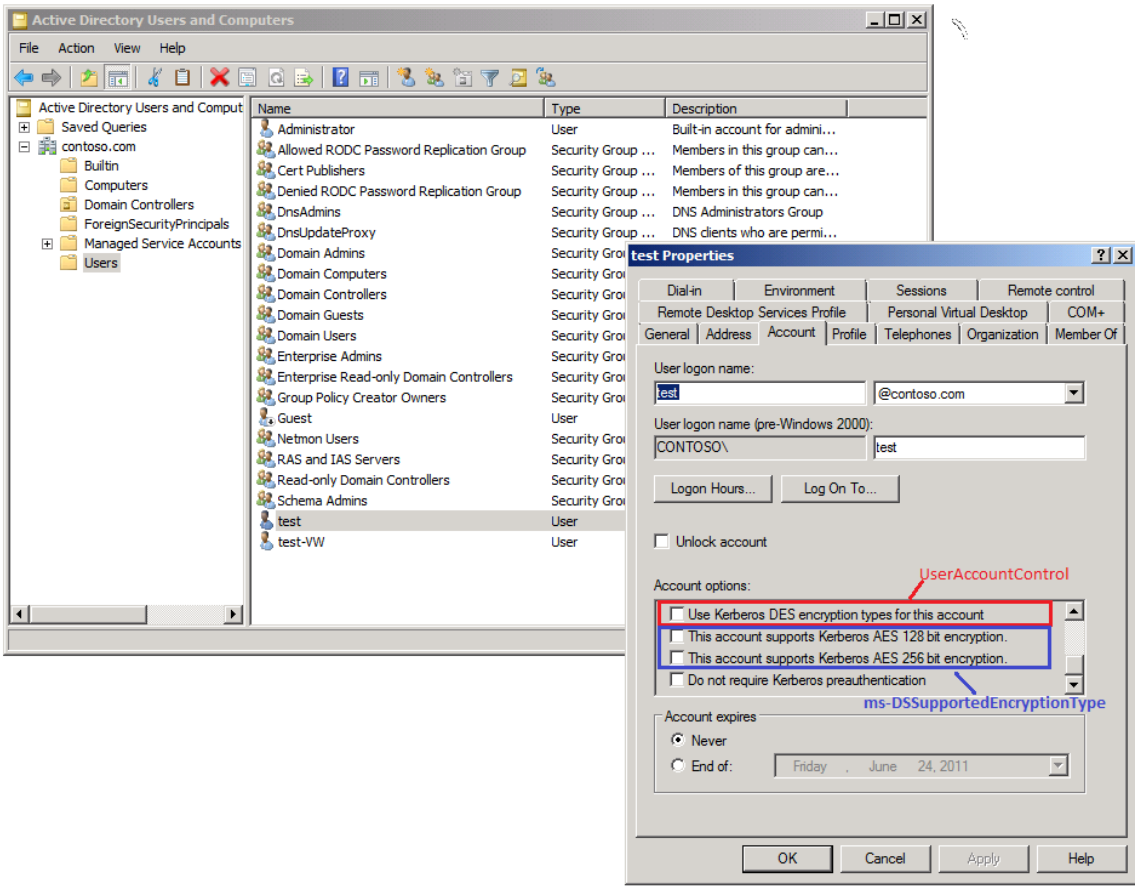
Windows Configurations for Kerberos Supported Encryption Type

- Article
- 05/30/2011

In one of my previous blog(https://blogs.msdn.com/b/openspecification/archive/2010/11/17/encryption-type-selection-in-kerberos-exchanges.aspx) , I have talked about how the encryption types of the various encrypted parts of the Kerberos exchanges are selected. The selections of these encryption types are dependent on some Active Directory attributes and policy settings. It is important to understand how these settings are configured from the Windows interface. There are several places to edit the settings. Sometime it could be confusing. In this blog, we will take a quick look at the interface with screen shots attached and its relationship with the backend attributes and policy settings.

1. **User Account Encryption Type Setting**

The KDC will issue a ticket for the server service and the client will forward the service ticket to the server for authentication. A server service can run under a user account. The setting on the user account will affect the encryption type selection for the service ticket.



The following settings affect the selection of the encryption types:

- **Use Kerberos DES Encryption types for this account**

This setting is mapped to the UF_USE_DES_KEY_ONLY bit (0x200000) in the ***UserAccountControl*** attribute of the user object. When this setting is checked, the account only supports the DES encryption.

- **The account supports Kerberos AES 128 bit encryption**

This setting is mapped to the AES128-CTS-HMAC-SHA1-96 (0x08) (2.2.6 MS-KILE) in the **msDS-SupportedEncryptionTypes** attribute on the user account. When this setting is checked, AES128 will be supported on this account.

- **The account supports Kerberos AES 256 bit encryption**

This setting is mapped to the AES256-CTS-HMAC-SHA1-96 (0x10) in the **msDS-SupportedEncryptionTypes** attribute on the user account. When this setting is checked, AES256 will be supported on this account.

2. **Computer Account Encryption Type Setting**

Some services run under the computer account . Their SPNs are registered with the computer account. To change the encryption types supported on the computer account, we have to edit directly the**msDS-SupportedEncrytionTypes** and **UseAccountControl** attributes on the computer object in Active Directory using tools such as ADSI.exe. These attributes on the computer account are updated when the computer is joined to the domain. It could also be updated directly via LDAP interface. This may be the reason why there is no user interface in the same way as a user account does. Please note that **msDC-SupportedEncryptionTypes** attribute is only available on Windows server 2008 and later. The computer object for earlier OS will not have this attribute defined. The earlier versions of domain controllers (before Windows server 2008) will not be aware of this attribute. If it is not defined on the computer account, the domain controller will use DES and RC4 as encryption type unless the **UserAccountControl** attribute has the UF_USE_DES_KEY_ONLY bit set so only DES is supported.

When editing the **msDC-SupportedEncryptionTypes** attribute, you have to combine the following bits to get an integer value for the attribute

DES-CBC-CRC 0x01

DES-CBC-MD5 0x02

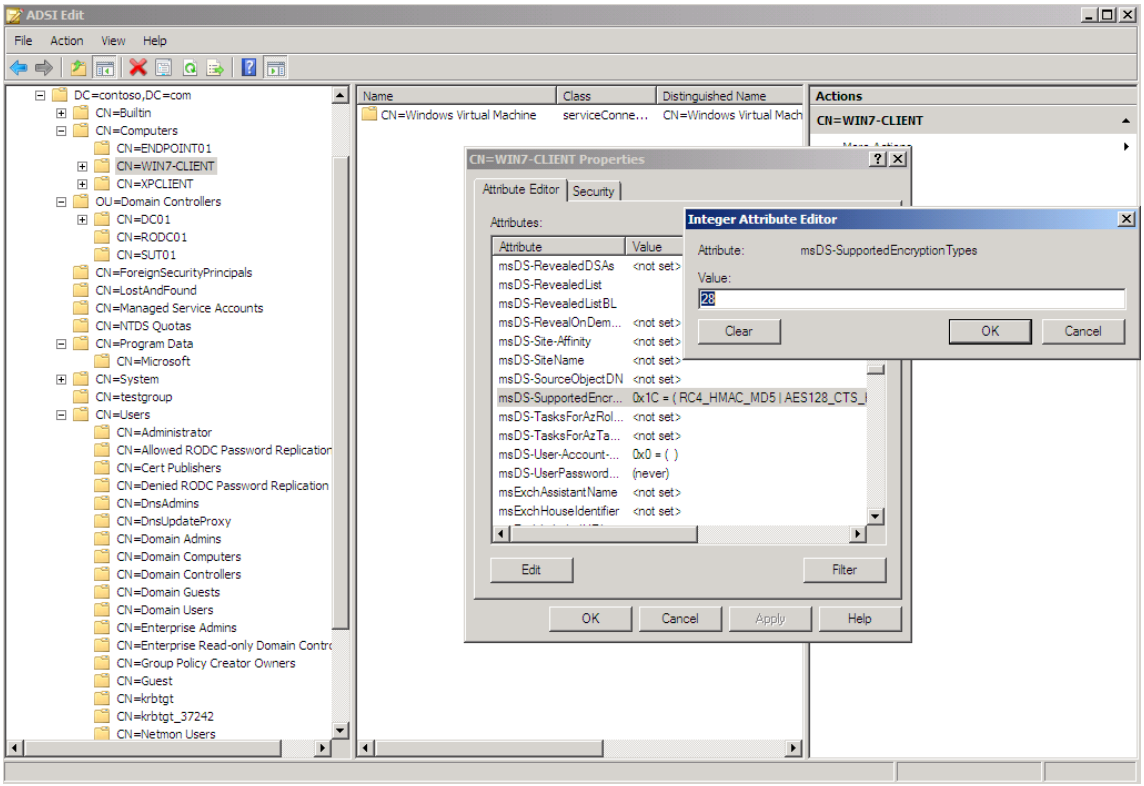
RC4-HMAC 0x04

AES128-CTS-HMAC-SHA1-96 0x08

AES256-CTS-HMAC-SHA1-96 0x10

When editing UserAccountControl attribute, you should add or remove bit 0x200000 to enable or disable DES key only.

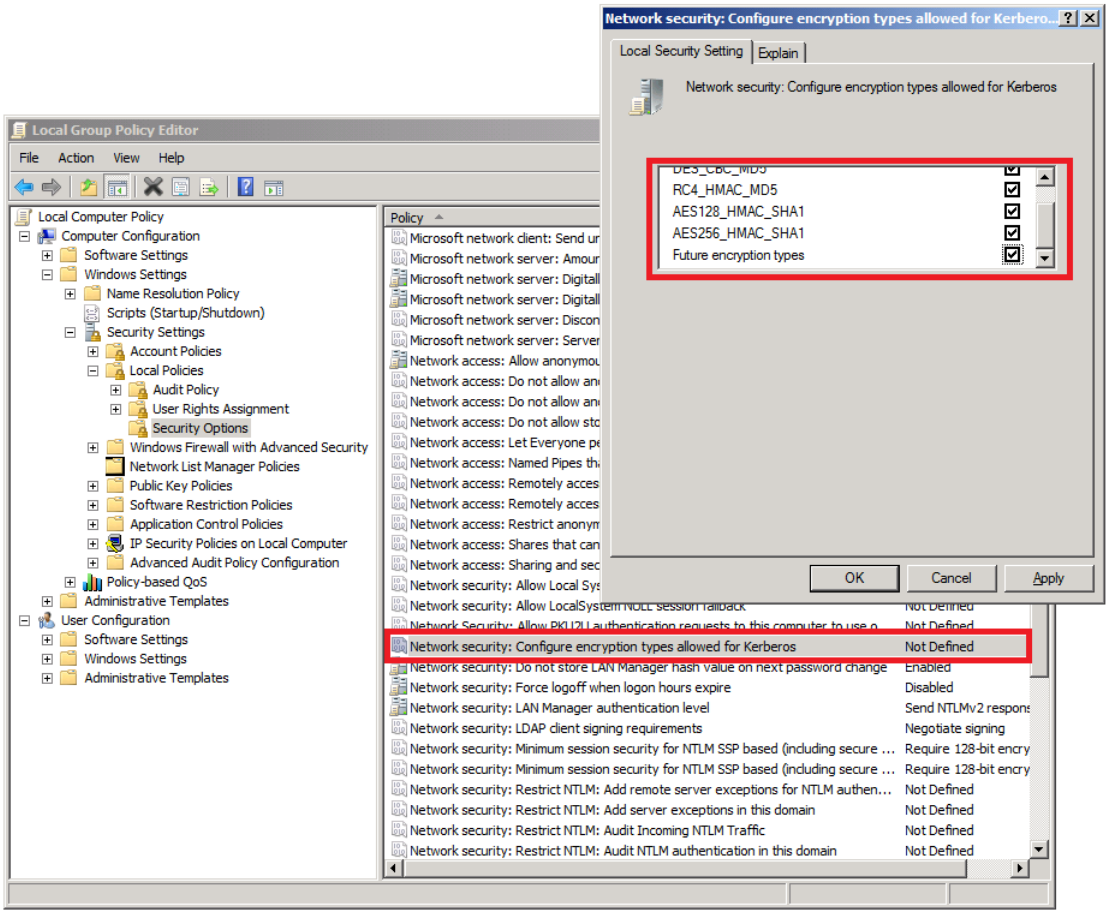
The following is a screen shot for editing the attributes.



3. **Allowed Encryption Types Local Group Policy Setting**

In Windows 7/Windows Server 2008R2, a new policy setting is introduced for specifying the encryption types allowed for Kerberos. This is a system wide global setting that will affect all the accounts on the computer where the policy is applied. With this setting, we can enable and disable the encryption/decryption capability of each Crypto system (AES256, AES128, RC4, DES etc). In this way, even an individual encryption type is included in the supported encryption type list as we discussed in the last two sections, it will not be selected.

What is the reason to introduce this setting? The main purpose is to disable DES encryption, which is widely considered not secure enough, in any Windows 7/Windows server 2008R2 computers by default. You may notice that the policy setting "***Network Security: Configure Encryption types allowed for Kerberos***" is "*Not Defined*" in a new system. When this policy setting is not defined, all Crypto systems except DES will be available for encryption. Users can define this policy setting to enable/disable each individual Crypto system, including DES. The following screen shot shows where the setting can be found.



Looking a little further, we can see this policy setting is mapped to the following registry DWORD key: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionT**

Each Crypto system will be represented by the same bit as in **msDC-SupportedEncryptionTypes**. For example, if all the encryptions are enabled, the value will be 0x1F. Another interesting option is “Future encryption types”. This option turns on the any future encryption types that could be added to the Windows by setting the first 31 bits in the 32 bit registry key value. If all the boxes are checked, the value will be 0x7fffffff. You can observe how the registry value changes when different encryption types are selected on the dialog.

You can use the Local Security Policy to change the setting on the local machine only, or an administrator can use group policy to apply it to multiple machines including DCs in the domain.

I hope that this summary can give you a help with how to configure Kerberos encryption types in Windows.

Reference:

[MS-KILE] https://msdn.microsoft.com/en-us/library/cc233855(v=prot.13).aspx

[KB977321] https://support.microsoft.com/kb/977321

Comments

- **Anonymous**
  April 26, 2013
  IAP v1.2 Section Requirements (paraphrased) ADDS Baseline Controls Baseline Gaps AM Proposal Remaining Gaps 4.2.3.4 Stored Authentication Secrets (S) Do not store passwords as plaintext....

- **Anonymous**
  January 27, 2017
  Very helpful, thanks for posting :)