Configurer le proxy NGINX pour l'intégration avec une solution d'assistance d'agent

Contenu

Introduction

Ce document décrit comment configurer un serveur proxy NGINX pour une intégration avec une solution Cisco Agents Assist.

Contribué par Gururaj B. T. et Ramiro Amaya, Ingénieurs Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services (WCCAI)
- Proxy NGINX
- Échange de certificats de sécurité

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services (WCCAI)
- Proxy NGINX
- Connecteur de socket Web (WSConnector)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Dans un déploiement Réponses d'agent, CUBE communique avec le service WSConnector déployé dans le cadre des services WCCAI. Pour que la communication soit établie, CUBE a besoin d'un accès à Internet. Certaines entreprises ont des restrictions pour fournir un accès direct à Internet aux composants de la solution. Dans ce scénario, Cisco recommande l'utilisation du proxy qui prend en charge WebSocket. Ce document explique la configuration requise pour le proxy NGINX qui a la prise en charge de websocket.

Configuration

Déploiement

CUBE —<websocket>—proxy NGINX —<websocket>—WSconnector

Actuellement, CUBE ne prend pas en charge la méthode CONNECT pour tunnel la connexion TCP de CUBE à WSConnector. Cisco recommande la connexion saut par saut via le proxy. Avec ce déploiement, NGINX dispose d'une connexion sécurisée à partir de CUBE sur le tronçon entrant et d'une autre connexion sécurisée sur le tronçon sortant vers WSConnector

Détails de l'installation de NGINX

Détails du système d'exploitation : Cent OS centos-release-7-8.2003.0.el7.centos.x86_64
Version NGINX : nginx/1.19.5

Configuration Steps

Étape 1. Installation de NGINX : Suivez les étapes d'installation à partir du portail NGINX. Suivez ce lien : Guide d'administration de NGINX.

Étape 2. Création d'un certificat et d'une clé signées automatiquement par NGINX. Exécutez cette commande sur le serveur proxy NGINX :

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

Étape 3. Modifiez le fichier **nginx.conf**.

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

événements{
worker_connections 1024 ;
}
```

```
http{
inclure mime.types ;
default_type application/octet-stream ;
sendfile on ;
keepalive_timeout 65 ;
serveur {
écoute 8096 ssl ;
nom_serveur ~.+;
# de résolveur dns utilisé par le proxy de transfert
résolveur <IP du serveur DNS : PORT>;
proxy_read_timeout 86400s ;
proxy_send_timeout 86400s ;
client_body_timeout 86400s ;
keepalive_timeout 86400s ;
# Proxy de transfert pour la requête non CONNECT
emplacement / {
proxy_pass https://$http_host ;
proxy_http_version 1.1 ;
mise à niveau de proxy_set_header $http_upgrade ;
proxy_set_header Connection $connection_upgrade ;
proxy_set_header Hôte $host ;
proxy_ssl_certificate <nginx_selfsigned_certificate>;
proxy_ssl_certificate_key <chemin_clé_certificat_nginx>;
proxy_ssl_trust_certificate <Certificat CA WsConnector>;
proxy_ssl_protocols TLSv1.2 ;
}
#ssl activé ;
ssl_certificate <chemin_certificat_nginx_selfsigned>;
ssl_certificate_key <chemin_clé_certificat_nginx>;
ssl_session_cache partagée : SSL : 1m ;
ssl_session_timeout 5 m ;
ssl_ciphers HIGH : ! aNULL : ! MD5 ;
ssl_preference_server_ciphers activé ;
 }

}
```

Étape 4. Pour vérifier l'état du proxy NGINX, exécutez la commande suivante : **systemctl status nginx**

Vérification

Voici quelques commandes que vous pouvez utiliser pour vérifier la configuration de NGINX.

a. Vérifier que la configuration NGNIX est correcte.
nginx -t
b. Pour redémarrer le serveur nginx
systemctl restart nginx
c. Pour vérifier la version de nginx
nginx -V
d. Pour arrêter le signe
systemctl stop nginx

e. Pour démarrer la commande nginx
systemctl start nginx

Dépannage

Il n'y a pas d'étapes pour dépanner cette configuration.

Informations connexes

- Guide d'administration de NGINX
- Exemples de commandes NGINX utiles
- Comment créer un certificat ssl autosigné pour NGINX
- **Support et documentation techniques - Cisco Systems**