通过LDAPS为SNA Manager访问配置外部身份验证和授权

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 步骤A.登录到AD域控制器并导出用于LDAP的SSL证书
- 步骤B.登录到SNA Manager以添加LDAP服务器的证书和根链
- 步骤C.添加LDAP外部服务配置
  - SNA 7.2或更高版本
  - SNA 7.1版
- 步骤D.配置授权设置。
  - 本地授权
  - 通过LDAP进行远程授权

验证

故障排除

相关信息

简介

本文档介绍使用轻量级目录访问协议(LDAP)通过SSL的安全网络分析管理器的基本配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure Network Analytics（以前称为Stealthwatch）
- 常规LDAP和SSL操作
- 常规Microsoft Active Directory管理

使用的组件

本文档中的信息基于以下组件：

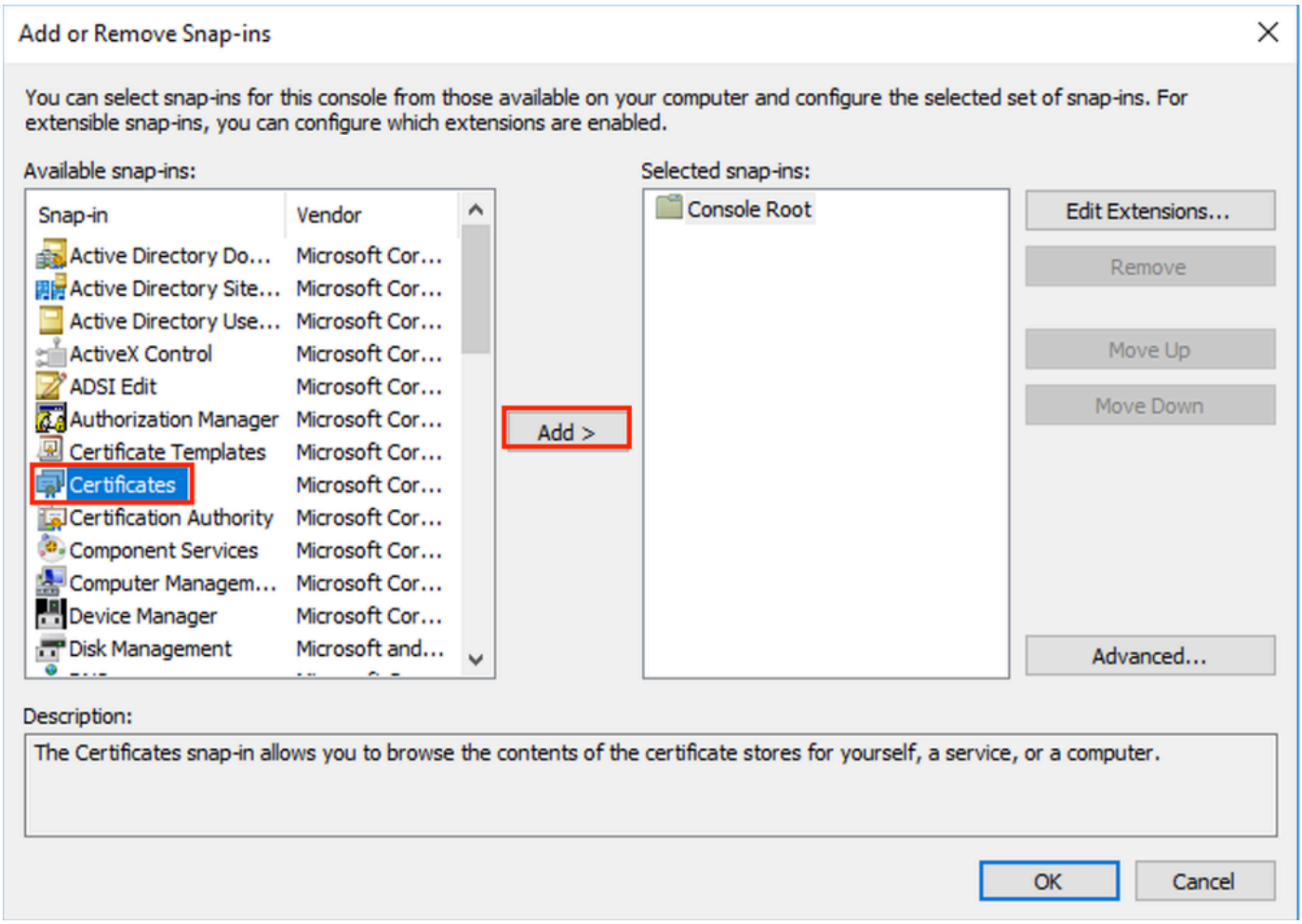
- 思科安全网络分析管理器（以前称为SMC）版本7.3.2
- 配置为Active Directory域控制器的Windows Server 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

步骤A.登录到AD域控制器并导出用于LDAP的SSL证书

1. 对于Windows Server 2012或更高版本，请从“开始”菜单中选择运行，然后输入certlm.msc并继续步骤8。
2. 对于较旧的Windows Server版本，从“开始”菜单中选择运行，然后输入mmc。
3. 从“文件”(File)菜单中，选择“添加/删除管理单元”(Add/Remove Snap In)。
4. 从Available snap-ins列表中，选择Certificates，然后单击Add。

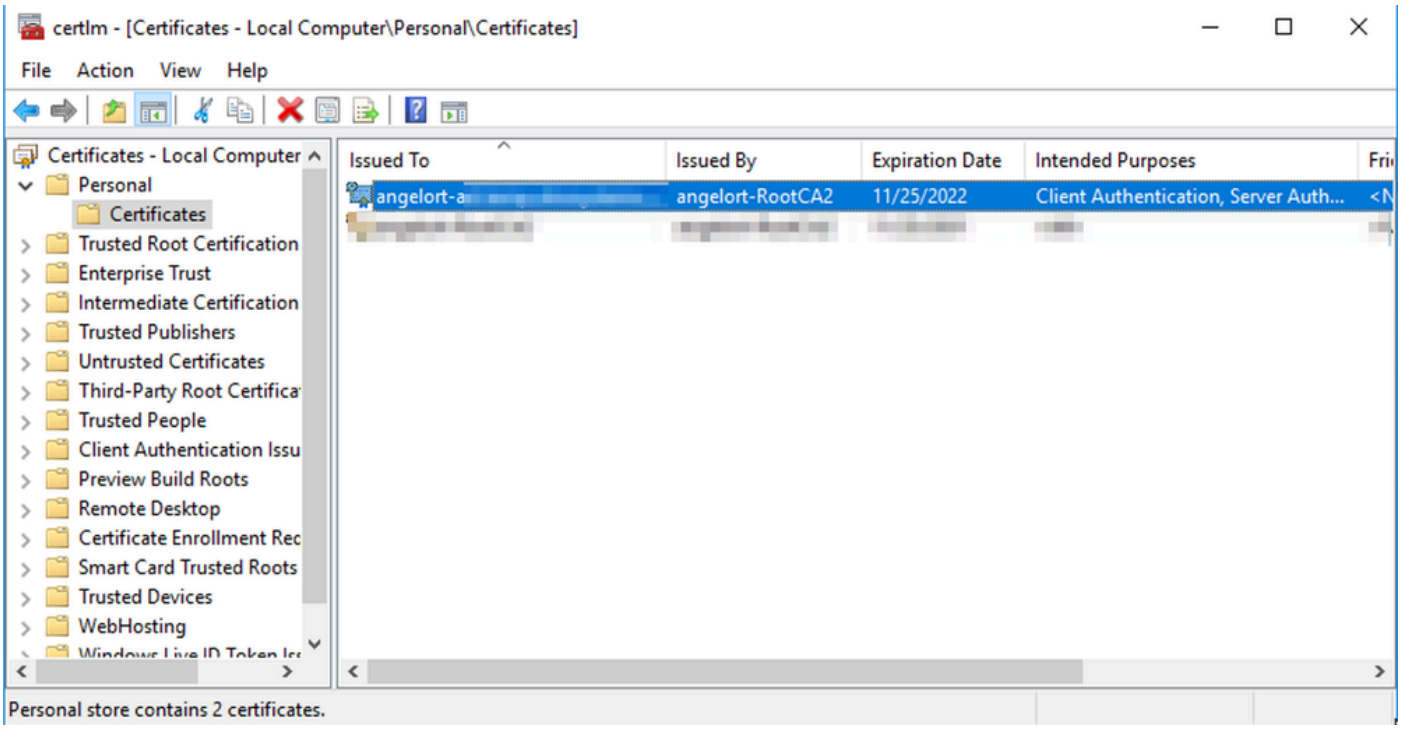


5.在证书管理单元窗口中，选择计算机帐户，然后选择下一步。

6.保持选中Local computer，然后选择Finish。

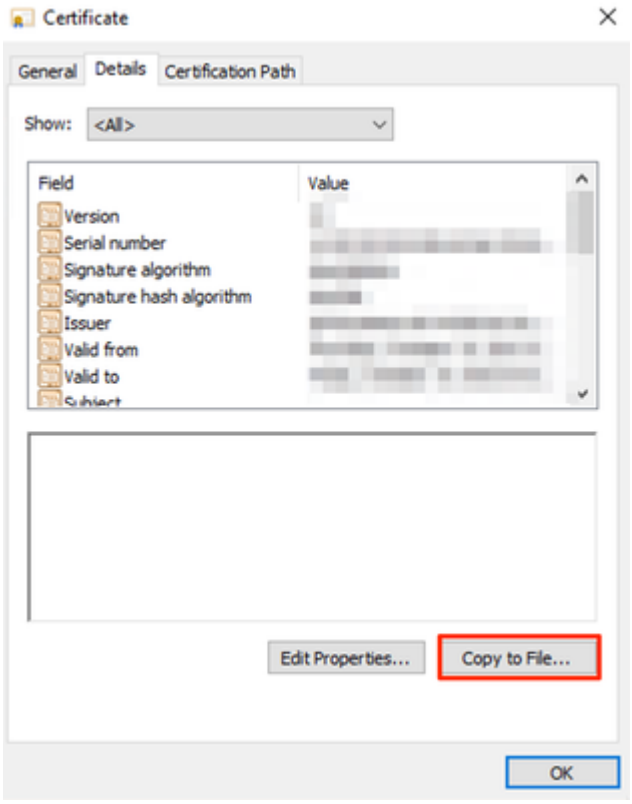
7.在“添加或删除管理单元”窗口中，选择确定。

8.导航到证书（本地计算机）>个人>证书



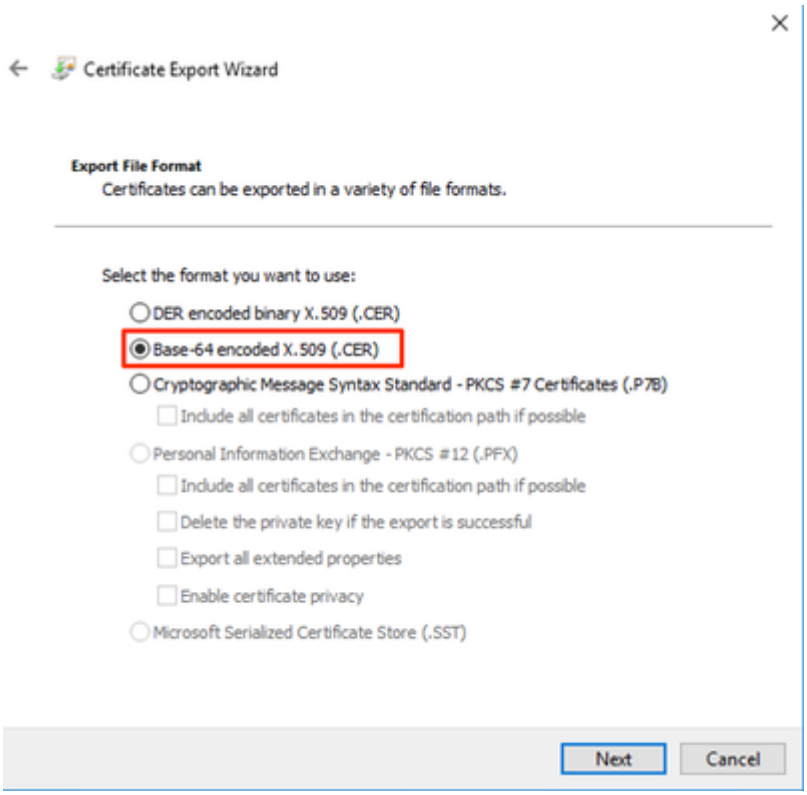
9.选择并右键单击域控制器上用于LDAPS身份验证的SSL证书，然后单击打开。

10.定位至“详细信息”选项卡>单击“复制到文件”>“下一步”

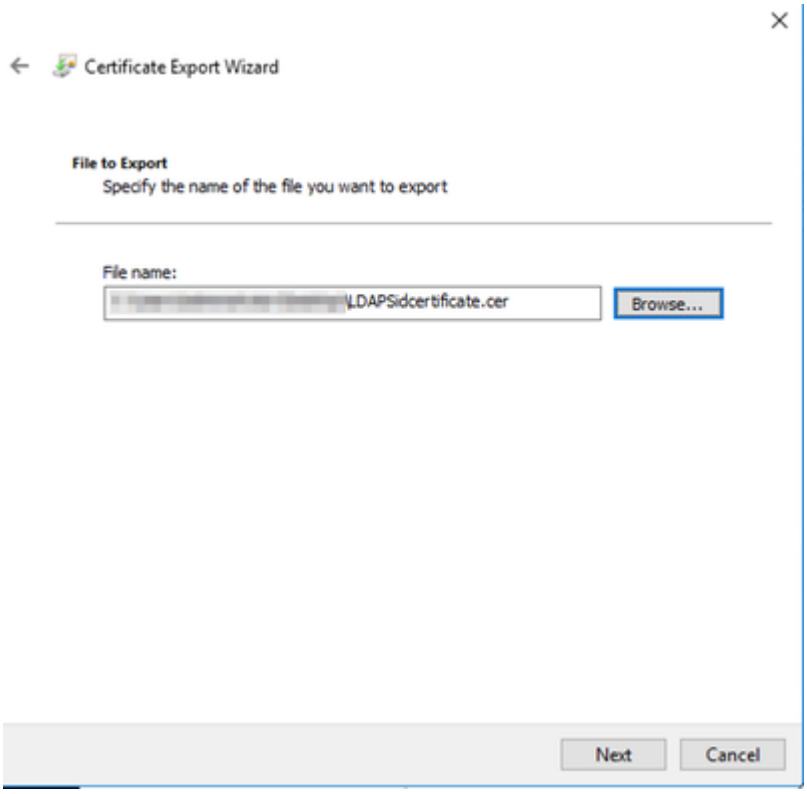


11.确保选中No， do not export private key（否，不导出私钥），然后点击Next（下一步）

12.选择Base-64编码X.509格式，然后单击下一步。



13.选择要存储证书的位置，命名文件，然后单击下一步。



14.单击Finish，必须获得“导出成功”消息。 邮件.

15.返回用于LDAPS的证书，然后选择Certification Path选项卡。

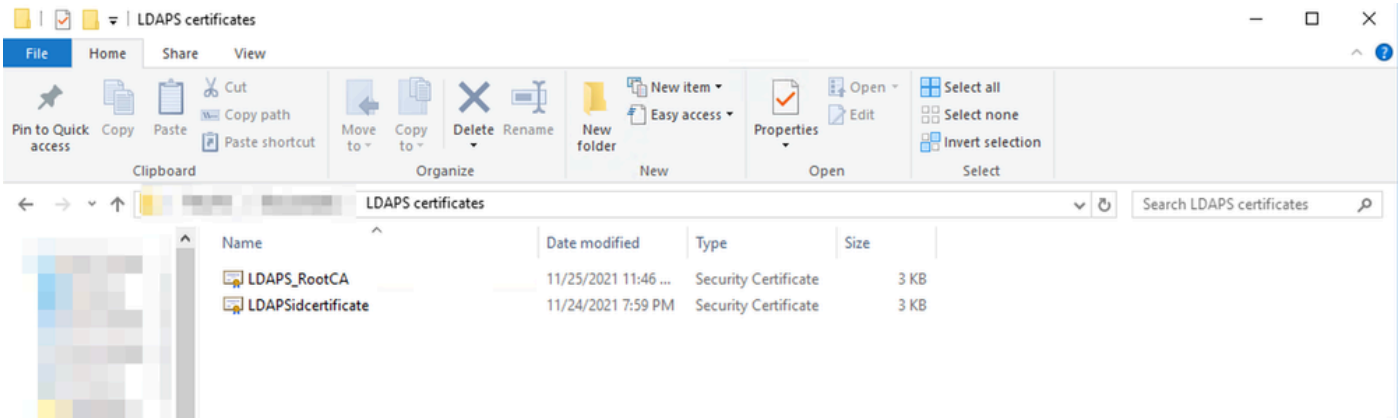
16.选择证书路径顶部的根CA颁发者，然后单击查看证书。



17.重复步骤10-14以导出对用于LDAPS身份验证的证书进行签名的根CA的证书。

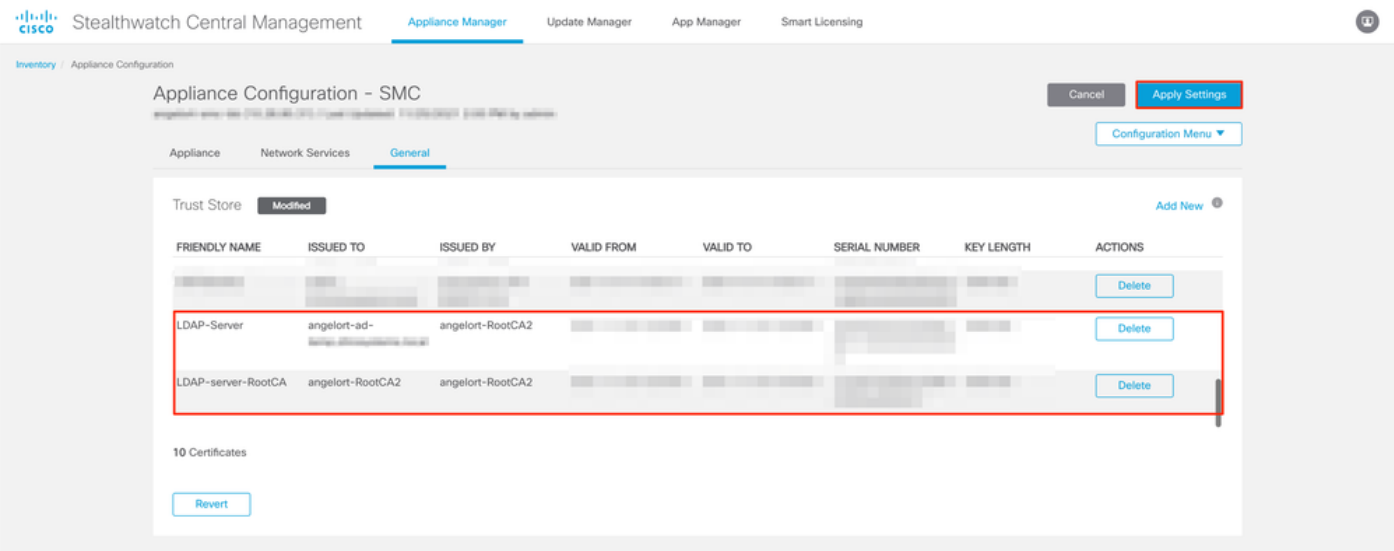
注意：您的部署可以具有多层CA层次结构，在这种情况下，您需要使用相同的过程导出信任链中的所有中间证书。

18.在继续之前，请确保LDAPS服务器和证书路径中的每个颁发机构有一个证书文件：根证书和中间证书（如果适用）。



步骤B.登录到SNA Manager以添加LDAP服务器的证书和根链

1. 导航到中央管理>资产。
2. 找到SNA Manager设备，然后单击操作>编辑设备配置。
3. 在Appliance Configuration窗口中，导航到Configuration Menu > Trust Store > Add New。
4. 键入Friendly Name，单击Choose File并选择LDAP服务器的证书，然后单击Add Certificate。
5. 重复上一步添加根CA证书和中间证书（如果适用）。
6. 验证上传的证书是否正确，然后单击Apply Settings。

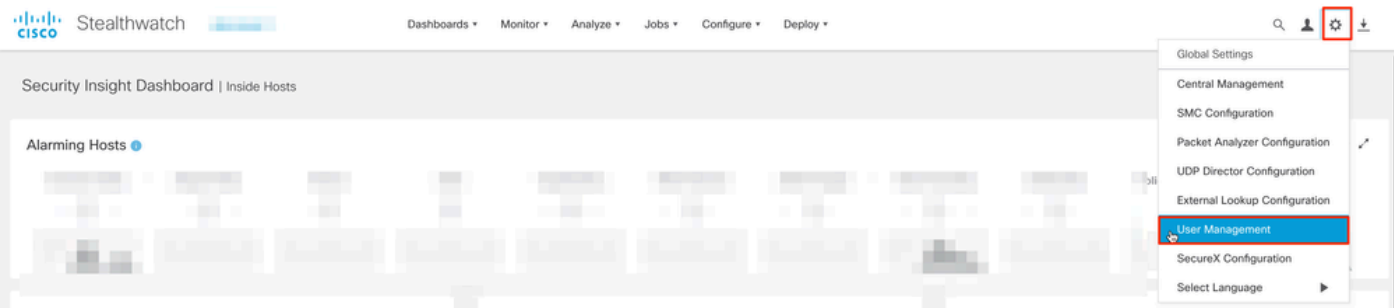


7.等待应用更改，并等待Manager状态变为Up。

步骤C.添加LDAP外部服务配置

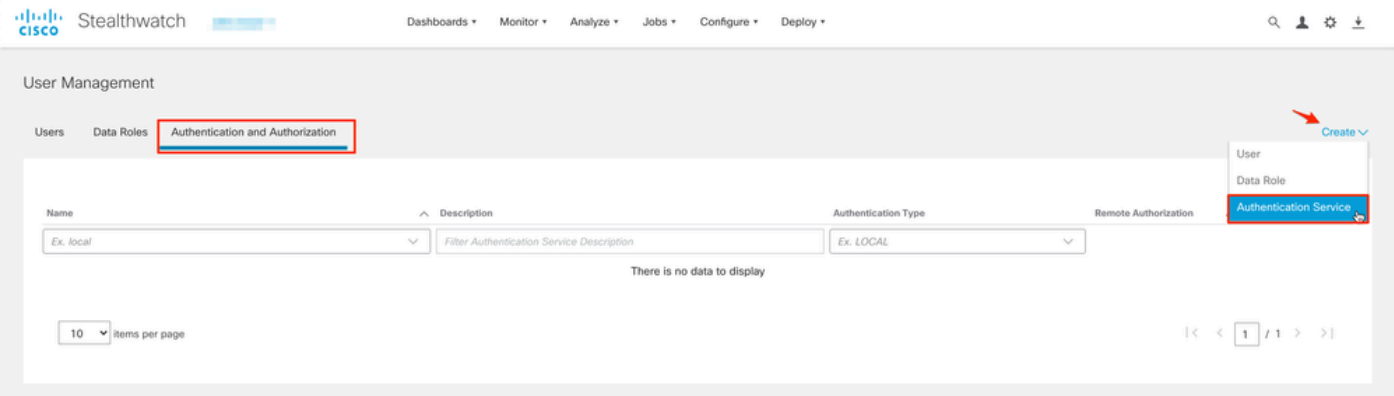
SNA 7.2或更高版本

1.打开Manager主控制面板，然后导航到全局设置 > 用户管理。



2.在“用户管理”窗口中，选择Authentication and Authorization选项卡。

3.单击创建 > 身份验证服务。



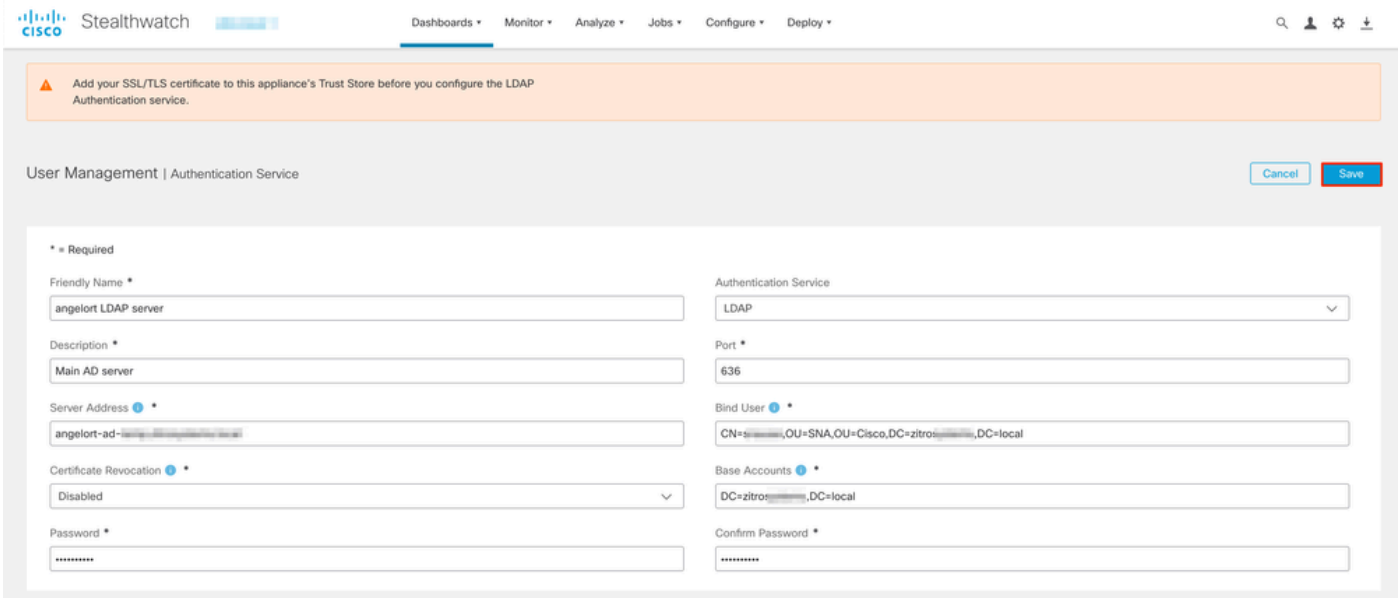
4.从Authentication Service下拉菜单中选择LDAP。

5.填写必填字段。

字段	备注
友好名称	输入LDAP服务器的名称。
描述	输入LDAP服务器的说明。
服务器地址	输入在LDAP服务器证书的主题备用名称(SAN)字段中指定的完全限定域名。 • 如果SAN字段仅包含IPv4地址，请在服务器地址字段中输入IPv4地址。 • 如果SAN字段包含DNS名称，请在Server Address字段中输入DNS名称。 • 如果SAN字段同时包含DNS和IPv4值，请使用列出的第一个值。
端口	输入为安全LDAP通信（通过TLS的LDAP）指定的端口。 LDAPS的公认TCP端口是636。
绑定用户	输入用于连接到LDAP服务器的用户ID。例如：CN=admin，OU=企业用户，DC=example，DC=com

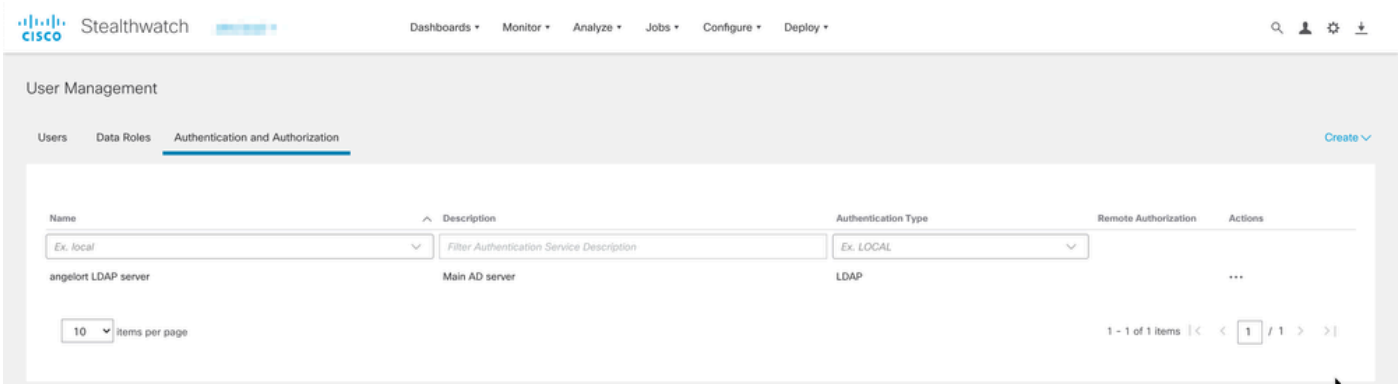
	注意：如果已将用户添加到内置AD容器（例如，“Users”），则绑定用户的绑定DN必须将规范名称(CN)设置为内置文件夹（例如，CN=username， CN=Users，DC=domain， DC=com）。 但是，如果已将用户添加到新容器，则绑定DN必须将组织单位(OU)设置为新容器名称（例如，CN=username， OU=Corporate Users， DC=domain， DC=com）。 注意：查找绑定用户的绑定DN的一种有用方法是查询与Active Directory服务器连接的Windows Server上的Active Directory。要获取此信息，您可以打开Windows命令提示符并键入命令dsquery user dc=<distinguished>,dc=<name> -name <user>。例如：dsquery user dc=example，dc=com -name user1。结果类似于“CN=user1,OU=Corporate Users，DC=example，DC=com”
密码	输入用于连接到LDAP服务器的绑定用户密码。
基本帐户	输入可分辨名称(DN)。 DN适用于必须开始搜索用户的目录的分支。它通常位于目录树（您的域）的顶部，但您也可以指定目录中的子树。“绑定用户”和要进行身份验证的用户必须可从基本帐户访问。 例如：DC=示例，DC=com

6.单击保存。



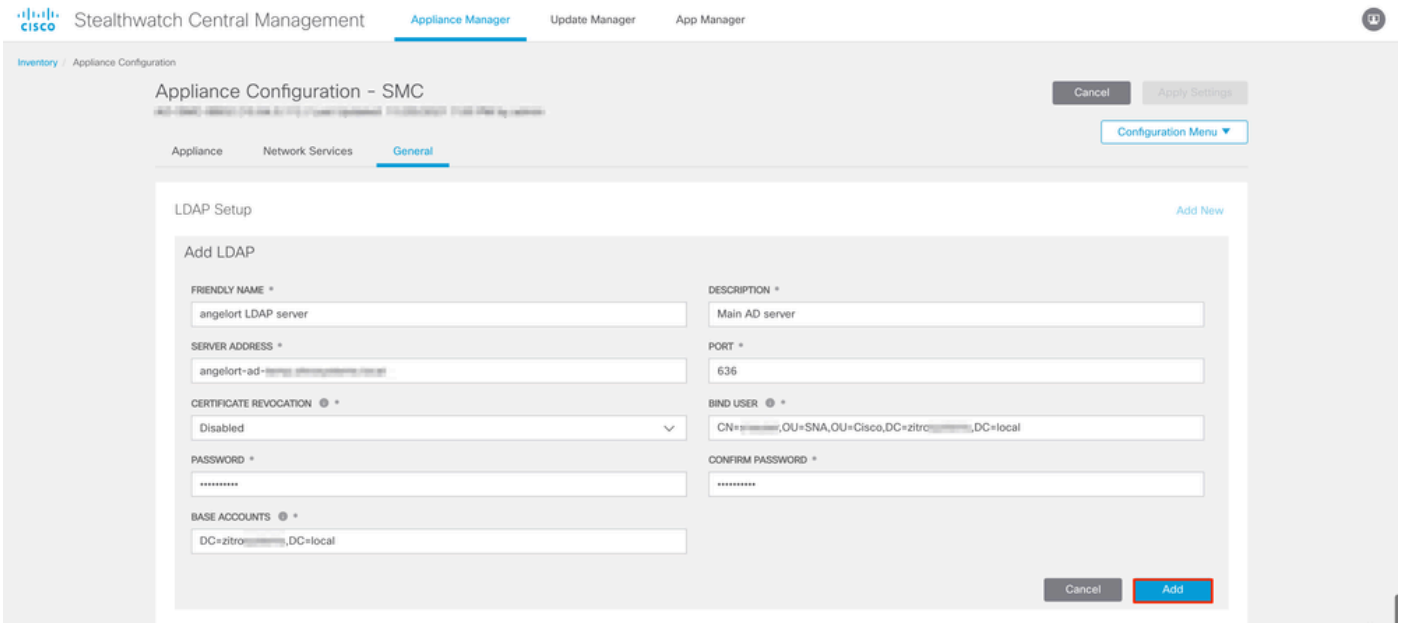
7.如果输入的设置和添加到信任存储的证书正确，您会收到标You've successfully saved your changes语。

8.已配置的服务器必须显示在User Management > Authentication and Authorization下。



SNA 7.1版

1. 导航到Central Management > Inventory。
2. 找到SMC设备，然后单击操作 > 编辑设备配置。
3. 在Appliance Configuration窗口中，导航到Configuration Menu > LDAP Setup > Add New。
4. 按照SNA 7.2版或更高版本第5步中的说明填写必填字段。



5.单击Add。

6.单击应用设置。

7.一旦输入的设置和添加到信任存储的证书正确，Manager上的更改就会生效，设备状态必须为Up。

步骤D.配置授权设置。

SNA通过LDAP支持本地和远程授权。通过此配置，AD服务器的LDAP组映射到内置或自定义SNA角色。

通过LDAP支持的SNA身份验证和授权方法如下：

- 远程身份验证和本地授权
- 远程身份验证和远程授权（仅支持SNA 7.2.1或更高版本）

本地授权

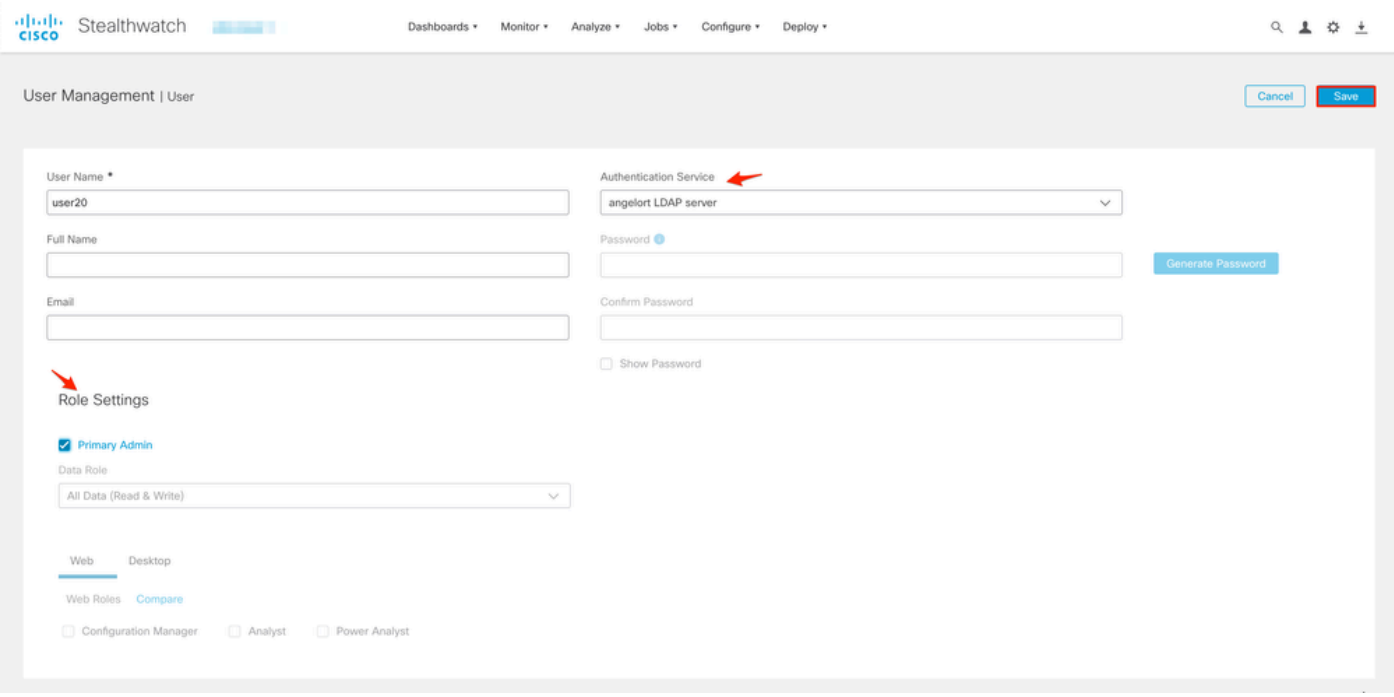
在这种情况下，用户及其角色需要在本地定义。为此，请按照以下步骤操作。

1.再次定位至用户管理，然后单击用户选项卡> 创建 > 用户。

2.定义要使用LDAP服务器进行身份验证的用户名，并从Authentication Service下拉菜单中选择已配

置的服务器。

3.定义用户在LDAP服务器对管理器进行身份验证后必须拥有的权限，然后单击Save。



通过LDAP进行远程授权

Secure Network Analytics版本7.2.1首次支持通过LDAP进行远程身份验证和授权。

注意：版本7.1不支持使用LDAP进行远程授权。

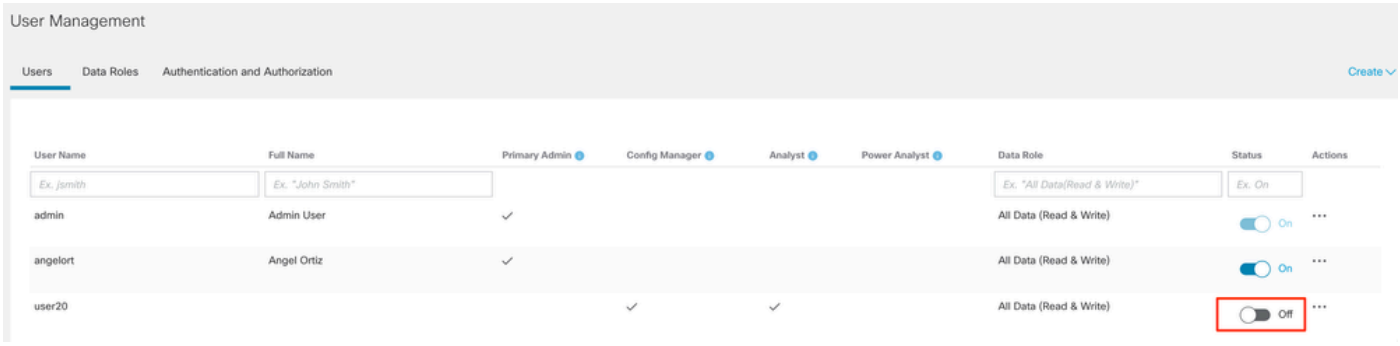
值得一提的是，如果用户是在本地定义和启用的（在Manager中），则用户会进行远程身份验证，但在本地授权。用户选择过程如下：

1. 在欢迎页面上输入凭证后，Manager将查找具有指定名称的本地用户。
2. 如果找到本地用户并启用了本地用户，则远程对其进行身份验证（如果之前配置了具有本地授权的LDAP远程身份验证），但使用本地设置进行授权。
3. 如果远程授权已配置并启用，且未在本地找到用户（未配置或禁用），则身份验证和授权均在远程执行。

因此，下面将介绍成功配置远程身份验证的步骤。

步骤D-1.禁用或删除打算使用远程授权但在本地定义的用户

1. 打开Manager主控制面板，然后导航到全局设置>用户管理。
2. 禁用或删除通过LDAP使用远程身份验证和授权的用户（如果存在），但要在本地进行配置。

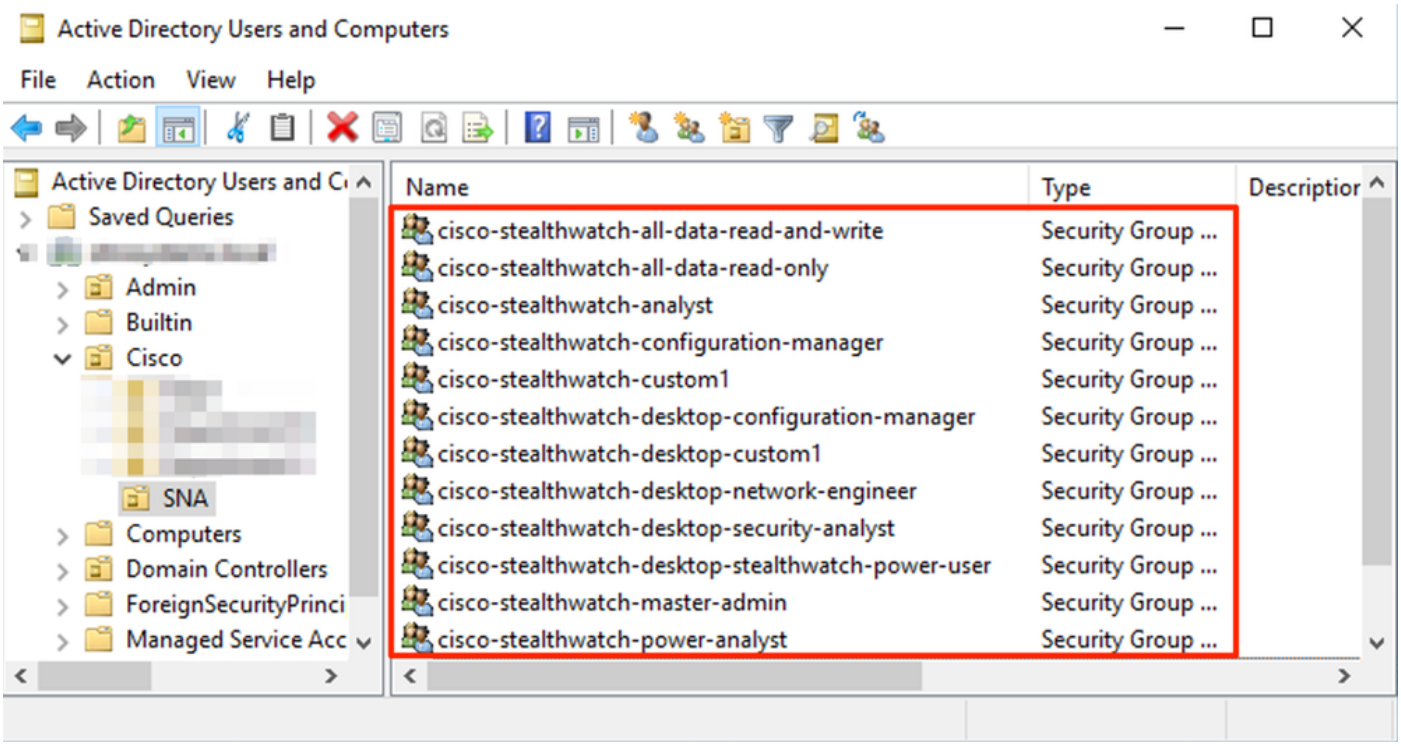


步骤D-2.在Microsoft AD服务器中定义cisco-stealthwatch组。

对于通过LDAP用户的外部身份验证和授权，密码和cisco-stealthwatch组在Microsoft Active Directory中远程定义。要在AD服务器中定义的cisco-stealthwatch组与SNA具有的不同角色相关，必须按如下方式定义。

SNA角色	组名称
主管理员	• cisco-stealthwatch-master-admin
数据角色	• cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom>（可选） 注意：确保自定义数据角色组以“cisco-stealthwatch —”开头。
Web功能角色	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
桌面功能角色	• cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineer • cisco-stealthwatch-desktop-security-analyst

	• cisco-stealthwatch-desktop-<custom>（可选） 注意：确保自定义桌面功能角色组以“cisco-stealthwatch-desktop —”开头。

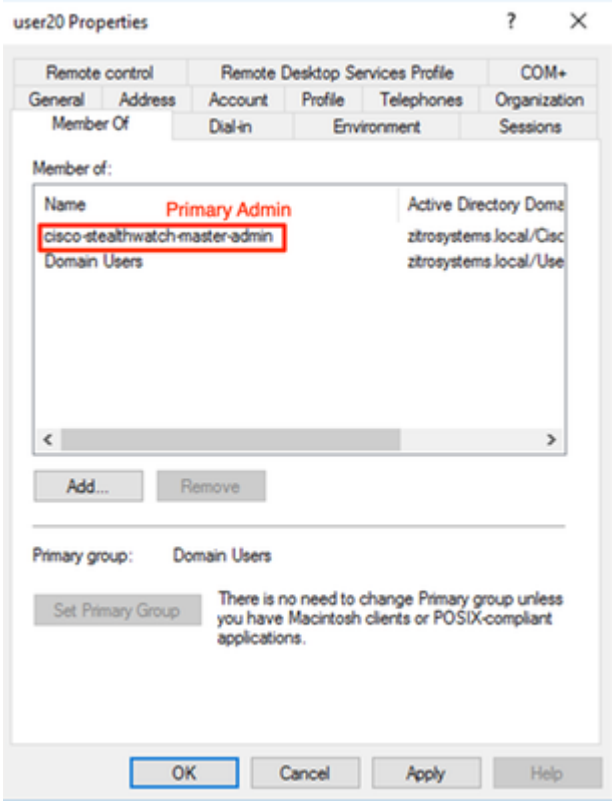


注意：如前所述，只要组名前面有正确的字符串，则支持“数据角色”和“桌面功能角色”的自定义组。必须在SNA Manager和Active Directory服务器中定义这些自定义角色和组。例如，如果在SNA Manager中为桌面客户端角色定义自定义角色“custom”，则必须将其映射到Active Directory中的cisco-stealthwatch-desktop-custom。 请注意，虽然可以创建具有此中数字值的角色和组，但这会使用(IllegalRolesException)中断LDAP/TACACS日志。 此缺陷记录在思科漏洞ID CSCww下00167 . . 因此，我们建议在创建这些角色/组时不要使用数值。

步骤D-3.定义用户的LDAP授权组映射

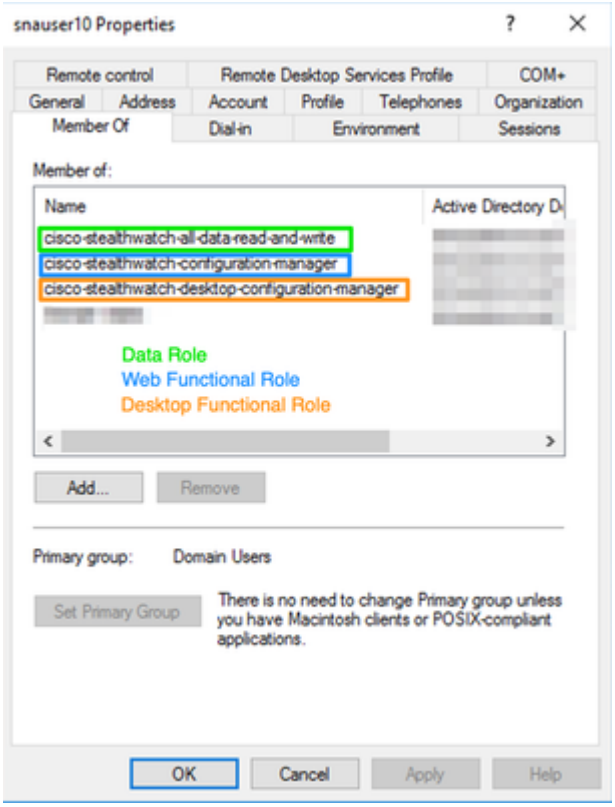
在AD服务器中定义了cisco-stealthwatch组后，我们可以将想要访问SNA Manager的用户映射到必要的组。必须按如下方式完成此操作。

- Primary Admin用户必须分配给cisco-stealthwatch-master-admin组，且不能是任何其他cisco-stealthwatch组的成员。



- 除主管理员用户以外的每个用户都必须分配到具有下一个条件的每个角色组。

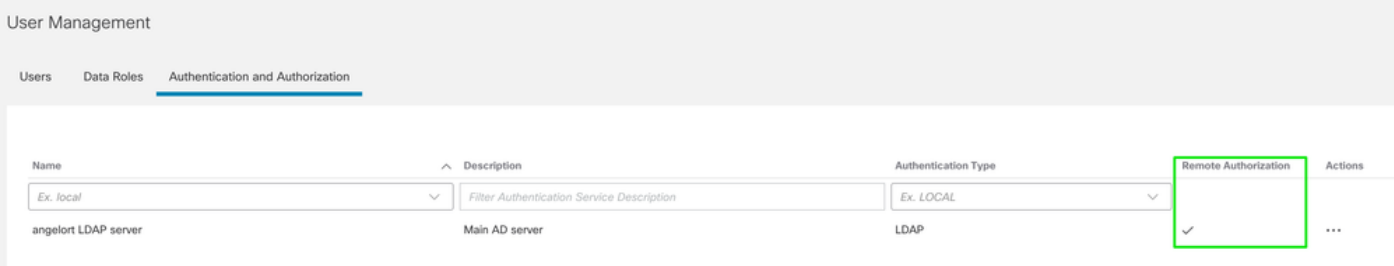
a. 数据角色:必须将用户仅分配到一个组。
b. Web功能角色:必须将用户分配至至少一个组。
c. 桌面功能角色:必须将用户分配至至少一个组。



步骤D-4.在SNA管理器上通过LDAP启用远程授权。

1. 打开Manager主控制面板，然后导航到全局设置 > 用户管理。
2. 在User Management窗口中，选择Authentication and Authorization选项卡。
3. 找到步骤C中配置的LDAP身份验证服务。
4. 单击操作 > 启用远程授权。

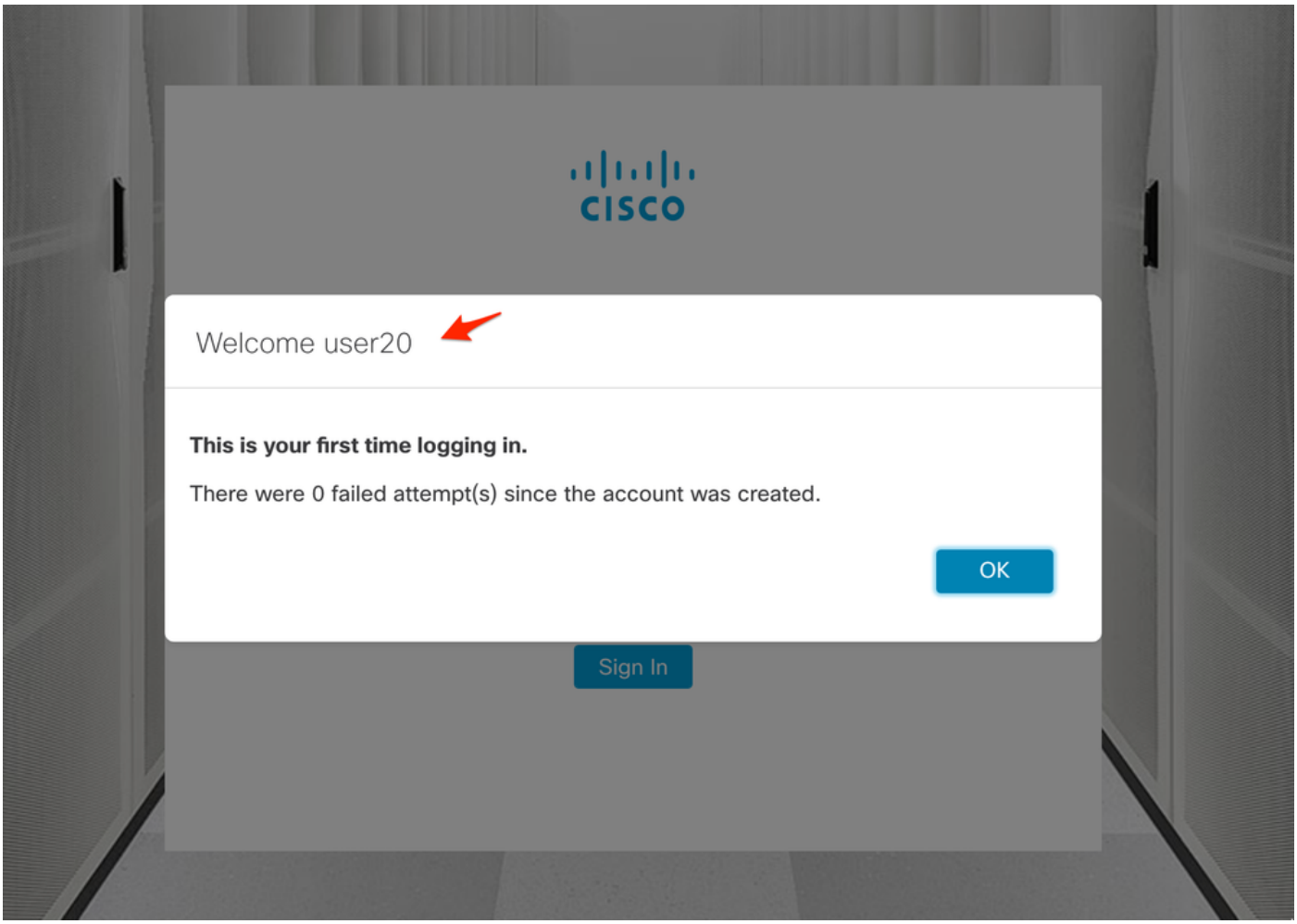
注意：一次只能使用一个外部授权服务。如果另一个授权服务已在使用中，则会自动禁用该授权服务，并启用新的授权服务，但是通过以前的外部服务获得授权的所有用户都将注销。在任何操作发生之前，系统都会显示确认消息。



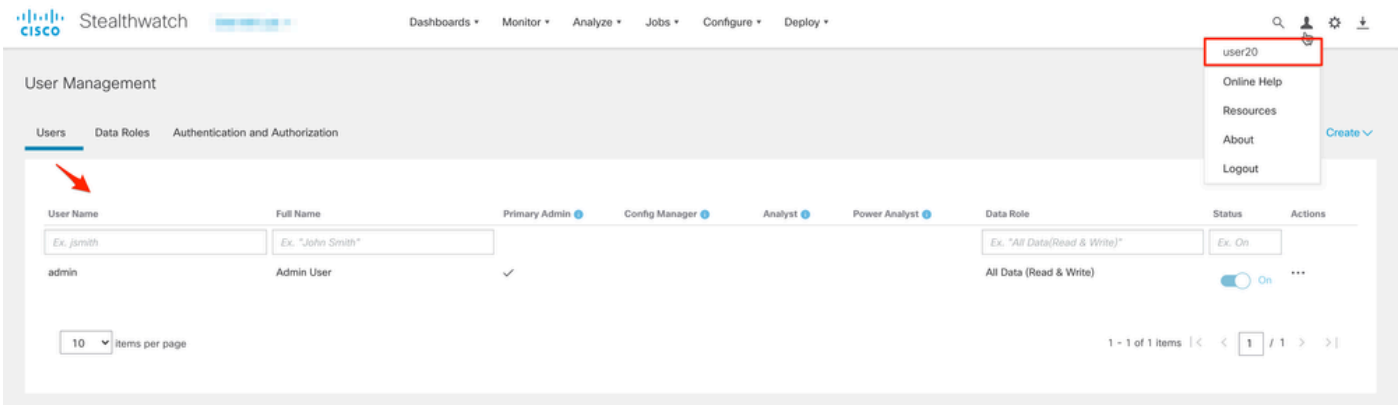
验证

使用本部分可确认配置能否正常运行。

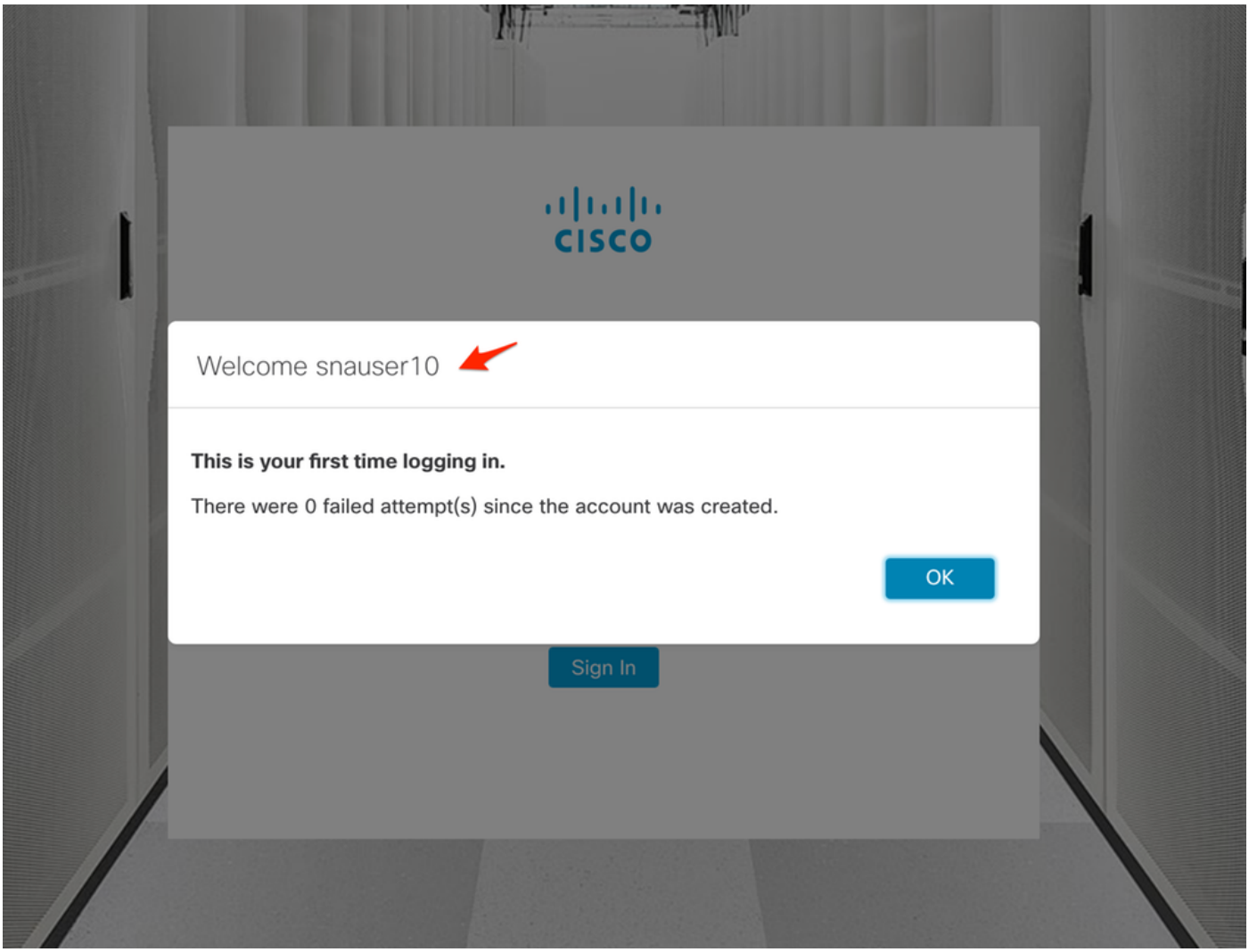
用户可以使用AD服务器上定义的凭据登录。



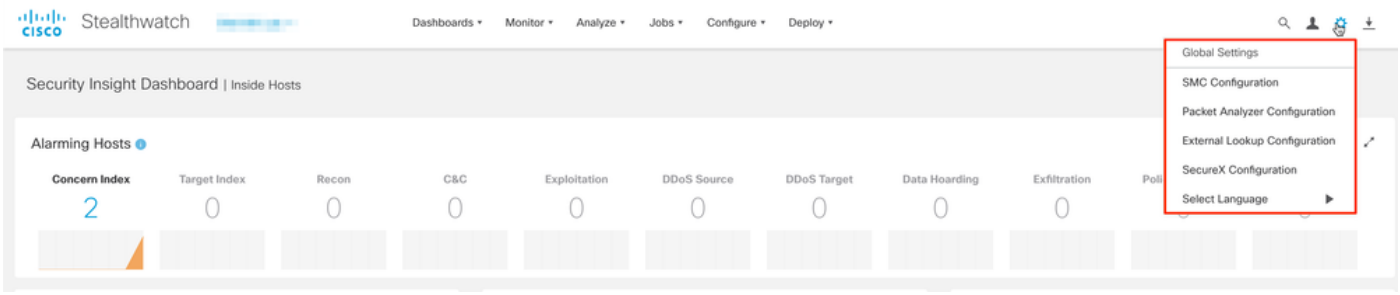
第二个验证步骤与授权有关。在本示例中，用户“user20”成为AD服务器中cisco-stealthwatch-master-admin组的成员，并且您可以确认该用户具有Primary Admin权限。用户未在本地用户中定义，因此您可以确认Authorization属性是由AD服务器发送的。



在本示例中“snauser10”中对其他用户执行相同的验证。 您可以使用AD服务器上配置的凭证确认身份验证成功。



对于授权验证，由于此用户不属于主要管理员组，因此某些功能不可用。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

如果无法成功保存身份验证服务的配置，请验证：

1. 您已将LDAP服务器的正确证书添加到Manager的信任存储中。
2. 已配置的Server Address在LDAP服务器证书的Subject Alternative Name(SAN)字段中指定。
    - 如果SAN字段仅包含IPv4地址，请在服务器地址字段中输入IPv4地址。
    - 如果SAN字段包含DNS名称，请在Server Address字段中输入DNS名称。
    - 如果SAN字段同时包含DNS和IPv4值，请使用列出的第一个值。
3. 配置的Bind User和Base Account字段正确，如AD域控制器所指定。

相关信息

- 如需其他帮助，请联系思科技术支持中心(TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。