Configurazione del proxy NGINX per l'integrazione con una soluzione Agent Assist

Sommario

Introduzione

Questo documento descrive come configurare un server proxy NGINX per l'integrazione con una soluzione Cisco Agents Assist.

Contributo di Gururaj B. T. e Ramiro Amaya, Cisco Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services (WCCAI)
- Proxy NGINX
- Scambio certificati di sicurezza

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sfondo

In un'implementazione di Agent Answers CUBE comunica con il servizio WSConnector distribuito come parte dei servizi WCCAI. Per poter stabilire la comunicazione, CUBE ha bisogno di accesso a Internet. Alcune aziende hanno delle restrizioni per fornire l'accesso diretto a Internet ai componenti della soluzione. In questo scenario, Cisco consiglia l'utilizzo di proxy che supporta WebSocket. Questo documento spiega la configurazione richiesta per il proxy NGINX che supporta websocket.

Configurazione

Implementazione

CUBE —<websocket>—NGINX Proxy —<websocket>—WSconnector

Attualmente CUBE non supporta il metodo CONNECT per il tunnel della connessione TCP da CUBE a WSConnector. Cisco consiglia la connessione hop-by-hop attraverso il proxy. Con questa distribuzione NGINX ha una connessione protetta da CUBE sulla gamba in entrata e un'altra connessione protetta sulla gamba in uscita verso WSConnector

Dettagli sull'installazione di NGINX

Dettagli sistema operativo: Centos Cent OS-release-7-8.2003.0.el7.centos.x86_64
Versione NGINX: Inginx/1.19,5

Procedura di configurazione

Fase 1. Installazione di NGINX: Seguire i passaggi di installazione dal portale NGINX. Fare clic sul collegamento seguente: Guida per l'amministratore di NGINX.

Passaggio 2. Creazione di chiavi e certificati autofirmati NGINX. Eseguire questo comando sul server proxy NGINX:

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

Passaggio 3. Modificare il file **nginx.conf**.

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

eventi{
worker_connections 1024
```

```
}
http {
includere mime.types;
applicazione default_type/ottetto-stream;
invia file il;
keepalive_timeout 65;
server{
ascoltare 8096 ssl;
nome_server ~.+;
# resolver dns utilizzato dal proxy di inoltro
resolver <DNS _Server IP:PORT>;
proxy_read_timeout 86400s;
proxy_send_timeout 86400s;
client_body_timeout 86400s;
keepalive_timeout 86400s;
# inoltro proxy per richiesta di mancata connessione
posizione / {
proxy_pass https://$http_host;
proxy_http_version 1.1
proxy_set_header Aggiornamento $http_upgrade;
proxy_set_header: connessione $connection_upgrade;
proxy_set_header Host $host;
proxy_ssl_certificate <nginx_selfsigned_certificate>;
proxy_ssl_certificate_key <nginx_certificate_key_path>;
proxy_ssl_trusted_certificate <Certificato CA WsConnector>;
proxy_ssl_protocols - TLSv1.2;
}
#ssl attivo;
ssl_certificate <nginx_selfsigned_certificate_path>;
ssl_certificate_key <nginx_certificate_key_path>;
ssl_session_cache condiviso:SSL:1m;
ssl_session_timeout 5m;
ssl_ciphers HIGH:!aNULL:!MD5;
ssl_preferire_server_ciphers attivato;
 }

}
```

Passaggio 4. Per controllare lo stato del proxy NGINX, eseguire il comando: **systemctl status index**

Verifica

Di seguito sono riportati alcuni comandi che è possibile utilizzare per verificare la configurazione NGINX.

r. Verificare che la configurazione di NGNIX sia corretta.
indice -t
b. Per riavviare il server Inginx
systemctl restart nginx
c. Per controllare la versione di Inginx
Inginx -V

d. Per arrestare l'indice
systemctl stop nginx
e. Per avviare l'indice
systemctl start ginx

Risoluzione dei problemi

Non sono disponibili procedure per la risoluzione dei problemi relativi a questa configurazione.

Informazioni correlate

- Guida per l'amministratore di NGINX
- Esempi utili di comandi NGINX
- Come creare un certificato SSL autofirmato per NGINX
- **Documentazione e supporto tecnico – Cisco Systems**