**Role Management in TopBraid Suite**

TopBraid Suite 4.4

1. Installation and Admin Setup 2

1.1 Access to Server Administration Page 2

1.2 AdministratorGroup 2

2. The Role Management User Interface 2

2.1 Defining New Groups 3

2.2 Defining Asset Permissions 3

2.3 Associating Roles with Groups 4

3. Getting Started 5

4. Asset Permissions 7

4.1 Asset Types 7

4.2 Defined ANY Asset Types 7

4.3 Access Types (CRUD+E) 7

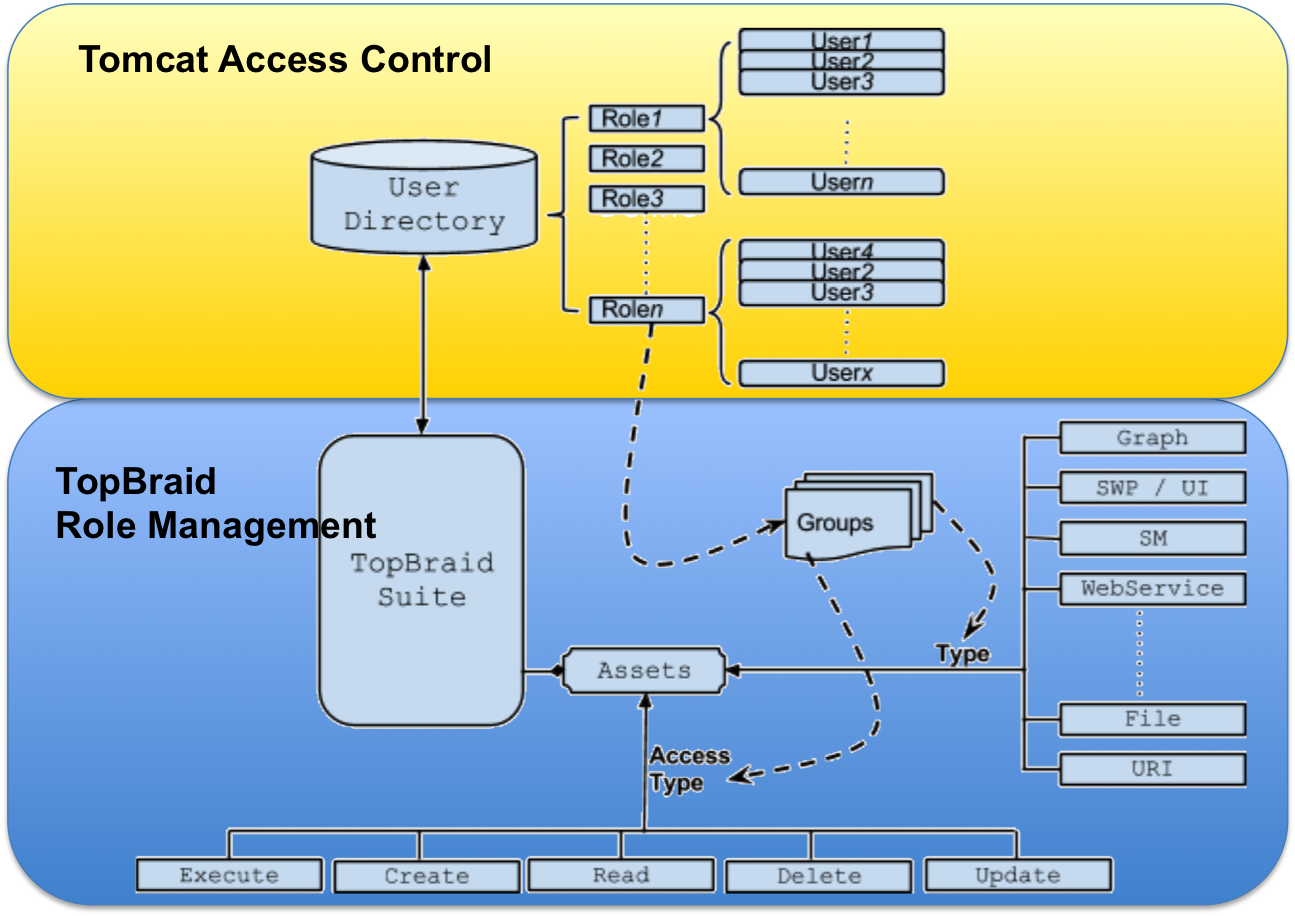
5. Suggested setup for TopBraid EVN 8

6. TopBraid EVN User Roles 9

**Introduction**

The TopBraid Role Management utility is found in the Server Administration page for all TopBraid server products. It provides a way to manage access controls to TopBraid Assets such as graphs, files, Eclipse/Equinox projects, Web services, etc. Access control Groups are defined in Role Management to define access rights to Assets and associate the Groups to Roles defined in Tomcat Realms, such LDAP, and LDAP/MS Active Directory, and Tomcat’s in-memory user database (conf/tomcat-users.xml).

The overall access control design is depicted in the diagram below. Note that Roles and user associations with Roles are defined outside of TopBraid by Tomcat Realm administration, such as LDAP/MS Active Directory.



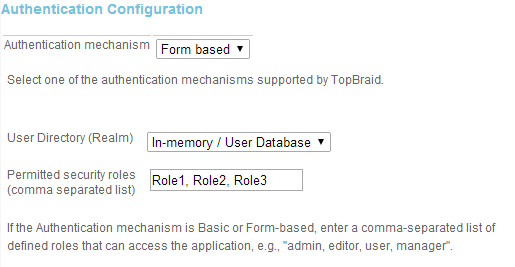
# Installation and Admin Setup

Initial role setup occurs during installation. Please refer to the Installation guide for the TopBraid Suite product you are using (EVN, TBI, TopBraid Live, etc.) – see for example http://www.topquadrant.com/docs/tbl/42install/installation.html.

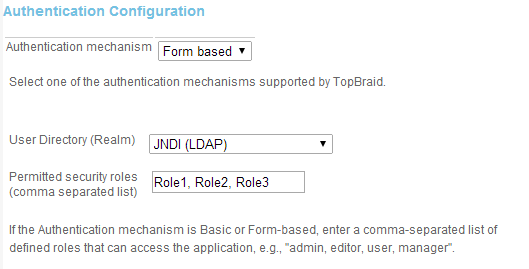
For a Role to be used in a TopBraid server, the role must:

1. Be defined in a Tomcat Realm, such as LDAP, and
2. Appear in the Permitted security roles setup of the TopBraid (which define entries for security-constraint tags in the application’s web.xml).

To define Roles in the Permitted security roles, enter a comma-delimited list of Roles in the TopBraid Deployment Descriptor Configuration Page during installation. The following figures show the most common setups for LDAP and in-memory database (conf/tomcat-users.xml), where the role names in either case are Role1, Role2 and Role3. Note that these roles are defined in LDAP/Tomcat and are not editable from within TopBraid.



In-memory user database (e.g. conf/tomcat-users.xml)



LDAP User Directory

## Access to Server Administration Page

Once installation is completed, the Server Administration page can be access by users associated with a Role with access to the asset ANY\_ASSET. The Role Management page is found at Server Administration > Role Management.

This setup replaces the Superuser setting in versions of TopBraid Suite prior to version 4.4.

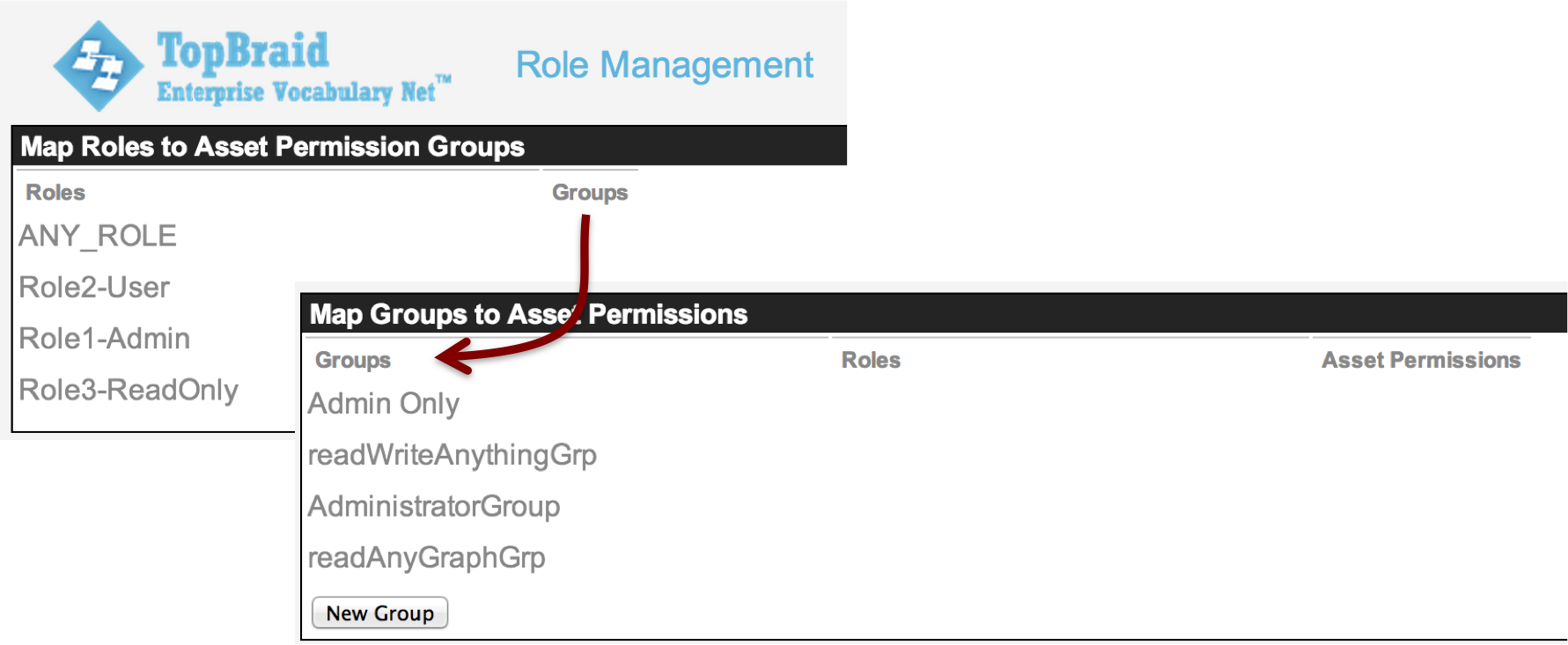
## AdministratorGroup

TopBraid Role Manager includes a default administrator group, named AdministratorGroup, which allows access to all assets. The group must be defined for at least one Role to prevent being locked out of the system. By default, all Roles are defined to have this group.

To remove AdminstratorGroup for a specific role the user must define another role for the group. If AdministratorGroup is defined for at least one other role it can be removed (deleted) from a given role. However, if no other roles are associated with AdministratorGroup, it cannot be deleted from a role.

# The Role Management User Interface

The Role Management UI consists of two views: Role Management and Group Management. To navigate between them, click on the column name as shown in the following figure.



Role Management Views.

Definitions for concepts appearing in this user interface are as follows:

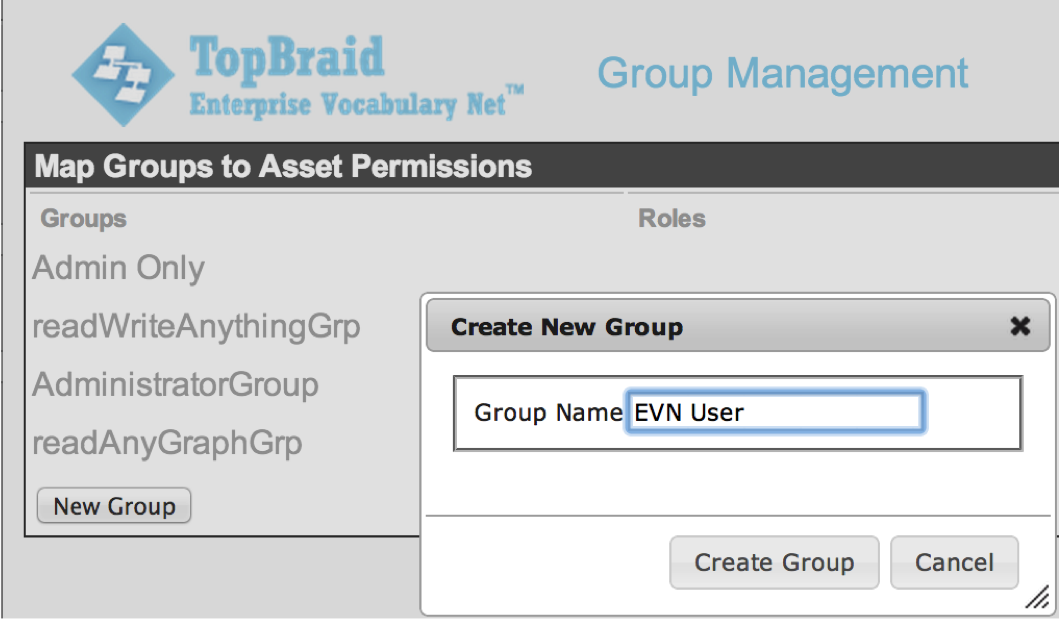
**Roles:** Roles are defined in LDAP/Tomcat and cannot be edited in this interface – a systems administrator will need to modify these using LDAP/AD, tomcat-users.xml, etc. A Role can be associated with one or more Groups.

**Groups**: A group is defined within TBS and it identifies a group of assets, their respective access types and role/s defined in a user directory that it maps to.

**Asset**: An asset is an instance of a resource that can be uniquely identified within TBS. Example of an asset is graph, SM script, an exposed Web service, a file etc. The approach controls access to individual asset or a group of assets.

**Asset Permissions**: Each asset type allows a set of asset permissions. These permission types are **C**reate, **R**ead, **U**pdate, **D**elete and **E**xecute. E.g. for a graph CRUD access can be specified, for a SM script CRUD+E are relevant whereas for an exposed Web service only E access is relevant.

## Defining New Groups

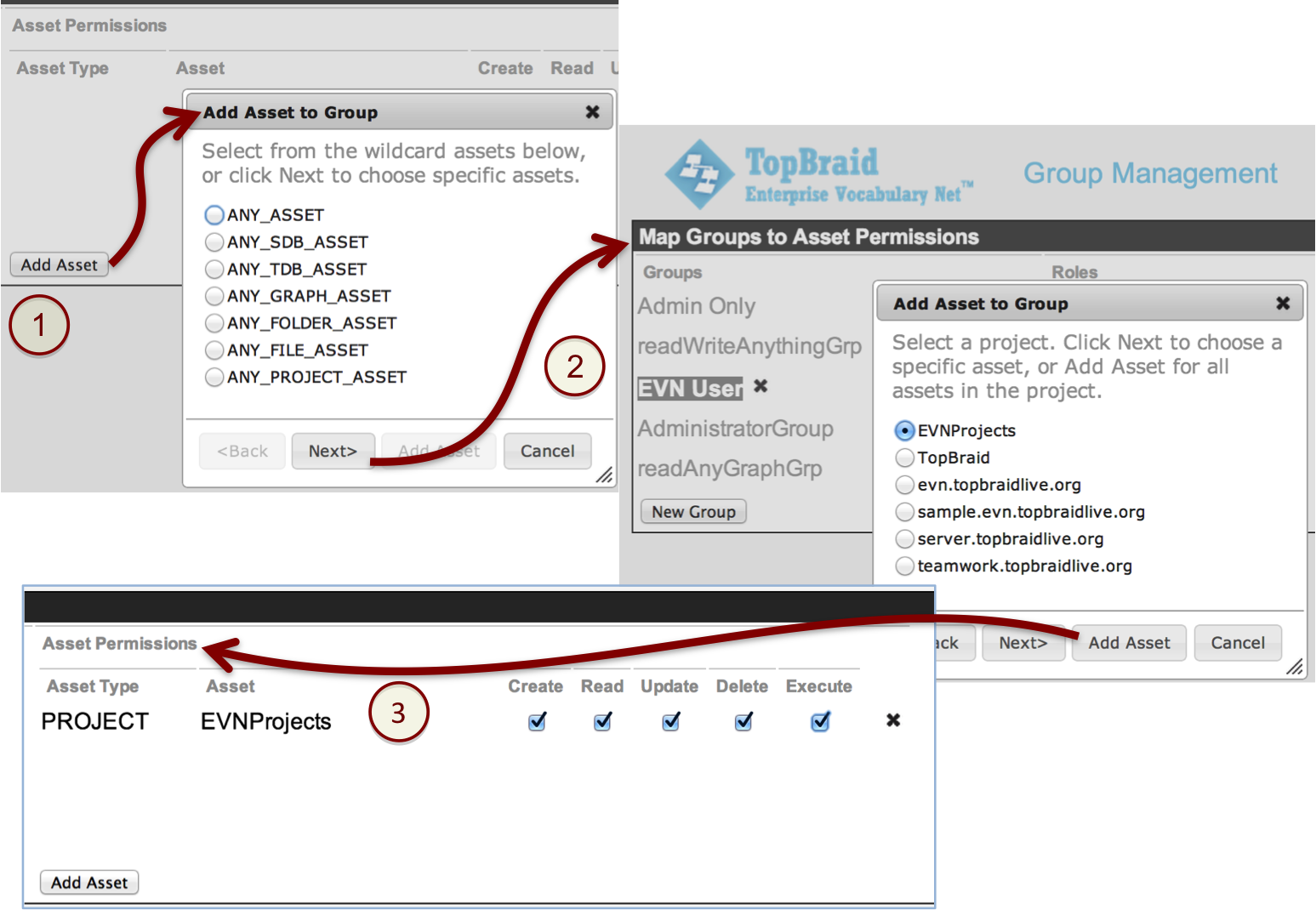


To define a new group, click on the Groups column and click on the Add Group button. Provide a name as shown in in the figure. Groups can be associated with one or more Asset with access permissions

## Defining Asset Permissions

Asset Permissions are defined with the Add Asset button on the Group Management view (1 in the figure). Asset Types are defined in Section 4. You can choose a listed wildcard asset type OR click ‘next’ to choose from a list of specific assets. For example, click “Next>” and the full set of Eclipse/Equinox projects from the TopBraid workspace will be displayed (2 in the figure). In this example, which corresponds to a TopBraid EVN setup, the default EVNProjects project name has been chosen. Upon choosing the asset type the Group Management view will display a set of permissions corresponding to the aforementioned CRUD+E asset permissions. In this figure all asset permission have been chosen – meaning that any role assigned to the group EVN User has access to all graphs and Web services defined for the project “EVNProjects” (3 in the figure).

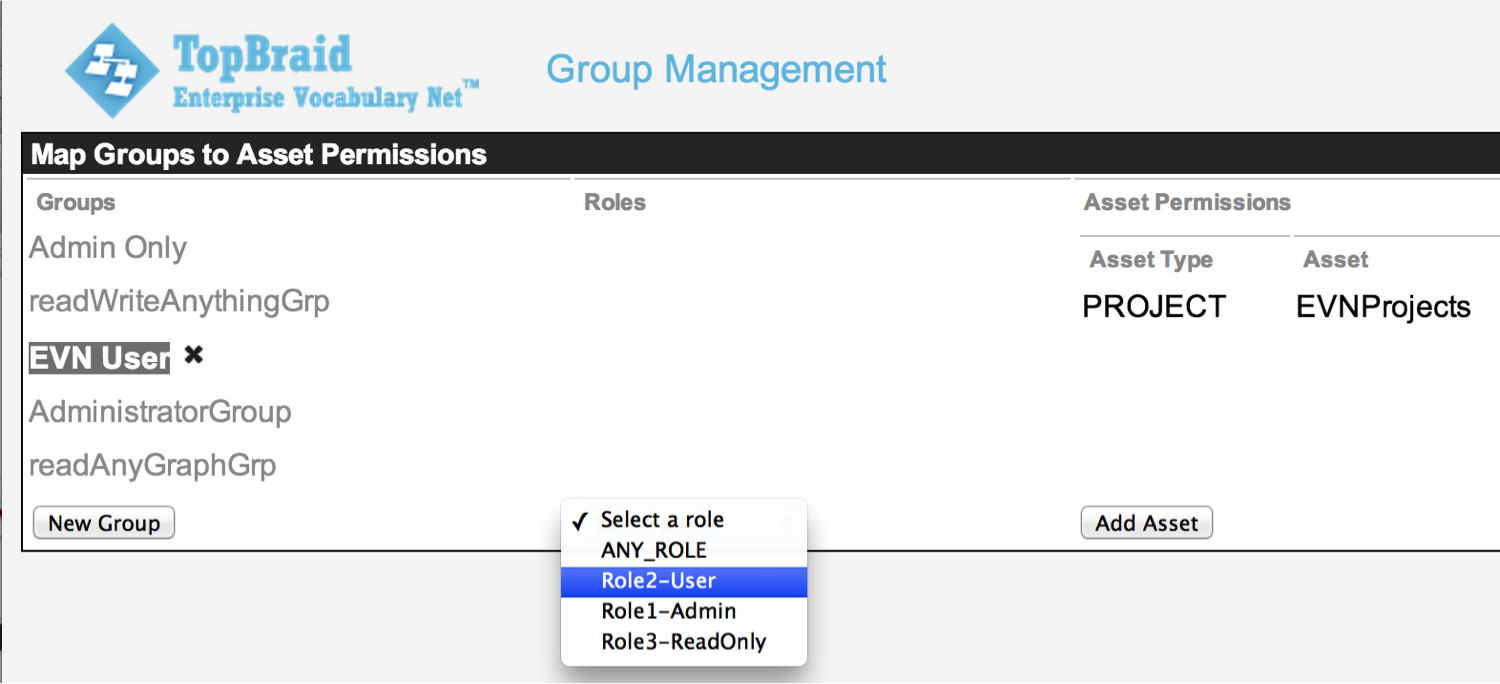
This corresponds to a suggested setup for TopBraid EVN where all users have access rights so that users with EVN “manager” roles (EVN User Roles) are free to define EVN-based access rights (see Section 5).



Creating Asset Permissions.

## Associating Roles with Groups

Once a Group is defined, it can be associated with a Role. This can be accomplished from either the Group Management or Role Management view. In the Group Management view, click on the Group and choose the Add Role button. In the Role Management view, click the Role and add the Group. Examples of both are shown in the following figures.



Role-to-Group association in Group Management.

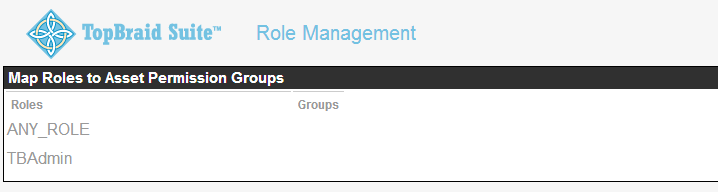
# Getting Started

This new feature replaces previous ‘Superuser’ functionality, allowing a set of users identified by a role access to full or limited administrative functions.  Generally, roles are defined in a User Directory such as those defined in LDAP and Tomcat’s in-memory user database.

Choose **Role Management** from the Administrative Functions Menu.

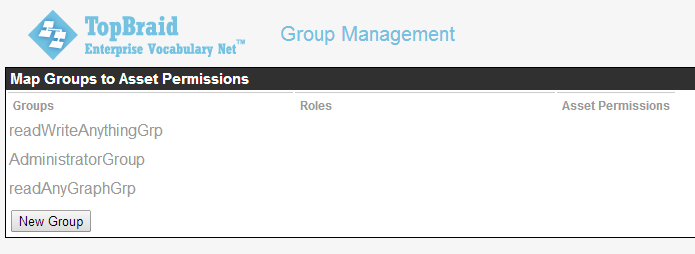


Choose **Groups** from the Role Management Menu

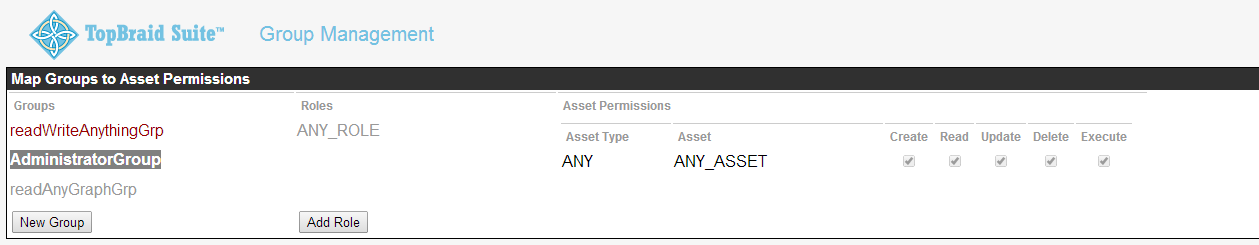


AdministrationGroup is a system group that allows for administration access. Users belonging to role(s) assigned to the AdministrationGroup will have administrative access.

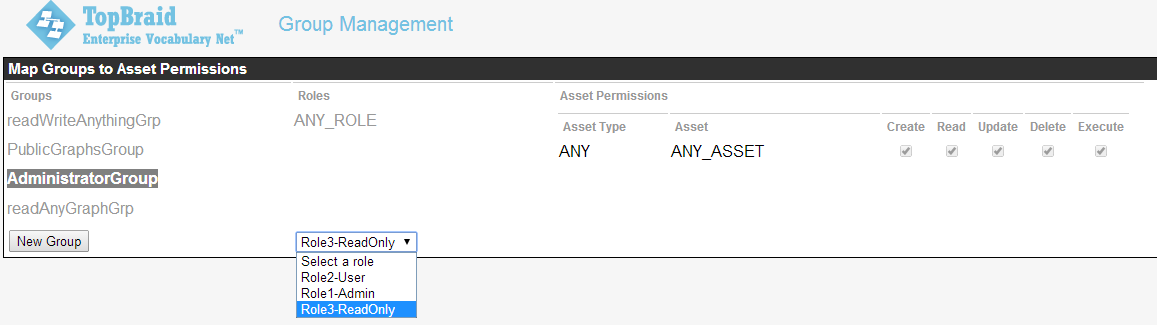
Choose **AdministratorGroup** from the Group Management Menu



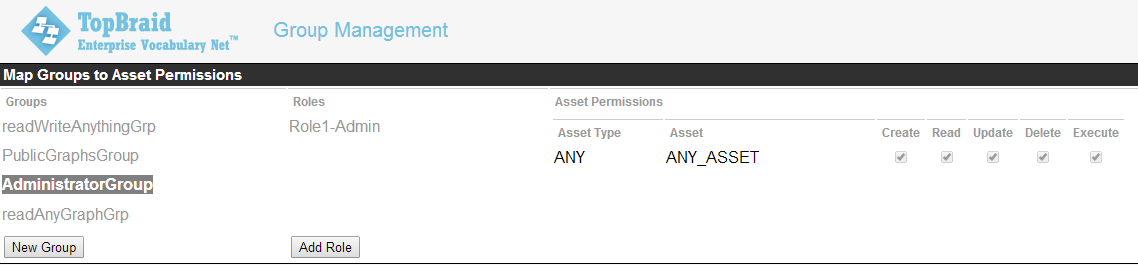
Choose **AdministrationGroup**



Choose **‘Add Role’** and choose name from the drop-down.

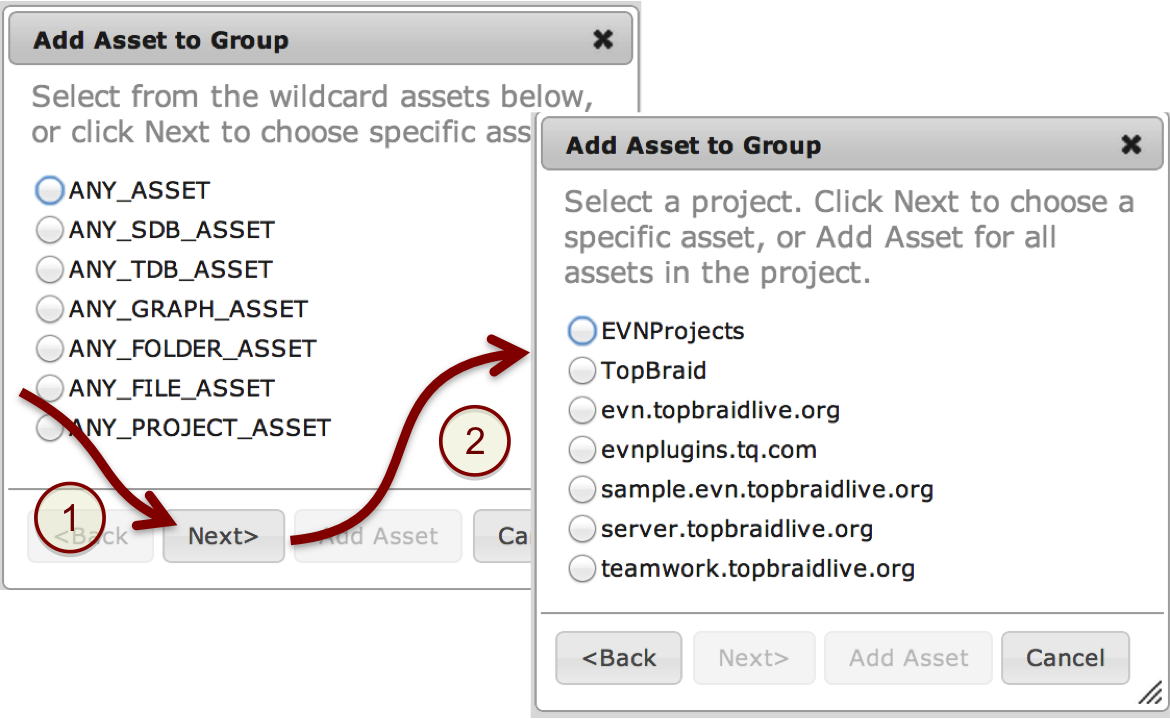


ANY\_ROLE is a system defined role which identifies all the roles allowed access to the application. If you do not want to give administrative access to all the users then delete ANY\_ROLE from the AdministrativeGroup

**Delete** ANY\_ROLE

# Asset Permissions

One or more asset definition is associated with each Group. The asset definition consists of an asset type, either PROJECT or ANY, an Asset, and the CRUD+E access type definition. The choices are described in the following sections.



## Asset Types

The two Asset types are PROJECT and ANY. To create a PROJECT type click “Next>” with no ANY radio buttons chosen (see figure). A list of Eclipse/Equinox projects in the workspace will appear. A PROJECT asset can be defined for only one project.

To define a ANY asset type, choose a radio button as shown in the left-hand window of the figure.

## Defined ANY Asset Types

The defined ANY asset types are as follows. These are defined to allow administrators to define the different kinds of assets available in TopBraid Suite.

**ANY\_ASSET:** Any asset defined by TopBraid.

**ANY\_SDB\_ASSET:** Any SDB data connector (.sdb file).

**ANY\_TDB\_ASSET:** Any TDB data connector (.tdb file).

**ANY\_GRAPH\_ASSET:** Any named graph in the TopBraid workspace. This is a superset of ANY\_SDB\_ASSET AND ANY\_TDB\_ASSET.

**ANY\_FOLDER\_ASSET:** Any folder in the TopBraid workspace.

**ANY\_FILE\_ASSET:** Any file that is not a graph, such a text, Excel, XML, etc.

**ANY\_PROJECT\_ASSET:** Any project in the TopBraid workspace. This differs from the PROJECT asset type in that this refers to all Eclipse/Equinox project in the workspace.

## Access Types (CRUD+E)

**Create:** Group members can create new assets.

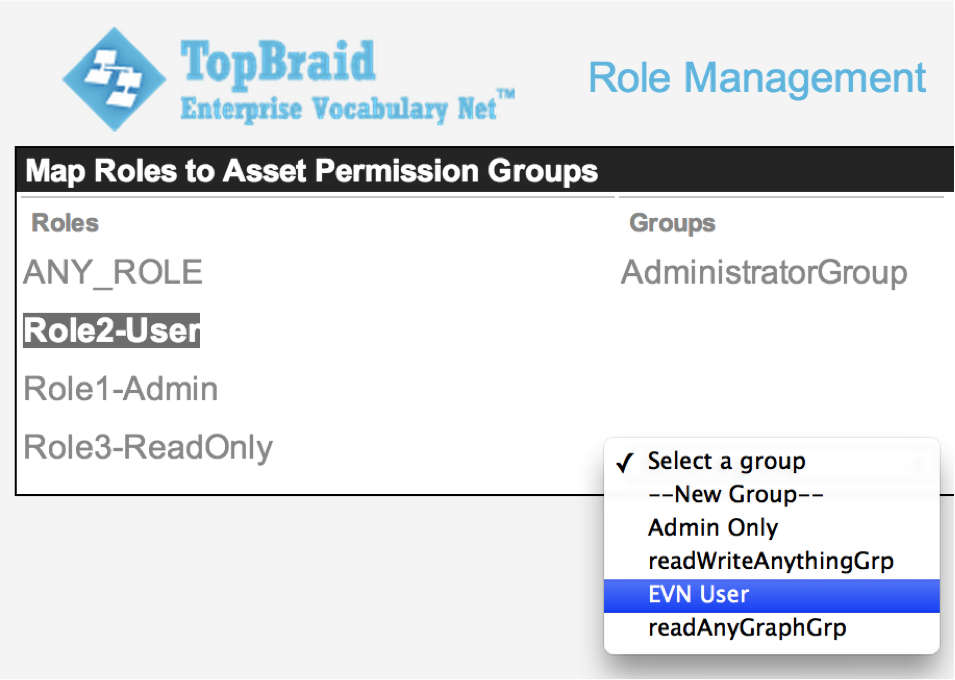
**Read:** Group members can read assets.

**Update:** Group members can update/modify assets.

**Delete:** Group members can delete assets.

**Execute:** Group members can execute server-side scripts.

# Suggested setup for TopBraid EVN



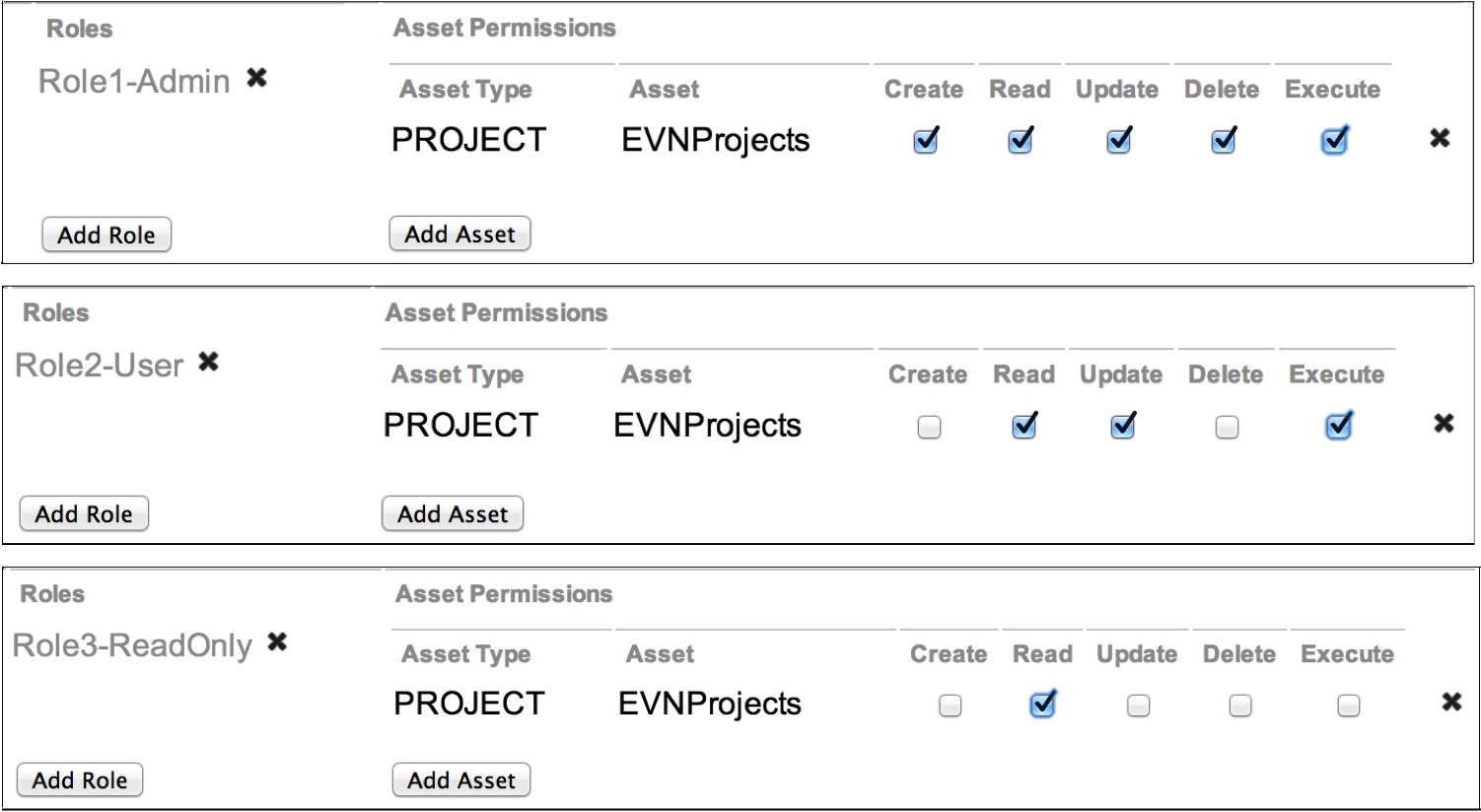
Role-to-Group association in Role Management.

TopBraid EVN supports features to easily manage EVN Projects (vocabularies, ontologies, tag sets, etc.) on a per-project basis. This is accomplished by defining user id’s or roles to EVN User Roles, ‘manager’, ‘editor’ and ‘viewer’ that can be edited by the manager of an EVN Project (for more, see http://download.topquadrant.com/evn/44doc/userguide.html#capabilities-and-assignment-of-user-roles--viewer--editor--and-manager).

Given the use of EVN User Roles, the best practice is to define a small set of group with access for the Eclipse/Equinox project that contains connectors to EVN data. One approach is to provide all EVN users (via their roles) full CRUD+E access. This is depicted in Section 2.2, where the Eclipse/Equinox project is the default “EVNProjects”.

Another approach is to define access groups for Admin, general user (read/update/execute), and read-only user. Start by creating three groups, named “EVN Admin Group”, “EVN User Group”, and “EVN Read-Only Group” in this example. Note the access types for each.

In this setup only users in Role1-Admin can create and delete EVN Projects. Users in the Role2-User role will be able manage, edit, and view EVN Projects, but not create or delete EVN Projects. Depending on the User Roles assigned in EVN, any user in Role1-Admin and Role2-Admin can be assigned ‘manager’, ‘editor’ or ‘viewer’ EVN User Roles. Users in the Role3-ReadOnly role can only read EVN projects. If a Role3-ReadOnly user is given ‘manager’ or ‘editor’ EVN User Roles, attempts to edit or delete data in an EVN Project will result in an exception and the operation will not be allowed.

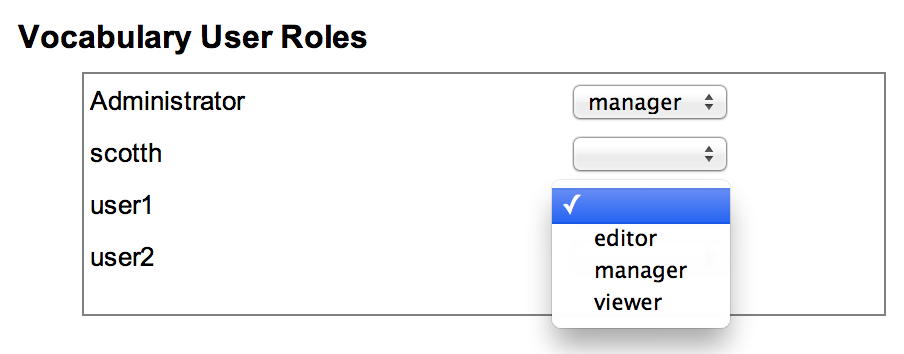


Users in multiple roles will be given the union of the assigned Group access rights.

# TopBraid EVN User Roles

The previous chapters in this document address role management for a TopBraid server workspace, such as TopBraid EVN, Insight, or Live. In addition, TopBraid EVN allows users to control access on individual EVN Projects. This provides flexibility to assign manager, editor, and viewer roles to each individual project without needing to get an LDAP administrator involved. These roles are described in the EVN Guide to Enterprise Vocabulary Net found on the EVN Home page. Navigate to the User Guide and the Chapter titled “Capabilities and assignment of EVN user roles: Viewer, Editor, and Manager”.

Once the Role Manager has been used to define Asset Permissions, any user with create privileges for the EVN project will be able to create new projects (vocabularies, ontologies, tag sets, custom projects). For example, a user in the Role1-Admin role will be able to create an EVN Project. The creator of a project is automatically given the Manager role for the project. They are then able to assign EVN User Roles to other users, as shown in this figure, including assigning others to the Manager role.



Assign EVN User Roles for an EVN Vocabulary

Currently, the list of users is drawn from a cache of users that have been authenticated by The Web container (Tomcat). This means users will need to log in once before appearing on this list of users. Future versions of TopBraid will have the ability to query LDAP for the users meeting the security-constraint criteria defined in web.xml, as well as the ability to assign roles to EVN User Roles.

Also note that access controls set in the EVN User Roles are superseded by the Asset Permissions. I.e. if a user is assigned an EVN Viewer role, but lacks the Read access in Asset Permissions, then the user will not be able to view the vocabulary.