Konfigurieren eines externen Syslog-Servers auf der ISE

Inhalt

 Einleitung

 Voraussetzungen

 Anforderungen

 Verwendete Komponenten

 Hintergrundinformationen

 Konfiguration

 Beispiel

 Konfigurieren des Remote-Protokollierungsziels (UDP-Syslog)

 Beispiel

 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 Menuicon (

), 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 enableden Befehl im gesamten PSN der Bereitstellung, um Folgendes zu überwinden:

Beispiel

• **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.

• Alarme für dieses Ziel einbeziehen, um es einfach zu halten, in diesem Konfigurationsbeispiel Alarme 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".

	dentity Services	Engine					Adm			Q	٨	?	Q			
Ц	Bookmarks	Deployment	Licensing	Certific	ates	Logging	Maintenance	Upgrade	Health Check	s Backup & Restore	Admin Access	Settings				
	Dashboard	Log Settings				Targets List	Remote Kiwi Svslog									
망	Context Visibility	Remote Logging	Targets	Lo	oqqinq Ta	raet										
*	Operations	Logging Catego Message Catalo	ries 9		00 0											
Ð	Policy	Collection Filters			* Name		Remote_Kiv	wi_Syslog	Target Type	UDP SysLog						
20	Administration				Description		Remote Log	ging Target	Status	Z Enabled 🗸						
1	Work Centers				* Host / IP Address		10.:									
					* Port		514		(Valid Range	1 to 65535)						
?	Interactive Help				Facility Cod	e	LOCAL6									
					* Maximum	Length	1024		(Valid Range	200 to 8192)						
					Include Alar	ms For this Ta	arget									
					Comply to R	FC 3164	0									
													Save		R	eset

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 ٠ 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:

•

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 Menuicon (

), 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 Availableenthält 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.

	dentity Services	Engine				Adm	inistration /	/ System				Q						
рц	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings							
==	Dashboard	Log Settings Remote Logging	Targets		Logging Categories List > Passed Authentications													
	Context Visibility	Logging Categor	ries	Logging	ing Category													
×	Operations	Message Catalo	9	Name	Name Passed Authentications													
U	Policy	Collection Filters	s	Log Sever	rity Level IN	NFO												
20	Administration				(L	og level can not be cha	nged.)											
តី	Work Centers			Local Log	ging	V												
				Targets	Av	vailable:	Sele	cted:										
	Interactive Help							ogCollector										
								emote_Kiwi_Syslog										
												Save						

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.

	dentity Services I	Engine	/ System	item									
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
52	Dashboard	Log Settings											
	Context Visibility	Remote Logging	Targets	Logo									
4	Operations	Logging Categor	ries										
2	B _11	Collection Filters	9 5										
~	Policy				Parent Categor	ny	Ca	ategory	Targets	Targets			Local Log
20	Administration			0	AAA Audit				LogCollector			INFO	enable
	Work Centers			0					LogCollector,	ProfilerRadiusProbe,Rei	mote_Kiwi_Syslog	INFO	enable
									LogCollector,	ProfilerRadiusProbe,Rei	mote_Kiwi_Syslog	INFO	enable
	Interactive Help			0	AAA Diagnostic	CS			LogCollector			WARN	enable
				0								WARN	enable
				0								WARN	enable
				0								WARN	enable
				0								WARN	enable
				0					LogCollector			WARN	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0					LogCollector			WARN	enable
				0	ACI Binding				LogCollector			INFO	enable
				0	Accounting				LogCollector			INFO	enable
				0					LogCollector,	ProfilerRadiusProbe,Rei	mote_Kiwi_Syslog	INFO	enable
				0					LogCollector			INFO	enable
				0	Administrative	and Operational Audit			dit LogCollector,	Remote_Kiwi_Syslog		INFO	enable
				0	External MDM				LogCollector			INFO	enable
				0	PassiveID				LogCollector			INFO	enable
				0	Posture and Cli	ient Provisioning Audit			udit ProfilerRadius	sProbe,LogCollector		INFO	enable
				0	Posture and Cli	ient Provisioning Diagn	ostics Po		agno LogCollector			WARN	enable
				0	Profiler				LogCollector			INFO	enable
				0	System Diagno	stics			LogCollector			WARN	enable
				0								WARN	enable
				0								WARN	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0	System Statisti	cs			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**.

=	dentity Services	Engine									Administration / System		
Į	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
53	Dashboard	Log Settings											
ris	Context Visibility	Remote Logging	Targets	Mess	age Ca	atalog							
- %	Operations	Message Catalog											
0	Policy	Collection Filters											
(2)	Administration			Category	/ Name			Message Class	Message Code	Message Text		Message Description	Severity
				snes									
-11	Work Centers			Guest				Guest	86001	Guest user has	s entered the guest portal login page	Guest user has entered the guest portal login page	INFO
				Guest				Guest	86002	Sponso Guest	t user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO
(?	Interactive Help			Guest				Guest	86003	Sponsor has e	nabled a guest user account	Sponsor has enabled a guest user account	INFO
				Guest				Guest	86004	Guest user has	s changed the password	Guest user has changed the password	INFO
				Guest				Guest	86005	Guest user has	s accepted the Use Policy	Guest user has accepted the use policy	INFO
				Guest				Guest	86006	Guest user act	count is created	Guest user account is created	INFO
				Guest				Guest	86007	Guest user act	count is updated	Guest user account is updated	INFO
				Guest				Guest	86008	Guest user act	count is deleted	Guest user account is deleted	INFO
				Guest				Guest	86009	Guest user is r	not found	Guest user record is not found in the database	INFO
				Guest				Guest	86010	Guest user aut	thentication failed	Guest user authentication failed. Please check your password and account permis.	. INFO
				Guest				Guest	86011	Guest user is r	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 four	nd	Portal is not found in the database. Please contact your system administrator	INFO
				Guest				Guest	86014	User is susper	nded	User authentication failed. User account is suspended	INFO
				Guest				Guest	86015	Invalid Passwo	ord Change	Invalid password change. Use correct password based on the password policy	INFO
				Quest				Quant	96016	Quest Timesud	Expended	Timpout from contrast has exceeded the threshold Disase contact your system ode	INFO

Nachrichtenkatalog

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.

\equiv $\frac{1}{cisco}$ Identity Services	Engine	Operations / Troubleshoot
Bookmarks	Diagnostic Tools Download L	Logs Debug Wizard
Dashboard	General Tools 🗸	TGP Dump > New
Context Visibility	RADIUS Authentication Troubl Execute Network Device Com	Add TCP Dump
Policy	Evaluate Configuration Validat Posture Troubleshooting	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
Administration	Agentiess Posture Troublesho EndPoint Debug	SSPT33A
H Work Centers	TCP Dump Session Trace Tests	Network Indeface' GlobbliEthernet 0 (Jus. Rumino) V ()
Interactive Help		
	Irustsec loois	Filer ip host 10.20
		E av (b) have 10 72 102 102 and not
		10.177.122.119
		File Name Remote Syslog Server Test
		Repository 🗸 🛈
		10 0 Mb
		Limit to 1
		Timu limit
		5 0 Minute(s)
		Promiscuous Mode
		Cancel Save and Run

TCP-Dump

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

•••																					SSPT33A_GigabitEthernet 5.pcap
4 🗖] 🦽	<u>(</u>	9			×	3	্	(۵	2	ি	♣			0	Ð, (a , (R, 1	•	
Apply a	a disp	olay fili	ter <	3\$/>																	
No.	T 1 2 2 2 3 2 4 2 5 2 6 2 7 2 8 2 9 2 10 2 11 2 12 2	ime 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4 2024-4	87-25 87-25 87-25 87-25 87-25 87-25 87-25 87-25 87-25 87-25 87-25 87-25	10:2 10:2 10:3 10:3 10:3 10:3 10:3 10:3 10:3 10:3	9:37. 9:49. 0:00. 1:12. 2:10. 2:10. 2:10. 2:10. 2:10. 2:10.	23544 05659 55929 79647 21778 38353 38366 38376 38380 38387 38394 38405	Sou 1 10 4 10 3 10 8 10 8 10 8 10 8 10 7 10 8 10 5 10 3 10	urce 201 201 201 201 201 201 201 201 201 201	231.6 231.6 231.6 231.6 231.6 231.6 231.6 231.6 231.6 231.6 231.6	7 7 7 7 7 7 7 7 7 7 7 7 7 7		Desti 10.2 10.2 10.2 10.2 10.2 10.2 10.2 10.2	nation 01.23 01.22 01.22 01.22 01.22 01.22 01.22 01.22 01.22 01.22 01.22 01.22	31.90 31.90 31.90 31.90 31.90 31.90 31.90 31.90 31.90 31.90		Prote Sys Sys Sys Sys Sys Sys Sys Sys Sys Sys	ocol log log log log wSER log log log log log	ļL	ength	385 423 385 423 243 520 519 516 516 528 517 505	Indo LGCL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 000000020 1 0 2024-07-25 11:29:37.224 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:29:06 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:29:06.558 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:30:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:06.558 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:30:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:06.558 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:31:12 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.382 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:39:10.383 -05:00 0000012005 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10.383 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000023 1 0 2024-07-25 11:32:10.383 -05:00 0000012001 LGCL6.NOTICE: Jul 25 11:32:10 SSPT3A CISE_Administrative_and_Operational_Audit 000000023 1 0 2024-07-25 11:32:10.383 -05:00 0000012001 LGCL6.NOTICE
<pre>> Frame > Ether > Inter > User < [tru 103 > Mes</pre>	1: net Data Incat 11 0 Sysl Sysl Sysl Sysl	385 II, 5 Prote sgram ted]S 101 = e [tr log t log h log p log m	bytes Src: \ Proto yslog Faci Leve uncat imest ostnal roces: essage	on v Mwar Jersi Jocol, mess lity l: N ded]: amp me: S s id: s id: e id	re_a5: on 4, Src age: LOC OTICE Jul (RFC3: SPT3: CISE [trun	3080 46:12 Src: Port: LOCAL AL6 - no 25 11 64): A cated	bits) (00: 3272 6.N01 rese mal :29:3 Jul :]: _/	, 38 50:5 24, C TICE: rved but 7 SS 25 12	85 byt6 66:a5:- 231.67 0st Po 5 Jul 1 for l signif PT33A L:29:3 nistra	es ca 46:12 , Dst rt: 5 25 11 .ocal ficant CISE_ 7 tive_	pture), Ds : 10. 14 :29:3 use (: conc Admir and_0	d (30 t: VM 201.2 7 SSF 22) litio istro	180 b: Nware_ 131.91 1733A n (5) ative	its) _a5:e5 0 CISE_ e_and_ L_Audi	5:86 (_Admin Opera it 000	(00:50 histra tiona	0:56: ative l_Aud 020 1	a5:e5 _and_ dit 0	:86) Opera 00000	ation 0020 7-25	hal_Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator Logged off, ConfigVersion 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator Logged off, ConfigVersionId=285, AdminInterf 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator Logged off, ConfigVersionId=285, AdminInterface=GUI, AdminI

Syslog-Datenverkehr

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.