您的潜力，我们的动力

Microsoft
微软（中国）有限公司

高级应用程序开发和 Windows XP Service Pack 2

钟卫

微软（中国）开发与平台技术部

msdn

MSDN Webcasts

概述

- Windows XP SP2 和 RPC 限制
- Windows XP SP2 和 DCOM
- 课时小结

Windows XP SP2 和 RPC 限制

- RPC 增强功能
- RestrictRemoteClients 注册表设置
- 解决 RPC 不兼容性的方法
- EnableAuthEpResolution 注册表设置

RPC 增强功能

Windows 防火墙只允许在本地系统、网络服务或本地服务安全上下文中运行的进程打开用于 RPC 通信的端口

默认情况下，RestrictRemoteClients 注册表项拒绝对系统上的 RPC 接口的远程匿名访问，但存在一些例外情况

EnableAuthEpResolution 使 RPC 客户端能够调用已在 Windows XP SP2 系统上注册了动态端点的 RPC 服务器

RestrictRemoteClients 注册表设置

RestrictRemoteClients 注册表项强制 RPC 为所有接口执行一些额外的安全检查（即使接口没有已注册的安全回调）

RestrictRemoteClients 注册表项值

- RPC_RESTRICT_REMOTE_CLIENT_NONE (0)：使系统避开新的 RPC 接口限制
- RPC_RESTRICT_REMOTE_CLIENT_DEFAULT (1)：使系统限制对所有 RPC 接口的访问
- RPC_RESTRICT_REMOTE_CLIENT_HIGH (2)：使系统拒绝使用 RPC 的匿名调用

解决 RPC 不兼容性的方法

- 要求您的 RPC 客户端在与服务器应用程序联系时使用 RPC 安全性
- 通过在接口注册期间设置 RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH 标志，免除接口的身份验证要求
- 通过将注册表项设置为 RPC_RESTRICT_REMOTE_CLIENT_NONE (0)，强制 RPC 表现出与早期版本的 Windows 相同的行为

EnableAuthEpResolution 注册表设置

与解析端点相关的问题

- 默认情况下，由于新的 RestrictRemoteClients 项的默认值的缘故，在 Windows XP SP2 上对端点映射器接口的匿名调用将失败
- 必须修改 RPC 客户端运行时，以便对端点映射器执行经过身份验证的查询

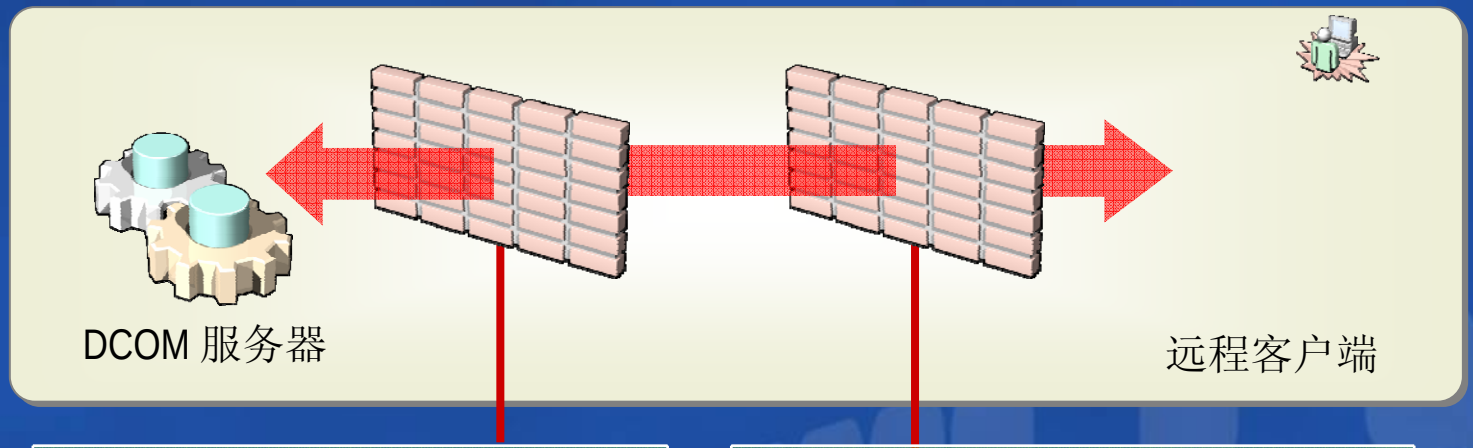
EnableAuthEpResolution 的用途

- 对于代表经过身份验证的调用执行的所有端点映射器查询，确保将使用 NTLM 或 Kerberos 身份验证执行这些查询
- 使 RPC 客户端能够调用已在运行 Windows XP SP2 的计算机上注册了动态端点的 RPC 服务器

Windows XP SP2 和 DCOM

- Windows XP SP2 DCOM 安全增强功能
- 针对 DCOM 的计算机范围的限制
- 细致的 COM 权限
- 细致的 COM 权限对自定义应用程序的意义

Windows XP SP2 DCOM 安全增强功能



特定的 COM 权限

能够限制用户可以获得的对各 COM 服务器的权限

计算机范围的限制

应用于 DCOM 激活、启动和调用特权的限制，以及区分本地和远程客户端的限制

针对 DCOM 的计算机范围的限制

Windows XP SP2 中的 DCOM

- 增加了计算机范围的访问控制，可管理对计算机中所有调用、激活或启动请求的访问
- 建立了额外的 AccessCheck
- 提供了要访问计算机上的 COM 服务器必须通过的最低授权“门槛”
- 提供了覆盖激活和启动的计算机范围的启动权限 ACL，以及覆盖调用的计算机范围的访问权限 ACL
- 提供了计算机范围的 ACL 这一替代方式，它替代了由特定的应用程序通过 CoInitializeSecurity 指定的弱安全设置

演示：将 Windows XP SP2 配置为 DCOM 服务器

在此演示中，您将学习如何将运行 Windows XP SP2 的计算机配置为 DCOM 服务器

细致的 COM 权限

本地和远程权限

- 管理员能灵活地根据“距离”概念控制计算机的 COM 权限策略
- 本地被定义为通过 LRPC 协议抵达的 COM 消息，而远程 COM 消息通过远程 RPC 协议（如 TCP/IP）抵达

分离调用和激活权限

- Windows XP SP2 改变了 COM 以分离调用和激活权限，并将激活权限从访问权限 ACL 移到启动权限 ACL
- 启动权限 ACL 可以在本地启动、远程启动、本地激活和远程激活权限中

细致的 COM 权限对自定义应用程序的意义

意义

- 使用默认安全设置的 COM 应用程序不会遇到兼容性问题
- 通过使用 COM 激活而动态启动的大多数应用程序将不会遇到兼容性问题，这是因为启动权限必须已包括能激活对象的任何人
- 对于已通过使用类似 Windows 资源管理器或服务控制管理器的机制启动的应用程序，可能会遇到兼容性问题

演示：配置 COM 权限

在此演示中，您将学习如何配置 COM 权限

课时小结

- Windows XP SP2 和 RPC 限制
- Windows XP SP2 和 DCOM

讲座评估

您的潜力，我们的动力

Microsoft
微软（中国）有限公司

msdn

MSDN Webcasts

获取更多MSDN资源

您的潜力，我们的动力

Microsoft
微软（中国）有限公司

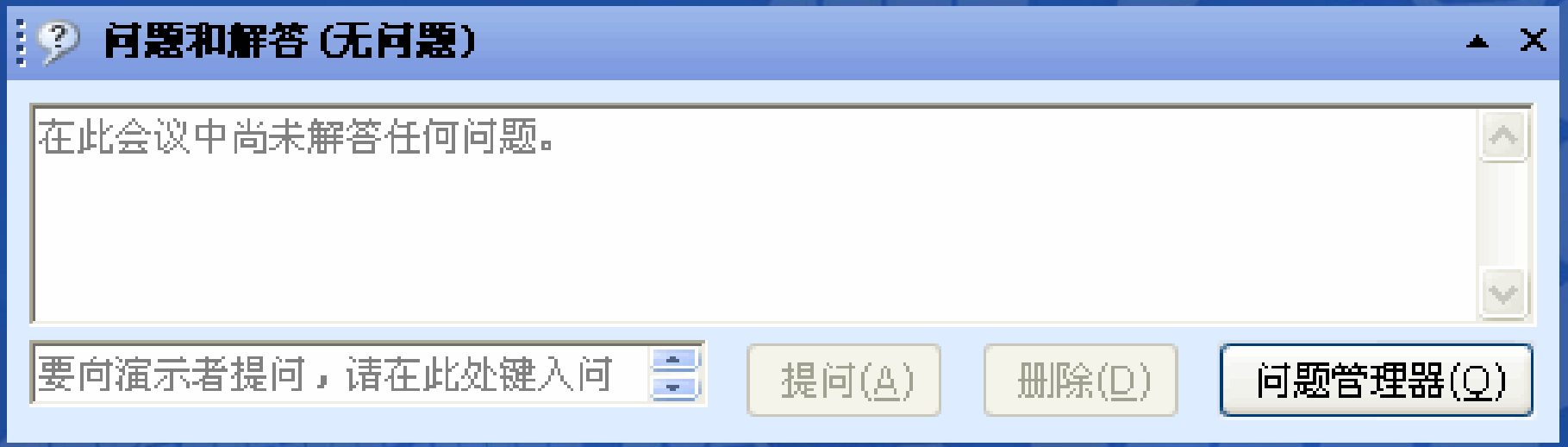
- MSDN中文网站
  http://www.microsoft.com/china/msdn
- MSDN中文网络广播
  http://www.msdnwebcast.com.cn
- MSDN Flash
  http://www.microsoft.com/china/newsletter/case/msdn.aspx
- MSDN开发中心
  http://www.microsoft.com/china/msdn/DeveloperCenter/default.mspx

Question & Answer

您的潜力，我们的动力

Microsoft
微软(中国)有限公司

如需提出问题，请单击“提问”按钮并在随后显示的浮动面板中输入问题内容。一旦完成问题输入后，请单击“提问”按钮。




您的潜力，我们的动力
Microsoft
微软（中国）有限公司
Microsoft
msdn
MSDN Webcasts