Expert Trail: Security

Revision 20220520

NOTE
This document is confidential and proprietary of **Denodo Technologies**.
No part of this document may be reproduced in any form by any means without prior written authorization of **Denodo Technologies**.

Copyright © 2022
Denodo Technologies Proprietary and Confidential

Denodo Inc.: 525 University Avenue, Suite 31, Palo Alto, CA 94301. USA www.denodo.com

CONTENTS

1 LOOKOUT.....2

2 THE HIKE.....3

3 EXPLORATION.....6

4 GUIDED ROUTES.....9
4.1 DENODO TRAINING COURSES.....9
4.2 TECHNICAL ADVISORY SESSIONS.....9
4.3 PROFESSIONAL SERVICES.....10

5 BIG HIKE PREP CHECK.....10

1 LOOKOUT

Expert trails guide Denodo users through all the relevant materials related to a specific topic, including official doc, KB articles, training, Professional Services offering, and more. The main goal is to give users a single place with references to all the information that they need to become a Denodo expert on any specific topic.

Security is a necessary part of every data project. By leveraging the security options available in Denodo, you will be able to seamlessly control security over all the data available in your organization in a single place, and make sure that all of the data going through Denodo is only accessed by authorized users.

2 THE HIKE

Stage 1: Securing Data in Motion; Configuration of Transport Layer Security (TLS)

The first step in making sure that the Denodo Platform is secured is making sure that none of the communications between the Denodo Platform components and other services are decipherable to unwanted listeners. This makes sure that information like the credentials of clients and sensitive data from the underlying sources can not be obtained by a malicious user.

To configure TLS in the Denodo Platform, the following steps must be performed in both the Virtual DataPort and Solution Manager installations:

- A private key must be configured, and a corresponding public key must be inserted into the Truststore of the Denodo Platform.
- The Virtual DataPort server must be configured to use TLS, and reference the Keystore and Truststore created in the previous step.
- The Tomcat instance handling web requests must reference the Keystore and Truststore, and the HTTPS connector must be enabled.
- Other Denodo components such as the Scheduler server must have TLS enabled.

For a step-by-step guide to implementing TLS in the Virtual DataPort server, you can follow along in the Enable SSL/TLS in the Denodo Platform page and the following pages of the Denodo Platform Installation Guide.
For changing the current certificate, the How to renew an SSL certificate in Denodo KB article provides the different required steps.

Stage 2: Securing Data at Rest; Configuring How Data is Stored by the Denodo Platform

To completely secure the data from being read by attackers without access to Denodo, the data that Denodo stores during operation must also be encrypted. In conjunction with encrypting data in motion, encrypting data at rest will prevent sensitive data in the filesystem or underlying data sources from being exposed. To secure data at rest, administrators of the Denodo Platform must ensure the following:

- The database used as cache stores data in an encrypted format. Since a Virtual DataPort server leveraging the cache will write data into a database, this data must be encrypted.
- If memory swapping is enabled, the Virtual DataPort server may need to send intermediate results to disk in order to avoid running out of heap space. In this case, the underlying filesystem can be configured to encrypt the location where intermediate data is swapped, or swapping can be disabled.
- Passwords stored by Denodo are automatically encrypted in the metadata database used by Denodo. Complete encryption of Denodo metadata can also be configured if necessary.

More information about the options in the Denodo Platform for securing data at rest can be found in the Swapping Parameters and Transparent Metadata Encryption pages from the Virtual DataPort Administration and Denodo Platform Installation Guides respectively.

Stage 3: Integration with a Centralized Authentication Server

After ensuring that sensitive data is not accessible to listeners in the network or users of the Virtual DataPort server's filesystem, permissions inside the Denodo Platform must be carefully configured to make sure that bad actors do not obtain permission to access the Denodo Platform. To manage authentication in a single location and increase traceability, Denodo Administrators can configure the Virtual DataPort server to delegate authentication to a Centralized Authentication Server. This is commonly implemented in the Virtual DataPort server in one of the following ways:

- Using an LDAP server: users can log in with their username and password, and the Virtual DataPort server can retrieve the groups of which the user is a part. Steps to configure LDAP Authentication can be found in the attached page from the Virtual DataPort Administration Guide.

- Leveraging Kerberos: this allows the Virtual DataPort server to accept and delegate Kerberos Tickets from a KDC, and also provides delegated authentication and authorization capabilities. More information about configuring Kerberos can be found on the Kerberos Authentication page of the Denodo Platform Administration Guide.
- In addition, users can authenticate to web services in the Denodo Platform using SAML or OAuth 2.0, through JDBC using OAuth, and can connect to other web services from Denodo using OAuth. Additional information about these functionalities can be found in the Web Services Authentication, OAuth Authentication, and OAuth Authentication (for HTTP sources) pages from the Virtual DataPort Administration Guide.
- Integration with Credentials Vault: Virtual DataPort provides support to obtain the credentials of JDBC data sources from an external *Credentials Vault*.

In Denodo 8.0, the Solution Manager can also act as a single point of access, allowing for Single Sign-on to the Virtual DataPort servers using Kerberos, OpenID, OAuth, or SAML in conjunction with Denodo Security Tokens, which delegate authentication from the Solution Manager to the Virtual DataPort servers. You can find more information about this on the Denodo Security Token page of the Solution Manager Administration Guide.

More information about each of the external authentication methods available in Denodo can be found on the Server Authentication page of the Virtual DataPort Administration Guide.

Stage 4: Configuring Permissions in Denodo

To make sure that authorized users only have the necessary privileges to perform their tasks, Denodo recommends that privileges are assigned to users based on the Principle of Least Privilege. To allow administrators to effectively follow this principle and implement it in their scenario, Denodo offers granular permissions, down to row and column level restrictions, as well as custom policies.

User and role-based permissions in Denodo allow for the authorization over all enterprise data to be managed at a single point, which simplifies governance and compliance with data privacy requirements. In addition, the Denodo Platform allows LDAP groups to be linked to roles in Denodo, which allows for groups already organized in a central authentication server to be provided permissions in the server. More information about the Denodo permissions system can be found on the User and Access Right in Virtual DataPort page of the Virtual DataPort Administration Guide.

Starting in Denodo Platform 8.0 update 20220126 and for Enterprise Plus licenses, the Denodo Platform includes Global Security policies that allow for the creation of Tag-based policies. "Tags" are labels that users can assign to views and corresponding columns. Global level policies are easier to manage than view restrictions (Row Restrictions and Column Privileges). The advantage of Tags is that they can assign a policy to multiple views and columns at the same time.

Stage 5: Auditing

Finally, with all of the security of the Denodo Platform configured, auditing allows

administrators to keep a record of actions performed on the Virtual DataPort server, to monitor for unexpected behaviors or compromise of the server.

The Denodo Platform generates an event for each operation performed on the Virtual DataPort server, which records which users had access to what resources, what changes they made, and when the operations were executed; these events can be recorded in log files or an external database, and they can be observed by external tools supporting SNMP, JMX, and WS-Management standards for integration into external Security Information and Event Management tools.

Additionally, access privileges, data lineage, auditing, and the masking of sensitive data help organizations comply with the requirements of GDPR.

More information about auditing the actions performed on the Virtual DataPort server can be found on the Auditing User Access in Virtual DataPort page of the Knowledge Base.

More information on how to monitor and audit can be found in the Expert Trail: Monitoring

3 EXPLORATION

Fill up your backpack with additional gear:

Setting up TLS in the Denodo Platform

NOTE: Only JKS format keystores can be used by the Denodo Platform; PKCS12 keystores will not work. Additionally, the certificate should contain Subject Alternate Names for the Virtual DataPort server and any load balancer.

Official Documentation	● Enabling SSL/TLS in the Administration Tool and Others — Installation Guide ● Importing the Certificates of Data Sources (SSL/TLS Connections) — Installation Guide ● Denodo SSL/TLS Configurator Script — Installation Guide
KB Articles	● SSL Self-Signed Cert Installation ● SSL connection from VDP to data sources ● Disabling the HTTP port of the embedded web container
Additional Resources	● Oracle Java keytool documentation (Windows) - Oracle ● Oracle Java keytool documentation (Unix) - Oracle

Configuring LDAP

NOTE: Setting the “UseLDAPDomainName” property with the following command `SET 'com.denodo.vdb.security.UserManager.UseLDAPDomainName' = 'true';`
Is necessary when selecting the “Use GSSAPI SASL authentication mechanism” option in LDAP data sources.

Official Documentation	● LDAP Sources — Virtual DataPort Administration Guide ● Useful Tools to Debug Issues with Active Directory or Other LDAP Servers — Virtual DataPort Administration Guide
KB Articles	● LDAP authentication best practices ● Connect to LDAP data source using SSL
Additional Resources	● LDAP Authentication at server level - Videos | Denodo ● Importing LDAP roles in Virtual DataPort - Videos | Denodo

Leveraging Kerberos

NOTE: If cross-realm, authentication will be used to connect to the Virtual DataPort server, the "Use GSSAPI SASL authentication mechanism" option must be selected in the LDAP data source associated with the Kerberos configuration of the Virtual DataPort server.

Official Documentation	● Setting-up Kerberos Authentication — Installation Guide ● Providing a Krb5 File for Kerberos Authentication ● Enabling Kerberos Authentication Without Joining a Kerberos Realm — Installation Guide
KB Articles	● Kerberos Overview ● Kerberizing Denodo for SSO - Step by step guide - Introduction (I) ● Kerberizing Denodo for SSO - Step by step guide - Domain Controller Configuration (II) ● Kerberizing Denodo for SSO - Step by step guide - Server Configuration (III) ● Kerberizing Denodo for SSO - Step by step guide - Clients Configuration (IV) ● Kerberos configuration and troubleshooting ● How to Debug Kerberos in Web Applications — Installation Guide ● How to set up SSO with pass-through for ODBC connections to Denodo

Utilizing Web-Based Authentication

Official Documentation	● Authenticating with Single Sign-On — Solution Manager Administration Guide
KB Articles	● How To Configure Okta for Single Sign-On in Denodo Solution Manager 8.0 ● How To Configure Keycloak for SSO in the Denodo Solution Manager ● How To Configure PingFederate for SSO in Denodo Solution Manager 8.0 ● How To Configure Published Web Services with Oauth and Azure AD ● SAML 2.0 Protocol Overview ● OAuth 2.0 Protocol Overview

Permissions in Denodo

Official Documentation	● Administration of Databases, Users, Roles, and Their Access Rights — Virtual DataPort Administration Guide ● Custom Policies — Virtual DataPort Developer Guide

	● CATALOG_PERMISSIONS — VQL Guide ● GET_CATALOG_EFFECTIVE_PERMISSIONS — VQL Guide
KB Articles	● Security: roles, users, permissions — Denodo Admin and Development Best Practices
Webinars	● Centralize Security and Governance with Data Virtualization

Global Security Policies and Tags

Official Documentation	● Global Security Policies — Virtual DataPort Administration Guide ● Global Security Policies — VQL Guide
Tutorial	● Global Security Policies and Tags

Auditing

Official Documentation	● Denodo Monitor — Virtual DataPort Administration Guide ● Monitoring with a Java Management Extensions (JMX) Agent — Virtual DataPort Administration Guide
KB Articles	● Auditing User Access in Virtual DataPort
Webinars	● GDPR Compliance Made Easy with Data Virtualization
Additional Resources	● Seamlessly Comply with the GDPR - Solution Brief | Denodo

Additional References

NOTE: We recommend reviewing the Denodo Security Overview Knowledge Base Article for a complete understanding of all the security options available in the Denodo Platform.

Official Documentation	● Avoiding SQL Injections
KB Articles	● Denodo Security Overview
Webinars	● Centralize Security and Governance with Data Virtualization

Additional Resources

- Denodo Data Virtualization Security Architecture & Protocols - Whitepaper | Denodo

4 GUIDED ROUTES

4.1 DENODO TRAINING COURSES

Denodo training courses provide expert data virtualization training for data professionals, including administrators, architects, and developers.
If you are interested in Security you should enroll in the following course:

- Denodo Security Management: This course covers the security mechanisms included in Denodo Platform 8.0 (security in transit, security at rest). It also talks about different authentication protocols and how to configure Single Sign-On.

4.2 TECHNICAL ADVISORY SESSIONS

Denodo Customers with active subscriptions have access to request Meet a Technical Advisory sessions.
These are the sessions available related to performance.

Security of Denodo Platform components: Protocols	**Security Architecture** 	Understand the Denodo Platform Security Architecture. Overview and advice to adapt it to your needs: - Authentication and Authorization model. - Secure connections: between Denodo Platform components, from clients (Northbound), and to data sources (Southbound). Pass-through credentials. - Secure passwords of Denodo Platform components (Denodo Monitor, SSL, scripts, etc.). - Integration with Vault Security Solutions (Protegrity, HPVoltage). - Define Admin privileges, passwords, and access. - Data in motion (SSL/TLS).
	SSL/TLS Configuration 	Steps to set up SSL/TLS in the Denodo Platform Components.
	LDAP/AD Configuration 	Steps to set up LDAP in the Denodo Platform Components.
	Single Sign-on	Review how to configure SSO for the Denodo

	Configuration: SSO 	Platform Components that can be accomplished through any of the following protocols: Kerberos, Oauth, SAML, OpenID.
Security: Data Access	**Authorization Model** 	Guidance on defining your authorization model to adapt it to your needs. Some suggested topics: - Business user model vs developer model. - Effectively leveraging LDAP Groups. - Inheritance and reusability. - User and role-based authorization. - Principle of Least Privilege. - Fine-grained authorization: masking, row, and column restrictions. - Data encryption. - Planning for Self Service/Discovery. - Managing authorization through promotions. - Service accounts. - Pass-through credentials. - Define policies to connect and request access from clients (Data Catalog, data services, BI tools, etc.).

4.3 PROFESSIONAL SERVICES

Denodo Professional Services can help you at the start or any part of your query performance trail. You can find information about the Denodo Professional Services offering in:
Professional Services for Data Virtualization | Denodo

In particular, you may be interested in the following module:

- **Operations Quick Start**

Additional other related modules could be:

- **Vision and Strategy**

If you are a Denodo customer, you can reach out to your Customer Success Manager for details about any Guided Route that you need.

5 BIG HIKE PREP CHECK

Let's see if you are ready to start your big trail. Take this 5-question questionnaire to check your readiness for an enjoyable hike.
Read the questions below, think about the solution and check if you got them right by looking at the solution. Have you become an expert?

1. Does Denodo provide a script to generate a private key and certificates for the Denodo Platform?

   Click here to check if you got it right

   No, you will need to configure the private key and public certificates for the Virtual DataPort server yourself. To configure these keys and certificates, the Denodo Platform Installation Guide contains detailed information for configuring certificates for the following scenarios:
   - If you do not have an SSL private key, you can create a Keystore with a self-

signed private key.
- If you do not have an SSL private key, you can send a request to a certificate authority (CA) and create a Keystore with the certificate reply.
- If you have a PFX file with the private key, you can create a Keystore with its content.

You can find more information about each one of these scenarios on the Obtaining and Installing an SSL/TLS Certificate page.

Although certificates must be manually configured, the Denodo Platform does provide the "denodo_tls_configurator" script, which allows you to configure TLS in the Denodo Platform with a single script! This automatically takes care of modifying each of the configuration files for the Denodo Platform components, imports the public certificate and certificate chain into the corresponding store, configures the embedded Tomcat instance to use only HTTPS connections, and more. You can find more details about the syntax and functionality of the "denodo_tls_configurator" script in the Denodo SSL/TLS Configurator Script page from the Denodo Platform Installation Guide.

2. Do users connecting through LDAP and Kerberos all have the same permissions?
Click here to check if you got it right

No. Permissions of LDAP or Active Directory users can be customized by importing the LDAP or Active Directory groups of the users to the Virtual DataPort server as roles; this creates a link from a group defined in the centralized authentication server to a role in the Virtual DataPort server. Then, when a user authenticates and is part of that group in the centralized authentication server, they will be assigned the corresponding role in the Virtual DataPort server that was imported previously.

The roles created from this process can be treated like any other roles in the Virtual DataPort server, providing the full Role-based permissions available in the Denodo Platform to users connecting with LDAP or Kerberos. You can find more information about importing LDAP and Kerberos groups into the Denodo Platform in the Wizard "Import Roles from LDAP" section of the Virtual DataPort Administration Guide.

3. Can administrators impose restrictions on only certain types of queries?
Click here to check if you got it right

Yes. Using Custom Policies, custom restrictions can be defined in Java and applied to elements in the Virtual DataPort server. When a user queries a view with a custom policy assigned, the policy can take one of the following actions:
- Stop the query.
- Allow the query to execute without restrictions.
- Allow the query to execute, but with restrictions such as limiting the rows returned by the query or adding a filter condition.

To determine how the policy should react to a user querying the view, the policy can take into account many aspects of the query's context such as:
- The query the user wants to execute.
- The name of the user and their privileges.
- A JMX connection to the Server, which can be used to reference usage parameters of the Virtual DataPort server's JVM.
- And more.

Note that custom policies are not applied to administrator users.

Using custom policies, even more specific restrictions can be developed; such as limiting the number of concurrent requests a user can make over a view. For more information about Custom Policies, you can refer to the Custom Policies page of the Virtual DataPort Developer Guide.

4. Does Denodo allow administrators to redact information to unauthorized users?
Click here to check if you got it right

Yes; the Denodo Platform includes the ability to assign Column Privileges and Row Restrictions to roles and users, which help restrict sensitive output from being returned in queries made by users without the correct permissions.

Column restrictions prevent users with execute privileges from querying certain columns in a view; they would not be able to see the column when executing a query, they could not define logic in their queries that references these columns, and they would not be able to modify these columns with INSERT, UPDATE, or DELETE statements.

On the other hand, row restrictions provide the expected redaction behavior when a user queries a view (they can also be configured to remove sensitive rows entirely from a query, or remove sensitive rows from a query when specific columns are used). When configuring a row restriction, Denodo Administrators will define a condition on the rows of the view. Only the rows that do not meet the condition will be automatically returned to the user. For the rows that match the condition, the row will be removed or masked (depending on the configuration of the row restriction) when the query is executed by restricted users.

Note that the query optimizer takes into account row restrictions and column privileges automatically when generating the query plan of a view, and these restrictions are not applied to administrator users.

With column privileges and row restrictions, Denodo Administrators have fine-tuned control over the information that users can see in Denodo views, even if they have EXECUTE, INSERT, UPDATE, or DELETE privileges over the views.

5. How would I find out who is changing the descriptions of my views?
Click here to check if you got it right

The Denodo Platform includes the Denodo Monitor, which is a program that records the actions performed on the Virtual DataPort server as well as other parameters of the JVM. In addition to information about the memory usage, CPU usage, thread count, and garbage collection information from the JVM, this would also record the queries executed on the Virtual DataPort server; the list of queries executed would contain any modifications to the elements in the catalog, and more information about the changes to your view. The Denodo Monitor can be configured to write to logs or to a database.

To more easily review the Denodo Monitor information instead of searching text files or in a database, you could use the Diagnostic and Monitoring Tool; then, you would be able to search for queries executed on your view based on multiple

parameters such as the name of the view, time the query was executed, users executing the query, and more. From here, you would be able to find the pesky user that is changing your laboriously crafted descriptions.

You can find more information about the Denodo Monitor in the Denodo Monitor and the following pages of the Virtual DataPort Administration Guide. For the steps to create a Diagnostic in the Diagnostic and Monitoring Tool to search your log files, you can reference the Creating Diagnostics page from the Diagnostic & Monitoring Tool Guide.