Kerberizing Denodo for SSO - Step by step guide - Introduction (I)

Revision 20200604

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

This Step by Step guide is a series of four documents that provide a detailed explanation on how to configure Kerberos in the Denodo server and the client tools. It includes a practical example covering the full process starting with the configuration for the Domain Controller, then the Denodo Server and finally the clients' configuration.

Note: For practical reasons, the document is split into four parts, being this one the Introduction and three additional documents covering every section. We recommend following this example in the suggested order:

1. Kerberizing Denodo for SSO - Step by step guide - Introduction (I) (this document)
2. Kerberizing Denodo for SSO - Step by step guide - Domain Controller Configuration (II)
3. Kerberizing Denodo for SSO - Step by step guide - Server Configuration (III)
4. Kerberizing Denodo for SSO - Step by step guide - Clients Configuration (IV)

1 KERBEROS BACKGROUND

Kerberos is a key component of providing access control in today's enterprises.

At the beginning of the workday, users log into Kerberos (typically log into their Operating System, for example, Windows), obtaining credentials once and then using applications throughout the day.

Using Kerberos guarantees that these applications need not ask for a username or password again as they will be able to use a Kerberos ticket created (typically) by the Operating System at logon time.

Other benefits:

- Each application gets a consistent way of naming users (all applications use the same LDAP users).
- The organization gets a single point at which to enforce security policy (users are members of one or several groups in the LDAP).

As stated before, the most visible benefit to Kerberos for end-users is **single sign-on (SSO)**. The user does not sign onto each application but instead can sign onto their computer once (by means of a login/password, fingerprint, PIN, smart card or whatever system is used for sign-in).

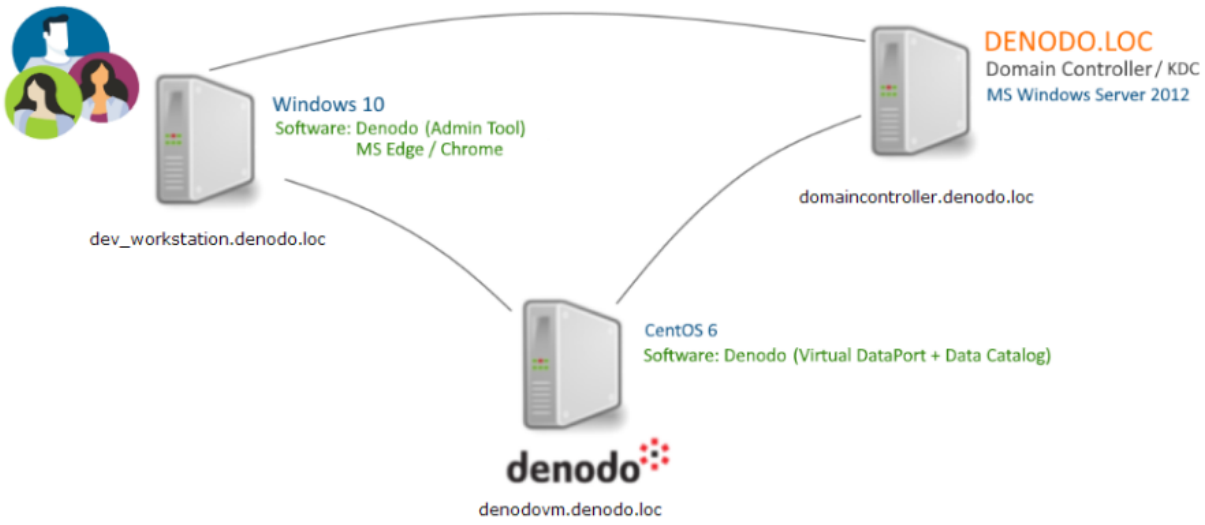
Kerberos accomplishes single sign-on by storing credentials that typically last approximately one workday. When the user signs onto the computer, the local Kerberos implementation contacts the **Key Distribution Center (KDC)** to authenticate the user to the KDC (typically the KDC is an MS Active Directory domain controller server).

When authentication succeeds, the KDC issues a **ticket**. The ticket is a time-limited message from the KDC to itself attesting to successful authentication. This ticket along with a session key known only to the local computer and the KDC forms a credential that can be used to sign onto applications.

When Kerberos is used for authentication in an application, it presents the ticket along with proof that the session key is known by the client to the KDC and receives a *new service ticket* for the application that is being contacted. The KDC serves as a central point to enforce the organization's authentication policy and to enforce general policies about user management.

2 ENVIRONMENT

Let's see a working example of Single Sign-on in Denodo applications (Virtual DataPort and Data Catalog). We have used the following environment:



Basically, it consists of 3 servers:

- **domaincontroller.denodo.com**: this is the domain controller (DC) of the DENODO.LOC domain. Users configured in this domain will be able to login to the computers of the domain.
- **denodovm.denodo.loc**: this is a Linux server with an installation of Denodo (Virtual DataPort and Data Catalog). Denodo is configured as a service using an admin account and users don't have privileges to modify the configuration.
- **dev_workstation.denodo.loc**: this is a Windows 10 workstation. Users will login to this machine to do their daily work. They have a Denodo Administration Tool for connecting to the Denodo installation

In a typical architecture, the users of `dev_workstation.denodo.loc` will be able to connect to Virtual DataPort using their Administration Tool and using a normal user (for example, the default admin/admin user).

This guide will explain the steps done for configuring Kerberos in this environment, so users will log in to Denodo using SSO (no user/password will be needed to access Denodo applications).

3 STEP-BY-STEP GUIDE

This guide will list the steps needed in each server. The guide is divided into 3 documents covering every point of the mentioned architecture.

We recommend following the steps in the order described:

1. Configuring the Domain Controller: Kerberizing Denodo for SSO - Step by step guide - Domain Controller Configuration (II).
2. Enabling Kerberos in the Denodo Server: Kerberizing Denodo for SSO - Step by step guide - Server Configuration (III).
3. Configuring Kerberos in Client Applications (VDP Administration Tool, Web browsers, JDBC/ODBC clients...): Kerberizing Denodo for SSO - Step by step guide - Clients Configuration (IV).

If you find any issue during the process, we recommend checking the Kerberos configuration and troubleshooting document, that provides guidance and advice on how to solve the most common problems when configuring Kerberos.