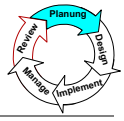
CUSTOMER
LOGO

Screenplay Upgrade R80.20
Perimeter Cluster

IT Operations & Engineering

Version V1.0

Document Name: Screenplay_Upgrade_R80-20



Document Control

Version	Date	Änderungsnotiz	Affected pages	Status	Author
V1.0	24.07.2019	Initial Version		Valid	Peter Schumacher

Distribution List

Name	Organization	Function
		Security Engineer
Carlos Smith	Customer	Head of Networking & Voice

Conventions

In configuration examples, the system output is always shown in

Courier new 7 pt schwarz fett.

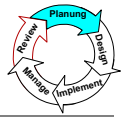
User input is represented in

Courier new 7 pt blue bold with yellow background

Title rows in tables for internal actions are blue, for external activities are red

Table of Contents

Table directory



1. Introduction

Version R77.30 of the Check Point software reaches the end of the supportcycle in September 2019. Therefore, all components of the check point infrastructure must be raised to the actual level R80.20.

1.1. Starting point

The SmartCenter my-smartcenter has already migrated to the release R80.20.

1.2. Untersuchungsbereich

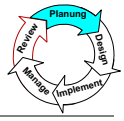
The scope of the migration to R80.20 includes the following elements:

- Perimeter cluster with the two machines
  - cl-member-1
  - cl-member-2

1.3. Objective

The objectives for the use of the script are:

- List all migration steps in full
- Perform all migration steps in the correct order



2. Concept

The perimeter firewall cluster is migrated for both members (the backup member cl-member-2 first) using the new flashing mechanism and includes the following steps:

- Get the configuration file of the gateway
- Create a snapshot for rollback
- Exporting the snapshot
- Transferring and unpacking the blink images
- Preparing the necessary control file cl-memberxxx_answers.xml
- Stop der Check Point Software
- Unpacking the Blink Archive and Starting the Reinstallation
- Setting the bash shell for the admin user
- Transfer and loading of the configuration file
- Customizing the object version R80.20 for the firewall GW
- SIC reset with the SmartCenter
- Check Gateway Definitions on the SmartCenter
- Installing the Security Policy (twice)
- Loading the gateway data and checking the GW status
- Installing the latest HFA
- Basic tests
- Switching the Backup Member with Tests
- Testing connections
- Setting up the backup mechanism

The steps marked in blue may be performed before the, the steps marked in red only in the maintenance window.

The migration starts on the backup system. After successful migration and complete synchronization with the active system (which is still running on R77.30), we increase the VRRP priority to backup system so that this master becomes. If the tests show that this system is running successfully and correctly, then we will start the upgrade process on the second cluster member.

2.1. Backing up the configuration file

The current GAIA configuration is backed up as a file. This file will be read back later. Copy the backed-up filer via WinSCP to a network storage

N	What	Where	Who	Status

1.	Create configurationfile:
	
	`[Expert@cl-member-2:0]# clish`
	`cl-member-2> save configuration cl-member-2.conf`
	`cl-member-2> exit`
	`[Expert@cl-member-2:0]#`
	
	`[Expert@cl-member-1:0]# clish`
	`cl-member-2> save configuration cl-member-1.conf`
	`cl-member-2> exit`
	`[Expert@cl-member-1:0]#`
		cl-member-2
		
		cl-member-1
				OK
				
				OK

2.	Copy files cl-member-2.conf and cl-member-1.conf via WinSCP to network storage	Laptop		.

Table 1 Backing up the configuration

2.2. Creating a snapshot

In case of rollback, we create a snapshot of the current configuration:

N	What	Where	Who	Status

3.	Create a snapshot
	`cl-member-2> add snapshot cl-member-2 desc "Rollback Point Pre R80-20 Upgrade using Blink"`
	`Taking snapshot. You can continue working normally.`
	`You can use the command 'show snapshots' to monitor creation progress.`
	`cl-member-2>`
	
	`cl-member-1> add snapshot cl-member-1 desc "Rollback Point Pre R80-20 Upgrade using Blink"`
	`Taking snapshot. You can continue working normally.`
	`You can use the command 'show snapshots' to monitor creation progress.`
	`cl-member-1>`
		cl-member-2
		
		cl-member-1
				OK
				
				OK

Table 2 Create Snapshot

2.3. Exporting the snapshot

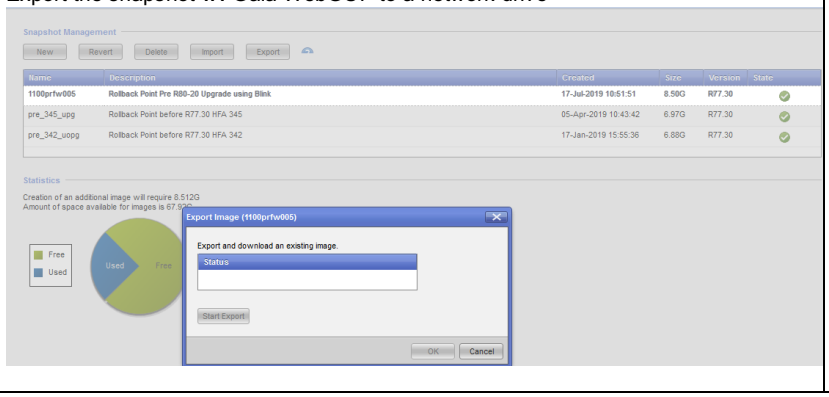
N	What	Where	Who	Status
1.	Export the snapshot in Gaia WebGUI to a network drive 	cl-member-2 cl-member-1		OK OK

Table 3 Exporting the Snapshot

2.4. Transferring and unpacking the blink images

The blinking mechanism (see Check Point sk120193) works with 2 software components:

1. Blink Utility and
2. Blink Image. (different versions, depending on appliance)

The Blink Image for R80.20 contains the Linux kernel, the Check Point software and the current hotfix Accumulator (HFA 302). The two images are as follows:

- blink_12072019_R80.20.tar (with MD5 Checksum: 50972aa74812fd75a920a20994b228c6)
- blink_image_1.1_Check_Point_R80.20_Gateway.tgz (with md5 Checksum 74a9250beec6ff958663a394df7deba6)

The image "blink_12072019_R80.20.tgz" must be unpacked in a first step on Windows to “blink_12072019_R80.20.tar” before it can be transferred to the Gaia machine.

N	What	Where	Who	Status
1.	The blink images "blink_12072019_R80.20.tar" and "blink_image_1.1_Check_Point_R80.20_Gateway.tgz » transfer to the directory /var/log/blink	cl-member-2 cl-member-1		OK
2.	Compare the md5 checksum: [Expert@cl-member-2:0]# cd /var/log/blink [Expert@cl-member-2:0]# md5sum blink_12072019_R80.20.tar 50972aa74812fd75a920a20994b228c6 blink_12072019_R80.20.tar [Expert@cl-member-2:0]#md5sum blink_image_1.1_Check_Point_R80.20_Gateway.tgz 74a9250beec6ff958663a394df7deba6 blink_image_1.1_Check_Point_R80.20_Gateway.tgz [Expert@cl-member-2:0]# #	cl-member-2 cl-member-1		OK OK
3.	Unpack the Blink Utility [Expert@cl-member-2:0]# tar -xvf blink_12072019_R80.20.tar blink [Expert@cl-member-2:0]#	cl-member-2 cl-member-1		OK OK

Table 4 Transfer and Unpack blink utility

2.5. Preparing the necessary .xml file

In the blinking mechanism, the step of the "first-time wizard" for the initial configuration of the gateway is done automatically, provided that the blinking utility is given the control file"cl-member-2_answers.xml".

It has the following content for cl-member-2 (analogous for cl-member-1):

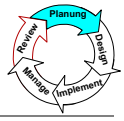
```
<properties xmlVersion="1.1">
                <installation>
                        <reboot_delay>10</reboot_delay>
                </installation>
                <machine_configuration>
                        <perform>true</perform>
                        <hostname>cl-member-2</hostname>
                        <password_hash>$1$Zms7a5dm$eGHbcvu9Ym3ss3HoOwJ.K1</password_hash>
                        <network>
                                <ipv4addr>172.16.9.79</ipv4addr>
                                <masklength>22</masklength>
                                <interface>eth3-01</interface>
                                <default_gw>172.16.8.1</default_gw>
                        </network>
                        <role_configuration>
                                <gateway>
                                        <!--  activation_key must be in base64 encoding -->
                                        <activation_key>Z2FpYTEyMw==</activation_key>
                                        <cluster>true</cluster>
                                </gateway>
                                <management>
                                        <credentials>
                                                <use_gaia_admin>true</use_gaia_admin>
                                                <!--  Relevant only if use_gaia_admin is false -->
                                                <admin_name>MGMT_ADMIN_FIELD</admin_name>
                                                <!--  admin_password must be in base64 encoding -->
                                                <admin_password>Z2FpYTEyMw==</admin_password>
                                        </credentials>
                                </management>
                        </role_configuration>
                        <send_data_to_usercenter>false</send_data_to_usercenter>
                        <enable_download_from_checkpoint>true</enable_download_from_checkpoint>
                </machine_configuration>
                <user_updates>
                        <entry_point>install_content.sh</entry_point>
                </user_updates>

                <!--
                logging - Used in order to filter the logs saved to files, displayed on the screen or sent
to the syslog.
                Supported logging levels: DEBUG, NORMAL, ERROR, ALWAYS, NEVER
                Colors - Should be set to true for displaying log messages in color on the screen.
                -->
                <logging>
                        <file_level>DEBUG</file_level>
                        <screen_level>NORMAL</screen_level>
                        <sys_log_level>NORMAL</sys_log_level>
                        <colors>true</colors>
                </logging>
        </properties>
```

N	What	Where	Who	Status

1.	Transfer the answers.xml control file from the workstation PC via WINSCP to /var/log/blink and convert it to Unix format.
	
	`[Expert@cl-member-2:0]# dos2unix cl-member-2_answers.xml`
	`dos2unix: converting file cl-member-2_answers.xml to UNIX format ...`
	`[Expert@cl-member-2:0]#`
		cl-member-2
		cl-member-1
				OK
				OK

Table 5 Transfer and Convert the .xml File

Attention:
The next steps2.6 to 2.18 may only be completed in the maintenance window!
They apply to both cluster members, but not at the same time!



2.6. Stop the Check Point Software

After that we stop the Check Point SoftwareSuite

N	What	Where	Who	Status
1.	Check point Software stop im CLI `[Expert@cl-member-2:0]# cpstop`	cl-member-2 cl-member-1		

Table 6 Stop Check Point Software

2.7. Unpacking the Blink Archive and Starting the Installation

In the next step, we unpack the Blink archive with the Blink utility and start the installation. The flash command shown in Table 7 starts the installation with the following properties (see also CP sk120193):

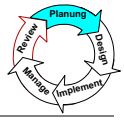
- The blink image is extracted in the output directory /var/log/blink
- The installation starts automatically
- The First Time Wizard runs automatically andconfats based on the information in the /var/log/blink/answers.xml file
- Validation for an already configured machine is skipped (--reimage)
- No snapshot of the existing installation is created (since -delete-old-partition is already done).

N	What	Where	Who	Status

1.	Unpacking the Blink Archive with
	
	`[Expert@cl-member-2:0]# cd /var/log/blink`
	`[Expert@cl-member-2:0]# ./blink -a /var/log/blink/cl-member-2_answers.xml --reimage --delete-old-partition`
		cl-member-2
		cl-member-1		

Table 7 Unpack Blink Archive and Start Installation

```
Thu Sep  5 20:03:50 2019 *A* [Main]: Blink image execution started
Thu Sep  5 20:03:50 2019 *A* [Main]: Blink Utility version: 1.1
Thu Sep  5 20:03:50 2019 *N* [Main]: Extracting image content to: /var/log/blink/launcher/files/
Thu Sep  5 20:04:12 2019 *N* [Main]: Verifying main engine integrity
Thu Sep  5 20:04:12 2019 *A* [Main]: Verified OK
Thu Sep  5 20:04:12 2019 *N* [Main]: Loading engine configurations
Thu Sep  5 20:04:15 2019 *A* [Main]: Image Version: R80.20
Thu Sep  5 20:04:15 2019 *A* [Main]: Blink Engine Version: 1.1
Thu Sep  5 20:04:15 2019 *N* [Main]: Image Used: blink_image_1.1_Check_Point_R80.20_Gateway.tgz
Thu Sep  5 20:04:15 2019 *N* [Main]: Answer File Used: /var/log/blink/cl-member-2_answers.xml
Thu Sep  5 20:04:15 2019 *N* [Main]: Executing the main engine
Thu Sep  5 20:04:15 2019 *A* [Main]: Starting Blink engine process
Thu Sep  5 20:04:15 2019 *N* [Main]: Preparing required installation files
Thu Sep  5 20:04:15 2019 *N* [Main]: Verifying the integrity of the image files
Thu Sep  5 20:04:27 2019 *A* [Main]: Verification succeeded
Thu Sep  5 20:04:27 2019 *A* [Main]: Starting installation of 'Security Gateway' image
Thu Sep  5 20:04:27 2019 *N* [Main]: Executing stage - Create Partition
Thu Sep  5 20:04:36 2019 *N* [Main]: Executing stage - Extract Image
Thu Sep  5 20:05:24 2019 *N* [Main]: Executing stage - Merge /var/log files
Thu Sep  5 20:05:25 2019 *N* [Main]: Executing stage - Create Snapshot
Thu Sep  5 20:05:29 2019 *N* [Main]: Executing stage - Machine Configuration
Thu Sep  5 20:05:33 2019 *N* [Main]: Executing stage - Gateway Configuration
Thu Sep  5 20:05:33 2019 *N* [Main]: Executing stage - Blink Wizard Configurations
Thu Sep  5 20:05:33 2019 *N* [Main]: Executing stage - Blink Updates Configurations
Thu Sep  5 20:05:33 2019 *N* [Main]: Skipping 'Blink Updates Configurations' stage.
Thu Sep  5 20:05:33 2019 *N* [Main]: Executing stage - User Updates Configurations
Thu Sep  5 20:05:33 2019 *N* [Main]: Skipping 'User Updates Configurations' stage.
Thu Sep  5 20:05:33 2019 *N* [Main]: Executing stage - Post Installation Actions
Thu Sep  5 20:05:51 2019 *N* [Main]: Executing stage - Finalize Installation
Thu Sep  5 20:05:51 2019 *N* [Main]: Total time for gateway 'Security Gateway': 0 hours 1 minutes 24
seconds
Thu Sep  5 20:05:51 2019 *A* [Main]: Security Gateway execution finished
Thu Sep  5 20:05:51 2019 *N* [Main]: Total Blink engine execution time: 0 hours 1 minutes 36 seconds
Thu Sep  5 20:05:51 2019 *N* [Main]: The machine will go to reboot in 10 seconds!
Thu Sep  5 20:05:51 2019 *A* [Main]: The installation has finished successfully and is pending reboot!
[Expert@cl-member-2:0]#
Broadcast message from admin (Thu Sep  5 20:06:02 2019):

The system is going down for reboot NOW!
```



2.8. Setting the bash shell for the admin user

N	What	Where	Who	Status
1.	Admin shell on bash set in clish: [Expert@cl-member-2:0]# clish cl-member-2> set user admin shell /bin/bash cl-member-2> save config	cl-member-2 cl-member-1		

2.9. Transfer and loading of the configuration file

The configuration file extracted in section 0 serves as the basis for restoring the original configuration.
Before transferring the file to the gateway, the following modifications must be made (depending on your situation):

In the radiusand tacacs-server definitions replace the stars after "secret" with the real radius passwords.

```
set aaa tacacs-servers state off
add aaa radius-servers priority 0 host 172.16.201.202 port 1812 secret ***** timeout 3
add aaa radius-servers priority 1 host 172.16.201.203 port 1812 secret ***** timeout 3
```

Delete the line for backup cron job:

```
add cron job Weekly_fw_backup command "/home/admin/scripts/config_export.sh >> /var/log/config_export.log
2>&1" recurrence weekly days 6 time 22:30
```

Delete the line for the Expert Password hash:

```
set expert-password-hash $1$BB[BBBcW$16jXi4g2rL2OnpqBozZk2.
```

Delete the line for the User admin password hash:

```
set user admin password-hash $1$6hJuzN8f$/dgzLGFbx1j0H6GElOqQ50
```

Delete the line for the user monitor password hash:

```
set user monitor password-hash *
```

Delete the 3 lines for the user's definition "cfgrdr"

```
add user cfgrdr uid 0 homedir /home/cfgrdr
set user cfgrdr gid 80 shell /bin/bash
set user cfgrdr password-hash *
```

If present, delete the bash shell definition for all users:

```
set user  gid 0 shell /bin/bash
```

Delete the following add rba role statements:

```
add rba role TACP-15
add rba role radius-group-monitor
add rba role radius-group-supporter
```

Delete the entry for 32 (or 64) bit version:

```
set edition 32-bit
```

N	What	Where	Who	Status
1.	Transfer of the modified configuration file via WinSCP from the PC to the gateway	Laptop cl-member-2 cl-member-1		

2.	Convert transferred config file to UNIX format.
	
	`[Expert@cl-member-2:0]# dos2unix cl-member-2.conf`
	`dos2unix: converting file cl-member-2.conf to UNIX format ...`
	`[Expert@cl-member-2:0]#`
		cl-member-2
		cl-member-1		

3.	Loading the configuration file in clish
	`cl-member-2> load configuration cl-member-2.conf`
	`In order to complete the configuration, you also need to save configuration and reboot.`
	`SNMP mode is already "default"`
	`Command (tecli) already exist in the database.`
	`Check for updates period set to 3 hours`
	`WARNING Must set password and a role before user can login.`
	`- Use 'set user USER password' to set password.`
	`- Use 'add rba user USER roles ROLE' to set a role.`
	
	`Warning: Auto negotiation is on, therefore new link-speed will only be updated but not applied.`
	`WARNING this may take a while; please be patient`
	`WARNING this may take a while; please be patient`
	`WARNING this may take a while; please be patient`
	`WARNING this may take a while; please be patient`
	`Done.`
	`cl-member-2>`
		cl-member-2
		cl-member-1		

4.	Delete Default Route from blink installation
	`1100prfw005> set static-route default nexthop gateway address 172.16.8.1 off`
	`1100prfw005> save config`
	`1100prfw005>`
		cl-member-2
		cl-member-1		

5.	Reboot of the gateway `cl-member-2> reboot`	cl-member-2 cl-member-1		

Table 8 Transfer and load of the configuration file

2.10. Customize Object Version

In the Object Database of the SmartCenter, the version of the firewall object is still defined to R77.30. The version is now set to R80.20. And for the perimeter firewall also the hardware type has to be adapted.

N	What	Where	Who	Status
2.	Hardware type and software Version for cluster object set to R80.20 .	Cluster Object		

Table 9 Customize Version of firewall object

2.11. SIC reset with the SmartCenter

After the first time wizard step, the gateway is ready to be integrated into the SmartCenter. To do this, we need to reset the SIC (Secure internal Communication) on the SmartCenter.

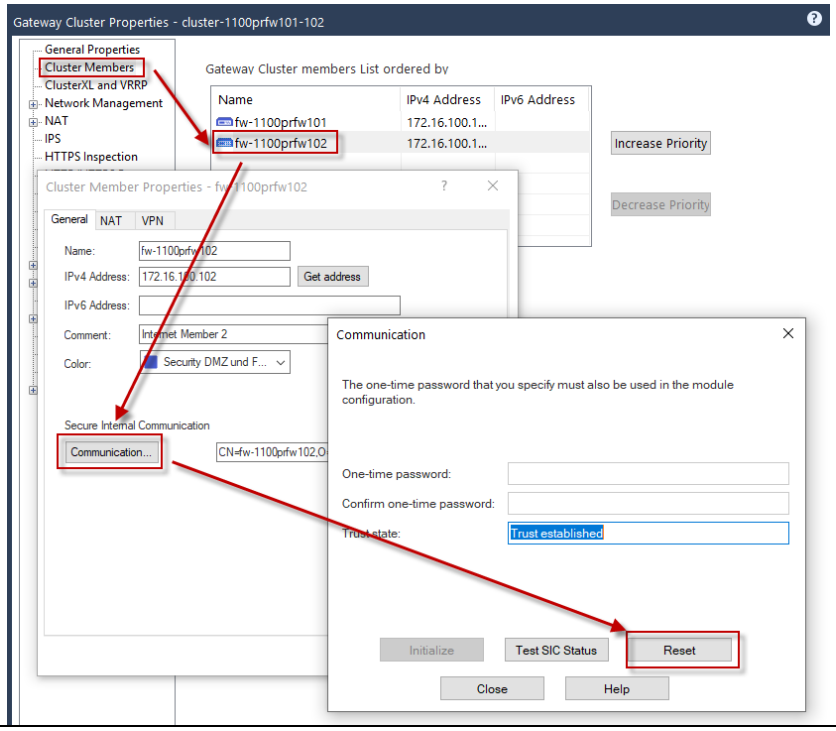
N	What	Where	Who	Status
1.	SIC reset with: Double-click cluster → Cluster Members fw-→cl-member-2→ Communication Reset→ 	SmartDashboard GUI for cl-member-2 for cl-member-1		

Table 10 SIC Reset

With SIC reset, the SmartCenter picks up the network topology from the network and redefines the antispoofing settings and zone definitions.

2.12. Check Gateway Definitions on the SmartCenter

Here, the following parameters of the gateway must check whether the settings are still correct:

- Licenses
- Contract Infos
- Security Zones
- Antispoofing Definitions

2.13. Installing the Security Policy

The Cluster Member is now ready to install the Security Policy.
The installation is done in 2 steps, first loading only the security policy and then the threat prevention policy.

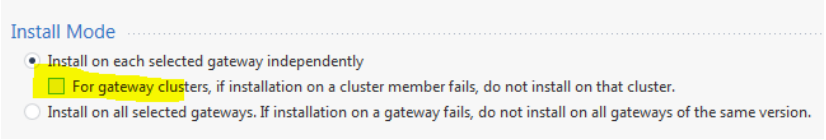
N	What	Where	Who	Status
1.	Install Security Policy on the clustercl-member-1_102. Eliminate the condition that the Force Policy must be installed on both members. 	SmartDashboard GUI		

Table 11 Policy Installation

2.14. Installing the latest HFA

Before we install the HFA, we make a backup copy via snapshot, analogous to chapter 2.2.
After that we install the latest HFA for R80.20 via WebGUI

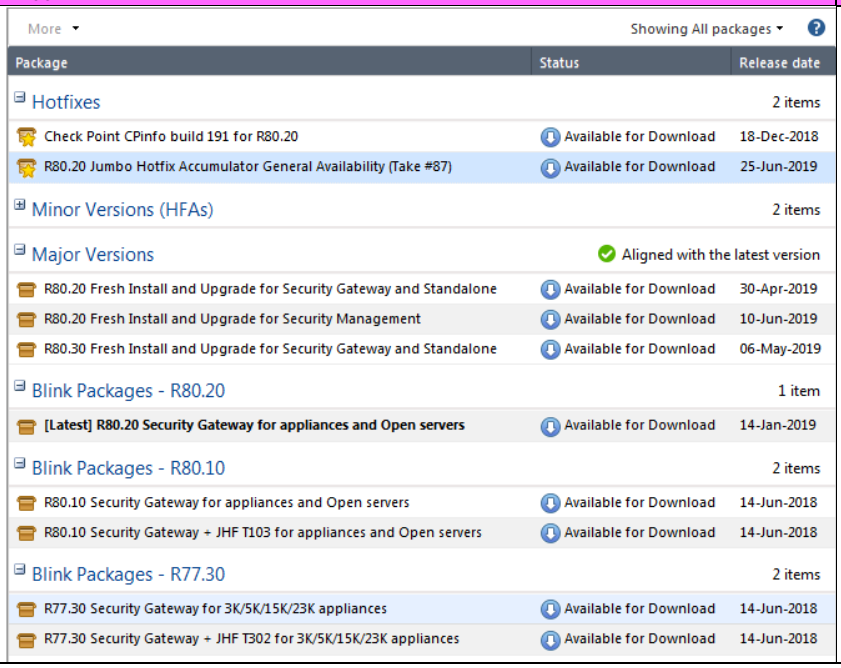
N	What	Where	Who	Status
1.		SmartDashboard GUI		

Table 12 Installation HFA

2.15. Basic Tests

Simple basic tests are designed to ensure that the migrated cluster members work correctly.

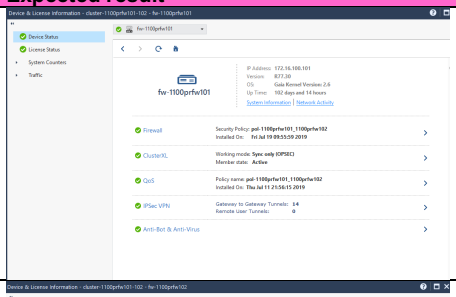
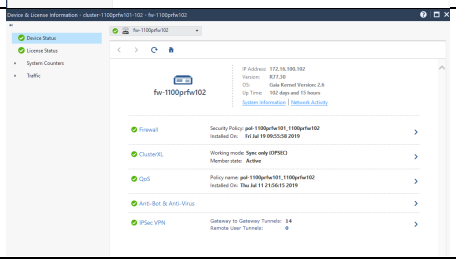
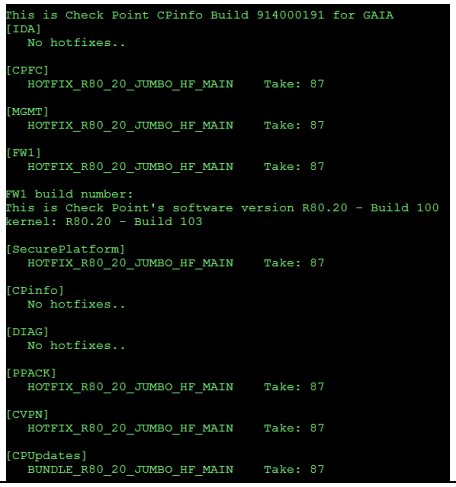
N	Test / Designation	Expected result	Where	Who	Status
1.	Firewall Blades Check Condition in SmartCenter Monitor for cl-member-1		SmartCenter		
2.	Firewall Blades Check Condition in SmartCenter Monitor for cl-member-2		SmartCenter		
3.	Check correct OS version **cpinfo -y all**		cl-member-2 cl-member-1		
4.	Check Custer Status VRRP (in clish) to cl-member-2 **show vrrp summary**		cl-member-2		
5.	Check Custer Status VRRP (in clish) to cl-member-1 **show vrrp summary**		cl-member-1		
6.	Check firewall logs. Logs from the perimeter cluster must be visible in the logwiever		SmartCenter		

Table 13 Basic Tests

2.16. Switching the Backup Member with Tests

1.	Failover to the Backup Member
	`clish`
	`set mcvr vrid 250 priority 254`
	
	`clish`
	`set mcvr vrid 250 priority 245` (to switch back after upgrade of Cluster Member 1)
		cl-member-2
		
		cl-member-2		

Table 14 Switching to Backup Member

2.17. Testing connections

Using the migrated perimeter cluster, we test selected applications::

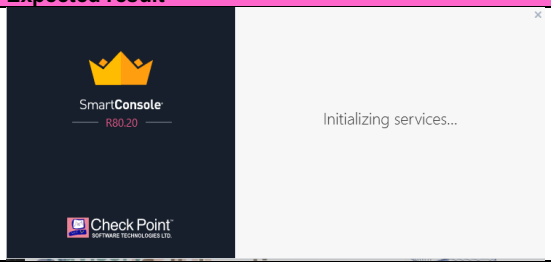
N	Test / Designation	Expected result	Where	Who	Status
1.	Access to Check Point Mgmt Server via SmartConsole R80.20		Internal Client		
2.					
3.					
4.	Internet access via browser `https://www.verrucktigschicht.ch/`		Internal Client		

Table 15 Connection Tests

2.18. Setting up the backup mechanism

To set up the backup process, refer to the appropriate documentation