

KIP-702: The control plane needs to force the validation of requests from the controller

- [Status](#)
- [Motivation](#)
- [Public Interfaces](#)
- [Proposed Changes](#)
- [Compatibility, Deprecation, and Migration Plan](#)
- [Rejected Alternatives](#)

Status

Current state: *"Under Discussion"*

Discussion thread: <https://lists.apache.org/thread.html/r0de1dfb885c3e47039f57edc4cf9e192f6b4f3e1ff947a651b1605de%40%3Cdev.kafka.apache.org%3E>

JIRA: [KAFKA-10891](#)

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

Motivation

This KIP is an extension of [KIP-291](#).

At present, data requests and control requests use different endpoints, these endpoints are all registered to ZooKeeper.

The client can define the "bootstrap-servers" as the control plane, this causes the control plane to regress to the data plane. This would violate the design work of KIP-291.

Whether it is used unintentionally or intentionally, this is the problem faced by the current control plane.

When the user administrator wants to deny the data request access control plane completely, this cannot be done now.

So we need to provide a way for the control plane to reject data requests.

Also, when the control plane is enabled, the broker needs to communicate with the controller using the control plane to send the controlled shutdown request.

Public Interfaces

Add an optional configuration on the broker side:

- `control.plane.force.controller.requests.enable` : If this configuration is true, the control plane will reject data requests completely, default is false.

Proposed Changes

Add `isControlPlane` to the constructor of the processor, this value is passed in when the processor associated with the data plane and the control plane is created. "`control.plane.force.controller.requests.enable`" is disabled by default. The default control plane does not reject data requests, which can remain compatible when the user uses the control plane for data requests.

If `control.plane.force.controller.requests.enable` is true, the control plane should allow only four kinds of requests: `LeaderAndIsrRequest`, `UpdateMetadataRequest`, `StopReplicaRequest`, `ControlledShutdownRequest`.

Processor

```
class Processor(val id: Int,
                time: Time,
                maxRequestSize: Int,
                requestChannel: RequestChannel,
                connectionQuotas: ConnectionQuotas,
                connectionsMaxIdleMs: Long,
                failedAuthenticationDelayMs: Int,
                listenerName: ListenerName,
                securityProtocol: SecurityProtocol,
                config: KafkaConfig,
                metrics: Metrics,
                credentialProvider: CredentialProvider,
                memoryPool: MemoryPool,
                logContext: LogContext,
                connectionQueueSize: Int = ConnectionQueueSize,
                isPrivilegedListener: Boolean = false,
                allowDisabledApis: Boolean = false,
                isControlPlane: Boolean = false)
```

Compatibility, Deprecation, and Migration Plan

This KIP is consistent with KIP-291.

- Impacts: Controller-related requests will be made entirely through the control plane, and completely separate control requests from data requests.
- Migration plan: 2 rounds of rolling upgrades are needed to pick up the proposed changes in this KIP. The goal of the first round is to add the controller endpoint, without adding the `"control.plane.listener.name"` config. Specifically, an endpoint with the controller listener name should be added to the "listeners" config, e.g. `"CONTROLLER://192.1.1.8:9091"`; if the `"advertised.listeners"` config is explicitly configured and is not getting its value from "listeners", the new endpoint for controller should also be added to "advertised.listeners". After the first round is completed, controller to brokers communication should still behave in the same way that uses the **inter-broker-listener-name**, since the `"control.plane.listener.name"` is not set yet. In the 2nd round, the `"control.plane.listener.name"` config should be set to the corresponding listener name, e.g. `"CONTROLLER"` and set `"control.plane.force.controller.requests.enable=true"` if the control plane is required to force the validation of the control request. During rolling upgrade of the 2nd round, controller to brokers traffic will start using the `"control.plane.listener.name"`, and go through the proposed changes in this KIP.
- No special migration tools are needed.

Rejected Alternatives