Linux - Security - Active Directory

Purpose

Trying to connect a CentOS Linux box to a Microsoft Windows Active Directory Domain.

Version

Client or Server	Product	Command	Version
Client - Linux			
	Linux - OS - Kernel	uname -r	4.18.0-147.5.1.el8_1.x86_64
	Linux - OS - Redhat	lsb_release -d	CentOS Linux release 8.1.1911 (Core)
	sssd	sssd --version	2.2.0
Server - Windows			
			MS Windows 2003

TroubleShooting

kinit

Syntax

kinit -V {username}@{domain}

Sample

KRB5_TRACE=/dev/stdout kinit -V dadeniji@lab.org

Output

>KRB5_TRACE=/dev/stdout kinit -V dadeniji@lab.org.

Using default cache: 1000
Using principal: dadeniji@lab.org.
[2448] 1588503907.189313: Getting initial credentials for dadeniji@lab.org.
[2448] 1588503907.189315: Sending unauthenticated request
[2448] 1588503907.189316: Sending request (224 bytes) to lab.org.
[2448] 1588503907.189317: Sending DNS URI query for _kerberos.lab.org.
[2448] 1588503907.189318: No URI records found
[2448] 1588503907.189319: Sending DNS SRV query for _kerberos._udp.lab.org.
[2448] 1588503907.189320: SRV answer: 0 100 88 "dc01.lab.org."
[2448] 1588503907.189321: Sending DNS SRV query for _kerberos._tcp.lab.org.
[2448] 1588503907.189322: SRV answer: 0 100 88 "dc01.lab.org."
[2448] 1588503907.189323: Resolving hostname dc01.lab.org.
[2448] 1588503907.189324: Sending initial UDP request to dgram 10.0.4.6:88
[2448] 1588503907.189325: Received answer (104 bytes) from dgram 10.0.4.6:88
[2448] 1588503907.189326: Sending DNS URI query for _kerberos.lab.org.
[2448] 1588503907.189327: No URI records found
[2448] 1588503907.189328: Sending DNS SRV query for _kerberos-master._udp.lab.org.

[2448] 1588503907.189329: No SRV records found
[2448] 1588503907.189330: Response was not from master KDC
[2448] 1588503907.189331: Received error from KDC: -1765328370/KDC has no support for encryption type
[2448] 1588503907.189332: Retrying AS request with master KDC
[2448] 1588503907.189333: Getting initial credentials for dadeniji@lab.org.
[2448] 1588503907.189335: Sending unauthenticated request
[2448] 1588503907.189336: Sending request (224 bytes) to lab.org. (master)
[2448] 1588503907.189337: Sending DNS URI query for _kerberos.lab.org.
[2448] 1588503907.189338: No URI records found
[2448] 1588503907.189339: Sending DNS SRV query for _kerberos-master._udp.lab.org.
[2448] 1588503907.189340: Sending DNS SRV query for _kerberos-master._tcp.lab.org.
[2448] 1588503907.189341: No SRV records found
kinit: KDC has no support for encryption type while getting initial credentials

Error

Error Message

kinit: KDC has no support for encryption type while getting initial credentials

adcli

Syntax

Adcli join {domain-name} -U {username} -v

Sample

adcli join lab.org -U dadeniji -v

Output

```
>sudo adcli join lab.org -U dadeniji -v
 * Using domain name: lab.org
 * Calculated computer account name from fqdn: ADRIEL
 * Calculated domain realm from name: lab.org
 * Discovering domain controllers: _ldap._tcp.lab.org
 * Sending netlogon pings to domain controller: cldap://10.0.4.6
 * Received NetLogon info from: dc01.lab.org
 * Wrote out krb5.conf snippet to /tmp/adcli-krb5-vHcn5L/krb5.d/adcli-krb5-conf-G0KCpp
Password for dadeniji@lab.org:
 ! Couldn't authenticate as: dadeniji@lab.org: KDC has no support for encryption type
adcli: couldn't connect to lab.org domain: Couldn't authenticate as: dadeniji@lab.org: KDC has no support for encryption type
```

Configuration

Configuration Files

/etc/krb5.config

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

# Temporarily enable logging
debug_level=10

[logging]
    default = FILE:/var/log/krb5libs.log
```

```
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_ccache_name = KEYRING:persistent:%{uid}
    default_tgs_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
    defaukt_tkt_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
    permitted_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
    allow_weak_crypto = true
    dns_lookup_kdc = true

[realms]
# EXAMPLE.COM = {
#     kdc = kerberos.example.com
#     admin_server = kerberos.example.com
# }



[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
```

Active Directory

User Configuration

Here are the changes made to the specific accounts that will be using Linux machines, but need to be authenticated via AD.

1. Do not require Kerberos preauthentication
2. Use DES Encryption types for this account

Question & Thoughts

Supported Server Version

Does the latest Kerberos clients from Redhat\CentOS still support MS Windows 2003.

Blog Posts suggests that if I customize kerb5.conf, I should be good.

Here are the configurations, I have tried thus far.

```
default_tgs_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
defaukt_tkt_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
permitted_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
allow_weak_crypto = true
```

Basically, the changes are to explicitly specify the encryption types supported by MS Windows 2003.

And, let the Linux machine know that it is OK to use "***weak***" cryptography.

Remediation

Encryption Type

Outline

1. Typo
    a. defaukt_tkt_enctypes
    b. default_tkt_enctypes

Original

```
default_tgs_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
defaukt_tkt_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
permitted_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
allow_weak_crypto = true
```

Revised

```
default_tgs_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
default_tkt_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
permitted_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
allow_weak_crypto = true
```