変更後のタスクと検証

Cisco Unified Communications Manager ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

ステップ 1 Cisco Unified Communications Manager サーバ内で DNS が設定されている場合、正引きおよび逆引き参照ゾーンが設定され、DNS が到達可能で作動していることを確認します。

ステップ 2 アクティブな ServerDown 警告が出ていないことを確認し、クラスタ内のすべてのサーバが稼働していて利用可能であることを確かめます。最初のノードで、Cisco Unified Real-Time Monitoring Tool （RTMT） またはコマンド ライン インターフェイス（CLI）のいずれかを使用します。

a) Unified 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。

b) 最初のノードで CLI を使用して確認するには、次の CLI 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 3 クラスタにあるすべての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。

IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベース パブリッシャ 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ます。

Unified RTMT または CLI を使用します。すべてのノードで **2** のステータスが表示される必要があります。

a) 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。

b) CLI を使用して確認するには、**utils dbreplication runtimestate** を入力します。

出力例については、データベース レプリケーションの出力例に関するトピックを参照してください。詳細な手順およびトラブルシューティングについては、データベース レプリケーションおよびデータベース レプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 4 次の例に示されているように CLI コマンド **utils diagnose** を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
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:
```

変更前のシステム ヘルス チェックを行っている場合には、これで完了です。そうでない場合には、変更後の確認手順を続行してください。

ステップ 5 Cisco Unified Communications Manager サーバ リストに新しいホスト名または IP アドレスがあることを確認します。[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[システム（System）] > [サーバ（Server）]** を選択します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

ステップ 6 IPアドレス、ホスト名、またはその両方に加えられた変更がネットワーク上で確実に実装されていることを確認します。クラスタ内の各ノードで CLI コマンド **show network cluster** を入力します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

出力には、ノードの新しい IP アドレスまたはホスト名が含まれている必要があります。

例：

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber
cups DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher
callmanager DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

ステップ 7 ホスト名に対する変更内容がネットワークで完全に実装されていることを確認します。クラスタ内の各ノードで CLI コマンド **utils network host** <***new_hostname***> を入力します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

出力で、新しいホスト名が対象 IP アドレスに外部解決されていることを確認してください。

例：

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

タスク。

ステップ 8 セキュリティが有効になっているクラスタ（クラスタ セキュリティ モード 1 - 混合）の場合、CTL ファイルを更新し、クラスタ内のすべてのノードを再起動してから、システム ヘルス チェックと他の変更後タスクを実行します。

詳細については、マルチサーバ クラスタ電話機の証明書と ITL の再生成 （6 ページ）を参照してください。

ステップ 9 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した場合、リリース 8.0 以降のノードの IP アドレスまたはホスト名を変更した際は、Initial Trust List（ITL; 初期信頼リスト）ファイルと ITL の証明書を再生成する必要があります。クラスタ セキュリティの有効化に証明書信頼リスト（CTL）ファイルと USB eToken を使用していない場合は、このステップをスキップしてください。

ステップ 10 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、『*Administration Guide for Cisco Unified Communications Manager*』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 11 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 12 [Cisco Unified Communications Manager Administration] を使用して、関連するすべての IP フォン サービスを更新します。**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** と選択します。

ステップ 13 Unified RTMT 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 Unified 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 Unified 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 14 Cisco Unified Communications Manager で動作する統合 DHCP サーバを使用している場合は、DHCP サーバを更新します。

ステップ 15 その他の関連する Cisco Unified Communications コンポーネントに対して、必要な設定変更を検査して実行します。

検査対象のコンポーネントの一部を次に示します。

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity 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
- CDR エクスポート用の Cisco Unified Communications Manager のトレース収集、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

（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 Unified Communications Manager ノードのセキュリティを有効にしたクラスタ タスク

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） 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。

クラスタ セキュリティが有効になっていない場合は、シングルサーバ クラスタまたはマルチサーバ クラスタでこの手順を実行して電話をリセットします。

シングルサーバ クラスタ電話機の証明書と ITL の再生成

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際に、ITL ファイルを使用する場合、以下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。

手順

ステップ 1 更新された ITL を処理できるようにすべての電話機が登録され、オンラインであることを確認します。この手順を実行するときに電話機がオンラインでない場合は、ITL を手動で削除する必要があります。

ステップ 2 Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを True に設定します。すべての電話機は自動的にリセットされ、空の信頼検証サービス（TVS）と 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 3 電話機で、**[設定（Settings）]** > **[セキュリティ（Security）]** > **[信頼リスト（Trust List）]** > **[ITL ファイル（ITL File）]** の順に選択し、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 4 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 5 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。

次のタスク

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 クラスタ電話機の証明書と ITL の再生成

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 クライアントまたは CLI コマンド set **utils ctl** を再実行します。

IM and Presence Service ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。

⚠

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

ステップ 1 ホスト名または IP アドレスに対する変更内容が、Cisco Unified Communications Manager サーバ上で更新されていることを確認します。

ステップ 2 変更したノードのネットワーク接続と DNS サーバの設定を確認してください。

（注） 異なるサブネットに IP アドレスを変更した場合は、ネットワーク アダプタが正しい VLAN に接続されていることを確認します。また、IP アドレスの変更後に IM and Presence Service ノードが別のサブネットに属している場合、Cisco XCP Router サービス パラメータの [ルーティング通信タイプ（Routing Communication Type）] フィールドが [ルータ間（Router to Router）] に設定されていることを確認してください。その他の場合には、[ルーティング通信タイプ（Routing Communication Type）] フィールドは [マルチキャスト DNS（Multicast DNS）] に設定する必要があります。

ステップ 3 IPアドレス、ホスト名、またはその両方への変更がネットワークで完全に実装されていることを確認してください。

ステップ 4 ホスト名を変更した場合は、ネットワークでホスト名の変更が確実に実装されていることを確認します。

ステップ 5 データベース レプリケーションが正常に確立されたことを確認します。すべてのノードのスタータスが2で、[接続済み（Connected）]になっている必要があります。レプリケーションがセットアップされていない場合、データベース レプリケーションのトラブルシューティングに関するトピックを参照してください。

ステップ 6 SAMLシングル サインオン（SSO）を無効にした場合、ここで有効にできます。SAML SSOの詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ステップ 7 ホスト名を変更した場合、cup、cup-xmpp、およびTomcatの証明書に新しいホスト名が含まれていることを確認する必要があります。

a) Cisco Unified OS Administration GUI から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
b) 信頼証明書の名前に新しいホスト名が含まれていることを確認します。
c) 証明書に新しいホスト名が含まれない場合、証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 8 ノードのIPアドレスを変更したら、Cisco Unified Real-Time Monitoring Tool（RTMT）のカスタム アラートと保存済みプロファイルを更新してください。

- 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アドレスで更新する必要があります。

ステップ 9 その他の関連するCisco Unified Communicationsのコンポーネント（たとえばCisco Unified Communications Managerの SIP トランクなど）に必要な設定変更を確認し、変更を行ってください。

ステップ 10 Cisco Unified Serviceabilityを使用してCUPサービス グループの下にリストされるすべてのネットワーク サービスを開始するには、**[ツール（Tools）] > [コントロール センターのネットワーク サービス（Control Center - Network Services）]** を選択します。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。これらの名前を変更した場合、ネットワーク サービスは自動的に開始します。しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべてのネットワーク サービスが確実に開始されるようにしてください。

次の順序で CUP サービスのネットワーク サービスを開始する必要があります。

1. Cisco IM and Presence Data Monitor
2. Cisco Server Recovery Manager
3. Cisco Route Datastore
4. Cisco Login Datastore
5. Cisco SIP Registration Datastore
6. Cisco Presence Datastore
7. Cisco XCP Config Manager
8. Cisco XCP Router
9. Cisco OAM Agent
10. Cisco Client Profile Agent
11. Cisco Intercluster Sync Agent
12. Cisco Config Agent

ステップ 11 Cisco Unified Serviceability を使用してすべての機能サービスを開始するには、**[ツール（Tools）]**>**[コントロール センターの機能サービス（Control Center - Feature Services）]** を選択します。機能サービスを開始する順序は重要ではありません。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。これらの名前を変更した場合、機能サービスは自動的に開始します。しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべての機能サービスが確実に開始されるようにしてください。

ステップ 12 ハイ アベイラビリティを再度有効にする前に Cisco Jabber セッションが再作成されたことを確認します。そうしないと、セッションが作成された Jabber クライアントは接続できなくなります。

すべてのクラスタ ノードで `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行します。アクティブ セッションの数は、ハイ アベイラビリティを無効にした際に記録したユーザ数と一致するはずです。セッションの開始に 30 分以上かかると、システムの問題が大きくなる可能性があります。

ステップ 13 変更前のセットアップ中にハイ アベイラビリティ（HA）を無効にした場合、すべてのプレゼンス冗長グループの HA を有効にします。

ステップ 14 IM and Presence Service が変更後に正しく機能していることを確認します。

a) Cisco Unified Serviceability GUI から、**[システム（System）]**>**[プレゼンス トポロジ（Presence Topology）]** を選択します。

- HA が有効の場合は、すべての HA ノードが [正常（Normal）] 状態であることを確認します。
- すべてのサービスが開始されていることを確認します。

b) Cisco Unified CM IM and Presence Administration GUI からシステム トラブルシュータを実行し、失敗したテストがないことを確認します。**[診断（Diagnostics）]**>**[システム トラブルシュータ（System Troubleshooter）]** を選択します。

ステップ 15 ノードの IP アドレスまたはホスト名を変更した後は、手動でディザスタ リカバリ システム 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。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。