

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 :

- Identity Services Engine (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 > Cliquez sur Add.



Remarque : cet exemple de configuration est basé sur une capture d'écran intitulée : Configuration de la cible de journalisation à distance.

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

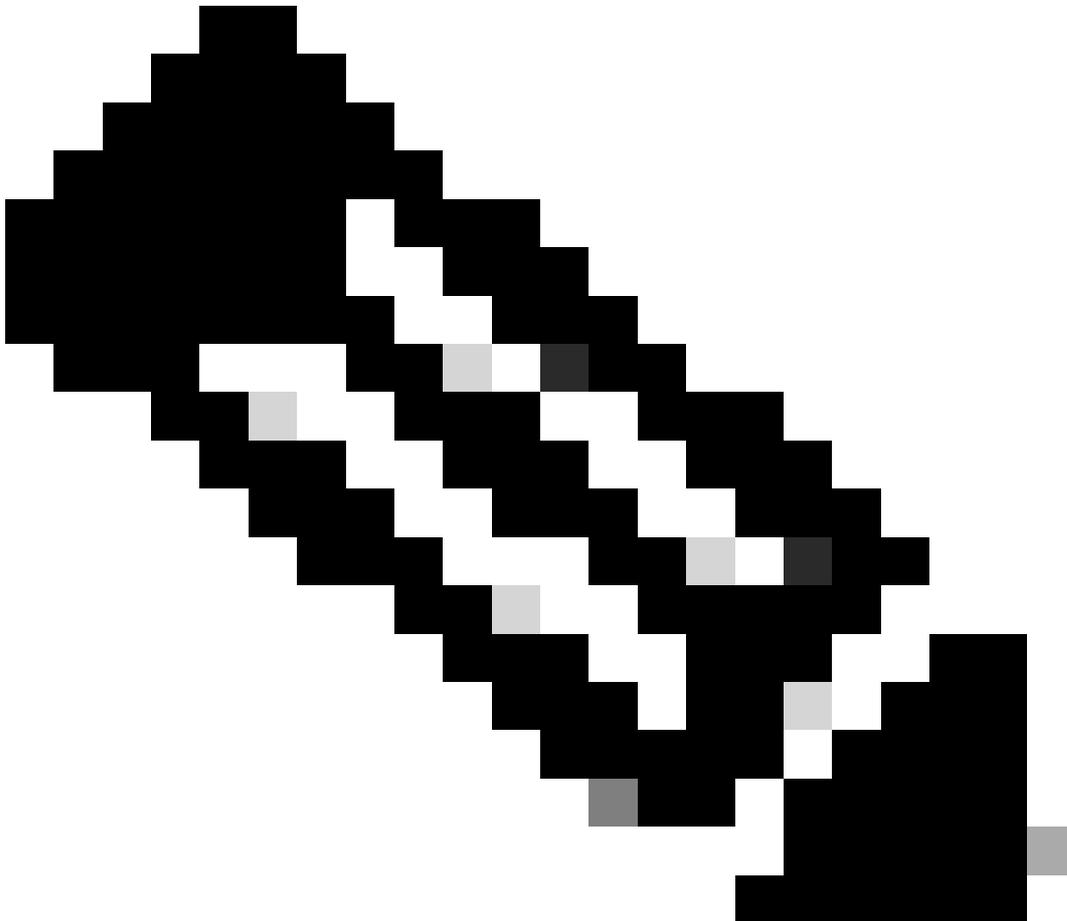
UDP Syslog : utilisé pour l'envoi de messages Syslog sur UDP, adapté à la journalisation légère et rapide.

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

Syslog sécurisé : ce terme fait référence aux 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.
-



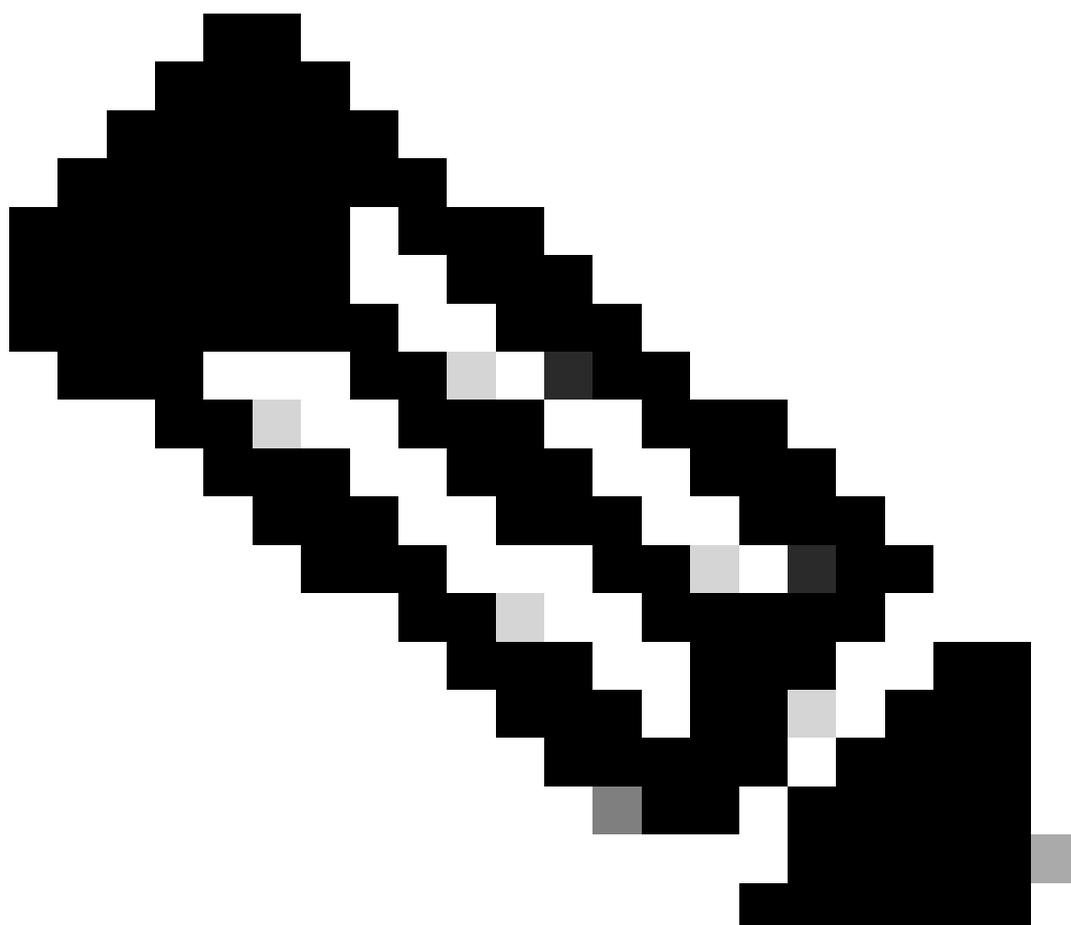
Remarque : il est essentiel de mentionner que si vous allez configurer un serveur Syslog avec FQDN, vous devez configurer la mise en cache DNS pour éviter l'impact sur les performances. Sans mise en cache DNS, ISE interroge le serveur DNS chaque fois qu'un paquet syslog doit être envoyé à la cible de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

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

Exemple

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

- **Port** as **514**, dans cet exemple de configuration, le serveur Syslog Kiwi écoute dans le port **514** qui est le port par défaut pour les messages Syslog UDP. Cependant, les utilisateurs peuvent modifier ce numéro de port sur n'importe quelle valeur comprise entre 1 et 65535. Assurez-vous que le port souhaité n'est bloqué par aucun pare-feu.
 - **Facility Code** en tant que **LOCAL6**, vous pouvez choisir le code de l'utilitaire syslog qui doit être utilisé pour la journalisation, dans la liste déroulante. Les options valides sont Local0 à Local7.
 - **Maximum Length** as **1024**, où vous pouvez entrer 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 1024 octets.
-

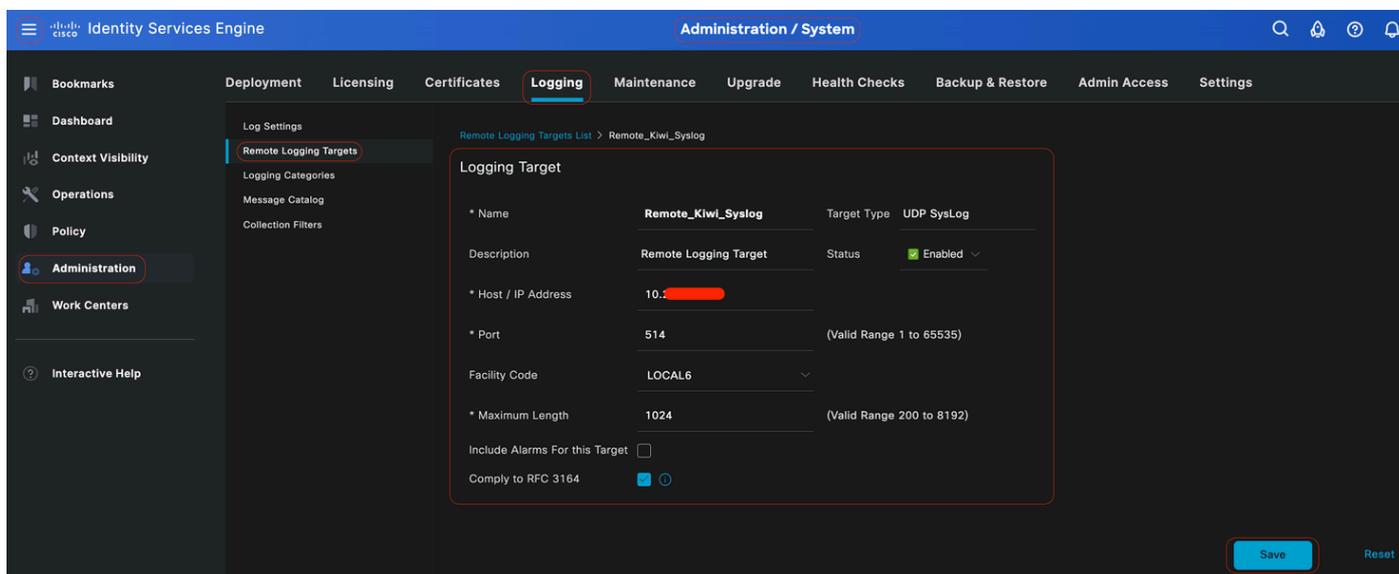


Remarque : pour éviter d'envoyer des messages tronqués à votre cible de journalisation distante, vous pouvez modifier la longueur maximale en 8192.

- **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 ; cependant, lorsque vous cochez cette case, les messages d'alarme sont également envoyés au serveur distant.
- **L'option Conformité à la RFC 3164** est cochée. Lorsque vous cochez cette case, les délimiteurs (, ; { } \ \) des messages syslog envoyés aux serveurs distants ne sont pas protégés 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 ensuite mapper la **cible de journalisation distante** aux catégories prévues pour transférer les événements pouvant être audités.

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

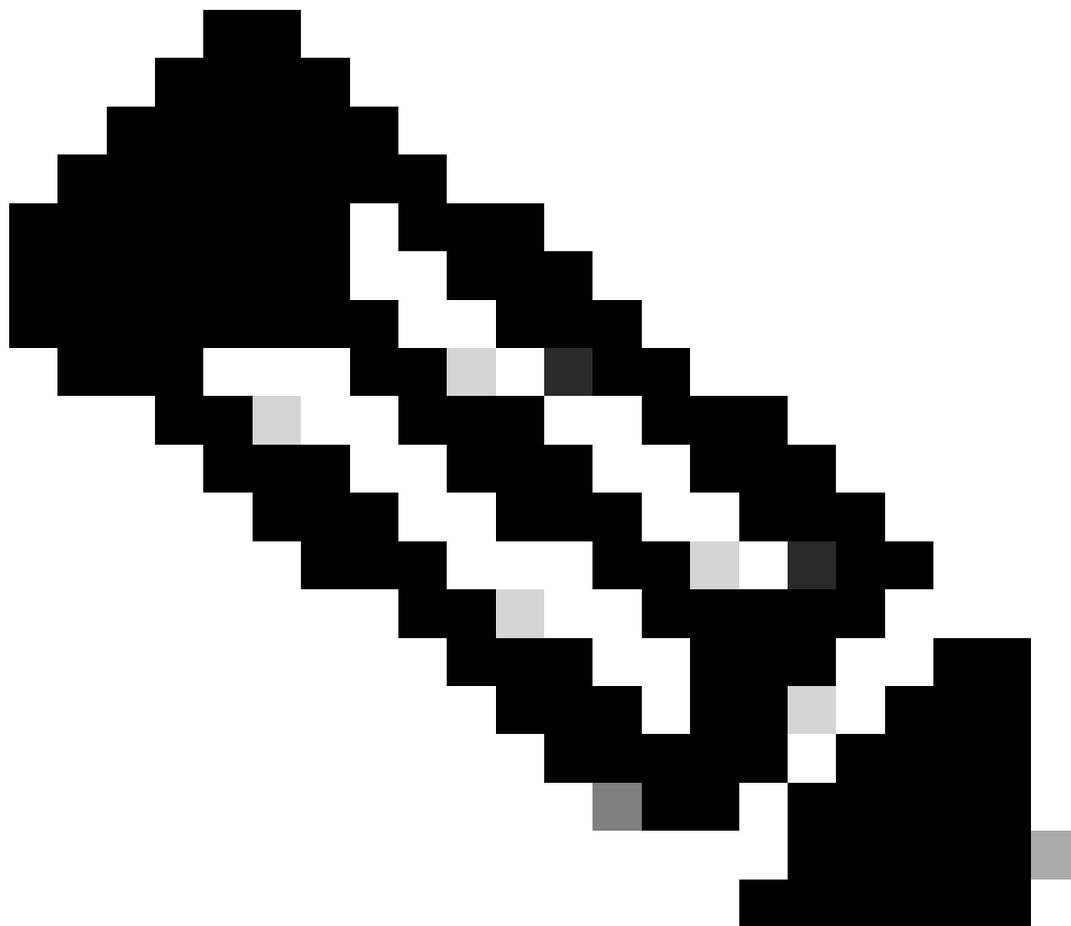
-

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 : **Authentications 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 intitulée : Configuration de la cible de



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 (**Authentications réussies, Tentatives échouées et Comptabilité Radius**).

Étape 1 - Consignez le niveau de gravité : 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 un état normal mais significatif. Il s'agit du niveau par défaut défini pour de nombreuses catégories de journalisation.

-

INFO : ce niveau indique un message d'information.

-

DEBUG : ce niveau indique un message de bogue de diagnostic.

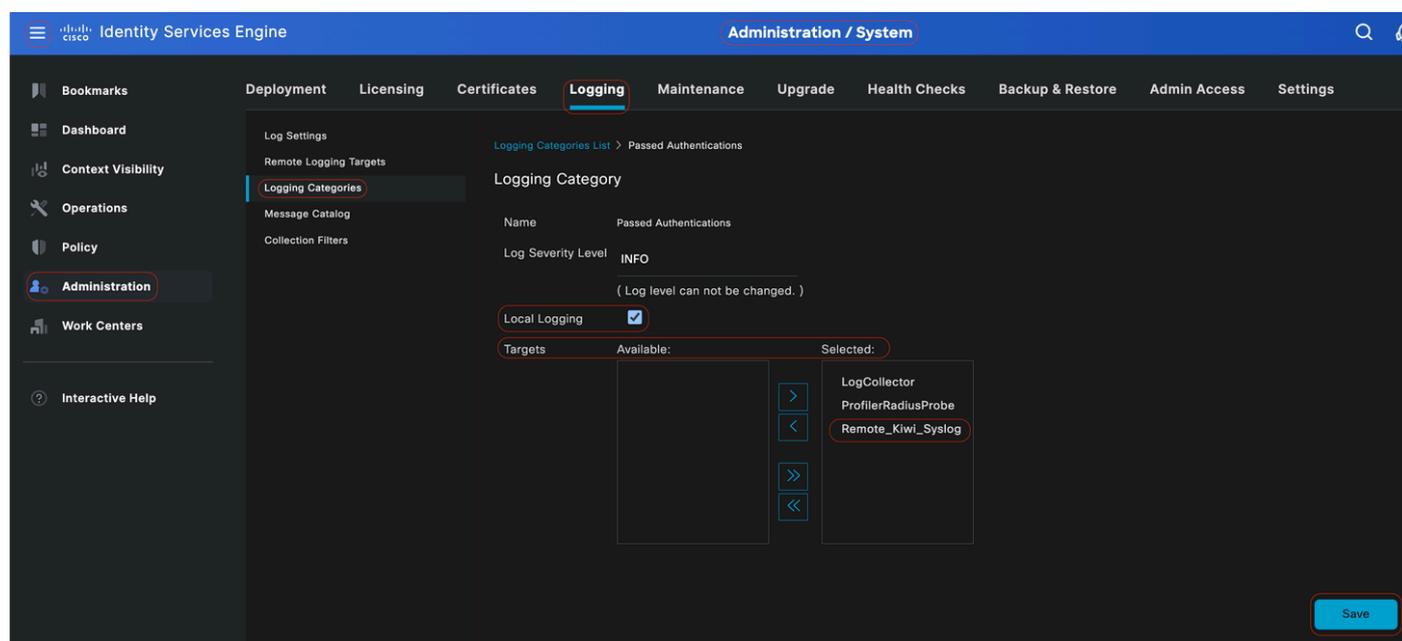
Étape 2 - Journalisation locale : cette case à cocher active la génération du journal local. Cela signifie que les journaux générés par les PSN sont également enregistrés sur le PSN spécifique générant le journal. Nous vous recommandons de conserver la configuration par défaut

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 Sélectionnées à l'aide des icônes fléchées gauche et droite.

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

La zone Sélectionné, 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 de 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.

The screenshot shows the Cisco Identity Services Engine Administration / System page. The 'Logging' tab is selected, displaying a table of logging categories. The table has columns for Parent Category, Category, Targets, Severity, and Local Log. Several rows are highlighted with red circles, including 'Failed Attempts', 'Passed Authentications', 'Administrative and Operational Audit', and 'Accounting'.

Parent Category	Category	Targets	Severity	Local Log ...
AAA Audit	AAA Audit	LogCollector	INFO	enable
	Failed Attempts	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
	Passed Authentications	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
AAA Diagnostics	AAA Diagnostics	LogCollector	WARN	enable
	Administrator Authentication and Auth...		WARN	enable
	Authentication Flow Diagnostics		WARN	enable
	Identity Stores Diagnostics		WARN	enable
	Policy Diagnostics		WARN	enable
	RADIUS Diagnostics	LogCollector	WARN	enable
	Guest	LogCollector	INFO	enable
	MyDevices	LogCollector	INFO	enable
	AD Connector	LogCollector	INFO	enable
	TACADS Diagnostics	LogCollector	WARN	enable
ACI Binding	ACI Binding	LogCollector	INFO	enable
Accounting	Accounting	LogCollector	INFO	enable
	RADIUS Accounting	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
	TACADS Accounting	LogCollector	INFO	enable
	Administrative and Operational Audit	LogCollector,Remote_Kiwi_Syslog	INFO	enable
External MDM	External MDM	LogCollector	INFO	enable
PassiveID	PassiveID	LogCollector	INFO	enable
Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	ProfilerRadiusProbe,LogCollector	INFO	enable
Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagno...	LogCollector	WARN	enable
Profiler	Profiler	LogCollector	INFO	enable
System Diagnostics	System Diagnostics	LogCollector	WARN	enable
	Distributed Management		WARN	enable
	Internal Operations Diagnostics		WARN	enable
	Licensing	LogCollector	INFO	enable
	Threat Centric NAC	LogCollector	INFO	enable
System Statistics	System Statistics	LogCollector	INFO	enable

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 Gestion des comptes 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 classé comme **Guest Category**. Cette catégorie Invité a une catégorie parent appelée **Diagnostics AAA**.

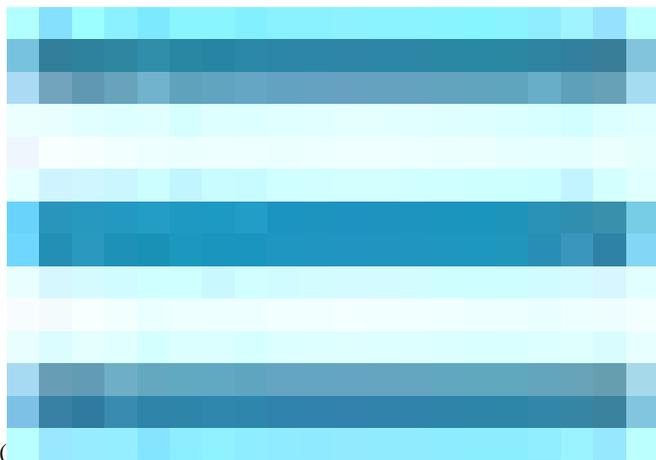
Category Name	Message Class	Message Code	Message Text	Message Description	Severity
Guest	Guest	86001	Guest user has entered the guest portal login page	Guest user has entered the guest portal login page	INFO
Guest	Guest	86002	Sponsor: Guest user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO
Guest	Guest	86003	Sponsor has enabled a guest user account	Sponsor has enabled a guest user account	INFO
Guest	Guest	86004	Guest user has changed the password	Guest user has changed the password	INFO
Guest	Guest	86005	Guest user has accepted the Use Policy	Guest user has accepted the use policy	INFO
Guest	Guest	86006	Guest user account is created	Guest user account is created	INFO
Guest	Guest	86007	Guest user account is updated	Guest user account is updated	INFO
Guest	Guest	86008	Guest user account is deleted	Guest user account is deleted	INFO
Guest	Guest	86009	Guest user is not found	Guest user record is not found in the database	INFO
Guest	Guest	86010	Guest user authentication failed	Guest user authentication failed. Please check your password and account permis...	INFO
Guest	Guest	86011	Guest user is not enabled	Guest user authentication failed. User is not enabled. Please contact your system ...	INFO
Guest	Guest	86012	User declined Access-Use Policy	Guest User must accept Access-Use policy before network access is granted	INFO
Guest	Guest	86013	Portal not found	Portal is not found in the database. Please contact your system administrator	INFO
Guest	Guest	86014	User is suspended	User authentication failed. User account is suspended	INFO
Guest	Guest	86015	Invalid Password Change	Invalid password change. Use correct password based on the password policy	INFO
Guest	Guest	86016	Guest Timeout Exceeded	Timeout from server has exceeded the threshold. Please contact your system adm...	INFO

Catalogue de messages

Vérification et dépannage

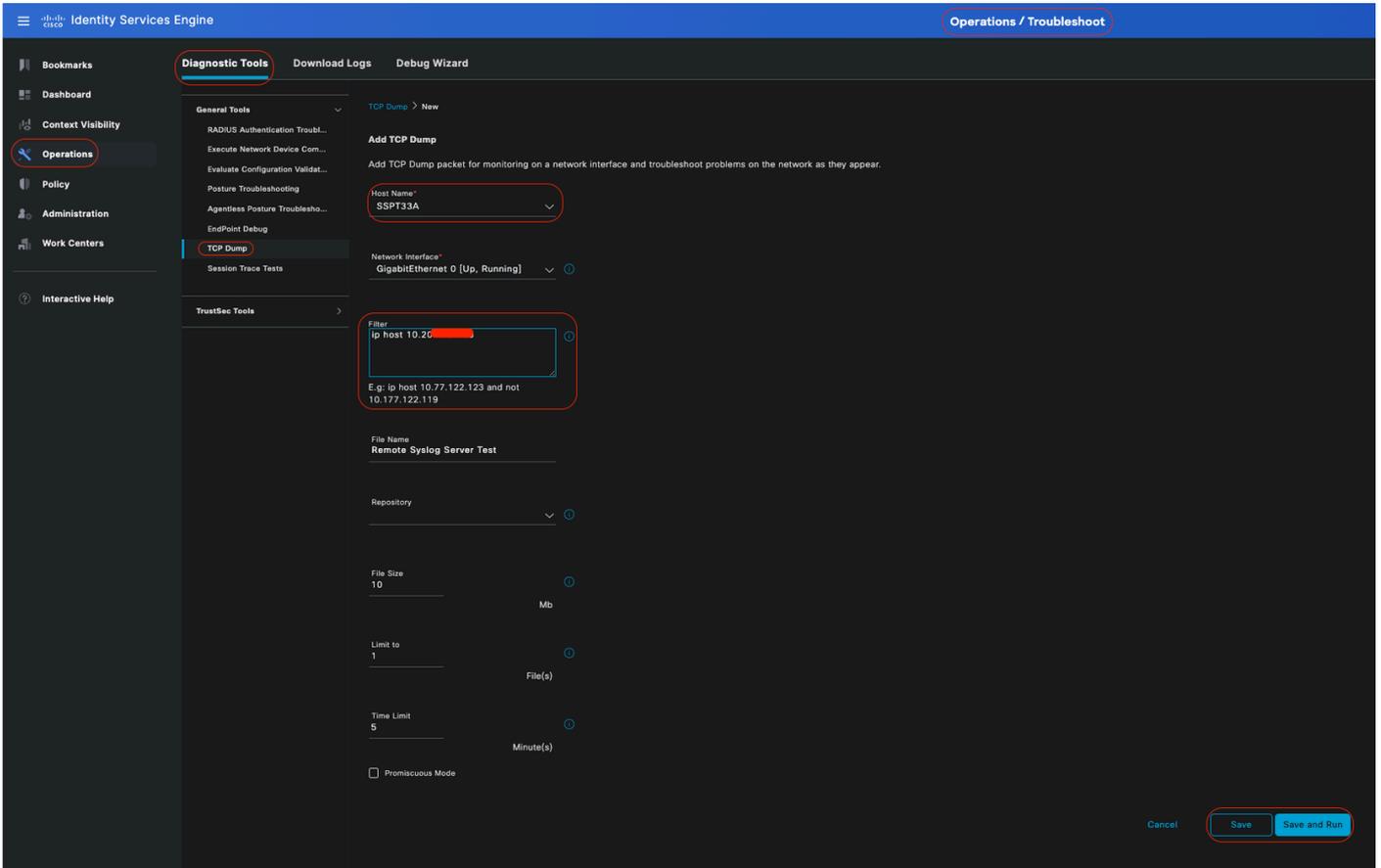
L'étape de dépannage et de vérification la plus rapide consiste à effectuer un vidage TCP sur la cible de journalisation distante pour vérifier si des événements de journalisation sont envoyés ou non.

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



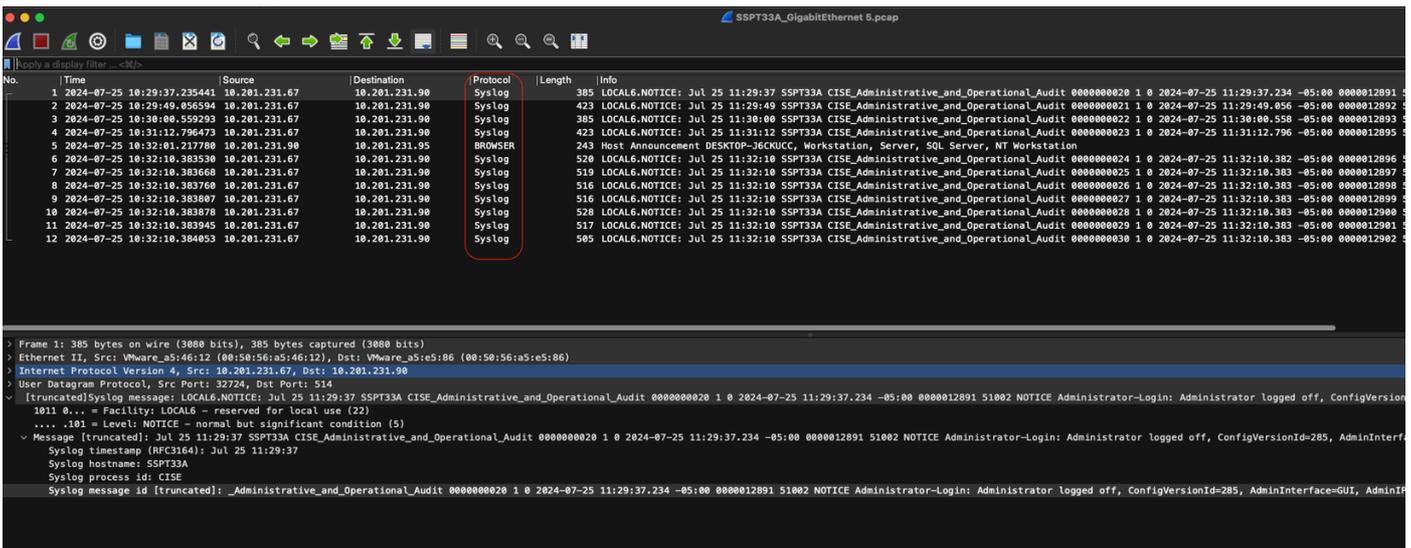
Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu () et choisissez **Operations > Troubleshoot > TCP Dump > Click on Add.**

- Vous devez filtrer le trafic, ajouter le champ de filtre ip host <remote_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.



Traffic 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.