

# 使用 BlockIP2 加强 WebSphere MQ 的安全性

刘睿

## 1 WebSphere MQ 提供的安全设施概述

### 1.1 WebSphere MQ 的用户和授权机制

WebSphere MQ 的用户其实就是队列管理器所在的操作系统的用户。WebSphere MQ 的管理员就是操作系统的 mqm 组的成员，比如 UNIX 上都有一个 mqm 用户。注意修改用户是否从属于 mqm 组后，可能需要重新启动 WebSphere MQ 的队列管理器，才能使新的安全配置生效。

WebSphere MQ 的管理员可以使用 setmqaut 命令来给其他用户授权。可授权的 WebSphere MQ 对象类型包括队列管理器、队列、通道、侦听器、主题等等，可被授权的主体类型包括用户和组。可以使用 dspmqaut 命令来查看用户和组针对某一 WebSphere MQ 对象实例的权限。以上操作也可以通过 PCF 编程来实现。

例如：观察某用户 user1 针对队列管理器 VENUS 及其队列 Q1 的权限，可使用以下的命令：

```
dspmqaut -m VENUS -t qmgr -p user1
dspmqaut -m VENUS -t queue -n Q1 -p user1
```

假如用户 user1 不属于 mqm 组，授权 user1 可以通过 WebSphere MQ 客户机远程连接队列管理器，并读写队列 Q1，可使用以下命令：

```
setmqaut -m VENUS -t qmgr -p user1 +connect
setmqaut -m VENUS -t queue -p user1 +get +put +browse
```

### 1.2 WebSphere MQ 支持 SSL/TLS

WebSphere MQ 支持 Secure Sockets Layer (SSL)和 Transport Layer Security (TLS)协议。为实现对 SSL/TLS 的支持，与 SSL 相关的通道属性包括：SSLCIPH，SSLPEER，和 SSLCAUTH，其中 SSLCIPH 是最基本的。与 SSL 相关的队列管理器属性包括：SSLKEYR，SSLCRLNL，SSLCRYP，SSLTASKS，SSLRKEYC，和 SSLFIPS，其中 SSLKEYR 是最基本的。

WebSphere MQ 的 SSL/TLS 的支持的相关配置，在联机文档中有详尽的说明，这里就不再赘述。

### 1.3 WebSphere MQ 的通道出口程序和 BlockIP2 项目

WebSphere MQ 支持四类通道出口程序：

- Security exit
- Message exit
- Send exit
- Receive exit

其中 Security exit 最常被用来做安全控制。Security exit 对消息通道和 MQI 通道都起作用。设置 Security exit 的方法是设置通道的 SCYEXIT 属性。在 WebSphere MQ 的示例程序中，有一个 amqsaxe0.c 就是通道出口程序。

本文重点介绍的 BlockIP2 就是基于 Security exit 的一个开源的免费软件。BlockIP2 项目由 Joergen H. Pedersen 先生于 2002 年 12 月最初发布，目前(2008 年 11 月 12 日)的版本是 2.6.9。BlockIP2 支持的操作系统的至少包括 Z/OS，AIX，HP-UX，Solairs，Linux 和 Windows。可查阅其官方网站：<http://www.mrmq.dk/>

BlockIP2 可以大大增强 WebSphere MQ 消息通道和 MQI 通道(本文以下简称通道)的安全性，至少包含以下功能：

- 对 IP 地址进行过滤
- 根据 IP 地址和用户，以及 SSL 证书动态设置通道的实际用户 MCAUSER
- 访问通道的日志

## 2 . 使用 BlockIP2 增强 WebSphere MQ 通道的安全性

### 2.1 下载和安装 BlockIP2

用户可以从 <http://www.mrmq.dk/> 网站免费下载 BlockIP2。BlockIP2 的产品包包括源程序和以下平

台的编译版本：

- Z/OS
- AIX
- HP-UX
- Solaris
- Linux
- Windows

产品附带了红皮书文件 BlockIP2.pdf。在其中的“Compilation”一章中介绍了在各个操作系统平台

上使用的编译命令。

例如 WebSphere MQ for AIX v6.0 的编译命令如下：

```
xlc_r -q64 -e MQStart -bE:BlockIP2.exp -o BlockIP2 BlockIP2.c -I/usr/mqm/inc -L/usr/mqm/lib64
-lmqm_r -D_REENTRANT -DUNIX -DHNLUP -DAIX
cp ./BlockIP2 /var/mqm/exits64/
chgrp mqm /var/mqm/exits64/BlockIP2
chmod 750 /var/mqm/exits64/BlockIP2
```

其它平台的编译命令请参照 BlockIP2.pdf 中的说明。即使有了已经编译好的版本，重新进行编

译也是一个良好的习惯。注意 WebSphere MQ v7.0 的编译方式相对 v6.0 基本上没有什么变化。

安装 BlockIP2 的步骤非常简单：

1. 拷贝出口程序到 WebSphere MQ 默认的出口程序目录

a) 对于 UNIX 系统，执行以下命令：

```
cp /BlockIP2 /var/mqm/exits64/  
chgrp mqm /var/mqm/exits64/BlockIP2  
chmod 750 /var/mqm/exits64/BlockIP2
```

b) 对 Windows 系统，拷贝 BlockIP2.DLL 和 BlockIP2S.exe 到 %MQ\_FILE\_PATH%\exits 目录。

2. 针对通道，定义一个 BlockIP2 的配置文件(相关的说明参见下文)，假设名称为 BlockIP2.txt。

3. 设置通道安全出口程序

以下是一个实例，使用 runmqsc：

a) 对于 UNIX 系统，执行以下命令：

```
ALT CHL(TO.QM1) CHLTYPE(SVRCONN) SCYDATA('FN=C:\PATH\BlockIP2.txt;')  
SCYEXIT('BlockIP2(BlockExit)')
```

b) 对 Windows 系统，执行以下命令：

```
ALT CHL(TO.QM2) CHLTYPE(SVRCONN) SCYDATA('FN=/PATH/BlockIP2.txt;')  
SCYEXIT('BlockIP2(BlockExit)')
```

注意 SCYDATA 的值里面的分号不能被省略。

## 2.2 BlockIP2 的配置文件

编写 BlockIP2 的配置文件是使用 BlockIP2 的主要工作量。下面举一个比较实用的例子：

```
ASC=Y;  
  
Patterns=192.168.0.*,192.168.1.*,9.181.3.*;  
  
Userids=liurui,ad,user1;  
SSL=CN=mqli.ad;MCA=liurui;  
CON=192.168.1.*;MCA=user1;
```

```
CON=192.168.3.*;*;MCA=liurui;  
  
#LogPath=/logs/wmq
```

文件的第一行是“ASC=Y”，意思是允许 SSL 自签证书(Allow Selfsigned Certificates)，很多用户都是这样的用法。

BlockIP2 配置文件的每行的第一个词必须是一个 BlockIP2 规定的关键字，或者是代表注释行的“#”字符。BlockIP2 的关键字的详细说明可以参见红皮书文件 BlockIP2.pdf。注意分号是一个语法单句的结束，或者一个子句的结束，不可以忽略。注意每个语法句不能超过 4096 个字符。

这个作为示例的 BlockIP2 的配置文件包括了以下内容：

- IP 过滤
- 用户与 IP 的过滤和映射
- 日志

以下将分别予以说明。

## 2.3 设置 BlockIP2 来过滤非法的 IP

使用老式的 SNA 网络协议配置连接，双方都需要设置匹配才行。而 TCP/IP 的网络连接一般不需要服务器方知道发起连接的是谁。使用 WebSphere MQ 在 TCP/IP 网络中，如果黑客知道系统中的某 WebSphere MQ 服务器的侦听器的 IP 地址、端口以及相关通道的名称，就可以在任何一台网络可连接的机器直接进行访问，甚至以 mqm 用户的名义和权限建立通道，这就给系统的安全性造成了很大的麻烦。

BlockIP2 的最基本的特性就是可以对 IP 地址进行限制，防止与非法的 IP 建立通道连接。

可以使用 Patterns 语句定义允许访问的 IP 地址的列表。例如：

```
Patterns=192.168.0.*,192.168.1.*,9.181.3.*;
```

表示只允许 192.168.0.\*, 192.168.1.\*, 9.181.3.\* 这三类的 IP 地址来访问本通道。从这里也可以看出，

在 IP 地址中可以使用通配符“\*”和“?”。

Patterns 语句可以有多个，相互之间的关系是“或”的意思。例如：

```
Patterns=1.2.3.4,1.2.3.5,1.2.3.6; /* hosts 4,5,6 in the 1.2.3 network */  
Patterns=1.2.1.4,1.2.1.5,1.2.1.6; /* hosts 4,5,6 in the 1.2.1 network */
```

还可以使用更复杂的语法，例如以上两句与下面的一句相当：

```
Patterns=1.2.3.[4-6],1.2.1.[4-6];
```

还可以使用域名，例如：

```
Patterns=mrmqdk01.mrmq.dk,mrmqdk02.mrmq.dk,spyder,10.31.*;
```

## 2.4 设置 BlockIP2 来进行用户和 IP 的过滤和映射

对用户进行过滤可以使用 Userids 语句，指定所有允许访问通道的用户列表，例如：

```
Userids=liurui,ad,user1;
```

表示只允许 liurui, ad, user1 三个用户访问通道。

另一种常见的应用是根据 SSL 证书映射到某一个 MCA 用户，例如：

```
SSL=CN=mqli.ad;MCA=liurui;
```

表示如果 SSL 证书中指定 CN=mqli.ad，则映射为 MCA 用户 liurui。

注意有一个特殊的用户叫做“BLOCK”，意思是拒绝访问，例如：

```
SSL=CN=mqli.tom;MCA=BLOCK;
```

表示如果 SSL 证书中指定 CN=mqcli.tom，则拒绝访问。

根据 SSL 证书进行映射的语法有很多，详细的内容请参见产品的红皮书文件 BlockIP2.pdf。

另外，还可以使用一组 CON 语句，根据源 IP 地址以及用户名，匹配到真正使用的 MCA 用户。

CON 语句的规则是找到第一个匹配即停止搜索。以下举几个例子：

```
CON=192.168.1.*;*;MCA=user1;  
CON=192.168.3.*;*;MCA=liurui;
```

表示把所有 192.168.1.\* 的访问映射为 MCA 用户 user1，表示把所有 192.168.3.\* 的访问映射为 MCA 用户 liurui。

```
CON=*;mqm;MCA=BLOCK;
```

表示拒绝所有使用 mqm 用户的访问。

```
CON=10.31.*;usr*;MCA=BLOCK
```

表示所有来自 10.31.\*，且用户名称以 usr 打头的访问被拒绝。

```
CON=172.20.10.31;master03;
```

表示允许来自 172.20.10.31 且用户名为 master03 的访问。

```
CON=10.*;spider;MCA=master04;
```

表示来自 10.\* 且用户名为 spider 的访问使用 MCA 用户 master04。

```
CON=*;*;MCA=BLOCK;
```

表示拒绝所有的访问。

## 2.5 设置 BlockIP2 来做通道访问的日志

许多用户希望记录通道被访问的情况。BlockIP2 就可以被用来做这个事情。BlockIP2 配置文件有

许多语句来定义日志的写法，即使不定义，也会默认在 WebSphere MQ 的 exits 目录里面生成若干个日志文件，名称为“BlockIP200#.txt”，并循环使用，这种做法很象 WebSphere MQ 中“AMQERR0#.LOG”文件的使用方法。

一段典型的日志如下文所示：

```
2008-11-11|14:25:23|Channel closed [VENUS.SVRCONN] Connection Name [192.168.1.3]
2008-11-11|14:25:27|CON Set MCA userid to [user1] from [ad] [i1 e16]
2008-11-11|14:25:27|Connection accepted, Channel [VENUS.SVRCONN] ConName [192.168.1.3]
Flags [ASC=Y] User [ad]
2008-11-11|14:25:27|Channel closed [VENUS.SVRCONN] Connection Name [192.168.1.3]
2008-11-11|14:25:31|CON Set MCA userid to [user1] from [ad] [i1 e16]
2008-11-11|14:25:31|Connection accepted, Channel [VENUS.SVRCONN] ConName [192.168.1.3]
Flags [ASC=Y] User [ad]
2008-11-11|14:25:35|CON Set MCA userid to [user1] from [ad] [i1 e16]
2008-11-11|14:25:35|Connection accepted, Channel [VENUS.SVRCONN] ConName [192.168.1.3]
Flags [ASC=Y] User [ad]
2008-11-11|14:25:35|Channel closed [VENUS.SVRCONN] Connection Name [192.168.1.3]
2008-11-11|14:27:08|Channel closed [VENUS.SVRCONN] Connection Name [192.168.1.3]
2008-11-11|18:04:12|CON Set MCA userid to [user1] from [ad] [i1 e16]
2008-11-11|18:04:12|Connection accepted, Channel [VENUS.SVRCONN] ConName [192.168.1.3]
Flags [ASC=Y] User [ad]
2008-11-11|18:04:21|Channel closed [VENUS.SVRCONN] Connection Name [192.168.1.3]
```

下面简要地介绍一下与日志有关的比较常用的配置语句(详细说明请参见红皮书文件 BlockIP2.pdf)：

LogPath 指定日志文件的路径，默认是在 WebSphere MQ 的 exits 目录。

LogFileName 指定日志文件名，默认是 BlockIP2。

LogCount 指定日志文件的个数，默认是 3，最大是 99。

LogSize 指定日志文件的最大大小，默认是 200KB，最小是 100KB。

LogFormat 指定日志文件的格式，详见 BlockIP2.pdf。

### 3 . 结束语

自从 BlockIP2 发布以来，得到了世界各地很多 WebSphere MQ 用户的青睐，使用范围遍及 IBM 大型主机、各种UNIX 以及 Linux 和 Windows 平台。如果您也是一位WebSphere 的用户或者技术人员，我相信您也会从中受益。