Erzwingen Sie die Aktualisierung der TETRA-Definitionen manuell - Cisco Secure Endpoints

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt das Verfahren, um die neuen TETRA-Definitionen in Cisco Secure Endpoints (AMP) manuell zu erzwingen.

Verfasst von Jesus Javier Martinez und Uriel Torres und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Windows-Betriebssystem
- AMP für Endgeräte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Endpoint (AMP) für Windows.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Umgebung erstellt:

- Windows 10-Gerät
- AMP Connector 7.0.5 Version

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 potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Informationen hierzu finden Sie im Benutzerhandbuch. Tetra ist eine vollständige Antivirus-Lösung für Cisco Secure Endpoint Solution. Sie sollte zusammen mit Cisco Secure Endpoint verwendet werden, um den bestmöglichen Schutz zu gewährleisten. Wenn ein Drittanbieter-AV installiert ist, sollten wir den anderen A/V entfernen, um die ordnungsgemäße Installation und den ordnungsgemäßen Betrieb von TETRA sicherzustellen. TETRA kann beim Herunterladen der Definitionen auch beträchtliche Bandbreite beanspruchen.

Vorsicht: Tetra muss vor einer großen Bereitstellung in einer Testumgebung angewendet werden.

Da die AMP-Version 6.3.1 bei Aktivierung der TETRA-Engine und der Aktualisierung der Definitionen deaktiviert werden muss, muss Windows Defender deaktiviert werden. Daher wird Cisco Secure Endpoint als aktiver Antivirus- und Bedrohungsschutz-Anbieter festgelegt.

Die Definitionen werden automatisch heruntergeladen, Sie können jedoch eine manuelle Aktualisierung der TETRA-Definitionen erzwingen.

Fehlerbehebung

Hinweis: Auf Cisco Secure Endpoint Version 7.2.7 und höher können Sie den Connector zwingen, die Aktualisierungen mithilfe des Arguments '-forceupdate' abzurufen.

C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate

Um Definitionsaktualisierungen unter Version 7.2.7 zu erzwingen, können Sie diesem Handbuch folgen.

Schritt 1: Beenden Sie den AMP-Dienst.

• Wenn Sie keinen Kennwortschutz haben

Schritt 1.1: Öffnen Sie Services.msc, wie im Bild gezeigt.



Schritt 1.2: Navigieren Sie zu Services > Cisco AMP für Endpoints Connector 7.0.5 wie im Bild gezeigt.



Schritt 1.3: Beenden Sie den AMP-Dienst, wie im Bild gezeigt.

Windows is attempting to stop the following service on Local Computer Cisco AMP for Endpoints Connector 7.0.5					
Close					

Wenn Sie über Kennwortschutz verfügen

Schritt 1.4: Öffnen Sie die AMP-Benutzeroberfläche, und wählen Sie **Einstellungen** aus, wie im Bild gezeigt.





Cisco AMP for Endpoints

	Scar	n Now
	His	story
	Set	tings
S S P Is	Status: Scanned: Policy: solation:	Connected 12/5/2019 10:37:08 AM Windows10 Not Isolated

cisco

Schritt 1.5: Navigieren Sie zu Cisco AMP für Endgeräte-Einstellungen wie im Bild gezeigt.

General Settings	•
Scan Settings	•
Notification Settings	•
Proxy Settings	•
Cisco AMP Connector Settings	•]
Service Status:	Started
Password:	
Stop Service	
Debug Logging Status:	Stopped
Enable Debug Logging	

Schritt 1.6: Geben Sie das Kennwort ein, und klicken Sie auf **Service beenden**, wie im Bild gezeigt.

General Settings				
Scan Settings	•			
Notification Settings				
Proxy Settings	T			
Cisco AMP Connector Setting	js 🔺			
Service Status:	Stopped			
To start the service please	use the Windows	Service Contr	ol Manager	
Debug Logging Status:	Stopped			
Enable Debug Logging				

Schritt 2: Navigieren Sie zum AMP-Ordner, der sich normalerweise in C:\Program Files\Cisco\AMP befindet, wie im Bild gezeigt.

Schritt 2.1: Löschen Sie alle Inhalte im Ordner C:\Program Files\Cisco\AMP\tetra\Plugins\, wie im Bild gezeigt

File Home	gins Share	View			
← → × ↑ 📙	> This	PC > Local Disk (C:) > Program Fil	es > Cisco > AMP > tetra >	Plugins	
		Name	Date modified	Туре	Size
Cuick access		7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
Desktop	1	File Access Denied	-	0 X	6 K.B
Downloads	*				17 KB
Documents	*	You'll need to provide administr		6 KB	
Pictures	*	7zip.xmd		48 KB	
AMP	*	Type: XMD File	13 KB		
Music	*	Date modified: 11/	2 KB		
Videos					1 KB
		Do this for all current items			10 KB
 OneDrive 		Continue	Skip C	ancel	652 KB
_	_	Contained			12.405.KB

Schritt 2.2: Löschen Sie alle Inhalte im C:\Program Files\Cisco\AMP\update\Plugins\ -Ordner, wie im Bild gezeigt.

🔜 l 🕑 📙 🖬 l Plu	gins				
File Home	Share	View			
← → * ↑ 📒	> This	PC > Local Disk (C:) > Program Files	> Cisco > AMP > update	> Plugins	
		Name	Date modified	Туре	Size
Quick access		7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
Desktop	1	File Access Denied	-	• ×	6 KB
Downloads	~		17 KB		
Documents		You'll need to provide administrato	6 KB		
E Pictures	1	arjamd	48 KB		
AMP	1	Type: XMD File		13 KB	
h Music	*	Date modified: 10/14/	2 KB		
Videos			1 KB		
		Do this for all current items	10 KB		
 OneDrive 		Continue	Skip Cu	ancel	652 KB
	_				13.405.60

schritt 3: Starten Sie den Dienst Cisco AMP für Endgeräte Connector 7.0.5, wie im Bild gezeigt.

Services (Local)

Cisco AMP for Endpoints Connector 7.0.5

Start the service

Description: Cisco AMP for Endpoints Connector 7.0.5

schritt 4: Öffnen Sie die AMP-Benutzeroberfläche, wie im Bild gezeigt.

Schritt 4.1: Klicken Sie auf Einstellungen wie im Bild gezeigt.





Cisco AMP for Endpoints

Scan Now History Settings Status: Connected Scanned: 12/5/2019 10:37:08 AM Policy: Windows10 Isolation: Not Isolated



cisco

Schritt 4.2: Wählen Sie Synchronisierungsrichtlinie wie im Bild gezeigt aus.



schritt 5: Wenn die pópolicy synchronisiert wird, werden die Tetra-Definitionen heruntergeladen.

Hinweis: Sobald die Definitionen heruntergeladen wurden, ist der AMP-Anschluss der Standard-AV, wie im Bild gezeigt.

♡ Virus & threat protection

Protection for your device against threats.

Cisco AMP for Endpoints

Cisco AMP for Endpoints is turned on.

Current threats

No actions needed.

Protection settings

No actions needed.

Protection updates

No actions needed.

Open app

Auch wenn die TETRA-Definitionen automatisch heruntergeladen werden, können Sie manuell eine Definitions-Aktualisierung erzwingen. Das hängt von Ihren Anforderungen ab.

Zugehörige Informationen

- <u>AMP4E Video zu TETRA-Definitionen</u>
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>