Connecting

- NATS URL
  - Connecting to clusters
- Authentication details
  - Runtime configuration
- Connection Options
- See Also

In order for a NATS client application to connect to the NATS service, and then subscribe or publish messages to subjects, it needs to be able to be configured with the details of how to connect to the NATS service infrastructure and of how to authenticate with it.

NATS URL

1. A 'NATS URL' is a string (in a URL format) that specifies the IP address and port where the NATS server(s) can be reached, and what kind of connection to establish:
   - TLS encrypted *only* TCP connection (i.e. NATS URLs starting with `tls://...`)
   - TLS encrypted if the server is configured for it or plain un-encrypted TCP connection otherwise (i.e. NATS URLs starting with `nats://...`)
   - Websocket connection (i.e. NATS URLs starting with `ws://...`)

Connecting to clusters

Note that when connecting to a NATS service infrastructure with clusters there is more than one URL and the application should allow for more than one URL to be specified in its NATS connect call (typically you pass a comma separated list of URLs as the URL, e.g. `"nats://server1:port1,nats://server2:port2"`).

When connecting to a cluster it is best to provide the complete set of 'seed' URLs for the cluster.

Authentication details

1. If required: authentication details for the application to identify itself with the NATS server(s). NATS supports multiple authentication schemes:
   - Username/Password credentials (which can be passed as part of the NATS URL)
   - Decentralized JWT Authentication/Authorization (where the application is configured with the location of 'credentials file' containing the JWT and private Nkey)
   - Token Authentication (where the application is configured with a Token string)
   - TLS Certificate (where the client is configured to use a client TLS certificate and the servers are configured to map the TLS client certificates to users defined in the server configuration)
   - NKEY with Challenge (where the client is configured with a Seed and User NKeys)

Runtime configuration

Your application should expose a way to be configured at run time with the NATS URL(s) to use. If you want to use a secure infrastructure, the application must provide for the definition of either the credentials file (.creds) to use, or the means to encode the token, or Nkey, in the URL(s).

Connection Options

Besides the connectivity and security details, there are numerous options for a NATS connection ranging from timeouts to reconnect settings to setting asynchronous error and connection event callback handlers in your application.

See Also

WebSocket and NATS

https://www.youtube.com/watch?v=AbAR9zgJnjY WebSocket and NATS | Hello World

NATS WebSockets and React

https://www.youtube.com/watch?v=XS_Q0i6orSk NATS WebSockets and React

---

□□□ #3
□ cocobook-sync □□□ 2026-10-28 11:11:01 UTC
□ cocobook-sync □□□ 2026-10-29 01:42:35 UTC