# How to fix problems after upgrade to Check Point Multi-Domain management R75.30

Vložil/a <u>cm3l1k1</u> [1], 29 Červen, 2012 - 15:57

- <u>Check Point</u> [2]
- <u>Networks & Protocols</u> [3]

In previous post we focus on installation of MDM/MDS R75.30. As usual upgrade is not straightforward so I will show you what should be checked and how can be fixed common problems. Problems described here:

- After upgrade to R75.30 secondary CMA/CLM still shows R75.20 in SmartDashboard
- Problems with IP Pool NAT
- CP\_default\_Office\_Mode\_addresses\_pool
- Problem with MDS permission profiles

# // After upgrade to R75.30 secondary CMA/CLM still shows R75.20 in SmartDashboard

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\_do... [4]

Because of this bug you will have problem with CMA synchronization which would be visible in SmartDomain Manager -> High Availability

en Henepe	CH4							Construct of L
10-10-10	C. 141 A 10							/ Ed SmartDomain Manage
cke-Ba	High Arabababa Portan Conta	-						
Constant of Constant	Owner-Centerty	1P Address	Mut-Donar Sever	384	Adva Sanby	Sysc Status	Last Status Redification	
100 C	U 2 HA-Const Security Wanaperson							
	9 T		-	1000		Tarved	He 2 202 N 24 28	
1000				A 2840	ador.		Mey 2, 2012 14, 24 08	
		-		A plane	an dy		May 2, 2012 14 24 28	
		-	_		and a	Shrows.	May 2 2010 192000	
and the second se	1	and the second second	2000	of Second	1000		May 1 1910 M NOT	
Change and	and the second sec	_				turnet.	May 1 1810 18 1910	
6.00	10	-	and the second se	- Seriel	att-4	-	May 2 2012 14 24 56	
	14			w fight	mandra		Mey 2 2010 19 34 08	
and the second	- 1- Billion and B					Second	May 2, 2012 14 29 05	
contented	19		-	V Same	atten.		May 2, 2012 14 24 28	
	- P		1.00	V Saled	medy		Mey 2 2012 19 24 08	
	A CONTRACTOR	-				Second	Mey 2, 2012; 14 24 58	
and the second second	-		1.000	V Satel	8549		May 2 2012 14:34 08	
and the second second	19 Land		-	3044	andy.		Mb 3, 2010 14 24 28	
Cierce								
100								
- landsen								
1000								
1								
Lonsen								
and a local division of								
PELL RG								Multi-Donan Supervise

You're able to fix this easily on CLMs, but not on CMAs. You need to perform same actions through all secondary CLM/CMAs.

**To fix CLM version** open SmartDashboard of one CMA and open Check Point CLM object. In general properties you will see wrong version, but you're able to re-select Hardware (for example OpenServer) in Platform section which will make drop down menu "Version" visible and you can

Publikováno na serveru Security-Portal.cz (https://security-portal.cz)

#### change it to R75.30. Do so and change back correct Hardware type.

Make this as well on others CLMs and "Install Database" to reflect this change. Please don't confuse it with "Install Policy" which will not promote changes to CMA/CLMs but to firewalls.

General Properties Topology NAT	Check Point Host - General Machine	al Properties		
- Logs and Masters	Name:		Col	r: 📕 Black 👻
	IP Address:	Besolve from Nar	me 🔄 Dynamic Address	
	Comment: Provider-10	CLM		
	Secure Internal Communicat	ion .		
	Communication	ficate State: Trust established	6	Test SIC Status
	Data			
	Hartow Drug war	Version (1770-10)	08 Currentintum	-
	UTM-1	• • • • • • • • • • • • • • • • • • •	· US Secureriation	• Get
	Software Blac Power-1 Smart-1	1	and the second second	
	Open server	• Manage	mere babes: SM1003	•
	Network Sec. Other	agenere(1)		
	- Feewal	Application Control	IP Sec VPN	
	DIPSec VPN	URL Filtering	Sophisticated but simple	to manage
	Mobile Access	C QoS	Site-to-Site VPN and fite Access working seanle	vible Remote ssly with a
		Dynamic Routing O	variety of VPN agents.	
	C Idenity Awareness	Acceleration & Clustering Secure 2, 0		
	Arth Malware			
	Email Security		the later is the	
	Data Loss Prevention		- IN	and the second second
	C rowing		More Info	•
	1			
				IK Cancel

**To fix that on secondary CMAs** you need to use GuiDBedit because you cannot change Hardware type as in previous case.

How to fix problems after upgrade to Check Point Multi-Domain management R75.30

Publikováno na serveru Security-Portal.cz (https://security-portal.cz)

opology	Check Point Host - General Properties
ogs and Masters	Name: Color Black -
ther	IP Address: Beacive from Name
	Comment: Provider-1 CMA
	Secure Internal Communication
	Commyrication Cetificate State: Trust established Test SIC Status
	Pation
	Hardware: Other + Version: R75.30 + 05: SecurePlatform + Get
	Software Bades
	Network Securty Blades: SG103    Management Blades: SM1003
	Management (3)
	Network Policy Management     User Directory     Network Policy Management
	Secondary Server Provisioning Comprehensive security policy
	Endpoint Policy Management SmattReporter management using SmattDashboard - a single, united console for all reputy
	Ucoging & Status SnartEvent functionalities.
	Montoing SnatEvent
	Correlation Unit Management Potal SinatEvent Into
	Wołdow
	More Info

## // GuiDBedit

From CP website: "The Check Point Database Tool, also referred to as GuiDBedit, is a graphical user interface (GUI) that enables its users to edit objects and properties in the SmartCenter management database. This Database Tool allows users to change properties that cannot be edited using SmartDashboard."

Database Tool - GuiDBedit.exe - is located in the same folder where the SmartConsole is installed. Usually folder C:\Program Files\CheckPoint\SmartConsole\<version>\PROGRAM\

First of all close SmartDashboard windows and open GuiDBedit. Connect to one of CMA (not to Provider-1/MDS) and search in database field "**svn\_build\_num**". When you find first match also check that you have found this in secondary CMA object name (in our example CMA2) with class name host\_ckp (top right box). If it isn't correct field simply use "F3" to find next occurrence. When you find it check that Value is "983000000" (which means R75.20) and change it to "983625000". When finish save DB, open SmartDashboard and check that version is OK now. If so make this on all others secondary CMAs.

Publikováno na serveru Security-Portal.cz (https://security-portal.cz)



Now you can synchronize active and standby CMAs in SmartDashboard -> Policy -> High Availability

Server Name	Туре	Mode	Status	Note		
	Primary	Active				
< [		ш.				F
eer Status:						
Server Name	Туре	Reachable	Mode	Status	Note	
	Secondary	Yes	Standby	Synchronized		
< [		18				

# // Problems with IP Pool NAT

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\_do... [10]

IP Pool NAT enables N hosts to be NATed using M IP addresses (N:M, where N > M), unlike Static NAT which translates N:N IP addresses (from subnet to subnet), or Hide NAT which translates N:1 and does not support incoming connections. This allows also back-connections because it provides a

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

unique IP per NATed host.

This mapping/setup has been historically configured in file \$FWDIR/lib/user.def which has been replaced by several files during upgrades (I don't know why). So when you upgrade to R75.30 be sure that it is different file. Here you have file location which is also in relation to SPLAT version running on firewalls (why not bring some chaos into)

#### R75:

- R75 Management Managing R70/R71 Gateways: \$FWDIR/conf/user.def.FLICMP
- **R75** Management Managing **R75** Gateways: \$FWDIR/conf/user.def.NGX\_R75
- R75.20 Management Managing R75/R75.10 Gateways: user.def.R75CMP
- **R75.20** Management Managing **R75.20** Gateways: user.def.NGX\_R75.20
- R75.40 Management Managing R65 Gateways: user.def.NGXCMP
- R75.40 Management Managing R70/R71 Gateways: user.def.FLICMP
- R75.40 Management Managing R75/R75.10 Gateways: user.def.R75CMP
- R75.40 Management Managing R75.20/R75.30 Gateways: user.def.R7520CMP
- R75.40 Management Managing R75.40 Gateways: user.def.Fiber

If you're using this feature please update new file by simply copying configuration lines via text editor. As you see not all possible scenarios are described there, so if unsure copy config to many of them... yes, it is little bit confusing.

## // CP\_default\_Office\_Mode\_addresses\_pool

I'm not sure why, because we never use it, but after upgrade this object take its position in object database and what is worse enable automatic NAT. It means that when you're using range dedicated for Office Mode (172.16.10.0/24) in your network it can overwrite your NAT rules! If deleted, it must be specified for each gateway individually (in the VPN Clients page Advanced section).

Solution: Disable automatic NAT on CP\_default\_Office\_Mode\_addresses\_pool object.

How to fix problems after upgrade to Check Point Multi-Domain management R75.30

	Publikováno na	serveru Security-Portal.cz	(https://security-portal.cz)
--	----------------	----------------------------	------------------------------

Add Automatic Address T	ranslation rules	
anslation method:	Hide ~	
Ide behind Gateway	M	
Hide behind IP Address	55	
stall on Gateway:	😿 All View	
Apply for Security Gatewa	ay gontrol connections	

## // Problem with MDS permission profiles

This problem seems to be related to users who don't have Multi-Domain Superuser permissions. In our case we have accounts with read-only permissions to selected CMAs (for policy review, etc.) and those accounts were unable login into MDS.

Permission profiles has been changed and you need to reselect current roles.

Permission Profile Name:	Read_Write_All_Profile_no_DLP	-	Configuration
To edit global permis	None_All_Profile     Read_Only_All_Profile     Read_Write_All_Profile		
	Read_Write_All_Profile_no_DLP		Cancel

I don't remember other main problems. Simply check that High Availability is OK (if not synchronize CMA) and also check that SmartView Monitor see all firewalls.

That's all for now, be cool and ready for <u>R75.40 Gaia OS</u> [13]! :]

#### URL článku:

https://security-portal.cz/clanky/how-fix-problems-after-upgrade-check-point-multi-domain-managem ent-r7530

#### Odkazy:

#### How to fix problems after upgrade to Check Point Multi-Domain management R75.30

Publikováno na serveru Security-Portal.cz (https://security-portal.cz)

[1] https://security-portal.cz/users/cm3l1k1

[2] https://security-portal.cz/category/tagy/check-point

[3] https://security-portal.cz/category/tagy/networks-protocols

[4] https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\_doGoviewsolutiondetails =&solutionid=sk68563

[5] https://security-portal.cz/sites/default/files/SmartDomain-Manager-High-Availability.png

[6] https://security-portal.cz/sites/default/files/SmartDashboard-CLM-General.png

[7] https://security-portal.cz/sites/default/files/SmartDashboard-CMA-General.png

[8] https://security-portal.cz/sites/default/files/GuiDBedit-svn\_build\_num.png

[9] https://security-portal.cz/sites/default/files/SmartDashboard-Policy-High-Availability.png

[10] https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\_doGoviewsolutiondetai ls=&solutionid=sk62590

[11] https://security-portal.cz/sites/default/files/SmartDashboard-Office-mode-NAT.png

[12] https://security-portal.cz/sites/default/files/SmartDomain-Manager-Administrators-Assign-Permis sions.png

[13] http://www.checkpoint.com/gaia/