Externe systeemserver op ISE configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een Externe Syslog Server op ISE kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE).
- Syslogservers

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE) 3.3 versie.
- Kiwi Syslog Server v1.2.1.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

.

Syslog-berichten van ISE worden verzameld en opgeslagen door logboekverzamelaars. Deze logbestanden worden toegewezen aan bewakingsknooppunten zodat MnT de verzamelde logbestanden lokaal opslaat.

Om logboeken extern te verzamelen, vormt u externe syslog servers, die doelstellingen worden genoemd. Logbestanden worden ingedeeld in verschillende vooraf gedefinieerde categorieën.

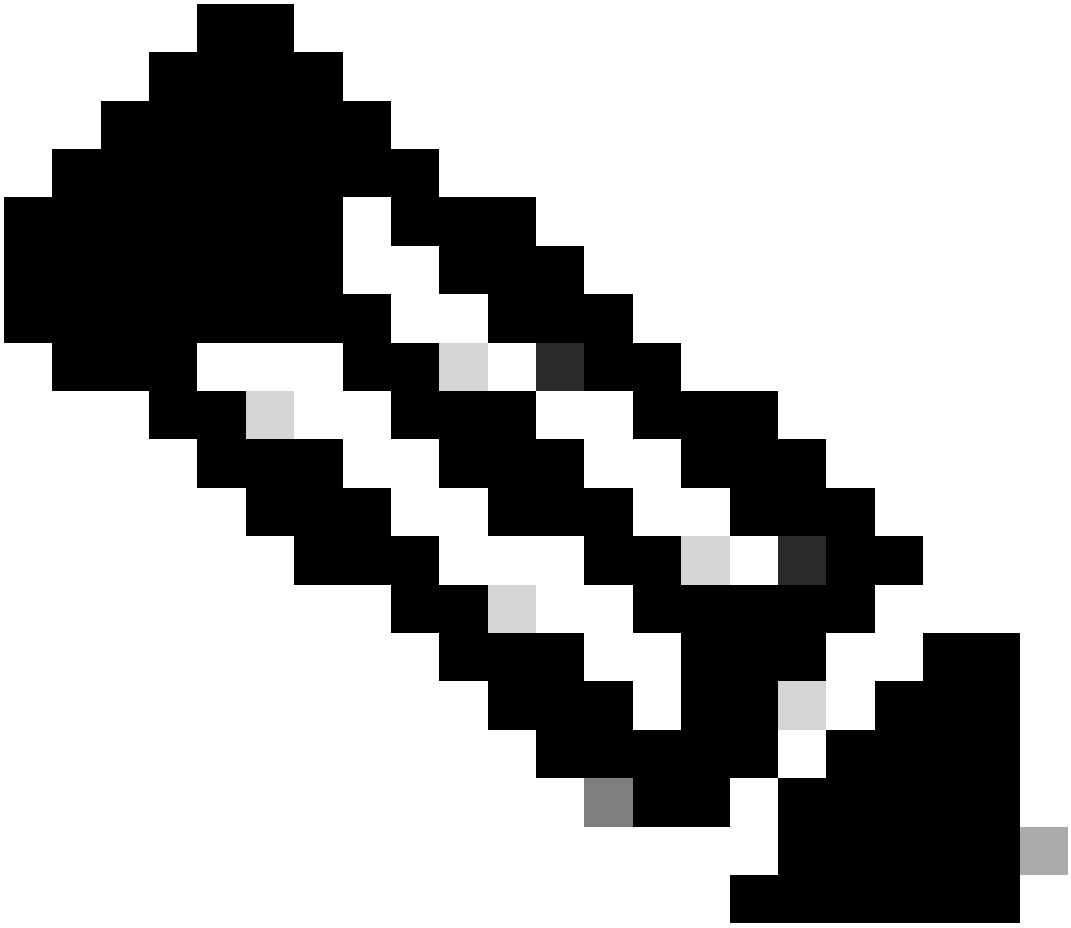
U kunt logboekoutput aanpassen door de categorieën met betrekking tot hun doelstellingen, strengheidsniveau, etc. uit te geven.

Configuratie

U kunt de web interface gebruiken om externe syslog server doelen te maken waarnaar systeem log berichten worden verzonden. Log berichten worden verzonden naar de verre syslog serverdoelstellingen in overeenstemming met de syslog protocolnorm (zie RFC-3164).

Remote Logging Target (UDP-syslog) configureren

In de Cisco ISE GUI, klik op het pictogram Menuicon () en kies Beheer>Systeem>Vastlegging>Doelstellingen voor externe vastlegging > Klik op Add.



Opmerking: Dit configuratievoorbeeld is gebaseerd op screenshot met de naam: Remote Logging Target configureren.

- Naam als Remote_Kiwi_Syslog, hier kunt u de naam van de Remote Syslog server invoeren, dit wordt gebruikt voor beschrijvende doeleinden.
- Target Type als UDP Syslog, in dit configuratievoorbeeld wordt UDP Syslog gebruikt; u kunt echter meer opties instellen in de vervolgkeuzelijst Target Type:

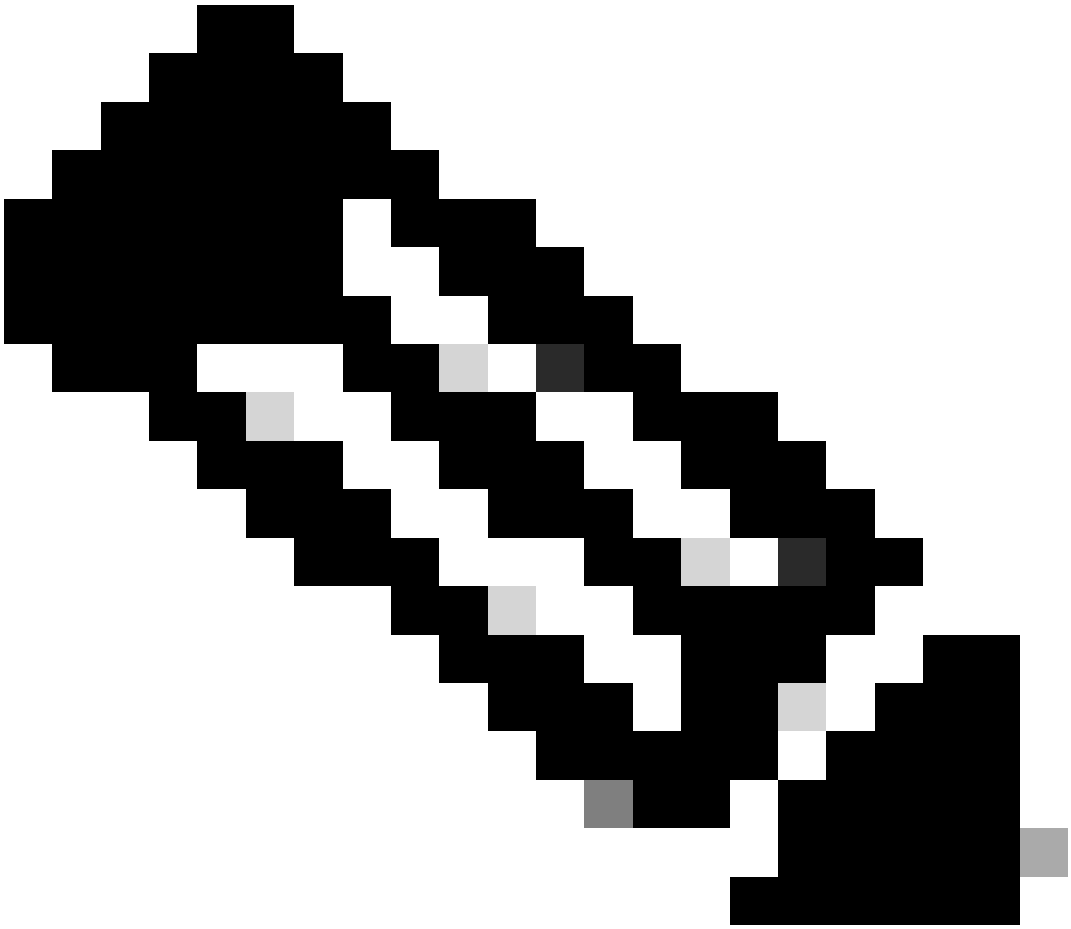
UDP Syslog: Gebruikt voor het verzenden van syslog berichten via UDP, geschikt voor lichtgewicht en snelle vastlegging.

TCP Syslog: wordt gebruikt voor het verzenden van syslog-berichten via TCP, die betrouwbaarheid biedt met foutcontrole en wederuitzendmogelijkheden.

Secure Syslog: het verwijst naar syslog berichten die over TCP met TLS-encryptie worden verzonden, die gegevensintegriteit en vertrouwelijkheid verzekeren.

- Status zoals ingeschakeld, moet u in de vervolgkeuzelijst Status Enabled kiezen.

- Beschrijving, naar keuze kunt u een korte beschrijving van het nieuwe doel invoeren.
- Host / IP-adres, hier voert u het IP-adres of hostnaam in van de doelserver die de logbestanden opslaat.Cisco ISE ondersteunt IPv4- en IPv6-formaten voor vastlegging.



Opmerking: het is essentieel om te vermelden dat als u een syslogserver met FQDN gaat configureren, moet u DNS-caching instellen om invloed op de prestaties te voorkomen. Zonder DNS-caching, vraagt ISE DNS-server elke keer dat een syslogpakket moet worden verzonden naar het externe logboekdoel dat met FQDN is geconfigureerd. Dit heeft ernstige gevolgen voor de ISE-prestaties.

Gebruik service cache enablede opdracht in alle PSN van de inzet om dit te overwinnen:

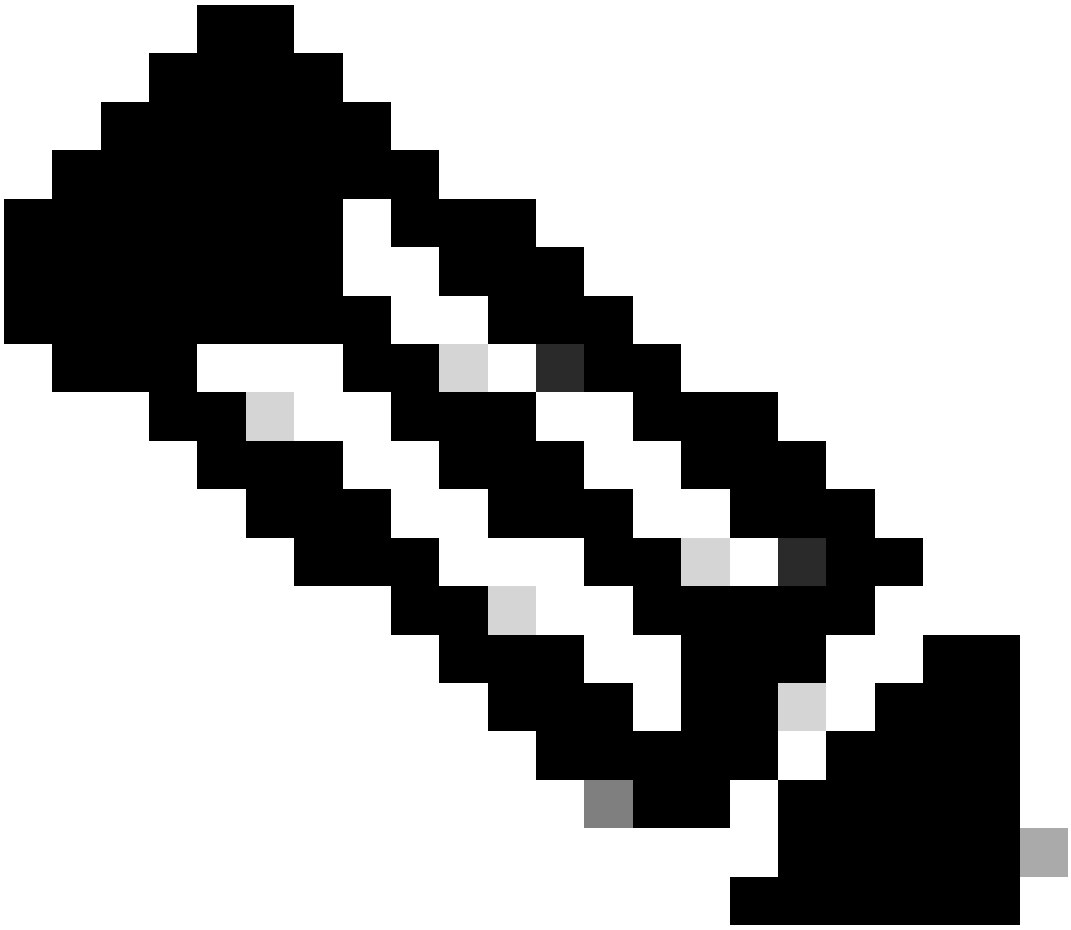
Voorbeeld

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

• **Poort** als **514**, in dit configuratievoorbeeld, de Kiwi Syslog Server luistert in poort **514** die de standaardpoort voor UDP syslog berichten. Gebruikers kunnen dit poortnummer echter wijzigen in een waarde tussen 1 en 65535.Zorg ervoor dat de gewenste poort niet wordt geblokkeerd door een firewall.

• **Faciliteitscode** als **LOCAL6**, kunt u de syslogcode kiezen die moet worden gebruikt voor vastlegging, uit de vervolgkeuzelijst. Geldige opties zijn Local0 tot en met Local7.

• **Maximale lengte** als **1024**, hier kunt u de maximale lengte van de externe log-doelberichten invoeren. De maximale lengte is standaard ingesteld op **1024** door ISE 3.3 versie, waarden zijn van 200 tot 1024 bytes.



Opmerking: Om te voorkomen dat ingekorte berichten naar uw Remote-logboekdoel worden verzonden, kunt u de Maximale lengte

wijzigen als 8192.

- **Omvat Alarmen voor dit Doel,** om het eenvoudig te houden, in dit configuratievoorbeeld, **omvat Alarmen voor dit Doel** wordt niet gecontroleerd; echter, wanneer u dit controlevakje controleert, worden de alarmberichten eveneens verzonden naar de verre server.

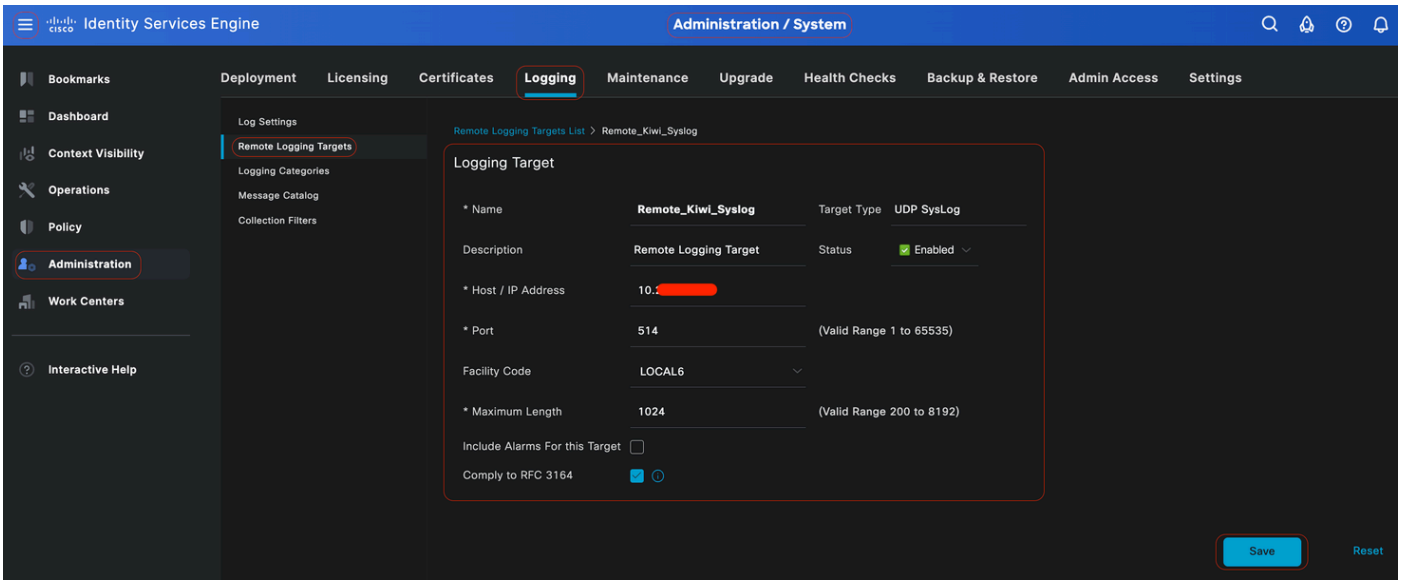
- **Voldoen aan RFC 3164** is ingeschakeld wanneer u dit selectievakje aanvinkt, worden de scheidingstekens (; {} \ \) in de syslog-berichten die naar de externe servers worden verzonden niet ontsnapt, zelfs als een backslash (\) wordt gebruikt.

-

Klik op **Opslaan** als de configuratie is voltooid.

-

Zodra u opslaat, zal het systeem deze waarschuwing weergeven: **U hebt ervoor gekozen om een onveilige (TCP/UDP) verbinding met de server te maken. Weet u zeker dat u wilt doorgaan?**, klikt u op **Ja**.



Remote-doel configureren

Afstandsdoel configureren onder registratiecategorieën

Cisco ISE stuurt controleerbare gebeurtenissen naar het syslogdoel. Zodra u uw Remote logging Target hebt geconfigureerd, moet u de **Remote Logging Target** aan de beoogde categorieën koppelen om de controleerbare gebeurtenissen door te sturen.

De logdoelen kunnen dan worden toegewezen aan elk van deze logboekcategorieën. Gebeurtenislogboeken uit deze logcategorieën worden alleen gegenereerd van PSN-knooppunten en kunnen worden geconfigureerd om de relevante logbestanden naar de Remote Syslog-server te sturen, afhankelijk van de services die zijn ingeschakeld op die knooppunten:

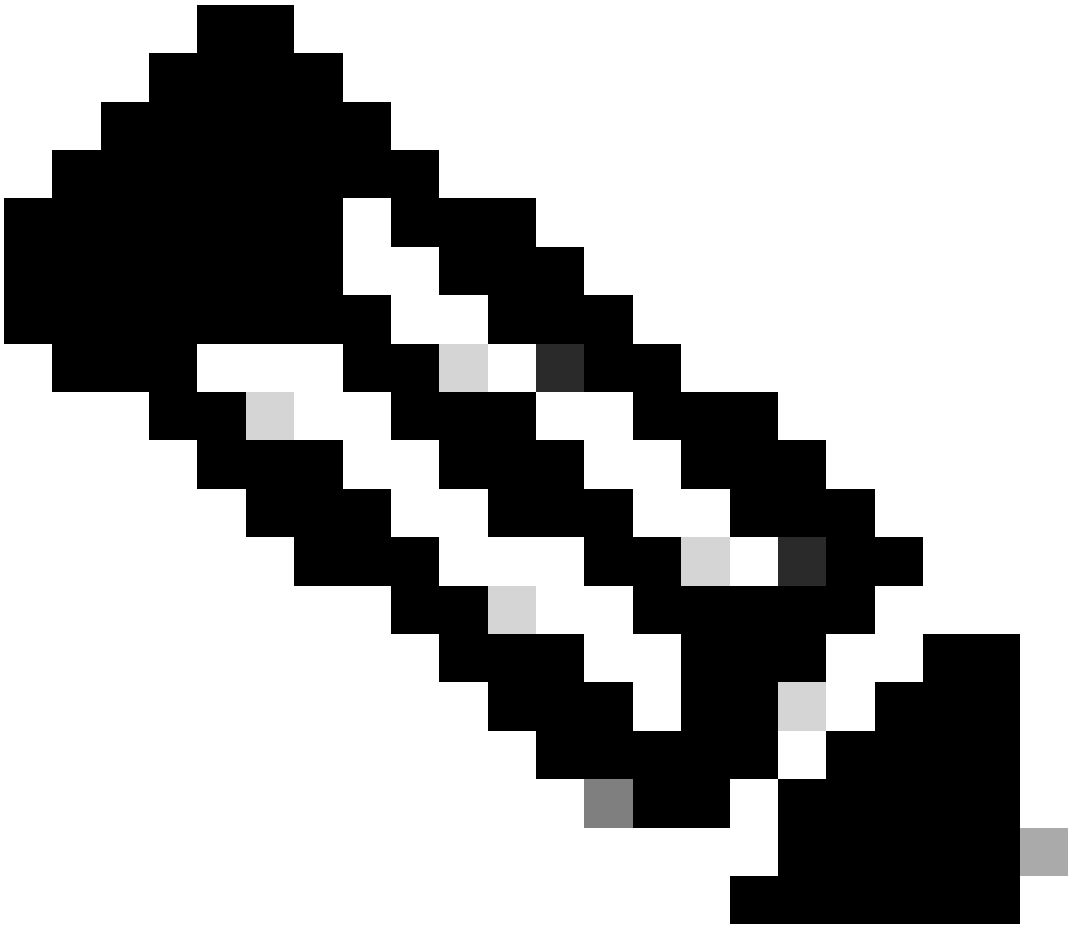
- **AAA-audit**
- **AAA-diagnostiek**
- **Accounting**
- **Externe MDM**
- **Passieve ID**
- **Auditing van houding en clientprovisioning**
- **Positie- en clientprovisioningdiagnostiek**
- **profiler**

Gebeurtenislogboeken uit deze logcategorieën worden gegenereerd van alle knooppunten in de implementatie en kunnen worden geconfigureerd om de relevante logbestanden naar de Remote Syslog-server te verzenden:

- **Administratieve en operationele audits**
- **Systeemdiagnostiek**

- **Systeemstatistieken**

In dit configuratievoorbeeld, gaat u Remote Target configureren onder vier registrerende Categorieën, deze 3 om verificatieverkeerslogboeken te verzenden: **Passed Authentications**, **Mislukte pogingen** en **Radius Accounting,** en deze categorie voor ISE Administrator logboekverkeer:



Opmerking: **Dit configuratievoorbeeld is gebaseerd op screenshot met de naam: Remote Logging Target configureren**

In de Cisco ISE GUI, klik op het pictogram Menu () en kies **Beheer>Systeem>Vastlegging>Categorieën vastlegging** en klik op de gewenste categorie (**Geselecteerde verificaties, mislukte pogingen en RADIUS-accounting).**

Stap 1: Een gebeurtenisbericht wordt gekoppeld aan een prioriteitsniveau, waarmee een beheerder de berichten kan filteren en hieraan prioriteit kan geven. Selecteer het gewenste niveau voor de ernst van het logbestand. Voor sommige registratiecategorieën wordt deze waarde standaard ingesteld en u kunt deze niet bewerken. Voor sommige registrerencategorieën, kunt u één van deze strengheidsniveaus van een vervolgkeuzelijst kiezen:

- **FATAL**: Noodtoestand. Dit niveau betekent dat u geen Cisco ISE kunt gebruiken en dat u onmiddellijk de benodigde actie moet ondernemen.
- **FOUT**: Dit niveau geeft een kritische foutconditie aan.
- **WAARSCHUWING**: Dit niveau duidt op een normale, maar significante aandoening. Dit is het standaardniveau dat is ingesteld voor vele registratiecategorieën.
- **INFO**: Dit niveau geeft een informatieve boodschap aan.
- **DEBUG**: Dit niveau geeft een diagnostisch bugbericht aan.

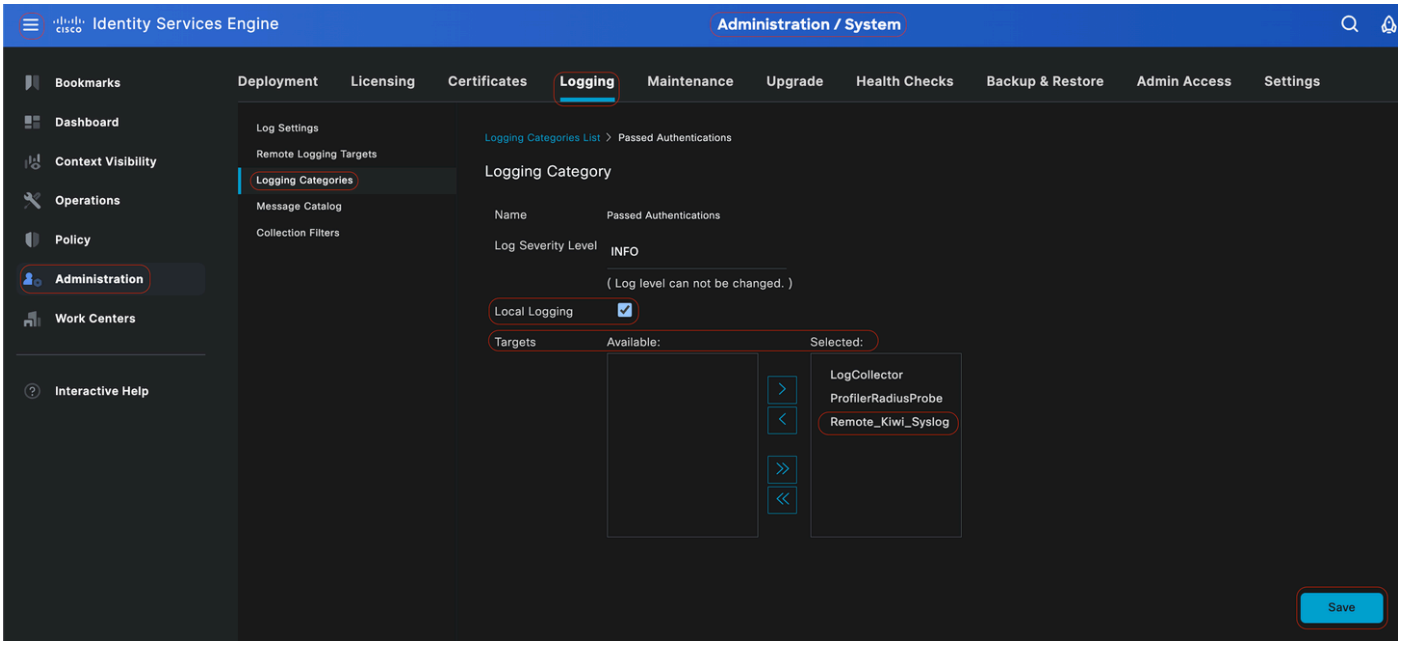
Stap 2 - Lokale vastlegging: Dit selectievakje maakt de lokale loggeneratie mogelijk. Dit betekent dat de logbestanden die door de PSN's worden gegenereerd, ook worden opgeslagen op het specifieke PSN dat het logbestand genereert. We raden aan de standaardconfiguratie te behouden

Stap 3 - Doelstellingen: Dit gebied staat u toe om de doelen voor een registrerencategorie te kiezen door de doelen tussen de Beschikbare en de geselecteerde gebieden over te brengen met behulp van de linker en rechter pijlpictogrammen.

Het beschikbare gebied bevat de bestaande logboekdoelstellingen, zowel lokaal (vooraf gedefinieerd) als extern (door de gebruiker gedefinieerd).

Het geselecteerde gebied, dat in eerste instantie leeg is, geeft vervolgens de doelen weer die voor de categorie zijn gekozen.

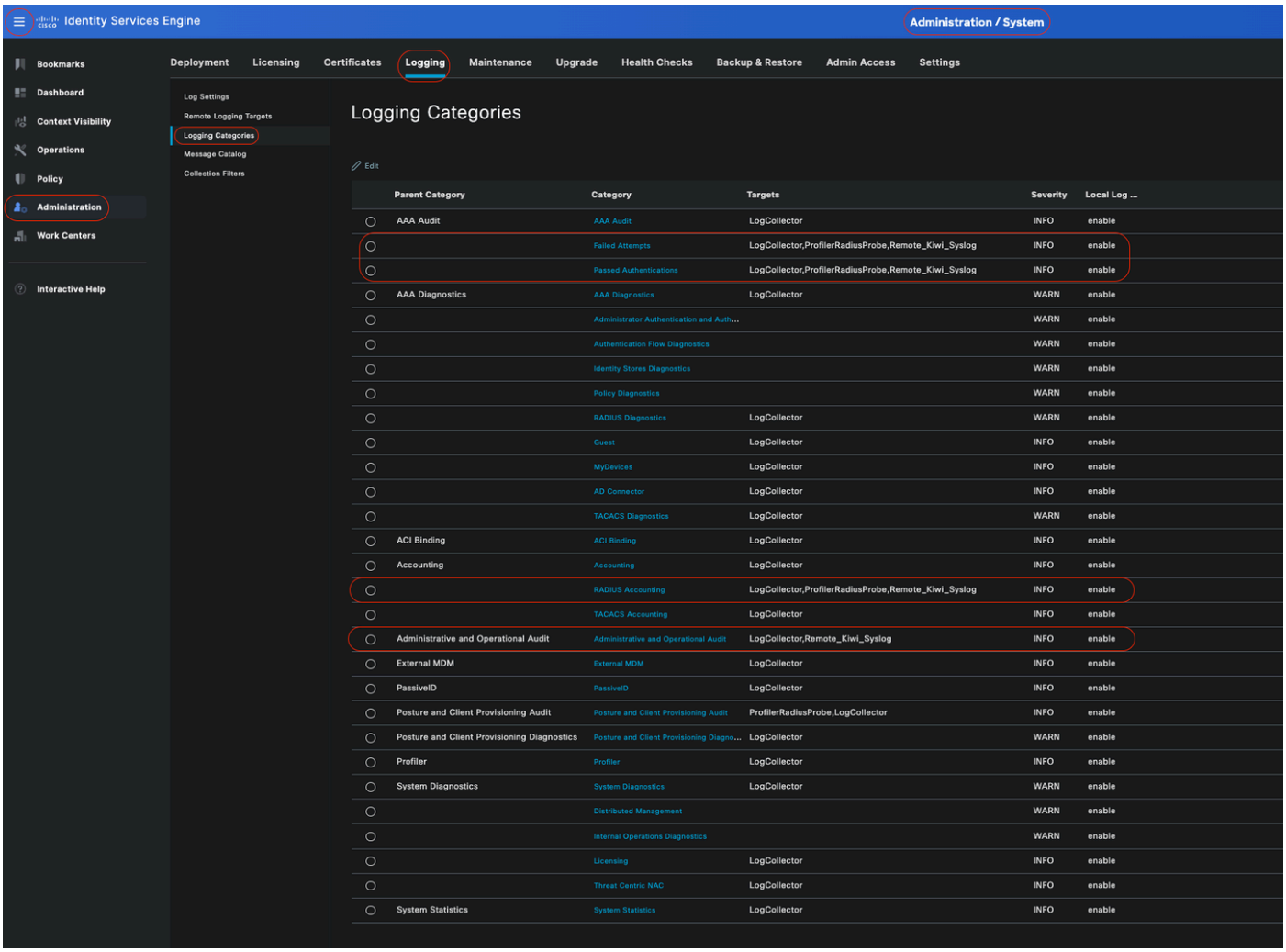
Stap 4- Herhaal van stap 1 tot stap 3 om Remote Target toe te voegen onder **Mislukte Pogingen en Radius Accounting** categorieën.



Toewijzing van externe doelen aan beoogde categorieën

Stap 5- Controleer dat uw Remote Target onder de vereiste categorieën valt.U moet in staat zijn om het externe doel te zien dat u zojuist hebt toegevoegd.

In deze screenshot, kunt u het afgelegen doel **Remote_Kiwi_Syslog** zien toegewezen aan de vereiste categorieën.



Categorieën controleren

Categorieën begrijpen

Er wordt een bericht gegenereerd wanneer er een gebeurtenis plaatsvindt. Er zijn verschillende soorten gebeurtenisberichten gegenereerd vanuit verschillende faciliteiten zoals de kernel, post, gebruikersniveau, etc.

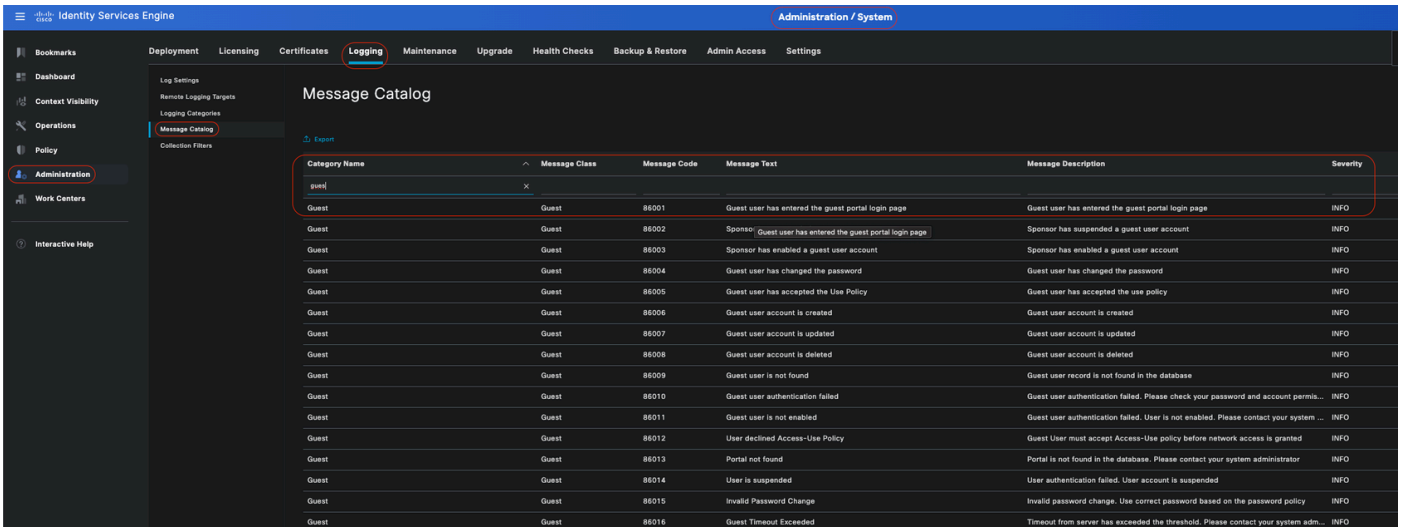
Deze fouten zijn gecategoriseerd in de Berichtencatalogus en deze gebeurtenissen zijn ook hiërarchisch georganiseerd in categorieën.

Deze categorieën hebben Oudercategorieën die een of meer categorieën bevatten.

Oudercategorie	Categorie
AAA-audit	AAA-audit Mislukte pogingen Genormaliseerde verificatie
AAA-diagnostiek	AAA-diagnostiek Beheerderverificatie en -autorisatie

	Verificatie en Flow Diagnostics Identity Store-diagnostiek Beleidsdiagnostiek Radius-diagnostiek gast
Accounting	Accounting Radius-accounting
Administratieve en operationele audits	Administratieve en operationele audits
Auditing van houding en clientprovisioning	Auditing van houding en clientprovisioning
Positie- en clientprovisioningdiagnostiek	Positie- en clientprovisioningdiagnostiek
profiler	profiler
Systeemdiagnostiek	Systeemdiagnostiek Gedistribueerd beheer Interne operationele diagnostiek
Systeemstatistieken	Systeemstatistieken

In deze screenshot kunt u zien dat **Guest** een Message Class is en gecategoriseerd als **Guest Category**. Deze gastcategorie heeft een oudercategorie die **AAA Diagnostics** wordt genoemd.



Berichtencatalogus

Verificatie en probleemoplossing

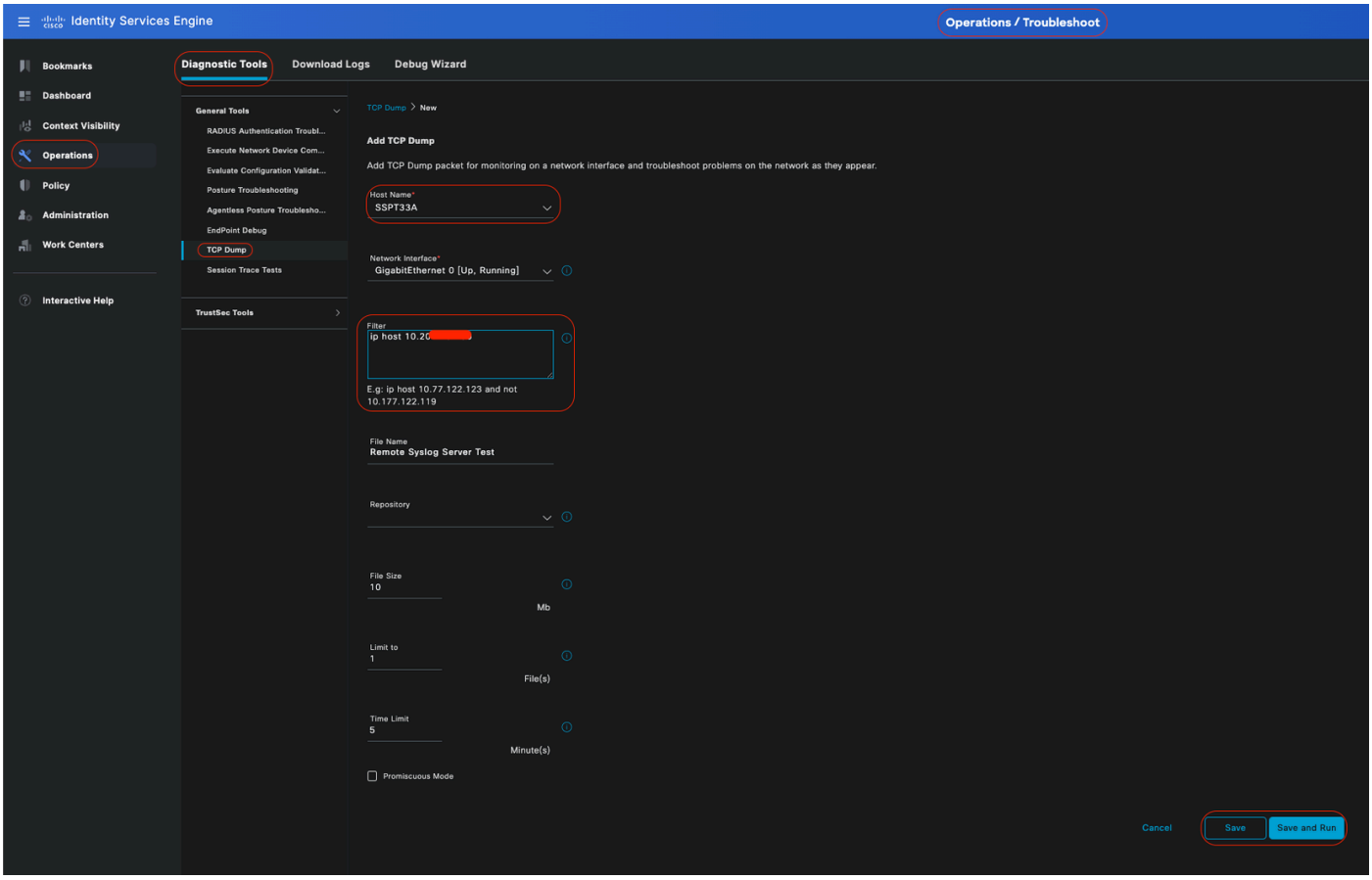
Het nemen van een TCP Dump tegen de Remote Logging Target is de snelste probleemoplossing en het verifiëren van stap om te bevestigen of er loggebeurtenissen worden verzonden of niet.

Capture moet worden gehaald uit het PSN dat de gebruiker authenticeert, omdat PSN logberichten gaat genereren en deze berichten naar het Remote Target zullen worden verstuurd

In de Cisco ISE GUI, klik op het pictogram Menuicon ( ) en kies **Operations**> **Probleemoplossing**>**TCP Dump**> Klik op **Add**.

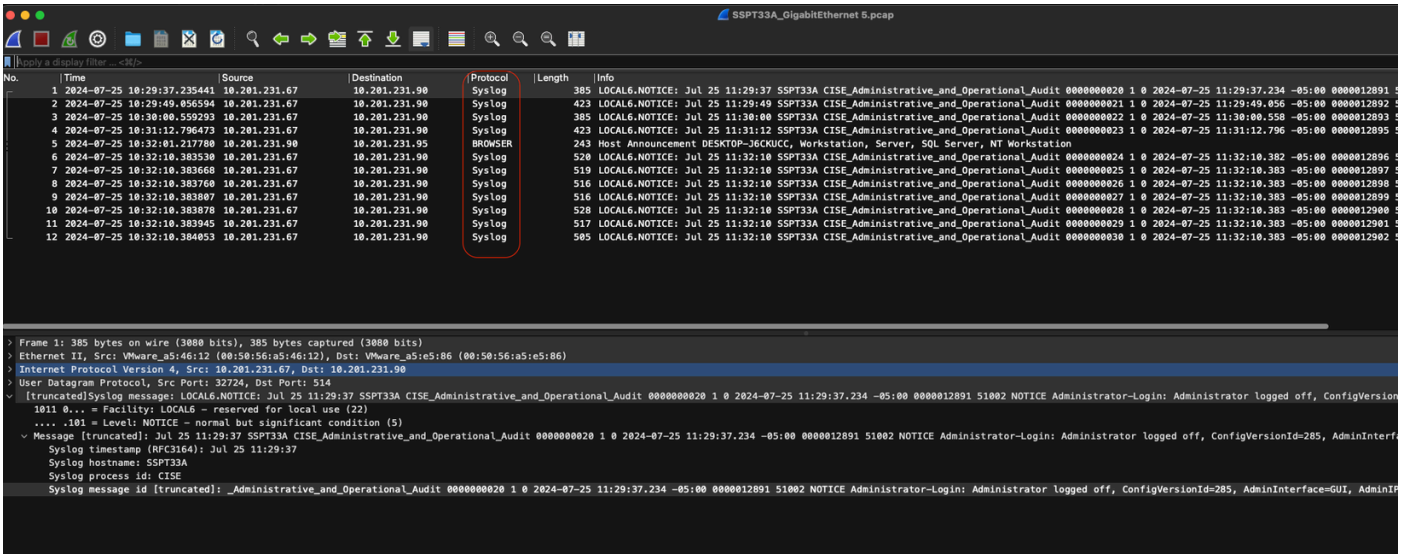
- U moet verkeer filteren, ip-host toevoegen <remote_target_IP_address> filter veld.

- U moet opnamen maken van PSN-bewerkingen voor verificaties.



TCP-pomp

In deze screenshot kunt u zien hoe ISE Syslog-berichten verstuurt voor het logboekverkeer van ISE-beheerders.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.