How To Easily Convert a Large Scale VRRP Cluster to an IP Cluster

11 April 2012
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=15442

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/11/2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Easily Convert a Large Scale VRRP Cluster to an IP Cluster).
How To Easily Convert Large Scale VRRP Cluster to an IP Cluster

Objective

This document provides a script and explains the steps to convert a large scale legacy or simplified VRRP cluster into an IP Cluster. The procedure is most suited for VRRP migrations where many VRRP virtual addresses are configured and the task to migrate them to an IP cluster virtual addresses takes a long time.

Supported Versions

NGX R65 and later

Supported OS

IPSO 6.2 and later

Supported Appliances

Any IP Appliance

Before You Start

Assumed Knowledge

VRRP and IPSO clustering as well as Check Point Firewall administration.

Related Documentation


Impact on the Environment and Warnings

- This procedure disrupts the passage of traffic through the cluster. Perform it during a maintenance break.
- Migration of configurations where VRRP is configured on multi-homed addresses is not supported.
- The conversion script does not work on IPSO versions prior to IPSO 6.2. On non-legacy IP appliances, upgrade to IPSO 6.2 before you convert the VRRP configuration to IP Clustering.

Converting Large Scale VRRP
Clusters to an IP Cluster

To Copy the Configuration File:
1. Fail-over the VRRP Master so that the normal VRRP Backup Firewall assumes the Master role.
2. Log into the command line on the previously Master appliance (now in Backup role).
   Make a copy of the active initial file on the system. To identify the correct file, examine the symbolic link in the /config directory with: cd /config and ls -l. Check which file is linked to Active with:
   active
   For example: active -> /config/db/initial_6.2v6
3. Copy the file in the symbolic link to a sub-directory in the home directory and rename it to raw_initial.
   For example: cp /config/db/initial_6.2v6 /var/emhome/admin/script/raw_initial

To Upload the Cluster Migration Script to the Security Gateway Computer:
1. Copy the script below to a plain text editor, and save it as a Unix Script file named: cluster_migrate.sh.
2. Copy the script file with FTP or WinSCP in binary mode to the directory that contains the raw_initial file.

```bash
#!/bin/bash
echo "Enter the number to be used for the Cluster ID and then press ENTER: "
read id
#Global count variable for counting lines output.
active_file="raw_initial"
clish_script="clish_cluster.txt"

if [ ! -f "$active_file" ];
  then
    echo "Sorry, active file does not exist. Please make sure the name is correct."
    exit 1
fi

grep vrrp:interface $active_file > vrrp-filtered.txt
if [ ! -f "vrrp-filtered.txt" ];
  then
    echo "Sorry, vrrp-filtered.txt does not exist. Please make sure the name is correct."
    exit 1
fi

grep address vrrp-filtered.txt > vrrp-address.txt
input_file="vrrp-address.txt"
while read inputline;
do
  ipsrd=`echo $inputline | cut -d':' -f1`
  instance=`echo $inputline | cut -d':' -f2`
  default=`echo $inputline | cut -d':' -f3`
  vrrp=`echo $inputline | cut -d':' -f4`
  interface=`echo $inputline | cut -d':' -f5`
  logical_interface=`echo $inputline | cut -d':' -f6`
  virtrouter=`echo $inputline | cut -d':' -f7`
  # vrid=`echo $inputline | cut -d':' -f8`
  address=`echo $inputline | cut -d':' -f9`
  addr=`echo $inputline | cut -d':' -f10`
  vip=`echo $inputline | cut -d':' -f11`
  vip_ip=`echo $vip | { read first rest ; echo "$first"; }`
  # create clish cluster script
```
To Run the cluster_migration.sh Script:
The script does not change the current configuration.

1. Run the cluster_migration.sh script.
2. When prompted, enter a Cluster ID number. You need to enter the same ID number when you setup the basic IP Cluster configuration.
3. To grant rights to the script file, run: chmod +x cluster_migration.sh
4. To run the script, run: ./cluster_migration.sh
5. The script produces several text files. The useful output is in the clish_cluster.txt file. This file contains a set of clish commands that are used to configure the cluster virtual IP addresses. Make sure that the clish_cluster.txt file is produced and contains a list of clish commands similar to: add cluster id 100 interface eth1c0 cluster address 10.1.1.65

To Delete the VRRP Configuration:
1. In the Voyager tree view, select Configuration > System configuration > VRRP.
2. Below Simplified VRRP or Legacy VRRP (the one configured), select the delete box for the defined VRID(s) and then click Save. The VRRP configuration is deleted.

To Setup the Basic IP Cluster Configuration:
1. In the Voyager tree view, select Configuration > System Configuration > Clustering > Cluster Configuration.
2. Specify the cluster ID to be used to form the IP cluster with the same ID entered for the migration script.
3. Select the Cluster Topology type you want.
4. Enter a cadmin password of your choice in the cadmin password fields.
5. Click Save.

To Migrate the Virtual IP Addresses:
1. To get the configuration lock to be able to configure the cluster virtual IP addresses in Clish, log out of Voyager.
2. On the command line, go to the directory that contains the clish_cluster.txt file created by the script, and run: clish -f clish_cluster.txt
3. Log back into Voyager, and finalize the cluster configuration.

To Finalize the IP Cluster Configuration:
1. In the Voyager tree view, select Configuration > System Configuration > Clustering > Cluster Configuration. Click Manually Configure IPSO Cluster, and select the Primary and Secondary cluster networks.
2. Set the cluster state to UP.
3. In Cluster Mode, select the mode you want.
4. In Work Assignment, select the one you want, Static or Dynamic.
5. To allow the cluster to form without dependency on the monitored firewall-1 processes, make sure the Enable VPN-1/Firewall-1 Monitoring check box is clear.
6. Click Save. The Appliance comes up as the cluster Master (if the clustered interfaces are Up).

To Configure the IP Cluster Partner Appliance:
1. To create a backup of the initial file, repeat To Copy the Configuration File procedure (the first one in this process). Do not copy the script file over to the second box.
Completing the Procedure

2. In the Voyager tree view, select **Configuration > System configuration > VRRP**. Select the **Delete** box for the defined VRID, and click **Save**. The VRRP configuration is deleted. To verify, check the **VRRP Monitor**.

3. Add the partner appliance to the first box:
   a) In the Voyager tree view, select **Configuration > System Configuration > Clustering > Simplified Clustering Configuration**.
   b) Enter the Cluster ID used to configure the first appliance.
   c) Enter the password used on the first appliance.
   d) In **Specify cluster member address to obtain the rest of the configuration**, enter the Primary IP cluster address used on the first appliance.

4. Click **Save**.

5. To verify, select **Monitoring > Clustering Monitor**.

   ![Note] - If all the clustered interfaces are up, the cluster comes up. The first box has the Master role, and the other box becomes the Member when it joins the cluster. If the performance rating is adjusted on an appliance so it is higher than the other box, it takes over the Master state and becomes the active appliance even if it is the last box to boot.

To Edit the Cluster Object:

1. In **Third Party Configuration**, make sure that **Load Sharing** and the 3rd party solution **Nokia IP clustering** are selected. Make sure that the other options below are also selected.
2. Push the policy to the cluster and check that the cluster is still up and operational.
3. To verify the cluster functions properly, perform several pushes.

Completing the Procedure

To Enable Firewall Monitoring and Fail-over Testing:

1. Log into the cluster virtual IP address with the user **cadmin** and the cluster password.
2. In the Voyager tree view, select **Monitor > Cluster Monitor**, and check the state of the cluster. If all the clustered interfaces are Up, the cluster should be formed with 2 members (one Master and the other Member).
3. In the Voyager tree view, select **Configuration > VRRP > Clustering > Simple Cluster Configuration**, Set **Firewall Monitoring** to **ON**, and click **Apply > Save**.
4. To make sure that the cluster is still Up, in the Voyager tree view, select **Monitor > Cluster Monitor**.

Verifying the Procedure

To test cluster integrity, unplug one of the clustered links so it removes the affected firewall from the cluster. When the test is complete, leave **Firewall Monitoring** ON, and make sure **Save** is performed in Voyager.