Il servizio del database Cisco Firepower User Agent non si riavvia dopo un arresto

Sommario

Introduzione Sintomi Soluzione Riferimenti

Introduzione

Un agente utente Cisco può monitorare il server Microsoft Active Directory (AD) e segnalare le attività di accesso e disconnessione autenticate da un server LDAP. Un centro di gestione Firepower (FMC) integra queste attività con gli eventi di sicurezza che raccoglie da un dispositivo gestito Firepower. Questo documento fornisce una soluzione a un problema quando l'agente utente non viene avviato dopo l'arresto del servizio.

Sintomi

È possibile utilizzare la soluzione in questo documento se si notano i seguenti sintomi con il servizio Agente utente:

- Nell'interfaccia Agente utente il servizio viene visualizzato come Non in esecuzione.
- In Console servizi Windows, services.msc, lo stato di Cisco User Agent è vuoto e non è possibile avviare il servizio.
- Nel registro eventi di Windows viene visualizzato un errore simile a "Relazione di trust non riuscita tra il dominio primario e il dominio trusted"
- Un file UserEncryptionBytes.bin viene creato in C:\ con dimensioni pari a zero byte.
- La modalità di debug di un client agente utente visualizza i seguenti messaggi di errore nella scheda Log dell'agente utente:

,"debug","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
The trust relationship between the primary domain and the trusted domain failed.."

,"error","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
Specified key is not a valid size for this algorithm.."

,"error","[0002] - Error connecting to 10.85.3.122: System.UnauthorizedAccessException: Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)) Soluzione

Passaggio 1: Eseguire Microsoft Windows Services Console, services.msc. Consente di disabilitare o abilitare un servizio Windows.



Passaggio 2: Fare clic con il pulsante destro del mouse sul servizio Cisco User Agent e selezionare **Stop** (Arresta) per arrestare il servizio.

🔍 Services

File Action View Help

_	×
	~

	2 🗟 🛛 📷 🕨 🔲 II 🕪					
Services (Local)	Services (Local)					
	Cisco Firepower User Agent for	Name	Description	Status	Startup Type	Log ^
	Active Directory	🎑 AppX Deployment Service (Provides inf	Running	Manual	Loc
	Stop the service	🎑 Arellia Agent	Arellia Man	Running	Automatic	Loc
	Restart the service	🍓 Auto Time Zone Updater	Automatica		Disabled	Loc
		🔍 Background Intelligent Tran	. Transfers fil	Running	Automatic (D	Loc
	Description	🗛 Background Tasks Infrastru	Windows in	Running	Automatic	Loc
	Polls network logon information	🗛 Base Filtering Engine	The Base Fil	Running	Automatic	Loc
	from Active Directory servers and	🗛 BitDefender Threat Scanner	scan		Manual	Loc
	reports user to IP address mappings	BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Loc
	to Firepower Management Centers	Block Level Backup Engine	The WBENG		Manual	Loc
		Bluetooth Handsfree Service	Enables wir		Manual (Trig	Loc
		Bluetooth Support Service	The Bluetoo		Manual (Trig	Loc
		SranchCache	This service		Manual	Net
		Certificate Propagation	Copies user	Running	Manual	Loc
		Cisco AnyConnect Secure	Cisco AnyC	Running	Automatic	Loc
		Cisco Firepower Us Star	t	Running	Automatic	Loc
		Cisco Media Servic	5	Running	Automatic	Loc
		Cisco MSI Manage		Running	Automatic	Loc
		Client License Serv	se		Manual (Trig	Loc
		CNG Key Isolation Resi	ume	Running	Manual (Trig	Loc
		Code42 CrashPlan Rest	tart	Running	Automatic	Loc
		COM+ Event Syste	Tasks >	Running	Automatic	Loc Y
	Estanded (Standard (×				,
	Extended Standard	Refr	esh			
Stop service Cisco Firep	oower User Agent for Active Directory or	n Local Computer Pro	perties			
		Hel	p	11		

Passaggio 3: Passare alla scheda C: unità.

" <u></u>	bare View	Drive Tools	OSDisk (C:)						-	
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare$	> This PC > (DSDisk (C:) >				~	Ō	Search	OSDisk (C:)	
✓	^ Name	^		Date modified	Туре		Size			
Desktop 🛪	99	sgsccmclient		7/19/2016 1:07 PM	File folder					
Documents	, п_	Logs		4/4/2017 8:58 AM	File folder					
	Ora	acle		4/4/2017 8:57 AM	File folder					
Distures d	Per	rfLogs		10/30/2015 3:24 AM	File folder					
Pictures y	Pro	ogram Files		4/4/2017 9:22 AM	File folder					
Desktop	Pro	ogram Files (x86)		4/4/2017 9:20 AM	File folder					
Music	Us	ers		7/18/2016 2:04 PM	File folder					
Temp	- Wi	ndows		4/4/2017 10:04 AM	File folder					
📑 Videos	📑 Cis	coUserAgent		4/4/2017 10:27 AM	SQL Server Compact Edition Database File			212 KB		
TI: DC	🚳 ms	dia80.dll		9/22/2005 8:39 PM	Application extension			874 KB		
	📄 trig	ggerfullhinv		7/18/2016 7:02 PM	Text Document			1 KB		
> 📃 Desktop	📋 Us	erAgentEncryption	Bytes.bin	4/4/2017 10:16 AM	BIN File			1 KB		
> 🔮 Documents										
> 👆 Downloads										
> 🁌 Music										
> 📰 Pictures										
> 📑 Videos										
> 🏪 OSDisk (C:)										
> 🛖 Shared Folders	c									
> A Network 12 items	~									

Passaggio 4: Eliminare il file UserAgentEncryptionBytes.bin.

File	Home	Share	View						~ 🤇
← →	· ↑ 🛓	> This	PC > OS	Disk (C:) >		~	ē	Search OSDisk (C:)	Q
* C	uick access	^	Name	^	Date modified	Туре	Size		
	Desktop	*	ggsgs	sccmclient	7/19/2016 1:07 PM	File folder			
A	Documents		IT_Lo	gs	4/4/2017 8:58 AM	File folder			
	Downloads	<u>_</u>	Oracl	e	4/4/2017 8:57 AM	File folder			
	Distures	1	PerfL	ogs	10/30/2015 3:24 AM	File folder			
	Pictures	*	- Progr	am Files	4/4/2017 9:22 AM	File folder			
<u> </u>	Desktop		Progr	am Files (x86)	4/4/2017 9:20 AM	File folder			
J.	Music		Users		7/18/2016 2:04 PM	File folder			
	Temp		Wind	ows	4/4/2017 10:04 AM	File folder			
	Videos		暗 Cisco	UserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File		212 KB	
	his DC		🗟 msdia	a80.dll	9/22/2005 8:39 PM	Application extension		874 KB	
-	nis PC		📄 trigge	erfullhinv	7/18/2016 7:02 PM	Text Document		1 KB	
	Desktop		User/	contEncontionPutor hin	4/4/2017 10:16 AM	BIN File		1 KB	
*	Documents			Open with					
-	Downloads			Scan with Windows Defender					
۵.	Music			💙 Scan for threats					
	Pictures			Sourcefire	>				
	Videos			Restore previous versions					
-	OSDisk (C:)			Send to	>				
Ŧ	Shared Folde	ers (Cut					
1 N	letwork	~		Conv					
12 item	s 1 item s	elected 2	24 bytes						
				Create shortcut			1		
				V Delete					
				🧡 Rename					
				Properties					

Passaggio 5: Eliminare il file CiscoUserAgent, che è un file di database di SQL Server Compact Edition.

> • 🛧 🏪 > This	s PC > OSI	Disk (C:) >				~	ڻ Sea	rch OSDisk (C:)
A Quick access	Name	^	Date me	odified	Туре		Size	
Desktop 🖈	📙 ggsgs	ccmclient	7/19/20	16 1:07 PM	File folder			
	IT_Lo	gs	4/4/201	7 8:58 AM	File folder			
Downloads *	- Oracl	e	4/4/201	7 8:57 AM	File folder			
Dictures	PerfL	ogs	10/30/2	015 3:24 AM	File folder			
Pictures /	- Progr	am Files	4/4/201	7 9:22 AM	File folder			
	Progr	am Files (x86)	4/4/201	7 9:20 AM	File folder			
J Music	Users		7/18/20	16 2:04 PM	File folder			
Temp	- Wind	ows	4/4/201	7 10:04 AM	File folder			_
Videos	Cisco	UserAgent	4/4/201	7 10:28 AM	SQL Server Compact Edition Database File		212	KB
This PC	S .	Scan with Windows Defender		05 8:39 PM	Application extension		874	(B
Dealter	i t	Open with		16 7:02 PM	Text Document		11	(B
		Scan for threats						
Documents		Sourcefire						
Downloads		Bestere per investering						
Music		Restore previous versions						
Pictures		Send to	>					
🚆 Videos		Cut						
Los OSDisk (C:)		Сору						
🛖 Shared Folders (Create shortcut						
	-							

Passaggio 6: Tornare a services.msc. Fare clic con il pulsante destro del mouse sul servizio Cisco User Agent, selezionare **Proprietà**, quindi selezionare **Log On** tab (Accedi) e configurare un utente come accesso utente AD. Al termine, fare clic su **Apply** (Applica).

Services				—	\times
File Action View H	Help				
File Action View H File Action View H Services (Local) C A D P fr ret to	Help Cisco Firepower User Agent for Active Directory Properties (Local C × General Log On Recovery Dependencies Log on as:	cription litates t /ides su :esses in /ides inf lia Man omatica omatica sfers fil dows in Base Fil	Status Running Running Running Running Running Running	Startup Type Manual (Trig Manual Manual Manual Automatic Disabled Automatic (D Automatic Automatic Manual	Log ^ Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc
	OK Cancel Apply	SVC hos WBENG bles wir Bluetoo service ies user o AnyC s netwo bles Cis bles Cis vides inf	Running Running Running Running Running	Manual (Trig Manual (Trig Manual (Trig Manual (Trig Manual Manual Automatic Automatic Automatic Automatic Manual (Trig	Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc

Passaggio 7: Nel file services.msc fare clic su Start per il servizio Cisco Firepower User Agent per Active Directory.

🔍 Services					- 🗆	×
File Action View	Help					
🗢 🔿 🗔 🖂 🧇) 📑 🛛 📷 🕨 🔲 II IV					
🥥 Services (Local)	Services (Local)					
	Cisco Firepower User Agent for	Name	Description	Status	Startup Type	Log ^
	Active Directory	Application Information	Facilitates t	Running	Manual (Trig	Loc
	Start the service	Application Layer Gateway	Provides su		Manual	Loc
		Application Management	Processes in	Running	Manual	Loc
	Description.	AppX Deployment Service (Provides inf		Manual	Loc
	Polls network logon information	Arellia Agent	Arellia Man	Running	Automatic	Loc
	from Active Directory servers and	Auto Time Zone Updater	Automatica		Disabled	Loc
	reports user to IP address mappings	Background Intelligent Tran	Transfers fil	Running	Automatic (D	Loc
	to Firepower Management Centers	Background Tasks Infrastru	Windows in	Running	Automatic	Loc
		🎑 Base Filtering Engine	The Base Fil	Running	Automatic	Loc
		🌼 BitDefender Threat Scanner	scan		Manual	Loc
		🎇 BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Loc
		🌼 Block Level Backup Engine	The WBENG		Manual	Loc
		Bluetooth Handsfree Service	Enables wir		Manual (Trig	Loc
		Bluetooth Support Service	The Bluetoo		Manual (Trig	Loc
		SranchCache	This service		Manual	Net
		🖏 Certificate Propagation	Copies user	Running	Manual	Loc
		Cisco AnyConnect Secure	Cisco AnyC	Running	Automatic	Loc
		Cisco Firepower User Agent	Polls netwo		Automatic	Loc
		Cisco Media Services Interfa	Enables Cis	Running	Automatic	Loc
		Cisco MSI Management Ser	Enables Cis	Running	Automatic	Loc
		Client License Service (ClipS	Provides inf		Manual (Trig	Loc 🗸
		<				>
	Extended Standard					

Passaggio 8: Verificare le dimensioni del file UserAgentEncryptionBytes.bin. Non deve essere 0 KB.

→ * 个 当 > Thi	is PC → OSDisk (C:)			✓ ひ Search OSDisk (C:)	
Quick access	Name	Date modified	Туре	Size	
Desktop 🖈	ggsgsccmclient	7/19/2016 1:07 PM	File folder		
Documents 🖈	IT_Logs	4/4/2017 8:58 AM	File folder		
L Downloads 🖈	Oracle	4/4/2017 8:57 AM	File folder		
Dictures *		10/30/2015 3:24 AM	File folder		
Pictures y		4/4/2017 9:22 AM	File folder		
Desktop	Program Files (x86)	4/4/2017 9:20 AM	File folder		
Music	Users	7/18/2016 2:04 PM	File folder		
Temp	Windows	4/4/2017 10:04 AM	File folder		
Videos	CiscoUserAgent	4/4/2017 10:36 AM	SQL Server Compact Edition Database File	212 KB	
This PC	Simular msdia80.dll	9/22/2005 8:39 PM	Application extension	874 KB	
Delter	itriggerfullhinv	7/18/2016 7:02 PM	Text Document	1 KB	
Desktop	UserAgentEncryptionBytes.bin	4/4/2017 10:35 AM	BIN File	1 KB	
Documents					
Downloads					
Music					
Pictures					
Videos					
OSDisk (C:)					
Shared Folders (\\\)					

Passaggio 9: Aggiungere i controller di dominio e Firepower Management Center al client agente utente. Accertarsi di aggiungere i controller di dominio/l'host locale prima di aggiungere Firepower Management Center all'agente utente.

Active Directory Servers						
Host	Polling Status	Last Polled	Real-time Statu	s Last Real-tir	me Report	Real-time
distr.	Active Directory Server (Configur —		1		
Ser	ver Name/IP Address:					
	Domain:	lomain				
Active Directory Server Po	Authorized User:					
Active Directory Server Mi	Password:				Add	Remove
L	ocal Login IP Address:	<select></select>	~			
		Process real-time eve	ents			

Riferimenti

- Guida alla configurazione di Firepower User Agent, 2.3
- L'Agente Utente interrompe la derivazione se non è in grado di convertire l'account del servizio in SecurityIdentifier (CSCuw20184)
- <u>Concedere autorizzazioni minime a un account utente di Active Directory utilizzato dall'agente utente Sourcefire</u>