# 安全網路分析(SNA)故障排除 — 身份服務引擎 (ISE)整合「連線失敗 — 在此ISE群集上找不到服 務」

# 目錄

<u>簡介</u> <u>Cisco ISE整合</u> <u>潜在故障原因</u> <u>驗證和疑難排解</u> <u>已知原因</u> <u>ISE部署中的複製問題</u> 驗證ISE PxGrid證書鏈

#### 簡介

本文檔介紹如何驗證SMC 7.3.2版以後的ISE整合問題。SNA為版本7.3.2的ISE整合元件引入了 PxGrid v2.0。本文重點介紹在版本7.3.2及更高版本上配置思科ISE整合時可能會遇到的某些特定錯 誤消息。

有關PxGrid v2.0及其功能的詳細資訊,請訪問-PxGrid v2.0

#### Cisco ISE整合

當SMC與ISE整合時,它會根據在配置UI中選擇的覈取方塊發出訂閱相應服務的請求—

Integration	options 0
-------------	-----------

Integrated Product 0

- Cisco ISE
- Cisco ISE PIC (Passive Identity Connector)
- Adaptive Network Control
- Static SGT Classifications 0
- Sessions 0
  - Track sessions derived from machine authentications

ISE服務

#### 根據選定的覈取方塊,SMC可以請求 —

服務:com.cisco.ise.config.anc

服務:com.cisco.ise.trustsec

服務:com.cisco.ise.session

服務:com.cisco.ise.pubsub

反過來,對於這些服務,SMC會與ISE節點通訊以訂閱該服務。 當SMC向ISE節點發出服務請求時 ,它希望知道哪些ISE節點可以提供該主題或服務。

#### 潛在故障原因

- "連線狀態:在此ISE群集上找不到失敗服務com.cisco.ise.pubsub"
- "連線狀態:在此ISE群集上找不到失敗服務com.cisco.ise.anc。"
- "連線狀態:在此ISE群集上找不到失敗的服務com.cisco.ise.session。"
- "連線狀態:在此ISE群集上找不到失敗的服務com.cisco.ise.trustsec。"

#### 驗證和疑難排解

導航到管理> PxGrid服務>診斷>測試並運行運行狀況監控測試工具(ISE 3.0及更高版本)



對於ISE 2.4、2.6和2.7:



運行狀況監控測試工具

可以在頁面頁尾中註明Connected via XMPP <hostname>的PXGrid節點的CLI中檢視測試結果。

#### 運行命令「show logging application pxgrid/pxgrid-test.log」

連線並成功時的輸出表示:

asc-ise24p12-347/admin# show logging application pxgrid/pxgrid-test.log 2021-10-29 01:46:32 INFO TestGridConnection:55 — 正在啟動pxgrid測試連線...... 2021-10-29 01:46:33 INFO TestGridConnectionHelper:307 - SUMMARY> Subscribe=CONNECTING, session-cnt=0;BulkDownload=NOT STARTED, bd-session-cnt=0 2021-10-29 01:46:33資訊配置: 313 — 連線到主機asc-ise24p12-347.rtpaaa.net 2021-10-29 01:46:33資訊配置: 318 — 連線正常到主機asc-ise24p12-347.rtpaaa.net 2021-10-29 01:46:33資訊配置: 343 — 客戶端登入到主機asc-ise24p12-347.rtpaaa.net 2021-10-29 01:46:34資訊配置: 345 — 客戶端登入正常訪問主機asc-ise24p12-347.rtpaaa.net 2021-10-29 01:46:35 INFO NotificationHandlerSmack:70 — 已完成刷新連線狀態。 2021-10-29 01:46:35 INFO TestGridConnectionHelper:312 - SUMMARY> Subscribe=CONNECTED, session-cnt=0;BulkDownload=NOT STARTED, bd-session-cnt=0 2021-10-29 01:50:36 INFO TestGridConnection:164 - SUMMARY> Subscribe=CONNECTED, session-cnt=0;BulkDownload=SUCCESS,bd-session-cnt=0 2021-10-29 01:50:36 INFO NotificationHandlerSmack:81 — 已清除連線狀態...... 2021-10-29 01:50:36 INFO TestGridConnectionHelper:322 — 客戶端已斷開連線 2021-10-29 01:50:36 INFO TestGridConnection:75 - SUMMARY> Subscribe=DISCONNECTED, session-cnt=0;BulkDownload=DISCONNECTED, bd-sessioncnt=0

#### 驗證是否啟用用於將SMC連線到ISE的帳戶:

驗證該客戶端是否已批准,如果該客戶端處於掛起狀態,則批准該客戶端

ISE 3.0及更高版本:

管理> PxGrid服務>客戶端管理>客戶端:

Cisco ISE			Ad	Administration - pxGrid Services		
Summary	Client Management	Diagnostics Sa	mings			
Clients	C	lients				
Rolley		- Usemane configured on SMC				
Carolepe Carolifications						
	0	Annual II fram v 2	Let O Endle O Disable & Approve	Decline		
		Name	Description	Officert Groups	Status	
		cinco ana	Account for SMC Publicit Integration	See.	· Tautier	

#### ISE 2.4、2.6和2.7:

管理> PxGrid服務>所有客戶端

h-h- identity Services Engine Home + Com	et Visibility + Operations + Policy	+ Administration + Work Center	
System + Identity Management + Network Resource	s + Device Portal Management peGrid Ser	vices + Feed Service + Threat	Centric NAC
All Cherts Web Clients Capabilities Live Log	Setings Certificates Permissions		
/Cubie O Cauble O Approve O Croup 👎 Decline 🧯	Delete + 🧐 Refresh: "Skal Pending Approval)	1) *	
Clerit Norre Clerit Description	n Capabilities	Status	Client Group(s)
Ise-mit-esc-ie24p12-347	Capabilities(2 Puls, 1 Sult)	Online (10499)	Internal
Ise-pubsub-asc-ise24p12-347	Capabilities(0 Pub, 0 Sub)	Online (104PP)	Internal
Ise-fanout-asc-ise24p12-347	Capabilities(0 Pub, 0 Sub)	Online (IMPP)	Internal
Ise-admin-asc-ise24p12-347	Capabilities(3 Pub, 2 Sub)	Online (10/079)	Internal
ise-bridge-asc-ise/Hp12-347	Capabilities(2 Pub, 5 Sub)	Online (10499)	Internal
Class-sna Account for SW	Capabilities(0 Pub, 0 Sub)	Pending	
Г			
Check this box a	ind click approve		

要檢查SMC PxGrid客戶端的連線狀態及其所連線的ISE節點,請導航到**管理> PxGrid服務>診斷>** WebSocket

II Chece 134			Administra	aton-jadina Services		
Summary Clienchianagem	ort Dispersion Ser	ings				
Network	WebSocket					
1.4	Owita Turks					
3.03						
	Ginera					
					danafage <u>1 v</u> K.C. <u>1</u>	
	(C rener					
	Port line	Class: Notes	Portus	Connect %	hubor-prises	Parather (ACTION record)
	× line line	61A	A 201000 - 1		Bulane (prison)	Dentition (Add Televiser (up)
	00.00000000	E100-794	<ul> <li>Germanian</li> </ul>	10.40701.01		10.30.30.11

### 已知原因

- 啟用PxGrid角色的節點在ISE部署中面臨複製問題
- PxGrid證書信任問題

# ISE部署中的複製問題

複製對於維護部署中所有成員節點的最新資訊至關重要。如果運行PxGrid角色的節點報告複製問題,則可能沒有有關它可以為PxGrid客戶端提供的主題和服務的最新資訊。

如果節點報告複製失敗警報或複製速度緩慢:

8	Replication Failed			
或				
	Slow Replication Error			

要採取糾正措施,請執行以下操作:

驗證與ISE節點的IP連線,通過SSH登入並通過發出以下命令驗證服務是否正在運行:

# show application status ise

例如

asc-ise30p2-353/admin# show application status ise

ISE進程名稱狀態進程ID

資料庫監聽程式運行24872 運行114個進程的資料庫伺服器 應用程式服務器運行40137 Profiler資料庫正在運35916 ISE索引引擎已禁用 AD聯結器運行40746 已禁用M&T會話資料庫 已禁用M&T日誌處理器 證書頒發機構服務正在運行40609 EST服務運行77903 SXP引擎服務已禁用 Docker後台程式正在運28517 TC-NAC服務已禁用 pxGrid基礎結構服務已禁用 pxGrid發佈伺服器訂戶服務已禁用 pxGrid連線管理器已禁用 pxGrid控制器已禁用 已禁用PassiveID WMI服務 PassiveID系統日誌服務已禁用 PassiveID API服務已禁用 已禁用PassivelD代理服務 已禁用PassiveID終結點服務 已禁用PassiveID SPAN服務 已禁用DHCP伺服器(dhcpd) 已禁用DNS伺服器(已命名) 運行Web的ISE消息服29277 ISE API網關資料庫服務運行32173 ISE API網關服務運行38161 已禁用分段策略服務 REST身份驗證服務已禁用 SSE聯結器已禁用

在Administration > System > Deployment下對受影響的節點執行手動同步

選擇報告問題的節點,然後按一下Syncup

# Deployment Nodes Edit Register Syncup Hostname Personas

附註:這會導致正在同步的節點上的服務重新啟動,並且可能導致節點停止服務30分鐘。建議在受 控更改視窗中執行此活動。

# 驗證ISE PxGrid證書鏈

在ISE GUI上導航到Administration > System > Certificates

每個啟用PxGrid角色的節點都有一個證書,該證書具有與其關聯的PxGrid角色。

這些證書可以由第三方CA或ISE內部CA簽名。 選中證書旁邊的框並點選檢視 — 該檢視必須列出證 書詳細資訊和證書鏈。 憑證詳細資訊中亦有一個狀態指示器,指出憑證是否良好或憑證鏈結是否不 完整。

如果證書由ISE內部CA簽名:

# Certificate Hierarchy

Certificate Services Root CA - asc-ise30p2-249 Certificate Services Node CA - asc-ise30p2-249 Certificate Services Endpoint Sub CA - asc-ise30p2-249 asc-ise30p2-249.rtpasa.net asc-ise30p2-249.rtpasa.net Issued By : Certificate Services Endpoint Sub CA - asc-ise30p2-249 Expires : Sun, 14 Jun 2026 16:44:47 UTC

Certificate status is good

共有四個級別,從頂部開始:

1. ISE根CA — 這是CA證書,每個部署只有1個ISE根CA,這是主管理節點。

2. ISE節點CA — 這是一個中間CA,其證書由ISE根CA頒發,也是主管理節點

3. ISE終端子CA — 這是第3級和PxGrid身份證書的頒發者。 部署中的每個節點都有其自己的ISE終 端子CA,由ISE節點CA(主管理節點)頒發

4. PxGrid身份證書 — 這是ISE節點在整合和通訊期間向PxGrid客戶端(即SMC)提供的證書

如果您擁有由貴組織的CA簽署且獨立於ISE和/或第三方公認的CA的證書:

驗證根CA和簽署PxGrid證書的任何中間CA是否安裝在ISE上的受信任安全證書儲存中,位於**管理 >系統>證書>證書管理>受信任證書** 

在這兩種情況下,當您檢視證書時,UI必須指示「Certificate Status is good」。

錯誤條件:

8 Certificate trust chain is incomplete

#### PxGrid證書信任問題

如果使用ISE內部CA時證書信任鏈不完整,則需要重新生成ISE根CA,然後作為流程的一部分重新 生成ISE PxGrid證書。 使用主管理員新生成的ISE根CA和ISE節點CA以及每個PxGrid節點的ISE終 端子CA證書更新SMC的信任儲存。

要替換ISE根CA鏈,請導航到**管理>系統>證書>證書管理>證書簽名請求**,然後選擇**生成證書簽名請** 求(顯示此UI):

a Ones 191	Administration - System	1.0 28 4
Dumpoint Lowing	Certification Logging Mandemance Logginde Health Cancel. Kashing & Besture Admin. Samin Samings	
Aarthon Kangonee v Apan Jankan Naad Jalkes Saat Jalkes Gariban Katig Apan Ka Cariban Katig Apan Ka	Certificate Signing Request: Institute was at wass different advances the unique, the latitude within advances of unique on respective advances that a state to the unique of the uniqu	
	Enage instruments with we count the	

在下拉選單中,選擇ISE Root CA,然後選擇Replace ISE Root CA Certificate Chain

如果使用外部CA時,證書信任鏈不完整,請將缺少的證書新增到ISE信任儲存下的Administration > System > Certificates > Certificate Management > Trusted Certificates,然後在ISE CLI上發出「 application stop ise」命令,然後發出「application start ise」命令,重新啟動節點上的服務。 CA證書是通過訪問Primary admin節點上ISE部署的GUI新增的,但需要在顯示證書狀態錯誤的節點 上通過CLI重新啟動服務。

#### 附註:重新啟動服務將使節點離線15-20分鐘。

如果在採取這些糾正步驟後問題仍然存在,請聯絡支援以獲得幫助。

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。