# 변경 후 작업 및 확인



## Cisco Unified Communications Manager 노드에 대한 변경 후 작업

모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

⚠

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

프로시저

단계 **1** Cisco Unified Communications Manager 서버의 모든 곳에 DNS가 구성되어 있는 경우 정방향 및 역방향 조회 영역이 구성되어 있고 DNS에 연결할 수 있으며 작동하는지 확인하십시오.

단계 **2** 모든 활성 ServerDown 알림을 확인하여 클러스터의 모든 서버가 작동하고 사용 가능한지 확인합니다. 첫 번째 노드에서 Cisco Unified Real-Time Monitoring Tool(RTMT) 또는 CLI(command-line interface)를 사용합니다.

a) Unified RTMT를 사용하여 확인하려면 알림 센트럴에 액세스하고 ServerDown 알림을 확인합니다.

b) 첫 번째 노드에서 CLI를 사용하여 확인하려면 다음 CLI 명령을 입력하고 애플리케이션 이벤트 로그를 검사합니다.

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

단계 **3** 클러스터의 모든 노드에서 데이터베이스 복제 상태를 확인하여 모든 서버가 데이터베이스 변경을 성공적으로 복제하고 있는지 확인합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 CLI를 사용하여 데이터베이스 게시자 노드의 데이터베이스 복제 상태를 확인합니다.

통합 RTMT 또는 CLI를 사용합니다. 모든 노드에 **2**의 상태가 표시되어야 합니다.

a) RTMT를 사용하여 확인하려면 데이터베이스 요약에 액세스하고 복제 상태를 검사합니다.
b) CLI를 사용하여 확인하려면 **utils dbreplication runtimestate**를 입력합니다.

   예를 들어 출력은 예제 데이터베이스 복제 출력과 관련된 항목을 참조하십시오. 자세한 절차 및 문제 해결은 데이터베이스 복제 확인 및 문제 해결 데이터베이스 복제와 관련된 항목을 참조하십시오.

단계 **4** 다음 예제와 같이 CLI 명령 **utils diagnose**를 입력하여 네트워크 연결 및 DNS 서버 구성을 확인합니다.

예제:

```
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:
```

변경 전 시스템 상태 확인을 수행하는 경우에는 작업이 완료된 것입니다. 그렇지 않으면 변경 후 확인 단계를 계속 수행합니다.

단계 **5** 새 호스트 이름 또는 IP 주소가 Cisco Unified Communications Manager 서버 목록에 표시되는지 확인합니다. Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

단계 **6** IP 주소, 호스트 이름 또는 둘 다에 대한 변경 사항이 네트워크에서 완벽하게 구현되었는지 확인합니다. 클러스터의 각 노드에 CLI 명령 **show network cluster**를 입력합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

출력에는 노드의 새 IP 주소 또는 호스트 이름이 포함되어야 합니다.

예제:

```
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
```

단계 **7** 호스트 이름에 대한 변경 사항이 네트워크에서 완전히 구현되었는지 확인합니다. 클러스터의 각 노드에 CLI 명령 **utils network host** <***new_hostname***>을 입력합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

출력에서 새 호스트 이름이 IP 주소로 로컬 및 외부에서 해결되는지 확인해야 합니다.

예제:

```
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
```

tasks.

단계 **8** 보안을 사용하는 클러스터(클러스터 보안 모드 1 - 혼합)의 경우 시스템 상태 확인 및 기타 변경 후 작업을 수행하기 전에 CTL 파일을 업데이트하고 클러스터의 모든 노드를 다시 시작합니다.

자세한 내용은 다중 서버 클러스터 전화기에 대한 인증서 및 ITL 재생성, 5 페이지 섹션을 참고하십시오.

단계 **9** CTL(Certificate Trust List) 파일 및 USB eTokens을 사용하여 클러스터 보안을 활성화한 경우, 릴리스 8.0 이상 노드에 대한 IP 주소 또는 호스트 이름을 변경한 경우 ITL(초기 신뢰 목록) 파일 및 ITL의 인증서를 다시 생성해야 합니다. CTL(Certificate Trust List) 파일 및 USB eTokens를 사용하여 클러스터 보안을 활성화하지 않은 경우 이 단계를 건너뜁니다.

단계 **10** 수동 DRS 백업을 실행하여 모든 노드 및 활성 서비스가 성공적으로 백업되도록 합니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

참고 노드의 IP 주소를 변경한 다음에는 반드시 수동 DRS 백업을 실행해야 합니다. 서로 다른 IP 주소 또는 호스트 이름을 포함한 DRS 파일로는 노드를 복원할 수 없기 때문입니다. 변경 후 DRS 파일에 새 IP 주소 또는 호스트 이름이 포함됩니다.

단계 **11** 모든 관련 IP 전화기 URL 매개 변수를 업데이트합니다.

단계 **12** Cisco Unified Communications Manager 관리를 사용하여 관련된 모든 IP 전화기 서비스를 업데이트합니다. 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **13** Unified RTMT 사용자 정의 알림 및 저장된 프로파일을 업데이트합니다.

- 성능 카운터에서 파생되는 Unified RTMT 사용자 정의 알림에는 하드 코딩된 서버 IP 주소가 포함됩니다. 이러한 사용자 정의 알림을 삭제하고 다시 구성해야 합니다.
- 성능 카운터가 있는 Unified RTMT 저장된 프로파일은 하드코딩된 서버 IP 주소를 포함합니다. 이러한 카운터를 삭제하고 다시 추가한 다음 프로파일을 저장하여 새 IP 주소로 업데이트해야 합니다.

단계 **14** Cisco Unified Communications Manager에서 실행되는 통합 DHCP 서버를 사용하는 경우, 해당 DHCP 서버를 업데이트하십시오.

단계 **15** 관련된 다른 Cisco Unified Communications 구성 요소에 필요한 구성을 확인하여 변경합니다.

다음은 확인할 몇 가지 구성 요소의 일부 목록입니다.

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 트렁크
- IOS 게이트키퍼
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express

- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 전화기에 대한 DHCP 범위
- CDR 내보내기에 대한 Cisco Unified Communications Manager 추적 모음 또는 DRS 백업 대상으로 사용되는 SFTP 서버
- Cisco Unified Communications Manager에 등록되는 IOS 하드웨어 리소스(컨퍼런스 브리지, 미디어 종료 지점, 트랜스코더, RSVP 에이전트)
- Cisco Unified Communications Manager를 등록하거나 통합하는 IPVC 비디오 MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 연결된 라우터 및 게이트웨이

참고 필요한 구성을 변경하는 방법을 결정하려면 제품 설명서를 참조하십시오.

# Cisco Unified Communications Manager 노드에 대한 보안 활성화 클러스터 작업

## 초기 신뢰 목록 및 인증서 재생성

Cisco Unified Communications Manager 릴리스 8.0 이상 클러스터에서 서버의 IP 주소 또는 호스트 이름을 변경하는 경우 ITL(Initial Trust List) 파일 및 ITL의 인증서가 다시 생성됩니다. 재생성된 파일은 전화기에 저장된 파일과 일치하지 않습니다.

참고 CTL(Certificate Trust List) 파일 및 USB eToken을 사용하여 클러스터 보안을 활성화하는 경우, 신뢰가 eTokens에 의해 유지되고 eToken이 변경되지 않으므로 다음 절차의 단계를 수행할 필요가 없습니다.

클러스터 보안이 활성화되지 않은 경우 단일 서버 클러스터 또는 다중 서버 클러스터 절차의 단계를 수행하여 전화기를 재설정합니다.

## 단일 서버 클러스터 전화기에 인증서 및 ITL 다시 생성

Cisco Unified Communications Manager 릴리스 8.0 이상 단일 서버 클러스터에서 서버의 IP 주소 또는 호스트 이름을 변경하고 ITL 파일을 사용 중인 경우 다음 단계를 수행하여 전화기를 재설정합니다.

서버의 IP 주소 또는 호스트 이름을 변경하기 전에 롤백을 활성화합니다.

프로시저

단계 **1** 업데이트된 ITL을 처리할 수 있도록 모든 전화기가 온라인 상태이고 등록되어 있는지 확인합니다. 이 절차를 수행할 때 온라인 상태가 아닌 전화기의 경우 ITL을 수동으로 삭제해야 합니다.

단계 **2** 롤백을 위한 준비 클러스터를 8.0 이전 엔터프라이즈 매개 변수를 True로 설정합니다. 모든 전화기는 빈 TVS(신뢰 확인 서비스) 및 TFTP 인증서 섹션을 포함하는 ITL 파일을 자동으로 재설정하고 다운로드합니다.

단계 **3** 전화기에서 설정 > 보안 > 신뢰 목록 > **ITL** 파일을 선택하여 ITL 파일의 TVS 및 TFTP 인증서 섹션이 비어 있는지 확인합니다.

단계 **4** 서버의 IP 주소 또는 호스트 이름을 변경하고 롤백을 위해 구성된 전화기가 클러스터에 등록되도록 합니다.

단계 **5** 모든 전화기가 클러스터에 성공적으로 등록되면 8.0 이전으로 롤백하기 위한 엔터프라이즈 매개 변수 준비 클러스터를 **False**로 설정합니다.

다음에 수행할 작업

CTL 파일 또는 토큰을 사용하는 경우 서버의 IP 주소 또는 호스트 이름을 변경한 후에 CTL 클라이언트를 다시 실행하거나, DNS 도메인 이름을 변경한 후에 CTL 클라이언트를 다시 실행합니다.

## 다중 서버 클러스터 전화기에 대한 인증서 및 ITL 재생성

다중 서버 클러스터에서 전화기에는 재생성된 ITL 파일 및 인증서를 확인하는 기본 및 보조 TV 서버가 있어야 합니다. 전화기가 기본 TV 서버에 연결할 수 없는 경우(최근 구성 변경으로 인해) 보조 서버로 대체됩니다. TV 서버는 전화기에 할당된 CM 그룹으로 식별됩니다.

다중 서버 클러스터에서는 한 번에 하나의 서버에서만 IP 주소 또는 호스트 이름을 변경해야 합니다. CTL 파일 또는 토큰을 사용하는 경우 서버의 IP 주소 또는 호스트 이름을 변경한 후 또는 DNS 도메인 이름을 변경한 후 CTL 클라이언트 또는 CLI 명령 집합 **utils ctl**을 다시 실행합니다.

# IM and Presence Service 노드에 대한 변경 후 작업

모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

⚠

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

프로시저

단계 **1** 호스트 이름 또는 IP 주소에 대한 변경 사항이 Cisco Unified Communications Manager 서버에서 업데이트되는지 확인합니다.

단계 **2** 변경된 노드에서 네트워크 연결과 DNS 서버 구성을 확인합니다.

참고 IP 주소를 다른 서브넷으로 변경한 경우 네트워크 어댑터가 이제 올바른 VLAN에 연결되어 있는지 확인합니다. 마찬가지로, IP 주소를 변경한 후 IM and Presence Service 노드가 다른 서브넷에 속하는 경우에는 Cisco XCP 라우터 서비스 매개 변수의 라우팅 통신 유형 필드가 라우터간으로 설정되어 있는지 확인합니다. 그렇지 않으면 라우팅 통신 유형 필드를 멀티캐스트 DNS로 설정해야 합니다.

단계 **3** IP 주소, 호스트 이름 또는 둘 다에 대한 변경 사항이 네트워크에서 완벽하게 구현되었는지 확인합니다.

단계 **4** 호스트 이름을 변경한 경우 호스트 이름이 네트워크에 완전히 구현되었는지 확인합니다.

단계 **5** 데이터베이스 복제가 성공적으로 설정되었는지 확인합니다. 모든 노드에서 상태를 2로 표시하고 연결되어 있어야 합니다. 복제가 설정되지 않은 경우 데이터베이스 복제 문제 해결 관련 항목을 참조하십시오.

단계 **6** SAML SSO(Single Sign-On, 단일 인증를 비활성화한 경우에는 지금 활성화할 수 있습니다. SAML SSO에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 구축 설명서를 참조하십시오.

단계 **7** 호스트 이름을 변경한 경우 cup, cup-xmpp 및 Tomcat 인증서에 새 호스트 이름이 포함되어 있는지 확인해야 합니다.

a) Cisco Unified OS 관리 GUI에서 보안 > 인증서 관리를 선택합니다.
b) 신뢰 인증서의 이름에 새 호스트 이름이 포함되어 있는지 확인합니다.
c) 인증서에 새 호스트 이름이 포함되어 있지 않으면 인증서를 재생성합니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

단계 **8** 노드의 IP 주소가 변경된 경우 Cisco Unified Real-Time Monitoring Tool(RTMT) 사용자 지정 경고 및 저장된 프로파일을 업데이트합니다.

- 성능 카운터에서 파생되는 RTMT 사용자 지정 경고에는 하드코딩된 서버 주소가 포함됩니다. 이러한 사용자 정의 알림을 삭제하고 다시 구성해야 합니다.
- 성능 카운터가 있는 RTMT 저장된 프로파일은 하드코딩된 서버 주소를 포함합니다. 이러한 카운터를 삭제하고 다시 추가한 다음 프로파일을 저장하여 새 주소로 업데이트해야 합니다.

단계 **9** 다른 관련 Cisco Unified Communications 구성 요소(예: Cisco Unified Communications Manager의 SIP 트렁크)에서 필요한 구성을 확인하여 변경합니다.

단계 **10** Cisco 통합 서비스 가용성을 사용하여 CUP 서비스 그룹 아래에 나열된 모든 네트워크 서비스를 시작하고 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

팁 IP 주소, 호스트 이름 또는 IP 주소와 호스트 이름을 모두 변경하는 경우 이 단계를 완료할 필요가 없습니다. 이러한 이름 변경의 경우 네트워크 서비스가 자동으로 시작됩니다. 그러나, 변경 후에도 일부 서비스가 자동으로 시작되지 않으면 이 단계를 완료하여 모든 네트워크 서비스가 시작되었는지 확인하십시오.

다음 순서에 따라 CUP 서비스 네트워크 서비스를 시작해야 합니다.

1. Cisco IM and Presence 데이터 모니터
2. Cisco 서버 복구 관리자
3. Cisco 라우트 데이터 저장소
4. Cisco 로그인 데이터 저장소
5. Cisco SIP 등록 데이터 저장소
6. Cisco Presence 데이터 저장소
7. Cisco XCP 구성 관리자
8. Cisco XCP 라우터
9. Cisco OAM 에이전트
10. Cisco 클라이언트 프로파일 에이전트
11. Cisco 클러스터 간 동기화 에이전트
12. Cisco 구성 에이전트

단계 **11** Cisco 통합 서비스 가용성을 사용하여 모든 기능 서비스를 시작하려면 도구 > 제어 센터 - 기능 서비스를 선택합니다. 기능 서비스를 시작하는 순서는 중요하지 않습니다.

팁 IP 주소, 호스트 이름 또는 IP 주소와 호스트 이름을 모두 변경하는 경우 이 단계를 완료할 필요가 없습니다. 이러한 이름 변경의 경우 기능 서비스가 자동으로 시작됩니다. 그러나, 변경 후에도 일부 서비스가 자동으로 시작되지 않으면 이 단계를 완료하여 모든 기능 서비스가 시작되었는지 확인하십시오.

단계 **12** 고가용성을 다시 활성화하기 전에 Cisco Jabber 세션이 다시 생성되었는지 확인하십시오. 그렇지 않으면 세션이 생성된 Jabber 클라이언트가 연결할 수 없게 됩니다.

모든 클러스터 노드에서 `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 명령을 실행합니다. 활성 세션 수는 고가용성을 비활성화할 때 기록한 사용자 수와 일치해야 합니다. 세션을 시작하는 데 30분 이상 소요되는 경우 더 큰 시스템 문제가 있을 수 있습니다.

단계 **13** 변경 전 설정 중에 HA를 비활성화한 경우 모든 프레즌스 이중화 그룹에서 HA(고가용성)를 활성화합니다.

단계 **14** 변경 후 IM and Presence Service가 제대로 작동하는지 확인하십시오.

a) Cisco 통합 서비스 가용성 GUI에서 시스템 > 프레즌스 토폴로지를 선택합니다.

- HA가 활성화된 경우 모든 HA 노드가 정상 상태인지 확인합니다.
- 모든 서비스가 시작되었는지 확인합니다.

b) Cisco Unified CM IM and Presence 관리 GUI에서 시스템 문제 해결 도구를 실행하고 실패한 테스트가 없는지 확인합니다. 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **15** 노드의 IP 주소 또는 호스트 이름을 변경한 다음에는 반드시 수동 재해 복구 시스템 백업을 실행해야 합니다. 서로 다른 IP 주소 또는 호스트 이름을 포함한 DRS 파일로는 노드를 복원할 수 없기 때문입니다. 변경 후 DRS 파일에 새 IP 주소 또는 호스트 이름이 포함됩니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.