KIP-553: Disable all SSL protocols except TLSV1.2 by default.

Status

Current state: *Accepted*

Discussion thread: Dev-list discussion

JIRA: KAFKA-9460

Motivation

In KAFKA-7251 support of TLS1.3 was introduced.

For now, only TLS1.2 and TLS1.3 are recommended for the usage, other versions of TLS considered as obsolete:

- https://www.rfc-editor.org/info/rfc8446
- https://en.wikipedia.org/wiki/Transport_Layer_Security#History_and_development

But testing of TLS1.3 incomplete, for now.

We should enable actual versions of the TLS protocol by default to provide to the users only secure implementations.

Users can enable obsolete versions of the TLS with the configuration if they want to.

Public Interfaces

There are no changes in public interfaces.

Proposed Changes

Change the value of the `SslConfigs.DEFAULT_SSL_ENABLED_PROTOCOLS to "TLSv1.2"`

Compatibility, Deprecation, and Migration Plan

Compatibility: There are no compatibility issues.

Migration: Users who are using TLSv1.1 and TLSv1 should enable these versions of the protocol with the explicit configuration property `"ssl.enabled.protocols"`

Deprecation: TLSv1.1, TLLv1 will become deprecated.

Rejected Alternatives

There is no rejected alternatives.