

局部重要的证书(LSC)与WLC和Windows服务器2012配置示例

TAC

文档ID118838

已更新：2015年3月17日

贡献用罗马Manchur和尼古拉斯Darchis，Cisco TAC工程师。



[下载 pdf文档](#)



[打印](#)

[反馈](#)

相关产品

- [Certificate Authority \(CA\)](#)
- [公用密钥基础结构 \(PKI\)](#)
- [Cisco无线LAN控制器软件](#)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[MS Windows服务器配置](#)

[WLC 配置](#)

[验证](#)

[故障排除](#)

[相关的思科支持社区讨论](#)

简介

本文描述如何配置局部重要的证书(LSC)与无线局域网控制器(WLC)和一新安装的MS Windows服务器2012个R2。

注意：实时部署在许多点也许有所不同，并且您应该有设置的完全控制和知识在MS Windows服务器2012的。此配置示例为Cisco用户只提供，参考模板实现和适用他们的MS Windows服务器配置为了做LSC工作。

先决条件

要求

若需要您应该了解做的每个变化在MS Windows服务器上 and 检查相关Microsoft文档。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC版本7.6
- MS Windows服务器2012个R2

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

MS Windows服务器配置

此配置在一新安装的MS Windows服务器2012显示如执行。您必须适应步骤您的域和您的配置。

1. 安装活动目录角色的域服务并且以向导为特色。

在安装以后，您必须促进服务器到域控制器。

因为这是一个新的设置，您配置一个新的森林;但是典型地在现有部署，您配置在现有的域控制器的这些点。这里，您选择LSC2012.com域。这激活域名服务器(DNS)功能。

2. 在重新启动，安装Certificate Authority (CA)服务后以及Web登记。

配置他们。

选择企业CA并且留下一切作为默认。

3. 点击Microsoft Windows/开始菜单。

点击**管理工具**。点击**激活目录用户和计算机**。展开域，用鼠标右键单击**用户文件夹**，并且选择**新的对象>用户**。

在本例中，它被命名**APUSER**。一旦创建，您必须编辑用户和点击**MemberOf选项卡**，并且做它成员**IIS_IUSRS**组。

4. 安装网络设备登记服务(NDES)。

选择**IIS_USRS**组的帐户成员，在本例中的**APUSER**，作为NDES的服务帐户。

5. 导航到管理工具。

点击**互联网信息服务(IIS)**。展开**Server>站点>默认网站> Cert Srv**。对于**mscep**和**mscep_admin**，请点击**验证**。确保匿名验证启用。用鼠标右键单击**windows验证**并且选择**供应商**。确保**NT LAN Manager (NTLM)**是第一在列表。

6. 禁用在注册表设置的身份验证质询，否则简单认证登记协议(SCEP)期待私钥保护密码验证，WLC不支持。

打开**regedit**应用程序。去**HKEY_LOCAL_MACHINE \软件\ MICROSOFT \加密算法\ MSCEP **。设置**EnforcePassword**对**0**。

7. 点击Microsoft Windows/开始菜单。

键入**MMC**。在文件菜单，请选择**添加/删除管理单元**。选择**证书颁发机构**。用鼠标右键单击**认证模板文件夹**并且单击**管理**。用鼠标右键单击一个现有的模板，例如**用户**，并且选择**重复的模板**。

选择**CA是Microsoft Windows 2012个R2**。在常规选项卡，请添加一显示名称例如**WLC**和一个有效性周期。在主题名称选项卡，请确认在**请求的供应**选择。

点击**出版物需求选项卡**。思科建议您留下出版物在一个典型的分层的CA环境的策略空白：

点击**扩展选项卡**，**应用程序策略**，然后**编辑**。单击**添加**，并且保证客户端验证被添加作为应用程序策略。单击**Ok**。

点击**安全选项卡**，然后**添加....**保证在NDES服务安装中定义的**SCEP**服务帐户有模板的完全控制，然后单击**OK**键。

返回到证书颁发机构GUI界面。用鼠标右键单击**认证模板目录**。导航对**新>发出的认证模板**。以前选择WLC模板配置，并且点击OK键

更换在注册表设置的默认SCEP模板在**计算机> HKEY_LOCAL_MACHINE>SOFTWARE> Microsoft >加密算法> MSCEP**下。更改从IPsec (脱机请求)的EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate密钥到以前创建的WLC模板。

重新启动系统。

WLC 配置

1. 在WLC，请导航对Security菜单。点击**证书> LSC**。
2. 检查在**控制器复选框**。的**Enable (event) LSC**
3. 输入您的MS Windows服务器2012 URL。默认情况下，它带有**/certsrv/mscep/mscep.dll**。
4. 输入您的在**配置**部分的详细信息。
5. 应用更改。
6. 点击在上面的CA线路的蓝色箭头并且选择**添加**。它应该更改从**不现在的状态提交**。
7. 点击**AP Provisioning选项**。
8. 检查设置**Enable复选框**下面的AP并且点击**更新**。
9. 重新启动您的接入点他们是否未重新启动。

验证

接入点，在重新启动以后，加入返回和与LSC的显示作为在无线菜单的证书类型。

故障排除

目前没有针对此配置的故障排除信息。

本文档是否是有用？[有没有](#)

感谢您的反馈。

[打开支持案例](#)（需要[思科服务合同](#)。）

相关的思科支持社区讨论

[思科支持社区](#)是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 [Cisco Technical Tips Conventions](#)。

已更新：2015年3月17日

文档ID118838