
# 创建网络访问隔离控制

# 创建网络访问隔离控制

NAQC(Network Access Quarantine Control，网络访问隔离控制)可以阻止从远程地址不受阻碍、自由地访问网络，直到目标计算机已经证明远程计算机的配置可以满足脚本中列出的特定要求和标准。

## NAQC 工作原理

为了使用 NAQC，你的远程访问客户必须在 Windows 98 Second Edition、Windows 千年版、Windows 2000、或 Windows XP Home 或 Windows XP Professional 上运行。

- NAQC 1：如何工作

## NAQC 创建过程

在创建 NAQC（(Network Access Quarantine Control，网络访问隔离控制）您需要创建确实能够访问的资源、编写在客户端运行的基线脚本、安装收听组件、创建隔离链接配置、给远程用户分配配置等步骤。

- NAQC 2：创建隔离源
- NAQC 3：编写基线脚本
- NAQC 4：安装收听组件
- NAQC 5：创建隔离链接配置
- NAQC 6：给远程用户分配配置

## NAQC 隔离策略

创建 NAQC 的最后一步是在 RRAS 内制定实际的隔离策略。如果你已经把配置安装器上传到作为隔离源功能的 Web 服务器上了，在这一部分中，我将要在 RRAS 中创建隔离策略。

### ❖ NAQC 7：制定隔离策略

## NAQC 1：如何工作

NAQC(Network Access Quarantine Control，网络访问隔离控制)可以阻止从远程地址不受阻碍、自由地访问网络，直到目标计算机已经证明远程计算机的配置可以满足脚本中列出的特定要求和标准。

为了使用 NAQC，你的远程访问客户必须在 Windows 98 Second Edition、Windows 千年版、Windows 2000、或 Windows XP Home 或 Windows XP Professional 上运行。这些 Windows 版本支持 connectoid，这只是一种拨号上网或者虚拟专用网(VPN)连接形式，位于用户界面中“网络连接”的要素之中，它包括三个基本要素：

- 连接信息，比如远程服务器 IP 地址、加密要求等等。
- 基线脚本，这是一个简单的批处理文件或程序，用来评定客户机的适配性（可能功能更多一点）。
- 通知人构件，该构件与目的网络的后端机器对话，并协商提高或降低客户机的隔离状态。

使用 Windows Server 2003 中的连接系统管理工具包（CMAK）可以将这三个要素集合为一种形式。此外，你在后端至少需要一台 Windows Server 2003 机器运行一个经批准的监听部件；出于该指南的目的，我将假设你正在运行 Windows Server 2003 Resource Kit 中的远程登录隔离代理（通常称为 rqs.exe），由于到发稿时为止，这是仅有的一种代理器。最后，你需要一种服从 NAQC 的 RADIUS 服务器，比如 Windows Server 2003 中的 Internet 验证服务，这样在连接过程中就可以使用指派的特殊 RADIUS 特性来限制网络访问。这里有一个详细的列表：假设你在来自 CMAK 的客户机终端上使用的是 rqc.exe，并且在来自 Resource Kit 的后端中使用的是 rqs.exe，在这种情况下，连接和隔离过程是如何工作的：

1．远程用户连接其计算机，在激活的隔离连接点使用隔离 CM connectoid，这是一台运行 RRAS 的计算机。

2．远程用户认证。

3．RRAS 向 RADIUS 服务器发送一个 RADIUS 访问-请求信息——这种情况下，Windows Server 2003 计算机运行 IAS。

4．IAS 服务器可以成功地核实远程用户的证书，并且核查其远程访问策略。连接目的需要与隔离策略的配置相匹配。

5．虽然接受了连接，但是得有隔离限制在适当的位置。IAS 服务器向 RRAS 发送一个 RADIUS 访问-接受信息，其中包括 MS-Quarantine-IPFilter 和 MS-Quarantine-Session-Timeout 特性。

6．远程用户采用 RRAS 服务器，完成了远程访问连接。包括租用一个 IP 地址，并建立其它网络设置。

7．目前在隔离模式下，RRAS 为连接配置 MS-Quarantine-IPFilter 和 MS-Quarantine-Session-Timeout。在这一点上，远程用户只能发送与隔离过滤器相匹配的通信，所有其他的通信都被过滤掉，在运行隔离基线脚本和结果返回给 RRAS 前，用户只能在几秒钟内，与 MS-Quarantine-Session-Timeout 特性保持连接。

8．CMAK 形式运行隔离脚本，目前被定义为“后连接行为”。

9．隔离脚本运行并检验远程访问客户机的配置是否满足基线。如果满足，脚本使用其命令行参数运行 rqc.exe，包括代表正在使用的隔离脚本版本的文字字串。

10．rqc.exe 向 RRAS 发送一个通知，表明脚本成功结束。

11．rqs.exe 在后端接收该通知。

12. 在 RRAS 服务器上的监听部件，使用配置在 RRAS 注册表中的字符串，来检验通知信息中的脚本的版本字符串，并返回表明脚本的版本是否有效的信息。

13. 如果脚本的版本是可以接受的，rqs.exe 调用 MprAdminConnectionRemoveQuarantine API，它向 RRAS 表明，应该从连接中移走 MS-Quarantine-IPFilter 和 MS-Quarantine-Session-Timeout 设置，并重新配置正常网络访问的期限。

14. 一旦这样做，远程用户就可以正常访问网络上的资源。

15. rqs.exe 在系统事件日志中，创建一个描述隔离连接的事件。

*（作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国）*

## NAQC 2：创建隔离源

对于远程客户端，当隔离封包过滤器在适当的位置时，您需要创建确实能够访问的资源。这样的资源例子包括 DNS 服务器和 DHCP 服务器，使得能够找回 IP 地址和其他链接信息，如后缀地址、DNS 服务器地址等等；文件服务器能够下载适当的软件更新出问题的机器；如果发生任何问题，Web 服务器能够描述隔离过程，或者允许远程用户通过 e-mail 联系 IT 支持商。

您可以用两种方法指定和使用隔离资源。第一个是找出某些服务器，它可以像那些隔离资源一样，能够覆盖您的网络。这可以让你使用一个现有的机器来放置隔离资源，但是您也必须为每一个现有的机器的隔离资源，创建单独的封包过滤器。考虑到性能和开支原因，最好在某个时期限制单独封包过滤器的数量。

如果您决定采取这种方法，您需要启动下表中列出的封包过滤器：

表 1 分布式隔离资源封包过滤器

| 通信类型 | 源端口 | 目的端口 | 替代品（而不是指定的端口信息） |
|---|---|---|---|
| 隔离 Notifier | 无 | TCP 7250 | 无 |
| DHCP | UDP 68 | UDP 67 | 无 |
| DNS | 无 | UDP 53 | 您也可以指定任何 DNS 服务器的 IP 地址。 |
| WINS | 无 | UDP 137 | 您也可以指定任何 WINS 服务器的 IP 地址。 |
| HTTP | 无 | TCP 80 | 您也可以指定任何 web 服务器的 IP 地址。 |
| NetBIOS | 无 | TCP 139 | 您也可以指定任何文件服务器的 IP 地址。 |
| Direct Hosting | 无 | TCP 445 | 您也可以指定任何文件服务器的 IP 地址。 |

您也可以设定任何其他的，针对您机构的特别的封包过滤器。

另一种方法是把您的隔离资源限制在一定 IP 子网。这样，您只需要一个封包过滤器，用以对一个远程用户隔离通信，但是您可能需要重新给机器分配地址，在大多数情况下，要把他们从现有服务中拿出或者购买新的。

使用这种方法，封包过滤器的要求比较简单。您只需在目的端口 TCP 7250 上，为 notifier 流量打开一个；在远端口 UDP 68 和目的端口 IDP 67 上，为 DHCP 流量打开一个；在专用隔离资源子网的地址范围，为其余的流量打开一个。其次，您也可以专门针对您的机构设定任何其它的封包过滤器。

*（作者：SearchWindowsSecurity.com 译者：李娜娜 来源：TT 中国）*

## NAQC 3：编写基线脚本

本文是创建 NAQC 的第三步：编写在客户端运行的基线脚本。你可以在你的 Windows 客户支持的脚本环境中，或者作为一个编译 EXE 程序编写脚本。这种脚本可以检测你想要检测的任何东西——基线水平没有标准，因为它只是你想要放到你的网络上的东西。你也可以使用脚本环境允许的任何类型的程序。基线脚本非常灵活，可以使用一所拥有的任何软件资源。

下面是批处理文件脚本：

```
@echo off

echo Your remote connection is %1

echo Your tunnel connection %2

echo Your Windows domain is %3

echo Your username is %4

set MYSTATUS=

REM Baselining checks begin here

REM Verify Internet Connection Firewall is enabled. Set CHECKFIRE

to 1-pass, 2-fail.

REM Verify virus checker installed and sig file up. CHECKVIRUS is
```

```
1-pass, 2-fail.

REM Pass results to notifier or fail out with message to user.

if "%CHECKFIRE%" = = "2" goto :NONCOMPLIANT

if "%CHECKVIRUS%" = = "2" goto :NONCOMPLIANT

rqc.exe %1 %2 7250 %3 %4 Version1-0

REM These variables correspond to arguments and switches for RQC.EXE

REM %1 = %DialRasEntry%

REM %2 = %TunnelRasEntry%

REM RQS on backend listens on port 7250

REM %3 = %Domain%

REM %4 = %UserName%

REM The version of the baselining script is "Version1-0"

REM Print out the status

if "%ERRORLEVEL%" = = "0" (

set ERRORMSG=Successful baseline check.

) else if "%ERRORLEVEL%" = = "1" (

set ERRORMSG=Can’t contact the RRAS server at the corporate
```

```
network. Contact a system administration.
) else if "%ERRORLEVEL%" = = "2" (
set ERRORMSG=Access is denied. Please install the Connection
Manager profile from http://location and attempt a connection
again.
) else (
set ERRORMSG=Unknown failure. You will remain in quarantine
mode until the session timeout is reached.
)
echo %ERRORMSG%
goto :EOF
:NONCOMPLIANT
echo
echo Your computer has failed a baseline check for updates on
echo your machine. It is against corporate policy to allow out of
echo date machines to access the network remotely. Currently
echo you must have Internet Connection Firewall enabled and
```

```
echo an updated virus scanning software package with the

echo latest virus signature files. For information about how to

echo install or configure these components, surf to

echo http://location.

Echo You will be permitted to access only that location until

Echo your computer passes the baselining check.

:EOF
```

当然，这个批处理文件非常简单。我已经在脚本中添加了必要的评论，这样你就可以跟着学习每一步了。有一点很重要，就是要记住你可以随心所欲的编写复杂的脚本；甚至可以编译特别的程序，因为 CMAK 中的 post-connect 脚本选项允许.exe 文件运行。

每个基线脚本的要求之一是，如果基线遵从检查成功而且包含一下参量，它就必须运行 rqc.exe：

```
rqc ConnName TunnelConnName TCPPort Domain Username ScriptVersion
```

这些切换和参数的解释如下：

ConnName 是远程访问服务器连接的名称，通常从连接管理器配置文件的%DialRasEntry%变量继承的。

TunnelConnName 是远程访问服务器隧道连接的名称，通常是从连接管理器配置文件的%TunnelRasEntry%变量继承的。

TCPPort 是 notifier 用来发送成功信息的端口。默认是 7250。

域名是远程用户的 Windows 安全域名，通常是从连接管理器配置文件%Domain%变量继承的。

用户名，如你所想，是远程用户，通常是从连接管理器配置文件%UserName%变量继承的。

ScriptVersion 参数是一个文本字符串，含有可以和 RRAS 服务器配合的脚本译本。你可以使用任何键盘字符，但是不能连续使用/0。

*（作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国）*

## NAQC 4：安装收听组件

远程访问隔离代理服务器，也就是众所周知的 rqs.exe，必须安装在 Windows Server 2003 上，使用 RRAS 接受外来呼叫。RQS 在 Windows Server 2003 资源工具包下载的地方，你可以在微软的网站 http://www.microsoft.com/windowsserver 上找到。一旦你运行了这个工具的安装，就要在开始菜单上的程序组中选择“Command Shell”选项，并运行 RQS_SETUP /INSTALL。这些文件将把合适的二进制复制你的系统上的“%SystemRoot%System32RAS”文件夹，并修改服务和注册设置，这样当系统启动的时候就可以听众就就可以自动开始了。

尽管如此，还需要一写手动设置来完成安装：你需要为基线脚本指定版本字符串。听众服务将会和远程计算机向存储在 RRAS 计算机上的值报告的版本相搭配，这样可以确保客户端使用一个脚本的最新的可接受版本。这是强制修改你的基线脚本的很好的方式：如果用户没有使用脚本的最新版本（也因此没有进行基于你的需求德最新的系统分析），他就不能从隔离状态中解放出来。

在运行从工具中下载的 RQS_SETUP 后，可以用以下步骤进行手动修改：

1. 打开注册表编辑器

2. 打开 HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Rqs

3. 右击右边的窗体，并选择新的字符串。

4. 给 AllowedValue 字符串命名

5. 然后双击新入口，加入关联到脚本的可接受版本字符串。

*(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国)*

## NAQC 5：创建隔离链接配置

下一步是创建隔离链接管理配置。它是你可能会为任何标准的拨号上网或 VPN 链接创建的普通配置，只是有一些改动。对于一个配置，你需要增加 post-connect 行为，这样你的基线脚本就可以运行，并向 RRAS 机返回成功或失败的信息。你还需要在配置中增加通知器。

让我们看看使用 CMAK 创建一个定制关联，包括必须的 NAQC 组件。

1. 管理工具菜单打开 CMAK，然后点击下一步离开介绍页面。

2. 选择创建一个新的服务配置，然后点击下一步。

3. 在服务名中，键入你想要这个链接使用的名称。这对于用户来说，应该是熟悉的，例如“链接到公司内网”或类似的事情。

4. 在文件名中，键入你想要服务配置使用的名称。这个名称是 CMAK 在奖励服务配置的时候创建的文件所使用的。在文件名中不要使用以下字符：

< SPACE > ! , ; * = / : ? ’ ″ < >

5. 点击下一步。

6. 假设你没有需要合并的 CM 配置，这样就可以简单地点击下一步，绕过显示页面。这个显示页面会要求你合并配置信息。

7. 如果你想要在登录上网页增加一行支持信息，就在支持信息窗口中键入——例如，“用户支持，发电子邮件到 support@hasselltech.net.”这是一个选择。王成后点击下一步。

8.指定服务是否需要界名，然后点击下一步。

9.如果你想要配置用户拨号上网网络登录，点击增加。在电话簿的拨号上网网络登录对话框中，键入你想要的拨号上网网络登录。点击下一步。

10.指定你是否想要分配详细的 DNS 或者 WINS 服务器地址或者拨号网络脚本，然后点击 OK。点击下一步。

11.如果你想要在服务配置中增加 VPN 支持，点击选择“本服务配置”检查栏，然后点击下一步。指定服务期地址栏中的服务器，指定你是否想要分配详细的 DNS 或 WINS 服务器地址，以及是否使用用于拨号连接的用户信任状，然后点击 OK。点击下一步。

12.（从这里开始隔离步骤）用户行为窗口出现。

13.从行为类型列表窗口中选择 Post-Connect，然后点击新按钮增加一个行为。新的用户行为对话框就出现了。

14.在描述窗口中，为 post-connection 行为键入一个描述性标题。在将要运行的程序中，输入你的基线脚本的名称。你也可以使用浏览器按钮查看。在参数栏中键入命令行转换和他们的参数。最后，检查下面的两个窗口，包括这个服务配置的用户行为程序和与用户互动的程序。

15.点击 Ok，然后你应该返回用户行为窗口。点击下一步。

16.继续适当地填充指导页面，指导你来到附加的文件页面。

17.点击增加，然后在下一步出现的对话中，输入 rqc.exe。你可以使用浏览器按钮进行图性搜索。一旦你完成了，就点击 OK。

18.你会回到附加的文件页面，在这里可以看到列出的 rqc.exe。点击下一步。

19.适当地完成剩余的指导。

*(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国)*

## NAQC 6：给远程用户分配配置

配置是创建在可执行文件里面的。你可以把这些文件分配给远程用户，这样他们就可以在他们的系统上自动运行，并在不需要任何干涉的情况下创建配置。在实际把可执行文件分配给你的用户时有几种选择。

你可以把可执行文件作为电子邮件信息的附件发送，或者更好的是，作为一个某个地方的 Web 服务器中的可执行文件的链接。在邮件信息中，你可以包含一个运行文件和使用所有远程访问的新连接的指导。你还可以运行可执行文件，作为登录上网下网的脚本，但是为了这么做，你需要让你的用户通过拨号连接登录，或者等到移动用户回到家庭网络，并且把公司链接到网络上。

无论你选择哪一种方法向你的用户传输配置安装器，你总是应该把配置安装器的最新版本放在隔离源的某个地方，这样那些没有绕过你的基线脚本的法规遵从检查的客户计算机，就可以在网站上冲浪，并下载最新版本而不需要危及将来网络的完整性。

*(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国)*

## NAQC 7：制定隔离策略

这个过程的最后一步是在 RRAS 内制定实际的隔离策略。如果你已经把配置安装器上传到作为隔离源功能的 Web 服务器上了，在这一部分中，我将要在 RRAS 中创建隔离策略。

1. 打开 RRAS 管理器

2. 在左边的窗口中，右击远程访问策略，然后选择从内容菜单中选择“新远程策略”。点击介绍页面中的下一步。

3. 策略制定方法页面显示出来了。进入隔离 VPN 远程访问链接找到策略名称。结束的时候，点击下一步。

4. 下一步显示的是访问方法页面。选择 VPN，点击下一步。

5. 在用户或群访问页面，选择群，点击增加。

6. 键入群名称。它应该允许存在于你网络上 VPN。如果所有的域名用户都有这个能力，输入每个人或者授权用户。我将会假设这个域有一个叫做 VPNUsers 的群，而它可以访问 VPN。点击 OK。

7. 你会回到用户或者群访问页面，而且你会看到你增加的群名称显示在列表框中。如果都正确，就点击下一步。

8. 认证方法页面显示。为了使这个例子显得简单，使用 MS-CHAP v2 认证协议，而它是由默认选择的。点击下一步。

9.在策略加密等级页面，确保最强的加密设置是只需要检查的选项。然后，点击下一步。

10.点击完成结束向导。

11.回到 RRAS 管理器，并点击新的隔离 VPN 远程访问链接策略，从内容菜单中选择功能。

12.进入高级标签，点击增加，在列表中包含入另一个属性。

13.增加属性的回话框就出现了。

14.点击 MS-Quarantine-Session-Timeout，然后点击增加。

15.在属性信息对话框，在属性参数框中键入隔离部分的时间。使用 60 的样本值，为了实验的目的，它将会以秒计算。点击 OK，然后再一次点击 OK 回到高级标签。

16.点击增加。在属性列表中，点击 MS-Quarantine-IPFilter，然后再次点击增加。一可以看到 IP 过滤器属性信息页面。

17.点击输入过滤器按钮，这样会显示入站过滤器会话框。

18.点击新建，增加第一个过滤器。增加 Ip 过滤器对话框就出现了。在协议区域，选择 TCP。在目标断电去，输入 7250。点击 OK。

19.现在，回到入站过滤器页面，只选择允许单选按钮下的信息包。

20.点击新建，为 DHCP 流量增加入站过滤器，重复上面的步骤，并包括先前描述的适当的端口数字和类型。遵循同样的指导，允许 DNS 和 WINS 流量。

21.点击新建，为隔离源增加一个输入过滤器，例如安置配置安装器的 Web 服务器。在有增加 IP 过滤器页面的目标网络中为隔离源指定合适的 IP 地址。

22. 最后，点击入站过滤器会话框中的 OK，保存过滤器列表。

23. 在编辑拨号配置对话框中，点击 OK，保存配置设置的改变。

24. 然后，再点击一次 OK。保存策略的改变。

*(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TT 中国)*