Agent Assist 솔루션과의 통합을 위해 NGINX 프록시 구성

목차

소개

이 문서에서는 Cisco Agents Assist 솔루션과의 통합을 위해 NGINX 프록시 서버를 구성하는 방법에 대해 설명합니다.

기고자: Guraj B. T. 및 Ramiro Amaya, Cisco 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CUBE(Unified Border Element)
- Webex Contact Center WCACI(인공 인텔리전스 서비스)
- NGINX 프록시
- 보안 인증서 교환

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco CUBE(Unified Border Element)
- Webex Contact Center WCACI(인공 인텔리전스 서비스)
- NGINX 프록시
- 웹 소켓 커넥터(WSConnector)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경

Agent Answers 구축에서 CUBE는 WCACI 서비스의 일부로 구축된 WSConnector 서비스와 통신합니다. 통신을 설정하려면 CUBE에 인터넷 액세스가 필요합니다. 일부 기업에서는 솔루션 구성 요소에 직접 인터넷 액세스를 제공할 수 없습니다. 이 시나리오에서는 WebSocket을 지원하는 프록시의 사용을 권장합니다. 이 문서에서는 웹 소켓을 지원하는 NGINX 프록시에 필요한 컨피그레이션에 대해 설명합니다.

구성

구축

CUBE —<websocket>—NGINX 프록시 —<websocket>—WSconnector

현재 CUBE는 CUBE에서 WSConnector로 TCP 연결을 터널링하는 CONNECT 메서드를 지원하지 않습니다. Cisco는 프록시를 통한 hop-by-hop 연결을 권장합니다. 이 구축에서는 NGINX가 들어오는 레그의 CUBE와 아웃바운드 레그의 다른 보안 연결을 WSConnector로 연결했습니다

NGINX 설치 세부 정보

OS 세부 정보: Cent OS centos-release-7-8.2003.0.el7.centos.x86_64
NGINX 버전: nginx/1.19.5

구성 단계

1단계. NGINX 설치: NGINX 포털의 설치 단계를 따릅니다. 다음 링크를 따릅니다. NGINX 관리 설명서.

2단계. NGINX 자체 서명 인증서 및 키 생성. NGINX 프록시 서버에서 다음 명령을 실행합니다.

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt

3단계. nginx**.conf** 파일**을** 편집합니다.

worker_processes 1;
error_log logs/error.log 디버그

이벤트 {
worker_connections 1024;
}
http {
mime.types 포함
default_type application/octet-stream

전송 날짜
keepalive_timeout 65;
서버{
8096 ssl 수신
server_name ~.+;
전달 프록시에 사용되는 dns 확인자 수
해결 프로그램 <DNS _Server IP:PORT>;
proxy_read_timeout 86400s;
proxy_send_timeout 86400s;
client_body_timeout 86400s;
keepalive_timeout 86400s;
비 CONNECT 요청에 대한 전달 프록시 수
위치 / {
proxy_pass https://$http_host;
proxy_http_version 1.1
proxy_set_header 업그레이드 $http_upgrade;
proxy_set_header 연결 $connection_upgrade;
proxy_set_header 호스트 $host;
proxy_ssl_certificate <nginx_selfsigned_certificate>;
proxy_ssl_certificate_key <nginx_certificate_key_path>;
proxy_ssl_trusted_certificate <WsConnector CA 인증서>;
proxy_ssl_protocols TLSv1.2;
}
#ssl
ssl_certificate <nginx_selfsigned_certificate_path>;
ssl_certificate_key <nginx_certificate_key_path>;
ssl_session_cache 공유:SSL:1m;
ssl_session_timeout 5m;
ssl_ciphers 높음:!aNULL:!MD5;
ssl_prefer_server_ciphers 켜짐
}

}

4단계. NGINX 프록시의 상태를 확인하려면 다음 명령을 실행합니다. **systectl 상태 nginx**

다음을 확인합니다.

다음은 NGINX 컨피그레이션을 확인하는 데 사용할 수 있는 몇 가지 명령입니다.

a. NGNIX 컨피그레이션이 올바른지 확인합니다.
nginx -t
b. nginx 서버를 다시 시작하려면
systectl restart nginx
c. nginx 버전을 확인하려면
nginx -V
d. nginx를 중지하려면
systectl stop nginx
e. nginx를 시작하려면
systemctl 시작 nginx

문제 해결

이 컨피그레이션을 트러블슈팅하는 단계는 없습니다.

관련 정보

- NGINX 관리 설명서
- 유용한 NGINX 명령 예
- NGINX용 자체 서명 ssl 인증서를 만드는 방법
- **기술 지원 및 문서 – Cisco Systems**