Autentizace a účty v AD

Autentizace stanice v AD

Domain Controller
dc02.fi.muni.cz
147.251.10.4

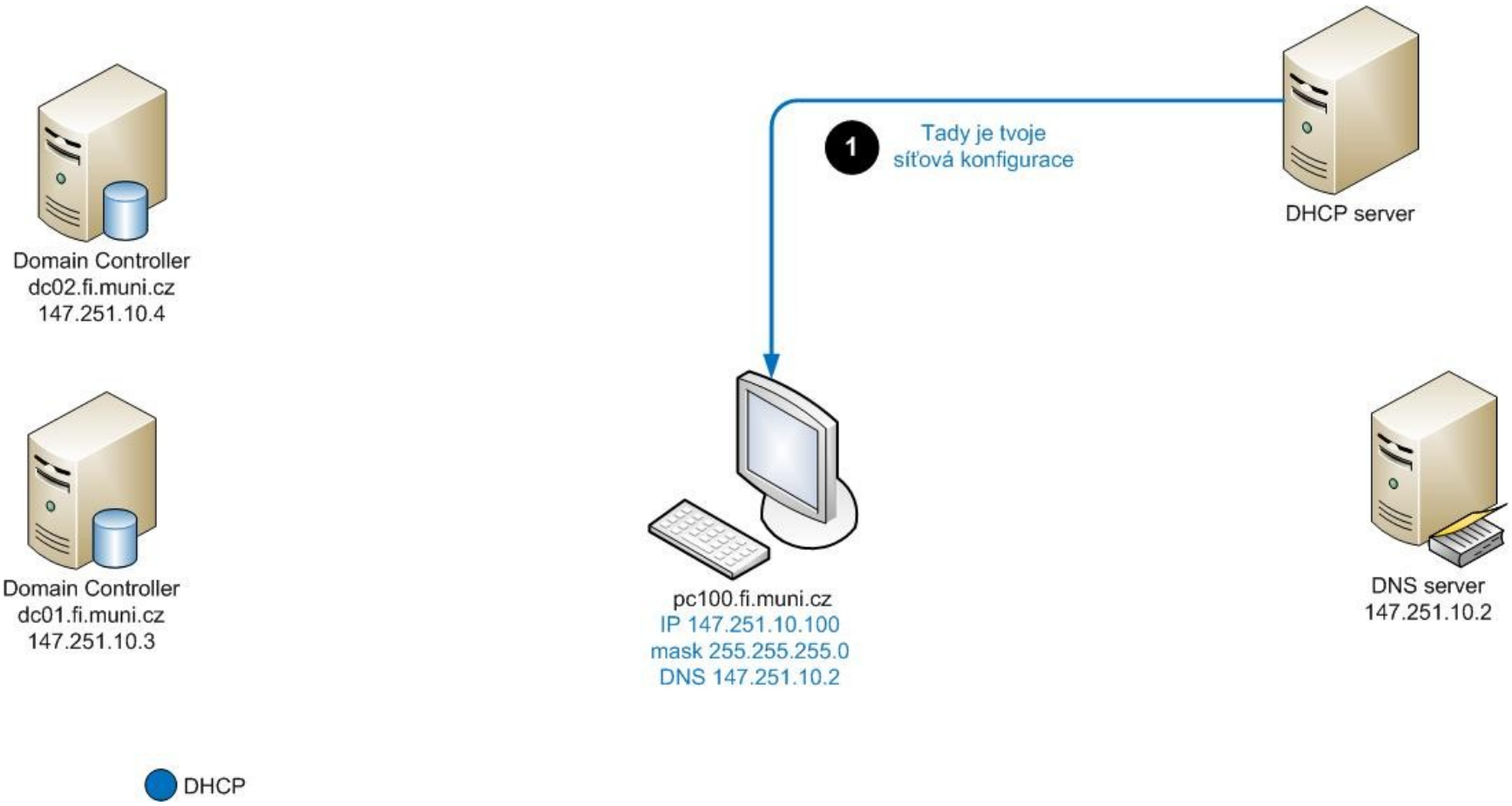
DHCP server

Domain Controller
dc01.fi.muni.cz
147.251.10.3

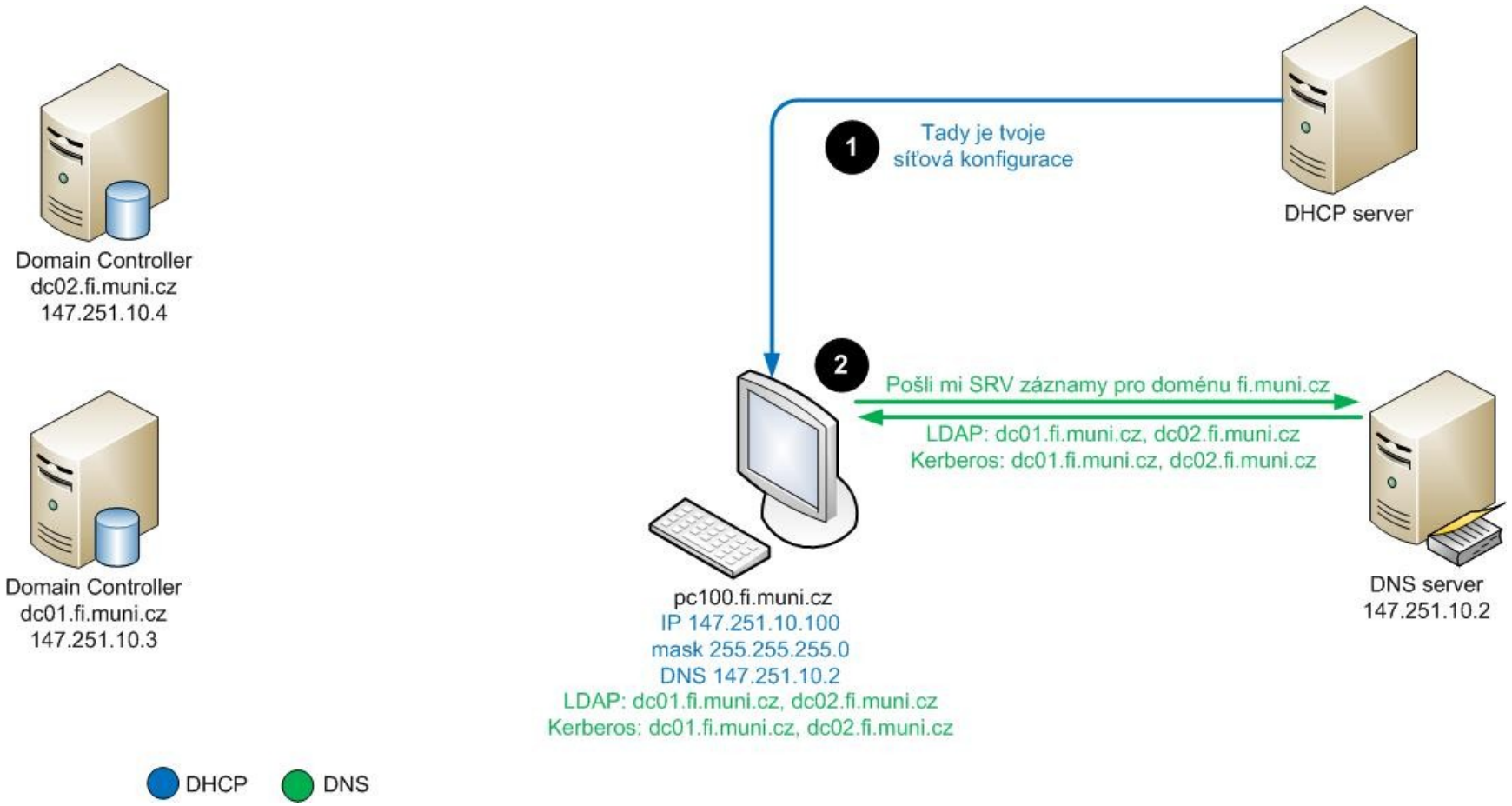
pc100.fi.muni.cz

DNS server
147.251.10.2

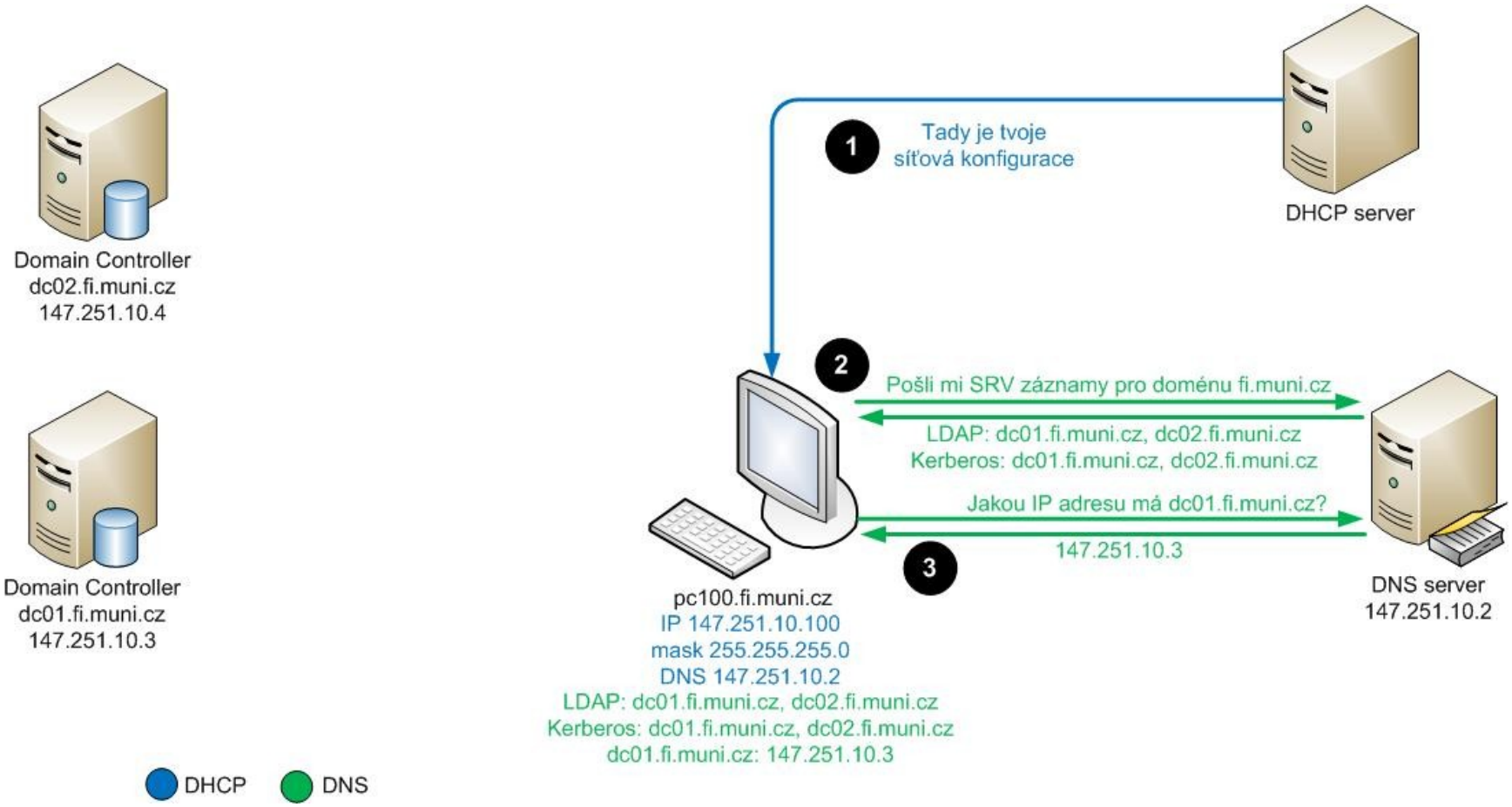
Autentizace stanice v AD



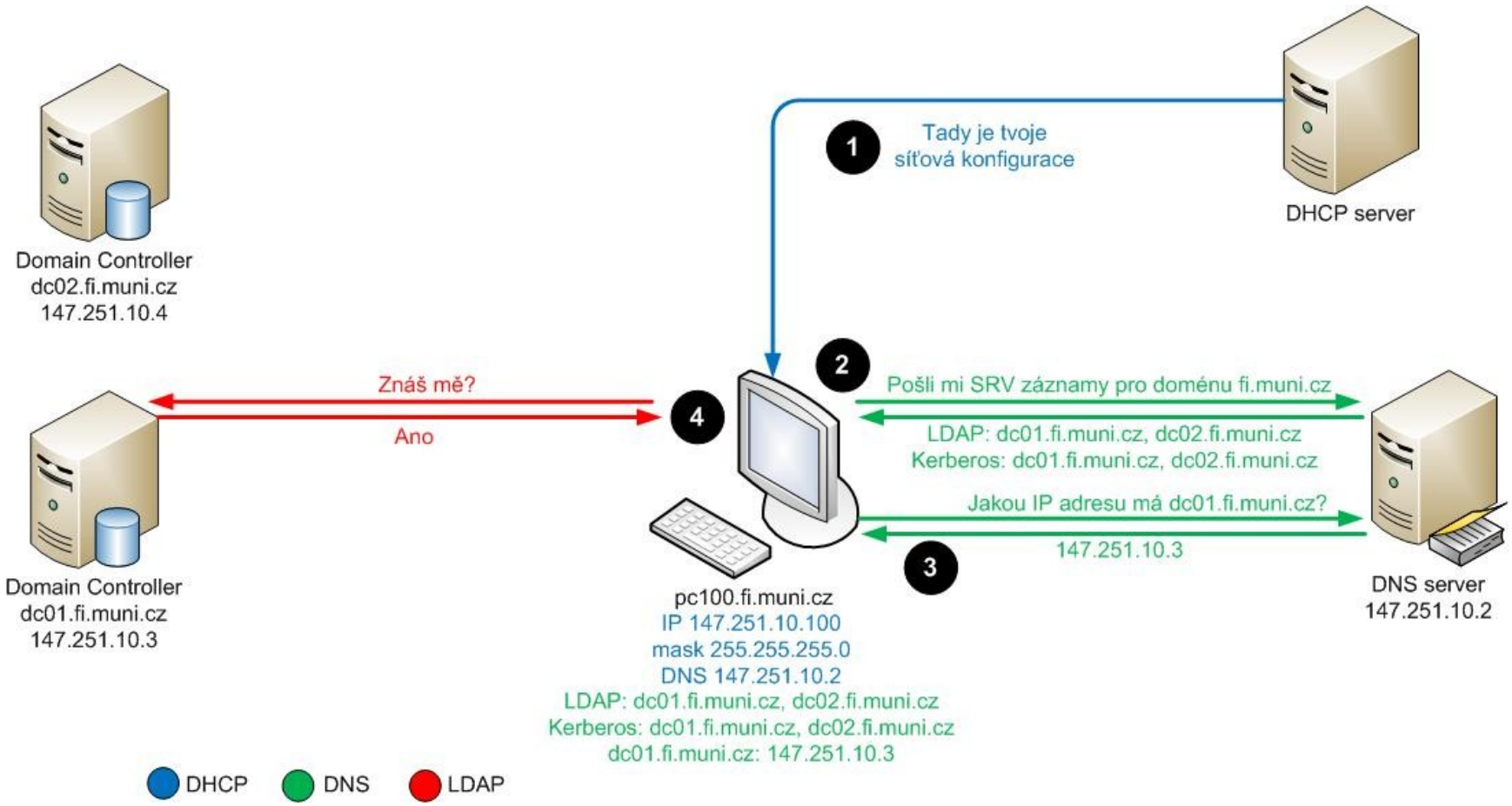
Autentizace stanice v AD



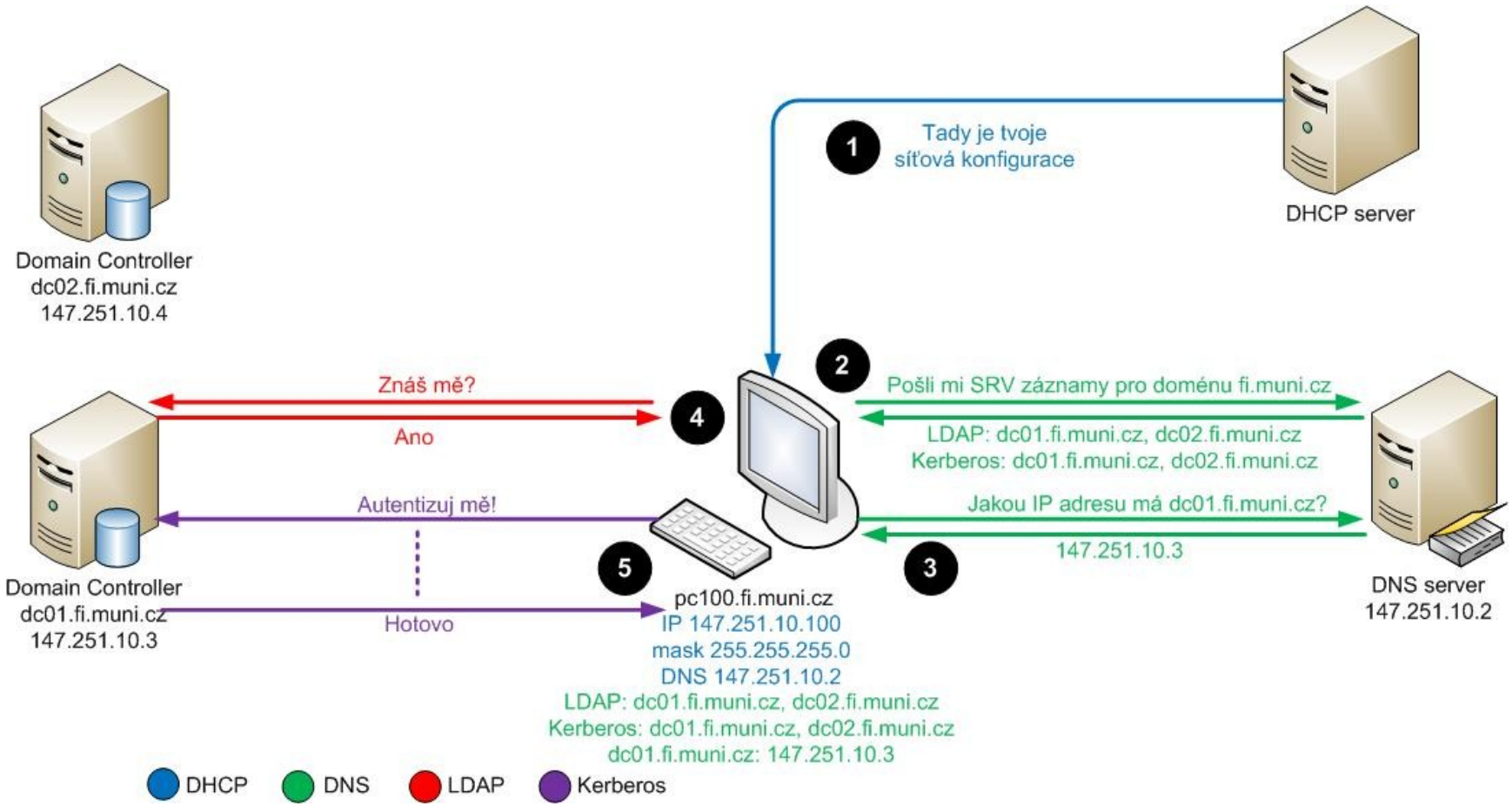
Autentizace stanice v AD



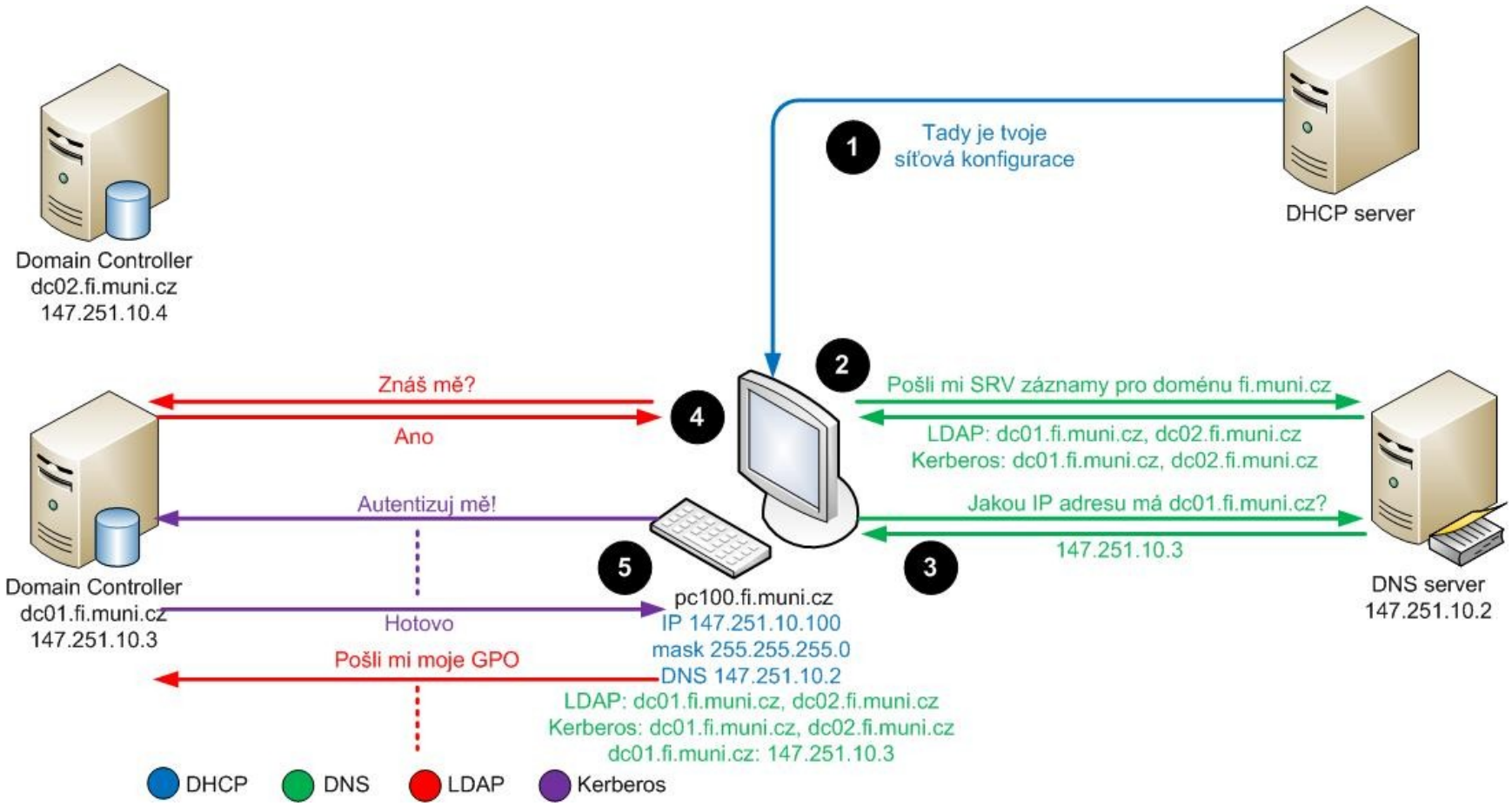
Autentizace stanice v AD



Autentizace stanice v AD



Autentizace stanice v AD



Účty

- Typy účtů
  - Lokální
    - Uložený lokálně na počítači
  - Doménový
    - Uložený na doménovém řadiči
    - Doménové řadiče nemají lokální účty, ale ostatní počítače zařazené v doméně je mít mohou

Účty v AD

- Uživatelský účet
  - Nutný pro přihlášení člověka k doméně
  - Ustanovuje uživateli identitu, kterou operační systém následně používá pro autentizaci na síti a autorizaci prováděných činností
- Účet počítače
  - Ustanovuje identitu počítače, která se používá pro autentizaci, autorizaci a audit
  - Pod účtem počítače běží všechny systémové procesy
- Účet skupiny
  - Účet sdružující a zastupující jiné účty
  - Může obsahovat účty uživatelů, počítačů i dalších skupin
  - Každý účet (i účet skupiny) může být členem libovolného množství skupin
  - Zjednodušuje administraci a správu přístupu ke zdrojům

Skupinové účty

- Bezpečnostní – využívají se k přidělování práv a oprávnění a k jemnému nastavení zásad skupiny
- Distribuční – používají se k vytváření skupin osob pro použití při emailové komunikaci

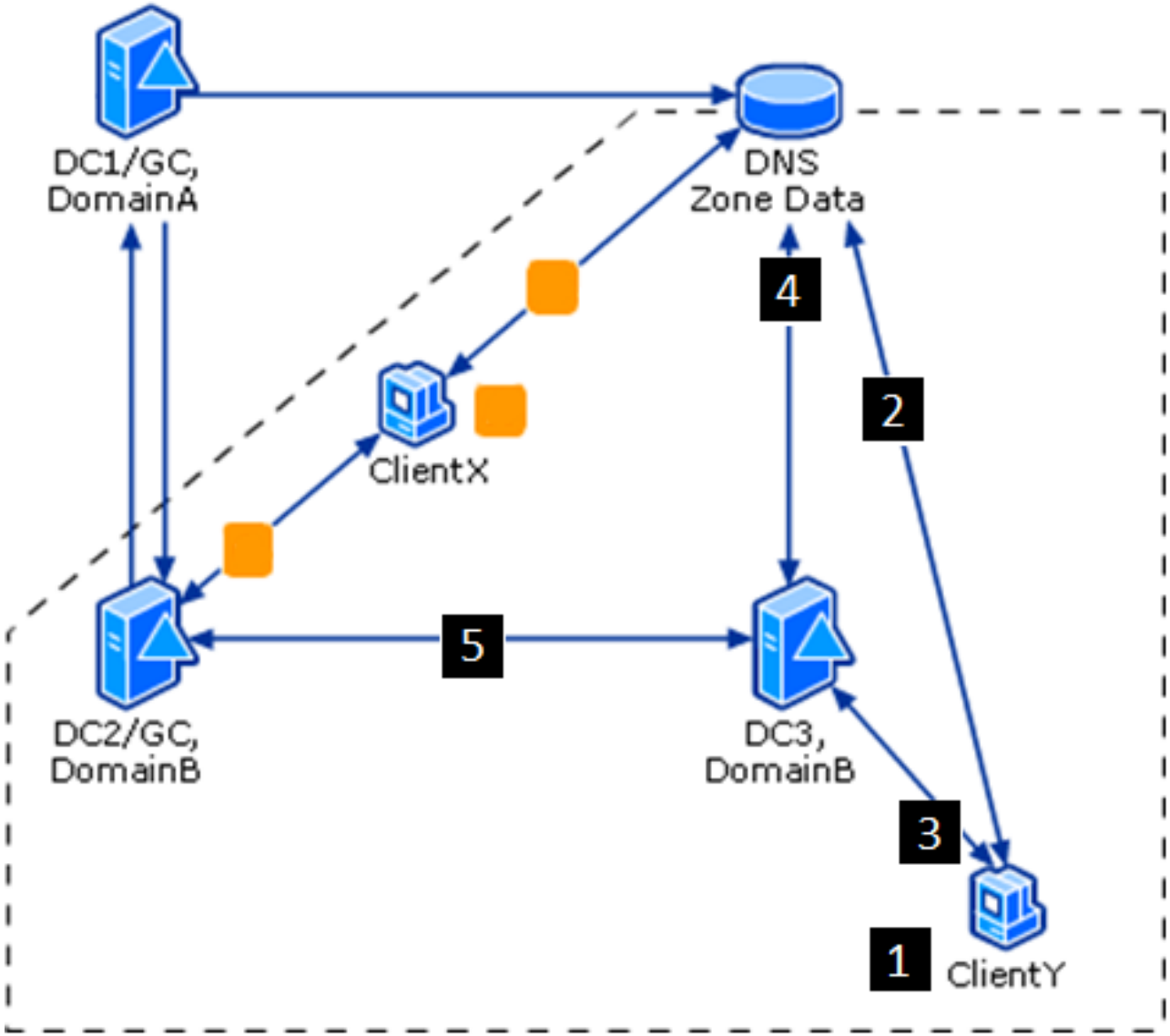
Skupinové účty

- Globální skupiny (G)
  - Členství: Členy mohou být pouze účty a skupiny ze stejné domény jako je daná skupina
  - Oprávnění: Globální skupině mohou být udělena oprávnění k libovolným objektům v celém lese
- Doménové lokální skupiny (DL)
  - Členství: Členy doménové lokální skupiny mohou být účty a skupiny z celého vlastního lesa
  - Oprávnění: Doménové lokální skupině mohou být udělena oprávnění pouze v rámci její domény
- Univerzální skupiny (U)
  - Členství: Členy mohou být účty a skupiny z libovolné domény v lese
  - Oprávnění: Univerzálním skupinám mohou být přiřazena oprávnění k libovolným objektům v celém lese
  - Univerzální skupiny jsou ukládány pouze na tzv. globálním katalogu

Globální katalog (GC)

- Doménové řadiče s rozšířenou databází
  - Kromě všech atributů objektů z vlastní domény obsahují i omezenou množinu atributů všech objektů z celého lesa
  - Nutné pro přihlášení uživatelů
  - Umožňují rychlé vyhledávání v objektech lesa

Autentizace uživatele v AD



Autentizace uživatele v AD

1. Uživatel zadává svůj login a heslo.
2. Stanice se ptá DNS, kde se nachází LDAP a Kerberos služba pro uživatelovu doménu. DNS poskytuje odpověď.
3. Stanice kontaktuje DC, jehož IP adresu dostala, a žádá o autentizaci uživatele.
4. DC ověřuje platnost loginu a hesla, jsou platné. DC ale není GC, takže kontaktuje DNS a žádá o SRV záznamy o GC. DNS poskytuje odpověď.
5. DC se ptá GC, zda je uživatel členem nějaké univerzální skupiny, která nedovoluje přihlášení na dané stanici. Pokud není, DC povoluje uživateli přihlášení na stanici.

Významné účty skupin

- Domain Users
  - Skupina všech uživatelských účtů v doméně
- Domain Computers
  - Skupina všech účtů počítačů v doméně
- Domain Controllers
  - Skupina všech účtů doménových řadičů v doméně

Významné účty skupin

- Domain Admins
  - Správci domény, mají nejvyšší možná práva v rámci své domény
- Enterprise Admins
  - Správci organizace, mají nejvyšší možná práva ve všech doménách celého lesa
  - Mohou vytvářet nové domény a navazovat nové vztahy důvěry mezi doménami
  - Tato skupina se nachází pouze ve forest-root doméně lesa
- Schema Admins
  - Členové této skupiny mohou provádět změny schématu Active Directory
  - Tato skupina se nachází pouze ve forest-root doméně lesa

Vytváření a správa účtů

- Malá organizace/výjimečné požadavky
  - Active Directory Users and Computers
    - Základní grafický nástroj pro správu účtů a organizačních jednotek
- Střední organizace/občasné hromadné změny
  - Skripty a nástroje příkazové řádky
    - dsadd, dsmod, dsquery, dsget, dsmove, dsrm
    - ldifde
    - Csvde
    - Visual Basic Script
- Velká organizace/dynamicky se měnící prostředí
  - Propojení s existujícím personálním systémem
  - Proprietární řešení

Vlastnosti uživatelských účtů

- Hesla
  - User must change password at next logon
  - User cannot change password
  - Password never expires
  - Account is disabled
- Unikátní
  - Common name v rámci nejbližšího kontejneru
  - Login v rámci celé domény

ds nástroje

- dsadd – přidání objektu
- dsmod – úprava objektu
- dsget – zobrazení vlastností objektu
- dsquery – nalezení objektů v adresáři
- dsmove – přesun objektu
- dsrm – odstranění objektu

- Př.:

  dsadd user CN=Homer,CN=Users,DC=springfield,DC=local -samid Homer -pwd Pa$$w0rd

ldifde

- LDAP Data Interchange format directory exchange
- import/export účtů ve velkém množství
  - Import: ldifde –i –f INPUT.LDF
  - Export: ldifde –f OUTPUT.LDF
- Struktura souboru:

```
dn: CN=Bart Simpson,OU=SotB,OU=Student,DC=springfield,DC=local
changetype: add
cn: Bart Simpson
objectclass: user
givenname: Bart
sn: Simpson
```

csvde

- Comma-separated values directory exchange
- import/export účtů ve velkém množství
  - Import: csvde –i –f INPUT.CSV
  - Export: csvde –f OUTPUT.CSV
- Struktura souboru:

dn,UserPrincipalName,objectClass,givenName,sn
"CN=Bart Simpson,OU=SotB,OU=Student,
DC=springfield,DC=local",bart@springfield.local,user,Bart,Simpson

Úkoly

1. Zapojit do domény klientský počítač
2. Vytvořit uživatelský účet nástrojem AD Users and Computers
3. Zakázat/povolit tento účet
4. Resetovat účtu heslo
5. Vytvořit skupinu v AD Users and Computers
6. Vložit do skupiny další účty i další skupiny
7. Zkontrolovat access token (whoami /all)
8. Vytvořit účet příkazem dsadd a upravit ho přes dsmod
9. Vytvořit účty nástrojem ldifde