对过期ISE管理员证书进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

ISE管理员证书（已过期）

- 验证管理员证书状态
- 行动计划

故障排除

- 使用案例1:已注销的辅助节点停滞在分布式状态(ise-psn1)
  - 验证状态
  - 解决方法
- 使用案例2:取消注册的辅助节点GUI无法访问(ise-psn2)
  - 验证状态
  - 解决方法

相关信息

简介

本文档介绍如何对过期的思科身份服务引擎(ISE)管理员证书进行故障排除和续订。

先决条件

要求

思科建议您了解以下主题：

- Cisco ISE部署。
- Cisco ISE中的证书管理。

使用的组件

本文档中的信息基于以下软件版本：

- 思科身份服务引擎(ISE)版本3.3补丁4。

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。

背景信息

本文档重点介绍分布式部署；但是，您可以在独立节点上使用相同的故障排除计划。

在ISE分布式部署中，节点是主管理节点(PPAN)或辅助节点。

本文档使用ISE管理员证书作为自签名证书以演示证书过期的影响，但不建议将此方法用于生产系统。最好使用授权签名的证书作为管理员使用。

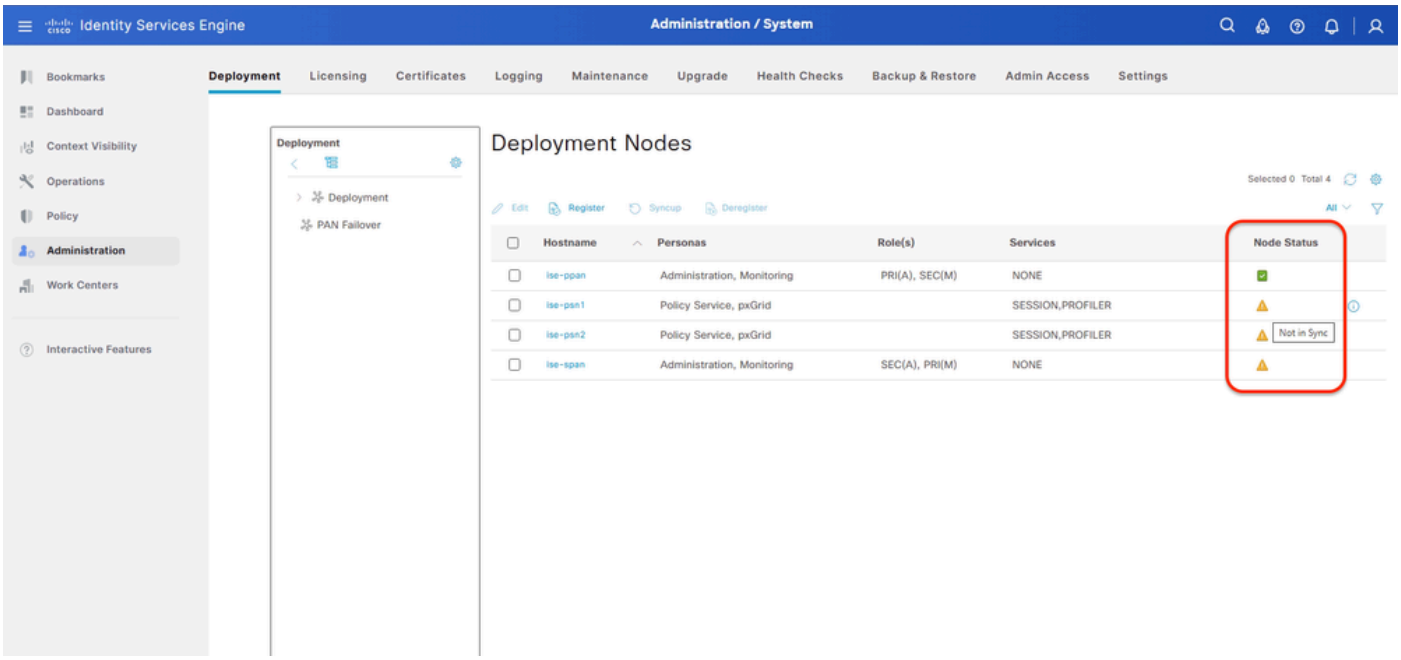
注意：思科建议您保持管理员证书处于健康状态并提前计划续订，请查找本指南以帮助您跟踪和续订ISE系统证书（在ISE上配置证书续订）。

ISE管理员证书（已过期）

验证管理员证书状态

步骤1.检查部署状态。导航到管理>系统>部署。

您可以检查辅助节点状态，如图所示，三个辅助节点是（不同步）。

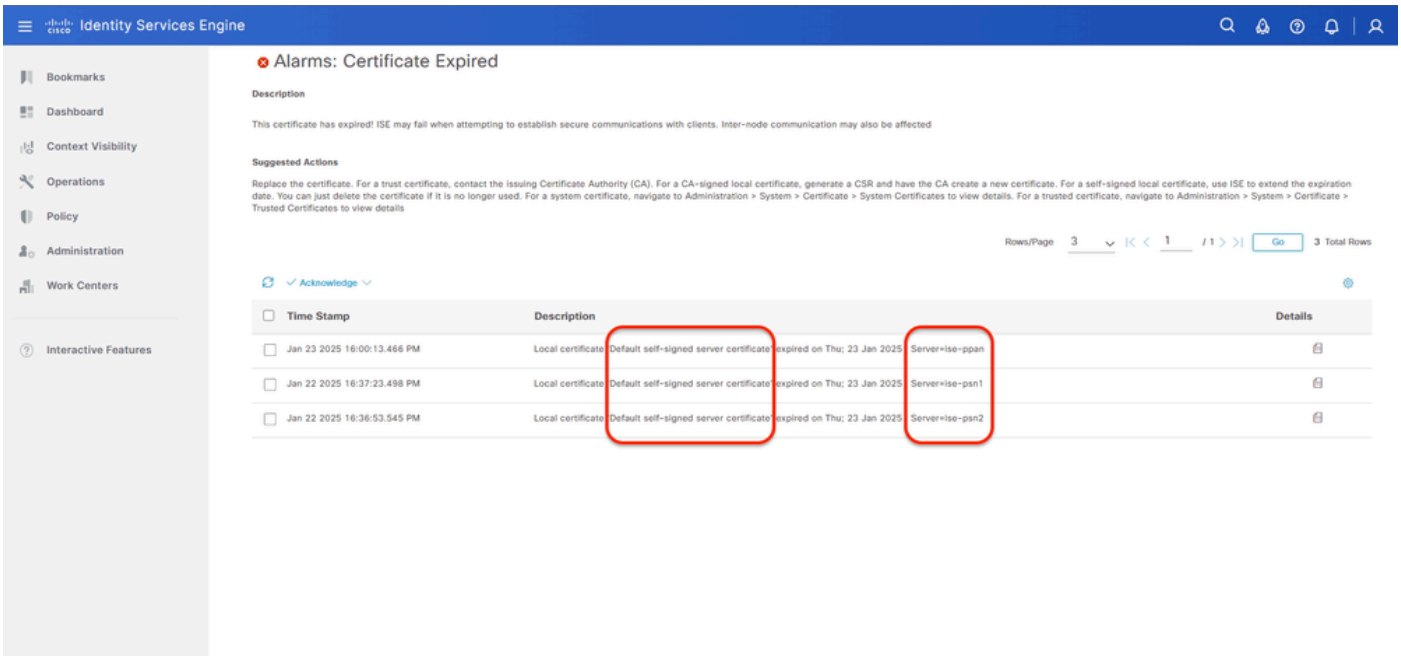


部署状态

步骤2.复查警报。导航至控制面板>警报>（证书已过期）。

确认哪个节点和哪个证书已过期。

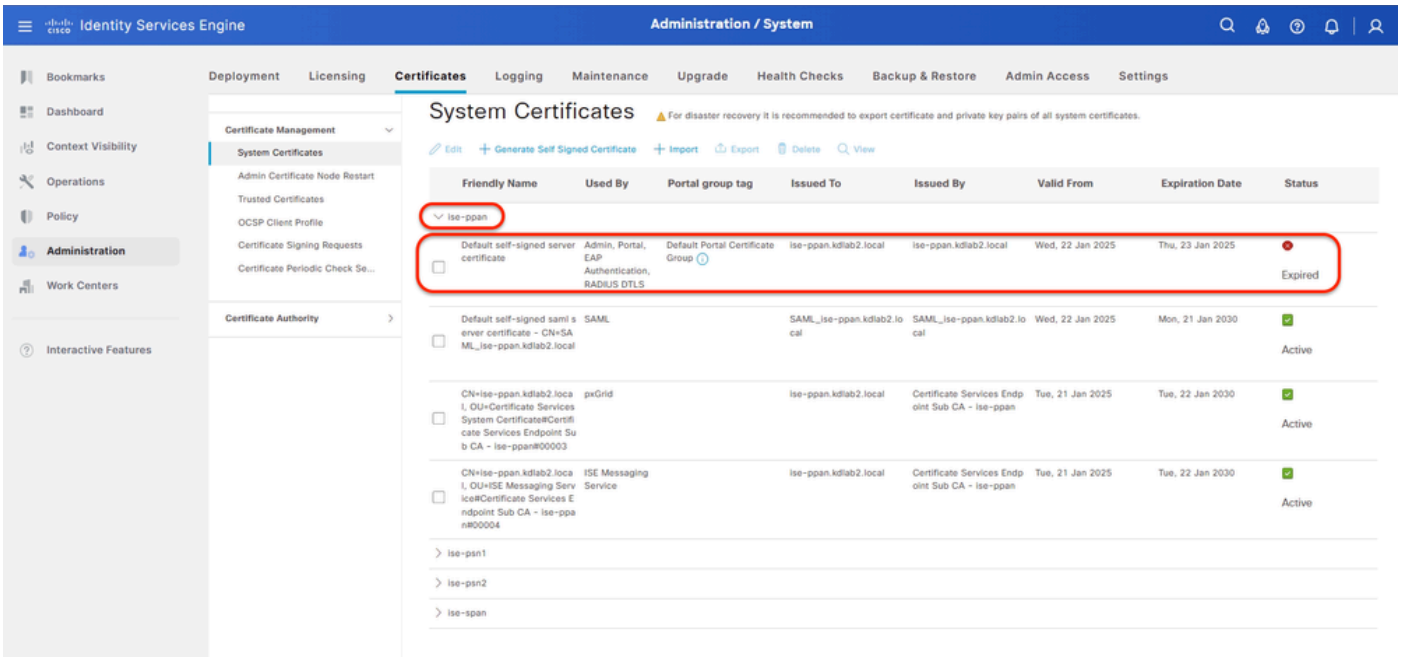
注意：如果主管理节点(PPAN)在任何辅助节点之前过期，您将无法从该节点看到任何警报，这就是此警报中辅助管理节点(SPAN)所发生的情况。



警报（证书已过期）

步骤3.检查管理员证书状态。导航到Administration > System > Certificates > Certificate Management > System Certificates > Expand node。

1.主管理节点(PPAN):

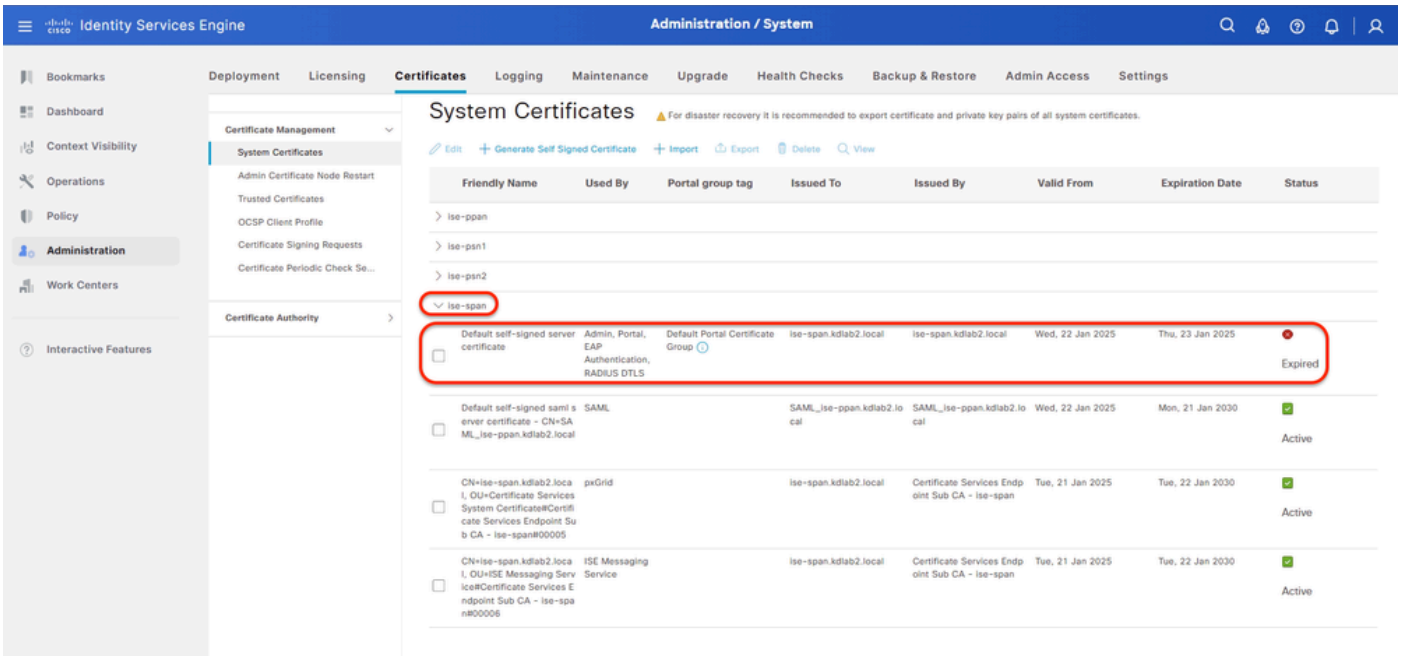


PPAN管理员证书状态

2.辅助节点。

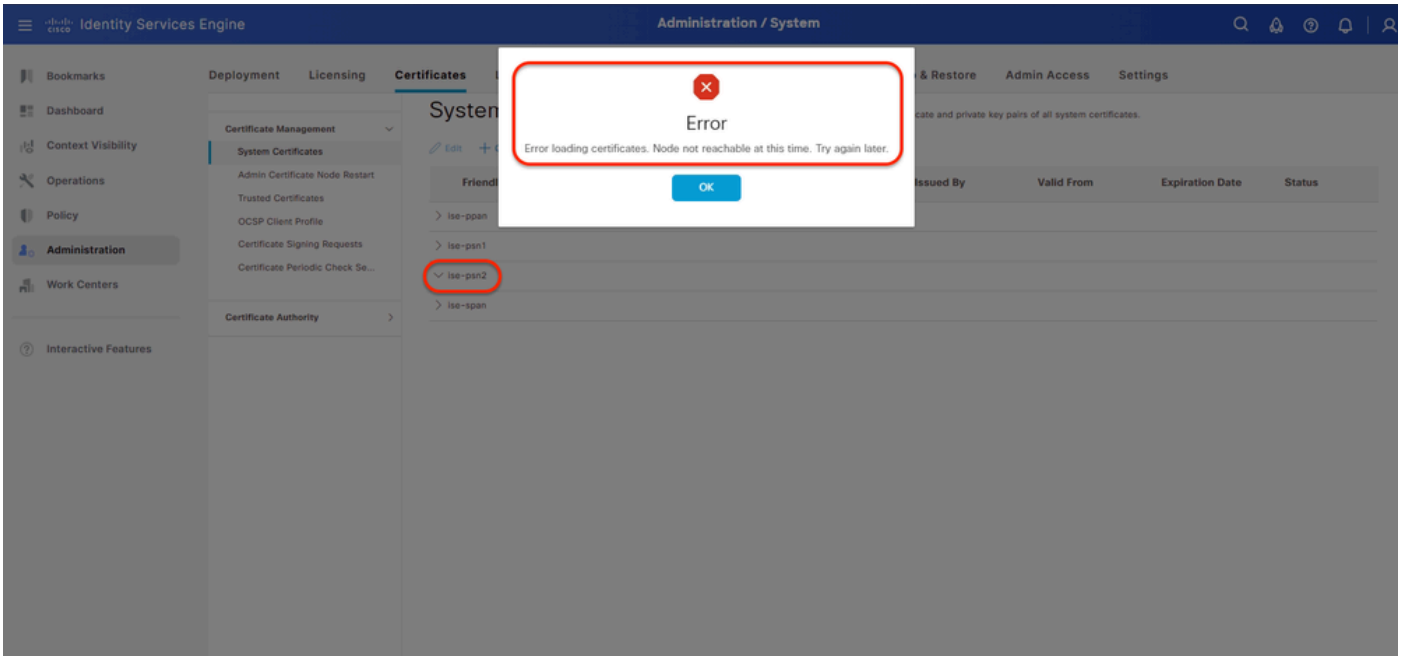
对于辅助节点，它可以是两个选项中的一个，并且在这两种情况下，您必须应用相同的行动计划：

A.可以展开节点系统证书并确认管理员证书已过期：



辅助节点管理员证书状态

B.引发错误(“加载证书时出错。此时无法到达节点。请稍后重试。”)，如所示(ise-psn2)。



辅助节点不可达

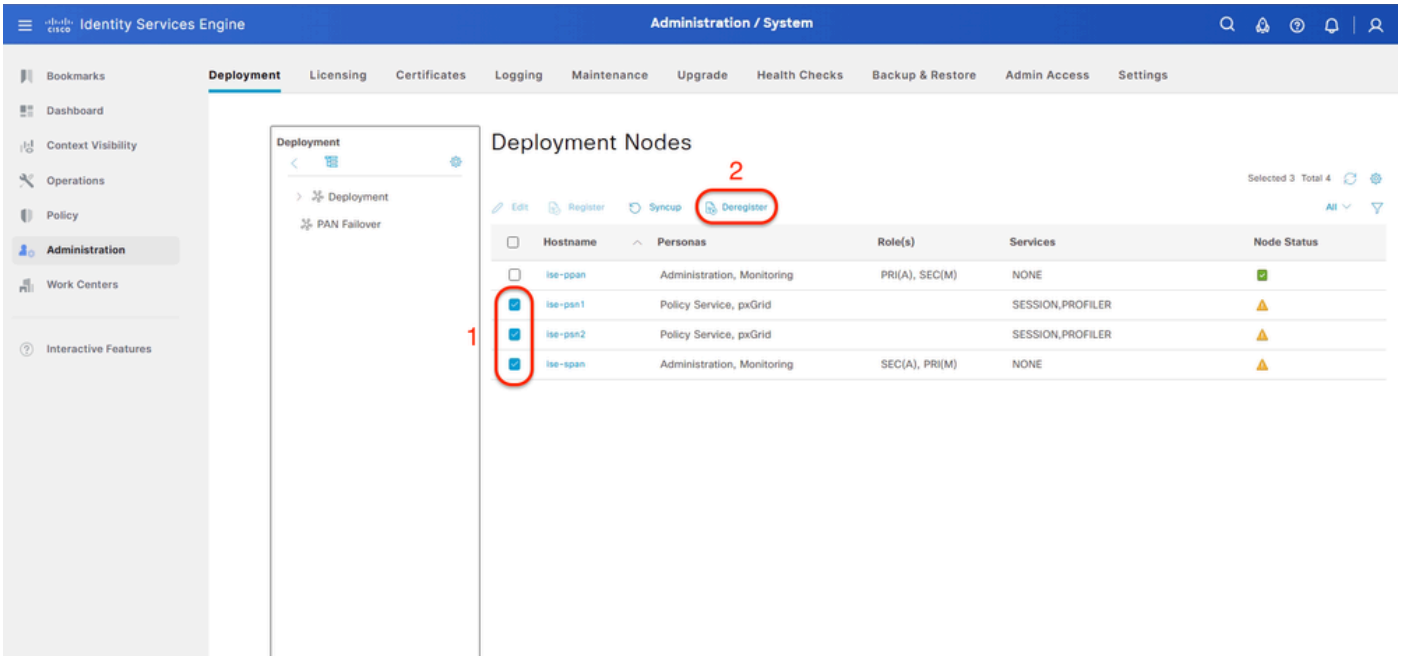
行动计划

确认所有4个节点的管理员证书过期后，必须应用以下步骤：

步骤1.从分布式部署中取消注册所有辅助节点（仅当管理员证书过期时）。

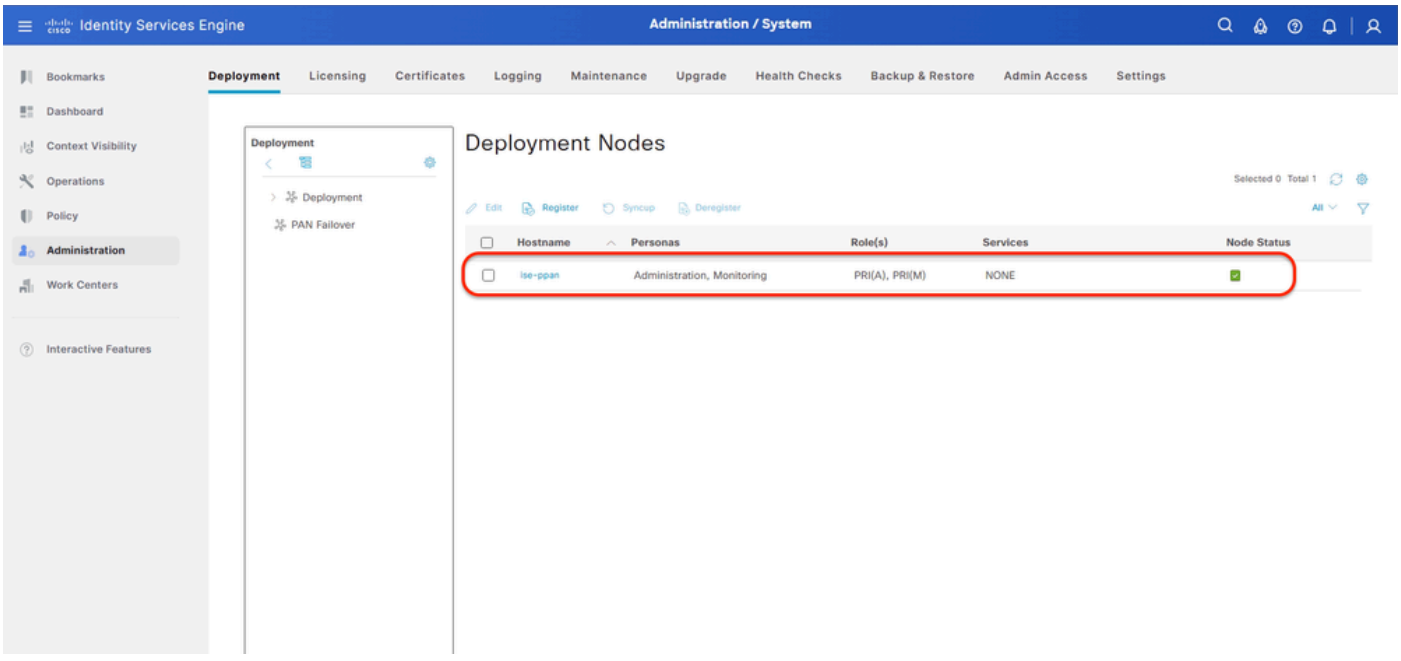
导航到辅助节点的Administration > System > Deployment > Check [√]，然后点击Deregister。

注意：取消注册节点意味着节点已移至独立状态。然后，您可以在此节点上续订管理员证书。



取消注册辅助节点

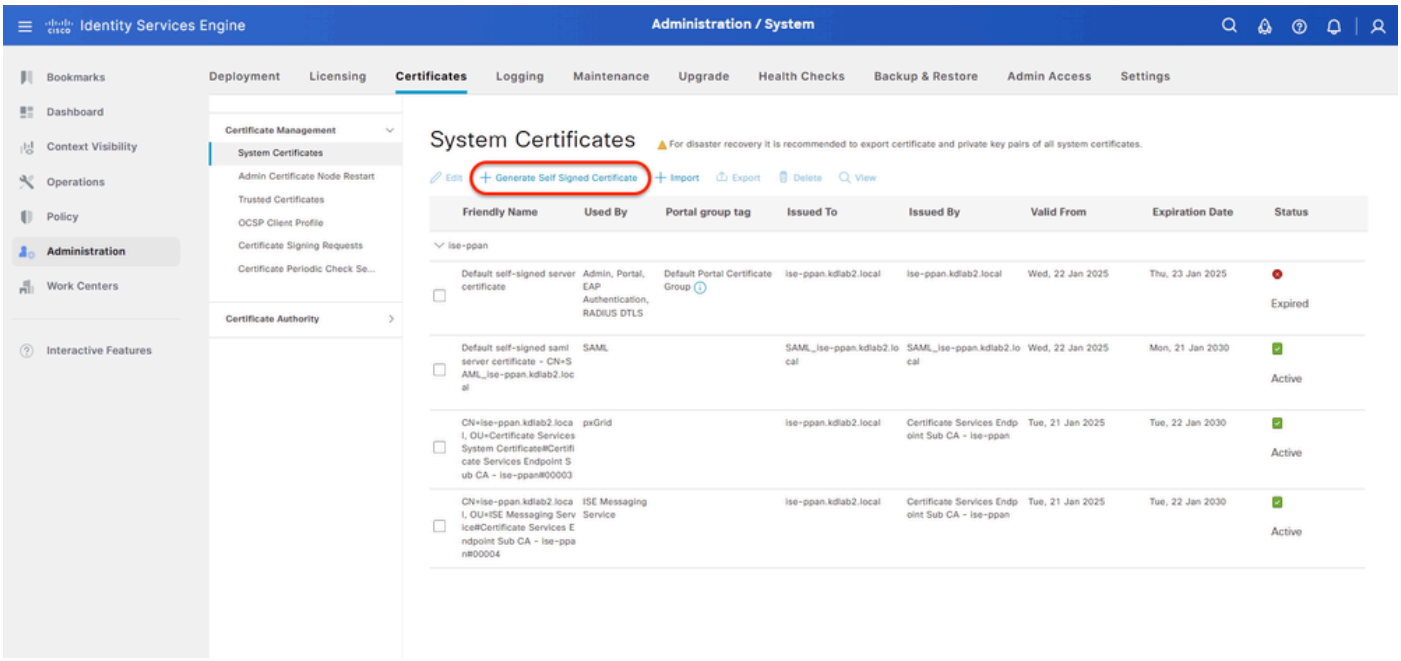
注意：请记住，仅取消注册管理员证书已过期的辅助节点，保留其余节点。在本文档中，所有辅助节点都已过期。



取消注册所有辅助节点

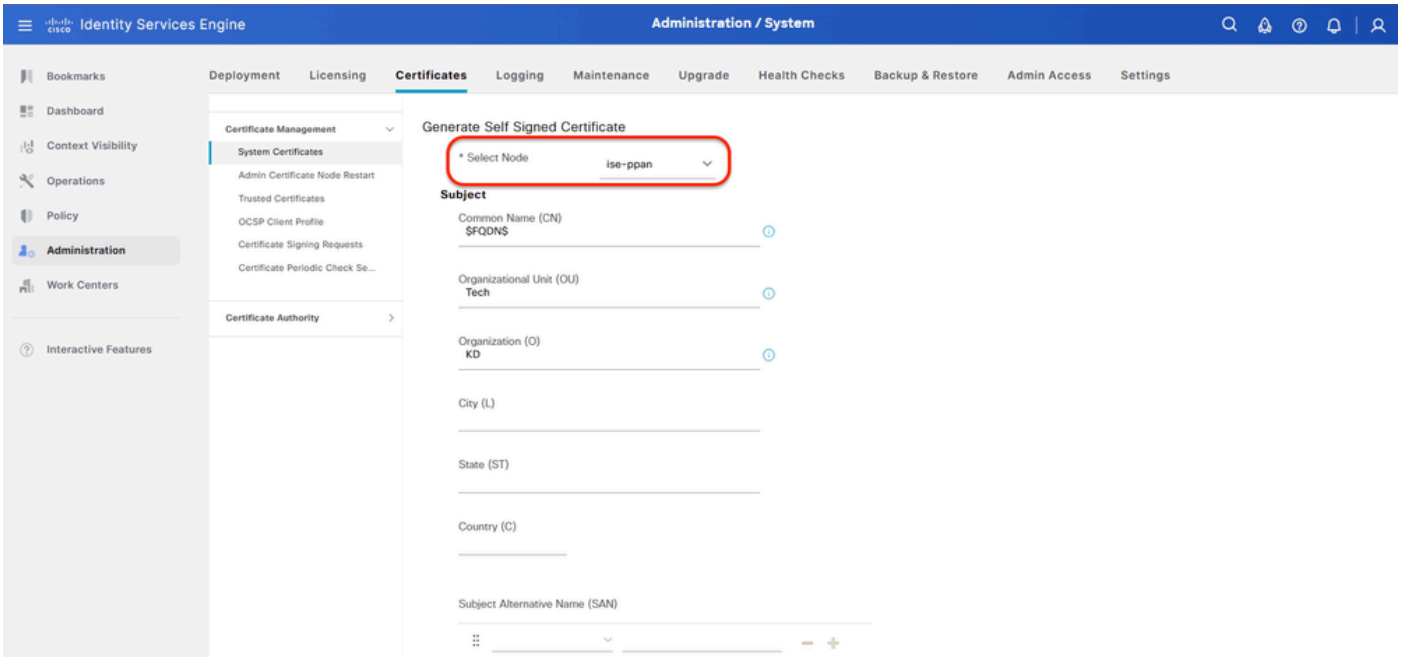
步骤2.更新主管理节点(PPAN)的管理员证书。

1. 导航到管理>系统>证书>证书管理>系统证书。单击+生成自签名证书:



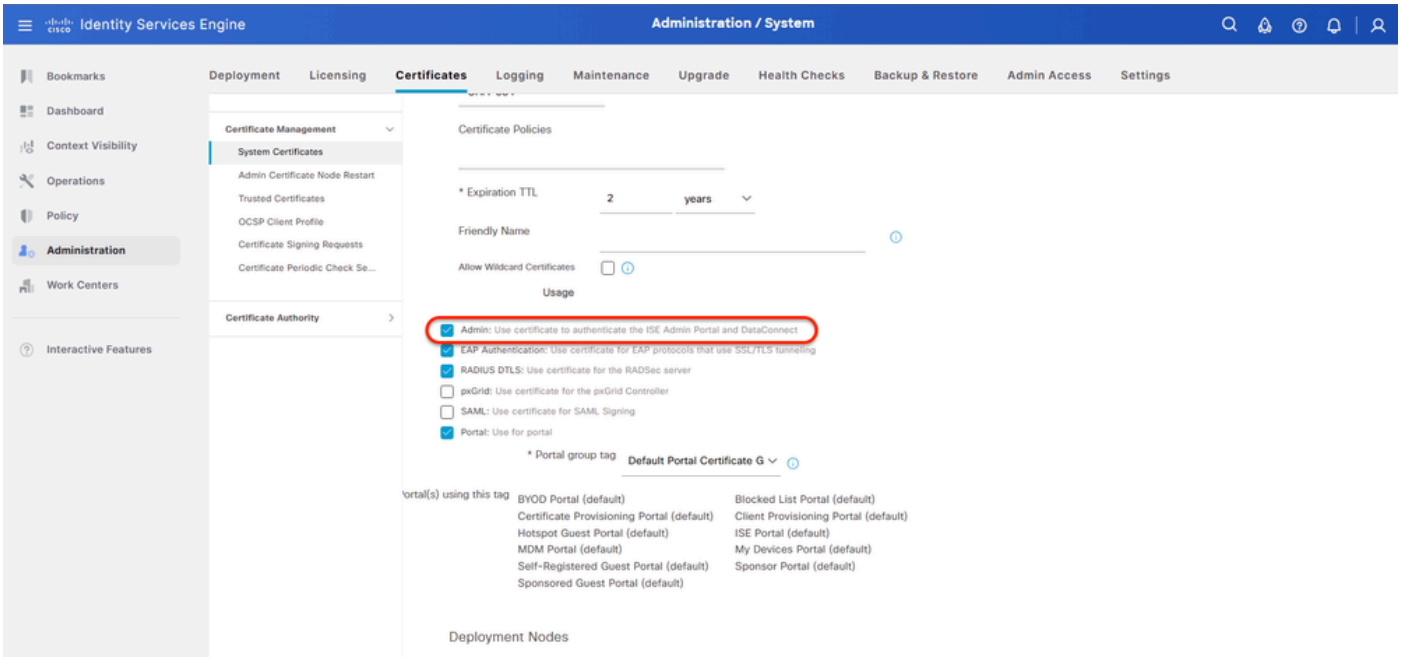
生成新的自签名管理员证书

2.选择Primary Admin Node(PPAN)(ise-ppan)并填写证书信息:



选择主管理节点(PPAN)

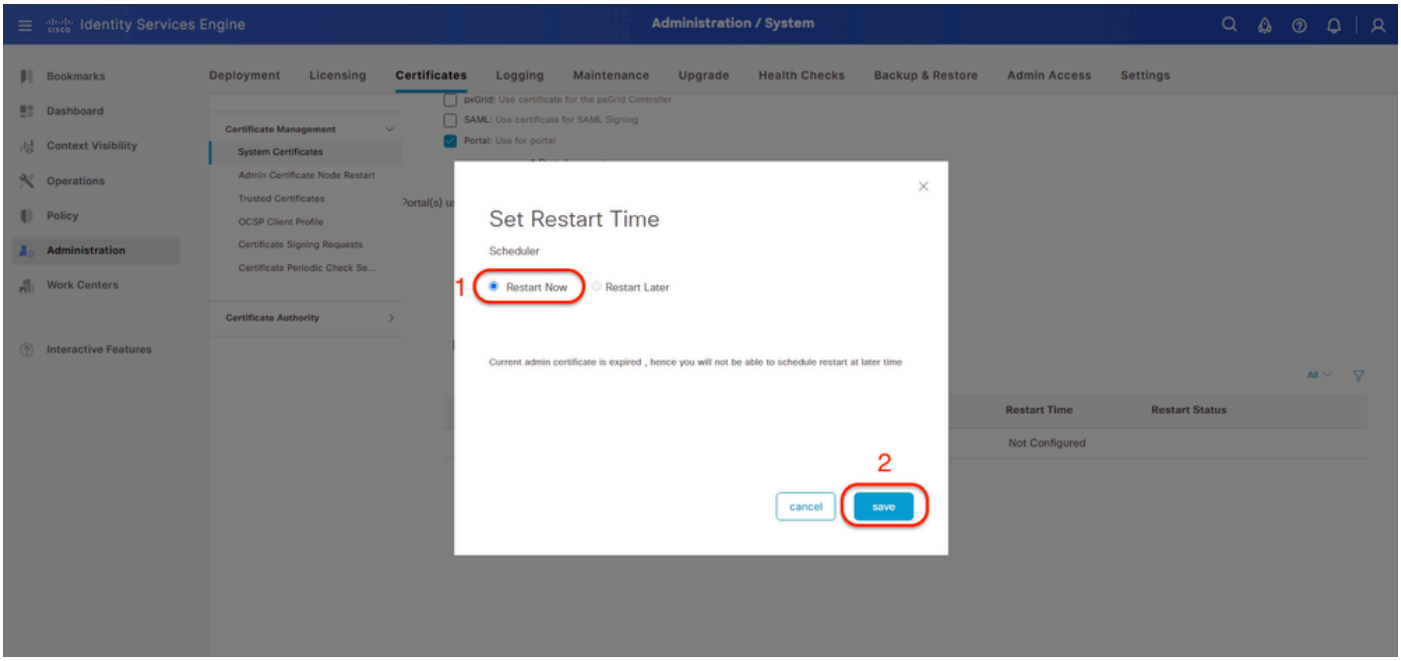
3.选中[√] Admin用法。



管理员使用情况

4.为主管理节点(PPAN)将Restart Time设置为Restart Now。 将部署上的所有节点设置为Restart Now或Restart Later。

在主管理节点(PPAN)上续订管理员证书（为管理员使用配置的证书）后，必须重新启动部署中的所有节点。



将重新启动时间设置为现在

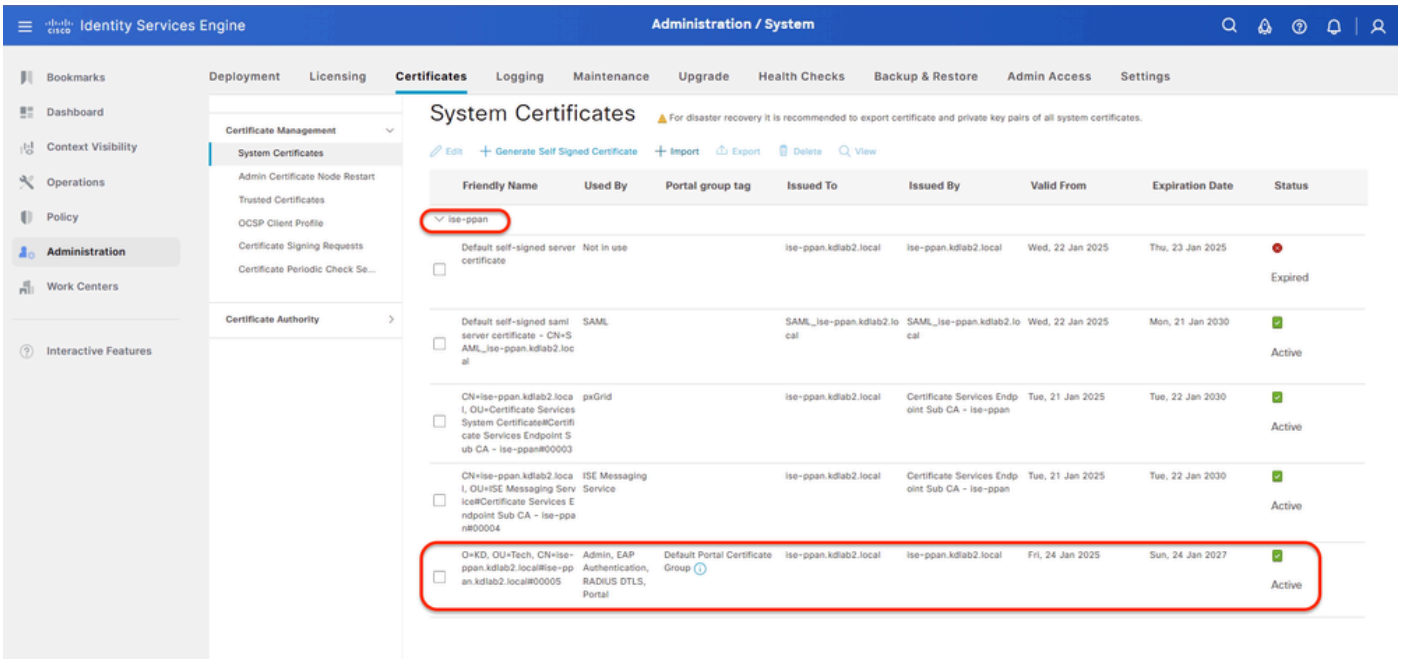
5.单击提交。

注意：在主管理节点(PPAN)上续订管理员证书（为管理员使用配置的证书）后，必须重新启动部署中的所有节点。您可以立即重新启动每个节点，也可以安排以后重新启动。通过此功能，您可以确保任何正在运行的进程都不会因自动重新启动而中断，从而更好地控制进程。

您可以在Administration > System > Certificates > Admin Certificate Node Restart窗口中查看和编辑计划的重新启动，该窗口在Cisco ISE版本3.3中可用。

6.验证主管理节点(PPAN)的新管理员证书。

导航到管理>系统>证书>证书管理>系统证书>扩展(ise-ppan)。

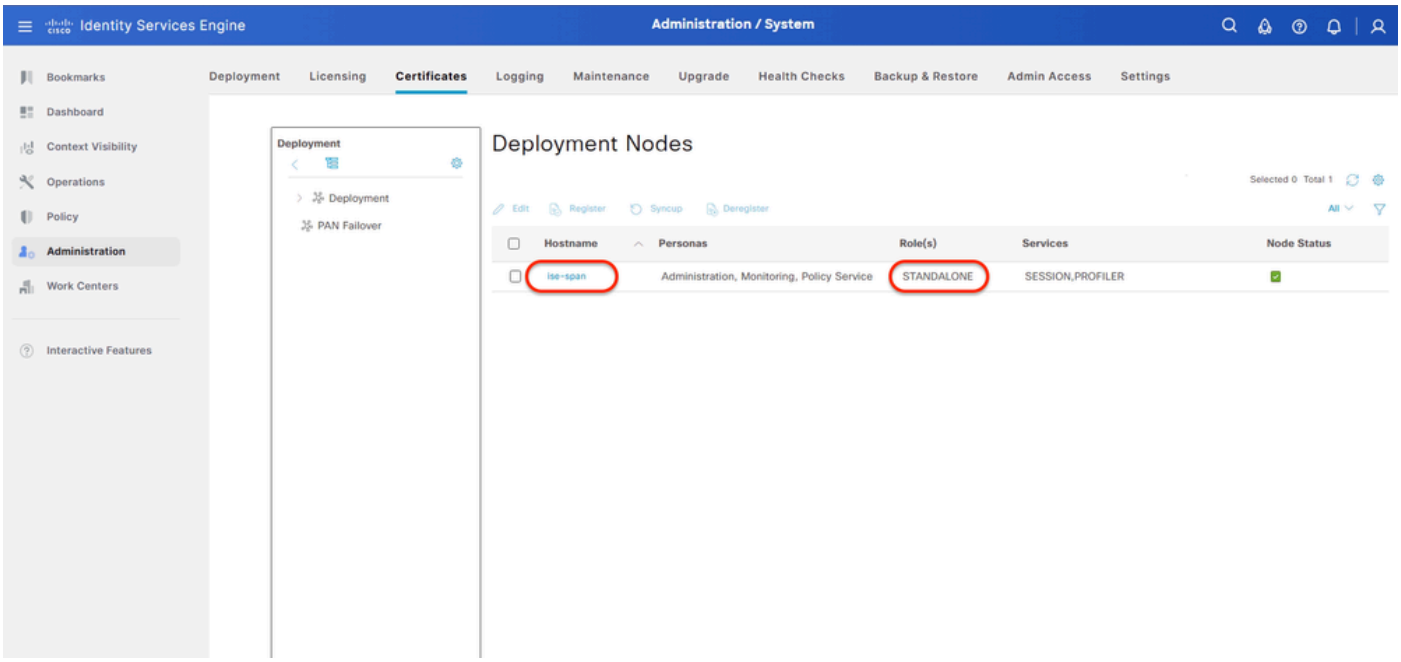


新管理员证书(ise-ppan)

步骤3.更新辅助节点的管理员证书。

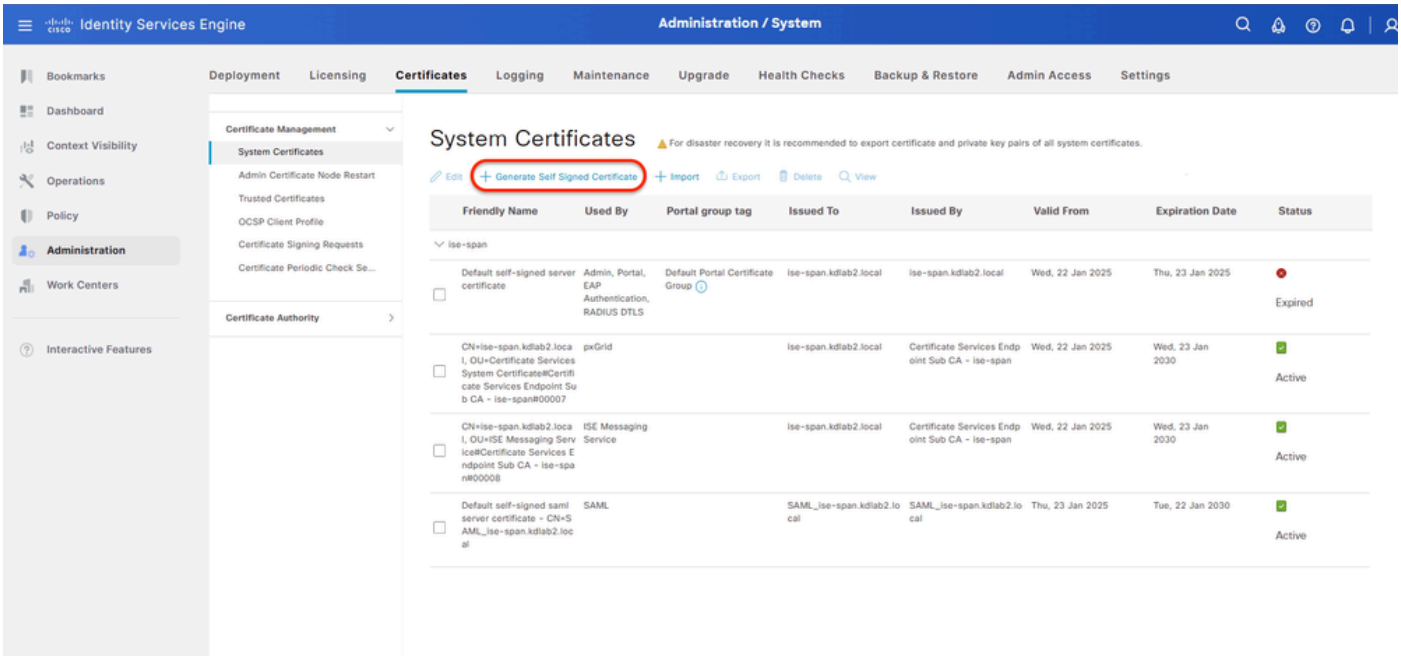
1.从分布式部署取消注册后，确认独立部署上的辅助节点。

通过GUI浏览节点(https://<FQDN/IP>)，然后导航到管理(Administration)>系统(System)>部署(Deployment)。



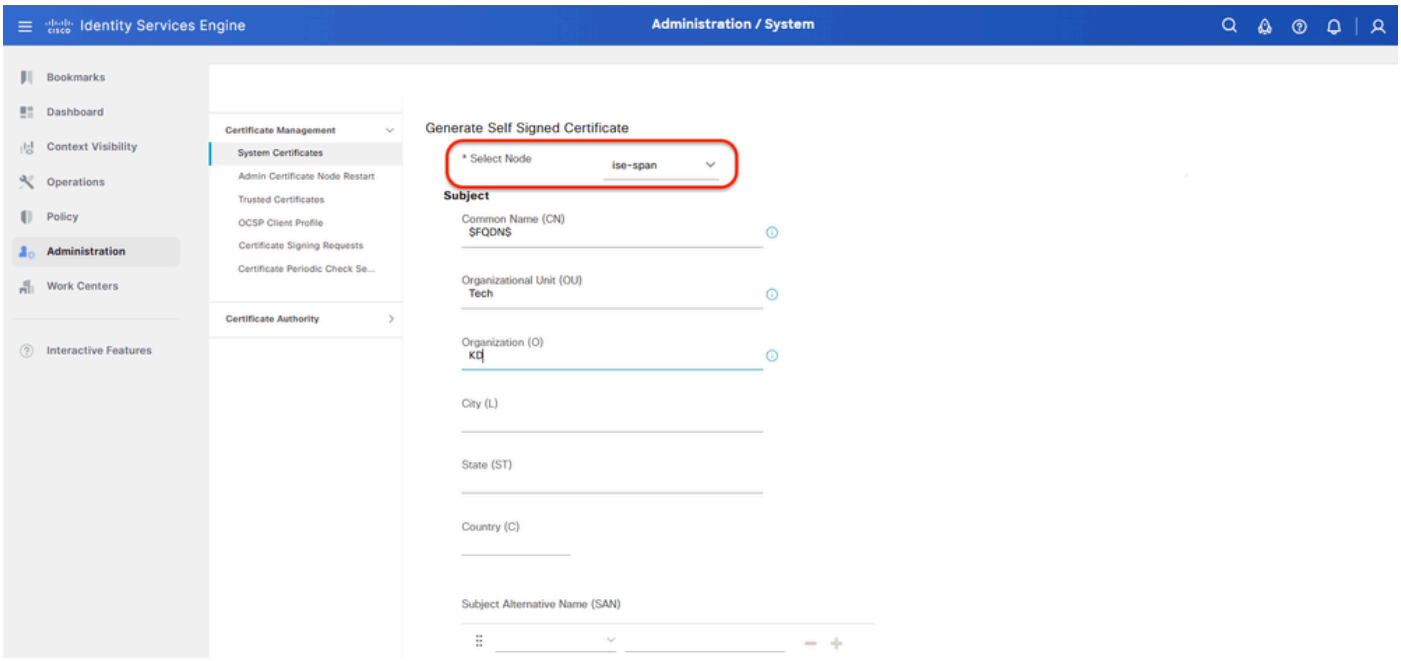
独立部署上的(ise-span)

2.导航到管理>系统>证书>证书管理>系统证书。单击+Generate Self Signed Certificate。



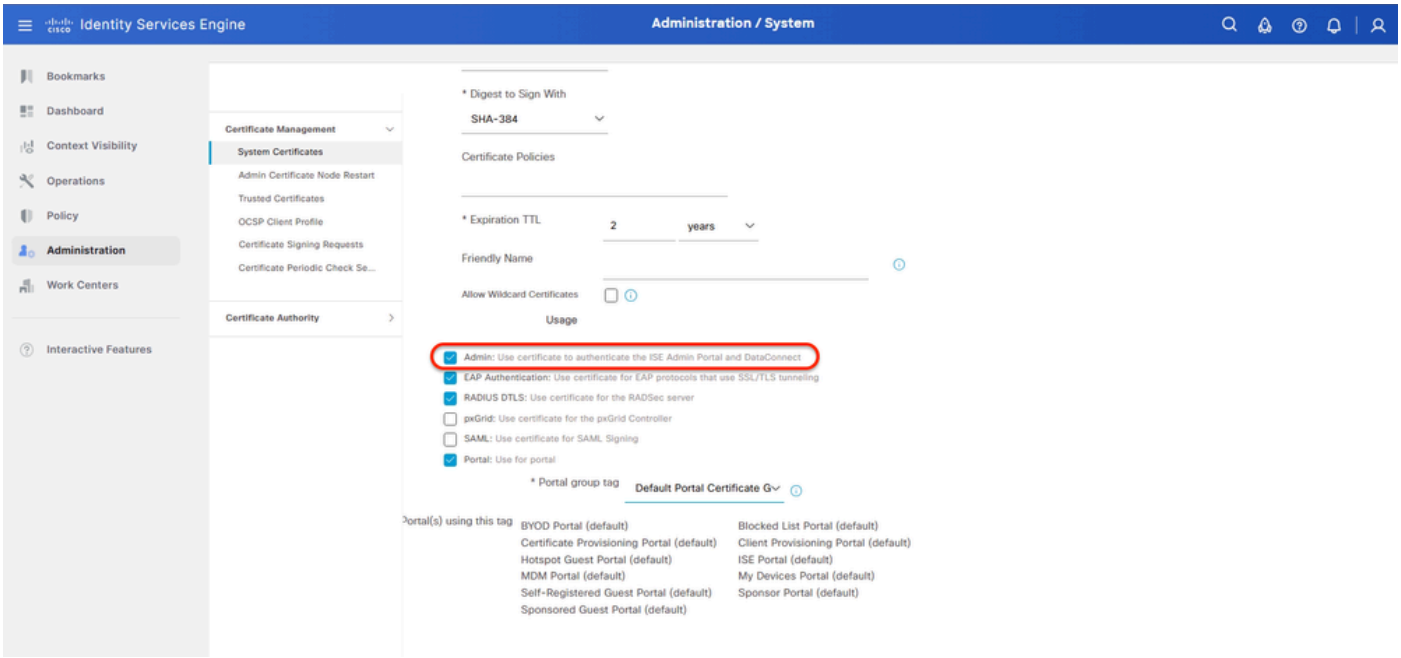
生成新的自签名管理员证书

3.选择(ise-span)并填写证书信息。



选择节点

4.选中[√] Admin用法。



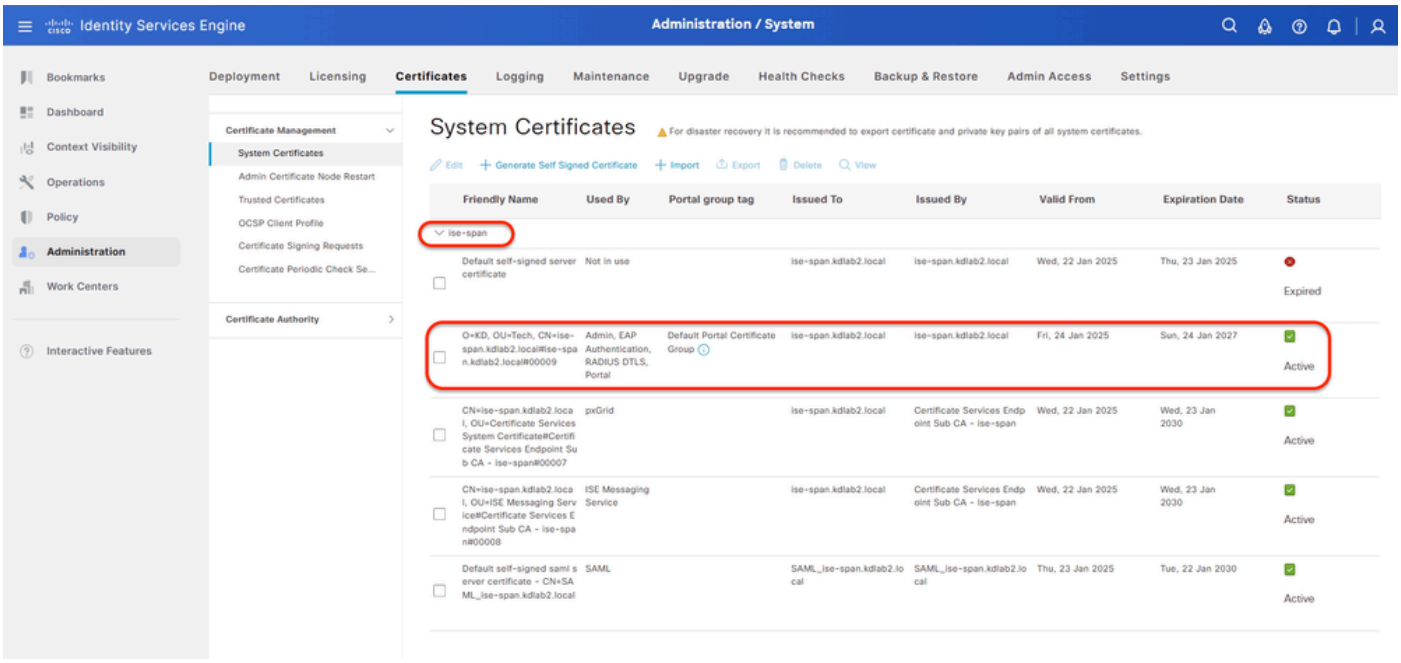
管理员使用情况

注意：在ISE节点上更改管理员角色证书的证书会重新启动服务。

5.单击提交。

6.验证上的新管理员证书(ise-span)。

导航到管理>系统>证书>证书管理>系统证书> 扩展(ise-span)。

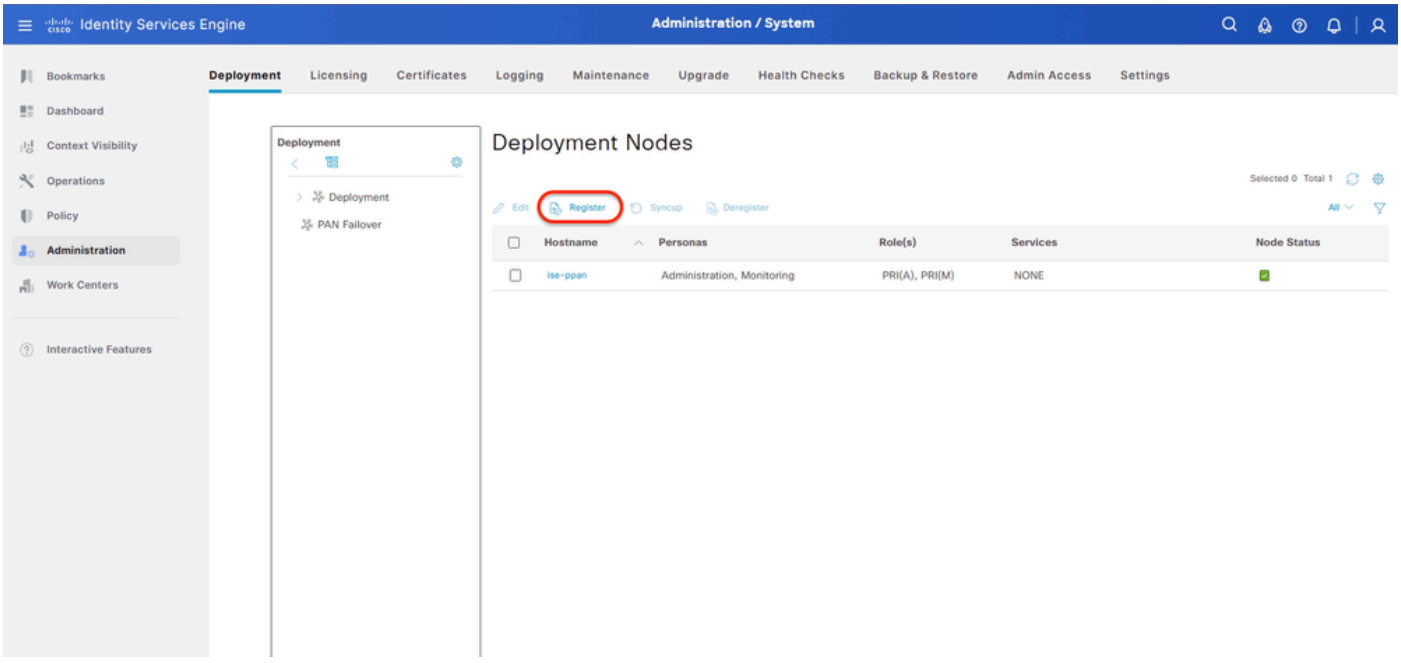


新管理员证书(ise-span)

步骤4.将辅助节点注册到分布式部署。

像以前一样设置您的部署角色和角色（Admin、MNT、PSN等）。

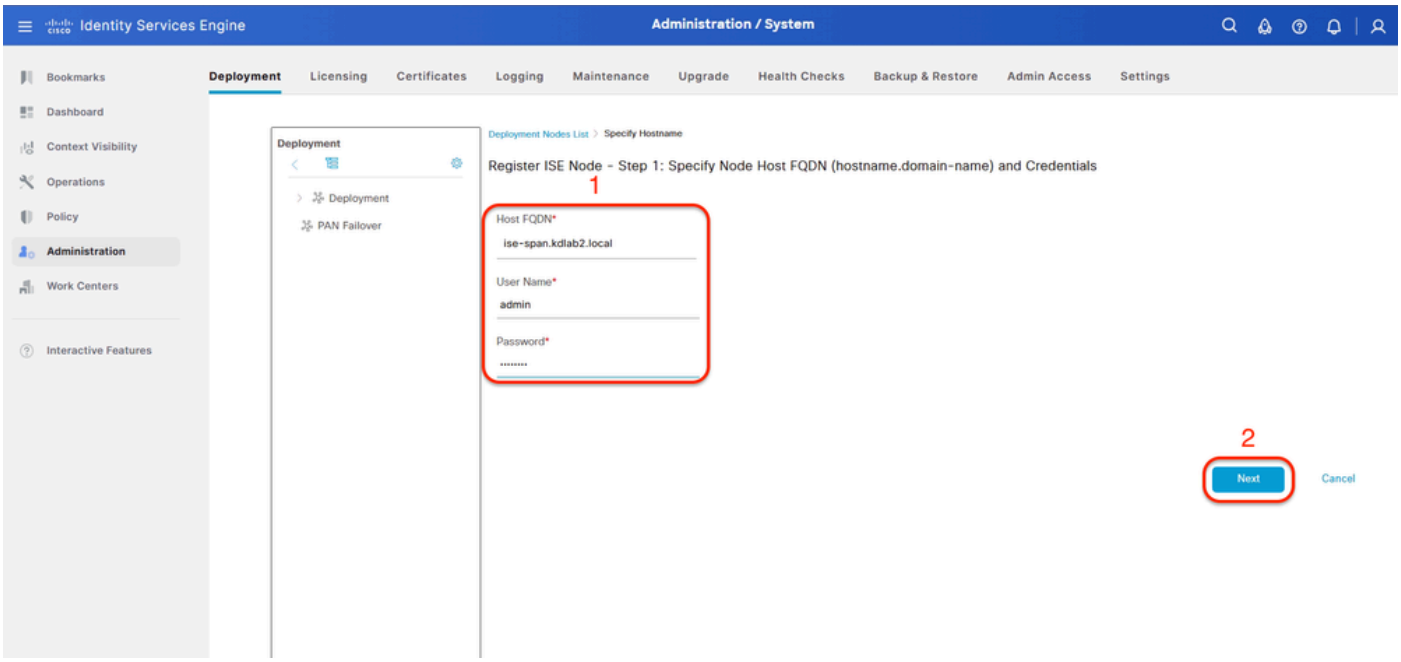
1.从主管理节点(PPAN)GUI中。导航到管理>系统>部署。单击“注册”。



主管理节点(PPAN)GUI

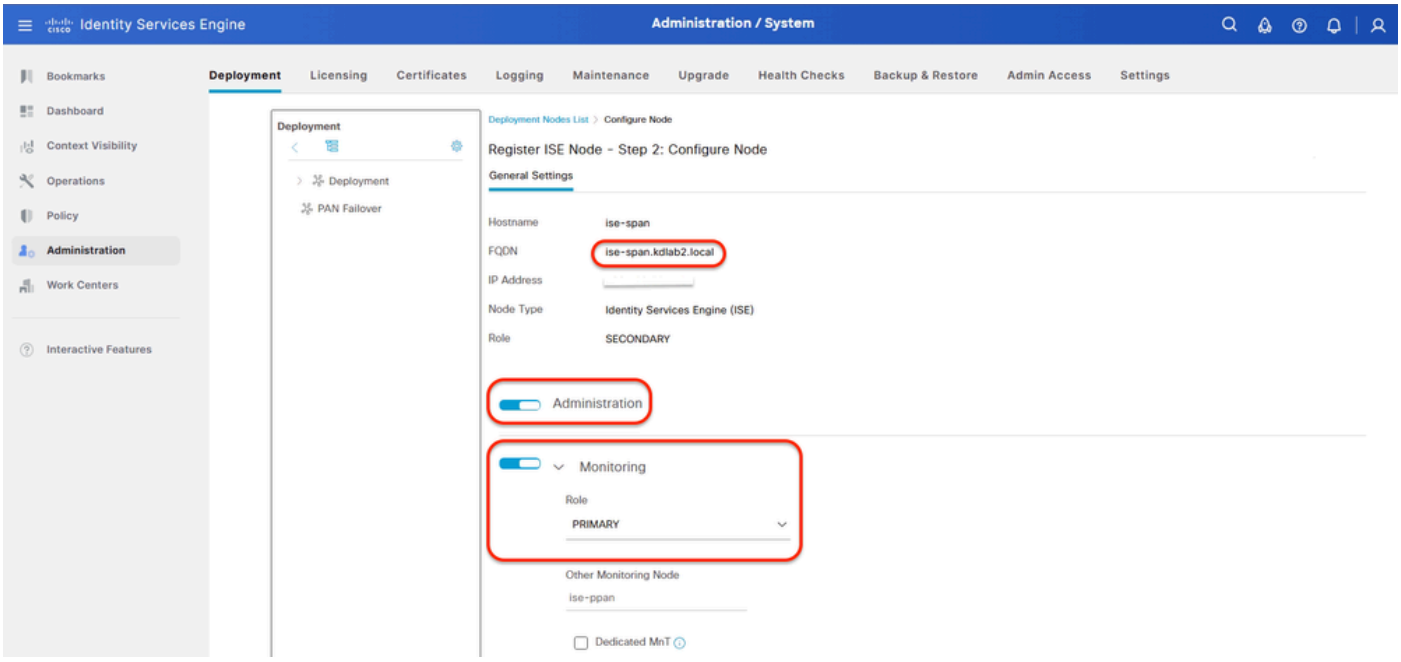
2.输入辅助节点的FQDN和凭证（用户名/密码）。

输入要注册的独立节点的DNS可解析的完全限定域名(FQDN)。(PPAN)的FQDN和要注册的节点必须能够彼此解析。



输入辅助节点访问

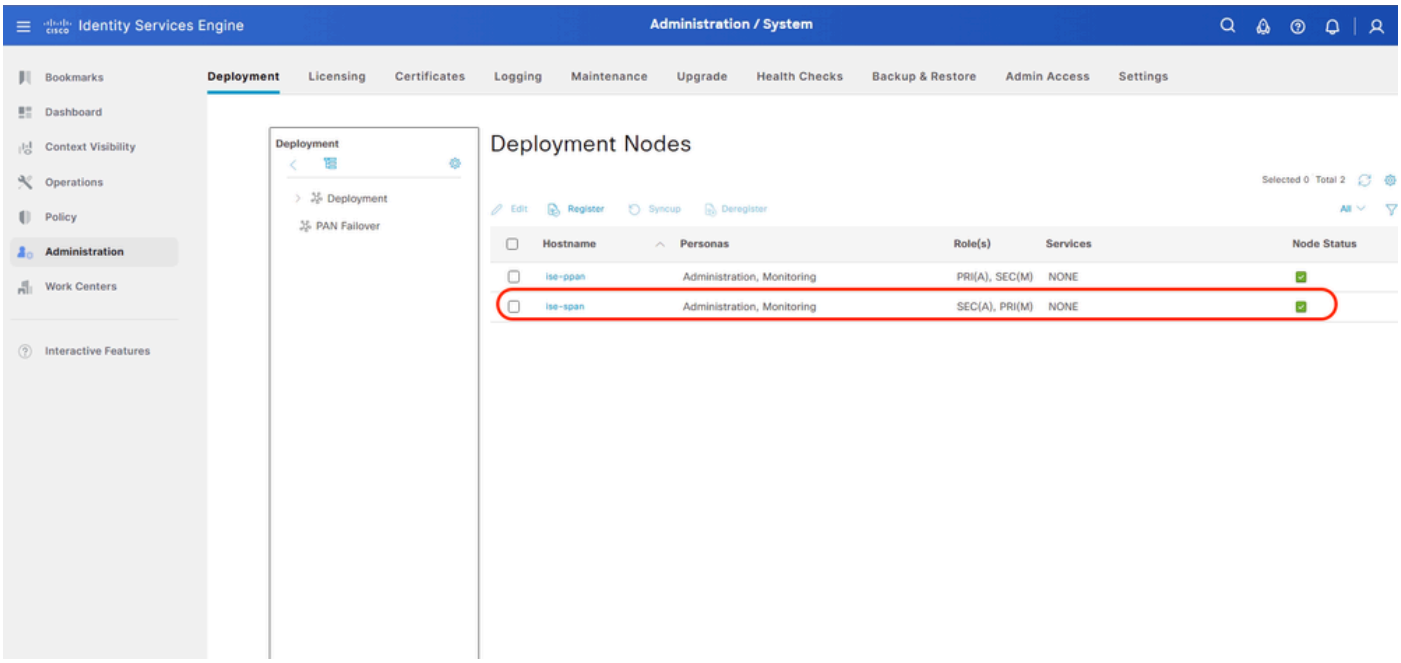
3.启用正确的人员和服务。



注册辅助节点(ise-span)

步骤5.检验部署状态。

导航到管理>系统>部署。



(ise-span)已添加到部署

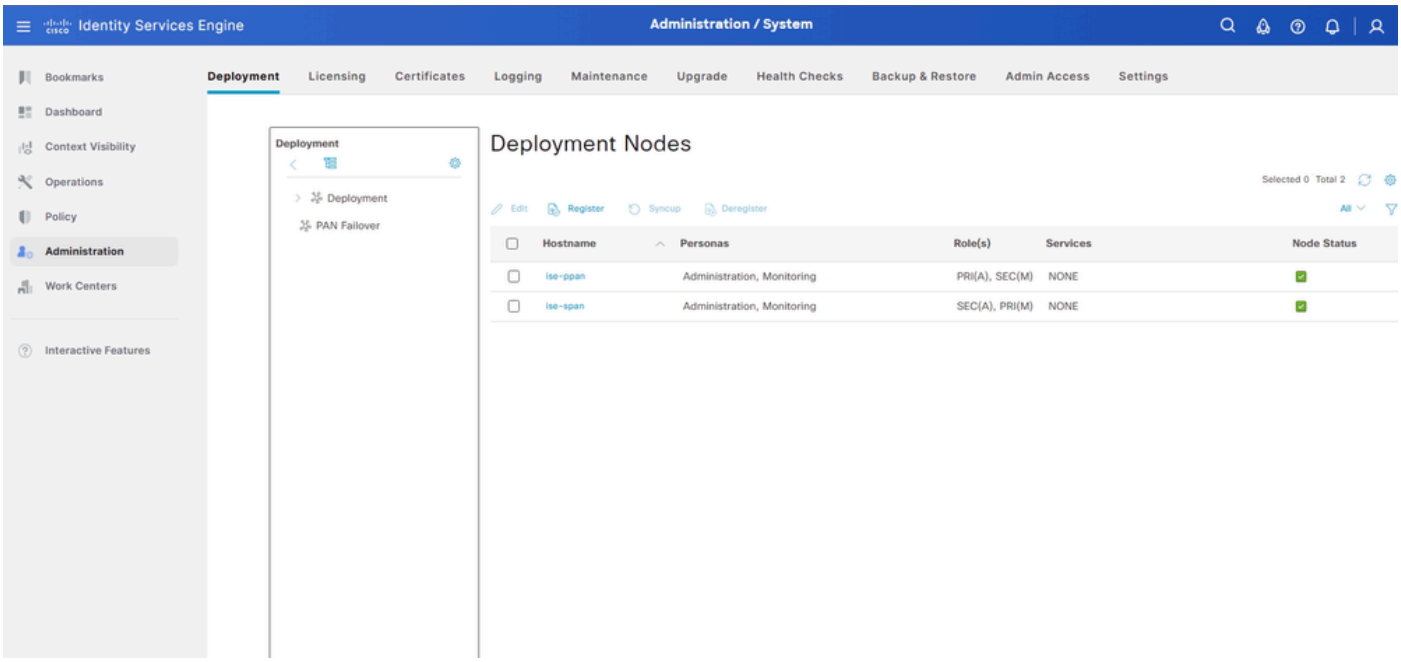
故障排除

使用案例1:已注销的辅助节点停滞在分布式状态(ise-psn1)

验证状态

步骤1.确认分布式部署状态。

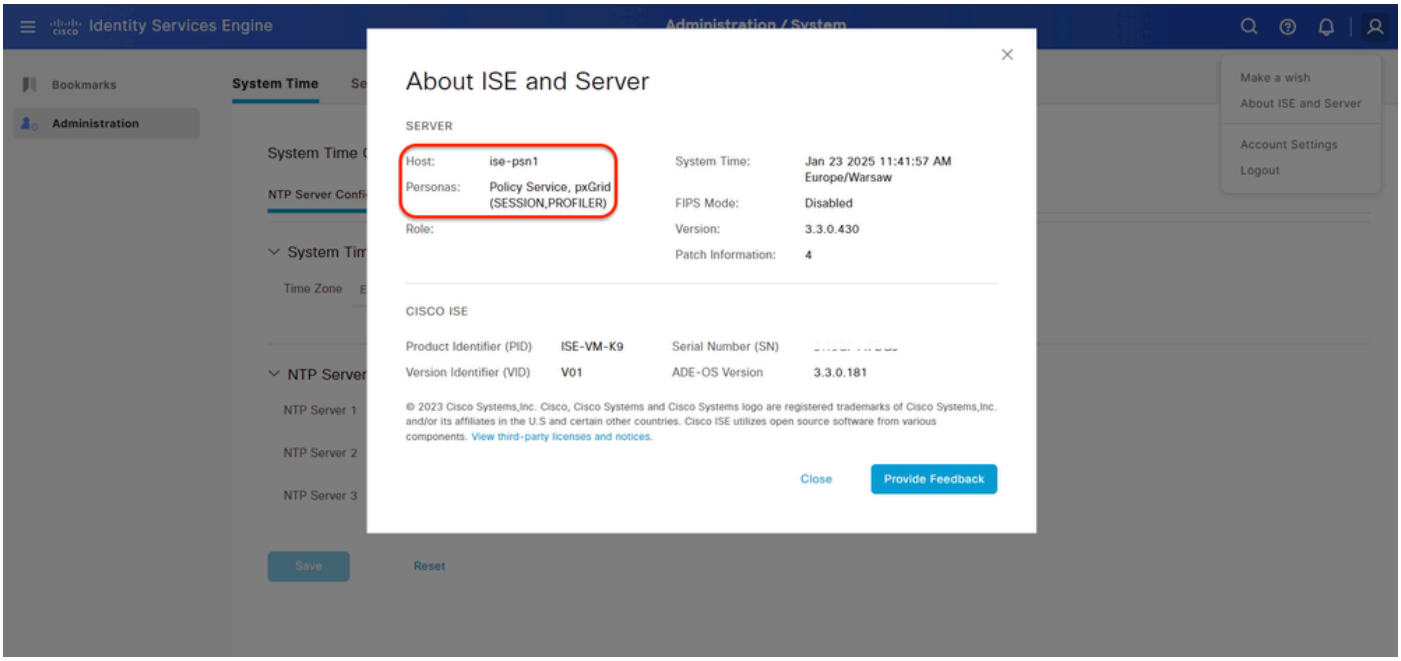
从主管理节点(PPAN)GUI。导航到管理>系统>部署。您可以确认此节点(ise-psn1)已取消注册。



(PPAN)部署节点

步骤2.确认(ise-psn1)节点状态。

通过GUI（KD实验室本地）浏览辅助节点，并导航登录>关于ISE和服务器。

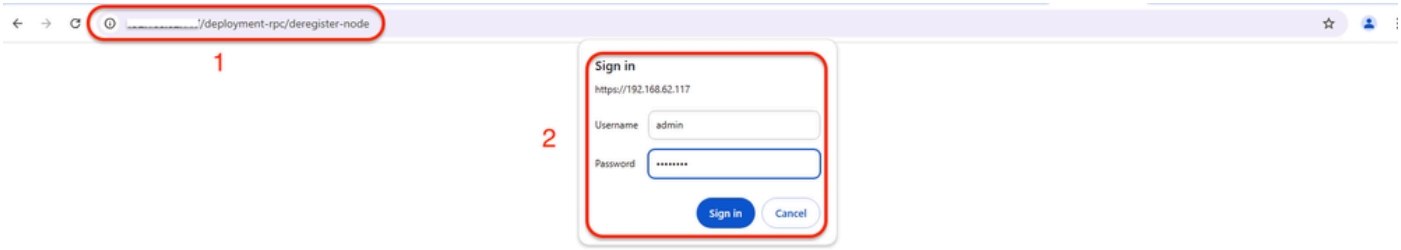


辅助节点(ise-psn1)停滞在分布式部署状态

解决方法

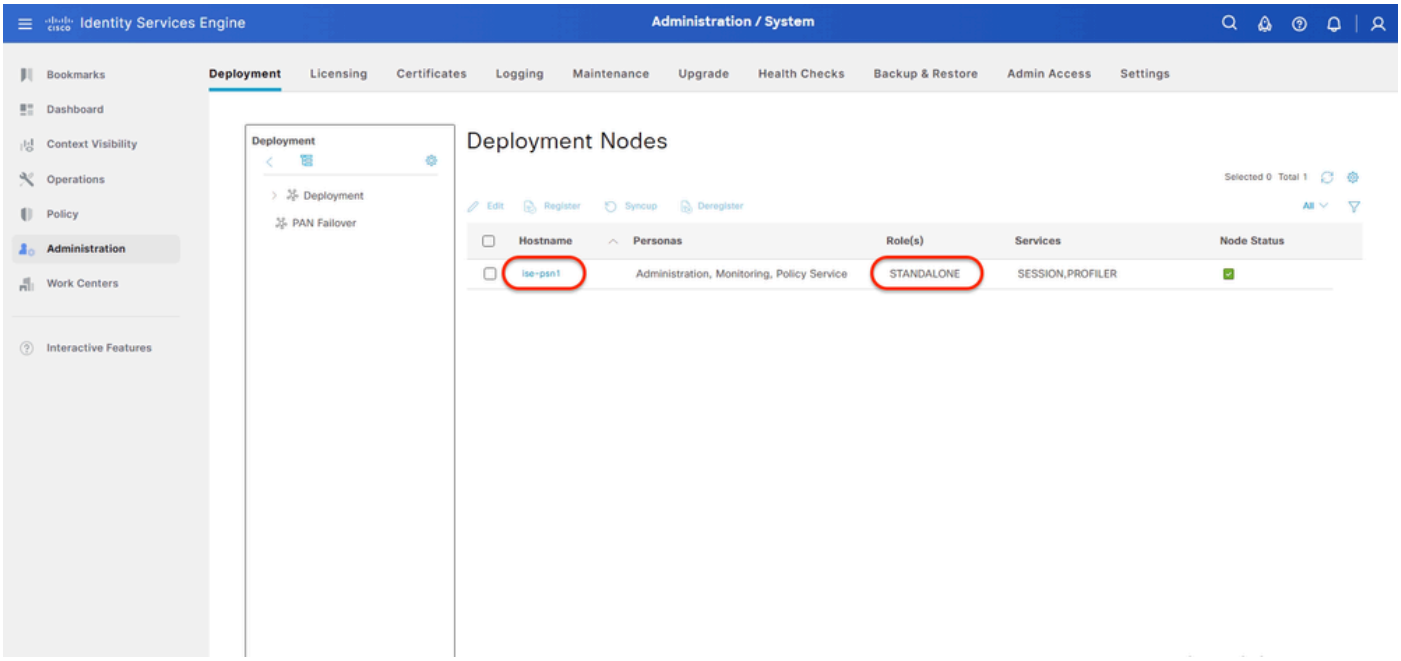
步骤1.手动注销(ise-psn1)节点。

通过GUI(Deregister Node)将(ise-psn1)节点实施到独立部署。



手动取消注册节点 — GUI

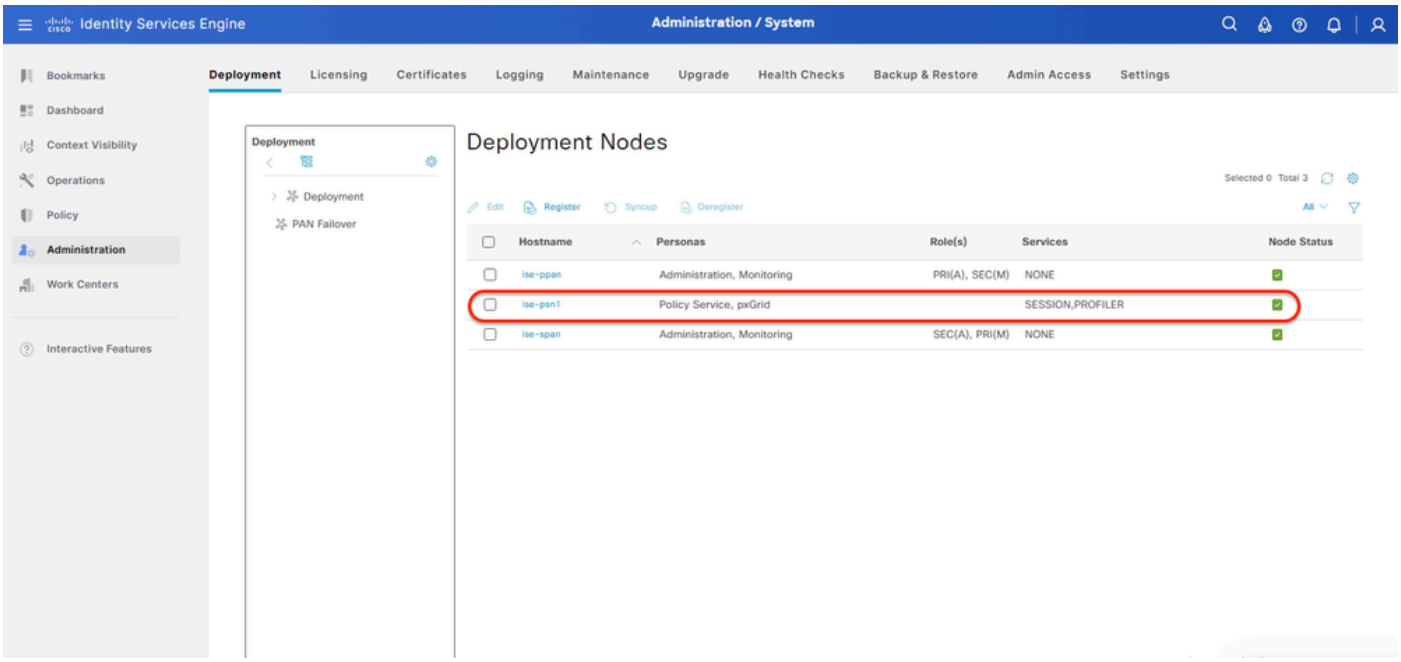
步骤2.在独立部署上，现在验证(ise-psn1)。



独立部署上的(ise-psn1)

步骤3.一旦确认节点处于独立状态，请继续执行Action Plan部分中的相同步骤：

1. 更新(ise-psn1)节点的管理证书。
2. 将(ise-psn1)节点注册到分布式部署。
3. 验证部署状态。



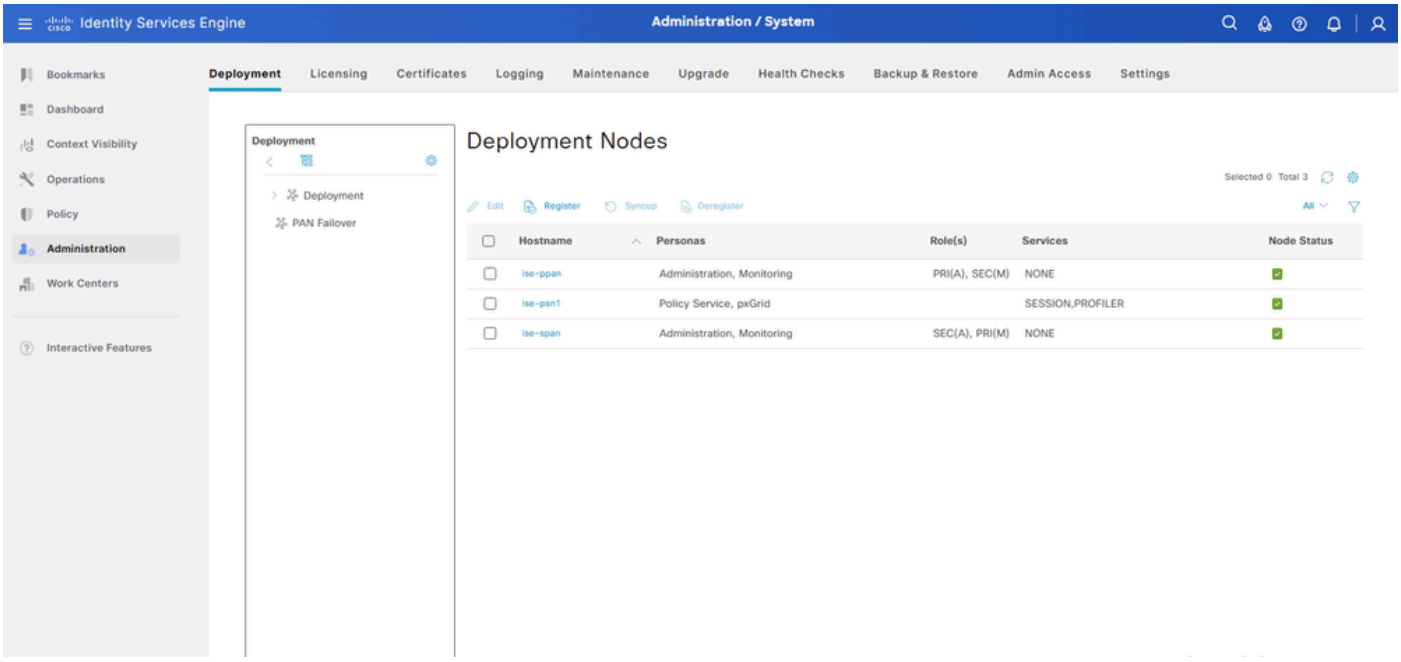
(ise-psn1)已添加到部署

使用案例2:取消注册的辅助节点GUI无法访问(ise-psn2)

验证状态

步骤1.确认分布式部署状态。

从主管理节点(PPAN)GUI。导航到管理>系统>部署。您可以确认此节点(ise-psn2)已取消注册。



(PPAN)部署节点

步骤2.确认(ise-psn2)节点状态。

由于管理员证书在某些情况下已过期，因此您可能会遇到以下症状：

- (ise-psn2)GUI无法访问。
- (ise-psn2)CLI(show application status ise)ISE应用停滞在（initializing或not running）。
- (ise-psn2)CLI(show tech)节点已在独立部署中。

```
*********************************************
Displaying ISE deployment ...
*********************************************
Node Config Details

NAME                PERSONA          ROLE       ACTIVE     REPLICATION
------------------- ---------------- ---------- ---------- ---------------
ise-psn2            PAN,MNT,PSN      STANDALONE ACTIVE     SYNC COMPLETED
```

(ise-psn2)在独立部署上

解决方法

第1步：更新(ise-psn2)节点的管理证书。

1. 通过CLI登录到(ise-psn2)。
2. 输入application configure ise。
3. 输入31（[31]生成自签名管理员证书）。
4. 是否要继续？y/[n]:y
5. 是否要在生成后替换现有证书？y/[n]:y

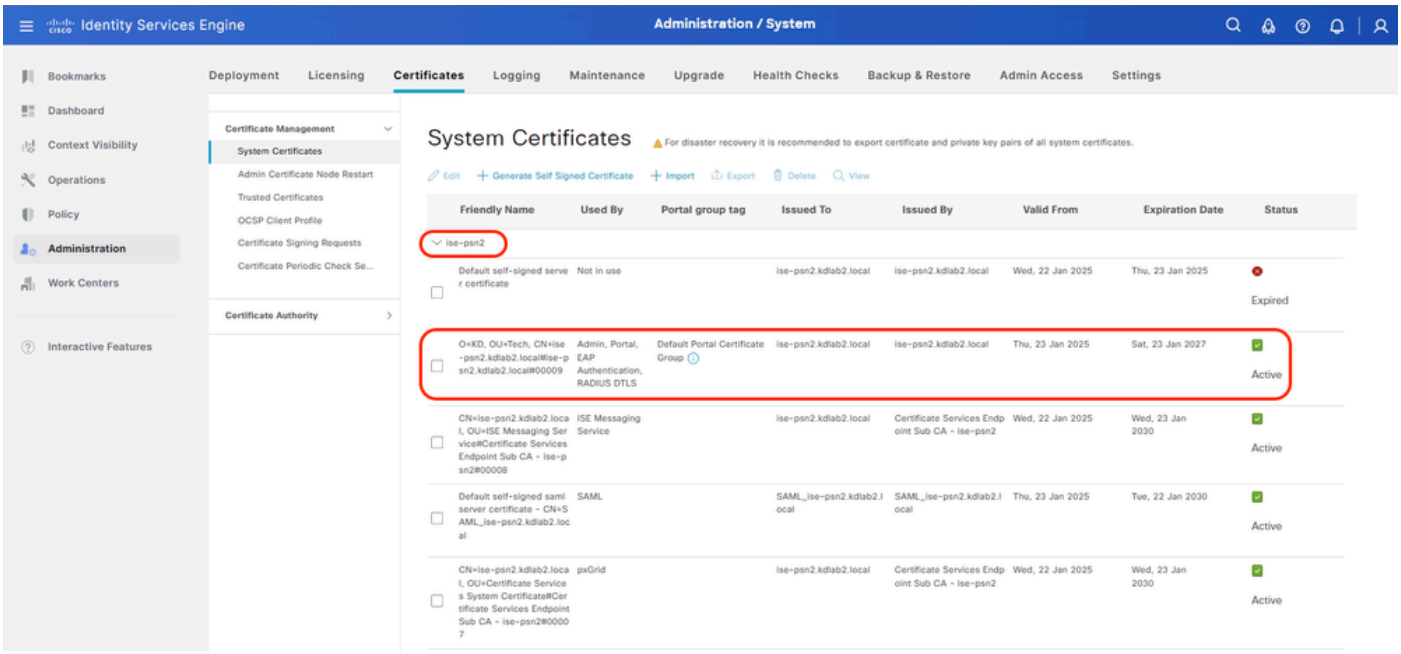
```
ise-psn2/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[31]Generate Self-Signed Admin Certificate
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[39]Reset System 360 Monitoring Page
[40]Enable/Disable Explicit EC Check
[41]Gather Diagnostic data for Certificates
[42]Enable/Disable Parse SAN DirName Extension
[0]Exit

31
After this operation, the ISE node will restart
Do you want to continue? y/[n]: y
Certificate Subject
  *Common Name (CN) : ise-psn2.kdlab2.local
  Enter Organization Unit (OU) : Tech
  Enter Organization (O) : KD
Do you want to replace existing certificate after generation? y/[n]: y
Old Memory Size : 32639004
```

续订(ise-psn1)管理员证书

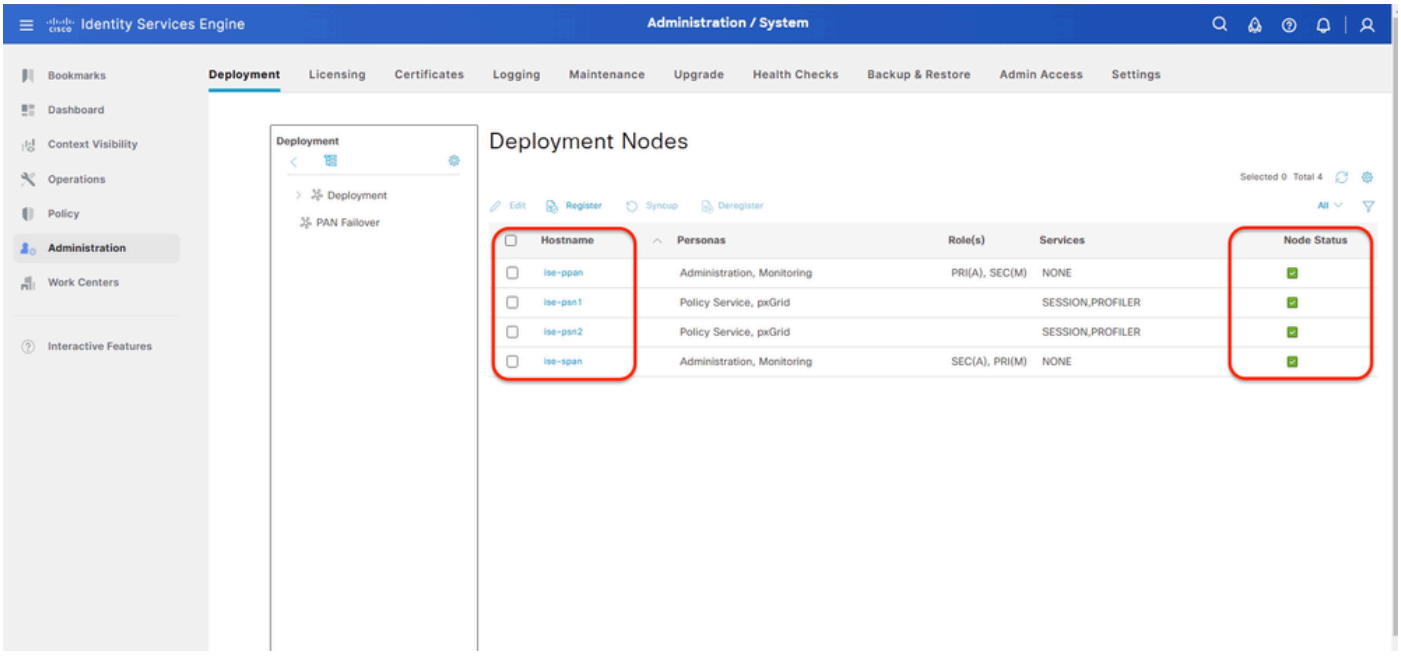
6.验证上的新管理员证书(ise-psn2)。



新管理员证书(ise-psn2)

步骤2.将(ise-psn2)节点注册到分布式部署。

步骤3.检验部署状态。



部署再次同步！

相关信息

- 思科ISE的部署

- Cisco ISE中的证书管理
- 在ISE上配置证书续订

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）。