Correggere il problema di recupero del gruppo di Active Directory ERROR_TOKEN_GROUPS_INSufficient_PERMI SSIONS su Identity Services Engine

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Problema Soluzione

Introduzione

In questo documento viene descritto come risolvere il problema relativo al recupero del gruppo di Active Directory (AD) durante l'autenticazione, mentre l'errore viene visualizzato nei log attivi:

ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Services Engine
- Microsoft Active Directory

Componenti usati

Il documento può essere consultato per tutte le versioni software di Identity Services Engine (ISE).

Problema

Il problema è che l'account utente utilizzato per aggiungere ISE ad AD non dispone dei privilegi corretti per ottenere tokenGroups. Ciò non si verifica se per aggiungere ISE ad AD è stato utilizzato l'account Domain Admin. Per risolvere il problema, aggiungere uno o più nodi ISE all'account utente e fornire le autorizzazioni ai nodi ISE:

- Contenuto elenco
- Leggi tutte le proprietà

• Autorizzazioni di lettura

Questo problema si verifica, anche se le autorizzazioni per l'utente sembrano essere corrette (verificare rispetto a <u>ISE 1.3 AD Authentication Fail with Error: "Privilegio insufficiente per</u> recuperare i gruppi di token"). Tali debug sono riportati in ad-agent.log:

```
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol:
LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/auth-providers/ad-open-
provider/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
```

Soluzione

Per fornire le autorizzazioni necessarie per l'account utente, effettuare le seguenti operazioni:

1. in Active Directory passare a Proprietà per l'account utente AD:

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

2. Scegliere la scheda Protezione e fare clic su Aggiungi:

		veronika	a Prope	erties		? X
Published C	Certificates	Member Of	Passwo	rd Replica	ation D)ial-in Object
Remote	Desktop S	ervices Profile	(COM+	Att	ribute Editor
General	Address	Account	Profile	Teleph	nones	Organization
Security	E	nvironment	Ses	sions	Ren	mote control
Group or u	iser names:					
Se Every	/one					^
SELF						_
& Authe	enticated U	sers				=
SYS1	EM					
A DR-IS	SE-SEC\$	(C 1 E 21 70	E2000E 2	000000000000000000000000000000000000000	420202	0702 1
Acco	unt Unkno ain Admine	WN(5-1-5-21-70	omain Ad	SUPOPOLS [mine]	9-423332	3/02-1
- Dours			omainAu	nim iəj		
				Add		Remove
Permission	s for Every	one		A	llow	Deny
Full con	trol			[
Read				C		
Write				C		
Create a	all child obj	ects		E		
Delete a	all child obj	ects				
Allowed	to authent	icate				
For specia Advanced	l permission	ns or advanced	settings,	click	Ą	Advanced
	0	к с	ancel	Ap	ply	Help

3. Selezionare i tipi di oggetto:

Select Users, Computers, Service A	Accounts, 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. Selezionare Computer e fare clic su OK:

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

5. Inserire il nome host ISE (VCHRENEK-ISE4 nell'esempio) e fare clic su OK:

Select Users, Computers, Service Accounts,	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. Selezionare il nodo ISE e fare clic su Advanced:

			veroni	ka	Prope	rties		?	X
Published (Certific	ates	Member 0	IF I	Passwor	d Replica	ation [Dial-in	Object
Remote	Desk	top Se	rvices Profi	le	C	OM+	At	tribute E	ditor
General	Ado	dress	Account		Profile	Telepł	nones	Organ	nization
Security		En	vironment		Sess	ions	Re	mote co	ntrol
Group or u	iser n	ames:							
Admi Acco Re Pre-V Wind Term R ENTI	nistrat unt O Vindo lows A inal S ERPR	tors (E) perator ws 200 Authoria erver L ISE D1	(AMPLEOV is (EXAMPL IO Compatit zation Acce icense Serr DMAIN COI	Admin EOV ole Ar ss G vers I NTR	nistrators Account ccess (E roup (E> (EXAMP OLLERS	i) Operato XAMPLE (AMPLE) LE0\Ten	rs) O\Pre-V I\Windo minal Se	/indows ws Aut rver Lic.	· =
VCH	RENE	K-ISE4	(EXAMPL	EO\V	CHREN	EK-ISE4	\$]		~
Permission	ve for 1	VCHER	NEKICEA			Add		Remo	ve
Full com	trol	· Crinic	mentioes				7		
Read	aoi							H	
Lukika							-	H	
Create	أنطص الم	ld obier	ale.				4	H	
Delete	all chi	ld objet	do No			L [4	H	
Allowed	Uo au	shantic	ate			L [4	H	
Change		an renaul	ale				-		\sim
For specia Advanced	l pern I.	nissions	or advanc	ed s	ettings, o	lick	4	Advance	ed
		OK		Car	ncel	Ap	ply	ŀ	lelp

7. Da Advanced Security Settings selezionare ISE machine account e fare clic su Edit:

	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. Fornire queste autorizzazioni all'account del computer ISE e fare clic su OK:

1	L.		Permission Entry for veronika	_		×	
	Principal: Type: Applies to:	VCHRENEK-ISE4 (EXAMPLEØ\VCHRENEK-ISE4\$) Allow This object only	Select a principal				Î
	Permissions	C Full control C List contents C Read all properties C Delete D Delete Read permissions Modify permissions All validated writes All extended rights	Create all child objects Delete all child objects Create ms-net-ieee-80211-GroupPolicy objects Delete ms-net-ieee-80211-GroupPolicy objects Create ms-net-ieee-8023-GroupPolicy objects Delete ms-net-ieee-8023-GroupPolicy objects Allowed to authenticate Change password Receive as Send as				
	Properties:	Read all properties	✓ Read msDS-OperationsForAzTask8L				
		Write all properties	Read msDS-parentdistname				~
			OK		Cance	;I]

Dopo queste modifiche, i gruppi AD devono essere recuperati senza problemi:

Test User Authentication					
* Username	veronika				
* Password	•••••				
Authentication Type	MS-RPC 👻				
Authorization Data	✓ Retrieve Groups ✓ Retrieve Attributes				
	Test				
Authentication Result	Groups Attributes				
Test Username ISE NODE Scope Instance Authentication Result	: veronika : vchrenek-ise4.example.com : Default_Scope : AD1 : SUCCESS				
Authentication Domain User Principal Name User Distinguished Name Groups Attributes	: example.com : veronika@example.com : CN=veronika,CN=Users,DC=example,DC=com : 1 found. : 36 found.				

Questa operazione deve essere eseguita per tutti gli utenti e le modifiche devono essere replicate in tutti i controller di dominio del dominio.