TAC를 사용하여 케이스 열기

이 섹션에서는 TAC 및 TAC 직원과 공유하는 방법에 대한 정보를 제공하는 데 필요한 정보 유형에 대한 세부 정보를 제공합니다.

유효한 Cisco 서비스 계약을 맺은 모든 고객, 파트너, 리셀러 및 유통업체의 경우 Cisco 기술 지원 부서는 하루 24시간, 수상 경력에 빛나는 기술 지원을 제공합니다. Cisco 기술 지원 웹 사이트는 Cisco 제품 및 기술 관련 문제를 해결할 수 있는 온라인 문서 및 도구를 제공합니다. 웹 사이트는 하루 24시간, 365일 *http://www.cisco.com/techsupport* URL에 사용 가능 상태로 유지됩니다.

가장 신속하게 S3 및 S4 서비스 요청을 하려면 온라인 TAC 서비스 요청 도구를 사용합니다. (S3 및 S4 서비스 요청은 네트워크가 약간 손상되었거나 사용자가 제품 정보를 요구하는 상황을 지정합니다.) 상황을 설명하고 나면 TAC 서비스 요청 도구는 자동으로 권장 솔루션을 제공합니다. 권장 자원을 사용하여 문제를 해결할 수 없으면 서비스 요청이 Cisco TAC 엔지니어에게 할당됩니다. *http://www.cisco.com/techsupport/servicerequest* URL에서 TAC 서비스 요청 도구를 찾습니다.

S1 또는 S2 서비스 요청을 하거나 인터넷으로 액세스할 수 없는 경우 Cisco TAC에 전화로 문의하십시오. (S1 또는 S2 서비스 요청은 운영 네트워크가 작동하지 않거나 심각한 성능 저하가 있는 상황을 나타냅니다.) 비즈니스 운영을 원활하게 유지할 수 있도록 S1 및 S2 서비스 요청은 즉시 Cisco 엔지니어에게 할당됩니다.

전화로 서비스 요청을 열려면 다음 번호 중 하나를 사용하십시오.

아시아 태평양: +61 2 8446 7411(오스트레일리아: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

Cisco TAC 연락처의 전체 목록을 보려면 다음 URL *http://www.cisco.com/techsupport/contacts*을 방문하십시오.

• 원격 계정 설정, 7 페이지

필요한 정보

Cisco TAC에서 케이스를 열 때 문제를 더 잘 파악하고 정규화하려면 사전 정보를 제공해야 합니다. 문제의 성격에 따라 추가 정보를 제공해야 할 수도 있습니다. 서비스 케이스를 연 후 엔지니어 요청이 있을 때까지 다음 정보를 수집하기 위해 대기하면 해결 지연이 발생합니다.

관련 항목

Cisco Live!, 5 페이지
Cisco 보안 텔넷, 6 페이지
일반 정보, 3 페이지
네트워크 레이아웃, 2 페이지
온라인 케이스, 4 페이지
문제 설명, 3 페이지
Remote Access, 5 페이지
필수 예비 정보, 2 페이지

필수 예비 정보

모든 문제에 대해 다음 정보를 항상 TAC에 제공하십시오. 이 정보를 수집 및 저장하여 TAC 케이스를 열고 변경 사항에 따라 정기적으로 업데이트합니다.

관련 항목

일반 정보, 3 페이지
네트워크 레이아웃, 2 페이지
문제 설명, 3 페이지

네트워크 레이아웃

물리적 및 논리적 설정에 대한 자세한 설명과 음성 네트워크에 관련된 모든 네트워크 요소(해당하는 경우)를 제공합니다.

- Unified Communications Manager
  - 버전(Unified Communications Manager 관리에서 세부 정보 선택)
  - Unified Communications Manager의 수
  - 설정(독립 실행형, 클러스터)
    - Unity
  - 버전(Unified Communications Manager 관리에서)

- 통합 유형
  - 애플리케이션
- 설치된 애플리케이션 목록
- 각 애플리케이션의 버전 번호
  - IP/음성 게이트웨이
- OS 버전
- 기술 표시(IOS 게이트웨이)
- Unified Communications Manager 로드(Skinny 게이트웨이)
  - 전환
- OS 버전
- VLAN 컨피그레이션
  - 다이얼 계획 - 번호 매기기 방식, 통화 라우팅

이상적으로는 Visio 또는 JPG와 같은 기타 세부 다이어그램을 제출합니다. 화이트보드를 사용하여 Cisco Live! 세션을 통해 다이어그램을 제공 할 수도 있습니다.

문제 설명

문제가 발생할 때 사용자가 수행한 작업에 대한 단계별 세부 정보를 제공합니다. 세부 정보에 다음이 포함되어 있는지 확인하십시오.

- 예상된 동작
- 관찰된 세부 동작

일반 정보

다음 정보를 사용할 수 있는지 확인하십시오.

- 새로운 설치입니까?
- 이전 버전의 Unified Communications Manager 설치인 경우 이 문제가 처음부터 발생했습니까? (그렇지 않은 경우 최근에 시스템에 수행한 변경 사항은 무엇입니까?)
- 문제를 재현할 수 있습니까?
  - 재현할 수 있는 경우 정상 또는 특별한 상황입니까?
  - 재현할 수 없는 경우 발생할 때 특별한 점이 있습니까?

- 발생 빈도는 어떻습니까?

- 영향을 받는 장치는 무엇입니까?
  - 특정 장치가 영향을 받는 경우(임의) 공통점은 무엇입니까?
  - 문제에 관련된 모든 장치에 대한 DN 또는 IP 주소(게이트웨이)를 포함하십시오.
- 통화 경로에 있는 장치는 무엇입니까(해당되는 경우)?

온라인 케이스

Cisco.com을 통해 온라인으로 케이스를 열면 다른 모든 케이스 열기 방법보다 초기 우선 순위가 부여됩니다. 우선 순위가 높은 케이스(P1 및 P2)는 이 규칙에 대한 예외를 제공합니다.

케이스를 열 때 정확한 문제 설명을 제공합니다. 문제에 대한 설명은 즉각적인 솔루션을 제공할 수 있는 URL 링크를 반환합니다.

문제에 대한 해결 방법을 찾을 수 없는 경우에는 해당 케이스를 TAC 엔지니어에게 보내는 과정을 계속 진행합니다.

서비스 가용성 커넥터

서비스 가용성 커넥터 개요

Webex 서비스 가용성 서비스를 사용하여 로그를 쉽게 수집할 수 있습니다. 이 서비스는 진단 로그 및 정보의 찾기, 검색 및 저장 작업을 자동화합니다.

이 기능은 사용자의 온프레미스에 배포된 서비스 가용성 커넥터를 사용합니다. 서비스 가용성 커넥터는 네트워크의 전용 호스트(' 커넥터 호스트')에서 실행됩니다. 다음 구성 요소 중 하나에 커넥터를 설치할 수 있습니다.

- 엔터프라이즈 컴퓨팅 플랫폼(ECP) — 권장

  ECP는 Docker 컨테이너를 사용하여 서비스를 격리, 보호 및 관리합니다. 호스트 및 서비스 가용성 커넥터 애플리케이션이 클라우드에서 설치됩니다. 최신 상태 및 보안을 유지하기 위해 수동으로 업그레이드할 필요는 없습니다.

  중요 ECP를 사용하는 것이 좋습니다. 향후 개발은 이 플랫폼에 중점을 둘 것입니다. Expressway에 서비스 가용성 커넥터를 설치하는 경우 몇 가지 새로운 기능을 사용할 수 없습니다.

- Cisco Expressway

다음과 같은 목적으로 서비스 가용성 커넥터를 사용할 수 있습니다.

- 서비스 요청에 대한 자동 로그 및 시스템 정보 검색
- Cloud-Connected UC 구축의 통합 CM 클러스터 로그 수집

두 사용 사례 모두에 대해 동일한 서비스 가용성 커넥터를 사용할 수 있습니다.

서비스 가용성 서비스 사용의 이점

이 서비스는 다음과 같은 이점을 제공합니다.

- 로그 수집 속도를 빠르게 합니다. TAC 엔지니어가 문제 진단을 수행하는 동안 관련 로그를 검색할 수 있습니다. 추가 로그를 요청하고 수동 수집 및 전달을 기다리는 지연을 방지할 수 있습니다. 이 자동화는 문제 해결 시간을 며칠 정도 단축시킬 수 있습니다.
- TAC의 협업 솔루션 분석기 및 해당 진단 서명 데이터베이스와 함께 작동합니다. 시스템은 자동으로 로그를 분석하고 알려진 문제를 식별하며 알려진 수정 사항 또는 해결 방법을 권장합니다.

서비스 가용성 커넥터에 대한 TAC 지원

서비스 가용성 커넥터에 대한 자세한 내용은 https://www.cisco.com/go/serviceability을 참조하거나 TAC 담당자에게 문의하십시오.

Cisco Live!

안전하고 암호화된 Java 애플릿인 Cisco Live!를 사용하면 사용자와 Cisco TAC 엔지니어가 협업 웹 브라우징/URL 공유, 화이트보드, 텔넷 및 클립보드 도구를 사용하여 더 효과적으로 공동 작업을 수행할 수 있습니다.

Cisco Live! 액세스 URL은 다음과 같습니다.

`http://c3.cisco.com/`

Remote Access

원격 접속은 모든 필요한 장비에 터미널 서비스(원격 포트 3389), HTTP(원격 포트 80) 및 텔넷(원격 포트 23) 세션을 설정할 수 있는 기능을 제공합니다.

⚠

주의 다이얼인을 설정할 때 시스템이 취약해지므로 로그인**:cisco** 또는 암호**:cisco**는 사용하지 마십시오.

다음 방법 중 하나를 사용하여 장치에 대한 TAC 엔지니어 원격 접속을 허용함으로써 많은 문제를 신속하게 해결할 수 있습니다.

- 공개 IP 주소가 있는 장치.

- 다이얼인 액세스 - 기본 설정의 내림 차순으로 아날로그 모뎀, ISDN(Integrated Service Digital Network) 모뎀, VPN(Virtual Private Network)을 선택합니다.
- NAT(Network Address Translation) - 개인 IP 주소가 있는 장비에 대한 액세스를 허용하기 위한 IOS 및 PIX(사설 인터넷 교환).

엔지니어 간섭 중에 방화벽에서 IOS 트래픽 및 PIX 트래픽을 방해하지 않으며, 터미널 서비스와 같은 필요한 모든 서비스가 서버에서 시작되는지 확인합니다.

참고 TAC는 모든 액세스 정보를 최대한 신중하게 처리하며, 고객 동의 없이 변경 사항이 시스템에 적용되지 않습니다.

Cisco 보안 텔넷

Cisco 보안 텔넷은 사이트의 Unified Communications Manager 서버에 Cisco의 CSE(Cisco Service 엔지니어) 투명 방화벽 액세스를 제공합니다.

Cisco 보안 텔넷은 방화벽 뒤에 있는 텔넷 데몬에 연결하기 위해 Cisco Systems 방화벽 내에서 텔넷 클라이언트를 활성화하여 작동합니다. 이 보안 연결을 사용하면 방화벽을 수정할 필요 없이 Unified Communications Manager 서버의 원격 모니터링 및 유지 관리를 수행할 수 있습니다.

참고 Cisco는 사용자가 허가한 경우에만 사용자 네트워크에 액세스합니다. 프로세스를 시작하는 데 도움이 되도록 사이트에서 네트워크 관리자를 제공해야 합니다.

방화벽 보호

사실상 모든 내부 네트워크는 방화벽 애플리케이션을 사용하여 내부 호스트 시스템에 대한 외부 액세스를 제한합니다. 이러한 애플리케이션은 네트워크와 공용 인터넷 간의 IP 연결을 제한하여 네트워크를 보호합니다.

방화벽은 이런 액세스를 허용하도록 소프트웨어를 다시 구성하지 않는 한 외부에서 시작된 TCP/IP 연결을 자동으로 차단하도록 작동합니다.

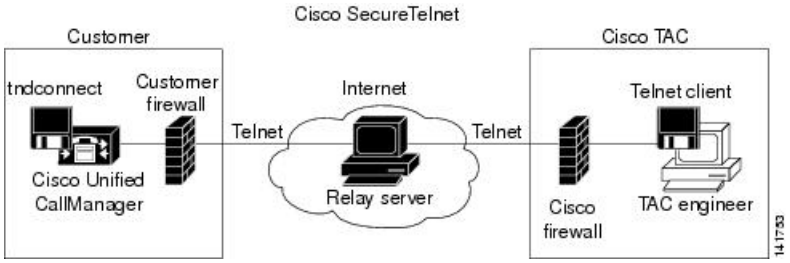
회사 네트워크는 일반적으로 공용 인터넷과의 통신을 허용하지만, 외부 호스트에 대한 연결이 방화벽 내부에서 시작되는 경우에만 가능합니다.

Cisco 보안 텔넷 설계

Cisco 보안 텔넷은 텔넷 연결을 방화벽 뒤에서 쉽게 시작할 수 있다는 사실을 이용합니다. 시스템은 외부 프록시 시스템을 사용하여 방화벽의 뒤에 있는TCP/IP 통신을 *Cisco* 기술 지원 센터(TAC)에서 다른 방화벽 뒤에 있는 호스트로 릴레이합니다.

이 릴레이 서버를 사용하면 두 방화벽의 무결성을 유지하면서 보호된 원격 시스템 간의 보안 통신이 지원됩니다.

그림 *1: Cisco* 보안 텔넷 시스템



Cisco 보안 텔넷 구조

외부 릴레이 서버는 텔넷 터널을 작성하여 네트워크와 Cisco 시스템 간의 연결을 설정합니다. 이를 통해 Unified Communications Manager 서버의 IP 주소 및 암호 식별자를 CSE로 전송할 수 있습니다.

참고 암호는 관리자와 CSE가 상호 일치하는 텍스트 문자열로 구성됩니다.

관리자가 방화벽 내부에서 공용 인터넷의 릴레이 서버로 TCP 연결을 설정하는 텔넷 터널을 시작하여 프로세스를 시작합니다. 그런 다음 텔넷 터널은 로컬 텔넷 서버에 또 다른 연결을 설정하여 엔터티 간에 양방향 링크를 만듭니다.

참고 Cisco TAC의 텔넷 클라이언트는 Windows NT 및 Windows 2000 또는 UNIX 운영 체제에서 실행되는 시스템을 준수하여 실행됩니다.

사이트의 Cisco Communications Manager에서 암호를 승인한 후에는 Cisco TAC에서 실행되는 텔넷 클라이언트가 방화벽 뒤에서 실행되는 텔넷 데몬에 연결됩니다. 결과적으로 투명한 연결은 시스템을 로컬로 사용하는 것과 동일한 액세스를 허용합니다.

텔넷 연결이 안정화된 후에는 CSE가 모든 원격 서비스 가용성 기능을 구현하여 Unified Communications Manager 서버에서 유지 보수, 진단 및 문제 해결 작업을 수행할 수 있습니다.

CSE에서 전송하는 명령과 Unified Communications Manager 서버에서 발생하는 응답을 볼 수 있지만, 명령과 응답은 항상 완전히 포맷되지 않을 수 있습니다.

원격 계정 설정

Cisco 지원이 일시적으로 문제 해결을 위해 시스템에 액세스할 수 있도록 Unified Communications Manager에서 원격 계정을 구성합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 서비스 > 원격 지원을 선택합니다.

단계 **2** 계정 이름 필드에 원격 계정의 이름을 입력합니다.

단계 **3** 계정 기간 필드에 계정 기간(일)을 입력합니다.

단계 **4** 저장을 클릭합니다.
시스템에서 암호화된 암호구를 생성합니다.

단계 **5** Cisco 지원에 연락하여 원격 지원 계정 이름 및 암호를 제공하십시오.