# Configuración del servidor Syslog externo en ISE

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configuración
Configuración del destino de registro remoto (UDP Syslog)
Ejemplo:
Configuración del Destino Remoto en Categorías de Registro
Descripción de categorías
Verificación y resolución de problemas

## Introducción

Este documento describe cómo configurar el servidor Syslog externo en ISE.

### Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE).
- Servidores Syslog

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine (ISE) versión 3.3.
- Servidor Kiwi Syslog v1.2.1.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Antecedentes

Los recopiladores de registros recopilan y almacenan los mensajes de Syslog de ISE. Estos recopiladores de registros se asignan a los nodos de supervisión para que MnT almacene los registros recopilados localmente.

Para recopilar registros externamente, debe configurar servidores syslog externos, que se denominan destinos. Los registros se clasifican en varias categorías predefinidas.

Puede personalizar la salida de registro editando las categorías con respecto a sus destinos, nivel de gravedad, etc.

# Configuración

Puede utilizar la interfaz web para crear destinos de servidor syslog remotos a los que se envían mensajes de registro del sistema. Los mensajes de registro se envían a los destinos del servidor syslog remoto de acuerdo con el estándar del protocolo syslog (consulte RFC-3164).

Configuración del destino de registro remoto (UDP Syslog)



En la GUI de Cisco ISE, haga clic en el icono de menú (

) y seleccione Administración>Sistema>Registro>Destinos de registro remoto > Haga clic en Agregar.



Nota: Este ejemplo de configuración se basa en la captura de pantalla denominada: Configuración del Destino de Registro Remoto.

- Nombre como Remote\_Kiwi\_Syslog, aquí puede introducir el nombre del servidor de Syslog remoto, que se utiliza con fines descriptivos.
- Target Type as UDP Syslog, en este ejemplo de configuración, UDP Syslog se está utilizando; sin embargo, puede configurar más opciones de la lista desplegable Target Type:

UDP Syslog: Se utiliza para enviar mensajes de syslog a través de UDP, adecuado para un registro ligero y rápido.

TCP Syslog: se utiliza para enviar mensajes de syslog a través de TCP, lo que proporciona fiabilidad con funciones de comprobación de errores y retransmisión.

Syslog seguro: hace referencia a los mensajes de syslog que se envían a través de TCP con cifrado TLS, lo que garantiza la integridad y confidencialidad de los datos.

• Status as Enabled, debe elegirEnabled en la lista desplegable Status (Estado).

- Descripción, si lo desea, puede introducir una breve descripción del nuevo destino.
- Host/Dirección IP, donde debe introducir la dirección IP o el nombre de host del servidor de destino que almacena los registros.Cisco ISE admite los formatos IPv4 e IPv6 para el registro.



Nota: Es esencial mencionar que si va a configurar un servidor syslog con FQDN, debe configurar el almacenamiento en caché de DNS para evitar el impacto en el rendimiento. Sin almacenamiento en caché de DNS, ISE consulta al servidor DNS cada vez que debe enviarse un paquete syslog al destino de registro remoto configurado con FQDN. Esto tiene un gran impacto en el rendimiento de ISE.

Utilice service cache enableel comando en todas las PSN de la implementación para superar esto:

**Ejemplo:** 

• **Puerto** como **514**, en este ejemplo de configuración, el servidor Syslog Kiwi escucha en el puerto **514** que es el puerto predeterminado para los mensajes syslog UDP. Sin embargo, los usuarios pueden cambiar este número de puerto a cualquier valor entre 1 y 65535.Asegúrese de que ningún firewall está bloqueando el puerto deseado.

• Facility Code como LOCAL6, puede elegir el código de recurso de syslog que se debe utilizar para el registro, en la lista desplegable. Las opciones válidas son de Local0 a Local7.

• Longitud máxima como 1024, aquí puede ingresar la longitud máxima de los mensajes de destino del registro remoto. La longitud máxima está establecida en 1024 de forma predeterminada en la versión 3.3 de ISE, los valores van de 200 a 1024 bytes.



Nota: Para evitar el envío de mensajes truncados al destino de registro remoto, puede modificar la Longitud máxima como 8192.

• Incluir alarmas para este destino, para que sea sencillo, en este ejemplo de configuración, Incluir alarmas para este destino no está marcado; sin embargo, cuando marca esta casilla de verificación, los mensajes de alarma también se envían al servidor remoto.

• La opción Cumplir con RFC 3164 está marcada, cuando se marca esta casilla de verificación, los delimitadores (, ; { } \) de los mensajes de syslog enviados a los servidores remotos no escapan aunque se utilice una barra diagonal inversa (\).

Una vez finalizada la configuración, haga clic en Save.

Una vez guardado, el sistema mostrará esta advertencia: Ha elegido crear una conexión no segura (TCP/UDP) con el servidor. ¿Está seguro de que desea continuar?, haga clic en Sí.

	dentity Services	Engine					Administration				Q	٩	0	Q	
Щ	Bookmarks	Deployment	Licensing	Certifica	tes Logging	Maintena	nce Upgrade	Health Check	s Backup & Restore	Admin Access	Settings				
==	Dashboard	Log Settings Remote Logging	Targets			it > Remote_Kiwi_									
*	Context Visibility Operations	Logging Categor Message Catalog	ries g	Log	ging Target										
0	Policy	Collection Filters		* I De	lame	Remo	e Logging Target	Target Type Status	UDP SysLog						
<u>م</u>	Administration Work Centers			•	lost / IP Address	10.									
				•	Port	514		(Valid Range	1 to 65535)						
?	Interactive Help			Fa	cility Code	LOC	AL6	→ ()/elid Dange	200 to 8102)						
				In	clude Alarms For thi	s Target			200 (0 8192)						
				Co	mply to RFC 3164	0									
												Save			

Configuración del destino remoto

#### Configuración del Destino Remoto en Categorías de Registro

Cisco ISE envía eventos auditables al destino de syslog. Una vez configurado el destino de registro remoto, deberá asignar el **destino de registro remoto** a las categorías deseadas para reenviar los eventos auditables.

Los destinos de registro se pueden asignar a cada una de estas categorías de registro. Los registros de eventos de estas categorías de registro se generan sólo a partir de nodos PSN y se pueden configurar para enviar los registros relevantes al servidor Syslog remoto, en función de los servicios que estén habilitados en esos nodos:

#### Auditoría AAA

•

.

#### Diagnóstico de AAA

.

#### Contabilidad

•

#### MDM externa

.

#### ID pasiva

•

#### Auditoría de aprovisionamiento de clientes y estado

.

#### Diagnósticos de aprovisionamiento de clientes y estado

•

#### Profiler

•

٠

Los registros de eventos de estas categorías de registro se generan a partir de todos los nodos de la implementación y se pueden configurar para enviar los registros relevantes al servidor Syslog remoto:

#### Auditoría administrativa y operativa

Estadísticas del sistema

En este ejemplo de configuración, va a configurar el destino remoto en cuatro categorías de registro, estas 3 para enviar registros de tráfico de autenticación: Autenticaciones pasadas, Intentos fallidos y Contabilización de radio y esta categoría para el tráfico de registro del administrador de ISE:



Nota: Este ejemplo de configuración se basa en la captura de pantalla denominada: Configuración del Destino de Registro Remoto



En la GUI de Cisco ISE, haga clic en el icono de menú (

•

) y seleccione Administration>System>Logging>Logging Categories, y haga clic en la categoría requerida (Autenticaciones pasadas, Intentos fallidos y Contabilización RADIUS).

Paso 1-Nivel de gravedad del registro:Un mensaje de evento se asocia a un nivel de gravedad, que permite a un administrador filtrar los mensajes y asignarle prioridad. Seleccione el nivel de gravedad del registro según sea necesario. Para algunas categorías de registro, este valor se establece de forma predeterminada y no se puede editar. Para algunas categorías de registro, puede elegir uno de estos niveles de gravedad en una lista desplegable:

**MORTAL**: Nivel de emergencia. Este nivel significa que no puede utilizar Cisco ISE y que debe tomar inmediatamente las medidas necesarias.

ERROR: este nivel indica una condición de error crítico.

**ADVERTENCIA**: Este nivel indica una condición normal pero significativa. Este es el nivel predeterminado establecido para muchas categorías de registro.

INFO: Este nivel indica un mensaje informativo.

Paso 2: **Registro Local: Esta casilla de verificación habilita la generación de registro local.** Esto significa que los registros generados por los PSN también se guardan en el PSN específico que genera el registro. Se recomienda mantener la configuración predeterminada

**Paso 3: Destinos:** Esta área permite elegir los destinos de una categoría de registro mediante la transferencia de los destinos entre las áreasDisponible y Seleccionadasmediante los iconos de flecha hacia la izquierda y hacia la derecha.

El área Disponible contiene los destinos de registro existentes, tanto locales (predefinidos) como externos (definidos por el usuario).

El área Seleccionado, que inicialmente está vacía, muestra los destinos que se han seleccionado para la categoría.

Paso 4- Repita del paso 1 al paso 3 para agregar el destino remoto en las categorías Intentos fallidos y Contabilización de radio.

	dentity Services	Engine					QQ					
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
19	Dashboard Context Visibility	Log Settings Remote Logging	Targets	Logging Cate	gories List >	Passed Authentications						
×	Operations	Logging Categor Message Catalo	ries 9	Name								
0	Policy	Collection Filters	s	Log Severi	ty Level	INFO						
20	Administration					Log level can not be cha	inged. )					
កា	Work Centers			Local Logo	ging A		Sa	lected				
?	Interactive Help			( largets		vanabie:	> < < <	logCollector ProfilerRadiusProbe Remote_Kiwi_Syslog				
											s	ave

Asignación de destinos remotos a las categorías deseadas

Paso 5- Compruebe que el destino remoto se encuentra en las categorías requeridas.Debe poder ver el destino remoto que acaba de agregar.

En esta captura de pantalla, puede ver el destino remoto Remote\_Kiwi\_Syslog asignado a las categorías requeridas.

	alialia Identity Services E	es Engine Administration / System													
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & R	estore A	dmin Access	Settings			
	Dashboard	Log Settings													
	Context Visibility	Remote Logging	Targets	Logo	ing Cat	egories									
<b>a</b> 2	Operations	Logging Categor	ies												
2	<b>B</b> _11	Collection Filters	9 1												
	Policy				Parent Catego	ry	Ca	itegory	Target	ts			Severity	Local Log	
20	Administration			0	AAA Audit				LogCi	ollector			INFO	enable	
ก็เ	Work Centers			0					LogCi	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable	
				0					LogCi	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable	
	Interactive Help			0	AAA Diagnosti	cs			LogC	ollector			WARN	enable	
				0	O Administrator Authentication and Auth								WARN	enable	
				0									WARN	enable	
				0									WARN	enable	
				0									WARN	enable	
				0					LogCi	ollector			WARN	enable	
			O Guest LogCollector							INFO	enable				
				O MyDevices LogCollector								INFO	enable		
				0					LogCi	ollector			INFO	enable	
				0					LogCi	ollector			WARN	enable	
				0	ACI Binding				LogC	ollector			INFO	enable	
				0	Accounting					ollector			INFO	enable	
				0					LogCi	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable	
				0					LogC	ollector			INFO	enable	
				( 0	Administrative	and Operational Audit			LogCe	ollector,Remote	e_Kiwi_Syslog		INFO	enable	
				0	External MDM				LogC	ollector			INFO	enable	
				0	PassiveID				LogC	ollector			INFO	enable	
				0	Posture and CI	ient Provisioning Audit			Audit Profile	erRadiusProbe,	LogCollector		INFO	enable	
				0	Posture and Cl	ient Provisioning Diagr	nostics Po		Diagno LogCi	ollector			WARN	enable	
					Profiler				LogCi	ollector			INFO	enable	
				0	System Diagno	stics			LogC	ollector			WARN	enable	
				0									WARN	enable	
				0									WARN	enable	
				0					LogC	ollector			INFO	enable	
									LogC	ollector			INFO	enable	
				0	System Statisti	ics			LogCi	ollector			INFO	enable	

Verificación de categorías

#### Descripción de categorías

Se genera un mensaje cuando se produce un evento. Existen diferentes tipos de mensajes de eventos generados a partir de varios recursos, como el núcleo, el correo, el nivel de usuario, etc.

Estos errores se categorizan dentro del Catálogo de mensajes y estos eventos también se organizan jerárquicamente en categorías.

Estas categorías tienen categorías principales que contienen una o algunas categorías.

Categoría principal	Categoría
Auditoría AAA	Auditoría AAA Intentos fallidos Autenticación superada
Diagnóstico de AAA	Diagnóstico de AAA Autenticación y autorización del administrador

	Diagnóstico de flujo de autenticación Diagnóstico del almacén de identidades Diagnóstico de políticas Diagnóstico de Radius Guest
Contabilidad	Contabilidad Contabilización RADIUS
Auditoría administrativa y operativa	Auditoría administrativa y operativa
Auditoría de aprovisionamiento de clientes y estado	Auditoría de aprovisionamiento de clientes y estado
Diagnósticos de aprovisionamiento de clientes y estado	Diagnósticos de aprovisionamiento de clientes y estado
Profiler	Profiler
Diagnóstico del sistema	Diagnóstico del sistema Administración distribuida Diagnóstico de operaciones internas
Estadísticas del sistema	Estadísticas del sistema

En esta captura de pantalla puede ver que **Guest** es una clase de mensaje y está categorizada como **Guest Category**. Esta categoría de invitado tiene una categoría principal denominada **Diagnósticos AAA**.

=	dentity Services	Engine			(Administration / System)										
Į	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
53	Dashboard	Log Settings													
1 <sup>1</sup> 6	Context Visibility	Remote Logging	Targets	Mess	sage Ca	atalog									
- 95	Operations	Message Catalog	•												
0	Policy	Collection Filters													
(2)	Administration			Category	y Name			Message Class	Message Code	Message Tex			Message Description	Severity	
				anal											
-11	Work Centers			Guest				Guest	86001	Guest user ha	s entered the guest portal login page		Guest user has entered the guest portal login page	INFO	
				Guest				Guest	86002	Sponso Gues	t user has entered the guest portal login page		Sponsor has suspended a guest user account	INFO	
?	Interactive Help			Guest	Guest Guest			Guest	86003	Sponsor has	mabled a guest user account		Sponsor has enabled a guest user account	INFO	
				Guest				Guest	86004	Guest user ha	s changed the password		Guest user has changed the password	INFO	
				Guest				Guest	86005	Guest user ha	s accepted the Use Policy		Guest user has accepted the use policy	INFO	
				Guest				Guest	86006	Guest user ac	count is created		Guest user account is created	INFO	
				Guest				Guest	86007	86007 Guest user account is updated			Guest user account is updated	INFO	
				Guest				Guest	86008	Guest user ac	count 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 au	thentication 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 fou	nd	Portal is not found in the database. Please contact your system administrator	INFO		
				Guest				Guest	86014	User is suspe	nded		User authentication failed. User account is suspended	INFO	
				Guest				Guest	86015	Invalid Passw	ord Change		Invalid password change. Use correct password based on the password policy	INFO	
Ε.				0				0	00010				The second data and the second of the thread of the second of the second s	INFO	

Catálogo de mensajes

#### Verificación y resolución de problemas

Realizar un volcado TCP contra el destino de registro remoto es el paso más rápido de solución de problemas y verificación para confirmar si se están enviando o no eventos de registro.

La captura se debe realizar desde el PSN que autentica al usuario porque PSN va a generar mensajes de registro y estos mensajes se van a enviar al destino remoto



En la GUI de Cisco ISE, haga clic en el icono Menú (

) y seleccione Operaciones> Solucionar problemas> Volcado TCP> Haga clic en Agregar.

• Debe filtrar el tráfico, agregar el campo de filtro de host IP <remote\_target\_IP\_address>.

• Debe tomar la captura de las autenticaciones de gestión de PSN.

	ahale Identity Services E	Engine			Operations / Troubleshoot	
Щ	Bookmarks	Diagnostic Tools Download Lo	ogs Debug Wizard			
5	Dashboard	General Tools 🗸	TCP 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	vork interface and troubleshoot problems on the network as they appear.		
<b>å</b> 0	Administration	Agentiess Posture Troublesho	SSPT33A ~			
ส์เ	Work Centers	TCP Dump	Network Interface*			
?	Interactive Help	Session irace lests	Gigabitethernet o [Op, kunning] V			
		TrustSec Tools >	Filter ip host 10.20			
			E.g: ip host 10.77.122.123 and not 10.177.122.119			
			File Name Remote Syslog Server Test			
			× (			
			File Size			
			10 (C			
			Limit to			
			File(s)			
			Time Limit 5			
			Minute(s)			
						Save Save and Run

Volcado de TCP

En esta captura de pantalla, puede ver cómo ISE envía mensajes de Syslog para el tráfico de registro del administrador de ISE.

																								<b>d</b> 9997	133A	Gigal	hitEth	arnat P	5 nca	n															
	_				_	_		_		Ι,		<u> </u>	_ 6	_										_ 0011	1004	_orgu	DILLUI	ionnet t	o.pea	ч <b>Р</b>															
	4	🛯 💿			🗙		1 '	৾৻৾৾৻	÷ •	۽	<b>2</b>	<u></u>	些 .	-		_⊕ <b>_</b>	୍କ୍	୍	• •																										
Apply	a disp	olay filter																																											
No.	1	ime					Sourc	e			D	estina	tion		(F	rotoco	al 🔪	Leng	th	Info																									
E.	1 2	2024-07-	-25 1	0:29:	37.235	6441	10.2	01.23	1.67		10	0.201	.231.5	90	5	Syslog	,		385	5 LOCA	6.NOTIC	CE: Jul	l 25	11:29	:37 9	SSPT3	33A CI	ISE_Ad	dmini:	strat:	ive_an	d_0per	ationa	l_Audi	t 000	000020	010	2024-0	7-25	11:29:	37.234	-05:	00 00	20001	2891
	2 2	2024-07-	-25 1	0:29:	19.056	594	10.20	01.23	1.67		10	0.201	.231.9	90	5	Syslog	9		423	B LOCA	6.NOTIC	CE: Jul	ι 25	11:29	1:49 9	SSPT3	33A CI	ISE_Ad	dmini	strat:	ive_an	d_0per	ationa	l_Audi	t 000	800002	110	2024-0	7–25	11:29:	49.056	-05:	00 00	80001	2892
	3 2	2024-07-	-25 1	0:30:	0.559	293	10.2	01.23	1.67		10	0.201	.231.9	90	1	iyslog	9		385	5 LOCA	6.NOTIC	CE: Jul	l 25	11:30	:00 \$	SSPT3	33A CI	ISE_Ad	dmini	strat	ive_an	d_0per	tiona	l_Audi	t 000	900002	210	2024-0	7–25	11:30:	00.558	-05:	00 00	20001	2893
	4 4	2024-07-	-25 1	0:31:	2.796	6473	10.20	01.23	1.67		10	0.201	.231.9	90		yslog	2		423	3 LOCA	6.NOTIC	CE: Jul	ι 25	11:31	:12 9	SSPT3	33A CI	ISE_Ad	dmini:	strat:	ive_an	d_0per	tiona	L_Audi	t 000	9000023	310	2024-0	7-25	11:31:	12.796	-05:	00 00	80001	2895
	5 2	2024-07-	-25 1	0:32:	91.217	780	10.20	01.23	1.90		10	0.201	.231.9	95		ROWSE	ER		243	3 Host	Annound	cement	DESP	KTOP-J	IECKU0	CC, W	orkst	tation	n, Sei	rver,	SQLS	erver,	NT Wo	rkstat	10n										
		2024-07-	-25 1	0:32:	. 38:	530	10.20	01.23	1.67		10	0.201	.231.9	90		yslog	2		520	0 LUCA	6.NUTIC	CE: Jul	1 25	11:32	. 10 5	SSP13	SA CI	ISE_Ad	3m1n1:	strat	ive_an	d_Oper	itiona	L_AUG1	T 000	000024	410	2024-0	7-25	11:32:	10.382	-05:	00 00	80001	2896
		024-07-	-25 1	0:32:	0.383	1760	10.2	01.23	1.67		1	a 201	231.9	10		yslog	2		519	S LOCAL	6 NOTIC	CE: JUL	1 25	11:32	. 10 3	CCDTO		ISE_AO	dmini:	strat	ive_an	d_Oper	tiona	L_AUG1	+ 000	000002:	610	2024-0	7-25	11:32:	10.383	-05:	00 00	20001	2897
		024-07-	-25 1	a.32.	0.383	1807	10.2	a1 23	1.67		1	3 201	231	0 00		velo			516	5 LOCA	6 NOTIC	CE: 300	1 25	11.32	. 10 0	SSPT3	34 (1	TSE Ad	imini:	strat.	ive an	d Oper	tiona	L Audi	+ 000	000002	710	2024-0	7-25	11.32.	10.383	-05.	00 00	20001	2890
	10	024-07-	-25 1	0:32:	0.383	878	10.2	01.23	1.67		1	0.201	.231.9	90		vslo			528	B LOCA	6.NOTIC	CE: Jul	1 25	11:32	10 9	SSPT3	33A CI	ISE_Ad	imini	strat:	ive an	d Oper	tiona	l Audi	t 000	0000021	810	2024-0	7-25	11:32:	10.383	-05:	00 00	20001	2900
	11 2	024-07-	-25 1	0:32:	0.383	945	10.2	01.23	1.67		1	0.201	.231.9	90		vslo	í.		517	7 LOCA	6.NOTIC	CE: Jul	ι 25	11:32	:10 9	SSPT3	33A CI	ISE Ad	dmini	strat:	ive an	d Oper	tiona	l Audi	t 000	00002	910	2024-0	7-25	11:32:	10.383	-05:	00 00	20001	2901
L	12 2	024-07-	-25 1	0:32:		053	10.2	01.23	1.67		1	0.201	.231.9	90	9	syslog	í.		505	5 LOCA	6.NOTIC	CE: Jul	l 25	11:32	:10 9	SSPT3	33A CI	ISE_Ad	dmini	strat	ive_an	d_0per	tiona	L_Audi	t 000	00003	010	2024-0	7-25	11:32:	10.383	-05:	00 00	20001	2902
										_																																	_		
> Fram	e 1:	385 by	tes d	n wir	(308	30 bi	ts),	385 t	oytes	captu	ired	(3080	bits	)																															
> Ethe	rnet	II, Sre	c: VN	ware_	5:46:	12 (	80:50	9:56:a	5:46:		Dst:	VMwa	re_a5	:e5:86	5 (00	:50:5	6:a5:	e5:86																											
> Inte	rnet	Protoco	ol Ve	rsion		rc: 10	9.201	1.231.	.67, C	st: 1	0.20	1.231	.90																																
> User	Data	agram Pi	rotoc	ol, S	rc Por		2724,	Dst	Port:	514																																			
~ [tr	uncat	ted]Sys	log m	iessag	e: LOC	AL6.	NOTIC	:E: Ju	Jl 25	11:29	:37	SSPT3	3A CI	SE_Adr	ninis	trati	ve_ar	nd_0pe	ratio	onal_Au	dit 000	0000002	0 1	0 2024	4-07-	-25 1	1:29:	37.234	4 -05	5:00 0	000001	2891 51	002 N	DTICE .	Admini	strato	or-Log	in: Adı	minist	trator	logge	d off	, Con	figVe	ersio
16	011 O	= F	acil	ity: L	OCAL6	- re	serv	ed fo	r loc	al us	e (22	.)																																	
		101 = L	.evel	: NOTI	CE -	norma	lbu	t sig	nific	ant c	ondit	ion	(5)																																l
∨ Me	essag	e [trun	icate	d]: Ju	l 25	11:29	:37	SSPT3	BA CI	SE_Ad	minis	trat	ive_an	id_0pe	ratio	onal_/	Audit	0000	00026	010	024-07-	-25 11:	:29:3	37.234	1 -05	:00 0	999993	12891	5100	2 NOT	FICE AG	iminist	rator-	Login:	Admi	nistra	tor lo	igged a	111, C	ionfig\	/ersio	sz=bIr	35, AG	dminI	nterf
	Sys	log tim	estar	10 (KP	L3104.	): Ju	L 25	11:23	9:37																																				
	Sys		coss	:: 33P	TCE																																								
	Svs	log mes	sage	id [t	runcat	tedl:	Ada	ninist	trativ	ve and	1 One	ratio	nal A	udit (		00020	1 0	2024-	07-25	5 11:29	37.234	1 -05:0	10 00	00012	891 5	51002	NOTT	CE Ad	iminis	strate	or-loa	in: Adr	inist	rator	logger	off.	Confi	oVersi	on T d=	285. A	dminTn	terfa	ce=GII	IT. Δ	dminT
	593	cog mea	sage	10-10	ancu			20123	chart a	e_une	Tobe			and a c		00020		2024	01-23		10112.04			100012		1002		nere- Au		seruce	o. Log	All Au	2		togget		CONT 2	J.C. 31		2004	din 211 A 11		00-00		
_																																													

Tráfico de Syslog

### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).