predstavljamo vam

WINDOWS SERVER 2008

Saša Prudkov

kompjuter biblioteka

Top 10 razloga da pređete na njega

Prošlo je mnogo vremena od kada smo videli novu verziju Windows Server-a. Teško je poverovati da je prošlo pet godina od kada je izašao Windows Server 2003. E pa ove godine možemo da prestanemo da čekamo. Windows Server 2008 je zvanično izašao ovog meseca i sada imamo pristup svim njegovim elementima. Prošlo je mnogo vremena i Microsoft je uložio jako mnogo truda i rada u Windows Server 2008 kako bi bio najbolji do sada.

Napravljeno je hiljade izmena u Windows Server-u 2008 u poređenju sa Windows Server-om 2003. Neke su veoma male, ali neke su veoma velike i značajne. Ali pitanje koje svi postavljaju je šta to Windows Server 2008 nudi da vredi nadgraditi na njega? Odgovor na ovo pitanje će biti glavna tema ove serije kratkih članaka.

Postoji suviše mnogo izmena i poboljšanja u Windows Server-u 2008 da bi mogla sva da se pokriju u jednom članku, zato ćemo izlaganje podeliti na nekoliko kraćih članaka. U ovim člancima fokusiraćemo se samo na funkcije i mogućnosti za koje mi mislimo da su one zbog kojih vredi nadgraditi na Windows Server 2008.

Mnogi će pomisliti da sam izostavio neke važne stvari u ovom opisu mogućnosti Windows Server-a 2008 i biće u pravu, jer nisu svima bitne iste stvari. Zato ću ja ovde govoriti samo o velikim izmenama za koje se ja nadam da će usrećiti većinu korisnika.

Sledi lista novosti i pobljšanja kojima ćemo se baviti u ovim člancima o Windows Server-u 2008 jer mislimo da će one biti najzaslužnije za prelazak korisnika sa Windows Server-a 2003 na Windows Server 2008.

- Server Manager i Advanced Event Viewer
- Server Core
- Terminal Services Gateway
- Terminal Services RemoteApps
- Izvorna podrška za IPv6
- Read Only kontroleri domena
- Hyper-V

- Network Access Protection (NAP)
- Secure Sockets Tunneling Protocol (SSTP)
- Windows Advanced Firewall QoS zasnovan na polisama

Server Manager i napredni Event Viewer

Windows Server 2008 poseduje potpuno novi interfejs za upravljanje poznat pod imenom Server Manager. Server Manager je jedino mesto koje će vam trebati za konfigurisanje, upravljanje i praćenje servera. On nije kao menadžeri servera koje ste koristili u prošlosti; ovaj stvarno radi i njega ćete definitivno koristiti svaki dan za upravljanje Windows Server 2008 računarima.

U Server Manager, vi možete da instalirate Server Roles-ove (kao što je DNS, DHCP, Active Directory) i Role servise (kao što je Terminal Services Gateway i RRAS). Kada instalirate Server Roles-ove (serverske uloge) i Role Services-e (servise uloga), MMC konzole za ove servise se instaliraju u Server Manager-u. Više ne treba da kreirate sopstvene MMC-ove!

Server Manager takođe može da se pohvali sa novim Event Viewer-om. Ovo nije Event Viewer vašeg oca koji poseduje samo System, Security i Application nodove. Windows Server 2008 Event Viewer vam obezbeđuje logove događaja koje možete da koristite. Tu su standardni Windows Event Log-ovi: Application, Security i System. Ali sada imate mogućnost da vidite događaje za sve aplikacije i servise instalirane na računaru. Pored toga, vi možete da kreirate Custom View-ove Event Log-ova, tako da možete da kreirate sopstvene kontejnere za događaje na osnovu filtera koje izaberete.

Jedna od novih Event Log funkcija koja mi se sviđa je mogućnost da se prijavite za događaje na drugim mašinama u mreži. To vam omogućuje da skupljate Event Log podatke sa drugih mašina, na osnovu filtera koje ste obezbedili. Na taj način, vi možete da konfigurišete filtere za kritične događaje na najvažnijim serverima u vašoj mreži. Iako mu nedostaje prefinjenost kompletnog rešenja za nadgledanje kao što je System Center Operations Manager, ovo je veoma dobro rešenje za nadgledanje za one kompanije koje ne žele da plate za mogućnosti koje nudi SCOM.

Server Core

Windows Server 2008 može da se instalira na dva načina: kompletna instalacija full ili samo jezgro servera. Server Core instalacija instalira podset binarnih fajlova koji su neophodni da bi jezgro operativnog sistema radilo. Nikakvi opcioni servisi se ne instaliraju niti se aktiviraju. Nema korisničkog interfejsa osim komandne linije. Nema školjke Windows Explorer-a i celokupna konfiguracija mora da se uradi lokalno u komandnoj liniji, ili udaljeno pomoću MMC konzole ili nove Windows Remote Shell (WinRS) aplikacije za udaljeno upravljanje (slično SSH-u).

Cilj jezgra servera nije da bude teži za upravljanje (mada upravljanje jeste teže u određenom stepenu jer se mnogi zadaci moraju obavljati iz komandne linije i ne mogu da se urade udaljeno preko MMC konzole). Pravi cilj Server Core-e je da se redukuje površina za napad i da se smanji broj ažuriranja servera. Pošto većina bezbednosnih ažuriranja Windows-a obično uključuje servise i aplikacije koje ni ne koristite (kao što je Windows Media Player ili Internet Explorer) na serveru, vi onda ni ne morate da ažurirate ove komponente. A zahvaljujući znatno smanjenom broju servisa i aplikacija koji rade na jezgru servera, površina koja može da se napadne je značajno smanjena.

Jezgro servera pokreće ograničeni broj uloga servera (Server Roles), što znači da morate da se postarate da je uloga servera koja vas interesuje podržana od strane instalacije jezgra servera. Takođe, neke od uloga servera nisu u celosti podržane, kao što je Web Server uloga. Server Core ne podržava .NET upravljani kod, i zbog toga nećete moći da koristite IIS konzolu kao udaljeni MMC. Ovo izaziva ozbiljne upravljačke glavobolje zato što IIS konfiguracija na mašini jezgra servera mora da se uradi u komandnoj liniji pomoću appcmd.exe-e. Ako ste administrator Apache-a, bićete jako sretni. Ako ste povremeni administrator IIS-a, verovatno ćete želeti da pričekate na unapređenja u radu sa jezgrom servera.

Server Core je definitivno korak u dobrom smeru. Međutim, u ovom trenutku treba ga posmatrati kao 1.0 izdanje. Sigurni smo da je cilj Server Core-a da se smanji površina za napade i smanji potreba za ažuriranjem, a ne da se njime teško upravlja. Očekujemo da će sledeća ažuriranja Windows Server-a 2008 omogućiti lakše ažuriranje i tako ispuniti svačija očekivanja.

Terminal Services Gateway

Jedna od prepreka za potpuno anagažovanje Terminal Services za udaljeni pristup korisnika je bila činjenica da veliki broj administratora nije imao poverenja u sekvencu autentifikacije i nivo šifrovanja RDP tunela. Drugi problem na koji su naišli je činjenica da veliki broj firewall-ova na udaljenim lokacijama nisu dozvoljavali izlazni TCP 3389. Microsoft je rešio ovaj problem tako što je predstavio Terminal Services Gateway u Windows Server-u 2008.

Terminal Services Gateway je tip SSL VPN-a, na isti način na koji je RPC/HTTP za Outlook-ov pristup ka Exchange Server-u SSL VPN. SSL VPN tip je onaj od proksija protokola aplikacije. Terminal Services Gateway radi sa RDP 6.0+ klijentom kako bi omogućio inkapsulirane RDP konekcije ka TS Gateway računarima.

RDP klijent u stvari inkapsulira RDP protokol u dva druga protokola. Prvo, RDP protokol se inkapsulira u RPC zaglavlje, a onda se inkapsulira drugi put pomoću šifrovanog HTTP zaglavlja (SSL). Protokol koji se koristi za konektovanje sa TS Gateway-om je u stvari RDP/RPC/HTTP. Microsoft je najverovatnije ovo uradio kako bi mogao da koristi postojeći RPC/HTTP kod koji su već imali za svoj RPC/HTTP proksi. Kada konekcija stigne do TS Gateway mašine, TS Gateway uklanja RPC i HTTP zaglavlja i prosleđuje RDP konekcije ka odgovarajućem Terminal Server ili Remote Desktop računaru.

Connection Authorization Policy ili CAP-ovi se koriste da se odredi koji korisnici mogu da pristupe resursima kroz ovaj TS Gateway računar. Windows Server 2008 poseduje konfiguracioni interfejs za povezivanje sertifikata sa TS Gateway sajtom kako bi bile omogućene bezbedne SSL konekcije.

Terminal Services Gateway takođe podržava Smart Card autentifikaciju a vi takođe imate opciju da uvedete NAP klijentsku kontrolu pristupa. Terminal Services Gateway je definitivno jedan od glavnih razloga da nadgradite na Windows Server 2008.

Terminal Services RemoteApps

Cilj svakog administratora zaduženog za bezbednost je da svaki korisnik ima što je moguće manje privilegija. To posebno važi za ostvarivanje konekcija na daljinu. Administratori zaduženi za bezbednost ne mogu noću da spavaju razmišljajući o obezbeđivanju potpune udaljene desktop konekcije korisnicima koji nisu administratori. Sve što je potrebno da bi neki haker stekao potpunu kontrolu nad desktop okruženjem i kompromitovao vašu mrežu je otkrivanje korisničkog imena i lozinke jednog korisnika. To je zastrašujuća pomisao.

Ali zar korisnicima stvarno treba potpuni pristup desktopu? Ili im treba samo pristup aplikacijama na desktopu? Najverovatnije im treba samo pristup aplikacijama i podacima. U tom slučaju, Windows Server 2008 vam obezbeđuje rešenje koje se zove Terminal Services RemoteApp. Terminal Services RemoteApp vam omogućava da obezbedite korisnicima pristup samo ka specifičnim aplikacijama preko RDP kanala. Na taj način, korisnici ne mogu da izazovu probleme na čitavom desktopu, a ako neki haker otkrije podatke datog korisnika, sve što će moći da kontroliše je aplikacija, koja ima mnogo manju površinu koja se može napasti nego celokupan desktop.

TS RemoteApps je veoma fleksibilan. Vi možete da kontrolišete kojim aplikacijama korisnik može da pristupi i kako će im pristupati preko svojih sopstvenih računara. TS Remote Apps zajedno sa TS Gateway-om čine Windows Server 2008 Terminal Server veoma privlačnim za kompanije koje su zainteresovane za bezbedno RDP zasnovano rešenje za udaljeni pristup.

Pored toga, aktiviranje i podešavanje TS RemoteApps-a je veoma lako i trebaće vam samo nekoliko minuta.

Pa šta biste još mogli da poželite pored ovoga?!

Izvorna podrška za IPv6

Windows Server 2008 je prva verzija Windows Server-a koja ima izvornu podršku za IPv6 kao deo IP steka. U prethodnim verzijama Windows-a pre Viste, IPv6 podrška je bila rađena paralelno sa IPv4, i nije postojala integrisana podrška za IPv6 koja bi bila uključena u mrežu infrastukture servisa kao što je DNS i DHCP. To više nije slučaj i sada je IPv6 utkan u mrežni stek Windows Server-a 2008 i servise infrastrukture.

Pošto Windows Server 2008 DNS sada podržava IPv6, vi možete da kreirate Quad A (AAAA) izveštaje a možete da kreirate i IPv6 reverse lookup zone.

DHCP servis je takođe ažuriran tako da podržava IPv6. Vi možete da konfigurišete mrežne interfejse da koriste statične IPv6 adrese, ili mogu da koriste DHCP kako bi pribavile informacije o IP adresama.

Windows Server 2008 RRAS serveri koji se ponašaju kao ruteri mogu da se konfigurišu kao IPv6 ruteri i obezbeđuju informacije u porukama rutiranja u zavisnosti od toga kojeg su prefiksa informacije koje koristi klijent, i da li treba ili ne treba da koriste informacije adresiranja od DHCP servera.

Windows Server 2008 takođe podržava IPv6 tranzicione tehnologije, kao što su ISATAP, 6to4 i Teredo. Bilo koji Windows Server 2008 računar može da se konfiguriše kao ISATAP ruter pomoću Netsh interfejsa komandne linije.

Read Only Domain Controller

Sa razvojem kancelarijskih ogranaka u mnogim organizacijama, mnogi su shvatili da postoji problem vezan za autentifikaciju. Ogranci firmi obično dobijaju kontroler domena preko kojeg se korisnici mogu autentifikovati u lokalnom DC-u umesto da moraju da idu na spori, ili čak srušeni, WAN link, koji može da dovede do grešaka ili blokiranja autentifikacije i nemogućnosti da pristupite čak i lokalnim resursima.

Rešenje je bilo da se postave kontroleri domena u kancelarijskim ograncima. Iako je ovo rešilo inicijalni problem autentifikacije, javili su se bezbednsoni problemi. Pošto većina ogranaka kancelarija nema isti nivo IT stručnosti kao glavna kancelarija, a svakako nemaju isti nivo fizičke bezbednosti, kontroleri domena ogranaka kancelarija postaju veoma slabe tačke u čitavoj Active Directory infrastrukturi. Promene koje napravi nestručan korisnik u ogranku kancelarija može da ima efekte na čitavu organizaciju i ako neko ukrade DC u ogranku kancelarije, to potencijalno može da kompromituje sve naloge u organizaciji.

Rešenje Windows Server-a 2008 je Read Only Domain Controller (RODC). RODC sadrži read only kopiju Active Directory baze podataka i jedine informacije o nalozima koje se skladište u RODC-u su za naloge u ogranku kancelarije. Pošto se nikakve izmene u Active Directory-ju ne mogu napraviti u RODC-u, ne postoji bojazan da će nestručni korisnik napraviti nepopravljivu štetu u Active Directory-u. I pošto obično nema administrativnih korisnika u ograncima kancelarija, postoji relativno mali rizik da će RODC u ograncima kancelarija posedovati naloge administratora koji se mogu kompromitovati u slučaju krađe RODC-a.

RODC-ovi se takođe mogu konfigurisati da keširaju samo određene naloge. I u slučaju da se RODC ukrade, lista keširanih korisničkih naloga na RODC-u je dostupna kroz administraciju Active Directory-ja u glavnoj kancelariji. To omogućuje administratoru Active Directory-ja da isključi ili resetuje prava pristupa ovih naloga iz glavne kancelarije.

Hyper-V

Hyper-V je hipervizor Windows Server-a 2008 koji vam omogućuje da pokrećete virtualne mašine na Windows Server 2008 računarima. Hyper-V zamenjuje Virtual Server 2005 i sada je integralni deo operativnog sistema, koji dobijate kao deo paketa.

Krajnji delovi Hyper-V-a nisu još dostupni, zato ćemo se u ovom trenutku uzdržati od konačnih zaključaka vezanih za Hyper-V. Ali, sudeći po onome što smo do sada videli, mi smo veoma impresionirani onim što su uradili sa virtualizacijom Windows Server-a 2008.

Ako tražite rešenje za virtualizaciju koje vas neće koštati ni dinara, onda treba samo da nadgradite računar na Windows Server 2008 i nećete pogrešiti.

Network Access Protection (NAP)

Network Access Protection vam omogućuje da kontrolišete pristup sa svih računara koji su konektovani u vašu mrežu. Prema Microsoft-u, Network Access Protection (NAP) nije toliko bezbednosna metodologija koliko je mehanizam namenjen očuvanju zdravlja klijenta. NAP vam omogućuje da kreirate polise koje određuju minimalni nivo zdravlja koji klijent mora da ima pre nego što mu se dozvoli da se konektuje na drugi naračunar u mreži.

NAP zavisi od infrastrukture Windows Server-a 2008. Trebaće vam Windows Server 2008 Network Policy Server za skladištenje vaših polisa zdravlja. Postoji nekoliko načina na koje možete da kontrolišete pristup u mreži: IPsec restrikcije, DHCP restrikcije, 801.x restrikcije i VPN restrikcije. Hostovima koji ne ispunjavaju zahteve za bezbednom konfiguracijom se zabranjuje pristup u mreže koje koriste bilo koji od ovih metoda.

Međutim, NAP vam dozvoljava da kreirate mreže u karantinu na koje klijenti koji ne ispunjavaju bezbednosne zahteve mogu da se konektuju kako bi se "izlečili". Čim softver NAP klijenta detektuje da računar ispunjava bezbednosne zahteve, on će poslati informaciju komponenti NAP servera koja će informisati NAP klijenta da sada može da se konektuje na mrežu.

NAP je izuzetno moćan metod za kontrolu pristupa u vašoj mreži, i on je ono što smo čekali od kada je najavljen daleke 2003. godine, i početkom 2004. Iako čekanje od pet godina da se NAP pojavi izgleda dugo, mogu slobodno da kažem da se isplatilo. Administratori velikog broja mreža smatraju da je NAP glavni razlog za nadgranju na Windows Server 2008.

Teško da postoje ikakvi argumenti pomoću kojih bi mogao da opovrgnem mišljenje ovih administratora.

Secure Socket Tunneling Protocol (SSTP) je pravi SSL VPN. Pod terminom “pravi” SSL VPN mislim na to da SSTP obezbeđuje potpuni mrežni VPN pristup ka korporativnim mrežama, na isti način na koji to obezbeđuju PPTP i L2TP/IPSec protokoli. Međutim, prednost SSTP-a je to što za razliku od PPTP i L2TP/IPSec protokola, vi ne morate da brinete o firewall-ovima koji blokiraju spoljšanji pristup ka SSTP konekcijama.

SSTP je u suštini PPP/SSL. Pošto su PPP konekcije ubačene u bezbedno HTTP zaglavlje (SSL), SSTP može da prođe kroz bilo koji firewall ili Web proksi uređaj koji dozvoljava SSL ka spolja.

Više nećete morati da rešavate probleme korisnika u hotelima i konferencijskim salama koji se žale na to da im firewall-ovi na njihovim lokacijama ne dozvoljavaju da VPN-uju u mrežu.

Još jedna lepa stvar u vezi SSTP-a je to što ne morate da dozvolite pristup ka napolje SSTP konekcijama samo zato što ste dozvolili spoljašnje SSL-ove. Postoji vrednost u

CONNECT zaglavlju koje možete da konfigurišete na vašem ISA Firewall-u koje vam omogućava da blokirate SSTP konekcije i dozvolite ostale SSL konekcije.

SSTP će vam znatno olakšati udaljeni pristup ka VPN konekcijama.

Samo ovaj SSTP pristup je dovoljan razlog da nadgradite na Windows Server 2008.

Windows Advanced Firewall

Windows Vista korisnici će u ovom naslovu prepoznati Windows Advanced Firewall. Sada u Windows Server-u 2008 dobijate istu onu funkciju koja već postoji u Visti. Ono što je još bolje je da vi sada možete da koristite grupne polise (Group Policy) u Windows Server 2008 centralizovanom upravljanju sa Windows Advanced Firewall-om. Ako još niste koristili Vistin firewall, bićete prijatno iznenađeni ovom novom funkcijom Windows Servera 2008.

Windows Advanced Firewall koji dolazi sa Vistom i Windows Server-om 2008 vam omogućuje da fino podesite kontrole spoljašnjeg i unutrašnjeg pristupa. Kontrole spoljašnjeg pristupa su bile nedostajući delić u Windows XP firewall-u. Sada vi imate kontrolu nad spoljšanjim konekcijama, tako da ako detektujete u vašem firewall-u da su hostovi inficirani virusima ili crvima koji napadaju određene portove ili kolekcije portova, vi možete iz centra da blokirate svakog hosta zahvaljujući grupnim polisama.

Da bi vam rad sa novom funkcijom bio još lakši, Windows Server 2008 dolazi sa novim Inbound Rule Wizard-om. Ovaj čarobnjak, kojeg možete da koristite preko Group Policy Management konzole, vam omogućuje da veoma lako konfigurišete unutrašnja pravila. Postoji i Outbound Rule Wizard koji vam omogućuje da blokirate spoljašnje konekcije. Vi možete da kontrolišete UDP ili TCP portove, kao i ICMP tipove poruka, ili možete da blokirate aplikaciju po aplikaciju.

Jedna od najimpresivnijih karakteristika Windows Firewall-a je to koliko su pojednostavljene IPsec polise. U prošlosti, podešavanje IPsec polisa se svodilo na pokušaje i pogreške. Vi ste prolazili kroz opcije čarobnjaka i mogli ste samo da se nadate da ste sve dobro podesili.

To više nije slučaj sa Windows Advanced Firewall-om, jer sada imate na raspolaganju New Connection Security Rule Wizard-a, koji omogućava lako kreiranje IPsec polisa za izolovanje domena, polise za izuzetke od autentifikacije, kao i IPsec konekcije i IPsec tunele od servera do servera.

Tako je Windows Advanced Firewall promenio način definisanja IPsec polisa iz posla koji vas užasava u nešto što ćete voleti da radite.

Isprobajte ovu novu funkciju, siguran sam da će vam se svideti.

Secure Socket Tunneling Protocol (SSTP)

Još jedno veliko unapređenje u Windows Server-u 2008 je centralizovano upravljanje QoS polisama kroz grupne polise (Group Policy). Prethodne verzije Windows-a su posedovale QoS funkciju, ali pošto ona nije bila zasnovana na standardima, jako malo ljudi je uopšte koristilo. Windows Server 2008 je ovo promenio tako što je uveo novu QoS funkciju koja je zasnovana na polisama, koju ćete moći odmah da počnete da koristite.

Postoje dva načina na koje možete da implementirate QoS polise – možete da tvrdo kodirate throughput vrednosti ili možete da iskoristite Differentiated Services Code Point (DSCP) vrednosti koje su konfigurisane na vašem mrežnom ruteru. DSCP je standardni industrijski metod za implementiranje QoS-a u korporativnim mrežama. Međutim, čak i ako nemate DSCP osposobljeni ruter, ili čak i ako ne koristite DSCP, vi i dalje možete da podesite polise tako da lokalni hostovi sprovode kontrolu protoka u TCP ili UDP portovima, ili u specifičnim aplikacijama.

Vi možete da izaberete na koje hostove će ova polisa biti primenjena. Na primer, možda nećete želeti da smanjite protok na vašem SMTP serveru, ali ćete možda želeti da ograničite SMTP saobraćaj hostova u vašoj mreži. Na taj način, možete da kontrolišete koliko će spemom inficiran računar moći da pošalje podataka pre nego što ustanovite da se mašina eksploatiše.

Zaključak

Windows Sever 2008 sadrži stotine novih mogućnosti i funkcija, i svaka od njih može da predstavlja vrednu nadgradnju za vašu organizaciju. U ovim člancima mi smo se fokusirali samo na manji deo novih i pobojšanih funkcija za koje mi mislimo da su one zbog kojih najviše vredi da nadgradite na Windows Server 2008.

Za još više informacija o Windows Server-u 2008 i kompletnijem listingu novih i poboljšanih funkcija, idite na Windows Server 2008 Technical Library.