Configure cipher suites

Ciphers are algorithms that help secure connections between clients and servers. You can change the ciphers to improve the security of your Redis Enterprise cluster and databases. The default settings are in line with industry best practices, but you can customize them to match the security policy of your organization.

Default cipher:

```plaintext
HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH
```

Configure cipher suites

The communications for which you can modify ciphers are:

- **Control plane** - The TLS configuration for cluster administration.
- **Data plane** - The TLS configuration for the communication between applications and databases.
- **Discovery service (Sentinel)** - The TLS configuration for the discovery service.

You can configure ciphers with the `rladmin` commands shown here or with the REST API.

When you modify your cipher suites, make sure:

- The configured TLS version matches the required cipher suites.
- The certificates in use are properly signed to support the required cipher suites.

**Note:**

- Redis Enterprise Software doesn't support static Diffie–Hellman key exchange ciphers.
- It does support Ephemeral Diffie–Hellman key exchange ciphers on RHEL8 and Bionic OS.

Control plane

6.0.8 or earlier

See the example below to configure cipher suites for the control plane:

```plaintext
```

6.0.12 or later

Control plane cipher suites use the BoringSSL library format for TLS connections to the admin console. See the BoringSSL documentation for a full list of available BoringSSL configurations.

See the example below to configure cipher suites for the control plane:
Data plane

6.0.20 or later

Data plane cipher suites use the OpenSSL library format. See the OpenSSL documentation for a list of available OpenSSL configurations.

See the example below to configure cipher suites for the data plane:

```bash
rladmin cluster config data_cipher_list AES128-SHA:AES256-SHA
```

Discovery service

6.0.20 or later

Sentinel service cipher suites use the golang.org OpenSSL format for discovery service TLS connections. See their documentation for a list of available configurations.

See the example below to configure cipher suites for the sentinel service:

```bash
rladmin cluster config sentinel_cipher_suites
TLS_RSA_WITH_AES_128_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

Updated: April 15, 2022