Microsoft

Windows Server® 2008

Dokumentace k systému Windows Server 2008 pro osoby s rozhodovací pravomocí v technické oblasti – zkrácená verze

Obsah

Microsoft

Úvod

Přehled

Systém Microsoft® Windows Server® 2008 byl navržen tak, aby se stal nejproduktivnější platformou pro virtualizaci provozu organizací, podporu aplikací a ochranu sítí. Nabízí zabezpečenou a snadno spravovatelnou platformu pro vývoj a spolehlivé hostování webových aplikací a služeb. Bez ohledu na to, zda je systém Windows Server 2008 provozován v pracovní skupině či datovém centru, poskytuje atraktivní nové funkce a zásadní vylepšení základního operačního systému.

Více kontroly

Díky systému Windows Server 2008 budou mít IT specialisté serverovou a síťovou infrastrukturu pod lepší kontrolou, takže se mohou soustředit na klíčové potřeby firmy. IT specialisté mohou využít zlepšeného skriptování a možností pro automatizaci úkolů, např. Windows PowerShell, k automatizaci běžných úkolů v IT provozu. Nástroj Server Manager umožňuje instalaci a správu založenou na rolích a usnadňuje tím správu a zabezpečení různých serverových rolí v rámci rozsáhlé sítě. Nová konzola Správce serveru představuje jednotné umístění pro správu konfigurace serveru a informací o systému. Pracovníci IT oddělení mohou nainstalovat pouze role a funkce, které jsou právě potřebné. Navíc lze mnoho časově náročných úkolů při nasazení systémů automatizovat pomocí průvodců. Zlepšené nástroje pro správu systému, např. sledování výkonu a spolehlivosti, zprostředkují informace o systémech a upozorní pracovníky IT oddělení na potenciální problémy, dříve než se projeví.

Lepší ochrana

Systém Windows Server 2008 obsahuje řadu nových a zdokonalených technologií zabezpečení, které zlepšují ochranu operačního systému a poskytují pevný základ pro provoz a další rozvoj podniku. Mezi novinky v oblasti zabezpečení patří například technologie PatchGuard, která omezuje možnosti útoku na jádro systému a zvyšuje tak bezpečnost i stabilitu serverového prostředí. Technologie Windows Service Hardening zlepšuje bezpečnost systémů tím, že brání napadení nejdůležitějších serverových služeb prostřednictvím abnormálních akcí v systému souborů, v registru a v síti. Následující technologie přispívají k lepšímu zabezpečení operačního systému Windows Server 2008: Network Access Protection (NAP), řadič domény jen pro čtení (Read-Only Domain Controller – RODC), vylepšení infrastruktury PKI (Public Key Infrastructure), Windows Service Hardening, nová obousměrná brána Windows Firewall a podpora nejnovějších kryptografických standardů.

Větší flexibilita

Systém Windows Server 2008 je navržen tak, aby správce mohl upravit infrastrukturu podle měnících se potřeb firmy a aby byl systém zároveň stále dostatečně flexibilní. Mobilní uživatelé mohou využít větší flexibility díky technologiím, které jim umožní pracovat s programy z libovolného vzdáleného umístění, například Vzdálená aplikace RemoteApp a Brána Terminálové služby. Služba nasazení systému Windows (Windows Deployment Services – WDS) v systému Windows Server 2008 urychluje nasazení a údržbu IT systémů a technologie Virtualizace systému Windows Server (WSv) pomáhá při konsolidaci serverů. Organizacím, které potřebují umístit do jednotlivých poboček řadiče domény, nabízí systém Windows Server 2008 novou možnost konfigurace: řadič domény jen pro čtení (RODC), který v případě napadení řadiče domény chrání uživatelské účty před zneužitím.

Virtualizace

Úvod

Řada produktů Windows Server 2008 bude obsahovat výkonnou virtualizační technologii Virtualizace systému Windows Server (Windows Server virtualization – WSv), která poskytuje účinné funkce pro správu a zabezpečení. WSv umožní podnikům uplatnit stávající znalosti správy serverů na platformě Windows při využívání výhod, které virtualizace nabízí v oblastech flexibility a bezpečnosti. Přitom nebude třeba pořizovat další software od jiného výrobce. Společnost Microsoft a její partneři poskytují komplexní podporu pro hostování operačních systémů Windows a podporovaných verzí systému Linux. Technologie WSv představuje vysoce flexibilní, výkonnou a nákladově efektivní virtualizační platformu s výbornou podporou.

Zabezpečení

Zabezpečení je jedním z nejdůležitějších aspektů každé serverové implementace. Server, který je hostitelem několika virtuálních počítačů (Virtual Machines – VM), zvaný též konsolidovaný server, je vystaven stejným bezpečnostním rizikům jako nekonsolidované servery, ale navíc je třeba vzít v úvahu rozdělení správcovských rolí. Technologie WSv pomáhá zvýšit zabezpečení konsolidovaných serverů a vyřešit rozdělení správcovských rolí. K těmto účelům dává technologie WSv k dispozici tyto funkce:

- Přísné oddělení: Virtuální počítač (VM) pracuje jako nezávislý objekt obsahující operační systém, který je zcela izolován od ostatních virtuálních počítačů běžících na tomtéž fyzickém serveru.
- Zabezpečení na úrovni hardwaru: V novějším serverovém hardwaru jsou k dispozici funkce jako prevence spouštění dat (Data Execution Prevention – DEP), které pomáhají zabránit spuštění mnoha běžných virů a červů.
- Virtualizace systému Windows Server: Technologie WSv chrání před riziky

virtuální počítače, v nichž jsou uloženy citlivé informace, i hostitelský systém před napadením ze strany hostovaného operačního systému.
- Funkce zabezpečení sítě: Doporučujeme povolit automatický překlad síťových adres (NAT), bránu firewall a funkci NAP (Network Access Protection).
- Minimální základ pro zabezpečený počítač: Omezuje riziko napadení a usnadňuje optimalizaci virtualizační architektury s minimálním zatížením systému. Tato funkce podstatně zlepšuje spolehlivost virtuálních počítačů na platformě WSv.

Konfigurace konsolidovaného serveru, který poskytuje nejlepší zabezpečení a prostředí operačního systému pro každou aplikaci, může být v některých případech dosti náročná. Díky technologii WSv lze nakonfigurovat každou úlohu v ideálním prostředí operačního systému i profilu zabezpečení. Tím řeší technologie WSv problémy s rozdělením rolí správců. WSv chrání virtuální počítače i hostitelský operační systém před vzájemným napadením, protože jednotlivé virtuální počítače fungují pod účtem služby pouze s nezbytně nutnými oprávněními. Technologie WSv chrání hostitelský operační systém a omezuje potenciální škodu, kterou může způsobit napadený virtuální počítač ostatním virtuálním počítačům.

Systémová izolace Výkon

Pokroky v návrhu a integraci hardwaru podporujícího virtualizaci umožňují, aby technologie WSv virtualizovala mnohem náročnější aplikace než předchozí verze při zachování flexibilnějšího přidělování prostředků.

Výkon byl zlepšen v následujících oblastech:
- Virtualizační architektura s nízkým zatížením systému je založena na 64bitovém hypervizoru. Hardware s podporou virtualizace (technologie Intel VT a AMD „Pacifica“) umožňují vyšší výkon hostovaných operačních systémů.
- Podpora vícejádrových procesorů. Každému virtuálnímu počítači lze přidělit až osm logických procesorů. Díky tomu lze virtualizovat velké úlohy s vysokými výpočetními nároky, které mohou využít paralelního zpracování ve víceprocesorovém jádru virtuálního počítače.
- Podpora 64bitových hostitelských i hostovaných operačních systémů. Technologie WSv pracuje v 64bitové verzi systému Windows Server 2008, která může hostovaným virtuálním počítačům zpřístupnit velkou paměťovou kapacitu. Úlohy, které kladou vysoké nároky na paměť a v 32bitovém operačním systému by je zpomalovalo časté odkládání do stránkovacího souboru, lze s úspěchem virtualizovat pomocí technologie WSv. WSv podporuje také souběžné hostování 64bitových a 32bitových operačních systémů na tomtéž konsolidovaném serveru.
- Podpora role Server Core. Technologie WSv může být provozována i v případě, že je hostitelským operačním systémem instalace Server Core systému Windows Server 2008. Minimální velikost instalace a zatížení systému, které instalace Server Core vykazuje, umožňuje věnovat maximum výpočetní kapacity hostitelského serveru spuštěným virtuálním počítačům.
- Transparentní přístup k diskům. Hostitelským operačním systémům je možné přímo zpřístupnit místní úložiště nebo úložiště v síti iSCSI SAN (Storage Area Network). Tím se zvýší výkon aplikací náročných na vstupně-výstupní operace, například SQL Server™ nebo Microsoft Exchange.

Mnoho serverových úloh klade velké nároky na výpočetní kapacitu serveru a jeho vstupně-výstupní subsystémy. Aplikace, jako jsou SQL Server a Microsoft Exchange, jsou známé svými vysokými nároky na paměť a propustnost disků, a dosud tedy existovaly pochybnosti, zda lze takovéto úlohy virtualizovat. Díky 64bitovému hypervizoru technologie WSv s funkcemi jako Transparentní přístup k diskům je nyní virtualizace takových náročných úloh nejen možná, ale často i velmi vhodná.

Zjednodušená správa

V instalacích v datových centrech a vzdálených pobočkách, kde je nasazena technologie WSv, jsou vyžadovány výkonné možnosti správy a automatizace. Jen díky nim je možné proměnit potenciál virtualizace na skutečnou úsporu nákladů. Technologie WSv je připravena tuto problematiku řešit a nabízí následující funkce pro správu a automatizaci:
- Rozšiřitelná správa: Technologie WSv je navržena pro spolupráci s produkty Microsoft System Center Operations Manager (SCOM) a System Center Virtual Machine Manager (SCVMM). Tyto produkty pro správu poskytují nástroje pro generování sestav, automatizaci, nasazení a uživatelskou svépomoc na platformě WSv.
- Rozhraní konzoly MMC 3.0 pro správu virtuálních počítačů: Ke správě konfigurace WSv a nastavení virtuálních počítačů slouží známé rozhraní konzoly Microsoft Management Console (MMC), takže osvojení práce s technologií WSv je mnohem snadnější.
- Rozhraní WMI (Windows Management Instrumentation): Technologie WSv obsahuje zprostředkovatele WMI, který zpřístupňuje informace o systému a skriptování úkolů správce.
- Skriptování PowerShell: Ke konfiguraci hostitele WSv i virtuálních počítačů lze použít nástroj Windows PowerShell.
- Správa objektů zásad skupiny: Technologie WSv může ke správě hostitele virtualizace WSv i ke konfiguraci virtuálních počítačů využívat konfiguračních a správních možností objektů zásad skupiny.

Funkce produktů SCOM a SCVMM umožňují efektivní správu instalací WSv v datacentrech i ve vysoce distribuovaných nasazeních. Následujícím způsobem lze například použít skriptovaný přístup ke zprostředkovateli WMI pro automatizaci intervalů údržby na několika hostitelských počítačích s technologií WSv: Hostované virtuální počítače budou vypnuty a poté spuštěny na záložním serveru. Mezitím je možné provést údržbu hostitelského serveru a následně obnovit virtuální počítače v původním hostitelském systému. Přidání produktu System Center Virtual Machine Manager navíc umožní automatizaci této operace, takže u mnoha aplikací nedojde k žádnému zřetelnému výpadku.

Shrnutí

Technologie Virtualizace systému Windows Server kombinuje funkce, které řešení mnoho komplikovaných problémů souvisejících s virtualizací, mezi jinými: zabezpečení konsolidovaných serverů, řešení dynamického zatížení, dosažení vysokého výkonu a škálovatelnosti virtualizovaných úloh a zjednodušení správy. Kombinace funkcí pro zabezpečení a systémová izolace virtuálních počítačů umožňuje na hostitelských serverech s technologií WSv konsolidovat heterogenní úlohy při zachování flexibility i bezpečnosti. Architektura 64bitového hypervizoru, která je základem technologie WSv, poskytuje vysoký výkon i pro velmi náročné úlohy. V neposlední řadě jsou v produktech Windows Server 2008, System Center Operations Manager a System Center Virtual Machine Manager k dispozici efektivní integrované funkce pro správu, které poskytují správcům automatizovanou a účinnou kontrolu nad širokou škálou virtualizovaných prostředí.

Webová a aplikační platforma

Úvod

Systém Windows Server 2008 nabízí zabezpečenou platformu se snadnou správou pro vývoj a spolehlivé hostování aplikací a služeb, které mají fungovat na serveru nebo přes web. Mezi nové funkce patří: zjednodušená správa, vyšší zabezpečení a zlepšení v oblastech výkonu i rozšiřitelnosti. Navíc budou mít podniky k dispozici efektivnější správu aplikací a služeb, rychlejší nasazení a konfiguraci webových aplikací a služeb a bezpečnější, optimalizovanou a přizpůsobitelnou webovou platformu. Systém Windows Server 2008 poskytuje webovým aplikacím a službám vyšší výkon i škálovatelnost a správcům lepší kontrolu a přehled nad využíváním klíčových prostředků operačního systému jednotlivými aplikacemi a službami.

Internetová informační služba 7.0 (IIS7)

Systém Windows Server 2008 nabízí jednotnou platformu pro publikování na webu, která integruje Internetovou informační službu 7.0 (IIS7) a služby ASP.NET, Windows Communication Foundation a Windows SharePoint® Services. Služba IIS7 představuje významné vylepšení existujícího webového serveru IIS a hraje centrální úlohu při integraci technologií pro webovou platformu. K nejdůležitějším výhodám služby IIS7 patří efektivnější funkce pro správu, vyšší zabezpečení a nižší náklady na podporu. Tyto funkce pomáhají vytvořit jednotnou platformu, která nabízí jednotný konzistentní model pro vývoj a správu webových řešení.

Vylepšené nástroje pro správu

Nový nástroj pro správu Správce služby IIS, který je součástí služby IIS7, nabízí efektivnější způsob správy webového serveru. Podporuje nastavení konfigurace služeb IIS a ASP.NET, data o uživatelích a získávání diagnostických informací za běhu. Nové uživatelské rozhraní také umožňuje hostitelům a správcům webů delegovat kontrolu nad správou vývojářům nebo vlastníkům obsahu, což umožňuje snížit náklady na vlastnictví a zátěž z hlediska správy pro správce. Nové rozhraní Správce služby IIS podporuje vzdálenou správu přes protokol HTTP a umožňuje integrovanou místní, vzdálenou i internetovou správu bez nutnosti otevírat na bráně firewall porty pro správu nebo službu DCOM.
Součástí instalace je i program appcmd.exe, nový nástroj pro správu webových serverů, webů a webových aplikací v příkazovém řádku. Rozhraní příkazového řádku zjednodušuje časté úkoly při správě webových serverů. Program appcmd.exe může například vytvořit výpis požadavků na webový server, které musely čekat déle než 500 milisekund. Tyto informace pak slouží k odstraňování potíží s aplikacemi, jejichž výkon se snížil. Výstup z programu appcmd.exe lze propojit s jinými příkazy, které jej mohou dále zpracovat.

Modulární instalace podle funkcí

IIS7 se skládá z více než 40 samostatných funkčních modulů. Pouze polovina z nich je zahrnuta ve výchozí instalaci, a správce se proto může rozhodnout nainstalovat nebo odebrat libovolné funkční moduly. Tento modulární přístup umožňuje správcům nainstalovat pouze nezbytné moduly a šetří čas tím, že snižuje počet funkcí, které je nutné spravovat a aktualizovat. Navíc je zlepšeno zabezpečení a omezeno riziko napadení webového serveru, neboť není činný žádný nadbytečný software.

Model distribuované konfigurace

IIS7 přináší podstatná zlepšení ve způsobu uložení konfiguračních dat a přístupu k nim. K hlavním cílům uvedení služby IIS7 patřilo umožnit distribuovanou konfiguraci nastavení služby IIS, která dá správcům možnost zadávat nastavení konfigurace IIS do souborů uložených současně s kódem a obsahem.
Distribuovaná konfigurace umožní správcům uložit nastavení konfigurace webu nebo aplikace do stejného adresáře, ve kterém je uložen kód nebo obsah. Nastavení konfigurace je v modelu distribuované konfigurace zadáno v jediném souboru, takže je možné delegovat správu určitých funkcí webu nebo webových aplikací na ostatní uživatele. Je například možné delegovat web tak, aby jeho výchozí dokument mohl být nakonfigurován vývojářem aplikace. Správce má také možnost uzamknout některá nastavení konfigurace, aby je žádný jiný uživatel nemohl změnit. Tuto funkci lze využít k tomu, aby vývojář obsahu, kterému byl delegován přístup k danému webu pro správu, nemohl přepsat zásady zabezpečení, které zakazují spouštění skriptů. Při použití distribuované konfigurace je možné nastavení konfigurace určitého webu či aplikace kopírovat mezi počítači, když aplikace přejde z fáze vývoje do testování a následně do provozního nasazení.

Diagnostika a řešení potíží

Integrovaná podpora diagnostiky a trasování ve službě IIS7 usnadňuje řešení potíží s webovým serverem. Správce získá podrobné diagnostické informace o stavu webového serveru v reálném čase. Funkce pro diagnostiku a řešení potíží zpřístupní vývojářům a správcům požadavky, které server momentálně zpracovává. Součástí služby IIS7 jsou také nové objekty pro sledování a řízení stavu za běhu, které v reálném čase poskytují informace o fondech aplikací, pracovních procesech, webech, aplikačních doménách i zpracovávaných požadavcích. Z těchto informací lze například zjistit, který požadavek v pracovním procesu spotřebovává 100 % výkonu procesoru. Součástí služby IIS7 jsou dále podrobné trasovací události rozmístěné v průběhu celého postupu zpracování požadavku a odpovědi, pomocí kterých mohou vývojáři a správci trasovat požadavek putující zpracujícím kanálem IIS do libovolného existující kódu na úrovni stránky a pak zpět do odpovědi. Díky těmto podrobným trasovacím událostem může vývojář zjistit postup požadavku i případné informace o chybách, ke kterým při jeho zpracování došlo, ale také dobu zpracování a další informace užitečné při ladění všech druhů chyb.
IIS7 také zjednodušuje odstraňování potíží díky chybovým zprávám, které obsahují mnohem více podrobností a doporučení k nápravě. Nový modul vlastních chyb umožňuje předávání podrobných informací o chybě zpět do prohlížeče (ve výchozím nastavení do místního hostitele) a konfigurovatelných informací do ostatních vzdálených klientů. Namísto strohého chybového kódu uvidí nyní správce podrobnosti o požadavku, potenciální problémy, které mohly chybu způsobit, i doporučení k nápravě.
K nejdůležitějším funkcím zlepšujícím podporu řešení potíží ve službě IIS7 patří rozhraní API pro sledování a řízení stavu za běhu (Runtime Status and Control API – RSCA), které za běhu zprostředkovává interní podrobnosti o stavu serveru. RCSA poskytuje přehled a správu různých entit, například webů, fondů aplikací a dokonce aplikačních domén technologie.NET. RCSA také v reálném čase zpřístupňuje požadavky, které jsou právě zpracovávány serverem. Data z rozhraní RCSA jsou k dispozici ve zprostředkovateli WMI a ve spravovaném rozhraní API (Microsoft.Web.Administration). Správci mají k těmto datům přístup také v grafickém uživatelském rozhraní služby IIS7 pro správu a v nástroji pro příkazový řádek.

Rozšiřitelná modulární architektura

V předchozích verzích služby IIS byly všechny funkce standardně integrovány a nebylo možné snadno rozšířit ani nahradit žádné z těchto funkcí. Jak bylo již uvedeno, jádro služby IIS7 je rozděleno do více než 40 samostatných funkčních modulů. Jádro obsahuje také nové rozhraní Win32® API pro vývoj modulů pro jádro serveru. Moduly pro jádro serveru představují novou a výkonnější náhradu filtrů a rozšíření ISAPI (Internet Server Application Programming Interface). IIS7 však nadále podporuje filtry a rozšíření ISAPI. Všechny funkce služby IIS pro jádro serveru byly vyvinuty pomocí nového rozhraní Win32 Module API služby IIS7 jako samostatné funkční moduly, a proto mohou uživatelé přidávat, odebírat a dokonce nahradit jednotlivé funkční moduly služby IIS.

Přizpůsobitelnost díky flexibilnímu modelu rozšiřitelnosti

Služba IIS7 umožňuje vývojářům rozšířit službu IIS tak, aby poskytovala funkce podle vlastní potřeby novým a výkonnějším způsobem. To je zčásti umožněno novým rozhraním API pro jádro serveru, které podporuje vývoj funkčních modulů v nativním (C/C++) i spravovaném kódu (jazyky jako C# nebo Visual Basic® 2005, které využívají rozhraní.NET Framework). Většina funkcí služby IIS7 pro zpracování požadavků a aplikací byla ve skutečnosti implementována právě pomocí těchto rozhraní API. Služba IIS7 dále podporuje rozšiřitelnost funkčních sad pro konfiguraci, skriptování, protokolování událostí i nástrojů pro správu a představuje tedy komplexní serverovou platformu, na které mohou vývojáři budovat rozšíření webových serverů.

Skutečné nasazení aplikací pomocí pouhého příkazu xcopy

IIS7 umožňuje uložení nastavení konfigurace služby IIS do souboru web.config, což podstatně usnadňuje kopírování aplikací na různé webové servery pouhým příkazem xcopy. Není zapotřebí nákladné replikace náchylné k chybám, ruční synchronizace ani následné pracné konfigurace.

Shrnutí

Strukturální změny služby IIS7 vedly k vytvoření velmi flexibilního systému pro webové aplikace. Přístup ke konfiguraci IIS prostřednictvím grafického uživatelského rozhraní i nástroje appcmd.exe pro příkazový řádek poskytuje efektivní nástroje začínajícím webovým správcům se základními znalostmi i pokročilým správcům, kteří spravují několik serverů najednou pomocí skriptovaných nástrojů. Součásti služby IIS pro trasování a řešení potíží poskytují podrobné a užitečné informace, které pomáhají správcům a vývojářům aplikací vypátrat nefunkční stránky a kód. Modulární funkce a podrobný model pro správu služby IIS7 usnadňují správci serveru vytvoření právě takového serveru, který odpovídá jeho požadavkům, a udělení minimálních nutných přístupových oprávnění správcům jednotlivých webů a obsahu.

Správa serveru

Úvod

Hlavním tématem mnoha vylepšení zahrnutých do systému Windows Server 2008 je zjednodušení běžných složitých úkolů správce serveru, počínaje optimalizací konfigurace nových serverů a konče automatizací opakovaných úkonů. Nástroje pro centralizovanou správu, intuitivní

rozhraní a funkce pro automatizaci usnadňují IT specialistům správu síťových serverů, služeb a tiskáren umístěných v ústřední síti i ve vzdálených umístěních, například na pobočkách.

Úlohy počáteční konfigurace

Optimalizovaný proces instalace systému Windows Server 2008 není přerušován konfiguračními úkony, které vyžadují zásah uživatele. Tyto úkoly a dialogová okna se zobrazí až po dokončení primární instalace, takže správce nemusí v průběhu instalace u serveru setrvávat a zadávat různé informace.
Okno Úlohy počáteční konfigurace je novou funkcí systému Windows Server 2008, která správci pomůže nastavit a zprovoznit nový server. Zahrnuje mimo jiné nastavení hesla správce, změnu názvu účtu Administrator, která přispívá k většímu zabezpečení serveru, připojení serveru do stávající domény a aktivaci brány Windows Firewall a služby Windows Update.

Konzola Správce serveru

Nová konzola Správce serveru slouží v systému Windows Server 2008 k usnadnění správy a zabezpečení různých serverových rolí v organizaci. Konzola Správce serveru představuje jednotné umístění pro správu konfigurace serveru a informací o systému, zobrazení stavu serveru, hledání problémů v konfiguraci rolí serveru a správu všech rolí, které jsou na serveru nainstalovány.
Podokno hierarchie ve Správci serveru obsahuje rozbalitelné uzly, pomocí nichž lze přímo přejít na konzoly pro správu jednotlivých rolí, nástroje pro řešení potíží nebo vyhledání možností pro zálohování a zotavení po havárii.
Správce serveru konsoliduje různá rozhraní a nástroje pro správu do jednotné správcovské konzoly, ve které mohou správci provádět běžné úkoly správy bez nutnosti přecházet do jiných rozhraní, nástrojů a dialogových oken.

Průvodci Správce serveru

Průvodci ve Správci serveru zjednodušují úkoly při nasazení serverů do rozlehlé sítě a zkracují tak dobu potřebnou k nasazení oproti předchozím verzím systému Windows Server. Mnoho běžných úkolů konfigurace, například konfigurování nebo odebrání role, nastavení několika rolí najednou a služeb rolí, lze nyní provést pomocí průvodců Správce serveru v průběhu jediné relace.
Systém Windows Server 2008 provede v každém okně průvodců Správce serveru kontrolu závislostí, takže všechny služby potřebné pro danou roli budou nainstalovány a nebudou odebrány žádné služby, které může vyžadovat některá z rolí či služeb rolí, která zůstává na serveru aktivní.

Prostředí Windows PowerShell

Prostředí příkazového řádku Microsoft Windows PowerShell a příslušný skriptovací jazyk pomáhají IT specialistům v automatizaci běžných úkolů. Nový skriptovací jazyk zaměřený na správu, přes 120 standardních nástrojů pro příkazový řádek s konzistentní syntaxí a další nástroje – díky těmto možnostem prostředí Windows PowerShell je správa systému snazší a automatizace rychlejší. Windows PowerShell se správce snadno naučí a začne používat, protože je kompatibilní se stávající infrastrukturou IT a stávajícími skriptovacími prostředky. Umožňuje uživatelům automatizovat správu systému, ať se jedná o základní úkoly správy serverů, nebo o konkrétní serverové role, například terminálový server.
Windows PowerShell integruje prostředí příkazového řádku a skriptovací jazyk, takže správce může efektivněji provádět a automatizovat opakované úkoly správy systému. Windows PowerShell představuje vylepšení příkazového řádku systému Windows a nástroje Windows Script Host (WSH). Obsahuje nástroje pro příkazový řádek označované jako cmdlet, které mají přesně stejnou syntax jako skriptovací jazyk. Příkaz, který uživatel zadá do příkazového řádku Windows PowerShell, se shoduje s příkazem, který by byl použit k automatizaci téhož úkolu na několika různých serverech.
PowerShell podporuje stávající skripty, které jsou v organizaci již k dispozici (například v souborech VBS, BAT nebo PERL), takže není nutné před nasazením prostředí Windows PowerShell provést migraci skriptů. Stávající nástroje pro příkazový řádek systému Windows lze spustit i v příkazovém řádku prostředí Windows PowerShell. Díky konzistentní syntaxi a konvencím vytváření názvů a také integraci skriptovacího jazyka do interaktivního prostředí přispívá Windows PowerShell ke zjednodušení a zrychlení automatizace úkolů správy systému.

Windows Remote Management (WS-Management)

Rostoucí počet vzdálených serverů v pobočkách a na dalších místech vyžaduje lepší a efektivnější možnosti správy externích serverů. Technologie Windows Remote Management představuje způsob snadné správy vzdálených serverů, který je skriptovatelný a nenáročný na šířku přenosového pásma.
Nástroj Windows Remote Manager představuje implementaci protokolu WS-Management, standardního protokolu založeného na standardu SOAP, který umožňuje spolupráci hardwaru a operačních systémů. Správci mohou využívat skriptovaných objektů technologie Windows Remote Management, nástroje Windows Remote Management pro příkazový řádek nebo nástroje Windows Remote Shell pro příkazový řádek. Touto cestou lze získat data potřebná pro správu (například informace o objektech, jako jsou disky, síťové adaptéry, služby nebo procesy) z místních i vzdálených počítačů. Jestliže je v počítači provozován operační systém Windows, který podporuje technologii Windows Remote Management, budou data pro správu zprostředkována rozhraním WMI (Windows Management Instrumentation).

Server Core

Počínaje verzí Windows Server 2008 se mohou správci rozhodnout pro minimální instalaci systému Windows Server, která

obsahuje jen určité funkce, a nikoli nepotřebné součásti. V prostředí instalace Server Core lze provozovat jednu nebo více z následujících rolí serveru:

- Virtualizace systému Windows Server
- Server DHCP (Dynamic Host Configuration Protocol)
- Server DNS (Domain Name System)
- Souborový server
- Služba AD DS (Active Directory® Directory Services)
- Služba AD LDS (Active Directory® Lightweight Directory Services)
- Služba Windows Media Services
- Správa tisku

Instalace Server Core nabízí organizacím tyto hlavní výhody:

- Menší nároky na údržbu softwaru: V instalaci Server Core jsou zahrnuty pouze ty součásti, které jsou nezbytné pro provoz a správu serveru a provoz podporovaných rolí serveru, a proto server klade nižší nároky na údržbu softwaru. Menší instalace Server Core snižuje počet nutných aktualizací a oprav, takže se šetří šířka pásma spotřebovávaná servery i čas, který IT specialisté potřebují na správu.
- Menší riziko napadení: Počet souborů, které jsou na serveru nainstalovány a spuštěny, je nižší, a proto je v síti vystaven menší počet zranitelných bodů, a riziko napadení se tedy snižuje. Správce může nainstalovat pouze konkrétní služby vyžadované daným typem serveru a naprosto tak minimalizovat riziko útoku.
- Méně časté restartování a menší nároky na místo na disku: V minimální instalaci Server Core je počet nainstalovaných součástí, které je nutno aktualizovat nebo opravovat, nižší, a proto není nutné tak často restartovat systém. Instalace Server Core obsahuje jen minimální počet souborů nezbytně nutných k zajišťování požadovaných funkcí, takže potřebná kapacita disku na serveru se sníží. Volbou instalační možnosti Server Core může správce snížit nároky na správu a aktualizace softwaru a zároveň i omezit bezpečnostní rizika.
- Instalační možnost Server Core v systému Windows Server 2008 slouží ke snížení nároků na průběžnou údržbu serveru a zjednodušení jeho správy. Díky tomu, že minimální instalace Server Core obsahuje pouze požadované funkce, se mohou pracovníci IT oddělení omezit pouze na instalaci oprav a aktualizací, které přímo souvisejí s nainstalovanými soubory.

Správa tisku v systému Windows Server 2008

Čím větší je organizace, tím více tiskáren je připojených k síti a tím více času potřebují IT specialisté k instalaci a údržbě. Tyto faktory následně přispívají ke zvyšování provozních nákladů. Součástí systému Windows Server 2008 je Správa tisku, modul snap-in pro konzolu MMC, který poskytuje správcům jednotné rozhraní pro správu, sledování a údržbu všech tiskáren v organizaci, včetně vzdálených poboček.
Správa tisku zprostředkovává v jediné konzole aktuální informace o stavu všech tiskáren a tiskových serverů v síti. Správa tisku může vyhledat tiskárny, na kterých došlo k chybě, a může také odesílat e-mailem upozornění nebo spouštět příslušné skripty v případě, že tiskárna nebo tiskový server vyžaduje údržbu. Jestliže daný model tiskárny poskytuje webové rozhraní, může Správa tisku taková data využít. To usnadňuje správu informací o zásobách papíru a toneru i v případě, že jsou tiskárny umístěny ve vzdálených pobočkách. Dále může Správa tisku automaticky hledat a instalovat síťové tiskárny do místní podsítě místních tiskových serverů. Správa tisku šetří správci tisku značné množství času souvisejícího s instalací tiskáren do klientských počítačů a se správou a sledováním tiskáren. Není nutné v jednotlivých počítačích instalovat a konfigurovat připojení k tiskárnám. Namísto toho lze pomocí Správy tisku a zásad skupiny automaticky přidávat připojení k tiskárnám do složky Tiskárny a faxy v klientských počítačích. Jedná se o efektivní a úsporný způsob zpřístupnění tiskáren velkému počtu uživatelů, kteří požadují přístup k téže tiskárně, např. všichni uživatelé ve stejném oddělení nebo na stejné pobočce.

Možnosti automatizace a centralizované řídicí rozhraní, které nabízí Správa tisku a které umožňuje instalaci, sdílení a správu tiskáren, usnadňuje správu a šetří čas, který IT specialisté potřebují k nasazení tiskáren.

Zabezpečení a vynucování zásad

Úvod

Windows Server 2008 obsahuje mnoho funkcí, které zlepšují zabezpečení a soulad se zákonnými požadavky. Mezi tato vylepšení patří:

- Vynucení stavu klientských počítačů: Technologie NAP (Network Access Protection) umožňuje správcům nakonfigurovat a vynucovat požadavky na stav a zabezpečení klientů, dříve než klient získá přístup k síti.
- Sledování certifikačních autorit: Podniková infrastruktura PKI zlepšuje možnosti sledování různých certifikačních autorit (CA) a případné řešení potíží.
- Zlepšení brány firewall: Nová brána Windows Firewall s pokročilým zabezpečením zahrnuje celou řadu vylepšení v oblasti zabezpečení.
- Šifrování a ochrana dat: Technologie BitLocker chrání citlivá data zašifrováním obsahu disku.
- Kryptografické nástroje: Šifrování nové generace poskytuje flexibilní platformu pro vývoj kryptografických nástrojů.
- Oddělení serverů a domén: Serverové a doménové prostředky lze izolovat a poskytnout k nim přístup pouze ověřeným a oprávněným uživatelům.
- Řadič domény jen pro čtení (Read-Only Domain Controller – RODC): RODC představuje nový typ možnosti při instalaci řadiče domény. Je vhodný k instalaci do vzdálených poboček, které disponují nižší úrovní fyzického zabezpečení.

Tato vylepšení pomáhají správcům zvýšit úroveň zabezpečení organizace a zjednodušit správu i nasazení konfigurací a nastavení, které se zabezpečením souvisejí.

Architektura NAP (Network Access Protection)

Technologie NAP (Network Access Protection) brání nezabezpečeným počítačům v přístupu k síti organizace a případnému zavlečení nákazy. NAP slouží k nakonfigurování a následnému vynucování požadavků na stav klientských počítačů. Klientské počítače, které požadavkům nevyhovují, musí být před připojením k podnikové síti aktualizovány nebo jinak opraveny. NAP dává správcům možnost nakonfigurovat zásady stavu, které definují položky jako požadavky na software, požadavky na aktualizace zabezpečení a požadované nastavení konfigurace, které platí pro počítače připojující se k síti organizace.
Při vynucování požadavků na stav vyhodnotí služba NAP stav klientského počítače a omezí přístup k síti v případě, že klientský počítač požadavkům nevyhovuje. Na nápravě situace u nevyhovujících počítačů se podílí součásti na straně serveru i klienta. Jakmile je počítač opraven, může získat neomezený přístup k síti. Jestliže služba zjistí, že klientský počítač nevyhovuje požadavkům, může mu odepřít přístup k síti nebo okamžitě provést aktualizace potřebné k tomu, aby počítač požadavkům vyhovoval. Metody vynucení, které architektura NAP využívá, podporují čtyři technologie přístupu k síti, které při vynucování požadavků na stav spolupracují se službou NAP: vynucení pomocí protokolu IPsec (Internet Protocol security), vynucení pomocí protokolu 802.1X, vynucení pomocí virtuální privátní sítě (VPN) pro službu Směrování a vzdálený přístup a vynucení pomocí protokolu DHCP (Dynamic Host Configuration Protocol).

Funkce brány Windows Firewall s pokročilým zabezpečením

Brána Windows Firewall s pokročilým zabezpečením v systému Windows Server 2008 je stavová hostitelská brána firewall, která povolí nebo blokuje síťové přenosy v souladu s nastavenou konfigurací a podle požadavků spuštěných aplikací. Tak chrání síť před napadením útočníky nebo škodlivými programy.
Mezi nové funkce patří schopnost brány firewall blokovat příchozí i odchozí přenosy. Správce sítě může novou bránu Windows Firewall nastavit například tak, že jsou blokovány veškeré přenosy odeslané na určité porty, například porty využívané známými viry, nebo na určité adresy, které obsahují citlivý nebo nevhodný obsah. Tím je počítač chráněn před viry, které by se mohly v síti šířit, a síť je chráněna před viry, které by se mohly pokusit o rozšíření z napadeného systému.
Možnosti konfigurace brány Windows Firewall se zvětšily, a proto byl pro zjednodušení správy vytvořen modul snap-in pro konzolu MMC nazvaný Brána Windows Firewall s pokročilým zabezpečením. Tento nový modul snap-in slouží správcům sítě ke vzdálené konfiguraci nastavení brány Windows Firewall v klientských pracovních stanicích a na serverech, což zjednodušuje vzdálenou konfiguraci a správu. Tato funkce nebyla v předchozích verzích brány firewall k dispozici a bylo nutné použít připojení ke vzdálené ploše.
V předchozích verzích systému Windows Server bylo nutné konfigurovat bránu Windows Firewall a zabezpečení IPsec odděleně. V systému Windows lze k blokování a povolení příchozího síťového přenosu použít jak hostitelskou bránu firewall, tak protokol IPsec, a bylo tedy možné vytvořit duplicitní i protichůdné výjimky brány firewall a pravidla IPsec. Nová brána Windows Firewall v systému Windows Server 2008 kombinuje konfiguraci obou síťových služeb do stejného grafického uživatelského rozhraní a stejných příkazů pro příkazový řádek. Integrace brány firewall a nastavení protokolu IPsec zjednodušuje konfiguraci a pomáhá předcházet vzniku duplicitních a protichůdných nastavení.

BitLocker Drive Encryption

BitLocker Drive Encryption je důležitá nová funkce zabezpečení v systému Windows Server 2008, která pomáhá chránit servery, pracovní stanice i mobilní počítače. Je k dispozici také v systémech Windows Vista™ Enterprise a Windows Vista™ Ultimate, kde slouží k ochraně klientských a mobilních počítačů. Technologie BitLocker zašifruje obsah disku. Útočník, který používá paralelní operační systém nebo jiné softwarové nástroje, pak nemůže prolomit ochranu souborů a systému, ani prohlížet soubory uložené na chráněné jednotce offline.
BitLocker zlepšuje ochranu dat díky kombinaci dvou hlavních dílčích funkcí: šifrování systémové jednotky a kontroly integrity součástí používaných v prvních fázích spouštění systému. Je zašifrována celá systémová jednotka, včetně stránkovacího a hibernačního souboru, což zvyšuje zabezpečení vzdálených serverů umístěných na pobočkách. BitLocker předchází krádežím dat a únikům informací ze ztracených, ukradených nebo nevhodně zlikvidovaných počítačů. BitLocker dále přispíván v organizacích k zajištění souladu s legislativními požadavky, jako jsou zákony Sarbanes-Oxley nebo HIPAA, které kladou velmi vysoké nároky na zabezpečení a ochranu dat.

Podniková infrastruktura PKI (PKIView)

V operačních systémech Windows Server 2008 a Windows Vista byl implementován velký počet vylepšení infrastruktury PKI (Public Key Infrastructure). Usnadnila se správa všech aspektů infrastruktury PKI v systému Windows, byly přepracovány služby pro odvolání a snížilo se riziko napadení během zápisu. Mezi hlavní vylepšení infrastruktury PKI patří:

- Podniková infrastruktura PKI (PKIView): Původně byl tento nástroj součástí sady Microsoft Windows Server™ 2003 Resource Kit pod názvem PKI Health, ale v systému Windows Server 2008 je PKIView modulem snap-in pro konzolu MMC. Slouží k analýze stavu certifikačních autorit a k zobrazení podrobností o certifikátech certifikačních autorit, které jsou publikovány prostřednictvím služby AD CS.
- Protokol OCSP (Online Certificate Status Protocol): V případech, kdy není optimálním řešením použití běžného seznamu odvolaných certifikátů, je možné

použít online respondér, který spravuje a distribuuje informace o odvolaných certifikátech pomocí protokolu OCSP. Online respondér lze nakonfigurovat buď na jediném počítači, nebo jako pole online respondérů.
- Služba zápisu síťových zařízení (Network Device Enrollment Service – NDES): V systému Windows Server 2008 představuje Služba zápisu síťových zařízení implementaci protokolu SCEP (Simple Certificate Enrollment Protocol) od společnosti Microsoft. Jde o komunikační protokol, který umožňuje softwaru fungujícímu na síťových zařízeních, např. směrovačích a přepínačích, který obvykle nelze v síti ověřit, zápis pro certifikát standardu x509 vydaný certifikační autoritou.
- Webový zápis: Nový ovládací prvek webový zápis disponuje lepším zabezpečením, snadněji se skriptuje a aktualizuje než předchozí verze.
- Zásady skupiny a infrastruktura PKI: Nastavení certifikátů v zásadách skupiny umožní soustředit správu nastavení certifikátů pro všechny počítače v doméně do jediného místa.

Rozhraní Cryptography Next Generation (CNG)

Rozhraní Cryptography Next Generation (CNG) představuje flexibilní platformu pro vývoj kryptografických nástrojů, která dává IT specialistům prostor k vytváření, aktualizaci a používání vlastních šifrovacích algoritmů v kryptografických aplikacích, jako jsou služba Active Directory Certificate Services (AD CS) nebo protokoly SSL (Secure Sockets Layer) a IPsec (Internet Protocol security). CNG implementuje kryptografické algoritmy předepsané doporučením Suite B vlády USA, mezi které patří algoritmy pro šifrování, digitální podpisy, výměnu klíčů a algoritmus hash.
CNG poskytuje sadu rozhraní API, které slouží k provádění základních kryptografických operací, například vytvoření, uložení a načtení kryptografického klíče. Podporuje také instalaci a použití dalších kryptografických zprostředkovatelů. CNG dává organizacím a vývojářům možnost používat vlastní kryptografické algoritmy nebo implementaci standardních kryptografických algoritmů.
Rozhraní CNG podporuje aktuální sadu algoritmů z rozhraní CryptoAPI 1.0 a poskytuje také podporu algoritmů ECC (Elliptic Curve Cryptography). Určitý počet algoritmů ECC je vyžadován v rámci doporučení Suite B vlády USA.

Řadiče domény jen pro čtení

Řadič domény jen pro čtení (Read-Only Domain Controller – RODC) je nový typ řadiče domény, který je k dispozici v systému Windows Server 2008 a je určen zejména pro nasazení v prostředí poboček. Řadič RODC může omezit riziko související s nasazením řadiče domény ve vzdáleném umístění, například na pobočce, kde nelze zaručit fyzické zabezpečení.
V řadiči RODC jsou uloženy všechny objekty a atributy služby AD DS (Microsoft Active Directory Domain Services) stejně jako v řadiči domény, do kterého lze zapisovat, s výjimkou hesel k účtům. Klientské počítače však nemohou ukládat změny přímo do řadiče RODC. Jelikož se změny nezapisují přímo do řadiče RODC, a nemají tedy místní původ, nemusí řadiče domény, do kterých lze zapisovat a které jsou replikačními partnery, stahovat z řadiče RODC změny. Zásady oddělení rolí správce stanoví, že místní správa řadiče RODC může být delegována libovolnému uživateli v doméně, aniž by bylo nutné udělit tomuto uživateli oprávnění k doméně jako takové nebo k jiným řadičům domény.

Oddělení serverů a domén

V síti se systémem Microsoft Windows mohou správci logicky izolovat prostředky serveru a domény, aby byl přístup udělen pouze ověřeným a oprávněným uživatelům. Uvnitř stávající fyzické sítě lze například vytvořit logickou síť z počítačů, které vyhovují společné sadě požadavků na zabezpečenou komunikaci. Každý počítač v této logicky oddělené síti musí před navázáním připojení předat dalším počítačům v oddělené síti ověřovací pověření.
Takováto izolace brání neoprávněným počítačům a programům v přístupu k nežádoucím prostředkům. Požadavky od počítačů, které nejsou členy oddělené sítě, budou ignorovány. Oddělení serverů a domén pomáhá chránit určité kritické servery a data a také spravované počítače před nespravovanými počítači a nedisciplinovanými uživateli.
Síť lze chránit pomocí dvou typů izolace:
- Oddělení serveru: Při oddělení serverů jsou určité servery nakonfigurovány pomocí protokolu IPsec tak, aby od jiných počítačů přijímaly pouze ověřená připojení. Databázový server lze například nakonfigurovat, aby přijímal pouze připojení od serveru webových aplikací.
- Oddělení domény: Hodlá-li správce oddělit doménu, může využít členství v doméně Active Directory a zajistit, že počítače, které jsou členy domény, budou přijímat pouze ověřené a zabezpečené přenosy od dalších počítačů, které jsou členy domény. Oddělená síť je tvořena pouze počítači, které jsou členy domény. Oddělení domény chrání pomocí zásad IPsec přenosy mezi členy domény, včetně všech klientských počítačů i serverů.

Shrnutí

Systém Windows Server 2008 poskytuje organizacím nebývalé možnosti zabezpečení prostřednictvím funkcí zabezpečení založených na zásadách, jak je architektura NAP. Posouzení a řízení stavu a zabezpečení připojovaných počítačů podstatně zlepšuje zabezpečení organizace. Nová rozhraní systému Windows Server 2008 pro správu zjednodušují procesy správy, konfiguraci a údržbu všech serverů v organizaci a snižují náklady na správu rozlehlé sítě.

Centralizovaný přístup k aplikacím

Úvod

Systém Windows Server 2008 obsahuje vylepšení a inovace Terminálové služby, které nezahrnují pouze zpřístupnění aplikací, ale zlepšují také pohodlí uživatele tím, že vzdálené aplikace mohou běžet na místní ploše hned vedle místních aplikací. K dispozici je také možnost centrálního přístupu k dostupným aplikacím prostřednictvím funkce Webový přístup Terminálové služby.

K novým součástem Terminálové služby patří:

- Vzdálená aplikace RemoteApp Terminálové služby: Pomocí nové verze klienta Připojení ke vzdálené ploše 6.0 mohou uživatelé provozovat vzdálené programy systému Windows na své vlastní ploše vedle místních aplikací. Tuto funkci zajišťuje Vzdálená aplikace RemoteApp® Terminálové služby.
- Brána Terminálové služby: Funkce Brána Terminálové služby (Brána TS) rozšiřuje dosah Terminálové služby za podnikovou bránu firewall a poskytuje zabezpečený přístup k terminálovým serverům a sdíleným plochám bez nutnosti využít infrastrukturu virtuální privátní sítě (VPN).
- Webový přístup Terminálové služby: Funkce Webový přístup Terminálové služby představuje řešení vzdálených aplikací, které správci zjednodušuje proces publikování vzdálených aplikací a zároveň usnadňuje uživateli vyhledání a spuštění vzdálené aplikace.
- Jednotné přihlašování: Jednotné přihlašování zpříjemňuje vzdálenému uživateli práci tím, že jej zbavuje povinnosti opakovaně zadávat pověření.

Terminálová služba

Terminálová služba v systému Windows Server 2008 zahrnuje nové základní funkce, které zvyšují pohodlí uživatele při připojení k terminálovému serveru se systémem Windows Server 2008. Nové funkce zahrnují:

- Připojení ke vzdálené ploše 6.0: Uživatelé musí k přístupu k Terminálové službě použít klienta Připojení ke vzdálené ploše 6.0. Je součástí systémů Windows Server 2008 i Windows Vista™ a uživatelé systémů Windows® XP a Windows Server 2003 si jej mohou bezplatně stáhnout.
- Vylepšení zobrazení v programu Připojení ke vzdálené ploše 6.0: Software Připojení ke vzdálené ploše 6.0 obsahuje nově podporu stolních počítačů s vysokým rozlišením (až 4096 x 2048) a zobrazení na více monitorech, ze kterých se skládá jediná velká plocha. Uživatelé klienta Připojení ke vzdálené ploše 6.0 mohou využívat nové monitory s vysokým rozlišením a moderními formáty zobrazení (širokoúhlý formát 16 : 9 nebo 16 : 10), které neodpovídají předchozímu standardu 4 : 3.
- Možnosti práce s počítačem: Klient Připojení ke vzdálené ploše 6.0 reprodukuje plochu vzdáleného počítače na klientském počítači uživatele. Pokud je na serveru Windows Server 2008 nainstalována funkce Možnosti práce s počítačem, může vzdáleně připojený uživatel využívat funkcí systému Windows Vista, například programu Windows Media® Player, motivů plochy a správy fotografií. Funkce Možnosti práce s počítačem a nastavení priority zobrazení (určené k synchronizaci klávesnice a myši se zobrazením na monitoru i v podmínkách velkého vytížení šířky pásma) zvyšují pohodlí uživatele při připojení k terminálovému serveru se systémem Windows Server 2008.

Jednotné přihlašování

Jednotné přihlášení umožní uživatelům s doménovým účtem jednorázové přihlášení k relaci Terminálové služby, a to pomocí hesla nebo karty Smart Card, a tím získat přístup ke vzdáleným serverům a aplikacím. Další výzvy k zadání pověření se již nezobrazí. Jednotné přihlašování zpříjemňuje uživatelům práci tím, že je zbavuje povinnosti zadávat pověření při každém zahájení vzdálené relace.

Vzdálená aplikace RemoteApp Terminálové služby

Vzdálená aplikace RemoteApp Terminálové služby představuje novou metodu prezentace vzdálených aplikací, která je k dispozici v systému Windows Server 2008. RemoteApp doplňuje standardní metodu prezentace Terminálové služby, která prezentuje uživateli celou vzdálenou plochu a uživatel pak používá aplikace v jejím okně. V systému Windows Server 2008 se interakce uživatele se vzdálenými aplikacemi podstatně liší. Na ploše klientského počítače se spustí a ve vlastním okně běží jednotlivá vzdálená aplikace, nikoli celá vzdálená plocha. Pokud daný program využívá ikonu v oznamovací oblasti hlavního panelu, zobrazí se tato ikona na hlavním panelu klientského počítače. Dialogová okna jsou přesměrována na místní plochu a místní jednotky a tiskárny jsou přesměrovány a zpřístupněny ve vzdáleném programu. Mnoho uživatelů nepostřehne žádný rozdíl mezi vzdáleným programem a ostatními místními aplikacemi, vedle nichž vzdálený program na ploše běží.

Vzdálená aplikace RemoteApp snižuje nároky na správu, neboť postačí udržovat jedinou aplikaci na centrálním serveru namísto jednotlivých instalací ve stolních počítačích roztroušených po celé organizaci. Navíc zpříjemňuje práci uživatelům, protože vzdálená aplikace je přímo integrována na plochu klientského počítače.

Brána Terminálové služby (Brána TS)

Brána Terminálové služby je role Terminálové služby, která umožňuje připojení oprávněných vzdálených uživatelů v internetu k terminálovým serverům a pracovním stanicím v podnikové síti. To umožňuje organizacím snadno a bezpečně zpřístupnit určité servery a pracovní stanice vzdáleným a cestujícím pracovníkům bez nutnosti použít připojení pomocí virtuální privátní sítě.

Mezi hlavní výhody Brány TS patří:

- Umožňuje zabezpečené připojení vzdálených uživatelů z internetu k prostředkům v podnikové síti a přitom eliminuje

složitost připojení pomocí virtuální privátní sítě (VPN).
- Využívá zabezpečení a snadnou dostupnost protokolu HTTPS k poskytování Terminálové služby bez předchozí konfigurace na straně klienta.
- Zahrnuje komplexní model konfigurace zabezpečení, který umožňuje správcům řídit přístup ke konkrétním prostředkům v síti.
- Umožňuje vzdálené připojení k terminálovým serverům a vzdáleným pracovním stanicím přes bránu firewall nebo zařízení NAT.
- Zahrnuje model s vyšším zabezpečením, který uživatelům zpřístupňuje pouze vybrané servery a pracovní stanice namísto celé podnikové sítě, jak je tomu v případě VPN.

Brána Terminálové služby poskytuje snadný a bezpečný způsob, kterým mohou organizace zpřístupnit vzdáleným uživatelům servery a pracovní stanice v síti, aniž by bylo nutné nainstalovat a nakonfigurovat připojení VPN. Komplexní funkce pro zabezpečení navíc umožňují správcům řídit přístup ke konkrétním prostředkům.

Webový přístup Terminálové služby

Funkce Webový přístup Terminálové služby je role Terminálové služby, která umožňuje správcům zpřístupnit Vzdálené aplikace RemoteApp Terminálové služby uživatelům s webovým prohlížečem, aniž by uživatel musel instalovat další software. Pokud je nainstalována funkce Webový přístup Terminálové služby, uživateli stačí navštívit určený web a zvolit z nabídky dostupných aplikací. Jakmile uživatel některý z uvedených programů spustí, bude automaticky zahájena relace Terminálové služby na terminálovém serveru se systémem Windows Server 2008, na kterém je požadovaná aplikace hostována. Uživateli zobrazí webové rozhraní centrální nabídku všech aktuálně dostupných vzdálených aplikací. Ke spuštění vzdálené aplikace stačí vybrat požadovaný program z nabídky.
Funkce Webový přístup Terminálové služby pomáhá snížit náklady na správu. Programy jsou snadno přístupné v centrálním umístění. Programy běží na terminálovém serveru a nikoli v klientském počítači, takže IT specialistům stačí udržovat a aktualizovat jedinou instalaci dané aplikace.

Řešení pro pobočky

Úvod

K podnikovým prioritám často patří přibližování k zákazníkům a přesun pracovníků z ústředí do poboček. Se zvyšujícím se počtem poboček rostou i nároky na správu IT a na zabezpečení těchto vzdálených pracovišť. Společnost Microsoft si je vědoma potřeb této rostoucí skupiny pracovníků a potřeby nových řešení, která se budou soustředit na problémy specifické pro pobočky.
Pobočky málokdy mívají interního IT specialistu, a proto servery v nich umístěné přinášejí několik rizik pro správce IT. Software běžící na serverech musí efektivně využívat pomalejší připojení k síti WAN, aby nespotřeboval celou šířku pásma, nezpomalil přenos kritických dat a neměl zásadní dopad na výkon aplikací provozovaných uživateli na pobočce. Zabezpečení představuje v pobočkách vyšší riziko, neboť nelze vždy zaručit fyzické zabezpečení serverů. Většina IT specialistů není na pobočce k dispozici, a proto jsou pro pobočky preferována serverová řešení podporující centrální či vzdálenou správu a vzdálené nasazení.
Společnost Microsoft začala řešit problémy a potřeby poboček v systému Windows Server 2003 R2. Vydání systému Windows Server 2008 zahrnuje mnoho dalších vylepšení, která poskytují správcům lepší přehled o situaci v pobočkách a zlepšují ochranu poboček i ústřední sítě a dat organizace. IT specialistům pak nabízí vyšší flexibilitu nutnou při plnění specifických požadavků dané organizace.
Hlavní výhody systému Windows Server 2008 v oblasti řešení pro pobočky lze rozdělit do tří kategorií:
- Zlepšení efektivity nasazení a správy serveru pobočky
- Zmírnění bezpečnostních rizik v pobočkách
- Zvýšení efektivity komunikace v síti WAN a využití šířky pásma

Řešení společnosti Microsoft pro pobočky a systém Windows Server 2008 řeší základní potřeby poboček pomocí celé řady nových a vylepšených funkcí, které zjednodušují nasazení a efektivní správu hlavních serverových rolí, zlepšují zabezpečení a poskytují architekturu, která optimalizuje výkon a zajišťuje spolehlivost služeb.

Nasazení a správa

Správa serverů, služeb a zabezpečení ve vzdálených pobočkách představuje pro IT specialisty dlouhodobý problém. Windows Server 2008 zjednodušuje vzdálené nasazení a průběžnou správu serverů umístěných na pobočkách.
Změny a vylepšení adresářové služby Active Directory, uvedení řadičů domény jen pro čtení, BitLocker, oddělení rolí a instalace Server Core patří mezi konkrétní funkce systému Windows Server 2008, které řeší jedinečné nároky poboček a zvyšují efektivitu IT oddělení při správě vzdálených pracovišť.

Řadiče domény jen pro čtení

Řadič domény jen pro čtení (Read-Only Domain Controller – RODC) je nový typ řadiče domény, který je k dispozici v systému Windows Server 2008. Je určen zejména pro nasazení v prostředí poboček. Pomocí řadičů RODC může organizace omezit riziko související s nasazením řadiče domény na místech, jako jsou pobočky, kde nelze zaručit fyzické zabezpečení.
V řadiči RODC jsou uloženy všechny objekty a atributy služby AD DS (Microsoft Active Directory Domain Services) stejně jako v řadiči domény, do kterého lze zapisovat, s výjimkou hesel k účtům. Klientské počítače však nemohou ukládat změny přímo do řadiče RODC. Jelikož se změny nezapisují přímo do řadiče RODC, a nemají tedy místní původ, nemusí řadiče domény, do kterých lze zapisovat a které jsou replikačními

partnery, stahovat z řadiče RODC změny. Tím se snižuje zatížení bridgehead serverů v ústředí a nároky na monitorování replikace. Zásady oddělení rolí správce stanoví, že místní správa řadiče RODC může být delegována libovolnému uživateli v doméně, aniž by bylo nutné udělit tomuto uživateli oprávnění k doméně jako takové nebo k jiným řadičům domény. V takové situaci se místní uživatel na pobočce může přihlásit k řadiči RODC a provést potřebnou údržbu serveru, například upgrade ovladače, a přitom nemá přístup k doménovým prostředkům mimo pobočku.

BitLocker Drive Encryption

BitLocker Drive Encryption je důležitá nová funkce zabezpečení v systému Windows Server 2008, která pomáhá chránit servery na pobočkách. Je k dispozici také v systémech Windows Vista™ Enterprise a Windows Vista™ Ultimate, kde slouží k ochraně klientských počítačů a mobilních počítačů cestujících uživatelů. Technologie BitLocker zašifruje obsah disku. Útočník, který používá jiný operační systém nebo jiné softwarové nástroje, pak nemůže prolomit ochranu souborů a systému, ani prohlížet soubory uložené na chráněné jednotce offline.
BitLocker zlepšuje ochranu dat díky kombinaci dvou hlavních dílčích funkcí: šifrování systémové jednotky a kontroly integrity součástí používaných v prvních fázích spouštění systému. Je zašifrována celá systémová jednotka, včetně stránkovacího a hibernačního souboru, což zvyšuje zabezpečení vzdálených serverů umístěných na pobočkách. BitLocker předchází krádežím dat a únikům informací ze ztracených, ukradených nebo nevhodně zlikvidovaných počítačů. To je v pobočkách důležitý aspekt, neboť nelze vždy zaručit fyzické zabezpečení serverů.

Server Core

Počínaje verzí Windows Server 2008 se mohou správci rozhodnout pro minimální instalaci systému Windows Server, která obsahuje jen určité funkce, a nikoli nepotřebné součásti. V prostředí instalace Server Core lze provozovat jednu nebo více z následujících rolí serveru, které bývají často nasazeny v pobočkách:

- Server DHCP (Dynamic Host Configuration Protocol)
- Server DNS (Domain Name System)
- Souborový server
- Služba AD DS (Active Directory Domain Service)
- Služba AD LDS (Active Directory® Lightweight Directory Services)
- Služba Windows Media Services
- Správa tisku
- Virtualizace systému Windows Server

V pobočkách nabízí instalace Server Core následující hlavní výhody:

- Menší nároky na údržbu softwaru: Menší instalace Server Core snižuje počet nutných aktualizací a oprav, takže se šetří šířka pásma WAN spotřebovávaná pobočkovými servery i čas, který IT specialisté potřebují na správu.
- Menší riziko napadení: Správce může nainstalovat pouze konkrétní služby vyžadované danou pobočkou a naprosto tak minimalizovat riziko útoku.
- Méně časté restartování a menší nároky na místo na disku: V minimální instalaci Server Core je počet nainstalovaných součástí, které je nutno aktualizovat nebo opravovat, nižší, a proto není nutné tak často restartovat systém. Instalace Server Core obsahuje jen minimální počet souborů nezbytně nutných k zajišťování požadovaných funkcí, takže potřebná kapacita disku na pobočkovém serveru se sníží.

Snazší správa služby Active Directory

Systém Windows Server 2008 obsahuje vylepšení služby Active Directory Domain Services, které zjednodušují její správu a poskytují správcům vyšší flexibilitu nutnou pro potřeby poboček. Mezi tato vylepšení patří:

- Aktualizovaný průvodce instalací služby Active Directory Domain Services (AD DS)
- Změny konzoly MMC, která slouží ke správě služby AD DS
- Nové možnosti při instalaci řadičů domény
- Aktualizovaný instalační průvodce, který zjednodušuje instalaci služby AD DS
- Vylepšené rozhraní a možnosti správy služby AD DS
- Vylepšené nástroje pro vyhledávání řadičů domény v rozlehlé síti

V novém průvodci instalací jsou všechny související funkce seskupeny dohromady, což zrychluje proces instalace a šetří čas při nasazení. Bezobslužná instalace systému Windows Server 2008 nevyžaduje žádné zadání informací do uživatelského rozhraní a dále tím zjednodušuje vzdálenou instalaci. Díky tomu je také možné nainstalovat službu AD DS na instalaci Server Core. Na základě možností vybraných při instalaci je v nově nainstalovaném serveru DNS automaticky nakonfigurováno nastavení klientů DNS, serverů pro předávání i odkazy na kořenové servery, takže server DNS ihned správně funguje.
Tato vylepšení rozhraní služby AD DS, která jsou k dispozici v systému Windows Server 2008, přispívají ke snížení časových nároků na správu IT, protože zkracují počáteční nasazení a zjednodušují správu serverů na pobočkách.

Vysoká dostupnost

Úvod

Zajištění stálé dostupnosti kritických aplikací je klíčovou odpovědností IT oddělení, a proto se mnohá vylepšení v systému Windows Server 2008 zaměřují právě na dosažení vysoké dostupnosti. Clustering s podporou převzetí služeb při selhání, vyrovnávání zatížení sítě a nové funkce systému Windows Server 2008 pro zálohování a obnovení představují kombinaci, která organizacím poskytuje vysoce dostupné řešení a zajišťuje, že kritické aplikace, služby a informace budou vždy všem uživatelům k dispozici.

Clustering s podporou převzetí služeb při selhání

Cluster s podporou převzetí služeb při selhání, dříve označovaný jako cluster serverů, je skupina nezávislých počítačů, které spolupracují na zvýšení dostupnosti aplikací a služeb. Servery v clusteru, tzv. uzly, jsou propojeny fyzickou kabeláží i softwarově. Dojde-li k selhání jednoho z clusterů serveru, převezme jiný uzel v clusteru úlohy vyřazeného uzlu, takže uživatelé téměř nepostřehnou výpadek služby. Clustery s podporou převzetí služeb při selhání používají IT specialisté, kteří jsou zodpovědní za zajištění vysoké dostupnosti kritických služeb a aplikací.

Vylepšení v podobě clusterů s podporou převzetí služeb při selhání v systému Windows Server 2008 jsou zaměřena na zjednodušování clusterů, jejich lepší zabezpečení a zvýšení jejich stability. Instalace a konfigurace clusterů byla v systému Windows Server 2008 zjednodušena pomocí nového ověřovacího průvodce, který umožní uživatelům potvrdit, zda je systém, úložiště a konfigurace sítě vhodná pro cluster. Mezi testy prováděné novým ověřovacím průvodcem patří:

- Testy uzlů: Potvrzují, zda je na serverech nainstalována stejná verze operačního systému a stejné aktualizace softwaru.
- Testy sítě: Určují, zda plánovaná síť clusteru splňuje určité požadavky, například zda obsahuje nejméně dvě samostatné podsítě, které zajistí redundanci sítě.
- Testy úložiště: Analyzují konfiguraci úložiště a ověřují, zda všechny uzly mají přístup ke všem sdíleným diskům a zda disky splňují stanovené požadavky.

Windows Server 2008 podporuje pro účely clusterového úložiště disky s oddíly GPT (GUID Partition Table). Disky GPT mohou mít oddíly větší než 2 TB a na rozdíl od disků s hlavním spouštěcím záznamem (MBR – master boot record) mohou mít integrovanou redundanci. K dalším výhodám disků s oddíly GPT v porovnání s oddíly s hlavním spouštěcím záznamem patří podpora až 128 oddílů na každém disku, podpora svazků až do kapacity 18 exabajtů, primární a záložní tabulka oddílů pro redundanci a podpora jedinečných identifikátorů disků i oddílů.

Správa clusteru je zjednodušena díky vylepšením rozhraní pro správu, která správcům umožňují soustředit se na správu aplikací a dat, nikoli clusteru. Nové rozhraní se soustředí na úkoly a je intuitivnější a využívá podpory průvodců, kteří provedou správce operacemi, které byly dříve velmi složité.

Clustery s podporou převzetí služeb při selhání mají v systému Windows Server 2008 lepší funkce a spolehlivost než serverové clustery v předchozích verzích. Mezi hlavní vylepšení patří:

- **Dynamické přidávání diskových prostředků:** Závislosti prostředků lze upravovat v době, kdy jsou prostředky online, což znamená, že správci mohou například zpřístupnit další diskové úložiště bez přerušení přístupu k aplikaci, která ho bude používat.
- **Vyšší výkon a stabilita datového úložiště:** Když cluster s podporou převzetí služeb při selhání komunikuje se sítí SAN (storage area network) nebo s úložištěm DAS (direct attached storage), používá takové příkazy, které co nejméně narušují probíhající operace – k resetování sběrnice SCSI dochází méně často. Disky nejsou nikdy ponechány v nechráněném stavu, což znamená nižší riziko poškození svazku. Clustery s podporou převzetí služeb při selhání také podporují vylepšené metody zjišťování a obnovování disků. Clustery s podporou převzetí služeb při selhání podporují tři typy připojení úložiště: Serial Attached SCSI (SAS), iSCSI a Fibre Channel.
- **Snazší údržba disků:** Režim údržby byl podstatně zdokonalen, aby mohli správci používat nástroje pro snazší kontrolu, opravu, zálohování a obnovování disků s daleko menším narušením činnosti clusteru.

Správci, kteří zajišťují řešení s vysokou dostupností pomocí clusteru, získají se systémem Windows Server 2008 podstatné usnadnění nasazení i správy clusteru a zvýšení výkonu i spolehlivosti.

Vyrovnávání zatížení sítě

Vyrovnávání zatížení sítě (Network Load Balancing, NLB) je funkce, která rozděluje zatížení síťových aplikací založených na modelu klient-server mezi několik serverů v rámci clusteru NLB. Funkci NLB využijí organizace, které potřebují rozdělit požadavky od klientů mezi několik serverů. Je vhodná zejména pro zajištění škálovatelnosti bezstavových aplikací, např. webových aplikací běžících nad Internetovou informační službou (IIS), přidáním dalších serverů, pokud se zvýší zatížení. NLB zajišťuje škálovatelnost tím, že je možné na zvýšení zatížení reagovat přidáním dalších serverů. NLB zvyšuje také spolehlivost, neboť server, který nefunguje, lze snadno vyměnit. Windows Server 2008 obsahuje následující vylepšení funkcí vyrovnávání zatížení sítě:

- Podpora protokolu IPv6: NLB plně podporuje protokol IPv6 pro veškeré komunikace.
- Podpora rozhraní NDIS 6.0: Ovladač NLB byl zcela přepracován a nyní využívá model jednoduchých filtrů NDIS 6.0. NDIS 6.0 zachovává zpětnou kompatibilitu s předchozími verzemi rozhraní NDIS. Vylepšení návrhu rozhraní NDIS 6.0 zahrnují vyšší výkon ovladače, škálovatelnost a zjednodušený model ovladače NDIS.
- Vylepšení rozhraní WMI: Vylepšení rozhraní WMI v oboru názvů MicrosoftNLB zajišťují podporu protokolu IPv6 a více dedikovaných adres IP.
- Třídy v oboru názvů MicrosoftNLB: Podporují adresy IPv6 (i adresy IPv4).
- Třída MicrosoftNLB_NodeSetting: Podporuje více dedikovaných adres IP, které je možné zadat do atributů DedicatedIPAddresses a DedicatedNetMasks.
- Vylepšená spolupráce se serverem ISA: V situacích, kdy mezi klienty jsou přenosy IPv4 i IPv6, může ISA Server nakonfigurovat více dedikovaných adres IP pro každý uzel NLB. Klienti IPv4 i IPv6 musí přistupovat k určitému serveru ISA, který řídí provoz. ISA Server může předat NLB také upozornění na útok SYN nebo nedostatek časovačů. (K těmto situacím obvykle dochází, pokud je počítač přetížen nebo napaden virem z internetu.)

- Podpora více dedikovaných adres IP pro každý uzel: NLB plně podporuje definování více než jedné dedikované adresy IP na uzel (dříve byla podporována pouze jediná dedikovaná adresa IP na každý uzel), takže mohou být na stejném clusteru NLB hostovány různé aplikace v případě, že každá z nich vyžaduje vlastní dedikovanou adresu IP.
- Tyto funkce poskytují lepší podporu nových oborových standardů, zvyšují výkon, zlepšují možnosti spolupráce, posilují zabezpečení a zvětšují flexibilitu při nasazení a konsolidaci aplikací.

Windows Zálohování

Zálohování je třetí důležitou součástí systému Windows Server 2008, která byla navržena s ohledem na vysokou dostupnost služeb. Program Zálohování poskytuje řešení zálohování a obnovení pro server, na kterém je nainstalován. Obsahuje novou technologii zálohování a obnovení, která nahrazuje předchozí zálohovací funkce dostupné ve starších verzích operačního systému Windows. Program Zálohování lze použít ke spolehlivé a účinné ochraně celého serveru, aniž by bylo nutné zabývat se technickým mechanismem zálohování a obnovení. Uživateli zjednoduší proces plánování automatického zálohování, vytvoření ruční zálohy a obnovení položky či celého svazku příslušný průvodce. Program Zálohování v systému Windows Server 2008 lze použít k zálohování celého serveru nebo jen vybraných svazků.

Zálohování využívá službu Stínová kopie svazku a technologii zálohování na úrovni bloku a zvyšuje tak efektivitu zálohování i obnovení operačního systému, souborů, složek i svazků. Po prvním vytvoření zálohy pořizuje program Zálohování inkrementální zálohy, které obsahují pouze data změněná od posledního zálohování. Na rozdíl od předchozích verzí se již správce nemusí starat o ruční plánování úplných nebo inkrementálních záloh.

Obnovení dostálo v systému Windows Server 2008 vylepšení a zjednodušení. Položky lze nyní obnovit tím, že uživatel zvolí zálohu, ze které chce obnovit, a poté položky, které hodlá obnovit. Je možné obnovit určité soubory nebo celý obsah složky. Pokud byla určitá položka v minulosti uložena v inkrementální záloze, bylo nutné ji ručně obnovit z několika různých záloh. Nyní stačí pouze vybrat datum, kdy byla zálohována verze, kterou chce uživatel obnovit.

Systém Windows Server 2008 poskytuje řešení zálohování a obnovení, které je nezbytné k vytvoření vysoce dostupného řešení, jež chrání data organizace i operační systémy na serverech v síti. Současně snižuje nároky kladené na správce při zajišťování správných záloh kritických dat a urychluje jejich obnovení.

Shrnutí

Microsoft Windows Server 2008 představuje novou generaci systému Windows Server. Díky systému Windows Server 2008 budou mít IT specialisté serverovou a síťovou infrastrukturu pod lepší kontrolou, takže se mohou soustředit na klíčové potřeby firmy. Přispívá ke zvýšení zabezpečení operačního systému a k ochraně síťového prostředí. Poskytuje IT specialistům také flexibilitu, urychluje nasazení a správu systémů IT, zjednodušuje konsolidaci a virtualizaci serverů i aplikací a obsahuje intuitivní nástroje pro správu. Windows Server 2008 poskytuje nejlepší základnu pro serverovou a síťovou infrastrukturu každé organizace.