CENTRAL ACCESS POLICY

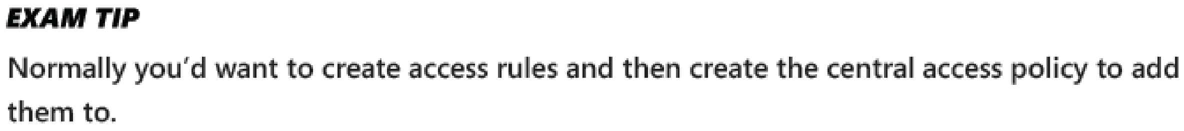
Configuring access policies

Finally, you are ready to create access policies after you have assigned attributes to users, devices, and files. To configure access policies, you need to perform the following steps:

1. Create a claims-based central access policy.
2. Use Group Policy to deploy this central access policy to your file servers.

Step 1: Create a central access policy that includes claims

This step consists of two parts, both of which you can perform in Active Directory Administrative Center. First, you create one or more central access rules that include claims. Then, you add those rules to a central access policy.



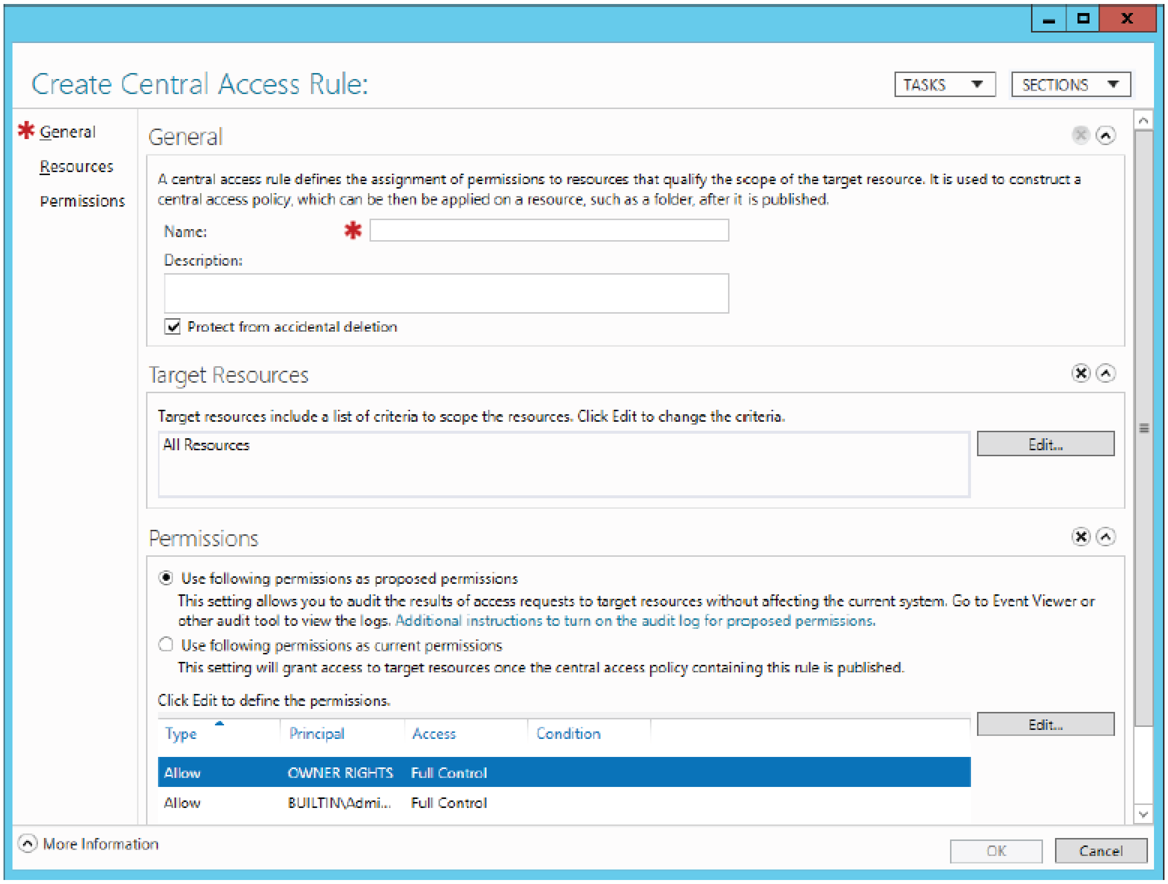
EXAM TIP

Normally you'd want to create access rules and then create the central access policy to add them to.

CREATE A NEW CENTRAL ACCESS RULE

A central access rule is similar to an ACL in that it describes which conditions must be met for access to be granted to a resource.

To create a new central access rule, in Active Directory Administrative Center, select tree view in the navigation pane and then select Central Access Rules. In the Tasks pane, click New, and then click Central Access Rule. This step opens the Create Central Access Rule page, shown in Figure 11-15.



General

A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: *

Description:

☑ Protect from accidental deletion

Target Resources

Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.

All Resources

Permissions

● Use following permissions as proposed permissions

This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other audit tool to view the logs. Additional instructions to turn on the audit log for proposed permissions.

○ Use following permissions as current permissions

This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

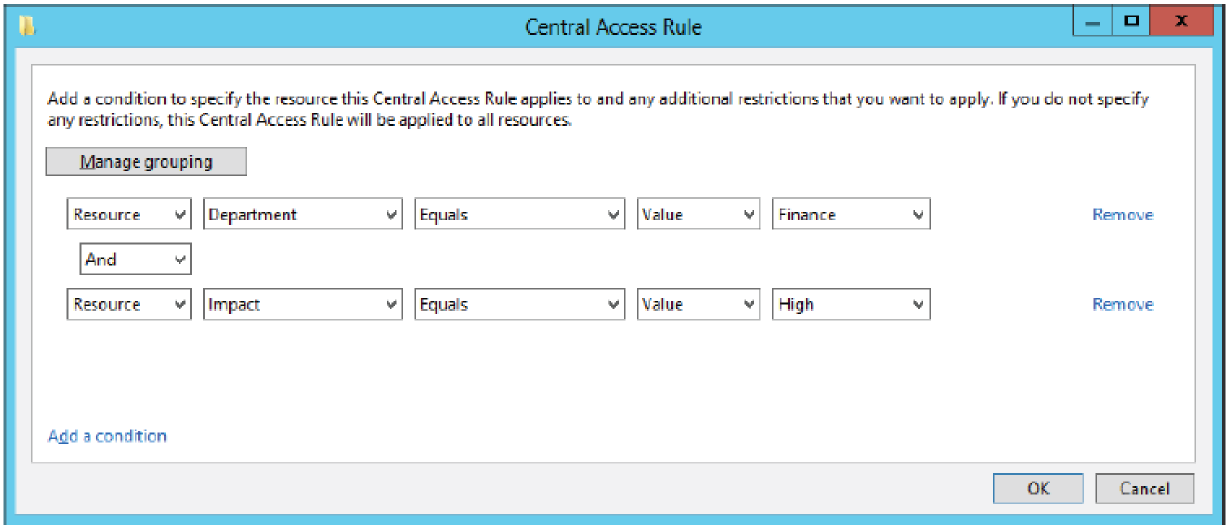
Type	Principal	Access	Condition
Allow	OWNER RIGHTS	Full Control	
Allow	BUILTIN\Admi...	Full Control	

FIGURE 11-15 Creating a new central access rule.

Use the following instructions to complete the page:

1. In the Name text box, type the name you want to give to the rule.

2. In the Target Resources section, click Edit, and in the Central Access Rule dialog box, add the conditions that match the target resources for which you want to define access. For example, if your goal is to define access permissions to resources that have been configured both with a Department classification property of Finance and with an Impact classification property of High, then you want to add the two conditions configured as shown in Figure 11-16.



Add a condition to specify the resource this Central Access Rule applies to and any additional restrictions that you want to apply. If you do not specify any restrictions, this Central Access Rule will be applied to all resources.

Resource | Department | Equals | Value | Finance

And

Resource | Impact | Equals | Value | High

FIGURE 11-16 Configuring matching conditions for target resources.

3. In the Permissions section of the Create Central Access Rule page, select Use Following Permissions As Current Permissions, and then click Edit. In the Advanced Security Settings For Permissions dialog box, click Add to open the Permission Entry For Permissions dialog box, shown in Figure 11-17. In this dialog box, do the following:

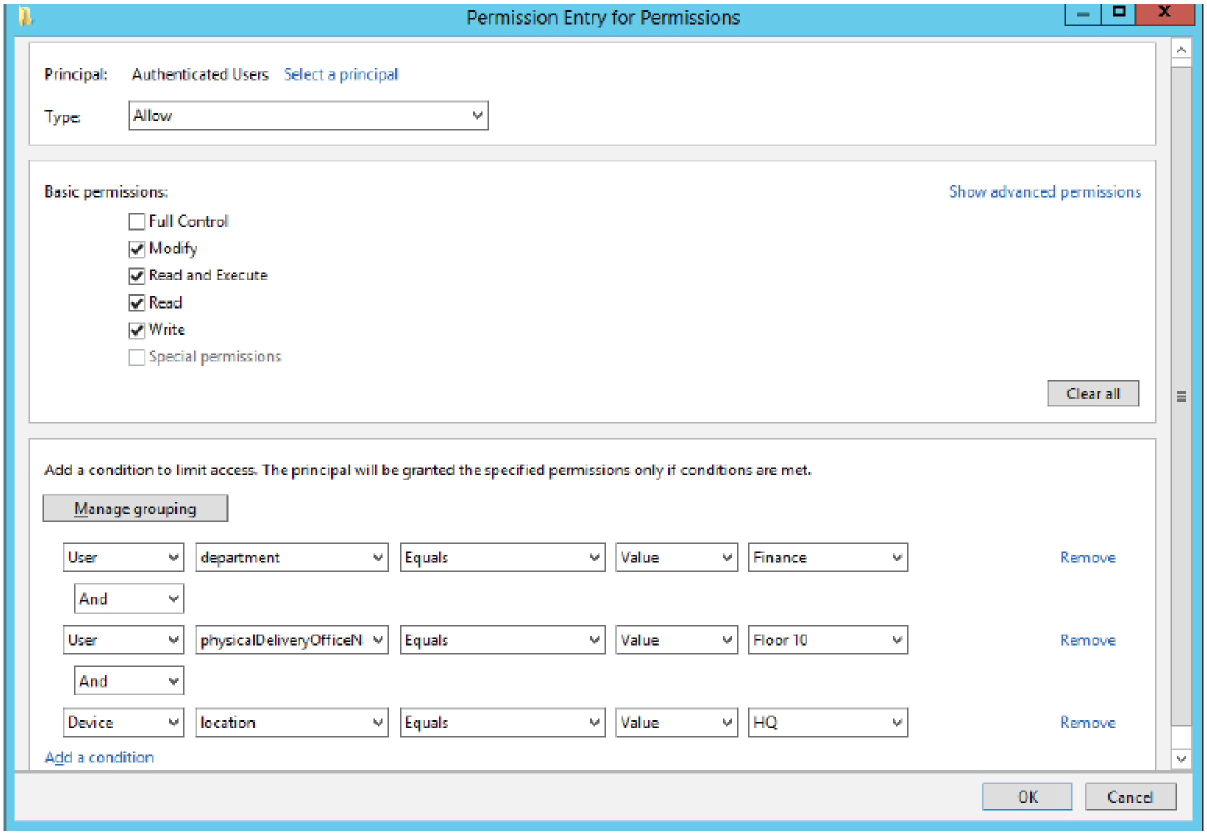
A. Near the top of the dialog box, click Select A Principal. A principal is another name for a user or group account. To configure DAC, you normally want to select Authenticated Users as the principal. (Remember this point both for the real world and the exam.)

B. In the middle of the dialog box, beneath Basic Permissions, select the permissions that you want to assign to users who match the conditions in your rule.

C. Near the bottom of the dialog box, add conditions that match the users for whom you want to define access. For example, if you want to provide access only to users whose accounts in Active Directory have defined a Department value of Finance and an Office value of Floor 10, and who are signed on to computers whose accounts in Active Directory have defined a Location value of HQ, then you want to add the three conditions configured as shown in Figure 11-17. Remember that if Authenticated Users attempt to access the target resource and do not match these conditions, the users will be completely denied access (with the exception of the file owner).

EXAM TIP

As an alternative to step 3, you can leave selected the "Use Following Permissions as Proposed Permissions" option, which you can see in Figure 11-15. This option is used to stage a policy rule. Staging policies can be used to monitor the effects of a new policy entry before you enable it. You can use this option with the Group Policy setting name Audit Central Access Policy Staging. For more information, see the procedure described at the following address: *http://technet.microsoft.com/en-us/library/hh846167.aspx#BKMK_1_2*.



Principal: Authenticated Users

Type: Allow

Basic permissions:

☐ Full Control
☑ Modify
☑ Read and Execute
☑ Read
☑ Write
☐ Special permissions

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

User | department | Equals | Value | Finance
And
User | physicalDeliveryOfficeN | Equals | Value | Floor 10
And
Device | location | Equals | Value | HQ

FIGURE 11-17 Configuring permissions and matching conditions for users and devices.

4. Click OK three times to finish and return to Active Directory Administrative Center.

ADD CENTRAL ACCESS RULE(S) TO A CENTRAL ACCESS POLICY

In the navigation pane of Active Directory Administrative Center, select tree view and then click Central Access Policies. In the Tasks pane, click New, and then click Central Access Policy.

On the Create Central Access Policy page that opens, do the following:

1. In the Name text box, type the name you want to assign to the policy.

2. In Member Central Access Rules, click Add and then add the desired central access rules you have created. Click OK twice to return to Active Directory Administrative Center.

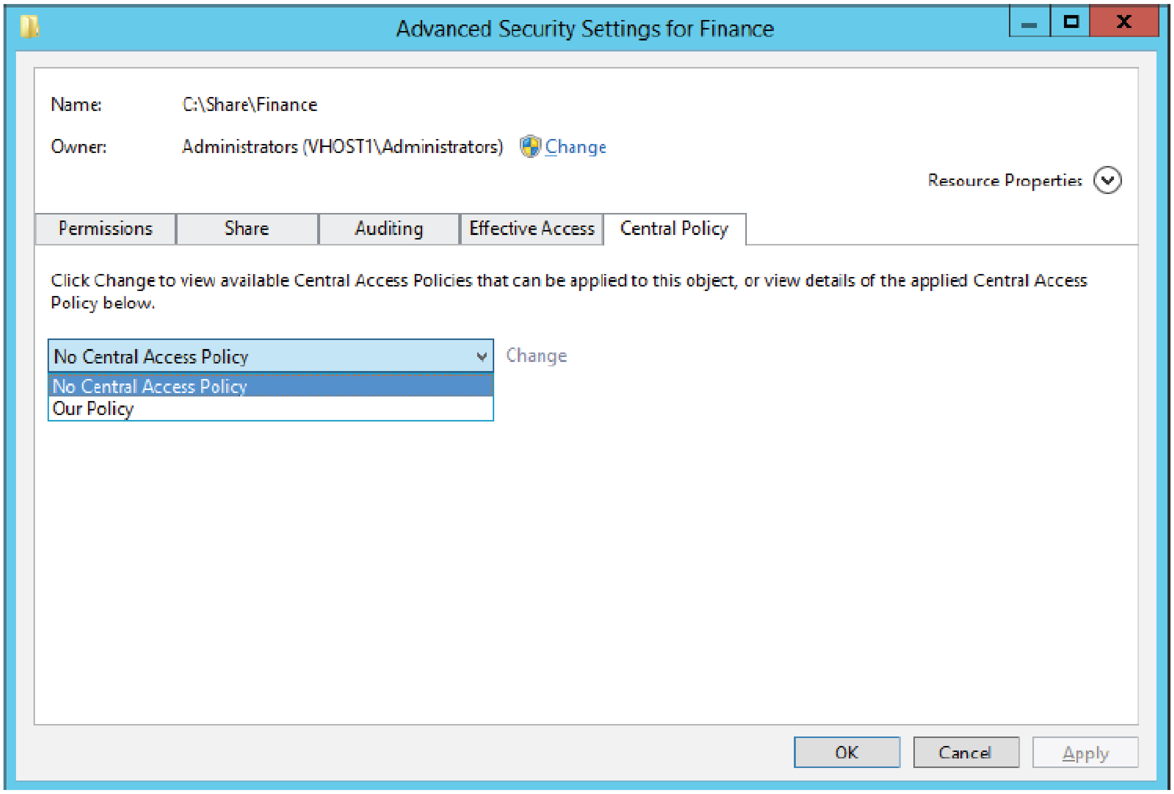
MULTIPLE CENTRAL ACCESS RULES When you include multiple access rules in a policy, all the rules will be applied along with that policy when the policy is applied. The most restrictive access permissions always take effect when two rules provide different levels of access to the same user.

Step 2: Deploy central access policy to file servers

In this step, you configure a policy setting at the domain level that will deliver chosen central access policies to your file servers. Note that you can’t actually *enforce a central access policy* by using Group Policy. You use Group Policy only to make desired central access policies available for selection in the Advanced Security Settings dialog box of all objects within the folder structure on file servers. The policy must then be applied to the object (usually a folder) manually.

To make your central access policies available to objects on file servers, in a GPO linked to the domain, navigate to Computer Configuration/Policies/Windows Settings/Security Settings/File System, and then click Central Access Policy. On the Action menu, select Manage Central Access Policies. In the Central Access Policies Configuration dialog box, add the central access policies that you want to make available to file servers, and then click OK.

When this Group Policy policy setting is enforced, the central access policies appear on a new Central Policy tab of this dialog box, shown in Figure 11-18. A particular central access policy applies to a folder or file object only when an administrator selects and applies it manually in these advanced security settings.



Name: C:\Share\Finance

Owner: Administrators (VHOST1\Administrators) Change

Click Change to view available Central Access Policies that can be applied to this object, or view details of the applied Central Access Policy below.

No Central Access Policy

No Central Access Policy
Our Policy

FIGURE 11-18 The Central Policy tab of the Advanced Security Settings dialog box.