Configuración de la Autenticación y Autorización Externas a través de LDAPS para el Acceso Secure Network Analytics Manager

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Configurar Paso A. Inicie sesión en el controlador de dominio AD y exporte el certificado SSL utilizado para LDAP. Paso B. Inicie sesión en el administrador SNA para agregar el certificado del servidor LDAP y la cadena raíz. Paso C. Agregue la configuración del servicio externo LDAP. SNA versión 7.2 o posterior SNA versión 7.1 Paso D. Configure los parámetros de autorización. Autorización local Autorización remota a través de LDAP Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe la configuración básica de una versión 7.1 o posterior de Secure Network Analytics Manager (anteriormente Stealthwatch Management Center) para utilizar la autenticación externa y, con la versión 7.2.1 o posterior, para utilizar la autorización externa con LDAPS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Network Analytics (anteriormente StealthWatch)
- Operación general LDAP y SSL
- Administración general de Microsoft Active Directory

Componentes Utilizados

La información de este documento se basa en estos componentes:

- Cisco Secure Network Analytics Manager (anteriormente SMC) versión 7.3.2
- Windows Server 2016 configurado como controlador de dominio de Active Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso A. Inicie sesión en el controlador de dominio AD y exporte el certificado SSL utilizado para LDAP.

- 1. Para Windows Server 2012 o posterior, seleccione **Ejecutar** en el menú Inicio, luego ingrese **certIm.msc** y continúe con el paso **8**.
- 2. Para versiones anteriores de Windows Server, seleccione **Ejecutar** en el menú Inicio y, a continuación, introduzca **mmc**.
- 3. En el menú Archivo, seleccione Agregar o quitar ajuste.
- 4. En la lista Complementos disponibles, seleccione **Certificados** y, a continuación, haga clic en **Agregar**.

Add or Remove Snap-ins				×
You can select snap-ins for this co extensible snap-ins, you can conf	onsole from the	ose cten	available on your computer and configure the selected s nsions are enabled.	et of snap-ins. For
Available snap-ins:			Selected snap-ins:	
Snap-in Ven	ndor	^	Console Root	Edit Extensions
Active Directory Do Micr	rosoft Cor rosoft Cor			Remove
Active Directory Use Micr	rosoft Cor rosoft Cor			Move Up
Authorization Manager Micr	rosoft Cor rosoft Cor rosoft Cor		Add >	Move Down
Certificates Micr	rosoft Cor rosoft Cor			
Computer Managem Micr	rosoft Cor			
Disk Management Micr	rosoft and	~		Advanced
Description:				
The Certificates snap-in allows y	you to browse t	the	contents of the certificate stores for yourself, a service,	, or a computer.
				OK Cancel

5. En la ventana **del complemento Certificados**, seleccione **Cuenta de equipo** y, a continuación, seleccione **Siguiente**.

6. Deje el equipo local seleccionado y, a continuación, seleccione Finalizar.

7. En la ventana Agregar o quitar complemento, seleccione Aceptar.

8. Vaya a Certificados (equipo local) > Personal > Certificados

🚡 certIm - [Certificates - Local Computer\Personal\Certificates] - 🛛 🗙						
File Action View Help						
🗢 🔿 🙋 📷 🖌 🛍 🗙 🖼 😼 🛛 🖬						
Certificates - Local Computer A Issued To	Issued By	Expiration Date	Intended Purposes		Frie	
V Personal	angelort-RootCA2	11/25/2022	Client Authentication, S	erver Auth.	<n< td=""></n<>	
Certificates	approximity of	1.11.101	- 89		-	
> 📫 Enterprise Trust						
> 📔 Intermediate Certification						
> 🧮 Trusted Publishers						
> 🦳 Untrusted Certificates						
> 🧮 Third-Party Root Certifica						
> 🧮 Trusted People						
> 🧮 Client Authentication Issu						
> 🧮 Preview Build Roots						
> 📔 Remote Desktop						
> 📔 Certificate Enrollment Rec						
> 📔 Smart Card Trusted Roots						
> 📔 Trusted Devices						
> 📔 WebHosting						
Windowe Live ID Token lee					>	
Personal store contains 2 certificates.					-	

9. Seleccione y haga clic con el botón derecho del ratón en el certificado SSL utilizado para la autenticación de LDAPS en su controlador de dominio y haga clic en **Abrir**.

10. Vaya a la pestaña Detalles > haga clic en Copiar a archivo > Siguiente

💼 Certificate

General	Details	Certification	Path	
Show:	<all></all>		~	
Field Ser Sig Sig Sig Val	rsion nature al nature ha uer id from id to	er gorithm ash algorithm	Value	~
			Edit Properties	Copy to File
				ОК

11. Asegúrese de que No, no exporte la clave privada está seleccionado y haga clic en Siguiente

12. Seleccione Base-64 codificado X.509 format y haga clic en Next.

←	£.	Certificate	Export	Wizard
---	----	-------------	--------	--------

Export File Format

Certificates can be exported in a variety of file formats.

Base-64 encoded X.509 (.CER)	
) Cryptographic Message Syntax Standar	d - PKCS #7 Certificates (.P78)
Include all certificates in the certificates	ation path if possible
Personal Information Exchange - PKCS	#12 (.PFX)
Include all certificates in the certificates	ation path if possible
Delete the private key if the export	is successful
Export all extended properties	
Enable certificate privacy	
Microsoft Serialized Certificate Store (.S	ST)

13. Seleccione una ubicación para almacenar el certificado, asigne un nombre al archivo y haga clic en **Siguiente**.

e file you want to expo	rt	
LDAPSidcer	tificate.cer	Browse
	e file you want to expo	e file you want to export UDAPSidcertificate.cer

14. Haga clic en **Finalizar**, debe obtener una "La exportación se realizó correctamente". mensaje.

15. Vuelva al certificado utilizado para LDAPS y, a continuación, seleccione la pestaña **Ruta de certificación**.

16. Seleccione el emisor de CA raíz en la parte superior de la trayectoria de certificación y haga clic en **Ver certificado**.

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

17. Repita los pasos 10-14 para exportar el certificado de la CA raíz que firmó el certificado utilizado para la autenticación de LDAPS.

Nota: Su implementación puede tener una jerarquía de CA de varios niveles, en cuyo caso debe seguir el mismo procedimiento para exportar todos los certificados intermedios en la cadena de confianza.

18. Antes de continuar, asegúrese de tener un archivo de certificado para el servidor LDAPS y para cada autoridad emisora en la ruta de certificación: Certificado raíz y certificados intermedios (si procede).



Paso B. Inicie sesión en el administrador SNA para agregar el certificado del servidor LDAP y la cadena raíz.

- 1. Vaya a Administración central > Inventario.
- 2. Busque el dispositivo SNA Manager y haga clic en **Acciones > Editar configuración del dispositivo**.
- 3. En la ventana Configuración del dispositivo, navegue hasta **Menú de configuración >** Almacén de confianza > Agregar nuevo.
- 4. Escriba el nombre descriptivo, haga clic en **Elegir archivo** y seleccione el certificado del servidor LDAP y luego haga clic en **Agregar certificado**.
- 5. Repita el paso anterior para agregar el certificado de CA raíz y los certificados intermedios (si procede).
- 6. Verifique que los certificados cargados sean los correctos y haga clic en **Aplicar configuración**.

cisco	Stealthv	vatch Central Mana	igement Appl	lance Manager	Update Manager	App Manager	Smart Licensing			Θ
Inventory	/ Appliance Confi	Appliance Config Appliance Networ	guration - SMC	0001 2100 PMIN	-				Cancel Apply Settings Configuration Menu V	
		Trust Store Mod	fied						Add New 🔍	
		FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS	
		-	-						Delete	
		LDAP-Server	angelort-ad-	angelort-RootCA	2		-		Delete	
		LDAP-server-RootCA	angelort-RootCA2	angelort-RootCA	2		-		Delete	
		10 Certificates							1	
		Revert								

7. Espere a que se apliquen los cambios y a que el estado del jefe sea **Up**.

Paso C. Agregue la configuración del servicio externo LDAP.

SNA versión 7.2 o posterior

1. Abra el panel principal del jefe y navegue hasta **Configuración global > Administración de usuarios**.

cisco Stealthwatch	Dashboards * Monitor * Analyze * Jobs * Configure *	Deploy *	۹ ا ♦ ±
			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.		day.	SecureX Configuration
			Select Language

- 2. En la ventana Administración de usuarios, seleccione la ficha Autenticación y autorización.
- 3. Haga clic en **Crear > Servicio de autenticación**.

cisco S	tealthwatch	Dashboards • N	Monitor • Analyze •	Jobs *	Configure *	Deploy *				९ 💶 🌣 ±
User Man	agement									
Users	Data Roles Authentication and Authorization									Create ~
										User
										Data Role
Name		A Description					Authentication Type		Remote Authorization	Authentication Service
Ex. local	(V Filter Authent	tication Service Descript	lan			Ex. LOCAL	~		
				There is no	o data to display					
10	Y items per page								122	DUD D
10	Rems per page									

- 4. En el menú desplegable Servicio de autenticación seleccione LDAP.
- 5. Complete los campos obligatorios.

Campo	Notas
Nombre descriptivo	Ingrese un nombre para elLDAPserver.
Descripción	Introduzca una descripción para el servidor LDAF Introduzca el nombre de dominio completo segúr especificado en el campo Nombre alternativo del sujeto (SAN) del certificado del servidor LDAP. • Si el campo SAN contiene sólo la dirección II introduzca la dirección IPv4 en el campo Ser
Dirección del servidor	 Address (Dirección del servidor). Si el campo SAN contiene el nombre DNS, introduzca el nombre DNS en el campo Direc de servidor.
Puerto	 Si el campo SAN contiene valores DNS e IPo utilice el primer valor enumerado. Introduzca el puerto designado para la comunica LDAP segura (LDAP sobre TLS). El conocido pue TCP para LDAPS es 636. Introduzca el ID de usuario utilizado para conecta servidor LDAP. Por ejemplo: CN=admin,OU=Usu corporativos,DC=ejemplo,DC=com
Usuario de enlace	Nota: Si ha agregado usuarios a un contene AD integrado (por ejemplo, "Usuarios"), el D enlace del usuario de enlace debe tener el nombre canónico (CN) establecido en la car integrada (por ejemplo, CN=username, CN=Users, DC=domain, DC=com). Sin emb si ha agregado usuarios a un nuevo contene el DN de enlace debe tener la unidad organizativa (OU) configurada en el nuevo nombre del contenedor (por ejemplo, CN=username, OU=Corporate Users, DC=domain, DC=com).
	Nota: Una forma útil de encontrar el DN de enlace del usuario de enlace es consultar A

Directory en un servidor Windows que tenga conectividad con el servidor de Active Direct Para obtener esta información, puede abrir u símbolo del sistema de Windows y escribir e comando dsquery user dc=<distinguido>,dc=<nombre> -name <usuario>. Por ejemplo: dsquery user dc=example,dc=com -name user1. El resulta es como "CN=user1,OU=Corporate Users,DC=example,DC=com"
Introduzca la contraseña de usuario de enlace utilizada para conectarse al servidor LDAP. Introduzca el nombre distinguido (DN). El DN se aplica a la rama del directorio en la que

deben iniciarse las búsquedas de usuarios. A me es la parte superior del árbol de directorios (su dominio), pero también puede especificar un sub-

dentro del directorio. El usuario de enlace y los usuarios que se pretende autenticar deben estar

accesibles desde las cuentas base. Por ejemplo: DC=ejemplo,DC=com

Cuentas base

Contraseña

6. Click Save.

Dashboards • Monitor • Analyze • Job	s • 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 🌒 *	Bind User 👔 🔹
angelort-ad-	CN=sOU=SNA,OU=Cisco,DC=zitrosDC=local
Certificate Revocation 📀 *	Base Accounts 📀 •
Disabled	DC=zitrosDC=local
Password *	Confirm Password *

7. Si la configuración introducida y los certificados agregados al almacén de confianza son correctos, debe conseguir un banner que diga "Ha guardado correctamente los cambios".

8. El servidor configurado debe mostrarse en **User Management > Authentication and Authorization**.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy •		< ⊥ ☆ ±
User Management			
Users Data Roles Authentication and Authorization			Create ~
Name	∧ Description	Authentication Type	Remote Authorization Actions
Ex. local	Filter Authentication Service Description	Ex. LOCAL V	
angelort LDAP server	Main AD server	LDAP	
10 v items per page			1 - 1 of 1 items < < 1 / 1 > >

SNA versión 7.1

- 1. Vaya a Administración central > Inventario.
- 2. Busque el dispositivo SMC y haga clic en Acciones > Editar configuración del dispositivo.
- 3. En la ventana Configuración del dispositivo, navegue hasta **Menú de configuración > Configuración LDAP > Agregar nuevo**.
- 4. Complete los campos obligatorios tal y como se describe en el paso 5 de SNA versión 7.2 o posterior.

cisco Stealthwa	atch Central Management Appliance Manager Update Manager	App Manager	•
Inventory : Appliance Configu	Appliance Configuration - SMC Appliance Network Services General		Cancel Apply Settings Configuration Menu 🔻
	LDAP Setup		Add New
	Add LDAP FREHDLY NAME * angelort LDAP server SERVER ADDRESS * angelort-ad- CERTIFICATE REVOCATION * Disabled ADDRESS ADDRESS CERTIFICATE REVOCATION * Disabled CERTIFICATE REVOCATION * Disabled CERTIFICATE REVOCATION * Disabled CERTIFICATE REVOCATION * Disabled CERTIFICATE REVOCATION * * CERTIFICATE REVOCATION * CERTIFICATION * CERTIFICATION * CERTIFICATION * CERTIFICATION * CERTIFICATION * * * CERTIFICATION * * * * * * * * * * * * *	DESCRIPTION * Main AD server PORT * 636 BIND USER @ * CN====;OU=SNA_OU=Cisco,DC=zitrc==,DC=local CONFIRM PASSWORD * 	Cancel

- 5. Haga clic en Add (Agregar).
- 6. Haga clic en Aplicar configuración.

7. Una vez que la configuración introducida y los certificados agregados al almacén de confianza son correctos, se aplican los cambios en el administrador y el estado del dispositivo debe ser **Up**.

Paso D. Configure los parámetros de autorización.

SNA admite autorización local y remota a través de LDAP. Con esta configuración, los grupos LDAP del servidor AD se asignan a funciones SNA integradas o personalizadas.

Los métodos de autenticación y autorización soportados para SNA vía LDAP son:

• Autenticación remota y autorización local

 Autenticación remota y autorización remota (solo compatible con SNA versión 7.2.1 o posterior)

Autorización local

En este caso, los usuarios y sus funciones deben definirse localmente. Para lograrlo, proceda como se indica a continuación.

1. Navegue de nuevo a User Management, haga clic en la pestaña Users > Create > User.

2. Defina el nombre de usuario para autenticarse con el servidor LDAP y seleccione el servidor configurado en el menú desplegable **Servicio de autenticación**.

3. Defina los permisos que el usuario debe tener sobre el administrador una vez que haya sido autenticado por el servidor LDAP y haga clic en **Guardar**.

CISCO Stealthwatch Dashboards * Monitor * Analyze * Jobs * Configure * Deploy *	< ≰ \$ ±
User Management User	Cancel Save
User Name • Authentication Service 👉	
user20 angelort LDAP server V	
Full Name Password ()	
Generate Passw	rd
Email Confirm Password	
Show Password	
Role Settings	
Z Primary Admin	
Data Role	
All Data (Read & Write) 🗸	
Web Desktop	
Web Roles Compare	
Configuration Manager Analyst Power Analyst	

Autorización remota a través de LDAP

La autenticación y autorización remotas a través de LDAP fue admitida por primera vez en Secure Network Analytics versión 7.2.1.

Nota: La autorización remota con LDAP no se soporta en la versión 7.1.

Es importante mencionar que si un usuario se define y se habilita localmente (en el Administrador), el usuario se autentica de forma remota, pero se autoriza localmente. El proceso de selección del usuario es el siguiente:

- 1. Una vez introducidas las credenciales en la página de bienvenida del jefe, éste busca un usuario local con el nombre especificado.
- 2. Si se encuentra un usuario local y está habilitado, se autentica remotamente (si la autenticación remota a través de LDAP con autorización local se configuró previamente)

pero se autoriza con la configuración local.

3. Si se configura y habilita la autorización remota y el usuario no se encuentra localmente (no está configurado o desactivado), tanto la autenticación como la autorización se realizan de forma remota.

Por esta razón, los pasos para configurar correctamente la autenticación remota son t..

Paso D-1. Desactive o elimine los usuarios que pretendan utilizar la autorización remota pero que se definan localmente.

- 1. Abra el panel principal del jefe y navegue hasta Configuración global > Administración de usuarios.
- 2. Desactive o elimine los usuarios (si existen) que pretenden utilizar la autenticación y autorización remotas a través de LDAP, pero que están configurados localmente.

030	a management								
U	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)	O n	
	angelort	Angel Ortiz	~				All Data (Read & Write)	On	
	user20			~	~		All Data (Read & Write)	Off Off	

Paso D-2. Defina los grupos cisco-stealthwatch en el servidor de Microsoft AD.

Para la autenticación y autorización externas a través de usuarios LDAP, las contraseñas y los grupos *cisco-stealthwatch* se definen remotamente en Microsoft Active Directory. Los grupos *cisco-stealthwatch* que se definirán en el servidor AD están relacionados con las diferentes funciones que tiene SNA, deben definirse de la siguiente manera.

Función SNA	Nombre del grupo
Admin principal	 cisco-stealthwatch-master-admin
	 cisco-stealthwatch-all-data-read-and-write
	 Cisco-stealthwatch-all-data-read-only
	 cisco-stealthwatch-<custom> (opcional)</custom>
Función de datos	Nota: Asequírese de que los grupos de funci
	de datos personalizados empiecen por "ciso stealthwatch-".
	 Cisco-stealthwatch-configuration-manager
Función Web	 cisco-stealthwatch-power-analyst
	 cisco-stealthwatch-analyst
	 cisco-stealthwatch-desktop-stealthwatch-pov user
	 cisco-stealthwatch-desktop-configuration-ma
Función funcional dal appritaria	 Cisco-stealthwatch-desktop-network-Engine
Funcion funcional del eschiono	 cisco-stealthwatch-desktop-security-analyst
	 cisco-stealthwatch-desktop-<custom> (opcio</custom>
	Nota: Asegúrese de que los grupos de funci

Active Directory Users and Computers -					
File Action View Help Image: Second s] 🛯 🖻 🛛 🗊 🗏 📚 🛅 🍸 💆 🍇				
Active Directory Users and Co Saved Queries Admin Admin Builtin Cisco SNA SNA Computers Domain Controllers ForeignSecurityPrinci Managed Service Acc	Name Cisco-stealthwatch-all-data-read-and-write Cisco-stealthwatch-all-data-read-only Cisco-stealthwatch-analyst Cisco-stealthwatch-configuration-manager Cisco-stealthwatch-custom1 Cisco-stealthwatch-desktop-configuration-manager Cisco-stealthwatch-desktop-custom1 Cisco-stealthwatch-desktop-network-engineer Cisco-stealthwatch-desktop-security-analyst Cisco-stealthwatch-desktop-stealthwatch-power-user Cisco-stealthwatch-desktop-stealthwatch-power-user Cisco-stealthwatch-desktop-stealthwatch-power-user Cisco-stealthwatch-desktop-stealthwatch-power-user Cisco-stealthwatch-desktop-stealthwatch-power-user	Type Security Group Security Group	Descriptior ^		
			,		

Nota: Como se ha descrito anteriormente, los grupos personalizados se admiten para "Función de datos" y "Función funcional de escritorio" siempre que el nombre del grupo vaya precedido de la cadena adecuada. Estas funciones y grupos personalizados deben definirse tanto en el administrador SNA como en el servidor de Active Directory. Por ejemplo, si define una función personalizada "custom1" en el Administrador SNA para una función de cliente de escritorio, se debe asignar a cisco-stealthwatch-desktop-custom1 en Active Directory.

Paso D-3. Definir asignaciones de grupo de autorización LDAP para los usuarios.

Una vez que los grupos *cisco-stealthwatch* se han definido en el servidor AD, podemos asignar los usuarios que pretenden tener acceso al administrador SNA a los grupos necesarios. Esto debe hacerse de la siguiente manera.

• Un usuario Admin principal debe estar asignado al grupo *cisco-stealthwatch-master-admin* y no debe ser miembro de ningún otro grupo de cisco-stealthwatch.

user20 Properties				? ×		
Remote control	COM+					
General Address	Account	Profile	Telephones	Organization		
Member Of	Dial-in	Envi	ronment	Sessions		
Member of:						
Name Pri	mary Admin		Active Dire	ectory Doma		
cisco-stealthwatch-m	aster-admin		zinsvelen	s local/Cisc		
Domaio Lisers	dater darini		simevelor	e local/Lise		
			<i>Larooyo</i> con			
<				>		
Add	lemnue					
700	icinove					
Primary group: Do	omain Users					
	There is n	o need to d	hance Primary o	roup unless		
Set Primary Group	you have	Macintosh	clients or POSIX	compliant		
	application	15.				
01	OK Cancel Apply					

- Cada usuario, que no sea el usuario Admin principal, debe estar asignado a un grupo de cada función con las siguientes condiciones.
- 1. Función de datos: El usuario debe estar asignado a sólo un grupo.
- 2. Función Web: El usuario debe estar asignado a al menos un grupo.
- 3. Función funcional del escritorio: El usuario debe estar asignado a al menos un grupo.

snauser10 Properties					?	×
Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dial-in Environment				COM+ Organization Sessions		
Member of:						
Name cisco-steathwatch-a cisco-steathwatch-o cisco-steathwatch-o Data Ro Web Fut Desktop	I-data-read-an onfiguration-m esktop-configu- esktop-configu- nctional Rol Functional	d-write anager rration-mar le Role	ager	Active	Directory	D
<						>
Add R Primary group: Do Set Primary Group	main Users There is n you have application	o need to o Macintosh 1s.	change Pr clients or	imary g POSIX	roup unle compliar	ess t
OF	(C	ancel	Αρς	sły	Н	elp

Paso D-4. Habilite la Autorización Remota a través de LDAP en el Administrador SNA.

- 1. Abra el panel principal del jefe y navegue hasta **Configuración global > Administración de usuarios**.
- 2. En la ventana Administración de usuarios seleccione la ficha Autenticación y autorización.
- 3. Localice el servicio de autenticación LDAP que se configuró en el Paso C.
- 4. Haga clic en Acciones > Habilitar autorización remota.

Nota: Sólo un servicio de autorización externo puede estar en uso a la vez. Si otro servicio de autorización ya está en uso, se inhabilita automáticamente y el nuevo se habilita; sin embargo, todos los usuarios autorizados con el servicio externo anterior se desconectan. Se muestra un mensaje de confirmación antes de que se realice alguna acción.

Us	er Man	agement							
U	lsers	Data Roles	Authentication and Authorization						
	Name			^	Description	Authentication Type	1	Remote Authorization	Actions
	Ex. local		~		Filter Authentication Service Description	Ex. LOCAL V	2		
	angelort l	DAP server			Main AD server	LDAP		~	

Verificación

Los usuarios pueden iniciar sesión con las credenciales definidas en el servidor AD.

	cisco	4
Welcome us	ser20	
This is your firs	t time logging in.	
There were 0 fa	iled attempt(s) since the account was created.	
		ОК
	Sign In	

El segundo paso de verificación se refiere a la autorización. En este ejemplo, el usuario "user20" se convirtió en miembro del grupo *cisco-stealthwatch-master-admin* en el servidor AD, y podemos confirmar que el usuario tiene permisos de administrador primario. El usuario no está definido en los usuarios locales, por lo que podemos confirmar que los atributos de autorización fueron enviados por el servidor AD.

cisco Stealthwatch	Dashboards *	Monitor * Analyze	 Jobs * Configure 	 Deploy • 			۹.	± ≎ ±
User Management							Online Help	
Users Data Roles Authentication and	Authorization						Resources	Create 🗸
							Logout	
User Name	Full Name	Primary Admin 🌖	Config Manager 🌖	Analyst 😗	Power Analyst 🌖	Data Role	Status Ac	tions
Ex. jsmith	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 >	e >i

La misma verificación se realiza para el otro usuario en este ejemplo "snauser10". Podemos confirmar la autenticación correcta con las credenciales configuradas en el servidor AD.



Para la verificación Autorización, dado que este usuario no pertenece al grupo Admin principal, algunas funciones no están disponibles.

1
1

Troubleshoot

Si la configuración del servicio de autenticación no se puede guardar correctamente, verifique que:

- 1. Ha agregado los certificados adecuados del servidor LDAP al almacén de confianza del administrador.
- 2. La dirección del servidor configurada es la especificada en el campo Nombre alternativo del sujeto (SAN) del certificado del servidor LDAP. Si el campo SAN contiene sólo la dirección IPv4, introduzca la dirección IPv4 en el campo Server Address (Dirección del servidor).Si el campo SAN contiene el nombre DNS, introduzca el nombre DNS en el campo Dirección de

servidor.Si el campo SAN contiene valores DNS e IPv4, utilice el primer valor enumerado.

3. Los campos **Bind User** y **Base Account** configurados son correctos, según lo especificado por AD Domain Controller.

Información Relacionada

Para obtener asistencia adicional, póngase en contacto con el Centro de asistencia técnica de Cisco (TAC). Se requiere un contrato de soporte válido: <u>Contactos de soporte a nivel mundial de Cisco.</u>