tls events

ONTAP EMS reference

NetApp
November 18, 2025

Table of Contents

tls events

tls.insecure events

tls.insecure.cipher

Severity

ERROR

Description

This message occurs when during the TLS handshake a peer negotiates a cipher suite that is no longer considered sufficiently secure to be enabled in the default configuration. TLS connections with this peer should be be presumed insecure, and could be disrupted.

Corrective Action

The issue primarily needs to be resolved on the peer side. Typically, the problem is that the SSL/TLS libraries on the peer are outdated and don’t support more modern cipher suites. Once all peers identified by this event have been resolved and the event is no longer being observed, it is advised to disable the cipher suite in question on this system via the "security config modify" command.

Syslog Message

A TLS peer with IP %s has been connected with using the insecure cipher suite %s.

Parameters

ip (STRING): IP address of the offending peer.
cipher_suite (STRING): Cipher suite used by the offending peer.

tls.insecure.protocol

Severity

ERROR

Description

This message occurs when during the TLS handshake a peer negotiates a protocol level that is no longer considered sufficiently secure to be enabled in the default configuration. TLS connections with this peer should be be presumed insecure, and could be disrupted.

Corrective Action

The issue primarily needs to be resolved on the peer side. Typically, the problem is that the SSL/TLS libraries on the peer are outdated and don’t support more modern protocol levels. Once all peers identified by this event have been resolved and the event is no longer being observed, it is advised to disable the protocol level in question on this system via the "security config modify" command.

Syslog Message

A TLS peer with IP %s has been connected with using the insecure protocol level %s.

Parameters

ip (STRING): IP address of the offending peer.
protocol_level (STRING): Protocol level used by the offending peer.

tls.unused events

tls.unused.cipher

Severity

INFORMATIONAL

Description

This message occurs when a cipher suite that is enabled in the configuration has not been used in any TLS handshakes for a user-specified duration of time.

Corrective Action

Confirm that all known TLS peers have connected to the system within the specified duration of time. If this is not the case, consider increasing the used-age-threshold parameter of the "security config modify" command. Otherwise, consider disabling the unused cipher suite using the supported-cipher-suites parameter of the same command, as this will increase the security of the system with respect to TLS.

Syslog Message

The TLS cipher suite %s has not been used for at least %s.

Parameters

cipher_suite (STRING): Cipher suite that is unused.
duration (STRING): Length of time (D/H/M/S) that the cipher suite has been unused.

tls.unused.protocol

Severity

INFORMATIONAL

Description

This message occurs when a protocol level that is enabled in the configuration has not been used in any TLS handshakes for a user-specified duration of time.

Corrective Action

Confirm that all known TLS peers have connected to the system within the specified duration of time. If this is not the case, consider increasing the used-age-threshold parameter of the "security config modify" command. Otherwise, consider disabling the unused protocol level using the supported-protocols parameter of the same command, as this will increase the security of the system with respect to TLS. For example, if only TLSv1.2 is in use, disabling TLSv1.1 (and lower) is advised.

Syslog Message

The TLS protocol level %s has not been used for at least %s.

Parameters

protocol_level (STRING): Protocol level that is unused.
duration (STRING): Length of time (D/H/M/S) that the protocol level has been unused.

Copyright information

Trademark information