



Received error from KDC: -1765328368/KDC has no support for padata type

- 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:

```
2022-03-16 13:27:29.812414 someawinguhost
awingu-worker-smc.service[manage.py:1763]: Processed
[nitrogen-alaska-social-pip]
2022-03-16 13:27:34.439388 someawinguhost
awingu-worker-smc.service[manage.py:16443]: Process-1:8 processing
cdsessions.tasks.refresh_sso_certificate [fifteen-ink-london-mike]
2022-03-16 13:27:34.460661 someawinguhost
awingu-worker-smc.service[python3:858]: Generating a RSA private key
2022-03-16 13:27:34.592015 someawinguhost
awingu-worker-smc.service[python3:858]:
.....
2022-03-16 13:27:34.621520 someawinguhost
awingu-worker-smc.service[python3:858]: .....+++++
2022-03-16 13:27:34.621769 someawinguhost
awingu-worker-smc.service[python3:858]: writing new private key to
'private_key.pem'
2022-03-16 13:27:34.621897 someawinguhost
awingu-worker-smc.service[python3:858]: -----
2022-03-16 13:27:34.674429 someawinguhost
awingu-worker-smc.service[python3:858]: writing RSA key
2022-03-16 13:27:34.776781 someawinguhost
awingu-worker-smc.service[manage.py:16443]:
2022-03-16 13:27:34.777026 someawinguhost
awingu-worker-smc.service[manage.py:16443]: Using specified cache:
/etc/awingu/DOMAINS/WORKSPACEDOMAIN/0e3dd051-bf28-4410-9369-a8e42357b677/kerberos/ke
Using principal: someuser\@somedomain.org@SOMEDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/DOMAINS/WORKSPACEDOMAIN/0e3dd051-bf28-4410-9369-a8e42357b677/certif
[17231] 1647437254.679700: Getting initial credentials for
someuser\@somedomain.org@SOMEDOMAIN.ORG
[17231] 1647437254.679702: Sending unauthenticated request
[17231] 1647437254.679703: Sending request (240 bytes) to SOMEDOMAIN.ORG
[17231] 1647437254.679704: Resolving hostname SOMEHOST.somedomain.org
[17231] 1647437254.679705: Sending initial UDP request to dgram 10.1.2.3:88
[17231] 1647437254.679706: Received answer (227 bytes) from dgram 10.1.2.3:88
[17231] 1647437254.679707: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[17231] 1647437254.679708: No URI records found
[17231] 1647437254.679709: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
```

[17231] 1647437254.679710: SRV answer: 0 100 88 "somehost.somedomain.org."
[17231] 1647437254.679711: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[17231] 1647437254.679712: SRV answer: 0 0 88 "somehost.somedomain.org."
[17231] 1647437254.679713: Response was not from master KDC
[17231] 1647437254.679714: Received error from KDC: -1765328359/Additional
pre-authentication required
[17231] 1647437254.679717: Preauthenticating using KDC method data
[17231] 1647437254.679718: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[17231] 1647437254.679719: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGsomeuser", params ""
[17231] 1647437254.679720: PKINIT loading CA certs and CRLs from FILE
[17231] 1647437254.679721: PKINIT client computed kdc-req-body checksum
9/BD355C58F5C6B6CDC6E558B6C0108CDCA8A5AECB
[17231] 1647437254.679723: PKINIT client making DH request
[17231] 1647437254.679724: Preauth module pkinit (16) (real) returned:
0/Success
[17231] 1647437254.679725: Produced preauth for next request: PA-PK-AS-REQ
(16)
[17231] 1647437254.679726: Sending request (4976 bytes) to SOMEDOMAIN.ORG
[17231] 1647437254.679727: Resolving hostname SOMEHOST.somedomain.org
[17231] 1647437254.679728: Initiating TCP connection to stream 10.1.2.3:88
[17231] 1647437254.679729: Sending TCP request to stream 10.1.2.3:88
[17231] 1647437254.679730: Received answer (151 bytes) from stream
10.1.2.3:88
[17231] 1647437254.679731: Terminating TCP connection to stream 10.1.2.3:88
[17231] 1647437254.679732: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[17231] 1647437254.679733: No URI records found
[17231] 1647437254.679734: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[17231] 1647437254.679735: SRV answer: 0 100 88 "somehost.somedomain.org."
[17231] 1647437254.679736: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[17231] 1647437254.679737: SRV answer: 0 0 88 "somehost.somedomain.org."
[17231] 1647437254.679738: Response was not from master KDC
[17231] 1647437254.679739: Received error from KDC: -1765328368/KDC has no
support for padata type
[17231] 1647437254.679741: Recovering from KDC error 16 using preauth mech
PA-PK-AS-REQ (16)
[17231] 1647437254.679742: Preauth tryagain input types (16): (empty)
[17231] 1647437254.679743: Preauth module pkinit (16) tryagain returned:
-1765328360/Preauthentication failed
[17231] 1647437254.679744: Retrying AS request with master KDC
[17231] 1647437254.679745: Getting initial credentials for
someuser\@somedomain.org@SOMEDOMAIN.ORG
[17231] 1647437254.679747: Sending unauthenticated request
[17231] 1647437254.679748: Sending request (240 bytes) to SOMEDOMAIN.ORG
(master)
[17231] 1647437254.679749: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[17231] 1647437254.679750: No URI records found
[17231] 1647437254.679751: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[17231] 1647437254.679752: SRV answer: 0 100 88 "somehost.somedomain.org."
[17231] 1647437254.679753: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.

```

[17231] 1647437254.679754: SRV answer: 0 0 88 "somehost.somedomain.org."
[17231] 1647437254.679755: Resolving hostname somehost.somedomain.org.
[17231] 1647437254.679756: Sending initial UDP request to dgram 10.1.2.3:88
[17231] 1647437254.679757: Received answer (227 bytes) from dgram 10.1.2.3:88
[17231] 1647437254.679758: Received error from KDC: -1765328359/Additional
pre-authentication required
[17231] 1647437254.679761: Preauthenticating using KDC method data
[17231] 1647437254.679762: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[17231] 1647437254.679763: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGsomeuser", params ""
[17231] 1647437254.679764: PKINIT loading CA certs and CRLs from FILE
[17231] 1647437254.679765: PKINIT client computed kdc-req-body checksum
9/188D18301E7E52D58A7B1D48DDC215D18DE3AFA4
[17231] 1647437254.679767: PKINIT client making DH request
[17231] 1647437254.679768: Preauth module pkinit (16) (real) returned:
0/Success
[17231] 1647437254.679769: Produced preauth for next request: PA-PK-AS-REQ
(16)
[17231] 1647437254.679770: Sending request (4977 bytes) to SOMEDOMAIN.ORG
(master)
[17231] 1647437254.679771: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[17231] 1647437254.679772: No URI records found
[17231] 1647437254.679773: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[17231] 1647437254.679774: SRV answer: 0 100 88 "somehost.somedomain.org."
[17231] 1647437254.679775: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[17231] 1647437254.679776: SRV answer: 0 0 88 "somehost.somedomain.org."
[17231] 1647437254.679777: Resolving hostname somehost.somedomain.org.
[17231] 1647437254.679778: Resolving hostname somehost.somedomain.org.
[17231] 1647437254.679779: Initiating TCP connection to stream 10.1.2.3:88
[17231] 1647437254.679780: Sending TCP request to stream 10.1.2.3:88
[17231] 1647437254.679781: Received answer (151 bytes) from stream
10.1.2.3:88
[17231] 1647437254.679782: Terminating TCP connection to stream 10.1.2.3:88
[17231] 1647437254.679783: Received error from KDC: -1765328368/KDC has no
support for padata type
[17231] 1647437254.679785: Recovering from KDC error 16 using preauth mech
PA-PK-AS-REQ (16)
[17231] 1647437254.679786: Preauth tryagain input types (16): (empty)
[17231] 1647437254.679787: Preauth module pkinit (16) tryagain returned:
-1765328360/Preauthentication failed
kinit: KDC has no support for padata type while getting initial credentials

```

Cause

Currently, this has only been observed when the Kerberos Domain Controller presented a certificate issued by a Root CA whose Certificate Revocation List (CRL) was unavailable.

It may also occur when a domain controller doesn't have a certificate installed for smart cards (Domain Controller or Domain Controller Authentication templates).

Resolution

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

Also, make sure the CRL of the Root CA is available.

If still not resolved, contact the support team.

© 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.