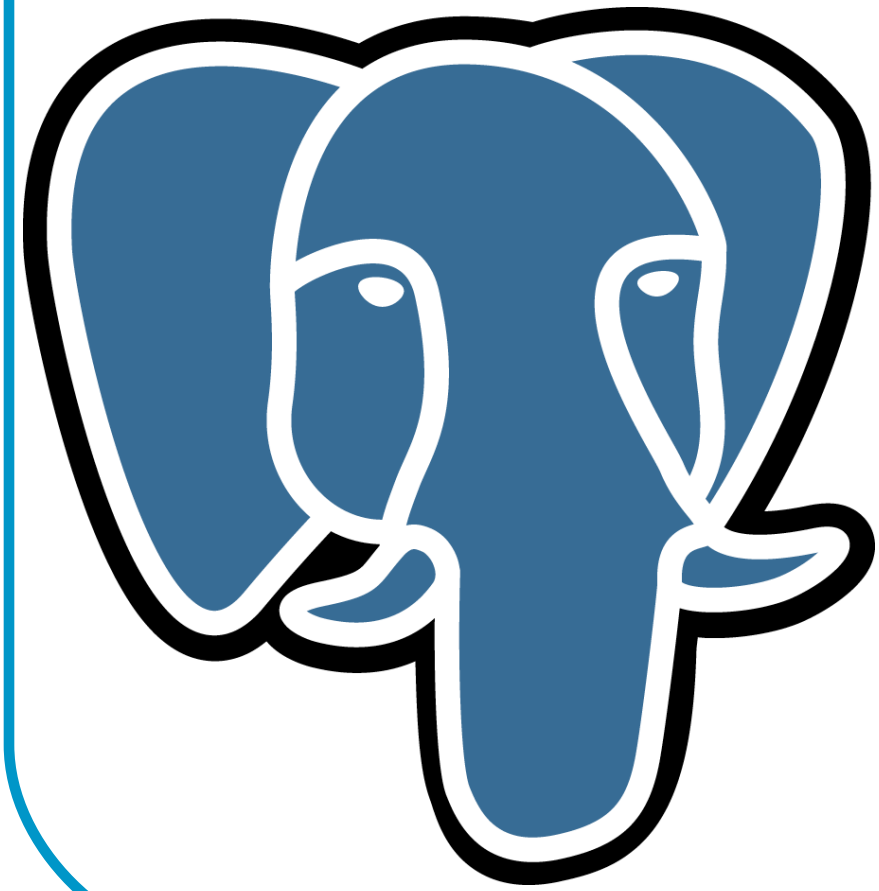
Deploying PostgreSQL in a Windows Enterprise



Magnus Hagander
magnus@hagander.net

PGCon 2008

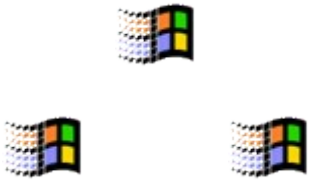
Ottawa, Canada
May 2008

Agenda

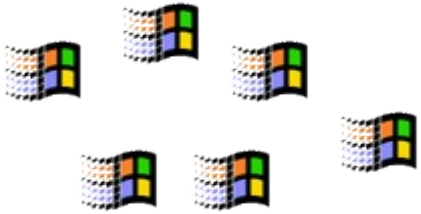
- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

What is a Windows Enterprise?

Servers



Clients

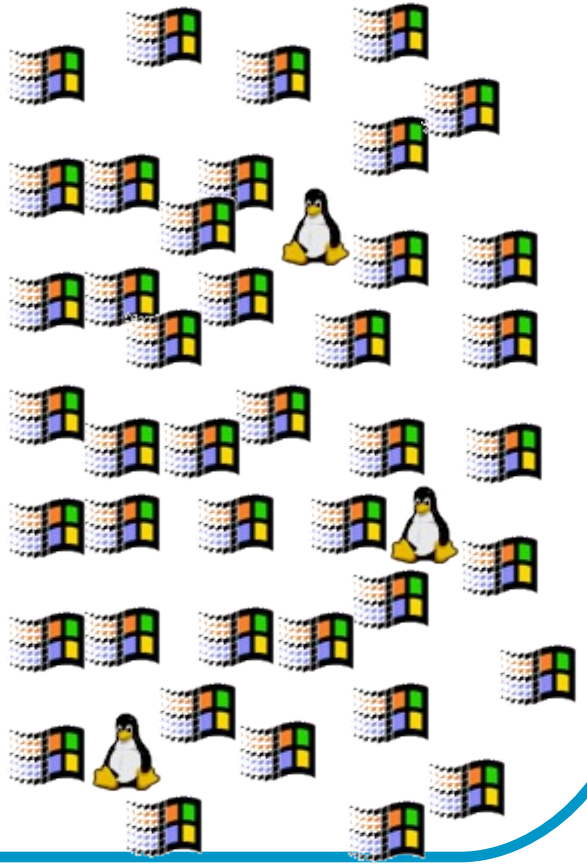


What is a Windows Enterprise?

Servers

WEB

Clients

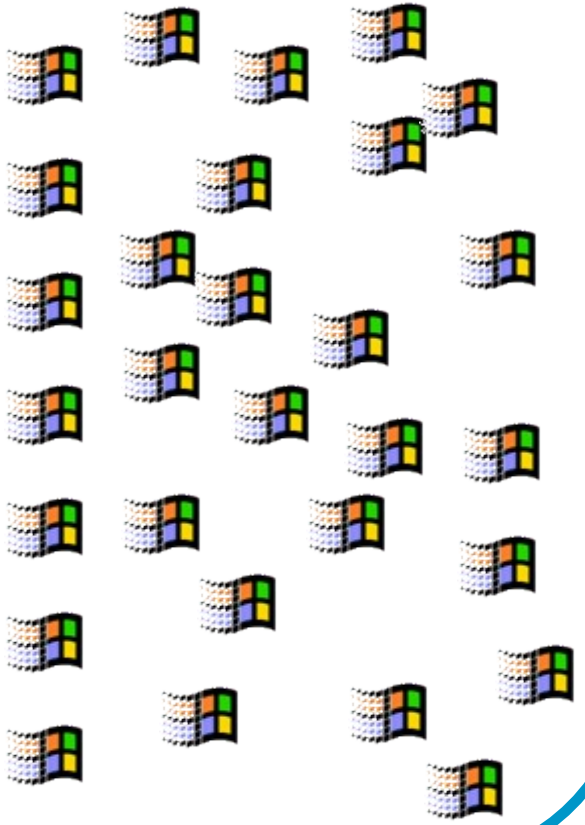


What is a Windows Enterprise?

Servers

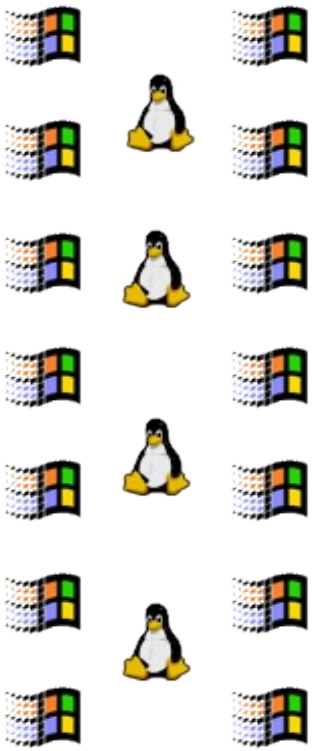
Active Directory

Clients



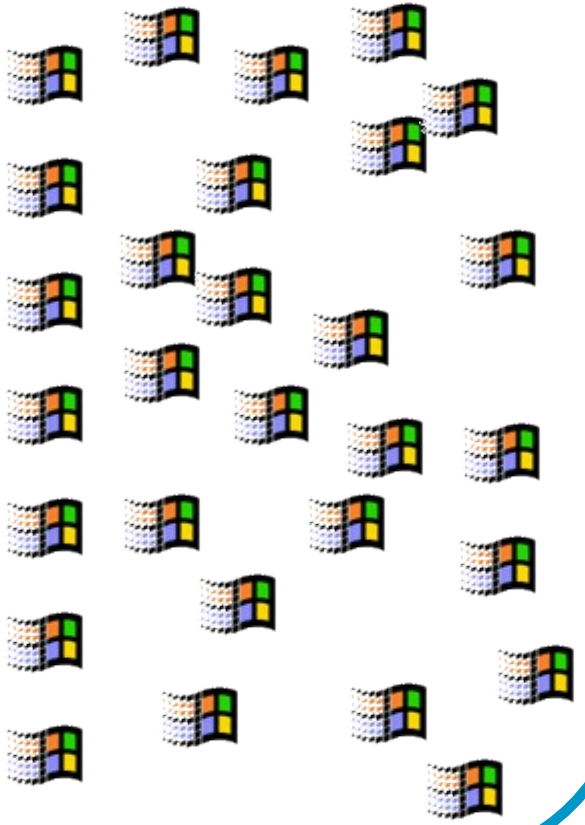
What is a Windows Enterprise?

Servers



Active Directory

Clients



Agenda

- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

Installation

- MSI installer
- Integrates with existing products
- Installs all dependencies
- Create account, sets permissions
- Supports silent install
- Server only, Server+client, Client only

Installation

- ”xcopy deployment”
- No registry entries required!
  - Well, there's ODBC...
- binaries-no-installer.zip
- Dependencies, account, permissions
- Custom build

Agenda

- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

Active Directory authentication

- ”Integrated authentication”
  - Already logged in, why do it again?
- Fat clients
  - Web apps usually uses password to db
- Very common for SQL Server/Access
- Still need to create db user!

Active Directory authentication

- Client interface dependent
- libpq or ”built on libpq”
- ODBC
- JDBC
- npgsql

Active Directory authentication

- Windows-to-windows trivial

```
host all all 0.0.0.0/0 sspi
```

- Set your AD policies!
- Always included

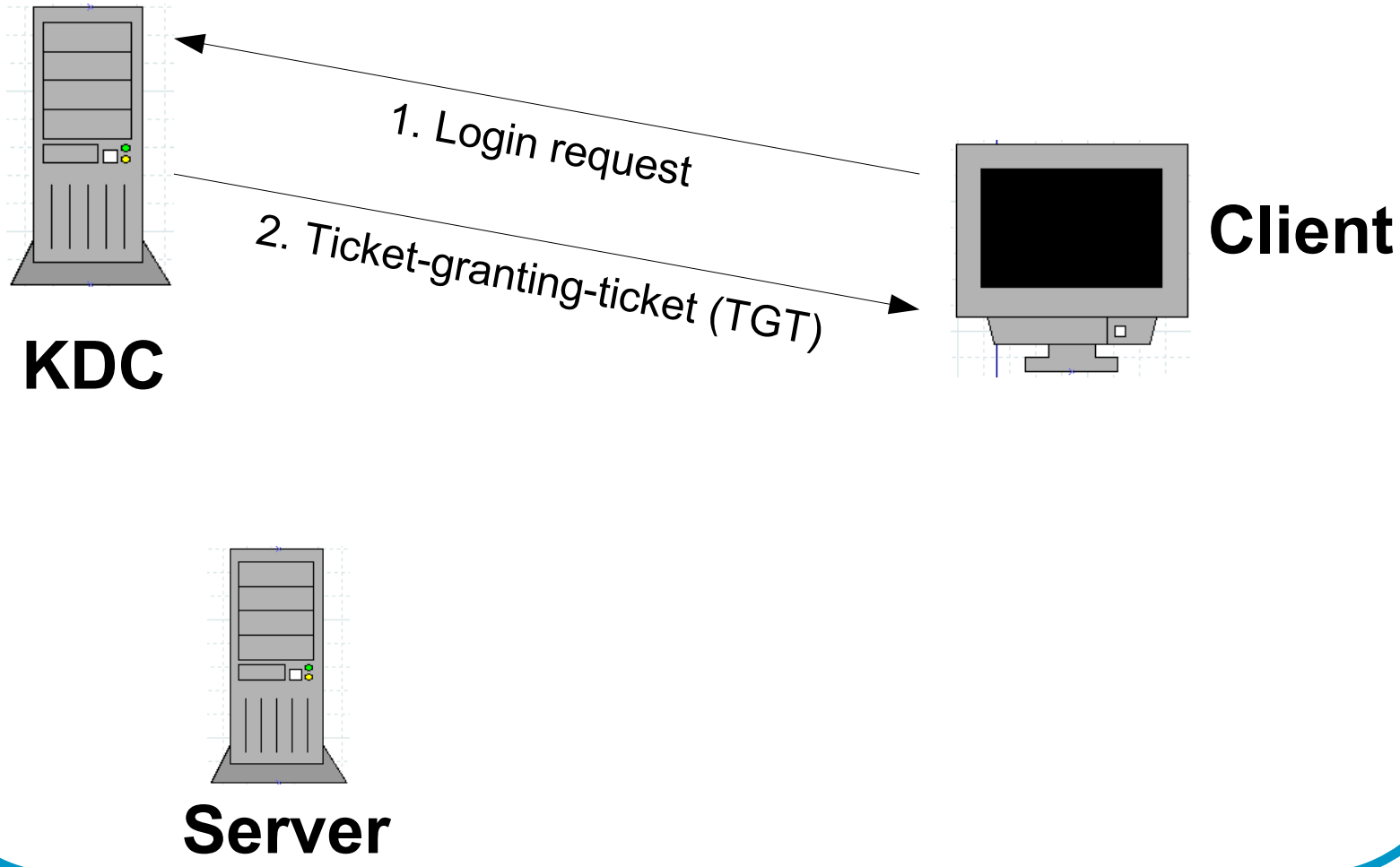
Active Directory authentication

- Windows-to-unix a bit more work
- Kerberos only

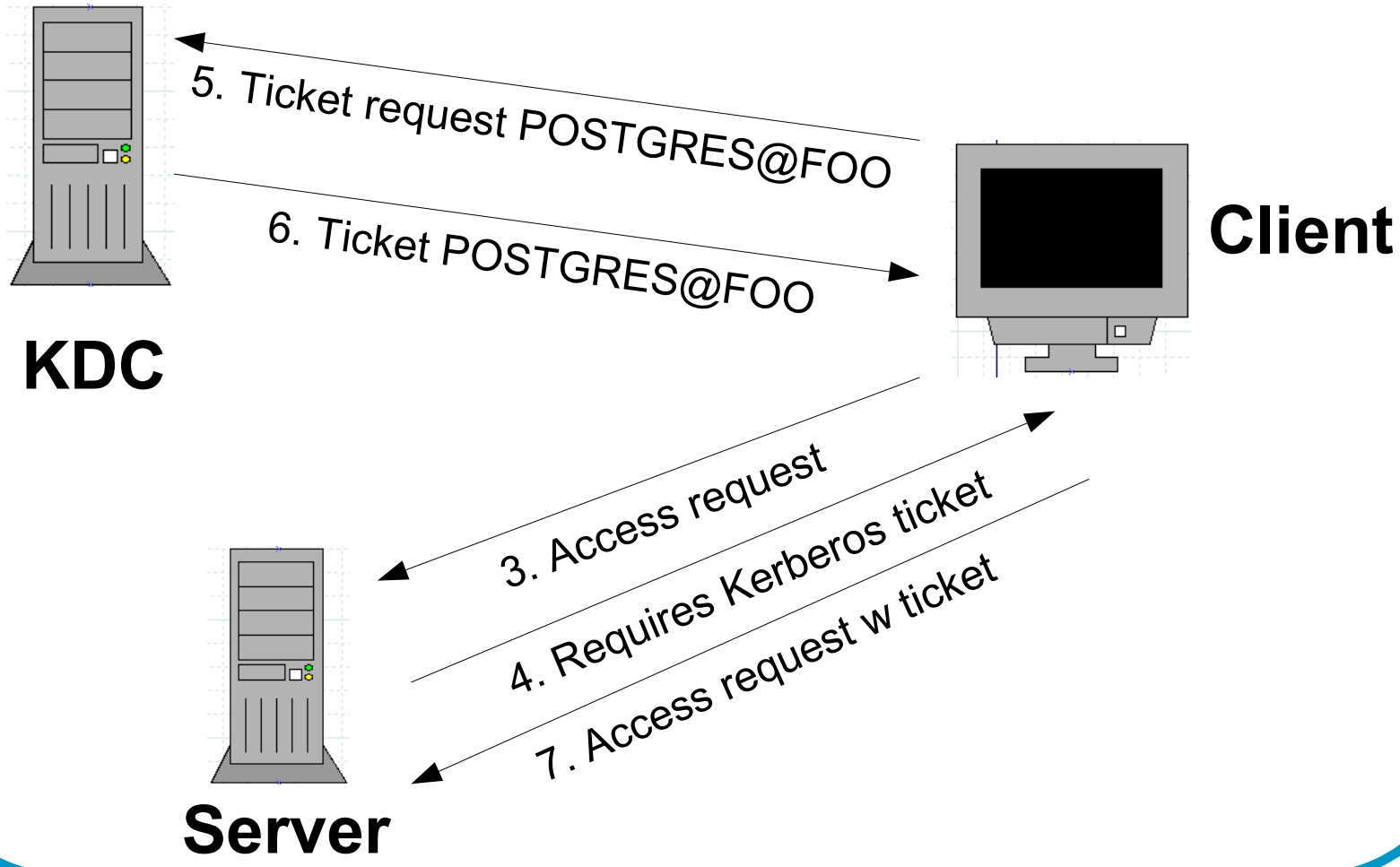
Kerberos 101

- Cross platform, standards-based, secure, distributed authentication
- Shared secrets between hosts
- Maintained and controlled by KDC
- Trusted tickets
- Single sign-on

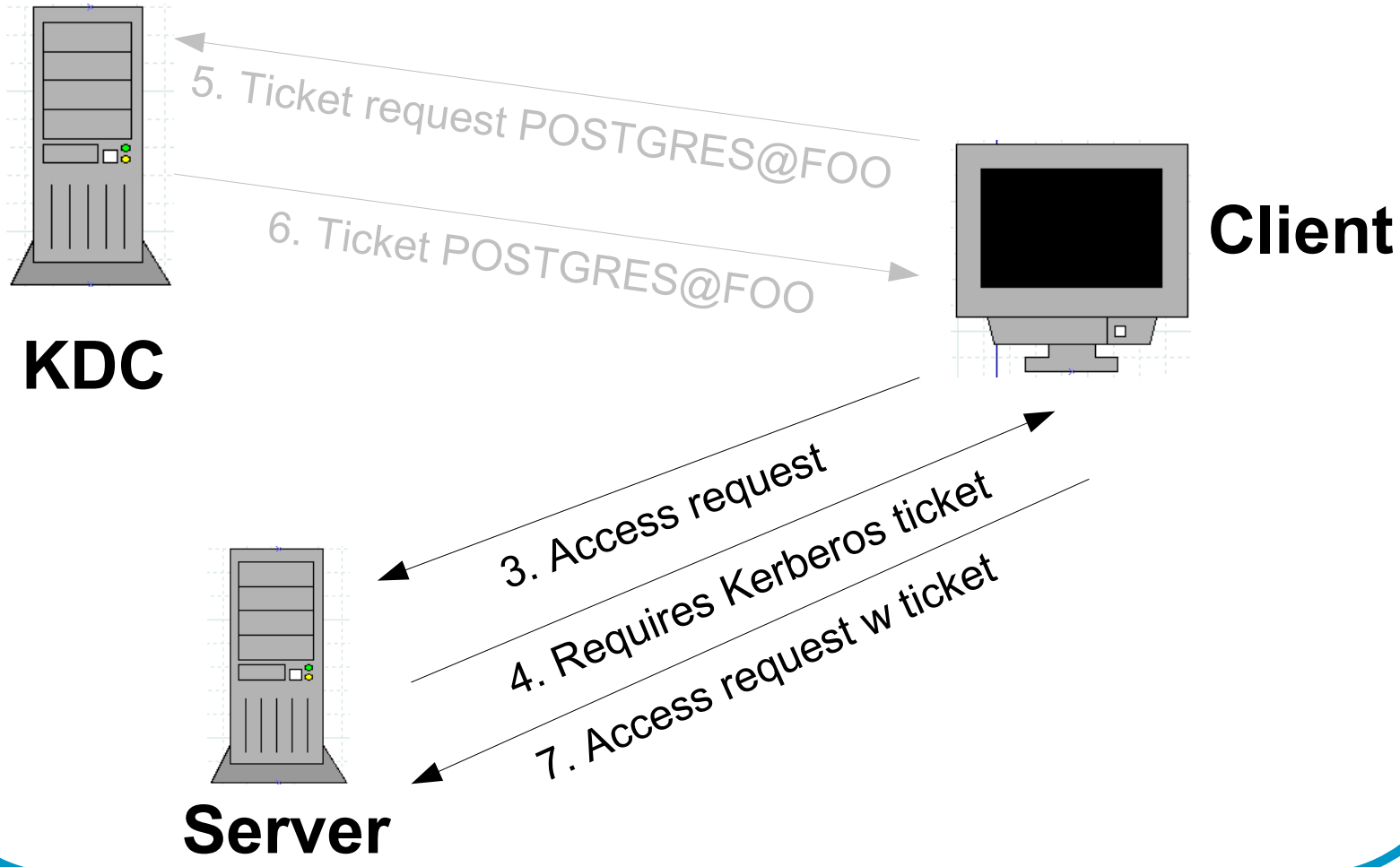
Kerberos 101



Kerberos 101



Kerberos 101



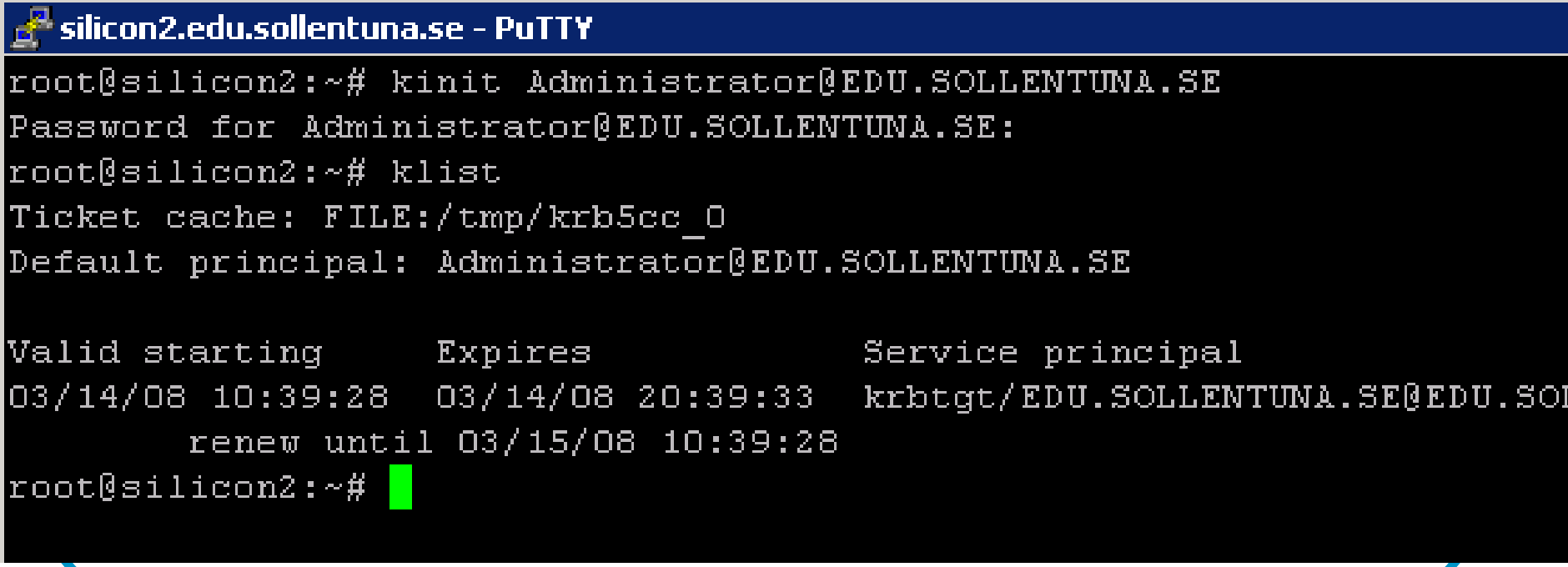
Active Directory authentication

- Windows-to-unix a bit more work
- Kerberos only, requires service principals
  - AD enforces non-standard name
- Basic Kerberos first!
  - /etc/krb5.conf

```
[libdefaults]
 default_realm = DOMAIN.COM
 [domain_realm]
 domain.com = DOMAIN.COM
 .domain.com = DOMAIN.COM
```

Active Directory authentication

- Verify with kinit/klist
  - kinit administrator@DOMAIN.COM

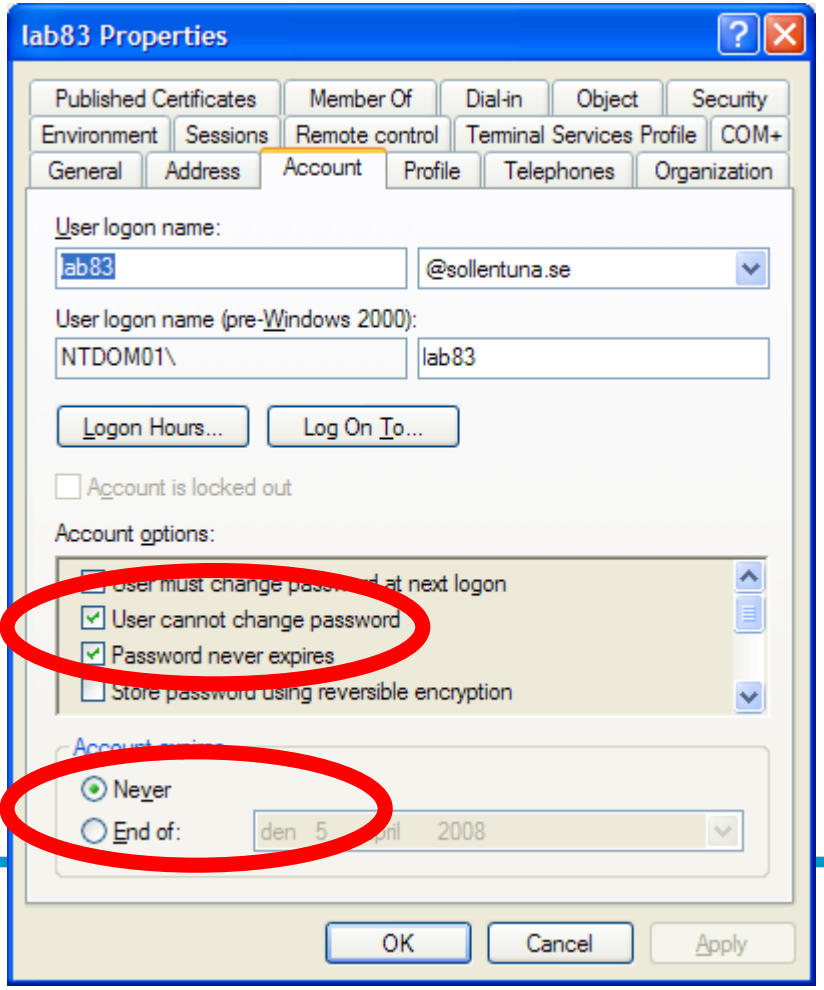


Active Directory authentication

- Install required build packages
- ./configure --with-gssapi
- Build + install as usual
- Initdb as usual

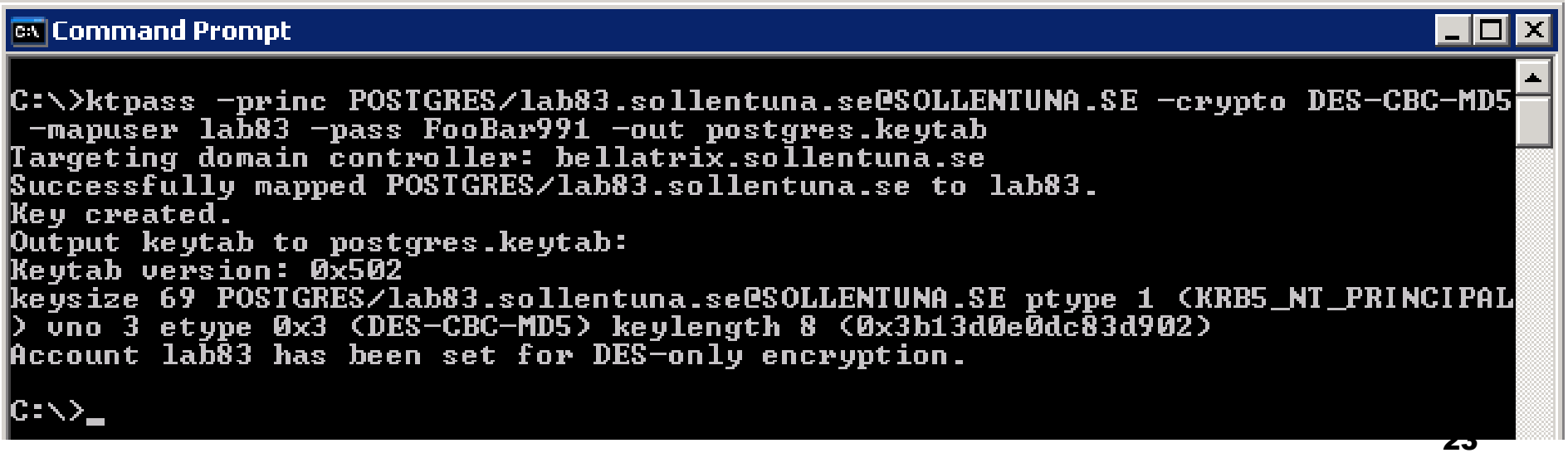
Active Directory authentication

- Create service principal (ordinary user)



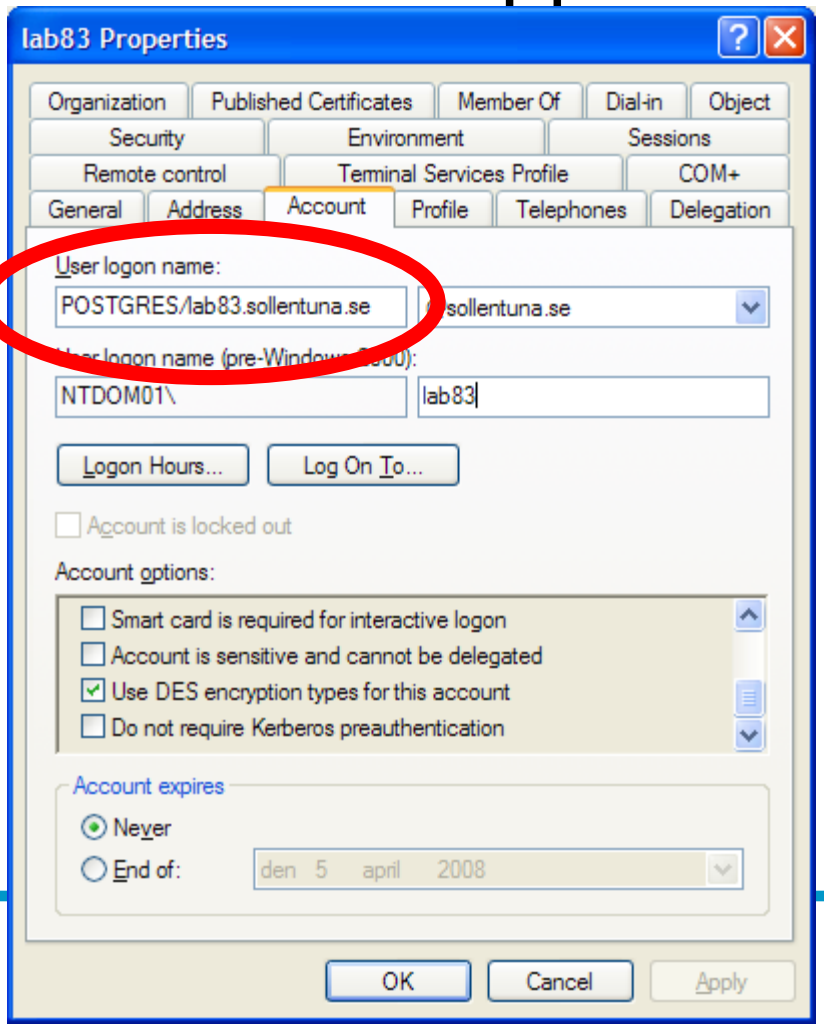
Active Directory authentication

- Create Kerberos principal mappnig
- **ktpass**
  -princ POSTGRES/lab83.domain.com@DOMAIN.COM
  -crypto DES-CBC-MD5
  -mapuser lab83
  -pass FooBar991
  -out postgres.keytab



Active Directory authentication

- Verify account is mapped



Active Directory authentication

- postgresql.conf

```
listen_addresses = '*'
krb_server_keyfile =
   '/var/pgsql/data/postgres.keytab'
krb_srvname = 'POSTGRES'
```

- pg_hba.conf

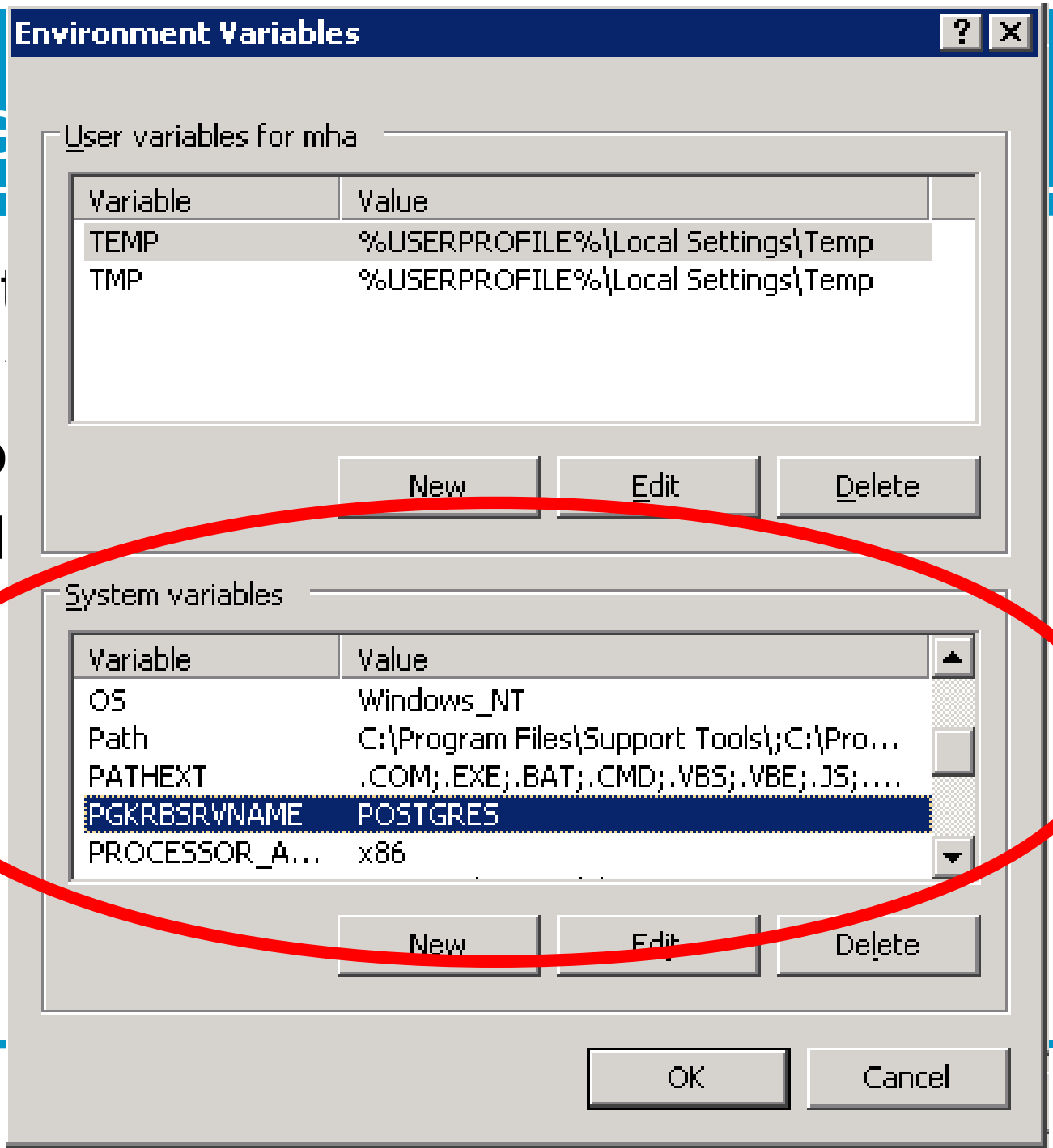
```
host all all 0.0.0.0/0 gss
```

Active Directory authentication

- Client side principal name
  - Environment: PGKRBSRVNAME
  - Connection string: krbsrvname
- Needed on both Windows and Unix

Active

- Client
  - En
  - Co
- Need



LDAP Authentication

- For clients that don't support GSS/SSPI
- If you actually *want* passwords
- Looks like password prompt to client
- pg_hba.conf

```
host all all 0.0.0.0/0 ldap
 "ldap://dc.domain.com/dc=domain,dc=com;DOMAIN\"
```

Agenda

- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

Access AD data

- dblink-ldap (pgfoundry)
- Build from source only
- Create VIEWs of LDAP data
- Read-only

Access AD data

```
CREATE VIEW users AS

  SELECT * FROM dblink_ldap(
   'dc.domain.com',
   'CN=Users, DC=domain, DC=com',
   E'DOMAIN\\User', 'password',
   '(objectClass=user)',
   'distinguishedName,cn,displayName')

  t(dn, cn, displayName)
```

Access AD data

```
postgres=# SELECT * FROM users;
                     dn                          |      cn       |   displayname
-------------------------------------------------------------------------------
CN=mha,CN=Users,DC=domain,DC=com                 | mha           | Magnus Hagander
CN=Administrator,CN=Users,DC=domain,DC=com       | Administrator | Admin
(2 rows)
```

Agenda

- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

Monitoring

- Performance Monitor for system parameters
- pgsnmpd (unix only)
- pg_stat_xyz views

Future directions

- schannel encryption
- schannel certificate authentication
- Better monitoring support
  - pgsnmpd on windows or
  - native performance monitor plugin

Thank you!

Questions?