Configurer le serveur Syslog externe sur ISE

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configuration

- Configuration de la cible de journalisation distante (UDP Syslog)
- Exemple
- Configuration de la cible distante sous Catégories de journalisation

Présentation des catégories

Vérification et dépannage

Introduction

Ce document décrit comment configurer le serveur Syslog externe sur ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Moteur du service de vérification des identités (ISE)
- Serveurs Syslog

Composants utilisés

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

- Identity Services Engine (ISE) version 3.3.
- Serveur Syslog Kiwi v1.2.1.4

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.

Informations générales

.

Les messages Syslog d'ISE sont collectés et stockés par les collecteurs de journaux. Ces collecteurs de journaux sont affectés aux noeuds de surveillance afin que MnT stocke localement les journaux collectés.

Pour collecter des journaux en externe, vous devez configurer des serveurs syslog externes, appelés cibles. Les journaux sont classés en différentes catégories prédéfinies.

Vous pouvez personnaliser la sortie de journalisation en modifiant les catégories en fonction de leurs cibles, de leur niveau de gravité, etc.

Configuration

Vous pouvez utiliser l'interface Web pour créer des cibles serveur syslog distantes vers lesquelles les messages du journal système sont envoyés. Les messages de journalisation sont envoyés aux cibles du serveur syslog distant conformément à la norme de protocole syslog (voir RFC-3164).

Configuration de la cible de journalisation distante (UDP Syslog)

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu (☰) et choisissez Administration > System > Logging > Remote Logging Targets, puis cliquez sur Add.

Remarque : Cet exemple de configuration est basé sur une capture d'écran nommée : Configuration de la cible de journalisation distante.

- Name as Remote_Kiwi_Syslog, ici vous pouvez entrer le nom du serveur Syslog distant, qui est utilisé à des fins descriptives.
- Target Type as UDP Syslog, dans cet exemple de configuration, UDP Syslog est utilisé ; toutefois, vous pouvez configurer plus d'options à partir de la liste déroulante Target Type :

Syslog UDP : Utilisé pour l'envoi de messages syslog sur UDP, adapté à la journalisation légère et rapide.

Syslog TCP : Utilisé pour l'envoi de messages Syslog sur TCP, qui fournit une fiabilité avec des fonctionnalités de contrôle des erreurs et de retransmission.

Syslog sécurisé : désigne les messages syslog envoyés via TCP avec cryptage TLS, garantissant l'intégrité et la confidentialité des données.

- État activé, vous devez sélectionner Activé dans la liste déroulante État.
- Description, vous pouvez éventuellement saisir une brève description de la nouvelle cible.
- Hôte / Adresse IP, où vous entrez l'adresse IP ou le nom d'hôte du serveur de destination qui stocke les journaux. Cisco ISE prend en charge les formats IPv4 et IPv6 pour la journalisation.



Remarque : Il est essentiel de mentionner que si vous allez configurer un serveur syslog avec FQDN, vous devez configurer la mise en cache DNS pour éviter l'impact sur les performances. Sans mise en cache DNS, ISE interroge le serveur DNS chaque fois qu'un paquet syslog doit être envoyé à la cible de journalisation distante configurée avec FQDN. Cela a un impact important sur les performances ISE.

Utilisez la`service cache enable`commande dans tous les PSN du déploiement pour surmonter ceci :

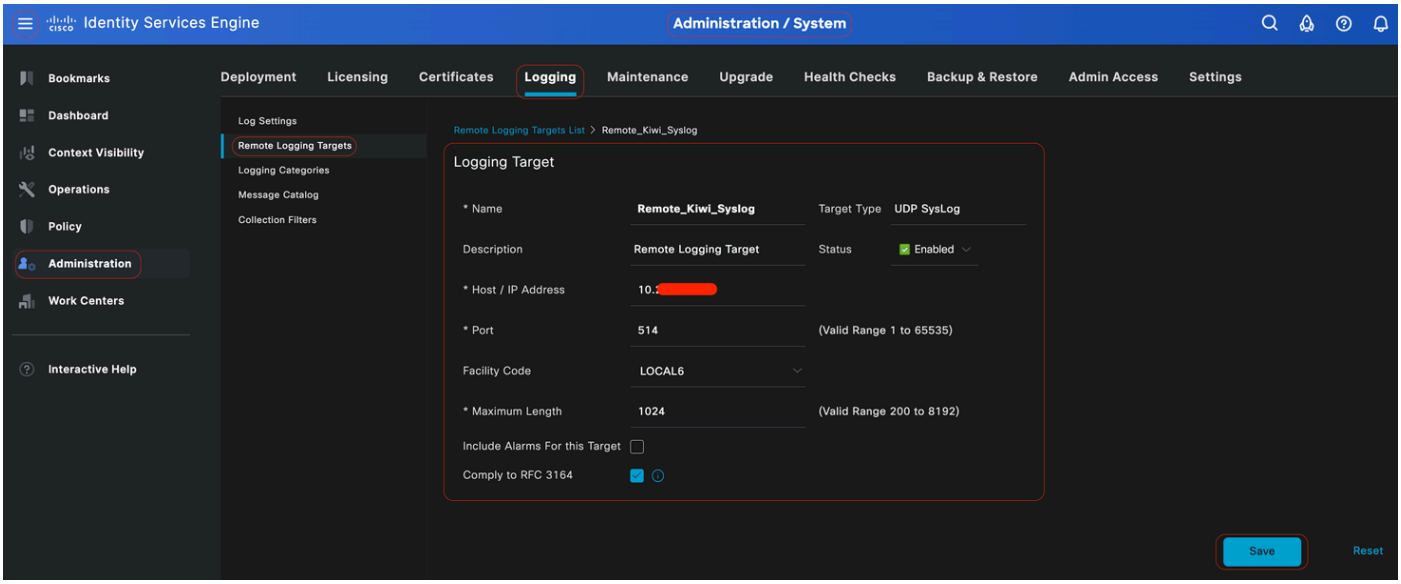
Exemple

```
ise/admin(config)# service cache enable hosts ttl 180
```

- Port 514, dans cet exemple de configuration, le serveur Syslog Kiwi écoute sur le port 514 qui est le port par défaut pour les messages Syslog UDP. Cependant, les utilisateurs peuvent modifier ce numéro de port à n'importe quelle valeur comprise entre 1 et 65535.Assurez-vous que le port souhaité n'est pas bloqué par un pare-feu.
- Facility Code : en tant que LOCAL6, vous pouvez choisir le syslog facility code qui doit être utilisé pour la journalisation, dans la liste déroulante. Les options valides sont Local0 à Local7.
- Longueur maximale : 1024. Vous pouvez entrer ici la longueur maximale des messages cible du journal distant. La longueur maximale est définie sur 1024, par défaut dans la version ISE 3.3. Les valeurs sont comprises entre 200 et 8192 octets.

Remarque : Pour éviter d'envoyer des messages tronqués à votre cible distante, vous pouvez définir la longueur maximale sur 8192. Vous pouvez identifier les messages tronqués en effectuant une capture.

- Inclure les alarmes pour cette cible. Pour rester simple, dans cet exemple de configuration, l'option Inclure les alarmes pour cette cible n'est pas cochée ; toutefois, lorsque vous cochez cette case, les messages d'alarme sont également envoyés au serveur distant.
- La case Conformité à la RFC 3164 est cochée, lorsque vous cochez cette case, les séparateurs (, ; { } \) dans les messages syslog envoyés aux serveurs distants ne sont pas échappés même si une barre oblique inverse (\) est utilisée.
- Une fois la configuration terminée, cliquez sur Save.
- Une fois l'enregistrement effectué, le système affiche l'avertissement suivant : Vous avez choisi de créer une connexion non sécurisée (TCP/UDP) au serveur. Êtes-vous sûr de vouloir continuer ?, cliquez sur Oui.



Configuration de la cible distante

Configuration de la cible distante sous Catégories de journalisation

Cisco ISE envoie des événements pouvant être audités à la cible Syslog. Une fois que vous avez configuré votre cible de journalisation distante, vous devez mapper la cible de journalisation distante aux catégories prévues pour transférer les événements pouvant faire l'objet d'un audit.

Les cibles de journalisation peuvent ensuite être mappées à chacune de ces catégories de journalisation. Les journaux d'événements de ces catégories de journaux sont générés uniquement à partir des noeuds PSN et peuvent être configurés pour envoyer les journaux

appropriés au serveur Syslog distant en fonction des services qui sont activés sur ces noeuds :

- Audit AAA
- Diagnostics AAA
- Gestion de comptes
- MDM externe
- ID passif
- Audit de la position et du provisionnement client
- Diagnostics de positionnement et de provisionnement client
- Profileur

Les journaux d'événements de ces catégories de journaux sont générés à partir de tous les noeuds du déploiement et peuvent être configurés pour envoyer les journaux appropriés au serveur Syslog distant :

- Audit administratif et opérationnel
- Diagnostics du système
- Statistiques système

Dans cet exemple de configuration, vous allez configurer la cible distante sous quatre catégories de journalisation, ces 3 catégories pour envoyer des journaux de trafic d'authentification : Authentifications réussies, tentatives échouées et comptabilité Radius, et cette catégorie pour le trafic de journalisation de l'administrateur ISE :

Remarque : Cet exemple de configuration est basé sur une capture d'écran nommée : Configuration de la cible de journalisation distante

---

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu (☰) et choisissez Administration > System > Logging > Logging Categories, et cliquez sur la catégorie requise (Passed Authentications, Failed Attempts and Radius Accounting).

Étape 1 - Niveau de gravité du journal : un message d'événement est associé à un niveau de gravité, ce qui permet à un administrateur de filtrer les messages et de les hiérarchiser. Sélectionnez le niveau de gravité du journal comme requis. Pour certaines catégories de

journalisation, cette valeur est définie par défaut et vous ne pouvez pas la modifier. Pour certaines catégories de journalisation, vous pouvez choisir l'un des niveaux de gravité suivants dans une liste déroulante :

- FATAL : Niveau d'urgence Ce niveau signifie que vous ne pouvez pas utiliser Cisco ISE et que vous devez immédiatement prendre les mesures nécessaires.
- ERREUR : Ce niveau indique une condition d'erreur critique.
- AVERTISSEMENT : Ce niveau indique une condition normale mais significative. Il s'agit du niveau par défaut défini pour de nombreuses catégories de journalisation.
- INFOS : Ce niveau indique un message d'information.
- DEBUG : Ce niveau indique un message de bogue de diagnostic.

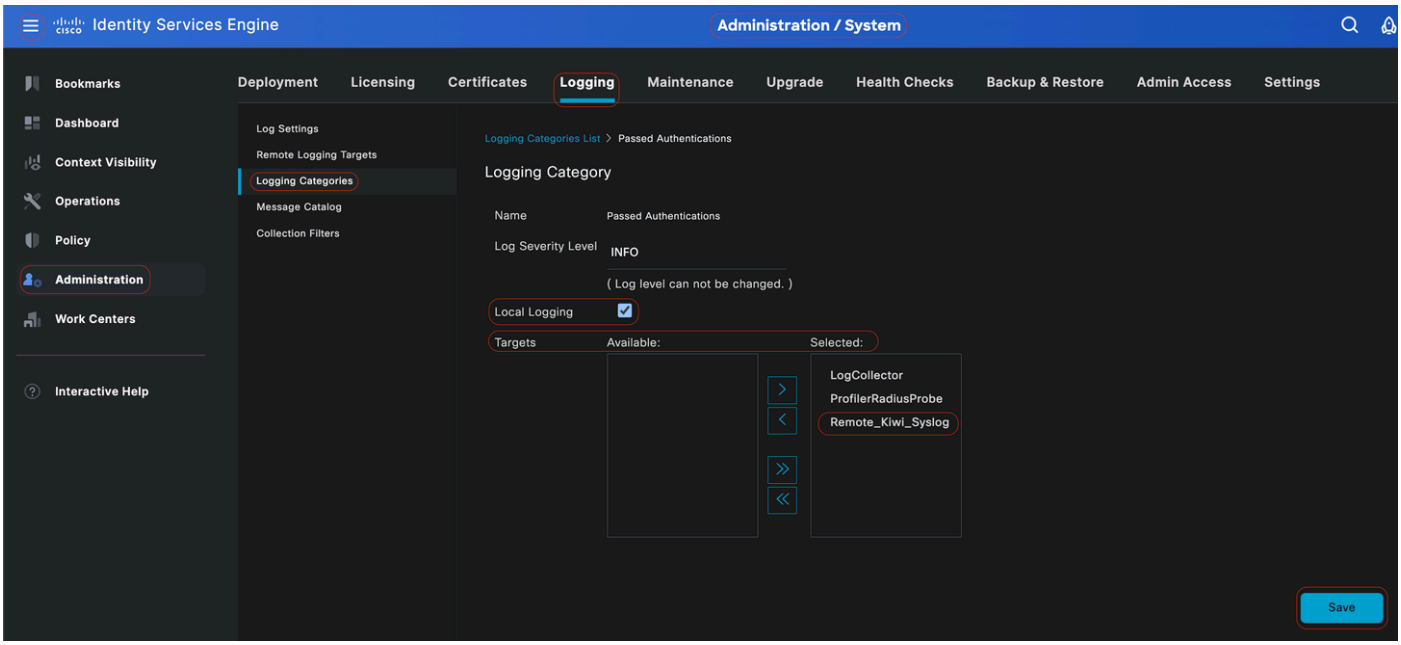
Étape 2 - Journalisation locale : cette case à cocher active la génération du journal local. Cela signifie que les journaux générés par les PSN sont également enregistrés sur le PSN spécifique générant le journal. Nous vous recommandons de conserver la configuration par défaut

Étape 3 - Cibles : cette zone vous permet de choisir les cibles d'une catégorie de journalisation en transférant les cibles entre les zones Disponible et Sélectionné à l'aide des flèches gauche et droite.

La zone Disponible contient les cibles de journalisation existantes, à la fois locales (prédéfinies) et externes (définies par l'utilisateur).

La zone Sélectionné, qui est initialement vide, affiche ensuite les cibles qui ont été choisies pour la catégorie.

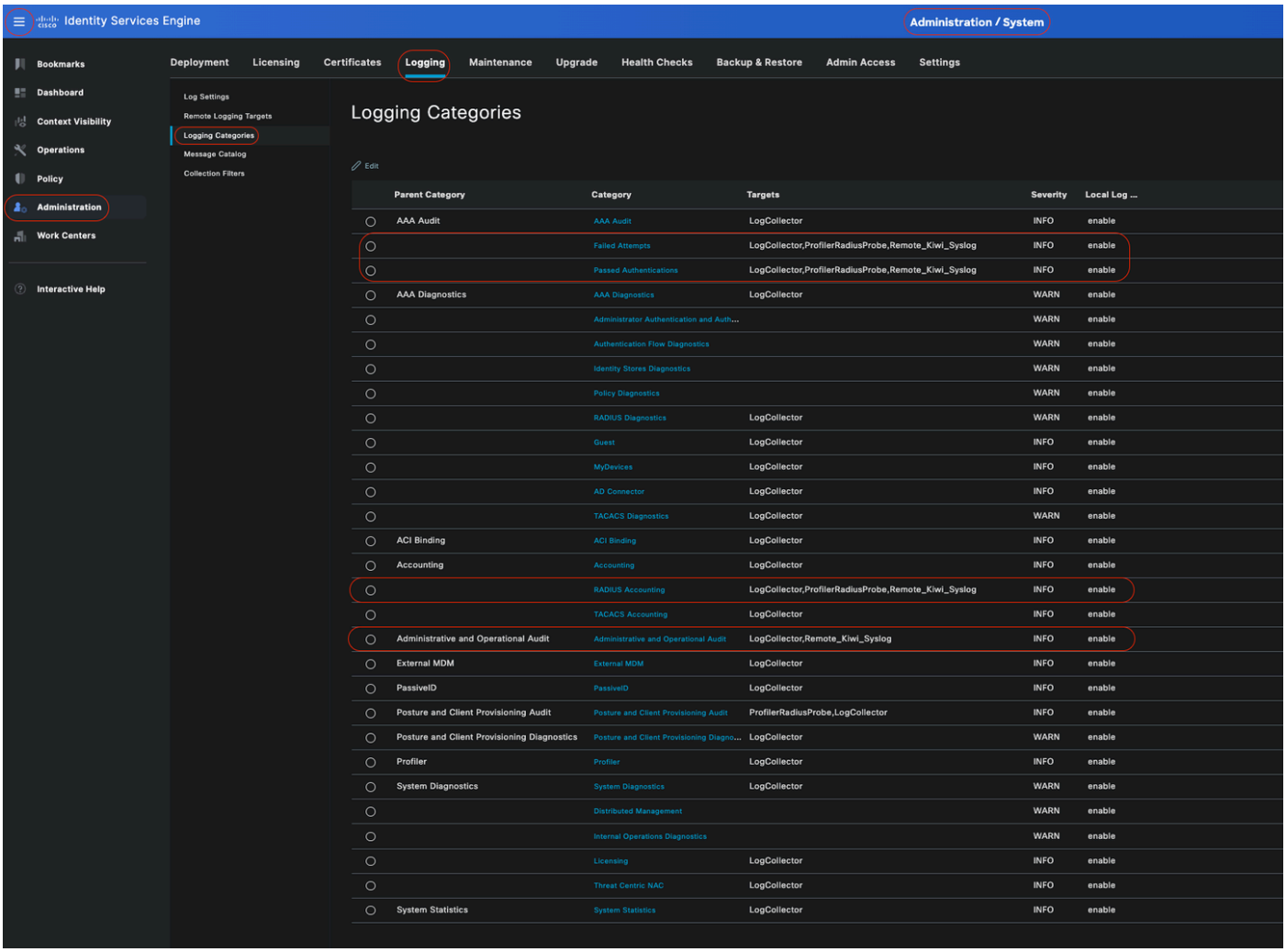
Étape 4 - Répétez les étapes 1 à 3 pour ajouter une cible distante sous Tentatives infructueuses et catégories Comptabilité Radius.



Mappage des cibles distantes aux catégories prévues

Étape 5 - Vérifiez que votre cible distante se trouve dans les catégories requises.Vous devez pouvoir voir la cible distante que vous venez d’ajouter.

Dans cette capture d'écran, vous pouvez voir la cible distante Remote_Kiwi_Syslog mappée aux catégories requises.



Vérification des catégories

Présentation des catégories

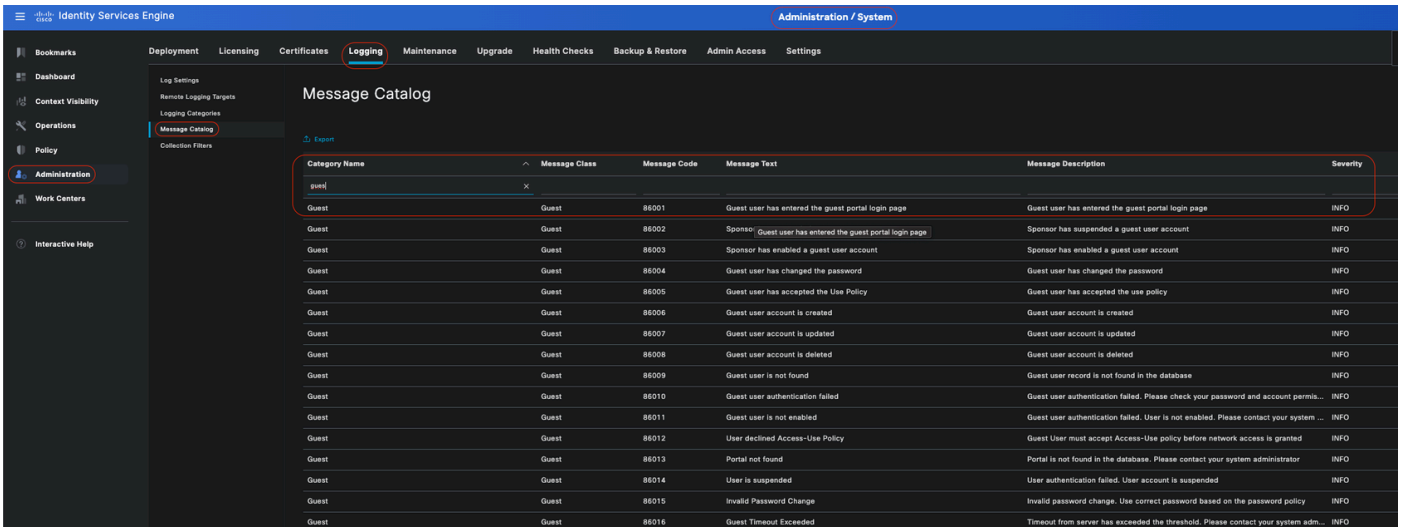
Un message est généré lorsqu'un événement se produit. Il existe différents types de messages d'événement générés à partir de plusieurs installations, telles que le noyau, le courrier, le niveau utilisateur, etc.

Ces erreurs sont classées dans le catalogue de messages et ces événements sont également organisés hiérarchiquement en catégories. Ces catégories ont des catégories parentes contenant une ou plusieurs catégories.

Catégorie parente	Catégorie
Audit AAA	Audit AAA Tentatives ayant échoué Authentification réussie

Diagnostics AAA	Diagnostics AAA Authentification et autorisation de l'administrateur Diagnostics de flux d'authentification Diagnostics du magasin d'identités Diagnostics de stratégie Diagnostics Radius Invité
Gestion de comptes	Gestion de comptes Comptabilité Radius
Audit administratif et opérationnel	Audit administratif et opérationnel
Audit de la position et du provisionnement client	Audit de la position et du provisionnement client
Diagnostics de positionnement et de provisionnement client	Diagnostics de positionnement et de provisionnement client
Profileur	Profileur
Diagnostics du système	Diagnostics du système Gestion distribuée Diagnostics des opérations internes
Statistiques système	Statistiques système

Dans cette capture d'écran, vous pouvez voir que Guest est une classe de message et catégorisée comme une catégorie d'invité. Cette catégorie d'invité a une catégorie parente appelée Diagnostics AAA.



Catalogue de messages

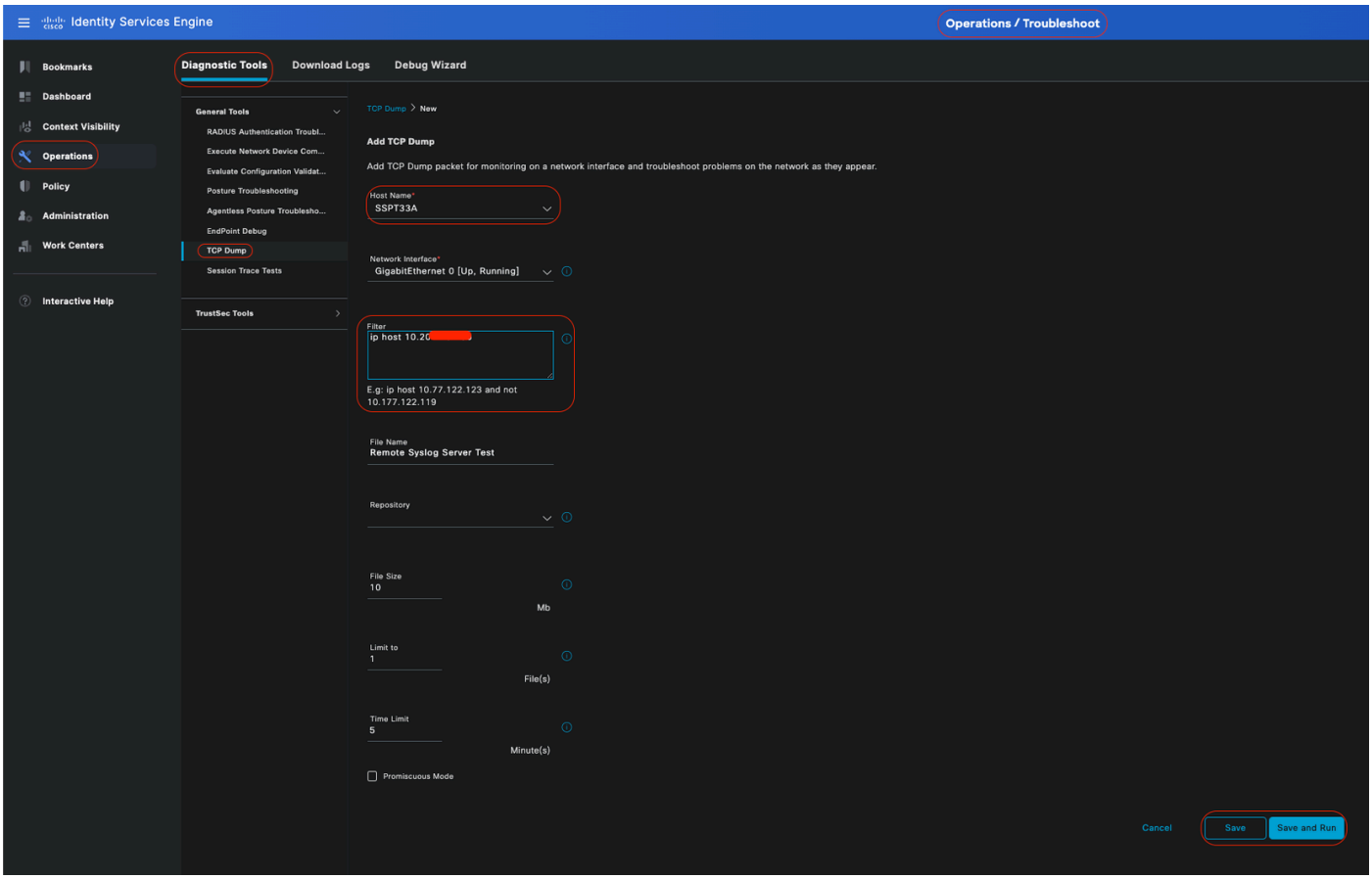
Vérification et dépannage

L'étape de dépannage et de vérification la plus rapide consiste à effectuer un vidage TCP sur la cible de journalisation distante pour vérifier si des événements de journalisation sont envoyés ou non.

La capture doit être effectuée à partir du PSN qui authentifie l'utilisateur, car PSN va générer des messages de journal et ces messages vont être envoyés à la cible distante

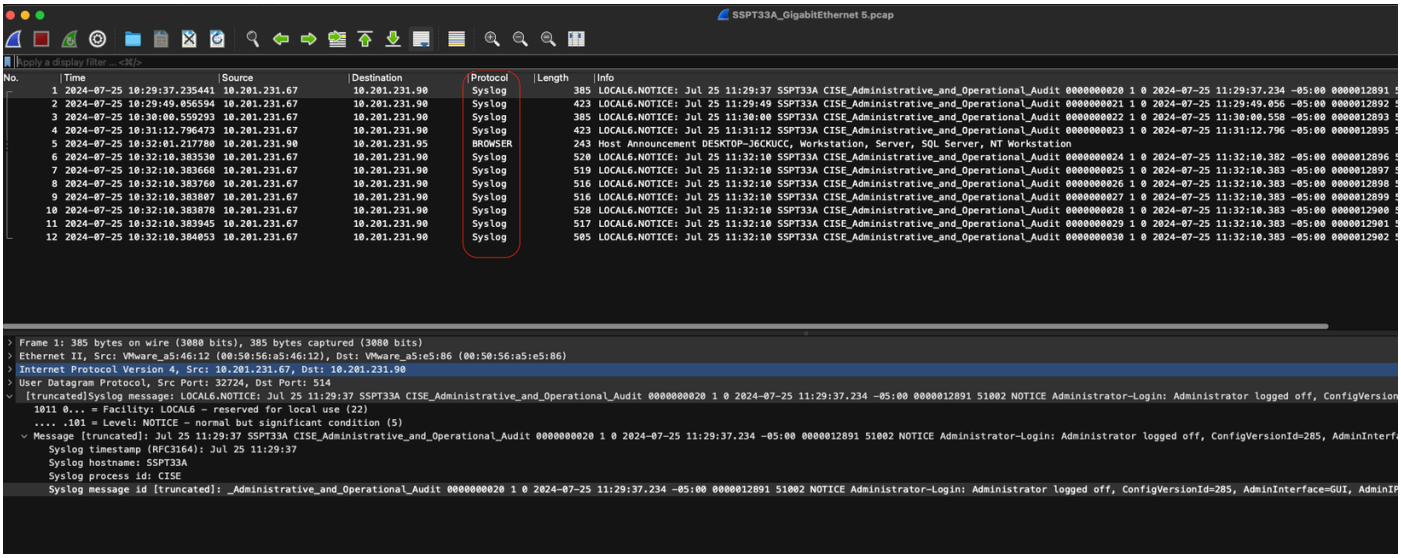
Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu (☰) et choisissez Operations > Troubleshoot>TCP Dump. Cliquez sur Add.

- Vous devez filtrer le trafic, ajouter le champ de filtre ip host <remote_target_IP_address>.
- Vous devez effectuer une capture à partir de PSN traitant les authentifications.



Dépôt TCP

Dans cette capture d'écran, vous pouvez voir comment ISE envoie des messages Syslog pour le trafic de journalisation de l'administrateur ISE.



Trafic Syslog

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.