バックアップとリカバリ

この章では、Cisco Prime Network Registrar データベースを維持する方法について説明します。

- データベースのバックアップ （1 ページ）
- シンタックスと位置 （2 ページ）
- バックアップ戦略 （2 ページ）
- CNRDB データのバックアップ （4 ページ）
- tar または類似のツールを使用したすべての CNRDB のバックアップ （6 ページ）
- データベース リカバリ戦略 （6 ページ）
- リージョン クラスタ データベース問題からの回復 （11 ページ）
- Cisco Prime Network Registrar 実行中のウイルス スキャン （15 ページ）
- データベースのトラブルシューティング （15 ページ）

データベースのバックアップ

Cisco Prime Network Registrar データベースはさまざまなメモリ キャッシングを実行し、いつでもアクティブにすることができるため、サードパーティのシステム バックアップを使用してデータベースを保護することはできません。これらでは、バックアップデータの不整合や、使用できない交換データベースが発生することがあります。

この目的のために、Cisco Prime Network Registrar はシャドウ バックアップ ユーティリティ、**cnr_shadow_backup** を提供します。1 日に 1 回、Cisco Prime Network Registrar は重要なファイルのスナップショットを取ります。このスナップショットは、データベースの一貫性のあるビューであることが保証されています。

推奨

Cisco Prime Network Registrarの 11.0 よりも前のバージョンから 11.0（またはそれ以降）にアップグレードする場合、および DHCPv6 リース（または DHCPv6 リース履歴レコード）の数が多い場合、アップグレード後に DHCPv4 データベースのサイズを減らすために、DHCP データベースのダンプとロード（ cnrdb_util ユーティリティの使用 （20 ページ） を参照）をスケジュールする必要があります。DHCPv6 リース（アクティブ + 履歴）が新しい dhcp6.ndb に移動されるとき、アップグレードによって元の dhcp.ndb データベースのサイズが縮小されること

はなく、元のデータベースのサイズを減らす唯一の方法は、ダンプとロードを実行することです。dhcp6.ndb ファイルのサイズを表示すると（ls コマンドを使用）、減らすことができるデータベースのサイズを推計できます。

関連項目

シンタックスと位置 （2 ページ）

バックアップ戦略 （2 ページ）

データベース リカバリ戦略 （6 ページ）

CNRDB データのバックアップ （4 ページ）

tar または類似のツールを使用したすべての CNRDB のバックアップ （6 ページ）

バックアップからの CNRDB データのリカバリ （9 ページ）

tar または類似のツールを使用したすべての CNRDB のリカバリ （9 ページ）

tar または類似のツールからの単一の CNRDB のリカバリ （10 ページ）

Cisco Prime Network Registrar 実行中のウイルス スキャン （15 ページ）

シンタックスと位置

以下の項の「.../data/db」という表記は、Cisco Prime Network Registrar 製品のデータのロケーションパスのディレクトリを指しています。「.../data」はデータディレクトリを意味し、デフォルトでは /var/nwreg2/{local | regional}/data になっています。

以下の項で説明する Cisco Prime Network Registrar データベース ユーティリティプログラムは「.../bin」ディレクトリにあり、フルパス名で実行します。「.../bin/*program*」は bin ディレクトリのプログラムファイルを意味し、デフォルトでは /opt/nwreg2/{local | regional}/usrbin/*program* になっています。

（注） データベースのタイプごとに、承認済みのユーティリティのみを使用してください。

バックアップ戦略

バックアップ戦略には、次のいずれかが含まれます。

CCM を使用して夜間のシャドウバックアップを実行し（自動バックアップ時間の設定 （3 ページ） を参照）、パーマネントバックアップ用にシャドウバックアップを使用してから、明示的なバックアップを実行します。**cnr_shadow_backup** ユーティリティを使用して、バックアップファイル（*.bak DB）をバックアップします。

または

Cisco Prime Network Registrar をシャットダウンし、TAR またはその他同様のツールを使用してバックアップを実行します。

手動バックアップ (cnr_shadow_backup ユーティリティを使用)

cnr_shadow_backup ユーティリティを使用して、次のデータベースをバックアップします。

- **CNRDB databases** - ...data/dhcp、...data/dns/cstdb、...data/dns/rrdb、...data/cdns、...data/leasehist、...data/leasefhist、...data/subnetutil、...data/mcd、...data/replica、および ...data/ccm/ndb
- **スマート ライセンス データベース**：...data/sanosync.data、...data/sapiidsync.data、および ...data/satimeflagsync.data

バックアップ戦略の最も基本的なコンポーネントは、毎日のシャドウバックアップです。運用データベースで問題が発生した場合は、前日のシャドウバックアップに基づいて回復を試みることが必要になる場合があります。したがって、バックアップの成功を妨げる問題を認識し、修正する必要があります。

最も一般的な問題は、ディスク領域の枯渇です。必要なディスク領域を大まかに見積もるには、.../data ディレクトリのサイズを取得し、10 倍します。使用パターン、アプリケーション ミックス、Cisco Prime Network Registrar 自体の負荷などのシステム負荷によって、より大きな容量の予約が使用可能であることが示される場合があります。

将来のリカバリのために、既存のシャドウバックアップを定期的に（テープ、他のディスク、または他のシステムなどに）アーカイブしておく必要があります。

⚠

注意 推奨されるタイプとは異なるタイプのデータベースでユーティリティを使用すると、データベースが破損する可能性があります。示されているユーティリティのみを使用してください。また、運用データベースではデータベース ユーティリティを使用せず、コピーでのみ使用してください。

関連項目

自動バックアップ時間の設定 （3 ページ）

手動バックアップの実行 （4 ページ）

cnr_shadow_backup を使用したサードパーティ製バックアップ プログラムの使用 （4 ページ）

自動バックアップ時間の設定

cnr.conf ファイル（.../conf 内）を編集することによって、自動バックアップを実行する時間を設定できます。**cnr.backup-time** 変数を自動シャドウ バックアップの時間と分に24 時間の *HH*:*MM* 形式で変更して、サーバー エージェントを再起動します。たとえば、次のようなプリセット値があります。

```
cnr.backup-time=23:45
```

（注） **cnr.backup-time** に加えた変更を有効にするには、Cisco Prime Network Registrar を再起動する必要があります。

手動バックアップの実行

cnr_shadow_backup ユーティリティを使用して手動バックアップを開始することもできますが、これにはルート権限が必要です。バックアップを実行するには、プロンプトで **cnr_shadow_backup** コマンドを入力します。

（注） バックアップよりも最新のフェールオーバー パートナーから DHCP データを復元するには、フェールオーバー サーバーからの DHCP データの復元 （23 ページ） を参照してください。

cnr_shadow_backup を使用したサードパーティ製バックアップ プログラムの使用

cnr_shadow_backup が動作している間は、サードパーティのバックアップ プログラムをスケジュールしないようにする必要があります。サードパーティのバックアップ プログラムは、cnr_shadow_backup 操作よりも前または後のいずれかの時刻に実行する必要があります。自動バックアップ時間の設定 （3 ページ） で説明されているように、デフォルトのシャドウ バックアップ時間は毎日 23:45 です。

Cisco Prime Network Registrar の運用データベースのディレクトリとファイルをスキップし、シャドウ コピーのみをバックアップするように、サードパーティのバックアップ プログラムを設定します。

運用ファイルは、バックアップ戦略 （2 ページ） に記載されています。Cisco Prime Network Registrar は、次のディレクトリのロックファイルも保持します。

- Cisco Prime Network Registrar サーバー プロセス - /var/nwreg2/local/temp/np_destiny_trampoline または /var/nwreg2/regional/temp/np_destiny_trampoline

ロック ファイルは再起動時に再作成されます。これらのファイルは、システムの実行中は重要です。メンテナンス プロセス（ウイルススキャンやアーカイブなど）では、一時ディレクトリ、運用データベース ディレクトリ、およびファイルを除外する必要があります。

CNRDB データのバックアップ

CNRDB データベースの場合、**cnr_shadow_backup** ユーティリティは、データベースとすべてのログファイルを、インストールされている Cisco Prime Network Registrar 製品のディレクトリツリー内のセカンダリディレクトリにコピーします。手順は次のとおりです。

- **DHCP**：運用データベースは .../data/dhcp/ndb、.../data/dhcp/ndb6、および .../data/dhcp/clientdb ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは、.../data.bak/dhcp/ndb、.../data.bak/dhcp/ndb6、および..../data.bak/dhcp/clientdb ディレクトリにあります。
- **DNS**：運用データベースは .../data/dns/rrdb ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。重要な運用コンポーネントは、.../data/dns/hadb ディレクトリにある高可用性（HA）DNS であり、ログファイルは .../data/dns/hadb/logs ディレクトリにあります。シャドウコピーは .../data.bak/dns ディレクトリにあります。
- **CCM**：運用データベースは .../data/ccm/ndb、.../data/ccm/rrdb、および .../data/ccm/clientdb ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは .../data.bak/ccm ディレクトリにあります。
- **MCD change log**：運用データベースとログファイルは .../data/mcd/ndb ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。シャドウ コピーは .../data.bak/mcd ディレクトリにあります。変更ログのエントリがない場合、MCD 変更ログ データベースは存在しない可能性があります。また、MCD 変更ログの履歴が除去されたとき、または開始する MCD 変更ログ データがないときにも、データベースは削除されます。
- **Lease history**：運用データベースとログファイルは .../data/leasehist および .../data/lease6hist ディレクトリにあり、データベースログファイルはこれらのディレクトリの logs サブディレクトリにあります。シャドウ コピーは .../data.bak/leasehist および .../data.bak/lease6hist ディレクトリにあります。
- **DHCP utilization**：運用データベースとログファイルは .../data/subnetutil ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。シャドウ コピーは .../data.bak/subnetutil ディレクトリにあります。
- **Replica**：運用データベースとログファイルは .../data/replica ディレクトリにあり、データベースログファイルは logs サブディレクトリにあります。

次の表に、Cisco Prime Network Registrar のデータベースファイルを示します。

表 *1*：データベース ファイル

ディレクトリ	サブディレクトリ	ファイル名
dhcp	.../data/dhcp/ndb	dhcp.ndb
	.../data/dhcp/ndb6	dhcp6.ndb
	.../data/dhcp/clientdb	*.db
dns	.../data/dns/csetdb	dnscset.db
	.../data/dns/hadb	dnsha.db
	.../data/dns/rrdb	*.db

ディレクトリ	サブディレクトリ	ファイル名
ccm	.../data/ccm/clientdb	changelog.db config.db
	.../data/ccm/ndb	*.db
	.../data/ccm/rrdb	changelog.db config.db

ログファイルは、log.0000000001 ー log.9999999999 として示されます。ファイルの番号は、サーバーに対する変更の頻度によって異なります。通常は、少数の番号しかありません。サイトの特定のファイル名拡張子は、データベースが使用される時間の経過とともに変化します。これらのログ ファイルは人間に読める形式ではありません。

tarまたは類似のツールを使用したすべてのCNRDBのバックアップ

ここでは、tar または類似のツールを使用して、すべての Cisco Prime Network Registrar データベースをバックアップする手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。

Cisco Prime Network Registrar が実行している場合、tar または類似のツールを使用してバックアップを実行することはできません。

ステップ 2 data ディレクトリとサブディレクトリ全体をバックアップします。

```
> /var/nwreg2/local/data or /var/nwreg2/regional/data
> /var/nwreg2/local/conf or /var/nwreg2/regional/conf
```

ステップ 3 バックアップが完了したら、Cisco Prime Network Registrarを再起動します。

（注） 技術的には、バックアップには、夜間のシャドウ バックアップが含まれているため、*.bak ディレクトリ（およびそれらのディレクトリのサブディレクトリ）を含める必要はありません。ただし、使用可能なストレージ領域が非常に制限されている場合を除き、シャドウ バックアップを含め、data ディレクトリ（およびサブディレクトリ）全体の完全バックアップを推奨します。

データベース リカバリ戦略

Cisco Prime Network Registrar は CNRDB データベースを使用します。次の表に、バックアップとリカバリが必要な CNRDB データベースのタイプを示します。

表 *2 :* リカバリのための *Cisco Prime Network Registrar* データベース

サブディレクトリ	クラスタ	タイプ	説明
mcd	ローカル	CNRDB	MCD 変更ログ データ。除去されていない MCD 変更ログ履歴がある限り、8.0 以前のデータベースからのアップグレードのためにのみ存在します。
ccm	ローカル、リージョン	CNRDB	中央構成管理データベース。ローカルの一元管理対象のクラスタと SNMP サーバー データを格納します。
dns	ローカル	CNRDB	DNS データベース。ゾーンの状態情報、保護された RR の名前、および DNS サーバーのゾーン設定データを格納します。
cdns	ローカル		DNS データベースをキャッシュしています。最初の DNSSEC ルート トラスト アンカーおよびルート ヒントを格納します。
dhcp[1]	ローカル	CNRDB	DHCP データベース。DHCP サーバーのリース状態データを格納します。
dhcpeventstore	ローカル		Cisco Prime Network Registrar が、LDAP および DHCPv4 DNS アップデートの相互作用など、外部サーバーと対話するために維持するキュー。リカバリは必要ありません。

サブディレクトリ	クラスタ	タイプ	説明
tftp	ローカル		TFTP サーバーのデフォルトのデータディレクトリ。リカバリは必要ありません。
レプリカ	リージョン	CNRDB	ローカルクラスタのレプリカデータを格納します。
lease6hist	リージョン	CNRDB	DHCPv6 リース履歴データベース。
leasehist	リージョン	CNRDB	DHCPv4 リース履歴データベース。
subnetutil	リージョン	CNRDB	DHCP 使用率データベース。サブネットとプレフィックスのデータベースが個別に含まれます。

[1] DHCP データベース（.../data/dhcp/ndb および .../data/dhcp/ndb6）をバックアップから復元することは推奨されません。このデータは、DHCP サーバーの実行中は常に変化するためです（このサーバーまたはパートナーのいずれかでクライアントアクティビティとリースの期限が切れているため）。したがって、バックアップから DHCP ndb/ndb6 データベースを復元すると、サーバーのクロックが元に戻りますが、クライアントのクロックは元に戻りません。そのため、DHCP サーバーのデータベースはバックアップからリカバリするよりも保持する方が望ましく、または、リカバリが必要な場合は、データベースを削除して、フェールオーバーを介してパートナーから現在のリースをリカバリする方が望ましいです（フェールオーバー サーバーからの DHCP データの復元 （23 ページ） を参照）。

Cisco Prime Network Registrarのインストールをリカバリする一般的なアプローチは、次のとおりです。

1. Cisco Prime Network Registrar サーバー エージェントを停止します。
2. データを復元または修復します。
3. サーバー エージェントを再起動します。
4. サーバーでエラーがないかモニターします。

データベースリカバリが正常に実行されたことが確認できたら、常に手動で**cnr_shadow_backup** ユーティリティを実行して、現在の設定と状態のバックアップを作成します。

バックアップからの CNRDB データのリカバリ

サーバー ログ メッセージや欠落しているデータなど、何らかの理由でデータベースの回復に失敗した場合は、現在のシャドウ バックアップ（Cisco Prime Network Registrar のインストール ツリー）でリカバリの試行が必要になることがあります。手順は、次のとおりです。

ステップ 1 Cisco Prime Network Registrar サーバー エージェントを停止します。

ステップ 2 運用データベース ファイルを別の一時的な場所に移動します。

ステップ 3 各 .../data/*name*.bak ディレクトリを .../data/*name* にコピーします。たとえば、.../data/ccm.bak を .../data/ccm にコピーします。

（注） cnr.conf ファイル cnr.dbrecover 変数を false に設定して、cnr_shadow_backup の夜間のバックアップ時のリカバリを無効にした場合は、次の手順の一部として、リカバリも実行する必要があります。

ステップ 4 ファイルの名前を変更します。

CNRDB データベースは一元管理される設定データを維持し、これはサーバー設定データベースと同期されます。

ステップ 5 新しいデータ ディレクトリを作成し、バックアップされたディレクトリを解凍または回復します。

DB ディレクトリとリカバリ ツールを実行して、データベースが正常であることを確認することをお勧めします。

（注） logs サブディレクトリが同じディレクトリに存在するか、または logs パスが DB_CONFIG ファイルに記載されていることを確認します。

ステップ 6 サーバー エージェントを再起動します。

（注） リカバリが失敗した場合は、現在のシャドウ バックアップが単に破損したファイルのコピーである可能性があるため、以前の最新のシャドウ バックアップを使用します。これは、シャドウ バックアップを定期的にアーカイブする必要があることを示しています。以前のシャドウ バックアップ ファイルに動作ログ ファイルを追加することはできません。シャドウ バックアップの作成後にデータベースに追加されたすべてのデータが失われます。

データベースのリカバリが成功したら、**cnr_shadow_backup** ユーティリティを使用して即時バックアップを開始し、ファイルをアーカイブします（手動バックアップの実行 （4 ページ） を参照）。

tar または類似のツールを使用したすべての CNRDB のリカバリ

ここでは、tar または類似のツールを使用して、すべての Cisco Prime Network Registrar データベースを回復する手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。**systemctl stop nwreglocal** を実行して Cisco Prime Network Registrar がダウンしていることを確認します。

ステップ 2 アクティブなデータ ディレクトリの名前を変更します（mv data old-data など）。

（注） データ ディレクトリ（およびそのサブディレクトリ内のすべてのファイル）の 2 倍のサイズに対応できる十分なディスク領域が必要です。十分なディスク領域がない場合は、アクティブなデータ ディレクトリを別のドライブに移動します。

ステップ 3 新しいデータ ディレクトリを作成し、バックアップされたディレクトリを解凍または回復します。

CNRDB ディレクトリとリカバリ ツールを実行して、データベースが正常であることを確認することをお勧めします。

ステップ 4 Cisco Prime Network Registrar を起動します。

（注） 技術的には、復元には、夜間のシャドウバックアップが含まれているため、* .bak ディレクトリ（およびそれらのディレクトリのサブディレクトリ）を含める必要はありません。ただし、使用可能なストレージ領域が非常に制限されている場合を除き、シャドウ バックアップを含むデータ ディレクトリ（およびサブディレクトリ）全体を完全に復元することをお勧めします。

tar または類似のツールからの単一の CNRDB のリカバリ

このセクションでは、tar または類似のツールを使用して単一のデータベースを回復する手順について説明します。

ステップ 1 Cisco Prime Network Registrar をシャットダウンします。**systemctl stop nwreglocal** を実行して Cisco Prime Network Registrar がダウンしていることを確認します。

ステップ 2 アクティブなデータ ディレクトリの名前を変更します（mv data old-data など）。

（注） データ ディレクトリ（およびそのサブディレクトリ内のすべてのファイル）の 2 倍のサイズに対応できる十分なディスク領域が必要です。十分なディスク領域がない場合は、アクティブなデータ ディレクトリを別のドライブに移動します。

ステップ 3 新しいデータ ディレクトリを作成し、そのディレクトリ（およびそのサブディレクトリ）内のファイルのみをバックアップから解凍または回復します。

CNRDB 整合性およびリカバリ ツールを実行して、CNRDB が正常であることを確認することをお勧めします。

ステップ 4 回復する必要があるその他の DB について、**ステップ 2** ~**ステップ 3**を繰り返します。

ステップ 5 Cisco Prime Network Registrar を起動します。

リージョン クラスタ データベース問題からの回復

リージョンクラスタには高可用性ソリューションはありません。リージョンクラスタは、ローカル クラスタの動作にとって重要ではありません（ライセンスを除く）。最悪の事態が発生し、バックアップ（夜間のシャドウ バックアップなど）からの復元が失敗した場合は、リージョン クラスタを再構築できます。

リージョン クラスタ データベースは非常に信頼性が高くなっていますが（トランザクションベースであるため）、いくつかの状況では（たとえば、ディスク領域の不足や、不良ブロックなどの物理ディスク問題）、データベースの問題が発生する可能性があり、CCM が起動できなかったり、特定の機能を実行できないことがあります。

リージョン クラスタでは、主に 4 つのデータベースが使用されます。

- 設定オブジェクトを含む CCM データベース（ccm ディレクトリ）。
- ローカルクラスタから収集されたリース履歴（有効な場合）を含むリース履歴データベース（lease6hist および leasehist）。
- 時間の経過とともに収集されたスコープとプレフィックス使用率の履歴（有効な場合）を含むサブネット使用率データベース（subnetutil）。
- ローカルクラスタから定期的にプルされた設定を含むレプリカ データベース（replica）。

次の項では、これらのデータベースの 1 つ以上で問題が発生した場合に使用する手順について説明します（これは、config_ccm_1_log ファイルとこのファイルで報告されているエラーから判断でき、リージョンの開始不能が含まれている場合もあります）。

（注） これらの手順を実行する前に、データベースのトラブルシューティング （15 ページ） セクションがデータベースの修正に役立つかどうかを最初に確認してください。修正に役立たない場合は、復元できる可能性がある最新のバックアップが使用可能かどうかを確認してください。

リース履歴データベース問題の処理

リース履歴データベースは、データが保存される期間とクライアントアクティビティのレートによっては、非常に大きくなる可能性があります。このデータベースが破損し、復元できない場合、リージョン クラスタ操作を回復する方法の 1 つは、このデータベースを削除することです（これにより、リース履歴が失われます）。

次のステップを実行します。

ステップ 1 リージョン クラスタを停止します。

ステップ 2 Lease6hist および/または leasehist データベース ディレクトリを削除（または名前を変更）します。問題が発生したデータベースのみを削除（または名前変更）します。

（注） これらのデータベースの1つまたは両方を最近のバックアップから復元できた場合は、バックアップ lease6hist および/または leasehist ディレクトリ（およびその下にあるすべてのファイルとディレクトリ）をコピーして、削除された（または名前が変更された）データベースを置き換えることができます。

ステップ 3 リージョン クラスタを起動します。

（注） これらの手順は、リース履歴を収集する必要がなく、すべての履歴を削除したい場合にも使用できます。ステップ 1 を実行する前に、すべてのリース履歴収集を無効にしてください。

サブネット使用率データベース問題の処理

サブネット/プレフィックス使用率のデータベースは、データが保存される期間、ポーリングの頻度、サブネット/プレフィックスの数に応じて非常に大きくなる可能性があります。このデータベースが破損し、復元できない場合、リージョン クラスタ操作を回復する方法の 1 つは、このデータベースを削除することです（これにより、使用率の履歴が失われます）。

次のステップを実行します。

ステップ 1 リージョン クラスタを停止します。

ステップ 2 subnetutil データベース ディレクトリを削除（または名前変更）します。

（注） 最近のバックアップから subnetutil データベースを復元できる場合は、バックアップ subnetutil ディレクトリ（およびその下にあるすべてのファイルとディレクトリ）をコピーして、削除された（または名前が変更された）データベースディレクトリを置き換えることができます。

ステップ 3 リージョン クラスタを起動します。

（注） これらの手順は、使用率データを収集する必要がなくなり、収集したすべてのデータを削除したい場合にも使用できます。ステップ 1 を実行する前に、すべての使用率履歴収集を無効にしてください。

レプリカ使用率データベース問題の処理

レプリカ データベースは、ローカル クラスタから簡単に再作成できます（各ローカル クラスタの設定のコピーを保存するため）。このデータベースが破損している場合は、このデータベースを削除するのが最善の方法です。

次のステップを実行します。

ステップ 1 リージョン クラスタを停止します。

ステップ 2 レプリカ データベース ディレクトリを削除（または名前を変更）します。

（注） このデータベースは、ローカル クラスタから簡単に再構築できるため、バックアップから復元しないことをお勧めします。

ステップ 3 リージョン クラスタを起動します。

ステップ 4 各ローカル クラスタからレプリカ データのプルを開始します（これは数時間以内にローカル クラスタごとに自動的に行われるため、発生するまで待機することもできます）。

リージョン クラスタがローカル クラスタと一致することを保証するために、通常、レプリカ データベースが更新されたら、（DHCP を使用している場合は）（IPv4 および IPv6）アドレス空間とゾーン データをプルすることをお勧めします。

リージョンクラスタの再構築

ccmデータベースが破損しており、バックアップからのリカバリが不可能である場合や、インデックスの再構築（rebuild_indexes ツールの詳細については、Cisco Technical Assistance Center（TAC）に連絡してください）では問題を解決できない場合は、リージョンを完全に再構築しなければならないことがあります。場合によっては、新しいシステムにリージョン クラスタを再構築する必要がある場合があります。

既存のリージョン クラスタが動作している場合は、設定データを抽出できる可能性があります。ただし、これは、古いデータや破損したデータを抽出する可能性もあるため、問題です（データベースの破損によっては、同じデータのエクスポートが繰り返される場合もあります）。これを行うには、cnr_exim ツールを実行して、バイナリ モードで設定をエクスポートします（**-x** オプションを使用します）。成功した場合は、後でインポートすることができます。ただし、すべてのデータがインポートされるわけではないため、次の手順に従うことが重要です。

新しいシステムの場合は、次のようになります。

ステップ 1 Cisco Prime Network Registrar リージョン クラスタをインストールします。

ステップ 2 管理者アカウントをセットアップし、ライセンスを追加します。

ステップ 3 すべてのローカル クラスタをリージョンに登録します。このためには、**license register**コマンドを発行する必要があります。リージョンのアドレスとポートが変更されていない場合は、リージョン サーバーのアドレスとポートを指定する必要はありません。

ステップ 4 古いリージョン クラスタからデータをエクスポートするためにcnr_exim を使用した場合は、cnr_exim を使用してこれをインポートできます。

ステップ 5 「既存のリージョン クラスタ」の手順をスキップして、以下の「共通の手順」に進みます。

既存のリージョン クラスタの場合は、次のようになります。

ステップ 1 リージョン クラスタが実行している場合は、停止します。

ステップ 2 /Var/nwreg2/regional/data ディレクトリ（その下のすべてのファイルとディレクトリ）を削除します。

（注） lease6hist、leasehist、および/または subnetutil ディレクトリ（およびこれらのディレクトリのすべてのファイル）が破損していず、この履歴情報を保持する場合は、これらのデータベースを保持できます。削除すると、この履歴データは失われます。

（注） ccm データベースが削除された場合、そのデータは使用できないため、レプリカデータベースを保持しておかないでください。レプリカ データベースを削除しないと、重大な問題が発生する可能性があります。

ステップ 3 空の /var/nwreg2/regional/data ディレクトリを作成します（完全に削除または移動した場合）。

ステップ 4 リージョン クラスタを起動します。

ステップ 5 管理者アカウントをセットアップし、ライセンスを追加します。

ステップ 6 古いリージョン クラスタからデータをエクスポートするためにcnr_exim を使用した場合は、cnr_exim を使用してこれをインポートできます。

ステップ 7 リージョン クラスタを再起動します（すべてのサービスが実行されていることを保証するために必要です）。

ステップ 8 すべてのローカル クラスタをリージョンに再登録します。このためには、**license register** コマンドを発行する必要があります（これは、ローカルサーバー、IP アドレス、およびポートの既存のリージョン情報に再登録されるため、追加のパラメータは必要ありません）。

ステップ 9 次の共通の手順に進みます。

共通の手順（新規または既存のリージョン クラスタの場合）:

ステップ 1 すべてのレプリカ データが最新であることを確認します。このためには、ローカル クラスタごとに（Web UI で、または **cluster** *name* **updateReplicaData** コマンドを使用して）レプリカをプルします。

ステップ 2 DHCP を使用している場合は、v4 および v6 アドレス空間をプルします（Web UI で、または **ccm pullAddressSpace** および **ccm pullIPv6AddressSpace** コマンドを使用して）。

ステップ 3 DNS を使用している場合は、ゾーン データをプルします（Web UI で、または **ccm pullZoneData** コマンドを使用して）。

ステップ 4 この情報を持つローカル クラスタの 1 つから、適切な管理者またはその他のオブジェクト（ポリシー、テンプレートなど）をプルします（Web UI で、または **pull** サブコマンドを使用して）。

Cisco Prime Network Registrar 実行中のウイルス スキャン

システムでウイルス スキャンが有効になっている場合は、特定の Cisco Prime Network Registrar ディレクトリをスキャン対象から除外するように設定することをお勧めします。これらのディレクトリを含めると、Cisco Prime Network Registrar の動作が妨げられる可能性があります。除外できるのは、.../data、.../logs、および .../temp ディレクトリとそのサブディレクトリです。

データベースのトラブルシューティング

以下のセクションでは、Cisco Prime Network Registrar データベースのトラブルシューティングについて説明します。

関連項目

cnr_exim データ インポートおよびエクスポート ツールの使用 （15 ページ）

cnrdb_recover ユーティリティの使用 （18 ページ）

cnrdb_verify ユーティリティの使用 （19 ページ）

cnrdb_checkpoint ユーティリティの使用 （20 ページ）

cnrdb_util ユーティリティの使用 （20 ページ）

フェールオーバー サーバーからの DHCP データの復元 （23 ページ）

cnr_exim データ インポートおよびエクスポート ツールの使用

cnr_exim データのインポートおよびエクスポートツールは、特定のテナントに制限されていないユーザーについて、次をサポートするようになりました。

- すべてのデータのエクスポート
- コア データがあるかどうかにかかわらず、テナントに固有のデータのエクスポート
- ライセンス関連データのエクスポートとインポート
- すべてのデータのインポート
- テナントに固有のデータのインポートと、オプションで、コア データの有無にかかわらず、新しいテナントへのマッピング。これにより、新しいテナントの基本設定を作成できます。テナント タグを指定すると、インポートしたデータを使用して古いテナント ID が検索され、現在の設定が新しいテナント ID の検索に使用されます。

マルチテナントアーキテクチャの使用には、テナントの設定を別のクラスタに移動して、テナント テンプレート データをエクスポートし、そのデータを別のテナントとしてインポートできるという利点があります。

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

cnr_exim ツールは、保護されていないリソースレコードの情報をエクスポートするためにも機能します。ただし、**cnr_exim** は既存のデータに上書きするだけで、競合の解決を試行しません。

（注） Cisco Prime Network Registrar の別のバージョンにデータをインポートまたはエクスポートするために **cnr_exim** ツールを使用することはできません。これは、Cisco Prime Network Registrar の同じバージョンからのデータのインポートまたはエクスポートにのみ使用できます。

cnr_exim を使用する前に CLI を終了してから、*install-path*/usrbin ディレクトリでツールを見つけます。

インポートされたデータをアクティブにするには、サーバーをリロードする必要があります。

テキストのエクスポートは読み取り専用であることに注意してください。再インポートすることはできません。

テキストのエクスポートでは、ユーザー名とパスワードの入力が求められます（クラスタはデフォルトでローカル クラスタになります）。構文は、次のとおりです。

```
> cnr_exim -e exportfile [-N username -P password -C cluster]
```

（インポート可能な）raw データをエクスポート するには、**–x** オプションを使用します。

```
> cnr_exim -e exportfile -x
```

DNS サーバーおよびゾーン コンポーネントをバイナリ データとして raw 形式でエクスポートするには、**–x** および **–c** オプションを使用します。

```
> cnr_exim -e exportfile -x -c "dnsserver,zone"
```

データ インポートの構文は、次のとおりです（インポート ファイルは raw 形式である必要があります）。

```
> cnr_exim -i importfile [-N username -P password -C cluster]
```

また、**–o** オプションを使用して、既存のデータに上書きすることもできます。

```
> cnr_exim -i importfile -o
```

次の表では、**cnr_exim** ツールのすべての修飾オプションについて説明します。

表 *3 : cnr_exim* オプション

オプション	説明
–a	保護された、または保護されていない RR のエクスポートとインポートを許可します。有効な値は、次のとおりです。 **protectedRR**、 **unprotectedRR**、および **none** **Export**： デフォルトではすべての RR がエクスポートされるため、オプション「-a protectedRR」、「-a unprotectedRR」、または「-a none」を使用して、保護された RR または保護されていない RR のエクスポートを明示的に指定する必要があります。このオプションが指定されなかった場合は、すべての RR がエクスポートされます。 **Import:** デフォルトではすべての RR がインポートされるため、オプション「-a protectedRR」または「-a unprotectedRR」を使用して、保護された RR または保護されていない RR のインポートを明示的に指定する必要があります。このオプションが指定されなかった場合は、すべての RR がインポートされます。
–b	コア（基本）オブジェクトをインポート/エクスポートに含めることを指定します。これには、明示的な *tenant-id* が 0 であるすべてのオブジェクトと、*tenant-id* 属性を持たないすべてのオブジェクトが含まれます。
–c	Cisco Prime Network Registrar コンポーネントを、引用符で囲まれたカンマ区切りの文字列としてインポートまたはエクスポートします。**–c help** を使用して、サポートされているコンポーネントを表示します。デフォルトでは、ユーザーはエクスポートされません。このオプションを使用して明示的にエクスポートする必要があります。ユーザーは、定義されたグループとロールで常にグループ化されます。秘密はエクスポートされません。 （注） 管理者名をインポートした後は、新しいパスワードを設定する必要があります。グループとロールをユーザー名（デフォルトではエクスポートされない）とは別にエクスポートすると、ユーザー名との関係が失われます。
–C クラスタ	指定されたクラスタからインポートまたはエクスポートします。**localhost** に事前設定されています。
–d	cnr_exim ログ ファイルのディレクトリ パスを指定します。
–e *exportfile*	指定されたファイルに設定をエクスポートします。
–f	ソーステナントを指定します。エクスポートおよびインポートについて有効です。

オプション	説明
–g	デスティネーション テナントを指定します。インポートの場合のみ有効です。*tenant-id* は、データをエクスポートするときに変更することはできず、データがインポートされるときにのみ変更できます。
–h	サポートされているオプションのヘルプ テキストを表示します。
–i *importfile*	指定されたファイルに設定をインポートします。インポート ファイルは raw 形式である必要があります。
–N *username*	指定されたユーザー名を使用してインポートまたはエクスポートします。
–o	**–i**（インポート）オプションとともに使用すると、既存のデータに上書きします。
–p *port*	SCP サーバーへの接続に使用されるポート。
–P *password*	指定されたパスワードを使用してインポートまたはエクスポートします。
–t *exportfile*	エクスポート先のファイル名を指定し、データを s 式形式でエクスポートします。
–v	バージョン情報を表示します。
–w	エクスポートするビュータグを指定します。このオプションを使用すると、ユーザーは、「w」オプションで説明されているように、同じビュータグを持つゾーンおよび RR データをエクスポートできます。他のすべてのオブジェクトでは、このオプションは考慮されず、使用されている場合も以前と同じようにエクスポートされます。
–x	**–e**（エクスポート）オプションとともに使用すると、バイナリ データを（インポート可能な）raw 形式でエクスポートします。

cnrdb_recover ユーティリティの使用

cnrdb_recover ユーティリティは、システム障害後に Cisco Prime Network Registrar データベースを一貫した状態に復元するのに役立ちます。通常、このコマンドには **–c** オプションと **–v** オプションを使用します。次の表で、すべての修飾オプションについて説明します。ユーティリティは *install-path*/bin ディレクトリにあります。

表 *4 : cnrdb_recover* オプション

オプション	説明
–c	通常のリカバリではなく、致命的なリカバリを実行します。存在するすべてのログ ファイルを検査するだけでなく、ファイルが欠落している場合は現在または指定されたディレクトリに .ndb（または .db）ファイルを再作成し、存在する場合は更新します。
–e	リカバリの実行後に環境を維持します。ホーム ディレクトリに DB_CONFIG ファイルがない場合は、ほとんど使用されません。
–h *dir*	データベース環境のホーム ディレクトリを指定します。デフォルトでは、現在の作業ディレクトリが使用されます。
–t	可能な最新の日付ではなく、指定された時刻に回復します。時刻の形式は *[[CC]YY]MMDDhhmm[.ss]* です（角カッコは省略可能なエントリを示し、年を省略した場合は、デフォルトで現在の年に設定されます）。
–v	冗長モードで実行します。
–V	標準出力にライブラリのバージョン番号を書き込み、終了します。

致命的な障害が発生した場合は、すべてのデータベース ファイルのスナップショットを、スナップショット後に書き込まれたすべてのログ ファイルとともに復元します。致命的でない場合は、障害発生時のシステム ファイルだけが必要です。ログ ファイルが欠落している場合、**cnrdb_recover –c** は欠落しているものを特定して失敗します。その場合は、復元して、リカバリを再度実行する必要があります。

致命的リカバリ オプションを使用することを強く推奨します。このようにして、リカバリ ユーティリティは使用可能なすべてのデータベース ログ ファイルを順に再生します。何らかの理由でログ ファイルが欠落している場合は、リカバリ ユーティリティはエラーを報告します。たとえば、次のログ ファイルのギャップが表示されます。

```
log.0000000001
log.0000000053
```

次のエラーが発生し、TAC ケースを開くことが必要になる場合があります。

```
db_recover: Finding last valid log LSN:file:1 offset 2411756
db_recover: log_get: log.0000000002: No such file or directory
db_recover: DBENV->open: No such for or directory
```

cnrdb_verify ユーティリティの使用

cnrdb_verify ユーティリティは、Cisco Prime Network Registrar データベースの構造を確認するのに役立ちます。このコマンドは、ファイル パラメータを必要とします。このユーティリティは、ファイルを変更しているプログラムが実行していないことがわかっている場合にのみ使用してください。次の表では、すべての修飾オプションについて説明します。ユーティリティは *install-path*/bin ディレクトリにあります。

構文については、コマンドを実行するときの使用方法で説明します。

```
./cnrdb_verify
```

```
usage: cnrdb_verify [-mNoqV] [-b blob_dir] [-h home] [-P password] db_file ...
```

表 *5 : cnrdb_verify* オプション

オプション	説明
–h *home*	データベース環境のホーム ディレクトリを指定します。デフォルトでは、現在の作業ディレクトリが使用されます。
–N	実行中の共有リージョンロックの取得を防止します。これは、エラーのデバッグのみを目的としているため、他の状況では使用しないでください。
–o	データベースのソートまたはハッシュの順序を無視して、デフォルト以外の比較またはハッシュ設定で **cnrdb_verify** を使用できるようにします。
–P *password*	ユーザーパスワード（ファイルが保護されている場合）。
–q	終了の成功または失敗以外のエラー説明の表示を抑制します。
–V	標準出力にライブラリのバージョン番号を書き込み、終了します。

cnrdb_checkpoint ユーティリティの使用

cnrdb_checkpoint ユーティリティは、データベース ファイルのチェックポイントを設定して、最新の状態に保つのに役立ちます。ユーティリティは *install-path*/bin ディレクトリにあります。

構文については、コマンドを実行するときの使用方法で説明します。

```
./cnrdb_checkpoint
```

```
usage: cnrdb_checkpoint [-1Vv] [-h home] [-k kbytes] [-L file] [-m msg_pfx] [-P
password][-p min]
```

cnrdb_util ユーティリティの使用

cnrdb_util ユーティリティは、Cisco Prime Network Registrar データベースのダンプとロードに役立ちます。さらに、このユーティリティを使用して、Cisco Prime Network Registrar データベースのシャドウバックアップとリカバリを実行したり、ログファイルをクリアしたり、データベースのページサイズを変更したりすることができます。

このユーティリティは *install-path*/usrbin ディレクトリにあります。

重要 Cisco Prime Network Registrar データベースで操作を実行する前に、バックアップを実行することを強くお勧めします。既存のバックアップ ファイルが保持される場合は、それらもバックアップする必要があります。

cnrdb_util ユーティリティは、次の 2 つのモードで動作します。

- **インタラクティブモード** - ユーザーに操作とオプションを求めるプロンプトを表示します。
- **バッチモード** - このユーティリティの実行中に、引数として情報（操作とオプションの両方）が必要です。

構文については、コマンドを実行するときの使用方法で説明します。

```
./cnrdb_util -h
```

次の表では、すべての修飾操作とオプションについて説明します。

表 *6 : cnrdb_util* の操作

操作	説明
-d	1 つまたはすべての Cisco Prime Network Registrar データベースをダンプします。
–l	1 つまたはすべての Cisco Prime Network Registrar データベースをロードします。
–b	すべての Cisco Prime Network Registrar データベースのシャドウバックアップを作成します。
-r	シャドウバックアップから 1 つまたはすべての Cisco Prime Network Registrar データベースを復元します。
–c	1 つまたはすべての Cisco Prime Network Registrar データベース内の sleepycat ログファイルをクリーンアップします。
–h	サポートされているオプションのヘルプ テキストを表示します。

重要 一度に実行できる操作は 1 つだけです。

表 *7: cnrdb_util* のオプション

オプション	説明
-m { local | regional }	Cisco Prime Network Registrar のインストール モードを指定します。指定されていない場合、この情報は cnr.conf ファイルから読み取られます。ファイルが見つからない場合は、デフォルトでローカル モードが使用されます。
-prog *path*	ダンプ、ロード、またはシャドウ バックアップ実行可能ファイルのパスを指定します。指定しない場合は、Cisco Prime Network Registrar のインストールパスから取得されます。
-db *db-path*	ダンプ、ロード、またはシャドウ バックアップ実行可能ファイルのパスを指定します。指定しない場合は、Cisco Prime Network Registrar のインストールパスから取得されます。
-db_pagesize *number*	新しいデータベースを作成するときに使用するデータベース ページのサイズ（バイト数）を指定します。 最小ページ サイズは 512 バイトであり、最大ページ サイズは 64K バイトであり、2 の累乗にする必要があります。ページ サイズが指定されていない場合、ページ サイズは、基盤となるファイル システムの I/O ブロック サイズに基づいて選択されます。（この方法で選択されるページ サイズは、512 バイトを下限とし、16K バイトを上限とします）。 通常、デフォルトは適切です。ただし、大きなページ サイズはパフォーマンスが良好でない可能性があります。通常、4096 と 8192 は良好なサイズです。**cnrdb_stat** ユーティリティを使用して、データベースのページ サイズを決定できます。

オプション	説明
-n { ccm | dhcp | dns | mcd | leasehist | lease6hist | replica | subnetutil | all }	「-d」ダンプ、「-l」ロード、または「-r」リカバリ操作のソース データベースの名前を指定します。指定しない場合、操作はデータベース パスに存在するすべてのデータベースに対して実行されます。このオプションは、「-b」バックアップ操作には適用されません。 • ローカル モードの有効なデータベース名は {ccm | dhcp | dns | mcd | all} です。 • リージョン モードの有効なデータベース名は { ccm | dns | leasehist | lease6hist | replica | subnetutil | all } です。
-s	実行している場合、Cisco Prime Network Registrar サーバーエージェントの停止を試みることを指定します。
-out *path*	出力ファイルのデスティネーション パスを指定します。指定しない場合は、ソース db パスが使用されます。このオプションは、「-b」バックアップおよび「-c」クリーンアップ操作には適用されません。

重要 ソースとターゲットのディレクトリが同じ場合、ダンプおよびロード操作は、ターゲット ファイルが作成されると、ソース ファイルを削除します。これは、ダンプ/ロード操作が実行されて、大きなデータベース ファイルの未使用領域を再キャプチャする際のディスク領域の要件を最小限に抑えるために行われます。

（注） ダンプ操作は、「.dbdump」を付加したデータベース ファイル名を使用して、各データベースを指定された場所のファイルにダンプします。ロード操作は、*. dbdump ファイルが見つかった場合にのみデータベース ファイルをロードします。データベース ファイルの名前は、「.dbdump」のない名前です。

フェールオーバー サーバーからの DHCP データの復元

フェールオーバー サーバーから、シャドウ バックアップの結果よりも新しい DHCP データを復元できます。フェールオーバー パートナーの設定が同期されていることを確認します。また、不正なフェールオーバーパートナー（つまり、データベースが不良なパートナー）で次の手順が実行され、復元する必要があることを確認します。

1. サーバー エージェントを停止します。

   ```
   systemctl stop nwreglocal
   ```

2. 実行中のプロセスを確認します。

   ```
   /opt/nwreg2/local/usrbin/cnr_status
   ```

3. 残りのプロセスをキルします。

   ```
   kill -9 pid
   ```

4. eventstore、ndb、および logs ディレクトリを削除します。

   ```
   rm /var/nwreg2/data/dhcpeventstore/*.*

   rm -r /var/nwreg2/data/dhcp/ndb/
   rm -r /var/nwreg2/data/dhcp/ndb6/
   ```

   警告 いずれかの DHCP データベースを削除する場合は、両方を削除する必要があります。DHCPv4（data/dhcp/ndb）または DHCPv6（data/dhcp/ndb6）リースデータベース。1 つだけ削除して、もう 1 つをそのままにしておくことはサポートされず、予期しない結果が生じる可能性があります。

5. サーバー エージェントを再起動します。

   ```
   systemctl start nwreglocal
   ```