

Serverové systémy Microsoft Windows

IW2/XMW2 2020/2021

Peter Solár

solar@aps-brno.cz

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně
Božetěchova 2, 612 66 Brno

Revize 12. 4. 2021

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 rozprostření řadičů domény

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

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 po **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 plnit 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

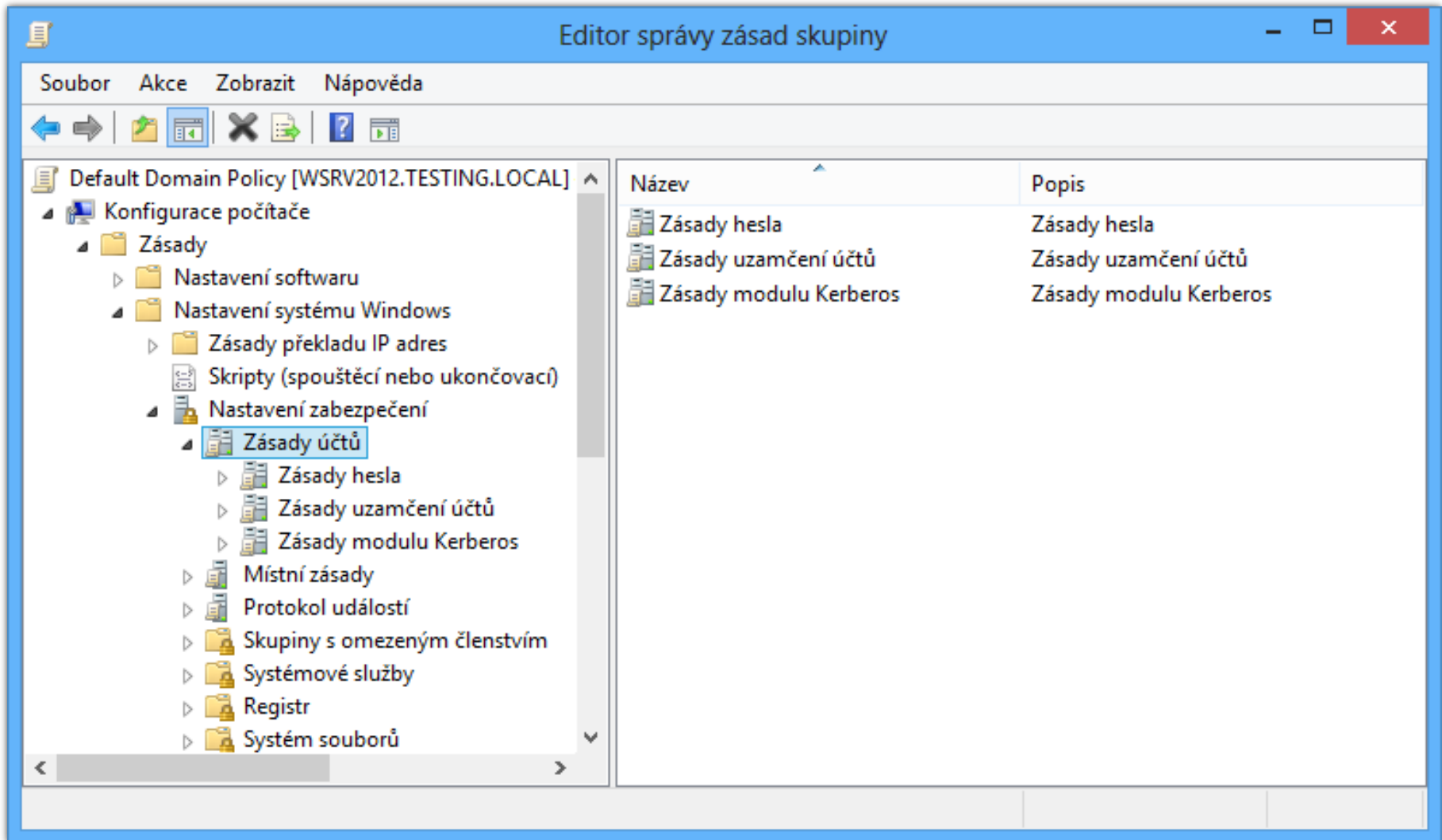
- **Stejný postup** jako u normálních řadičů domény
 - 1) Instalace **Doménových služeb Active Directory**
 - 2) Povýšení serveru do role read-only řadiče domény
 - Pomocí nástroje **Správce serveru** (*Server Manager*)
 - Pomocí nástrojů pro **Windows PowerShell** (*cmdletů*)
- Lze **delegovat** i na uživatele, jenž **nejsou** správci domény (nejsou členy **Domain Admins**)
 - **Předpřípravení** účtu pro RODC řadič domény
 - 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 **uživatelé** 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



Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TESTING.LOCAL]

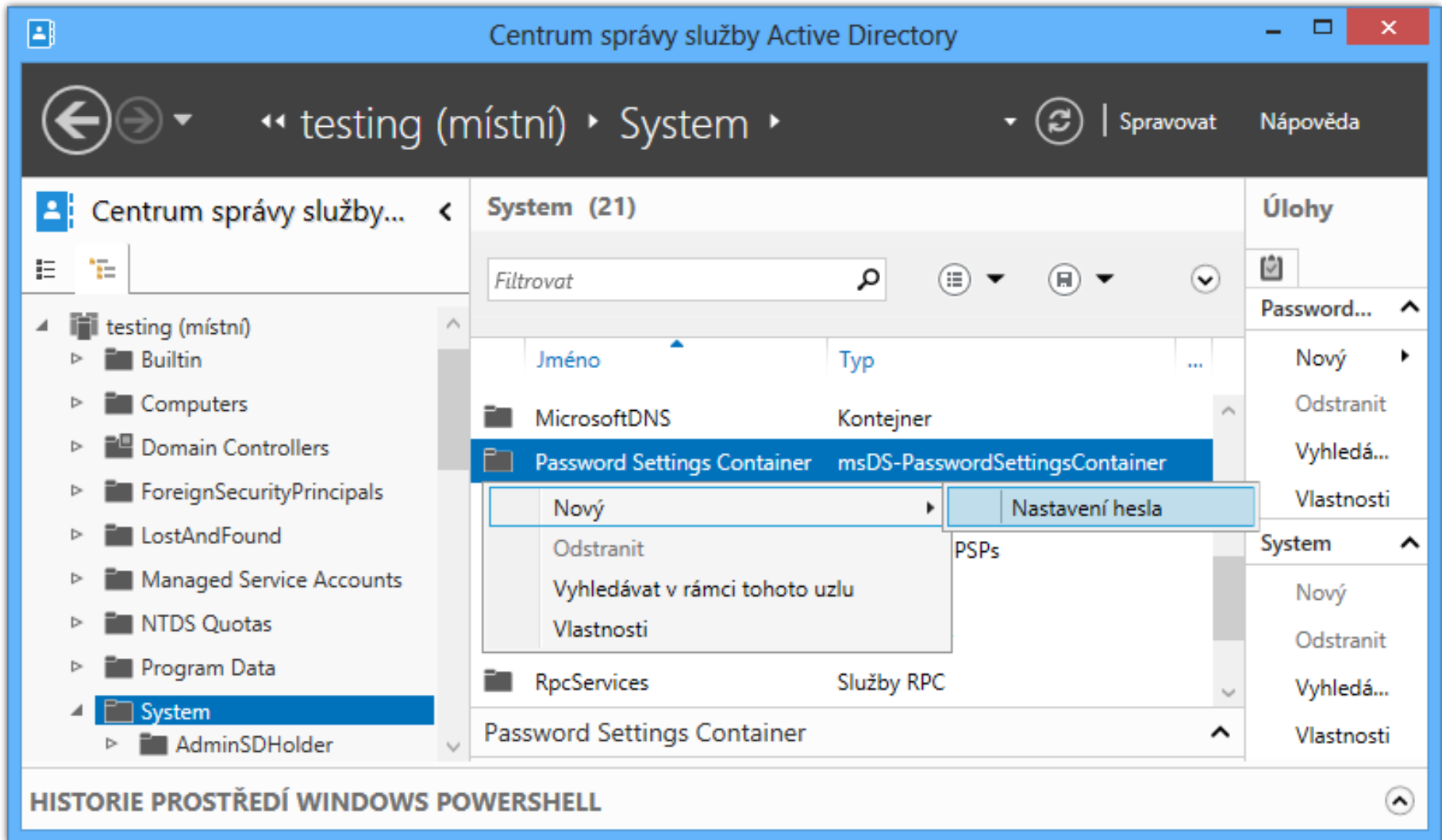
- Konfigurace počítače
 - Zásady
 - Nastavení softwaru
 - Nastavení systému Windows
 - Zásady překladu IP adres
 - Skripty (spouštěcí nebo ukončovací)
 - Nastavení zabezpečení
 - Zásady účtů**
 - Zásady hesla
 - Zásady uzamčení účtů
 - Zásady modulu Kerberos
 - Místní zásady
 - Protokol událostí
 - Skupiny s omezeným členstvím
 - Systémové služby
 - Registr
 - Systém souborů

Název	Popis
Zásady hesla	Zásady hesla
Zásady uzamčení účtů	Zásady uzamčení účtů
Zásady modulu Kerberos	Zásady modulu Kerberos

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 definují **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 uchovány u každého uživatele ve formě **atributu** objektu uživatele **msDS-ResultantPSO**
- 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 pocházejí 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** jinou (**důvěryhodnou**) doménou a umožňuje jim **přístup** ke svým **prostředkům**

Vytvoření vztahu důvěry

The image shows two overlapping windows from the Windows Server management console. The left window, titled "Domény a vztahy důvěry", displays a tree view of domains with "testing.local" selected. A context menu is open over "testing.local", with "Vlastnosti" (Properties) highlighted. A large blue arrow points from this menu item to the right window. The right window, titled "testing.local – vlastnosti", shows the "Vztahy důvěryhodnosti" (Trust Relationships) tab. It contains two empty tables for listing trusted domains and domains trusted by the current one. At the bottom of this window, the "Nový vztah důvěryhodnosti..." (New Trust Relationship...) button is highlighted with a blue box. The status bar at the bottom of the left window reads "Otevře dialog vlastností pro aktuální výběr." (Opens the properties dialog for the current selection.)

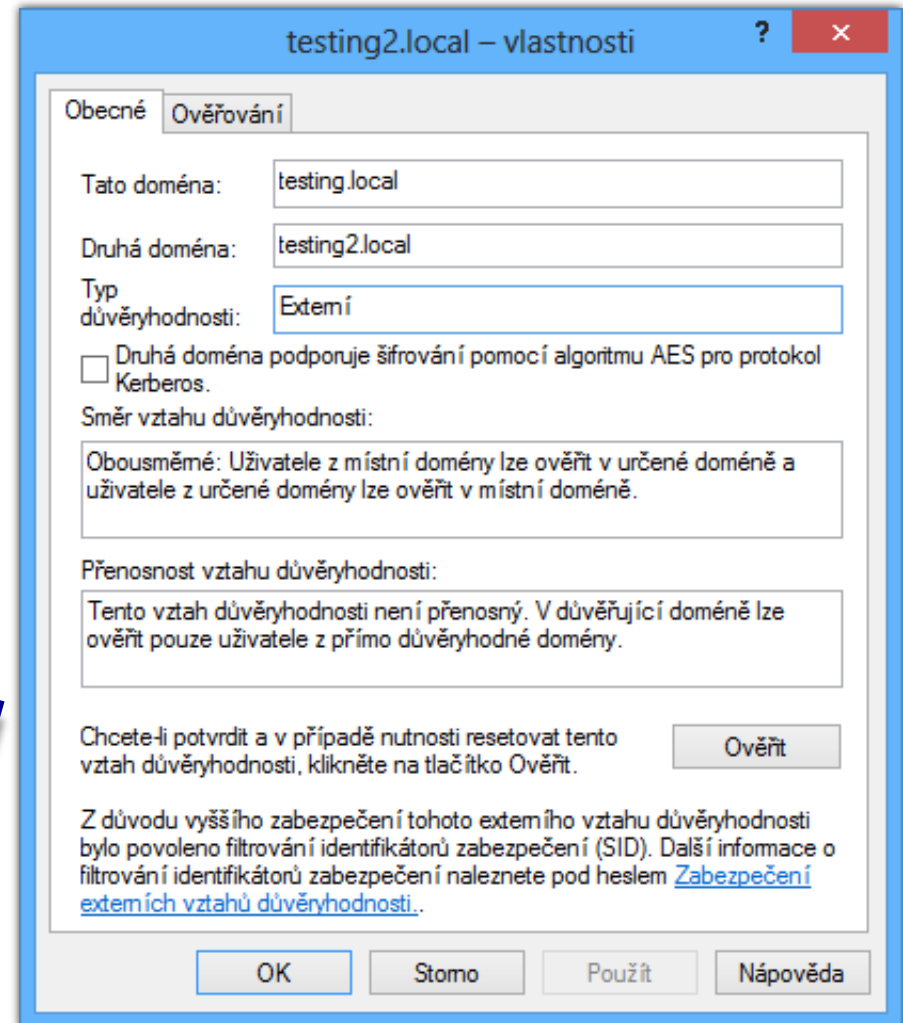
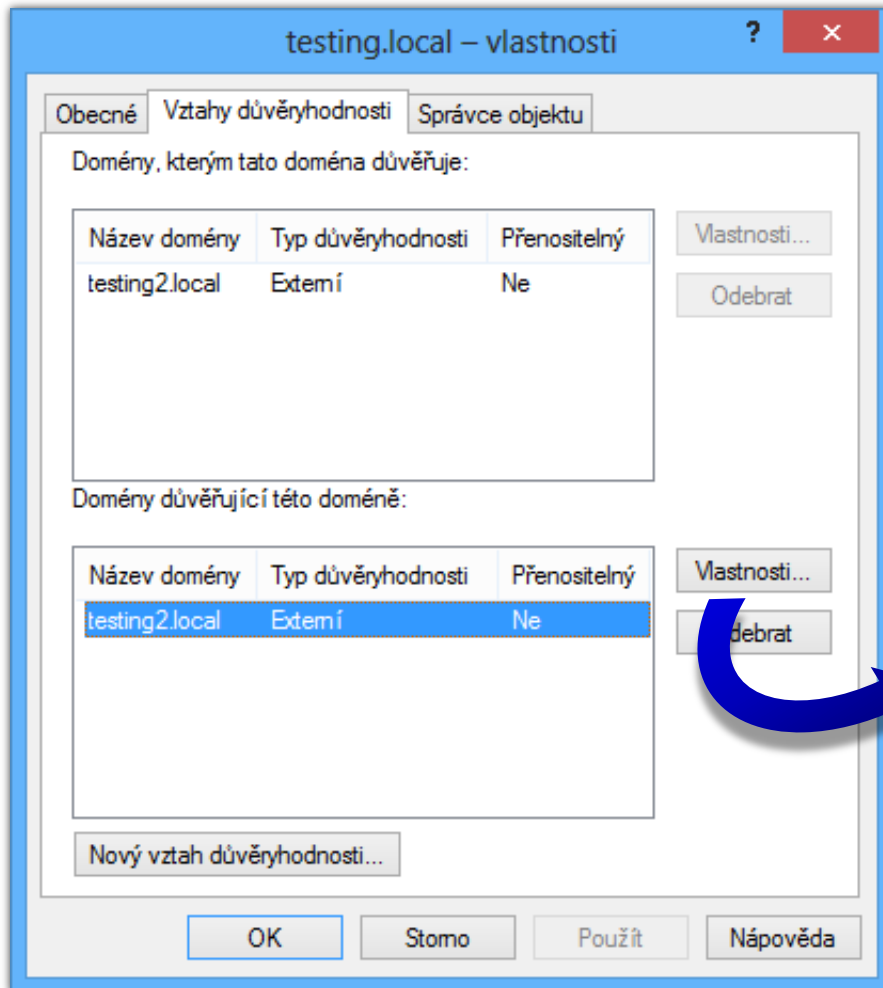
Možnosti identit v důvěřující doméně

- Identity
 - Mohou přistupovat k **prostředkům**
- Uživatelé
 - Lze jim přidělovat **práva** (*rights*)
 - Mohou se **přihlašovat** na počítače
 - ...
- Uživatelé a globální (bezpečnostní) skupiny
 - Lze je přidávat do **ACL seznamů** prostředků
 - ...

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**

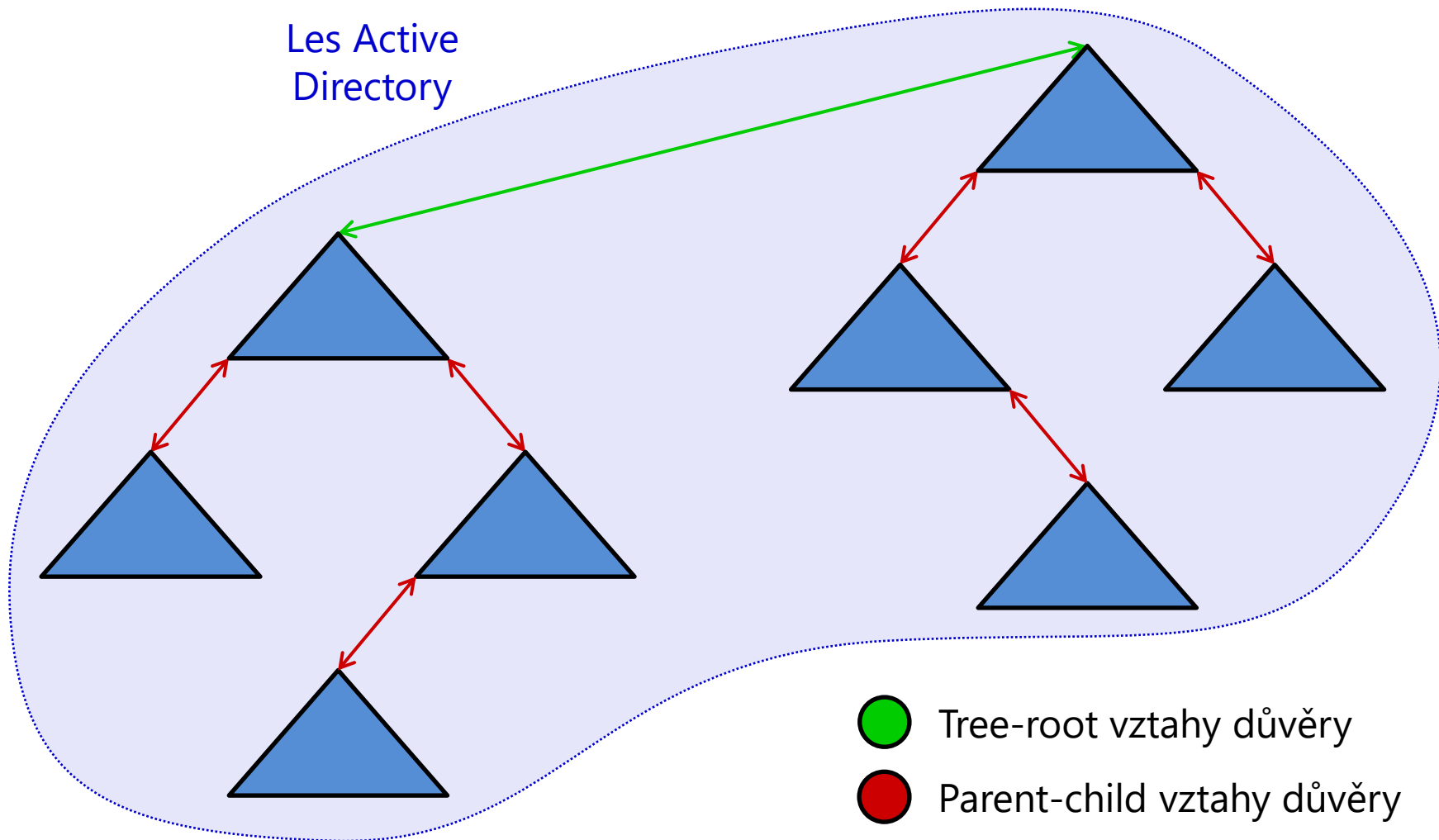
Zobrazení vlastností vztahu důvěry



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



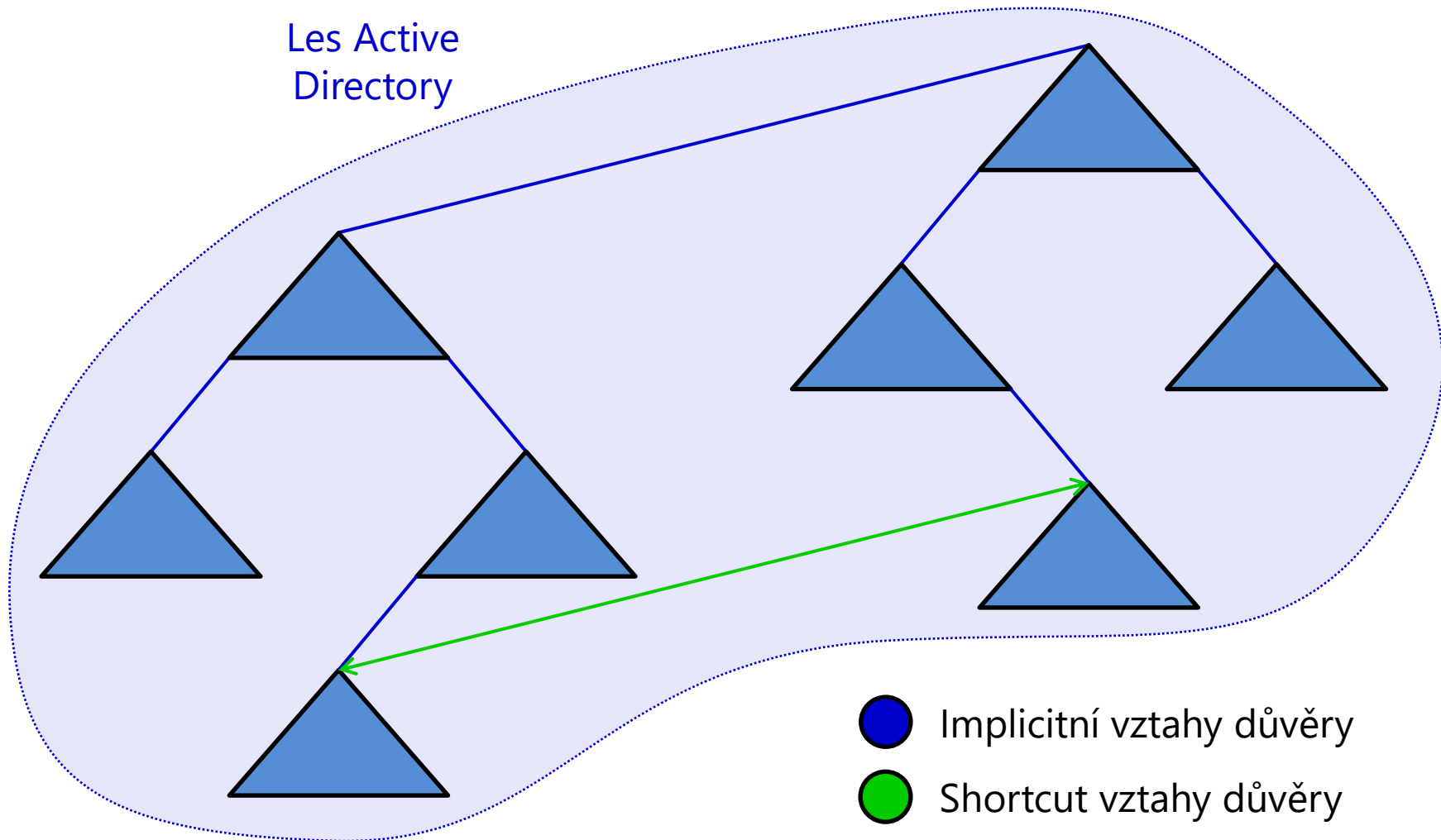
Manuálně vytvářené vztahy důvěry

- 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** k prostředkům z jiné domény lesa
 - Není potřeba vyhodnocovat všechny tranzitivní vztahy na cestě z důvěřující domény do důvěryhodné domény
 - Ověření pouze jediného vztahu důvěry namísto celé cesty

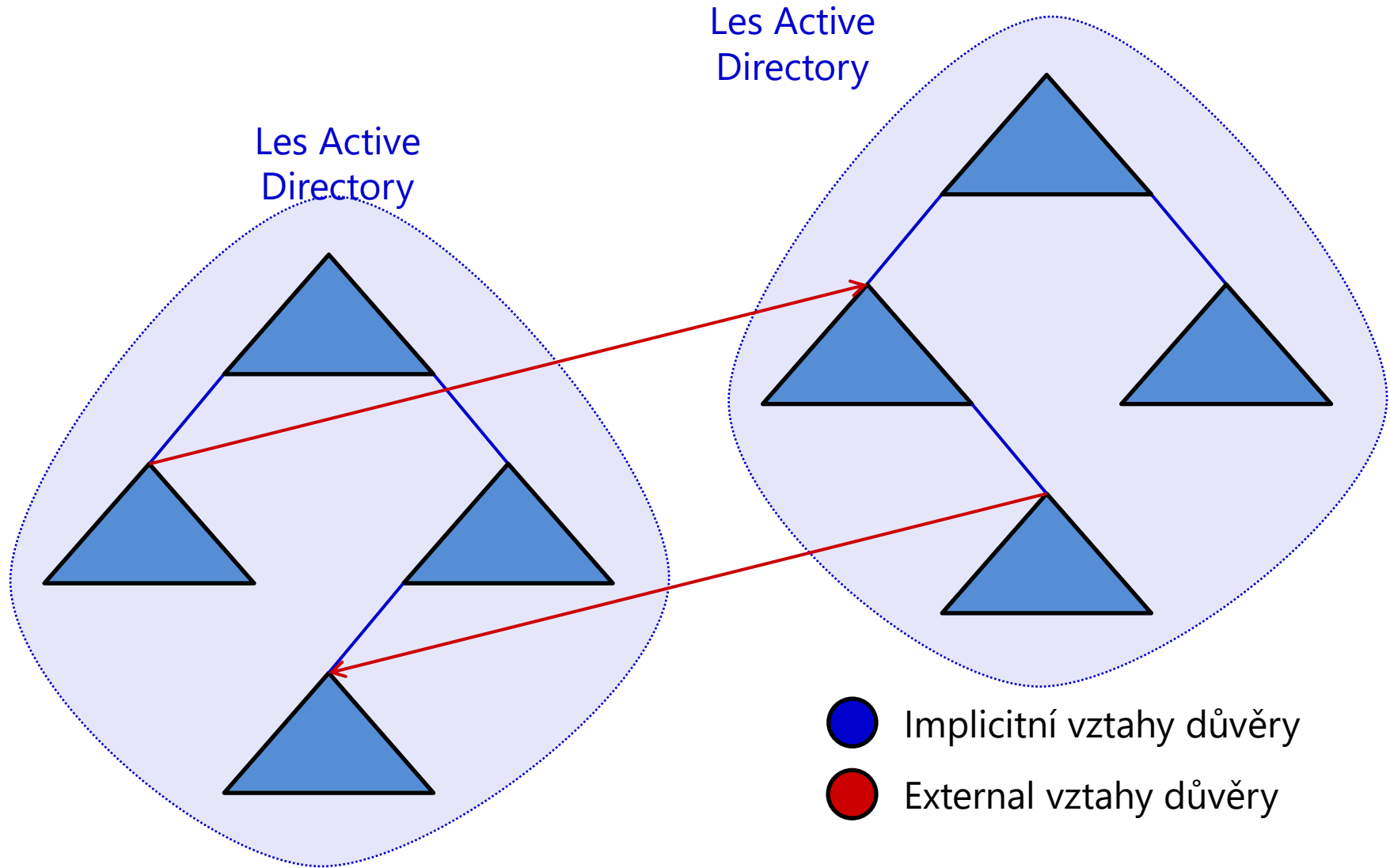
Ilustrace shortcut vztahů důvěry



External vztahy důvěry

- Vlastnosti
 - Jednosměrné i obousměrné
 - 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 použity v ACL seznamech prostředků)
 - Lze využít **výběrovou autentizaci** a **doménovou karanténu**

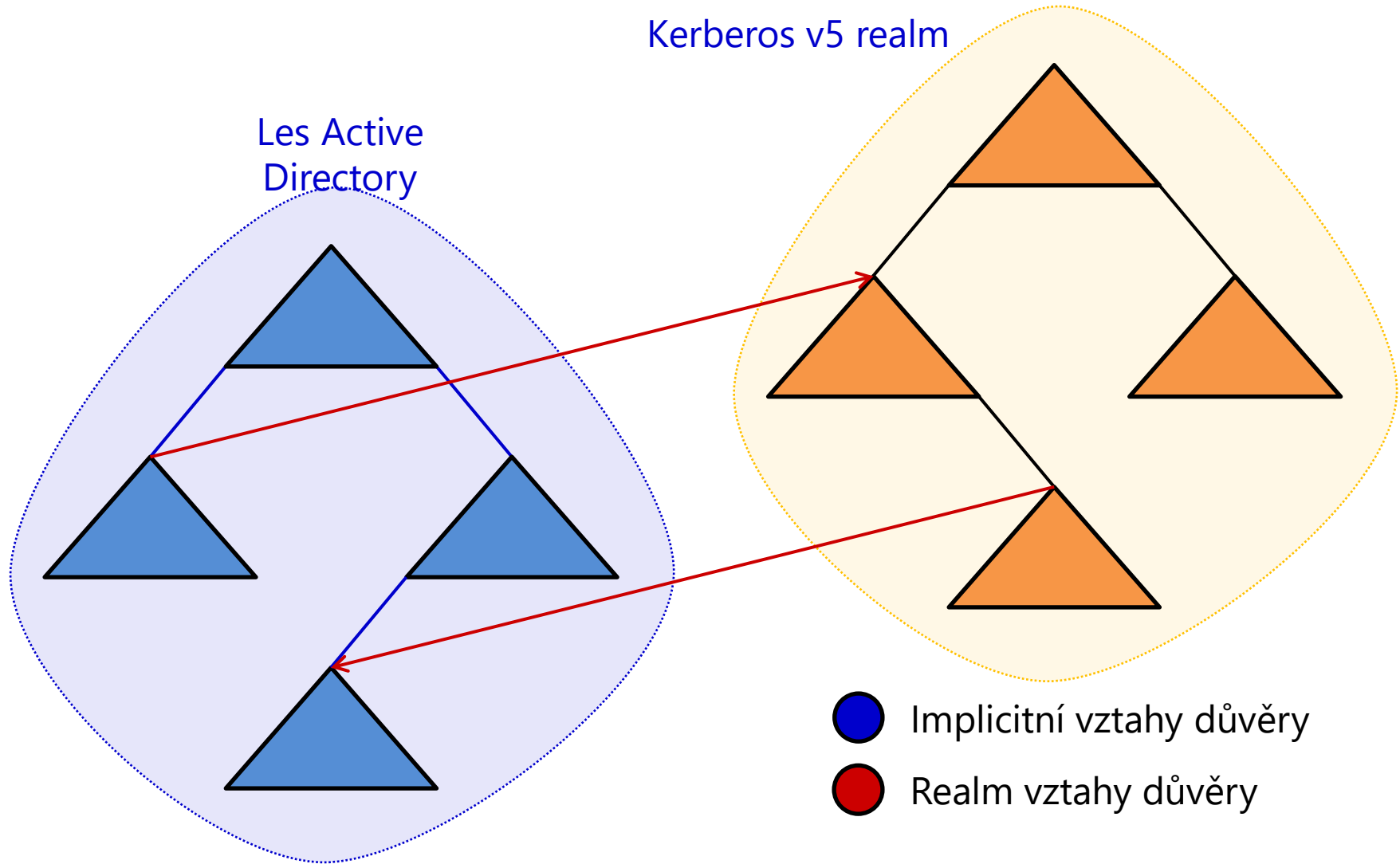
Ilustrace external vztahů důvěry



Realm vztahy důvěry

- Vlastnosti
 - Jednosměrné i obousměrné
 - 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)

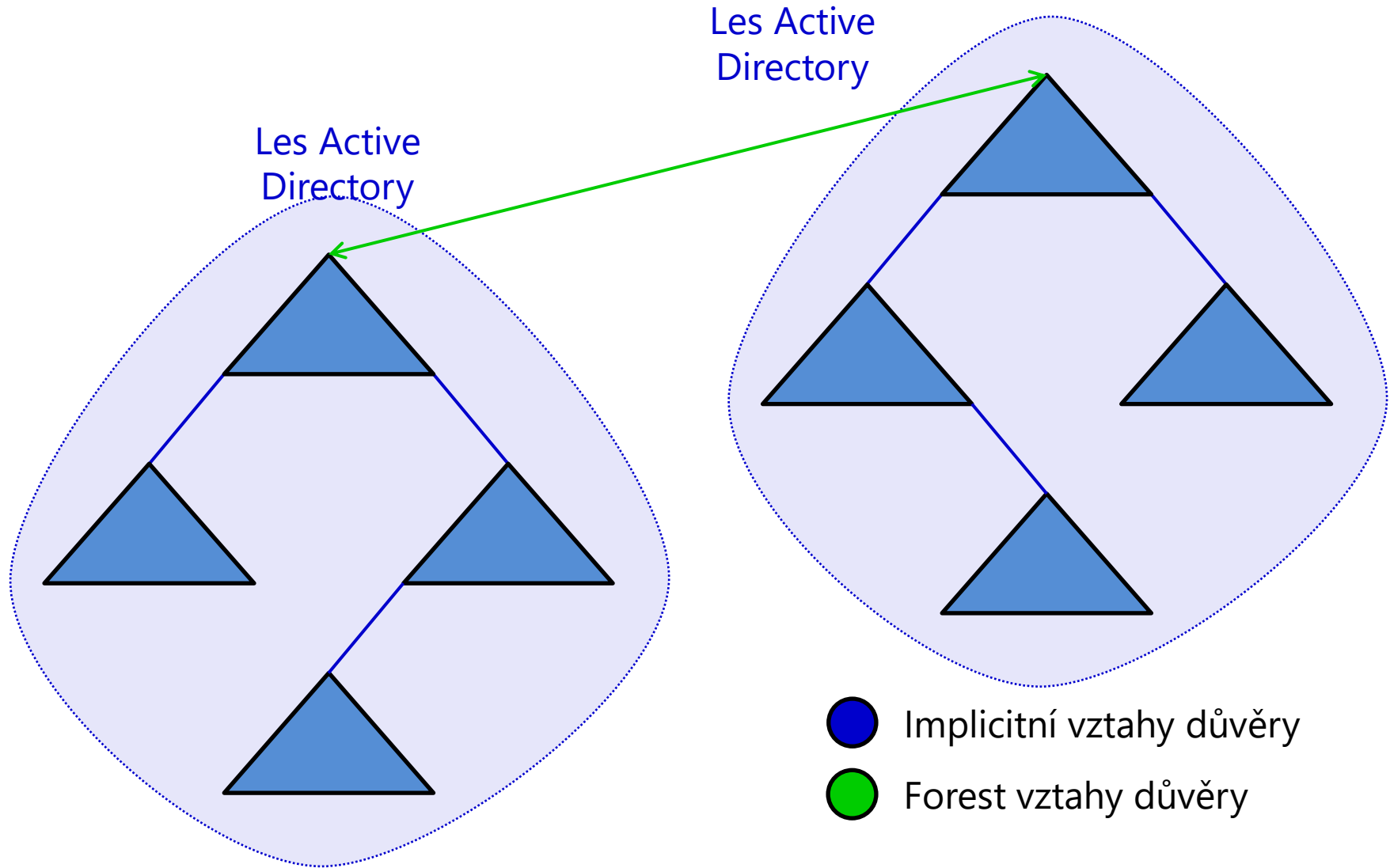
Ilustrace realm vztahů důvěry



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

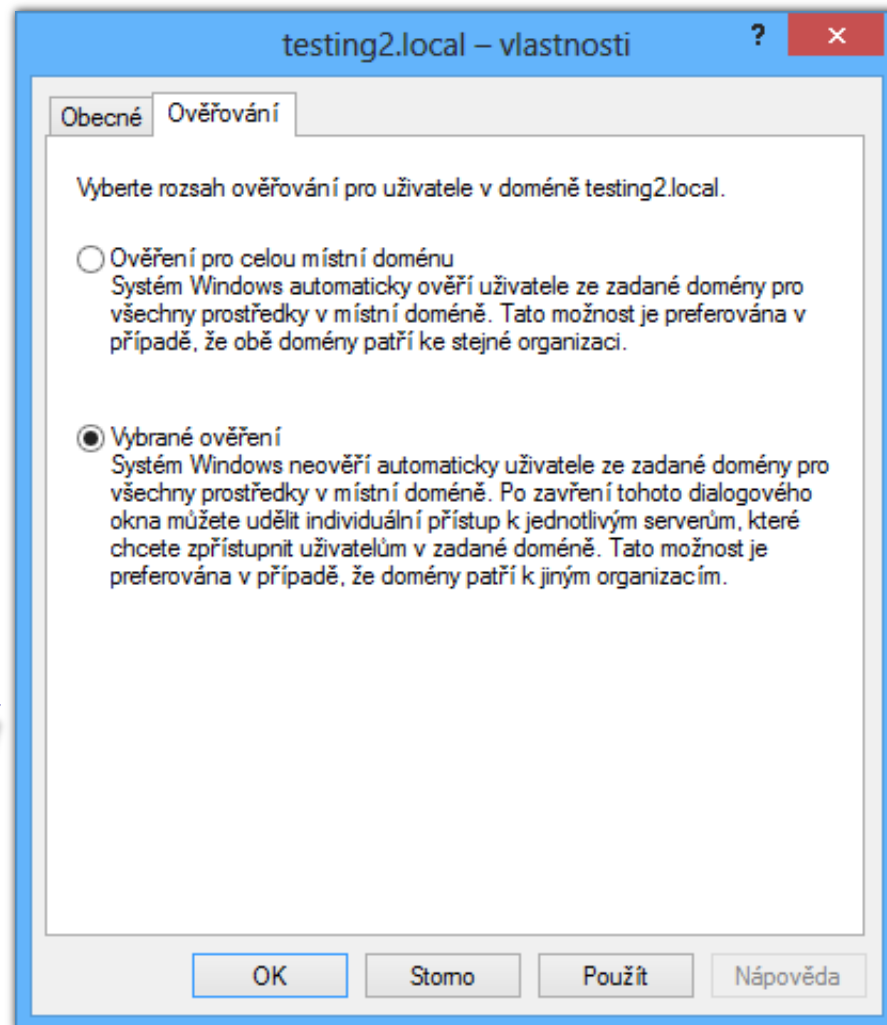
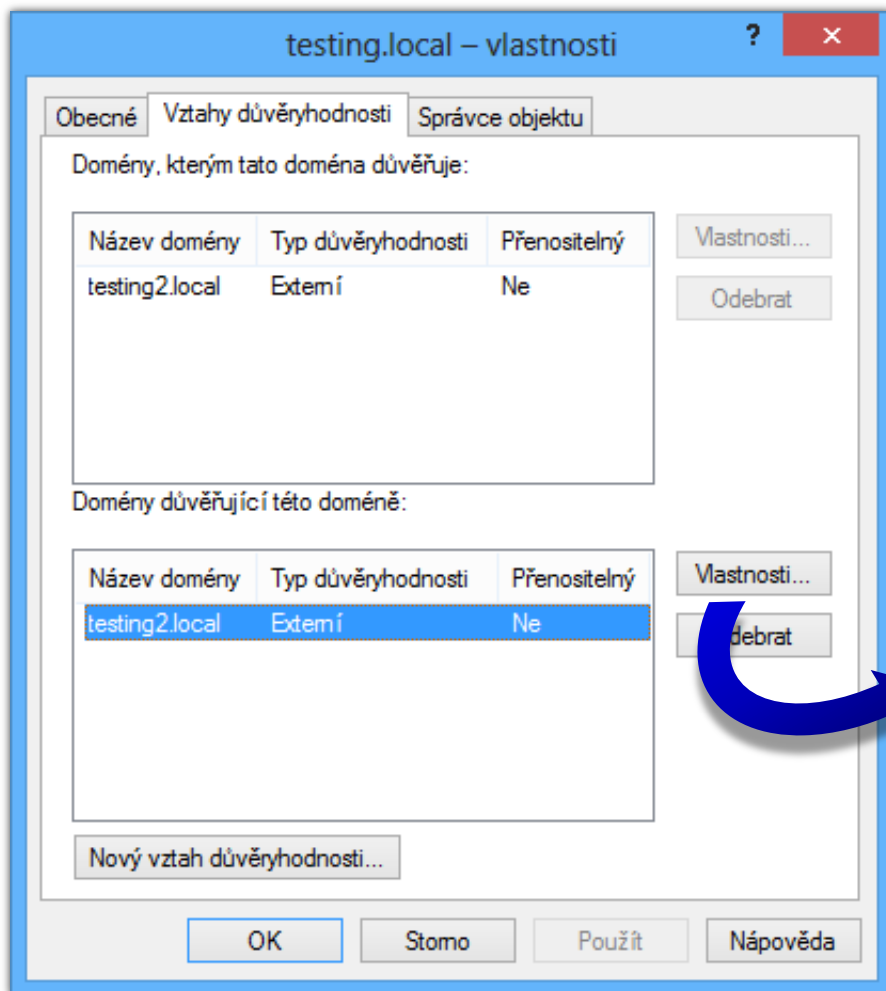
Parametry pro spojení s důvěryhodnou doménou daného vztahu důvěry

<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 **prostředkům** (ani pokud má všechna potřebná oprávnění pro tento přístup)
- Lze povolit na **external** a **forest** vztazích důvěry

Povolení selektivní autentizace



Nastavení oprávnění pro autentizaci

The image shows two overlapping windows from Windows Server 2012. The left window is the 'Uživatelé a počítače služby' (Services) console. The right window is the 'Vlastnosti' (Properties) dialog for the 'WSRV2012' service, with the 'Zabezpečení' (Security) tab selected. The 'Authenticated Users' group is selected in the list, and the 'Ověření povoleno' (Authentication is allowed) permission is checked in the permissions table.

Uživatelé a počítače služby (Left Window):

- Menu: Soubor, Akce, Zobrazit, nápověda
- Panel: Uložené dotazy, testing.local
- Strom: Built-in, Computers, Domain Controllers, ForeignSecurityPrinc, LostAndFound, Managed Service Acc, Program Data, System, Users, NTDS Quotas, TPM Devices
- Tabulka:

Název	Typ	Typ řad
WSRV2012	Počítač	GC
- Právník: Přidat do skupiny..., Mapování názvů..., Resetovat účet, Přesunout..., Spravovat, Všechny úkoly, Vyjmout, Odstranit, **Vlastnosti**, nápověda

WSRV2012 – vlastnosti (Right Window):

- Tabulka:

Obecné	Operační systém	Je členem	Delegování	Umístění
Správce objektu	Objekt	Zabezpečení	Telefonické připojení	Editor atributů
- Název skupiny nebo jméno uživatele:
 - Everyone
 - SELF
 - Authenticated Users
 - SYSTEM
 - Domain Admins (TESTING\Domain Admins)
 - Cert Publishers (TESTING\Cert Publishers)
 - Enterprise Admins (TESTING\Enterprise Admins)
- Právník: Přidat..., Odebrat
- Oprávnění pro Authenticated Users:

Oprávnění pro Authenticated Users	Povolit	Odepřít
Vytvářet všechny podřízené objekty	<input type="checkbox"/>	<input type="checkbox"/>
Odstraňovat všechny podřízené objekty	<input type="checkbox"/>	<input type="checkbox"/>
Odeslat jako	<input type="checkbox"/>	<input type="checkbox"/>
Ověření povoleno	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ověřený zápis hlavního názvu služby	<input type="checkbox"/>	<input type="checkbox"/>
Ověřený zápis názvu hostitele DNS	<input type="checkbox"/>	<input type="checkbox"/>
Přijmout jako	<input type="checkbox"/>	<input type="checkbox"/>
- Text: Kliknutím na tlačítko Upřesnit můžete nastavit oprávnění k zvláštnímu přístupu či upřesnit nastavení.
- Text: [Další informace o řízení přístupu a oprávněních](#)
- Právník: OK, Storno, Použít, nápověda