Dépannage des terminaux sécurisés isolés grâce aux méthodes de récupération

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Arrêter l'isolation Arrêter la session d'isolation à partir de la console Arrêter la session d'isolation à partir de la ligne de commande Dépannage de récupération Récupération Mac : Récupération Windows : Méthode d'isolation de récupération à partir de la ligne de commande Méthode d'isolation de récupération sans ligne de commande Vérifier Informations connexes

Introduction

Ce document décrit le processus de récupération d'un terminal avec le connecteur Secure Endpoint installé à partir du mode d'isolation.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur de terminal sécurisé
- Console Secure Endpoint
- Fonction Endpoint Isolation

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console Secure Endpoint version 5.4.2021092321
- Connecteur Windows Secure Endpoint version v7.4.5.20701
- Connexion Mac Secure Endpoint version 1.21.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La procédure décrite dans ce document est utile dans les situations où le périphérique d'extrémité est bloqué dans cet état et où il n'est pas possible de désactiver le mode d'isolation.

L'isolation des terminaux est une fonctionnalité qui vous permet de bloquer l'activité réseau (ENTRÉE et SORTIE) sur un ordinateur afin d'empêcher les menaces telles que l'exfiltration des données et la propagation des programmes malveillants. Il est disponible sur :

- Versions 64 bits de Windows prenant en charge la version 7.0.5 et les versions ultérieures du connecteur Windows
- Versions Mac prenant en charge les versions 1.21.0 et ultérieures du connecteur Mac.

Les sessions d'isolation des terminaux n'affectent pas la communication entre le connecteur et le cloud Cisco. Le niveau de protection et de visibilité de vos terminaux est le même qu'avant la session. Vous pouvez configurer l'option IP Isolation Allow Lists of addresses (Autoriser les listes d'adresses d'isolation IP) afin d'éviter que le connecteur ne bloque les adresses IP en question pendant qu'une session d'isolation de point d'extrémité active est active. Vous pouvez consulter des informations plus détaillées sur la fonctionnalité Endpoint Isolation <u>ici</u>.

Arrêter l'isolation

Une fois que vous souhaitez arrêter l'isolation des points de terminaison sur un ordinateur, effectuez ces étapes rapides via la console ou la ligne de commande Secure Endpoint.

Arrêter la session d'isolation à partir de la console

Afin d'arrêter une session d'isolation et de restaurer tout le trafic réseau vers un point d'extrémité.

Étape 1. Dans la console, accédez à **Gestion > Ordinateurs**.

Étape 2. Localisez l'ordinateur sur lequel vous souhaitez mettre fin à l'isolement et cliquez pour afficher les détails.

Étape 3. Cliquez sur le bouton Stop Isolation, comme illustré dans l'image.

DESKTOP-075I5MB in group testing bremarqu								
► Ss Isolated								
Hostname	DESKTOP-075I5MB	Group 😃	testing bremarqu					
Operating System	Windows 10 Pro	Policy	Copy of bremarqu_mssp					
Connector Version	7.4.5.20701	Internal IP						
Install Date	2021-09-28 20:02:16 CDT	External IP	$\overline{}$					
Connector GUID	0101000-000-1700-00-00000000-	Last Seen	2021-09-28 23:39:08 CDT					
Definition Version	TETRA 64 bit (daily version: 85768)	Definitions Last Updated	2021-09-28 21:28:59 CDT					
Update Server	tetra-defs.amp.cisco.com							
Processor ID	0000777044440044							
) Events 🤌 Device Trajectory 😲 Diagnostics 🕚 View Changes								
🐹 Stop Isolation 🔍 Scan 😲 Diagnose 🍱 Move to Group 👕 Delete								

Étape 4. Entrez des commentaires expliquant pourquoi vous avez arrêté la fonction d'isolation sur le point d'extrémité.

Arrêter la session d'isolation à partir de la ligne de commande

Si un terminal isolé perd sa connexion au cloud Cisco et que vous ne parvenez pas à arrêter la session d'isolement à partir de la console. Dans ces situations, vous pouvez arrêter la session localement à partir de la ligne de commande avec le code de déverrouillage.

Étape 1. Dans la console, accédez à **Gestion > Ordinateurs**.

Étape 2. Localisez l'ordinateur sur lequel vous souhaitez mettre fin à l'isolement et cliquez pour afficher les détails.

Étape 3. Notez le code de déverrouillage, comme illustré dans l'image.

	DESKTOP-075I5MB in group testing bremarqu					 Definitions Up To Date 	
,	Stated						
	2021-09-28 21:33:48 CDT		Isolated for less than a min	nute	1	Unlock Code:f	wq8qw
	Isolated	2021-09-28 21:33:48 CDT					
	Isolating	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw			

Étape 4. Vous pouvez également rechercher le **code de déverrouillage** si vous naviguez vers **Compte > Journal d'audit**, comme indiqué dans l'image.

Isolation Started DESKT	DP-07515MB	bremarqu+mmp2@cisc	\sim	2021-09-28 21:33:48 CDT		
▼ Isolation Start Requested □ DESKT	P-075I5MB			2021-09-28 21:33:46 CDT		
Attribute	Old	Old		New		
Comment	None	lone No.				
ID	None		07200270 0000 40			
Unlock Code	None		fwq8qw			

Étape 5. Sur l'ordinateur isolé, ouvrez une invite de commandes avec des privilèges

d'administrateur.

Étape 6. Accédez au répertoire dans lequel le connecteur est installé

Windows : C:\Program Files\Cisco\AMP\[numéro de version]

Mac : /opt/cisco/amp

Étape 7. Exécuter la commande stop

Windows: sfc.exe -n [unlock code]

C:\Program Files\Cisco\AMP\7.4.5.20701>sfc.exe -n fwq8qw C:\Program Files\Cisco\AMP\7.4.5.20701>

Mac: ampcli isolate stop [unlock code]

Attention : si le code de déverrouillage n'est pas saisi correctement 5 fois, il est nécessaire d'attendre 30 minutes avant d'effectuer une nouvelle tentative de déverrouillage.

Dépannage de récupération

Si vous avez épuisé toutes les possibilités et que vous ne parvenez toujours pas à récupérer un point de terminaison isolé à partir de la console Secure Endpoint ou localement avec le code de déverrouillage, vous pouvez récupérer le point de terminaison isolé avec les méthodes de récupération d'urgence.

Récupération Mac :

Supprimez la configuration d'isolation et redémarrez Secure Endpoint Service

sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist

Récupération Windows :

Méthode d'isolation de récupération à partir de la ligne de commande

Dans les situations où votre périphérique d'extrémité est bloqué en isolement et qu'il n'est pas possible de désactiver l'isolement via la console Secure Endpoint ou avec le code de déverrouillage, procédez comme suit.

Étape 1. Arrêtez le service de connecteur via l'interface utilisateur du connecteur ou les **services Windows**.

Étape 2. Localisez le service Secure Endpoint connector et arrêtez-le.

Étape 3. Sur l'ordinateur isolé, ouvrez une invite de commandes avec des privilèges d'administrateur.

Étape 4. Exécutez la commande **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** comme indiqué dans l'image.



Étape 5. Le message **L'opération a réussi** indique que l'opération a été terminée. (Si un autre message s'affiche, comme « Erreur : l'accès est refusé », vous devez arrêter le service du connecteur Secure Endpoint avant d'exécuter la commande.)

Étape 6. Démarrez le service de connecteur Secure Endpoint.

Conseil : si vous ne parvenez pas à arrêter le service de connecteur Secure Endpoint à partir de l'interface utilisateur du connecteur ou des services Windows, vous pouvez effectuer un démarrage sécurisé.

Sur le point de terminaison isolé, accédez à **Configuration système > Boot > Boot options** et sélectionnez **Safe boot**, comme indiqué dans l'image.

System Configuration		
nera Boot Services Startup	Tools	
Vindows 10 (C:\Windows) : Curre	nt OS; Default OS	
Advanced options Set a	as default Delete	
Boot options		Timeout:
Safe boot	No GUI boot	30 seconds
Minimal	Boot log	
 Alternate shell 	Base video	
Active Directory repair	OS boot information	Make all boot settings
O Network		permanent
-		
-		

Méthode d'isolation de récupération sans ligne de commande

Si votre périphérique d'extrémité est bloqué en isolement et qu'il n'est pas possible de désactiver l'isolement via la console Secure Endpoint ou avec le code de déverrouillage, ou même si vous ne pouvez pas utiliser la ligne de commande, procédez comme suit : Étape 1. Arrêtez le service de connecteur via l'interface utilisateur du connecteur ou les **services Windows**.

Étape 2. Accédez au répertoire dans lequel le connecteur est installé (C:\Program Files\Cisco\AMP\) et supprimez le fichier **jobs.db**, comme indiqué dans l'image.

•	Cisc	co > AMP > V	ō	, Search AMP	
		Name		Date modified	Туре
s		contential		0/20/2021 0.01 0.4	File felder
	A	tatra		9/20/2021 0:01 PM	File folder
5	*	tmo		9/28/2021 9:23 PM	File folder
s	\mathcal{A}	update		9/28/2021 9:27 PM	File folder
	\mathcal{A}	URLScanner		9/28/2021 8:01 PM	File folder
		2021-09-28 20-02-11.etl		9/28/2021 9:23 PM	ETL File
		🗟 cache		9/28/2021 9:23 PM	Data Base File
		i event		9/28/2021 9:23 PM	Data Base File
		🖹 filetypes	/	9/28/2021 8:01 PM	XML Document
		istory		9/28/2021 9:23 PM	Data Base File
	-	🗟 historyex 🦯		9/28/2021 9:23 PM	Data Base File
		🗟 jobs		9/28/2021 9:23 PM	Data Base File
		local.old		9/28/2021 9:23 PM	OLD File
		🖹 local		9/28/2021 9:23 PM	XML Document

3. Redémarrez l'ordinateur.

En outre, si l'événement Isolation s'affiche dans la console, vous pouvez accéder à **Error Details** afin de vérifier le code d'erreur et sa description, comme illustré dans l'image.

Failed to stop isolation			💶 🖉 Isolation Stop Failed	2021-12-15 21:27:51 UT
Connector Details	Error Code	3240624137		
Comments	Description	Invalid unlock code		
Error Details	Q Run Scan			

Vérifier

Afin de vérifier que le point de terminaison est de nouveau isolé ou n'est plus isolé, vous pouvez voir l'interface utilisateur du connecteur de point de terminaison sécurisé affiche l'état d'isolation comme **Non isolé**, comme illustré dans l'image.



Àpartir de la console Secure Endpoint, si vous naviguez dans **Management > Computers**, et localisez l'ordinateur en question, vous pouvez cliquer pour afficher les détails. L'état Isolation affiche **Not Isolated**, comme indiqué dans l'image.

🗌 🔻 🗱 DESKTOP-075I5MB in group testing bremarque 🖌 Definitions Up To Date 🕅			🗆 🔻 🛍 DESKTOP-03	75I5MB in group testing bremarqu		✓ Definitions Up To Date (IN	
► Se Isolated				 St Not Isolated 			
Hostname	DESKTOP-075I5MB	Group da	testing bremarqu	Hostname	DESKTOP-075I5MB	Group da	testing bremarqu
Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_mssp	Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_mssp
Connector Version	7.4.5.20701	Internal IP		Connector Version	7.4.5.20701	Internal IP	
Install Date	2021-09-28 20:02:16 CDT	External IP		Install Date	2021-09-28 20:02:16 CDT	External IP	
Connector GUID		Last Seen	2021-09-29 10:37:11 CDT	Connector GUID		Last Seen	2021-09-29 10:39:58 CDT
Definition Version	TETRA 64 bit (daily version: 85769)	Definitions Last Updated	2021-09-28 23:01:58 CDT	Definition Version	TETRA 64 bit (daily version: 85769)	Definitions Last Updated	2021-09-28 23:01:58 CDT
Update Server	tetra-defs.amp.cisco.com			Update Server	tetra-defs.amp.cisco.com		
Processor ID				Processor ID			
4 Events 12 Device Trajectory 13 Diagnostics 3 View Changes			4 Events 12 Device Trajectory 13 Diagnostics (3) View			Device Trajectory 🕲 Diagnostics 💿 View Changes	
🎇 Stop Isolation 🔍 Scan 🕅 Diagnose 📾 Move to Group) 🗃 Delete			Start Isolation Q, Scan V Diagnose & Move to Group			Diagnose 4 Move to Group 🗑 Delete	

Informations connexes

- Guide de l'utilisateur Secure Endpoint
- <u>Technical Support & Documentation Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.