



Preauth module pkinit (17) (real) returned: -1765328308/KDC name mismatch

- 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:

```
2021-09-10 11:41:32.493618 awingu awingu-worker-smc.service[python3:1194]:
Generating a 2048 bit RSA private key
2021-09-10 11:41:32.510919 awingu awingu-worker-smc.service[python3:1194]:
.....+++
2021-09-10 11:41:32.512982 awingu awingu-worker-smc.service[python3:1194]:
.+++
2021-09-10 11:41:32.513234 awingu awingu-worker-smc.service[python3:1194]:
unable to write 'random state'
2021-09-10 11:41:32.513385 awingu awingu-worker-smc.service[python3:1194]:
writing new private key to 'private_key.pem'
2021-09-10 11:41:32.513532 awingu awingu-worker-smc.service[python3:1194]:
-----
2021-09-10 11:41:32.561966 awingu awingu-worker-smc.service[python3:1194]:
writing RSA key
2021-09-10 11:41:32.685396 awingu awingu-worker-smc.service[manage.py:16603]:
Password for someuser\@somedomain.org@SOMEDOMAIN.ORG:

2021-09-10 11:41:32.685611 awingu awingu-worker-smc.service[manage.py:16603]:
Using specified cache:
/etc/awingu/domains/SOMEAWINGUDOMAIN/0f5854e8-8775-4604-a4fd-919391b078f4/kerberos/k
Using principal: someuser\@somedomain.org@SOMEDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/domains/SOMEAWINGUDOMAIN/0f5854e8-8775-4604-a4fd-919391b078f4/certi
[24324] 1631274092.590565: Getting initial credentials for
someuser\@somedomain.org@SOMEDOMAIN.ORG
[24324] 1631274092.590567: Sending unauthenticated request
[24324] 1631274092.590568: Sending request (211 bytes) to SOMEDOMAIN.ORG
[24324] 1631274092.590569: Resolving hostname 10.1.2.3
[24324] 1631274092.590570: Sending initial UDP request to dgram 10.1.2.3:88
[24324] 1631274092.590571: Received answer (202 bytes) from dgram 10.1.2.3:88
[24324] 1631274092.590572: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[24324] 1631274092.590573: No URI records found
[24324] 1631274092.590574: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[24324] 1631274092.590575: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[24324] 1631274092.590576: No SRV records found
[24324] 1631274092.590577: Response was not from master KDC
[24324] 1631274092.590578: Received error from KDC: -1765328359/Additional
```

```
pre-authentication required
[24324] 1631274092.590581: Preauthenticating using KDC method data
[24324] 1631274092.590582: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[24324] 1631274092.590583: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGSomeUser", params ""
[24324] 1631274092.590584: PKINIT loading CA certs and CRLs from FILE
[24324] 1631274092.590585: PKINIT client computed kdc-req-body checksum
9/8C2B5A6C5555AF5D9A19ADFFF88D4114CB5764A1
[24324] 1631274092.590587: PKINIT client making DH request
[24324] 1631274092.590588: Preauth module pkinit (16) (real) returned:
0/Success
[24324] 1631274092.590589: Produced preauth for next request: PA-PK-AS-REQ
(16)
[24324] 1631274092.590590: Sending request (4908 bytes) to SOMEDOMAIN.ORG
[24324] 1631274092.590591: Resolving hostname 10.1.2.3
[24324] 1631274092.590592: Initiating TCP connection to stream 10.1.2.3:88
[24324] 1631274092.590593: Sending TCP request to stream 10.1.2.3:88
[24324] 1631274092.590594: Received answer (5450 bytes) from stream
10.1.2.3:88
[24324] 1631274092.590595: Terminating TCP connection to stream 10.1.2.3:88
[24324] 1631274092.590596: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[24324] 1631274092.590597: No URI records found
[24324] 1631274092.590598: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[24324] 1631274092.590599: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[24324] 1631274092.590600: No SRV records found
[24324] 1631274092.590601: Response was not from master KDC
[24324] 1631274092.590602: Processing preauth types: PA-PK-AS-REP (17)
[24324] 1631274092.590603: PKINIT client verified DH reply
[24324] 1631274092.590604: PKINIT client config accepts KDC dNSName SAN
10.1.2.3
[24324] 1631274092.590605: PKINIT client config accepts KDC dNSName SAN
10.1.2.4
[24324] 1631274092.590606: PKINIT client config accepts KDC dNSName SAN
10.1.2.3
[24324] 1631274092.590607: PKINIT client config accepts KDC dNSName SAN
10.1.2.4
[24324] 1631274092.590608: PKINIT client found dNSName SAN in KDC cert:
somehost1.somedomain.org
[24324] 1631274092.590609: PKINIT client found dNSName SAN in KDC cert:
somehost2.somedomain.org
[24324] 1631274092.590610: PKINIT client found dNSName SAN in KDC cert:
SOMEHOST
[24324] 1631274092.590611: PKINIT client found no acceptable SAN in KDC cert
[24324] 1631274092.590612: Preauth module pkinit (17) (real) returned:
-1765328308/KDC name mismatch
[24324] 1631274092.590613: Produced preauth for next request: (empty)
[24324] 1631274092.590614: Getting AS key, salt "SOMEDOMAIN.ORGSomeUser",
params ""
kinit: Cannot read password while getting initial credentials
```

Cause

The certificate presented by the Kerberos Domain Controller (KDC) is missing the Subject Alternative Name (SAN) for the KDC itself.

Resolution

See [Reissue KDC Authentication certificate for domain controllers](#)

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.