# الصإ محالص Sctive معومجم دادرت و الكشم حال Directory ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PE ميوهلا تامدخ كرحم ىلع RMISSIONS

## تايوتحملا

<u>ةمدقملا</u> <u>قمدقملا</u> <u>تابلطتملا</u> <u>مدختسملا تانوكملا</u> <u>قلكشملا</u> لحلا

## ەمدقملا

ءانثأ Active Directory (AD) ةعومجم دادرتسإ ءانثأ ةلكشملا لح ةيفيك دنتسملا اذه حضوي ةرشابملا تالجسلا يف أطخلا اذه ةظحالم متي امنيب ،ةقداصملا:

ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PERMISSIONS

## ةيساسألا تابلطتملا

### تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- Cisco نم ةيوەلا تامدخ كرحم •
- Microsoft Active Directory

#### ةمدختسملا تانوكملا

انم ةددحم جمارب تارادصإ ىلع دنتسملا اذه رصتقي ال Identity Services Engine (ISE).

## ةلكشملا

سيل AD ىلإ ISE ىلإ مامضنالل مدختسملا مدختسملا مدختسملا باسح نأيه ةلكشملا باسح مادختسا مت اذإ كلذ ثدحي نلو .TokenGroups ىلع لوصحلل ةحيحص تازايتما هيدل الا الا (دقع) ةدقع ةفاضإ بجي ،ةلكشملا هذه لحل .AD ىلإ ISE يل مامضنالل ISE (دقع) الا ياسح الا جاسح المال باسح الا المالي المالي المالي المالي العالي المالي العالي المالي المالي الم

- ةمئاقلا تايوتحم •
- صئاصخلا ةفاك ةءارق •

ةءارقلا تانوذأ • <u>ا قارد م</u> لباقم قيقدت) قحيحص ودبت مدختسملل تانوذألا نأ مغر ،رادصإ اذه تيأر adagent.log:

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

## الحل

:ةيلاتلا تاوطخلا ذيفنتب مق ،مدختسملا باسحل ةبولطملا تانوذألا ريفوتل

1. مدختسم باسح **صۂاصخ** یل AD یلع لقتنا

🕹 userA 🏂 userB ዿ userC	Delete Rename	
vchrenek	Properties	
💐 vchrenek 🕹	Help	

:**ةفاضإ** قوف رقناو **نيمأت** بيوبت ةمالع رتخأ .2

		veronika	a Prope	rties		? X	
Published C	ertificates	Member Of	Passwor	d Replica	tion [	Dial-in Objec	
Remote	Desktop Se	rvices Profile	COM+ A		At	Attribute Editor	
General	Address	Account	Profile	Teleph	phones Organiz		
Security	En	vironment	Sess	sions	Re	mote control	
Group or u	ser names:						
St. Every	one					^	
SELF							
& Authe	nticated Us	ers				=	
SYST 88	EM						
🔏 DR-IS	E-SEC\$						
Acco	unt Unknow	m(S-1-5-21-70	538695-79	30656579	429392	29702-1	
M Doma	ain Admins (I	EXAMPLEU\D	omain Adr	ninsj		×	
				Add		Remove	
Permission	s for Everuo	ne	_	۵	low	Denv	
Full con	kol			г	<u>ר</u>		
Read					i		
Write					i		
Create a	l child obie	cts			i	H I	
Delete a	ll child obje	cts			ĩ	H H	
Allowed to authenticate							
Change					2		
For specia Advanced	permission:	s or advanced	settings, o	click	Å	Advanced	
	01	/ C	maal	4.0	al.	Lisla	

3. **نﺉﺍﻙﻝﺍ ﻉﺍﻭﻥﺃ** ﺩﻱﺩﺡﺕ:

Select Users, Computers, Service	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):		
		Check Names
Advanced	OK	Cancel

. **ق. قاوم** قوف رقناو **رتويبمكلا ةزەجأ** ددح

Object Types	x
Select the types of objects you want to find. Object types: Built-in security principals Service Accounts Computers Groups Users	
OK Cancel	

5. قوف رقناو (لاثملا اذه يف ISE (VCHRENEK-ISE4 فيضملا مسا جردأ SE:

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

:**ةمدقتم تارايخ** قوف رقناو ISE ةدقع ددح .6

		veronika	a Prope	rties		?	x
Published Cert	ficates	Member Of	Passwor	d Replica	tion D	)ial-in	Object
General A	ddraee	Account	Profile	Teleph		Organi	zation
Security	uuless En	vironment	Sace	ione	Re	olgani mote.com	trol
Group or user	names:	THOILING IN	0000		110		
Administ Account Pre-Win Window Terminal	rators (E> Operato dows 200 s Authoria Server L PRISE DI	AMPLE0\Adr (EXAMPLE) Compatible zation Access icense Server DMAIN CONT	ninistrators )\Account Access (E) Group (EX s (EXAMP ROLLERS	) Operator XAMPLE XAMPLE0 LE0\Terr	s) 0\Pre-W \Windo ninal Se	/indows ws Aut rver Lic	· II
VCHRE	NEK-ISE	(EXAMPLEO	WCHREN	EK-ISE4	\$)		~
Permissions fr		NEK-ISE4		Add		Remov	e
Full control					<u></u>		
Read					7	H	
Write					2	H	
Create all c	hild obie	ste			i	H	
Delete all c	hild obje	oto ato			i	H	
Allowed to	authentic	ate					~
For special pe Advanced.	ermissions	or advanced	settings, c	lick	4	, i i	ť
	OK		ancel	Ap	ply	Н	elp

7. **ريرحت** قوف رقناو ISE زاهج باسح ددح ،ةمدقتملا نامألا تادادعإ نم.

	Ad	dvanced Security Setti	ings for veronika	_	
Owner:	Domain Admins (EXAMPLEO)	Domain Admins) Change			
Permissions	Auditing Effective A	ccess			
For addition: Permission e	al information, double-click a per ntries:	mission entry. To modify a	permission entry, se	lect the entry and click Edit (if ava	ailable).
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	defaults
				OK Cancel	Apply

8. ق**فاوم** قوف رقناو ISE زاهج باسحل تانوذألا هذه ريفوتب مق

1	l.		Permission Entry for veronia	(a	Ŀ		×	:
	Principal: Type: Applies to:	VCHRENEK-ISE4 (EXAMPLEØ\VCHRENEK-ISE4\$) Allow This object only	elect a principal					^ III
	Permissions		Create all chi Delete all chi Create ms-ne Delete ms-ne Create ms-ne Delete ms-ne Allowed to an Change pass Receive as Reset passwo Send as	ld objects d objects t-ieee-80211-GroupPolicy objects t-ieee-80211-GroupPolicy objects t-ieee-8023-GroupPolicy objects t-ieee-8023-GroupPolicy objects uthenticate word				
	Properties:							
		Read all properties	Read msDS-0	)perationsForAzTaskBL				
		Write all properties	Read msDS-p	arentdistname				~
				[	0K	Cance	el	

لكاشم يأ نود AD تاعومجم دادرتسإ بجي ،تارييغتلا هذه دعب:

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

ةفاك ىلإ الثامتم اخسن تارييغتلا خسن بجيو نيمدختسملا ةفاكل ءارجإلا اذه ذيفنت بجي لاجملا يف لاجملاب مكحتلا تادحو.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما