

Serverové systémy Microsoft Windows

IW2/XMW2 2010/2011

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 4.4.2011

Read-only řadiče domény

Read-only řadiče domény (RODC)

- Speciální typ řadičů domény určený k nasazování do tzv. vedlejších míst (*branch office*)
 - Nižší úroveň zabezpečení
 - Špatné nebo nespolehlivé spojení s ostatními místy
 - Omezený personál pro správu a údržbu
- K dispozici od Windows Server 2008
- Cíle RODC řadičů
 - Zajistit autentizaci, přístup ke službám a vyhledávání
 - Zaručit konzistenci a bezpečnost dat, usnadnit správu

Nevýhody centralizace řadičů domény

- Autentizace identit
 - Ztráta spojení znemožňuje přihlašování do domény
- Přístup ke službám
 - Přístup ke službám Active Directory vyžaduje ověření řadičem domény (vydání tzv. *service ticket*)
 - Pomalé spojení zpomaluje také přístup ke službám
- Vyhledávání
 - Globální katalogy umístěny v jediném místě
 - Všechny dotazy musí být směrovány do tohoto místa

Nevýhody rozproštění řadičů domény

- Správa řadičů domény
 - Údržbu mohou provádět pouze správci domény (jenž jsou lokálními správci na řadičích domény)
 - Správci řadičů domény mohou zasahovat do domény
- Konzistence dat databáze Active Directory
 - Chybná data v databázi replikována do celé domény
- Bezpečnost dat databáze Active Directory
 - Každý řadič domény obsahuje kopii dat celé domény
 - Odcizením řadiče domény je možné získat tajná data

Autentizace identit

- RODC řadiče neobsahují tajné informace (hesla)
 - Požadavky na autentizaci uživatelů jsou přeposílány normálním řadičům domény (v hlavním místě)
- Možnost *kešovat* pověření (*credentials*) uživatelů
 - Výběr těchto uživatelů pomocí **zásad replikace hesel** (PRP, *Password Replication Policy*)
 - Normální řadiče domény monitorují, která pověření jsou *kešována* na kterých RODC řadičích
 - Možnost resetu hesel *kešovaných* pověření při odstranění účtu RODC řadiče z Active Directory

Konzistence databáze Active Directory

- RODC řadiče obsahují kopii databáze AD určenou pouze pro čtení (*read-only*)
 - Aplikace, jenž chtějí zapisovat, jsou přesměrovány na normální řadiče domény
- Jednosměrná replikace dat
 - Změny replikovány jen z normálních na RODC řadiče
 - Zabraňuje replikaci podvržených či poškozených dat
 - Týká se i systémového oddílu (adresáře SYSVOL)
 - Lze do něj zapisovat, ale data se nikdy nereplikují na jiné (normální) řadiče domény

Správa a omezení

- RODC řadiče umožňují delegovat funkci lokálního správce na doménové uživatele (nebo skupiny)
 - Vždy se týká jednoho konkrétního RODC řadiče
 - Umožňuje provádět údržbu RODC řadičů bez potřeby dát jejich správcům nadměrná oprávnění (k doméně)
- RODC řadiče nemohu být operačními servery
- Replikace může probíhat pouze z řadičů domény s alespoň Windows Server 2008
 - Starší řadiče domény neumí s RODC řadiči pracovat

RODC řadiče jako DNS servery

- Omezení u zón integrovaných v Active Directory
 - Určeny pouze pro čtení (obdoba sekundárních zón)
 - Aktualizace obsahu zón možná pouze skrz replikaci
 - Nepodporují dynamické aktualizace (*dynamic DNS*)
- Dynamické aktualizace u integrovaných zón
 - RODC řadič vrací při požadavku na aktualizace DNS záznamů klienta klientovi odkaz na jiný DNS server
 - RODC řadič si poté vyžádá DNS záznam, jenž klient aktualizoval, od tohoto cílového DNS serveru
 - Replikuje se jen aktualizovaný DNS záznam, žádné jiné

Požadavky na instalaci a příprava lesa

- Požadavky na Active Directory
 - Funkční úroveň lesa alespoň Windows Server 2003
 - Přítomnost minimálně jednoho (normálního) řadiče domény, na kterém běží Windows Server 2008
 - V případě, že RODC řadič bude plnit i funkci DNS serveru, musí jeden z těchto řadičů plni také funkci DNS serveru
- Příprava lesa Active Directory
 - Aktualizace schématu lesa AD pro možnost použití
 - Řadičů s Windows Server 2008 (**adprep /forestprep**)
 - RODC řadičů (**adprep /rodcprep**)

Instalace

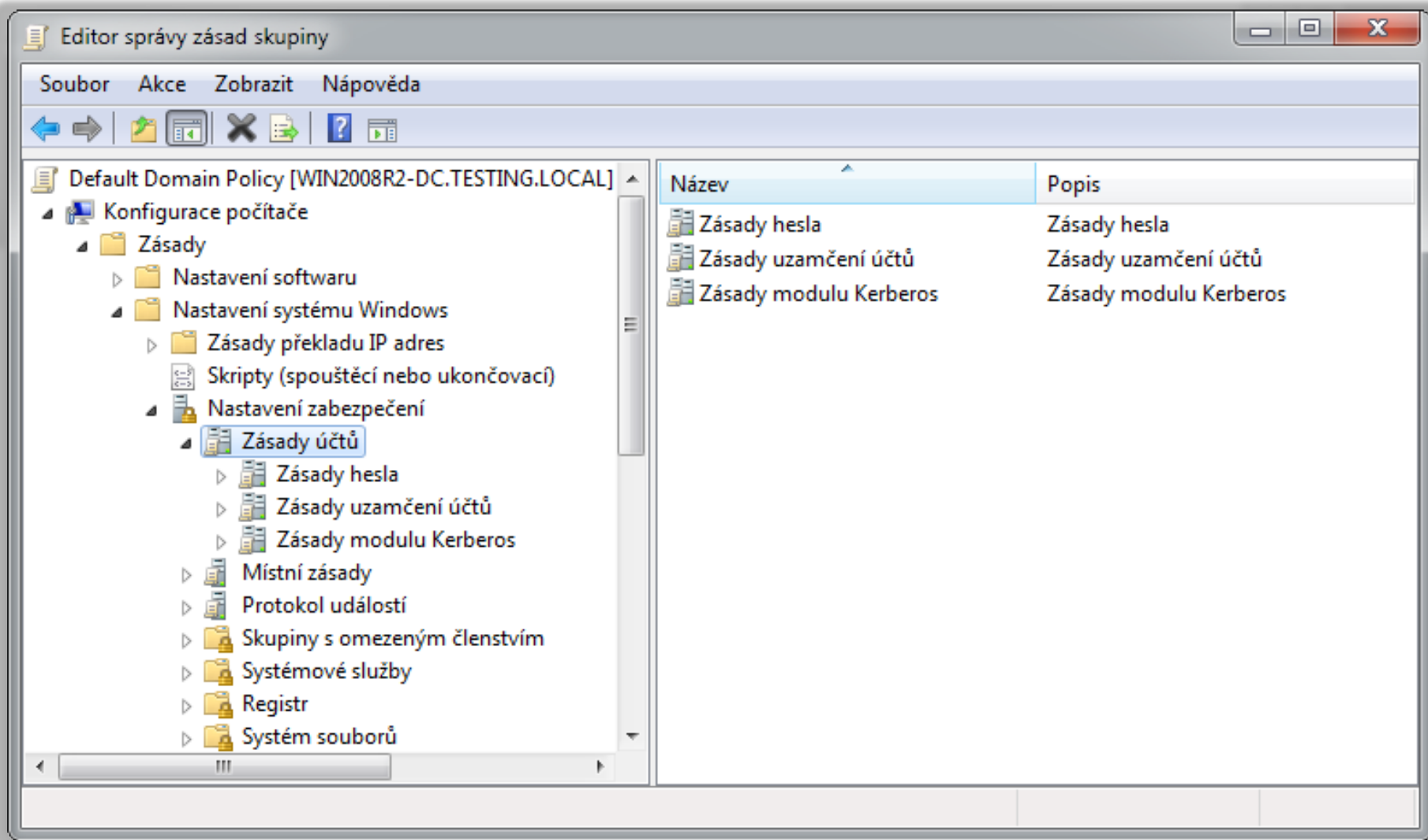
- Stejný postup jako u normálních řadičů domény
 - U standardní instalace Windows Server (2008 a vyšší)
 - Pomocí **dcpromo** (průvodce)
 - U Server Core instalace
 - Pomocí **dcpromo /unattend** (bezobslužná instalace)
- Lze delegovat i na uživatele, jenž nejsou správci domény (nejsou členy **Domain Admins**)
 - Předpřípravení účtu pro RODC řadič
 - Umístěn v organizační jednotce **Domain Controllers**
 - Specifikace účtu, jenž bude použit pro jeho připojení

Fine-grained zásady hesel

Fine-grained zásady hesel

- Umožňují nastavit zásady hesel a uzamykání účtů pro jednotlivé uživatele nebo skupiny v doméně
 - Normálně se na uživatele aplikují nastavení obsažená v GPO objektu [Výchozí zásady domény](#)
- K dispozici od Windows Server 2008
 - Vyžadují funkční úroveň domény alespoň Windows Server 2008

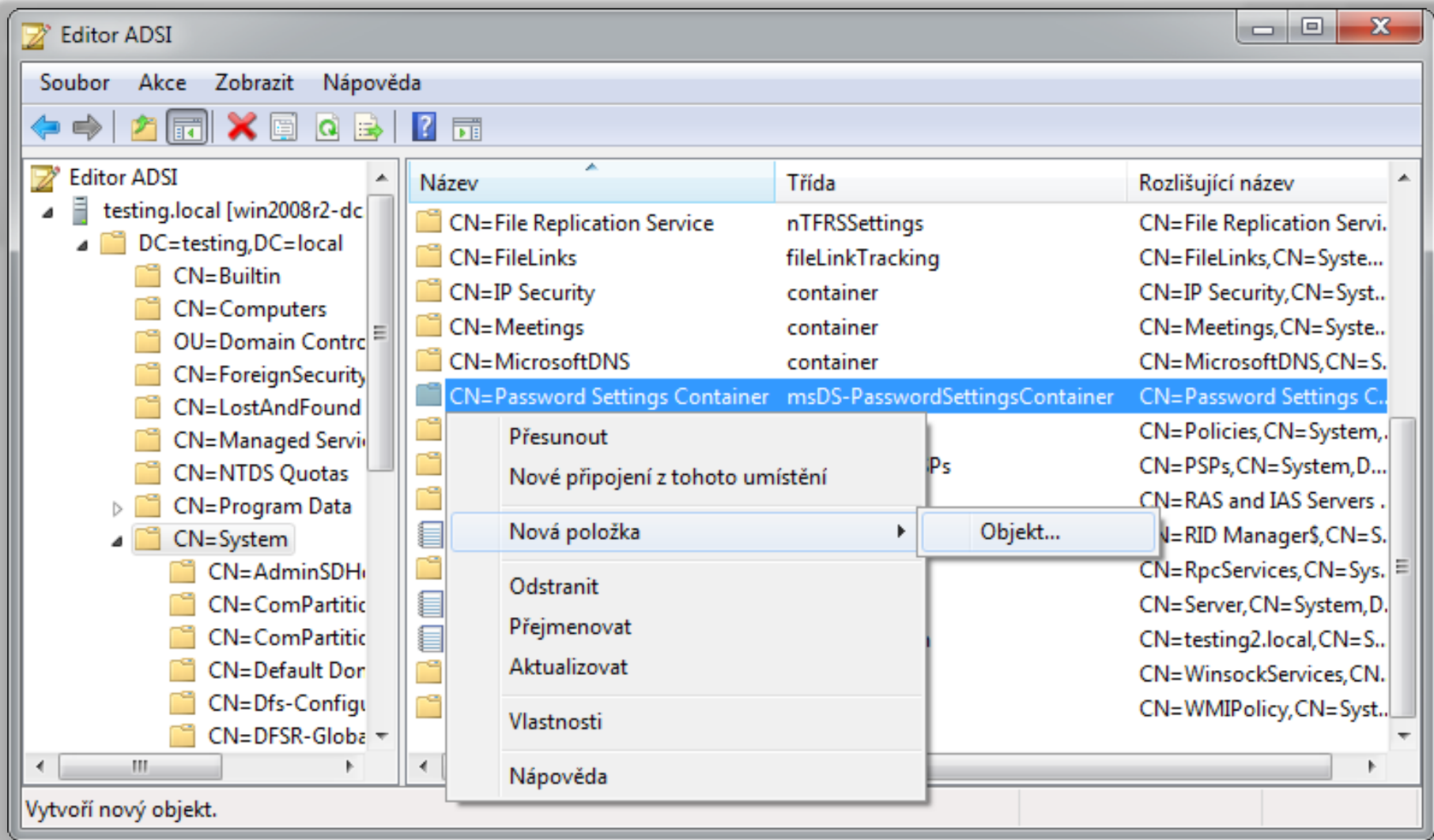
Zásady hesel a zásady uzamykání účtů



Objekty nastavení hesel (PSO)

- Objekty Active Directory, jenž obsahují nastavení zásad hesel a zásad uzamykání účtů
 - Nejsou aplikovány spolu s GPO objekty
- Mohou být připojovány k jedné či více globálním bezpečnostním skupinám nebo uživatelům
 - Nedají se připojit k organizačním jednotkám (OU)
- Vždy nedefinují veškeré zásady
 - Výsledná nastavení určuje vždy jen jediný PSO objekt

Vytvoření PSO objektu



Výsledné PSO objekty

- PSO objekty, jejichž nastavení jsou aplikována na konkrétní uživatele v doméně
 - Na každého uživatele aplikován jen jeden PSO objekt
 - Informace o tomto objektu uchována u každého uživatele ve formě atributu objektu uživatele
- Určeny na základě priority
 - Každý PSO objekt obsahuje číslo určující jeho prioritu
 - Uložena jako atribut PSO objektu (nižší číslo, vyšší priorita)
 - PSO objekty připojené k uživateli mají vyšší prioritu než PSO objekty připojené ke skupině

Určení výsledného PSO objektu

- 1) Pokud existují PSO objekty připojené k uživateli, vybere se ten s nejvyšší prioritou
 - Pokud má více PSO objektů stejnou prioritu, vybere se ten s nejnižší hodnotou GUID identifikátoru
- 2) Pokud existují PSO objekty připojené ke skupině, jenž obsahuje daného uživatele, vybere se ten s nejvyšší prioritou
 - Pokud má více PSO objektů stejnou prioritu, vybere se ten s nejnižší hodnotou GUID identifikátoru
- 3) Použije se nastavení z **Výchozích zásad domény**

Vztahy důvěry

Vztahy důvěry (*trusts*)

- Umožňují doménám důvěřovat identitám, které pocházející z jiných (i externích) domén
- Každý vztah důvěry zahrnuje právě dvě domény, důvěryhodnou doménu a důvěřující doménu
- Důvěryhodná doména (*trusted domain*)
 - Zajišťuje autentizaci (svých) identit
- Důvěřující doména (*trusting domain*)
 - Důvěřuje identitám autentizovaným důvěryhodnou doménou a umožňuje jim přístup ke svým zdrojům

Vytvoření vztahu důvěry

Domény a vztahy důvěryhodnosti služby Active Directory

Soubor Akce Zobrazit Nápověda

Domény a vztahy důvěryhodnosti služby Active Directory

testing.local

- Spravovat
- Zvýšit úroveň funkčnosti domény...
- Zobrazení
- Exportovat seznam...
- Vlastnosti**
- Nápověda

Otevře dialog vlastností pro aktuální výběr.

testing.local – vlastnosti

Obecné Vztahy důvěryhodnosti Správce objektu

Domény, kterým tato doména důvěřuje:

Název domény	Typ důvěryhodnosti	Přenositelný
--------------	--------------------	--------------

Vlastnosti...
Odebrat

Domény důvěřující této doméně:

Název domény	Typ důvěryhodnosti	Přenositelný
--------------	--------------------	--------------

Vlastnosti...
Odebrat

Nový vztah důvěryhodnosti...

OK Storno Použít Nápověda

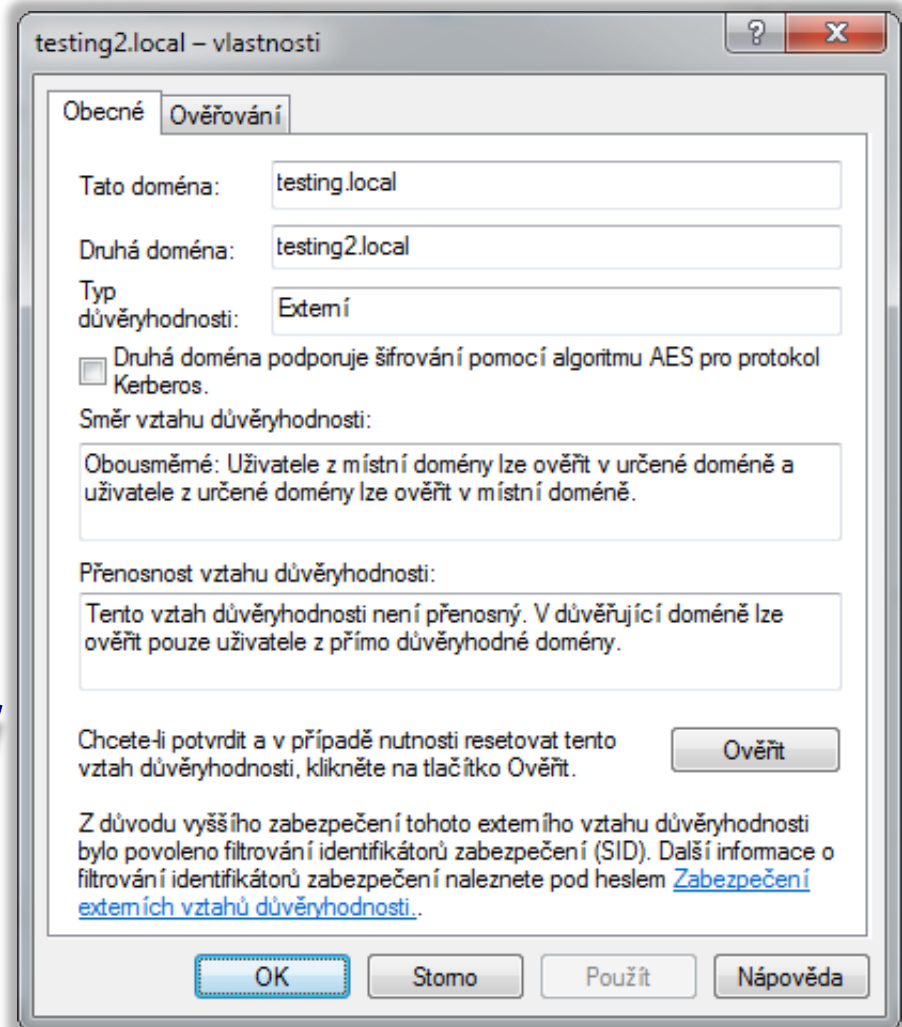
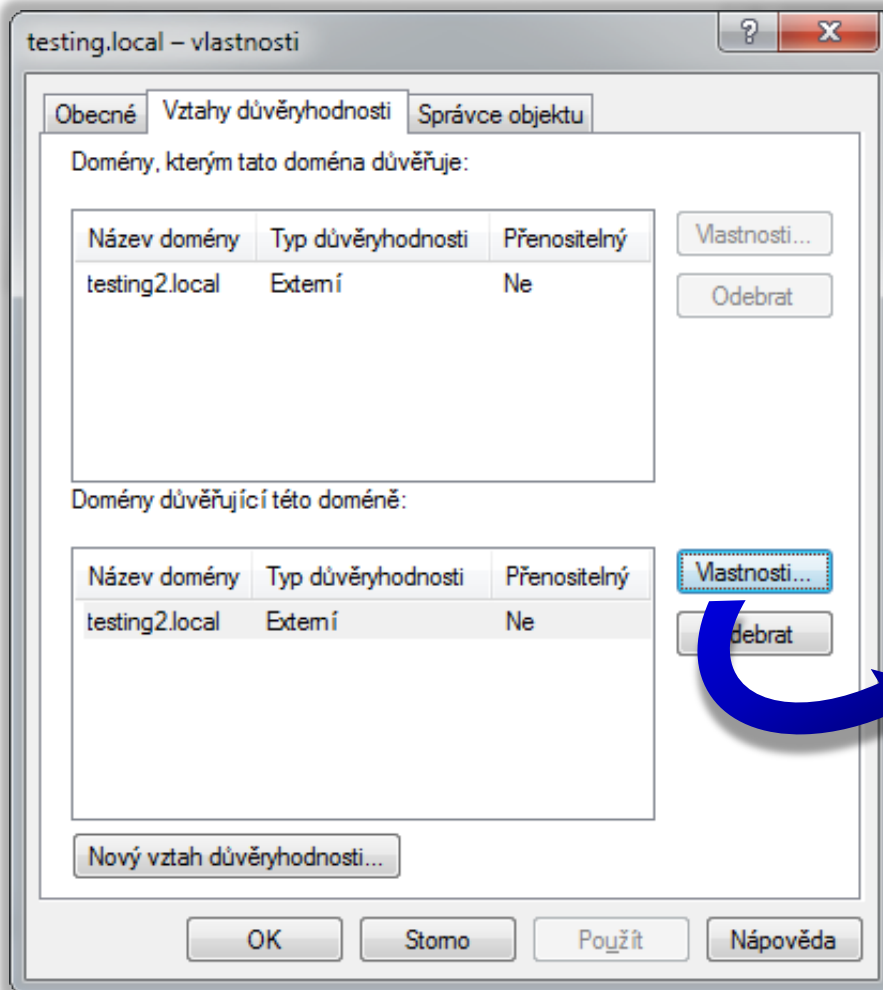
Možnosti identit v důvěřující doméně

- Identity
 - Mohou přistupovat ke zdrojům
- Uživatelé
 - Lze jim přidělovat práva (*rights*)
 - Mohou se přihlašovat na počítače
 - ...
- Uživatelé a globální (bezpečnostní) skupiny
 - Mohou být přidáváni do ACL seznamů zdrojů
 - ...

Základní vlastnosti vztahů důvěry

- Tranzitivita
 - Každý vztah důvěry může nebo nemusí být tranzitivní
 - Mějme domény **A**, **B** a **C**. Pokud **A** důvěřuje **B** a **B** zase **C** a pokud jsou oba tyto vztahy důvěry tranzitivní, tak platí také, že **A** důvěřuje **C**
- Směr
 - Každý vztah důvěry může být jednosměrný (*one-way*) nebo obousměrný (*two-way*)
 - V případě obousměrného vztahu jsou obě obsažené domény zároveň důvěryhodné i důvěřující

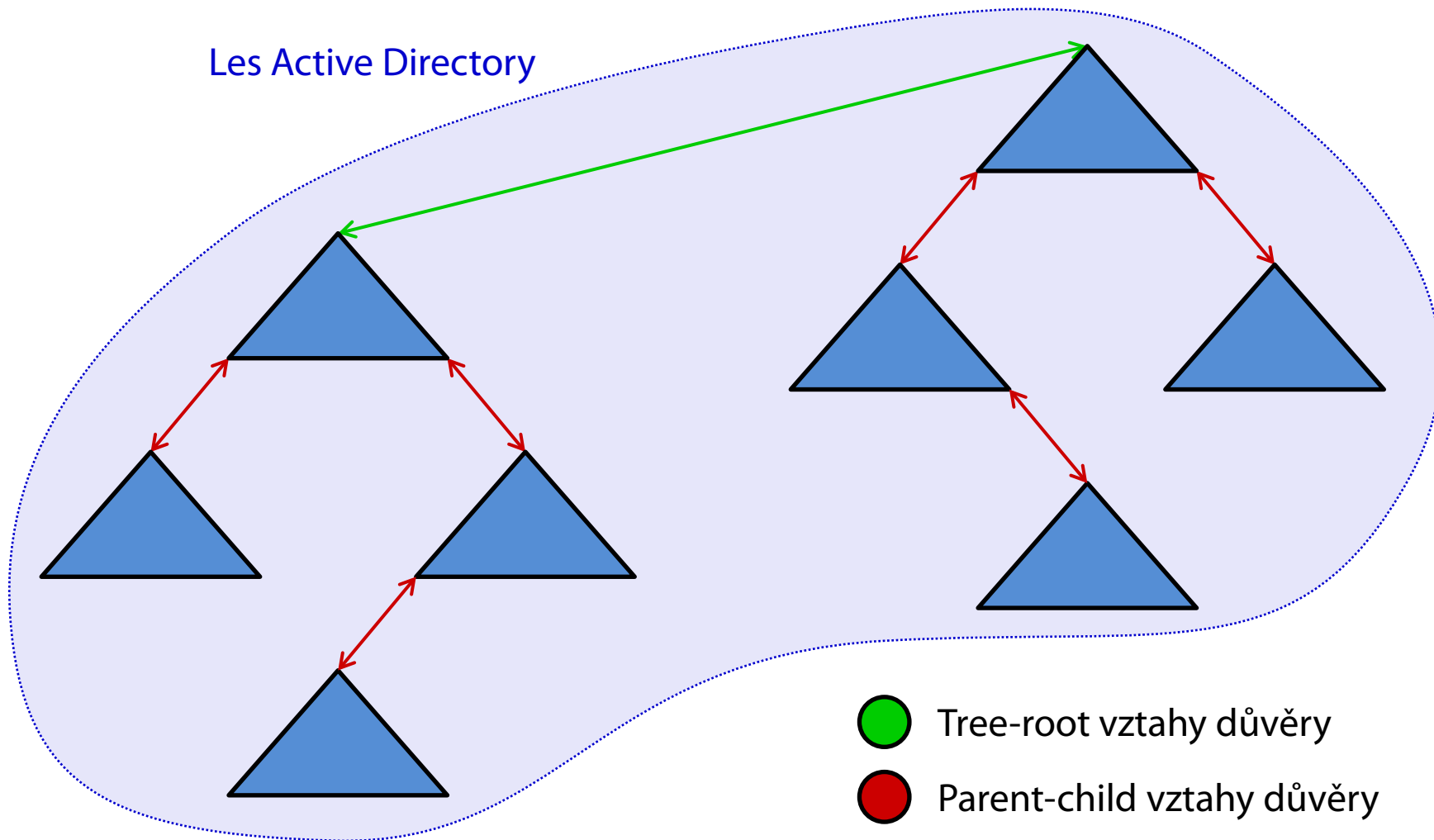
Vlastnosti vztahu důvěry



Vztahy důvěry v lese Active Directory

- Kořenová doména každého doménového stromu důvěřuje kořenové doméně lesa
- Podřízená (*child*) doména každého doménového stromu důvěřuje nadřízené (*parent*) doméně
- Všechny vztahy důvěry jsou tranzitivní a zároveň obousměrné
 - Každá doména lesa důvěřuje všem ostatním
 - Vytvářeny automaticky při vytváření domén

Ilustrace vztahů důvěry v lese



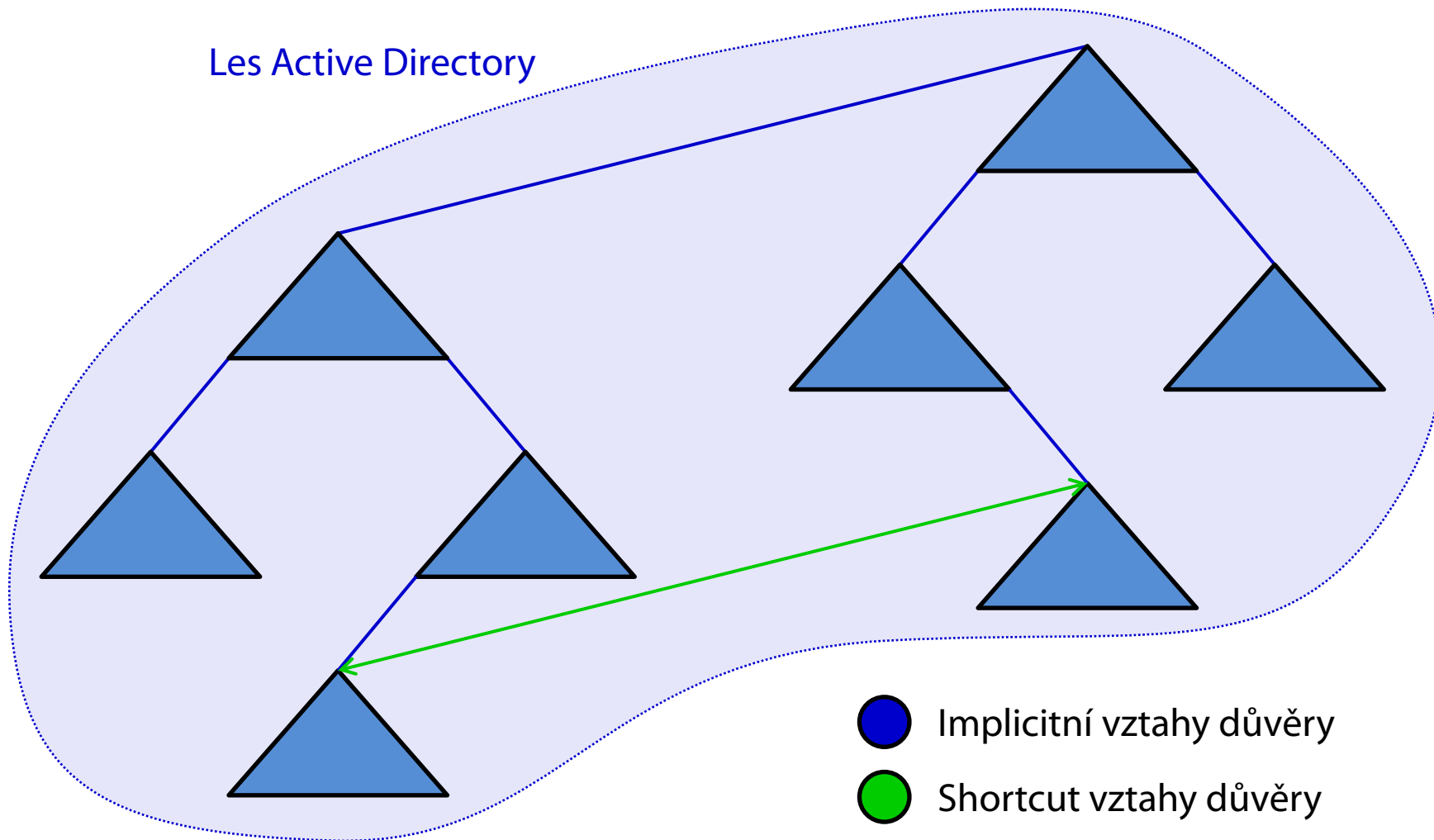
Manuálně vytvářené vztahy důvěry

- Celkem 4 typy vztahů důvěry
 - Shortcut
 - External
 - Realm
 - Forest
 - Od funkční úrovně lesa [Windows Server 2003](#) výše
- Vytváření a nastavení v konzoli [Domény a vztahy důvěryhodnosti služby Active Directory](#)

Shortcut vztahy důvěry

- Vlastnosti
 - Jednosměrné i obousměrné
 - Vždy tranzitivní
- Důvěra mezi
 - Doménami ze stejného lesa
- Použití
 - Urychlení přístupu ke zdrojům z jiné domény v lese
 - Není potřeba vyhodnocovat všechny tranzitivní vztahy na cestě z důvěřující domény do důvěryhodné domény
 - Ověření pouze jediného vztahu důvěry namísto celé cesty

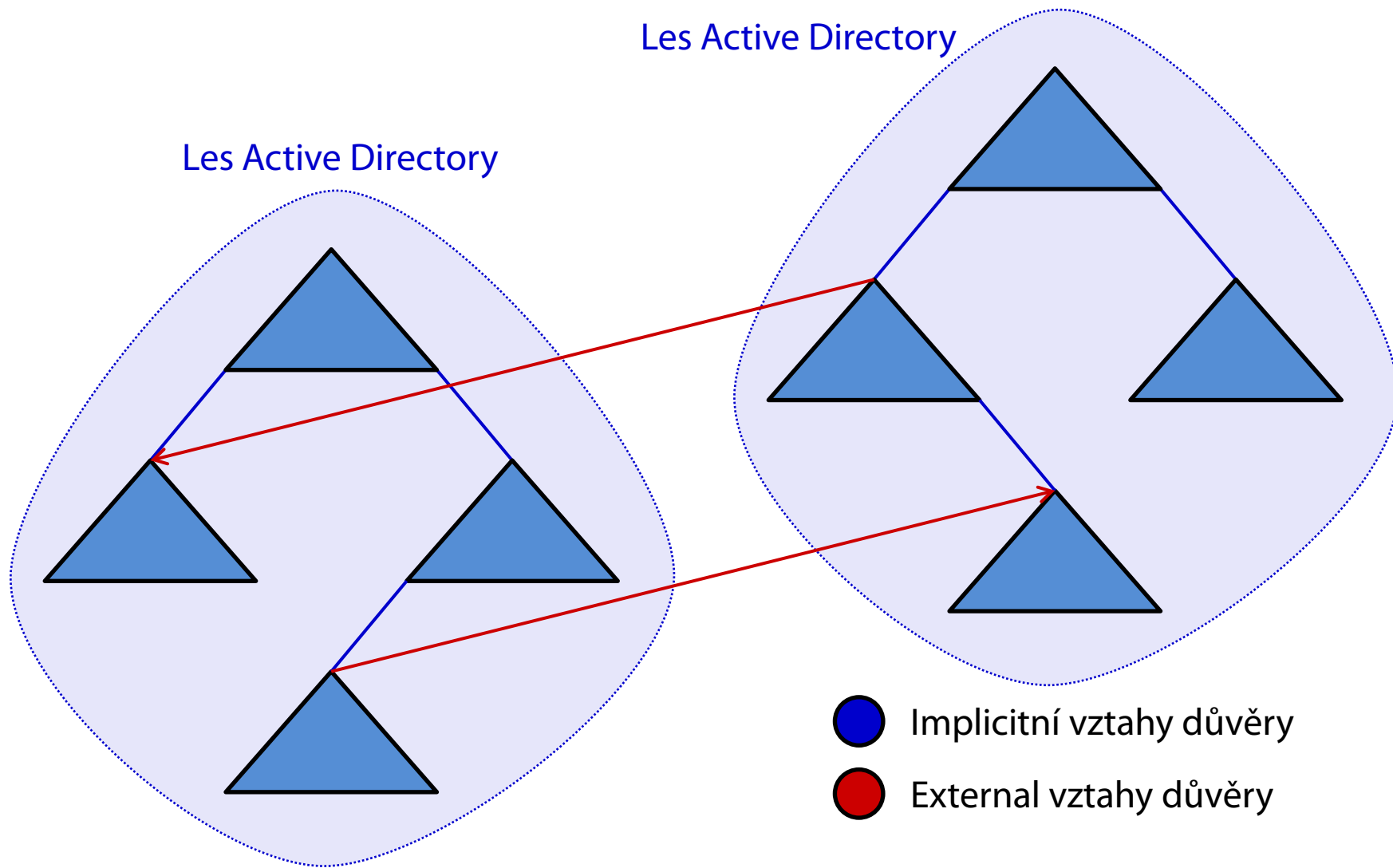
Ilustrace shortcut vztahů důvěry



External vztahy důvěry

- Vlastnosti
 - Jednosměrné
 - Nejsou tranzitivní
- Důvěra mezi
 - Doménami různých lesů
- Použití
 - Spolupráce s externími doménami systému Windows
 - Vytvoření cizích identit pro každou identitu z důvěryhodné domény (mohou být přidávány do ACL seznamů zdrojů)
 - Lze využít výběrovou autentizaci a doménovou karanténu

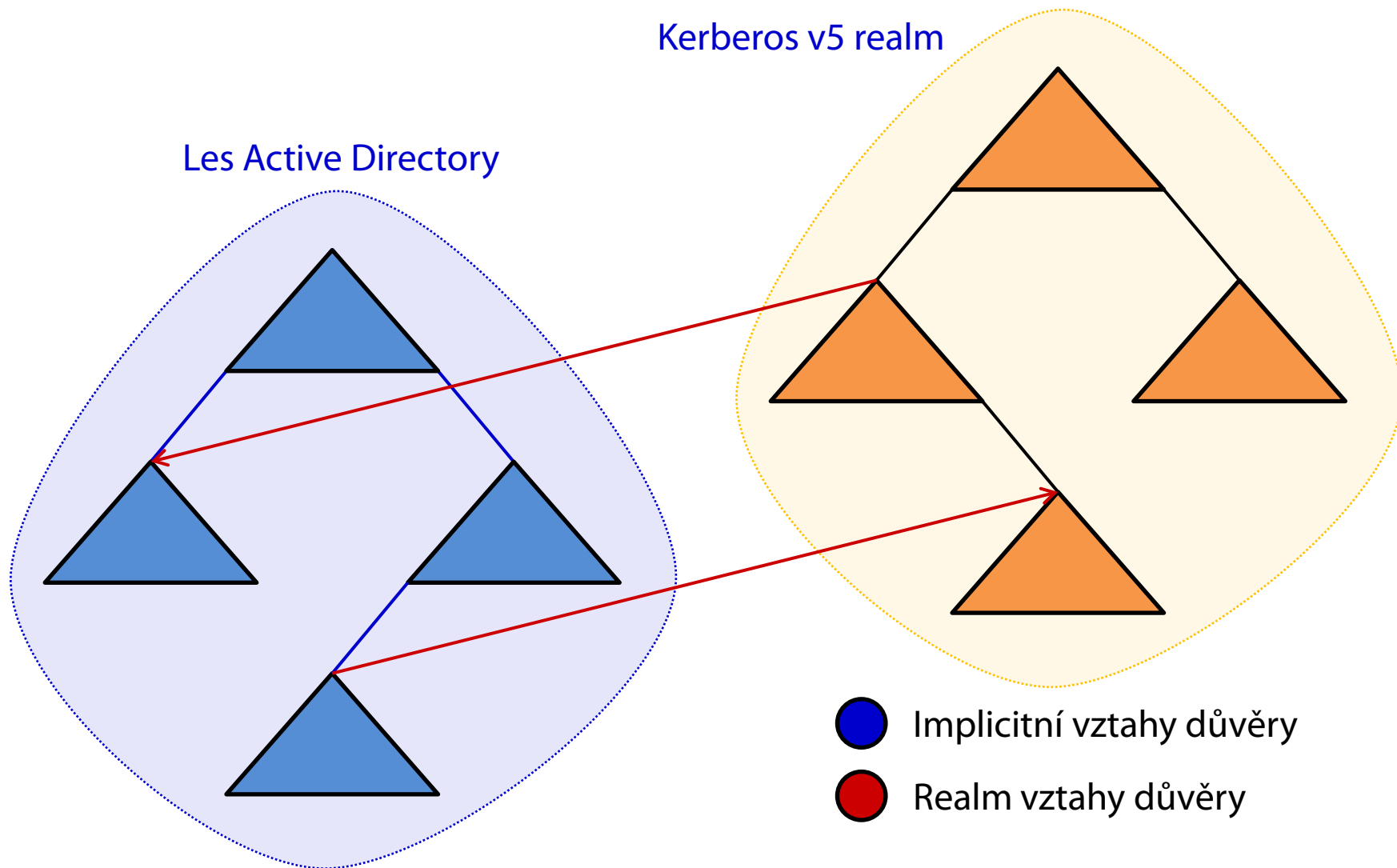
Ilustrace external vztahů důvěry



Realm vztahy důvěry

- Vlastnosti
 - Jednosměrné
 - Nejsou tranzitivní (lze je ovšem tranzitivními učinit)
- Důvěra mezi
 - Bezpečnostními službami založenými na protokolu Kerberos v5
- Použití
 - Spolupráce s jinými implementacemi řešení identity a přístupu než je Active Directory (např. FreeIPA pro systémy Linux/UNIX)

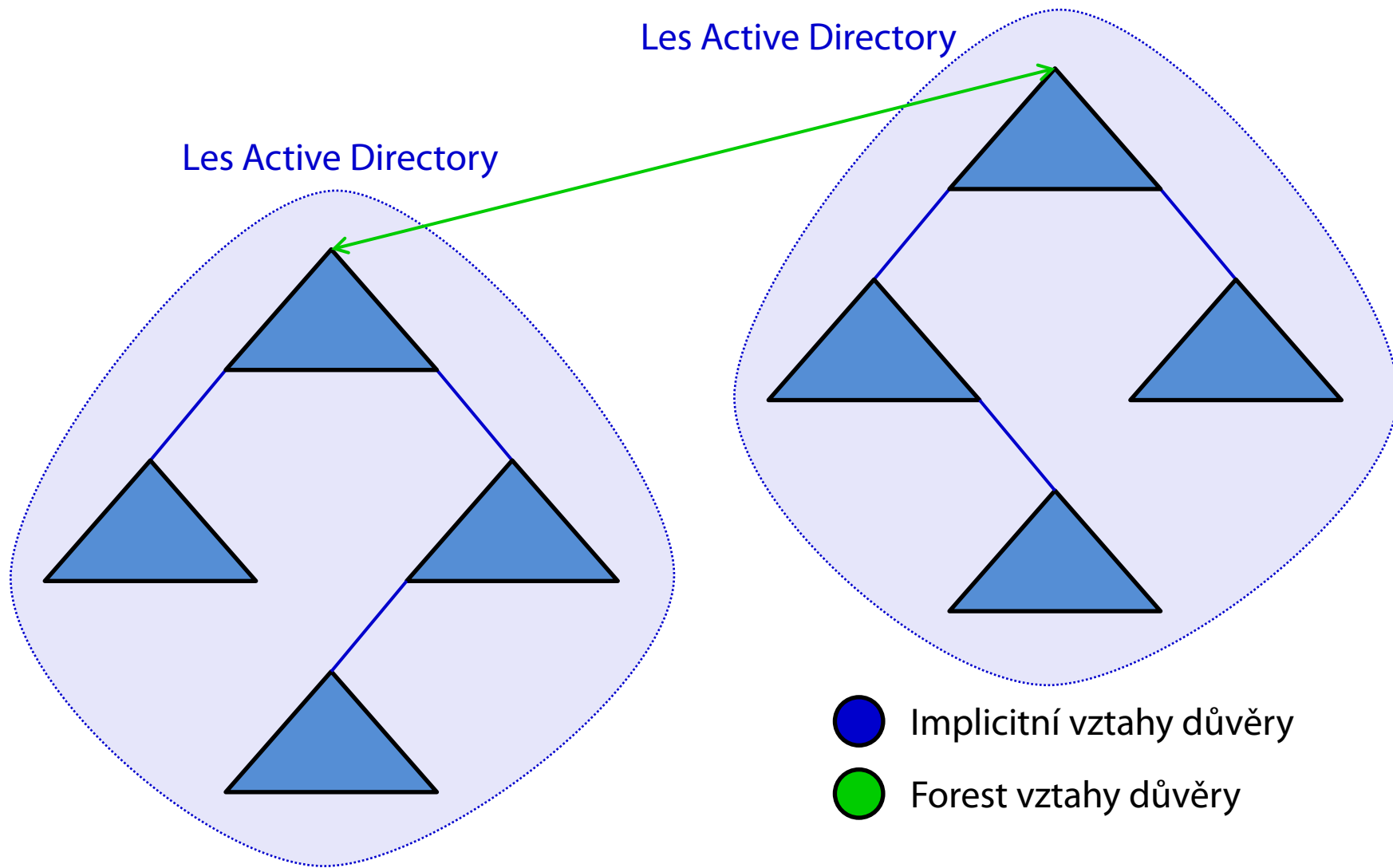
Ilustrace realm vztahů důvěry



Forest vztahy důvěry

- Vlastnosti
 - Jednosměrné i obousměrné
 - Vždy tranzitivní (ale pouze v rámci domén obou lesů)
 - Nejsou tranzitivní navzájem (pokud les **A** důvěřuje lesu **B** a les **B** zase lesu **C**, tak neplatí, že les **A** důvěřuje také lesu **C**)
- Důvěra mezi
 - Lesy (kořenovými doménami lesů)
- Použití
 - Spolupráce mezi dvěma organizacemi
 - Vyžaduje správné nastavení systému DNS

Ilustrace forest vztahů důvěry



Doménová karanténa

- Zajišťuje ignorování SID identifikátorů uživatele, které nepocházejí z důvěryhodné domény
 - Chrání proti nebezpečí podstrčení SID identifikátorů důležitých účtů (např. správců) z důvěřující domény
- Podstrčení SID identifikátorů
 - Vložení SID identifikátorů do SID historie uživatele
 - Uživatel se autorizuje SID identifikátorem ze své SID historie (např. SID správce domény) namísto svým
- Ve výchozím nastavení povolena na všech *forest* a *external* vztazích důvěry

Nastavení doménové karantény

- **Povolení / zakázání** doménové karantény
 - `netdom trust <důvěřující> /domain:<důvěryhodná> /quarantine:{ yes | no } /userD:<jméno> /passwordD:<heslo>`

Parametry pro identifikaci vztahu důvěry

<důvěřující>	Název důvěřující (<i>trusting</i>) domény v cílovém vztahu důvěry
<důvěryhodná>	Název důvěryhodné (<i>trusted</i>) domény v cílovém vztahu důvěry

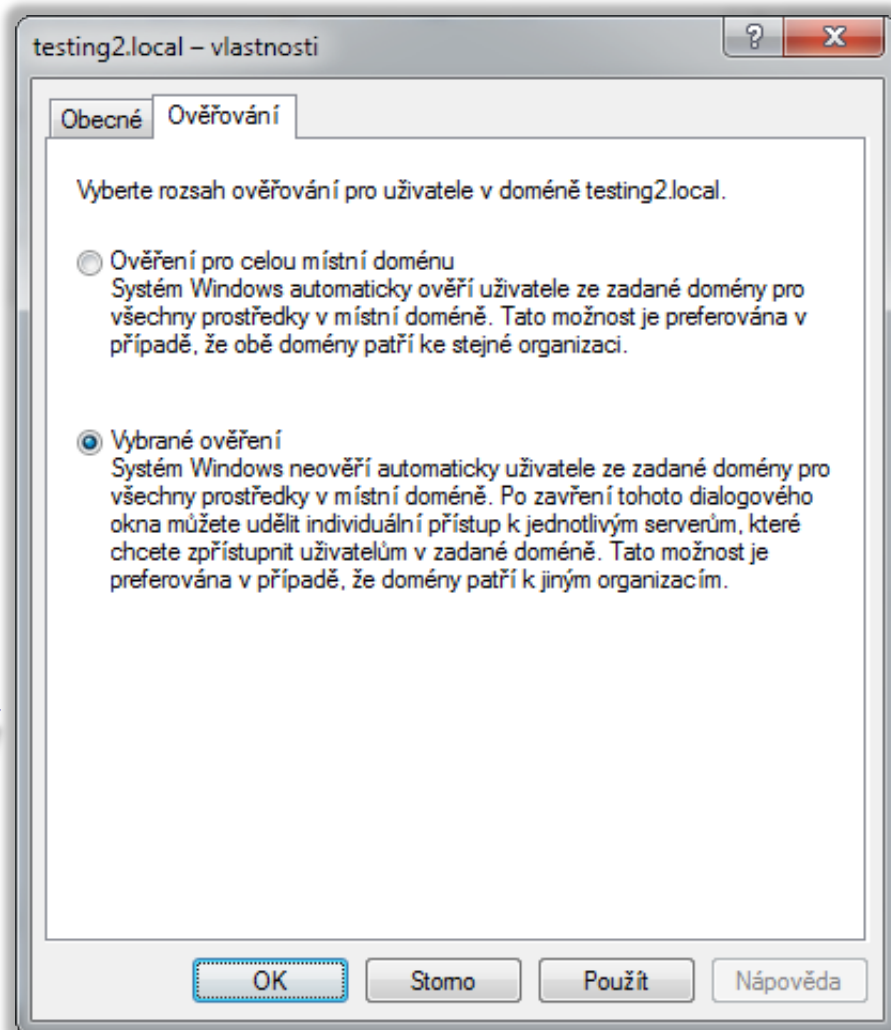
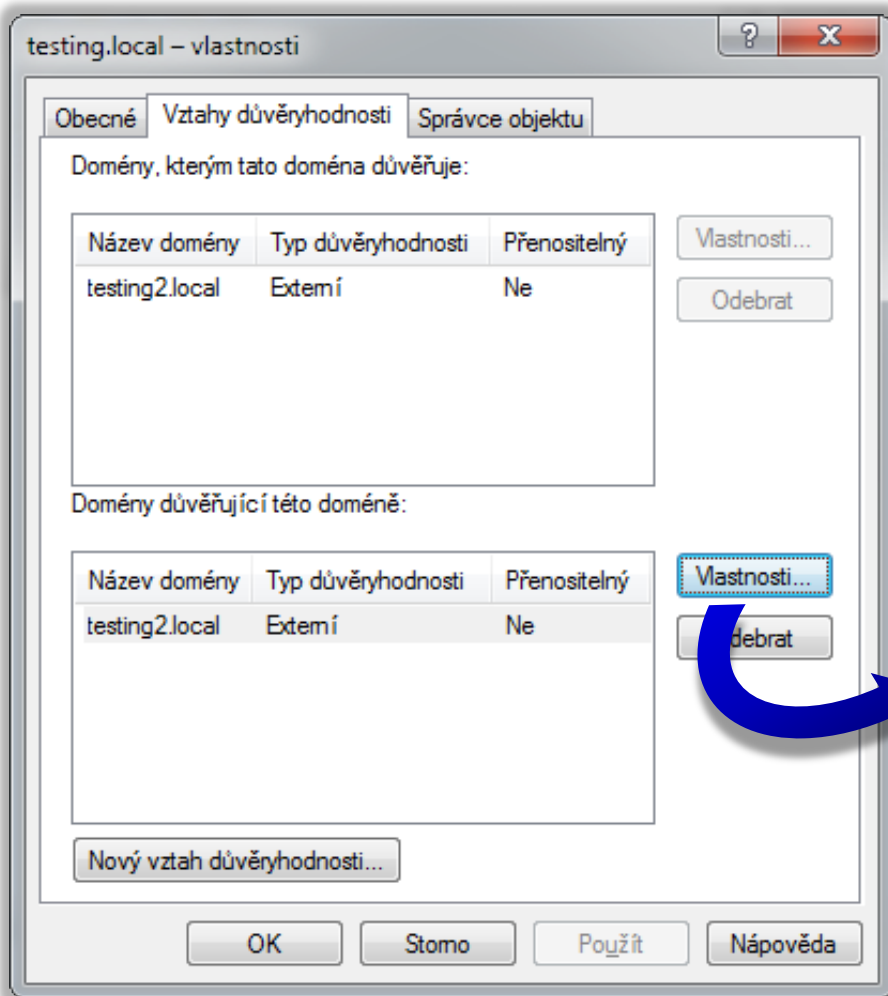
Parametry pro spojení s důvěryhodnou doménou daného vztahu důvěry

<jméno>	Uživatelské jméno správce z důvěryhodné domény
<heslo>	Heslo správce z důvěryhodné domény

Selektivní autentizace

- Umožňuje specifikovat uživatele a skupiny, kteří mohou využívat služby na konkrétním počítači
 - Specifikace přiřazením oprávnění **Ověření povoleno** (*Allowed to authenticate*) uživateli nebo skupině na konkrétním účtu počítače
- Pokud uživatel nemůže využívat služby počítače
 - Nemůže se na něj přihlásit
 - Nemůže přistupovat k jeho zdrojům a to i v případě, že má potřebná oprávnění pro tento přístup
- Lze povolit na *external* a *forest* vztazích důvěry

Povolení selektivní autentizace



Nastavení oprávnění pro autentizaci

The image shows two windows from the Windows Server 2008 R2 Active Directory console. The left window, titled 'Uživatelé a počítače služby Active Directory', displays a tree view of the directory structure. The 'Domain Controllers' folder is expanded, and 'WIN2008R2-DC' is selected. A context menu is open over the selected item, with the 'Vlastnosti' (Properties) option highlighted. A blue arrow points from this option to the right window.

The right window, titled 'WIN2008R2-DC - vlastnosti', shows the 'Zabezpečení' (Security) tab. The 'Název skupiny nebo jméno uživatele:' list contains several entries, including 'Authenticated Users'. Below this list, the 'Oprávnění pro Authenticated Users' section is visible. The 'Ověření povoleno' (Authentication allowed) checkbox is checked, and it is circled in blue. Other permissions like 'Vytvářet všechny podřízené objekty' and 'Odstraňovat všechny podřízené objekty' are unchecked. At the bottom of the dialog, there are buttons for 'OK', 'Storno', 'Použít', and 'Nápověda'.