Externe systeemserver op ISE configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configuratie Remote Logging Target configureren (UDP Syslog) Voorbeeld Afstandsdoel configureren onder registratiecategorieën Categorieën begrijpen Verificatie en probleemoplossing

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 syslogberichten 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.

	dentity Services	Engine						Adn	ninistration /	/ System				Q	۵	?	¢
Щ	Bookmarks	Deployment	Licensing	Cer	tificates	Logging	Mai	intenance	Upgrade	Health Chec	ks Backup & Resto	e Admin Acces	s Settings				
22	Dashboard	Log Settings					> Remo	ote_Kiwi_Syslog									
ц.	Context Visibility	Remote Logging	Targets		Logging	Target											
×	Operations	Message Catalo	9		* Name			Remote Ki	wi Svslog	Target Type	UDP SysLog						
•	Policy	Collection Filters															
20	Administration				Descriptio	on		Remote Log	ging Target	Status	Enabled ~						
គា	Work Centers				* Host / If	P Address		10.:									
					* Port			514		(Valid Range	e 1 to 65535)						
?	Interactive Help				Facility Co	ode		LOCAL6									
					* Maximu	m Length		1024		(Valid Range	e 200 to 8192)						
					Include A	larms For this 1	Target										
					Comply to	o RFC 3164		0									
														Save			

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

٠

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.

	dentity Services	Engine				Adm	inistrati	on / System				Q	۵
Į	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrad	e Health Checks	Backup & Restore	Admin Access	Settings		
≡≡ .ud	Dashboard	Log Settings Remote Logging	Targets			Passed Authentications							
16	Context Visibility	Logging Categor	ries	Logging (Category								
~~	Operations	Message Catalog	9	Name	Pa	ssed Authentications							
U	Policy	Collection Filters	5	Log Sever	^{ty Level} I	NFO							
20	Administration				(1	Log level can not be cha	inged.)						
កា	Work Centers			Local Logg	jing								
				Targets	A	vailable:		Selected:					
?	Interactive Help							LogCollector ProfilerRadiusProbe					
								Remote_Kiwi_Syslog					
_													
_											9	Save	J

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.

	ahaha Identity Services I	Engine									(Administration /	System	
Щ	Bookmarks	Deployment L	Licensing (Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup	& Restore	Admin Access	Settings		
52	Dashboard	Les Catilans												
	Context Visibility	Remote Logging Tar	rgets	Logg	ing Cat	egories								
	Context visibility	Logging Categories												
×	Operations	Message Catalog												
	Policy	Collection Filters			Parent Categor	v	c	Category		Targete		Severity	Local Log	
20	Administration									ogCollector			INFO	enable
	Work Centers			6	/ corridon				-	ogCollector Pro	filerRadiusProbe Rem	note Kiwi Suslag	INFO	enable
									-	LogCollector, PromerkadiusProbe, Remote_Kiwi_Syslog			INFO	enable
	Interactive Help				AAA Diagnosti	:8			-	ogCollector		loto_ktm_oyslog	WARN	enable
				0									WARN	enable
													WARN	enable
								fentity Stores Diagnostics					WARN	enable
													WARN	enable
				0						ogCollector			WARN	enable
				0						ogCollector			INFO	enable
				0						ogCollector			INFO	enable
				0						ogCollector			INFO	enable
				0						ogCollector			WARN	enable
				0	ACI Binding					ogCollector			INFO	enable
				0	Accounting					ogCollector			INFO	enable
				0						ogCollector,Pro	filerRadiusProbe,Rem	note_Kiwi_Syslog	INFO	enable
				0						ogCollector			INFO	enable
				0	Administrative	and Operational Audit				ogCollector,Rer	mote_Kiwi_Syslog		INFO	enable
				0	External MDM					ogCollector			INFO	enable
				0	PassiveID					ogCollector			INFO	enable
				0	Posture and Cli	ent Provisioning Audi			Audit P	rofilerRadiusPro	obe,LogCollector		INFO	enable
				0	Posture and Cli	ent Provisioning Diag	nostics P			ogCollector			WARN	enable
				0	Profiler					ogCollector			INFO	enable
				0	System Diagno	stics				ogCollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0						ogCollector			INFO	enable
				0						ogCollector			INFO	enable
				0	System Statisti	CS				ogCollector			INFO	enable

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.

=	dentity Services I	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	italog							
- %	Operations	Message Catalog											
0	Policy	Collection Filters											
G	Administration			Category	Name			Message Class	Message Code	Message Text		Message Description	Severity
				gues									
-1	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	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	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	hentication 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	d	Portal is not found in the database. Please contact your system administrator	INFO
				Guest				Guest	86014	User is susper	ded	User authentication failed. User account is suspended	INFO
				Guest				Guest	86015	Invalid Passwo	rd Change	Invalid password change. Use correct password based on the password policy	INFO
								0	00010			The set of the second back and the three hold. Block and the second second	11/20

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.

\equiv $\frac{1}{cisco}$ Identity Services	s Engine	Operations / Troubleshoot	
Bookmarks	Diagnostic Tools Download L	ogs Debug Wizard	
Dashboard	General Tools ~	TCP Dump > New	
Context Visibility	RADIUS Authentication Troubl Execute Network Device Com	Add TCP Dump	
	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 V	
	TCP Dump Session Trace Tests	Network Interface"	
Interactive Help	Trustes Tech		
		Filer lip host 10.20	
		E n: (n knot 10 77 122 123 and ext	
		10.177.122.119	
		File Name Remote Syslog Server Test	
		Repository	
		File State 10 O	
		Mb	
		Limit to 1	
		File(a)	
		Time Limit 0 5	
		Promiscuous Mode	
			Icel Save Save and Run

TCP-pomp

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

• • •																					SSPT33A_GigabitEthernet 5.pcap
4		0				×	6	্		⇒	2	$\overline{\mathbf{O}}$	4	Ŀ			⊕ `	Q	Q	•	
Apply	a disp	olay filter	· <‡	/>																	
No.	T	ime					Sou	irce				Des	tinatio	on		P	otoco	1	Leng	th	th Info
Г	1 2	2024-07	-25 :	10:29	:37.2	35441	L 10.	201.	231.6	7		10.	201.	231.9	3	S	slog			385	385 LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 00000000020 1 0 2024-07-25 11:29:37.234 -05:00 00000128
	2 2	2024-07	-25 :	10:29	:49.6	156594	10.	.201.	231.6	7		10.	201.	231.9	8	S	/slog			423	423 LOCAL6.NOTICE: Jul 25 11:29:49 SPF13A CISE_Administrative_and_Operational_Audit 0000000021 1 0 2024-07-25 11:29:49.056 -05:00 00000128
	3 2	2024-07	-25	10:30	:00.5	59293	3 10.	.201.	231.6	/		10.	201.	231.9	9	S	/slog	,		385	385 LOCAL6.NOTICE: JUL 25 11:30:00 SSPT33A CISE_Administrative_and_Operational_Audit 0000000022 1 0 2024-07-25 11:30:00.558 -05:00 00000128
Į.	4 2	2024-07	-25	0:31	:12.7	96473	3 10.	201.	231.6	<u></u>		10.	201.	231.9	0 -	5	SLOG) 10		423	423 LUCAL5.NOTICE: JUL 25 11:31:12 SPT33A CISE_Administrative_and_Operational_Audit 0000000023 1 0 2024-07-25 11:31:12.796 -05:00 00000128
1	6 2	024-07	-25 :	10:32	.101.4	1//8) 10. 10	201.	231.9	0 7		10.	201.	231.9	2	B	Close	:K		243	243 HOST ANNOUNCEMENT UESKIUP-JOKUUC, WORKSTATION, SERVER, SUL SERVER, NI WORKSTATION 520 LORALE NOTICE: 11/ 21 11/22/18 CEDT224 CTCE Administrative and Constraines) Audia 4000000071 1 0 2024-07-25 11/22/18 202 -05:00 00000110
	7 3	024-07	-25	10.32	-10.3	193669	10	201.	231.6	,		10.	201.	231.9	a	5				510	510 ICCC.0.1001.0C1 JUL 25 11:32:10 53-1354 C132_AUMINISCIGUET_AIN_04011 000000024 1 0 2024-07-25 11:32:10:352 -05:00 000000155 12 302-05:00 000000000000000000000000000000000
	8 2	024-07	-25	0.32	10.3	83766	10	201	231.6	,		10	201	231.9	à	5	slog			516	516 [OCAL6.NOTICE: JUL 25 11:32:10 35 F334 CICE Administrative_interpolational Audit 000000025 1 0 202-07-25 11:32:10:303 -05:00 00000020
	9 2	024-07	-25	0:32	:10.3	18380	10	201.	231.6	,		10.	201.	231.9	à	s	slog			516	516 LOCALE.NOTICE: Jul 25 11:32:10 SSPT33A CISE Administrative and Operational Audit 000000027 1 0 2024-07-25 11:32:10.383 -05:00 00000020
	10 2	024-07	-25	10:32	:10.3	83878	3 10.	201.	231.6	,		10.	201.	231.9	3	s	slog			528	528 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE Administrative and Operational Audit 0000000028 1 0 2024-07-25 11:32:10.383 -05:00 00000129
	11 2	024-07	-25 :	10:32	:10.3	83945	5 10.	.201.	231.6	7		10.	201.	231.9	9	S	slog			517	517 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000029 1 0 2024-07-25 11:32:10.383 -05:00 00000129
L	12 2	024-07	-25 :	10:32	:10.3	84053	3 10.	201.	231.6	7		10.	201.	231.9	9	s	slog			505	505 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000030 1 0 2024-07-25 11:32:10.383 -05:00 00000129
	_		_	_	_	_	_	_		_	_	_	_			_	_	_			
> Eram	e 1:	385 by	tes	on wi	re (3	1080	its)	. 38	5 byte	is ca	oture	d (3	080	bits)							
> Ethe	rnet	II, Sr	c: V	ware	_a5:4	6:12	(00:	50:5	6:a5:4	6:12), Ds	t: V	Mwar	e_a5:	e5:86	(00:	50:5	6:a5:	e5:86		
> Inte	rnet	Protoc	ol V	ersio	n 4,	Src:	10.2	01.2	31.67,	Dst	: 10.	201.	231.	90							
> User	Data	agram P	roto	:ol,	Src F	Port:	3272	4, D	st Por		14										
∨ [tr	uncat	ted]Sys	log i	nessa	ge: I	OCAL	5.NOT	ICE:	Jul 2	25 11	:29:3	7 SS	РТ33	A CIS	E_Adm:	inist	rati	ve_ar	id_0pe	ratio	rational_Audit 0000000000 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVers
10	011 0	•••• = F	Facil	ity:	LOCA	L6 –	rese	rved	for l	ocal	use	(22)									
		101 = L	Level	: NO	TICE	- nor	mali	but s	ignif	icant	con	litio	on (!	5)							
∨ Me	essag	e [trur	ncate	:d]: .	Jul 2	5 11:	29:3	7 SSF	тзза	CISE_	Admi	hist	rati	ve_and	l_0per	atio	nal_/	Audit	0000	0002	000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInt
	Syst	log tim	esta	mp (F	FC31	54): :	Jul 2	15 11	:29:37	7											
	Sys	log hos	tnam	e: 55	PT33/	1															
	Sys	log pro	cess	10:	CISE	at od	1. 4	denio	ister	ilue.	and C	Dort	*1.00	-1 4.	di+ 0	20000	0020	1.0	2024	07 75	07 JE 11.70.37 J24 _0E.00 000001303 E1003 NOTTLE Administrator Lamin, Administrator Lamad off ConfigurationId-20E. Administratorian-CUI Adm
	Sys	tog-mes	sage	10	run	ared.	, <u> </u>	ium1h	istra	nve_	and_u	pera	rc ron	a C_Au	arc ø		0020	1.0	2024-	67-25	€/≈23 11:23:37:234 ≈63.60 0000012691 51002 NOTICE Administrator=Login: Administrator Logged off, ConfigVersionia=265, Administrate=501, Adm

Syslog-verkeer

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.