1. Introduction

This document describes the concept of fine-grained RBAC (Role-based Access Control) feature, which is a new and advanced feature in NetScaler MAS (Management and Analytics System) to provide enhanced security, that is, by controlling the user access at a granular level and also the common implementation scenarios of fine-grained RBAC in NetScaler MAS.

2. Overview

As NetScaler MAS manages, monitors, and provides visibility into analytics data of all Citrix network devices. Hence, there is need a for enhanced security to reduce the risk of unauthorized users from viewing or performing operations on analytics data. Controlled access to data and operations is a key element of system security.

3. Security in NetScaler MAS

NetScaler MAS uses a RBAC model of access control mechanism in which a layer of roles exists between users and access privileges. This ensures that users have sufficient privileges to perform various system operations. RBAC offers a simple and manageable approach to access management (User role management), which is less error-prone than individually assigning permissions to users.

3.1 RBAC Model

The concept of RBAC is to create a set of permissions and assign these permissions to a user or group. In RBAC model, each user is given one or more roles. Each role is given a specific set of privileges and authorizations. Thus, with the help of these privileges, only limited access is provided to users, therefore, increasing the level of security. The following figure depicts the typical RBAC model in an IT industry.

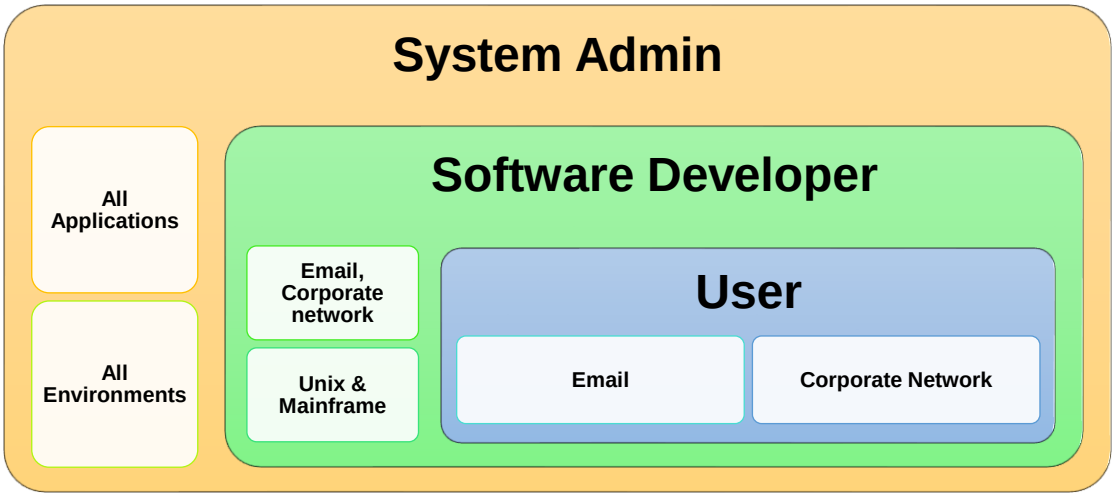

Figure 1 RBAC Model in an IT Industry

In this model, System admin has a full accessibility over all applications and environments. Software developer has a limited accessibility, only few applications and few environments. Normal user has a closed accessibility, only applications and no environments.

3.1.1 Coarse-Grained RBAC Approach

Coarse-grained RBAC approach is a high-level authorization mechanism where NetScaler MAS admin has only less control over unauthorized users and access management.

The following are the features of coarse-grained RBAC approach:

- Authorization – Access is governed based on roles and instance IPs associated to the group to which a user belongs.
- User or a group can have only two predefined roles, that is, either `admin` or `read-only` role.
- Same role is applied across all the available features of NetScaler MAS
- Same permissions are applied for all the available features of NetScaler MAS.

Limitations:

These above features restrict the NetScaler MAS admin in handling certain scenarios, for example, when a user needs to access only specific environment, job configurations, or when a user needs a custom role to perform an operation. In such cases, a much more flexible and advanced authorization design is required which gives the way forward for *Fine-grained RBAC* approach.

3.1.2 Fine-Grained RBAC Approach

Fine-grained RBAC approach is an advanced or granular level authorization mechanism where NetScaler MAS admin has more control over unauthorized users and access management.

The following are the features of a fine-grained RBAC approach:

- Authorization – Access is governed based on roles, features or even resources associated to the group to which a user belongs.
- User or a group can have the following predefined roles and with associated permissions.

Role	Permission
Admin	`read, create, update, delete, execute`
Creator	`read, create, update`
Executor	`read, execute`
Observer	`read`

- Support for creating custom permissions – Same or different permissions can be applied for all the available features of NetScaler MAS.
- Support for creating custom roles – Roles with different combinations of permissions are created based on user preferences.
- Support for configuring feature specific resource properties (specific entities or functions) upon granting required permissions.

a. User can modify the roles or permissions for the following features in NetScaler MAS:

   - Applications
   - Style Books
   - Instance operations
   - Configuration Jobs
   - Configuration Audit
   - SSL Dashboard
   - Events
   - Analytics
   - Orchestration
   - System Administration

b. User can be granted roles or permissions for the following resources in NetScaler MAS:
   - Instance IP/hostname/sysname
   - Instance Type
   - Instance group
   - Application Name
   - Config Job Name
   - Certificate Name
   - Style books (TBD)

- Provides a flexible design of authorization for new or upcoming features of NetScaler MAS.
- Support for both local and external authentication servers,
- Support for Multi-Tenant deployment – Tenants and Tenants groups can be created with the required roles and permissions of user preferences.

3.2 Summary of Functional Change

The following table describes the functional changes that exist between coarse-grained and fine-grained authorisation (RBAC) approaches in NetScaler MAS.

Functions	Fine-grained RBAC	Coarse-grained RBAC
Number of Pre-defined roles	Four roles (`Admin, Creator, Executor, and Observer`)	Two roles (`Admin and Read-only`)
User-defined roles	Yes	No
Support for feature or resource-based access	Yes	No
Flexible design for adapting new feature	Yes	No
Support for various Authentication methods (Local and External)	Yes	No
Multi-tenant support	Yes	No

4. Common Deployment Scenarios for Fine-grained RBAC

4.1 Use Predefined Roles or Create Custom Roles Based on Need

Fine-grained RBAC approach helps users to create custom roles or use additional pre-defined roles based on user preferences.

Example

ABC company has the following 4 different admins with unique permissions to perform various operations

ABC Admins	Permission	Accessibility Level
Super	`read, create, update, delete, execute`	Full
Observer	`read-only`	Level-1
Creator	`create, update, read`	Leve-3
Executor	`read and execute`	Level-2

In this example, only Super user has the full access over system operations, whereas, other admins have their role-specific (limited) permissions to perform operations. Thus, fine-grained RBAC provides the accessibility in a more controlled manner.

4.2 Grant Accessibility for Specific Resource

Fine-grained RBAC approach helps users to control accessibility based on resources of user preferences. It provides a granular RBA framework across various resources such as instances, applications, certificates, configuration jobs, and so on.

Example

Tony and Bravo are two different admins in an ABC company. Tony is the super admin and Bravo is an application admin. Both have different levels of access and permissions. Tony must ensure that Bravo can access only those resources which are under his umbrella. For example, Bravo must be able to access only specific applications (virtual servers) and only specific configuration jobs.

ABC Admins	Permission	Accessibility Level	Resource accessibility
Super	`read, create, update, delete, execute`	Full	CF1, CF2, CF3, all applications
Application	`read, create, update, and execute`	Level-3	CF2, Virtual Server

In this example, Tony as a super admin has full access over resources: Can perform operations on all the applications and various configuration jobs (CF1, CF2, and CF3). Bravo as application admin has only limited access over resources, that is, he can access only virtual server application, and can perform operations only on CF2 configuration job.

4.3 Grant Accessibility for Specific Feature

Fine-grained RBAC approach helps users to control accessibility based on features that are assigned to different users with unique permissions. It provides a granular RBA framework, such as unique permissions across various features of MAS such as Certificate Management, System Administration, Orchestration and so on.

Example

Tony and Garry are two different admins in an ABC company. Tony is the super admin and Garry is the security admin. Tony must be able to grant access to various admins based on their job profile. Tony must ensure that Garry must have complete access (read, create, update, delete, execute) for SSL Certificate management and monitoring operations, but must have read only access for Orchestration or system administration operations.

ABC Admins	Permission	Accessibility Level	Feature accessibility
Super	`read, create, update, delete, and execute`	Full[1]	SSL Certificate Management, Monitoring, Orchestration, and System Administration
Security	`read, create, update, delete, and execute`	Full[2]	SSL Certificate Management, Monitoring
	`read-only`	Partial; Level-1	Orchestration, System Administration

Note:
1. Full access is available over all features for the user
2. Full access is provided only for those features that are assigned to the user.

In this example, Tony has full access (full permissions) over all the MAS features (SSL Certificate Management, Monitoring, Orchestration, and System Administration), whereas Garry has full permissions only for SSL (Secure Sockets Layer) Certificate Management and Monitoring, and only `Read-only` permission for Orchestration and System Administration features of MAS.

4.4 RBAC Support for All Users–Local or External or Multi-Tenant Environment

Fine-grained RBAC approach provides a more flexible design of authorization to all types of users, that is, local and external users. This approach also handles the accessibility requirements of various tenants available in multiple environments.

Example

In NetScaler MAS, users can be locally authenticated or externally authenticated (authentication takes place through an external server, such as RADIUS, LDAP, and so on.).

In this example, both the users (local and externally authenticated) are given required permissions and privileges based on their role, required features, or resources available in NetScaler MAS. Fine-grained RBAC settings are enabled in such a way that all authenticated users are benefited irrespective of the authentication methods adopted.

5. Glossary

LDAP Lightweight Directory Access Protocol

MAS Management and Analytics System

RADIUS Remote Authentication Dial-In User Service

RBAC Role-Based Access Control

SSL Secure Sockets Layer