API - Suporte #2245

Acesso a máquina virtual

10/31/2011 02:08 PM - Miguel Lopes Luis

Status:	Fechado	**Start date:**	10/31/2011
Priority:	Imediata	**Due date:**	
Assignee:	Tiago Simoes Batista	**% Done:**	0%
Category:	Servidor Linux	**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Boa tarde,

nao consigo aceder à maquina virtual.
Não responde a pings.
Quando poderei ter acesso?

Obrigado.

History

#1 - 10/31/2011 03:05 PM - Tiago Simoes Batista

- Status changed from Novo to Fechado

Quando te apanhar na praça pagas-me um copo que te lixas!!!!

Já fiz reset às regras da tua firewall..... O que vale é que trancas a casa toda mas deixas a fechadura debaixo do tapete :D

Bom trabalho

#2 - 10/31/2011 03:22 PM - Miguel Lopes Luis

A conta de root muda de password quando faz reboot?

#3 - 10/31/2011 03:24 PM - Tiago Simoes Batista

Sim, é um bug que eu ainda não corrigi.... não pensei que voces andassem a fazer reboot das máquinas!

Na proxima versão da coisa prometo que verifico isso!

#4 - 11/02/2011 04:13 PM - Miguel Lopes Luis

Como é que é suposto actualizar o kernel no Scientific Linux?

#5 - 11/03/2011 09:26 AM - Tiago Simoes Batista

Já te destranquei a máquina de novo... para a próxima, por favor começa por usar um script decente para criares a firewall, recomendo o que deixo abaixo. Tens que editar as redes administrativas (aqui apenas mostro a do IT) e os portos que queres abrir ao publico e/ou para as rede administrativas.

Não recomendo que tentes filtrar tráfego de saída num servidor, isso dá jeito é num router, mas num servidor tens total controlo sobre o que está a correr... Se tiveres desconfianças, adiciona as regras que quiseres ao OUTPUT, e no fim mete um -J LOG (não metas a politica DROP), por forma a gravares tudo o que sai fora dos padrões autorizados, a partir da informação recolhida então faz uma versão melhorada do filtro.

Com relação ao kernel... Esta uma máquina como outra qualquer... A documentação para RHEL6, CENTOS6 e SL6 deverá ser toda válida! Mas se vais trabalhar nisso recomendo VIVAMENTE que testes numa VM local antes de tentares meter nesta!

Este script não foi testado em SL6, apenas em CENTOS 5.6 onde está a gerir uma firewall simples mas funcional. Não sei se em SL6 continuam a

existir todos os módulos, existe a possibilidade de alguns terem mudado de nome e de outros virem potencialmente simplificar este script....

```
#!/bin/sh
# Autor: Tiago Simoes Batista a19944@gmail.com
#
#
# Hosts do IT:
#    193.136.92.0/255.255.254.0
#
#
# Portos públicos:
#     443  (https)
#     80   (http)
#
# Portos administrativos:
#     7002 (weblogic admin sobre https)
#     7003 (weblogic Server-0 sobre http para testes)
#     7004 (seblogic Server-0 sobre https para testes, self signed)
#     8081 (oracle apex)
#     8443 (tomcat sobre https)
#     3306 (mysql)
#     1521 (oracle XE)
#     22   (ssh)
#
# Protocolos extra a aceitar:
#     icmp (throthled)
#
# Interfaces onde tudo é permitido:
#     lo
#

PUBLIC_PORTS="443,80" #https, httpd

ADMIN_PORTS="7002,7003,7004,8443,8081,3306,1521,22" #wl admin, wl Server0 (http), wl Server0 (https), tomcat,
apex, mysql, oracle XE, ssh

# Redes separadas por espacos
ADMIN_NETS="193.136.92.0/255.255.254.0 192.168.0.0/255.255.0.0 172.16.0.0/255.240.0.0 10.0.0.0/255.0.0.0"

######### binaries #############
IPTABLES=`which iptables`
IP6TABLES=`which ip6tables`

if [ "X`whoami`" != "Xroot" ]; then
    IPTABLES="`which sudo` $IPTABLES"
    IP6TABLES="`which sudo` $IP6TABLES"
fi

# reset, iniciar tudo a partir de um estado conhecido:
$IPTABLES -F
$IPTABLES -X
for i in `cat /proc/net/ip_tables_names`; do
    $IPTABLES -t $i -F
    $IPTABLES -t $i -X
done

# Ignora tudo o que vem do exterior a não ser que seja permitido explicitamente
# Nota: Se for necessário auditar tráfego nesta máquina, isto tem que mudar
$IPTABLES -P INPUT DROP

$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A FORWARD -i lo -j ACCEPT

# Aceitar icmp apenas se o rate não for muito elevado
$IPTABLES -A INPUT -p icmp -m limit --limit 10/min -j ACCEPT

# Aceitar sessões já estabelecidas
$IPTABLES -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Permitir acesso do exterior
$IPTABLES -A INPUT -p tcp -m tcp -m multiport --dports $PUBLIC_PORTS -m conntrack --ctstate NEW -j ACCEPT

# Permitir acesso administrativo
for NET in $ADMIN_NETS; do
    $IPTABLES -A INPUT -s $NET -p tcp -m tcp -m multiport --dports $ADMIN_PORTS -m conntrack --ctstate NEW -j
```

```
ACCEPT
done

# Repetir tudo para IPV6, se o modulo estiver disponivel

[ ! -f  /proc/net/if_inet6 ] && exit 0

# reset, iniciar tudo a partir de um estado conhecido:
$IP6TABLES -F
$IP6TABLES -X
for i in `cat /proc/net/ip6_tables_names`; do
    $IP6TABLES -t $i -F
    $IP6TABLES -t $i -X
done

# Ignora tudo o que vem do exterior a não ser que seja permitido explicitamente
# Nota: Se for necessário auditar tráfego nesta máquina, isto tem que mudar
$IP6TABLES -P INPUT DROP

# Impedir o forward de uma placa para outra
$IP6TABLES -P FORWARD DROP

# Tráfego gerado por nos pode sair
$IP6TABLES -P OUTPUT ACCEPT

# Aceitar (e encaminhar) tudo em lo
$IP6TABLES -A INPUT -i lo -j ACCEPT
$IP6TABLES -A FORWARD -i lo -j ACCEPT

# Aceitar icmp apenas se o rate não for muito elevado
$IP6TABLES -A INPUT -p icmpv6 -m limit --limit 10/min -j ACCEPT

# Aceitar sessões já estabelecidas
$IP6TABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Permitir acesso público
$IP6TABLES -A INPUT -p tcp -m tcp -m multiport --dports $PUBLIC_PORTS -m state --state NEW -j ACCEPT
# permitir acesso administrativo
for NET in $ADMIN6_NETS; do
    $IP6TABLES -A INPUT -s $NET -p tcp -m tcp -m multiport --dports $ADMIN_PORTS -m state --state NEW -j ACCEP
T
done
```

#6 - 11/03/2011 12:32 PM - Miguel Lopes Luis

OK, obrigado pelo script, vou dar uma olhadela.

Em relação ao kernel, a minha questão é que um 'yum update' faz download do novo kernel e não conheço outra forma de o carregar a não ser por reboot, por isso estranhei quando disseste que nao pensasses que se fizessem reboots às máquinas.