How to upgrade Check Point Multi-Domain management from R71.20 to R75.30

Vložil/a cm3l1k1 [1], 17 Květen, 2012 - 10:10

- Check Point [2]
- Networks & Protocols [3]

The main reason for writing this post is due to the fact that there is absolutely no information regarding this topic. I had to reinstall whole LAB environment five times before I found a breakthrough. Check Point Multi-Domain management (Provider-1) is a centralized solution for firewall management used in big environments. You can assign global policies, IPS settings, separate countries/regions into CMAs and share objects between them. You also have the ability for primary-slave CMAs and CLMs (centralized logging server) so in case a datacenter goes down, you can manage firewalls via slave MDS. In R75.30 you can also export/import objects between CMAs but let's talk about it later.

In this post I will describe the upgrade process on real data, real management which maintains around 25-30 firewall clusters and something about 100.000 objects. It's not similar to available "HowTo Guide" where you only have some patching etc. on Any/Any firewall.

As usual it hasn't been painless, but I will describe what issues can happen and how to fix them.

More information:
Multi-Domain Management / Provider-1 - https://supportcenter.checkpoint.com [4]

// Preparation

There are two possible upgrade paths:
a] **R71.20 -> R75 -> R75.20 -> R75.30**
b] **R71.20 -> R71.30 -> R75.20 -> R75.30**

Preferable though is option A because R75 has the ability to upgrade from R71.20 from its beginning and it seems to be tested closely and deeper than option B.

You have to download these files:

```
MD5                                 Filename
0849c4b9e33acaa79b4fb0fcd2dcf028  Check_Point_R75.20_MD.Splat.iso
bba969430026f70e2c79735ce1db87f9  Check_Point_R75.30_Upgrade.Splat.tgz
7cb63392cb267c6e696a7528fc028437  Check_Point_R75_MD.Splat.iso
```

Simply search for the filename on Check Point support website and ensure to check the md5sum of each file to be sure that you download it correctly. Store the files on some linux box because, from my past experience, SCP is best file transfer option.

Our environment (MDS/MLM) is running on OpenServers so re-select packages accordingly to your situation.

Please note the whole upgrade process occurs in CLI (bash - expert mode). I would not recommend using WebUI. I already experienced that the upgrade process "finished without problems" but box itself has been unstable and a lot of essential applications for management have had to be deleted (mdsstat, mdsstart, cpconfig, ...). Regarding logs I did find that at the end of upgrade process, the installer deletes those scripts, then it wants to check for licenses and after that wants to install new

version of them. But script for checking licenses fails and new versions is never installed... so, be careful and follow me on CLI.

In my case I did the upgrade in three steps:

1] Upgrade of primary MDS
2] Upgrade of standby MDS and primary MLM
3] Upgrade of standby MLM

During upgrade process nobody should change anything on MDS environment.

LAB in VirtualBox (optional)

I was able to make whole upgrade in VirtualBox [5] environment as well. Just ensure that your LAB can't reach firewalls which can possibly affect them. For this is best option Host-Only network [6] where your testing server can reach only host running VirtualBox.

// Update MDS licenses

You are unable to update your actual licenses in Check Point support section to R75, YOU MUST contact account services to do that (believe me).
This part is essential and can't be skipped. If you don't update licenses your upgrade will fail and you have to recover it from backup. Again, this is not a joke. I had to recover MDS twice because of this.

Print your actual licenses by command:
`cplic print`

Send output to Account Services if they can update your actual licenses or if provided one are already prepared for R75.

Here you have example of output:

```
Host              Expiration  Features
192.168.11.10      never       CPSB-BASE CPSB-NPM CPSB-EPM CPSB-LOGS CK-736456283846
192.168.11.10      never       CPSB-BASE CK-736456283846
192.168.11.10      never       CPPR-MDS-MC10-NGX CK-878789789795

Contract Coverage:

 #   ID          Expiration   SKU
===+===========+============+====================
1  | 1ASDF234   | 30Jun2012  | CPCES-CO-PREMIUM
   +-----------+------------+--------------------
   |Covers:     CPPR-MDS-MC10-NGX CK-878789789795
   |            CPSB-BASE CK-736456283846
   |            CPSB-BASE CPSB-NPM CPSB-EPM CPSB-LOGS CK-736456283846
===+===========+============+====================
```

// MDS Backup

First of all you have to make backup of MDS. Create some directory in /var, cd into it and run:
`mds_backup`

This will generate 4 files. All of them (!) copy to your PC or different server (compare md5sum after that).
Check Point also provides you something called "System Snapshot" for whole appliance/server backup with all partitions etc. DO NOT use it! It doesn't work in some cases and if it happens you're simply ... out of recovery :]

Exclude logs and db_versions from mds_backup (optional)

If you don't need backup of logs you can add exception which tells mds_backup to not do so.

Edit file $MDSDIR/conf/mds_exclude.dat and append two lines:
```
log/*
db_versions/*
```

Delete logs on MLM/CLM

Delete logs on MLM because otherwise they will be re-duplicated to every upgraded version (another bug) and MLM will be soon out of disk space.

Logs can be found here: /var/opt/CPmds-R71/customers/$CUSTOMER_NAME/CPsuite-R71/fw1/log/
You can safely leave last log file (fw.log) only and deleted or move the rest to different server.

Fixing DBImage issue

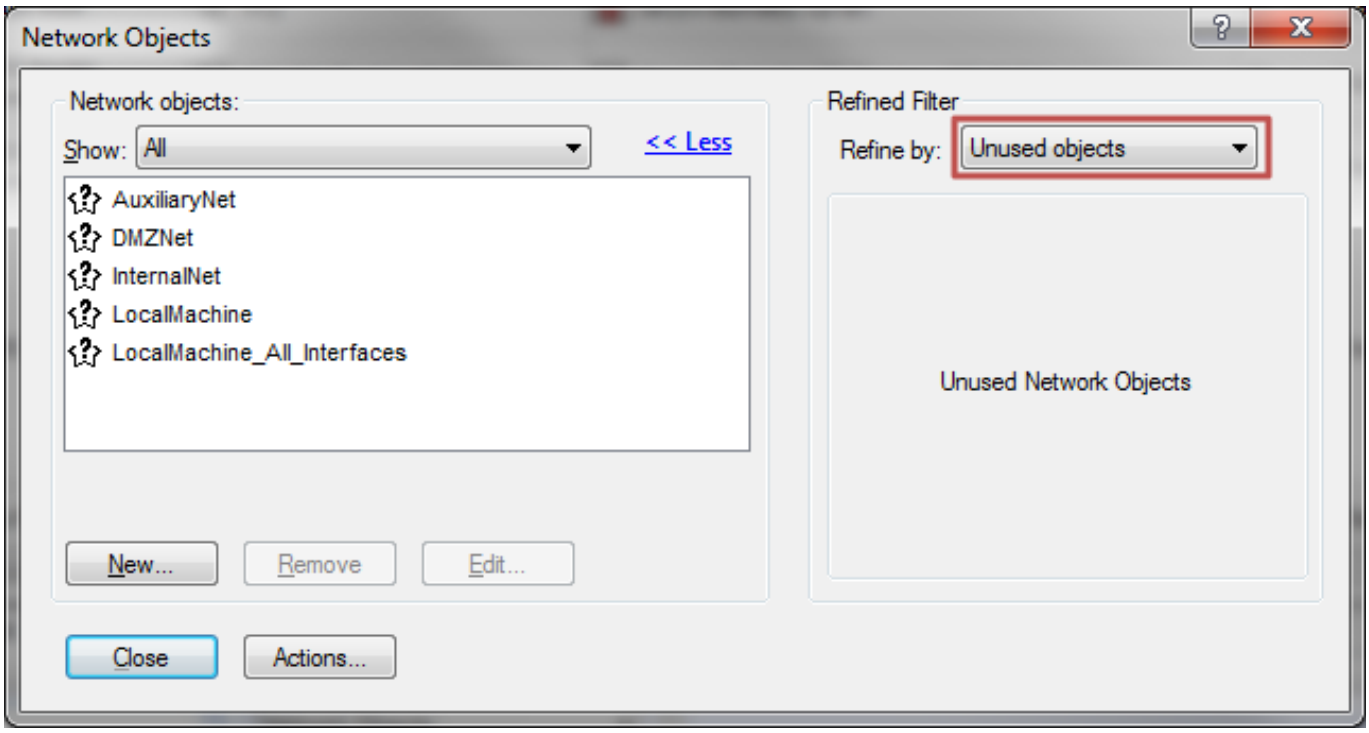
In my case mds_backup failed on standby MDS, because there is bug in R71.x which will create tons of DBImage files on standby CMA (one file for each policy installation). Due to this, mds_backup failed when compressing folder (too much arguments).

I have found SK describing this problem and only solution provided was delete those files.

```
rm -r /var/opt/CPmds-R71/customers/*/CPsuite-R71/fw1/conf/DBImage/*
```

Delete unused objects (optional)

Your management can be overloaded by many unused objects. It's always a good habit to delete them from time to time.
It can speed-up policy verification, SmartDashboard loading and also this upgrade because during upgrade process Check Point rebuilding object database.
You can find Unused objects in SmartDashboard by Query object and then select "Unused objects"



Delete everything except the five items which can't be deleted. So select all objects, remove from selection specified items and delete them. It can take a lot of time if you're deleting (for example) 5k objects. If possible, make this on some server accessible via RDP where it can run over night. This step is not mandatory for the upgrade.

// Upgrade from R71.20 to R75

On MDS/MDM (at this moment still Provider-1) create dir in /var and allow scp transfers for the admin account.

```
echo "admin" > /etc/scpusers
mkdir /var/mdsupgrade
chown admin /var/mdsupgrade
```

Make sure that you have valid MDS backup saved somewhere else.

Now copy from your server/PC installation DVD for R75. For example via scp:

```
scp Check_Point_R75_MD.Splat.iso
admin@192.168.11.10:/var/mdsupgrade/Check_Point_R75_MD.Splat.iso
```

It's also good idea to double-check file md5sum on destination MDS.

Mount DVD on MDS and run upgrade process

```
cd /var/mdsupgrade

# mount DVD to /mnt/cdrom
mount -t iso9660 -o loop Check_Point_R75_MD.Splat.iso /mnt/cdrom
cd /mnt/cdrom/linux/p1_install/

# disable login timeout
TMOUT=0

# stop MDS service
```

```
mdsstop

# run upgrade process
./mds_setup
```

Example of ./mds_setup output:

```
[Expert@cp-mdm-test]# ./mds_setup

*****************************************************************************
 Welcome to the Check Point setup center for Multi-Domain Security Management.
 This utility will guide you through the installation or upgrade process.

 Version: R75
*****************************************************************************

Checking for installed components. This may take a few seconds.
Please wait...

mds_setup has detected that your system has:
Provider-1 R71 installed

Please choose one of the following:

(1) Run Pre-upgrade verification only [recommended before upgrade]
(2) Upgrade to R75
(3) Backup current Multi-Domain Server
(4) Export current Multi-Domain Server
    Or 'Q' to quit.

Please enter your choice: 1
```

Select first option and read all problems which could occur. Some of them can be irrelevant and can be ignored.
Otherwise don’t go through upgrade until all issues are resolved.

Run ./mds_setup again and select option 2 - Upgrade to R75

```
mds_setup identified that you have a High Availability Multi-Domain Server
environment.

Please refer to the 'Upgrading in a High Availability Multi-Domain Server
Environment' section of
Multi-Domain Security Management Upgrade Guide for detailed upgrade instructions.

Would you like to proceed with the upgrade anyway [yes/no] ? yes

The Multi-Domain Security Management installation includes several
infrastructure packages. These packages will be installed now.

- Installing package <CPsuite-R75-00> ...
- Installing package <CPV40Cmp-R75-00> ...
- Installing package <CPEdgecmp-R75-00> ...
- Installing package <CPNGXCMP-R75-00> ...
- Installing package <CPCON62CMP-R75-00> ...
- Installing package <CPCON66CMP-R75-00> ...
- Installing package <CPSG80CMP-R75-00> ...
```

```
- Installing package <CPR71CMP-R75-00> ...
- Installing package <CPmds-R75-00> ...
Performing post install operations

Upgrade ended successfuly.

Summary of Upgrade operation:

==========================================================================

Multi-Domain Server databases - Success
Domain Management Server ASIA-DC-CMA1 database - Success
Domain Management Server EUROPE-DC-CMA1 database - Success
Domain Management Server JAPAN-DC-CMA1 database - Success
Domain Management Server AMERICA-DC-CMA1 database - Success
Domain Management Server EUROPE-DC-DMZ-CMA1 database - Success

==========================================================================
```

It can take 1-2 hours.
You will be then asked if you want to add another leading interface, MDS administrators, GUI clients, Groups, ... leave all as is.

If you think that upgrade is completed please double-check this file:

```
tail -f /opt/CPInstLog/install_status.log
```

If you see that installation is really completed and no new lines appear then you can be sure that the installation is complete. I saw that post-installation process is still rebuilding CMA database even if upgrade process has to be finished...
Or you can check system load via "top" command. When you see that system isn't working on something else, you can safely reboot system.

```
reboot
```

// Upgrade from R75 to R75.20

After reboot MDS will start all CMAs. It will take more than usual time so be patient.

When all CMAs are up:

```
[cp-mdm-test]# expert
Enter expert password:

You are in expert mode now.

[Expert@cp-mdm-test]# mdsstat
+-----------------------------------------------------------------------------------------
-----+
|                           Processes status checking
    |
+-----+------------------+----------------+------------+----------+----------+-----
-----+
| Type| Name              | IP address      | FWM        | FWD      | CPD      | CPCA
    |
+-----+------------------+----------------+------------+----------+----------+-----
```

```
-----+
| MDS |            -      | 192.168.11.10    | up 2912    | up 2911  | up 2910  | up
3399 |
+-----+------------------+----------------+------------+----------+----------+-----
-----+
| CMA |ASIA-DC-CMA1       | 192.168.11.13    | up 2872    | up 2868  | up 2820  | up
3405 |
| CMA |EUROPE-DC-CMA1     | 192.168.11.11    | up 2888    | up 2887  | up 2837  | up
3408 |
| CMA |JAPAN-DC-CMA1      | 192.168.11.14    | up 2874    | up 2867  | up 2819  | up
3397 |
| CMA |AMERICA-DC-CMA1    | 192.168.11.15    | up 2878    | up 2877  | up 2843  | up
3409 |
| CMA |EUROPE-DC-DMZ-CMA1 | 192.168.11.12    | up 2885    | up 2883  | up 2839  | up
3413 |
+-----+------------------+----------------+------------+----------+----------+-----
-----+
| Total Domain Management Servers checked: 5     5 up   0 down
     |
| Tip: Run mdsstat -h for legend
     |
+-------------------------------------------------------------------------------
-----+
```

Check license status:

```
[Expert@cp-mdm-test]# cplic print
Host             Expiration  Features
192.168.11.10     never       CPSB-BASE CPSB-NPM CPSB-EPM CPSB-LOGS CK-736456283846
192.168.11.10     never       CPSB-BASE CK-736456283846
192.168.11.10     never       CPPR-MDS-MC10-NGX CK-878789789795

Contract Coverage:

 #   ID          Expiration   SKU
===+===========+============+====================
1  | 1ASDF234   | 30Jun2012  | CPCES-CO-PREMIUM
   +-----------+------------+--------------------
   |Covers:     CPPR-MDS-MC10-NGX CK-878789789795
   |            CPSB-BASE CK-736456283846
   |            CPSB-BASE CPSB-NPM CPSB-EPM CPSB-LOGS CK-736456283846
===+===========+============+====================
```

You shouldn’t encounter a problem there. If so, you have to make rollback, update license and try upgrade again.
Rollback means that you will reinstall server to R71.10, upgrade ro R71.20 and then import previous mds_backup.

Run the script that checks (fixes) that database have correct version.
`/opt/CPmds-R75/scripts/mds_fix_cmas_clms_version -c ALL -n $mds-hostname`

Where $mds-hostname is name of your MDS server (without domain).

Example output:
`[Expert@cp-mdm-test]# /opt/CPmds-R75/scripts/mds_fix_cmas_clms_version -c ALL -n global-mds`

```
Examining EUROPE-DC-CMA1 database...
Object EUROPE-DC-CMA1 is already updated.
No changes required - Database of Domain Management Server EUROPE-DC-CMA1 was not
updated.
```

Make reboot once more (just to be sure).

Moving on to the next upgrade:

-> copy file to MDS

```
scp Check_Point_R75.20_MD.Splat.iso
admin@192.168.11.10:/var/mdsupgrade/Check_Point_R75.20_MD.Splat.iso
```

```
cd /var/mdsupgrade

# delete previous package
rm Check_Point_R75_MD.Splat.iso

mount -t iso9660 -o loop Check_Point_R75.20_MD.Splat.iso /mnt/cdrom

TMOUT=0

# stop MDS service
mdsstop

# run upgrade
patch add cd
```

Example output:

```
Choose a patch to install:

1) SecurePlatform R75.20 Upgrade Package (CPspupgrade_R75.20.tgz)
2) Exit

Your choice:
 1

Calculating the MD5 checksum of the package.
The MD5 checksum is: 3da513e7eb2e009c6bfee8284fc763cf
Is that right (Y/N)? y
Extracting /mnt/cdrom/SecurePlatform/patch/CPspupgrade_R75.20.tgz package ..

Start Upgrading ..

Do you want to create a backup image for automatic revert (y/n)?: n
Verifying ..

Extracting files ..
Extracting files completed successfully.
Upgrade program will now upgrade your system. This process may take several minutes
..
```

Rest of output is same as in previous update. As I stated above backup image is not needed and just

waste your time.

When all is done and system does not show some load (top command) you can safely reboot server to R75.20

// Upgrade to R75.30

When all CMAs are UP (mdsstat), run script checking version again.

```
/opt/CPmds-R75.20/scripts/mds_fix_cmas_clms_version -c ALL -n $mds-hostname
```

Copy upgrade package to MDS

```
scp Check_Point_R75.30_Upgrade.Splat.tgz
admin@192.168.11.10:/var/mdsupgrade/Check_Point_R75.30_Upgrade.Splat.tgz
```

```
mkdir /var/mdsupgrade/R753 && cd /var/mdsupgrade/R753
# unzip
gtar -zxvf Check_Point_R75.30_Upgrade.Splat.tgz

mdsstop
TMOUT=0

# run upgrade
./UnixInstallScript
```

Example output:

```
************************************************************
Welcome to Check Point R75.30 installation
************************************************************
Verifying installation environment for R75.30...Done!
The following components will be installed:
* R75.30
Installation program is about to stop all Check Point Processes.
Do you want to continue (y/n) ? y

Stopping Check Point Processes...Done!
Installing Security Gateway / Security Management R75.30...Done!
Installing R71 Compatibility Package R75.30...Done!
Installing UTM-1 Edge compatibility Package R75.30...Done!
Performance Pack R75.20 is not installed. Skipping installation.
Installing MDS R75.30...Done!
Installing SecurePlatform R75.30...Done!

*********************************************************************
Package Name                                                  Status
------------                                                  ------
Security Gateway / Security Management R75.30                 Succeeded
R71 Compatibility Package R75.30                              Succeeded
UTM-1 Edge compatibility Package R75.30                       Succeeded
Performance Pack R75.30                                       Skipped
MDS R75.30                                                    Succeeded
SecurePlatform R75.30                                         Succeeded
*********************************************************************
```

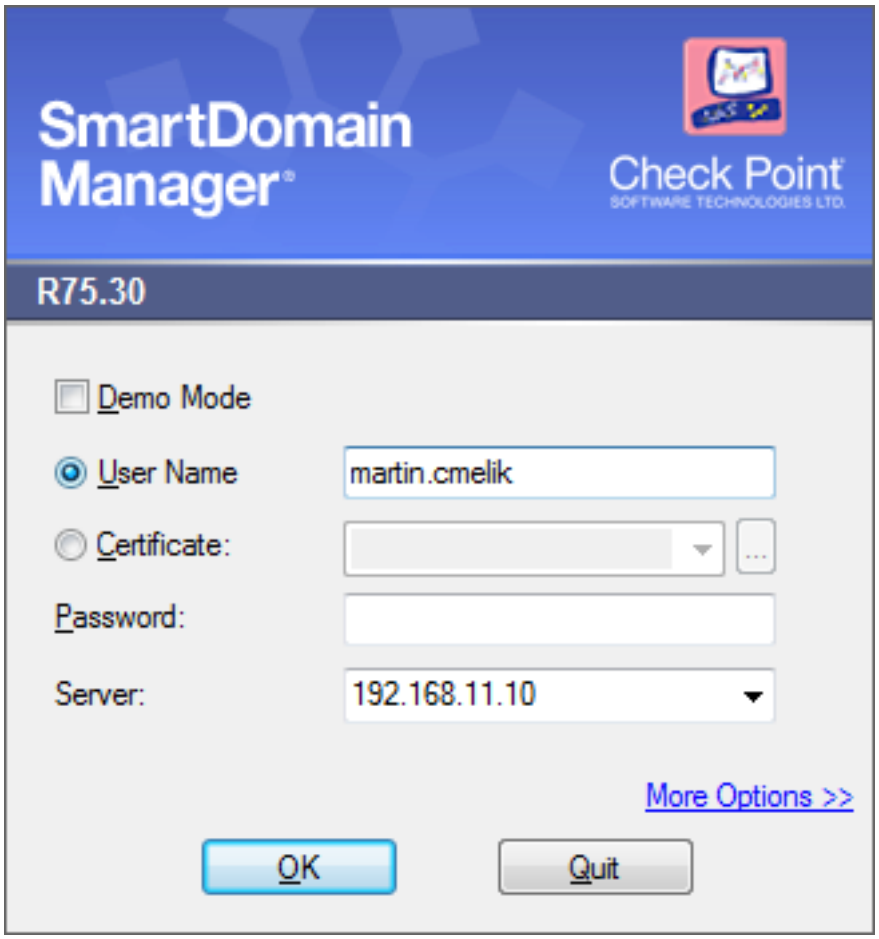
```
Installation program completed successfully.
Do you wish to reboot your machine (y/n) ? y

Broadcast message from root (pts/0) (Wed May  2 13:54:04 2012):
The system is going down for reboot NOW!
```

Cool... after reboot we have to be on R75.30
Just check all as before: mdsstat, cplic print, delete /var/mdsupgrade

```
[Expert@cp-mdm-test]# fw ver
This is Check Point VPN-1(TM) & FireWall-1(R) R75.30 - Build 066
```

Now you can login via R75.30 SmartDomain Manager.

You need to install Check_Point_R75.30_SmartConsole.Windows.exe and after that Check_Point_R75.30_SmartDomain_Manager.Windows.exe



If you're able to login you can continue with upgrading rest of servers.

In next part I will focus on problems after upgrade and how to fix them.

Next part: [How to fix problems after upgrade to Check Point Multi-Domain management R75.30] [7]

URL článku:
https://www.security-portal.cz/clanky/how-upgrade-check-point-multi-domain-management-r7120-r7530

Odkazy:

[1] https://www.security-portal.cz/users/cm3l1k1
[2] https://www.security-portal.cz/category/tagy/check-point
[3] https://www.security-portal.cz/category/tagy/networks-protocols
[4] https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doShowproductpage&productTab=overview&product=166
[5] https://www.virtualbox.org/
[6] http://www.virtualbox.org/manual/ch06.html#network_hostonly
[7] https://www.security-portal.cz/clanky/how-fix-problems-after-upgrade-check-point-multi-domain-management-r7530