cluster, fortigate, ha

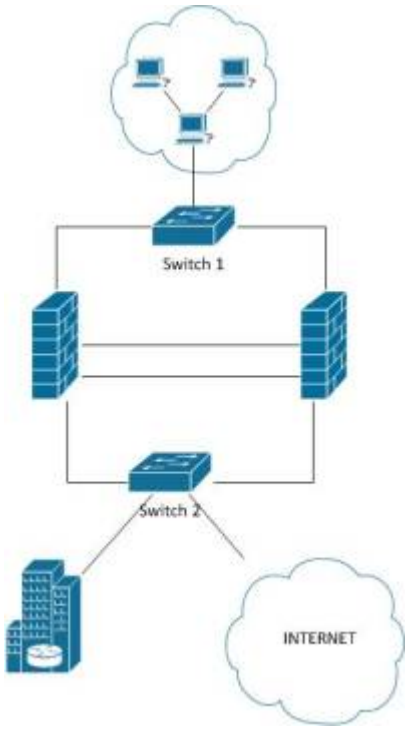
Cluster de Alta disponibilidad con Fortigate

Requisitos

- Dos equipos Fortigate iguales, mismo hardware, mismo disco, etc
- Misma versión del Firmware
- Mismo modo (NAT o transparente)
- Mismo modo VDOM

recomendaciones

- Usar diferentes nombres de host para cada nodo
- Habilitar load-balance-all
- Usar enlaces hearbeat dedicados. Si sólo son dos nodos podemos conectarlos entre si.
- Usar al menos dos interfaces para heartbeat
- No monitorizar enlaces heartbeats
- Usar Session Pickup (seguimiento de las sesiones) sólo con ciertos modelos de Fortigate y además que tengan enlaces de heartbeat dedicados.
- Si vamos a usar session pickup utilizar la opción de delay para mejorar el rendimiento.
- Usar enlaces agregados (802.3ad) para conectar los nodos a la red.



Cluster Activo - Activo

Paso para crear el cluster:

- Backup de la configuración actual.

- Habilitar el modo activo-activo
- Poner la prioridad del nodo que queramos poner como primario a 255
- Conectar el segundo nodo con el primero (interfaces hearbeat)
- Habilitar en el segundo no el modo cluster pero dejando la prioridad como está (128)

Las dos unidades del cluster tienen que tener los mismos interfaces conectados a los mismos switchs de manera que NO tengamos un punto único de fallo. La idea es tener varios puerto en trunk en cada cortafuegos conectados a distintos switchs

le ponemos un nombre distinto a cada cortafuegos

```
config system global
set hostname cortafuegos1
end
```

Para definir quien será el nodo primario hay que poner dicho nodo con mayor prioridad que el otro.

```
config system ha
set priority 200
end
```

Configuramos el grupo de alta disponibilidad

```
config system ha
set mode a-a
set group-name grupodeha
set password contraseñadelgrupo
set hbdev port15 50 port16 50
end
```



No se puede crear el cluster si uno de los interfaces está configurado para obtener la dirección ip por DHCP o PPPoE.

Si esto ocurre el equipo Fortigate vuelve al modo standalone cuando presionas ok sin dar ningún mensaje de aviso o error. Para solucionarlo basta con poner en todos los interfaces en modo manual.



De un cluster HA en modo activo-activo desapare la opción de configurar cualquier interfaz como PPPoE

Para ver la configuración del cluster

```
get system ha
```

Para conocer el estado

```
get system ha status
```

Forzar devolver el control al master

```
diag sys ha reset-uptime
```

https://kb.fortinet.com/kb/viewContent.do?externalId=FD33114

Reiniciar uno de los nodos de un cluster

Lo primero es saber el id que tiene asignado el fortigate que queremos reiniciar

```
get system ha status
```

Una vez que sabemos el id nos conectamos al equipo

```
execute ha manage id
```

y lo reiniciamos

```
execute reboot
```

- http://www.shogan.co.uk/how-tos/how-to-restart-a-slave-fortigate-firewall-in-an-ha-cluster/

Actualizar el firmware del cluster

Para actualizar el firmware de cluster tenemos que actualizar el firmware de la unidad **master** y automáticamente la unidad **slave** se actualizará.

Solucionar problemas de sincronización

https://kb.fortinet.com/kb/documentLink.do?externalID=FD36494

Referencias

- http://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-high-availability-52/HA_config

_troubleshooting.htm?Highlight=cluster%20problem

- Guía HA FortiOS 5.0 http://docs.fortinet.com/fgt/handbook/50/fortigate-ha-50.pdf
- http://docs.forticare.com/cb/fortigate-cookbook.pdf
- http://www.soportejm.com.sv/kb/index.php/article/virtual_cluster
- http://docs-legacy.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/clustering.082.34.html

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

Permanent link:
https://wiki.intrusos.info/doku.php?id=hardware:fortigate:cluster

Last update: **182023/01/ 13:36**