配置NGINX代理以便與代理協助解決方案整合

目錄

簡介

本文檔介紹如何配置NGINX代理伺服器以與Cisco Agents Assist解決方案整合。

作者：Gurururaj B. T.和思科工程師Ramiro Amaya。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合邊界元件(CUBE)
- Webex客服中心人工智慧服務(WCCAI)
- NGINX代理
- 安全證書交換

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科整合邊界元件(CUBE)
- Webex客服中心人工智慧服務(WCCAI)
- NGINX代理
- Web插座聯結器(WSConnector)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

在Agent Answers部署中，CUBE與作為WCAI服務的一部分部署的WSConnector服務通訊。為了建立通訊，CUBE需要訪問Internet。有些企業對解決方案元件提供直接Internet訪問受到限制。在此案例中，思科建議使用支援WebSocket的Proxy。本檔案將說明支援Websocket的NGINX代理的必要組態。

設定

部署

CUBE ----<websocket> - NGINX代理服----器<websocket> - WSconnector

目前，CUBE不支援將TCP連線從CUBE隧道連線到WSConnector的CONNECT方法。思科建議透過代理進行逐跳連線。通過此部署，NGINX具有從傳入分支上的CUBE到傳出分支上的安全連線以及另一個指向WSConnector的安全連線

NGINX安裝詳細資訊

作業系統詳細資訊：Cent OS centos-release-7-8.2003.0.el7.centos.x86_64
NGINX版本：nginx/1.19.5

配置步驟

步驟1.安裝NGINX:按照NGINX門戶的安裝步驟操作。請點選此連結：NGINX管理員指南。

步驟2.建立NGINX自簽名證書和金鑰。在NGINX代理伺服器上執行以下命令：

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

步驟3.編輯**nginx.conf**檔案。

```
worker_processes 1;
error_log logs/error.log debug;

活動{
worker_connections 1024;
}
http {
包括mime.types;
default_type application/octet-stream;
sendfile on;
keepalive_timeout 65;
伺服器{
偵聽8096 ssl;
server_name ~.+;
轉發代理使用的dns解析器數量
```

```
解析程式<DNS _Server IP:PORT>;
proxy_read_timeout 86400s;
proxy_send_timeout 86400s;
client_body_timeout 86400s;
keepalive_timeout 86400s;
#用於非CONNECT請求的轉發代理
位置/ {
proxy_pass https://$http_host;
proxy_http_version 1.1;
proxy_set_header升級$http_upgrade;
proxy_set_header Connection $connection_upgrade;
proxy_set_header主機$host;
proxy_ssl_certificate <nginx_selfsigned_certificate>;
proxy_ssl_certificate_key <nginx_certificate_key_path>;
proxy_ssl_trusted_certificate <WsConnector CA Certificate>;
proxy_ssl_protocolsv1.2;
}
#ssl;
ssl_certificate <nginx_selfsigned_certificate_path>;
ssl_certificate_key <nginx_certificate_key_path>;
ssl_session_cache shared:SSL:1m;
ssl_session_timeout 5m;
ssl_ciphers HIGH:!aNULL:!MD5;
ssl_prefer_server_ciphers on;
 }

}
```

步驟4.要檢查NGINX代理的狀態，請執行以下命令：**systemctl status nginx**

驗證

以下是可用於驗證NGINX配置的一些命令。

a.檢查NGNIX配置是否正確。
nginx -t
b.重新啟動nginx伺服器
systemctl restart nginx
c.檢查nginx版本
nginx -V
d.為了阻止敵軍
systemctl stop nginx
e.啟動nginx
systemctl start nginx

疑難排解

沒有步驟可對此配置進行故障排除。

相關資訊

- NGINX管理員指南
- 有用的NGINX命令示例
- 如何為NGINX建立自簽名ssl證書
- **技術支援與文件 - Cisco Systems**