

Kontrola stavu antivírusu cez CM zjednodušuje správu antivírového programu. Toto riešenie nemá za cieľ nahradiť administrátorské konzoly od jednotlivých výrobcov, ale má vám dať rýchlu informáciu o chybnom stave, v mnohých prípadoch aj o konfigurácii antivírových programov rôznych výrobcov na jednom mieste. Prostredníctvom funkcie CM <u>Vzdialené inštalácie a skripty</u> [1] je možné niektoré z nich aj jednoducho updatovať.

Poznámka : Ak máte na počítačoch antivírový program, ktorý CM nepozná alebo je nedostatočne detekovaný a máte vážny záujem o jeho implementáciu do CM, napíšte nám na support@customermonitor.eu

Ako funguje kontrola stavu antivírusu cez riešenie CUSTOMER MONITOR[®] ?

- CM Server pomocou C-Deskriptu prehľadne zhromažďuje informácie o nainštalovanom antivírusovom softvéri. Informácie získané C-Deskriptom odosiela C-Monitor na CM Server raz za deň, ak nie je predvolený interval vykonávania C-Deskriptu pozmenený.

 C-Deskript vyčítava informácie o vtbraných verziách antivírusového softvéru, verziách vírusových databáz, spustenia antivírusov, aktualizačnej cesty, autentifikácie pre aktualizáciu, vytváraní mirroru, expirácii licencie, prípadne ďaľšie užitočné informácie. Zobrazené údaje sa líšia podľa typu antivírusového programu.

- Upozorňuje na problémy s nenainštalovaným antivírusom, aktualizáciou antivírusu, či nebežiacim antivírusom

- CM Server poskytuje informácie o antivírusových softvéroch Eset Antivirus, Eset Security, Eset File Server Security, Eset Mail Security, Kaspersky.

Možnosti kontroly stavu antivírusu cez CM portál

 Informácie o aktuálnom stave antivírusov sú zhromaždené na Customer Monitor portáli. Prístup k údajom je cez "CM IT monitoring" > "Zóny" a zvolením filtra "Antivírusy"



Kontrola stavu Antivírusu cez CM

Zverejnené na Customer Monitor (https://www.customermonitor.sk)

CDESK		Admin zóna	CM IT monitorin	1. CD	ESK		Slovensky Kred	it Manual Operátor: Meno (Operátora 🗸
<u>√</u> •	Zobrazenia C	🚦 Zóny							? 9
Oblübené	💬 Počilače		Spoločnosť		Počitač 8 Umiestnenie	Positivat	er		_
	7 Online informácie	Arthitusy 3. •	Operátor		Zoradiť podľa CM-D 💌	Zoredit	iko Vzosłupne 🔻	Hladať	× ×
Upozomenia	Walches		08		🗹 Zahrnüt ruöne zadanè polit	ale 🗵 Ler	online politale		
	🐟 Internet bandwidth monitor	Zóna Antivirusy [20braz	ené 4 položity]						
201 Zobrazonia	🔿 Zbny 2.	Parameter	1. SEANB050	2. SEANDOO			3. SEANB36	4. OTSNB53	
	😨 Zmeny na počitači	History	Show history	Show history			Show history	Show history	
\sim	Foto dokumentácia	Network Name	TOMAS-NB	JURAJ-HP			SEANB036	SEANB056	
N		User	Tomes	Juraj			Miro	Sonka - test	
Apikačné zbru	S CMDB Dashboard	Current Login	tomes-nil/tomes	Juraj-HPJuraj			SEANB036/miro	SEANB059/sonka	
		Location	Tomas	Topolova			Bratislava	dnv	
Systémové		Security Center	1. SEAMB050	2. <u>SEANDOO</u>			3. SEANB36	4. OTSNB53	
zóny		Product	Windows Defender	ESET Endpoint A	Anthritrus 5.0		Hicrosoft Security Essentials	ESET NOD32 Antivirus 4.2	
1		Antivirus health	Good	Good			Good	Good	
		Product	Windows Defender	FSFT Fadaoint J	officieure 5.0		Herman & Sacurity Paparitais	ESET MODIZ Astronom 4.2	
Manacherské jednomácie		Anthinus health	Good	Good			Good	Good	
		Product		Nod Antivir 5.0				Nod Artivir 4.0	
		Version		8014 (20130215	5)			8011 (20130214)	
		Product version		5.0.2126.4				4.2.71.2	
		Product type		ESET Endpoint A	Indivirus			Home Edition	
		Expiration date		01.10.2013				01.10.2013	
		User name		EAV-58353800				EAV-58353800	
		Modules		perseus, system	nstatus, hips, amon, translator, protoso	an, db		perseus, systematatus, selfde	fense, amon
		Program status		Running				Running	
		Mirror configured		No				No	
		Update user		EAV-59353800				EAV-59353800	

Obrázok: Príklad informácí v CM portáli o antivírusovom softvéri ESET NOD 32 a Microsoft Security Essentials

Informácie o antivírusových poruchách sa nachádzajú v CM IT monitoring -> Poruchy

CDESK		,	Admin zór	na 🧧	M IT monitorin	• •	DESK			Slovensky	Gredit Manua	il Operátor: Meno Operátora v	/
1.0	Upozornenia 🔍	8	Poru	ichy									?
Obliberel	× Poruchy	Spol	teonio		Poditač & Umiestnenie		PouEvater	Operato	×	Тур			_
1	Of Historia ponich	121.0	and the last setting of	W Altern	Zilohovanie	a Image (všetky) defense a Tit Note	•				Hfadaf	
Uporomenia	🕎 Poruchy na počítačoch	• K	micky alarm	n 🖄 Alerim I	Varovanie 🗆 Bei	z chyby 🗆 Ne	definiovane 🖭 Blokk	wane 📖 cakajuca i	la uzavretie				
		MDTSV04 - MEDITOP-SQL2005 : Zoznam poruchových stavov (zobrazená 1 položka)								Potendiť označené poruchy			
Zobrazenia		x	ы	Ûroveñ	Trvanie poruchy	 Popis poruchy 	Dátum poslednej správnej zálohy	Meno úlohy zálohovania z rozvrhu	CM-ID počitača	Meno počitača v sleti	Pouffwater	Spoločnosť	
			13688094	•	10h 21m 38s	Zálohovanie - NT Backup	14.00.2012	SystemState	MOTSVOM	SQL2005		MED, is co.	Detail

Obrázok: Príklad zaznamenaných porúch antivírusov na CM portáli

O vzniknutí poruchy antivírusového softvéru CM Server vygeneruje notifikačný E-mail.



Obrázok: Príklad E-mailovej notifikácie o antivírusovej poruche

Odstránenie poruchy

K zaniknutiu poruchy príde ihneď po prijatí C-Deskriptu z C-Monitoru, kde už je zóna vyhodnotená s bezchybným stavom. Predchádza tomu zásah technika do nastavení antivírusu priamo na počítači.

Poruchu je možné potvrdiť v "CM IT monitoring" > "Poruchy" otvorením konkrétnej poruchy a kliknutím na "**Potvrdiť poruchu**".



Kontrola stavu Antivírusu cez CM

Zverejnené na Customer Monitor (https://www.customermonitor.sk)

Úplne **zablokovať vyhodnocovanie alebo notifikovanie porúch** antivírusu je možné v "Admin zóna" > "Počítače", kde po rozkliknutí príslušného počítača a kliknutí na záložku "Vyhodnocovanie zón" možno vyhodnocovanie zóny úplne zablokovať, prípadne zablokovať notifikáciu o vzniku poruchy.

CD	ESK	Admin zóna 1. CM IT monitoring CDESK	Slove
5.0	Hlavné menu 🔹	3 Nastavenie C-Monitora na PC	
Oblübené	7ákozníci – postovonia	Spoločnosť Počítač &	Použiv./Email
<mark>≈</mark> 2.	Počilače 3,	Licencia	OS Hiradat
Havné menu	La Audit SW a evidencia HW	Počitač SEANB33 (JANO_W7) 4.	
გუ		Všeobecné nastavenia Online spojenie Vycoohooovani	e zon Vzdialený prístup SMS kontakty pre Watches Nastavenia C-
Používatelia		Blokovanie spúšťania vyhodnocovania zón	
		Blokované je spůšťanie označených zón	
8		🖾 Antivírus - aktualizácia	📰 Disk - voľné miesto, Windows NT, ME, 98
CMDB		🖾 Antivírus - nenainštalovaný antivírus	📰 Emailové súbory - Exchange - veľkosť edb a stm súborov
CHILD D		🖾 Antivírus - stav spustenia/zapnutia	Emailové súbory - Exchange - veľkosť emailových schránok
1.6		Antivirus - vypršanie platnosti licencie na počitači	Emailové súbory - Outlook - veľkosť pst súborov
		C-Monitor - POP3 komunikácia	Emailové súbory - Outlook Express - veľkosti dbx súborov
Admin. nástroje		C-Monitor - aktivita SMTP spojenia	Externé programy
		C-Monitor - aktualizácia Complete konfigurácie SDF v CM	Internet - obmedzenie pristupu
C		C-Monitor - detekcia chýb na počítači	OS - aktualizācia Windows
C-Monitor		C-Monitor - komunikácia, množstvo dát	OS - vytváranie bodov obnovy vo Windows
latent		C-Monitor - neplatný podpis súboru	Permission Explorer - rozvrh, vytváranie spd súborov
5		C-Monitor - rozvrh, aktualizácia v CM	Permission Explorer - st'ahovanie spd súborov do CM
ک		C-Monitor - rozvrh, chybné nastavenie pre C-Descript	Sledované súbory - sledovanie zmien
Komunikácia		C-Monitor - rozvrh, vypršanie platnosti úlohy	Zálohovanie - C-Backup potvrdený od používateľa
		C-Monitor - vypršanie platnosti licencie	Zálohovanie - C-Backup s intervalom do 6 dni
- <u>L</u>		C-Monitor - zaseknutá úloha	Zálohovanie - C-Backup s intervalom od 7 dni
Externé		Disk - SMART parametre (existujúce poruchy treba potvrdiť)	Zálohovanie - NT Backup
programy		Disk - kontrola pritomnosti	Zálohovanie - Windows Backup
		Disk - stav Raid poli (Linux / FreeBSD)	Zálohy - VCB Images
		Disk - voľné miesto na sieťových diskoch	Zálohy C-Images
Archiv		Disk - voľné miesto, Linux, FreeBSD	Zálohy C-Images s potvrdením od používateľa
414		Disk - voľné miesto, Windows 2000 a vyšši	
I I I Parametre		Online spojenie	Watch (Online)
		Blokovanie emailovej notifikácie jednotlivých zón	
		Blokované sú emaily z označených zón (toto nastavenie má najvyššiu	prioritu, t.j. ak je označená niektorá zóna, tak emaily sú vždy blokované všetkým)
		Antivirus - aktualizácia	Disk - voľné miesto, Windows NT, ME, 98
		C Antivirus - nenainštalovaný antivirus	Emailové súbory - Exchange - veľkosť edb a stm súborov
		C Antivirus - stav spustenia/zapnutia	Emailové súbory - Exchange - veľkosť emailových schránok
		Antivirus - vypršanie platnosti licencie na počitači	Emailové súbory - Outlook - veľkosť pst súborov

Obrázok: Príklad nastavenia blokovania vyhodnocovania a notifikácie antivírusovej zóny Date:



[5]

Odkazy

- [1] https://www.customermonitor.sk/node/575
- [2] https://www.customermonitor.sk/sites/default/files/antivirus.png
- [3] https://www.customermonitor.sk/sites/default/files/Poruchy.png



[4] https://www.customermonitor.sk/sites/default/files/notifikacny%20mail.png [5] https://www.customermonitor.sk/sites/default/files/blokovanie%20poruch.png