RoleType

Description

A role in the extended Role-Based Access Control (RBAC) sense. The roles specify privileges that the user (or other object) should have.

The role may "grant" accounts on resources, attributes and entitlements for such accounts. The role can also assign organizational units, other roles or various IDM objects that can be assigned directly to user. From this point of view the role is in fact just a named set of assignments.

The roles form the basic building block of midPoint's extended role-based access control (RBAC) mechanism. It defines what rights (e.g. accounts) should be given to user, how they should look like (attributes) and what groups or native roles to assign to them (entitlements).

Roles can also specify user authorizations to access specific parts of midPoint. This is used to implement fine-grained authorization mechanism. When combined with organizational structure it forms a delegated administration mechanism.

Roles can also be conditional, i.e. applicable only if a specific condition is true. Roles can be parametric, e.g. the expressions inside the role can use parameters that were specified at the time when the role was assigned (as opposed to parameters defined when the role was defined).

RoleType, as all the midPoint objects, is a subtype of ObjectType. Therefore it has all the basic properties such as `name` and `description`.

RoleType is also a focal type. Therefore it can behave as a "focus" (authoritative object) in midPoint synchronization. If this mechanism is used to apply a role to another roles (or other non-user object) then it becomes a meta-role.

SchemaDoc

Following links can be used to get full an authoritative description of the role object schema:

Relase	SchemDoc link
Latest stable	RoleType
Development	RoleType

Important Items

User object contains following frequently used items:

Property	Type	Description
roleType	string optional	Type of a role, usually denotes a "layer" or "purpose" of the role. Such as "business", "IT", "asset", etc. This field has no special meaning in the IDM computation logic. Its purpose is to organize roles for presentation (GUI) and management. Therefor it is assumed that the values of the roleType will be an enumeration. Examples: *application, business*, *it*, *technical*, *asset*
displayName	PolyString optional	Human-readable name of the role. It may be quite long, container national characters and there is no uniqueness requirement. It is used if the "name" property contains a code that is not entirelly user-friendly.
assignment, inducement	AssignmentType optional, multi	See Assignment and Assignment vs Inducement.
authorization	AuthorizationType optional, multi	Set of role authorizations. Authorization define fine-grained access to midPoint objects and system functionality. The authorizations that are defined in a role apply to all users that have this role assigned (such user is a "subject" of the authorizations). See Authorization
riskLevel	string optional	Indication of the level of risk associated with the persissions that this role assigns. This may be a numeric value, textual label are any other suitable machine-processable indication.
ownerRef	ObjectReferenceType optional	Owner of this role. The owner is a person (or group) that is responsible for maintenance of role definition. This reference may point to object of type UserType of OrgType.

approverRef	ObjectReferenceType optional, multi	Approvers for this role. The approver is a person (or group) that approves assignment of this role to other users. This reference may point to object of type UserType of OrgType.
condition	MappingType optional	The role is applied only if the condition is evaluated to true. The condition is used to define conditional roles.
policyConstraints	PolicyConstraintsType optional	Set of governance, risk management, compliance (GRC) and similar policy constraints that influence the identity model. (since midPoint 3.1.1)

Full list of items can be found by using the SchemaDoc links above.

See Also

- UserType
- OrgType
- Assignment vs Inducement
- Roles, Metaroles and Generic Synchronization