ESA/CES:クラスタ化アプライアンスをエンド ポイント用AMPに登録する手順

内容

<u>概要</u>

<u>問題</u>

<u>解決方法</u>

<u>ステップ1:ログインし、ESA/CESの[AMP]ページに移動します。</u> <u>ステップ2:設定モードを変更します。</u> <u>ステップ3:マシンオーバーライドモードに切り替えます。</u> <u>手順4:マシン設定のエンドポイント用AMPを登録します。</u> <u>ステップ5:クラスタモードに切り替えます。</u> 関連情報

概要

このドキュメントでは、クラスタ化設定環境のCisco Eメールセキュリティアプライアンス (ESA)/クラウドEメールセキュリティ(CES)アプライアンスをエンドポイント用Advanced Malware Protection(AMP)に登録する手順について説明します。

問題

注:このドキュメントは、ESA/CES AsyncOS 11.1で作成されました。ESA/CESのドキュ メントの詳細については、ユーザガイドおよびドキュメントを参照し<u>てください。</u>

[Security Services] > [File Reputation and Analysis]ページのGUIからESA/CESクラスタをエンド ポイント用AMPに登録しようとすると、[*Register Appliance with AMP for Endpoints]ボタンがグ レー表示され、登録を完了できませ*ん。

次の図に示します。

✓ Advanced Settings for File Reputation	File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)	
	AMP for Endpoints Console Integration \textcircled{O}	Register Appliance with AMP for Endpoints	
	SSL Communication for File Reputation:	Use SSL (Port 443)	
		Tunnel Proxy (Optional):	
		Server:	

解決方法

ESA/CESアプライアンスをクラスタ構成でエンドポイント用AMPに登録するには、マシンレベル の上書きでこの処理を行う**必要があります**。これは、クラスタ内の各マシンに対して、個別の上 書き設定が優先されることを意味します。

ステップ1:ログインし、ESA/CESの[AMP]ページに移動します。

[セキュリ**ティサービス] > [ファイルレピュテーションと分析]に移動**し、現在の設定モードを確認 します。これは、指定された出力のMode - Clusterによって示されます。

File Reputation and Analysis

Mode — Cluster: AMPTEST ange Mode • •					
Advanced Malware Protection					
File Reputation:	Enabled				
File Analysis:	Enabled				
	Edit Global Settings				

Click here to group or view appliances for File Analysis reporting.

ステップ2:設定モードを変更します。

[Centralized Management Options] > [Manage Settings]をクリックします。

Mode - Cluster: AMPTEST Change Mode.					
Settings are defined: Delete Settings for this feature at this mode. You can also Manage Settings.					
Advanced Malware Protection					
File Reputation:	Enabled				
File Analysis:	Enabled				

[Manage Settings]で、クラスタ**からログインしたそれぞれの**マシンに構成をコピーします。選択 したら、変更を**送信して確定**します。

Mode — Cluster: AMPTEST Change Mode ▼ Centralized Management Options
Manage Settings for Cluster: AMPTEST
Cluster: AMPTEST Cancel Submit

ステップ3:マシンオーバーライドモードに切り替えます。

[Change Mode...]**ドロップダウンをクリック**し、設定するオーバーライド付きのマシンを選択します。

File Reputation and Analysis

Mode Cluster: AMPTEST	Chappen Mode			
	Change Mode			
Centralized Management Options	* Cluster: AMPTEST (current mode)			
	Group: Main_Group			
Advanced Malware Protection	Machine: ESA.cisco.com			
Machine: esa4.aricent.com				
	File Analysis: Enabled			

手順4:マシン設定のエンドポイント用AMPを登録します。

設定モードをマシンに切り替えた後:<マシン名>。

[グローバル**設定の編集…]をクリックします。**次に、[ファイル解析]**コンポーネントの[詳細設定**]を展開します。

[Register Appliance with AMP for Endpoints]ボタンをクリックして、登録を完了します。

Mode — Machine: esa4.aricent.com Change Mode Centralized Management Options						
Advanced Malware Protection						
Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.						
File Reputation Filtering:	C Enable File Reputation					
File Analysis: ⑦						
	File Reputation Server: AMP for Endpoints Console Integration ⑦	AMERICAS (cloud-sa.amp.cisco.com) Register Appliance with AMP for Endpoints				
	SSL Communication for File Reputation:	Use SSL (Port 443) Tunnel Proxy (Optional):				

クラスタ内の残りのマシンで手順1~4を繰り返し、エンドポイント用AMPに登録します。

警告:不具合IDの影響を受けるESA/CESソフトウェアのバージョン:<u>CSCvp23281</u>は、不 具合の回避策に記載されているように、ステップ5をスキップする必要があります。

ステップ5:クラスタモードに切り替えます。

各マシンがエンドポイント用AMPに登録された後、[Centralized Management Options] > [Manage Settings]でファイルレピュテーションと分析のマシンレベルの上書きを削除し、モード をクラスタに戻します。 クラスタリングが正常に動作するには、すべてのデバイス設定が一致し ている必要があります。 [Register Appliance with AMP for Endpoints]ボタンは引き続きグレー表 示され、クラスタモードでは使用できません。

関連情報

- <u>テクニカル サポートとドキュメント Cisco Systems</u>
- ・エンドポイント向けCisco AMP ドキュメントポータル
- <u>CiscoクラウドEメールセキュリティ エンドユーザガイド</u>
- <u>Cisco E メール セキュリティ アプライアンス: エンドユーザ ガイド</u>