Cisco Unified Communications Manager の IP アドレスおよびホスト名の変更、リリース 9.1(1)

発行日：2012 年 12 月 20 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルでは、Cisco Unified Communications Manager サーバの IP アドレスまたはホスト名を変更する手順を説明します。この IP アドレスの変更が必要になる理由として、サーバを別のセグメントに移動する場合や IP アドレスが重複している問題を解決する場合など、さまざまな状況が考えられます。

このガイドは、次のセクションから構成されています。

作業前のチェックリスト

次の作業を実行して、ご使用のシステムで IP アドレスの変更が可能であることを確認します。

（注） Cisco Unified Communications Manager サーバで設定された DNS がある場合は、IP アドレスを変更する前に次の条件が満たされていることを確認してください。

- 順方向および逆方向のルックアップ ゾーンが設定されている。
- DNS が到達可能であり、稼働している。

（注） アドレスの変更が可能であることを示す結果がこの作業の実行で得られない場合は、見つかった問題をすべて解決するまでこの手順を実行しないようにしてください。

手順

ステップ 1 クラスタにあるすべてのサーバを調べ、それらのノードの定義で IP アドレスを使用しているか、ホスト名を使用しているかを確認します。

- 最初のノードの Cisco Unified CM の管理 で [システム（System）] > [サーバ（Server）] を選択して [検索（Find）] をクリックします。

  クラスタにあるすべてのサーバが一覧表示されます。
- あとで参照できるように、このサーバのリストを記録しておきます。

ステップ 2 クラスタにあるノードごとに、ホスト名と IP アドレスの両方のインベントリが保存されていることを確認します。

ステップ 3 アクティブな ServerDown 警告が発生していないか調べ、クラスタにあるすべてのサーバが正常に稼働していて、利用可能であることを確認します。これを確認するには、最初のノードで Real Time Monitoring Tool（RTMT）またはコマンドライン インターフェイス（CLI）を使用します。

- RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。
- 最初のノードで CLI を使用して確認するには、次のコマンドを入力してアプリケーションのイベント ログを調べます。

```
file search activelog syslog/CiscoSyslog ServerDown
```

ステップ 4 クラスタにあるすべての Cisco Unified Communications Manager ノードでデータベース レプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。これを確認するには、RTMT または CLI コマンドを使用します。

- RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。

- CLI を使用して確認するには、次の例のようにコマンドを入力します。

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :

        - Perf class (Number of Replicates Created and State of Replication)
    has instances and values:
        ReplicateCount  -> Number of Replicates Created   = 344
        ReplicateCount  -> Replicate_State                = 2
```

この場合に Replicate_State オブジェクトが 2 の値を示すことに注意してください。次に、Replicate_State が取ることのできる値を示します。

- 0：レプリケーションは開始されていません。これは、サブスクライバが存在していないか、またはサブスクライバをインストールした後に Database Layer Monitor サービスが実行されていないことが原因です。
- 1：レプリケーションは作成されていますが、そのカウントが正しくありません。
- 2：レプリケーションは正常です。
- 3：このクラスタではレプリケーションが正常に実行されていません。
- 4：レプリケーションのセットアップに失敗しました。

ステップ 5 ネットワークの接続と DNS サーバの設定を確認するには、次の例のように CLI コマンドを入力します。

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

ステップ 6 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。詳細については、次の URL で、ご使用のリリースの『*Disaster Recovery System Administration Guide*』を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

ステップ 7 セキュリティが有効なクラスタ（クラスタ セキュリティ モード 1 - 混合）について、証明書信頼リスト（CTL）ファイルを更新します。

（注） セキュリティをサポートしているすべての IP 電話では、CTL ファイルが必ずダウンロードされます。このファイルには、その電話からの通信が許可されている TFTP サーバの IP アドレスが記述されています。TFTP サーバの IP アドレスを変更した場合は、その新しい IP アドレスを CTL ファイルに追加する必要があります。これにより、該当の電話からその TFTP サーバと通信できるようになります。

注意 通信不可能な時間が無駄に発生しないように、TFTP サーバの新しい IP アドレスで CTL ファイルを更新してから、TFTP サーバの IP アドレスを変更するようにします。この手順を実行しない場合は、セキュリティが有効なすべての IP 電話を手動で更新する必要があります。

既存の CTL ファイルへの新しい TFTP サーバの追加など、CTL ファイルの更新と管理の方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』*Release 8.6(1)* を参照してください。

このドキュメントは次の URL にあります。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

初期信頼リストおよび証明書の再生成

Cisco Unified Communications Manager リリース 8.0 リリース以降のクラスタでサーバの IP アドレスまたはホスト名を変更すると、ITL の初期信頼リスト（ITL）ファイルと証明書が再生成されます。再生されたファイルは、電話機に保存されたファイルと一致しません。

（注） クラスタ上でサーバのホスト名を変更する場合は、電話機が新しい ITL ファイルを受け入れることができるように、電話機の ITL ファイルを手動で削除する必要があります。

クラスタ セキュリティが有効になっていない場合は、次の手順を実行して電話機をリセットします。

（注） 証明書信頼リスト（CTL）ファイルと USB eToken を使用してクラスタ セキュリティを有効にする場合は、eToken によって信頼が保持され、eToken は変更されないため、次の手順を実行する必要はありません。

シングルサーバ クラスタ

Cisco Unified Communications Manager リリース 8.0 以降のシングルサーバ クラスタでサーバの IP アドレスまたはホスト名を変更する場合、および ITL ファイルを使用する場合は、次の手順を実行して電話機をリセットします。

サーバの IP アドレスまたはホスト名を変更する前に、ロールバックを有効にします。

ステップ 1 エンタープライズ パラメータ Prepare Cluster for Rollback to pre-8.0 を **True** に設定します。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話機をリセットします。

電話機に空の TVS および TFTP 証明書セクションを含む ITL ファイルがダウンロードされます。

ステップ 4 電話機で [設定（Settings）] > [セキュリティ（Security）] > [信頼リスト（Trust List）] > [ITL] を選択し、ITL ファイルの TVS および TFTP 証明書セクションが空であることを確認します。

ステップ 5 サーバの IP アドレスまたはホスト名を変更し、クラスタへの登録がロールバックされるように電話機を設定します。

ステップ 6 すべての電話機がクラスタに正常に登録されたら、エンタープライズ パラメータ Prepare Cluster for Rollback to pre-8.0 を **False** に設定します。

ステップ 7 TVS および TFTP を再起動します。

ステップ 8 すべての電話機をリセットします。

CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントを再実行します。

マルチサーバ クラスタ

マルチサーバ クラスタでは、電話機が、再生成された ITL ファイルおよび証明書を確認するためのプライマリおよびセカンダリ TVS サーバを持つ必要があります。電話機がプライマリ TVS サーバに（最近の設定変更により）接続できない場合は、セカンダリ サーバにフォール バックされます。TVS サーバは、電話機に割り当てられた CM グループによって識別されます。

マルチサーバ クラスタでは、一度に 1 つのサーバだけで IP アドレスまたはホスト名を変更するようにしてください。CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントを再実行します。

IP アドレスで定義されたサーバの IP アドレスの変更

この手順では、Cisco Unified Communications Manager 内で、IP アドレスで定義されたパブリッシャまたはサブスクライバ サーバの IP アドレスを変更する方法について説明します。特に指定のない限り、次のステップは、Cisco Unified Communications Manager クラスタ内のパブリッシャおよびサブスクライバ サーバの両方に適用されます。

注意 Cisco Unified Communications Manager クラスタにあるどのノードで IP アドレスを変更しても、コール処理やその他のシステム機能が中断する可能性があります。また、IP アドレスの変更によって、ServerDown や SDLLinkOOS などの特定のアラームや警告が発生することや、バックアップ サーバへの自動的なフェールオーバーが機能しなくなることもあり得ます。このような影響の発生が考えられるので、IP アドレスの変更は、定期的なメンテナンスの時間帯で実施する必要があります。

（注） Cisco Unified Communications Manager のパブリッシャ サーバに対するサブスクライバ サーバを定義する場合、またはサブスクライバ サーバの定義方法を指定する場合は、[システム（System）] > [サーバ（Server）] を選択します。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

手順

ステップ 1 Cisco Unified CM の管理 から、[システム（System）] > [サーバ（Server）] を選択します。

[サーバの検索と一覧表示（Find and List Servers）] ウィンドウが表示されます。

ステップ 2 [サーバの検索と一覧表示（Find and List Servers）] ウィンドウで、IP アドレスを変更するサーバを選択します。

ステップ 3 サーバの IP アドレスを変更して、新しい IP アドレスを反映させます。

ステップ 4 クラスタにあるすべてのノードで CLI コマンド **run sql select name,nodeid from ProcessNode** を入力して、IP アドレスの変更がサーバのデータベースに複製されていることを確認します。このコマンドの出力例を次に示します。

```
admin: run sql select name,nodeid from ProcessNode
name                nodeid
================== ======
```

```
EnterpriseWideData 1
10.3.90.21         4
10.3.90.5          2
```

ステップ 5 IP アドレスを変更するサーバがパブリッシャ サーバの場合は、クラスタ内の各サブスクライバ サーバにログインし、サブスクライバ サーバの IP アドレス マッピングをクラスタのパブリッシャ サーバに変更します。この作業は、[Cisco Unified Communications オペレーティング システム Administration] ウィンドウから、または CLI コマンドを使用して実行できます。

- Cisco Unified Communications Operating System Administration からマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、次の作業を実行します。
  a. [設定（Settings）] > [IP] > [パブリッシャ（Publisher）] を選択します。
  b. パブリッシャ サーバの IP アドレスを変更します。
- network CLI コマンドでマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、**set network cluster publisher ip** *ipaddress* CLI コマンド（*ipaddress* はパブリッシャ サーバ IP アドレスを表す）を使用してマッピングをパブリッシャ サーバの IP アドレスに変更します。

ステップ 6 新しいデフォルト ゲートウェイ アドレスを必要とする別のサブネットにサーバを移動する場合は、次の例のように **set network gateway** CLI コマンドを使用してデフォルト ゲートウェイを変更します。

```
admin:set network gateway 10.3.90.2
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

ステップ 7 サーバの IP アドレスを変更します。これは CLI コマンドを使用して実行するか、または Cisco Unified Communications オペレーティング システム Administration から実行できます。

- CLI コマンドを使用して IP アドレスを変更するには、次の手順を実行します。
  a. CLI コマンド **set network ip eth0** *ip_address netmask* を入力します。このコマンドでは、*ip_address* でサーバの新しい IP アドレスを指定し、*netmask* でサーバの新しいネットワーク マスクを指定します。

     次の出力が表示されます。

```
admin: set network ip eth0 10.3.90.21 255.255.255.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
=======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

  b. **Yes** と入力して Enter キーを押します。

- Cisco Unified Communications オペレーティング システム Administration から IP アドレスを変更するには、次の手順を実行します。
  a. [設定（Settings）] > [IP] > [イーサネット（Ethernet）] を選択します。
  b. IP アドレスを変更し、必要に応じてデフォルト ゲートウェイを新しいアドレスに変更します。
  c. [保存（Save）] ボタンをクリックします。サーバが新しい変更内容で自動的にリブートされます。

ステップ 8 サーバのリブート後に、クラスタ内の他のすべてのサーバをリブートして、hosts、rhosts、sqlhosts、services などのローカル名解決ファイルを更新します。

（注） システムを再起動しないと、これらのファイルは更新されません。また、これらのファイルを更新した後は、Cisco DB や Cisco Tomcat などのコア ネットワーク サービスを再起動する必要があります。サーバを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、IP アドレスの変更を有効にすることができます。

ステップ 9 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。詳細については、『*Disaster Recovery System Administration Guide*』を参照してください。

（注） クラスタにある複数のサーバの IP アドレスを変更するには、次の作業を実行します。

- 1 台のサーバの IP アドレスを変更します。
- クラスタをリブートします。
- レプリケーションのステータスを確認します。

  変更した IP アドレスが正しく反映されている場合は、次のサーバで同じ手順を実行します。反映されていない場合は、他のサーバの IP アドレスを変更しないでください。

警告 **複数のサーバで並行して同時に変更を行わないようにしてください。同時に変更を行うと、クラスタ内で .rhosts ファイルと sqlhosts ファイルが同期しない場合があります。**

ホスト名で定義されたサーバの IP アドレスの変更

この手順では、Cisco Unified Communications Manager 内で、ホスト名で定義されたパブリッシャまたはサブスクライバ サーバの IP アドレスを変更する方法について説明します。特に指定のない限り、次のステップは、Cisco Unified Communications Manager クラスタ内のパブリッシャおよびサブスクライバ サーバの両方に適用されます。

注意 特定のホスト名を持つサーバで作成した DRS バックアップは、別のホスト名を持つサーバには復元できません。これは復元先のサーバがパブリッシャ サーバでもサブスクライバ サーバでも同様です。また、そのノードを再インストールしても復元はできません。

手順

ステップ 1 新しい IP アドレスを指すようにサーバの DNS レコードを変更します。必ず順方向（A）レコードと逆方向（PTR）レコードの両方を正しく更新します。これらのレコードを正しく更新するには、DNS キャッシュをリフレッシュする必要があります。

（注） DNS サーバは、ネットワーク インフラストラクチャを構成する要素の 1 つです。Cisco Unified Communications Manager サーバは、DNS サービスを実行せず、また実行することもできません。

ステップ 2 すべてのクラスタ ノードで **utils network host** CLI コマンドを使用して、ホスト名と IP アドレスの関連付けが他のノードに反映される準備が完了していることを確認します。

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
```

ステップ 3 IP アドレスを変更するサーバがパブリッシャ サーバの場合は、クラスタ内の各サブスクライバ サーバにログインし、IP アドレス マッピングをクラスタのパブリッシャ サーバに変更します。この作業は、Cisco Unified Communications オペレーティング システム Administration から、または CLI コマンドを使用して実行できます。

- Cisco Unified Communications Operating System Administration からマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、次の作業を実行します。
  a. [設定（Settings）] > [IP] > [パブリッシャ（Publisher）] を選択します。
  b. パブリッシャ サーバの IP アドレスを変更します。
- network CLI コマンドを使用してマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、**set network cluster publisher ip** *ipaddress* CLI コマンド（*ipaddress* はパブリッシャ IP アドレスを表す）を使用してマッピングをパブリッシャ サーバの IP アドレスに変更します。

ステップ 4 新しいデフォルト ゲートウェイ アドレスを必要とする別のサブネットにサーバを移動する場合は、次の例のように **set network gateway** CLI コマンドを使用してデフォルト ゲートウェイを変更します。

```
admin:set network gateway 14.86.13.1
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

ステップ 5 次の作業を実行して、サーバの IP アドレスを変更します。

a. CLI コマンド **set network ip eth0** *ip_address netmask* を入力します。

このコマンドでは、サーバの新しい IP アドレスを *ip_address* で指定し、サーバの新しいネットワーク マスクを *netmask* で指定します。

次の出力が表示されます。

```
admin: set network ip eth0 14.86.13.11 255.255.255.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
```

```
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

b. **yes** と入力して Enter キーを押します。

（注） Cisco Unified Communications オペレーティング システム を使用してデフォルト ゲートウェイとサーバの IP アドレスを変更することもできます。Cisco Unified Communications オペレーティング システム Administration から、[設定（Settings）] > [IP] > [イーサネット（Ethernet）] を選択します。

ステップ 6 サーバのリブート後に、クラスタ内の他のすべてのサーバをリブートして、hosts、rhosts、sqlhosts、services などのローカル名解決ファイルを更新します。

（注） システムを再起動しないと、これらのファイルは更新されません。また、これらのファイルを更新した後は、Cisco DB や Cisco Tomcat などのコア ネットワーク サービスを再起動する必要があります。サーバを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、IP アドレスの変更を有効にすることができます。

（注） 複数のサーバの IP アドレスを変更する場合は、次の作業を実行します。

- 1 台のサーバの IP アドレスを変更します。
- クラスタをリブートします。
- レプリケーションのステータスを確認します。

  変更した IP アドレスが正しく反映されている場合は、次のサブスクライバ サーバで同じ手順を実行します。反映されていない場合は、他のサーバの IP アドレスを変更しないでください。

警告 **複数のサーバで並行して同時に変更を行わないようにしてください。同時に変更を行うと、クラスタ内で .rhosts ファイルと sqlhosts ファイルが同期しない場合があります。**

ステップ 7 すべてのクラスタ ノードで **utils network host** および **show tech network hosts** CLI コマンドを使用して、ステップ 4 で行われた変更に対するホスト名と IP アドレスの関連付けの変更が他のノードに反映されていることを確認します。

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network ---------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
```

```
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

ステップ 8 IP アドレスを変更するサーバがパブリッシャ サーバの場合は、次の作業を実行します。

a. [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] を選択します。

b. 電話の URL パラメータで、変更前の IP アドレスで記述されているすべての URL を新しい IP アドレスによる記述に変更します。

ステップ 9 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。詳細については、ご使用のリリースの『*Disaster Recovery System Administration Guide*』を参照してください。

IP アドレスで定義されたサーバのホスト名の変更

この手順では、Cisco Unified Communications Manager で、IP アドレスで定義されたサーバのホスト名を変更する方法について説明します。特に指定のない限り、この手順の各ステップは、パブリッシャおよびサブスクライバ サーバの両方に適用されます。

手順

ステップ 1 新しい IP アドレスを指すようにサブスクライバ サーバの DNS レコードを変更します。IP アドレスが同時に変更されている場合は、DNS サーバに IP アドレスが反映されていることを確認します。順方向（A）レコードと逆方向（PTR）レコードが正しく更新されていることを確認します。

（注） DNS サーバは、ネットワーク インフラストラクチャを構成する要素の 1 つです。Cisco Unified Communications Manager サーバは、DNS サービスを実行せず、また実行することもできません。

ステップ 2 次のいずれかの作業を実行します。

- ホスト名だけを変更する場合は、ステップ 6 に進みます。
- ホスト名と IP アドレスの両方を変更する場合は、ステップ 3 に進みます。

ステップ 3 [Cisco Unified CM の管理] ウィンドウで、次の作業を実行します。

a. [システム（System）] > [サーバ（Server）] を選択します。

b. [サーバの設定（Server Configuration）] で、サーバの IP アドレスを変更します。

ステップ 4 CLI コマンド **`run sql select name,nodeid from ProcessNode`** を入力して、ステップ 3 で行った変更内容がクラスタにあるすべてのノードにレプリケートされていることを確認します。

ステップ 5 クラスタにあるすべてのノードでこの手順を繰り返します。

ステップ 6 ホスト名を変更するサーバがパブリッシャ サーバの場合は、クラスタ内の各サブスクライバ サーバにログインし、クラスタのパブリッシャ サーバのホスト名マッピングを変更します。この作業は、Cisco Unified Communications オペレーティング システム Administration から、または CLI コマンドを使用して実行できます。

- Cisco Unified Communications Operating System Administration からマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、次の作業を実行します。
  - **a.** [設定（Settings）] > [IP] > [パブリッシャ（Publisher）] を選択します。
  - **b.** パブリッシャ サーバのホスト名を変更します。
- network CLI コマンドを使用してマッピングを変更するには、クラスタ内の各サブスクライバ サーバにログインし、**set network cluster publisher hostname** *hostname* CLI コマンド（*hostname* はパブリッシャ ホスト名を表す）を使用してマッピングをパブリッシャ サーバの IP アドレスに変更します。

ステップ 7 サーバのホスト名を変更します。これは CLI コマンドを使用して実行するか、または Cisco Unified Communications オペレーティング システム Administration から実行できます。

- CLI コマンドを使用してホスト名を変更するには、次の手順を実行します。
  - **c.** CLI コマンド **set network hostname** *ホスト名*を入力します。
  - **d.** **Yes** と入力して Enter キーを押します。このコマンドにより、このサーバが新しいホスト名で自動的にリブートされます。
- Cisco Unified Communications オペレーティング システム Administration からホスト名を変更するには、次の手順を実行します。
  - **a.** [設定（Settings）] > [IP] > [イーサネット（Ethernet）] を選択します。
  - **b.** IP アドレスを変更し、必要に応じてデフォルト ゲートウェイを新しいアドレスに変更します。
  - **c.** [保存（Save）] ボタンをクリックします。サーバが新しい変更内容で自動的にリブートされます。

（注） ホスト名を変更すると、自己署名証明書が自動的に再生成されます。サーバが自動的にリブートしても、CTL クライアントを新規に実行して CTL ファイルを更新しないと、このサーバへのセキュア接続はできません。

ステップ 8 サーバがリブートされたら、ホスト名を変更したサーバの Admin CLI を起動して、**utils dbreplication dropadmin db** コマンドを実行します。

ステップ 9 ホスト名と同時に IP アドレスも変更され、サーバが新しいサブネットに移動する場合は、**set network gateway** *ipaddress* CLI コマンドを使用して、サーバのデフォルト ゲートウェイを新しいアドレスに変更します。

（注） デフォルト ゲートウェイを変更する場合は、次のステップの前に、サーバが新しいサブネットに移動していてデフォルト ゲートウェイにアクセスしていることを確認します。Cisco Unified Communications Manager サーバが起動するとき、デフォルト ゲートウェイにサーバがアクセスできるかどうかの確認が Verify Network スクリプトで行われます。サーバが起動時にデフォルト ゲートウェイと通信できないと Verify Network スクリプトが失敗するため、起動に時間がかかることがあります。DHCP を手動で設定していて DHCP にアクセスできない場合、またはサーバに対して IP アドレスを指定していない場合、システムは起動せず、Verify Network の起動処理段階で待機状態を継続します。

ステップ 10 パブリッシャ サーバも含め、クラスタにある他のすべてのサーバをリブートし、hosts、rhosts、sqlhosts、service などのローカル名解決ファイルを更新します。

（注） システムを再起動しないと、これらのファイルは更新されません。また、これらのファイルを更新した後は、Cisco DB や Cisco Tomcat などのコア ネットワーク サービスを再起動する必要があります。サーバを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、IP アドレスの変更を有効にすることができます。

ステップ 11 すべてのクラスタ ノードで **utils network host** および **show tech network hosts** CLI コマンドを使用して、ステップ 7 で行われたホスト名と IP アドレスの関連付けの変更が他のノードに反映されていることを確認します。

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

すべてのクラスタ ノードで **utils diagnose module validate_network** コマンドを使用する方法もあります。この診断モジュールでは、DNS クライアント サービスが正しく設定されているかどうか、サーバから DNS サーバに接続できるかどうか、順方向（A）レコードと逆方向（PTR）レコードが存在し、サーバの IP アドレスとホスト名に合わせて設定されているかどうかを確認できます。

（注） 変更がすべてのノードに反映されるまで、次の手順に進まないでください。

ステップ 12 パブリッシャ サーバで **utils dbreplication reset all** を実行して、もう一度クラスタ全体のレプリケーションを設定します。

ホスト名で定義されたサーバのホスト名の変更

前提条件のチェックリスト

ホスト名を変更する前に、次の前提条件を実行する必要があります。

- クラスタを監査して、現在のすべてのノードの IP アドレスとホスト名を識別します。
- 外部 DNS サーバに移動し、それを更新する準備が完了していることを確認します。サーバの DNS レコードを変更して新しく変更する IP アドレスを指すようにし、順方向（A）レコードと逆方向（PTR）レコードが正しく更新されるようにします。
- クラスタ ノード間のネットワークが正常に動作しており、クラスタが有効なセキュリティ パスワードを持っていることを確認します。
  - クラスタ ノード間のクラスタ セキュリティ パスワードとネットワークは、パブリッシャ ノードで「show network cluster」CLI コマンドを実行して確認できます。
  - クラスタにあるすべてのノード（パブリッシャ以外）が認証状態になると、クラスタ セキュリティ パスワードが一致していて、パブリッシャからサブスクライバへのネットワーク接続が正しく動作していると見なすことができます。
- サーバを移動する前に、クラスタのデータベース レプリケーションが正しく機能していることを確認します。
  - クラスタのデータベース レプリケーションのステータスは、パブリッシャ ノードで「utils dbreplication runtimestate」CLI コマンドを実行することにより、最もすばやく確認できます。
  - [レプリケーションのセットアップ（RTMT）および詳細（Replication Setup (RTMT) & details）] というカラムは、特定のノードでの現在のデータベース レプリケーションのステータスを示します。クラスタ内でデータベース レプリケーションが正しく動作している場合は、カラムに「(2) Setup Completed」と表示されます。
- クラスタの DRS バックアップを実行します。

（注） DNS サーバは、外部ネットワーク インフラストラクチャを構成する要素の 1 つです。Unified CM ノードは、DNS サービスをホストまたは提供することはできません。

（注） 新しいホスト名がクラスタ間で一意であることを確認してください。DNS サービスを使用している場合は、次に進む前に新しいホスト名で DNS 設定の更新を完了する必要があります。新しいホスト名を認識するには、クラスタ内のすべてのノードを手動でリブートする必要があります。ホスト名を仮想環境で変更した場合は、ライセンスを再ホストする必要があります。

ホスト名で定義されたサーバのホスト名を変更する方法は 2 種類あります。

- 「Unified Communications Operation System Administration GUI を使用したホスト名の変更」（P.14）
- 「Unified Communications Operation System Admin CLI を使用したホスト名の変更」（P.15）

Unified Communications Operation System Administration GUI を使用したホスト名の変更

この手順では、Unified CM で、ホスト名で定義されているパブリッシャまたはサブスクライバ サーバのホスト名を変更するために GUI を使用する方法について説明します。

特に指定のない限り、この手順の各ステップは、パブリッシャおよびサブスクライバ サーバの両方に適用されます。

手順

ステップ 1 「前提条件のチェックリスト」（P.13）の操作を実行します。

ステップ 2 ホスト名と IP アドレスを変更し、必要に応じてデフォルト ゲートウェイを新しいアドレスに変更するには、次の作業を実行します。

a. [設定（Settings）] > [IP] > [イーサネット（Ethernet）] を選択します。

b. ホスト名と IP アドレスを変更し、必要に応じてデフォルト ゲートウェイを新しいアドレスに変更します。

c. [保存（Save）] をクリックすると、サーバが新しい変更内容で自動的にリブートされます。

（注） ホスト名を変更すると、自己署名証明書が自動的に再生成されます。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

（注） クラスタ セキュリティが混合モードにある場合は、サーバが自動的にリブートされた後、CTL クライアントを実行し、CTL ファイルを更新するまで、このサーバへのセキュア接続が失敗します。

ステップ 3 サーバがリブートされたら、ホスト名を変更したサーバの Admin CLI を起動して、**utils dbreplication dropadmin db** コマンドを実行します。

ステップ 4 各サーバで個別に変更が行われた後は、クラスタ全体のリブートが必要です（毎回リブートする必要はありません）。

Cisco Unified Communications Operating System Administration または CLI から、最初にパブリッシャ サーバをリブートし、続いてクラスタ内の他のすべてのサーバをリブートして、hosts、rhosts、sqlhosts、service などのローカル名解決ファイルを更新します。

（注） サーバを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、IP アドレスの変更を有効にすることができます。

ステップ 5 すべてのクラスタ ノードで **utils network host** および **show tech network hosts** CLI コマンドを使用して、ステップ 2 で行われたホスト名と IP アドレスの関連付けが他のノードに反映されていることを確認します。

```
admin:utils network host pub-4
Hostname sub-4 resolves to 198.50.103.11

admin:show tech network hosts
-------------------- show platform network --------------------

/etc/hosts File:
```

```
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

192.0.2.0 localhost
198.51.100.10 pub-1.cisco.com pub-1
198.51.100.11 tftp-1.cisco.com tftp-1
198.51.100.12 tftp-2.cisco.com tftp-2
198.51.100.10 sub-1.cisco.com sub-1
198.51.100.11 sub-3.cisco.com sub-3
198.50.103.10 sub-2.cisco.com sub-2
198.50.103.11 sub-4.cisco.com sub-4
198.51.100.12 sub-5.cisco.com sub-5
198.51.100.13 sub-7.cisco.com sub-7
198.50.101.12 tftp-3.cisco.com tftp-3
198.51.109.20 cups1.heroes.com cups1
198.50.103.13 sub-6.cisco.com sub-6
admin:
```

すべてのクラスタ ノードで **utils diagnose module validate_network** コマンドを使用する方法もあります。この診断モジュールでは、DNS クライアント サービスが設定されているかどうか、DNS サーバに接続できるかどうか、順方向（A）レコードと逆方向（PTR）レコードが存在し、サーバの IP アドレスとホスト名に合わせて設定されているかどうかを確認できます。

注意 新しいホスト名が正しい IP アドレスに解決されない場合は、次の手順に進まないでください。

ステップ 6 パブリッシャ ノードで **utils dbreplication reset all** を実行して、もう一度クラスタ全体のレプリケーションを設定します。

Unified Communications Operation System Admin CLI を使用したホスト名の変更

この手順では、Unified CM で、ホスト名で定義されているパブリッシャまたはサブスクライバ サーバのホスト名を変更するために CLI コマンドを使用する方法について説明します。

特に指定のない限り、この手順の各ステップは、パブリッシャおよびサブスクライバ サーバの両方に適用されます。

手順

ステップ 1 「前提条件のチェックリスト」（P.13）を完了します。

ステップ 2 ホスト名と IP アドレスを変更し、必要に応じてデフォルト ゲートウェイを新しいアドレスに変更するには、次の作業を実行します。

a. CLI コマンド **set network hostname** ホスト名を入力します。

b. **Yes** と入力して Enter キーを押します。このアクションによって、このサーバが新しいホスト名で自動的にリブートされます。

（注） ホスト名を変更すると、自己署名証明書が自動的に再生成されます。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

（注） クラスタ セキュリティが混合モードにある場合は、サーバが自動的にリブートされた後、CTL クライアントを実行し、CTL ファイルを更新するまで、このサーバへのセキュア接続が失敗します。

ステップ 3 サーバがリブートされたら、ホスト名を変更したサーバの Admin CLI を起動して、**utils dbreplication dropadmin db** コマンドを実行します。

ステップ 4 **admin:set network ip eth0 ?** CLI コマンドを使用して、IP アドレスの設定（IP アドレス自体を含む）、ネットワーク マスク、デフォルト ゲートウェイを変更します。

```
admin:set network ip eth0 192.168.1.5 255.255.255.0 192.168.1.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
          ***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================


Continue (y/n)?y
```

ステップ 5 各サーバで個別に変更が行われた後は、クラスタ全体のリブートが必要です（毎回リブートする必要はありません）。

Cisco Unified Communications Operating System Administration または CLI から、最初にパブリッシャ サーバをリブートし、続いてクラスタ内の他のすべてのサーバをリブートして、hosts、rhosts、sqlhosts、service などのローカル名解決ファイルを更新します。

（注） サーバを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、IP アドレスの変更を有効にすることができます。

ステップ 6 すべてのクラスタ ノードで **network host** および **show tech network hosts** CLI コマンドを使用して、ステップ 4 で行われたホスト名と IP アドレスの関連付けが他のノードに反映されていることを確認します。

```
admin:utils network host pub-4
Hostname sub-4 resolves to 198.50.103.11

admin:show tech network hosts
-------------------- show platform network --------------------

/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

192.0.2.0 localhost
198.51.100.10 pub-1.cisco.com pub-1
198.51.100.11 tftp-1.cisco.com tftp-1
```

```
198.51.100.12 tftp-2.cisco.com tftp-2
198.51.100.10 sub-1.cisco.com sub-1
198.51.100.11 sub-3.cisco.com sub-3
198.50.103.10 sub-2.cisco.com sub-2
198.50.103.11 sub-4.cisco.com sub-4
198.51.100.12 sub-5.cisco.com sub-5
198.51.100.13 sub-7.cisco.com sub-7
198.50.101.12 tftp-3.cisco.com tftp-3
198.51.109.20 cups1.heroes.com cups1
198.50.103.13 sub-6.cisco.com sub-6
admin:
```

すべてのクラスタ ノードで utils diagnose module validate_network コマンドを使用する方法もあります。この診断モジュールでは、DNS クライアント サービスが設定されているかどうか、DNS サーバに接続できるかどうか、順方向（A）レコードと逆方向（PTR）レコードが存在し、サーバの IP アドレスとホスト名に合わせて設定されているかどうかを確認できます。

注意 新しいホスト名が正しい IP アドレスに解決されない場合は、次の手順に進まないでください。

ステップ 7 パブリッシャ ノードで utils dbreplication reset all を実行して、もう一度クラスタ全体のレプリケーションを設定します。

変更後の作業リスト

クラスタの IP アドレスを変更した後、次の作業を実行します。

手順

ステップ 1 セキュリティが有効なクラスタ（クラスタ セキュリティ モード 1 - 混合）について、CTL ファイルを更新します。

既存の CTL ファイルへの新しい TFTP サーバの追加など、CTL ファイルの更新と管理の方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』*Release 8.6(1)* を参照してください。

このドキュメントは次の URL にあります。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

ステップ 2 CTL ファイルを更新した後は、クラスタにあるすべてのノードを再起動します。

ステップ 3 アクティブな ServerDown 警告が発生していないか調べ、クラスタにあるすべてのサーバが正常に稼働していて、利用可能であることを確認します。これを確認するには、最初のノードでリアルタイム監視ツール（RTMT）またはコマンドライン インターフェイス（CLI）を使用します。

- RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。
- 最初のノードで CLI を使用して確認するには、次のコマンドを入力してアプリケーションのイベント ログを調べます。

  ```
  file search activelog syslog/CiscoSyslog ServerDown
  ```

ステップ 4 クラスタにあるすべての Cisco Unified Communications Manager ノードでデータベース レプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。これを確認するには、RTMT または CLI コマンドを使用します。

- RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
- CLI を使用して確認するには、次の例のようにコマンドを入力します。

```
admin: utils dbreplication runtime

==>query class :
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created = 344
ReplicateCount -> Replicate_State = 2
```

この場合に Replicate_State オブジェクトが 2 の値を示すことに注意してください。次に、Replicate_State が取ることのできる値を示します。

- 0：レプリケーションは開始されていません。これは、サブスクライバが存在していないか、またはサブスクライバをインストールした後に Database Layer Monitor サービスが実行されていないことが原因です。
- 1：レプリケーションは作成されていますが、そのカウントが正しくありません。
- 2：レプリケーションは正常です。
- 3：このクラスタではレプリケーションが正常に実行されていません。
- 4：レプリケーションのセットアップに失敗しました。

ステップ 5 Cisco Unified レポート ツールで Unified CM Database Status レポートを生成します。そのレポートにエラーや警告が記録されていないか確認します。

ステップ 6 Cisco Unified レポート ツールで Unified CM Cluster Overview レポートを生成します。そのレポートにエラーや警告が記録されていないか確認します。

ステップ 7 **utils netdump** CLI コマンドを使用して、netdump サーバとクライアントを再設定します。詳細については、『Cisco Unified Communications Operating System Administration Guide』の「付録 A」を参照してください。

ステップ 8 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。詳細については、ご使用のリリースの『*Disaster Recovery System Administration Guide*』を参照してください。

（注） ノードの IP アドレスを変更した後は手動で DRS バックアップを実行する必要があります。これは、DRS ファイルでノードを復元するには、DRS ファイルとノードで IP アドレスとホスト名が一致している必要があるからです。変更後の DRS ファイルには、新しい IP アドレスや新しいホスト名が記録されています。

ステップ 9 関連する IP フォンの URL パラメータをすべて更新します。

ステップ 10 Cisco Unified Communications Manager Administration で [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] を選択し、関連する IP フォン サービスをすべて更新します。

ステップ 11 Cisco Unified Communications Manager で終端する IPSec トンネルを更新します。

ステップ 12 次のように RTMT のカスタム警告と保存済みプロファイルを更新します。

- パフォーマンス カウンタから得られた RTMT カスタム警告には、サーバの IP アドレスがハードコードで記録されています。これらのカスタム警告を削除し、再設定する必要があります。

- パフォーマンス カウンタを備えた RTMT 保存済みプロファイルには、サーバの IP アドレスがハードコードで記録されています。これらのカウンタをいったん削除してから追加し直した後、プロファイルを保存して新しい IP アドレスで更新する必要があります。

ステップ 13 Cisco Unified Communications Manager で実行している DHCP サーバを更新します。

ステップ 14 関連する他の Cisco Unified Communications コンポーネントで設定上の変更が必要ないか確認し、適宜変更します。このコンポーネントには次のものがあります。

（注） 必要に応じて設定を変更する方法については、ご使用の製品のマニュアルを参照してください。

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 トランク
- IOS Gatekeeper
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 電話向け DHCP Scopes
- Cisco Unified Communications Manager のトレース収集、CDR エクスポート、または DRS バックアップの保存先として使用する SFTP サーバ
- Cisco Unified Communications Manager に登録されている IOS ハードウェア リソース（会議ブリッジ、メディア ターミネーション ポイント、トランスコーダ、RSVP エージェント）
- Cisco Unified Communications Manager に登録または統合した IPVC ビデオ MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 関連するルータおよびゲートウェイ

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。

http://www.access.gpo.gov/bis/ear/ear_data.html

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/