# ESA/CES — 将集群设备注册到面向终端的 AMP的过程

# 目录

<u>简介</u>

<u>问题</u>

<u>解决方案</u>

<u>第1步 — 登录并导航至ESA/CES上的AMP页面。</u>

第2步 — 更改配置模式。

- 第3步— 切换到Machine Override模式。
- <u>第4步 注册面向终端的AMP以进行计算机设置。</u>
- 第5步 切换到集群模式。

<u>相关信息</u>

# 简介

本文档介绍在集群配置环境中将思科邮件安全设备(ESA)/云邮件安全(CES)设备注册到面向终端的 高级恶意软件防护(AMP)的过程。

# 问题

**注意:**本文档自ESA/CES AsyncOS 11.1起编写。有关ESA/CES文档的详细信息,请参阅用 <u>户指南和文档。</u>

尝试从**Security Services > File Reputation and Analysis**页面的GUI向面向终端的AMP注册 ESA/CES集群,**Register Appliance with AMP for Endpoints将呈灰色显示,且无法完成注册。** 

如图所示:

$\triangledown$ 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:	

# 解决方案

要在集群配置中将ESA/CES设备注册到面向终端的AMP,必须使用计算机级**别覆盖完成**。这意味着 对于集群中的每台计算机,它将具有优先的单个覆盖设置。

要完成的步骤如下:

## 第1步 — 登录并导航至ESA/CES上的AMP页面。

导航至安全服务>文件信誉和分析并验证当前配置模式。这由提供的输出中的Mode - Cluster表示。

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

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

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

### 第2步 — 更改配置模式。

#### 单击Centralized Management Options > Manage Settings。

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			

#### 在管理设置下,**将配置从集群复**制到登录的相应计算机。选择后,**提交并提**交更改。

Mode - Cluster: AMPTEST	Change Mode	•	
	change Hodel		
Manage Settings for Cluster: Al	MPTEST		
Copy      settings to:     Copy      Settings to:     Copy      Copy      Settings to:     Copy      Copy      Copy      Copy      Copy      Copy      Settings to:     Copy      Copy      Settings to:     Copy      Settings to:     Copy      Copy      Settings to:     Copy      Settings to:     Copy      Settings to:     Seting to:     Settings to:     Settings to:     Settings to:     Set	t mode) 🔺		
<ul> <li>Delete settings from:</li> <li>Cluster: AMPTEST</li> </ul>			
Cancel			Submit

## 第3步— 切换到Machine Override模式。

单击"更**改模式……"**下拉菜单,并选择要配置的覆盖的相应计算机。

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

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

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

## 第4步 — 注册面向终端的AMP以进行计算机设置。

将配置模式切换到"计算机:<计算机名称>。

单击编辑全局设置…… 然后展开"文件分析"组件的"高级设置"。

单击"向面向终端的AMP注册设备"的按钮完成注册。

Mode Machine: esa4.aricent.com Change Mode   Change Mode  Change Mode  Change Mode					
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:	C Enable File Reputation				
File Analysis: (?)	<ul> <li>Enable File Analysis</li> <li>Select All Expand All C</li> <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>	ollapse All Reset			
	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):			

在集群中的其余计算机上重复步骤1-4,注册面向终端的AMP。

**警告:**受缺陷ID影响的ESA/CES软件版本:<u>CSCvp23281</u>应跳过步骤5,如缺陷解决方法中所 述。

## 第5步 — 切换到集群模式。

每台计算机向面向终端的AMP注册后,通过删除"集中管理选项">"管理设置"下的"文件信誉和分析 "的计算机级别覆盖,将模**式改回集群**。 所有设备设置必须匹配才能使集群成功运行。 Register Appliance with AMP **for Endpoints(向终端注册AMP的设备)**按钮仍将呈灰色显示,在集群模式下 不可用。

# 相关信息

- <u>技术支持和文档 Cisco Systems</u> <u>面向终端的思科AMP 文档门户</u>
- 思科云电邮安全 最终用户指南
- 思科邮件安全设备 最终用户指南