# 修復Active Directory組檢索在Identity Services引 擎上發出 ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PE RMISSIONS

## 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>問題</u> 解決方案

# 簡介

本文描述如何在驗證期間解決Active Directory(AD)組檢索問題,而即時日誌中會顯示此錯誤:

ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PERMISSIONS

必要條件

#### 需求

思科建議您瞭解以下主題:

- 思科身分識別服務引擎
- Microsoft Active Directory

#### 採用元件

本文檔不限於身份服務引擎(ISE)的特定軟體版本。

### 問題

問題在於用於將ISE加入AD的使用者帳戶沒有獲取令牌組的正確許可權。如果使用域管理員帳戶將 ISE加入AD,則不會發生這種情況。要解決此問題,您必須將ISE節點新增到使用者帳戶並為這些 ISE節點提供這些許可權:

- •列出內容
- •讀取所有屬性
- •讀取許可權

即使使用者的許可權似乎正確(檢查ISE 1.3 AD身份驗證失敗並出現錯誤:「許可權不足,無法提取

28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW\_ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PERMISSIONS),lsass/server/auth-providers/ad-openprovider/provider-main.c:7409 28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW\_ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PERMISSIONS),lsass/server/api/api2.c:2572

要為使用者帳戶提供所需的許可權,請執行以下步驟:

1.在AD上,導航到Properties for AD使用者帳戶:

🕹 userA 🏂 userB 🏂 userC	Delete Rename	
🕺 vchrenek	Properties	
🎎 vchrenek	Help	
👗 veronika 🗕		

2.選擇Security頁籤,然後按一下Add:

		veronika	a Prope	rties		? X	
Published C	Certificates	Member Of	Passwor	d Replica	tion [	Dial-in Object	
Remote Desktop Services Profile		ervices Profile	COM+		At	Attribute Editor	
General	Address	Account	Profile	Teleph	ones	Organization	
Security Environment			Ses	sions	Re	mote control	
Group or u	iser names:						
S. Even	vone					^	
SELF							
& Auth	enticated U	sers				=	
SYS1	TEM						
BR-I	SE-SEC\$						
Acco	unt Unknow	wn(S-1-5-21-70	538695-7	90656579	42939	29702-1	
M Dom	ain Admins (	EXAMPLE0\D	omain Adı	mins)		~	
Add. Bemove							
				Add		Remove	
			L	Add		Remove	
Permission	ts for Every	one		Add	llow	Remove Deny	
Permission Full con	ns for Every trol	one		Add A	llow	Deny	
Permission Full com Read	ns for Every trol	one		Add A		Deny	
Permission Full com Read Write	ns for Every Itrol	one		Add		Remove Deny	
Permission Full con Read Write Create a	ns for Every Itrol all child obje	one		Add A C C C C		Remove Deny	
Permission Full con Read Write Create a Delete a	ns for Every Atrol all child obje	one ects ects		Add A C C C C C		Remove Deny	
Permission Full con Read Write Create Delete	ns for Every trol all child obje all child obje I to authenti	one ects ects icate		Add		Remove Deny	
Permission Full con Read Write Create a Delete Allowed	all child obje trol all child obje all child obje	one ects ects icate		Add		Remove Deny	
Permission Full con Read Write Create & Delete & Allowed Create & Create & Create & Delete & Allowed	all child objet all child objet all child objet to authenti	one ects ects icate is or advanced	settings, o	Add		Remove Deny	
Permission Full con Read Write Create & Delete & Allowed Create & Allowed Create & Allowed Create & Allowed	all child obje all child obje all child obje all child obje to authenti d permission	one ects ects icate is or advanced	settings, o	Add		Remove Deny	
Permission Full con Read Write Create & Delete & Allowed For specia Advanced	all child obje all child obje all child obje to authenti d permission	one ects ects icate is or advanced	settings, (	Add		Remove Deny	
Permission Full con Read Write Create & Delete & Allowed Chanced	all child obje all child obje all child obje to authenti permission	one ects ects icate is or advanced	settings, o	Add		Remove Deny	

3.選擇**對象型別**:

Select Users, Computers, Service Acc	counts, or	Groups ×
Select this object type:		
Users, Groups, or Built-in security principals		Object Types
From this location:		
example.com		Locations
Enter the object names to select (examples):		
1		Check Names
Advanced	OK	Cancel

4.選擇Computers,然後按一下OK:

Object Types	x
Select the types of objects you want to find. Object types:	
OK Cancel	

5.插入ISE主機名(在本示例中為VCHRENEK-ISE4),然後按一下**OK**:

Select Users, Computers, Service Accounts	s, or Groups 🛛 🗙
Select this object type: Users, Computers, Groups, or Built-in security principals	Object Tupes
From this location:	
example.com	Locations
Enter the object names to select ( <u>examples</u> ):	
VCHRENEK-ISE4	Check Names
Advanced 0	K Cancel

6.選擇ISE節點,然後按一下**Advanced**:

		veronika	n Prope	rties		?	x
Published Certific Bernote Dest	cates	Member Of	Passwor	d Replica NM+	tion [	)ial-in	Object
General Ad	dieses	Account	Profile	Telenh	ones	Πισαni	zation
Security	Fn	vitonment	Sess	ions	Be	mote con	trol
Group or user r	Group or user names:						
Administra Account 0 Re-Windows Windows Enterprise	Administrators (EXAMPLE0\Administrators)     Account Operators (EXAMPLE0\Account Operators)     Account Operators (EXAMPLE0\Account Operators)     Windows 2000 Compatible Access (EXAMPLE0\Pre-Windows     Windows Authorization Access Group (EXAMPLE0\Windows Aut     Terminal Server License Servers (EXAMPLE0\Terminal Server Lic						
	EK-ISE 4	4 (EXAMPLEO	WCHREN	EK-ISE4	\$)		~
Permissions for	VCHR	ENEK-ISE4		Add	llow	Remov	re
Full control				Γ	7		^
Read					/		
Write				Ē	ī		
Create all ch	ild obje	cts		Ē	ī		
Delete all ch	ild obje	cts		Ē	ī		
Allowed to a	uthentio	ate		Ē	ī		
Channes and				r	-		~
For special permissions or advanced settings, click. Advanced Advanced.							
[	OK	< C	ancel	Ap	ply	Н	elp

7.從「高級安全設定」中選擇ISE電腦帳戶,然後按一下**編輯**:

homer:	Domain Admins (EXAMPLEO)	Domain Admins) Change			
Permission	Auditing Effective A	ccess			
or addition ermission e	al information, double-click a per entries:	mission entry. To modify a	permission entry, sele	ct the entry and click Edit (if av	ailable).
Туре	Principal	Access	Inherited from	Applies to	^
🕙 Allow	SELF	Special	None	This object only	-
🔒 Allow	Authenticated Users	Read permissions	None	This object only	1
🕙 Allow	SYSTEM	Full control	None	This object only	
😣 Allow	Domain Admins (EXAMPLE0	Full control	None	This object only	
🔏 Allow	Account Operators (EXAMPL	Full control	None	This object only	
Allow	VCHRENEK-ISE4 (EXAMPLE0\	Read	None	This object only	
🕹 Allow	Everyone	Change password	None	This object only	
🔏 Allow	SELF	Read/write web infor	None	This object only	
🕹 Allow	SELF	Read/write phone and	None	This object only	
🕹 Allow	SELF	Read/write personal in	None	This object only	
Add Disable in	Remove Edit			Restore	defaults

8.向ISE電腦帳戶提供這些許可權,然後按一下OK:

1			Permission Entry for vero	nika		-	•	×	
	Principal: Type: Applies to:	VCHRENEK-ISE4 (EXAMPLEØ\VCHRENEK-ISE4\$) Allow This object only	elect a principal						- =
	Permissions	<ul> <li>Full control</li> <li>✓ List contents</li> <li>✓ Read all properties</li> <li>Write all properties</li> <li>Delete</li> <li>Delete subtree</li> <li>✓ Read permissions</li> <li>Modify permissions</li> <li>Modify owner</li> <li>All validated writes</li> <li>All extended rights</li> </ul>	Create all Delete all Create ms Create ms Delete ms Delete ms Allowed t Change p Receive a Send as	child objects child objects -net-ieee-80211-GroupPolicy objects -net-ieee-80211-GroupPolicy objects -net-ieee-8023-GroupPolicy objects -net-ieee-8023-GroupPolicy objects o authenticate assword s					
	Properties:								
		Read all properties	🖌 Read msD	S-OperationsForAzTaskBL					
		Write all properties	Read msD	S-parentdistname					~
					OK		Cancel	1	]

Test User Authentication	
* Username	veronika
* Password	•••••
Authentication Type	MS-RPC 🔻
Authorization Data	Retrieve Groups
	Retrieve Attributes
	Test
Authentication Result	Groups Attributes
Test Username	: veronika
ISE NODE	: vchrenek-ise4.example.com
Scope	: Default_Scope
Instance	: AD1
Authentication Result	: SUCCESS
Authentication Domain	: example.com
User Principal Name	: veronika@example.com

User Distinguished Name : CN=veronika, CN=Users, DC=example, DC=com

: 1 found.

必須對所有使用者執行該操作,並且更改應複製到域中的所有域控制器。

: 36 found.

Groups

Attributes