Identity Services Engine の修正 Active Directory グループ検索問題 ERROR_TOKEN_GROUPS_INSUFFICIENT_PE RMISSIONS

目次

<u>はじめに</u> <u>前提条件</u> <u>要件</u> 使用するコンポーネント 問題 解決策

概要

このエラーはライブ ログで見られるがどのように回避策に認証かの間の Active Directory (AD) グループ検索における問題この資料に記述されています、:

ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Identity Services Engine
- Microsoft Active Directory

使用するコンポーネント

この資料は Identity Services Engine (ISE)の特定のソフトウェア バージョンに制限 されません 。

問題

問題は ISE に AD に加入するのに使用されるユーザアカウントが tokenGroups を得る正しい特権 がないことです。 これは ISE に AD に加入すればのにドメイン 管理者アカウントが使用された 場合起こりません。 この問題を解決するために、ユーザアカウントに ISE ノードを追加し、ISE ノードにそれらの権限を提供しなければなりません:

・リスト コンテンツ

- すべてのプロパティを読んで下さい
- 読み取り権限

この問題はユーザ向けの権限が正しいようであるのに、見られます(<u>ISE 1.3 AD 認証</u>に対するチ ェックは<u>エラーと失敗します: 「トークン グループ」を取出す不十分な特権</u>)。 それらのデバッ グは ad-agent.log で参照されます:

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

解決策

必要なアクセス許可をユーザアカウントに提供するために、それらのステップを実行して下さい:

1. AD で AD ユーザアカウントのための Properties にナビゲート して下さい:

🛃 userA 🛃 userB 尾 userC	Delete Rename	
🕺 vchrenek	Properties	
😣 vchrenek	Help	
👗 veronika 🗕		

2. タブを『Security』を選択し、『Add』 をクリック して下さい:

		veronika	a Prope	rties		? X	
Published Certificates Member Of Password Replication Dial-in Object							
Remote	Desktop Se	ervices Profile	0	OM+	At	tribute Editor	
General	Address	Account	Profile	Teleph	ones	Organization	
Security	Er	wironment	Ses	sions	Re	mote control	
Group or u	ser names:						
St. Even	vone					^	
SELF							
& Auth	enticated Us	sers				=	
SYS1	TEM						
A DR-I	SE-SEC\$						
Acco	unt Unknov	m(S-1-5-21-70	538695-7	90656579	42939	29702-1	
Mag Dom	aın Admins (EXAMPLEUND	omain Adi	minsj		~	
				Add		Remove	
Permission	ns for Everyo	ne	_	A	low	Deny	
Full con	trol			Γ	7		
Read				Ē	ī		
Write				Ē	5		
Create	all child obje	cts					
Delete	all child obje	cts					
Allowed	to authenti	cate					
Change							
For special permissions or advanced settings, click. Advanced							
Advanced	l.						
Advanced							

3. **オブジェクト タイプを**選択して下さい:

Select Users, Computers, Service Accounts, o	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. **コンピュータを**選択し、『OK』 をクリック して下さい:

Object Types	x
Select the types of objects you want to find. Object types:	
OK Cance	4

5. ISE ホスト名(この例の VCHRENEK-ISE4)を挿入し、『OK』 をクリック して下さい:

Select Users, Computers, Service A	ccounts, or (Groups 🛛 🗙
Select this object type: Users, Computers, Groups, or Built-in security principals		Object Types
From this location:		
example.com		Locations
Enter the object names to select (examples):		
VCHRENEK-ISE4		Check Names
Advanced	OK	Cancel

6. ISE ノードを選択し、『Advanced』 をクリック して下さい:

		veronika	a Prope	erties		?	x
Published Certifi	cates	Member Of	Passwo	rd Replica	ation	Dial-in (Dbject
Remote Des	ktop Se	rvices Profile	- (COM+	At	tribute Ed	itor
General Ad	dress	Account	Profile	Telepi	nones	Organia	zation
Security	Er	wironment	Ses	sions	Re	mote con	trol
Group or user r	names:						
& Administra	itors (E)	KAMPLE0VAd	ministrator	s)			~
& Account (Operato	rs (EXAMPLE)	0\Accour	t Operato	rs)		
Re-Windo	ows 200	00 Compatible	Access (I	EXAMPLE	0\Pre-V	Vindows	
Se Windows	Authori	zation Access	Group (E	XAMPLE	Windo	ws Aut	
S Terminal S	Server L	icense Server	rs (EXAMI	PLE0\Ten	minal Se	rver Lic	=
ENTERP	RISE D	omain cont	ROLLER	S			
VCHREN	EK-ISE	4 (EXAMPLEO	WCHRE	NEK-ISE4	\$]		\sim
			ſ	Add		Remov	e
			L				
Permissions for	VCHR	ENEK-ISE4		A	llow	Deny	
Full control				[^
Read					✓		
Write				[
Create all ch	ild obje	cts		[
Delete all ch	ild obje	cts		[
Allowed to a	uthentia	cate		[
Channes	a.d						~
For special permissions or advanced settings, click Advanced							
[01	< (Cancel	Ap	ply	He	elp

7. 拡張セキュリティ設定から ISE コンピューター アカウントを選択し、『Edit』 をクリック し て下さい:

	Ad	dvanced Security Setti	ings for veronika	ı [-	- 🗆
Owner:	Domain Admins (EXAMPLEO	Domain Admins) Change			
Permission	s Auditing Effective A	ccess			
or addition	al information, double-click a per entries:	mission entry. To modify a	permission entry, se	lect the entry and click Edit (if a	vailable).
Туре	Principal	Access	Inherited from	Applies to	^
Allow 🕺	SELF	Special	None	This object only	=
😫 Allow	Authenticated Users	Read permissions	None	This object only	_
😫 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	e defaults
				OK Cancel	Apply

8. それらの権限を ISE コンピューター アカウントに提供し、『OK』 をクリック して下さい:

1			Permission En	try for veronika		-	•	x	
	Principal: Type:	VCHRENEK-ISE4 (EXAMPLEØ\VCHRENEK-ISE4\$)	Select a principal						~ =
	Applies to:	This object only	~						
	Permissions	E Full control		Create all child objects Delete all child objects Create ms-net-ieee-80211-GroupPolicy objects Delete ms-net-ieee-8023-GroupPolicy objects Create ms-net-ieee-8023-GroupPolicy objects Delete ms-net-ieee-8023-GroupPolicy objects Allowed to authenticate Change password Receive as Reset password Send as					
	Properties:								
		Read all properties		Read msDS-OperationsForAzTask8L					
		Write all properties		✓ Read msDS-parentdistname					~
				(ЭК		Cance	I]

これらの変更が問題なしで、AD グループ取得する必要があった後:

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.exa	mple.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=Use	ers,DC=example,DC=com	
Groups Attributes	: 1 found. : 36 found.		

これはすべてのユーザ向けに実行されたなり、ドメインのすべてのドメインコントローラへの変 更は複製する必要があります。