KIP-277 - Fine Grained ACL for CreateTopics API

co-authored-by: Mickael Maison <mickael.maison@gmail.com>

Status

Current state: *APPROVED - voting thread*

Discussion thread: *mail-archives.apache.org/...*

JIRA: *KAFKA-6726*

Please keep the discussion on the mailing list rather than commenting on the wiki (wiki discussions get unwieldy fast).

Motivation

The current ACL required for a CreateTopicsRequest is only on the singleton Cluster Resource, does not permit granular permissions (e.g. allow a user only to create a defined set of topics) and it is not symmetric with the permissions required for a DeleteTopicsRequest, which check Delete permission on the named Topic Resources.

This makes it currently impossible to allow a user to manage the lifecycle of a defined set of topics, as she/he will be able to create any topics, but not necessarily to delete all of them.

Proposed Changes

Change the current ACL check for creating a topic T, from CREATE on Cluster, to CREATE on Cluster **OR** CREATE on Topic(T).

Note that the check is performed on two execution paths : explicit creation and auto creation of a topic.

Change the AclCommand CLI tool so that the `–producer` convenience option uses the new finer grained ACL on a given topic.

Public Interfaces

On failure from an authorization check, CreateTopicsRequest will return with an error code of TOPIC_AUTHORIZATION_FAILED(29) instead of CLUSTER_AUTHORIZATION_FAILED (31)

The script kafka-acls.sh will also accept --operation Create in combination with --topic T

Compatibility, Deprecation, and Migration Plan

- What impact (if any) will there be on existing users?
  - existing ACLs with CREATE permission on Cluster will still allow users to create any topics
  - clients expecting an error in CreateTopicResponse will receive TOPIC_AUTHORIZATION_FAILED(29) instead of CLUSTER_AUTHORIZATION_FAILED (31).
    in the Java client, both are mapped to subclasses of AuthorizationException;
    handling any auth error likely requires human intervention.
- If we need special migration tools, describe them here.
  - not needed

Rejected Alternatives

- Rejected the proposal of only checking for CREATE on Topic(T), (i.e. not checking anymore for CREATE on CLUSTER) because of backward compatibility.
- Rejected the idea of having, for symmetry, a DELETE check on Cluster meaning allowed to delete any topics. The resource value ANY should be used instead for the topic.