z/OS Communications Server

Documentation changes for APAR PH45902

AT-TLS support for x25519 and x448 key exchange for TLSv1.2

Version 2 Release 5

z/OS Communications Server

z/OS Communications Server

CONTENTS

NEW FUNCTION SUMMARY

AT-TLS support for x25519 and x448 key exchange for TLSv1.2

z/OS V2R5 Communications Server with APAR PH45902 provides AT-TLS support for a TLSv1.2 server to specify which elliptic curves can be used for the handshake key exchange when an ephemeral ECDH (Elliptic curve Diffie-Hellman) cipher is used. Support is also added for the x25519 and x448 curves for TLSv1.2 handshake key exchange.

These updates also apply to TLSv1.0 and TLSv1.1.

Restrictions:

For TLSv1.0, TLSv1.1, and TLSv1.2, curves x25519 and x448 are not enabled by default and must be configured explicitly both for the AT-TLS client and server.

Dependency:

z/OS V2R5 System SSL APAR OA61783 is required.

Using AT-TLS support for x25519 and x448 key exchange for TLSv1.2

To use AT-TLS support for x25519 and x448 key exchange for TLSv1.2, perform the tasks in Table 1. AT-TLS support for x25519 and x448 key exchange for TLSv1.2.

Table 1. AT-TLS support for x25519 and x448 key exchange for TLSv1.2

Task/Procedure	Reference
Understand the use of elliptic curves for a TLSv1.0 -TLSv1.2 negotiation	• Limiting Key Exchange Elliptic Curves for TLSv1.0, TLSv1.1, and TLSv1.2 in IP Configuration Guide
Configure a list of allowed elliptical curves for TLSv1.0-TLSv1.2 key exchange negotiations for an AT-TLS server.	• Online help of IBM Configuration Assistant for z/OS Communications Server • ServerKexECurves parameter on the TTLSSignatureParms statement in IP Configuration Reference
Configure support for elliptic curves x25519 and x448 for TLSv1.0-TLSv1.2 key exchange negotiations for an AT-TLS client.	• Online help of IBM Configuration Assistant for z/OS Communications Server • ClientECurves parameter on the

	TTLSSignatureParms statement in IP Configuration Reference
Display AT-TLS policy using the z/OS UNIX pasearch command to query information from the Policy Agent.	The z/OS UNIX pasearch command: Display policies in IP System Administrator's Commands
Display AT-TLS policy for an active connection using the Netstat TTLS/-x command.	Netstat TTLS/-x report in IP System Administrator's Commands

General updates for the non-PROFILE.TCPIP IP configuration files

Table 2. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R5 lists the general updates for the Communications Server IP configuration files.

Table 2. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R5

File	Statement/Entry	Description	Reason for change
AT-TLS policy files	TTLSSignatureParms	• New parameter ServerKexECurves • New values x25519 and x448 on the ClientECurves parameter	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

Netstat operator commands (DISPLAY TCPIP,,NETSTAT)

Table 3. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5 lists the new and updated Communications Server IP Netstat operator command DISPLAY TCPIP,,NETSTAT.

Table 3. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5

Parameter	Description	Reason for change
TTLS CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

NETSTAT TSO commands

Table 4. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5 lists the new and updated Communications Server NETSTAT TSO command.

Table 4. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5

Parameter	Description	Reason for change
TTLS CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

Netstat UNIX commands

Table 5. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5 lists the new and updated Communications Server z/OS UNIX netstat command.

Table 5. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5

Parameter	Description	Reason for change
–x CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

General updates of z/OS UNIX commands

Table 6. New and changed Communications Server z/OS UNIX commands for z/OS V2R5 lists the new and updated Communications Server z/OS UNIX non-netstat command.

Table 6. New and changed Communications Server z/OS UNIX commands for z/OS V2R5

Command	Parameter	Description	Reason for change

pasearch	-t	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

TCPIPCS subcommand

Table 7. New and changed Communications Server TCPIPCS subcommand options for z/OS V2R5 lists the TCPIPCS subcommand options.

Table 7. New and changed Communications Server TCPIPCS subcommand options for z/OS V2R5

Subcommand	Description	Reason for change
TTLS	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2

Limiting Key Exchange Elliptic Curves for TLSv1.0, TLSv1.1, and TLSv1.2

When using an Ephemeral Elliptic Curve Diffie Hellman cipher (TLS_ECDHE_xxx), each side of the connection being negotiated generates an elliptic curve key pair and exchanges the public key as part of the TLSv1.0, TLSv1.1, or TLSv1.2 handshake process. The elliptic curve is selected by the TLS server using a list of supported elliptic curves provided by the TLS client.

For a TLS client, the list of supported elliptic curves is defined using the ClientECurves parameter on the TTLSSignatureParms statement. This list represents the curves supported by the TLS client for the key exchange in the client's preferred order. This list also represents certificate elliptic curves supported when a server is using an elliptic curve public key certificate.

For a TLS server, the list of allowed curves is defined using the ServerKexECurves parameter on the TTLSSignatureParms statement. This list represents the allowed key exchange curves with no defined order.

Example:

For a TLS client that supports secp256r1 (0023) and secp384r1 (0024) and prefers that secp256r1 be used, ClientECurves would be configured as

```
ClientECurves 00230024
```

If the TLS server supports secp384r1 (0024), x25519 (0029) and secp256r1 (0023), ServerKexECurves would be configured as:

```
ServerKexECurves 002400290023
```

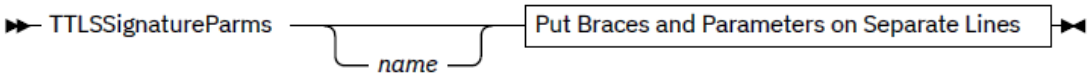
The TLS server selects the first elliptic curve in the client's list which is included in the server's supported list. In this example, the key exchange process for a connection between the client and server would use secp256r1 (0023).

For more information on configuring ClientECurves and ServerKexECurves, see the TTLSSignatureParms statement in IP Configuration Reference.

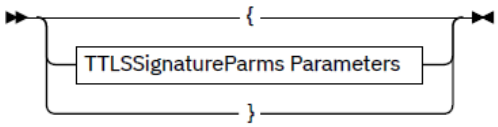
TTLSSignatureParms statement

Use the TTLSSignatureParms statement to define the client and server elliptic curve preferences and the client signature algorithm pair specifications for an AT-TLS environment or an AT-TLS connection. A TTLSSignatureParms statement can be specified inline in a TTLSEnvironmentAction or TTLSConnectionAction statement or referenced by a TTLSEnvironmentAction or TTLSConnectionAction statement.

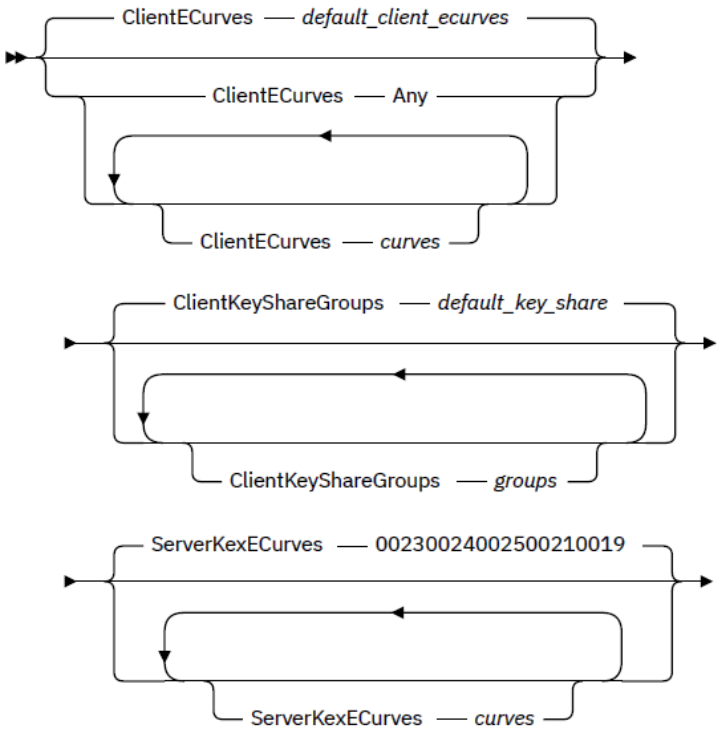
Syntax

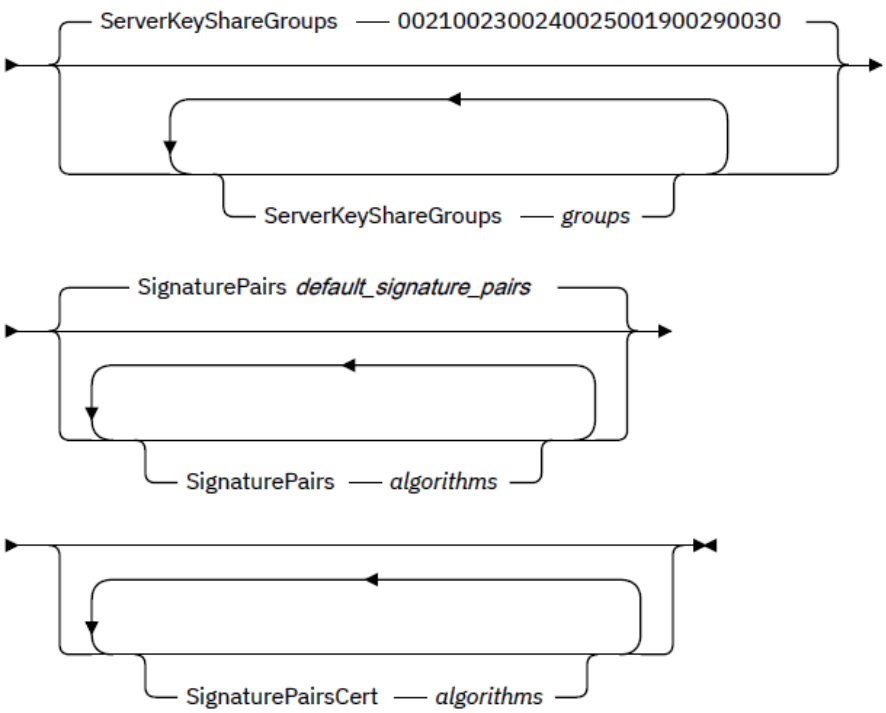


Put Braces and Parameters on Separate Lines



TTLSSignatureParms Parameters





Parameters

name

A string 1 - 32 characters in length that specifies the name of this TTLSSignatureParms statement.

Rule: If this TTLSSignatureParms statement is not specified inline in another statement, a name value must be provided. If a name is not specified for an inline TTLSSignatureParms statement, a nonpersistent system name is created.

ClientECurves

Specifies the list of ECDH (Elliptic curve Diffie-Hellman) curves that are supported by the client, in order of preference for use.

- For TLSv1.0, TLSv1.1, TLSv1.2: This list is used by the client to guide the server as to which elliptical curves are preferred when using cipher suites that use elliptical curve cryptography.
- For TLSv1.3: This list is used by the client to guide the server as to which elliptic curves are preferred and to guide group selection for encryption and decryption of handshake messages.

Only NIST recommended curves along with x25519 and x448 can be specified.

Restriction: For TLSv1.0, TLSv1.1, and TLSv1.2, if x25519 or x448 is specified and the partner is using an ECDSA certificate, the certificate's elliptic curve must also be included in the ClientECurves list of curves. AT-TLS does not support X25519 and x448 certificates.

For TLSv1.0, TLSv1.1, and TLSv1.2, to allow the use of Brainpool standard curve certificates for a TLS connection, the list must contain only the ANY curve name constant.

Restriction: Brainpool certificates cannot be used in FIPS mode or if the negotiated protocol is TLSv1.3.

Restriction: When TLSv1.3 is enabled, a value of ANY will result in a failure.

If a ClientECurves parameter is specified more than once, the values are concatenated to create a single list of elliptic curve enumerators. The ANY curve name constant cannot be specified in combination with any specific curve values. For System SSL, the GSK_CLIENT_ECURVE_LIST value is set to the concatenated value or to NULL if ANY is specified.

The curves value is a string of one or more 4-character curve enumerators or a single curve name constant. The curve string cannot have blanks between the curve enumerators. If duplicate curves are specified, the first instance is used and all other instances are ignored. The maximum number of curves is 16. For System SSL, see *Table 16. Supported elliptic curve (group) definitions for TLS V1.0, TLS V1.1, TLS V1.2, and TLS V1.3 and supported key share definitions for TLS V1.3* in *z/OS Cryptographic Services System SSL Programming* for a list of valid elliptic curves and the TLS versions for which the curves are supported. Table 73 ClientEcurves/ServerKexECurves lists the supported elliptic curve name constants.

default_client_ecurves

For an environment action, the default is dependent on whether TLSv1.3 is enabled for the environment action or not.

- If TLSv1.3 is enabled for the environment action, the default is 0021002300240025001900 29 which includes secp224r1, secp256r1, secp384r1, secp521r1, secp192r1, x25519.
- If TLSv1.3 is not enabled for the environment action, the default is 002100230024002500 19 which includes secp224r1, secp256r1, secp384r1, secp521r1, secp192r1.

For a connection action, if the TLSv1.3 parameter is explicitly configured for the connection action, the default is determined as follows:

- If TLSv1.3 is enabled for the connection action, the default is 0021002300240025001900 29 which includes secp224r1, secp256r1, secp384r1, secp521r1, secp192r1, x25519.
- If TLSv1.3 is disabled for the connection action, the default is 002100230024002500 19 which includes secp224r1, secp256r1, secp384r1, secp521r1, secp192r1.
- Otherwise, if TLSv1.3 is not configured for the connection action, there is no default and the setting is determined by the associated environment action.

Table 73 ClientEcurves / ServerKexECurves

Table 73 ClientEcurves / ServerKexECurves		
Elliptic curve name constants	Elliptic Curve Enumerator	Supported TLS versions

secp192r1	0019	TLS V1.0, V1.1, V1.2
secp224r1	0021	TLS V1.0, V1.1, V1.2
secp256r1	0023	TLS V1.0, V1.1, V1.2, V1.3
secp384r1	0024	TLS V1.0, V1.1, V1.2, V1.3
secp521r1	0025	TLS V1.0, V1.1, V1.2, V1.3
X25519	0029	TLS V1.0, V1.1, V1.2, V1.3
X448	0030	TLS V1.0, V1.1, V1.2, V1.3

...

ServerKexECurves

Specifies the list of ECDH (Elliptic curve Diffie-Hellman) curves that are supported by the server during a TLS V1.0, TLS V1.1, or TLS V1.2 handshake. This list is used by the server to limit which elliptic curves can be used for the handshake key exchange when an ephemeral ECDH cipher (TLS_ECDHE_xxx) is utilized.

The curves value is a string of one or more 4-character curve enumerators or a single curve name constant. The curve list cannot have blanks between the curve enumerators. If duplicate curves are specified, the first instance is used, and all other instances are ignored.

If a ServerKexECurves parameter is specified more than once, the values are concatenated to create a single list of curve enumerators. For System SSL, the GSK_SERVER_ALLOWED_KEX_ECURVES value is set to the concatenated value.

For System SSL, see *Table 29. Supported elliptic curve (group) definitions for TLS V1.0, TLS V1.1, TLS V1.2, and TLS V1.3 and supported key share definitions for TLS V1.3* in *z/OS Cryptographic Services System SSL Programming Guide* for a list of valid elliptic curves and the TLS versions for which the curve is supported. Table 73 ClientEcurves/ServerKexECurves lists the supported elliptic curve name constants.

For an environment action, the default value for ServerKexECurves is 00230024002500210019 which includes secp256r1, secp384r1, secp521r1, secp224r1, secp192r1.

For a connection action, there is no default for ServerKexECurves - the setting is determined by the associated environment action.

IP SYSTEM ADMINISTRATOR'S COMMANDS

Netstat TTLS/-x report

Displays Application Transparent Transport Layer Security (AT-TLS) information. AT-TLS supports only TCP protocol connections.

...

COon Report Examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX netstat command displays the data in the same format as the TSO NETSTAT command.

```
MVS TCP/IP NETSTAT CS V2R5       TCPIP Name: TCPCS           19:51:22
 ConnID: 000000B8
   JobName:      FTPD1
   LocalSocket:  ::ffff:127.0.0.1..21
   RemoteSocket: ::ffff:127.0.0.1..1030
   SecLevel:     TLS Version 1.2
   Cipher:       C001 TLS_ECDH_ECDSA_WITH_NULL_SHA
   KeyShare:     N/A
   CertUserID:   N/A
   MapType:      Primary
   FIPS140:      Off
   SessionID:    01000011 7F000001 04000000 00000000
                 00000000 00000000 5B79F9D8 00000001
   SIDReuseReq:  Off
 TTLSRule: ftp_serv_21
   TTLSGrpAction:  grp_act1
   TTLSEnvAction:  env_act_serv

MVS TCP/IP NETSTAT CS V2R5       TCPIP Name: TCPCS           19:51:53
ConnID: 000000B8
  JobName:      FTPD1
  LocalSocket:  ::ffff:127.0.0.1..21
  RemoteSocket: ::ffff:127.0.0.1..1030
  SecLevel:     TLS Version 1.2
  Cipher:       C001 TLS_ECDH_ECDSA_WITH_NULL_SHA
  KeyShare:     N/A
  CertUserID:   N/A
  MapType:      Primary
  FIPS140:      Off
  SessionID:    01000011 7F000001 04000000 00000000
                00000000 00000000 5B79F9D8 00000001
  SIDReuseReq:  Off
TTLSRule: ftp_serv_21
  Priority:       1
  LocalAddr:      All
  LocalPort:      21
  LocalPort:      2021
  LocalPortFrom:  620               LocalPortTo:  621
  RemoteAddr:     All
  RemotePort:     All
  Direction:      Inbound
  TTLSGrpAction:  grp_act1
    GroupID:                  00000006
    GroupUserInstance:        6
    TTLSEnabled:              On
    Envfile:                  /tmp/grp1.env
    CtraceClearText:          On
    Trace:                    255
    SyslogFacility:           Daemon
```

```
    SecondaryMap:               Off
    FIPS140:                    Off
  TTLSEnvAction:  env_act_serv
    EnvironmentUserInstance:    8
    HandshakeRole:              Server
    SuiteBProfile:              Off
    MiddleBoxCompatMode:        On
    Keyring:                    /u/user3/testdb
    KeyringPW:                  Yes
    V3CipherSuites:             C001 TLS_ECDH_ECDSA_WITH_NULL_SHA
                                C002 TLS_ECDH_ECDSA_WITH_RC4_128_S
                                     HA
                                C003 TLS_ECDH_ECDSA_WITH_3DES_EDE_
                                     CBC_SHA
                                C004 TLS_ECDH_ECDSA_WITH_AES_128_C
                                     BC_SHA
    CtraceClearText:            On
    Trace:                      255
    SSLV2:                      Off
    SSLV3:                      On
    TLSV1:                      On
    TLSV1.1:                    On
    TLSV1.2:                    On
    TLSV1.3:                    On
    ResetCipherTimer:           0
    ApplicationControlled:      On
    HandshakeTimeout:           10
    CertificateLabel:           ecdh_ecdsa_secp384r1
    SecondaryMap:               On
    TruncatedHMAC:              Off
    ClientMaxSSLFragment:       Off
    ServerMaxSSLFragment:       Off
```

```
ClientHandshakeSNI:          Off
ServerHandshakeSNI:          Off
ClientExtendedMasterSecret: On
ServerExtendedMasterSecret: On
ClientECurves:               0024 secp384r1
                             0025 secp521r1
ClientKeyShareGroups:        0025 secp521r1
ServerKeyShareGroups:        0025 secp521r1
ServerKexECurves:             0023 secp256r1
                             0024 secp384r1
                             0025 secp521r1
                             0021 secp224r1
                             0019 secp192r1
SignaturePairs:              0401 TLS_SIGALG_SHA256_WITH_RSA
                             0403 TLS_SIGALG_SHA256_WITH_ECDSA
                             0804 TLS_SIGALG_SHA256_WITH_RSASSA_PSS
SignaturePairsCert:          0401 TLS_SIGALG_SHA256_WITH_RSA
ClientAuthType:              Required
CertValidationMode:          Any
Renegotiation:               Default
RenegotiationIndicator:      Optional
RenegotiationCertCheck:      Off
3DesKeyCheck:                Off
ClientEDHGroupSize:          Legacy
ServerEDHGroupSize:          Legacy
PeerMinCertVersion:          Any
PeerMinDHKeySize:            1024
PeerMinDsaKeySize:           1024
PeerMinECCKeySize:           192
PeerMinRsaKeySize:           1024
ServerScsv:                  Off
GSK_V3_SESSION_TIMEOUT:      86400
GSK_V3_SIDCACHE_SIZE:        512
GSK_SYSPLEX_SIDCACHE:        Off
GSK_SESSION_TICKET_CLIENT_ENABLE:       On
GSK_SESSION_TICKET_CLIENT_MAXSIZE:      8192
GSK_SESSION_TICKET_SERVER_ENABLE:       On
GSK_SESSION_TICKET_SERVER_ALGORITHM:    AESCBC128
GSK_SESSION_TICKET_SERVER_COUNT:        2
GSK_SESSION_TICKET_SERVER_TIMEOUT:      300
GSK_SESSION_TICKET_SERVER_KEY_REFRESH: 300
GSK_CRL_CACHE_TIMEOUT:       0
HttpCdpEnable:               Off
HttpCdpProxyServerPort:      80
HttpCdpResponseTimeout:      15
HttpCdpMaxResponseSize:      204800
HttpCdpCacheSize:            32
HttpCdpCacheEntryMaxsize:    0
OcspAiaEnable:               Off
OcspProxyServerPort:         80
OcspRetrieveViaGet:          Off
OcspUrlPriority:             On
OcspRequestSigalg:           0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize:         256
OcspCliCacheEntryMaxsize:    0
OcspNonceGenEnable:          Off
OcspNonceCheckEnable:        Off
OcspNonceSize:               8
OcspResponseTimeout:         15
OcspMaxResponseSize:         20480
OcspServerStapling:          Off
```

Report field descriptions

The report fields are listed in alphabetical order. For more information about each field, see *AT-TLS policy statements* in *z/OS Communications Server: IP Configuration Reference*.

...

ServerKexECurves

The list of elliptic curves that are supported by the server during a TLS V1.0, TLS V1.1, or TLS V1.2 handshake. This list is used by the server to limit which elliptic curves can be used for the handshake key exchange when an ECDHE cipher is utilized.

Both the four-character value of the elliptic curve and the constant of the elliptic curve name are shown for each member of the list.

...

The z/OS UNIX pasearch command: Display policies

Parameters

...

-c

Display policy object information (for example, FLUSH or NOFLUSH, PURGE or NOPURGE). This option can be used with the image option (-p), or the policy type options (-i, -q, -R, -t, -v or -z). All other options are either ignored or are not valid.

See the following descriptions of policy object fields:

ConfigLocation

Indicates the source from which the policies were loaded. The following might be displayed on the policy server:

Local

Indicates that the policies were loaded from local configuration files, an LDAP server, or both.

Client

Indicates that the policies were loaded for a connected policy client.

The following might be displayed on the policy client:

Local

Indicates that the policies were loaded from local configuration files, an LDAP server, or both.

Remote

Indicates that the policies were loaded from the policy server.

LDAPServer

Indicates whether or not an LDAP server is used for local policies.

CommonFileName

Indicates the name of the common configuration file, if one exists.

ImageFileName

Indicates the name of the stack-specific configuration file.

ClientName

Indicates the policy client name.

ClientUserid

Indicates the user ID being used for a policy client.

PolicyServerAddr

Indicates the IP address of the policy server being used for remote policies.

PolicyServerPort

Indicates the port of the policy server being used for remote policies.

PolicyServSysname

Indicates the system name of the policy server being used for remote policies.

PolicyClientAddr

Indicates the IP address of a connected policy client.

PolicyClientPort

Indicates the port of a connected policy client.

ConnectTime

Indicates the time when a policy client connected to the policy server.

ApplyFlush

Indicates whether the policy type uses the PolicyFlush flag for FLUSH or NOFLUSH processing.

DeleteOnNoflush

Indicates whether or not NOFLUSH processing is honored.

ApplyPurge

Indicates whether the policy type uses the PurgePolicies flag for PURGE or NOPURGE processing.

AtomicParse

Indicates whether or not parsing of the policy type is atomic. With atomic parsing, any errors result in the entire set of policy changes for that policy type being discarded. Without atomic parsing, only objects found to be in error are discarded.

DummyOnEmptyPolicy

Indicates whether the TCP/IP stack is informed if no policies are configured for this type of policy.

ModifyOnIDChange

Indicates whether or not a rule or action object is considered changed if only the rule or action ID changes due to the order of policies.

PolicyFlush

For policy types that honor FLUSH, indicates whether FLUSH or NOFLUSH was configured on the TcpImage, PEPInstance, or specific type configuration statement (for example TTLSConfig).

PurgePolicies

For policy types that honor PURGE, indicates whether PURGE or NOPURGE was configured on the TcpImage, PEPInstance, or specific type configuration statement (for example TTLSConfig).

Configured

Indicates whether any policies were configured for this policy type.

UpdateInterval

Indicates the time interval (in seconds) for checking the creation or modification time of the configuration file or files, and for refreshing policies from the LDAP server.

PerfColEnabled

Indicates whether the PolicyPerformanceCollection statement was enabled.

InstanceId

An identification associated with the last update for this policy type.

LastPolicyChanged

The time stamp value that indicates when any policy rule, policy action, or table for this policy type was last updated.

Policy updated

The time stamp value that indicates when the IPSec policy object was last updated.

PAPI Qos Sub-version, PAPI Ids Sub-version, PAPI IPSec Sub-version, PAPI Routing Sub-version, PAPI TTLS Sub-version, PAPI ZERT Sub-version.

The negotiated PAPI sub-version level for each type of policy. These fields are only displayed when the PAPI version in the report header is 16 or greater.

...

Examples:

The following example shows policy object information for all types of policies:

```
================================================================================
================== pasearch -c =================================================
================================================================================

TCP/IP pasearch CS V2R5                  Image Name: TCPCS
  Date:                 08/03/2022        Time:  13:41:40
  PAPI Version:         16                 DLL Version:  16
Qos Policy Object:
  ConfigLocation:       Local             LDAPServer:        True
  ImageFileName:        /u/user10/pagallcimagea.conf
  ApplyFlush:           True              PolicyFlush:       True
  ApplyPurge:           True              PurgePolicies:     True
  AtomicParse:          False             DeleteOnNoflush:   False
  DummyOnEmptyPolicy:   False             ModifyOnIDChange:  True
  Configured:           True              UpdateInterval:    120
  PerfColEnabled:       False
  InstanceId:           1253294875
  LastPolicyChanged:    Fri Sep 18 13:27:55 2011
  PAPI Qos Sub-version:  0000000000000000

Ids Policy Object:
  ConfigLocation:       Local             LDAPServer:        True
  CommonFileName:
  ImageFileName:        /usr/lpp/tcpip/samples/pagent_IDS.conf
  ApplyFlush:           True              PolicyFlush:       True
  ApplyPurge:           True              PurgePolicies:     True
  AtomicParse:          False             DeleteOnNoflush:   False
  DummyOnEmptyPolicy:   False             ModifyOnIDChange:  False
  Configured:           True              UpdateInterval:    120
  InstanceId:           1253294875
  LastPolicyChanged:    Fri Sep 18 13:27:55 2011
  PAPI Ids Sub-version:  0000000000000000
```

```
IPSec Policy Object:
  ConfigLocation:       Remote            LDAPServer:        False
  ClientName:           VIC136_TCPCS1
  ClientUserid:         USER1
  PolicyServerAddr      9.42.104.23
  PolicyServerPort:     8211              PolicyServSysname: VIC137
  ClientSSLActive:      True
  ConnectTime:          Fri Sep 18 13:29:51 2011
  ApplyFlush:           False
  ApplyPurge:           False
  AtomicParse:          True              DeleteOnNoflush:   True
  DummyOnEmptyPolicy:   True              ModifyOnIDChange:  False
  IpSecEnabled IPv4:    True              IpSecEnabled IPv6: False
  IpSec3DESEnabled:     True              IpSecAESEnabled:   True
  IpSecAESGCM16Enabled: True
  UpdateInterval:       300
  InstanceId:           1253294993
  LastPolicyChanged:    Fri Sep 18 13:29:53 2011
  PAPI IPSec Sub-version: 0000000000000000
  IpFilter Policy Object:
   Configured:          True              PreDecapOn:        Off
   FilterLogging:       On                FilterLogImplicit: No
   AllowOnDemand:       No                ImplDiscardAction: Silent
   FIPS140:             No
  KeyExchange Policy Object:
   Configured:          True
   AllowNat:            No                NatKeepAliveIntvl: 20
   HowToInitiate:       Main              LivenessInterval:  30
   BypassIpValidation:  No                CertURLLookupPref: Tolerate
   RevocationChecking:  Loose
  LocalDynVpn Policy Object:
   Configured:          True
  Policy updated:       Fri Sep 18 13:29:53 2011

Routing Policy Object:
  ConfigLocation:       Local             LDAPServer:        False
  CommonFileName:
  ImageFileName:        /usr/lpp/tcpip/samples/pagent_Routing.conf
  ApplyFlush:           True              PolicyFlush:       True
  ApplyPurge:           True              PurgePolicies:     False
  AtomicParse:          True              DeleteOnNoflush:   False
  DummyOnEmptyPolicy:   True              ModifyOnIDChange:  False
  Configured:           True              UpdateInterval:    120
  InstanceId:           1253294871
  LastPolicyChanged:    Fri Sep 18 13:27:51 2011
  PAPI Routing Sub-version: 0000000000000000
```

```
TTLS Policy Object:
  ConfigLocation:       Remote            LDAPServer:        False
  ClientName:           VIC136_TCPCS1
  ClientUserid:         USER1
  PolicyServerAddr      9.42.104.23
  PolicyServerPort:     8211              PolicyServSysname: VIC137
  ClientSSLActive:      True
  ConnectTime:          Fri Sep 18 13:29:51 2011
  ApplyFlush:           True              PolicyFlush:       True
  ApplyPurge:           True              PurgePolicies:     True
  AtomicParse:          True              DeleteOnNoflush:   False
  DummyOnEmptyPolicy:   True              ModifyOnIDChange:  False
  Configured:           True              UpdateInterval:    300
  TTLS Enabled:         False
  InstanceId:           1253294993
  LastPolicyChanged:    Fri Sep 18 13:29:53 2011
  PAPI TTLS Sub-version: 0000000000000001

ZERT Policy Object:
  ConfigLocation:       Local             LDAPServer:        False
  ImageFileName:        /u/user1/pagent/policy_demo.zpe
  ApplyFlush:           True              PolicyFlush:       True
  ApplyPurge:           True              PurgePolicies:     False
  AtomicParse:          True              DeleteOnNoflush:   False
  DummyOnEmptyPolicy:   True              ModifyOnIDChange:  False
  Configured:           True              UpdateInterval:    99999
  ZERT Enabled:         True
  InstanceId:           1609939310
  LastPolicyChanged:    Wed Jan  6 08:21:50 2021
  PAPI ZERT Sub-version: 0000000000000000
```

The following example shows active AT-TLS policies:

```
================================================================================
================== pasearch -t  ================================================
================================================================================

policyRule:             Secure_Telnet_23_Debug
  Rule Type:            TTLS
  Version:              3                 Status:            Active
  Weight:               20                ForLoadDist:       False
  Priority:             20                Sequence Actions:  Don't Care
  No. Policy Action:    3
  policyAction:         grp_Production
   ActionType:          TTLS Group
   Action Sequence:     0
  policyAction:         Secure_Telnet_Env
   ActionType:          TTLS Environment
   Action Sequence:     0
  policyAction:         Secure_Telnet_Conn_Debug
   ActionType:          TTLS Connection
   Action Sequence:     0
  Time Periods:
   Day of Month Mask:
   First to Last:       11111111111111111111111111111111
   Last to First:       11111111111111111111111111111111
   Month of Yr Mask:    111111111111
```

```
  Day of Week Mask:    1111111  (Sunday - Saturday)
  Start Date Time:     None
  End Date Time:       None
  Fr TimeOfDay:        00:00            To TimeOfDay:      24:00
  Fr TimeOfDay UTC:    04:00            To TimeOfDay UTC:  04:00
  TimeZone:            Local
 TTLS Condition Summary:                NegativeIndicator: Off
  Local Address:
   FromAddr:           10.1.2.3
   ToAddr:             10.1.2.3
  Remote Address:
   FromAddr:           10.45.23.10
   ToAddr:             10.45.23.10
  LocalPortFrom:       23               LocalPortTo:       23
  RemotePortFrom:      0                RemotePortTo:      0
  JobName:                              UserId:
  ServiceDirection:    Inbound
 Policy created: Wed Mar  9 06:31:13 2011
 Policy updated: Wed Mar  9 06:31:13 2011

 TTLS Action:                  grp_Production
   Version:                    3
   Status:                     Active
   Scope:                      Group
   TTLSEnabled:                On
   CtraceClearText:            Off
   Trace:                      2
   FIPS140:                    Off
   TTLSGroupAdvancedParms:
    SecondaryMap:              Off
    SyslogFacility:            Daemon
   Policy created: Wed Mar  9 06:31:13 2011
   Policy updated: Wed Mar  9 06:31:13 2011

 TTLS Action:                  Secure_Telnet_Env
   Version:                    3
   Status:                     Active
   Scope:                      Environment
   HandshakeRole:              Server
   SuiteBProfile:              Off
   TTLSKeyringParms:
    Keyring:                   TCPCSsafkeyring
   TTLSEnvironmentAdvancedParms:
    SSLv2:                     Off
    SSLv3:                     On
    TLSv1:                     On
    TLSv1.1:                   On
    TLSv1.2:                   On
    TLSv1.3:                   On
    MiddleBoxCompatMode:       On
    ApplicationControlled:     On
    HandshakeTimeout:          5
    ClientAuthType:            Required
    ResetCipherTimer:          0
    TruncatedHMAC:             Off
    CertValidationMode:        Any
    ServerMaxSSLFragment:      Off
    ClientMaxSSLFragment:      Off
    ServerHandshakeSNI:        Off
    ClientHandshakeSNI:        Off
    ClientExtendedMasterSecret: On
    ServerExtendedMasterSecret: On
    Renegotiation:             Default
    RenegotiationIndicator:    Optional
    RenegotiationCertCheck:    Off
    3DesKeyCheck:              Off
    ClientEDHGroupSize:        Legacy
    ServerEDHGroupSize:        Legacy
    PeerMinCertVersion:        Any
    PeerMinDHKeySize:          1024
    PeerMinDsaKeySize:         1024
    PeerMinECCKeySize:         192
    PeerMinRsaKeySize:         1024
    ServerScsv:                Off
   TTLSSignatureParms:
    ClientECurves:
     0019  secp192r1
     0021  secp224r1
     0023  secp256r1
     0024  secp384r1
     0025  secp521r1
    ClientKeyShareGroups:
```

```
      0025  secp521r1
     ServerKeyShareGroups:
      0025  secp521r1
     ServerKexECurves:
      0023  secp256r1
      0024  secp384r1
      0025  secp521r1
      0021  secp224r1
      0019  secp192r1
     SignaturePairs:
      0401  TLS_SIGALG_SHA256_WITH_RSA
      0403  TLS_SIGALG_SHA256_WITH_ECDSA
      0501  TLS_SIGALG_SHA384_WITH_RSA
      0503  TLS_SIGALG_SHA384_WITH_ECDSA
      0804  TLS_SIGALG_SHA256_WITH_RSASSA_PSS
     SignaturePairsCert:
      0401  TLS_SIGALG_SHA256_WITH_RSA
    TTLSGskAdvancedParms:
     GSK_SYSPLEX_SIDCACHE:      Off
     GSK_V3_SESSION_TIMEOUT:    86400
     GSK_V3_SIDCACHE_SIZE:      512
     GSK_SESSION_TICKET_CLIENT_ENABLE:      On
     GSK_SESSION_TICKET_CLIENT_MAXSIZE:     8192
     GSK_SESSION_TICKET_SERVER_ENABLE:      On
     GSK_SESSION_TICKET_SERVER_ALGORITHM:   AESCBC128
     GSK_SESSION_TICKET_SERVER_COUNT:       2
     GSK_SESSION_TICKET_SERVER_KEY_REFRESH: 300
     GSK_SESSION_TICKET_SERVER_TIMEOUT:     300
     TTLSGskHttpCdpParms:
      HttpCdpEnable:            Off
      HttpCdpProxyServerPort:   80
      HttpCdpResponseTimeout:   15
      HttpCdpMaxResponseSize:   204800
      HttpCdpCacheSize:         32
      HttpCdpCacheEntryMaxsize: 0
     TTLSGskOcspParms:
      OcspAiaEnable:            Off
      OcspProxyServerPort:      80
      OcspRetrieveViaGet:       Off
      OcspUrlPriority:          On
      OcspRequestSigalg:
       0401  TLS_SIGALG_SHA256_WITH_RSA
      OcspClientCacheSize:      256
      OcspCliCacheEntryMaxsize: 0
      OcspNonceGenEnable:       Off
      OcspNonceCheckEnable:     Off
      OcspNonceSize:            8
      OcspResponseTimeout:      15
      OcspMaxResponseSize:      20480
      OcspServerStapling:       Off
    EnvironmentUserInstance:    0
    Policy created: Wed Mar  9 06:31:13 2011
    Policy updated: Wed Mar  9 06:31:13 2011

  TTLS Action:                  Secure_Telnet_Conn_Debug
    Version:                    3
    Status:                     Active
    Scope:                      Connection
    CtraceClearText:            On
    Trace:                      254
    Policy created: Wed Mar  9 06:31:13 2011
    Policy updated: Wed Mar  9 06:31:13 2011
```

TRADEMARKS