SUSE Linux Enterprise Server in an Active Directory Domain

Gábor Nyers
Systems Engineer @SUSE
gnyers@suse.com
Agenda

Introduction
Practical scenario's for SLES 11 SP2:
  › Participating in an Active Directory
  › Integration of Apache with Active Directory

Bleeding Edge Samba 4
  › Server side copy
  › Prototype implementation of “Previous versions”

Questions
Introduction
Data Center Interoperability
The Playfield

Platforms

Observable trends (in general):

- Legacy Unix holds or declines
- Mainframe:
  - z/OS holds
  - Linux on System z emerging
- Linux and Windows grow
Linux – Windows Interoperability
The playfield

Platforms

Interoperability Topics

Scope:

Services

Virtualization

Systems Management

Documents

Scripting Languages

Porting and running software
Linux – Windows Interoperability Scenario's
Practical scenario's

1. SLES Participating in an Active Directory domain

2. Integration of Apache with Active Directory
Linux – Windows Interoperability Scenario's
Practical value vs. Maturity

1. SLES Participating in an Active Directory domain
2. Integration of Apache on SLES with Active Directory
3. SLES and Samba as domain controller
4. Windows Remote Desktop on Linux
5. ODBC connection to MS SQL
6. Prototype Samba implementation of “Recovery Point”
Practical scenario's for SLES 11 SP2
Scenario 1:
SLES as member server in Active Directory domain

Role: Member server
AD: ad.demo.lan
Hostname: interop01

See also:
- more detailed documentation
- Interop Demo appliance
Scenario 1: Join as member server in Active Directory domain

• Pre-requisites
  › Correct NTP settings
  Correct timezone settings
  › Correct DNS name, forward and backward for all hosts
  › Authorized AD service account to join machines (typically “Administrator”)

• Concepts
  › Kerberos
    ♦ Principal / Service Principal
    ♦ Ticket Granting Ticket
    ♦ Keytab file
  › LDAP
    ♦ sssd (System Security Services Daemon)
  › PAM, NSS
  › SASL, GSSAPI, SPNEGO
Scenario 1: Join as member server in Active Directory domain

- **Steps on Linux**
  - openSUSE, SUSE Linux Enterprise:
    Join the AD domain using `YaST → Windows Domain Membership`
  - Other Linux distros:
    Join the AD domain with the **manual procedure**
    (smb.conf; krb5.conf; `net ads join -U Administrator%password`)

- **Required packages on SLES**:
  - samba-client,
  - samba-winbind(pam_winbind.so, libnss_winbind.so, idmap)
  - krb5 (libgssapi_krb5)

- **Steps on Active Directory**
  - No requisite steps
Scenario 1:
Use Case 1/a: Integrate PAM and nsswitch with AD

/etc/pam.d/common-auth

interop01:~ # cat /etc/pam.d/common-auth
#%PAM-1.0
auth    required    pam_env.so
auth    sufficient  pam_unix2.so
auth    required    pam_winbind.so  use_first_pass
interop01:~ #

/etc/nsswitch.conf

interop01:~ # cat /etc/nsswitch.conf
# [...]  
passwd: winbind compat
group:  winbind compat
# [...]  
interop01:~ #
Scenario 1:
Use Case 1/a: Integrate SSHD with AD

Configure SSHD
interop01:~ # cat /etc/ssh/sshd_config
# [...]  
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
ChallengeResponseAuthentication yes
# [...]  
interop01:~ #

Login from remote host
remote-host:~ $ ssh 'INTEROP\Administrator'@interop02
Password:
Creating directory '/home/INTEROP/administrator'.
INTEROP\administrator@interop02:~>

Kerberos credentials
INTEROP\administrator@interop02:~> klist
Ticket cache: FILE:/tmp/krb5cc_10000
Default principal: Administrator@AD.DEMO.LAN

Valid starting     Expires       Service principal
               04/06/13 10:22:28  04/06/13 20:22:28  krbtgt/AD.DEMO.LAN@AD.DEMO.LAN
            renew until 04/13/13 10:22:28
               04/06/13 10:22:28  04/06/13 20:22:28  INTEROP02$@AD.DEMO.LAN
            renew until 04/13/13 10:22:28

Kerberos 4 ticket cache: /tmp/tkt10000
klist: You have no tickets cached
INTEROP\administrator@interop02:~>
Scenario 1: Use Case 1/b: Restrict shell access to AD group

• Steps on SLES
  › Manually amend the pam_winbind configuration file to restrict allowed users

• Steps on Active Directory
  › Add group “SLES Shell Users”
  › Add user “Administrator” to “SLES Shell Users”

/etc/security/pam_winbind.conf

[global]
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
debug = yes
require_membership_of = "SLES Shell Users"

See also: Interop Demo appliance
Scenario 1:
Use Case 2: Integrate **SPNGO** enabled applications with AD

- Applications using GSSAPI, SASL or Java GSS libraries

- GSSAPI
  - SLES pkg: krb5 (1.6+)
  - C lib: /usr/lib64/libgssapi_krb5.so.2
  - Java lib: Java GSS
  - Applications:
    - Mod_auth_kerb (Apache), PostgreSQL, etc..

- SASL API
  - SLES pkg: cyrus-sasl
  - C lib: /usr/lib64/libsasl2.so.2
  - Java lib: Java SASL
  - Applications:
    - OpenLDAP2 (Server, clients)
    - Cyrus IMAP, etc...
    - Postfix
    - Libvirt
    - Evolution
Use Case 2: Integrate SPNGO enabled applications with AD: smbclient

• Steps
  • Request TGT with kinit or log in as an AD user
  • Access Windows share with smbclient

interop01:~ # id
uid=0(root) gid=0(root) groups=0(root)
interop01:~ # kinit demo@AD.DEMO.LAN
Password for demo@AD.DEMO.LAN: <PASSWORD>
interop01:/tmp # klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: demo@AD.DEMO.LAN

Valid starting     Expires            Service principal
03/07/13 10:08:48  03/07/13 20:08:55
krbtgt/AD.DEMO.LAN@AD.DEMO.LAN
  renew until 03/08/13 10:08:48
03/07/13 10:10:16  03/07/13 20:08:55
cifs/win200864@AD.DEMO.LAN
  renew until 03/08/13 10:08:48

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
interop01:~ #

interop01:~ # smbclient -k //win200864/Share
smb: \>
smb: \> exit

interop01:~ # klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: demo@AD.DEMO.LAN

Valid starting     Expires            Service principal
03/07/13 10:08:48  03/07/13 20:08:55
krbtgt/AD.DEMO.LAN@AD.DEMO.LAN
  renew until 03/08/13 10:08:48
03/07/13 10:10:16  03/07/13 20:08:55
cifs/win200864@AD.DEMO.LAN
  renew until 03/08/13 10:08:48

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
interop01:~ #
Use Case 2: Integrate SPNGO enabled applications with AD: OpenLDAP ldapsearch

· Steps
  ‣ Request TGT with `kinit` or log in as an AD user
  ‣ Run `ldapsearch`

```bash
interop01:~ # ldapsearch \\
   -h win200864 \\
   -b 'cn=Users,dc=ad,dc=demo,dc=lan' \\
   -LLL '(givenname=interop)' \\
   cn
SASL/GSSAPI authentication started
SASL username: Administrator@AD.DEMO.LAN
SASL SSF: 56
SASL data security layer installed.
dn: CN=Interop
Demo,CN=Users,DC=ad,DC=demo,DC=lan
cn: Interop Demo
interop01:~ #
```
Scenario 1:
Use Case 3: Mount a Windows share

- Mount manually
  - With plain passwords
    mount -o username=Administrator,password=MYSECRET //win200864/Share /mnt/win200864-Share
  - Using Kerberos
    kinit Administrator
    mount -o sec=krb5i //win200864/Share /mnt/win200864-share

- Mount at boot from fstab
  - Credentials file
    //win200864/Share       /mnt/win200864-Share    cifs
    credentials=/root/.smb.credentials      0 0
  - See also: man 8 mount.cifs
Scenario 1:
Use Case 4: Access a Samba share from Windows

- Transparently access Samba share
  Start → Run → \interop02<ENTER>
Scenario 2: Integration of Apache with Active Directory

SLES 11 SP2

Role: Member server
AD: ad.demo.lan
Hostname: interop04

mod_kerb_auth

Apache

/source

Windows 2008 R2

Role: AD Domain Controller
AD domain name: ad.demo.lan
NT-style domain name: INTEROP
Hostname: win200864

Active Directory (LDAP)
Kerberos

Firefox
Internet Explorer

Windows 7
(win764.ad.demo.lan)

See more detailed documentation
Scenario 2: Integration of Apache with Active Directory

Configuration steps

- **Steps on SLES**
  - Join domain
  - Create/amend keytab
  - **Configure** Apache

- **Steps on workstations**
  - Configure Integrated Authentication for
    - Firefox
    - Internet Explorer

- **Steps on Active Directory**
  - Add user “sles-apache”
  - Add group “SLES Web Users”
  - Add user “Administrator” to “SLES Web Users”

See also: [HTTP-Based Cross-Platform Authentication by Using the Negotiate Protocol](https://msdn.microsoft.com) (MSDN)
See also: Interop Demo appliance
Configure Apache for Kerberos authentication

**file**: /etc/apache/conf.d/apache-integration-with-ad.conf

```apache
LoadModule auth_kerb_module /usr/lib64/apache2/mod_auth_kerb.so
LoadModule ldap_module /usr/lib64/apache2/mod_ldap.so
LoadModule authnz_ldap_module /usr/lib64/apache2/mod_authnz_ldap.so

<Location /secure>
    # Configuration for auth_kerb
    AuthName "---Restricted Access, please use your Active Directory credentials---"
    AuthType Kerberos
    KrbMethodNegotiate on
    KrbMethodK5Passwd on
    Krb5Keytab /etc/krb5.keytab
    KrbAuthRealms AD.DEMO.LAN
    KrbServiceName HTTP/interop04.ad.demo.lan@AD.DEMO.LAN
    KrbLocalUserMapping On

    # Configuration for authnz_ldap
    AuthLDAPBindDN cn=sles-apache,cn=Users,dc=ad,dc=demo,dc=lan
    AuthLDAPBindPassword SecretPassword
    AuthLDAPURL "ldap://win200864.ad.demo.lan:389/dc=ad,dc=demo,dc=lan?sAMAccountName"
    AuthLDAPGroupAttribute member
    Require ldap-group cn=SLES Web Users,cn=Users,dc=ad,dc=demo,dc=lan
</Location>
```
Amend the keytab with HTTP principal

```
# net ads keytab add HTTP -U Administrator
Processing principals to add...
Enter Administrator's password:

# klist -k -e
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal

--+-----------------------------------------------+-----------------------------
| 2 host/interop04.ad.demo.lan@AD.DEMO.LAN (DES cbc mode with CRC-32) |
| 2 host/interop04.ad.demo.lan@AD.DEMO.LAN (DES cbc mode with RSA-MD5) |
| 2 host/interop04.ad.demo.lan@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC) |
| 2 host/interop04.ad.demo.lan@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC) |
| 2 host/interop04.ad.demo.lan@AD.DEMO.LAN (ArcFour with HMAC/md5) |
| 2 host/interop04@AD.DEMO.LAN (DES cbc mode with CRC-32) |
| 2 host/interop04@AD.DEMO.LAN (DES cbc mode with RSA-MD5) |
| 2 host/interop04@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC) |
| 2 host/interop04@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC) |
| 2 host/interop04@AD.DEMO.LAN (ArcFour with HMAC/md5) |
| 2 INTEROP04$@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC) |
| 2 INTEROP04$@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC) |
| 2 INTEROP04$@AD.DEMO.LAN (ArcFour with HMAC/md5) |
| 2 HTTP/interop04.ad.demo.lan@AD.DEMO.LAN (DES cbc mode with CRC-32) |
| 2 HTTP/interop04.ad.demo.lan@AD.DEMO.LAN (DES cbc mode with RSA-MD5) |
| 2 HTTP/interop04.ad.demo.lan@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC) |
| 2 HTTP/interop04.ad.demo.lan@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC) |
| 2 HTTP/interop04.ad.demo.lan@AD.DEMO.LAN (ArcFour with HMAC/md5) |
| 2 HTTP/interop04@AD.DEMO.LAN (DES cbc mode with CRC-32) |
| 2 HTTP/interop04@AD.DEMO.LAN (DES cbc mode with RSA-MD5) |
| 2 HTTP/interop04@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC) |
| 2 HTTP/interop04@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC) |
| 2 HTTP/interop04@AD.DEMO.LAN (ArcFour with HMAC/md5) |

#```
Create separate krb5.keytab for Apache

interop02:~ # ktutil
ktutil: list
slot KVNO Principal
--- ---- ------------------------------------------
ktutil: rkt /etc/krb5.keytab
ktutil: list
slot KVNO Principal
--- ---- ------------------------------------------
  1  2 host/interop02.ad.demo.lan@AD.DEMO.LAN
...  16  2 HTTP/interop02.ad.demo.lan@AD.DEMO.LAN
...  25  2 HTTP/interop02@AD.DEMO.LAN
ktutil: delent 1 # repeat sufficient nr. of times to get rid of all but HTTP entries
Ktutil: wkt /etc/apache2/conf.d/apache2-krb5.keytab

# klist -k -e /etc/apache2/conf.d/apache2-krb5.keytab
Keytab name: FILE:/etc/apache2/conf.d/apache2-krb5.keytab
KVNO Principal
--- ------------------------------------------
  2 HTTP/interop02.ad.demo.lan@AD.DEMO.LAN (DES cbc mode with CRC-32)
  2 HTTP/interop02.ad.demo.lan@AD.DEMO.LAN (AES-128 CTS mode with 96-bit SHA-1 HMAC)
  2 HTTP/interop02.ad.demo.lan@AD.DEMO.LAN (AES-256 CTS mode with 96-bit SHA-1 HMAC)
  2 HTTP/interop02.ad.demo.lan@AD.DEMO.LAN (ArcFour with HMAC/md5)
  2 HTTP/interop02@AD.DEMO.LAN (DES cbc mode with CRC-32)
  2 HTTP/interop02@AD.DEMO.LAN (AES-128 CTS mode with RSA-MD5)
  2 HTTP/interop02@AD.DEMO.LAN (AES-256 CTS mode with RSA-MD5)
  2 HTTP/interop02@AD.DEMO.LAN (ArcFour with HMAC/md5)
#
Configure Firefox for Integrated Authentication

- Firefox is by default not enabled for the “Negotiate” authentication
  - 1: Negotiate not enabled
  - 2: Enable Negotiate
  - 3: Transparent access!
Example HTTP request header using SPNEGO

GET /secure/ HTTP/1.1
Host: interop01.ad.demo.lan
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101
Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
If-Modified-Since: Mon, 11 Mar 2013 13:37:53 GMT
If-None-Match: "b75e-db-4d7a6479f2e40"
Cache-Control: max-age=0, max-age=0
Authorization: Negotiate YIGugYGKWYBBQUCoIIGrjCCBqggMDAuB ...
Configure Firefox for Integrated Authentication
Configure Firefox for Integrated Authentication

This is the secured part of interop04.ad.demo.lan

Congratulations

You're authenticated as user: Administrator.
The used authentication method is: Negotiate

Last modified: 03:14, Thursday November 01, 2012
Configure IE for Integrated Authentication

- IE is by default not enabled for the “Negotiate” authentication
Configure IE for Integrated Authentication

- IE is by default not enabled for the “Negotiate” authentication
Configure IE for Integrated Authentication
Bleeding Edge Samba 4

With thanks to David Disseldorp, Samba Team
Traditional Copy

- File data takes disk and network round-trips
- Duplicate data stored on disk
Server-Side Copy

- Network round-trip avoided
- Server copies file data locally
- Duplicate data stored on disk
Btrfs Enhanced Server-Side Copy

- Data avoids network and disk round-trips
- No duplication of file data
- Ideal for hypervisor based workloads
Prototype Samba implementation of “Recovery Point”

Features

‣ Through integration of Btrfs, Snapper and Samba, SLES 11 SP2 is providing a file share

‣ Automatic snapshots create by Snapper provide “Recovery Points” for files

‣ Through Windows Explorer clients may access older versions of a file

Technology components

‣ SLES 11 SP2
  ♦ Btrfs and Snapper(prototype)
  ♦ Samba 4(prototype)

‣ Windows XP and 7

See also: “Bleeding Edge Samba and Snapper” appliance
Prototype Samba implementation of “Recovery Point”

- Automatic snapshots by Snapper
- Previous versions of “test.txt” in Explorer
- File “test.txt” is changed
- File “test.txt” is created

Samba4 service
File share
Automated snapshots

SLES 11 SP2

Network share

Windows 7, Vista or XP

Now

File "test.txt" is changed

Automatic snapshots by Snapper

File "test.txt" is created

Previous versions of “test.txt” in Explorer

Automated snapshots
Questions
For more information please visit our website:
www.suse.com

Thank you.
Unpublished Work of SUSE. All Rights Reserved.
This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.