Role-Based Administration (RBA)

https://campus.barracuda.com/doc/4259970/

Introduction

Role-Based Administration (RBA) restricts access to system resources based on the roles assigned to users within an organization. The Barracuda Web Application Firewall is shipped with predefined roles, each with distinct operational and configuration privileges. In addition to predefined roles, the Barracuda Web Application Firewall allows you to create custom roles and define access privileges. These roles can be assigned to users to perform specific job functions. The **admin** role, by default, is assigned to the administrative user who has permission for role management.

Roles and Privileges

Roles

A role is a set of privileges or permissions for the available system resources, created for a specific job function. The **admin** role is allowed to create, modify, and delete roles. A role can be assigned to multiple users within an organization. Assigning a role to a user confers the set of privileges for the system resources included in the role definition. All users who assume that role can operate in the same environment and access the same resources. For example, an administrator assigned to the **audit-admin** role is only allowed to view logs on the system and is prevented from accessing any other objects.

Predefined Roles

The following table lists a predefined set of roles provided by the Barracuda Web Application Firewall. A predefined role cannot be modified or deleted.

Role	Description of Allowed Functions Associated with Role
admin	The super-administrator • All system operations Note: Only admin can create and assign roles
audit-manager	• Viewing Logs

certificate-manager	• Uploading certificates • Creating certificates • Uploading Trusted certificates
service-manager	• Adding a server • Creating URL ACLs • Configuring website translation rules • Adding URL and parameter profiles • Configuring traffic management rules Note: service-manager can create/delete services, add/delete service-groups
policy-manager	• Managing default and customized security policies • Modifying security policies Note: policy-manager can create/delete security policies
network-manager	• Advanced IP address configuration • Configuring SNAT and ACL's • Network troubleshooting
monitoring-manager	• View logs • Configuring email notifications • Exporting system logs, application logs and FTP access logs • Generating and scheduling reports
guest	• View all configurations Note: guest may not modify the configuration

Create a New Role

In addition to the factory shipped roles, the Barracuda Web Application Firewall enables you to create new roles. You can specify the privileges for these roles, and then assign them to users.

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **Administrator Roles** section, click **Add Administrator Role**.

3. In the **Add Administrator Role** window, enter a role name and specify the permissions for the role.
4. Click **Create Role**.

For more information, refer to the online **Help**.

Privileges

A *privilege* is an access right or permission for a system resource. Privileges are used to control access to the system. You can grant privileges to a role, and then assign the role to one or more users. There are two distinct categories of privileges:

- Object Privileges
- Screen and Operation Privileges

Object Privileges

The following table lists the key configuration objects that are classified in role-based administration:

Object	Description	Privileges
Vsites	Exhibits all Vsites to which the security groups and services are added.	Read: Enables the user to view the configuration of an object, but prohibits modifying the object. Write: Enables the user to view and modify the configuration of an object, but prohibits deleting the object. Read All: Enables the user to view and modify the configuration of all objects, but prohibits modifying objects. Write All: Enables the user to view and modify the configuration of all objects, but prohibits deleting the objects.
Security Groups	Exhibits the default and custom security groups to which the services are added.	
Services	Exhibits all services configured on the Barracuda Web Application Firewall.	
Security Policies	Exhibits the default and custom security policies.	
Authentication Services	Exhibits all authentication services such as Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS).	
API Privilege	Allows all the users having this role to access the Barracuda REST APIs.	

Screen and Operation Privileges

The Barracuda Web Application Firewall provides several distinct operations. These operations include tasks such as shutting down the system, changing the system time and date, backing up the system configuration, etc. You can grant permission to perform these operations to a role. A role can only execute operations for which it has permission, and is prevented from executing any other operation in the system. For example, when users are granted appearance operation permission, they can change the system name and reset the image used in the web interface.

To select an operation, ensure the corresponding secondary tab is selected in the **Web Interface Privileges** section. If you do not select the secondary tab, the corresponding operations become inaccessible. The **admin** user should determine the screens viewable by a user by selecting the secondary tabs.

Creating Users

Local Database Users

Local administrators or users are authenticated internally in the Barracuda Web Application Firewall. The **admin** user can create local users and associate each user with an administrator role. If you delete a local administrator account, that user is denied access to the system.

Assign Roles to Local Database Users

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **Administrator Accounts** section, click **Add Local Administrator** .
3. In the **Admin Access Control** window, enter the credentials, select the role, and enter the email address for the user.
4. Click **Add** . The local user then appears in the table in the **Administrator Accounts** section.

External Database Users

External administrators or users are part of an external authentication service like:

- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial In User Service (RADIUS)
- Security Assertion Markup Language (SAML).

For more information, see the External Database Users article.

Assigning Roles to Users

Barracuda Web Application Firewall users are assigned roles which determine the operations they can perform. A user may be either *local* or *external*. Users must be assigned a role when the user account is created. The user can then access the system. When a user attempts to log in, the Barracuda Web Application Firewall first tries to authenticate the user credentials against configured local administrators, then queries the configured external authentication service. Once authenticated, the user inherits privileges from the associated role.

RBA differences in UI vs API

1. For editing a sub-resource the user role needs
    1. **Write** permission on that sub-resource and at least a **Read** permission on it's object [via API]
    2. **Write** permission on that sub-resource and **Write** permission on it's object [via UI]
2. Any custom role should have at least **Read** permission on the service the role wants i n order to view access or firewall logs, .
3. If a user is creating/adding/editing a new object from the UI, the user role needs to have the following.
    1. a **Write** access directly on that object
    2. accessibility (either **Read**/**Write**) to it's parent object
    3. a **Write Permission** on that tab/screen that the role is creating the object from.
4. Granting permissions to an object from the **Administrator-Roles** API, will automatically grant the same permission for the dependent screen(s) of that object and vice-versa. (when done from the UI).

Related Articles:

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.