The return of the vampires

Günther Deschner
<gd@samba.org>

(Red Hat / Samba Team)
Windows replication protocols

- Windows NT 4
  - Single-Master replication
  - Per Domain: One primary (PDC) and many Backup Domain Controllers (BDC)
  - Pull replication of SAM (Security Account Manager) database over DCE/RPC

- Active Directory (Windows 2000 and later)
  - Multi-Master replication (legacy: PDC emulator role)
  - Pull replication of DS database over DCE/RPC or SMTP (!)
  - Pull replication of DS database over LDAP
  - Pull replication of SAM database over DCE/RPC (legacy)
Active Directory in mixed / native mode

- AD can be run in two different modes
  - Mixed mode
  - Native mode
- Mixed mode added to Windows 2000 in order to support mixed setups with Windows 2000 and NT4 Domain Controllers
- Replication OS version dependent:
  - Windows 2000 <-> NT4 replication uses old SAM replication protocol
Active Directory in mixed / native mode

- Mixed mode is default mode (native mode needs to switched on if desired)
- Enabling native mode can **not** be reverted
- Legacy participants in AD replication (NT4):
  - One DC is PDC (all NT4 BDCs pull from there)
  - PDC receives write operations (password changes, etc.)
- “Modern” participants in AD replication (Windows 2000 and above):
  - True multi-master replication
  - Any DC can receive write operations
Replication over LDAP: DIRSYNC

- Available since Windows 2000 (only in Active Directory)
- Used for **native and mixed mode** domains
- Requires caller to use privileged admin account in order to retrieve data (no join as BDC required)
- Full DS replication (except passwords)
- Not used very often (not tested by Samba testsuite)
Replication over DCE/RPC: NETLOGON

- Available since NT4 and also in Active Directory
- In Active Directory only used for **mixed mode** domains
- Requires caller to be joined as a Windows Backup Domain Controller
- Does only replicate NT and LM hash (and password history)
- By default no encryption at the transport layer (only password hashes are encrypted with session key)
Replication over DCE/RPC: DRSUAPI

- Available since Windows 2000 (only in Active Directory)
- Used for **native and mixed mode** domains
- Requires caller to use privileged admin account in order to retrieve credentials (no join as BDC required)
- Does replicate NT and LM hash (and password history)
- Does replicate supplementalCredentials
- Does full DS replication
- By default full transport layer encryption (NTLM or Kerberos based) for all data
- lzxpress and zip compression supported (to safe bandwidth)
**Overview:**

<table>
<thead>
<tr>
<th>Windows DC version</th>
<th>Domain Mode</th>
<th>User Password</th>
<th>Supplemental Credentials</th>
<th>LDAP Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT4</td>
<td>Mixed</td>
<td>* NT Hash (RC4) * LM Hash * Password history</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2000 2003 2008</td>
<td>Mixed</td>
<td>NT Hash (RC4) LM Hash Password history</td>
<td>* Kerberos (DES,AES) * Digest * Cleartext</td>
<td>unicodePwd dBCSPwd supplementalCredentials</td>
</tr>
<tr>
<td>2000 2003 2008</td>
<td>Native</td>
<td>NT Hash (RC4) LM Hash Password history</td>
<td>* Kerberos (DES,AES) * Digest * Cleartext</td>
<td>unicodePwd dBCSPwd supplementalCredentials</td>
</tr>
</tbody>
</table>
## Overview (contd.):

<table>
<thead>
<tr>
<th>Windows DC version</th>
<th>Replication Protocol</th>
<th>Filtering / Single Object</th>
<th>Delta:</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT4</td>
<td>NETLOGON</td>
<td>- / yes</td>
<td>Global sequence number</td>
<td>Joined as BDC</td>
</tr>
<tr>
<td>2000 2003 2008</td>
<td>NETLOGON</td>
<td>- / yes</td>
<td>Global sequence number</td>
<td>Joined as BDC</td>
</tr>
<tr>
<td>2000 2003 2008</td>
<td>DRSUAPI</td>
<td>LDAP subtree / yes</td>
<td>Up-to-dateness vector</td>
<td>No join required, privileged user account sufficient</td>
</tr>
</tbody>
</table>
## Replication implementation in Samba 3 / 4

<table>
<thead>
<tr>
<th>Samba version</th>
<th>Client NETLOGON</th>
<th>Client DRSUAPI</th>
<th>Client LDAP (DirSync)</th>
<th>Server NETLOGON</th>
<th>Server DRSUAPI</th>
<th>Server LDAP (DirSync)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3</td>
<td>net</td>
<td>net (see note in “Known issues”)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.0</td>
<td>net, testing tools</td>
<td>testing tools</td>
<td>ldb</td>
<td>-</td>
<td>samba</td>
<td>-</td>
</tr>
</tbody>
</table>
Client implementation in Samba 3

- Part of the “net” tool: “net rpc vampire”
- Used to “vampire” a domain controller
- Retrieved data can be
  - Displayed (net rpc samdump)
  - Transformed to internal Samba Account Database (the original vampire mode) (net rpc vampire or net rpc vampire passdb)
  - Transformed to ldif file (suiteable for Samba Account Database LDAP backend) (net rpc vampire ldif)
  - Stored in standard Kerberos 5 keytab file (new in Samba 3.3.0) (net rpc vampire keytab)
Client implementation in Samba 3

- net calls an internal libnet API
- That API has
  - common processing routines (NDR encoding, DCE/RPC transport, session setup, password decryption)
  - plugin specific callbacks for data processing
- All plugins (passdb, ldif, dump, keytab) transport the same replication data over the wire
- Not only passwords, all other account information (incl. e.g. group membership) is transported as well, just discarded in most plugins
net rpc vampire keytab

- Is available in recent Samba 3.3 tree (currently 3.3.3)
- Creates a keytab containing all passwords of all users and machines in a domain
- Initially designed as a developer tool for decrypting encrypted network traffic in wireshark on the fly
- Generated keytab keeps state of replication in keytab file (to achieve incremental replication)
- Depending on replication protocol, filters can be used and single entries replicated
Client implementation in Samba

- net rpc vampire keytab (using NETLOGON)
  - Creates a keytab file
  - Composes user principal name
  - Stores nt hash (arcfour-hmac-md5) in keytab
  - Stores global sequence number (for later incremental replication) in special entry (SEQUENCE_NUM/DOMAIN)
  - Can replicate single entries (user_rid=<RID>)
Video Demo

net rpc vampire keytab

Windows 2000 mixed mode domain
(using NETLOGON replication)
Client implementation in Samba

- **net rpc vampire keytab (using DRSUAPI)**
  - Creates a keytab file
  - Retrieves user principal name
  - Stores nt hash (arcfour-hmac-md5) in keytab
  - Also stores des-cbc-crc, des-cbc-md5
  - Also stores aes256-cts-hmac-sha1-96, aes128-cts-hmac-sha1-96 (available on a Windows 2008 KDC only)
  - Stores uptodateness vector (for later partial replication) in special entry (UPDV/DOMAIN_DN)
  - Can replicate single entries (<LDAP DN>)
Video Demo

net rpc vampire keytab

Windows 2008 native mode domain
(using DRSUAPI replication)
Vampire wish list:

- Make replication engine a public shared library
- Add pluggable, shared modules
- Add vampire to passdb using DRSUAPI for Samba 3
Known issues

- Replication with DRSUAPI on a Windows 2000 DC fails
  - MIT Kerberos library used by Samba3 cannot do sealing (encryption) of DRSUAPI traffic
  - Copy of Heimdal that Samba4 ships is suitable
  - MS documentation says DRSUAPI replication should always use Kerberos for sealing
  - Tests show that encryption using NTLM works just fine (except against Windows 2000 DCs)

- Documentation of available options
Further reading

- **Microsoft Protocol Documentation:**
  - NETLOGON replication ([MS-NRPC].pdf)
  - DRSUAPI replication ([MS-DRSR].pdf)
  - DIRSYNC draft

- **Microsoft Documentation:**
  - How the Active Directory Replication Model Works

- **DRSUAPI research (before documentation was available):**
Thank you for your attention!