

Windows Server 2008 Kerberos

Michiko Short

Program Manager

Microsoft Corporation

Agenda

- What's New in Windows Vista and Windows Server 2008
- Kerberos Tools Updates
- Configuring Interoperability with Windows



What's New

- AES Support
 - AES256-CTS-HMAC-SHA1-96 [17]
 - AES128-CTS-HMAC-SHA1-96 [18]
- IPv6 support
- Support for Read Only Domain Controller (RODC)
- KDC returns encryption types supported by server or service
- Group Policy Support for Realm & Host-to-Realm settings

Kerberos AES Support

Client	Server	KDC	
Down-level	Down-level	Server 2008	TGT may be encrypted with AES if necessary based on policy
Down-level	Vista	Server 2008	Service ticket encryption in AES
Vista	Vista	Server 2008	All messages in AES
Vista	Vista	Down-level	GSS encryption in AES
Vista	Down-level	Server 2008	AS-REQ/REP, TGS-REQ/REP in AES.
Down-level	Vista	Down-level	No AES
Vista	Down-level	Down-level	No AES
Down-level	Down-level	Down-level	No AES

For TGTs to be AES the domain must be Windows Server 2008 Functional Level.



PKInit

- Support for PA_PK_AS_REQ [16] & PA_PK_AS_REP [17]
- Support for Sha-1

Smart Card Support Changes

- Windows Server 2008 KDCs do not require the Smart Card OID
- User Certificates can be mapped by
 - UPN (supported down-level)
 - X.509 name
 - Certificate thumbprint
 - Subject key identifier
 - E-mail name

Kerberos Resources

- Kerberos: <http://www.microsoft.com/kerberos>
- Windows Vista Authentication Features:
<http://technet2.microsoft.com/WindowsServer2008/en/library/f632de29-a36e-4d82-a169-2b180deb638b1033.mspx>
- MSDN Authentication:
<http://msdn2.microsoft.com/en-us/library/aa374735.aspx>

Updated Tools

- Kerberos Setup (ksetup.exe)
- Kerberos Keytab Setup (ktpass.exe)
- SetSPN.exe

New to ksetup.exe

- /AddHostToRealmMap
- /DelHostToRealmMap

- /SetEncTypeAttr
- /GetEncTypeAttr
- /AddEncTypeAttr
- /DelEncTypeAttr



New to ktpass.exe

- [- /] crypto: All: All supported types

New to SetSPN.exe

- -F = perform the duplicate checking on forestwide level
- -P = do not show progress (useful for redirecting output to file)
- -S = add arbitrary SPN after verifying no duplicates exist
- -X = search for duplicate SPNs



Non-Windows Clients in Domains

1. Create new user account for host in AD
 - Enable AES256, if supported
2. On DC, create keytab file with ktpass
3. On host
 1. Merge keytab file w/ existing
 2. Edit krb5.conf to refer to DC as the Kerberos KDC
4. On both host and DC, ensure clocks are synchronized

Non-Windows Services in Domains

1. Create new user account for the service in AD
 - Enable AES256, if supported
2. On DC, create keytab file with ktpass
3. On host, merge keytab file w/ existing keytab file on the host



Windows Clients in Realms

1. On KDC, create host principal
2. On Windows client, configure with realm settings using ksetup
 - Set Realm
 - Add KDC and Kpasswd Server (optional)
 - If not specified, uses DNS SRV lookup
 - Set machine password
3. Restart client
4. On Windows client, configure account mappings



Trusts

1. On DC, configure realm with ksetup
2. On DC, create domain trust with AD Domains and Trusts MMC
 - If supported, enable AES256
3. On KDC, use kadmin to create cross-realm principals
4. If desired, create account mappings with AD Users and Computers MMC Advanced Features

Kerberos Resources

- Kerberos: <http://www.microsoft.com/kerberos>
- Solution Guide for Windows Security and Directory Services for UNIX:
<http://www.microsoft.com/downloads/details.aspx?FamilyId=144F7B82-65CF-4105-B60C-44515299797D&displaylang=en>
- Step-by-Step Guide to Kerberos Interoperability for Windows Server 2003
- Step-by-Step Guide to Kerberos 5 (krb5 1.0) Interoperability for Windows 2000:
<http://technet.microsoft.com/en-us/library/bb742433.aspx>

Summary

- What's New in Windows Vista and Windows Server 2008
- Kerberos Tools Updates
- Configuring Interoperability with Windows