Le service de base de données de l'agent utilisateur Cisco Firepower ne redémarre pas après un arrêt

Contenu

Introduction Symptômes Solution Références

Introduction

Un agent utilisateur Cisco peut surveiller le serveur Microsoft Active Directory (AD) et signaler les activités de connexion et de déconnexion authentifiées par un serveur LDAP. Un Centre de gestion Firepower (FMC) intègre ces activités aux événements de sécurité qu'il collecte à partir d'un périphérique géré Firepower. Ce document fournit une solution à un problème lorsque l'Agent utilisateur ne démarre pas après avoir arrêté son service.

Symptômes

Vous pouvez utiliser la solution de ce document si vous remarquez les symptômes suivants avec votre service Agent utilisateur :

- L'interface Agent utilisateur affiche le service comme Non en cours d'exécution.
- La console de service Windows, services.msc, affiche l'état de Cisco User Agent comme vide et ne démarre pas le service.
- Le journal des événements Windows affiche une erreur similaire à « Échec de la relation d'approbation entre le domaine principal et le domaine approuvé »
- Un fichier UserEncryptionBytes.bin est créé à l'adresse C:\ avec une taille zéro octet.
- Le mode de débogage d'un client Agent utilisateur affiche les messages d'erreur suivants dans l'onglet Journal de l'Agent utilisateur :

,"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)) Solution

Étape 1 : Exécutez Microsoft Windows Services Console, services.msc. Il vous permet de désactiver ou d'activer un service Windows.



Étape 2 : Cliquez avec le bouton droit sur le service Cisco User Agent et sélectionnez Arrêter pour arrêter le service.

🔍 Services

File Action View Help

_	×
	<i>'</i> `

♦ ♦ 1) 📑 🛛 📷 📄 🔲 🖬 🕩					
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
		🍓 BranchCache	This service		Manual	Net
		🍓 Certificate Propagation	Copies user	Running	Manual	Loc
		🍓 Cisco AnyConnect Secure	Cisco AnyC	Running	Automatic	Loc
		Cisco Firepower Us	rt	Running	Automatic	Loc
		Cisco Media Servic	n	Running	Automatic	Loc
		Cisco MSI Manage	۲	Running	Automatic	Loc
		Client License Serv	Ise		Manual (Trig	Loc
		CNG Key Isolation Res	ume	Running	Manual (Trig	Loc
		Code42 CrashPlan Res	tart	Running	Automatic	Loc
		COM+ Event Syste	Tasks >	Running	Automatic	Loc Y
		<	103103			>
	Extended Standard	Ref	resh			
Stop service Cisco Firep	oower User Agent for Active Directory or	n Local Computer	operties			
		He	p	1		

Étape 3 : Accédez à C : lecteur.

🏪 🛃 File	Home Share	e View Manage OSDisk (C:)					-	- 0
$\leftarrow \rightarrow$	~ 个 👆 > Ti	his PC > OSDisk (C:) >			~	Q	Search OSDisk (C	:)
🗸 🏄 Q	uick access	Name	Date modified	Туре		Size		
. (Desktop 🖈	ggsgsccmclient	7/19/2016 1:07 PM	File folder				
a	Documents 🖈	IT_Logs	4/4/2017 8:58 AM	File folder				
_ I	Downloads 🖈	Oracle	4/4/2017 8:57 AM	File folder				
	Distures a		10/30/2015 3:24 AM	File folder				
		Program Files	4/4/2017 9:22 AM	File folder				
<u> </u>	Desktop		4/4/2017 9:20 AM	File folder				
1	Music	Users	7/18/2016 2:04 PM	File folder				
	Temp	Windows	4/4/2017 10:04 AM	File folder				
E 1	Videos	🗎 CiscoUserAgent	4/4/2017 10:27 AM	SQL Server Compact Edition Database File			212 KB	
м 🗖 ТИ	his DC	🕙 msdia80.dll	9/22/2005 8:39 PM	Application extension			874 KB	
	nis PC	triggerfullhinv	7/18/2016 7:02 PM	Text Document			1 KB	
	Desktop	UserAgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File			1 KB	
> 🟥 [Documents							
> 🕂 เ	Downloads							
- > 🎝 I	Music							
> 📰	Pictures							
> 📑 ۱	Videos							
> = (OSDisk (C:)							
> = 9	Shared Folders (
> 💣 No 12 items	etwork 🗸							



File Home S	hare	View							~ (
← → ~ ↑ ^L	> This	PC > OS	Disk (C:) >			~	Q	Search OSDisk (C:)	,
📌 Quick access	^	Name	^	Date modified	Туре		Size		
Desktop 💉		📙 ggsgs	sccmclient	7/19/2016 1:07 PM	File folder				
Documents		IT_Lo	gs	4/4/2017 8:58 AM	File folder				
L Downloads		Oracl	le	4/4/2017 8:57 AM	File folder				
Dictures d		PerfL	ogs	10/30/2015 3:24 AM	File folder				
Pictures y		- Progr	ram Files	4/4/2017 9:22 AM	File folder				
Desktop		- Progr	ram Files (x86)	4/4/2017 9:20 AM	File folder				
J Music		Users	:	7/18/2016 2:04 PM	File folder				
Temp		Wind	lows	4/4/2017 10:04 AM	File folder				
🚪 Videos		💾 Cisco	bUserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File			212 KB	
This DC		🗟 msdia	a80.dll	9/22/2005 8:39 PM	Application extension			874 KB	
inis PC		📄 trigge	erfullhinv	7/18/2016 7:02 PM	Text Document			1 KB	
Desktop		User/	AgentEncountionPuter him	4/4/2017 10:16 AM	BIN File			1 KB	
Documents			Open with						
👆 Downloads			Scan with Windows Defender						
b Music			Scan for threats						
Pictures			Sourcefire	>					
📕 Videos			Restore previous versions						
🏪 OSDisk (C:)			Send to	>					
n Shared Folders	C		Cut						
💣 Network	~		Сору						
12 items 1 item sele	cted 2	24 bytes	Contratant						
			Create snortcut		A A A A A A A A A A A A A A A A A A A	alter and			
			Uerete						
			V Rename						
			Properties						

Étape 5 : Supprimez le fichier CiscoUserAgent, qui est un fichier de base de données SQL Server Compact Edition.

\leftarrow \rightarrow \checkmark \uparrow 🏪 \Rightarrow This	PC > OSI	Disk (C:) >			✓ Č Sea	rch OSDisk (C:)
A Quick access	Name	^	Date modified	Туре	Size	
Desktop 🖈	📙 ggsgs	sccmclient	7/19/2016 1:07 PM	File folder		
	IT_Lo	gs	4/4/2017 8:58 AM	File folder		
	- Oracl	e	4/4/2017 8:57 AM	File folder		
Distures	PerfL	ogs	10/30/2015 3:24 AM	File folder		
	📙 Progr	am Files	4/4/2017 9:22 AM	File folder		
Desktop	- Progr	am Files (x86)	4/4/2017 9:20 AM	File folder		
Music	Users		7/18/2016 2:04 PM	File folder		
- Temp	- Wind	ows	4/4/2017 10:04 AM	File folder		_
Videos	Cisco	UserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File	212 k	(B
This DC	S 1	Scan with Windows Defender	05 8:39 PM	Application extension	874 k	(B
	t	Open with	16 7:02 PM	Text Document	1 k	(B
	U	Scan for threats				
Documents		Coursefine				
🕂 Downloads	-	Destance and investmentions				
Music	_	Restore previous versions				
Pictures		Send to	>			
🚆 Videos		Cut				
Los OSDisk (C:)		Сору				
🛖 Shared Folders (Create shortcut				
A Network		Delete				
11 items 1 item colocted '	212 KB	Rename				

Étape 6 : Revenir à services.msc. Cliquez avec le bouton droit de la souris sur le service Cisco User Agent, sélectionnez **Propriétés**, puis **Ouvrir une session**, puis configurez un utilisateur en tant que connexion utilisateur AD. Cliquez sur **Apply** lorsque vous avez terminé.

Services					- 🗆	\times
File Action View	Help					
File Action View I File Action View I Services (Local) C A S R D P fr r t	Help Cisco Firepower User Agen General Log On Recover Log on as: O Local System account Allow service to inter O This account: Password: Confim password:	It for Active Directory Properties (Loca ny Dependencies Fract with desktop est Brows	e X cription litates t vides su. cesses in vides inf. lia Man. omatica. usfers fil. dows in Base Fil.	Status Running Running Running Running Running Running Running	Startup Type Manual (Trig Manual Manual Manual Automatic Disabled Automatic (D Automatic Automatic	Log ^ Loc Loc Loc Loc Loc Loc Loc Loc Loc
	Extended / Standard /	OK Cancel	Apply A A A A A A A A A A A A A A A A A A A	Running Running Running Running Running Running	Manual Manual (Trig Manual (Trig Manual (Trig Manual Manual Automatic Automatic Automatic Automatic Manual (Trig	Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc

Étape 7 : Sur services.msc, cliquez sur Démarrer pour le service Cisco Firepower User Agent pour Active Directory.

🍳 Services					- 🗆	×
File Action View	Help					
) 📑 🛛 📷 🕨 🔲 II ID					
🔍 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
	<u>Sur</u> the service	Application Management	Processes in	Running	Manual	Loc
		AppX Deployment Service (Provides inf		Manual	Loc
	Description:	🔍 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
		Q Client License Service (ClipS	Provides inf	-	Manual (Trig	Loc 🗸
		<				>
	Extended Standard					

Étape 8 : Vérifiez la taille du fichier UserAgentEncryptionBytes.bin. Elle ne doit pas être de 0 Ko.

→ * ↑	is PC → OSDisk (C:)			ڻ ~	Search OSDisk (C:)	
Quick access	Name	Date modified	Туре	Size		
Desktop 🖈		7/19/2016 1:07 PM	File folder			
Documents 🖈	IT_Logs	4/4/2017 8:58 AM	File folder			
Downloads 🖈	Oracle	4/4/2017 8:57 AM	File folder			
Distures		10/30/2015 3:24 AM	File folder			
Pictures 7	Program Files	4/4/2017 9:22 AM	File folder			
Desktop		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	2	12 KB	
71: 00	🚳 msdia80.dll	9/22/2005 8:39 PM	Application extension	8	74 KB	
This PC	Triggerfullhinv	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)						

Étape 9 : Ajoutez les contrôleurs de domaine et Firepower Management Center au client Agent utilisateur. Veillez à ajouter les contrôleurs de domaine/hôte local avant d'ajouter Firepower Management Center à l'agent utilisateur.

Active Directory Servers						
Host	Polling Status	Last Polled	Real-tim	ie Status	Last Real-time Report	Real-time
distri	Active Directory Server	Configur —		X		
	,		_	~		
Se	erver Name/IP Address:					
	Domain:	domain				
Active Directory Server Po	Authorized User:					
Active Directory Server Ma	Password:				Add	Remove
	Local Login IP Address:	<select></select>	~			
	2	Process real-time ev	/ents			

Références

- Guide de configuration de Firepower User Agent, 2.3
- L'agent utilisateur cesse de dériver s'il ne peut pas traduire le compte de service en SecurityIdentifier (CSCuw20184)
- Octroi d'une autorisation minimale à un compte d'utilisateur Active Directory utilisé par l'agent d'utilisateur Sourcefire