시스템 백업

백업 개요

일반 백업을 수행하는 것이 좋습니다. 재난 복구 시스템(DRS)을 사용하여 클러스터의 모든 서버에 대해 전체 데이터 백업을 수행할 수 있습니다. 언제든지 자동 백업을 설정하거나 백업을 호출할 수 있습니다.

재난 복구 시스템은 클러스터 수준 백업을 수행하며 중앙 위치로 Cisco Unified Communications Manager 클러스터의 모든 서버에 대한 백업을 수집하고 백업 데이터를 물리적 저장 디바이스에 보관합니다. 백업 파일은 암호화되고 시스템 소프트웨어에서만 열 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 디바이스 설정 및 예약 설정)을 복원합니다. DRS는 drfDevice.xml 및 drfSchedule.xml 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 디바이스 및 일정을 다시 구성할 필요가 없습니다.

시스템 데이터 복원을 수행하면 복원할 클러스터의 노드를 선택할 수 있습니다.

재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.
- 백업 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업 또는 (사용자가 호출한) 수동 백업.
- 원격 sftp 서버에 백업을 보관합니다.

필수 구성 요소 백업

- 버전 요구 사항을 충족하는지 확인하십시오.

- 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
- 모든 IM and Presence Service 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
- 백업 파일에 저장된 소프트웨어 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다. 백업 파일에 저장된 버전이 클러스터 노드에서 실행되는 버전과 일치하도록 소프트웨어 버전을 업그레이드할 때마다 시스템을 백업해야 합니다.

- DRS 암호화는 클러스터 보안 암호에 따라 달라집니다. 백업을 실행할 때 DRS은 암호화를 위해 임의의 암호를 생성한 다음, 임의의 암호를 클러스터 보안 암호로 암호화합니다. 백업하고 복원하는 사이에 클러스터 보안 암호가 변경된 경우 시스템을 복원하기 위해 해당 백업 파일을 사용하려면 백업 당시의 암호가 무엇인지 알고 있거나 보안 암호를 변경/재설정한 후 즉시 백업해야 합니다.
- 원격 디바이스로 백업하려는 경우 SFTP 서버를 설정했는지 확인하십시오. 사용 가능한 SFTP 서버에 관한 자세한 내용은 다음을 참조하십시오. 원격 백업용 SFTP 서버 , 9 페이지

백업 작업 흐름

백업을 구성하고 실행하려면 이러한 작업을 수행합니다. 백업이 실행되는 동안에는 OS 관리 작업을 수행하지 마십시오. 그 이유는 재난 복구 시스템이 플랫폼 API를 잠가 모든 OS 관리 요청을 차단하기 때문입니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용 하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	백업 디바이스 구성, 3 페이지	데이터를 백업할 디바이스를 지정합니다.
단계 **2**	백업 파일의 크기 계산, 4 페이지	SFTP 디바이스에 만들어지는 백업 파일의 크기를 예상합니다.
단계 **3**	다음 옵션 중 하나를 선택합니다. • 예약 백업 구성, 4 페이지 • 수동 백업 시작, 6 페이지	일정에 따라 데이터를 백업하는 백업 일정을 만듭니다. 필요한 경우 수동 백업을 실행합니다.

	명령 또는 동작	목적
단계 **4**	현재 백업 상태 보기, 7 페이지	(선택 사항) 백업의 상태를 확인합니다. 백업이 실행되는 동안 현재 백업 작업의 상태를 확인할 수 있습니다.
단계 **5**	백업 기록 보기, 7 페이지	(선택 사항) 백업 기록 보기

백업 디바이스 구성

최대 10개의 백업 디바이스를 구성할 수 있습니다. 백업 파일을 저장할 위치를 구성하려면 다음 단계를 수행합니다.

시작하기 전에

- 백업 파일을 저장할 SFTP 서버의 디렉터리 경로에 대한 쓰기 권한이 있는지 확인합니다.
- DRS 마스터 상담원이 백업 디바이스 구성의 유효성을 검사하므로 사용자 이름, 암호, 서버 이름 및 디렉터리 경로가 유효한지 확인합니다.

참고 네트워크 트래픽이 덜할 것으로 예상되는 기간 동안 백업을 예약합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 백업 디바이스를 선택합니다.

단계 **2** 백업 디바이스 목록 창에서 다음 중 하나를 수행합니다.

- 새 디바이스를 구성하려면 새로 추가를 클릭합니다.
- 기존 백업 디바이스를 편집하려면 검색 조건을 입력하고 [찾기]를 클릭하고 선택한 항목 편집을 클릭합니다.
- 백업 디바이스를 삭제하려면 백업 디바이스 목록에서 디바이스를 선택하고 선택한 항목 삭제를 클릭합니다.

백업 일정에서 백업 디바이스로 구성된 백업 디바이스는 삭제할 수 없습니다.

단계 **3** 백업 디바이스 이름 필드에 백업 이름을 입력합니다.

백업 디바이스 이름은 영숫자, 공백( ), 대시(-) 및 밑줄(_)만 포함합니다. 다른 문자는 사용하지 마십시오.

단계 **4** 대상 선택 영역의 네트워크 디렉터리에서 다음을 수행합니다.

- 호스트 이름/**IP** 주소 필드에 네트워크 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- 경로 이름 필드에 백업 파일을 저장하려는 디렉터리 경로를 입력합니다.

- 사용자 이름 필드에 유효한 사용자 이름을 입력합니다.
- 암호 필드에 유효한 암호를 입력합니다.
- 네트워크 디렉터리에 저장할 백업 수 드롭다운 목록에서 필요한 백업 수를 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

백업 파일의 크기 계산, 4 페이지

백업 파일의 크기 계산

하나 이상의 선택된 기능에 대한 백업 기록이 있는 경우에만 Cisco Unified Communications Manager는 백업 tar의 크기를 계산합니다.

계산된 크기는 정확한 값이 아니라 백업 tar의 예상 크기입니다. 크기는 이전의 성공적인 백업의 실제 백업 크기에 따라 계산되고, 마지막으로 백업한 이후 구성을 구성이 변경된 경우 다를 수 있습니다.

처음으로 시스템을 백업할 때가 아닌 및 이전 백업이 존재하는 경우에만 이 절차를 사용할 수 있습니다.

이 절차에 따라 SFTP 디바이스에 저장된 백업 tar의 크기를 예상합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.

단계 **2** 기능 선택 영역에서 백업할 기능을 선택합니다.

단계 **3** 예상 크기를 클릭하여 선택한 기능에 대한 백업의 예상 크기를 볼 수 있습니다.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 시스템을 백업합니다.

- 예약 백업 구성, 4 페이지
- 수동 백업 시작, 6 페이지

예약 백업 구성

백업 예약을 최대 10개까지 만들 수 있습니다. 각 백업 일정에 자동 백업 일정, 백업할 기능 집합 및 저장 위치를 포함하여 자체 속성 집합이 있는 경우.

백업 .tar 파일이 임의로 생성되는 암호로 암호화되었는지 확인하십시오. 이 암호는 클러스터 보안 암호를 사용하여 암호화되고 백업 .tar 파일이 함께 저장됩니다. 이 보안 암호를 기억하고 있거나 보안 암호를 변경 또는 재설정한 후 즉시 백업을 수행해야 합니다.

⚠

주의 통화 처리 중단을 방지하고 서비스에 영향을 주지 않으려면 사용량이 적은 시간 동안 백업을 예약합니다.

시작하기 전에

백업 디바이스 구성, 3 페이지

프로시저

단계 **1** 재난 복구 시스템에서 백업스케줄러를 선택합니다.

단계 **2** 일정 목록 창에서 다음 단계 중 하나를 수행하여 새 일정을 추가하거나 기존 일정을 편집합니다.

- 새 일정을 만들려면 새로 추가를 클릭합니다.
- 기존 일정을 구성하려면 [일정 목록] 열에서 이름을 클릭합니다.

단계 **3** 스케줄러 창에서 일정 이름 필드에 일정 이름을 입력합니다.

참고 기본 일정의 이름은 변경할 수 없습니다.

단계 **4** 백업 디바이스 선택 영역에서 백업 디바이스를 선택합니다.

단계 **5** 기능 선택 영역에서 백업할 기능을 선택합니다. 하나 이상의 기능을 선택해야 합니다.

단계 **6** 백업 시작 영역에서 백업을 시작할 날짜 및 시간을 선택합니다.

단계 **7** 빈도 영역에서 백업이 발생하도록 하려는 빈도를 선택합니다. 빈도는 매일 한 번, 주별 및 월별로 설정할 수 있습니다. 주별을 선택하는 경우 백업이 발생할 요일을 선택할 수도 있습니다.

팁 백업 빈도를 화요일부터 토요일까지 발생하는 주별로 설정하려면 기본 설정을 클릭합니다.

단계 **8** 이러한 설정을 업데이트하려면 저장을 클릭합니다.

단계 **9** 다음 옵션 중 하나를 선택합니다.

- 선택한 일정을 활성화하려면 선택한 일정 활성화를 클릭합니다.
- 선택한 일정을 비활성화하려면 선택한 일정 비활성화를 클릭합니다.
- 선택한 일정을 삭제하려면 선택한 항목 삭제를 클릭합니다.

단계 **10** 일정을 활성화하려면 일정 활성화를 클릭합니다.

다음 백업은 설정한 시간에 자동으로 발생합니다.

참고 클러스터의 모든 서버에서 동일한 버전의 Cisco Unified Communications Manager 또는 Cisco IM and Presence Service를 실행 중이고 네트워크를 통해 연결할 수 있는지 확인합니다. 예약 백업 실행 시 연결할 수 없는 서버는 백업되지 않습니다.

다음에 수행할 작업

다음 절차를 수행합니다.

- 백업 파일의 크기 계산, 4 페이지
- (선택 사항) 현재 백업 상태 보기, 7 페이지

수동 백업 시작

시작하기 전에

- 백업 파일에 대한 저장 위치로 네트워크 디바이스를 사용하는지 확인합니다. Unified Communications Manager의 가상화된 구축은 백업 파일을 저장할 테이프 드라이브 사용을 지원하지 않습니다.
- 모든 클러스터 노드에 동일한 버전의 Cisco Unified Communications Manager 또는 IM and Presence Service가 설치되었는지 확인하십시오.
- 백업 프로세스는 원격 서버의 사용 가능한 공간 부족 또는 네트워크 연결 중단으로 인해 실패할 수 있습니다. 백업이 실패한 원인이 되는 문제를 해결한 후 새로운 백업 시작해야 합니다.
- 네트워크 중단이 없는지 확인하십시오.
- 백업 디바이스 구성, 3 페이지
- 백업 파일의 크기 계산, 4 페이지
- 클러스터 보안 암호에 대한 기록이 있는지 확인합니다. 이 백업을 완료한 후 클러스터 보안 암호가 변경되는 경우 암호를 알고 있어야 합니다. 그렇지 않으면 백업 파일을 사용하여 시스템을 복원할 수 없습니다.

참고 백업이 실행되는 동안 재난 복구 시스템이 플랫폼 API를 잠가 모든 요청을 차단하기 때문에 Cisco Unified OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 작업을 수행할 수 없습니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.
단계 **2** 수동 백업 창의 백업 디바이스 이름 영역에서 백업 디바이스를 선택합니다.
단계 **3** 기능 선택 영역에서 기능을 선택합니다.
단계 **4** 백업 시작을 클릭합니다.

다음에 수행할 작업

(선택 사항) 현재 백업 상태 보기, 7 페이지

현재 백업 상태 보기

현재 백업 작업의 상태를 확인하려면 다음 단계를 수행합니다.

주의 원격 서버에 대한 백업이 20시간 내에 완료되지 않을 경우 백업 세션 시간이 초과되고 새로 백업을 시작해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 현재 상태를 선택합니다.
단계 **2** 백업 로그 파일을 보려면 로그 파일 이름 링크를 클릭합니다.
단계 **3** 현재 백업을 취소하려면 백업 취소를 클릭합니다.

참고 현재 구성 요소가 백업 작업을 완료한 후에 백업을 취소합니다.

다음에 수행할 작업

백업 기록 보기, 7 페이지

백업 기록 보기

백업 기록을 보려면 다음 단계를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 기록을 선택합니다.

단계 **2** 백업 기록 창에서 파일 이름, 백업 디바이스, 완료 날짜, 결과, 버전, 백업된 기능 및 실패한 기능을 포함하여 수행한 백업을 볼 수 있습니다.

참고 백업 기록 창에는 마지막 20개 백업 작업만 표시됩니다.

백업 상호 작용 및 제한 사항

백업 제한 사항

백업에 다음과 같은 제한 사항이 적용됩니다.

표 *1:* 백업 제한 사항

제한 사항	설명
클러스터 보안 암호	클러스터 보안 암호를 변경할 때마다 백업을 실행하는 것이 좋습니다. 백업 암호화는 클러스터 보안 암호를 사용하여 백업 파일의 데이터를 암호화합니다. 백업 파일을 만든 후 클러스터 보안 암호를 편집하는 경우 기존 암호가 기억나지 않으면 해당 백업 파일을 사용하여 데이터를 복원할 수 없습니다.
인증서 관리	재난 복구 시스템(DRS)은 Cisco Unified Communications Manager 클러스터 노드 사이에 인증 및 데이터 암호화를 위해 마스터 상담원과 로컬 상담원 간에 SSL 기반 통신을 사용합니다. DRS은 공개/개인 키 암호화를 위해 IPsec 인증서를 사용합니다. 인증서 관리 페이지에서 IPSEC truststore(hostname.pem) 파일을 삭제하는 경우 DRS는 예상대로 작동하지 않습니다. IPSEC-trust 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC-trust로 업로드해야 합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서의 “인증서 관리” 섹션을 참조하십시오.

원격 백업용 SFTP 서버

데이터를 네트워크의 원격 디바이스에 백업하려면 SFTP 서버를 구성해야 합니다. 내부 테스트의 경우 Cisco는 Cisco에서 제공하고 Cisco TAC에서 지원하는 Cisco Prime Collaboration Deployment(PCD)의 SFTP 서버를 사용합니다. SFTP 서버 옵션에 대한 요약은 다음 표를 참조하십시오.

다음 표에 있는 정보를 사용하여 시스템에서 사용하는 SFTP 서버 솔루션을 확인합니다.

표 *2: SFTP* 서버 정보

SFTP 서버	정보
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공 및 테스트하고 Cisco TAC에서 완벽하게 지원하는 유일한 SFTP 서버입니다. 버전 호환성은 Unified Communications Manager 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Unified Communications Manager를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 *Cisco Prime Collaboration Deployment* 관리 설명서를 참조하십시오.
기술 파트너의 SFTP 서버	이러한 서버는 타사에서 제공하고 타사에서 테스트했습니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지에서 버전 호환성 여부를 참조하십시오. https://marketplace.cisco.com
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Unified Communications Manager 버전의 호환성을 위해 최대한 노력합니다. 참고 이러한 제품은 Cisco에서 테스트하지 않았으므로 기능을 보증할 수 없습니다. Cisco TAC는 이러한 제품을 지원하지 않습니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

암호화 지원

Unified Communications Manager 11.5의 경우 Unified Communications Manager는 SFTP 연결에 대해 다음 CBC 암호화를 광고합니다.

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr

- aes256-ctr

참고 백업 SFTP 서버가 이러한 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.

Unified Communications Manager 12.0 릴리스부터는 CBC 암호화가 지원되지 않습니다. Unified Communications Manager는 다음 CTR 암호화만 지원하고 광고합니다.

- aes256-ctr
- aes128-ctr
- aes192-ctr

참고 백업 SFTP 서버가 이러한 CTR 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.