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 <-> Windows 2000 replication uses new DS replication protocol
  - Windows 2000 <-> NT4 replication uses old SAM replication protocol
- Mixed mode available for Windows 2000, 2003 and 2008

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:

Windows DC version	Domain Mode	User Password	Supplemental Credentials	LDAP Attributes
NT4	Mixed	* NT Hash (RC4) * LM Hash * Password history	-	-
2000 2003 2008	Mixed	NT Hash (RC4) LM Hash Password history	* Kerberos (DES,AES) * Digest * Cleartext	unicodePwd dBCSPwd supplementalCredentials
2000 2003 2008	Native	NT Hash (RC4) LM Hash Password history	* Kerberos (DES,AES) * Digest * Cleartext	unicodePwd dBCSPwd supplementalCredentials

Overview (contd.):

Windows DC version	Replication Protocol	Filtering / Single Object	Delta:	Prerequisites
NT4	NETLOGON	- / yes	Global sequence number	Joined as BDC
2000 2003 2008	NETLOGON	- / yes	Global sequence number	Joined as BDC
2000 2003 2008	DRSUAPI	LDAP subtree / yes	Up-to-dateness vector	No join required, privileged user account sufficient

Replication implementation in Samba 3 / 4

Samba version	Client NETLOGON	Client DRSUAPI	Client LDAP (DirSync)	Server NETLOGON	Server DRSUAPI	Server LDAP (DirSync)
3.3	net	net (see note in “Known issues”)	-	-	-	- (ldapsam replication)
4.0	net, testing tools	testing tools	ldb	-	samba	-

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 suiteable
  - 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

- **Mircrosoft Protocol Documentation:**
  - NETLOGON replication ([MS-NRPC].pdf)
    http://msdn.microsoft.com/en-us/library/cc207935.aspx
  - DRSUAPI replication ([MS-DRSR].pdf)
    http://msdn.microsoft.com/en-us/library/cc203213.aspx
  - DIRSYNC draft
- **Microsoft Documentation:**
  - How the Active Directory Replication Model Works
    http://technet.microsoft.com/en-us/library/cc772726.aspx
- **DRSUAPI research (before documentation was available):**
  - http://samba.org/~metze/presentations/2007/thesis/StefanMetzmacher_Bachelorthesis_ENG_Draft-9811557.pdf

Thank you for your attention!