# ESA/CES — 將集群裝置註冊到面向終端的 AMP的過程

## 目錄

<u>簡介</u>

<u>問題</u>

<u>解決方案</u>

<u> 第1步 — 登入並導航至ESA/CES上的AMP頁面。</u>

步驟2 — 更改配置模式。

步驟3 — 切換到Machine Override Mode。

第4步 — 為電腦設定註冊面向終端的AMP。

<u>第5步 — 切換到群集模式。</u>

<u>相關資訊</u>

## 簡介

本檔案介紹在叢集組態環境中將思科電子郵件安全裝置(ESA)/雲郵件安全(CES)裝置註冊到終端進 階惡意軟體防護(AMP)的程式。

## 問題

**附註**:本文檔是從ESA/CES AsyncOS 11.1開始編寫的。有關ESA/CES文檔的更多資訊,請 參閱<u>使用手冊和文檔。</u>

嘗試從Security Services > File Reputation and Analysis頁面內的GUI使用面向終端的AMP註冊 ESA/CES集群,*Register Appliance with AMP for Endpoints*按鈕呈灰色顯示,無法完成註冊。

如下圖所示:

$\bigtriangledown$ 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:

# 解決方案

要在集群配置中將ESA/CES裝置註冊到面向終端的AMP,必須通過電腦級**別覆蓋完成**。這意味著 ,對於群集中的每個電腦,它都將有一個單獨的覆蓋設定,該設定將優先。

要完成的步驟如下:

第1步 — 登入並導航至ESA/CES上的AMP頁面。

導覽至Security Services > File Reputation and Analysis,然後驗證當前配置模式。在所提供的輸出 中,Mode - Cluster表示此情況。

#### **File Reputation and Analysis**

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

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

## 步驟2—更改配置模式。

#### 按一下**集中管理選項>管理設定。**

Mode - Cluster: AMPTEST	Change Mode.	<b>T</b>		
Settings are defined: Delete Settings for this feature You can also Manage Settings.	at this mode.			
Advanced Malware Protection				
F	ile Reputation:	Enabled		

#### 在Manage Settings下,將**配置從群集復**制到登入的相應電腦。選擇後,**提交並提交**更改。

File Analysis: Enabled

Mode Cluster: AMPTEST	Change Mode	¥	
Manage Settings for Cluster: AN	aptest mode) A n com		
Cluster: AMPTEST			
Cancel			Submit

## 步驟3 — 切換到Machine Override Mode。

按一下Change Mode...下拉選單,並選擇要配置覆蓋的相應電腦。

#### **File Reputation and Analysis**

Mode -Cluster: AMPTEST	Change Mode	•
Centralized Management Options	Change Mode * Cluster: AMPT	EST (current mode)
Advanced Malware Protection	Group: Main_ Machine: B	Group SA.cisco.com
Fi	e Reputation: E	sa4.aricent.com
	File Analysis: E	inabled

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

## 第4步 — 為電腦設定註冊面向終端的AMP。

在配置模式切換到Machine: 之後<電腦名稱>。

按一下編輯全域性設定 ...... 然後展開Advanced settings for File Analysis 組件。

按一下Register Appliance with AMP for Endpoints按鈕以完成註冊。

Mode — Machine: esa4.aricent.com Change Mode   Centralized Management Options			
Advanced Malware Protection			
Advanced Malware Protection services require network communication	n to the cloud servers on ports 32137 or 443 (fo	r File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.	
File Reputation Filtering:	Cable File Reputation		
File Analysis: 🕐	Enable File Analysis     Select All Expand All C	vilanse All Deret	
	<ul> <li>Archived and compressed</li> <li>Configuration</li> <li>Database</li> <li>Document</li> <li>Email</li> <li>Encoded and Encrypted</li> <li>Executables</li> <li>Microsoft Documents</li> <li>Miscellaneous</li> </ul>		
	File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)	
	AMP for Endpoints Console Integration 🕐	Register Appliance with AMP for Endpoints	
	SSL Communication for File Reputation:	Use SSL (Port 443) Tunnel Proxy (Optional):	

在群集中其餘的電腦上重複步驟1-4,註冊面向終端的AMP。

警告:受缺陷id:CSCvp23281影響的ESA/CES軟體版本應跳過缺陷解決方法中提供的步驟5。

## 第5步 — 切換到群集模式。

每台電腦向面向終端的AMP註冊後,通過在**集中管理選項>管理設定**下刪除檔案信譽和分析的電腦 級別覆蓋,將模式切換回群集。 所有裝置設定必須匹配,群集才能成功運行。 Register Appliance with AMP for Endpoints按鈕仍呈灰色顯示,在群集模式下不可用。

## 相關資訊

- 技術支援與文件 Cisco Systems
- •思科終端進階惡意軟體防護 檔案入口網站
- Cisco Cloud Email Security 最終使用手冊
- Cisco Email Security Appliance 最終使用手冊