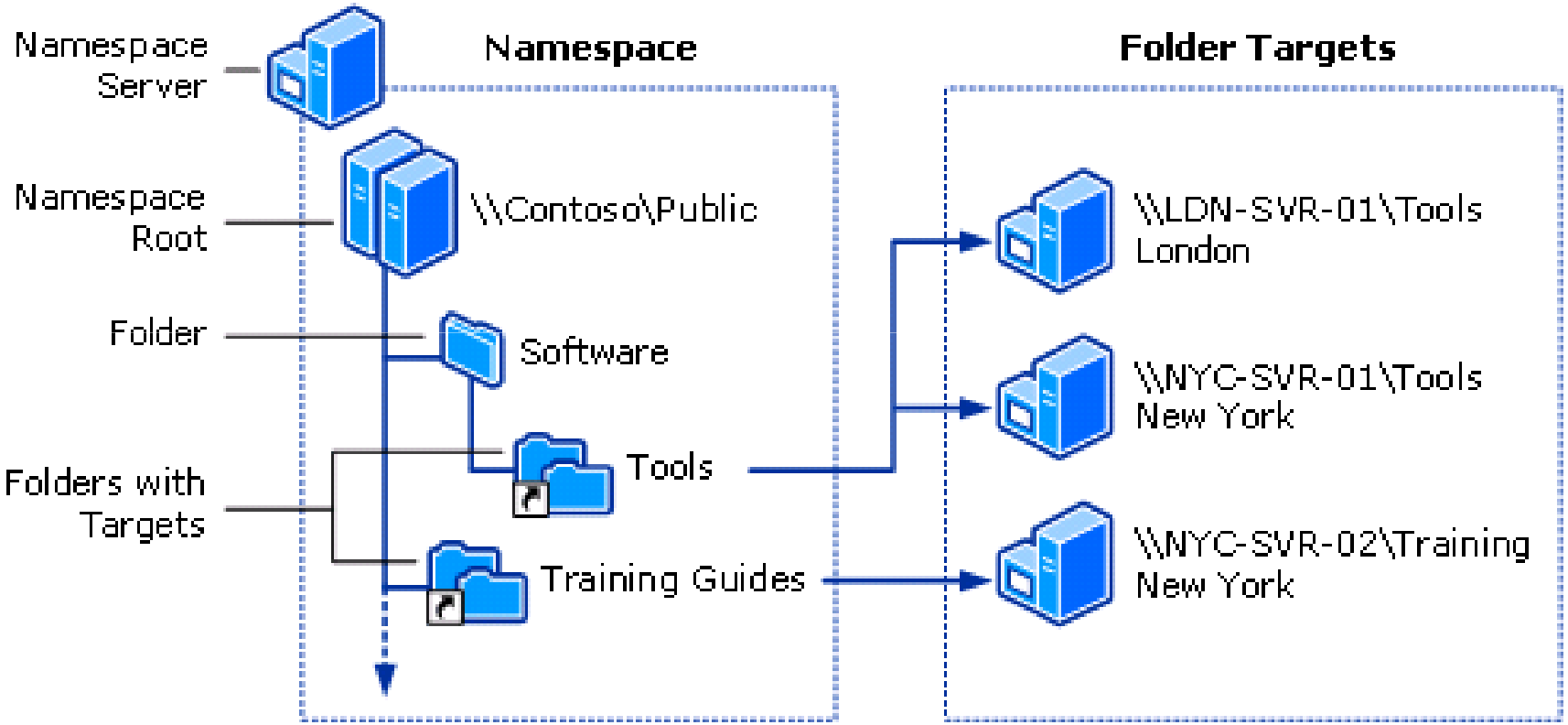
DFS

- Distributed File System
- Umožňuje organizovat víc SMB sdílení do jednoho logického adresáře
- Snižuje zatížení sítě, vysoká dostupnost dat, zjednodušení přístupu ke sdíleným složkám
- Access-based enumeration (Server 2008 mode)
- Dfsutil, dfscmd, dfsradmin, dfsdiag

DFSN


Namespace Server
Namespace
Folder Targets
Namespace Root
\\Contoso\Public
Folder
Software
Tools
Folders with Targets
Training Guides
\\LDN-SVR-01\Tools
London
\\NYC-SVR-01\Tools
New York
\\NYC-SVR-02\Training
New York

DFSN

- Domain-based namespace
  - \\domainName\dfsStore
  - Více namespace serverů
  - Namespace provázaný s názvem domény (DNS/netbios název)
  - Možnost replikace dat skrze DFSR
  - Nastavení uloženo v AD
- Stand-alone namespace
  - \\serverName\dfsStore
  - Jeden namespace server (Failover Cluster)
  - Namespace provázaný s názvem serveru
  - Nastavení uloženo v registrech

Porovnání DFS

Characteristic	Stand-Alone Namespace	Domain-based Namespace (Windows 2000 Server Mode)	Domain-based Namespace (Windows Server 2008 Mode)
Path to namespace	*ServerName**RootName*	*NetBIOSDomainName**RootName* *DNSDomainName**RootName*	*NetBIOSDomainName**RootName* *DNSDomainName**RootName*
Namespace information storage location	In the registry and in a memory cache on the namespace server	In AD DS and in a memory cache on each namespace server	In AD DS and in a memory cache on each namespace server
Namespace size recommendations	The namespace can contain more than 5,000 folders with targets	The size of the namespace object in AD DS should be less than 5 megabytes (MB) to maintain compatibility with domain controllers that are not running Windows Server 2008. This means no more than approximately 5,000 folders with targets.	The namespace can contain more than 5,000 folders with targets
Minimum AD DS forest functional level	AD DS is not required	Windows 2000	Windows Server 2003
Minimum AD DS domain functional level	AD DS is not required	Windows 2000 mixed	Windows Server 2008
Minimum supported namespace servers	Windows 2000 Server	Windows 2000 Server	Windows Server 2008

Porovnání DFS

Characteristic	Stand-Alone Namespace	Domain-based Namespace (Windows 2000 Server Mode)	Domain-based Namespace (Windows Server 2008 Mode)
Support for access-based enumeration (if enabled)	Yes, requires Windows Server 2008 namespace server	No	Yes
Supported methods to ensure namespace availability	Create a stand-alone namespace on a failover cluster.	Use multiple namespace servers to host the namespace. (The namespace servers must be in the same domain.)	Use multiple namespace servers to host the namespace. (The namespace servers must be in the same domain.)
Support for using DFS Replication to replicate folder targets	Supported when joined to an AD DS domain	Supported	Supported

DFSR

- Replikace SYSVOL pomocí modernějšího DFS namísto FRS
- Rychlejší, spolehlivější, lepší diagnostika (dfsrdiag)
- Nutný AD functional level alespoň 2008 a všechny servery alespoň Windows Server 2008
- Využívá Remote Differencial Compression (RDC) – po síti se přenáší jen změněné části souborů (delta files)
- Dojde k vytvoření nového SYSVOL adresáře (%windir%\SYSVOL_DFSR)
- dfsrmig

Delegování oprávnění

- Důvody
  - Bezpečnost (princip minimálních oprávnění)
  - Administrace (odchod, výměna, přidání pracovníka)
  - AGDLP

AGDLP & AGUDLP

- Doporučená strategie pro nastavení přístupu k doménovým prostředkům
- **A**ccounts -> **G**lobal groups ->**D**omain **L**ocal group -> **P**ermissions
- Global groups reprezentují pracovní role (G_Auditing_Specialists) a domain local groups oprávnění na zdroj (DL_NTFS_SHARED_REPORTS_MODIFY)
- Účty ani globální skupiny by neměly mít přímo přidělená oprávnění (jen skrze domain local g.)

AGDLP

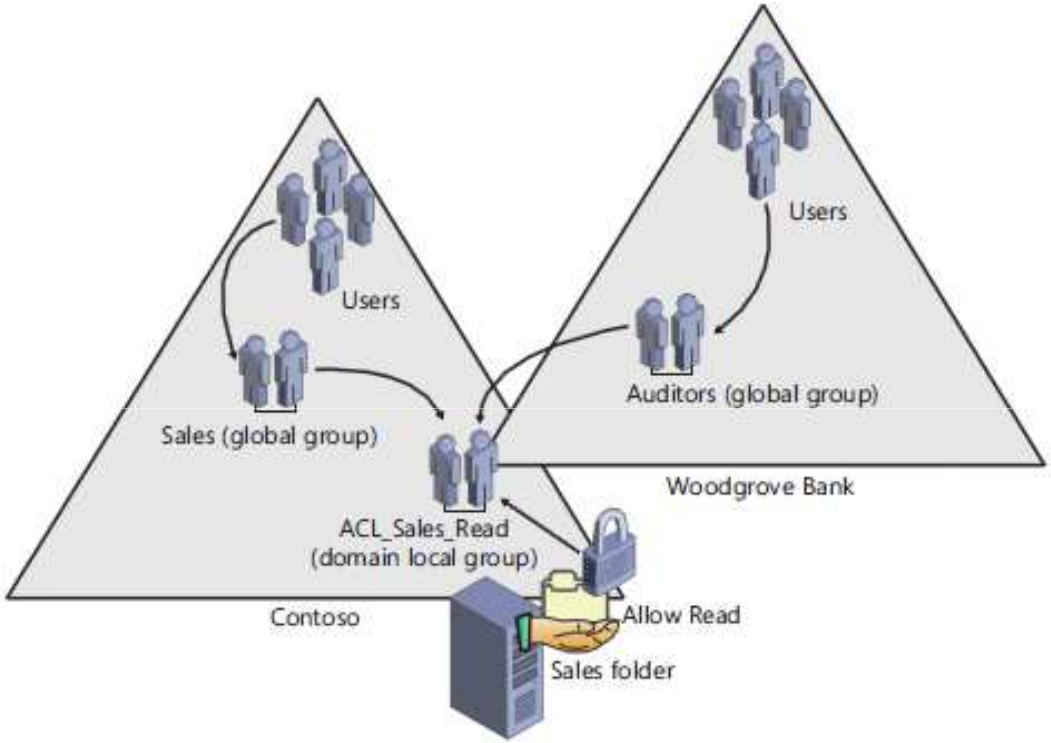


FIGURE 4-10 A group management implementation

převzato z MCTS Exam 70-640

Groups

- Replication, membership, availability
- Group scope
  - Local
  - Domain local
    - Členové z jakékoli důvěryhodné domény v lese
    - Přístup jen k prostředkům v rámci vlastní domény
  - Global
    - Členové jen z vlastní domény
    - Přístup ke všem prostředkům v lese
  - Universal
    - Členové z jakékoli domény krom externích
    - Přístup ke všem prostředkům v lese
    - Ukládají se na GC (replikace!)
    - Enterprise admin, Schema admins

Group membership

TABLE 4-1 Group Scope and Members

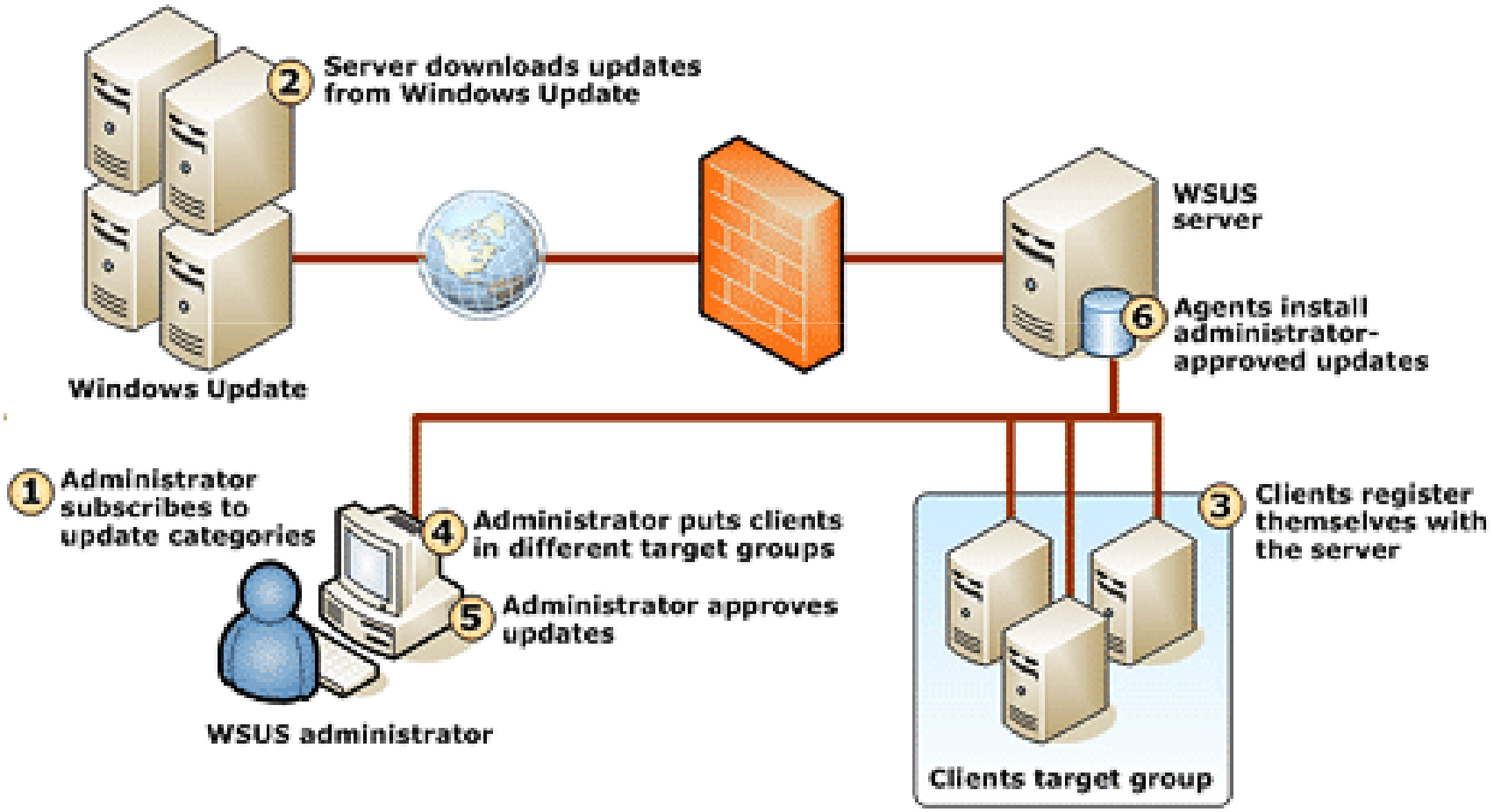
GROUP SCOPE	MEMBERS FROM THE SAME DOMAIN	MEMBERS FROM ANOTHER DOMAIN IN THE SAME FOREST	MEMBERS FROM A TRUSTED EXTERNAL DOMAIN
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Universal groups Domain local groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups	N/A
Global	Users Computers Global groups	N/A	N/A

převzato z MCTS Exam 70-640

WSUS

- Centrální řešení pro nasazení a správu aktualizací Windows produktů (i produktů třetích stran)
- Local Update Publisher & System Center Update Publisher (monitoring?)
- WSUS & GPO
- Jeden server na cca 25000 klientů
- Nativní podpora high availability architecture (clusters)
- BITS (Background Intelligent Transfer Service)
  - Omezení síťové komunikace
  - Peer caching
- WSUS SP2
  - Branch cache (jen enterprise edice win7!)
  - Podpora Win7 klientů

WSUS


2 Server downloads updates from Windows Update
Windows Update
WSUS server
6 Agents install administrator-approved updates
1 Administrator subscribes to update categories
4 Administrator puts clients in different target groups
5 Administrator approves updates
WSUS administrator
3 Clients register themselves with the server
Clients target group

WSUS architektura

- Centralized
  - Centrální server se replikuje na downstream servery
  - Malé možnosti adminů u replikovaných serverů
  - Povolování a plánování aktualizací se provádí na centrálním serveru
- Distributed
  - Admini mají větší „moc“, sami vytváří skupiny a povolují akt.
  - Cílem je spíš distribuce aktualizací než kontrola
- Disconnected
  - Data se importují z fyzického média (ne z internetu)
- Roaming
  - Pro mobilní klienty
  - Distribuují se jen metadata o povolených aktualizacích, ty se stahují přímo z MS serverů

Terminal Services Role

- Jedna z rolí Windows Server 2008 umožňující uživatelům nejen vzdálený přístup
- TS RemoteApp
- TS Printing
- TS Web Access
- TS Licensing
- TS Gateway
- TS Session Broker

TS RemoteApp

- slouží pro vzdálený přístup k nainstalovaným aplikacím na serveru
- Aplikace se jeví jako by běžela lokálně (včetně popup oken)
- Alespoň Windows XP SP2 (RDC 6.0)
- Přístup k app skrze
  - Rdp&MSI soubor distribuovaný administrátorem
  - Poklepání na soubor s koncovkou asociovanou k remoteApp aplikaci
  - Odkaz na TS Web Access (aspoň RDC 6.1 – XP SP3)

TS Web Access

- Role umožňující připojení skrze webový prohlížeč na vzdálenou plochu či ke spuštění remoteApp
- Nutnost nainstalovat i IIS
- TS Web Access server nemusí být terminal server

TS Printing

- Umožňuje klientům tisknout ze vzdálené plochy na jejich lokální tiskárně

TS Licensing

- Umožňuje efektivní správu CAL licencí (client access licence)

TS Session Broker

- Umožňuje session load balancing mezi terminálními servery v serverové farmě
- Směruje uživatele na server obsluhující nejméně session (sezení)

TS Gateway

- Role umožňující klientům přistupovat z internetu k intranetovým zdrojům skrze zabezpečené RDC spojení přes https bez nutnosti VPN
- Lokální zdroj může být samotný TS, stanice, TS s remoteApp
- Umožňuje přístup k zdrojům za NATem, firewallem,..(využívá port 443)
- Umožňuje využití NAP pro další zvýšení zabezpečení

Windows Deployment Service role

- Role vycházející ze starší Remote Installation Services umožňující vzdálené nasazení operačních systémů Windows
- Požadavky
  - NTFS file system pro ukládání obrazů OS
  - DNS a DHCP servery na síti
  - PXE (preboot execution environment)
  - AD doména
  - Pro nasazení image přes IPv6 je potřeba Windows Server 2008 R2
- Boot, installation, capture, discovery image, WAIK, MDT

SCCM

- System Center Configuration Manager
- Nástroj z rodiny produktů Systém Center pro centralizovanou správu Windows prostředí
  - Nasazení aplikací
  - Nasazení aktualizací
  - Nasazení Windows OS (zero touch)
  - Správa mobilních zařízení
  - Kontrola dodržování nastavených zásad (Desired Configuration Mng.)
  - Power management
  - NAP
  - Asset Intelligence
  - Inventory
  - Software metering
  - Monitoring