

Security Compliance Manager - Nova inačica odličnog alata



Ovih dana Microsoft je ažurirao **Security Compliance Manager** (SCM), jedan od alata svoje *Solution Accelerators suite*. Budući je riječ o aplikaciji koja je „must have“ za administratore Windows servera i stanica, dobro je znati da SCM, aktualne verzije 3.0, sada u potpunosti podržava Windows Server 2012, Windows 8 i Internet Explorer 10 te, za sada djelomično, SQL Server 2012.

Zašto je SCM obavezan alat za svakog Windows admina? Veseli činjenica što je besplatan, svakako, no za konačnu ocjenu, a ta je „odličan“, ipak su presudne njegove spoznajne i izvedbene funkcionalnosti. Ukoliko se prvi puta srećete s njime, osnovne informacije o SCM-u naći ćete već na [download](#) [1] stranici, stoga u nastavku slijedi ono što nije tako lako naći.

Spoznajna dimenzija SCM-a ilustrirana je slikama 1 i 2. Sigurnosna problematika za svaki MS-ov produkt učlanjen u SCM kvalitetno je obrađena u pripadajućem *Security Guideu*. U ovom slučaju, nažalost, kvaliteta utječe na kvantitetu pa je Security Guide za Windows Server 2012 „težak“ 268 stranica! No, bez zezanja, rabim SCM od njegove druge verzije te iz osobnog iskustva mogu reći da su ti vodiči prvorazredna literatura za Windows sistemca koji želi ovladati sigurnosnim aspektom nekog Microsoftovog proizvoda obuhvaćenog SCM-om. Također, da je obrazovna uloga SCM-a dobro promišljena, zaokružena, pokazuje nam i slika 2, naime, svaka opcija nekog security predloška opisana je pod svojim gumbom *Settings Details*. Ako pogledamo gornji dio slike 2, učit ćemo da njome prikazani predložak za *Domain Controllere* ima čak 436 opcija! Utoliko, zaista je praktična mogućnost da se informiramo tamo gdje konfiguriramo.

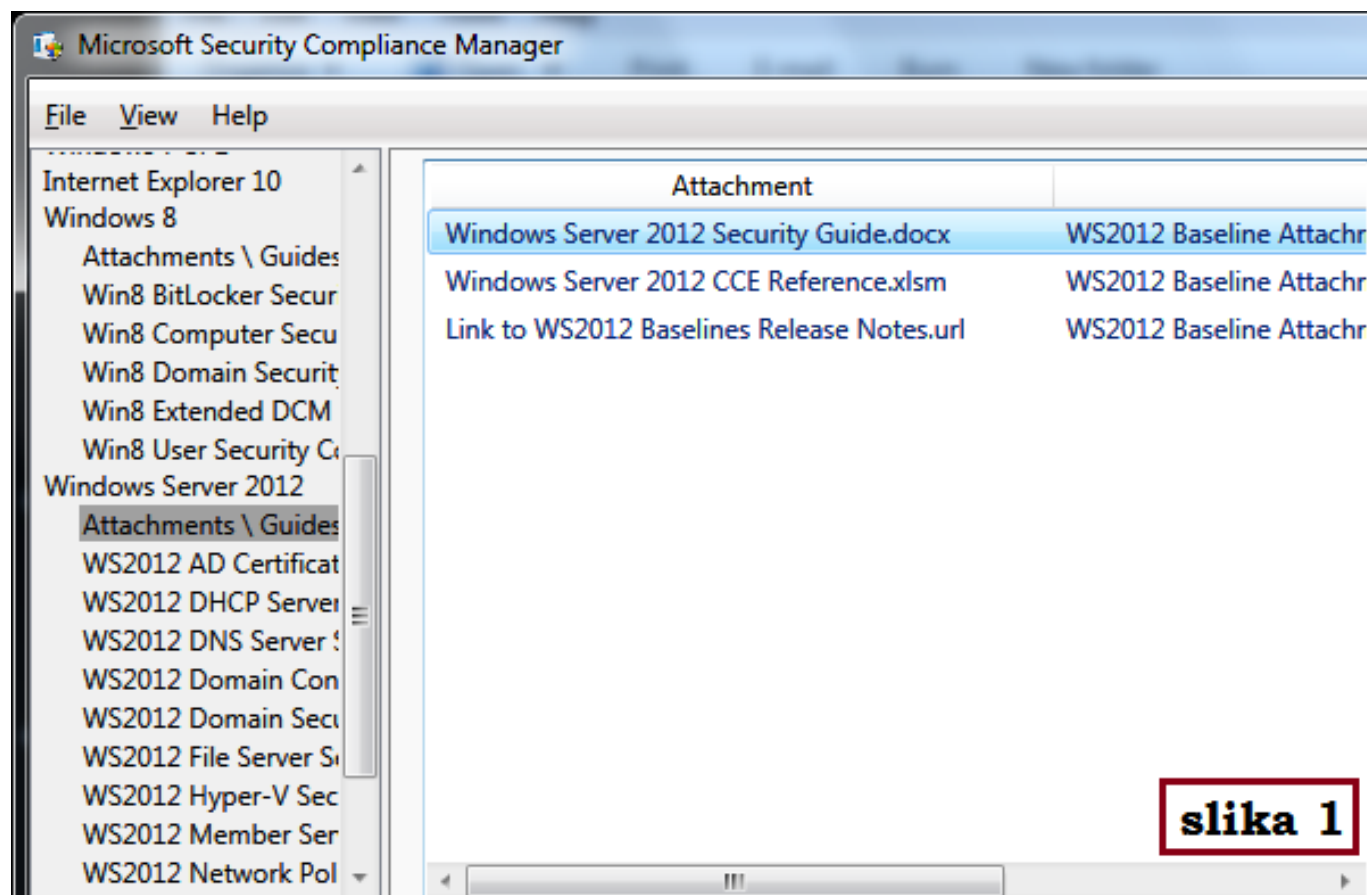
Sada malo o izvedbenoj, operativnoj strani SCM-a. To je u stvari aplikacija kojom obrađujemo – kreiramo, mijenjamo, spajamo, uspoređujemo, uvozimo-izvozimo... (bla-bla) security predloške. Zašto? Zato da bismo ih potom primijenili na Windows računala kao lokalne ili domenske *Group Policy* objekte. Alat ima dvojaku vrijednost: on izvanredno doprinosi radnoj efikasnosti Windows admina i zaštiti Windows instalacija, pri čemu ne ciljamo samo na razinu OS-a. Pogledajte lijevi stupac slike 3 i vidjet ćete na koje je MS-ove produkte primjenjiv. Desni stupac iste slike, pak, pokazuje da brojne opcije security predloška možemo strukturirati po oblastima, ako tako smatramo svrsishodnijim (jer postoji i tzv. *simple view*, nestrukturirani pregled).

Ovaj hvalospjev završavamo temom s kojom članak o nekom softveru obično započinje – instalacijom SCM-a na admin stanicu. Bijahu vremena kada je objašnjavanje kako instalirati neki MS-ov alat bilo ravno „otkrivanju tople vode“, dakle, nešto u osnovi suvišno. Iznenadjujuće, s aktualnom verzijom ovog alata to nije slučaj pa slijedi par sugestija na temu instalacije.

- Tijekom pokretanja downloadane **SCM-setup.exe**, održavati Internet vezu kako bi setup poskidao razne preduvjete;
- nakon instalacije preduvjeta, pokrenuti *Windows Update* da pokrpamo tek instalirani softver;
- ponovo pokrenemo SCM-ov setup, uključimo opciju za automatsko osvježavanje baze podataka (paketa) SCM-a;
- zanemariti eventualnu poruku tipa Compatibility Issues tijekom instalacije SQL Expressa;
- kad se SCM podigne i popije ažuriranja s Interneta, zaguglati za KB2546951 te skinuti i primijeniti x86 Service Pack 3 za SQL 2008 (bez obzira na arhitekturu OS-a odn. CPU-a).

Gornje se odnosi na „clean install“ SCM-a 3.0. Gospoda koja, poput moje malenkosti, na admin stanicima imaju prethodnu verziju SCM-a, trebaju iz konzole ove aplikacije odobriti nadogradnju instalirane verzije na noviju, potom samo vrte palčevima i čekaju...

Završni savjet: u radu kombinirajte MBSA 2.2 i SCM 3... i mirno spavajte. Davno su prošla vremena kad je Microsoft bio sinonim za nesiguran softver. I instalacije tipa Next > Next > Next, hohooo ;-).



WS2012 Domain Controller Security Compliance 1.0

436 unique setting(s)

Advanced View

Name	Default	Microsoft
Interactive logon: Require Domain Controller authenti	Disabled	Disabled
Network security: Minimum session security for NTLM	No minimum	Require NTLMv2
Network access: Let Everyone permissions apply to an	Disabled	Disabled
Collapse Severity: Critical Cus Value must be equal to Disabled. Customize setting value Disabled Comments:		
Setting Details		
Interactive logon: Require smart card	Disabled	Not Defined
Interactive logon: Smart card removal behavior	No Action	Lock Workstation
Network security: Minimum session security for NTLM	No minimum	Require NTLMv2
Network Security: Restrict NTLM: NTLM authenticator	Not defined	Not Defined
Network security: Do not store LAN Manager hash val	Enabled	

slika 2

The screenshot displays the Security Compliance Manager interface. On the left, a list of baselines is shown, with 'WS2012 Domain Controller Security Compliance 1.0' selected. On the right, the configuration for this baseline is shown, including a list of settings and their default values.

Left Panel (Baselines):

- tom Baselines
- rosoft Baselines
- Exchange Server 2007 SP3
- Exchange Server 2010 SP2
- Internet Explorer 10
- Internet Explorer 8
- Internet Explorer 9
- Microsoft Office 2007 SP2
- Microsoft Office 2010 SP1
- Windows 7 SP1
- Windows 8
- Windows Server 2003 SP2
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows Server 2012
 - Attachments \ Guides
- WS2012 AD Certificate Services Server Security 1.0
- WS2012 DHCP Server Security 1.0
- WS2012 DNS Server Security 1.0
- WS2012 Domain Controller Security Compliance 1.0**
- WS2012 Domain Security Compliance 1.0
- WS2012 File Server Security 1.0
- WS2012 Hyper-V Security 1.0
- WS2012 Member Server Security Compliance 1.0
- WS2012 Network Policy and Access Services Security 1.0
- WS2012 Print Server Security 1.0
- WS2012 Remote Access Services Security 1.0
- WS2012 Remote Desktop Services Security 1.0
- WS2012 Web Server Security 1.0
- Windows Vista SP2
- Windows XP SP3

Right Panel (WS2012 Domain Controller Security Compliance 1.0):

Advanced View 436 unique setting(s)

Name	Default
Authentication Types	21 Setting(s)
Encryption Configuration	15 Setting(s)
Event Logging	58 Setting(s)
Identity Management	3 Setting(s)
Key Management	2 Setting(s)
Least Functionality	29 Setting(s)
Least Privilege	47 Setting(s)
Log Access Limitation	1 Setting(s)
Logging Configuration	8 Setting(s)
Network Protection	31 Setting(s)
Password Attributes	7 Setting(s)
Protocol Configuration	51 Setting(s)
Session Configuration	10 Setting(s)
System Defaults	4 Setting(s)
System Integrity	14 Setting(s)
System Services	201 Setting(s)

slika 3

čet, 2013-02-21 10:19 - Ratko Žižek **Vote:** 5

Vaša ocjena: Nema Average: 5 (3 votes)

Source URL: <https://sysportal.carnet.hr/node/1212>

Links

[1] <http://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx>