

Vztahy důvěry

[Povinné]

V případě pracovní skupiny si každý počítač uchovává vlastní úložiště identit (*identity store*) ve formě **SAM** (*Security Accounts Manager*) databáze. Autentizace uživatelů probíhá oproti tomuto úložišti identit a pouze identity přítomné v tomto úložišti mohou mít definován přístup ke zdrojům na daném počítači. Pokud je počítač připojen do domény, vytvoří se vztah důvěry (*trust relationship, trust*) mezi tímto počítačem a doménou. Tento vztah důvěry způsobí, že uživatelé již nejsou autentizováni lokálním systémem oproti lokálnímu úložišti identit, ale autentizačními službami domény (tedy **AD DS**) oproti doménovému úložišti identit (tedy databázi **Active Directory**). Připojený počítač také dovolí identitám z domény přistupovat k jeho lokálním zdrojům a využívat je.

Tento základní koncept lze samozřejmě rozšířit i na vztahy důvěry mezi jednotlivými doménami. Vztah důvěry mezi dvěma doménami umožňuje jedné doméně věřit autentizačním službám a úložišti identit druhé domény a používat identity z druhé domény k zabezpečení zdrojů. Každý vztah důvěry zahrnuje právě dvě domény, důvěřující (*trusting*) doménu a důvěryhodnou (*trusted*) doménu. Důvěryhodná doména obsahuje úložiště identit a poskytuje autentizační služby pro uživatele z tohoto úložiště. Pokud se uživatel z důvěryhodné domény přihlásí nebo připojí ke zdroji (počítači, souboru atd.) v důvěřující doméně, nemůže být v této doméně autentizován, jelikož není přítomen v úložišti identit důvěřující domény. V tomto případě důvěřující doména přenechá autentizaci nějakému řadiči z důvěryhodné domény.

Protože důvěřující doména důvěřuje identitám z důvěryhodné domény, může důvěřující doména používat identity z důvěryhodné domény k zabezpečení svých vlastních zdrojů. Uživatelům z důvěryhodné domény lze přidělovat práva (*rights*) v důvěřující doméně, např. je možné uživatelům z důvěryhodné domény povolit přihlašovat se na počítače v důvěřující doméně. Uživatelé a globální skupiny z důvěryhodné domény mohou být také přidáni do doménově lokálních skupin v důvěřující doméně, případně i přímo do **ACL** seznamů jednotlivých zdrojů v důvěřující doméně.

Některé vztahy důvěry jsou vytvářeny automaticky, jiné musí být vytvořeny manuálně. V obou případech jsou ale tyto vztahy charakterizovány dvěma vlastnostmi:

- **Tranzitivita.** Vztahy důvěry mohou, nebo nemusí, být tranzitivní. Pokud doména **A** důvěřuje doméně **B** a doména **B** důvěřuje doméně **C** a oba tyto vztahy důvěry jsou tranzitivní, pak také doména **A** důvěřuje doméně **C**. V opačném případě, kdy některý ze vztahů není tranzitivní, to neplatí, doména **A** tedy nedůvěřuje doméně **C**.
- **Směr.** Vztahy důvěry mohou být jednosměrné (*one-way*) nebo obousměrné (*two-way*). V případě jednosměrného vztahu důvěry mohou uživatelé z důvěryhodné domény přistupovat ke zdrojům v důvěřující doméně, ovšem uživatelé z důvěřující domény nemohou přistupovat ke zdrojům v důvěryhodné doméně. U obousměrného vztahu důvěry mohou i uživatelé z důvěřující domény přistupovat ke zdrojům v důvěryhodné doméně.

V lese si všechny domény navzájem důvěřují. Přesněji kořenová doména každého doménového stromu v daném lese důvěřuje kořenové doméně lesa¹ a každá podřízená (*child*) doména důvěřuje své nadřízené (*parent*) doméně. Všechny tyto vztahy důvěry jsou tranzitivní a obousměrné. V konečném důsledku tedy každá doména důvěřuje všem ostatním.

Ostatní vztahy důvěry musí být vytvářeny manuálně. Existují celkem čtyři typy vztahů důvěry, jenž lze vytvořit manuálně:

- **Shortcut.** Tento vztah důvěry se používá, pokud je potřeba urychlit přístup ke zdrojům nějaké domény z jiné domény ve stejném lese. Jak již bylo zmíněno výše, všechny domény v daném lese si navzájem důvěřují, ovšem většinou jen nepřímou díky tranzitivitě vytvořených vztahů. Pokud se uživatel z jedné domény chce přihlásit na počítač v jiné doméně, musí proběhnout vyhodnocení všech tranzitivních vztahů po cestě do této cílové domény, kde se chce uživatel přihlásit, a ověřit tedy, že cílová doména důvěřuje výchozí doméně. Těchto vztahů ale může

¹ Kořenová doména lesa je první doména vytvořená v daném lese **Active Directory**

být mnoho a ověření tedy trvat příliš dlouho. *Shortcut* vztahy důvěry umožňují vytvořit vztah důvěry přímo mezi dvěma konkrétními podřízenými doménami. Díky tomu se důvěra mezi těmito doménami ověří jednoduše pomocí tohoto vztahu důvěry místo vyhodnocování všech vztahů důvěry po cestě z jedné domény do druhé. Tyto vztahy důvěry mohou být jednosměrné i obousměrné a jsou vždy tranzitivní, lze je tedy použít pro tvorbu nových, kratších, cest.

- **External.** Tento vztah důvěry se používá, pokud je potřeba pracovat s doménami, jenž neleží ve stejném lese. Vytváří vztah důvěry mezi dvěma doménami systému Windows z odlišných lesů. Všechny tyto vztahy důvěry jsou jednosměrné a nejsou tranzitivní. Pokud je vytvořen obousměrný *external* vztah důvěry, jsou místo něj ve skutečnosti vytvořeny dva jednosměrné vztahy důvěry, každý v jednom směru. V případě, že je vytvořen odchozí *external* vztah důvěry, vytvoří **Active Directory** cizí (*foreign*) bezpečnostní objekt pro každý bezpečnostní objekt z důvěryhodné domény. Tyto cizí bezpečnostní objekty pak mohou být přidány do doménově lokálních skupin a ACL seznamů v důvěřující doméně. Pro zvýšení bezpečnosti tohoto vztahu důvěry lze využít výběrovou autentizaci a doménovou karanténu (povolena ve výchozím nastavení), které budou zmíněny dále.
- **Realm.** Tento vztah důvěry se používá, pokud je potřeba pracovat s bezpečnostními službami založenými na protokolu Kerberos v5, jenž běží na jiných systémech, než je systém Windows. Tyto vztahy důvěry jsou jednosměrné. Pro vytvoření obousměrného vztahu důvěry je možné vytvořit jednosměrné vztahy důvěry v každém z obou směrů. Ve výchozím nastavení nejsou tyto vztahy důvěry tranzitivní, ale lze je tranzitivními učinit.
- **Forest.** Tento vztah důvěry se používá, pokud je potřeba spolupráce mezi dvěma organizacemi reprezentovanými pomocí dvou odlišných lesů. Vytváří vztah důvěry mezi kořenovými doménami obou lesů. Tyto vztahy mohou být jednosměrné i obousměrné a jsou vždy tranzitivní. Pokud existuje jednosměrný *forest* vztah důvěry mezi dvěma doménami, pak se uživatel z jakékoliv domény v důvěryhodném lese může přihlásit k jakémukoliv počítači v důvěřujícím lese (tedy k počítači v jakékoliv doméně v důvěřujícím lese). Pokud je tento vztah obousměrný, platí to i v opačném směru. *Forest* vztah důvěry má ve výchozím nastavení povolenou doménovou karanténu. Tento typ vztahů důvěry je vždy tranzitivní, ovšem pouze ve smyslu, že každá doména v důvěřujícím lese důvěřuje všem ostatním doménám v důvěryhodném lese. *Forest* vztahy důvěry nejsou tranzitivní navzájem. Tedy pokud les **A** důvěřuje lesu **B** a dále les **B** důvěřuje lesu **C**, pak neplatí, že les **A** důvěřuje lesu **C**. Aby bylo možné vytvořit *forest* vztah důvěry, je potřeba mít funkční úroveň lesa alespoň [Windows Server 2003](#) a také mít odpovídající **DNS** infrastrukturu.

Zabezpečení vztahů důvěry

[Povinné]

Samotný vztah důvěry sice neumožňuje uživatelům přistupovat ke zdrojům v důvěřující doméně, ale jeho vytvořením mohou uživatelé z důvěryhodné domény získat přístup k některým zdrojům v důvěřující doméně. Je to proto, že velká řada zdrojů je chráněna ACL seznamy, které mohou mít definovány oprávnění pro skupinu [Authenticated Users](#). Jelikož do této skupiny patří všichni autentizovaní uživatelé, tedy i autentizovaní uživatelé z důvěryhodných domén, mohou k těmto zdrojům přistupovat i tito uživatelé. Kromě toho mohou být samozřejmě uživatelé a globální skupiny z důvěryhodných domén přímo přidány do ACL seznamů a také do doménově lokálních skupin.

I pokud jsou správně nastavena oprávnění pro přístup ke zdrojům v důvěřující doméně, je zde pořád nebezpečí nepovoleného přístupu. Když se uživatel autorizuje do důvěřující domény, předkládá autorizační data, jenž obsahují, mimo jiné, **SID** identifikátory uživatele a skupin, jichž je daný uživatel členem. Ne všechny tyto identifikátory musí pocházet (být vytvořeny) z důvěryhodné domény. Např. pokud je uživatel přesunut z jiné domény, je mu vygenerován nový **SID** identifikátor. V tomto případě ale uživatel ztrácí přístup ke zdrojům, jenž mají v ACL seznamech definovány oprávnění pro jeho starý **SID** identifikátor. Proto lze uchovávat u uživatele historii jeho předchozích **SID** identifikátorů. Ovšem tímto vzniká nebezpečí podstrčení **SID** identifikátorů. Administrátor může před migrací

uživatelé do nové domény přiřadit tomuto uživateli jako předchozí **SID** identifikátory **SID** identifikátory důležitých účtů z cílové domény (např. **SID** účtu, jenž je v [Domain Admins](#)) a uživatel tak získá díky historii oprávnění správce domény. Tento problém řeší doménová karanténa (*domain quarantine*), jenž zajišťuje ignorování veškerých **SID** identifikátorů, které nepocházejí z důvěryhodné domény. Doménová karanténa je ve výchozím nastavení povolena na všech *external* a *forest* vztazích důvěry.

Jak již bylo zmíněno dříve, autentizovaní uživatelé z důvěryhodné domény jsou automaticky členy [Authenticated Users](#) a mohou tedy mít automaticky přístup k řadě zdrojů v důvěřující doméně. Tato situace nemusí být vždy žádoucí. V případě přístupu ke zdrojům to lze řešit aplikací [deny](#) nebo odebráním oprávnění skupině [Authenticated Users](#). Tímto postupem ale nelze omezit přístup ke službám jako je např. přihlašování ke stanicím v důvěřující doméně. Tento problém řeší výběrová autentizace (*selective authentication*), jenž umožňuje specifikovat, kteří uživatelé či skupiny mohou využívat služby na konkrétním počítači. Výběrovou autentizaci lze povolit u *external* a *forest* vztahů důvěry.

Společné úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server **file**: **nepal\hstudent** heslo: **aaa**
- Rozsah IP adres přidělených z *Default switch* se může od níže uvedeného rozsahu lišit.

Lab LS00 – konfigurace virtuálních stanic

[\[Provést \]](#)

Připojte síťové adaptéry stanic k následujícím virtuálním přepínačům:

| Adaptér (MAC suffix) | LAN1 (-01) | LAN2 (-02) | LAN3 (-03) | LAN4 (-04) |
|--------------------------|-------------|------------|-------------|-------------|
| D+R+C w2016-dc | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| D+R+C w2016-repl | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| D+R+C w2016-child | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| w2016-dc2 | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |

- V případech, kdy je potřeba přistupovat na externí síť, připojte adaptér **LAN1** k přepínači *Default switch*.
- Servery **D+R+C w2016-dc** a **D+R+C w2016-repl** je nutné spouštět společně.
- Na stanici **D+R+C w2016-dc** restartujte službu DHCP
 - DHCP MMC, vyberte w2016-dc.testing.local a z kontextové nabídky All Tasks – Restart
- Tip: stanice **D+R+C w2016-dc** a **D+R+C w2016-repl** spusťte na začátku cvičení.

Lektorské úkoly

Lab L01 – ADDT (Active Directory Domains and Trusts)

[Na cvičeních]

Cíl cvičení

Seznámení s ADDT konzolí

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)

w2016-repl (D+R+C w2016-repl)

[Provést]

Lab L02 – Vytvoření vztahů důvěry

Cíl cvičení

Vytvořit postupně *external* a *forest* vztahy důvěry, ověřit jejich funkčnost a seznámit se s jejich odlišnostmi při vyhodnocování důvěry mezi doménami

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)

w2016-repl (D+R+C w2016-repl)

w2016-child (D+R+C w2016-child)

w2016-dc2 (w2016-dc2)

Další prerekvizity

Účet uživatele **administrator** v doméně **testing2.local2**

1. Přihlaste se na **w2016-dc** jako **testing\administrator**
2. Přihlaste se na **w2016-dc2** jako **testing2\administrator**
3. Nastavte podmíněné přeposílání DNS dotazů mezi doménami **testing.local** a **testing2.local2**
 - a. Na **w2016-dc** otevřete **DNS**
 1. **Start** → **Administrative Tools** → **DNS**
 - b. Klikněte pravým na **Conditional Forwarders** a zvolte **New Conditional Forwarder...**
 - c. Do pole **DNS Domain** zadejte **testing2.local2** a pod **IP addresses of the master servers** níže vložte IP adresu **192.168.32.90** a potvrďte **OK**
 - d. Opakujte **body 1.a – 1.c** na **w2016-dc2**, tentokrát pro doménu **testing.local** a IP adresu **192.168.32.5**
 - e. Pomocí nástroje nslookup ověřte, že je nyní možné přeložit FQDN z opačné domény
2. Vytvořte nový *external* vztah důvěry tak, aby doména **child.testing.local** důvěřovala doméně **testing2.local2**
 - a. Na **w2016-dc** otevřete **ADDT (Active Directory Domains and Trusts)**
 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **child.testing.local** a zvolte **Properties**
 - c. Přejděte na záložku **Trusts** a zvolte **New Trust...**
 - d. V průvodci pokračujte **Next >**
 - e. V části **Trust Name** zadejte do pole **Name** doménu **testing2.local2** a pokračujte **Next >**
 - f. V další části **Direction of Trust** zvolte **One way: outgoing** a pokračujte **Next >**
 - g. V následující části **Sides of Trust** zvolte **Both this domain and the specified domain** a pak pokračujte **Next >**

- h. V další části **User Name and Password** zadejte účet uživatele **testing2\administrator** a heslo **aaa** a pokračujte **Next >**
- i. V části **Outgoing Trust Authentication Level – Local Domain** zvolte možnost **Domain-wide authentication** a pokračujte **Next >**
- j. Vytvořte nový vztah důvěry pomocí **Next >**
- k. Pokračujte **Next >**
- l. V části **Confirm Outgoing Trust** zvolte **Yes, confirm the outgoing trust** a pokračujte **Next >**
- m. Potvrďte pomocí **Finish**
- n. Přečtěte si upozornění o zapnutém **SID filtering** a potvrďte **OK**
3. Ověřte, že bodem 2.g došlo i k vytvoření jednosměrného příchozího vztahu důvěry v doméně **testing2.local2**
 - a. Na **w2016-dc2** otevřete **ADDT** (*Active Directory Domains and Trusts*)
 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **testing2.local2** a zvolte **Properties**
 - c. Přejděte na záložku **Trusts** a ověřte přítomnost **child.testing.local** mezi příchozími vztahy důvěry (**incoming trusts**)
4. Přihlaste se na **w2016-child** jako **child\administrator**
5. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **child.testing.local**
 - a. Na **w2016-child** otevřete **GPME** (*Group Policy Management Editor*)
 1. **Start** → **Administrative Tools** → **Group Policy Management**
 - b. Klikněte pravým na GPO objekt **Default Domain Controllers Policy** a zvolte **Edit...**
 - c. Vyberte uzel **Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignments**
 - d. Klikněte pravým na **Allow log on locally** a zvolte **Properties**
 - e. Zaškrtněte **Define these policy settings** a zvolte **Add User or Group...**
 - f. Zadejte **Everyone** a potvrďte **OK**
 - g. Potvrďte **OK** a zavřete **Group Policy Management Editor**
 - h. Aktualizujte nastavení zásad skupiny příkazem **gpupdate /force**
6. Přihlaste se na **w2016-child** jako uživatel **administrator@testing2.local2**
 - Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **child.testing.local**
7. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **testing2.local2** provedením postupu z **bodu 5** na **w2016-dc2**
8. Přihlaste se na **w2016-dc2** jako uživatel **administrator@child.testing.local**
 - Přihlášení nebude úspěšné, jelikož doména **child.testing.local** není důvěryhodnou doménou pro doménu **testing2.local2**, vytvořený vztah je jednosměrný
9. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **testing.local** provedením postupu **bodu 5** na **w2016-dc**
10. Přihlaste se na **w2016-dc** jako uživatel **administrator@testing2.local2**
 - Přihlášení nebude úspěšné, jelikož doména **testing2.local2** není důvěryhodnou doménou pro doménu **testing.local**
11. Smažte vytvořený *external* vztah důvěry mezi doménami **child.testing.local** a **testing2.local2**
 - a. Na **w2016-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **child.testing.local** a zvolte **Properties**

- c. Přejděte na záložku **Trusts**
 - d. Pod **Domains trusted by this domain (outgoing trusts)** vyberte v seznamu **testing2.local2** zvolte **Remove**
 - e. Vyberte **Yes, remove the trust from both the local domain and the other domain** a použijte účet uživatele **testing2\administrator** s heslem **aaa**
 - f. Potvrďte odebrání pomocí **Yes**
12. Vytvořte *forest* vztah důvěry tak, aby kořenová doména lesa **testing.local** důvěřovala kořenové doméně lesa **testing2.local2**
- a. Na **w2016-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
 - 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **testing.local** a zvolte **Properties**
 - c. Přejděte na záložku **Trusts** a zvolte **New Trust...**
 - d. V průvodci pokračujte **Next >**
 - e. V části **Trust Name** zadejte do pole **Name** doménu **testing2.local2** a pokračujte **Next >**
 - f. V další části **Trust Type** vyberte **Forest Trust** a pokračujte **Next >**
 - g. V následující části **Direction of Trust** zvolte **One way: outgoing** a pokračujte **Next >**
 - h. V části **Sides of Trust** ponechte **This domain only** a pokračujte **Next >**
 - i. V další části **Outgoing Trust Authentication Level** zvolte **Forest-wide authentication** a pokračujte **Next >**
 - j. V následující části **Trust Password** použijte heslo **aaaAAA111** a pokračujte **Next >**
 - k. Vytvořte nový vztah důvěry pomocí **Next >**
 - l. Pokračujete **Next >**
 - m. V části **Confirm Outgoing Trust** zvolte **No, do not confirm the outgoing trust** a pokračujte **Next >**
 - n. Potvrďte pomocí **Finish**
13. Dokončete vytvoření *forest* vztahu důvěry v doméně **testing2.local2**
- a. Na **w2016-dc2** otevřete **ADDT** (*Active Directory Domains and Trusts*)
 - 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **testing2.local2** a zvolte **Properties**
 - c. Přejděte na záložku **Trusts** a zvolte **New Trust...**
 - d. V průvodci pokračujte **Next >**
 - e. V části **Trust Name** zadejte do pole **Name** doménu **testing.local** a pokračujte **Next >**
 - f. V další části **Trust Type** vyberte **Forest Trust** a pokračujte **Next >**
 - g. V následující části **Direction of Trust** zvolte **One way: incoming** a pokračujte **Next >**
 - h. V části **Sides of Trust** ponechte **This domain only** a pokračujte **Next >**
 - i. V další části **Trust Password** zadejte heslo **aaaAAA111** a pokračujte **Next >**
 - j. Vytvořte nový vztah důvěry pomocí **Next >**
 - k. Pokračujte **Next >**
 - l. V části **Confirm Incoming Trust** zvolte **Yes, confirm the incoming trust** a zadejte účet uživatele **testing\administrator** a heslo **aaa** a pokračujte **Next >**
 - m. Potvrďte pomocí **Finish**
14. Přihlaste se na **w2016-dc** jako uživatel **administrator@testing2.local2**
- Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **testing.local**

15. Přihlaste se na **w2016-dc2** jako uživatel **administrator@testing.local**

- Přihlášení nebude úspěšné, jelikož doména **testing.local** není důvěryhodnou doménou pro doménu **testing2.local2**, vytvořený vztah je jednosměrný

16. Přihlaste se na **w2016-child** jako uživatel **administrator@testing2.local2**

- Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **testing.local**, doména **child.testing.local** důvěřuje své nadřízené (*parent*) doméně **testing.local**, doména **testing.local** zase důvěřuje **testing2.local2** doméně, oba tyto vztahy důvěry jsou tranzitivní, takže také doména **child.testing.local** důvěřuje doméně **testing2.local2**

Studentské úkoly

Lab S01 – Zabezpečení vztahů důvěry

[Povinné]

Cíl cvičení

Nastavit a ověřit výběrovou autentizaci, vypnout a zapnout doménovou karanténu

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)

w2016-child (D+R+C w2016-child)

w2016-dc2 (w2016-dc2)

Další prerekvizity

Dokončený úkol **Lab L02**

1. Přihlaste se na **w2016-dc** jako **testing\administrator**
2. Povolte výběrovou autentizaci pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
 - a. Na **w2016-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
 1. **Start** → **Administrative Tools** → **Active Directory Domains and Trusts**
 - b. Klikněte pravým na doménu **testing.local** a zvolte **Properties**
 - c. Přejděte na záložku **Trusts**
 - d. Pod **Domains trusted by this domain (outgoing trusts)** vyberte v seznamu **testing2.local2** zvolte **Properties...**
 - e. Přejděte na záložku **Authentication** a vyberte **Selective authentication**
 - f. Potvrďte dvakrát **OK**
3. Přihlaste se na **w2016-dc** jako uživatel **administrator@testing2.local2**
 - Přihlášení nebude úspěšné, jelikož po povolení selektivní *autentizace* nelze využívat žádné služby počítačů v důvěřující doméně
4. Přihlaste se na **w2016-dc** jako **testing\administrator**
5. Povolte využívání služeb **w2016-dc**
 - a. Na **w2016-dc** otevřete **ADUC** (*Active Directory Users and Computers*)
 1. **Start** → **Administrative Tools** → **Active Directory Users and Computers**
 - b. Povolte pokročilé možnosti zobrazení
 1. V menu konzole vyberte **View** a zvolte **Advanced Features**
 - c. Vyberte organizační jednotku **Domain Controllers**
 - d. Klikněte pravým na účet počítače **w2016-dc** a zvolte **Properties**
 - e. Přejděte na záložku **Security**, pak v seznamu pod **Group or user names** vyberte skupinu **Authenticated Users** a zaškrtněte **Allow** u **Allowed to authenticate**
 - f. Potvrďte **OK**
6. Přihlaste se na **w2016-dc** jako uživatel **administrator@testing2.local2**
 - Přihlášení již bude úspěšné, jelikož všichni uživatelé z důvěryhodných domén jsou členy skupiny **Authenticated Users** a ta má nyní oprávnění využívat služby tohoto počítače
7. Přihlaste se na **w2016-dc** jako **testing\administrator**

8. Vypněte doménovou karanténu pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
 - a. Na **w2016-dc** spusťte jako administrátor příkazový řádek
 - b. Spusťte příkaz **netdom trust testing.local /d:testing2.local2 /quarantine:no /userD:administrator@testing2.local2 /passwordD:aaa**
9. Zapněte doménovou karanténu pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
 - a. Na **w2016-dc** spusťte jako administrátor příkazový řádek
 - b. Spusťte příkaz **netdom trust testing.local /d:testing2.local2 /quarantine:yes /userD:administrator@testing2.local2 /passwordD:aaa**