发布ISE的证书撤销列表在Microsoft CA服务器配置示例

目录

简介

本文描述运行互联网信息服务微软认证授权(CA)服务器的配置(IIS)发布证书撤销列表(CRL)更新。它也解释如何配置思科身份服务引擎(ISE) (版本1.1和以上)获取更新用于证书确认。在证书确认使用的ISE可以配置获取多种CA根证明的Crl。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本1.1.2.145
- Microsoft Windows ®服务器® 2008 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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置

本文档使用以下配置：

- 部分1.创建并且配置在CA的一个文件夹安置CRL文件
- 部分2.创建IIS的一个站点显示新的控制分配点
- 部分3.配置Microsoft CA服务器发布CRL文件到分布点
- 部分4.验证CRL文件存在并且通过IIS是可访问
- 部分5.配置ISE使用新的控制分配点

部分1.创建并且配置在CA的文件夹安置CRL文件

首要任务是配置CA服务器的一个位置存储CRL文件。默认情况下， Microsoft CA服务器发布文件对C:\Windows\system32\CertSrv\CertEnroll\。而不是请使用此系统文件夹，请创建文件的一新文件夹。

1. 在IIS服务器上，请选择文件系统的一个位置并且创建新文件夹。在本例中，文件夹C:\CRLDistribution创建。
2. 为了CA能必须启用把CRL文件写到新文件夹，共享。用鼠标右键单击新文件夹，选择**属性**，点击**共享的**选项卡和然后单击**先进共享**。
3. 为了共享文件夹，请在共享Name字段检查**共享此文件夹**复选框然后添加美元的符号($)到共享名称的结尾隐藏共享。
4. 点击**权限**(1)，单击**加**(2)，点击**对象类型**(3)，并且检查**计算机**复选框(4)。
5. 为了返回对挑选用户，计算机，服务帐户或者组窗口，点击OK键。在回车对Select字段的对象名，输入CA服务器的计算机名称并且点击**检查名称**。如果输入的名称有效，名称刷新并且看上去加下划线。单击 **Ok**。
6. 在组或用户名名称字段，请选择CA计算机。检查**允许**完全控制授权对CA.单击**OK的**完全权限。再点击OK键关上先进的共享的窗口和返回到属性窗口。
7. 为了允许CA把CRL文件写到新文件夹，请配置适当的安全权限。点击**安全选项卡**(1)，单击**编辑**(2)，单击**加**(3)，点击**对象类型**(4)，并且检查**计算机**复选框(5)。
8. 在回车对Select字段的对象名，输入CA服务器的计算机名称并且点击**检查名称**。如果输入的名称有效，名称刷新并且看上去加下划线。单击 **Ok**。
9. 在组或用户名名称字段选择CA计算机然后检查**允许**完全控制授权对CA.单击**OK的**完全权限然后单击**接近**完整任务。

部分2.创建IIS的站点显示新的控制分配点

为了ISE能访问CRL文件，请做安置CRL文件可访问通过IIS的目录。

1. 在IIS服务器工具栏，请点击**开始**。选择**管理工具>互联网信息服务(IIS)管理器**。
2. 在左窗格中(叫作控制台结构树)，请展开IIS服务器名然后展开**站点。**
3. 用鼠标右键单击**默认网站**并且选择**添加虚拟目录**。
4. 在Alias字段，请输入一站点名称对于控制分配点。在本例中， CRLD被输入。
5. 在物理路径领域右边单击省略号(…)并且浏览到在创建的文件夹第1.部分精选文件夹并且点击OK键。点击OK键关上添加虚拟目录窗口。
6. 应该用左窗格突出显示在步骤输入的站点名称4。否则，当前请选择它。在中心的窗格中，请双击**目录浏览**。
7. 在右窗格中，请点击**Enable (event)**启用目录浏览。
8. 在左窗格中，再请选择站点名称。在中心的窗格中，请双击**配置编辑器**。
9. 在部分下拉列表中，请选择**system.webServer/安全/requestFiltering。在** allowDoubleEscaping的下拉列表中，请选择**真。在**右窗格中，请单击应用**。**

文件夹应该当前是可访问通过IIS。

部分3.配置Microsoft CA服务器发布CRL文件到分布点

即然新文件夹配置安置CRL文件，并且文件夹在IIS显示了，请配置Microsoft CA服务器发布CRL文件到新的位置。

1. 在CA服务器工具栏，请点击**开始**。选择**管理工具>认证机关**。
2. 在左窗格中，请用鼠标右键单击CA名称。选择**属性**然后单击**扩展**选项卡。为了添加新的控制分配点，请单击**添加**。
3. 在Location字段，请输入路径到在创建和共享的文件夹第1.部分。在第1部分的示例中，路径是：`\\RTPAAA-DC1\CRLDistribution$\`
4. 当Location字段填充，请从可变下拉列表选择**<CaName>**然后单击**插入键。**
5. 从可变下拉列表，请选择**<CRLNameSuffix>**然后单击**插入键。**
6. 在Location字段，请添附.crl对路径的末端。在本例中，位置是：`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`
7. 点击OK键返回到扩展选项卡。检查**发布Crl到此位置**复选框(1)然后单击**OK(2)**关上属性窗口。提示符出现为了权限能重新启动活动目录证书服务。点击**是**(3)。
8. 在左窗格中，请用鼠标右键单击**取消的证书**。选择**所有任务>发布**。保证新的CRL选择然后点击OK键**。**

Microsoft CA服务器应该创建在创建的文件夹的一个新的.crl文件第1.部分。如果新的CRL文件顺利地创建将没有对话，在好后单击。如果错误关于新的分布点文件夹返回，请仔细重复在此部分的每个步骤。

部分4.验证CRL文件存在并且通过IIS是可访问

验证新的CRL文件存在，并且那他们通过从另一个工作站的IIS是可访问，在您开始此部分前。

1. 在IIS服务器上，请打开在创建的文件夹第1.部分。应该有单个.crl文件现在用<CANAME>是CA服务器的名称的表<CANAME>.crl。在本例中，文件名是：`rtpaaa-CA.crl`
2. 从网络的一个工作站(理想地说在网络和ISE主要的Admin节点一样)，请打开Web浏览器并且浏览对<SERVER>是在配置的IIS服务器服务器名第2部分的http:// <SERVER>/<CRLSITE>，并且<CRLSITE>是为的第2.部分分布点选择的站点名称。在本例中， URL是：`http://RTPAAA-DC1/CRLD`目录索引显示，包含文件在step1观察了。

部分5.配置ISE使用新的控制分配点

在ISE配置获取CRL前，请定义间隔发布CRL。确定此间隔的策略是超出本文的范围之外。潜在的值(在Microsoft CA)是1个小时到411年，包括。默认值是1周。一旦确定了您的环境的一个适当的间隔，设置与这些说明的间隔：

1. 在CA服务器工具栏，请点击**开始**。选择**管理工具>认证机关**。
2. 在左窗格中，请展开CA.右键单击**取消的证书**文件夹并且选择**属性。**
3. 在CRL出版物间隔字段，请输入所需数量并且选择时间。点击OK键关上窗口和应用更改。在本例中，出版物间隔7天配置。您应该当前确认几注册表值，将帮助确定在ISE的CRL检索设置。
4. 输入**certutil - getreg CA \ Clock***命令确认ClockSkew值。默认值是10分钟。示例输出：
```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```
5. 输入**certutil - getreg CA \ CRLov***命令验证CRLOverlapPeriod是否手工设置。默认情况下CRLOverlapUnit值是0，表明手工的值未设置。除0之外，如果值是值，请记录值和单元。示例输出：
```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```
6. 输入**certutil - getreg CA \ CRLpe***命令验证CRLPeriod，在步骤3.设置。示例输出：
```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```
7. 计算CRL宽限期如下：如果CRLOverlapPeriod在步骤5设置：**重叠=** CRLOverlapPeriod，以分钟;：**重叠=** (CRLPeriod/10)，以分钟如果**重叠>** 720然后**重叠=** 720如果**重叠<** (1.5 * ClockSkewMinutes)然后**重叠=** (1.5 * ClockSkewMinutes)如果**重叠>** CRLPeriod，在分钟然后**重叠=** CRLPeriod以分钟宽限期= 720分钟+ 10分钟= 730分钟**示例：As stated above, CRLPeriod was set to 7 days, or 10248 minutes and CRLOverlapPeriod was not set.**

   a. OVERLAP = (10248 / 10) = 1024.8 minutes
   b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
   c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
   d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
   e. Grace Period = 720 minutes + 10 minutes = 730 minutes

   计算的宽限期是时间在之间，当CA发布下个CRL时，并且，当当前CRL超时时。ISE需要配置相应地获取Crl。
8. 登陆对主要的Admin节点并且选择**管理>System >证书**。在左窗格中，请选择**证书存储**。
9. 在您打算配置Crl的CA证书旁边检查证书存储复选框。单击 **Edit**。
10. 在窗口的底部附近，请检查**下载CRL**复选框。
11. 在CRL分类的URL字段，请输入路径对控制分配点，包含.crl文件，创建在第2.部分。在本例中， URL是：`http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. ISE可以配置定期获取CRL或根据，一般来说，也是固定间隔)的有效期(。当CRL发布时间隔是静态，更加及时的CRL更新获取，当使用时更加更高的选项。**自动地**单击单选按钮。
13. 少于在步骤计算的宽限期设置检索的值为值7。如果值集比宽限期长， ISE检查控制分配点，在CA发布下个CRL前。在本例中，宽限期计算是730分钟或者12个小时和10分钟。值10个小时将使用检索。
14. 设置重试间隔如适当为您的环境。如果ISE不能获取CRL在上一步的配置的时间间隔，将再试在此更短的间隔。
15. 请检查**旁路CRL验证，如果CRL不是**允许基于认证的验证的**接收的**复选框通常继续(和没有CRL检查)，如果ISE无法获取此CA的CRL在其最后下载尝试。如果此复选框没有被检查，与此CA发出的证书的所有基于认证的验证将发生故障，如果CRL不可能获取。

16. 检查**忽略CRL不是有效或已到期**复选框允许ISE使用已到期(或没有效) CRL文件，好象他们有效。如果此复选框没有被检查， ISE认为CRL无效在他们的有效日期之前和在他们的下一次更新时间之后。点击**“Save”**完成配置。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems