load the specified rule                class   run &lt;rule-match&gt; // 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)

## 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 クラスター)
- DHCP 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

- 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。*install-path/usrbin*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 11.1* インストールガイドを参照してください。

## ローカルおよびリージョン 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。

## ローカルおよびリージョン 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。  ( <code>dhcp getStats</code> )	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。  ( <code>dhcp getStats server sample</code> )

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)
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。  ( <b>dns getStats</b> )	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。  ( <b>dns getStats performance sample</b> )
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。  ( <b>cdns getStats server total</b> )	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。  ( <b>cdns getStats server sample</b> )

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 5: DHCP 統計、TFTPについては表 6: 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 統計情報の完全なリストについては、表 1 を参照してください。

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。
- [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 [,] cache [,] datastore [,] top-names [,]
dns-hhc | all> [total | sample]]
```

最も一般的に使用されているコマンドは **dns getStats all** であり、表 1 で説明されている統計情報を返します。**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)
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。

フィールド	統計	説明
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 サーバーの統計情報の完全なリストについては、表 1 を参照してください。

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** コマンドは表 1 に示す統計情報を紹介します。

## 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 統計情報の完全なリストについては、表 1 を参照してください。

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 オフナー 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]]]
```



最も一般的に使用されているのは `dhcp getStats all` コマンドで、表 1 で説明する統計情報を返します。 `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 5: 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 6: 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。
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。

フィールド	属性	説明
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。
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 11.1 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 11.1 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 11.1 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。

## 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 7: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 <i>name</i> remote server at address has <i>x</i> events, and has reached the info limit of <i>y/2</i> events out of an upper limit of <i>y</i> 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 <i>name</i> remote server at address 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>イベントに到達</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 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.</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 z, and the limit is z.</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 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 11.1 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 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 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 11.1 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）。

## 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、`/var/nwreg2/{local|regional}/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、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.https-port=8443
cnr.regional-ip=ipaddress
cnr.schemadir=/opt/nwreg2/local/schema
cnr.localhost-ipv6=2001:420:54ff:13::403:37
cnr.classesdir=/opt/nwreg2/local/classes
cnr.rootdir=/var/nwreg2/local
cnr.localhost-uuid=0e0eeab2-b235-4d01-81fe-12e042f8768f
cnr.regional-ccm-port=1244
cnr.services=dhcp,dns
cnr.tempdir=/var/nwreg2/local/temp
cnr.install-home=/opt/nwreg2/local
cnr.extensiondir=/opt/nwreg2/local/extensions
cnr.ccm-port=1234
cnr.propsdir=/opt/nwreg2/local/conf
cnr.backup-time=23:45
cnr.java-home=/usr/bin/java
cnr.confdir=/var/nwreg2/local/conf
cnr.ccm-mode=local
cnr.customextensiondir=/var/nwreg2/local/extensions
```

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 (:) を使用できません。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 \(6 ページ\)](#)）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。

時々問題を発生させる場合がある要因の 1 つは Java パスです。理想としては、Java をデフォルトの場所にインストールします。そのためには、次の行を **cnr.conf** ファイルに使用する必要があります。

```
cnr.java-home=/usr/bin/java
```

ただし、場合によっては異なるパスが使用され (11.0 より前のバージョンからアップグレードされた場合など)、Java へのより明示的なパスによって、Java がアップグレードされると Cisco Prime Network Registrar が正しく起動しなくなる可能性があります。したがって、**cnr.conf** ファイルでこのパスを確認し、インストールされた Java が正しく取得されるように (アップグレードされている場合も) 上記の行に置換してください。

## Syslog のサポート

Cisco Prime Network Registrar は 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。

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 サーバーへのロギングが Prime Network Registrar サーバーに対して有効にする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、このパラメータは無効になっています。
- `cnr.syslog.levels` : syslog に記録する重大度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 のログの出力元になるファシリティを指定します。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 と 4300 が syslog に記録され、メッセージ 4101 ~ 4200 は (他の syslog 設定に関係なく) ログに記録されません。



- (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 : 指定したサーバーに対して syslog を有効にするかどうかを指定します (そのサーバーの cnr.syslog.enable 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=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=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。

## 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。

### 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または無効にします。フェールオーバーパートナーのいずれかが動作していない場合は、実行中のサーバーを PARTNER-DOWN モードにします（パートナーがすぐにサービスに戻る可能性が低いと思われる場合）。
- 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。

### 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 `nwregregional`) 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。

```
systemctl stop nwreglocal or systemctl stop nwregregional
systemctl start nwreglocal or systemctl start nwregregional
```

- 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 `/var/nwreg2/{local | regional}/logs` ディレクトリにあります。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 (37 ページ)** の説明に従って TAC ツールを使用するか、またはコアファイルがあればそれを保存します。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。

## トラブルシューティング ツール

また、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 `install-path/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] [-c #-cores] [-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 (`/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)。Cisco Prime Network Registrar 11.0 以降、**cnr\_tactool**

はデフォルトでは3つのコアファイルのみを取得します。これらのファイルは経過日数が30日未満のもののみです。`-c #-cores` オプション（最大150コアファイル）を指定すると、より多くのコアファイルを収集できます。

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。`cnr_tactool` は、過去60日間のCisco Prime Network Registrarのsystemdジャーナルのエントリも抽出します。これは、製品の起動に関する問題を理解するのに役立つ場合があります。



- (注) Cisco Prime Network Registrarのコンテナの場合、コアファイルを収集で『Cisco Prime Network Registrar 11.1 インストールガイド』の「Running Cisco Prime Network Registrar Docker Container」の項に記載されている手順に従っていない場合は、Dockerホストマシンの/var/lib/systemd/coredumpディレクトリ（デフォルトの場所）から手動でtarおよびgzipを実行する必要があります。

## 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」に実行して履歴を収集し続けることに注意してください。`-i0`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、`-i0`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、ほとんど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
```

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 8: statscollector のオプション

オプション	説明
<b>-C</b> <i>cluster</i> :[ <i>port</i> ]	接続するローカルクラスタ（デフォルト：localhost）。
<b>-N</b> <i>admin</i>	管理者アカウント名。
<b>-P</b> <i>password</i>	管理者パスワード。
<b>-i</b> <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。
<b>-e</b> <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。 <b>注</b> ：-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）。
<b>-h</b> <i>file.html</i>	統計グラフを含む HTML ファイルを作成します。 <b>注</b> ：-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）。

オプション	説明
<b>-c</b> <i>charts.txt</i>	<b>-h</b> 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。
<b>-s</b> <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。
<b>-f</b> <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。
<b>-w</b> <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)。
<b>-j</b> <i>name,value</i>	Google 注釈グラフオプションを指定します。
<b>-t</b> " <i>title</i> "	グラフのタイトル (デフォルトを上書きする)。
<b>-u</b> <i>infile.html</i>	ソース HTML ファイル内のグラフを更新します。 <b>-h</b> オプションが必要です。
<i>file</i>	バイナリデータファイル ( <b>-e</b> または <b>-h</b> 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。

### 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。トレースは `/var/nwreg2/{local|regional}/logs/file_tftp_1_log` と `file_tftp_1_trace` ファイルに移動します。

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 ログイングの最適化

ログイ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) : サーバーログイ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、ログイ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 ログイングは行われません。
- **Log settings** (`log-settings` 属性を使用) - これはログイング制御の第 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、`/var/nwreg2/{local|regional}/data/tftp` に事前設定されています。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見捨て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` か、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。
-

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。