Neo4j Authentication (PC)

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up Neo4j authentication for compliance scans.

A few things to consider

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, it's required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up a Neo4j user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys Policy Compliance, complete these steps: 1) Add a Neo4j authentication record. 2) Launch a compliance scan. 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

Neo4j Credentials

We've provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. These scripts require a super-user account which has privilege to create users. For example, neo4j account or accounts with the admin role.

Please run the scripts provided, in the order shown.

1) Create a User Account

This script creates a user account to be used for scanning. Please provide a password before running the script. Tip – We recommend creating an account called qualys_scan.

```
CALL dbms.security.createUser('qualys_scan','[enter password here]',false);
```

Copyright 2021-2022 by Qualys, Inc. All Rights Reserved.

2) Grant Admin Role to Scan Account

We understand it is not typical to request for admin role, however in Neo4j, we do need this privilege in order to list configuration settings, list user info, and list roles info.

CALL dbms.security.addRoleToUser('admin', 'qualys_scan');

3) Verify Privileges on the Scan Account

Verify that the qualys_scan account has all the privileges in the admin database in order to run a successful compliance scan. Log into the instance using the “qualys_scan” account, then run the following queries to see if access is available to the account.

3a)

CALL dbms.listConfig() yield name return name limit 1

Sample Expected Output:

```
+--------------------+
| name               |
+--------------------+
| "bolt.ssl_policy" |
+--------------------+
```

3b)

CALL dbms.security.listUsers() yield username return username limit 1;

Sample Expected Output:

```
+----------+
| username |
+----------+
| "neo4j" |
+----------+
```

3c)

CALL dbms.security.listRoles() yield role return role limit 1;

Sample Expected Output:

```
+----------+
| role     |
+----------+
| "editor" |
+----------+
```

Did you get different results? Contact your Neo4j DBA to ensure that privileges are set up correctly.

Last updated: May 27, 2022