

Konfigurieren eines externen Syslog-Servers auf der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Konfigurieren des Remote-Protokollierungsziels \(UDP-Syslog\)](#)

[Beispiel](#)

[Konfigurieren des Remote-Ziels unter Protokollierungskategorien](#)

[Kategorien verstehen](#)

[Überprüfen und Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie den externen Syslog-Server auf der ISE konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE).
- Syslog-Server

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Syslog-Meldungen von der ISE werden gesammelt und von Protokollsammlern gespeichert. Diese Protokollsammler werden Überwachungsknoten zugewiesen, sodass MnT die gesammelten Protokolle lokal speichert.

Um Protokolle extern zu sammeln, konfigurieren Sie externe Syslog-Server, die als Ziele bezeichnet werden. Protokolle werden in verschiedene vordefinierte Kategorien eingeteilt.

Sie können die Protokollierungsausgabe anpassen, indem Sie die Kategorien in Bezug auf die Ziele, den Schweregrad usw. bearbeiten.

Konfiguration

Sie können die Webschnittstelle verwenden, um entfernte Syslog-Serverziele zu erstellen, an die Systemprotokollmeldungen gesendet werden. Protokollnachrichten werden gemäß dem Syslog-Protokollstandard (siehe RFC-3164) an die Remote-Syslog-Serverziele gesendet.

Konfigurieren des Remote-Protokollierungsziels (UDP-Syslog)



Klicken Sie in der Cisco ISE-GUI auf das Menüicon (), und wählen Sie Administration>System>Logging>Remote Logging Targets > Click Add (Verwaltung>Protokollierung> Remote-Protokollierungsziele).



Hinweis: Dieses Konfigurationsbeispiel basiert auf dem Screenshot "Configuring Remote Logging Target" (Remote-Protokollierungsziel konfigurieren).

-
- Name wie Remote_Kiwi_Syslog, hier können Sie den Namen des Remote-Syslog-Servers eingeben, dieser wird für beschreibende Zwecke verwendet.
 - Zieltyp als UDP-Syslog. In diesem Konfigurationsbeispiel wird UDP-Syslog verwendet. Sie können jedoch weitere Optionen aus der Dropdown-Liste Zieltyp konfigurieren:

UDP Syslog: Wird zum Senden von Syslog-Meldungen über UDP verwendet und eignet sich für eine einfache und schnelle Protokollierung.

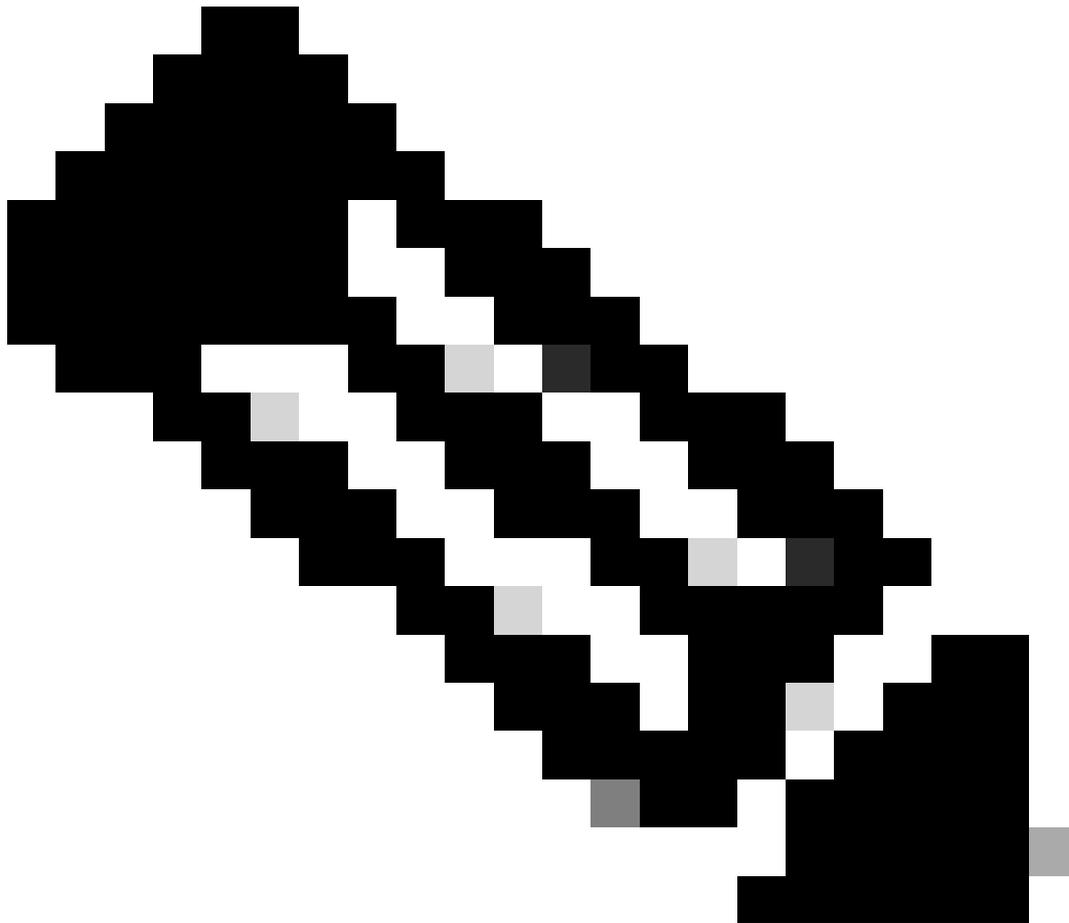
TCP-Syslog: Wird zum Senden von Syslog-Meldungen über TCP verwendet. Dadurch wird die Zuverlässigkeit durch Fehlerprüfung und Funktionen zur erneuten Übertragung gewährleistet.

Sicheres Syslog: Dies bezieht sich auf Syslog-Meldungen, die über TCP mit TLS-Verschlüsselung gesendet werden, um Datenintegrität und Vertraulichkeit zu gewährleisten.

- Status as Enabled (Aktiviert): Wählen Sie in der Dropdown-Liste "Status" die Option Enabled

(Aktiviert) aus.

- Beschreibung, optional können Sie eine kurze Beschreibung des neuen Ziels eingeben.
 - Host/IP-Adresse: Geben Sie hier die IP-Adresse oder den Hostnamen des Zielservers ein, auf dem die Protokolle gespeichert werden. Cisco ISE unterstützt IPv4- und IPv6-Formate für die Protokollierung.
-



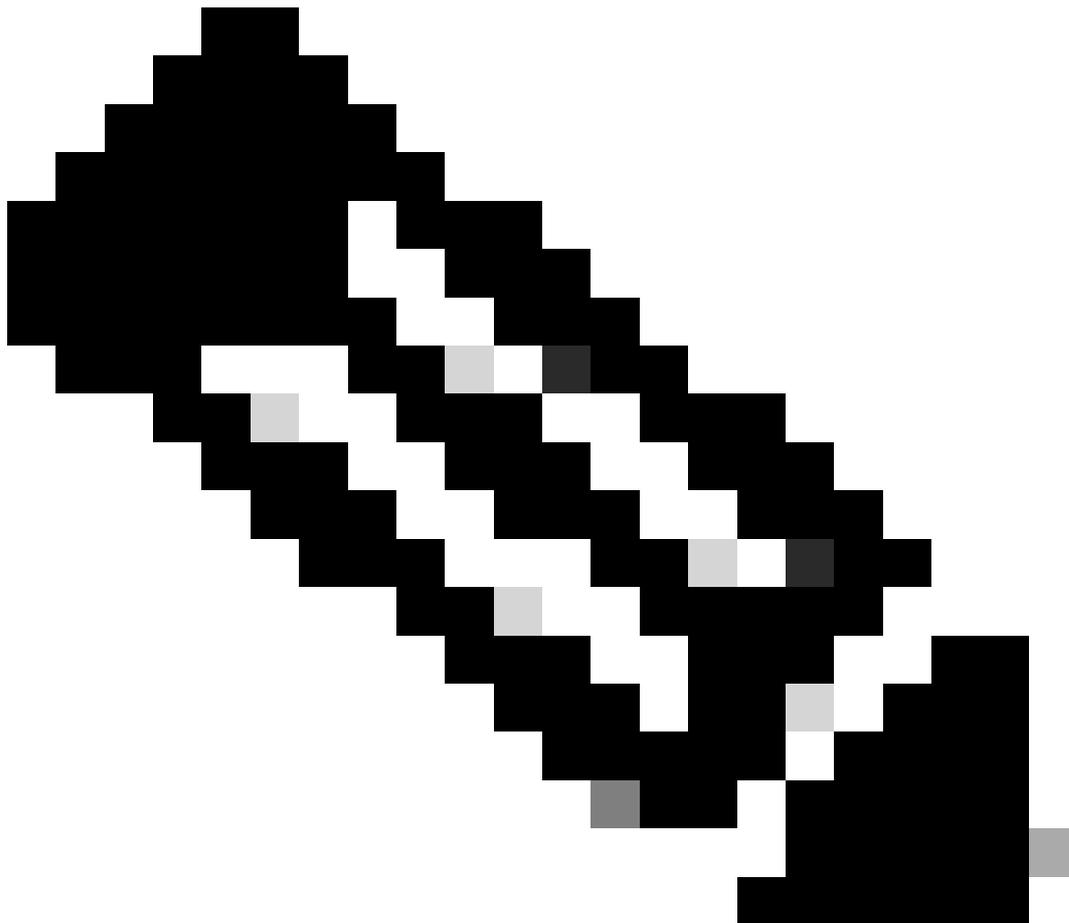
Hinweis: Wenn Sie einen Syslog-Server mit FQDN konfigurieren möchten, müssen Sie das DNS-Caching einrichten, um Beeinträchtigungen der Leistung zu vermeiden. Ohne DNS-Caching fragt die ISE den DNS-Server jedes Mal ab, wenn ein Syslog-Paket an das mit FQDN konfigurierte Remote-Protokollierungsziel gesendet werden muss. Dies hat gravierende Auswirkungen auf die ISE-Performance.

Verwenden Sie `service cache enabled` Befehl im gesamten PSN der Bereitstellung, um Folgendes zu überwinden:

Beispiel

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

- **Port als 514:** In diesem Konfigurationsbeispiel lauscht der Kiwi Syslog-Server Port **514**, der Standardport für UDP-Syslog-Meldungen. Benutzer können diese Portnummer jedoch auf einen beliebigen Wert zwischen 1 und 65535 ändern. Stellen Sie sicher, dass der gewünschte Port nicht von einer Firewall blockiert wird.
 - **Anlagencode als LOCAL6** können Sie den Syslog-Anlagencode, der für die Protokollierung verwendet werden soll, aus der Dropdown-Liste auswählen. Gültige Optionen sind Local0 bis Local7.
 - **Maximale Länge als 1024**, hier können Sie die maximale Länge der Remote-Log-Zielnachrichten eingeben. Die maximale Länge ist standardmäßig auf **1024** festgelegt (ISE 3.3-Version), die Werte liegen zwischen 200 und 1024 Byte.
-

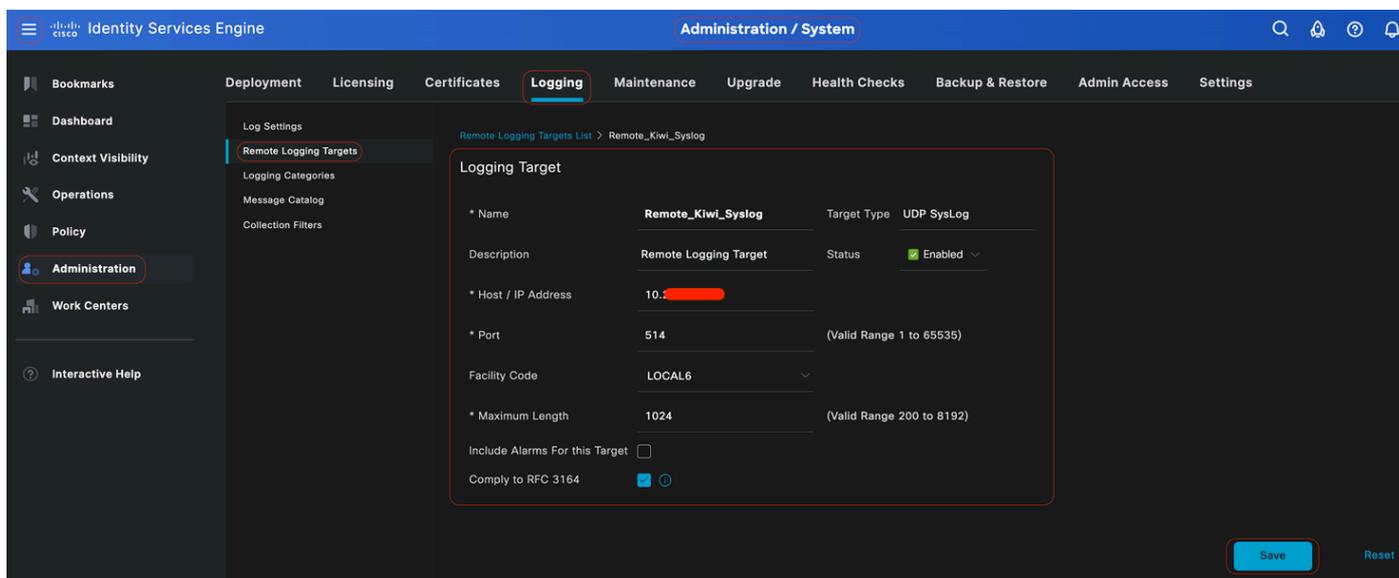


Hinweis: Um zu vermeiden, dass verkürzte Nachrichten an Ihr Remote-Protokollierungsziel gesendet werden, können Sie die Maximallänge auf 8192 einstellen.

- **Alarmer für dieses Ziel einbeziehen**, um es einfach zu halten, in diesem Konfigurationsbeispiel **Alarmer für dieses Ziel einschließen** ist nicht aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden jedoch auch Alarmmeldungen an den Remote-Server gesendet.
- **Compliance to RFC 3164** ist aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden die Trennzeichen (; { } \ \) in den an die Remoteserver gesendeten Syslog-Nachrichten nicht escaped, auch wenn ein umgekehrter Schrägstrich (\) verwendet wird.

Klicken Sie nach Abschluss der Konfiguration auf **Speichern**.

Nach dem Speichern zeigt das System folgende Warnung an: **Sie haben sich entschieden, eine unsichere (TCP/UDP) Verbindung zum Server herzustellen. Möchten Sie wirklich fortfahren?** Klicken Sie auf "Ja".



Konfigurieren des Remote-Ziels

Konfigurieren des Remote-Ziels unter Protokollierungskategorien

Die Cisco ISE sendet überprüfbare Ereignisse an das Syslog-Ziel. Nachdem Sie das Remote-Protokollierungsziel konfiguriert haben, müssen Sie das **Remote-Protokollierungsziel** den vorgesehenen Kategorien zuordnen, um die überprüfbaren Ereignisse weiterzuleiten.

Die Protokollierungsziele können dann jeder dieser Protokollierungskategorien zugeordnet werden. Ereignisprotokolle aus diesen

Protokollkategorien werden nur von PSN-Knoten generiert und können so konfiguriert werden, dass sie die relevanten Protokolle an den Remote-Syslog-Server senden, je nachdem, welche Dienste auf diesen Knoten aktiviert sind:

-

AAA-Audit

-

AAA-Diagnose

-

Buchhaltung

-

Externes MDM

-

Passive ID

-

Status- und Client-Bereitstellungs-Audit

-

Status- und Client-Bereitstellungsdiagnose

-

Profiler

Ereignisprotokolle aus diesen Protokollkategorien werden von allen Knoten in der Bereitstellung generiert und können so konfiguriert werden, dass die relevanten Protokolle an den Remote-Syslog-Server gesendet werden:

-

Verwaltungs- und Betriebsaudit

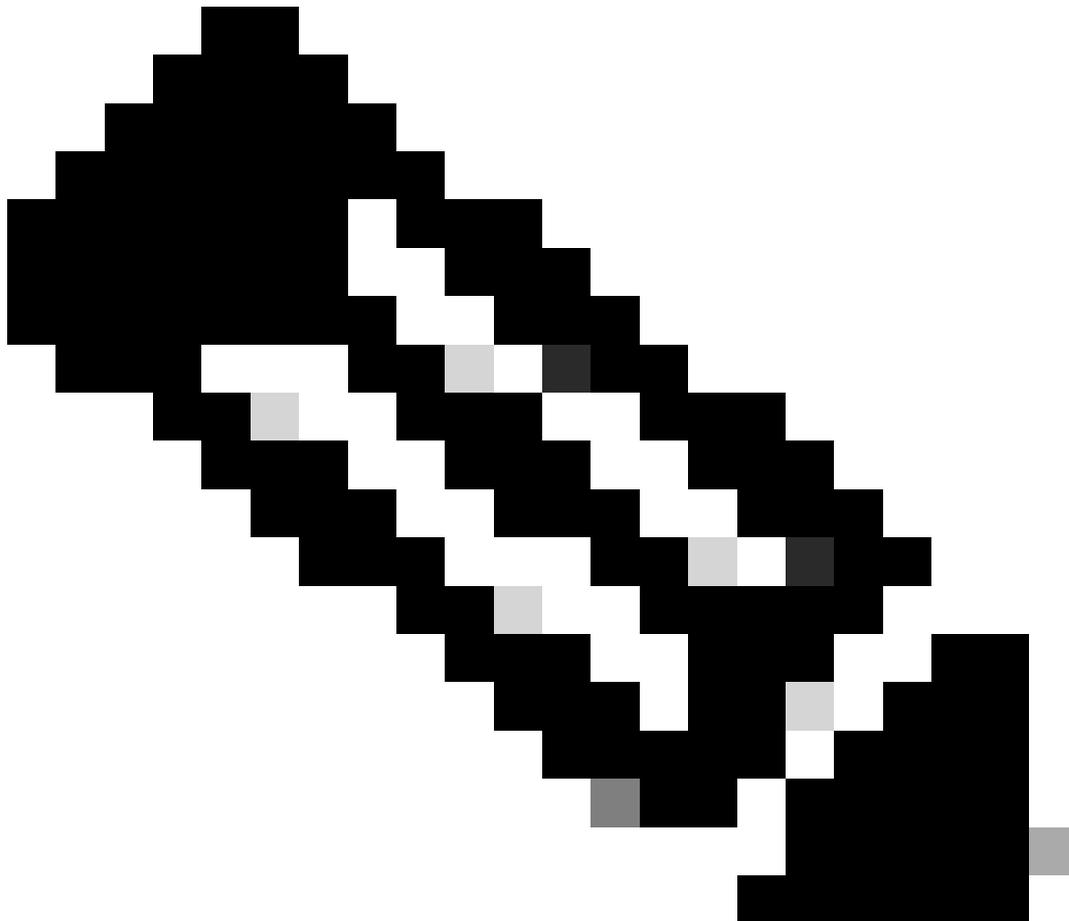
-

Systemdiagnose

-

Systemstatistiken

In diesem Konfigurationsbeispiel konfigurieren Sie Remote Target unter vier Protokollierungskategorien, diese 3 zum Senden von Authentifizierungs-Datenverkehrsprotokollen: **Erfolgreiche Authentifizierungen**, **Fehlgeschlagene Versuche** und **Radius-Abrechnung** sowie diese Kategorie für ISE-Administrator-Protokollierungsdatenverkehr:



Hinweis: Dieses Konfigurationsbeispiel basiert auf dem Screenshot mit dem Namen: Configuring Remote Logging Target (Remote-Protokollierungsziel konfigurieren)



Klicken Sie in der Cisco ISE-GUI auf das Menüicon (), wählen Sie **Administration>System>Logging>Logging Categories**, und klicken Sie auf die erforderliche Kategorie (Erfolgreiche Authentifizierungen, fehlgeschlagene Versuche und Radius-Accounting).

Schritt 1: Schweregrad protokollieren: Eine Ereignismeldung wird mit einem Schweregrad verknüpft, sodass ein Administrator die Meldungen filtern und priorisieren kann. Wählen Sie den Schweregrad des Protokolls nach Bedarf aus. Für einige Protokollierungskategorien ist dieser Wert standardmäßig festgelegt, und Sie können ihn nicht bearbeiten. Für einige Protokollierungskategorien können Sie einen der folgenden Schweregrade aus einer Dropdown-Liste auswählen:

-

FATAL: Notfallstufe. Diese Stufe bedeutet, dass Sie die Cisco ISE nicht verwenden können und sofort die erforderlichen Maßnahmen ergreifen müssen.

-

FEHLER: Dieser Wert gibt einen kritischen Fehlerzustand an.

-

WARNUNG: Dieser Wert gibt einen normalen, aber signifikanten Zustand an. Dies ist die Standardeinstellung für viele Protokollierungskategorien.

-

INFO: Diese Stufe gibt eine Informationsmeldung an.

•

DEBUG: Diese Stufe zeigt eine Diagnosefehlermeldung an.

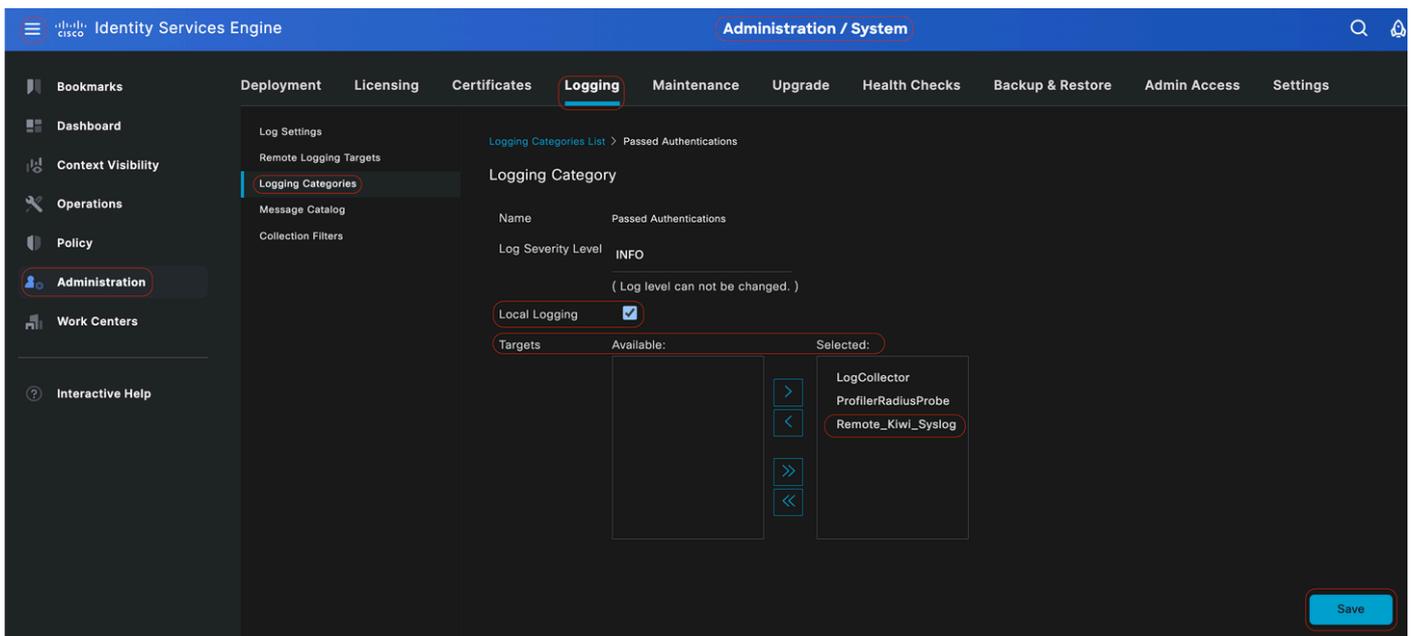
Schritt 2 - Lokale Protokollierung: Mit diesem Kontrollkästchen wird die lokale Protokollgenerierung aktiviert. Das bedeutet, dass die von den PSNs generierten Protokolle auch auf dem jeweiligen PSN gespeichert werden, der das Protokoll generiert. Wir empfehlen, die Standardkonfiguration beizubehalten.

Schritt 3 - Ziele: In diesem Bereich können Sie die Ziele für eine Protokollierungskategorie auswählen, indem Sie die Ziele mithilfe der Pfeilsymbole nach links und rechts zwischen den Verfügbaren und den Ausgewählten Bereichen verschieben.

Der Bereich Available enthält die vorhandenen Protokollierungsziele, sowohl lokale (vordefinierte) als auch externe (benutzerdefinierte) Ziele.

Der Bereich Selectedarea, der zunächst leer ist, zeigt dann die Ziele an, die für die Kategorie ausgewählt wurden.

Schritt 4 - Wiederholen Sie die Schritte 1 bis 3, um Remote Target unter **Failed Attempts (Fehlgeschlagene Versuche) und Radius Accounting (Radius-Abrechnung)** hinzuzufügen.



Remote-Ziele den gewünschten Kategorien zuordnen

Schritt 5: Überprüfen Sie, ob Ihr Remote-Ziel unter den erforderlichen Kategorien liegt. Sie müssen in der Lage sein, das gerade hinzugefügte Remote-Ziel anzuzeigen.

In diesem Screenshot sehen Sie das Remote-Ziel **Remote_Kiwi_Syslog**, das den erforderlichen Kategorien zugeordnet ist.

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	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

Überprüfen von Kategorien

Kategorien verstehen

Eine Meldung wird generiert, wenn ein Ereignis auftritt. Es gibt verschiedene Arten von Ereignismeldungen, die von verschiedenen Einrichtungen generiert werden, z. B. vom Kernel, von E-Mail, von der Benutzerebene usw.

Diese Fehler werden im Nachrichtenkatalog kategorisiert und die Ereignisse hierarchisch in Kategorien eingeteilt.

Diese Kategorien haben übergeordnete Kategorien, die eine oder einige Kategorien enthalten.

Übergeordnete Kategorie	Kategorie
AAA-Audit	AAA-Audit Fehlgeschlagene Versuche Authentifizierung bestanden
AAA-Diagnose	AAA-Diagnose Administrator-Authentifizierung und -Autorisierung

	Authentifizierungs-Ablaufdiagnose Identitätsspeicherdiagnose Richtliniendiagnose Radius-Diagnose Gast
Buchhaltung	Buchhaltung RADIUS-Abrechnung
Verwaltungs- und Betriebsaudit	Verwaltungs- und Betriebsaudit
Status- und Client-Bereitstellungs-Audit	Status- und Client-Bereitstellungs-Audit
Status- und Client-Bereitstellungsdiagnose	Status- und Client-Bereitstellungsdiagnose
Profiler	Profiler
Systemdiagnose	Systemdiagnose Verteilte Verwaltung Interne Betriebsdiagnose
Systemstatistiken	Systemstatistiken

In diesem Screenshot sehen Sie, dass **Guest** eine Message Class ist und als **Guest Category** kategorisiert ist. Diese Gastkategorie verfügt über eine übergeordnete Kategorie mit dem Namen **AAA Diagnostics**.

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

Nachrichtenatalog

Überprüfen und Fehlerbehebung

Ein TCP-Dump für das Remote-Protokollierungsziel ist der schnellste Fehlerbehebungs- und Verifizierungsschritt, um zu bestätigen, ob Protokollereignisse gesendet werden.

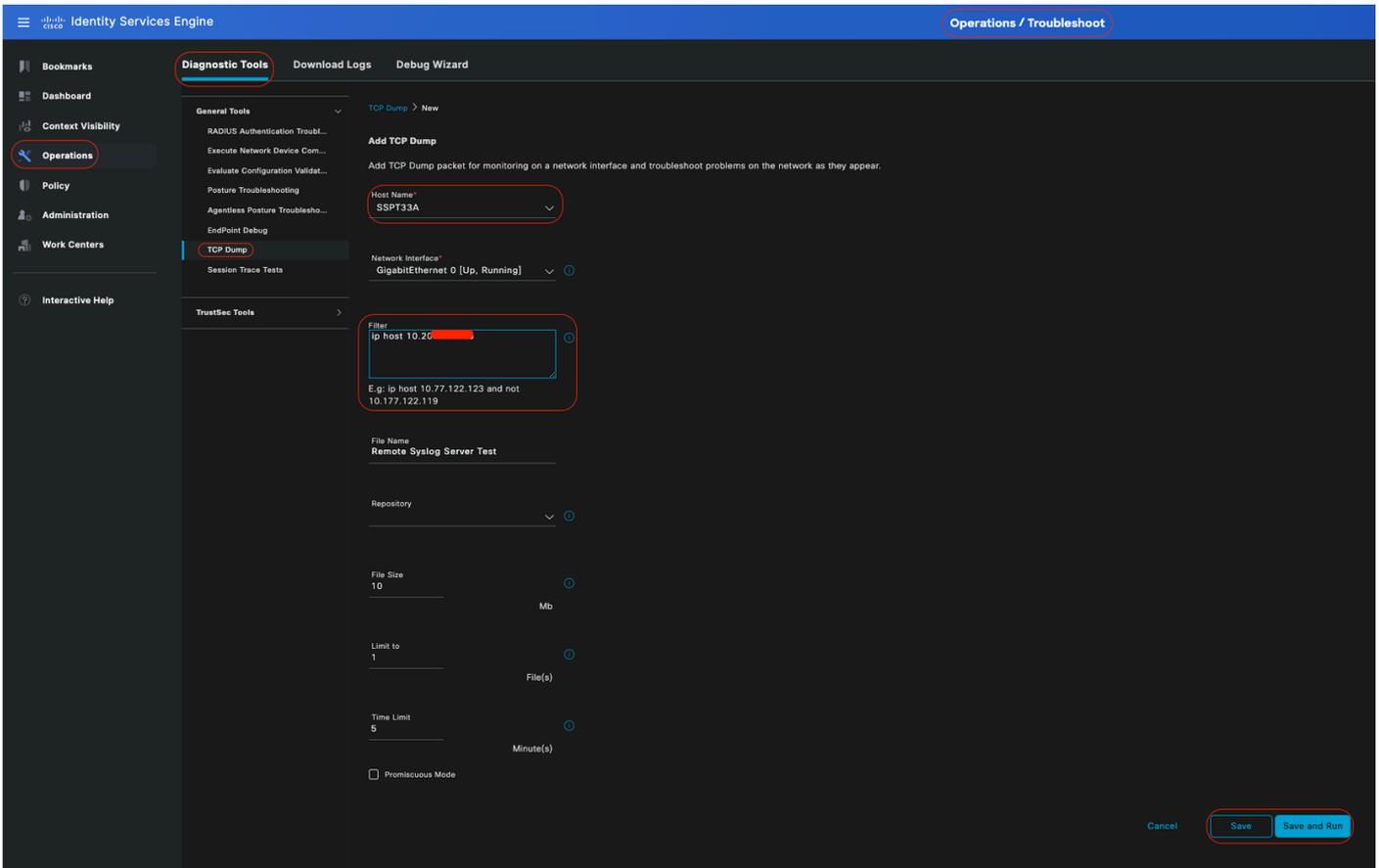
Die Erfassung muss vom PSN übernommen werden, der den Benutzer authentifiziert, da PSN Protokollmeldungen generieren wird und diese Meldungen an das Remote-Ziel gesendet werden.



Klicken Sie in der Cisco ISE-GUI auf das Menuicon () und wählen Sie **Operations> Troubleshoot>TCP Dump> Click on Add aus.**

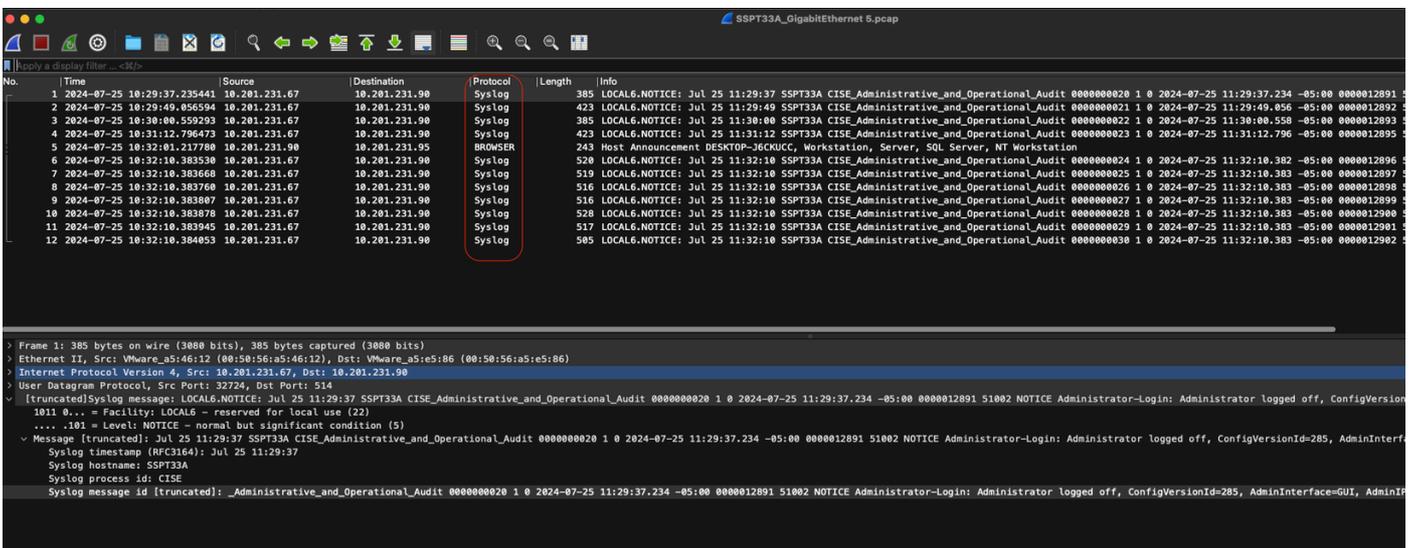
- Sie müssen den Datenverkehr filtern und das IP-Host-Filterfeld <remote_target_IP_address> hinzufügen.

- Sie müssen die Erfassung von der PSN-Verarbeitung von Authentifizierungen übernehmen.



TCP-Dump

In diesem Screenshot sehen Sie, wie die ISE Syslog-Meldungen für den Protokollverkehr des ISE-Administrators sendet.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.