DHCP フェールオーバーの管理

Cisco Prime Network レジストラーフェールオーバープロトコルは、何らかの理由でメインサーバーがオフラインになった場合に、バックアップDHCPサーバーが引き継がれるように設計されています。8.2より前のバージョンでは、このプロトコルはUDPベースで、IPv4経由でのみ動作し、DHCPv4のみをサポートしていました。8.2以降、このプロトコルはTCPベースで、IPv4またはIPv6のいずれかを使用するように構成でき、単一の接続でDHCPv4とDHCPv6の両方をサポートします。DHCPサーバーは、両方を使用するように構成されている場合、IPv4とIPv6の両方のトランスポートを試行し、最初に起動した接続を使用します。DHCPフェールオーバーでは、次の機能がサポートされています。

- DHCPv4アドレス
- DHCPv6アドレス(非一時および一時)
- DHCPv6プレフィックス委任

DHCPフェールオーバーは、DHCPv4サブネット割り当て(オンデマンドアドレスプール)には適用されません。

DHCP フェールオーバーの仕組み

DHCPフェールオーバーは、サーバーとパートナーの関係に基づいています。パートナーは、サーバーと同じ DHCPv4 スコープ、DHCPv6 プレフィックス、DHCPv6 リンク、予約、ポリシー、およびクライアントクラスを持つ必要があります。サーバーが起動すると、サーバーは互いに連絡を取ります。メインサーバーは、パートナーに DHCPv4 アドレスと DHCPv6 委任接頭部を提供し、そのパートナーをクライアント操作ごとに更新します。メインサーバーに障害が発生した場合、パートナーは、DHCPv4アドレスとDHCPv6委任プレフィックスを使用して、リースの提供と更新を引き継ぎます。メイン・サーバーが再び稼働可能になると、管理者の介入なしにパートナーと再統合されます。これらのサーバーは、フェールオーバー ペアと呼ばれる関係にあります。

次の場合、フェールオーバー プロトコルは DHCP を動作可能にします。

- **The main —server メイン**サーバーがダウンしている間に、パートナーが**fails**サービスを引き継ぎます。パートナーを更新する前にメイン サーバーで障害が発生した場合でも、サーバーは重複するアドレスを生成できません。
- **Communication**—パートナーは、相手サーバーか、またはパートナーとの通信で障害が発生したのかを判断できない場合でも、正しく動作**fails**できます。サーバーは、両方とも実行されていて、それぞれがクライアントのサブセットとしか通信できない場合でも、重複するアドレスを発行することはできません。

フェールオーバー ペアを構成した後:

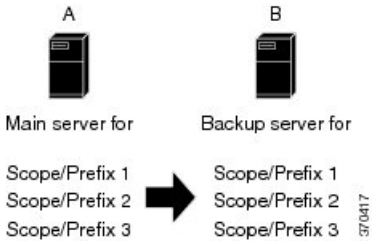
1. パートナーは接続します。
2. メイン サーバーは、既存のすべてのリースに関するデータをパートナーに提供します。
3. バックアップ サーバーは、メイン サーバーからバックアップ アドレスのプールを要求します。
4. メインサーバーは、各スコープまたはプレフィックスからパートナーに使用可能なアドレスの割合で応答します。
5. バックアップサーバーは、メインサーバーがダウンしているか、またはフェールオーバーペアの負荷分散が有効になっていると感じなければ、すべてのDHCPDISCOVER要求と送信要求要求を無視します。通常の操作では、バックアップサーバーは一部の更新要求と再バインド要求のみを処理します。
6. メイン サーバーは、すべてのクライアント操作の結果でパートナーを更新します。

フェールオーバーペアのサーバーの構成は自動的に同期化できます。2つのサーバーは、使用可能なリースの再調整を動的に行います。メインサーバーが利用可能なリースの大部分を引き渡す場合、パートナーからリースを回収できます。

DHCP シンプル フェールオーバー

Cisco プライムネットワーク レジストラーは、単純なフェールオーバー設定のみをサポートします。単純なフェールオーバーには、1 つのメイン サーバーと 1 つのバックアップ サーバーのペアが含まれます (下の図を参照)。この例では、メイン サーバー A には 3 つのスコープまたはプレフィックスがあり、バックアップ サーバー B で同じように構成する必要があります。

図 *1 :* 単純なフェールオーバーの例



DHCPv6 フェールオーバー

DHCPv6 フェイルオーバーは、DHCPv4 の単純なフェイルオーバー構成と非常によく似ています。DHCPv6 フェールオーバーパートナーは、ステートフルアドレスと委任されたプレフィックスリースで相互に更新を行い、通信が復元されたときに同期を実行し、一般的に DHCPv4 フェールオーバープロトコルの要件に従い、遵守します（ただし、DHCPv6 フェールオーバーパートナーは、ステートフルアドレスと委任されたプレフィックスリースを保持します）。

最大クライアント リード タイム (MCLT) とリース時間の制限は DHCPv6 リースに適用され、有効な有効期間と優先リースの有効期間は、フェールオーバー ペアに定義された MCLT に制限されます。フェールオーバーペアで許可される最長のリース時間が、構成された優先有効期間を超え、構成された優先有効期間が構成された有効な有効期間よりも短い場合にのみ、優先ライフタイムと有効なリースの有効期間が異なる場合があります。委任されたプレフィックスは、DHCPv4 アドレスと同様に管理され、バランスが取れています。

最も大きな違いは、DHCPv6 フェールオーバー サーバーが各プレフィックスで使用可能なアドレスのバランスを取らず、アルゴリズムを使用して各サーバーがリースできる新しいアドレスを決定することです。アルゴリズムはアドレスの最下位ビットを使用し、メインサーバーは奇数アドレスを割り当てますが、バックアップサーバーは偶数アドレスを割り当てます。これは、クライアントが要求し、ランダムに生成されたアドレスに適用され、次の場合は適用されません。

- リースは既にクライアントに割り当てられています。
- クライアントに予約が存在します。
- 割り当てアルゴリズムのインターフェイス識別子が設定され、使用されます。この場合、インターフェイス識別子(EUI-64)ビットは一意であると想定され、グローバル ビットが設定されると、これらのアドレスはグローバル ビットが設定されていないのでランダムに生成されたアドレスと競合しません。

- クライアント予約はプレフィックスで構成されます。
- 拡張機能はアドレスを提供します。

フェールオーバー サーバー ペアの設定

ローカル クラスターとリージョン クラスターでフェールオーバー ペアを作成および同期できます。

フェールオーバーペアには、構成とサーバーが保持する状態情報という2つの主要な要素があります。主要な構成属性は、フェールオーバーペアの名前、ローカルサーバーの役割(メインまたはバックアップ)、およびパートナーのアドレスです。フェールオーバー状態は、サーバーを再ロードし、サーバーが起動時にこの状態データを処理するときに定義されます。

（注） Cisco プライム ネットワーク レジストラー 8.2 以降の DHCP フェールオーバーは、Cisco Prime ネットワーク レジストラー 8.1 以前のリリースの DHCP フェールオーバーと相互運用されません。メインサーバーとバックアップサーバの両方を同じメンテナンス期間内にアップグレードする必要があります。

フェールオーバー ペアの追加

メイン サーバーとバックアップ サーバーのクラスタに基づいて、DHCP フェールオーバー ペアを作成します。次に、フェールオーバー ペアの構成を同期して、スコープ、プレフィックス、ポリシー、およびその他の DHCP プロパティがサーバー間で一致するようにします。

フェールオーバー ペアを追加するには、次の手順を実行します。

ローカルおよびリージョン Web UI

ステップ 1 **Deploy**メニューから、**FailoverPairsDHCP**サブメニューの下で選択し、「DHCP フェイルオーバー・ペアのリスト/追加」ページを開きます。

ステップ 2 [フェールオーバー ペア] ペインの**Pair**アイコンをクリックします。 **Add Failover**

ステップ 3 [DHCP フェールオーバー ペアの追加] ダイアログ ボックスで、フェールオーバー ペア名を追加します。

これは必須であり、任意の区別名を指定できます。（フェールオーバー ペア名の変更 （31 ページ） を参照）。

ステップ 4 メインの DHCP サーバーのクラスタを選択します。これは、ローカルホストまたはその他の定義されたクラスターです。

ステップ 5 バックアップ DHCP サーバーのクラスタを選択します。これは、メイン サーバー クラスタと同じにすることはできませんが、メイン クラスタが localhost でない場合は localhost にする必要があります。

ステップ 6 [**DHCP フェールオーバー ペアの追加]**をクリックします。フェールオーバー ペアが作成されます。

ステップ 7 クライアントの最大リードタイム*(mclt)*やバックアップ率*(backup-pct)*など、追加の属性を設定できます。ほとんどのデフォルト値は最適化されています。ペアのフェールオーバーを一時的に無効にする場合を除き、既定でフェールオーバー属性を有効のままにします。

メイン クラスタ オブジェクトとバックアップ クラスタ オブジェクトに対して構成されている値を上書きする場合、または特定のトランスポートを無効にする場合は、メイン サーバー属性、バックアップ サーバー属性、メイン*IP6* アドレス属性、またはバックアップ*IP6* アドレス属性を指定できます(0.0.0.0 または 0:0 を指定して)アドレスの場合)。IPv4 アドレスと IPv6 アドレスの両方が使用可能な場合、フェールオーバーは両方のトランスポートで接続を試み、最初に起動した接続を使用します。

また、リレーヘルスチェックの項で属性を設定して、DHCP リレーの状態チェックを構成することもできます（「DHCP リレー ヘルス チェック （48 ページ）」を参照）。

[保存（Save）] をクリックして、これらの変更を保存します。

[DHCPフェールオーバーペアの編集（Edit DHCP Failover Pair）] ページ（詳細モード）では、次の属性を構成できます。

表 *1*: フェールオーバー ペアの属性

属性	説明
Main Server (*main*)	フェールオーバー ペアのメイン サーバーを持つクラスターを識別します。
Backup Server (*backup*)	フェールオーバー ペアのバックアップ サーバーを含むクラスターを識別します。
Scope Template (*scopetemplate*)	スコープ テンプレートを指定したフェールオーバー ペアに関連付けます。
フェールオーバー設定	
failover	フェイルオーバー構成を有効にします。この属性を無効にすると、構成の基本を変更することなく、接続されているサブネットでのフェールオーバーをオフにします。
mclt	クライアントの最大リードタイムを秒単位で設定します。この属性は、クライアント・リースの有効期限を作成できるバックアップ・サーバーの前にどれだけの距離を設定するかを制御します。この値は、メインサーバーとバックアップ サーバーの両方で定義し、両方のサーバーで同じ値を指定する必要があります。

属性	説明
backup-PCt	メイン サーバーがバックアップ サーバーに送信する使用可能なアドレスの割合を制御します。この値をメインサーバーに設定します。バックアップ・サーバーに設定されている場合、(構成のコピーを有効にするために)無視されます。スコープでこの値を明示的に設定し、負荷分散を無効にしない限り、ここで設定した値が既定値になります。
dynamic-bootp-backup-pct	動的BOOTPが有効になっているスコープについて、メイン サーバーがバックアップ サーバーに送信する使用可能なアドレスの割合を決定します。定義されている場合は、メイン サーバーで定義する必要があります。バックアップ・サーバーで定義されている場合、(構成のコピーを有効にするために)無視されます。この値がまったく定義されていない場合、または値が 0 の場合は、代わりに *backup-pct*が使用されます。動的 BOOTP がスコープで有効になっている場合、サーバーは PARTNER-DOWN 状態であっても、他のサーバーで使用可能なアドレスにリースを付与することは決してないので、このパラメーターは「backup-pct」とは別です。. MCLT は動的 BOOTP リースには意味を持ちません。
load-balancing	フェールオーバー ペアでロード バランシング (RFC 3074) が有効かどうかを決定します。デフォルトではディセーブルになっています。有効にすると、バックアップ pct は無視され、メイン サーバーとバックアップ サーバーは、フェールオーバー 関係のすべてのスコープ (つまり、*backup-pct*が 50% で構成されているかのように) に対してクライアントの負荷と使用可能なリースを均等に分割します。

属性	説明
rebind-limit	T1 (リバインド時間) を超えて、通常は要求、書き換え、またはREBIND要求に応答しないフェイルオーバー・パートナーがパートナーの代わりに応答するときに使用するT2 (再バインド時間) の制限を設定します。 ゼロ以外の値に設定すると、クライアントが更新を開始し、フェールオーバーが通常の状態になると、クライアントがフェールオーバー パートナーによってサービスを受けるのに迅速にクライアントを返す速度が速まります。 クライアントは通常、数秒後に更新要求を再送信し、指数バックグラウンド アルゴリズムを使用して再試行するので、再バインド制限の妥当な値は 60 ~ 600 秒の範囲である可能性があります。 **注:**DHCPv6 の場合、サーバーが*server-id*オプションに基づいてサービスを提供する RENEW 要求をドロップすることもあります(フェールオーバーパートナーが操作可能でクライアントにサービスを提供する必要がある場合)。
safe-period	安全期間を秒単位で制御します。メイン サーバーとバックアップサーバーの両方で同じである必要はありません。これは、使用セーフ期間が有効になっている場合にのみ意味を持ちます。
use-safe-period	オペレーター・コマンドを使用せずに、サーバーが PARTNER-DOWN 状態に入ることができるかどうかを制御します。無効にした場合、サーバーはオペレーター・コマンドを指定せずに PARTNER-DOWN に入ることはありません。
リレー ヘルス チェック	
relay-health-check	正常な状態の状態で、正常性チェックが有効かどうか、およびフェールオーバー通信がNORMAL状態の場合にどのプロトコルに対して有効にするかを設定します。無効(デフォルト)、v4のみ、v6のみ、またはその両方に設定できます。
rhc-monitor-first-relay	最も内側の（最初の）リレーまたは最も外側のリレー（DHCP サーバーがメッセージを受信する場所）に基づいて、DHCPv6 トラフィックを監視するかどうかを決定します。最も外側のリレーに基づいてトラフィックを監視することをお勧めします。これにより、監視するリレーの数が減り、メモリ使用量が削減されます。

属性	説明
rhc-unresponsive-time	ヘルスチェックの応答なし時間を秒単位で設定します。これは、このサーバーが通信の問題があると想定して、パートナーに代わって要求に応答する前に、別のサーバー宛の (DHCPv4) DHCPREQUEST または (DHCPv6) 要求パケットを受信できない最小時間です。リレーとそのパートナーの間で。
rhc-request-count	ヘルスチェックパートナーリクエスト数を設定します。これは、(DHCPv4) DHCPDISCOVER または (DHCPv6) このサーバーが通常は応答しないクライアント要求に応答する前に、パートナーが応答できた要求の数です。
rhc-restart-time	ヘルスチェックの再起動時間を秒単位で設定します。この時間の間、パートナーが応答する (DHCPv4) DHCPDISCOVER または (DHCPv6) 要請要求を受信しない場合、監視対象リレーの時間とカウントが再開されます。これは、ヘルスチェックが非常に最近のデータに基づいていることを保証します。
rhc-warning-interval	パートナーとリレー エージェント間の通信に問題がある可能性があるために、サーバーがパートナーに応答する場合に警告メッセージをログに記録する間隔を最小間隔で設定します。
rhc-elapsed-time	パートナーとリレーの間の通信がダウンしていると判断されたときに、サーバーがパートナーに応答するまでに、クライアントが DHCPv4 秒フィールドまたは DHCPv6 経過時間 (8) オプションで報告する必要がある最小時間を設定します。 0 (推奨しない) に設定すると、サーバーはすべての要求に応答します。
rhc-server-preference	フェールオーバー パートナーの代理として要請に応答するときに使用する DHCPv6 サーバーの設定を設定します。サーバー設定オプションが設定されており、rhc-server-preference 値が低い場合にのみ使用されます。

属性	説明
rhc-response-time	ヘルスチェックの応答時間（秒単位）を設定します。これは、このサーバーが（DHCPv4）DHCPDISCOVER または（DHCPv6）パートナーに代わって要請要求に応答する時間です。これは、リレーとそのパートナーとの間に通信の問題があると想定しているためです。これは、クライアントがこのサーバーからのオファーを受け入れ続ける場合に、このサーバーが永久に応答しないようにするためです。 0 に設定すると、このサーバーは、別のサーバー宛ての（DHCPv4）DHCPREQUEST または（DHCPv6）要求パケットを受信するまで、クライアントに応答し続けます。
フェールオーバー サーバーアドレス	
main-server	メイン サーバーのフェールオーバー プロトコルに使用する IPv4 アドレスを制御します。この値が設定されていない場合は、メイン・クラスターに指定されたアドレスが使用されます。Cisco では、サーバーが設定管理およびクライアント要求に対して異なるインターフェイスで設定されている場合にのみ、この値を設定することを推奨します。 この値を 0.0.0.0 に設定すると、フェイルオーバー通信に IPv4 を使用できなくなります。 IPv4 と IPv6 の両方のアドレスが使用可能な場合、サーバーは TCP 接続用の両方のトランスポートを試み、最初に起動した場合はどちらを使用しても使用します。
backup-server	バックアップ サーバーのフェールオーバー プロトコルに使用する IPv4 アドレスを制御します。この値が設定されていない場合は、バックアップ クラスタに指定されたアドレスが使用されます。Cisco では、サーバーが設定管理およびクライアント要求に対して異なるインターフェイスで設定されている場合にのみ、この値を設定することを推奨します。 この値を 0.0.0.0 に設定すると、フェイルオーバー通信に IPv4 を使用できなくなります。 IPv4 と IPv6 の両方のアドレスが使用可能な場合、サーバーは TCP 接続用の両方のトランスポートを試み、最初に起動した場合はどちらを使用しても使用します。

属性	説明
main-ip6address	メイン サーバーのフェールオーバー プロトコルに使用する IPv6 アドレスを制御します。この値が設定されていない場合は、メイン クラスタで指定されているアドレスが使用されます。Cisco では、サーバーが設定管理およびクライアント要求に対して異なるアドレスで設定されている場合にのみ、この値を設定することを推奨します。 この値は 0:0 に設定できますを使用して、フェイルオーバー通信に対する IPv6 の使用を無効にします。 IPv4 アドレスと IPv6 アドレスの両方が利用可能な場合、サーバーは TCP 接続に両方のトランスポートを試行し、先に利用可能なものを使用します。
backup-ip6address	バックアップ サーバーのフェールオーバー プロトコルに使用する IPv6 アドレスを制御します。この値が設定されていない場合は、バックアップ クラスタで指定されているアドレスが使用されます。Cisco では、サーバーが設定管理およびクライアント要求に対して異なるアドレスで設定されている場合にのみ、この値を設定することを推奨します。 この値は 0:0 に設定できますを使用して、フェイルオーバー通信に対する IPv6 の使用を無効にします。 IPv4 アドレスと IPv6 アドレスの両方が利用可能な場合、サーバーは TCP 接続に両方のトランスポートを試行し、先に利用可能なものを使用します。

CLI コマンド

failover-pair *name* **create** *main-cluster/address backup-cluster/address* [*attribute=value ...*] を使用します。次に例を示します。

```
nrcmd> failover-pair example-fo-pair create Example-cluster Boston-cluster
```

関連項目

フェールオーバー チェックリスト （14 ページ）
フェールオーバー ペア名の変更 （31 ページ）
フェールオーバー ペアの同期 （11 ページ）
フェールオーバー サーバーの再起動 （31 ページ）

フェールオーバー ペアの同期

フェールオーバー ペアを作成したら、フェールオーバー ペアの構成を同期する必要があります。

ローカルおよびリージョン Web UI

ステップ 1 **Deploy**メニューから、**FailoverPairsDHCP**サブメニューの下で選択し、「DHCP フェイルオーバー・ペアのリスト/追加」ページを開きます。

ステップ 2 [フェールオーバー] ウィンドウでフェールオーバー ペアを選択します。

ステップ 3 [DHCP フェールオーバー ペアの一覧表示/追加] ページで、[**フェールオーバー ペアの同期]**タブをクリックします。

地域 Web UI での同期については、『 』の「*DHCP* フェールオーバー*Cisco Prime Network Registrar 11.1 Administration Guide*ペアの管理」セクションを参照してください。

ステップ 4 同期の方向を選択します。同期の方向は、メインからバックアップ サーバーへ、またはバックアップからメイン サーバーに行うことができます。

ステップ 5 バックアップ サーバーのオブジェクトを置き換える主なサーバー オブジェクトの程度に応じて、同期操作を選択します。サーバーで実行できる基本的な同期操作を次に示します。

- **Update operation**：これはデフォルトで最も過激な操作です。更新の同期には、バックアップ サーバーの一意のプロパティに対する影響が最も少ないという点で適切です。
- **Complete operation**：この操作は、すべての初期同期に適しています。バックアップ サーバーの一意のプロパティの多くはそのまま維持しながら、更新操作よりも完全です。
- **Exact operation**：この操作は、単純なフェイルオーバー構成に適しています。

この操作では、一意の DHCP サーバーとバックアップ サーバー上の拡張ポイントを保持しますが、2 つのサーバーは、可能な限り相互のイメージをミラー化します。

（注） 初期フェールオーバー構成の場合は、[完全（Exact）] または [完全（Complete）] 操作を使用します。

オブジェクトのクラスで実行される関数の理解を深めるには、次の例を考えてみます。ここでは、メインサーバーとそのバックアップサーバーと次のオブジェクトがあります。

メインサーバー上	バックアップサーバー上
Name1=A Name2=C	Name2=B Name3=D

（注） この例では、メイン サーバーからバックアップ サーバーへのフェールオーバー同期を検討します。

各操作は、オブジェクトのクラスに対して異なる関数の組み合わせを実行します。選択した操作に基づいてオブジェクトに対して実行される 4 つの関数を次に示します。

- 変更なし:バックアップ サーバーのプロパティまたは値のリストは変更されません。

たとえば、結果は Name2=B、名前 3=D になります。

- ensure：メインサーバーオブジェクトのコピーがバックアップに存在することを確認します。メインサーバー オブジェクトと同じ名前のターゲット サーバー オブジェクトは変更されず、ターゲットサーバー上にないオブジェクトは追加され、ターゲット サーバー上のオブジェクトだけが変更されません。

  たとえば、結果は、名前 1=A、名前 2=B、名前 3=D になります。

- replace：ターゲットサーバーの既存のオブジェクトが、同じ名前のメインサーバーオブジェクトに置き換えられることを確認します。また、ターゲット サーバー上にないオブジェクトも追加され、ターゲットサーバー上のオブジェクトだけが変更されません。唯一の例外は、オプション リストがリスト エントリを比較するために抽出されるポリシーとオプション定義セットです。

  たとえば、結果は、名前 1=A、名前 2=C、名前 3=D になります。

  （注） メインサーバー上のクライアントを削除し、フェールオーバー同期 Update または Complete 操作を実行してバックアップのエントリを削除した後、クライアントはバックアップから削除されません。バックアップのクライアントエントリをメインサーバーから削除した後に、クライアント エントリを削除する唯一のフェールオーバー同期操作は、フェールオーバー同期の正確な操作です。

- exact：メインサーバーオブジェクトの正確なコピーをバックアップサーバーに配置し、一意のものを削除します。つまり、ターゲットサーバーのオブジェクトは、メインサーバーのオブジェクトと同一になります。

  たとえば、結果は Name1=A、名前 2=C になります。

詳細については、次の表を参照してください。この表は、選択した操作（更新、完了、正確）に基づいてオブジェクトに対して実行される機能（変更なし、確認、置換、または正確な操作）に関する情報を提供します。

表 *2:* フェールオーバー ペアの同期関数

データの説明	更新（Update）	完了（Complete）	完全一致（Exact）
DHCP サーバー： クライアントクラス プロパティ クライアント ホスト名処理プロパティ 動的 DNS プロパティ フェールオーバー チューニングのプロパティ	置換	置換	置換
その他のすべてのプロパティ	変更なし	置換	置換
LDAP リモート サーバー	確認	置換	正確な操作

データの説明	更新（Update）	完了（Complete）	完全一致（Exact）
ポリシー： オプション リストのプロパティ パケット ブート ファイルのプロパティ その他のプロパティ	確認 確認 置換	置換 置換 置換	正確な操作 正確な操作 正確な操作
クライアント	正確な操作	正確な操作	正確な操作
クライアントクラス	置換	置換	正確な操作
スコープとスコープの予約	正確な操作	正確な操作	正確な操作
Links	正確な操作	正確な操作	正確な操作
プレフィックスとプレフィックス予約	正確な操作	正確な操作	正確な操作
DNS 更新 コンフィギュレーション	置換	置換	正確な操作
トラップの設定	確認	置換	正確な操作
VPNs	置換	置換	正確な操作
オプション キー（Keys）	置換	置換	正確な操作
拡張子(拡張ファイルをコピーする必要があります。	確認	置換	正確な操作
拡張ポイント	置換	置換	置換
オプションの定義： カスタム オプション リスト ベンダー オプション リスト	確認	置換	正確な操作
DHCP リスナー設定	確認	置換	正確な操作

ステップ 6 [**Report**フェールオーバー ペアの同期] ページをクリックします。

- 同期の方向を選択するオプションと、同期操作の目的のモードをチェックするオプションもあります(**更新**,**完了**,**正確**)。目的の値を確認し、[**レポート**] をクリックします。結果のページには、同期を実行した場合に同期が適用される変更セット エントリが表示されます。[**更新の実行**] をクリックするか、[**戻る**] をクリックして [フェールオーバー ペアの同期] ページに戻ります。

ステップ 7 **Save** をクリックして変更を保存します。

ステップ 8 [DHCP フェールオーバー ペアの一覧/追加] ページで、[**フェールオーバー サーバーの管理**] タブをクリックします。

ステップ 9 [**サーバーの再起動**]アイコンをクリックして、バックアップ サーバーをリロードします。

ステップ 10 リースを取得してみてください。

ステップ 11 [フェールオーバー サーバーの管理] タブで、サーバーの正常性を確認します。また、[**ログ**] タブをクリックして [サーバーのログ] ページのログ エントリを表示し、サーバーが NORMAL フェールオーバー モードになっていることを確認します。ログファイルには、次のような項目が含まれている必要があります。

```
06/19/2003  9:41:19 name/dhcp/1 Info Configuration 0 04092 Failover is enabled server-wide. Main
 server name: '192.168.0.1',
backup server name: '192.168.0.110', mclt = 3600, backup-pct = 10, dynamic-bootp-backup-pct = 0,
 use-safe-period: disabled,
safe-period = 0.
```

CLI コマンド

failover-pair 名前を **sync**使用**update**{ |**complete** |**exact**} [{**メインからバックアップ** |**メインへのバックアップ**}][-**レポートのみ**|-**レポート**]:

```
nrcmd> failover-pair example-fo-pair sync exact main-to-backup -report
```

フェールオーバー チェックリスト

フェールオーバー ペアを作成したら、フェールオーバー サーバーの構成を同期する必要があります。このチェックリストを使用して、有効なフェイルオーバー構成に備えます。

- DHCPv4 スコープ、DHCPv6 プレフィックス、DHCPv6 リンク、予約 (IPv4 および IPv6)、選択タグ、ポリシー、DHCP オプション、IP アドレス、クライアント クラス、動的 DNS 更新、動的 BOOTP、VPN、DHCP 拡張機能、DHCP 拡張、LDAP サーバー、およびアドレスを複製します。単純なフェールオーバー シナリオでフェールオーバー サーバー ペアを同期させることによって、パートナー サーバー上の構成。
- バックアップ サーバーが、メイン サーバーがダウンしている間に妥当な時間のリースを提供できるように、両方のパートナーが十分な範囲のアドレスで構成されていることを確認します。
- BOOTP (DHCP) リレー エージェント (IP ヘルパー) を使用する場合は、すべての BOOTP リレー エージェントが両方のパートナーを指するように構成します。Cisco プライムネットワーク レジストラーでは、この機能は自動的には検出されません。

  BOOTP 構成エラーを検出するには、ライブ テストを実行し、メイン サーバーを定期的にサービス停止にして、バックアップ サーバーが DHCP クライアントで使用できることを確認します。

シナリオに基づいたフェールオーバー パラメータの設定

設定する必要がある詳細なフェールオーバー プロパティを次に示します。

- バックアップの割合（バックアップの割合の設定 （15 ページ）を参照）
- バックアップ割り当ての境界（バックアップ割り当て境界の設定 （30 ページ）を参照）

- 最大クライアントリードタイム（MCLT）（最大クライアント リードタイムの設定 （17 ページ）を参照）
- 安全期間（フェールオーバー セーフ期間を使用して、サーバーを PARTNER-DOWN 状態に移行する （18 ページ）を参照）
- 要求および応答パケットバッファ（DHCP 要求と応答パケット バッファの設定 （21 ページ）を参照）
- ロードバランシング（ロード バランシングの設定 （21 ページ）を参照）

バックアップの割合の設定

ネットワーク パーティションに関係なくフェールオーバー パートナーを動作させ続けるには(両方のサーバーがクライアントと通信できるが、互いに通信できない場合)、単一サーバーのアドレスよりも多くのアドレスを割り当てます。メインサーバーを構成して、各スコープおよびプレフィックスの委任プレフィックスで現在使用可能なアドレスの割合をバックアップサーバーに割り当てます。これにより、これらのアドレスはメインサーバーで使用できなくなります。バックアップ サーバーは、メイン サーバーとの間で話ができず、ダウンしているのかどうかを確認できない場合に、これらのアドレスを使用します。

メイン サーバーがアドレス プールの残高が大幅に不足しているか、サーバーにリースがないことを検出した場合、フェールオーバーペアがNORMAL状態で機能している場合でも、使用可能なリースまたは他の利用可能なリースのプールは再調整されます。フェールオーバーペアはフェールオーバー中に注意深く監視する必要があり、フェールオーバーパートナーが長時間ダウンしている場合は、フェールオーバー パートナーを PARTNER-DOWN 状態に移行するためにオペレーターの介入が必要になる場合があります。

現在使用可能なアドレスの割合は、フェールオーバー ペアまたは DHCPv4 スコープ (CLI の名前**setfailbackup-pct**または**scope**名前**setbackup-pct)failover-pair**に*backup-pct*属性を設定することで設定できます。デフォルトのバックアップの割合は 50 % です。DHCPv6 プレフィックスの委任プレフィックスは、バックアップ pct に対応する 50% に固定されます。

フェールオーバー ペア レベルでバックアップの割合を設定すると、その属性で設定されていないすべてのスコープの値が設定されることに注意してください。ただし、スコープ レベルで設定すると、バックアップの割合はフェールオーバー ペア レベルのバックアップ率よりも優先されます。フェールオーバー**failover-pair**ペア(CLI の名前**enableload-balancing)**に対してロードバランシング属性が有効になっている場合、バックアップの割合は50%に固定され、(フェールオーバー ペアまたはスコープ上の) バックアップパーセンテージ属性は無視されます。

バックアップの割合は、メイン サーバーで障害が発生した場合にバックアップ サーバーが新しいクライアントにサービスを提供し続けることができるように、十分な大きさに設定する必要があります。バックアップの割合は、使用可能なアドレスの数に基づいて計算されます。通常のリース活動の過程でメイン サーバーの使用可能なアドレス プールがそれより低い場合、メイン サーバーは定期的にアドレスを (1 時間に 1 回) 回収するので、拡張停止が予想される場合は、バックアップ率を大きな値に設定しても問題ありません。定義済みの割合。たとえば、バックアップ率が 60% に設定されている場合、メイン サーバーはアドレス プールが 60% を下回るとアドレスを再利用します。

（注） フェールオーバーの負荷分散が有効な場合、メイン サーバーとバックアップ サーバーは、使用可能なリースのバックアップ率を維持するために、使用可能なリースをアクティブに移動します。ロード バランシングの設定 （21 ページ）を参照してください。

割合は、新しいクライアントの到着率とネットワーク オペレータの応答時間によって異なります。新しいDHCPクライアントの到着率とネットワーク管理スタッフの応答時間によって異なります。バックアップ サーバーは、メイン サーバーがダウンしているかどうかを認識できない時間に到着するすべての新しいクライアント要求を満たすのに、各スコープから十分なアドレスを必要とします。PARTNER-DOWN 状態の間でも、バックアップ サーバーは、リースを再割り当てする前に、最大クライアント リード タイム (MCLT) とリース時間の期限が切れるまで待機します。最大クライアント リードタイムの設定 （17 ページ）を参照してください。この時間が経過すると、バックアップサーバーは以下を提供します。

- プライベート プールからのリース。
- メイン サーバー プールからのリース。
- 新しいクライアントに期限切れのリース。

稼働時間内に、オペレーターは、2 時間以内に COMMUNICATIONS-INTERRUPTED 状態に応答して、メイン・サーバーが稼働しているかどうかを判別します。バックアップサーバーは、その2時間の間に到着する可能性のある新しいクライアントの数を適切に上限にサポートするのに十分なアドレスを必要とします。

営業時間外には、未知のクライアントの到着率は低くなる可能性があります。オペレータは通常、同じ状況に対して12時間以内に応答することができます。バックアップサーバーは、その12時間の間に到着する可能性のあるクライアント数の上限を十分にサポートするのに十分なアドレスを必要とします。

バックアップサーバーが単独で制御するアドレスの数は、2つの数値のうち大きい値です。この数値は、各スコープで現在利用可能な(未割り当て)アドレスの割合として表すことができます。クライアント クラスを使用する場合、一部のクライアントでは一部のスコープ セットしか使用できません。

（注） フェールオーバー中に、クライアントは、有効期限が構成されている量よりも短いリースを取得することがあります。これは、サーバー パートナーの同期を維持する通常の部分です。通常、これは最初のリース期間、または通信中断状態の間にのみ発生します。

関連項目

BOOTP バックアップの割合 （47 ページ）

最大クライアント リードタイムの設定

リース期間の調整を制御するフェールオーバーペアのプロパティ、つまりクライアントの最大リードタイム (MCLT) を設定できます。MCLT は、サーバー間の接続が不確実な時間帯に調整します。これは、1 つのサーバーが、最初にパートナーとの長い時間をネゴシエーションせずに、クライアントにリースを許可(または拡張) できる最大時間です。今回は、次の意味があります。

- クライアントは、MCLT の長さのリースのみを最初に (またはパートナーが通信していない場合) 受信することがあります。つまり、フェールオーバーを行わない場合よりも早くリースを更新する必要があります。この更新時に、クライアントは、(パートナーが通信していない場合を除き) 完全なリース時間を取得する必要があります。
- サーバーが PARTNER-DOWN 状態になると、パートナー・ダウン時間の後またはパートナーと通信した最新のリース有効期限が過ぎるまで、MCLTが終了するまで待たなければなりません。パートナーに通知される最新の最小有効期限は、通常、通信が中断される前の最後のクライアント リース要求のリース時間の 1.5 倍です。
- 1 つのパートナーが何をしたか(リース データベースを失ったときなど)について不確定な状態でフェールオーバー回復が発生した場合、パートナーはMCLT期間のリース活動を同期後に制限してから、フェールオーバーを通常の状態に戻す必要があります。操作。

デフォルト MCLT は 1 時間で、ほとんどの構成に最適です。フェールオーバー プロトコルで定義されているように、クライアントに対して指定されたリース期間は、MCLT にフェールオーバーパートナーから受信した最後の潜在的な有効期限を超える期間、または現在の時刻を超える値を超えることはありません。そのため、最初のリース期間は、更新の場合に予想よりも1時間長い場合があります。実際のリース時間は、メインサーバーが復帰したときに再計算されます。

フェールオーバーによる遅延更新の使用のためにMCLTが必要です。遅延更新を使用すると、サーバーはパートナーを更新する前にクライアントにリースを発行または更新し、更新をバッチ処理できます。サーバーがダウンしてリース情報をパートナーに伝えることができない場合、パートナーは、最後に有効期限が何であるかに基づいて、リースを別のクライアントに再提供しようとします。MCLTは、クライアントが更新する機会の追加ウィンドウがあることを保証します。MCLT とリースの提供と更新が機能する方法は次のとおりです。

1. クライアントはDHCPDISCOVERまたはDHCPv6要請をサーバーに送信し、必要なリース期間 (たとえば、3 日間) を要求します。サーバーは、MCLT (既定では 1 時間) の初期リース期間でDHCPOFFERまたはDHCPv6アドバタイズを使用して応答します。クライアントは MCLT リース期間を要求し、サーバーはそれを確認します。
2. サーバーは、パートナーに、クライアントのリース有効期限を含むバインド更新を、現在の時刻とMCLTとして送信します。更新プログラムには、現在の時刻にクライアントが希望する期間に加えて、クライアントの希望期間の半分 (3 +1.5 = 4.5 日) の有効期限が含まれます。パートナーは、潜在的な有効期限を確認し、それによってトランザクションを保証します。
3. クライアントがリースの途中で (100 分) で更新要求を送信すると、サーバーはクライアントの希望するリース期間 (3 日) を確認します。サーバーは、現在の時間に希望のリース期間 (3 日) を加えたリース期限と、潜在的な有効期限 (4.5 日) を持つパートナーを更新します。（**ステップ 2** の説明を参照）。パートナーは、この潜在的な有効期限が 4.5 日である

ことを確認します。このようにして、メインサーバーは、クライアントに常に提供できるように、クライアントリース期間を常に理解して、パートナーにクライアントを導いさせようとします。

MCLTに正しい値はありません。選択にはさまざまな要因の間には明確なトレードオフがあります。ほとんどの人は1時間のプリセット値を効果的に使用し、ほぼすべての環境でうまく機能します。短い MCLT と長い MCLT のトレードオフの一部を次に示します。

- **Short MCLT**—：MCLT 値が短い場合は、PARTNER-DOWN 状態に入った後、サーバーがパートナー IP アドレスを DHCP クライアントに割り当てるまで、少しだけ待つ必要があることを意味します。さらに、リースの期限が切れてから、そのアドレスを別のDHCPクライアントに再割り当てする必要があります。ただし、すべての新しいDHCPクライアントに提供される初期リース間隔が短くなるため、トラフィックが増加します。また、COMMUNICATIONS-INTERRUPTED状態のサーバーが与えることができるリース拡張は、サーバーが望ましいクライアントリース期間の前後にこの状態になった後にのみMCLTです。サーバーがその状態を長期間保持している場合、渡すリースは短くなり、そのサーバーの負荷が増加し、問題が発生する可能性があります。
- **Long MCLT**：MCLT の値が長い場合、初期リース期間が長くなり、COMMUNICATIONS-INTERRUPTED 状態のサーバーがリースを延長できる時間（必要なクライアントリース期間の前後にリースが延長された後）が長くなります。ただし、PARTNER-DOWN 状態になるサーバーは、パートナー アドレスを新しい DHCP クライアントに割り当てる前にMCLTを長く待つ必要があります。これは、この期間をカバーするために追加のアドレスが必要であることを意味する場合があります。また、PARTNER-DOWN 状態のサーバーは、アドレスを別の DHCP クライアントに再割り当てする前に、リースの有効期限が切れるまでMCLTが長くなってから待機する必要があります。

フェールオーバーセーフ期間を使用して、サーバーをPARTNER-DOWN状態に移行する

一方または両方のフェイルオーバー・パートナーが、通信中断状態に移行する可能性があります。この状態の間は、重複するアドレスを発行できません。ただし、サーバーが実行できる処理には制限があるため、長期間にわたってこの状態のサーバーを使用することはお勧めできません。メインサーバーは期限切れのリースを再割り当てできず、バックアップサーバーのプールからアドレスが不足する可能性があります。COMMUNICATIONS-INTERRUPTED 状態は、サーバーが数分から数日の一時的な通信障害を簡単に生き残るために設計されました。クライアントの到着と出発の速度によっては、サーバーがこの状態で短時間だけ効果的に機能する場合があります。その後、サーバーを PARTNER-DOWN 状態に移行して、サーバーが再同期するまでリース機能を完全に引き継ぐようにすることをおお方が良いでしょう。

サーバーが PARTNER-DOWN 状態に移行する方法は 2 つあります。

- **User action**：管理者は、実際の正確な評価に基づいて、サーバーを PARTNER-DOWN 状態に設定します。フェールオーバープロトコルがこれを正しく処理します。両方のパートナーを PARTNER-DOWN に設定しないでください。

- **Failover safe period expires**：サーバーが長時間無人で実行される場合、自動的に PARTNER-DOWN 状態を入力する方法が必要です。

ネットワークオペレータは、サーバーがダウンしているか、通信不能であることをすぐには感知しない場合があります。したがって、COMMUNICATIONS-INTERRUPTED 状態に移行するサーバーに応答する時間をネットワークオペレーターに提供するフェイルオーバーセーフ期間があります。セーフ期間中に、オペレータが両方のサーバーがまだ稼働していることを判断し、実行されている場合は、ネットワーク通信障害を修正するか、安全期間が経過する前にいずれかのサーバーを停止することが唯一の要件です。

セーフ期間の長さはインストールに固有であり、プール内の未割り当てアドレスの数と、アドレスを必要とする未知のクライアントの予想到着率によって異なります。

Cisco Prime Network レジストラー では、フェールオーバーペアに対して *use-safe-period* 属性がデフォルトで有効になり、デフォルトのセーフ期間は4時間です。これにより、フェールオーバー パートナーが 4 時間 COMMUNICATIONS-INTERRUPTED 状態になると、安全期間が過ぎた後に PARTNER-DOWN 状態が自動的に入力されます。この設定がネットワークに適しているかどうかを確認し、ネットワーク要件に基づいてセーフ期間を調整する必要があります。

さらに、この安全な期間中は、どちらのサーバーも既存のクライアントからの更新を許可しますが、重複アドレスを発行する可能性が大きなリスクがあります。これは、一方のサーバーが、もう一方のサーバーが動作中に突然PARTNER-DOWN状態に入る可能性があるためです。この問題を回避するには、使用セーフ期間のデフォルトの設定を変更するか、フェールオーバーペアが互いに接続できなくなると操作担当者に警告する運用手順を策定することが重要です。特に、ネットワーク通信障害が発生した場合、安全期間が経過する前にオペレーターの介入が必要です。いずれかのフェールオーバー サーバーをオフラインにするか、または安全期間の使用属性を両方のサーバーで無効にしてから、安全な期間を過ぎる必要があります。

（注） Cisco プライムネットワーク レジストラーでは、使用セーフ期間がデフォルトで有効になっています。これがネットワークに適しているかどうかを確認し、使用セーフ期間を無効にするか、ネットワーク要件と監視に基づいてセーフ期間を調整する必要があります。

安全期間に必要な追加アドレスの数は、サーバーが検出した新しいクライアントの予想される合計と同じにする必要があります。これは、未処理のリースの合計ではなく、新しいクライアントの到着率に依存します。たとえ短い安全期間しか与えられない場合でも、アドレスの不足や新しいクライアントの到着率が高いため、DHCPが1時間で修正可能な小さな問題を乗り越えることで、実質的に利益を得ることができます。重複アドレス割り当ての可能性が最小限であり、解決された障害後の再統合は自動的に行われ、オペレーターの介入は必要ありません。

フェールオーバー セーフ期間の長さが MCLT の長さを超え、フェールオーバー サーバーが安全な期間のために PARTNER-DOWN 状態になった場合、サーバーはパートナーの他のリースをDHCPクライアントにすぐに割り当て始めることができます。この利点は、サーバーに割り当てる追加のリースが必要です。ただし、ネットワーク通信障害が発生した場合に、安全な期間内にオペレーターの介入が必要になることが欠点です。フェールオーバー サーバーをオフラインにするか、または安全期間の両方で使用セーフ期間属性を無効にしてから、安全な期間が

経過する必要があります。オペレーターの介入がなければ、両方のフェイルオーバー・サーバーは PARTNER-DOWN 状態に移行し、パートナー・アドレスを新規の DHCP クライアントに割り当て始めます。

手動介入を使用するか、PARTNER-DOWN状態に移行するための安全な期間を使用するかを決定するために、従うガイドラインをいくつか示します。

- 企業ポリシーで手動による介入を最小限に抑える場合は、安全期間を設定します。セーフ期間を有効にするには、フェールオーバーペア属性の使用セーフ期間を有効にします。次に、DHCP 属性のセーフ期間を設定して、期間を設定します (デフォルトでは 4 時間)。この期間を十分に長く設定して、運用担当者が通信障害の原因を調査し、パートナーが本当にダウンしていることを確認できるようにします。

- 企業ポリシーがどのような状況でも競合を避ける場合は、明示的なコマンドを使用しない限り、どちらのサーバーも PARTNER-DOWN 状態にしないでください。管理カバレッジがない期間に新しいクライアント到着を処理できるように、バックアップ サーバーに十分なアドレスを割り当てます。パートナーが通信中断フェールオーバー状態の場合は、パートナーが [フェールオーバー サーバーの管理] タブで PARTNER-DOWN を設定できます**Set Partner Down**。この設定は、通信の開始中断属性の値に初期化されます。（通常の Web UI モードでは、この日付を初期化された日付より前の値に設定することはできません。エキスパート Web UI モードでは、この値を任意の日付に設定できます。

  パートナーサーバーの名前を指定して、CLI で **failover-pair name setPartnerDown** 日付を使用します。これにより、コマンドで日時を指定しない限り、パートナーとのフェイルオーバーを実行しているすべてのスコープがただちに PARTNER-DOWN 状態に移行します。この日時は、パートナーが最後に操作可能であることが判明した日時です。

  CLI で**setPartnerDown**を使用し、パートナーが最後に動作することが確認された日時を指定すると、フェールオーバー サーバーは setPartnerDown コマンドで指定された時刻から MCLT を計算します。setPartnerDown コマンドに日付と時刻が指定されていない場合、フェールオーバーサーバーが、COMMUNICATIONS-INTERRUPTED 状態に移行した時点から MCLT が計算されます。ネットワーク通信障害が発生した場合は、パートナーが最後に動作可能であることが判明した実際の時刻を setPartnerDown コマンドで指定することが重要です。そうしないと、重複する IP アドレスが発生する可能性があります。

  日付を指定する場合、次の 2 つの規則があります。

  - *–num* 単位（過去の時刻）は、*num* は 10 進数で、単位は秒、分、時、日、週の場合は *s*、*m*、*h*、*d*、または *w* です。たとえば、3 日間は -3d と指定します。
  - 月（名前またはその最初の 3 文字）、日、時（24 時間表記）、年 （完全に指定された年または最後の 2 桁）。この例では、2002 年 10 月 31 日の午前 12 時にメイン サーバーがダウンしたことをバックアップ サーバーに通知します。

    ```
    nrcmd> failover-pair dhcp2.example.com. setPartnerDown -3d

    nrcmd> failover-pair dhcp2.example.com. setPartnerDown Oct 31 00:00:00 2001
    ```

（注） CLI で日付と時刻を指定する場合は、**nrcmd** プロセスにローカルな時刻を入力します。サーバーがこのプロセスとは異なるタイム ゾーンで実行されている場合は、サーバーが実行されているタイム ゾーンを無視し、代わりにローカル時刻を使用します。

DHCP 要求と応答パケット バッファの設定

DHCP フェールオーバーでは、限られた数のバインド更新を未処理にできます ((エキスパートモードの)*max-unacked-bndupd* フェールオーバー ペア属性を使用して設定します。*max-un-bndupd* のデフォルト値は 1/5(20%)の値の最大-dhcp-requests値、および最低 100 および最大 dhcp 要求です。サーバーは、フェールオーバーに対応するために追加の要求バッファを割り当てます (フェールオーバーに使用できるリソースが必要なため)。

ロード バランシングの設定

通常のフェールオーバー モードでは、フェールオーバー パートナーが NORMAL 通信モードの場合、メイン DHCP サーバーはクライアントにサービスを提供する負担の大部分を担います。メイン サーバーは、すべての新しいクライアント要求に対応するだけでなく、バックアップパートナーからの要求の更新と再バインド、および期限切れのリースを処理する必要があります。単純なフェールオーバー設定シナリオで 2 台のサーバー間で負荷をより均等に分散するために、Cisco Prime Network レジストラーではロード バランシング機能が導入されました(RFC 3074 に基づく)。

フェールオーバー負荷分散により、両方のサーバーがクライアントに対してアクティブにサービスを提供し、両方のサーバーが同じクライアントにサービスを提供するリスクを冒さずに、各サーバーがサービスを提供する一意のクライアントを決定できます。フェールオーバー負荷分散は、サーバーが NORMAL モードの間にのみ適用されます。他の状態では、両方のサーバーがクライアントに応答できます。

RFC 3074 によると、サーバーはクライアント識別子オプションの値またはハードウェア アドレスに基づいて、サーバーが受信する要求ごとにハッシュ値を計算します。ハッシュ値がそのサーバーに割り当てられている場合、要求は処理されます。

フェールオーバー負荷分散が有効な場合、サーバーはクライアントの負荷を均等に分割します。メイン・パートナーはハッシュ値の 50% を処理し、バックアップ・パートナーは残りの 50% を処理します。

フェールオーバー パートナーは、バックアップ サーバーで利用可能なリースのバランスを定期的に調整するか、またはスコープまたはプレフィックスがリースから外れていると検出された直後に行います。

各パートナーは、パートナーが NORMAL モードでない場合は、すべてのクライアントに応答します。各パートナーは、割り当てられたハッシュ値のクライアントからのブロードキャスト DHCPDISCOVER メッセージまたは SOLICIT メッセージにのみ応答します。

ブロードキャスト DHCPREQUEST メッセージまたは REBIND メッセージの場合、サーバーは、(サーバー ID オプションに基づいて) 対象のメッセージである場合にのみ応答します。したがって、対象サーバーがメインサーバーであり、ダウンしている場合、バックアップはクライアントにサービスを提供しません(リースを解放しない限り)。また、ブロードキャストブート、DHCPINFORM、および情報要求要求も負荷分散されます。

フェールオーバー属性である再バインド制限は、クライアントを NORMAL 状態のフェールオーバー パートナーに戻す方法を提供します。再バインド制限値は 60 ~ 600 秒 (1 ~ 10 分) の範囲で設定することをお勧めします。この属性は、T2 (再バインド時間) を制限するために T1 に追加される時間間隔 (更新時間) を指定します。指定すると、フェールオーバー NORMAL 状態でクライアントに応答しなかったフェールオーバー パートナー (要請要求に応答しない) が、要求、書き換え、または REBIND にクライアントに応答すると、次の 2 つのことが発生します。

- T2 (再バインド時間) を T1 (更新時間) にこの属性値を加えた値に設定します。
- フェールオーバーが正常な状態の場合、このサーバーに送信された RENEW 要求には応答しません。

この 2 つのアクションにより、クライアントが更新を開始し、フェールオーバーが正常な状態になると、クライアントは他のパートナーからかなり迅速に処理されます。更新が行われるサーバーは応答せず、クライアントは REBIND 状態にかなり早く入ります (指定された再バインド制限に基づいて)。

ロード バランシングの設定

Web UI で、ペアのフェールオーバー プロパティを設定する場合（フェールオーバー サーバー ペアの設定 （4 ページ）を参照）、フェールオーバーの load-balancing を有効または無効にする必要に応じて、[フェールオーバー設定（Failover Settings）] 属性の *load-balancing* 属性を有効または無効にします。CLIで、**failover-pair** *name* **set load-balancing** を使用します。

（注） 変更を適用するには、メインとバックアップの両方で DHCP サーバーを再起動する必要があります。

DHCP フェールオーバーからの回復

通常どおり稼働している間、フェールオーバー パートナーは状態遷移を行います。フェールオーバー サーバーの 1 つに障害が発生した場合、パートナーはプライベート プールを使用してリースの提供と更新を引き継ぎます。メイン サーバーが再度動作すると、管理者が操作しなくても、パートナーと再統合されます。

次のセクションでは、DHCP フェールオーバーの確認方法、DHCP フェールオーバー イベントの監視方法、サーバーがさまざまな状態になったときの動作、およびサーバーの統合方法について説明します。

フェールオーバーの確認

フェイルオーバーを確認するには、次の手順に従います。

ステップ 1 1 つのサーバーから別のサーバーに ping を実行して、TCP/IP 接続を確認します。両方のサーバーにクライアントを転送するようにルーターが構成されていることを確認します。

ステップ 2 [DHCP サーバーの管理] ページまたは [DHCP フェールオーバー ペアの一覧/追加] ページの [**関連サーバー**]**dhcp getRelatedServers**アイコンをクリックするか、CLI で使用して、サーバーが通常モードであることを確認します。

ステップ 3 起動後、クライアントにリースを取得してもらいます。

ステップ 4 少なくともフェールオーバーの詳細を含むように、メイン サーバーのログ設定を設定します。

ステップ 5 メインサーバーの name_dhcp_1_log ログファイル（in /var/nwreg2/{local | regional}/logs）に、各サーバーからの DHCPBNDACK または DHCPBNDUPD メッセージ（IPv4 の場合）と BNDUPD6 または BNDACK6 メッセージ（IPv6 の場合）が含まれていることを確認します。

ステップ 6 フェールオーバーが正常な状態であるため、バックアップ サーバーがドロップするメッセージがバックアップ サーバーのname_dhcp_1_logログ ファイルに含まれていることを確認します。

ステップ 7 **手順 2** を繰り返します。

関連項目

統合中のステート移行 （26 ページ）

シナリオに基づいたフェールオーバー パラメータの設定 （14 ページ）

DHCP フェールオーバーのモニターリング

メイン・フェイルオーバー・サーバーがダウンすると、バックアップ・サーバーは COMMUNICATIONS-INTERRUPTED 状態に移行します。バックアップ サーバーは、メイン サーバーが停止しているか、バックアップ サーバーと通信できないかを判断できません。停止の性質に応じて、状況をモニターし、以下のステップに従う必要があります。

1. 両方のフェールオーバー サーバーを監視し、メイン サーバーがダウンした場合は直ちに処理を実行します。
2. バックアップ サーバーが最初に引き継いだ時点で、メイン サーバーを操作に戻します。
3. MCLT 内でメイン サーバーを運用できる場合は、これ以上必要はありません。
4. MCLT の期限が切れるまでメイン・サーバーが作動しない場合は、バックアップ・サーバーを PARTNER DOWN 状態に移動します。バックアップ サーバーで、**CLI でフェールオーバー ペア**名 **setPartnerDown** [日付] を使用します。

5. メイン サーバーが動作している場合は、再起動する前にバックアップ サーバーに接続できることを確認します。

詳細については、統合中のステート移行 （26 ページ）を参照してください。

フェールオーバーの状態と遷移

通常の運用中、フェールオーバーパートナーは状態間の移行を行います。状態遷移のすべてのアクションが完了するまで、現在の状態にとどまります。通信が失敗した場合、次の状態の条件が満たされるまで、現在の状態にとどまります。状態とその遷移については、次の「表 3 : フェールオーバーの状態と遷移」で説明します。

表 *3:* フェールオーバーの状態と遷移

状態	サーバーのアクション
STARTUP	パートナーに連絡して状態を確認し、短い時間(通常は数秒)の後に別の状態に移行します。
NORMAL	パートナーと通信できます。メイン サーバーとバックアップ サーバーは、次の状態で動作が異なります。 • メイン サーバーは、プールを使用してすべてのクライアント要求に応答します。パートナーがバックアップ プールを要求すると、メイン サーバーによってバックアップ プールが提供されます。 • バックアップ サーバーは、更新要求と再バインド要求にのみ応答します。メイン サーバーからバックアップ プールを要求します。

状態	サーバーのアクション
COMMUNICATIONS-INTERRUPTED	パートナーと通信できない場合、パートナーと通信している場合でも、そのパートナーとの通信がダウンしている場合でも、パートナーと通信することはできません。接続が失敗して回復したとき、または操作可能と非稼働状態の間でサーバーが循環する場合は、この状態と NORMAL 状態の間を循環します。この間、サーバーは重複するアドレスを提供できません。 この状態の間、通常は、サーバーを介入して PARTNER-DOWN 状態に移行する必要はありません。ただし、これは実用的でない場合もあります。この状態で実行されているサーバーは、使用可能なプールを効率的に使用していません。これにより、サーバーがクライアントに効果的にサービスを提供できる時間を制限できます。 サーバーは、通信中断状態で制限されます。 • 期限切れのアドレスを別のクライアントに再割り当てすることはできません。 • 現在のリース時間を超える最大クライアントリードタイム(MCLT)を超えるリースまたは更新を提供することはできません。MCLT は、バックアップ サーバーが考えているよりもクライアントリースの有効期限がどれくらい前に入っているかを制御する、わずかな追加時間です。 • バックアップ サーバーは、通常は小さなプールしか持っていないので、新しいクライアントにアドレスを使い果たすことができます。 サーバーは、割り当てられたアドレスの数と新しいクライアントの到着率によってのみ制限されます。新しいクライアントの到着率または離職率が高い場合は、サーバーをより迅速に PARTNER-DOWN 状態に移行する必要があります。
PARTNER-DOWN	次のいずれかの事実に基づいて、それが唯一の運用サーバーであるかのように動作します。 • パートナーはシャットダウン中に通知を行いました。 • 管理者は、サーバーを PARTNER-DOWN 状態にします。 • 安全期間が切れ、パートナーは自動的にこの状態に入りました。 この状態では、サーバーは、他のサーバーがまだ動作する可能性があることを無視し、別のクライアントのセットをサービスできます。すべてのアドレスを制御し、リースとエクステンションを提供し、アドレスを再割り当てすることができます。通信中断状態のサーバーに対する同じ制限は適用されません。 どちらのサーバーもこの状態にできますが、サーバーが重複アドレスを発行せず、後で適切に再同期できるように、一度に1つだけが存在する必要があります。それまでは、アドレスは保留中の状態です。

状態	サーバーのアクション
POTENTIAL-CONFLICT	自動再統合を保証せず、パートナーとの再統合を試みている状況である可能性があります。サーバーは、2 つのクライアント (動作していない可能性があります) が提供され、同じアドレスを受け入れたことを判断し、この競合を解決しようとします。
RECOVER	安定したストレージにデータがない、または、その安定ストレージをリフレッシュしようとしている PARTNER-DOWN 状態から回復した後に再統合しようとしています。この状態のメイン サーバーは、リースのサービスをすぐに開始しません。このため、この状態でサーバーを再ロードしないでください。
RECOVER-DONE	RECOVER または PARTNER-DOWN 状態から、または通信中断から通常状態に移行できます。
PAUSED	パートナーに、短時間サービスが切れであることを通知できます。その後、パートナーはCOMMUNICATIONS-INTERRUPTED 状態に移行し、クライアントのサービスを開始します。

統合中のステート移行

通常の運用中、フェールオーバー パートナーは状態間で移行します。状態遷移のすべてのアクションが完了し、通信が失敗した場合は、次の状態の条件が満たされるまで、現在の状態にとどまります。次の表は、サーバーがさまざまな状態に入ったときにどうなるか、およびサーバーが最初に統合して、後で特定の条件下で互いに再統合する方法を示しています。

表 *4:* フェールオーバー状態の移行と統合プロセス

統合	結果
NORMAL 状態で、バックアップ サーバーがメイン サーバーに初めて接続する場合	**1.** 新しく構成されたバックアップ サーバーは、メイン サーバーに接続します。 **2.** バックアップ・サーバーは新しいパートナーであるため、RECOVER状態になり、メインサーバーにバインド要求メッセージを送信します。 **3.** メイン サーバーは、リース状態データベースにリースを含むバインド更新メッセージを返します。 **4.** バックアップ サーバーがこれらのメッセージを確認すると、メイン サーバーは Binding Complete メッセージで応答します。 **5.** バックアップ サーバーは RECOVER-DONE 状態になります。 **6.** 両方のサーバーが NORMAL 状態になります。 **7.** バックアップ サーバーは、プール要求メッセージを送信します。 **8.** メイン・サーバーは、設定されたバックアップ*pct*に基づいて、バックアップ・サーバーに割り当てるリースに応答します。
通信後 -中断状態	**1.** サーバーが再起動し、この状態のパートナーと接続すると、戻りサーバーは同じ状態になり、その後すぐに NORMAL 状態になります。 **2.** パートナーも NORMAL 状態に移行します。
パートナーダウン状態の後	サーバーが復帰して、この状態のパートナーと接続すると、サーバーは、パートナーがこの状態になった時刻とダウンした時刻を比較します。 • サーバーがダウンしたことを検出し、パートナーが次の状態に移行した場合は、次の手順を実行します。 **1.** 戻りサーバーは RECOVER 状態に移行し、更新要求メッセージをパートナーに送信します。 **2.** パートナーは、以前に送信できなかったすべてのバインド データを返し、更新完了メッセージをフォローアップします。 **3.** 戻りサーバーは RECOVER-DONE 状態に移行します。 **4.** 両方のサーバーが NORMAL 状態になります。

統合	結果
	• 戻りサーバーが、パートナーが PARTNER-DOWN 状態になったときに、まだ動作していたことが検出された場合は、次の手順を実行します。 **1.** サーバーは潜在的な競合状態になり、パートナーもこの状態になります。 **2.** メイン サーバーは、バックアップ サーバーに更新要求を送信します。 **3.** バックアップ サーバーは、メイン サーバーに対するすべての未確認の更新に応答し、更新完了メッセージで終了します。 **4.** メインサーバーは NORMAL 状態に移行します。 **5.** バックアップ サーバーは、すべての確認応答されていない更新を要求する更新要求メッセージをメイン サーバーに送信します。 **6.** メイン サーバーはこれらの更新を送信し、更新完了メッセージで終了します。 **7.** バックアップ サーバーが NORMAL 状態になります。
サーバーがリース状態データベースを失った後	通常、戻りサーバーはリース状態データベースを保持します。ただし、致命的な障害や意図的な削除が原因で失われることもあります。 **1.** リース・データベースが欠落しているサーバーが、PARTNER-DOWN 状態または COMMUNICATIONS- INTERRUPTED 状態のパートナーと共に戻ると、サーバーは、そのパートナーが通信したことがあるかどうかを判別します。それがない場合は、データベースを失い、RECOVER 状態に移行し、更新要求メッセージをパートナーに送信します。 **2.** パートナーは、データベース内のすべてのリースに関するバインドデータで応答し、更新完了メッセージをフォローアップします。 **3.** 戻りサーバーは、クライアントの最大リードタイム(MCLT)期間(通常は1時間)を待機し、RECOVER-DONE状態に移行します。MCLT の詳細については、 を最大クライアント リードタイムの設定 （17 ページ）参照してください。 **4.** その後、両方のサーバーが NORMAL 状態になります。

統合	結果
リース状態データベースのバックアップ復元後	戻りサーバーが、そのリース状態データベースをバックアップから復元し、追加のデータを持たないパートナーと再接続する場合、まだ見ていないリースバインドデータのみを要求します。このデータは、期待するデータとは異なる場合があります。 **1.** この場合、バックアップが発生した時刻に設定されたフェールオーバー回復属性を使用して、戻りサーバーを構成する必要があります。 **2.** サーバーは RECOVER 状態に移行し、すべてのパートナー データを要求します。サーバーは、バックアップが実行されてRECOVER-DONE状態になったときからMCLT期間(通常は1時間)を待機します。MCLT の詳細は、「最大クライアント リードタイムの設定 （17 ページ）」を参照してください。 **3.** サーバーが NORMAL 状態に戻ったら、フェールオーバー リカバリ属性を設定解除するか、ゼロに設定する必要があります。 `nrcmd> dhcp set failover-recover=0`
運用サーバーでフェールオーバーが無効になった後	オペレーティング・サーバーでフェイルオーバーが有効になっていたり、無効にされた後に再び使用可能になった場合は、新しく構成されたバックアップ・サーバーを稼働させる際に特別な考慮事項を使用する必要があります。バックアップ サーバーには、リース状態データがなく、フェールオーバー リカバリ属性を現在の時刻から MCLT 間隔 (通常は 1 時間) を引いた値に設定する必要があります。MCLT の詳細は、「最大クライアント リードタイムの設定 （17 ページ）」を参照してください。 **1.** バックアップ サーバーは、メイン サーバーからすべてのリース状態データを要求することを認識します。このテーブルの「サーバーがリース状態データベースを失った後」で説明されているのとは異なり、バックアップ サーバーはメイン サーバーと通信した記録がないため、このデータを自動的に要求できません。 **2.** 再接続後、バックアップ・サーバーは RECOVER 状態になり、すべてのメイン・サーバー・リース・データを要求して、RECOVER-DONE 状態になります。 **3.** 両方のサーバーがNORMAL状態になります。この時点で、バックアップ・サーバーのフェイルオーバー・リカバリ属性を設定解除するか、ゼロに設定する必要があります。 `nrcmd> dhcp set failover-recover=0`

詳細なフェールオーバー属性の設定

設定する必要がある詳細なフェールオーバー プロパティは次のとおりです。

- バックアップ割り当ての境界の設定（バックアップ割り当て境界の設定 （30 ページ）を参照）
- DHCP リースクエリとフェイルオーバー（DHCPLEASEQUERY とフェールオーバー （30 ページ）を参照）

バックアップ割り当て境界の設定

スコープでフェールオーバー バックアップ- バックアップ割り当て境界属性を使用すると、バックアップ サーバーに割り当てるアドレスをより具体的に指定できます。この値として設定された IP アドレスは、バックアップ サーバーにアドレスを割り当てるアドレスの上限です。この境界の下のアドレスのみがバックアップに割り当てられます。この境界の下に使用可能なアドレスがない場合は、その上のアドレスが存在する場合は、バックアップに割り当てられます。実際の割り当てはこのアドレスから下に向かって行われますが、DHCP クライアントの通常の割り当てはスコープ内の最下位アドレスから上に向かって行われます。

スコープにフェールオーバーバックアップ-割り当て-境界を設定する場合は、割り当て先使用可能属性も有効にする必要があります。フェールオーバー-バックアップ- 割り当て - 境界が設定されていないか、ゼロに設定されている場合、使用される境界は、スコープ範囲の最初と最後のアドレスの中間になります。この境界の下に利用可能なアドレスがない場合は、最初に利用可能なアドレスが使用されます。

DHCPLEASEQUERY とフェールオーバー

プライマリサーバーがダウンしたときに DHCP フェールオーバー バックアップ サーバーに送信される DHCPLEASEQUERY メッセージに対応するために、プライマリサーバーは *relay-agent-info*(82) オプション値をパートナーサーバーに通知する必要があります。これを実現するために、プライマリサーバーは DHCP フェールオーバー更新メッセージを使用します。

フェールオーバー サーバー ペアの保守

このセクションでは、フェールオーバー サーバーペアを維持し、次の管理タスクを実行する方法について説明します。

- フェールオーバーペア名の変更（フェールオーバー ペア名の変更 （31 ページ）を参照）
- フェールオーバー サーバーの再起動（フェールオーバー サーバーの再起動 （31 ページ）を参照）

フェールオーバー ペア名の変更

フェールオーバー ペアの古い名前**セット名** =*new-name*を使用して、フェールオーバー ペアの名前を変更します。Web UI では、削除してから新しいオブジェクトを作成する必要があります (新しいオブジェクトが準備ができるまで DHCP サーバーを再ロードせずに削除します)。

（注） フェールオーバー関係のクラスターの役割が変更された場合 (メインからバックアップ、またはメインへのバックアップ)、そのリレーションシップの既存の状態情報は破棄されます。

フェールオーバー サーバーの再起動

フェールオーバー同期を有効にするには、メイン およびバックアップ フェールオーバー サーバーの両方に最初に接続して再起動する必要があります。

ステップ 1 [DHCP フェールオーバー ペアの一覧表示/追加] ページで、[フェールオーバー ペア] ペインでフェールオーバー ペアを選択します。

ステップ 2 メイン サーバーの [フェールオーバー サーバーの管理] タブで、再起動するサーバーを選択します。

ステップ 3 [サービスの再起動（Restart Service）] アイコンをクリックします。

関連項目

フェールオーバーの確認 （23 ページ）

フェールオーバー設定の回復

Cisco Prime Network レジストラーを最新バージョンにアップグレードすると、アップグレードが失敗した場合に備えて、以前のバージョンに戻すことができます。1 つのパートナーをアップグレードし、正常に動作している状態で NORMAL 状態に回復した後、もう一方のパートナーをアップグレードできます。

アップグレード中に作成されたアーカイブから回復できる場合がありますが、メンテナンス期間中にアップグレードがスケジュールされている場合は、次の作業を行う必要があります。

- **systemctl stop nwreglocal** 使用して、Cisco Prime Network Registrar を完全に停止させます。
- Cisco プライムネットワーク レジストラー DATADIR(/var/nwreg2/ローカル/データ)をターボル アップし、安全な場所に保存します。
- サーバーをアップグレードします。

失敗した場合は、次の手順を実行する必要があります。

- **systemctl stop nwreglocal** 使用して、Cisco Prime Network Registrar を完全に停止させます。

- Cisco プライムネットワーク レジストラー DATADIR の破損したバージョンを削除します(場所: /var/nwreg2/ローカル/データ)。
- 保存された Cisco プライムネットワーク レジストラー DATADIR tar ファイルを、そのパスから取得したパスに抽出します。
- 既存の DATADIR を検出して使用する Cisco プライムネットワーク レジストラーの元のバージョンをインストールします。

PARTNER-DOWN状態を使用してフェールオーバーパートナーなしでフェールオーバーサーバーを長時間動作する

一方または両方のフェイルオーバー・パートナーが、通信中断状態に移行する可能性があります。この状態の間は、重複するアドレスを発行できません。ただし、サーバーが実行できる処理には制限があるため、長期間にわたってこの状態のサーバーを使用することはお勧めできません。メインサーバーは期限切れのリースを再割り当てできず、バックアップサーバーのプールからアドレスが不足する可能性があります。COMMUNICATIONS-INTERRUPTED 状態は、サーバーが数分から数日の一時的な通信障害を簡単に生き残るために設計されました。クライアントの到着と出発の速度によっては、サーバーがこの状態で短時間だけ効果的に機能する場合があります。その後、サーバーを PARTNER-DOWN 状態に移行して、サーバーが再同期するまでリース機能を完全に引き継ぐようにすることをおお方が良いでしょう。

サーバーが PARTNER-DOWN 状態に移行する方法は 2 つあります。

- **User action**：管理者は、実際の正確な評価に基づいて、サーバーを PARTNER-DOWN 状態に設定します。フェールオーバープロトコルがこれを正しく処理します。両方のパートナーを PARTNER-DOWN に設定しないでください。
- **Failover safe period expires**：サーバーが長時間無人で実行される場合、自動的に PARTNER-DOWN 状態を入力する方法が必要です。

詳細については、フェールオーバー セーフ期間を使用して、サーバーを PARTNER-DOWN 状態に移行する （18 ページ）を参照してください。

（注） フェールオーバー ペアの 1 つのサーバーが長時間サービスを停止した場合、もう一方のサーバーを PARTNER-DOWN 状態にし、フェールオーバー リレーションシップを構成したままにすることを強くお勧めします。

フェールオーバー 関係を構成解除する代替方法は、サーバー上で動作を維持する場合とほぼ同じ効果を持ちますが、そのサーバーと戻ってくるフェールオーバーパートナーを、リースに影響を与えない作業フェールオーバー リレーションシップに再統合します。状態データは困難であり、不可能な場合があります。

フェールオーバー ペアの 1 台のサーバーがしばらくダウンした場合は、残りの動作中のサーバーを PARTNER-DOWN 状態にする必要があります。運用サーバーのフェールオーバー 関係を解除しないでください。

復帰するフェールオーバー パートナーの再統合

戻りサーバーが、無傷のリース状態データベースを保持している場合は、そのデータベースはサービスに戻され、運用サーバーとの接続を行う必要があります。

戻りサーバーが致命的な障害を起こして、そのままのリース状態データベースでサービスに戻ることができなかった場合、状況はもう少し複雑になります。この場合、Cisco Prime ネットワーク レジストラーの新規インストールは、通常、戻ってくるサーバー(同じ物理マシンではない場合もあります)に必要です。戻りサーバーは、障害が発生したサーバーと同じ IP アドレスを持ち、新しいCisco Prime ネットワーク レジストラー Cisco PrimeIPインストールは、障害が発生したサーバーと同じ設定にする必要があります。これは通常、運用サーバーと同じです。その後、新しいサーバーがサービスに移行し、既存の運用サーバーとの間に接続します。

（注） どちらの場合も、既存のオペレーション サーバーが実際に稼働しているサーバーがオンラインになった時点で動作することが重要です。運用サーバが何を行ったかを考慮または知らなくても、IP アドレスを配り始めます。

戻りサーバーが最初に起動すると、運用サーバーに接続し、最後に通信した時刻を交換します。

発生する可能性のある状況は 2 つあります。

- (Cisco Prime Network Primeが再インストールされなかった)、そのままのリース状態データベースを持つサーバーがサービスに復帰すると、しばらくサービスが終了したことをパートナーに連絡した後に確認し、RECOVER状態に移行し、そのパートナーはサービスを離れてから何が起きたかについての情報を送信します。この更新が完了すると、両方のサーバーが NORMAL 状態に移行します。
- Cisco Prime Network レジストラー Ciscoが再インストールされたサーバーがこの交換を完了すると、運用サーバーと通信したことがないことが認識され、オペレーションサーバーはサーバーと通信し(または先行サーバー)、新しく復元されたサーバーはリース状態データベースを失ったことに気付きます。RECOVER状態に移行し、すべてのリース状態情報の完全なダウンロードを運用サーバーから要求します。このダウンロードが完了すると(リース状態データベースのサイズとサーバーの負荷に応じて、数分または長くかかる場合があります)、両方のサーバーが NORMAL 状態に移行します。

スタンドアロン DHCP フェールオーバー サーバーの復元（チュートリアル）

ここでは、バックアップ サーバーをスタンドアロン モードにしたメイン サーバーとバックアップ サーバー間の DHCP フェールオーバー関係を再作成する方法について説明します。この状況はあまり起こらない。

メインサーバーが数分間を超えてサービスを停止している状況を処理する適切な方法は、バックアップ サーバーを PARTNER-DOWN 状態に設定することです。詳細については、PARTNER-DOWN 状態を使用してフェールオーバー パートナーなしでフェールオーバー サーバーを長時間動作する （32 ページ）を参照してください。

次の手順は、管理者が、メイン サーバーがサービスを提供しなき場合に、バックアップ サーバーをフェールオーバー関係から削除する方法が適切であると誤って考えた状況から回復するために提供されます。繰り返しますが、これは正しい手順ではありません。この間違いから立ち直るのは難しいですが、次の手順が役立ちます。

1. スタンドアロン サーバーは、メイン サーバーの役割を担います。
2. 元のメイン サーバーがバックアップ サーバーになります。
3. パートナーは同期します。
4. サーバーの役割を逆にする意図的に切断されるフェールオーバー 関係。
5. パートナーは、元のフェールオーバー ロールで再同期します。

バックグラウンド

このセクションの残りの部分では、メイン DHCP フェールオーバー サーバーはサーバー A (クラスタ A という名前のクラスタ オブジェクトを持つ) として識別され、バックアップ サーバーはサーバー B (cluster-B という名前のクラスタ オブジェクトを持つ) として識別されます。サーバー A が管理上または他の方法でシャットダウンされるか、Cisco Prime Network レジストラー サーバー エージェントが停止します。この時点で、サーバー B は通信中断モードに入ります。

システム管理者は、次のいずれかの方法を実行できます。

- **バックアップ サーバー B を通信中断モードで実行し続ける**：バックアップ サーバーを無期限にこのモードで実行するリスクは、バックアップ サーバーが新しいクライアントにサービスを割り当てる利用可能なアドレスの 10% のプールを使い果たす可能性があるというものです。
- **フェールオーバー関係を壊さずにサーバー B をパートナー ダウン モードにする**：フェールオーバーを中断せずに、バックアップ サーバーにアドレス空間のフル コントロールを与える 1 つの重要な注意点は、構成された最大クライアント リード タイム (MCLT) の後までアドレス空間所有権の完全な転送が行われないということです。MCLT は、メイン サーバーに設定された追加の期間で、バックアップ サーバーが検出した期間よりもクライアント リースの有効期限が先行する期間を制御します。MCLT は通常 60 分です。MCLT の有効期限が切れるまで、バックアップ サーバーの使用可能なアドレス プールは、割り当てられた予約に制限されます。
- **サーバー B をパートナー ダウン モードにしてフェールオーバー関係を解除する**：この方法では、バックアップ サーバーをスタンドアロン モードにし、管理者がこのシナリオで選択したアプローチになります。決定要因としては、メイン サーバーが長時間オフラインになると予想され、オンラインになる新しいデバイスの数が予想を上回ることが考えられます。バックアップ サーバーがサービスを提供できるアドレスの割合が低いと、新しいデバイスが停止する可能性があるため、管理者はサーバー B をスタンドアロン モードにします。このアプローチの欠点は、パートナーを元の関係に復元する際に、ネットワークの元の状態を維持するために必要な注意と労力です。

最初の 2 つのアプローチは、3 番目の方法よりも明確な利点があります。ほとんどの場合、MCLT の有効期限が切れるまで、バックアップ サーバーは新しく到着したクライアントをカバーするのに十分なアドレスを持っていると予想されます。3番目のアプローチを追求すると、不必要な管理上の負担とリスクが発生する可能性があります。

修復手順

修復手順は次のとおりです。

1. **バックアップ サーバー B にメイン フェールオーバー サーバーの役割を一時的に割り当てる**：フェールオーバー パートナーの役割を逆にすることで、サーバー A はサーバー B から現在のフェールオーバー状態を学習できます。
2. **サーバー A とサーバー B を元のフェールオーバーの役割に戻す**：目標は、サーバー A が元の状態をメインの DHCP フェールオーバー サーバーとして再取得することです。

前提は次のとおりです。

- 元のメイン サーバー A は非動作であり、Cisco Prime Network レジストラー は停止されます。
- 元のバックアップ サーバー B が動作しています。
- パートナー間のフェールオーバーは管理上無効です。
- 2 つのパートナーのフェールオーバーの役割を完全に取り消さないという決定が下されました。
- ドメイン ネーム システム (DNS) がどちらのフェールオーバー パートナーでも実行されていません。

（注） 例として使用される IP アドレスは、デモンストレーションのみを目的としたものです。

バックアップ サーバーのフェールオーバー ロールの反転

次の手順では、サーバーBを一時的にメインサーバーモードに移行することで、フェールオーバーを復元します。

サーバー B (クラスター B) で次の手順を実行します。

ステップ 1 フェールオーバーが無効になっていることを確認します。サーバーBがメイン、サーバーAがバックアップになるように、フェールオーバー構成を変更します。

```
nrcmd> failover-pair examplepair set failover=false
nrcmd> failover-pair examplepair set main=cluster-B backup=cluster-A
```

ステップ 2 変更を保存して、サーバーをリロードします。

```
nrcmd> save
nrcmd> dhcp reload
```

ステップ 3 フェールオーバーを再度有効にし、サーバーを再度リロードします。

```
nrcmd> failover-pair examplepair set failover=true
nrcmd> dhcp reload
```

サーバー B がメイン フェールオーバー サーバーとなり、パートナーが再び動作可能になる準備が整いました。その間にサーバー A がアドレスを提供し始めないようにするための、これ以上の操作は、現在の状態によって異なります。

サーバー A が次の場合:

- **電源オフ**：サーバー A の電源をオフにした状態での起動 （36 ページ） を参照してください。
- **Cisco Prime Network レジストラー DHCP が起動するように設定されていない状態で電源がオンに設定されている場合**は、サーバー A の電源をオンにし、DHCP サーバーを停止した状態での起動 （37 ページ）を参照してください。
- **別のマシンに置き換えられる場合**はサーバー A を置き換えての起動 （37 ページ）を参照してください。

サーバー A の電源をオフにした状態での起動

サーバー A の電源がオフになっている場合は、電源を再びオンにして続行する必要があります。次の手順では、IP アドレスの漏洩を防ぎながら、サーバー A がオンラインになっていることを確認します。

サーバー A (クラスタ A) で次の手順を実行します。

ステップ 1 サーバーの電源を入れる前に、クライアントとの通信を防ぐための手順を実行する必要があります。これを行う最善の方法は、ネットワークケーブルを手動で取り外してから、マシンを起動することです。次の手順を実行するには、ローカル コンソールが必要です。その他の方法としては、サーバーにパケットを転送しないようにリレー エージェントを再構成したり、コンピュータで受信する DHCP トラフィックを防止する (ファイアウォールに DHCP パケット用の一時的なフィルタをインストールするなど) などです。

（注） クライアント トラフィックがサーバーに到達するのを防ぐことができない場合は、DHCP サーバーが停止するまで、クライアントと通信を試みる誤った情報をクライアントに提供する可能性があります。したがって、次の手順で説明するように、サーバーをオンにした後、できるだけ早く DHCP サーバーを停止し、誤った情報を提供する可能性のあるクライアントの数を減らし、リースが重複する可能性があります。

ステップ 2 サーバーの電源をオンにします。

ステップ 3 DHCP サーバーをできるだけ早く停止します。

```
nrcmd> dhcp stop
```

ステップ 4 サーバー A の電源をオンにし、DHCP サーバーを停止した状態での起動 （37 ページ）に移動します。

サーバー A の電源をオンにし、DHCP サーバーを停止した状態での起動

サーバー A の電源がオンになっているが、Cisco Primeネットワーク レジストラー DHCP サーバーが停止しているポイントから開始します。

サーバー A（cluster-A）で、次の手順を実行します。

ステップ 1 サーバー A がバックアップ サーバーになるように、フェールオーバー構成を変更します。

```
nrcmd> failover-pair examplepair set main=cluster-B backup=cluster-A
```

ステップ 2 Cisco プライムネットワーク レジストラーを停止します。

```
systemctl stop nwreglocal
```

ステップ 3 DHCP ログを調べて、DHCP サーバーが動作していないことを確認します。

ステップ 4 サーバー A をネットワークに戻します。ネットワーク ケーブルを再接続するか、リレー エージェントを再構成するか、前のセクションで追加したファイアウォール フィルタを削除します。

ステップ 5 リース状態データベースとイベント ストアを削除します。

```
rm -rf /var/nwreg2/local/data/dhcpeventstore/
rm -rf /var/nwreg2/local/data/dhcp/ndb/
rm -rf /var/nwreg2/local/data/dhcp/ndb6/
```

警告　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。一方のみを削除する（そしてもう一方を残す）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。

ステップ 6 Cisco Prime Network レジストラー を起動します。

```
systemctl start nwreglocal
```

ステップ 7 再起動時に DHCP サービスを有効に設定し、DHCP サーバーを起動します。

```
nrcmd> dhcp enable start-on-reboot
nrcmd> dhcp start
```

ステップ 8 サーバー A への現在のリース状態の転送 （38 ページ）に進みます。

サーバー A を置き換えての起動

サーバー A が使用停止され、交換された場合は、Cisco Prime Network レジストラーをインストールし、サーバーBから新しいマシンにフェールオーバー設定をプッシュする必要があります。また、サーバーAに固有の顧客構成を復元する必要があります。これらの手順の後、Cisco プライムネットワーク レジストラーは開始しますが、アドレスは提供しません。

ステップ 1 **Server A**（クラスタ A）にて、Cisco Prime Network レジストラー をインストールします。

ステップ 2 Cisco ブロードバンド アクセス センターなどの付属ソフトウェアと必要な DHCP 拡張機能を復元して、Cisco Prime Network レジストラーのオペレーティング環境を再構築します。構成をサーバー B にプッシュするまで、構成に対して管理上の変更を行わないでください。

ステップ 3 **Server** Cisco **B** Primeネットワーク レジストラー Web UI を使用して、サーバ A に正確なフェールオーバー設定をプッシュします(クラスタ B)。これにより、サーバー A がバックアップ パートナーになります。

ステップ 4 **Server A** の場合

a) 必要に応じて、Cisco Primeネットワーク レジストラー設定を、運用環境に必要な設定(管理上の変更を含む) にカスタマイズします。

b) DHCP サーバーをリロードします。

```
nrcmd> dhcp reload
```

ステップ 5 サーバー A への現在のリース状態の転送 （38 ページ）に進みます。

サーバー A への現在のリース状態の転送

- この時点で、フェールオーバー パートナーシップが再確立し、両方のサーバーが状態を再同期します。
- サーバー A はバックアップ サーバーとして動作可能になります。
- MCLT 期間 (1 時間) の間、操作が一時停止し、両方のパートナーが通常の通信モードでフェールオーバー操作を再開します。

（注） パートナーが同期して通常パートナーを元の役割へ修復 （38 ページ）の通信を報告するまで、 に進まないでください。

パートナーを元の役割へ修復

両方のパートナーが完全に同期され、通常の通信を報告することを想定しています。フェールオーバー パートナーが元のロールを引き受けられるようにするには、次の手順を実行します。

ステップ 1 **Server A**（クラスタ A）では、DHCP サーバーを停止します。

```
nrcmd> dhcp stop
```

ステップ 2 **Server B**（クラスタ B）では、DHCP サーバーを停止します。

```
nrcmd> dhcp stop
```

ステップ 3 **Server A** の場合

a) フェイルオーバーを無効にしてから、サーバー A をメインサーバー、サーバー B をバックアップにします。

```
nrcmd> failover-pair examplepair set failover=false
nrcmd> failover-pair examplepair set main=cluster-A backup=cluster-B
```

b) 変更を保存し、DHCP をリロードします。

```
nrcmd> save
nrcmd> dhcp reload
```

c) 構成が適切で、現在実行中であることを確認します。この時点で、サーバー A は、アドレス プールの 100% を持つ唯一の運用 DHCP サーバーです。

d) フェールオーバーを再度有効にします。

```
nrcmd> failover-pair examplepair set failover=true
```

e) DHCP をリロードし、設定変更を再確認します。

```
nrcmd> dhcp reload
```

サーバー A は、サーバー B が動作可能になるのを待つフェールオーバー メイン サーバーになりました。

ステップ 4 **Server B:** の場合

a) サーバー A をメイン サーバー、サーバー B をバックアップにし、フェールオーバーを有効にします。

```
nrcmd> failover-pair examplepair set main=cluster-Abackup=cluster-B
nrcmd> failover-pair examplepair set failover=true
```

b) 新しい設定を保存しますが、サーバーをリロードしないでください。

```
nrcmd> save
```

c) サーバー B で DHCP サーバーを再起動します。

```
nrcmd> dhcp reload
```

この時点で、フェールオーバー パートナーシップは元の役割で自分自身を再確立し、両方のサーバーが状態を再同期し、サーバー B がバックアップ サーバーとして動作します。この操作は、1 時間の MCLT 期間の間一時停止し、両方のパートナーが通常の通信モードでフェールオーバー操作を再開します。

ステップ 5 **Server A** および **Server B** の場合

a) 両方のパートナーが通常のフェールオーバー状態にあるかどうかを検証します。

```
nrcmd> dhcp getRelatedservers
```

b) レポートを実行し、結果が両方のパートナーで一致することを確認し、パートナー間の実行時間の差を少しずらします。

フェールオーバー サーバー ロールの変更

⚠

注意 フェールオーバー サーバーの役割を変更する場合は注意が必要です。DHCPv4 スコープまたは DHCPv6 プレフィックスのすべてのアドレス状態は、そのスコープまたはプレフィックスを持たない状態で再ロードされた場合、サーバーから失われる点に注意してください。

スタンドアロンサーバーをメインとして使用したフェールオーバーの確立

既存のインストールを更新し、提供する DHCP サービスの可用性を向上させることができます。この手順は、スタンドアロン サーバーがフェールオーバーに参加したことがない場合にのみ使用できます。

ステップ 1 バックアップ サーバーとなるマシンに Cisco Prime Network レジストラーをインストールします。バックアップ サーバーの IP アドレスを記録します。

ステップ 2 クラスタを設定します。スタンドアロン サーバーでフェールオーバーを有効にし、メイン サーバーとして構成し、最近バックアップとしてインストールします。

クラスタをコンフィグレーションするには、**cluster** *name* **create** *address* | *ipv6-address* **scp-port**=*value* **admin**=*value* **password**=*value* を使用します。次に例を示します。

```
nrcmd> cluster backup create 10.65.201.23 scp-port=1234 admin=admin password=changeme
```

ステップ 3 メイン サーバーをリロードします。PARTNER-DOWN状態にする必要があります。バックアップサーバーがまだ構成されていないため、バックアップ サーバーを見つけることができません。この時点で、メイン サーバーの操作に変更はありません。

ステップ 4 構成を同期するには、フェールオーバー同期を使用して、メインからバックアップへの正確な同期を実行します。

ステップ 5 ブロードキャスト パケットをメイン サーバーおよびバックアップ サーバーに転送するように、すべての動作中の BOOTP リレーを再構成します。

ステップ 6 バックアップ サーバーをリロードします。

次のタスク

この手順を完了すると、次の状態に入ります。

1. バックアップ・サーバーはメインサーバーを検出し、RECOVER状態に移行します。
2. バックアップ・サーバーは、メイン・サーバーのリース・データを使用して安定したストレージを更新し、完了するとRECOVER-DONE状態に移行します。

3. メイン サーバーが NORMAL 状態に移行します。
4. バックアップ サーバーが NORMAL 状態に移行します。
5. バックアップ サーバーは、アドレスのプールを取得するためのプール要求を送信します。
6. これらのアドレスを割り当てた後、メイン サーバーはバックアップの割合に基づいてバックアップに IP アドレスを割り当てます。

ストレージに欠陥のあるサーバーの交換

フェールオーバー サーバーが安定した記憶域 (ハード ディスク) を失った場合、サーバーを交換して、パートナーから状態情報を回復させることができます。

ステップ 1 安定したストレージを失ったサーバーを特定します。

ステップ 2 CLI の**failover-pair**名前 **setPartnerDown***[date]*を使用して、パートナーがダウンしていることを他のサーバーに伝えます。時刻を指定しない場合は、現在の時刻が使用されます。

ステップ 3 サーバーが再び動作状態になったら、Cisco Primeネットワーク レジストラーを再インストールします。

ステップ 4 フェールオーバー同期を使用して、パートナー構成からサーバー構成を同期します。ただし、以前のバックアップまたはパートナー システムからリース データベースを回復しないでください。

ステップ 5 交換用のサーバーをリロードします。

次のタスク

この手順を完了すると、次の状態に入ります。

1. 回復されたサーバーは RECOVER 状態に移行します。
2. パートナーは、すべてのデータを送信します。
3. サーバーは、最大クライアントリードタイム(およびフェールオーバー・リカバリに設定された任意の時間)に達すると、*RECOVER-DONE*状態に移行します。
4. そのパートナーは NORMAL 状態に移動します。
5. 回復されたサーバーは NORMAL 状態に移行します。アドレスを要求できますが、パートナーが以前に割り当てたすべてのアドレスをすでに送信しているため、新しいアドレスを割り当てることは少なくなります。

バックアップ サーバーの削除とフェールオーバー操作の停止

バックアップ サーバーを削除し、すべてのフェールオーバー操作を停止する必要がある場合があります。

ステップ 1 バックアップ サーバーで、メイン サーバーへのバックアップとして指定されたすべてのスコープまたはプレフィックスを削除します。

ステップ 2 メイン サーバーで、バックアップ サーバーのメインだったスコープまたはプレフィックスからフェールオーバー機能を削除するか、構成されている場合はサーバー全体でフェールオーバーを無効にします。

ステップ 3 両方のサーバーを再ロードします。

既存のバックアップ サーバーへのメイン サーバーの追加

メイン サーバーには既存のバックアップ サーバーを使用できます。

ステップ 1 フェールオーバー同期を使用して、バックアップ サーバー上のメイン サーバー スコープ、ポリシー、およびその他の構成を同期します。

ステップ 2 フェールオーバーを有効にしてバックアップ サーバーをポイントするように、メイン サーバーを構成します。

ステップ 3 新しいメイン サーバーを指す新しいスコープのフェールオーバーを有効にするようにバックアップ サーバーを構成します。

ステップ 4 両方のサーバーを再ロードします。Cisco プライムネットワーク レジストラーは、でスタンドアロン サーバーをメインとして使用したフェールオーバーの確立 （40 ページ）説明されている手順と同じ手順を実行します。

複数インターフェイス ホストでのフェールオーバーの設定

複数のインターフェイスを持つサーバーホストでフェールオーバーを使用する場合は、ローカルサーバー名またはアドレスを明示的に構成する必要があります。これには追加のコマンドが必要です。たとえば、サーバー A とサーバー B の 2 つのインターフェイスを持つホストがあり、サーバー A をメイン フェールオーバー サーバーにする場合、バックアップ サーバー名 (外部サーバー B) を設定する前に、サーバー A をフェールオーバー メイン サーバーとして定義する必要があります。これを行わない場合、フェールオーバーが正しく初期化されず、間違ったインターフェイスを使用しようとする可能性があります。

フェールオーバーサーバー-メイン サーバーおよびフェールオーバーバックアップ サーバーの DHCP サーバー プロパティを設定する :

1 つのホストに複数のインターフェースがある場合は、1 つのアドレスまたはレコードのみを指すホスト名を指定する必要があります。ラウンドロビンをサポートするためにサーバーをセットアップすることはできません。

フェールオーバー パートナーの別ネットワークへの移動

フェールオーバー パートナーが動作している可能性があるネットワークの番号を変更したり、フェールオーバー パートナーを別のネットワーク セグメントに移動したりする必要が生じる場合があります。このような場合、サーバーの再起動が必要な構成変更が必要なため、サービスの停止が短時間で発生します。また、新しいサーバーアドレスにトラフィックを転送するために、リレー エージェントを更新する必要があります。

（注） 次の手順では、フェールオーバー ペア オブジェクトで明示的なアドレスが構成されていないと仮定します。メインおよびバックアップ クラスタ オブジェクトから通常継承されたアドレスを上書きするように明示的なアドレスが構成されている場合は、フェールオーバー ペア オブジェクトのアドレスを手動で更新する必要があります (手順 1 と 2)。

両方のフェールオーバー パートナーのアドレスを変更する場合は、次の手順を使用することをお勧めします。

ステップ 1 メインで、**クラスタ**名set ipaddr=アドレスまたは**クラスタ**名 **set ip6address=***address*コマンドを使用して、バックアップの新しいアドレスを使用するようにバックアップ クラスタ オブジェクトを再構成します。サーバーを再ロードしないでください。

（注） メインのクラスタ オブジェクトのアドレスを変更することはできません。これは、新しいサーバーが移動して起動すると自動的に変更されます。

ステップ 2 バックアップで、メインの新しいアドレスを使用するようにメイン クラスタ オブジェクトを再構成します。サーバーはリロードしません。

ステップ 3 バックアップを停止する前に、DHCP サーバーの起動を無効**にします(dhcp disable on reboot**コマンドを使用します)。これにより、サーバーをブートし、DHCP を自動的に実行することが可能になります。

ステップ 4 バックアップ サーバーでCisco プライム ネットワーク レジストラー Ciscoプライム IPを停止するか、シャットダウンします。DHCP サーバーが起動されないので、移動して再起動できます。

ステップ 5 バックアップ サーバーが長時間ダウンする場合 (物理的に移動する必要がある場合など)、メインをパートナーダウン状態に移行する必要があります(フェールオーバー**ペア**名 **setPartnerDown**コマンドを使用)。

ステップ 6 メイン サーバーをシャットダウンして移動します。この期間中、クライアントはリースを取得または更新できません。

ステップ 7 新しいアドレスでメインサーバーを起動します。メインのローカル クラスタ オブジェクトのアドレスが新しいアドレスであること、およびバックアップ クラスタ オブジェクトのアドレスが有効であることを検証します。また、DHCP トラフィックがリレーから到着していることを確認し、中継エージェントを構成し直して、新しいメイン サーバーアドレスとバックアップ サーバアドレスにトラフィックを適切に転送するようにします。

ステップ 8 バックアップ システムを新しいアドレスで起動します (手順 4 で開始していなかった場合)。バックアップのローカル クラスタ オブジェクトのアドレスが新しいアドレスであること、およびメイン クラスタ オブジェクトのアドレスが有効であることを検証します。

ステップ 9 バックアップで、起動時の再起動を有効にし、**dhcp enable-on-reboot**コマンドと**dhcp start**コマンドを使用してサーバーを起動します。

ステップ 10 フェールオーバー通信が動作していることを検証し、通常の状態に戻ります**(dhcp getRelatedServers**コマンドを使用して、いずれかまたは両方のクラスターのフェールオーバーステータスを表示します)。通信が速やかに再開されない場合は、バックアップで DHCP サーバーを停止し、クラスタ上のアドレスとフェールオーバー ペア オブジェクトの構成変更が正しく適用されていることを確認します。

ステップ 11 地域で、メインおよびバックアップ クラスタ オブジェクトを更新して、新しいアドレスを使用します。または、メイン クラスタとバックアップ クラスタの両方で**license register**コマンドを使用して、リージョンを更新することもできます。

フェールオーバーのトラブルシューティング

このセクションでは、フェールオーバー構成の誤りを回避し、フェールオーバー操作を監視し、ネットワークの問題を検出して処理する方法について説明します。

フェールオーバー操作のモニターリング

両方のパートナー サーバーの DHCP サーバー ログ ファイルを調べて、フェールオーバー構成を確認できます。

いくつかの重要なログとデバッグの設定を行って、フェールオーバーのトラブルシューティングを行うことができます。DHCPログ設定をフェールオーバーの詳細に設定し、ログに記録されたフェイルオーバー メッセージの数と詳細を追跡します。以前のメッセージが上書きされないようにするには、リストの最後にフェールオーバーの詳細属性を追加します。非フェールオーバー競合属性を使用して、ログ記録サーバーのフェールオーバー競合を禁止するか、または通常のサーバー フェールオーバー アクティビティのログ記録を禁止する非フェールオーバー アクティビティ属性を使用します。次に、サーバーを再ロードします。

また、[DHCP サーバーの管理] ページまたは [DHCP フェールオーバー ペアの一覧/追加] ページの [**関連サーバー**]**dhcp getRelatedServers**アイコンをクリックするか、CLI で使用することで、設定ミスをより簡単に切り分けることができます。

ネットワーク エラーの検出と処理

次の表に、フェールオーバーの問題に対する症状、原因、および解決策を示します。

表 *5:* 障害の検出と処理

症状	原因	ソリューション
新しいクライアントはアドレスを取得できません	バックアップ・サーバーが、アドレスが少なすぎる、COMMUNICATIONS-INTERRUPTED 状態です。	メイン サーバーのバックアップの割合を増やします。
スコープの不一致に関するエラー メッセージ	パートナー間でスコープ構成が一致しません。	サーバーを再構成します。

症状	原因	ソリューション
パートナーとの通信の失敗に関するメッセージをログに記録する	サーバーはパートナーと通信できません。	サーバーのステータスを確認します。
メイン サーバーに障害が発生しました。一部のクライアントは、リースを更新または再バインドできません。バックアップサーバーがアップ状態で、クライアント要求を処理している場合でも、リースは期限切れになります。	一部の BOOTP リレー エージェント (ip-helper) は両方のサーバーをポイントするように構成されていません。BOOTP リレーの設定 （47 ページ）を参照してください。	• BOOTP リレーを、メイン サーバーとバックアップ サーバーの両方を指す設定に戻します。 • ファイアードリルテストを実行する - メインサーバーを1日ほど停止し、ユーザーコミュニティがリースを取得して更新できるかどうかを確認します。
SNMP トラップ: 他のサーバーが応答しません	サーバーはパートナーと通信できません。	サーバーのステータスを確認します。
SNMP トラップ: DHCP フェールオーバー構成の不一致	パートナー間でのスコープ構成の不一致	サーバーを再設定します。
ユーザーが期待どおりにサービスやシステムを使用できないという苦情	パートナー間のポリシーとクライアント クラスの不一致	同一のポリシーを持つパートナーを再構成します。現在、パートナーに直接クライアントを登録している場合は、クライアント登録に LDAP を使用する可能性があります。

フェールオーバーに関連する問題のトラブルシューティング時に避けるべき事項

フェールオーバーを使用する場合、問題のトラブルシューティング時に行わない点がいくつかあります。

- フェールオーバー構成を削除しています。残りのサーバーを PARTNER-DOWN 状態に設定する方がはるかに良いです。リースの再利用に長い待ち時間が必要になる場合もありますが、フェールオーバーを設定して PARTNER-DOWN で動作する方がはるかに安全です。
- DHCP リース データベース (../data/dhcp/ndb および ./data/dhcp/ndb6) を一方のフェールオーバー パートナーから他方のフェールオーバー パートナーにコピーしないでください。

フェールオーバーパートナーからリースデータを回復する方法については、『*Cisco Prime Network Registrar 11.1 Administration Guide*』の「フェールオーバーサーバーからの DHCP データの復元」のセクションを参照してください。これが行われた場合は、データベースをコピーした後に server-duid を削除するために leaseadmin ツールを使用しなければなりません（leaseadmin ツールの詳細についてはサーバー間でのリースの移動を参照してください）。リースデータベースがコピーされるたびに、server-duid をコピーから削除する必要があります。Cisco Prime Network Registrar 10.0 以降、新しいデータベース（または、server-duid が削除されたデータベース）は、ローカルのクラスタ UUID を使用するため、すべてのデータベースに server-duid が格納されるわけではありません。

（注） server-duid を削除しないと、2 台のサーバーで同じ server-id を使用することができるため、DHCPv6 は意図したとおりに動作しません。これは、リージョンのリース履歴データに重大な影響を与える可能性があります。

フェールオーバーでの BOOTP クライアントのサポート

静的と動的の 2 種類の BOOTP クライアントをサポートするようにスコープを構成できます。

静的 BOOTP

DHCP 予約を使用して、静的 BOOTP クライアントをサポートできます。フェールオーバーを有効にする場合は、メイン サーバーとバックアップ サーバーの両方を同一の予約で構成してください。

動的 BOOTP

スコープで動的 bootp 属性を有効にすることで、動的 *BOOTP* クライアントを有効にすることができます。ただし、フェールオーバーを使用する場合、BOOTP クライアントは無期限の永続的なアドレスとリースを取得するため、このようなスコープでのアドレスの使用に関する追加の制限があります。

スコープの動的ブート オプションが有効になっていないサーバーが PARTNER-DOWN 状態になると、そのスコープから使用可能な(割り当てられていない)アドレスを割り当てることができます。ただし、動的ブートオプションを設定すると、各パートナーは独自のアドレスのみを割り当てることができます。したがって、*dynamic-bootp* オプションを有効にするスコープでは、フェールオーバーをサポートするためにより多くのアドレスが必要になります。

動的ブートを使用する場合:

- 動的 BOOTP クライアントを単一のスコープに分離します。スコープの *dhcp* 属性を無効にして、DHCP クライアントがそのスコープを使用できないようにします。

- 動的*bootp-backup-pct*フェールオーバー ペア属性を設定して、このスコープのバックアップ サーバーに対して、通常のバックアップの割合よりも 50% も高いアドレスを割り当てます。

BOOTP リレーの設定

Cisco Prime Network レジストラーフェールオーバー プロトコルは、サーバーにローカルに接続されていないDHCPクライアントをサポートするルータ機能であるBOOTPリレー(IPヘルパーとも呼ばれます)で動作します。

BOOTP リレーを使用する場合は、実装がメイン サーバーとバックアップ サーバーの両方を指していることを確認します。これらのパケットが失敗し、メイン サーバーに障害が発生した場合、クライアントはサービスを提供しません。2 つの異なるサーバーにブロードキャスト パケットを転送するようにBOOTP リレーを構成できない場合は、メイン サーバーとバックアップ サーバーの両方を含む可能性がある LAN セグメントのサブネット ローカル ブロードキャスト アドレスにパケットを転送するようにルーターを構成します。次に、メイン サーバーとバックアップ サーバーの両方が同じ LAN セグメント上にあることを確認します。

BOOTP バックアップの割合

動的BOOTPを有効にするスコープの場合、フェールオーバー ペアの*backup-pct*属性ではなく、動的ブート-バックアップ *pct*属性を使用します。動的 *bootp-backup-pct*は、BOOTP クライアントで使用するためにメイン・サーバーがバックアップ・サーバーに送信する必要がある使用可能なアドレスのパーセンテージです。

*DYNAMIC-bootp-backup-pct*は、スコープで BOOTP を有効にした場合、PARTNER-DOWN 状態であっても、サーバーが他のサーバーで使用可能なアドレスにリースを付与しないため、バックアップ *PCt*属性とは異なります。Cisco Prime Network レジストラーは、パートナーが動的 BOOTP を使用してリースを提供する可能性があるため、リースを許可しません。

（注） メイン・サーバー上で動的 BOOTP バックアップ率を定義する必要があります。バックアップ サーバーで定義した場合、Cisco Prime Network レジストラーは、これを無視します(スクリプトを使用した設定の複製を有効にするため)。これを定義しない場合、Cisco Prime Network レジストラーはフェールオーバー ペアまたはスコープにデフォルトのバックアップ*PCT*を使用します。

フェールオーバー プロトコルの使用中に動的 BOOTP を正しくサポートするには、BOOTP をサポートするすべての LAN セグメントで次の手順を実行します。

- 動的ブート・ブート用に 1 つのスコープを作成する
- ブートと動的ブートを有効にする
- そのスコープの DHCP を無効にする

DHCP リレー ヘルス チェック

フェイルオーバーを使用する場合、次の 3 つの異なる通信パスがあります。

- フェールオーバー パートナー間 (IPv4 または IPv6 経由)
- リレー エージェントとメイン フェールオーバー パートナーの間 (IPv4 および IPv6 の場合)
- リレー エージェントとバックアップ フェールオーバー パートナーの間 (IPv4 および IPv6 の場合)

これらのパスの 1 つ以上が壊れることがあります。たとえば、ルーティングの誤った設定やリンクの障害により、リレーエージェントとメインフェールオーバーパートナー間のトラフィック フローを防止できます。これにより、バックアップ フェールオーバー パートナーがこれらのパケットを受信した場合でも、一部のクライアントがオンラインにならないようにします (フェールオーバーがアップすると、通常はクライアントの要求に応答するため)。DHCP サーバーは、リレー エージェントを監視し、リレー エージェントがダウンしていると検出されたときに通常はフェールオーバー NORMAL 状態でサービスを提供しないクライアントに対して応答を有効にするように構成できます。

DHCP リレーの状態チェックを構成するには、[DHCP フェールオーバー ペアの一覧/追加] ページの [リレーヘルスチェック] セクションで属性を設定します。詳細については、フェールオーバー ペアの追加 （4 ページ）を参照してください。

Cisco Prime Network Registrar 11.0 において、IPv4 正常性チェックは、サーバーで使用される *dhcp-server-identifier* がサーバーのインターフェイスアドレスであり、高速コミットが許可されていない場合にのみ正しく動作します。したがって、*giaddr-as-server-id* が有効になっているポリシー、明示的な *dhcp-server-identifier* オプションが指定されているポリシー、または *allow-rapid-commit* が有効になっているポリシーは、IPv4 に対して自動的に無効になります。Cisco Prime Network Registrar 11.0.1 以降、この機能は拡張され、*giaddr-as-server-id* がポリシーで有効になっている場合でも IPv4 ヘルスチェックを有効にするようになりました。

IPv6 正常性チェックは、高速コミットが許可されていない場合にのみ正しく動作します。したがって、いずれかのポリシーで *allow-rapid-commit* が有効になっている場合、IPv6 の正常性チェックは自動的に無効になります。

ただし、サーバーのポリシーチェックでは、クライアントエントリを介して提供されるポリシーはチェックされません。したがって、クライアントポリシーで *giaddr-as-server-id*、明示的な *dhcp-server-identifier* オプション、または *Rapid-commit* が設定されている場合は、リレー正常性チェックを有効にしてください。

CLI コマンド

フェールオーバーが使用されており、ヘルスチェック機能が有効になっている場合は、 **dhcp getRelayState** [**all**] [**full**] コマンドを使用できます。これにより、フェールオーバー パートナーと各リレーエージェント間の通信の状態が報告されます。「すべて」を指定しない場合、フェー

ルオーバー パートナーとの通信に問題があると思われるリレー (つまり、中断状態の中継) のみが報告されます。"full" を指定すると、オブジェクトはテーブルではなく表示されます。

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。