NetApp® Knowledge Base

# Troubleshooting Workflow: CIFS Authentication failures

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Troubleshoot…

Updated: Mon, 23 Nov 2020 06:14:02 GMT

## Applies to

Clustered Data ONTAP 8

## Issue

CIFS Authentication fails

## Cause

There can be various causes for this issue. The causes and procedures to be performed to resolve this issue are described in the Solution section.

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.'

## Solution

### Cause 1: Time skew; error message displayed while using Kerberos

**How to determine if this is the cause**:

**Packet trace**:

- If Kerberos is being used (or attempted) for authentication, check this issue by taking a packet trace. A packet trace is required only from the client.

  Check the KRB5 packet for confirmation:

  ```
  1778 41.215954 172.17.193.122 10.53.21.46 SMB Session Setup AndX Request

  1779 41.227968 10.53.21.46 172.17.193.122 SMB KRB Error:
  KRB5KRB_AP_ERR_TKT_NYV, Error: STATUS_MORE_PROCESSING_REQUIRED

  A status_unsuccessful failure might be reported:

  1785 41.245534 172.17.193.122 10.53.21.46 SMB Session Setup AndX Request

  1786 41.254967 10.53.21.46 172.17.193.122 SMB Session Setup AndX Response,
  Error: STATUS_UNSUCCESSFUL

  secd.log:

  secd.log location - /mroot/etc/log/mlog
  ```

- If the clock skew error message is in the journal:

  ```
  ERR : RESULT_ERROR_SECD_NO_SERVER_AVAILABLE:6940 in
  secd_rpc_auth_extended_1_svc() at authentication/secd_rpc_auth.cpp:749

  debug: SecD RPC Server sending reply to RPC 151: secd_rpc_auth_extended {
  in secdSendRpcResponse() at server/secd_rpc_server.cpp:1405 }

  ERR : Error: User authentication procedure failed

  ERR : [ 0 ms] Login attempt by domain user 'CIFSLABAdministrator' using
  ```

```
NTLMv1 style security

ERR : [ 0] No servers available for MS_NETLOGON, vserver: 3, domain:
cifs.lab.netapp.com.

ERR : [ 22] Unable to connect to any of the provided DNS servers

ERR : [ 22] Connecting to NetLogon server a7-6.cifs.lab.netapp.com
(172.17.192.24)

ERR : **[ 22] FAILURE: Unexpected state: Error 6810 at file:Common/
ProtocolClientLibrary/Dns/DnsOps.cpp func:DnsNameLookup line:715

''' ERR : **[ 33] FAILURE: Cluster and Domain Controller times differ by
more than the configured clock skew'''

ERR : [ 104] Unable to connect to a7-6.cifs.lab.netapp.com through the
10.53.21.46 interface

ERR : [ 104] No servers available for MS_NETLOGON, vserver: 3, domain:
cifs.lab.netapp.com.

|-----------------------------------------------------------------------------
.

| RPC completed at Fri Oct 19 08:34:13 2012 |

| End of log for failed RPC secd_rpc_auth_extended |

'-----------------------------------------------------------------------------
'
```

- Is the time set on the cluster and the node correct? If it is resolving correctly, check the time on the cluster:

```
::*> system date show
```

Compare with the time on the host.

**Check the EMS messages**:

```
::*> event log show -messagename secd.*

10/18/2012 13:34:59 krbClus-01       ERROR         secd.kerberos.clockskew:
Kerberos client or node clock skew error (-1765328351).
```

**Resolution**:

If the time on the client, DC, and/or cluster (node) are outside the configured clock skew, then Kerberos will not work as per the default settings in Active Directory (AD).

For more information, see Microsoft article 884776: How to configure the Windows Time service against a large time offset

From the cluster shell, configure a time server or set the time to the correct value. On the node and the client, set the correct time.

### Cause 2: Machine password is out of sync; an error message is reported while using Kerberos despite the correct time.

**How to determine if this is the cause**:

1. Check for the journal error in the `secd.log` (location: `/mroot/etc/log/mlog`) file:

```
debug: SecD RPC Server sending reply to RPC 151: secd_rpc_auth_extended {
in secdSendRpcResponse() at server/secd_rpc_server.cpp:1405 }

ERR : Error: User authentication procedure failed

ERR : [ 0 ms] Login attempt by domain user 'CIFSLABAdministrator' using
NTLMv1 style security

ERR : [ 0] No servers available for MS_NETLOGON, vserver: 3, domain:
cifs.lab.netapp.com.

ERR : [ 62] Unable to connect to any of the provided DNS servers

ERR : [ 62] Connecting to NetLogon server a7-6.cifs.lab.netapp.com
(172.17.192.24)

ERR : **[ 62] FAILURE: Unexpected state: Error 6810 at file:Common/
ProtocolClientLibrary/Dns/DnsOps.cpp func:DnsNameLookup line:715
```

```
'''ERR : **[ 112] FAILURE: CIFS server account password does not match
password stored in Active Directory'''

ERR : [ 143] Unable to connect to a7-6.cifs.lab.netapp.com through the
10.53.21.46 interface

ERR : [ 143] No servers available for MS_NETLOGON, vserver: 3, domain:
cifs.lab.netapp.com.

|----------------------------------------------------------------------------
.

| RPC completed at Sat Oct 20 10:40:54 2012 |

| End of log for failed RPC secd_rpc_auth_extended |

'----------------------------------------------------------------------------
'
```

Note the error in the above journal.

```
ERR  :  **[   112] FAILURE: CIFS server account password does not match
password stored in Active Directory
```

The above error indicates that the machine account password is out of sync with the password set in the AD.

2. Check the EMS messages:

```
:

:*> event log show -messagename secd.*

Time Node Severity Event

------------------- ---------------- -------------
---------------------------

8/21/2012 17:44:43 krbClus-01 ERROR secd.kerberos.preauth: Kerberos pre-
authentication failure due to out-of-sync machine account password
```

```
     (-1765328360).
```

**Resolution**:

Run the following command:

```
::> cifs password-reset -vserver vserver

Please enter your userid: administrator

Please enter your password:
```

For more information, see BUG 380120.

**Cause 3: A machine account is deleted in AD**

**How to determine if this is the cause**:

Check for the error in the `secd.log (/mroot/etc/log/mlog)` file:

```
ERR : RESULT_ERROR_KERBEROS_C_PRINCIPAL_UNKNOWN:7507 in getKrbInitCreds() at
Common/SecLibrary/Src/GssapiCtx.cpp:676

ERR : getKrbInitCreds: Kerberos Error: (-1765328378)
```

**Resolution**:

To resolve this issue, create a machine account with the CIFS server name in AD.

```
cifs modify -vserver <vservername> -status-admin down
```

`cifs modify -vserver <vservername> -domain <fqdn` of domain, the system is joined to or needs to be joined to> (A username with the right to create and delete objects in the domain is required)

**Cause 4: Using a DNS alias/CNAME, without the SPN set for that alias**

**How to determine if this is the cause**:

When using a `\nameshare` convention, the Kerberos being attempted is expected to be displayed. If that does not occur, check the SPN for the CIFS Vserver.

From the cluster:

```
::*> cifs server show -vserver <vserver_name>
```

```
Vserver: vserver

CIFS Server NetBIOS Name: vserver <-- this is our CIFS server name/Computer
account name

NetBIOS Domain/Workgroup Name: DOMAIN

Fully Qualified Domain Name: DOMAIN.COM

Default Site Used by LIFs Without Site Membership:

Authentication Style: domain <-- this tells us to use Kerberos when possible
```

Check the secd logs for failures and turn on `trace-all`:

**Example**:

```
000000e5.001bd59b 00e687ef Wed Aug 03 2011 11:46:29 -04:00
[kern_secd:info:1735] | [000.023.897] ERR :

6942 in connectToDomainController() at connection_manager/
secd_connection.cpp:137

000000e5.001bd59c 00e687ef Wed Aug 03 2011 11:46:29 -04:00
[kern_secd:info:1735] | [000.023.910] debug:

Failed to connect to DC win2k3dc-rtp.rtp2k3dom.ngslabs.netapp.com { in
connectToDomainController() at connection_manager/secd_connection.cpp:147 }

000000e5.001bd5a3 00e687ef Wed Aug 03 2011 11:46:29 -04:00
[kern_secd:info:1735] | [000.024.101] debug:

Unable to make a connection (NetLogon:RTP2K3DOM.NGSLABS.NETAPP.COM), result:
6942 { in getConnection() at connection_manager/secd_connection_manager.cpp:631
}

000000e5.001bf09a 00e6880a Wed Aug 03 2011 11:46:30 -04:00
[kern_secd:info:1735] | [000.014.987] debug:

Querying config source 'MachineAccount' (with 3 rows of data) by keys vserver
```

```
id: '12' { in query() at configuration_manager/
secd_configuration_sources.cpp:1085 }

000000e5.001bf09b 00e6880a Wed Aug 03 2011 11:46:30 -04:00
[kern_secd:info:1735] | [000.016.498] debug:

Error!!! NtStatusError: NT_STATUS_AUTH_ACCOUNT_DISABLED { in LogNtStatusCode()
at Commands/Commands.cpp:381 }
```

**From DC:**

Run the `setspn` command (this can be located in the Windows 2000 resource kit) to view SPNs for the Vserver. If this command does not respond and displays the following output, check the computer account:

```
C:>setspn -L vserver

FindDomainForAccount: DsGetDcNameWithAccountW failed!

Cannot find account vserver
```

The output should appear similar to the following:

```
C:>setspn -L vserver

Registered ServicePrincipalNames for CN=VSERVER,CN=Computers,DC=domain,DC=com:

nfs/vserver.domain.com

nfs/VSERVER

HOST/vserver.domain.com

HOST/VSERVER
```

**Resolution**:

If using a DNS alias/CNAME, the SPN should be added for that alias to ensure that Kerberos is being used.

**Example:**

```
setspn -A HOST/alias vserver

setspn -A HOST/alias.domain.com vserver
```

**Cause 5: Using a DNS alias/CNAME for which SPN is set, but for a different account**

**How to determine if this is the cause**:

When using a `\nameshare` convention, a Kerberos is attempted. If that does not occur and if it is not an issue with clock skew or the machine account password, check if SPN in the Kerberos packet is for the right machine account.

From the packet, check for TGS-REQ, and check if the TGS-REP was received successfully. The output should appear similar to the following:

```
131               17.408937 172.17.193.122            172.17.193.
44                KRB5         TGS-REQ

132               17.410653 172.17.193.44              172.17.193.
122              KRB5         TGS-REP
```

In the TGS-REQ packet, check for the server name

```
Server Name (Service and Instance): cifs/spnTest.cifs.lab.netapp.com
```

**From DC:**

Use the `setspn` command (can be found in the Windows 2000 resource kit) to lookup spn and check if it is assigned to the right account.

```
C:>setspn -L vserver

FindDomainForAccount: DsGetDcNameWithAccountW failed!

Cannot find account vserver
```

The output should appear similar to the following:

```
C:Usersadministrator.CIFSLAB>setspn -Q cifs/spnTest.cifs.lab.netapp.com

Checking domain DC=cifs,DC=lab,DC=netapp,DC=com

CN=10-53-21-46,CN=Computers,DC=cifs,DC=lab,DC=netapp,DC=com

HOST/spnTest.cifs.lab.netapp.com

CIFS/spnTest.cifs.lab.netapp.com
```

```
Existing SPN found!

'''CN=10-53-21-46,CN=Computers,DC=cifs,DC=lab,DC=netapp,DC=com''' above is the
machine account for which spn is used.
```

**Resolution**:

If the above machine account is not the intended machine account, delete the spn for the machine account.

**Example**:

```
C:Usersadministrator.CIFSLAB>setspn -D cifs/spnTest.cifs.lab.netapp.com 10-53-

21-46

Unregistering ServicePrincipalNames for
CN=10-53-21-46,CN=Computers,DC=cifs,DC=l

ab,DC=netapp,DC=com

cifs/spnTest.cifs.lab.netapp.com

Updated object
```

Verify the following:

```
C:Usersadministrator.CIFSLAB>setspn -L 10-53-21-46

Registered ServicePrincipalNames for
CN=10-53-21-46,CN=Computers,DC=cifs,DC=lab,

DC=netapp,DC=com:
```

### Cause 6: A domain account is disabled and the local user requires a password change

If the `password chang`e error was not expected, the reason for this error could be that the domain account was disabled, and therefore authentication was attempted on a local user, and the local user required a password change.

For example, if the domain account is disabled, the local user is attempted. If this local user needs a password change, the `PASSWORD_MUST_CHANGE` error is returned to the user.

**How to determine if this is the cause**:

**Packet trace**:

The error STATUS_PASSWORD_MUST_CHANGE is displayed in frame 154.

```
149     2012-11-09 12:14:51.931831     10.38.18.67    10.53.35.223
SMB2    162        NegotiateProtocol Request

        150     2012-11-09 12:14:51.932250     10.53.35.223   10.38.18.
67     SMB2    308        NegotiateProtocol Response

        151     2012-11-09 12:14:51.933149     10.38.18.67    10.53.35.
223    SMB2    220        SessionSetup Request, NTLMSSP_NEGOTIATE

        152     2012-11-09 12:14:51.934442     10.53.35.223   10.38.18.
67     SMB2    393        SessionSetup Response, Error: STATUS_MORE_
PROCESSING_REQUIRED, NTLMSSP_CHALLENGE

        153     2012-11-09 12:14:51.934859     10.38.18.67    10.53.35.
223    SMB2    660        SessionSetup Request, NTLMSSP_AUTH, User:
CIFSLABusername1

        154     2012-11-09 12:14:51.939053     10.53.35.223   10.38.18.
67     SMB2    131        SessionSetup Response, Error: STATUS_PASSWORD_
MUST_CHANGE
```

secd.log (location of the log: /mroot/etc/log/mlog):

```
ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in getLocalUserHash() at
authentication/secd_seclibglue.cpp:826

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in doLocalUserAuth() at
Common/SecLibrary/Src/NtlmsspCtx.cpp:885

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in
handleAuthenticateMsg() at Common/SecLibrary/Src/NtlmsspCtx.cpp:821

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in acceptContext() at
Common/SecLibrary/Src/NtlmsspCtx.cpp:294

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in acceptContext() at
Common/SecLibrary/Src/SpnegoCtx.cpp:221

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in secd_rpc_auth_
extended_1_svc() at authentication/secd_rpc_auth.cpp:749

 debug:  SecD RPC Server sending reply to RPC 151: secd_rpc_auth_extended  { in
secdSendRpcResponse() at server/secd_rpc_server.cpp:1405 }

 ERR  :  Error: User authentication procedure failed

 ERR  :   [  0 ms] Login attempt by domain user 'CIFSLABusername1' using NTLMv2 style security

 ERR  :   [     0] Using a cached connection to a7-6.cifs.lab.netapp.com

 ERR  :   [     3] Authentication failed. (Status: 0xc0000072)

 ERR  :   [     3] Login attempt by local user 'username1' using NTLMv2 style security

 ERR  :  **[     3] FAILURE: Unexpected state: Error 335 at file:authentication/secd_seclibglue.cpp
func:getLocalUserHash line:826

 ERR  :  **[     3] FAILURE: Error case not correctly journaled

 |------------------------------------------------------------------------------.

 |                  RPC completed at Fri Nov  9 20:00:46 2012                    |

 |               End of log for failed RPC secd_rpc_auth_extended                |

 '------------------------------------------------------------------------------'
```

From the above `secd.lo g`, it can be seen that initially an attempt was made to authenticate the domain user '`CIFSLABusername1`'. However, the system received the `'0xc0000072' (Account disabled)` error from DC. Therefore, a local user was attempted as seen from message `'Login attempt by local user 'username1' using NTLMv2 style security'` .

**Resolution**:
Enable the domain account.

### Cause 7: A domain account must change password; XP client displays error 59

If the domain account needs a password change and if an XP client is used, the client displays `System error 59`.

**How to determine if this is the cause**:

**XP client**:

```
>net use * \10.53.35.223cifs_share1 /u:CIFSLABusername1 netapp12!@

System error 59 has occurred.

An unexpected network error occurred.
```

**Packet trace**:

If Kerberos is being used (or attempted) for authentication, verify using a packet trace. To confirm this, a packet trace from the client will be required. Verify using a KRB5 packet:

```
127     14.712941      172.17.193.58  172.17.193.44
KRB5                   AS-REQ

        128     14.819210      172.17.193.44  172.17.193.58
KRB5                   KRB Error: KRB5KDC_ERR_KEY_EXP NT Status: STATUS_
PASSWORD_MUST_CHANGE
```

**Resolution**:

The issue is with the XP client. The Win 7 client displays the correct error.

### Cause 8: A domain account expired; and the XP client displays error 59

If the domain account has expired and when an XP client is used, the client displays `System error 59`.

**How to determine if this is the cause:**

**XP client**:

```
>net use * \10.53.35.223cifs_share1 /u:CIFSLABusername1 netapp12!@

        System error 59 has occurred.


                    An unexpected network error occurred.
```

**Packet trace**:

If Kerberos is being used (or attempted) for authentication, verify using a packet trace. To confirm this, a packet trace from the client will be required. Verify using a KRB5 packet:

```
157     18.359405      172.17.193.58  172.17.193.44  KRB5    AS-REQ

        158     18.360464      172.17.193.44  172.17.193.58  KRB5    KRB
Error: KRB5KDC_ERR_CLIENT_REVOKED NT Status: STATUS_ACCOUNT_EXPIRED

        159     18.360690      172.17.193.58  10.53.35.223   SMB
Session Setup AndX Request, NTLMSSP_NEGOTIATE

        160     18.362408      10.53.35.223   172.17.193.58  SMB
Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_
```

```
PROCESSING_REQUIRED

        161     18.362579      172.17.193.58  10.53.35.223   SMB
Session Setup AndX Request, NTLMSSP_AUTH, User: CIFSLABusername1

        162     18.366784      10.53.35.223   172.17.193.58  SMB
Session Setup AndX Response, Error: STATUS_ACCOUNT_EXPIRED
```

**Resolution**:

The issue is with the XP client. The Win 7 client displays the correct error.

### Cause 9: A domain account has invalid logon hours; XP client displays error 59

If the domain account is configured with invalid logon hours and if an XP client is used, the client displays `System error 59`.

**How to determine if this is the cause:**
**XP client**:

```
>net use * \10.53.35.223cifs_share1 /u:CIFSLABusername1
netapp12

        System error 59 has occurred.


        An unexpected network error occurred.
```

**Packet trace**:

If Kerberos is being used (or attempted) for authentication, verify using a packet trace. To confirm this, a packet trace from the client will be required. Verify using a KRB5 packet:

```
1351 42.402610 172.17.193.58 172.17.192.24 KRB5 AS-REQ


1352 42.404662 172.17.192.24 172.17.193.58 KRB5 KRB Error:
KRB5KDC_ERR_CLIENT_REVOKED NT Status: STATUS_INVALID_LOGON_HOURS
```

**Resolution**:

The issue is with the XP client. The Win 7 client displays the correct error.

### Cause 10: No UNIX user is mapped to the Win user

This cause describes a use case where the mapping does not exist between the Win user and UNIX user.

**How to determine if this is the cause**:

```
secd.log:

| [000.005.980] ERR : RESULT_ERROR_SECD_NAME_MAPPING_DOES_NOT_EXIST:6916 in
secdGetUnixCredsForWindowsUser() at authentication/secd_rpc_auth.cpp:676

| [000.005.990] ERR : RESULT_ERROR_SECD_NAME_MAPPING_DOES_NOT_EXIST:6916 in
secdLoadUnixCredsFromContext() at authentication/secd_rpc_auth.cpp:276

| [000.005.999] ERR : RESULT_ERROR_SECD_NAME_MAPPING_DOES_NOT_EXIST:6916 in
secdLoadResponseFromContext() at authentication/secd_rpc_auth.cpp:396

| [000.006.009] ERR : RESULT_ERROR_SECD_NAME_MAPPING_DOES_NOT_EXIST:6916 in
secd_rpc_auth_extended_1_svc() at authentication/secd_rpc_auth.cpp:761

| [000.006.020] debug: SecD RPC Server sending reply to RPC 151:
secd_rpc_auth_extended { in secdSendRpcResponse() at server/
secd_rpc_server.cpp:1405 }

| [000.006.232] ERR : RESULT_ERROR_SECD_NAME_MAPPING_DOES_NOT_EXIST:6916 in
getFailureCode() at utils/secd_thread_task_journal.cpp:292

| [000.006.262] ERR : Error: User authentication procedure failed

| [000.006.268] ERR : [ 5] User 'CIFSLABAdministrator' authenticated using
NTLMv2 security

| [000.006.273] ERR : [ 5] Trying to map 'CIFSLABAdministrator' to UNIX user
'administrator' using implicit mapping

| [000.006.279] ERR : [ 5] Name 'administrator' not found in UNIX authorization
source LOCAL

| [000.006.284] ERR : [ 5] Could not get an ID for name 'administrator' using
any NS-SWITCH authorization source

| [000.006.289] ERR : [ 5] Trying to map user to the default UNIX name 'none'
| [000.006.295] ERR : [ 5] Name 'none' not found in UNIX authorization source
LOCAL

| [000.006.300] ERR : [ 5] Could not get an ID for name 'none' using any NS-
SWITCH authorization source

| [000.006.306] ERR : **[ 5] FAILURE: Unable to map Windows user
'CIFSLABAdministrator' to appropriate UNIX user

|------------------------------------------------------------------------------
.

| RPC completed at Mon Nov 12 19:56:35 2012 |

| End of log for failed RPC secd_rpc_auth_extended |

'------------------------------------------------------------------------------
'
```

From the above `secd.log`, it can be seen from the line `Trying to map 'CIFSLABAdministrator'` to `UNIX user 'administrator'` using implicit mapping that the user ' `CIFSLABAdministrator`' is attempted to map to the UNIX user `'administrator'`. It indicates that the name-mapping is not configured. Then, it attempts to map the user to the default UNIX user 'none', which is also not set correctly.

Check the name-mapping and the default UNIX user.

```
sn_burts::*> name-mapping show

          (vserver name-mapping show)

       Vserver        Direction Position

       -------------- --------- --------

       vserver2       win-unix  1        Pattern: cifslab\\Administrator

                                      Replacement: root

       vserver2       win-unix  2        Pattern: NFSQA-
CIFS\\Administrator

                                      Replacement: root
```

```
        vserver2       win-unix   3        Pattern: NFSQA\\Administrator
                                       Replacement: root
        vserver2       unix-win   1        Pattern: root
                                       Replacement: cifslab\\Administrator
        4 entries were displayed.
```

It can be seen from the above command output that no name-mapping is configured for Vserver1.
**Note:** See Important considerations when setting up CIFS and name-mapping in clustered Data ONTAP.

```
sn_burts::> cifs options show -vserver vserver1
                                                 Vserver: vserver1
                                       Default UNIX User: none
                            Read Grants Exec for Mode Bits: disabled
        Windows Internet Name Service (WINS) Addresses: 172.17.152.42
                       Default UNIX Group:
```

-

It can be seen from the above command output that, the default UNIX user is not set correctly.

**Resolution**:
Create a name mapping for win-unix. This can be done by running the `vserver name-mapping create` command.
Set the default UNIX user by running the `vserver cifs options modify` command.

### Cause 11: Trusted domain not configured in active directory

This cause describes a use case where authentication of a trusted domain user fails.

**How to determine if this is the cause:**

```
secd.log:

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in
getLocalUserHash() at authentication/secd_seclibglue.cpp:826
```

```
 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in
doLocalUserAuth() at Common/SecLibrary/Src/Nt4Ctx.cpp:283

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in
acceptContext() at Common/SecLibrary/Src/Nt4Ctx.cpp:147

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in secd_rpc_auth_
pass_through_1_svc() at authentication/secd_rpc_auth.cpp:866

 debug:  SecD RPC Server sending reply to RPC 152: secd_rpc_auth_pass_
through  { in secdSendRpcResponse() at server/secd_rpc_server.cpp:1405 }

 ERR  :  RESULT_ERROR_CIFS_SMB_PASSWORD_MUST_CHANGE:335 in
getFailureCode() at utils/secd_thread_task_journal.cpp:292

 ERR  :  Error: User authentication procedure failed

 ERR  :    [  0 ms] Login attempt by domain user 'nativelhadministrator'
using NTLMv2 style security

 ERR  :    [     0] Using a cached connection to cifsqa-dc-1.cifsqa.lab.
netapp.com

 ERR  :    [     1] Authentication failed. (Status: 0xc0000064)

 ERR  :    [     1] Login attempt by local user 'administrator' using
NTLMv2 style security

 ERR  :  **[     1] FAILURE: login-cifs failed

 debug:  Journaling CIFS auth with unhandled failureCode: 335  { in
secdLogJournal() at server/secd_rpc_server.cpp:932 }

 debug:  Logged EMS message for journal.  Status = 0  { in
secdLogJournal() at server/secd_rpc_server.cpp:982 }

 |-------------------------------------------------------------------------
------.

 |                   RPC completed at Mon Nov 12 22:30:23
2012                       |

 |              End of log for failed RPC secd_rpc_auth_pass_
through             |
 '-------------------------------------------------------------------------------------
-------'
```

It can be seen from the above `secd.log` that while attempting to authenticate a trusted domain user '`nativelhadministrator`', the DC returns the error `0xc0000064(STATUS_NO_SUCH_USER)`. Therefore, a local user is attempted, as seen from the message `Login attempt by local user 'administrator' using NTLMv2 style security.`

**Resolution**:

1. Log in to DC and open the **Active Directory Domains and Trusts** tool from **Start** >**Programs** >**Administrative Tools** >**Active Directory Domains and Trusts**
2. Select the domain and right-click it.
3. Go to **Properties** and click the **Trusts** tab.

Ensure your trusted domain is listed in the **Domains trusted by this domain** list. Then, select the trusted domain and click **Properties**.

A window will be displayed, attempt to validate the trusted domain by providing the credentials. Ensure that the validation succeeds.

## Additional Information

Add your text here.