VIP on PINsafe Appliances

Contents

Overview

This document covers the use of the VIP (Virtual IP Address) on Swivel appliances to provide redundancy in the event of a failure of one of the Swivel servers. The VIP is usually used for providing resilience to the single channel TURing image, but may also be used for Dual Channel message requests and the Security String index.

The VIP is often used with the Mon process, so when a monitored process fails, the VIP provides resilience to that process, see

The VIP is controlled by the heartbeat process.

What is a VIP?

The VIP is a Virtual IP address that can be bound to an Ethernet interface (ETH0) as a second IP address but can MOVE from one Swivel appliance to another. Swivel appliances are usually configured with an IP address on ETH0, and another IP address is assigned as the VIP. The VIP usually resides on the primary appliance and if there is a problem it is unbound from the Primary server and started on the standby server. Control of the VIP is by the Heartbeat process, which uses the Mon process to determine if the VIP should move from one appliance to another. The VIP IP must be on the same subnet as the Primary and Standby appliances ETH0 IP.

The VIP adds resilience to the appliances, and all traffic will be directed to one server. There is no session affinity.

Heartbeat Explained

Heartbeat regularly sends a UDP datagram on port 694 to the multicast address 225.0.0.1 announcing it is up and running and owns the VIP address. If the appliance it is running on shuts down for any reason, this stream of packets from the primary master stops and after a predetermined timeout, the standby master becomes master and assumes the VIP address. Through the webmin, Heartbeat can be configured to monitor certain resources on the appliance and give up the address if some conditions are met, see also MON Service Monitor How to guide.

Heartbeat uses gratutious ARP to announce the changing of the MAC address. (Unlike VRRPd which replaces the MAC address of the active machine with a virtual one).

Prerequisites

Swivel A/A appliances, see also High Availability with PINsafe

VIP deployment considerations

- Each Swivel appliance will need to be configured both for networking and Swivel configuration options.

- The VIP must be deployed on a pair of Swivel appliances within the same subnet.

- Three IP addresses within the subnet are required for ETH 0: Primary, Standby and VIP

- The Swivel appliances must be able to ping each other and the gateway IP address to ensure that each other is available and detect network failures. If the gateway is a firewall, then a rule may need to be created to allow the ping.

- Heartbeat status requires the appliances to be able to SSH each other. Verify that each appliance can ssh to the other by using ssh admin@hostname.

- Swivel A/A appliances use the cross over cable connection on ETH 1 directly between two appliances to detect that the difference between a network failure and the failure of a Swivel appliance. the **heartbeat** process monitors the network and controls where the VIP should be. The **mon** process monitors the VIP and provides alerting. If the cross over cable is not used, then communication for multicast traffic on UDP port 694 must be permitted between the appliances.

- Where the VIP is used to obtain a graphical TURing image, the real IP address of the Swivel appliance should be used for a RADIUS request since the Swivel appliance will respond with its real IP address which may cause the access device to drop the response as it will have come from a different IP. Primary and Secondary RADIUS servers may be configured. To overcome the possibility of the single channel image coming from one server and the RADIUS request going to another server one of the following should be enabled on the Primary Master and Standby Master:

Session Sharing

RADIUS Proxy see PINsafe RADIUS Proxy

VIP Configuration

The VIP should be configured from the CMI. The networking section allows the IP address of the Primary Master, Standby Master and VIP to be entered on each appliance.

To activate the VIP the heartbeat should be configured to start on system boot on the Primary Master and Standby Master, by selecting in the CMI Advanced, then Default Running Services, select Heartbeat so that it displays ON. To manually start heartbeat, in the CMI select Heartbeat then start.

Please Note: Do NOT use the VIP address as the RADIUS server address.

VIP Alerting

The Mon process monitors the Swivel Appliance Tomcat and can allow failover but also the Swivel appliance can be configured to send an email when a fail over occurs.

Note: using Webmin on older versions of the appliance, a semi colon may be added onto the end of the configuration which renders it useless.

Make a backup of /etc/ha.d/haresources

Edit /etc/ha.d/haresources

using command line, or by editing the file using WinSCP see WinSCP How To Guide, or a recent version of the Webmin and alter the first instance of root@localhost to be the new monitoring email address.

Default Primary haresources file

```
# Swivel Appliance Build primary haresources File
#
# Use this line if you are going to use mysql replication method.
primary.swivel.local 172.16.1.98 MailTo::root@localhost::PINsafePrimary
# primary.swivel.local 172.16.1.98 drbddisk::webapps Filesystem::/dev/drbd0::/dr bd::ext3 tomcat5 MailTo::root@localhost::PINsafePrimary

################################################################################
######################
standby.swivel.local MailTo::root@localhost::PINsafeStandby
```

Default Standby haresources file

```
# Swivel Appliance Build standby haresources File
#
# Use this line if you are going to use mysql replication method.
primary.swivel.local 172.16.1.98 MailTo::root@localhost::PINsafePrimary
# primary.swivel.local 172.16.1.98 drbddisk::webapps Filesystem::/dev/drbd0::/drbd::ext3 tomcat5 MailTo::root@localhost::PINsafePrimary

######################################################################################################
standby.swivel.local MailTo::root@localhost::PINsafeStandby
```

To see email alerts sent see, /var/log/maillog

cat /var/log/maillog

VIP Alerting destination email address

The VIP alerting is sent by the appliance email system. To specify a different email server edit the file /etc/mail/sendmail.cf and look for the line

```
"smart" relay host
DS
```

Edit this to add the email server, for example

```
"smart" relay host
DSmail.swivelsecure.net
```

Restart Sendmail from the CMI or from the command line *service sendmail restart*

Also consider the use of MON for monitoring Tomcat see MON Service Monitor How to guide

VIP Status

To verify the VIP status on a Swivel appliance see VIP Status

Testing

Known Issues

The VIP should primarily be used for the TURing image single channel authentication. RADIUS requests should be directed against the real IP address of the appliance rather than the VIP. Requests to the VIP will be returned by the appliance on the real IP address and the access device may reject the RADIUS response as the source and destination IP addresses do not match.

Troubleshooting

Heartbeat will not start, see Heartbeat issues