Monitorización, Allot

Instalación del servidor para Allot

Requisitos mínimos

- 4 GB RAM
- 2003 Server (en inglés o si es en español cambiar la configuración regional a inglés)

Instalación

- Instalar la máquina virtual de java
- Descomprimir el ejecutable
- Ejecutar setup.exe

Conexiones

- Conectar los interfaz del appliance con el bypass


externos con externos, internos con internos

- Conectar el cable de bypass al primary


Es muy importante a la hora de crear las políticas saber que interfaz está como externa o interna

Una vez instalado el servidor para configurar el usuario por defecto es admin y contraseña:allot


Para poder enviar los informes por correo el formato tiene que ser pdf


No puede haber un servicio en dos grupos

Configuración de las políticas

Line

```
Pipe
 Virtual Channel
```

En el momento en el que dentro de un line creamos un VC (Virtual Channel) con prioridad Qos, al resto de VC de ese line también hay que darles una prioridad.



Usar los line para clasificar el tráfico, y los VC para priorizar



En el failback no se pueden aplicar políticas Qos.

Restore Policy and Catalogs

Reclasifica todas las conexiones (pero no afecta al tráfico). Este comando es útil si modificamos las clasificaciones.

Configuración del appliance

Para ver la configuración

```
go config view
```

versión del AOS

```
actype
```

Configuración de la ip

para configurar la ip nos conectamos por consola con **login=sysadmin** **pass: sysadmin ** y ejecutamos

```
go config ips -ip dirección:máscara
go config ips -g gateway
go config ips -dns servidordns
```



Después de cambiar la ip hay que reiniciar la máquina con **ac_reboot**

Monitorización de conexiones

```
acmon
```

```
acstat -ifx ->conexiones activas
```



Si una vez instalado el servidor vamos a agregar al mismo el appliance y nos da un error de que no se puede conectar a esa ip por el puerto 161 tenemos que hacer lo siguiente: Entrar por ssh al appliance, ir al directorio $SWGC, dentro de ese directorio entrar en la carpeta SNMP, borrar todo el contenido de esa carpeta, reiniciar el equipo, volver a añadir al servidor



Es muy importante que el ntp este activado y con el mismo servidor de tiempos que el servidor donde tenemos instalado el allot

Actualizar el AOS (allot operating system)

Nos conectamos por ssh al equipo

Creamos una carpeta con el nombre dela nueva versión a instalar

```
mkdir AOS12.3.21
```

si utilizamos algún proxy para conectarnos a internet definimos la variables necesarias en el equipo

```
export http_proxy=http://ip_proxy:puerto
export ftp_proxy=http://ip_proxy:puerto
```

vamos a la carpeta creada y descargamos los ficheros de la nueva versión específica para nuestro aparato



lo más comodo es usar el navegador del escritorio para encontrar el enlace y pegarlo en la consola remota

```
 wget
ftp://ftp.allot.com/DPI_device/AC-3000/Maintenance/AOS.AC3K.12.3.21_B52/ac3k
-12.3.21-52.tgz
```

```
wget
ftp://ftp.allot.com/DPI_device/AC-3000/Maintenance/AOS.AC3K.12.3.21_B52/aos-
instl.sh
```

Le damos permisos de ejecución al script de instalación

```
chmod +x aos-instl.sh
```

y lo ejecutamos

```
 ./aos-instl.sh
```

```
script called with args=[]
Please wait; This can take some time...
.
.
Launching main installer...

---------- aos_install_main.sh started. ----------
aos_install_main.sh called with args []
Upgrade install: installing AC3000
WARNING: system is active, switch to bypass and install anyway? (yes/no)
yes
You chose to switch to bypass and continue installation.
================================================================================
aos_install_main.sh: using the following params:
  Product family        : ac3k
  Engineering           : No
  Slot                  : Standalone
  Options               :
  Logs Directory        :
/opt/allot/logs/install/install_2013-08-09_10-09-57_v12.3.21-52
  Archive file          : ac3k-12.3.21-52.tgz
  Version               : -12.3.21-52
  Force install         : 0
  Dry run               : 0
  Verbosity level       : 4
================================================================================

Performing pre install adjustments for verion -12.3.21-52 .
Unpacking main archive, please wait..
Finished unpacking main archive.
Extracting [1]...
---------- aos_install_s.sh started. ----------



aos_install_s.sh called with args [-p ac3k -l
/opt/allot/logs/install/install_2013-08-09_10-09-57_v12.3.21-52/install_main
.log -v 8 -q 4 -s -1 -w /tmp/install__1331_16280 -t 7 -A 259112 -a 0]
Detected H/W name: NGC
Starting modifications...
Checking and removing duplicate pkgs...
packages-mips-instl.sh called with args [-v 8 -l
/opt/allot/logs/install/install_2013-08-09_10-09-57_v12.3.21-52]
Extracting SP software. Please wait...
Upgrading SP software. Please wait...

Upgrading system software. Please wait...

Start pkg installation...
Installing package ipmc_utils-1.1-mips-1...
PACKAGE DESCRIPTION:
```

```
Executing install script for ipmc_utils-1.1-mips-1...

Pkg installation done (installed=1, install errors=0, missing pkgs=0)
Installing software. This may take a few minutes...
.....................................................................
.....................................................................
.....................................................................
.....................................................
.............
set_type.sh called with args=[ac3040 sfp]
Setting type: product= ac3040,  sub-type: sfp
Installing Host software now. This may take a few minutes...
.....................................................................
.....................................................................
.....................................................
Data base was installed successfully
<<<<<Key validation passed successfully>>>>>
Current protocol pack version is : 26
Version AOS.AC3K.12.3.21 Build 52
Cleanup. This may take a while...
----------aos_install_s.sh completed succesfully----------
----------aos_install_main.sh completed succesfully----------
Rebooting device.
```

FAQ

Actualizar las claves al cambiar de versión

Buscar en el Know Base la palabra generate new key y nos saldrá la página donde indica el procedimiento. https://c.eu1.visual.force.com/apex/KB?sfdc.tabName=01r200000001xai



En los recuadros marcados, donde indica las versiónes actuales, es donde primero hay que pulsar para cambiar la versión antes de poder generar la nueva clave.

Actualizar APU manualmente

Desde la página de Allot entrar como usuario y descargar el fichero de actualización de protocolos (APU) Descomprimir el zip en una carpeta por ejemplo c:\temp\allot



en el fichero comprimido suele haber otros zips (no descomprimir) y un fichero xml

desde el NetXplorer → Menú Tools → Protocol Updates →From Local Package

aprecerá un cuadro de diáogo donde hay que poner la ruta del directorio donde hemos descomprimido el zip

Problemas con la base de datos

En el servidor en la carpeta allot\bin hay varios scripts para reparar la base de datos. Hay tres bases de datos:

- LTC →la Bdd de eventos de largo plazo
- STC →la BDD de eventos de corto plazo (la que normalmente se suele corromper)
- CFG → la BDD de configuración

Para reparar la BDD paramos primero el servicio NetexplorerService y después ejecutar:

```
recreate_default_db.bat <base de datos>
```

Por ejemplo:

```
recreate_default_db.bat STC
```



si recreamos la base de datos CFG borramos toda la configuración



podemos recuperar una base de datos anterior copiando la base de datos desde c:\allot\data\backup\ a c:\allot\data\db

Cambiar la ip

Si cambiamos la ip deberíamos ejecutar el siguiente script set_nx_ip4ui.bat

Una vez cambiada la ip podemos comprobar las coenxiones haciendo por ejemplo un

```
netstat -an | find "80"
```

Problemas resolución DSN

The DNS configuration is part of the quartz jobs written in the nms.ear file. If you want to modify the frequency the DNS will be queried (increase it or decrease it) you can simply edit that file and give it your value. Eventually, you can also remove the DNS part of the nms.ear file if you simply want to turn off the DNS resolution. Please note that this file is a generic configuration file : you may save it for future use.

- Stop the NetXplorer service
- Create a new folder (close to C:\Allot\netxplorer\jboss-4.0.2\server\allot\deploy it will be easier for you).We will call it NewFolder for the rest of this document.

- Copy the nms.ear file from C:\Allot\netxplorer\jboss-4.0.2\server\allot\deploy to NewFolder
- Change the copied nms.ear suffix to .zip
- Open the nmz.zip with winzip the relevant files will be displayed
- go into lib directory
- Copy the nms-common.jar to NewFolder
- Change the nms-common.jar extension to .zip
- open nms-common.zip with winzip
- The relevant files within will be displayed
- Edit the quartz_jobs.xml with WordPad
- Locate <file>

< !> < category name="common"> . . . < property name="dnsSchedularLauncherCycle" value="300000"/> < !→ . . . < /category> </file>

- Change the value="300000" Change to what ever value you like.
- Save the modification
- Delete the quartz_jobs.xml from its original location and copy the new one instead.
- Rename the nms-common.zip to nms-common.jar
- Save the nms-common.jar into the nms.zip
- Rename the nms.zip to nms.ear
- Copy the newly saved nms.ear into C:\Allot\netxplorer\jboss-4.0.2\server\allot\deploy, by doing this you erase the original one (rename it before it you want to be safe)
- Start the NetXplorer service

Referencias

- http://foro.ingecom.net/viewforum.php?f=5

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=seguridad:monitorizacion:allot

Last update: **182023/01/ 13:37**