Received error from KDC: -1765328322/Client not trusted

- Parallels Secure Workspace

Symptoms

First, see How to analyze the log files to identify single-sign on (SSO) issues .

Single sign-on fails. In **awingu-worker-smc.service.log**, a similar error can be seen:

```
2023-01-26 07:54:34.551110 psw01 awingu-worker-smc.service[manage.py:25766]:
Using specified cache:
/etc/awingu/domains/WORKSPACEDOMAIN/9a98da27-9203-4510-b3f1-993997c20c84/kerberos/ke
Using principal: someuser\@somedomain.org@SOMEWINDOWSDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/domains/WORKSPACEDOMAIN/9a98da27-9203-4510-b3f1-993997c20c84/certif
[15543] 1674719674.309931: Getting initial credentials for
someuser\@somedomain.org@SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309933: Sending unauthenticated request
[15543] 1674719674.309934: Sending request (219 bytes) to
SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309935: Resolving hostname SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309936: Sending initial UDP request to dgram 10.1.2.3:88
[15543] 1674719674.309937: Received answer (214 bytes) from dgram 10.1.2.3:88
[15543] 1674719674.309938: Sending DNS URI query for
_kerberos.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309939: No URI records found
[15543] 1674719674.309940: Sending DNS SRV query for
_kerberos-master._udp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309941: Sending DNS SRV query for
_kerberos-master._tcp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309942: No SRV records found
[15543] 1674719674.309943: Response was not from master KDC
[15543] 1674719674.309944: Received error from KDC: -1765328359/Additional
pre-authentication required
[15543] 1674719674.309947: Preauthenticating using KDC method data
[15543] 1674719674.309948: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[15543] 1674719674.309949: Selected etype info: etype aes256-cts, salt
"SOMEWINDOWSDOMAIN.ORGsomeuser", params ""
[15543] 1674719674.309950: PKINIT loading CA certs and CRLs from FILE
[15543] 1674719674.309951: PKINIT client computed kdc-req-body checksum
9/2B2890045D086634ED8C98F640115ED6BCE72DF5
[15543] 1674719674.309953: PKINIT client making DH request
[15543] 1674719674.309954: Preauth module pkinit (16) (real) returned:
0/Success
[15543] 1674719674.309955: Produced preauth for next request: PA-PK-AS-REQ
(16)
[15543] 1674719674.309956: Sending request (5959 bytes) to
SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309957: Resolving hostname SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309958: Initiating TCP connection to stream 10.1.2.3:88
```

```
[15543] 1674719674.309959: Sending TCP request to stream 10.1.2.3:88
[15543] 1674719674.309960: Received answer (137 bytes) from stream
10.1.2.3:88
[15543] 1674719674.309961: Terminating TCP connection to stream 10.1.2.3:88
[15543] 1674719674.309962: Sending DNS URI query for
_kerberos.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309963: No URI records found
[15543] 1674719674.309964: Sending DNS SRV query for
_kerberos-master._udp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309965: Sending DNS SRV query for
_kerberos-master._tcp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309966: No SRV records found
[15543] 1674719674.309967: Response was not from master KDC
[15543] 1674719674.309968: Received error from KDC: -1765328322/Client not
trusted
[15543] 1674719674.309970: Recovering from KDC error 62 using preauth mech
PA-PK-AS-REQ (16)
[15543] 1674719674.309971: Preauth tryagain input types (16): (empty)
[15543] 1674719674.309972: Preauth module pkinit (16) tryagain returned:
-1765328360/Preauthentication failed
[15543] 1674719674.309973: Retrying AS request with master KDC
[15543] 1674719674.309974: Getting initial credentials for
someuser\@somedomain.org@SOMEWINDOWSDOMAIN.ORG
[15543] 1674719674.309976: Sending unauthenticated request
[15543] 1674719674.309977: Sending request (219 bytes) to
SOMEWINDOWSDOMAIN.ORG (master)
[15543] 1674719674.309978: Sending DNS URI query for
_kerberos.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309979: No URI records found
[15543] 1674719674.309980: Sending DNS SRV query for
_kerberos-master._udp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309981: Sending DNS SRV query for
_kerberos-master._tcp.SOMEWINDOWSDOMAIN.ORG.
[15543] 1674719674.309982: No SRV records found
kinit: Client not trusted while getting initial credentials
```

Cause

The client is not trusted by the Kerberos Domain Controller(s).

There are a variety of causes for this. Usually, the Windows Event Viewer of the Kerberos Domain Controller has a more specific indication.

Most common reasons:

- The Certification Revocation List (CRL) can not be reached.
- Windows Time Service is incorrect (or does not match the time of the Parallels Secure Workspace appliance).
- The Workspace SubCA certificate is not present on all Kerberos Domain Controllers, or it is no longer valid (expired or revoked).
- For this error, there is typically a very decent indication in the Windows Event Viewer of the KDC server. Check event 21: ?Windows Event Viewer - Kerberos events .

Resolution

Narrowing down the cause

The Windows Event Viewer on the Kerberos Domain Controllers helps to identify the cause.
After applying a solution, make sure to validate if it worked. If it's still not working, confirm whether the cause is still the same.

To find out the cause, try running the following PowerShell snippet as an administrator.
Mind adjusting the host names to match the domain controllers in this Windows environment.

```
Get-EventLog -LogName 'System' -Source 'KDC' -After
(Get-Date).AddDays(-1) -ComputerName dc01, dc02 | fl MachineName,
EventId, TimeGenerated, Message | Out-File
'$env:userprofile\desktop\kdc_events.txt'
```

Check the contents of the file.

Alternatively, at the individual Kerberos Domain Controller(s):

1. Open the Windows Event Viewer.
2. Navigate to **Custom Views > Administrative Events.**
3. Look for log entries with **Event ID 21** originating from **Kerberos-Key-Distribution-Center** ("source").

Mind that **Event ID 21** comes with a generic first part of the description: The client certificate for the user SOMEDOMAIN\someuser is not valid, and resulted in a failed smartcard logon. Please contact the user for more information about the certificate they're attempting to use for smartcard logon.

However, after that, one of these more specific messages will follow:

The chain status was : A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Most common cause: the time between the Kerberos Domain Controller(s) and the Parallels Secure Workspace appliance is not in sync. Try to have all of them in sync with real-world time.

See Check the time on an appliance .

The chain status was : A certification chain processed correctly, but one of the CA certificates is not trusted by the policy provider.

Import the Workspace SubCA certificate in the NTAuthStore.

```
certutil -dspublish -f workspace.cer NTAuthCA
certutil -enterprise -addstore NTAuth workspace.cer
```

Verify:
```
certutil -enterprise -viewstore NTAuth
```

If still not working:

- Make sure any intermediate certificates and the root CA certificate present in the Workspace SubCA certification path are also published.
- Make sure they're also present in the local certificate store of the Kerberos Domain Controllers.

The chain status was : The revocation function was unable to check revocation because the revocation server was offline.

See Microsoft Windows Server: Verify retrieval of Certificate Revocation List (CRL)

The chain status was : A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.

Most common cause: the time between the Kerberos Domain Controller(s) and the Parallels Secure Workspace appliance is not in sync. Try to have all of them in sync with real-world time.

See Check the time on an appliance .

Verify whether the Workspace SubCA certificate is properly imported in the NTAuth store
`certutil –viewstore –enterprise NTAuth`

Verify whether all the other certificates in the certification path of the Workspace SubCA are all trusted by the domain controller(s)

If the above solutions don't resolve the issue, please contact the support team.
