Cisco TMS에 대한 시스템 피드백 네트워크 또는 웹 서버에 의해 차단됨

목차

소개

이 문서에서는 네트워크 또는 웹 서버에서 차단되는 Cisco TelePresence Management Suite(TMS)에 대한 피드백 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco TMS에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco TMS를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Cisco TMS에 대한 시스템 피드백 네트워크 또는 웹 서버에 의해 차단됨

Cisco TMS는 시스템에서 보낸 피드백을 바탕으로 시리얼 번호, MAC 주소 및 IP 주소를 기반으로

엔드포인트에 연결하는 엔드포인트를 확인합니다.대부분의 Cisco TelePresence 및 서드파티 시스템은 익명 HTTP 또는 HTTPS 연결로 이 피드백을 보냅니다. 이 피드백은 인증이 필요한 네트워크에 웹 프록시가 있는 경우 차단될 수 있습니다.이 경우 프록시 관리자에게 문의하여 Cisco TMS로 향하는 트래픽에 대한 예외를 추가해야 합니다.

또한 방화벽이 시스템에서 Cisco TMS로의 새 연결을 차단할 경우 Cisco TMS에 대한 피드백을 차단할 수 있습니다.

> **팁**:Cisco TMS 지원 설명서에서는 각 시스템 유형에 사용할 수 있는 포트 및 프로토콜을 간략하게 설명합니다.

마지막으로 일반적인 연결 오류는 Cisco TMS가 설치된 후 관리자가 IIS(인터넷 정보 서비스) 구성을 수동으로 수정하고 웹 디렉터리에 대한 익명 액세스를 비활성화하는 경우에 발생합니다.

> **참고:**익명 액세스는 Cisco TMS의 특정 부분에만 열려 있으며, 시스템에서 피드백을 보낼 때 사용자 이름과 비밀번호를 사용하지 않으므로 비활성화하지 않아야 합니다.

IIS 구성 오류를 수정하려면 Cisco TMS를 제거한 후 다시 설치하십시오.데이터베이스가 그대로 유지되고 설치 프로그램이 웹 사이트 속성을 올바르게 재구축하는 경우 데이터가 손실되지 않습니다.