

NEO4J SECURITY BENCHMARK

Version 2025

10 May 2025

Contents

Version History 5

Introduction 6

Overview 6

Intended Audience 6

Changes in Neo4j 2025 6

Aura 6

Neo4j Security Policy 6

Installation and Patching 7

Ensure the appropriate Neo4j software version/patches are installed 7

Authentication 8

Ensure that authentication is enabled for Neo4j databases 8

Ensure that Minimum Password Length For Native Neo4j User Accounts Is At Least 8 Characters 10

Ensure authentication is enabled in the Neo4j cluster 11

Use Neo4j with an LDAP Authentication Service 12

Use Neo4j with an SSO Provider 14

Use Neo4j with Kerberos (Optional) 15

Configure User Authentication Maximum Failed Attempts 16

Configure User Authentication Lockout Time 17

Securing Configuration Settings 18

Use neo4j-ADMIN start --expand-commands 18

Encryption 20

Require TLS for Bolt Connections 20

Install a signed TLS certificate 21

Rotate TLS Certificates 22

OCSP Stapling 23

Disable HTTP Port 24

Neo4j Browser 25

Ensure Neo4j Browser does not cache login information 25

Implement Neo4j Browser Time-Out 26

Disable Neo4j Browser Outgoing Connections 27
Disable Client Telemetry 28
Configure CORS Headers 29
Set HTTP Strict-Transport-Security (HSTS) Response Header 30
Set CONTENT-SECURITY-POLICY Header 31
Data Encryption 32
Ensure TLS protects all network communications (Backups, Bolt, Browser and Cluster) 32
Encrypt Data Backups 35
Change default backup port 37
Use Volume Encryption 38
Activity Logging 39
Ensure that system activity is audited 39
Query Logging 41
Anonymous Usage Data Reporting 42
Disable Anonymous Usage Data Reporting 42
Operating System Hardening 43
Neo4j Database Running with Least Privileges 43
Ensure that Neo4j uses non-default ports 45
Ensure that operating system resource limits are set for Neo4j 47
Disable Deprecated Neo4j Utilities 48
JMX 48
Data Protections 49
IP Blocklist 49
Input Validation 50
Cypher Injection 50
Docker 51
Encryption 51
Sandbox Extensions 52
Sandboxing 52
Enabling Extensions 53
Role Based Access Control Authorization 54
RBAC 54

System Database 56
SYSTEM DATABASE 56
FIPS 140.2 Support 57
FIPS 140.2 Configuration 57
Changes, Deprecations and Removals 60
Changes 60
Deprecations 60
Removals 60

Version History

Version	Summary	Version Date	Author
2025.04	Include section on dynamic certificate rotation	10 May 2025	David Fauth
2025	Initial release for Neo4j 2025	14 March 2025	David Fauth

Introduction

OVERVIEW

This document, Neo4j Security Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Neo4j Enterprise Edition versions 2025.01 and higher. This guide was tested against Neo4j 2025.01 running on Amazon Linux 2023 AMI and Microsoft Windows Server 2022. This guide applies to other Linux distributions. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@neo4j.com.

(This document should integrate and incorporate present information on the public website available here: https://neo4j.com/docs/operations-manual/current/security/checklist/)

This guide is intended for self-managed Neo4j deployments. The Neo4j Aura Security Guide is available here.

INTENDED AUDIENCE

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Neo4j Enterprise Edition.

CHANGES IN NEO4J 2025

Neo4j 2025 provides the following enhancements regarding security configuration:

- Changed default ports
- Requires Java 21

AURA

Neo4j Aura security details can be found at https://neo4j.com/docs/aura/platform/security/

NEO4J SECURITY POLICY

Neo4j provides security policy documents and pen test results at https://trust.neo4j.com.

Installation and Patching

This section provides guidance on ensuring that the Neo4j software is up to date to eliminate easily avoidable vulnerabilities.

ENSURE THE APPROPRIATE NEO4J SOFTWARE VERSION/PATCHES ARE INSTALLED

DESCRIPTION:

The Neo4j installation version, along with the patch level, should be the most recent that is compatible with the organization's operational needs.

RATIONALE:

Using the most recent Neo4j software version along with all applicable patches helps limit the possibilities for vulnerabilities in the software. The installation version and/or patches applied should be selected according to the needs of the organization. At minimum, the software version should be supported. The latest releases can be found at: https://neo4j.com/deployment-center/. Neo4j 2025.02 is the latest released version as the time of writing this document.

Neo4j supported releases, release date and end of support date for the Neo4j releases are documented in the Neo4j Knowledge Base.

REMEDIATION:

Upgrade to the latest version of the Neo4j software. Refer to the online operations manual for the recommended upgrade in https://neo4j.com/docs/upgrade-migration-guide/current/version-2025/

DEFAULT VALUE:

None

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/installation/
2. https://support.neo4j.com/hc/en-us/articles/115013134648-Neo4j-Supported-Versions
3. https://support.neo4j.com/hc/en-us/articles/203307636-Downloads-for-Commercial-Customers
4. https://neo4j.com/developer/kb/neo4j-supported-versions/
5. https://neo4j.com/docs/upgrade-migration-guide/current/version-2025/

Authentication

This section contains recommendations for requiring authentication before allowing access to the Neo4j database.

ENSURE THAT AUTHENTICATION IS ENABLED FOR NEO4J DATABASES

DESCRIPTION:

This setting ensures that all clients, users, and/or servers are required to authenticate prior to being granted access to the Neo4j database.

RATIONALE:

Failure to authenticate clients, users, and/or servers can enable unauthorized access to the Neo4j database and can prevent tracing actions back to their sources.

REMEDIATION:

The authentication mechanism should be implemented before anyone accesses the Neo4j Server.

To enable the authentication mechanism: In the **neo4j.conf** file, uncomment the **dbms.security.auth_enabled** setting and set it to **true**:

```
# Whether requests to Neo4j are authenticated.
# To disable authentication, uncomment this line
dbms.security.auth_enabled=true
```

Modify the Neo4j user password, ensuring that its password meets organizationally defined password complexity requirements.

IMPORTANT: Use the **set-initial-password** command of **neo4j-admin dbms** to define the password for the native user **neo4j**. This must be performed before starting up the database for the first time.

DEFAULT VALUE:

Authentication is enabled by default. The default username is *neo4j* and the default password is *neo4j.*

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.auth_enabled
2. https://neo4j.com/docs/operations-manual/current/configuration/set-initial-password/

3. https://neo4j.com/docs/operations-manual/5/tools/neo4j-admin/

ENSURE THAT MINIMUM PASSWORD LENGTH FOR NATIVE NEO4J USER ACCOUNTS IS AT LEAST 8 CHARACTERS

DESCRIPTION:

This setting ensures that all Neo4j native user accounts have a minimum password length of 8.

RATIONALE:

Complex passwords make it more difficult to compromise a user account.

REMEDIATION:

To modify the default minimum password length of 8: In the **neo4j.conf** file, add the **dbms.security.auth_minimum_password_length** setting and set it to a number greater than 8:

```
dbms.security.auth_minimum_password_length = 12
```

DEFAULT VALUE:

The default minimum password length is 8.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.auth_enabled
2. https://neo4j.com/docs/operations-manual/current/configuration/set-initial-password/

ENSURE AUTHENTICATION IS ENABLED IN THE NEO4J CLUSTER

DESCRIPTION:

Authentication is enabled in a Neo4j cluster when keyfiles are created and configured for all components. This ensures that every client that accesses the cluster must provide credentials, to include Neo4j instances that access each other within the cluster.

RATIONALE:

Enforcing a key on a sharded cluster prevents unauthorized access to the Neo4j database and provides traceability of database activities to a specific user or component.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
2. https://neo4j.com/docs/operations-manual/current/security/ssl-framework/

USE NEO4J WITH AN LDAP AUTHENTICATION SERVICE

DESCRIPTION:

Configuring Neo4j to use an LDAP Auth provider offloads management of federated users to the LDAP service. The LDAP service facilities are used for administration.

RATIONALE:

Neo4j supports LDAP, which allows for integration with Active Directory (AD), OpenLDAP, or other LDAP-compatible authentication services. This means that you use the LDAP service for managing federated users, while the native Neo4j user and role administration are completely turned off.

An LDAP auth provider provides stronger user management (disable users, password changes, password complexity, etc.) than available with Neo4j native users. It also streamlines the user management across a cluster, as Neo4j does not centralize management of native users.

REMEDIATION:

The authentication mechanism should be implemented before anyone accesses the Neo4j Server.

All settings need to be defined at server startup time in the default configuration file **neo4j.conf**:

```
# Turn on security:
dbms.security.auth_enabled=true

# Choose LDAP connector as security provider for both authentication and
authorization:
dbms.security.authentication_providers=ldap
dbms.security.authorization_providers=ldap
```

See https://neo4j.com/docs/operations-manual/current/authentication-authorization/ldap-integration/ for details on configuring Neo4j to use an LDAP Auth provider.

In environments where you need both LDAP authentication as well as some native user accounts, there is a way to allow this in Neo4j 2025. Use the configuration setting **dbms.security.auth_providers** instead of the singular version **dbms.security.auth_provider**. This will allow you to supply a list of providers to use for authentication.

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/authentication-authorization/ldap-integration
2. https://support.neo4j.com/hc/en-us/articles/360049019173-Neo4j-LDAP-Integration
3. https://support.neo4j.com/hc/en-us/articles/360000586268-Configure-Neo4j-to-authenticate-users-from-different-OUsusing-the-Active-Directory-attribute-samAccountName
4. https://support.neo4j.com/hc/en-us/articles/115013527168-How-do-I-allow-for-authentication-using-Active-Directoryattribute-samAccountName
5. https://support.neo4j.com/hc/en-us/articles/115008871987-How-to-configure-mixed-mode-security-native-and-LDAP-inNeo4j

USE NEO4J WITH AN SSO PROVIDER

DESCRIPTION:

Configuring Neo4j to use a SSO provider allows customers to centrally manage authentication and authorization for their systems in an identity provider which provides single sign-on for their other systems.

RATIONALE:

Neo4j supports OpenID Connect (OIDC), which allows for integration with many identity providers including Okta, Microsoft Azure Active Directory, and Google. This integration permits federated users, managed by the identity provider, to access Neo4j instead of, or in addition to the native users and roles.

REMEDIATION:

See https://neo4j.com/docs/operations-manual/current/tutorial/tutorial-sso-configuration/ for details on configuring Neo4j to use various SSO providers.

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/tutorial/tutorial-sso-configuration/

USE NEO4J WITH KERBEROS (OPTIONAL)

DESCRIPTION:

The official Neo4j Kerberos add-on can be used to extend Neo4j with Kerberos authentication.

RATIONALE:

The official Neo4j Kerberos add-on provides authentication and should be used in conjunction with another provider such as LDAP for authorization.

REMEDIATION:

Consult with Neo4j Support to configure the Kerberos add-on.

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/download/neo4j-addon-kerberos/

CONFIGURE USER AUTHENTICATION MAXIMUM FAILED ATTEMPTS

DESCRIPTION:

When using Neo4j native user management, configure the maximum failed attempts to guard against brute force attacks.

RATIONALE:

Configuring the maximum failed attempts will help minimize the chance of a successful brute force attack (avoid an attacker guessing a password by constantly requesting authentication to the server).

REMEDIATION:

In the **neo4j.conf** file, add the **dbms.security.auth_max_failed_attempts** configuration parameter:

```
dbms.security.auth_max_failed_attempts=3
```

DEFAULT VALUE:

The default value for this parameter is 3.

NOTE:

Neo4j native user management does not have strong password requirements to include password length, complexity or expiration and may not meet stringent password requirements.

The settings are per-user, i.e. the server keeps a list of the number of consecutive failed attempts to login for each user.

The settings are global, i.e. they apply to all the users.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.auth_max_failed_attempts

CONFIGURE USER AUTHENTICATION LOCKOUT TIME

DESCRIPTION:

When using Neo4j native user management, configure the user lockout time after unsuccessful authentication attempts to guard against brute force attacks.

RATIONALE:

Configuring the user lockout time will help minimize the chance of a successful brute force attack (avoid an attacker guessing a password by constantly requesting authentication to the server).

REMEDIATION:

In the **neo4j.conf** file, add the **dbms.security.auth_lock_time** configuration parameter:

```
dbms.security.auth_lock_time=5s
```

DEFAULT VALUE:

The default value for this parameter is 5s. The default unit of measure for this parameter is seconds. Other valid units of measure include: ns, μs, ms, s, m, h, d.

NOTE:

Neo4j native user management does not have strong password requirements to include password length, complexity or expiration and may not meet stringent password requirements.

The settings are per-user, i.e. the server keeps a list of the number of consecutive failed attempts to login for each user.

The settings are global, i.e. they apply to all the users.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.auth_lock_time

Securing Configuration Settings

This section describes the use of neo4j expand-commands utility to minimize the exposure of sensitive username / passwords that would be stored in the neo4j.conf file.

USE NEO4J-ADMIN START --EXPAND-COMMANDS

RATIONALE:

The **--expand-commands** settings allows settings to be retrieved from a common repository and added to multiple instances. This allows DBAs to remove sensitive information stored in plain text in neo4j.conf.

REMEDIATION:

In addition to providing values directly for settings, each setting can optionally execute a custom script to provide the value, using the syntax **dbms.setting=$(script_to_execute).**

For example:

```
dbms.max_databases=$(expr 10 * 10)

dbms.ssl.policy.private_key_password=$(curl -E example.cert
https://example.com/password)
```

The Neo4j startup script and the neo4j service can expand and execute the external commands by using the argument --expand-commands.

For example:

```
bin/neo4j start --expand-commands
```

Neo4j performs the following basic security checks on the neo4j.conf file. If they fail, Neo4j does not evaluate the script commands in neo4j.conf, and the Neo4j process does not start.

On Unix (both Linux and Mac OS)

- The neo4j.conf file must, at least, be readable by its owner or by the user-group to which the owner belongs.
- The Neo4j process must run as a user who is either the owner of the neo4j.conf file or in the user-group which owns the neo4j.conf file.

On Windows

- The neo4j.conf file must, at least, be readable by the user that the Neo4j process runs as.

DEFAULT VALUE:

This feature needs to be explicitly enabled by providing the **--expand-commands** argument to the Neo4j start-up script. The server will fail to start if the config contains scripts, but the correct argument is not provided.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/command-expansion/

Encryption

This section contains recommendations for configuring Neo4j to use encryption ensuring that sensitive data and passwords are not passed over the network in clear text.

REQUIRE TLS FOR BOLT CONNECTIONS

RATIONALE:

The bolt protocol can operate either encrypted or unencrypted. This setting ensures that unencrypted mode may not be used by clients. This in turn ensures that unencrypted data and authorization information never crosses the wire.

REMEDIATION:

In the **neo4j.conf** file, configure the **server.bolt.tls_level** configuration parameter:

```
server.bolt.tls_level=REQUIRED
```

NOTE: Server Name Indication (SNI) is an extension to Transport Layer Security (TLS). SNI allows the client to pass the hostname that the client intends to talk to in the TLS handshake negotiation. SNI is implemented in all the Neo4j native language drivers, allowing applications to verify the hostname in the server certificate that they receive from Neo4j. This verifies that the server is a valid server (with a valid certificate) and ensures that the server is the one that the application intended to talk to (verifying that the hostname in the CN field of the server certificate matches the host in the application's connecting request URL).

DEFAULT VALUE:

The default value for this parameter is DISABLED.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_server.bolt.tls_level
2. https://neo4j.com/docs/operations-manual/current/security/ssl-framework/

INSTALL A SIGNED TLS CERTIFICATE

RATIONALE:

The SSL configuration requires SSL certificates to be issued by a Certificate Authority (CA). All certificates must follow the X.509 standard and be saved in a PEM-encoded file. Trusted certificates establish a chain of trust that verifies other certificates signed by the trusted roots — for example, to establish a secure connection to a web server.

REMEDIATION:

Use SSL certificates issued from a trusted Certificate Authority.

DEFAULT VALUE:

Not configured.

REFERENCES:

1. For configuring your Neo4j installation to use encrypted communication, refer to https://neo4j.com/docs/operations-manual/current/security/ssl-framework/
2. For configuring your Bolt and/or HTTPS connectors, refer to https://neo4j.com/docs/operations-manual/current/configuration/connectors/
3. If using LDAP, configure your LDAP system with encryption via StartTLS; see the section called "Use LDAP with encryption via StartTLS" (https://neo4j.com/docs/operations-manual/current/authentication-authorization/ldap-integration/#auth-ldap-encrypted-starttls).

ROTATE TLS CERTIFICATES

RATIONALE:

It is considered best practice to use certificates with reasonably short duration. This, however, requires the periodic rotation of certificates whereby old certificates are removed and the new ones are installed. Previous versions of Neo4j required a database restart for changes to be applied. Starting from 2025.03, new certificates can be rotated in, and SSL configuration can be updated without requiring a restart. This reduces undesirable effects of transient loss of cluster members.

REMEDIATION:

Enable the dynamic reloading of certificates on all cluster members. It is best to do this when the cluster is deployed as changing this configuration requires a restart.

In the **neo4j.conf** file, configure the **dbms.security.tls_reload_enabled** configuration parameter:

```
dbms.security.tls_reload_enabled =true
```

DEFAULT VALUE:

The default value for this parameter is FALSE.

REFERENCES:

1. Certificates Rotation: https://neo4j.com/docs/operations-manual/current/security/ssl-framework/#certificate-rotation

OCSP STAPLING

RATIONALE:

OCSP Stapling is a mechanism for managing certificate revocation. The protocol server must provide a proof of validity along with the certificate as part of TLS handshake. Most certificates and clients support OCSP, a protocol for querying a certificate's revocation status and confirming that it is still valid.

REMEDIATION:

In the **neo4j.conf** file, configure the **server.bolt.ocsp_stapling_enabled** configuration parameter:

```
server.bolt.ocsp_stapling_enabled=true
```

DEFAULT VALUE:

The default value for this parameter is FALSE.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_server.bolt.ocsp_stapling_enabled
2. https://neo4j.com/docs/api/java-driver/current/org.neo4j.driver/org/neo4j/driver/Config.TrustStrategy.html

DISABLE HTTP PORT

RATIONALE:

Data passed over the http port is unencrypted.

REMEDIATION:

You can disable the HTTP port by setting the **server.http.enabled** parameter to false:

```
# HTTP Connector. There can be zero or one HTTP connectors.
server.http.enabled=false
```

DEFAULT VALUE:

Default value for this parameter is **true**.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_server.http.enabled

Neo4j Browser

This section contains recommendations for enhancing the Neo4j browser security and other http security measures.

ENSURE NEO4J BROWSER DOES NOT CACHE LOGIN INFORMATION

DESCRIPTION:

The Neo4j browser requires a username / password for login. This setting ensures that all clients using the Neo4j browser are required to login each time and that the login credentials are not maintained.

RATIONALE:

Enforcing a login each time prevents unauthorized access to the Neo4j database and provides traceability of database activities to a specific user or component.

REMEDIATION:

Disabling the Neo4j browser from retaining connection credentials should be implemented before anyone accesses the Neo4j Server.

To disable the browser from retaining connection credentials:

Configure the **browser.retain_connection_credentials** configuration parameter in the **neo4j.conf** file:

```
browser.retain_connection_credentials=false
```

DEFAULT VALUE:

Default value for this parameter is **true**.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_browser.retain_connection_credentials

IMPLEMENT NEO4J BROWSER TIME-OUT

DESCRIPTION:

The Neo4j browser requires a username / password for login. This setting ensures that a client using the Neo4j browser will be logged out after a period of inactivity.

RATIONALE:

Enforcing a time-out after a period of inactivity prevents unauthorized access to the Neo4j database.

REMEDIATION:

The browser time-out setting should be implemented before anyone accesses the Neo4j Server.

To enable the browser time-out:

In the **neo4j.conf** file, add the **browser.credential_timeout** configuration parameter and configure it to the appropriate setting:

```
browser.credential_timeout=5m
```

DEFAULT VALUE:

Default value for this parameter is **0s.** Setting this to 0 indicates no time limit.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_browser.credential_timeout

DISABLE NEO4J BROWSER OUTGOING CONNECTIONS

DESCRIPTION:

The Neo4j browser can access websites and other resources outside of the Neo4j web server. This setting ensures that the Neo4j browser only connects to the Neo4j server. By disabling this capability, the Neo4j browser will not be able to submit crash reports, analytics, access the Neo4j changelog and load the default guides from guides.neo4j.com.

RATIONALE:

Disabling outgoing connections minimizes the potential for Neo4j to access untrusted or unsecure resources.

REMEDIATION:

The Disable Neo4j Browser Outgoing Connections setting should be implemented before anyone accesses the Neo4j Server.

In the **neo4j.conf** file, add the **browser.allow_outgoing_connections** configuration parameter and configure it to the appropriate setting:

```
browser.allow_outgoing_connections=false
```

DEFAULT VALUE:

Default value for this parameter is **true**.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_browser.allow_outgoing_connections

DISABLE CLIENT TELEMETRY

DESCRIPTION:

By default, the Neo4j Browser and Bloom client can send Product Analytics data to Neo4j. This setting will disable the Neo4j browser for sending product analytics data to Neo4j.

RATIONALE:

Disabling outgoing connections minimizes the potential for third parties from intercepting sensitive Neo4j data.

REMEDIATION:

The Client Allow Telemetry setting should be implemented before anyone accesses the Neo4j Server.

In the **neo4j.conf** file, add the **client.allow_telemetry** configuration parameter and configure it to the appropriate setting:

```
client.allow_telemetry=false
```

DEFAULT VALUE:

Default value for this parameter is **true**.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_client.allow_telemetry

CONFIGURE CORS HEADERS

DESCRIPTION:

The Access-Control-Allow-Origin response header indicates whether the response can be shared with resources with the given origin. For requests without credentials, the server may specify "*" as a wildcard, thereby allowing any origin to access the resource.

It may be necessary to specify the CORS response header to limit access to a specific URI.

RATIONALE:

Enabling a specific CORS response header limits the ability to access the website. Instead of using a wildcard (*) or arbitrary origin for the CORS policy, access should be provided only to specific, necessary and trusted domains. White listing is an often recommended approach where a list of trusted domains can be maintained to grant access. The list of allowed external domains should be carefully selected and revalidated on a regular schedule to prevent unauthorized data access via third-party security breaches.

REMEDIATION:

To specify a specific CORS response header:

In the **neo4j.conf** file, add the **dbms.security.http_access_control_allow_origin** parameter and configure it to the appropriate setting. The expected value is a string:

```
dbms.security.http_access_control_allow_origin=http://neo4j.com
```

DEFAULT VALUE:

dbms.security.http_access_control_allow_origin=*

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.http_access_control_allow_origin

SET HTTP STRICT-TRANSPORT-SECURITY (HSTS) RESPONSE HEADER

DESCRIPTION:

The HTTP Strict-Transport-Security (HSTS) header tells browsers that a webpage should only be accessed using HTTPS instead of HTTP. It is attached to every HTTPS response.

RATIONALE:

Enabling the HSTS Response Header ensures that the browser is only available via HTTPS.

REMEDIATION:

To enable the HSTS header:

In the **neo4j.conf** file, add the **dbms.security.http_strict_transport_security** parameter and configure it to the appropriate setting.

```
dbms.security.http_strict_transport_security=Strict-Transport-Security: max-age=31536000; includeSubDomains
```

DEFAULT VALUE:

Not set.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.security.http_strict_transport_security
2. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
3. https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

SET CONTENT-SECURITY-POLICY HEADER

DESCRIPTION:

Content Security Policy (CSP) is a security feature that is used to specify the origin of content that is allowed to be loaded on a website or in a web applications. It is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

RATIONALE:

Setting a Security Policy Header adds an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks.

REMEDIATION:

To configure the Security Policy Header being returned from the Neo4j server:

In the **neo4j.conf** file, add the **dbms.security.http_static_content_security_policy_header** parameter and configure it to the appropriate setting.

```
dbms.security.http_static_content_security_policy_header= default-src 'self';
script-src 'self' cdn.segment.com canny.io; img-src 'self' data:; style-src
'self' fonts.googleapis.com 'unsafe-inline'; font-src 'self'
fonts.gstatic.com; base-uri 'none'; object-src 'none'; frame-ancestors
'none'; connect-src 'self' api.canny.io api.segment.io ws: wss: http: https:
```

DEFAULT VALUE:

The default value is:

```
dbms.security.http_static_content_security_policy_header= default-src 'self';
script-src 'self' cdn.segment.com canny.io; img-src 'self' data:; style-src
'self' fonts.googleapis.com 'unsafe-inline'; font-src 'self'
fonts.gstatic.com; base-uri 'none'; object-src 'none'; frame-ancestors
'none'; connect-src 'self' api.canny.io api.segment.io ws: wss: http: https:
```

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_dbms.security.http_static_content_security_policy_header
2. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy
3. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#content-security-policy-csp
4. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

Data Encryption

ENSURE TLS PROTECTS ALL NETWORK COMMUNICATIONS (BACKUPS, BOLT, BROWSER AND CLUSTER)

DESCRIPTION:

Use TLSv1.2 or higher to protect all incoming and outgoing connections. This should include using TLS to encrypt communication between a Neo4j cluster, Neo4j backups as well as between all applications and Neo4j.

RATIONALE:

This prevents sniffing of cleartext traffic between Neo4j servers or performing a man-in-the-middle attack of Neo4j. For the strongest security, Neo4j recommends only enabling ciphers with the following attributes:

- Encryption: AES-GCM
- MAC Hashing: SHA384
- Key Exchange: ECDHE
- Authentication: RSA 4096 / SHA256
- Key Length: At least 256 bits
- Ensure a trusted SSL certificate is used.

AUDIT:

To verify that system activity is being audited for Neo4j, inspect the **neo4j.conf** file for the following settings:

```
nmap --script ssl-enum-ciphers -p 6000 localhost
nmap --script ssl-enum-ciphers -p 7000 localhost
nmap --script ssl-enum-ciphers -p 7473 localhost
```

REMEDIATION:

Configure Neo4j servers to require the use of SSL or TLS to encrypt all Neo4j network communications.

To implement SSL or TLS to encrypt all Neo4j network communication, review the referenced section of our manual.

1. Read the following 2 sections in the Operations Manual: https://neo4j.com/docs/operations-manual/current/security/ssl-framework/ and then read: https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption
2. Run **nmap --script ssl-enum-ciphers -p (port) localhost** to determine what ciphers are available.

3. Configure intermediate certificates and server certificates per https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
4. Configure **neo4j.conf** as follows:

```
server.bolt.tls_level=REQUIRED

# Backups SSL configuration
dbms.ssl.policy.backup.enabled=true
dbms.ssl.policy.backup.base_directory=certificates/default
dbms.ssl.policy.backup.private_key=neo4jCert.key
dbms.ssl.policy.backup.public_certificate=neo4jCert.crt
dbms.ssl.policy.backup.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.backup.client_auth=NONE
dbms.ssl.policy.backup.trusted_dir=certificates/bolt/trusted
dbms.ssl.policy.backup.tls_versions=TLSv1.3,TLSv1.2

# Bolt SSL configuration
dbms.ssl.policy.bolt.enabled=true
dbms.ssl.policy.bolt.base_directory=certificates/default
dbms.ssl.policy.bolt.private_key=neo4jCert.key
dbms.ssl.policy.bolt.public_certificate=neo4jCert.crt
dbms.ssl.policy.bolt.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.bolt.client_auth=NONE
dbms.ssl.policy.bolt.trusted_dir=certificates/bolt/trusted
dbms.ssl.policy.bolt.tls_versions=TLSv1.3,TLSv1.2

# Https SSL configuration
dbms.ssl.policy.https.enabled=true
dbms.ssl.policy.https.base_directory=certificates/default
dbms.ssl.policy.https.private_key=neo4jCert.key
dbms.ssl.policy.https.public_certificate=neo4jCert.crt
dbms.ssl.policy.https.trusted_dir=certificates/https/trusted
dbms.ssl.policy.https.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.https.client_auth=NONE
dbms.ssl.policy.https.tls_versions=TLSv1.3,TLSv1.2

# Cluster SSL configuration
dbms.ssl.policy.cluster.enabled=true
dbms.ssl.policy.cluster.base_directory=certificates/default
dbms.ssl.policy.cluster.private_key=neo4jCert.key
dbms.ssl.policy.cluster.public_certificate=neo4jCert.crt
dbms.ssl.policy.cluster.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.cluster.trusted_dir=certificates/bolt/trusted
dbms.ssl.policy.cluster.tls_versions=TLSv1.3,TLSv1.2
```

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/ssl-framework/
2. https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
3. https://neo4j.com/docs/java-manual/current/client-applications/#java-driver-connection-uris

NOTES:

Neo4j drivers enable TLSv1.2 by default. Ciphers may be listed but are not required.

Neo4j can be configured to list both TLSv1.2 and TLSv1.3. If both TLS are configured and you have specified ciphers, then you should specify specific ciphers for each TLS version.

ENCRYPT DATA BACKUPS

DESCRIPTION:

Use TLSv1.2 or higher to protect all data backups.

RATIONALE:

This prevents sniffing of cleartext traffic when performing a Neo4j backup.

AUDIT:

This prevents sniffing of cleartext traffic when performing a Neo4j backup:

```
nmap --script ssl-enum-ciphers -p 6362 localhost
```

NOTES:

Manage access to database dumps and to database backups.

REMEDIATION:

Configure Neo4j servers to require the use of TLS to encrypt all Neo4j network communications. Neo4j 2025 treats a single machine as a clustered server. Therefore, the cluster listen addresses is open by default. Backups can be taken against the backup port (default 6362) or the cluster listen address (default 6000). With this in mind, you must either include a cluster encryption policy or configure the backup port to be the same as the cluster listen address port.

To implement TLS to encrypt all Neo4j network communication, review the referenced section of our manual.

1. Read the following 2 sections in the Operations Manual: https://neo4j.com/docs/operations-manual/current/security/ssl-framework/ and then read: https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
2. Run **nmap --script ssl-enum-ciphers localhost** to determine what ciphers are available.
    a. Ciphers supported by the Oracle JRE can be found here: https://docs.oracle.com/en/java/javase/11/docs/specs/security/standard-names.html#jsse-cipher-suite-names
3. Configure intermediate certificates and server certificates per https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
4. Enable encryption on the backup service for Causal Clustering instances.
5. Configure **neo4j.conf** Backup SSL Policy:

```
# Backup SSL configuration
dbms.ssl.policy.backup.enabled=true
dbms.ssl.policy.backup.base_directory=certificates/default
dbms.ssl.policy.backup.private_key=neo4jCert.key
```

```
dbms.ssl.policy.backup.public_certificate=neo4jCert.crt
dbms.ssl.policy.backup.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.backup.client_auth=NONE
dbms.ssl.policy.backup.trusted_dir=certificates/bolt/trusted
dbms.ssl.policy.backup.tls_versions=TLSv1.2


# Cluster SSL configuration
dbms.ssl.policy.cluster.enabled=true
dbms.ssl.policy.cluster.base_directory=certificates/default
dbms.ssl.policy.cluster.private_key=neo4jCert.key
dbms.ssl.policy.cluster.public_certificate=neo4jCert.crt
dbms.ssl.policy.cluster.ciphers=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
dbms.ssl.policy.cluster.trusted_dir=certificates/bolt/trusted
dbms.ssl.policy.cluster.tls_versions=TLSv1.2
```

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/ssl-framework/
2. https://neo4j.com/docs/operations-manual/current/clustering/intra-cluster-encryption/
3. https://neo4j.com/docs/operations-manual/current/backup-restore/online-backup/#online-backup-ssl
4. https://neo4j.com/docs/operations-manual/5/backup-restore/online-backup/#online-backup-cluster

NOTES:

Neo4j can be configured to list both TLSv1.2 and TLSv1.3. If both TLS are configured and you have specified ciphers, then you should specify specific ciphers for each TLS version.

CHANGE DEFAULT BACKUP PORT

DESCRIPTION:

Modify backup address port from the default setting of 6362.

RATIONALE:

This prevents access to the backup by sniffing for servers with ports 6362. While this is the default port for remote backups, Neo4j also allows backups from the default cluster_listen_address. Both ports (backup and cluster_listen_address) should be protected with encryption (TLS) and placed behind a network firewall.

REMEDIATION:

Configure **neo4j.conf** to use a different backup port:

```
server.backup.listen_address=0.0.0.0:7362
```

DEFAULT VALUE:

0.0.0.0:6362

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/ports
2. https://neo4j.com/docs/operations-manual/5/backup-restore/online-backup/#online-backup-cluster

USE VOLUME ENCRYPTION

DESCRIPTION:

Use industry-standard methods for encrypting data when stored in disk ("data at rest").

REMEDIATION:

In Ubuntu, full-disk encryption is an option during the OS installation process. For other Linux distributions, the disk can be encrypted with dm-encrypt. For Windows, use volume encryption such as BitLocker.

For Cloud deployments (AWS, GCP, Azure), configure your storage so that the data is encrypted at rest using the Advanced Encryption Standard (AES).

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/checklist

Activity Logging

This section contains recommendations related to configuring activity logging in Neo4j.

ENSURE THAT SYSTEM ACTIVITY IS AUDITED

DESCRIPTION:

Track access to Neo4j. Neo4j Enterprise includes a system auditing facility that can record system events (e.g. user operations, connection events) on a Neo4j instance. These audit records permit forensic analysis and allow administrators to verify proper controls.

RATIONALE:

System level logs can be handy while troubleshooting an operational problem or handling a security incident.

AUDIT:

To verify that system activity is being audited for Neo4j, inspect the **neo4j.conf** file for the following settings:

```
server.directories.logs=logs
```

Configure the **conf/server-logs.xml** file to log in a JSON format.

```
<RollingRandomAccessFile name="SecurityLog"
fileName="${config:server.directories.logs}/security.log"
    filePattern="$${config:server.directories.logs}/security.log.%02i">
    <JsonTemplateLayout
eventTemplateUri="classpath:org/neo4j/logging/StructuredJsonLayout.json"/>
    <Policies>
        <SizeBasedTriggeringPolicy size="20 MB"/>
    </Policies>
    <DefaultRolloverStrategy fileIndex="min" max="7"/>
</RollingRandomAccessFile>


<!-- The security log, must be named "SecurityLogger" -->
<Logger name="SecurityLogger" level="INFO" additivity="false">
    <AppenderRef ref="SecurityLog"/>
```

```
</Logger>
```

NOTES:

The json format provides additional auditing details in the security.log file.

REMEDIATION:

1. In the neo4j.conf file, set the value of **server.directories.logs** to the appropriate destination.
2. In the server-logs.xml file, set the value of **SecurityLogger level** to the appropriate setting.
3. Set the value of **DefaultRolloverStrategy fileIndex max** to the appropriate number of logs to keep.
4. Set the logging template to JSON. JSON logging provides additional log entries.

DEFAULT VALUE:

dbms.directories.logs=logs

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/file-locations/
2. https://neo4j.com/docs/operations-manual/current/monitoring/logging/
3. https://neo4j.com/docs/operations-manual/current/monitoring/logging/#security-events-logging

QUERY LOGGING

DESCRIPTION:

Minimize the amount of sensitive data that may be logged into the Neo4j query log. Unnecessarily logging query parameters and literals could leak sensitive information into the query.log file.

RATIONALE:

Unnecessarily logging query parameters and literals could leak sensitive information into the query.log file.

REMEDIATION:

In the neo4j.conf file, set the following values:

```
db.logs.query.obfuscate_literals=true
db.logs.query.parameter_logging_enabled=false
```

DEFAULT VALUE:

db.logs.query.obfuscate_literals=false
db.logs.query.parameter_logging_enabled=true

Note: db.logs.query.obfuscate_literals setting should only be used when necessary.

Parameter logging should also only be used when necessary. Logging large number of parameters will reduce the amount of query logs available for debugging.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/ -config_db.logs.query.obfuscate_literals
2. https://neo4j.com/docs/operations-manual/current/reference/configuration-settings/#config_dbms.logs.query.parameter_logging_enabled

Anonymous Usage Data Reporting

The Neo4j Anonymous Usage Data Collector gathers usage data, reporting it to Neo4j (https://udc.neo4j.com). It does not collect any confidential or identifying data.

DISABLE ANONYMOUS USAGE DATA REPORTING

RATIONALE:

Disabling the Usage Data Collector prevents any data from being sent to a third-party server.

REMEDIATION:

Disabling the Usage Data Collector should be implemented before anyone accesses the

Neo4j Server.

To disable the Usage Data Collector:

In the Neo4j.conf file, add the dbms.usage_report.enabled configuration parameter and configure it as follows:

```
dbms.usage_report.enabled=false
```

DEFAULT VALUE:

- dbms.usage_report.enabled is set to true.

REFERENCES:

1. https://neo4j.com/docs/reference/usage-data/
2. https://neo4j.com/docs/operations-manual/current/configuration/configuration-settings/#config_dbms.usage_report.enabled

Operating System Hardening

This section contains recommendations related to hardening the operating system running below Neo4j.

NEO4J DATABASE RUNNING WITH LEAST PRIVILEGES

DESCRIPTION:

These recommendations help ensure that the Neo4j service runs as a least privileged user.

RATIONALE:

Anyone who has been a victim of viruses, worms, and other malicious software (malware) will appreciate the security principle of “least privilege”. If all processes ran with the smallest set of privileges needed to perform the user’s tasks, it would be more difficult for malicious and annoying software to infect a machine and propagate to other machines.

REMEDIATION:

Create a user that is only used for installing and running neo4j and directly related processes.

This user must not have administrative rights to the system.

The user that Neo4j runs as must have the following permissions:

Read Only

- certificates
- configuration directory
- import
- labs
- lib
- licenses
- plugins
- products

Read Only and Execute

- bin

Read and Write

- data
- logs
- metrics

- run

Execute

- tmp

```
If tmp is set to noexec, it is recommended to set server.jvm.additional=-
Djava.io.tmpdir=/home/neo4j in conf/neo4j.conf. Additionally, replace
/home/neo4j with a path that has exec permissions.

For /bin/cypher-shell, set this via an environment variable: export
JAVA_OPTS=-Djava.io.tmpdir=/home/neo4j and replace /home/neo4j with a path
that has exec permissions.

For the Neo4j's uses of the Java Native Access (JNA) library, set
server.jvm.additional=-Djna.tmpdir=/tmp in conf/neo4j.conf and replace
/tmp with a path that has exec permissions.
```

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/file-locations/#file-locations-permissions

ENSURE THAT NEO4J USES NON-DEFAULT PORTS

DESCRIPTION:

Changing the ports used by Neo4j makes it harder for attackers to find the database and target it.

RATIONALE:

Standard ports are used in automated attacks and by attackers to verify which applications are running on a server.

REMEDIATION:

Change the default ports used by the Neo4j server.

DEFAULT VALUE:

- server.backup.listen_address=0.0.0.0:6362
- server.bolt.listen_address=:7687
- server.bolt.advertised_address=:7687
- server.http.listen_address=:7474
- server.http.advertised_address=:7474
- server.https.listen_address=:7473
- server.https.advertised_address=:7473
- server.routing.listen_address=:7688
- server.routing.advertised_address=:7688
- server.cluster.listen_address=:6000
- server.cluster.advertised_address=:6000
- server.cluster.raft.listen_address=:7000
- server.cluster.raft.advertised_address=:7000

AUDIT:

Review the **neo4j.conf** file for:

- server.backup.listen_address
- server.bolt.listen_address
- server.bolt.advertised_address
- server.http.listen_address
- server.http.advertised_address
- server.https.listen_address
- server.https.advertised_address
- server.routing.listen_address
- server.routing.advertised_address
- server.cluster.listen_address
- server.cluster.advertised_address
- server.cluster.raft.listen_address
- server.cluster.raft.advertised_address

IMPACT:

Hackers frequently scan IP addresses for commonly used ports, so it is not uncommon to use a different port to "fly under the radar". This is just to avoid detection, other than that there is no added safety by using a different port.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/configuration/ports/

ENSURE THAT OPERATING SYSTEM RESOURCE LIMITS ARE SET FOR NEO4J

DESCRIPTION:

Operating systems provide ways to limit and control the usage of system resources such as threads, files, and network connections on a per-process and per-user basis.

RATIONALE:

These limits prevent a single user from consuming too many system resources.

AUDIT:

To verify the resource limits set for Neo4j on a Unix Operating System, run the following commands.

Extract the process ID for Neo4j:

```
ps -ef | grep neo4j
```

View the ulimits associated with that process number:

```
cat /proc/1322/limits
```

REMEDIATION:

Every deployment may have unique requirements and settings. Recommended thresholds and settings are particularly important for Neo4j deployments:

- f (file size): unlimited
- t (cpu time): unlimited
- v (virtual memory): unlimited[1]
- n (open files): 60000
- m (memory size): unlimited[1] [2]
- u (processes/threads): 64000

DEFAULT VALUE:

Not configured.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/performance/

2. https://neo4j.com/docs/operations-manual/current/installation/linux/tarball/#linux-open-files

Disable Deprecated Neo4j Utilities

This section contains recommendations related to disabling deprecated utilities.

JMX

DESCRIPTION:

This setting ensures that remote JMX monitoring is disabled.

RATIONALE:

JMX has several drawbacks:

- It is based on the obsolete RMI protocol
- It can trigger harmful functions like garbage collection
- It can be used for nasty exploits like invoking arbitrary code (https://issues.apache.org/jira/browse/COLLECTIONS-580)

REMEDIATION:

JMX is disabled by default for remote access. Neo4j provides other monitoring options which are described in our operations manual (https://neo4j.com/docs/operations-manual/current/monitoring/):

DEFAULT VALUE:

JMX is disabled.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/monitoring
2. https://neo4j.com/docs/java-reference/5/jmx-metrics/#jmx-remote

Data Protections

This section contains recommendations related to limiting Neo4j access to external IP addresses.

IP BLOCKLIST

DESCRIPTION:

This section describes configuring IP address ranges for the Neo4j DBMS to block.

RATIONALE:

Neo4j should only be able to access a secure set of IP addresses. When the DBMS attempts to make an IP request to a URL, after resolving the URL to an IP address, it ensures this address doesn't collide with any of the blocked IP ranges provided by the configuration setting. Because the control mechanism is applied at the IP network level, it will be applied to any HTTP and FTP requests made by Cypher features such as LOAD CSV.

REMEDIATION:

In the **neo4j.conf** file, add the **internal.dbms.cypher_ip_blocklist** parameter and configure it with a comma separated list of IPv4 and IPv6 CIDR-notation IP ranges.

Configure **neo4j.conf** to

```
internal.dbms.cypher_ip_blocklist= 10.0.0.0/8,ff:f::/64
# Blocks IPv4 traffic between 10.0.0.0 and 10.255.255.255.
# Blocks IPv6 traffic between ff:f:0:0:0:0:0:0 and ff:f:0:0:ffff:ffff:ffff:ffff.
```

DEFAULT VALUE:

Not enabled.

REFERENCES:

1. https://support.neo4j.com/s/article/8584271681427-Protecting-against-Server-Side-Request-Forgery-SSRF

Input Validation

This section contains recommendations related to validating input into Neo4j.

CYPHER INJECTION

DESCRIPTION:

This section contains recommendations related to validating input into Neo4j.

RATIONALE:

Cypher injection is a way for maliciously formatted input to jump out of its context, and, by altering the query itself, hijack the query and perform unexpected operations on the database.

REMEDIATION:

This is managed by submitting inputs as parameters to the query. See the documentation for more about ways to prevent Cypher injection and about Cypher parameters.

DEFAULT VALUE:

None.

REFERENCES:

1. https://neo4j.com/developer/kb/protecting-against-cypher-injection/?ref=neo4j-aura-security-guide-pdf
2. https://neo4j.com/docs/cypher-manual/current/syntax/parameters/?ref=neo4j-aura-security-guide-pdf

Docker

This section contains recommendations related to running Neo4j securely in Docker.

ENCRYPTION

DESCRIPTION:

This section describes security in Neo4j when running in a Docker container.

RATIONALE:

The Docker image can be configured to expose Neo4j's native TLS support.

REMEDIATION:

Docker must be run as a user with read access to the SSL files. You must also publish port 7473 to access the HTTPS endpoint. Refer to the detailed instructions listed in the Neo4j Operations Manual (https://neo4j.com/docs/operations-manual/current/docker/security/) section on deploying Docker with SSL.

```
docker run \ --publish=7473:7473 --publish=7474:7474 --publish=7687:7687 --
user="$(id -u):$(id -g)" -volume=$HOME/neo4j/certificates:/ssl --
volume=$HOME/neo4j/conf:/conf neo4j:5.18.1
```

DEFAULT VALUE:

Not enabled.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/docker/security/
2. https://neo4j.com/docs/operations-manual/current/docker/security/#ssl-envar_example

Sandbox Extensions

This section describes how to ensure the security of custom-written additions in Neo4j.

SANDBOXING

DESCRIPTION:

Neo4j provides sandboxing to ensure that procedures do not inadvertently use insecure APIs. For example, when writing custom code, it is possible to access Neo4j APIs that are not publicly supported, and these internal APIs are subject to change, without notice. Additionally, their use comes with the risk of performing insecure actions. The sandboxing functionality limits the use of extensions to publicly supported APIs, which exclusively contain safe operations, or contain security checks.

RATIONALE:

Neo4j can be extended by writing custom code which can be invoked directly from Cypher, as described in the Java Reference guide. Custom code could perform insecure actions.

REMEDIATION:

The configuration setting **dbms.security.procedures.unrestricted** defines a comma-separated list of procedures and/or user- defined functions that are allowed full access to the database. Configure this setting to allow the minimal set of procedures needed for the database:

```
dbms.security.procedures.unrestricted=apoc.*,my.extensions.example,my.procedures.*
```

DEFAULT VALUE:

Not enabled.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/securing-extensions/
2. https://neo4j.com/docs/java-reference/2025.02/extending-neo4j/

ENABLING EXTENSIONS

DESCRIPTION:

Users can configure Neo4j to only load a few extensions from a larger library.

RATIONALE:

Neo4j can be extended by writing custom code which can be invoked directly from Cypher, as described in the Java Reference guide. Custom code could perform insecure actions. Allow listing manages the custom code that can be invoked directly from Cypher by allowing the loading of a subset of extensions from a larger library.

REMEDIATION:

The configuration setting **dbms.security.procedures.allowlist** is used to name certain procedures that should be available from a library. It defines a comma-separated list of procedures that are to be loaded. Configure this setting to allow the minimal set of procedures or extensions needed for the database:

```
dbms.security.procedures.allowlist=apoc.coll.*,apoc.load.*
```

DEFAULT VALUE:

The default of the setting is *. This means that if you do not explicitly give it a value (or no value), all libraries in the plugins directory will be loaded.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/securing-extensions/
2. https://neo4j.com/docs/operations-manual/current/security/securing-extensions/#allow-listing
3. https://neo4j.com/docs/java-reference/2025.02/extending-neo4j/

Role Based Access Control Authorization

This section describes implementing Role Based Access Control (RBAC) Authorization in Neo4j 2025.

RBAC

DESCRIPTION:

Neo4j has a complex security model stored in the system graph, maintained in a special database called the system database. All administrative commands need to be executing against the system database.

Neo4j 3.1 introduced the concept of role-based access control. It was possible to create users and assign them to roles to control whether the users could read, write and administer the database.

In Neo4j 4.0 this model was enhanced significantly with the addition of privileges which are the underlying access-control rules by which the user's rights are defined. The original built-in roles still exist with almost the exact same access rights, but they are no-longer statically defined. Instead, they are defined in terms of their underlying privileges, and they can be modified by adding and removing these access rights. In addition, any new roles created can by assigned any combination of privileges to create the specific access control desired. A major additional capability is sub-graph access control whereby read-access to the graph can be limited to specific combinations of label, relationship-type(s) and property.

RATIONALE:

RBAC can grant or deny access to portions of the graph ensuring users only see the elements that they are entitled to.

By default, the PUBLIC role has access to the SYSTEM database and the user's HOME database. The other default roles (reader, editor, publisher, architect, admin) have access to all databases.

All users are granted the PUBLIC role, and it cannot be revoked or dropped. By default, it gives access to the default database and allows executing all procedures and user defined functions.

The PUBLIC role cannot be dropped or revoked from any user, but the specific privileges for the role may be modified. In contrast to the PUBLIC role, the other built-in roles can be granted, revoked, dropped, and re-created. The other default roles (reader, editor, publisher, architect, admin) have access to all databases.

Role	Privileges

PUBLIC	All users are granted the public role. By default, this role gives access to the default database and allows execution of procedures and user-defined functions.
Reader	The reader role can perform read-only queries on all graphs except for the system database.
Editor	The editor role can perform read and write operations on all graphs except for the system database, but cannot create new labels, property keys, or relationship types.
Publisher	The publisher role has all the same privileges as the editor, but can also create new labels, property keys, and relationship types.
Architect	The architect role has all the same privileges as the publisher, but can also create and manage indexes and constraints.
Admin	The admin role has all the same privileges as the architect, but can also manage databases, aliases, users, roles, and privileges.

REMEDIATION:

Design and implement RBAC according to your data security requirements. Refer to the Neo4j manual for examples.

Review the privileges of the PUBLIC role to ensure it meets security requirements as all Users are granted the PUBLIC role.

REFERENCES:

1. https://neo4j.com/docs/cypher-manual/current/access-control/
2. https://neo4j.com/docs/operations-manual/current/authentication-authorization/
3. https://neo4j.com/docs/operations-manual/current/authentication-authorization/built-in-roles/

System Database

This section outlines specific information related to the System Database.

SYSTEM DATABASE

DESCRIPTION:

All Neo4j servers will contain a built-in database called **system** which behaves differently than all other databases. In particular, when connected to this database you can only perform a specific set of administrative functions, as described in detail in the section on administration (https://neo4j.com/docs/operations-manual/current/database-administration/#manage-databases-system). Most of the available administrative commands can only be run by users with specific administrative privileges. Information on configuring the security privileges is described in the Operations Manual (https://neo4j.com/docs/operations-manual/current/) as well as in the section on security commands (https://neo4j.com/docs/operations-manual/current/authentication-authorization/).

REMEDIATION:

Configure and limit access to the System Database to those users with specific administrative privileges.

REFERENCES:

1. https://neo4j.com/docs/cypher-manual/current/databases/
2. https://neo4j.com/docs/operations-manual/current/security/
3. https://neo4j.com/docs/operations-manual/current/
4. https://neo4j.com/docs/cypher-manual/current/access-control/

FIPS 140.2 Support

This section outlines specific information related to FIPS 140.2 support.

FIPS 140.2 CONFIGURATION

DESCRIPTION:

The National Institute of Standards and Technology (NIST) developed the Federal Information Processing Standard (FIPS) Publication 140-2 as a security standard that sets forth requirements for cryptographic modules, including hardware, software, and/or firmware, for U.S. federal agencies. FIPS 140-2 Validated certification was established to aid in the protection of digitally stored unclassified, yet sensitive, information.

Neo4j can be configured to use Federal Information Processing Standard 140-2 (FIPS 140-2) cryptography for data transmitted across the network. Neo4j 4.4 officially supports FIPS 140-2 compliance. This is achieved through Neo4j 4.4 official support for the configuration of Neo4j to use a NIST FIPS 140-2 certified third-party OpenSSL cryptographic module and by using this module as the only provider of cryptographic services.

PREREQUISITES:

1. Provision server in FIPS 140-2 mode.
2. Deploy OpenSSL 3.0.8 / 3.0.9 in FIPS mode.

REMEDIATION:

1. Configure the OS to enable FIPS.
2. Install OpenSSL 3.0.8 or 3.0.9 in FIPS mode. OpenSSL 3.0.9 fixes a CVE in OpenSSL 3.0.8.
3. Set SSL Policies for the services you need. It is recommended that you set them for all services (Bolt, HTTPS, Backup, Clustering). See Section 5.1.
4. Installing a FIPS-certified Crypto Module.
    a. Configure **neo4.conf** to add:

    ```
    dbms.netty.ssl.provider=OPENSSL
    ```

    b. Remove all netty-tcnative-boringssl-static* files from the lib directory.
    c. Copy the netty-tcnative files from the <neo4j-directory>/lib/netty-tcnative directory to the <neo4j-directory>/lib directory.
    d. Restart Neo4j.
5. Configure each SSL policy to use a FIPS certified cipher.

DEFAULT VALUE:

FIPS 140.2 is not enabled by default.

SAMPLE NEO4J CONFIGURATION:

```
# Bolt connector
server.bolt.enabled=true
server.bolt.tls_level=REQUIRED
server.bolt.listen_address=:7687
server.bolt.advertised_address=:7687

# HTTPS Connector. There can be zero or one HTTPS connectors.
server.https.enabled=true
server.https.listen_address=:7473
server.https.advertised_address=:7473

# Bolt SSL configuration
dbms.ssl.policy.bolt.enabled=true
dbms.ssl.policy.bolt.base_directory=certificates/https
dbms.ssl.policy.bolt.private_key=private.key
dbms.ssl.policy.bolt.public_certificate=public.crt
dbms.ssl.policy.bolt.client_auth=NONE

# Https SSL configuration
dbms.ssl.policy.https.enabled=true
dbms.ssl.policy.https.base_directory=certificates/https
dbms.ssl.policy.https.private_key=private.key
dbms.ssl.policy.https.public_certificate=public.crt
dbms.ssl.policy.https.client_auth=NONE

dbms.ssl.policy.https.client_auth=NONE
dbms.netty.ssl.provider=OPENSSL
```

NOTE:

FIPS 140-2 support is not available in Windows because we cannot provide FIPS compliant netty-tcnative files.

REFERENCES:

1. https://neo4j.com/docs/operations-manual/current/security/ssl-framework/#ssl-providers
2. https://github.com/openssl/openssl/blob/master/README-FIPS.md
3. https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4282.pdf
4. https://neo4j.com/docs/operations-manual/5/configuration/file-locations/

Changes, Deprecations and Removals

This section describes security related changes, deprecations and removals to the Neo4j surface when migrating from Neo4j 5.x to Neo4j 2025 and beyond.

CHANGES

SSL-related configuration setting

Starting from 2025.01, the default value of dbms.ssl.policy.*.verify_hostname is changed from false to true.

DEPRECATIONS

The following configuration settings have been deprecated in Neo4j 2025.

- dbms.security.oidc.<provider>.auth_params
- dbms.security.oidc<provider>.client_id

REMOVALS

The following CBC-based ciphers are no longer supported in Neo4j 2025.

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

REFERENCES:

1. https://neo4j.com/docs/operations-manual/2025.02/changes-deprecations-removals/