Virtual Network Orchestrator (ViNO) Installation Guide

Software Version 1.0.1

February 3, 2020

Contents

List of Tables

Introduction

This document describes how to install and initialize a ViNO instance and how to create a realm in Keycloak.

ViNO uses the Keycloak authentication server to provide local authentication and the ability to incorporate federated authentication methods such as Kerberos or LDAP. In addition, ViNO can use Single Sign On (SSO) Identity Providers (IdPs) over SAML or OpenID Connect (OIDC).

In addition to this guide, ViNO documentation includes the *Virtual Network Orchestrator (ViNO) User Guide*.

The VINO project was developed and tested on CentOS release 7.6.

System Requirements

VINO is designed to be installed on a new minimal installation of CentOS 7.6. Ensure that your newly created CentOS machine is able to communicate on the internet because it needs to download several components as part of the VINO installation.

Before you download the VINO project, ensure that your workstation meets or exceeds the following hardware requirements:

- A minimum of 4 CPUs

- A minimum of 20 GB of free disk space

- A minimum of 8 GB of RAM

ViNO Installation Process

The following sections describe the complete process of installing and initializing ViNO in addition to creating and populating a Keycloak realm.

The order in which the process must be completed is as follows:

- ▪ Installing ViNO

- ▪ Creating a Keycloak Realm for ViNO

- ▪ Populating the Keycloak Realm for ViNO

- ▪ Initializing ViNO

Installing ViNO

To install an instance of ViNO instance:

1. Download the ViNO installation file (vino-product-docker.1.0.1-4.tar.gz) from Github. For example:

    curl https://github.com/CenturyLink-ViNO/vino-product/releases/download/1.0.1/vino-product-docker.1.0.1-9.tar.gz

2. Run the installation script: **sh ./binstall.sh**. The installation takes several minutes. When it installs successfully, the following messages are displayed:

    $ ViNO ---> The ViNO docker images have been loaded. Please see the *Virtual Network Orchestrator (ViNO) Installation Guide* for detailed instructions on how to set up and run ViNO.

    $ ViNO ---> log available in /var/log/vino.install/ViNO Docker Distribution_product_Install.1359.log.

    If the installation does not install properly, check the log file for error messages. Log files are located in /var/log/vino.install.

3. Proceed to Creating a Keycloak Realm for ViNO.

Creating a Keycloak Realm for ViNO

After ViNO has been installed, you must create a Keycloak realm. ViNO uses Keycloak for authorization.

To create a Keycloak realm:

1. Use the command line to navigate to the directory: **/opt/vino/vino-docker**.

2. From the directory, run the command **docker-compose -p vino up -d** to start the four docker containers for ViNO.

3. Open an internet browser and enter the IP address of your ViNO host in the URL bar followed by /auth (for example: 123.45.6.789/auth). This URL goes to the Keycloak homepage.

4. Click **Administration Console**, which prompts you to log with the default username **admin** and default password **changethis**. We recommend changing the default password.

5. From the **Master** drop-down, select **Add Realm**.

6. Enter **vino** in the **Name** field, then click Create.

Proceed to the next sections for information on:

▪ Keycloak roles and groups.

▪ Adding roles, groups, users, and clients in Keycloak.

ViNO Keycloak Roles and Groups

ViNO Keycloak roles each have unique permissions that apply to users assigned to a group or to multiple groups.

- **Roles** are permission-centric. Roles apply permissions to users.

- **Groups** are user-centric. They are a collection of users. Use groups to manage users.

Menu options differ depending on the role you are assigned. For example, a user assigned only the Operator role cannot view the **Service Manager**, **Activate a Service**, or **Application Settings** menus.

ViNO provides four roles that correspond to different permissions. Table 1 defines the roles and their permissions.

Table 1. ViNO Keycloak Roles and Permissions

Keycloak Role	Permissions
administrator	- Change settings in Settings Management. - View service details on the homepage.
designer	- Create and modify flows in Service Manager. - Activate services. - View Settings Management, but cannot edit the screen. - View service details on the homepage.
provisioner	- Activate and deactivate services. - View Settings Management, but cannot edit the screen. - View service details on the homepage.
operator	View service details on the homepage. This role is read-only.
user	Required role that provides basic access permissions to ViNO. **Note:** All users must be assigned this role in addition to at least one of the other four roles.

Table 2 provides a matrix of task-to-role permissions.

Table 2. Keycloak Task-to-Role Permissions

Task	Description	administrator	designer	provisioner	operator
View Main Menu		✓	✓	✓	✓
View Service Manager		—	✓	—	—
View Service Activation Menu		—	✓	✓	—
View Application Settings Menu		✓	✓	—	—
View Settings Management Menu		✓	✓	—	—
View User Management Menu		✓	—	—	—
View Help Menu		✓	✓	✓	✓
View Installed Docker Containers Details		✓	✓	✓	✓
View Web Service Documentation		✓	✓	✓	✓
GET /rest/services	Returns a list of registered ViNO services.	—	✓	✓	—
GET /rest/services/{serviceId}/template	Returns a template for activating the ViNO service with the given service ID.	—	✓	✓	—
POST /rest/services/{serviceId}/activate	Activates a ViNO service with the given service ID. Requires the template for the same service to be provided as the POST body.	—	✓	✓	—
GET /rest/services/{serviceId}/status/{jobId}	Returns the status of a service activation using the given service ID and job ID.	✓	✓	✓	✓

Task	Description	administrator	designer	provisioner	operator
GET /rest/services/{serviceId}/cancel/{jobId}	Issues a cancellation request to a currently activating ViNO service with the given service ID and job ID.	—	✓	✓	—
GET /rest/services/activationlog/{jobId}	Returns the activation log for a ViNO service with the given job ID.	✓	✓	✓	✓
DELETE /rest/services/{serviceId}/deactivate/{jobId}	Deactivates a ViNO service with the given service ID and job ID. If a deactivation flow is present in the service, it executes.	—	✓	✓	—
GET /rest/services/activated	Returns a list of all ViNO service activations.	✓	✓	✓	✓
GET /rest/services/activated/{jobId}	Returns the data for a ViNO service activation with the given job ID.	✓	✓	✓	✓
POST /rest/service/activated	Registers a ViNO service activation. This occurs automatically after a service has finished activating, and should not be called manually.	—	✓	✓	—
POST /rest/service/activated/{jobId}	Updates a ViNO service activation using the given job ID. This occurs automatically while a service is activating, and should not be called manually.	✓	—	—	—
POST /rest/service/activated/{jobId}/{visible}	Toggles the visibility of a ViNO service activation in the Service Activations table on the ViNO homepage.	✓	✓	✓	✓

Task	Description	administrator	designer	provisioner	operator
POST /rest/service/register	Registers a new ViNO service. This occurs automatically when services are saved in the Service Manager, and should not be called manually.	—	✓	—	—
DELETE /rest/service/unregister /{serviceId}	Unregisters a ViNO service using the given service ID. This occurs automatically when services are deleted in the Service Manager, and should not be called manually.	—	✓	—	—
GET /rest/settings/all	Returns a list of settings saved in Settings Management.	✓	✓	—	—
GET /rest/settings/system	Returns a list of ViNO system settings (currently unused).	✓	—	—	—
GET /rest/settings/system/{key}	Returns a ViNO system setting with the given key (currently unused).	✓	—	—	—
GET /rest/settings/group/{name}	Returns a settings group from Settings Management using the given name.	✓	✓	—	—
POST /rest/settings/group	Saves a new settings group and its contents to Settings Management. If the group already exists, the new content is merged.	✓	—	—	—
POST /rest/settings/defaults	Saves a new default settings group and its contents to Settings Management. If the group already exists, the new content is merged.	✓	—	—	—

Task	Description	administrator	designer	provisioner	operator
POST /rest/settings/replace	Saves a new settings group and its contents to Settings Management. If the group already exists, it is replaced with the new content.	✓	—	—	—
POST /rest/settings/system	Saves a new ViNO system setting (currently unused).	✓	—	—	—
DELETE /rest/settings/deleteRootGroup/ {rootGroupName}	Deletes a settings root group from Settings Management with the given root group name.	✓	—	—	—

Populating the Keycloak Realm for ViNO

To populate the Keycloak realm for ViNO, you need to add and configure a role, group, user, and client. Refer to the following sections for information on completing these tasks.

- Adding Roles in Keycloak
- Adding a Group in Keycloak
- Adding a User in Keycloak
- Adding a ViNO Client in Keycloak

Adding Roles in Keycloak

The following roles must be added in Keycloak. The roles must be added exactly as shown below for ViNO to function correctly.

- user
- operator
- provisioner
- designer
- administrator

To add roles:

1. Click on the Roles menu, and then click **Add Role**.
2. Enter **user** in the **Role Name** field.
3. Click Save to create the **user** role.
4. Repeat steps 1-3 to create four additional roles: **operator**, **provisioner**, **designer**, and **administrator**.

Adding a Group in Keycloak

Creating a group in Keycloak enables you to manage users. **Groups** are *user-centric*. They are a collection of users. For example, you may want to create a group named Administrators, which has been mapped to the administrator role. Then you would assign users to the new Administrators group to give them administrator permissions.

Note: Each ViNO group must contain the **user** role, which provides basic access permissions.

To add a group:

1. Select the **Groups** menu, and then click **New**.

2. Enter a group name in the **Name** field. Unlike roles, specific names for groups are not required.

3. Click Save to create the new group.

4. Select the **Role Mappings** menu.

5. Select roles from the **Available Roles** menu.

6. Click **Add Selected** to assign the roles to the new group. For example, you could add the **user** and the **administrator** roles to a new group. See Table 1 for a description of user roles and permissions.

Adding a User in Keycloak

This section describes how to add a new user to Keycloak.

To add a user:

1. Click the **Users** menu, and then click **Add User**.

2. Enter the new username in the **Username** field.

3. Change the **Email Verified** setting from Off to On to disable sending an email to the new user.

4. Click Save to save the new user.

5. Click the **Credentials** tab to configure a temporary password for the new user.

6. (Optional) Change the **Temporary** setting to Off to disable requiring the new user to change the default password at login.

7. Enter a password, confirm it, and click **Reset Password** to configure the new password.

8. Click the **Groups** tab, and then select the new group (that was previously created) from the **Available Groups** menu.

9. Click Join to add the new user to the selected group.

Adding a ViNO Client in Keycloak

Adding a client to Keycloak enables ViNO to request Keycloak to authenticate users.

To add a client:

1. Click the **Clients** menu, and then click Create.

2. Enter **vino-api** in the **Client ID** field, and then click Save to create the **vino-api** client.

3. Under the **Access Type** drop-down, select **Confidential**.

4. Type ***** in the **Valid Redirect URIs** field and in the **Web Origins** field, then click Save.

5. Click the **Credentials** tab to view the generated client secret.

6. Copy the value in the vino-api client **Secret** field for use in step 3 in Initializing ViNO.

Initializing ViNO

To initialize ViNO:

1. Run the command **./initialize.sh** using the command line in the /opt/vino/vino-docker directory.

2. Press Enter when the script prompts for Vino Name, Default route, and Keycloak host.

3. When the script prompts for the Keycloak client secret, paste the **vino-api** client secret that you copied in step 6 in Adding a ViNO Client in Keycloak, and then press Enter.

4. Press Enter for the remaining prompts. ViNO completes the initialization.

5. The next prompt enables you to add a signing certificate to the ViNO set of accepted CA certificates to securely communicate with upstream and downstream services: **Would you like to add an additional Root CA Certificate to the ViNO Node Runtime? (Yes/No)**

   Select:

   - **Yes** to add a signing certificate to facilitate SSL communications (such as, HTTPS or LDAPS).
   - **No** to bypass this option.

6. When the initialize.sh script has finished running, open a browser and enter the IP address of your ViNO host in the URL bar. This step navigates to the ViNO Login screen.

Logging in to ViNO

To log in to ViNO:

1. In the **Authentication Required** screen, click Authenticate.

2. In the **Log In** screen, enter the username and password that you created when generating the Keycloak realm, then click Log In. ViNO displays a blank homepage as shown below.
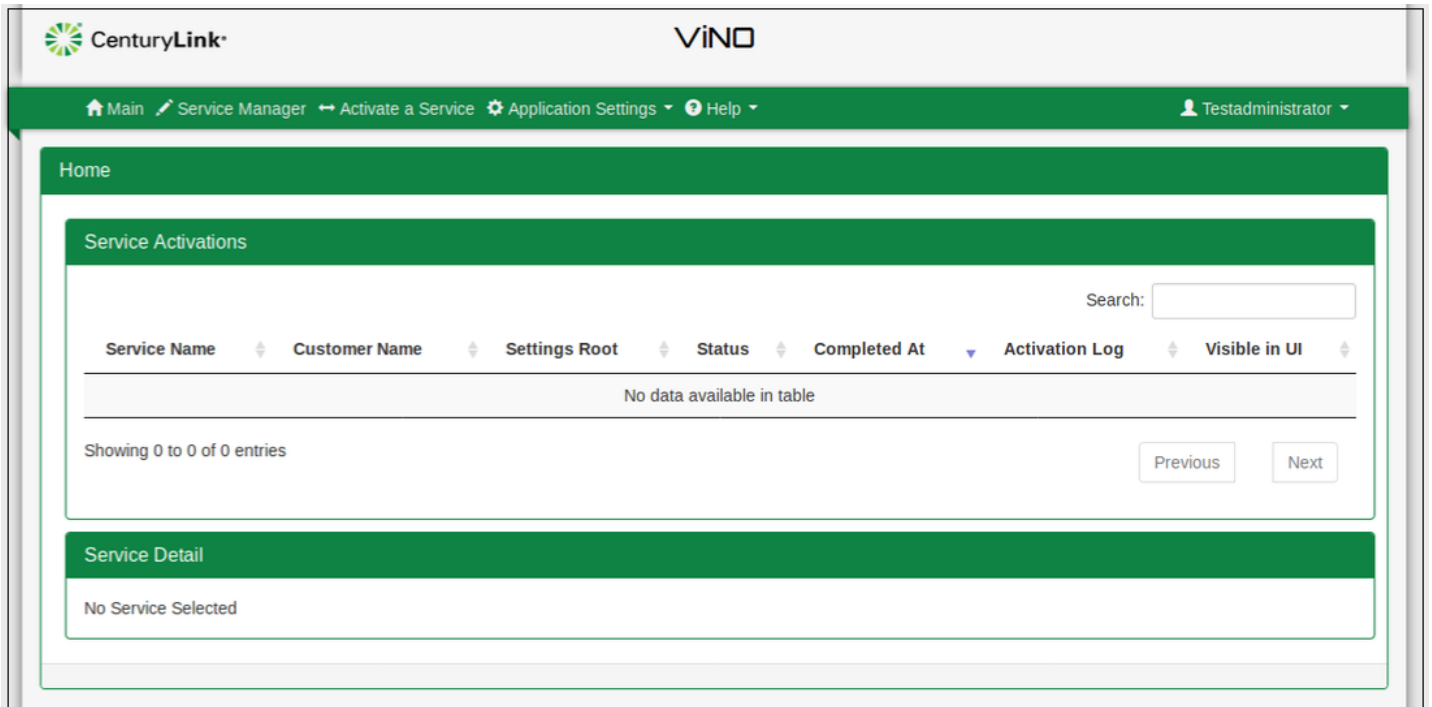
Caution: To avoid being logged out after 10 minutes while working in the Service Manager, you must open the Service Manager in a separate window. If you only have the Service Manager open, you are logged out of ViNO after 10 minutes with no warning. Even after being logged out, it appears that you can work and save in the Service Manager, but your changes are not saved.

3. Refer to the *Virtual Network Orchestrator (ViNO) User Guide* for information on using ViNO.