Chapter 5

Configuring Role-Based Access Control

This chapter describes how to configure role-based access control (RBAC) on the Cisco Application Control Engine (ACE) module.

This chapter contains the following sections:

• Information About Role-Based Access Control
• Configuring RBAC
• Configuration Example for Configuring RBAC
• Where to Go Next

Information About Role-Based Access Control

After reading this chapter, you should have a basic understanding of how the ACE provides security administration by using role-based access control (RBAC) and how to configure a server maintenance user with permission to access a subset of your network.

One of the most challenging problems in managing large networks is the complexity of security administration. The ACE allows you to determine the commands and resources available to each user through RBAC by associating users with domains and roles.

A domain is a collection of physical and virtual network resources such as real servers and virtual servers.

User roles determine user privileges, such as the commands that the user can enter and the actions the user can perform in a particular context. The ACE provides a number of predefined roles; context administrators can create new roles.

The ACE provides the following predefined roles, which you cannot delete or modify:

• Admin—If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire ACE. If created in a user context, gives a user complete access to and control over all policies, roles, domains, server farms, real servers, and other objects in that context.

• Network Admin—Has complete access to and control over the following features:
  – Interfaces
  – Routing
  – Connection parameters
  – Network Address Translation (NAT)
- VIPs
- Copy configurations
- `changeto` command

- Network-Monitor—Has access to all `show` commands and to the `changeto` command. If you do not explicitly assign a role to a user with the `username` command, this is the default role.

- Security-Admin—Has complete access to and control over the following security-related features within a context:
  - ACLs
  - Application inspection
  - Connection parameters
  - Interfaces
  - Authentication, authorization, and accounting (AAA)
  - NAT
  - Copy configurations
  - `changeto` command

- Server-Appln-Maintenance—Has complete access to and control over the following features:
  - Real servers
  - Server farms
  - Load balancing
  - Copy configurations
  - `changeto` command

- Server-Maintenance—Can perform real server maintenance, monitoring, and debugging for the following features:
  - Real servers—Modify permission
  - Server farms—Debug permission
  - VIPs—Debug permission
  - Probes—Debug permission
  - Load balancing—Debug permission
  - `changeto` command—Create permission

- SLB-Admin—Has complete access to and control over the following ACE features within a context:
  - Real servers
  - Server farms
  - VIPs
  - Probes
  - Load balancing (Layer 3/4 and Layer 7)
  - NAT
  - Interfaces
  - Copy configurations
  - `changeto` command
SSL-Admin—Can administer all SSL features:
- SSL—Create permission
- PKI—Create permission
- Interfaces—Modify permission
- Copy configurations—Create permission
- `changeto` command—Create permission

This chapter describes how to create a domain and a user, and how to associate the user with a predefined role and the new domain. For more information on advanced virtualization configuration, such as restricting user access, predefined roles and how to define a custom role, and creating a domain, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

## Configuring RBAC

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th><code>changeto context</code></th>
<th>Changes to the correct context if necessary. Check the CLI prompt to verify that you are operating in the VC_WEB context.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>host1/Admin# changeto VC_WEB</code></td>
<td></td>
</tr>
<tr>
<td><code>host1/VC_WEB#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th><code>config</code></th>
<th>Enters configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>host1/VC_WEB# config</code></td>
<td></td>
</tr>
<tr>
<td><code>host1/VC_WEB(config)#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th><code>domain name</code></th>
<th>Creates a domain for the context.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>host1/VC_WEB(config)# domain DOMAIN1</code></td>
<td></td>
</tr>
<tr>
<td><code>host1/VC_WEB(config-domain)#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><code>add-object all</code></th>
<th>Allocates all configuration objects in the VC_WEB context to the domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>host1/VC_WEB(config-domain)# add-object all</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>exit</code></th>
<th>Exits domain configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>host1/VC_WEB(config-domain)# exit</code></td>
<td></td>
</tr>
<tr>
<td><code>host1/VC_WEB(config)#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuration Example for Configuring RBAC

The following example shows how to configure RBAC. The commands that you have configured in this chapter are shown in bold text.

switch/VC_WEB(config)# do show running config
Generating configuration....

access-list INBOUND line 8 extended permit ip any any

class-map type management match-any REMOTE_ACCESS
description Remote access traffic match
2 match protocol ssh any
3 match protocol telnet any
4 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
class REMOTE_ACCESS
permit

service-policy input REMOTE_MGMT_ALLOW_POLICY

---

Step 6

**username user password 5 password role**
name1 domain name2

**Example:**
host1/VC_WEB(config)# username USER1
password 5
$1$vAN9gQDISMmbmjqQgJpJ56x0btzXpp8l role
Server-Maintenance domain DOMA1
host1/VC_WEB(config)# exit

**Purpose:**
Configures new user USER1, and assigns the predefined role SLB-Admin and the domain DOMA1 to USER1.
The 5 parameter for the **password** keyword requires that you enter an MD5 hash-encrypted password. You can obtain an MD5 hash password by first entering the **username** command with the 0 parameter and a clear-text password (for example, MYPASSWORD). Next, enter the **show running-config** command and copy the user’s encrypted password from the running-configuration file. Enter the username command again using the 5 parameter and the encrypted password.

---

Step 7

**exit**

**Example:**
host1/VC_WEB(config)# exit
host1/VC_WEB#

**Purpose:**
Exits configuration mode.

---

Step 8

**show running-config role**
**show running config domain**

**Examples:**
host1/VC_WEB# show running-config role
host1/VC_WEB# show running-config domain

**Purpose:**
Displays the user and domain configurations.

---

Step 9

**copy running-config startup-config**

**Example:**
host1/VC_WEB# copy running-config startup-config

**Purpose:**
(Optional) Copies the running configuration to the startup configuration.
interface vlan 400
description Client connectivity on VLAN 400
ip address 10.10.40.1 255.255.255.0
access-group input INBOUND
no shutdown

interface vlan 500
description Server connectivity on VLAN 500
ip address 10.10.50.1 255.255.255.0
no shutdown

ip route 0.0.0.0 0.0.0.0 172.25.91.1
domain DOMAIN1
add-object all
username USER1 password 5 $1$vAN9gQDI$NmbmjQgJPj45lxbtzXPpB1 role Server-Maintenance
domain DOMAIN1

Where to Go Next

In this chapter, you have created a user to perform a limited number of functions on a subset of your network. In the next chapter, you will create a virtual server for server load balancing.