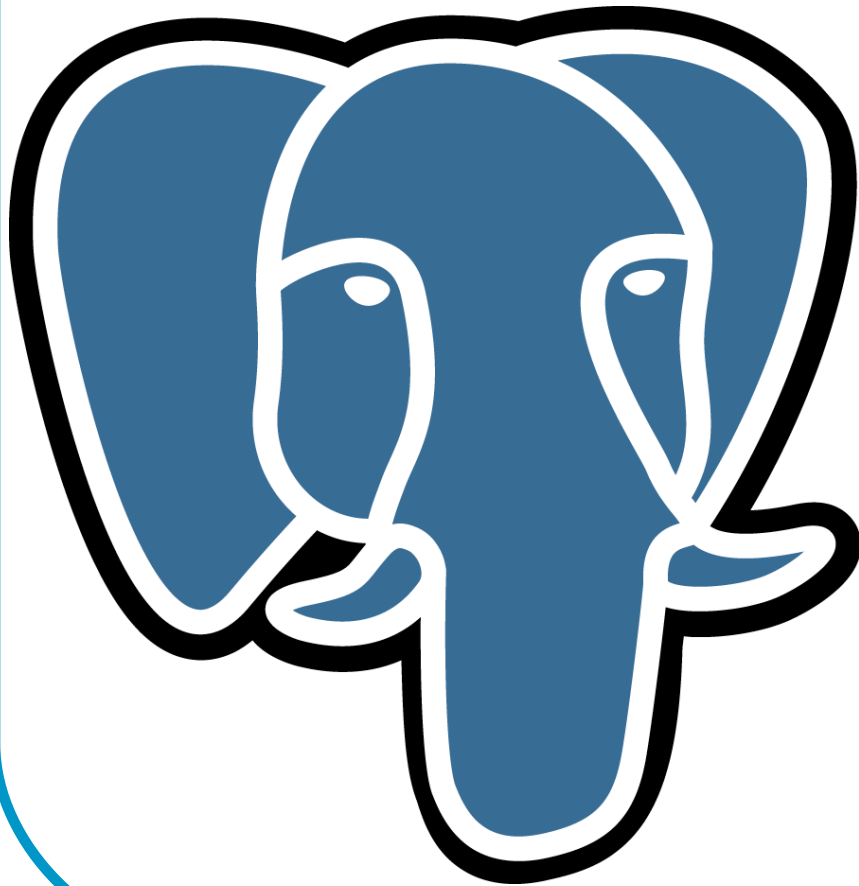


# Deploying PostgreSQL in a Windows Enterprise



Magnus Hagander  
magnus@hagander.net

PGCon 2008

Ottawa, Canada  
May 2008

# Agenda

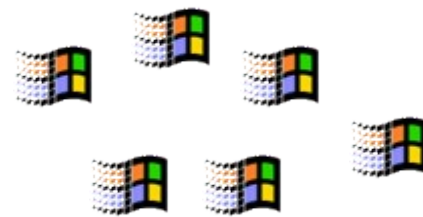
- Definition
- Installation
- Active Directory
  - Authentication - integrated
  - Authentication - LDAP
  - Data access
- Monitoring

# What is a Windows Enterprise?

Servers

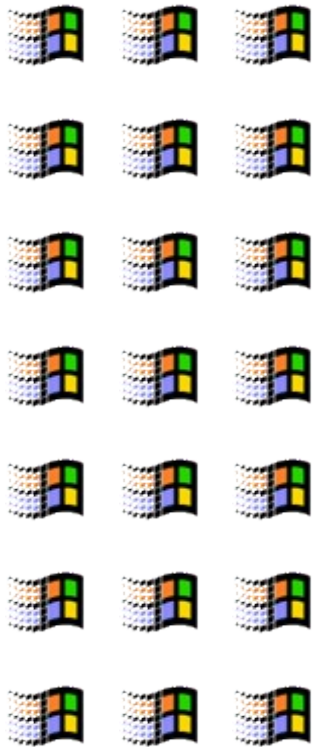


Clients



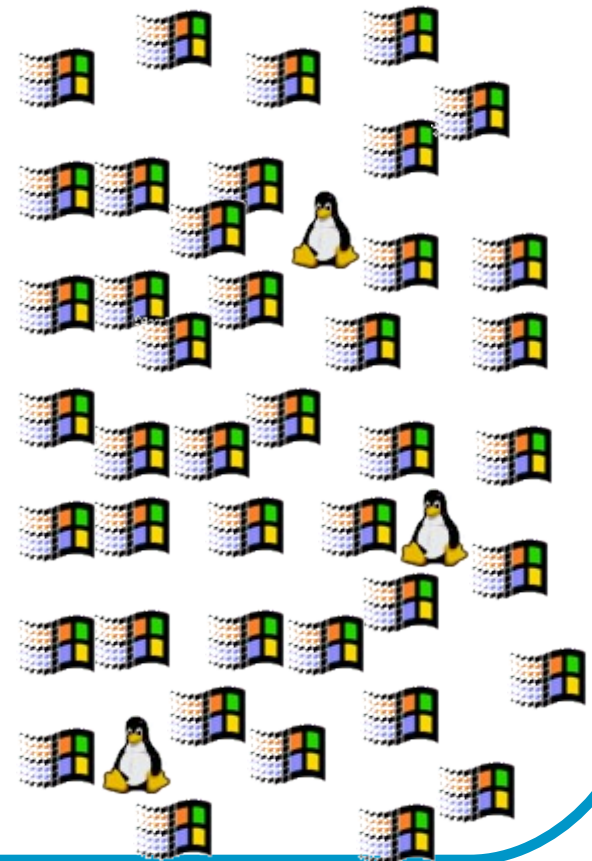
# What is a Windows Enterprise?

Servers



WEB

Clients



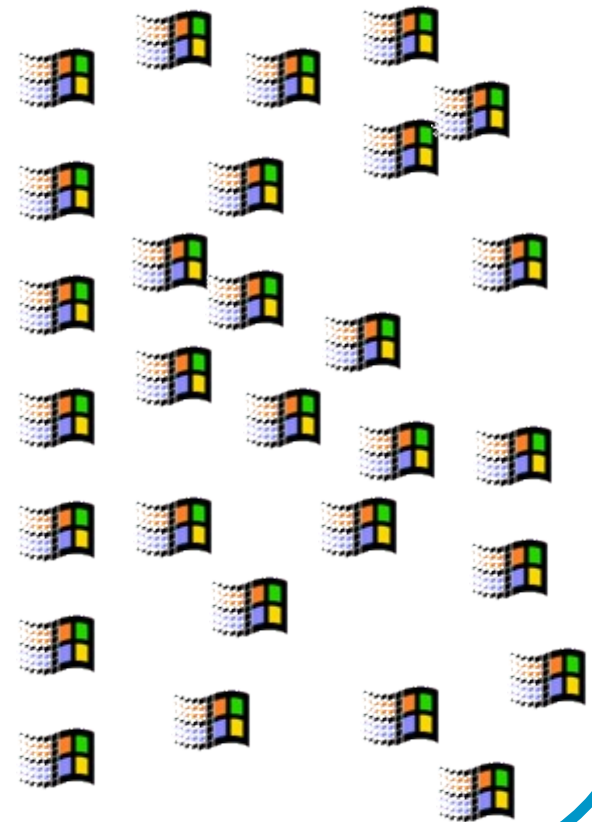
# What is a Windows Enterprise?

Servers



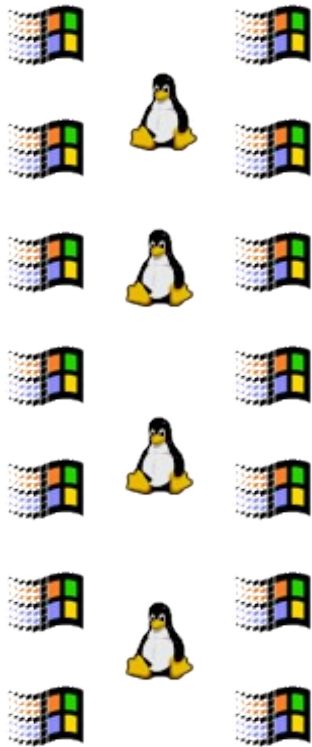
Active Directory

Clients



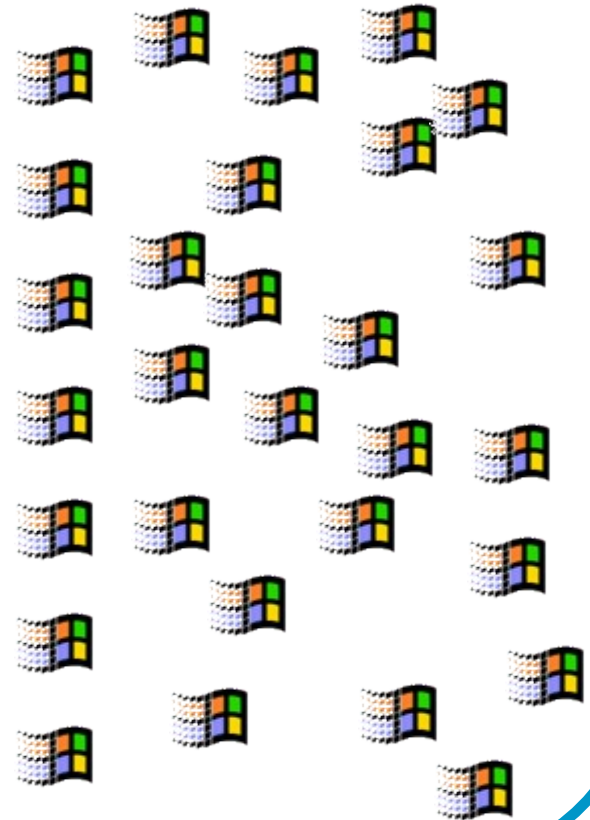
# What is a Windows Enterprise?

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

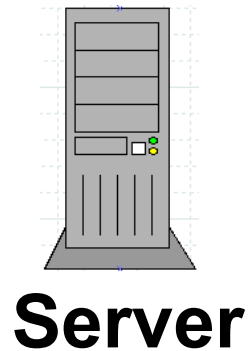
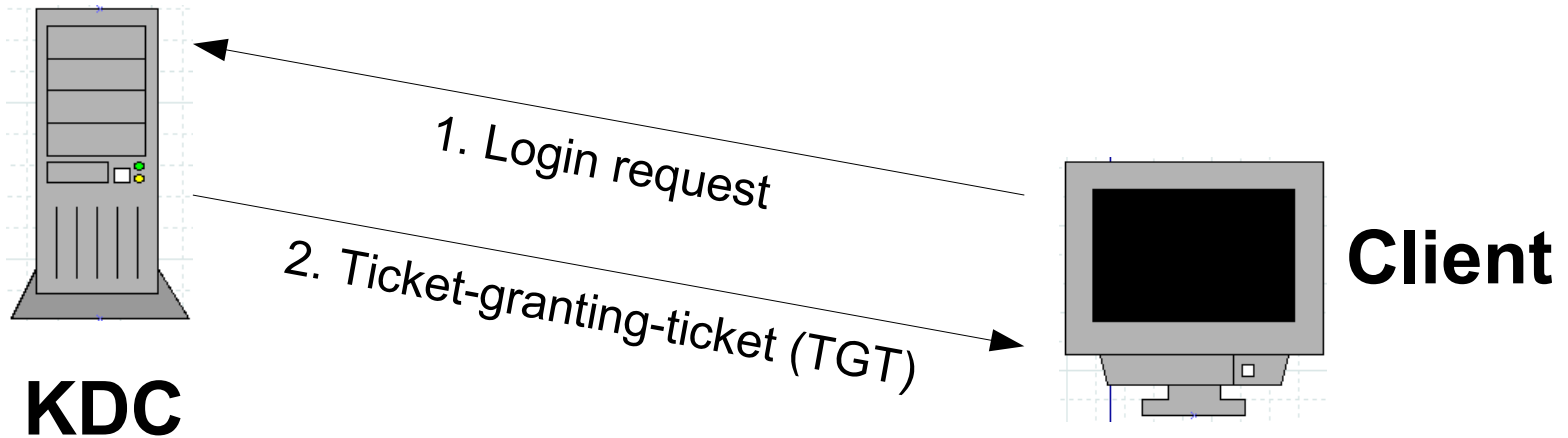
# Active Directory authentication

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

# Kerberos 101

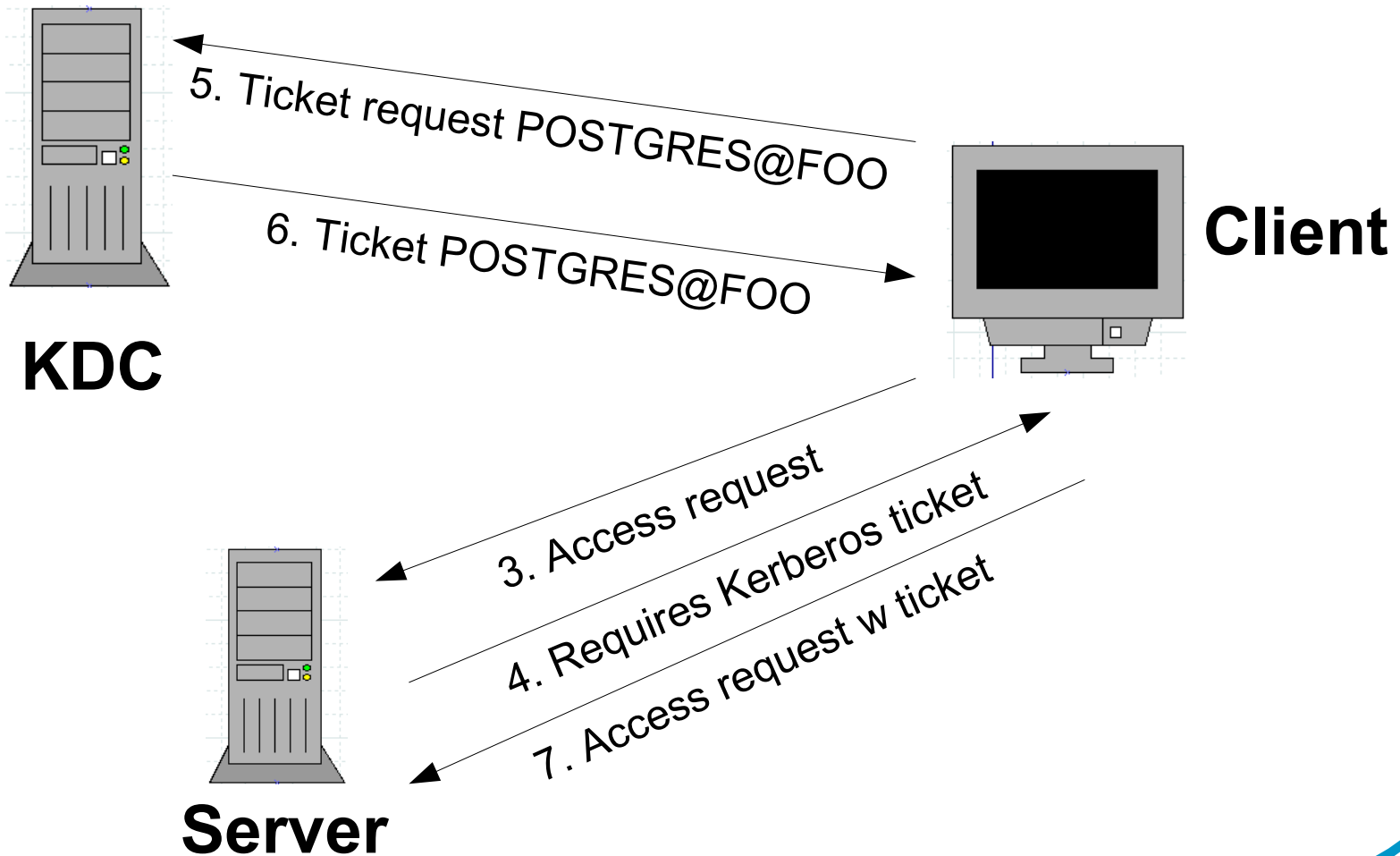
- Cross platform, standards-based, secure, distributed authentication
- Shared secrets between hosts
- Maintained and controlled by KDC
- Trusted tickets
- Single sign-on

# Kerberos 101

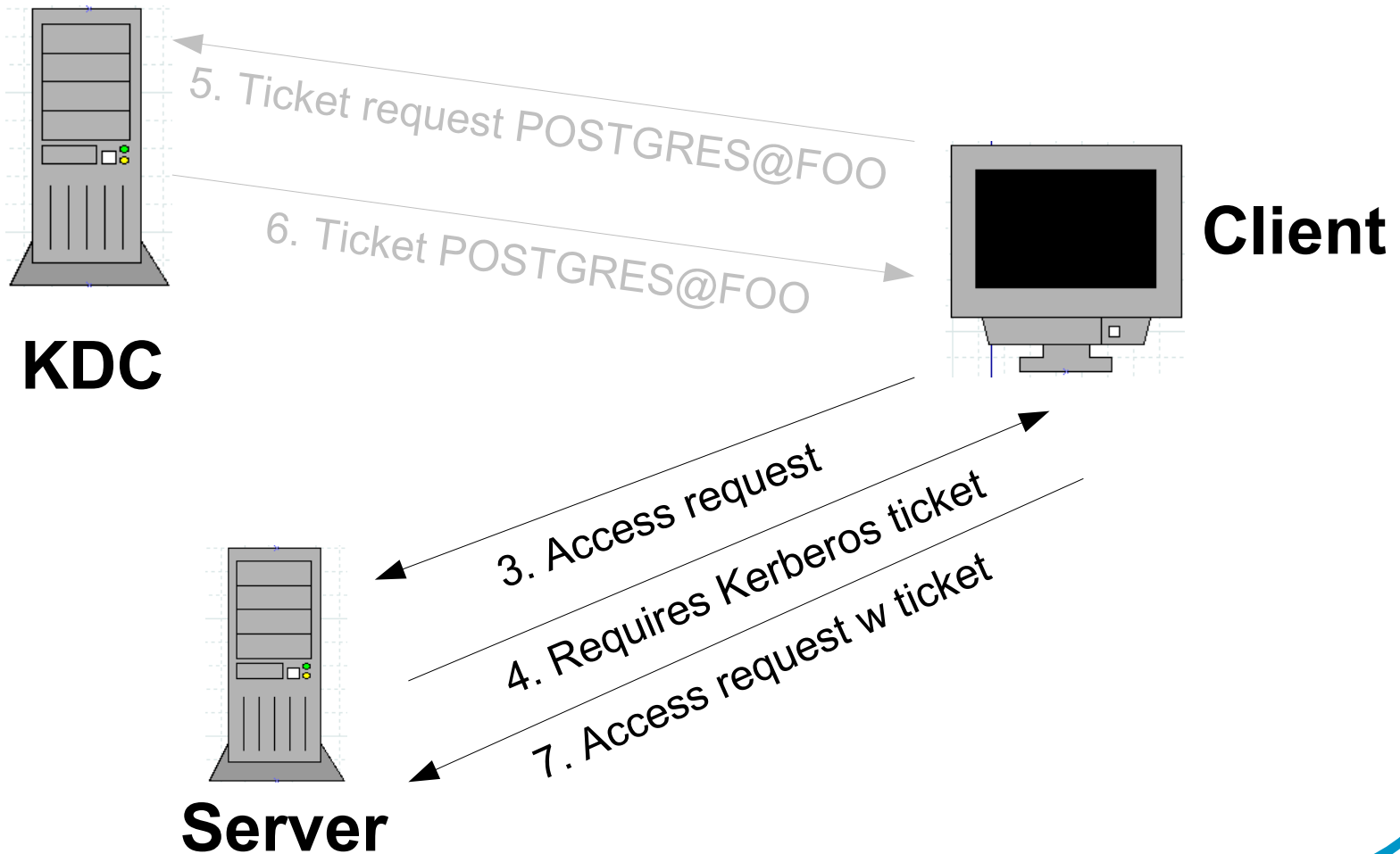




# Kerberos 101



# 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



silicon2.edu.sollentuna.se - PuTTY

```
root@silicon2:~# kinit Administrator@EDU.SOLLENTUNA.SE
```

```
Password for Administrator@EDU.SOLLENTUNA.SE:
```

```
root@silicon2:~# klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0
```

```
Default principal: Administrator@EDU.SOLLENTUNA.SE
```

```
Valid starting      Expires            Service principal
```

```
03/14/08 10:39:28   03/14/08 20:39:33   krbtgt/EDU.SOLLENTUNA.SE@EDU.SOLLENTUNA.SE
```

```
    renew until 03/15/08 10:39:28
```

```
root@silicon2:~# █
```

# 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)

The screenshot shows the 'lab83 Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'lab83@sollentuna.se'. The 'User logon name (pre-Windows 2000)' is 'NTDOM01\lab83'. The 'Account options' section has the following settings:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

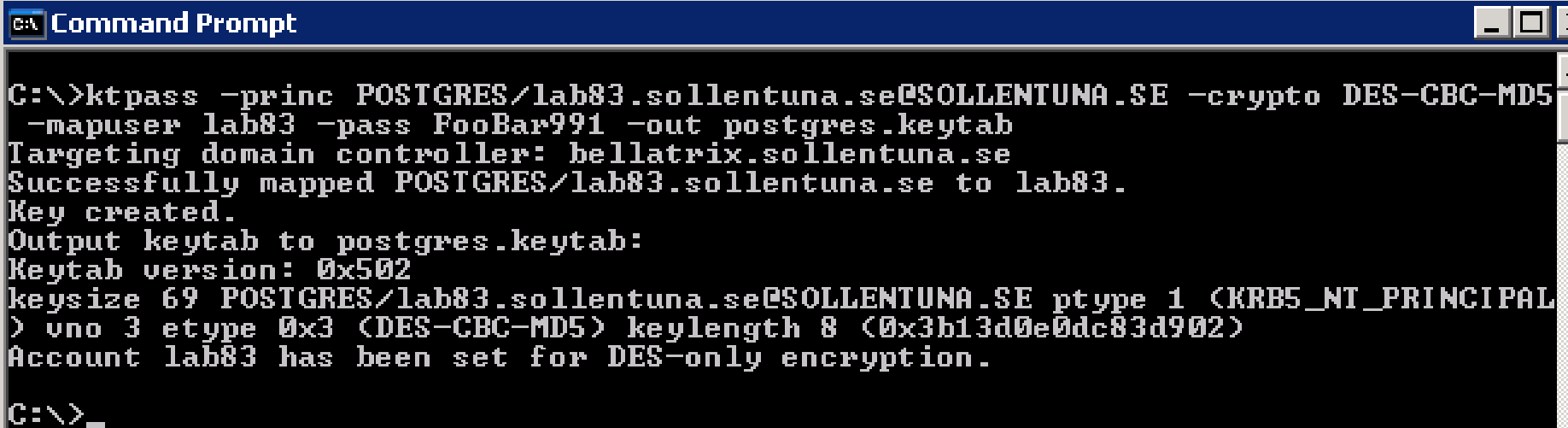
The 'Account expiration' section has the following settings:

- Never
- End of: den 5 april 2008

Red circles highlight the 'User cannot change password', 'Password never expires', and 'Never' options.

# 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

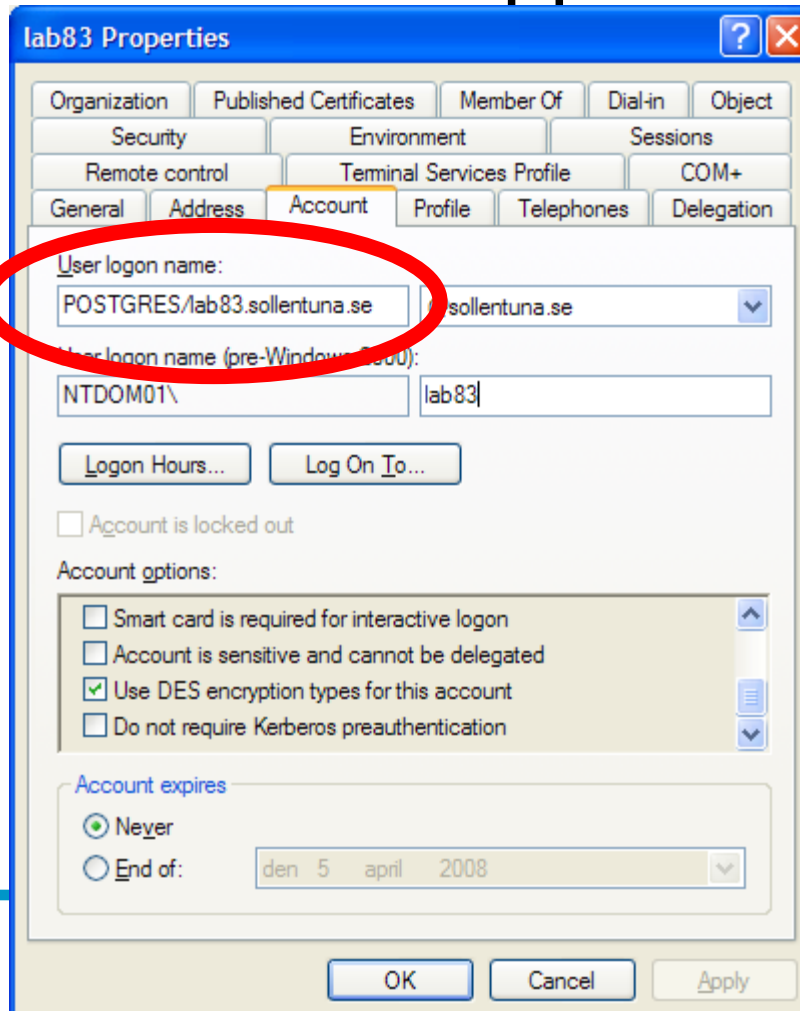


```
C:\>ktpass -princ POSTGRES/lab83.sollentuna.se@SOLLENTUNA.SE -crypto DES-CBC-MD5
-mapuser lab83 -pass FooBar991 -out postgres.keytab
Targeting domain controller: bellatrix.sollentuna.se
Successfully mapped POSTGRES/lab83.sollentuna.se to lab83.
Key created.
Output keytab to postgres.keytab:
Keytab version: 0x502
keysize 69 POSTGRES/lab83.sollentuna.se@SOLLENTUNA.SE ptype 1 (KRBS_NT_PRINCIPAL
) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0x3b13d0e0dc83d902)
Account lab83 has been set for DES-only encryption.

C:\>_
```

# Active Directory authentication

- Verify account is mapped



The screenshot shows the 'lab83 Properties' dialog box with the 'Account' tab selected. The 'User logon name' field is circled in red and contains the text 'POSTGRES/lab83.sollentuna.se'. Below it, the 'User logon name (pre-Windows 2000):' field contains 'NTDOM01\lab83'. The 'Account options' section has 'Use DES encryption types for this account' checked. The 'Account expires' section has 'Never' selected.

lab83 Properties

Organization Published Certificates Member Of Dial-in Object

Security Environment Sessions

Remote control Terminal Services Profile COM+

General Address Account Profile Telephones Delegation

User logon name:  
POSTGRES/lab83.sollentuna.se

User logon name (pre-Windows 2000):  
NTDOM01\lab83

Logon Hours... Log On To...

Account is locked out

Account options:

Smart card is required for interactive logon

Account is sensitive and cannot be delegated

Use DES encryption types for this account

Do not require Kerberos preauthentication

Account expires

Never

End of: den 5 april 2008

OK Cancel Apply



# Active Directory authentication

- postgresql.conf

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

- pg\_hba.conf

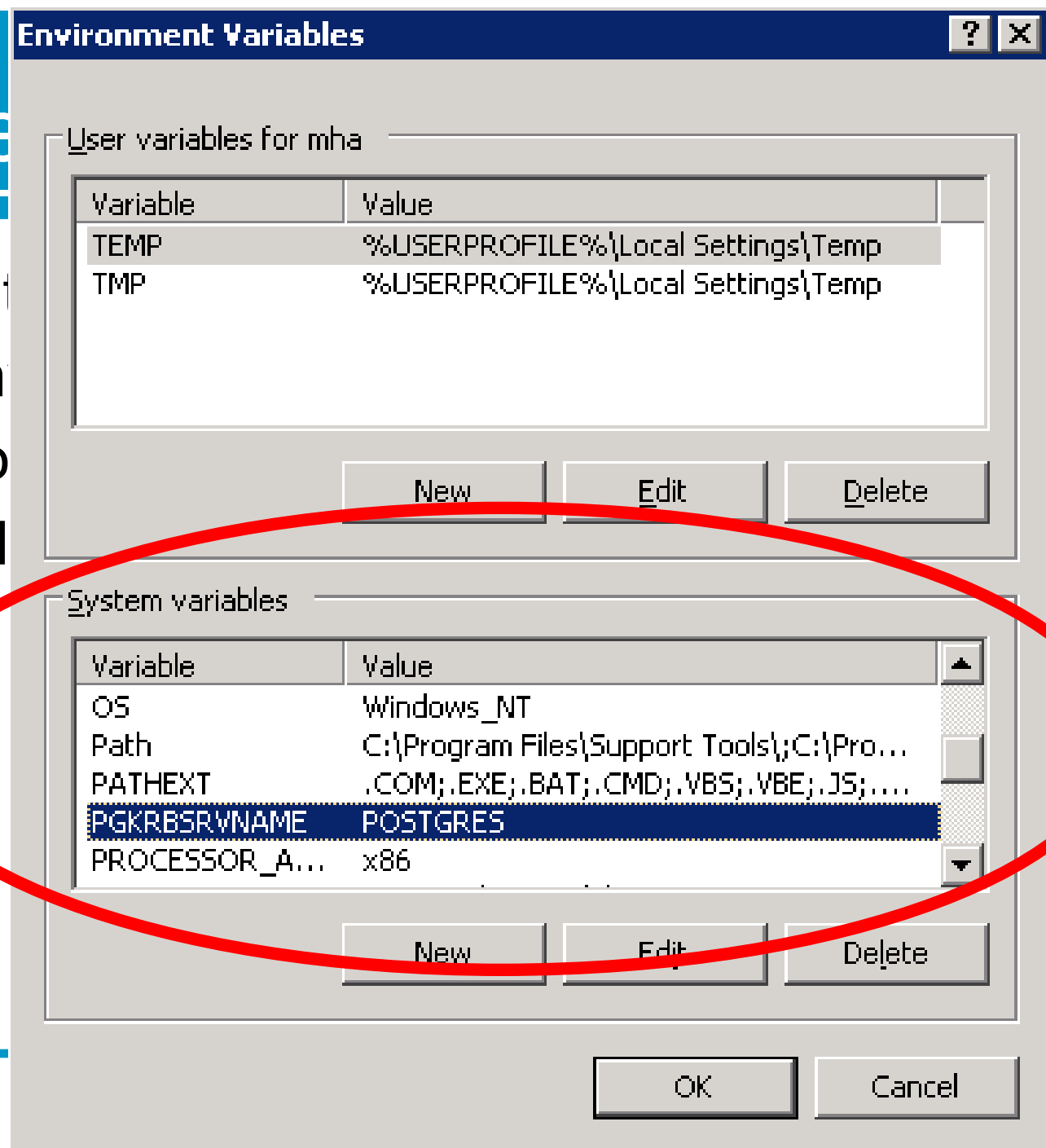
```
host all all 0.0.0.0/0 gss
```

# 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?