Implement Role-Based Administration

185 out of 221 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

You can use role-based administration to organize certification authority (CA) administrators into separate, predefined CA roles, each with its own set of tasks. Roles are assigned by using each user's security settings. You assign a role to a user by assigning that user the specific security settings that are associated with the role. A user that has one type of permission, such as Manage CA permission, can perform specific CA tasks that a user with another type of permission, such as Issue and Manage Certificates permission, cannot perform.

The following table describes the roles, users, and groups that can be used to implement role-based administration. To assign a role to a user or group, you must assign the role's corresponding security permissions, group memberships, or user rights to the user or group. These security permissions, group memberships, and user rights are used to distinguish which users have which roles.

Roles and groups	Security permission	Description
CA administrator	Manage CA	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate. These permissions are assigned by using the Certification Authority snap-in.
Certificate manager	Issue and Manage Certificates	Approve certificate enrollment and revocation requests. This is a CA role. This role is sometimes referred to as CA officer. These permissions are assigned by using the Certification Authority snap-in.
Backup operator	Back up file and directories Restore file and directories	Perform system backup and recovery. Backup is an operating system feature.
Auditor	Manage auditing and security log	Configure, view, and maintain audit logs. Auditing is an operating system feature. Auditor is an operating system role.
Enrollees	Read Enroll	Enrollees are clients who are authorized to request certificates from a CA. This is not a CA role.

All CA roles are assigned and modified by members of local **Administrators**, **Enterprise Admins**, or **Domain Admins**. On enterprise CAs, local administrators, enterprise administrators, and domain administrators are CA administrators by default. Only local administrators are CA administrators by default on a stand-alone CA. If a stand-alone CA is installed on a server that is joined to an Active Directory domain, domain administrators are also CA administrators.

The CA administrator and certificate manager roles can be assigned to Active Directory users or local users in the Security Accounts Manager (SAM) of the local computer, which is the local security account database. As a best practice, you should assign roles to group accounts instead of individual user accounts.

Only CA administrator, certificate manager, auditor, and backup operator are CA roles. The other users described in the table are relevant to role-based administration and should be understood before assigning CA roles.

Only CA administrators and certificate managers are assigned by using the Certification Authority snap-in. To change the permissions of a user or group, you must change the user's security permissions, group membership, or user rights.

To set CA administrator and certificate manager security permissions for a CA

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. Click the **Security** tab, and specify the security permissions.

Roles and activities

Each CA role has a specific list of CA administration tasks associated with it. The following table lists all the CA administration tasks along with the roles in which they are performed.

Activity	CA administrator	Certificate manager	Auditor	Backup operator	Local administrator	Notes
Install CAs					X	
Configure policy and exit modules	X					
Stop and start the Active Directory Certificate Services	X					

(AD CS) service						
Configure extensions	X					
Configure roles	X					
Renew CA keys					X	
Define key recovery agents	X					
Configure certificate manager restrictions	X					
Delete a single row in the CA database	X					
Delete multiple rows in the CA database (bulk deletion)	X	X				The user must be both a CA administrator and a certificate manager. This activity cannot be performed when role separation is enforced.
Enable role separation					X	
Issue and approve certificates		X				
Deny certificates		X				
Revoke certificates		X				
Reactivate certificates that are placed on hold		X				
Renew		X				

certificates						
Enable, publish, or configure certificate revocation list (CRL) schedules	X					
Recover archived keys		X				Only a certificate manager can retrieve the encrypted key data structure from the CA database. The private key of a valid key recovery agent is required to decrypt the key data structure and generate a PKCS #12 file.
Configure audit parameters			X			By default, the local administrator holds the **system audit** user right.
Audit logs			X			By default, the local administrator holds the **system audit** user right.
Back up the system				X		By default, the local administrator holds the **system backup** user right.
Restore the system				X		By default, the local administrator holds the **system backup** user

						right.
Read the CA database	X	X	X	X		By default, the local administrator holds the **system audit** and **system backup** user rights.
Read CA configuration information	X	X	X	X		By default, the local administrator holds the **system audit** and **system backup** user rights.

Additional considerations

- Enrollees are allowed to read CA properties and CRLs, and they can request certificates. On an enterprise CA, a user must have Read and Enroll permissions on the certificate template to request a certificate. CA administrators, certificate managers, auditors, and backup operators have implicit Read permissions.
- An auditor holds the **system audit** user right.
- A backup operator holds the **system backup** user right. In addition, the backup operator has the ability to start and stop the Active Directory Certificate Services (AD CS) service.

Assigning roles

The CA administrator for a CA assigns users to the separate roles of role-based administration by applying the security settings required by a role to the user's account. The CA administrator can assign a user to more than one role, but the CA is more secure when each user is assigned to only one role. When this delegation strategy is used, fewer CA tasks can be compromised if a user's account becomes compromised.

Administrator concerns

The default installation setting for a stand-alone CA is to have members of the local **Administrators** group as CA administrators. The default installation setting for an enterprise CA is to have members of the local **Administrators**, **Enterprise Admins**, and **Domain Admins** groups as CA administrators. To limit the power of any of these accounts, they should be removed from the CA administrator and certificate manager roles when all CA roles are assigned.

As a best practice, group accounts that have been assigned CA administrator or certificate manager roles should not be members of the local **Administrators** group. Also, CA roles should only be assigned to group accounts and not individual user accounts.