ربع نييجراخلا ضيوفتلاو ةقداصملا نيوكت LDAPs تاليلحت ريدم ىلإ نمآلا لوصولل ةكبشلا

تايوتحملا

<u>ةمدقملا</u> <u>ةيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>نىوكتلا</u> .LDAP ل ةمدختسملا SSL قداهش ردص AD لاجم مكحت قدحو <u>علا لوخدلا لجس A. قوطخلا</u> <u>رذجلا قلس لسو LDAP مداخ قداهش قفاض ال SNA رىدم ىل لوخدلا لجس ب قوطخلا.</u> <u>LDAP. ل ةىجراخلا ةمدخلا نىوكت فضاً .C ةوطخلا</u> <u>ثدحأ رادصا وأ 7.2 رادص الا</u> SNA <u>7.1 رادص ال SNA</u> <u>لى وختلا تادادعا نى وكت. D قوطخلا.</u> <u>يلحملا ضيوفتلا</u> LDAP ربع دعت نع ليوخت<u>اا</u> <u>ةحصلا نم ققحتلا</u> <u>اهحالصاو ءاطخاْلا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

ەمدقملا

اقباس فورعملا) ةنمآلا ةكبشلا تاليلحت ريدمل يساسألا نيوكتلا دنتسملا اذه فصي عمو ،ةيجراخلا ةقداصملا مادختسال ثدحأ رادصإ وأ 7.1 رادصإلا (Stealthwatch ةرادإ زكرم مساب (LDAP) رادصإلا نم لوصولا طاقن عم يجراخلا ليوختلا مادختسال ،ثدحأ رادصإ وأ 7.2.1 رادصإلا.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- (Stealthwatch مساب اقباس ةفورعملا) Cisco نم ةنمآلا ةكبشلا تاليلحت •
- SSL و ةماعلا LDAP ةيلمع •
- ال ةماع قرادا Microsoft Active Directory

ةمدختسملا تانوكملا

ةيلاتان الما على الما عن الما الذه الما الما المولعما الما المات :

- Cisco Secure Network Analytics Manager (رادصإلا، SMC)، رادصإلا، SMC)، رادصإلا،
- Active Directory ل لاجملاب مَحْجت ةدجوك Windows Server 2016 نيوكت مت •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

نيوكتلا

ل ةمدختسملا SSL ةداهش ردصو AD لاجم مكحت ةدحو ىلاٍ لوخدلا لجس A. قوطخلا LDAP.

- نم **ليغشت** ددح ،ثدحأ رادصإ وأ Windows Server 2012 ليغشتلا ماظنل ةبسنلاب .1 قوطخلا عم عباتو **certim.msc** لخدأ مث ،"أدبا" ةمئاقلا
- الخدأ مث ،"أدبا" ةمئاقلا نم **ليغشت** ددح ،مدقألاا Windows Server تارادصإل ةبسنلاب .2 MMC.
- . **باذجنا ةلاز/ةفاضإ** ددح ،فلم ةمئاق نم.

. **ةفاضاٍ** رقنا مث ،**تاداەش** ددح ،ةحاتملا ةيفاضإلا تاودألا ةمئاق نم .4

n-in Ve				
pin ve	endor	^	Console Root	Edit Extensions
Active Directory Do	icrosoft Cor			Damana
Active Directory Site Mi	icrosoft Cor			Remove
Active Directory Use Mi	icrosoft Cor			
ActiveX Control Mi	icrosoft Cor			Move Up
ADSI Edit Mi	icrosoft Cor			
Authorization Manager Mi	icrosoft Cor			Move Down
Certificate Templates Mi	icrosoft Cor		Add >	
Certificates Mi	icrosoft Cor			
Certification Authority Mi	icrosoft Cor			
Component Services Mi	icrosoft Cor			
Computer Managem Mi	icrosoft Cor			
Device Manager Mi	icrosoft Cor			
Disk Management Mi	icrosoft and			Advanced
	<u> </u>	~		Auvanceu
- Maran				
intion:				

- .ي**لاتلا** ددح مث ،**رتويبمكلا باسح** ددح ،**تاداەشلل ةيفاضإلا ةادألا** ةذفان يف .5
- . **ءاەناٍ** ددح مث ،اددحم **يلحملا رتويبمكلا** كرتأ.
- . قضاوم ددح ،**ةيفاضإ ةادأ ةلاازإ وأ ةفاضإ** ةذفان يف.
- **تاداەشلا < يصخش < (يلحملا رتويبمكلا) تاداەشلا** ىلا لقتنا .8



9. سواملا رزب رقناو لاجملاب مكحتلا ةدحو ىلع LDAP ةقداصمل ةمدختسملا SSL ةداهش ددح. **حتف** قوف نميألا.

يلاتلا < فلم ىلإ خسن قوف رقنا **< ليصافت** بيوبتلا ةمالع ىلإ لقتنا .10

💼 Certi	ficate			×
General	Details	Certification P	ath	
Show:	<all></all>		~	
Field Ver Sig Sig Sig Val	rsion rial numbe nature al nature ha uer id from id to hiect	er gorithm ash algorithm	Value	
I			Edit Properties	Copy to File
				ОК

يلاتلا قوف رقناو **صاخلا حاتفملا ريدصتب مقت ال ،ال** ديدحت نم دكأت .11

.ك**لذ دعب** رقناو Base-64 ل زمرملا X.509 قيسنت ددح .12

Export File Format				
Certi	icates can be exported in a variety of file formats.			
Selec	t the format you want to use:			
0	DER encoded binary X.509 (.CER)			
0	Base-64 encoded X.509 (.CER)			
0	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)			
	Include all certificates in the certification path if possible			
	Personal Information Exchange - PKCS #12 (.PFX)			
	Include all certificates in the certification path if possible			
	Delete the private key if the export is successful			
	Export all extended properties			
	Enable certificate privacy			
	Microsoft Serialized Certificate Store (.SST)			

.**يلاتلا** قوف رقناو فلملا ةيمستب مقو ،ةداهشلا نيزختل اعقوم ددح .

File to Export			
Specify the name of the	e file you want to export		
Hie name:	LDAPSidcertifi	cate.cer	Browse

.ةلااسر ."ريدصتلا حجن" ىلع لوصحلا بجي ،"**ءاەن|** قوف رقنا .14

دامتعالا راسم بيوبتلا ةمالع ددح مث ،LDAPs يف ةمدختسملا ةداهشلا ىلإ دع .15.

.**ةداەشلا ضرع** قوف رقناو ةداەشلا راسم ىلعأ رذجلا قدصملا عجرملا ردصم ددح .16

Certificate	\times
General Details Certification Path	
Certification path	
View Certificate]
Certificate status:	
This certificate is OK.	
OK	

ةداەشلا ىلع تعقو يتلا رذجلا قدصملا عجرملا ةداەش ريدصتل 14-10 تاوطخلا ررك -17 قداصم يف ةمدختسملا LDAPs.

،تاقبطلا ددعتم CA يمره لسلست كب ةصاخلا رشنلا ةيلمعل نوكي نأ نكمي :**قظحالم** يف ةطيسولا تاداهشلا عيمج ريدصتل ءارجإلا سفن عابتا ىلإ جاتحت ةلاحلا هذه يفو نامضلا ةلسلس.

راسم يف رادصإ ةەج لكلو LDAP مداخل دحاو ةداەش فلم دوجو نم دكأت ،ةعباتملا لبق .18 (نكمأ نן) ةطيسولا تاداەشلاو رذجلا ةداەشلا).

📙 🛃 🥃 LDAPS certificates						- 0	×
File Home Share View							^ 🕐
Pin to Quick access Copy Paste Copy path Paste shortcut Paste shortcut	Move Copy to*	New item •	Properties	Select all Select none			
Clipboard	Organize	New	Open	Select			
← → ∽ ↑	LDAPS certificates				~ Ö	Search LDAPS certificates	P
^ Name	Da	te modified Type	Size				
LDAPS_Root	CA 11,	/25/2021 11:46 Security	Certificate 3	KB			
LDAPSidcert	ificate 11,	/24/2021 7:59 PM Security	Certificate 3	KB			

ةلسلسو LDAP مداخ ةداهش ةفاضإل SNA ريدم ىلإ لوخدلا لجس .ب ةوطخلا

رذجلا.

- 1. نوزخملا < **ةيزكرملا ةرادإلا** ىلإ لقتنا.
- . **زاهجلا نيوكت ريرحت < تاءارجإ** قوف رقناو SNA ةرادإ زاهج عقوم ددح.
- .د**يدج ةفاضإ < ةقثلاً نزخم < "نيوكتلا" ةمئاق** ىلإ لقتنا ،"زاهجلاً نيوكت" ةذفان يف .3
- قوف رقنا مث ،LDAP مداخ صيخرت ددحو **فلم رايتخإ** قوف رقنا ،فولأملا مسالا بتكا .4 .**قداهش ةفاضإ**
- نإ) ةطيسولا تاداەشلاو رذجلا قدصملا عجرملا ةداەش ةفاضإل ةقباسلا ةوطخلا رركً .5 ننإ).
- قي الم ت قرف رقناو ةحيحصلا تاداهشلا يه اهليمحت مت يتلا تاداهشلا نأ نم ققحت .6 تادادع [لا

cisco	Stealthw	atch Central Mana	igement App	iance Manager	Update Manager	App Manager	Smart Licensing			۲
Inventory	Appliance Config	Appliance Config Appliance Netwo	guration – SMC	0001 2000 PACIN					Cancel Apply Settings Configuration Menu	
		Trust Store Mod	fied						Add New	
		FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS	
		-	The second						Delete	
		LDAP-Server	angelort-ad-	angelort-RootCA	2		-		Delete	
		LDAP-server-RootCA	angelort-RootCA2	angelort-RootCA	2	-	-		Delete	
		10 Certificates								
		Revert								

7. "ريدملا" ةلااح **عفر** متي ىتحو تارييغتلا قيبطت متي ىتح رظتنا".

LDAP. ل ةيجراخلا ةمدخلا نيوكت فضأ .C ةوطخلا

ثدحأ رادصإ وأ 7.2 رادصإلا SNA

. **مدختسملا قراداٍ < قماعلا تادادعإلاا** ىلإ لقتناو ريدملل ةيسيئرلاا تامولعملا ةحول حتفا.

cisco Stealthwatch	Dashboards • Monitor • Analyze •	Jobs * Configure * Deploy *		 ▲
				Global Settings
Security Insight Dashboard Inside Hosts				Central Management
				SMC Configuration
Alarming Hosts 💿				Packet Analyzer Configuration
				UDP Director Configuration
				External Lookup Configuration
				Juser Management
A.4.			dia.	SecureX Configuration
				Select Language

- 2. ضيوفتلاو ةقداصملا بيوبتلا ةمالع ددح ،مدختسملا ةرادا ةذفان يف.
- .**ةقداصملا ةمدخ < ءاشناٍ** قوف رقنا .3

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy •		9 ք 🔅 🛨
User Management			
Users Data Roles Authentication and Authorization			Create ~
			Data Role
Name	∧ Description	Authentication Type Remote Authorization	Authentication Service
Ex. local	Filter Authentication Service Description	Ex. LOGAL V	
	There is no data to display		
10 v Items per page		I e - e	1/1>>

4. ددح **ةقداصملا ةمدخ** ةلدسنملا ةمئاقلا نم LDAP.

.ةبولطملا لوقحلا لمكأ .5

لقحلا فولأم مسا فصولا	تاظحالم تاظحالم ل امسا لخدأ مداخل افصو لخدأ من يف "(SAN) عوضوملل ليدبلا مسالا" لقح مداخ LDAP.
مداخلا ناونع	يوتحي (SAN) نيزختلا ةكبش لقح ناك اذإ • قح يف IPv4 ناونع لخدأف ،طقف IPv4 ناونع مداخلا ناونع SAN مسا ىلع يوتحي SAN لقح ناك اذإ • مداخلا ناونع لقح يف DNS مسا يوتحي (SAN) نيزختلا ةكبش لقح ناك اذإ • ألا ةميةلا مدختساف ،اعم IPv4 و DNS ميق
ذفنملا	ةجردملا. انمآلا LDAP لاصتال صصخملا ذفنملا لخدأ. اول طاقنل اديج فورعملا TCP ذفنم. 636. وه (LDAP) لقألا ىوتسملا نم خب لاصتالل مدختسملا مدختسملا فرعم لخدأ LDAP. لايبس يلع cn=admin،ou=Corpo Users،dc=example،dc=com
مدختسملا طبر	ةفاضإب تمق دق تنك اذإ : قظحالم ىلع) ةنمضم AD ةيواح ىلإ نيمدختسملا نأ بجيف ،("نومدختسملا" ،لاثملا ليبس مسالا N لي في العام ل نوكي مضملا دلجملا ىلإ نيعملا (CN) ينوناقلا مضملا دلجملا ىل انيعملا (CN) ينوناقلا DC=domain، DC=com) ،لاثملا ليبس ىلع DC=domain، DC=com) ، تمق اذإ ،كلذ عمو نمديدج ةيواح ىلإ نيمدختسملا ةفاضإب DC اليبس ىلع) ديدجلا ةيواحلا مسا ىلع CN=username، OU=Corporate Users، DC=domain، DC=com).
	وا عدوث عليات قدوف مليا قير طليا وردحا فظحاليم

ىلع روثعلل ةديفملا قرطلا ىدحإ :**ةظحالم** نع مالعتسالا يه طبرلا مدختسمل طبرلا

	ذلبا Windows مراخ ىلع Active Directory ةمردخ صحلل .Active Directory مراخب لاصتا هيدل ماوا هجوم حتف كنكمي ،تامولعملا هذه ىلع Windows رمألا ةباتكو dsquery user dc= <distinguished>،dc=<name <use<br="">dc=<distinguished>،dc=<name <use<br="">to a c=dc=<distinguished> dc=<distinguished>،dc=<name <use<br="">dc=com -name user1 be com -name user1. لي م قجيتنل dc=example، dc=com"</name></distinguished></distinguished></name></distinguished></name></distinguished>
رورم∪ا ةملك	ةمدختسملا مدختسملا طبر رورم ةملك لخدأ LDAP. مداخب لاصتالل (DN) ذي مما ا مساليا ليخدأ
ةيساسألا تاباسحلا	نأ بجي يذلا ليلدلا عرف ىلع DN قيبطت متي اغ .نيمدختسملا نع ثحبلا تايلمع هيف أدبت نكمي نكلو ،(كلاجم) ليلدلا ةرجش ىلعأ نوكي بجي .ليلدلا لخاد ةيعرف ةرجش ديدحت اضيأ لا نيمدختسملاو طبرلا مدختسم ىلإ لوصولا .ةيساسألا تاباسحلا نم مهتقداصم .DC=Example،DC=com

.**ظفح** قوف رقنا .6

CISCO Stealthwatch Dashboards Monitor Analyze Jobs	Configure * Deploy * Q 🛓 🌣 🛓
Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.	
User Management Authentication Service	Cancel Save
* = Required	
Friendly Name *	Authentication Service
angelort LDAP server	LDAP V
Description *	Port *
Main AD server	636
Server Address 0 *	Bind User 0 *
angelort-ad-	CN=: ,OU=SNA,OU=Cisco,DC=zitro: ,DC=local
Certificate Revocation	Base Accounts 0 •
Disabled	DC=zitro: ,DC=local
Descend 1	Confere Descurved
Passwora -	Connim Password -

اهب قوثوملا نزخملا ىلا اهتفاضا تمت يتلا تاداهشلاو اهلاخدا مت يتلا تادادعإلا تناك اذا .7 "حاجنب اهتيرجأ يتلا تارييغتلا ظفحب تمق دقل" راعش ىلع لوصحلا بجيف ،ةحيحص.

8. ضيوفتلاو ةقداصملا < مدختسملا قرادا تحت ەنيوكت مت يذلا مداخلا ضرع بجي.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy •		9 🔳 🌣 🛨
User Management			
Users Data Roles Authentication and Authorization			Create 🗸
Name	∧ Description	Authentication Type	Remote Authorization Actions
Ex. local	V Filter Authentication Service Description	Ex. LOCAL ~	
angelort LDAP server	Main AD server	LDAP	
10 v Items per page			1 - 1 of 1 items $ \langle -\langle 1 \rangle / 1 \rangle \rangle$

7.1 رادصإلI SNA

- .نوزخملا < **ةيزكرملا ةرادإلا** ىلا لقتنا .1
- .زاهجلا نيوكت ريرحت < تاءارجا قوف رقناو SMC زاهج عقوم ددح .2
- .**ديدج ةفاضإ < LDAP دادعإ < "نيوكتلا" ةمئاق** ىلإ لقتنا ،"زاهجلا نيوكت" ةذفان يف 3.
- .5 **ةقحاللا** ةوطخلا **وأ SNA نم 7.2 رادصإلا** يف حضوم وه امك ةبولطملا لوقحلا لمكأ .4

cisco Stealti Watch Central Wahayennen Appliance managen oppare managen Ap	h, uan militar
Invertery Appliance Configuration - SMC Appliance Network Services General	Cancel Apply Settings Configuration Menu ▼
LDAP Setup	Add New
FRENDLY NAME * angelort LDAP server	DESCRIPTION * Main AD server
SERVER ADDRESS * angelort-ad-	PORT * 636
CERTIFICATE REVOCATION * Disabled	BIND USER + CN==,OU=SNA,OU=Cisco,DC=zitrc,DC=local
PASSWORD *	CONFIRM PASSWORD *
DC=zltro,DC=local	
	Cancel Add

.**ةفاضإ** قوف رقنا. 5

.**تادادعإلاا قيبطت** قوف رقنا .6

7. نزخملا ىلا اەتفاضا تمت يتلا تاداەشلاو اەلاخدا مت يتلا تادادعالا نوكت نأ درجمب د**يق** زاەجلا ةلاح نوكت نأ بجيو Manager ىلع تارييغتلا قيبطت متي ،ةحيحص اەب قوثوملا ل**يغشتلا**.

ليوختلا تادادعإ نيوكت .D ةوطخلا.

،نيوكتلا اذه مادختساب .LDAP ربع دعب نع ليوختلاو يلحملا ليوختلا نم الك SNA معدي قصصخملا وأ ةنمضملا SNA راودأل AD مداخ نم LDAP تاعومجم نييعت متي.

يه LDAP ربع SNA ل ةموعدملا ضيوفتلاو ةقداصملا بيلاسأ :

- يلحملا ضيوفتلاو دعب نع ةقداصملا •
- (ثدحألا وأ SNA نم 7.2.1 رادصإلل طقف همعد متي) دعب نع ضيوفتلاو دعب نع ةقداصملا •

يلحملا ضيوفتلا

ىلع ةعباتملاب مق ،كلذ قيقحتل .ايلحم مەراودأو نيمدختسملا فيرعت بجي ،ةلاحلا ەذە يف يلاتلا وحنلا.

ا < **ءاشنا < نومدختسملا** بيوبتلا ةمالع قوف رقنا ،ىرخأ ةرم **مدختسملا ةرادا** ىلإ لقتنا .1 .مدختسملا.

2. ةمئاقلا نم ەنيوكت مت يذلا مداخلا ددحو LDAP مداخ عم ةقداصملل مدختسملا مسا ددح. **قوداصملا ةمدخ** قلدسنمل.

اهتقداصم درجمب ريدملا ىلع مدختسملا اهكلتمي نأ بجي يتلا تانوذألا فيرعتب مق .3 مداخ ةطساوب.

Stealthwatch Dashboards • Monitor • A	nalyze • Jobs • Configure • Deptoy •	Q 💶 🌣 🛨
er Management User		Cancel Save
User Name *	Authentication Service	
user20	angelort LDAP server V	
Full Name	Password 💿	Generate Descurred
		Generale Password
Email	Confirm Password	
*	Show Password	
Role Settings		
Primary Admin		
Data Role		
All Data (Read & Write)		
Nub Destant		
vien Desktop		
Web Roles Compare		
Configuration Manager Analyst Power Analyst		

LDAP ربع دعب نع ليوختلا

ةكبشلا تاليلحت نم 7.2.1 رادصإلا يف الوأ LDAP ربع دعب نع ضيوفتلاو ةقداصملا معد مت ةنمآلا.

LDAP. مادختساب دعب نع ليوختلا 7.1 رادصإلا معدي ال :**قظحالم**

متت ەنإف ،(ريدملا يف) ايلحم ەنيكمتو مدختسملا فيرعت مت اذإ ەنأ ىلإ ةراشإلا مەملا نمو يلي امك يە مدختسملا ديدحت ةيلمع .ايلحم ەليوخت متي نكلو ،دعب نع مدختسملا ةقداصم:

- مدختسم نع ريدملا ثحبي ،ريدملاب بيحرتلا ةحفص يف دامتعالا تانايب لاخدا درجمب .1 ددحملا مسالاب يلحم.
- نيوكت ةلاح يف) دعب نع ەتقداصم متت ،ەنيكمتو يلحم مدختسم ىلع روثعلا ةلاح يف .2 ەليوخت نكلو (اقبسم يلحم ضيوفتب LDAP لوكوتورب ربع دعب نع ةقداصملا ةيلحملا تادادعإلا مادختساب.
- مل) ايلحم مدختسملا ىلع روثعلا مدعو ،ەنيكمتو دعب نع ضيوفتلا نيوكت ةلاح يف .3 دعب نع ضيوفتلاو ةقداصملا نم لك ءارجإ متي ،(ەليطعت وأ ەنيوكت متي.

..t يه حاجنب دعب نع ةقداصملا نيوكت تاوطخ نإف ،ببسلا اذهلو

دعب نع ليوختلا مادختسا يف نوبغري نيذلا نيمدختسملا فذح وأ ليطعتب مق .D-1 ةوطخلا ايلحم مەفيرعت مت نكلو.

- . مدختسملا ةرادإ < ةماعلا تادادعإلا ىلإ لقتناو ريدملل ةيسيئرلا تامولعملا ةحول حتفا.
- ةقداصملا مادختسال مەدصق مت نيذلا (نيدوجوم اوناك اذا) نيمدختسملا ليطعتب مق .2
- .ايلحم مەنېوكت مت نكلو ،LDAP ربع دعب نع ضيوفتلاو

User Management

Us	ers Data Roles Authentication and	Authorization							Create ~
	User Name	Full Name	Primary Admin 🔵	Config Manager 🔵	Analyst 🔵	Power Analyst 📀	Data Role	Status	Actions
	Ex, jsmith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On	
	admin	Admin User	~				All Data (Read & Write)	C On	
	angelort	Angel Ortiz	~				All Data (Read & Write)	On	
	user20			\checkmark	~		All Data (Read & Write)	O off	

Microsoft AD. مداخ يف Cisco-Stealthwatch تاعومجم فيرعتب مق D-2. ةوطخلا

رورملا تاملك ديدجت متي ،LDAP يمدختسم ربع ضيوفتلاو ةيجراخلا ةقداصملل ةبسنلاب Cisco-Stealthwatch تاعومجم وMicrosoft Active Directory. تاعومجمو امداخ يف اهفيرعت متيس يتلا SNA، اهيلع يوتحي يتلا ةفلتخملا راودألاب ةطبترم AD مداخ يف اهفيرعت متيس يتلا يلاتال وحنلا يلع اهفيرعت بجيو.

SNA رود	ةعومجملا (ءامسأ) مسا
يساسألا لوؤسملا	 Cisco-Stealthwatch-master-admin
	 Cisco-Stealthwatch-all-data-read-and-write
	 Cisco-Stealthwatch-all-data-read-only
	• Cisco-Stealthwatch- <custom> (يرايتخإ)</custom>
تانايبلا رود	
	تانايبلا راودأ تاعومجم نأ ٻم دكأت : ةظحالم
	."-Cisco-Stealthwatch" ب ادبت ةصصخملا
	 cisco-stealthwatch-configuration-manager
ېيولل يفيظولا رودلا	ت Cisco-Stealthwatch ةقاط للحم •
	• ل Cisco-Stealthwatch
	 Cisco-Stealthwatch-Desktop-Stealthwatch-po
	user
	• نيوكت ريدم Cisco-stealthwatch-desktop- configuration
	 cisco-stealthwatch-desktop-network-engineer
ويستلابها استبوعيه لابلا وفيعظوا ارودا	isco-Stealthwatch-Desktop نامأ للحم •
	• Cisco-Stealthwatch-Desktop- <custom> (إيتخإ</custom>
	بيظولا راودألا تاعومجم نأ نم دكأت : قظحالم Cisco" ب أدبت بتكملا حطسل ةصصخملا
	Stealthwatch-desktop-".

File Action View Help										
⊨ ⇒ 2 📰 🔏 📋 🗙 🖾 @ 🔒 🛛 🖬 🐍 📚 🛅 🔻 🛛 🍇										
Active Directory Users and C	Name	Туре	Descriptior	^						
> Saved Queries	🕮 cisco-stealthwatch-all-data-read-and-write	Security Group								
A durin	🕰 cisco-stealthwatch-all-data-read-only	Security Group								
> Admin	🏨 cisco-stealthwatch-analyst	Security Group								
> Builtin	acisco-stealthwatch-configuration-manager	Security Group								
	🕮 cisco-stealthwatch-custom1	Security Group								
and the second se	🎕 cisco-stealthwatch-desktop-configuration-manager	Security Group								
	🕰 cisco-stealthwatch-desktop-custom1	Security Group								
SNA	🕮 cisco-stealthwatch-desktop-network-engineer	Security Group								
> 🧮 Computers	🕰 cisco-stealthwatch-desktop-security-analyst	Security Group								
> 📓 Domain Controllers	🕰 cisco-stealthwatch-desktop-stealthwatch-power-user	Security Group								
> 📔 ForeignSecurityPrinci	🎕 cisco-stealthwatch-master-admin	Security Group								
> 📔 Managed Service Acc 🗸	disco-stealthwatch-power-analyst	Security Group		~						
< >	<		>							

×

رودلا"و "تانايبلا رود" ل ةصصخملا تاعومجملا معد متي ،اقبسم حضوم وه امك :**قظحالم** قلسلسلاب اقبسم ادهمم ةعومجملا مسا ناك املاط "يبتكملا رتويبمكلل يفيظولا مداخو SNA قرادا نم لك يف قصصخملا تاعومجملاو راودألا هذه ديدحت بجي .قبسانملا Active Directory. صصخم رود فيرعتب تمق اذا ،لاثملا ليبس ىلع .Cisco-Stealthwatch-Desktop-Custom1 يفرادا يف ،بتكم حطس ليمع رودل SNA

.نيمدختسملل LDAP ليوخت ةعومجم تانييعت ديدحت .D-3 ةوطخلا

Active Directory Users and Computers

نيذلاا نيمدختسملاا نييعت اننكمي ،AD مداخ يف *Cisco-Stealthwatch* تاعومجم ديدحت درجمب وحنلا ىلع كلذب مايقلا بجيو .ةيرورضلا تاعومجملا ىلإ SNA ريدم ىلإ لوصولا مەتين مت يلاتلا

user20 Properties				? ×							
Remote control	COM+										
General Address	Account	Profile	Telephones	Organization							
Member Of	Dial-in	Envi	ronment	Sessions							
Member of: Name Pri cisco-stealthwatch-m Domain Users	imary Admin laster-admin	1	Active Dire zitrosystem zitrosystem	ectory Doma ns.local/Cisc ns.local/Use							
< Add F	lemove	_		3							
Primary group: Do	Add Remove Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.										
0	K C	ancel	Apply	Help							

- عم رود لك نم ةعومجم ىلإ ،Primary Admin يمدختسم فالخب ،مدختسم لك نييعت بجي ةيلات اطورشلا.
- . **طقف ةدحاو ةعومجم** ىلإ مدختسملا نييعت بجي :**تانايبلا رود** .1
- .ل**قألاا ىلع ةدحاو ةعومجم** ىلإ مدختسملا نييعت بجي :**بيولل يفيظولا رودلا** .2

snauser10 Properties					?	×	
Remote control	Remote D	Remote Desktop Services Profile			COM+		
Member Of	Member Of Dial-in Environment						
Member of:							
Name			A	ctive D	Directory	D	
cisco-stealthwatch-a	I-data-read-an	d-write				il I	
cisco-stealthwatch-c	onfiguration-m	anager					
cisco-stealthwatch-d	esktop-configu	uration-mar	nager				
100.00						S. 1	
Data Ro Web Fu Desktop	le nctional Rol Functional	e Role					
<						>	
Add F	lemove						
Primary group: Do	omain Users					_	
Set Primary Group	There is n you have application	o need to o Macintosh ns.	change Prin clients or P	nary gro 'OSIX≺	oup unle complian	tss t	
0	< C	ancel	Apph	(He	slp	

SNA. ريدم ىلع LDAP ربع دعب نع ضيوفتلا نيكمتب مق .D-4 ةوطخلا

- . **مدختسملا قرادا < قماعلا تادادعإلاا** ىلإ لقتناو ريدملل ةيسيئرلا تامولعملا ةحول حتفا.
- 2. **ليوختلاو ةقداصملا** بيوبتلا ةمالع ددح **مدختسملا ةرادإ** راطإ يف.
- 3. **قوطخلا** يف اەنيوكت مت يتلا LDAP ةقداصم ةمدخ عقوم ددح **C**.
- . **دعب نع ضيوفتلا نيكمت<تاءارجإ** قوف رقنا .4

ةمدخ دوجو ةلاح يف **.ةرم لك يف طقف ةدحاو ةيجراخ ليوخت ةمدخ مادختسا نكمي :ةظحالم** ،ةديدجلا ةمدخلا نيكمتو ايئاقلت اهليطعت متي ،لعفلاب مادختسالا ديق ىرخأ ليوخت ةمدخلا مادختساب مهليوخت مت نيذلا نيمدختسملا عيمج جورخ ليجست متي كلذ عمو .ءارجإ يأ ذيفنت لبق ديكأت ةلاسر ضرع متي .ةقباسلا ةيجراخلا

Use	er Manager	ment						
Us	ers Data	Roles	Authentication and Authorization					
	Name			^	Description	Authentication Type	Remote Authorization	Actions
μ	Ex. local			~	Filter Authentication Service Description	Ex. LOCAL		
	angelort LDAP s	server			Main AD server	LDAP	~	

ةحصلا نم ققحتلا

AD. مداخ ىلع ةددحملا دامتعالا تانايب مادختساب لوخدلا ليجست نيمدختسملل نكمي

-1	cisco	1
	Welcome user20 K	
	This is your first time logging in. There were 0 failed attempt(s) since the account was created.	
	Sign In	

مدختسملا لعج مت ،لاثملا اذه يف .ضيوفتلاب قلعتت يەف ةيناثلا ققحتلا ةوطخ امأ "user20 مداخ يف AD، مداخ يف *Cisco-stealthwatch-master-admin* قعومجم يف اوضع "user20 نيمدختسملا يف مدختسملا فيرعت متي مل ."يساسألا لوؤسملا" تانوذأ هيدل مدختسملا AD، مداخ ةطساوب اهلاسرا مت ليوختلا تامس نأ ديكأت اننكمي اذل ،نييلحملا

cisco Stealthwatch =	Dashboards *	Monitor * Analyz	e • Jobs • Configu	re • Deploy •			Q	1 0 ±
User Management							Online Help	_
Users Data Roles Authenticatio	n and Authorization						Resources	Create 🗸
×							Logout	
User Name	Full Name	Primary Admin 🌖	Config Manager 🕘	Analyst 😑	Power Analyst 😗	Data Role	Status	Actions
Ex. jsmlth	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On	
admin	Admin User	~				All Data (Read & Write)	💽 On 🥈	
10 V items per page						1 - 1 of 1 items	< 1 / 1	> >1

ديكأت اننكمي ."Snauser10" لـاثملاا اذه يف رخآلا مدختسملل ققحتلا سفن ءارجإ متيو مداخ ىلع اەنيوكت مت يتلا دامتعالا تانايب مادختساب ةحجانلا ةقداصملا



،"يساسألا لوؤسملا" ةعومجم ىلإ يمتني ال مدختسملا اذه نأل ارظن ،ضيوفتلا نم ققحتلل، تازيملا ضعب رفوتت ال.

cisco Stealthw	atch		Dashboards • N	fonitor * Analyze *	Jobs * Configure	Deploy *				a 💶 🁸	<u>+</u>
										Global Settings	
Security Insight Da	ashboard Inside H	osts								SMC Configuration	
										Packet Analyzer Configuration	
Alarming Hosts 0										External Lookup Configuration	1
Concern Index	Target Index	Recon	040	Exploitation	DDoS Source	DDoS Tarnot	Data Hoarding	Exfiltration	Poli	SecureX Configuration	
0		0	0						P OII	Select Language	
2	0	0	0	0	0	0	0	0		0	-
_											

اهحالصإو ءاطخألا فاشكتسا

يلي امم ققحتف حاجنب ةقداصملا ةمدخ نيوكت ظفح رذعت اذإ:

- . ريدملاب صاخلا نامضلا نزخم ىلا DAP مداخل ةبسانملا تاداهشلا ةفاضإب تمق دقل .1
- "(SAN) عوضوملل ليدبلا مسالا" لقح يف ددحم وه امك وه هنيوكت مت يذلا **مداخلا** ناونع .2 ،طقف IPv4 ناونع ىلع يوتحي (SAN) نيزختلا ةكبش لقح ناك اذإ .LDAP مداخ ةداهشب لخدأف ،DNS مسا ىلع يوتحي SAN لقح ناك اذإ.مداخلا ناونع لقح يف IPv4 ناونع لخدأف ميق ىلع يوتحي (SAN) نيزختلا ةكبش لقح ناك اذإ.مداخلا ناونع لقح يف IPv4 و ميا ميق ىلع يوتحي (SAN) نيزختلا قكبش لقح ناك اذإ.مداخلا ناونع لقح يف IPv4 و ONS و DNS مسا
- ددحم وه امك ،ناحيحص امهنيوكت مت نيذللا **يساسألا باسحلاو طبرلا مدختسم** يلقح .3

AD. لاجملاب مكحتلا ةدحو ةطساوب

ةلص تاذ تامولعم

نم (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا ىجري ،ةيفاضإ ةدعاسم ىلع لوصحلل Cisco. مل عن من معد دقع مزلي . مل عن اعامناً عيمج يف Cisco معد لاصتا تامج.

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