Enable Active Directory Auditing

Configure audit policies for DCs running Windows Server 2008 R2 or higher

You can use the group policy editor to manage audit policy on Windows Server 2008 R2 or higher. You only need to implement the policy once, rather than having to repeat it for every domain controller

Activating the audit policy may be delayed on the domain controllers, depending on your replication interval.

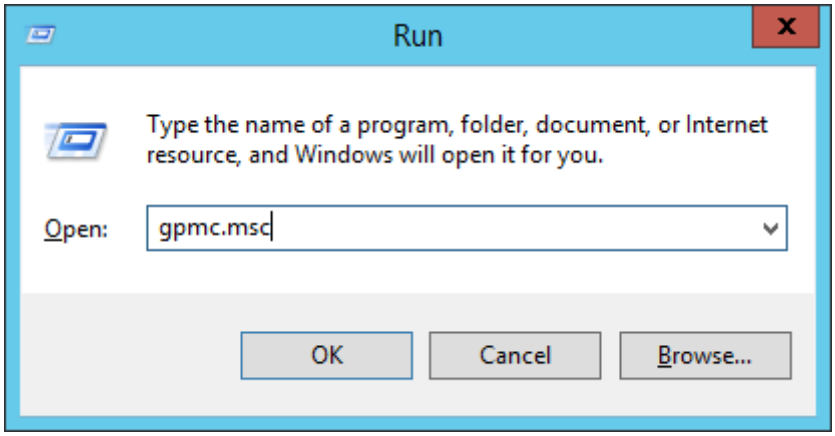
Once you complete these settings, perform the following procedures:

- Complete a manual policy update with the command "gpupdate /force"

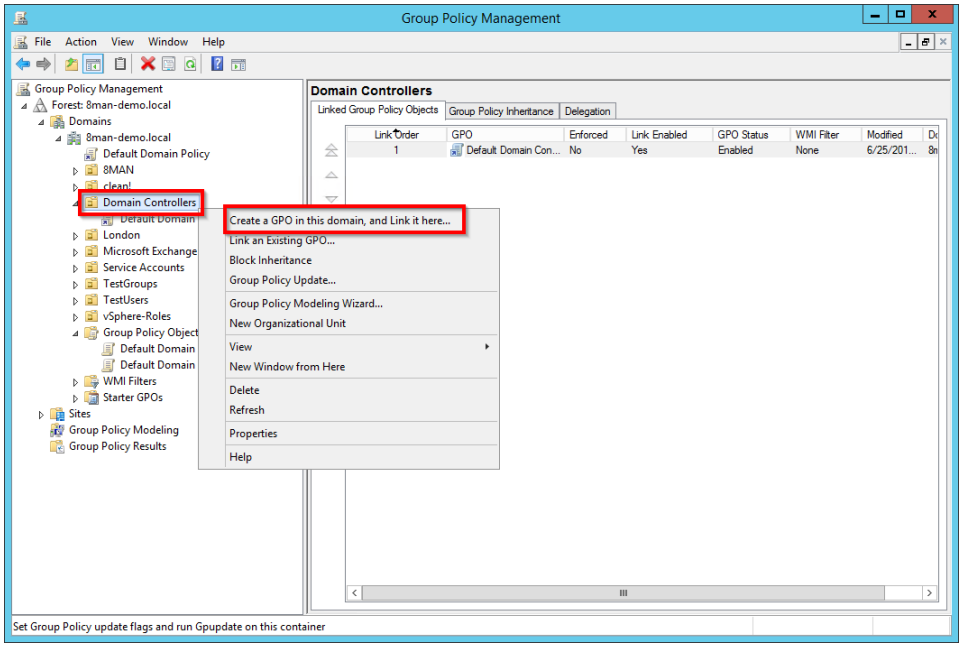
1. Open the Group Policy Management Console.

   Open a Run window and run the following command:

```
gpmc.msc
```



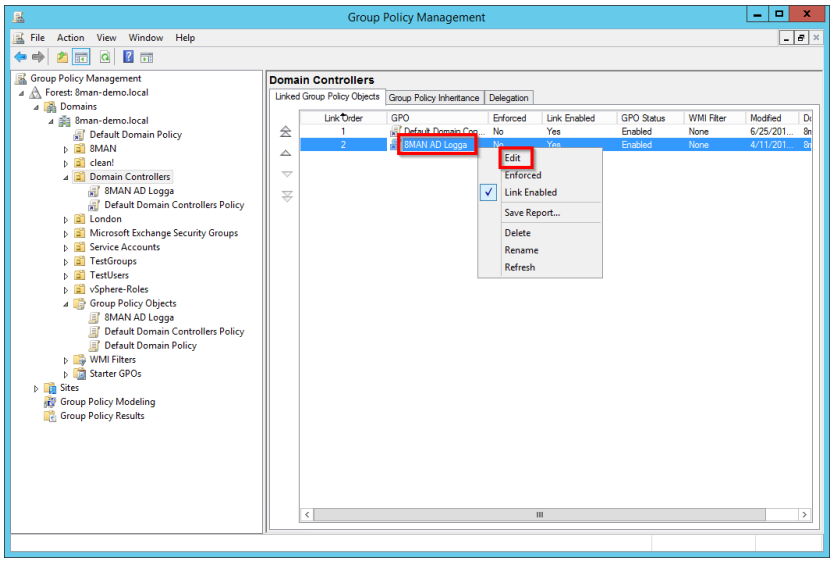
2. In the Group Policy Management console, create a new group policy.



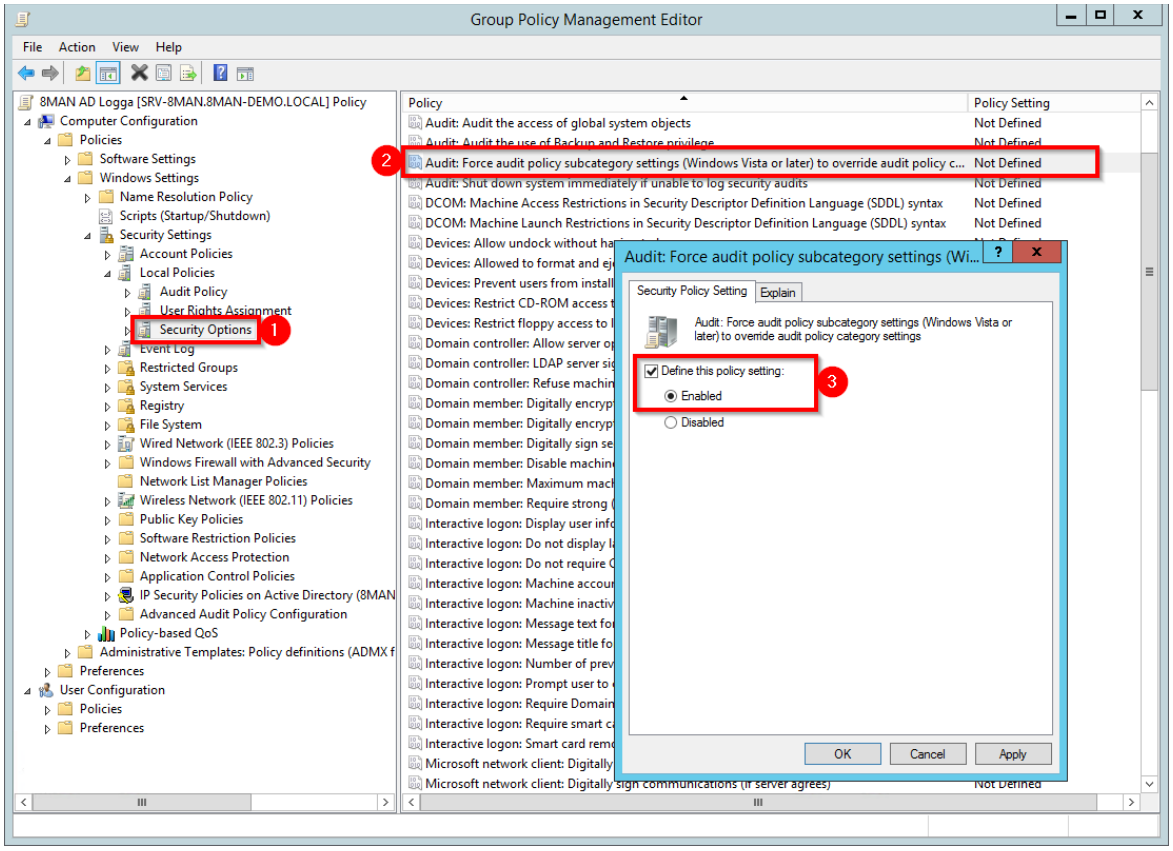
3. Select the organizational unit (OU) where the computer accounts are located. By default, they are located in the OU called Domain Controllers.

4. Ensure that the new policy is applied to the appropriate domain controllers (hierarchy and order).

5. Select the new group policy by right-clicking the policy and selecting Edit.



6. Enable the security policy.



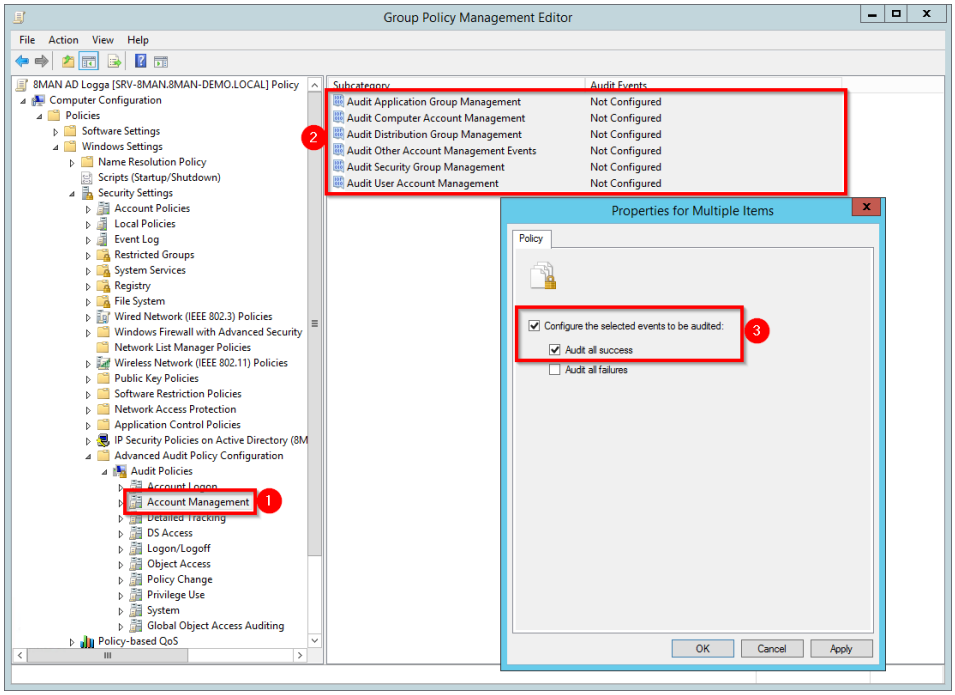
a. Navigate to Security Options

b. Double click the following policy:

Audit: Force audit policy subcategory settings...

c. Enable the security policy as shown above, and then click OK.

7. Activate the audit.

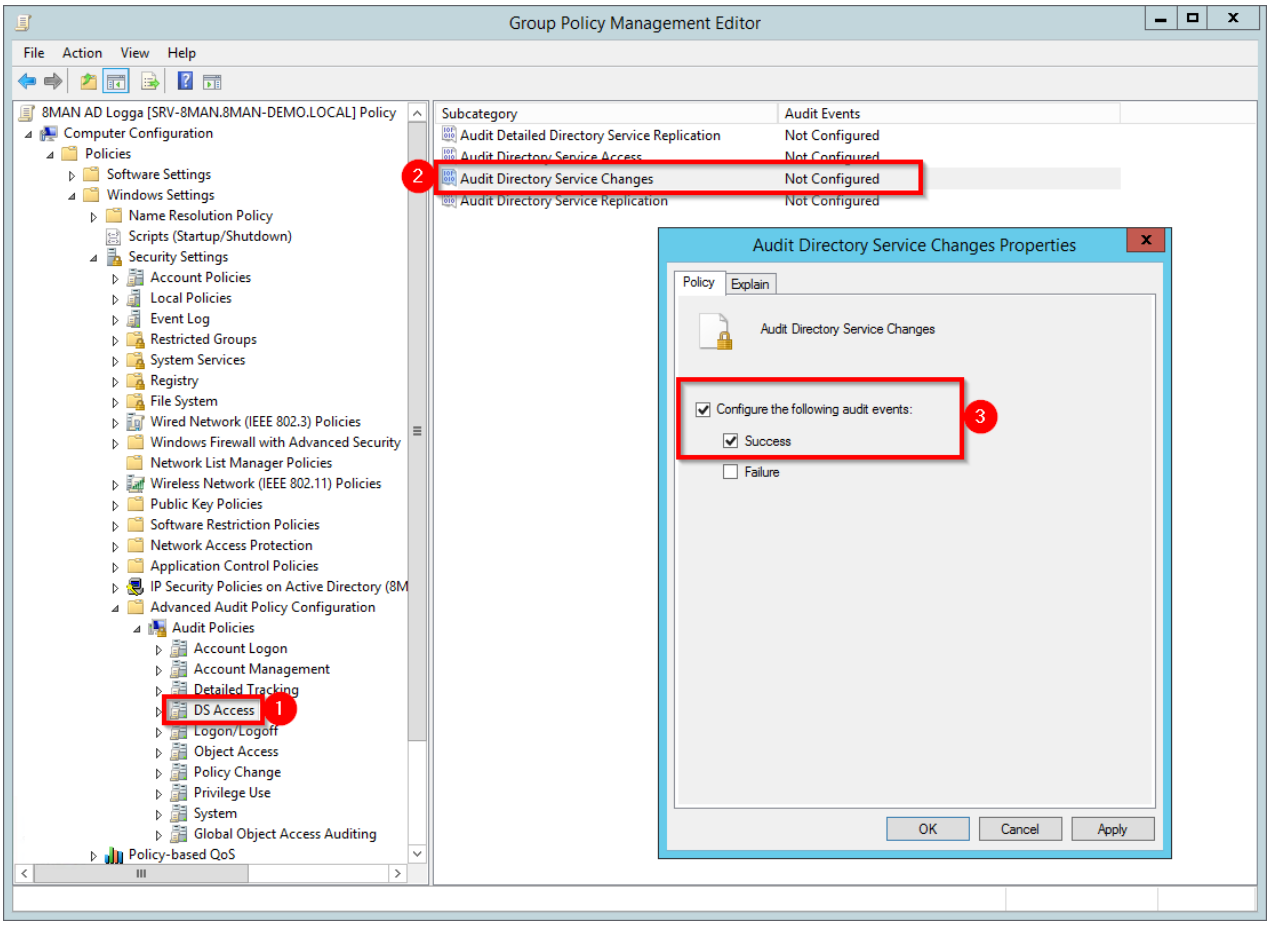


a. Navigate to Account Management.

b. Select all subcategories using multi-select, right-click, and select Properties.

c. In the Properties for Multiple Items window, select the highlighted checkboxes, click Apply, and then click OK.

8. Configure the audit directory service changes.



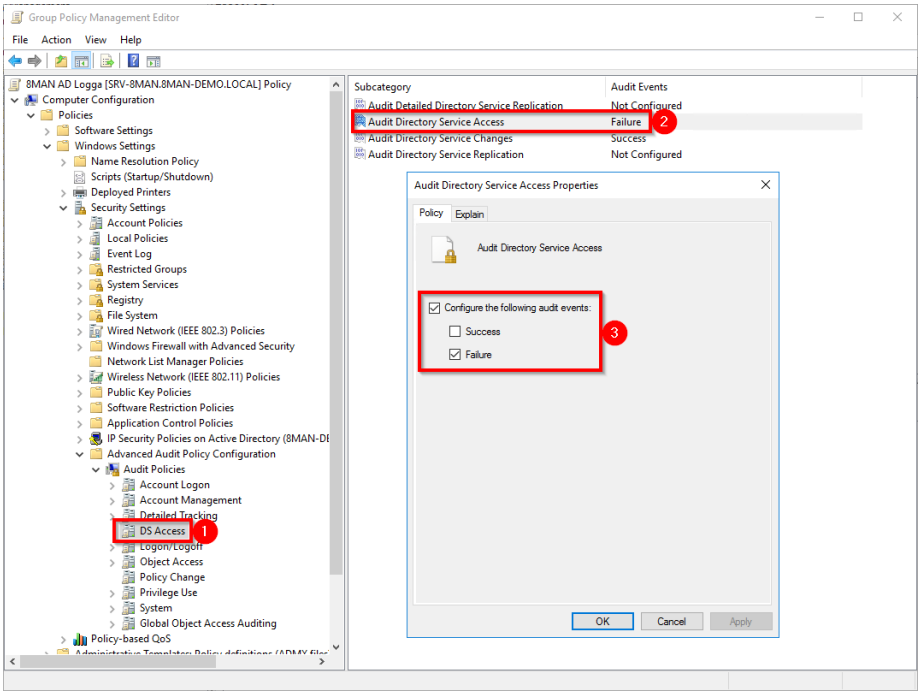
a. Navigate to DS Access.

b. Under Subcategory, double-click Audit Directory Service Changes.

c. In the Audit Directory Service Access Properties window, activate the audit as shown above.

d. Click Apply, and then click OK.

9. Configure the audit directory service access.



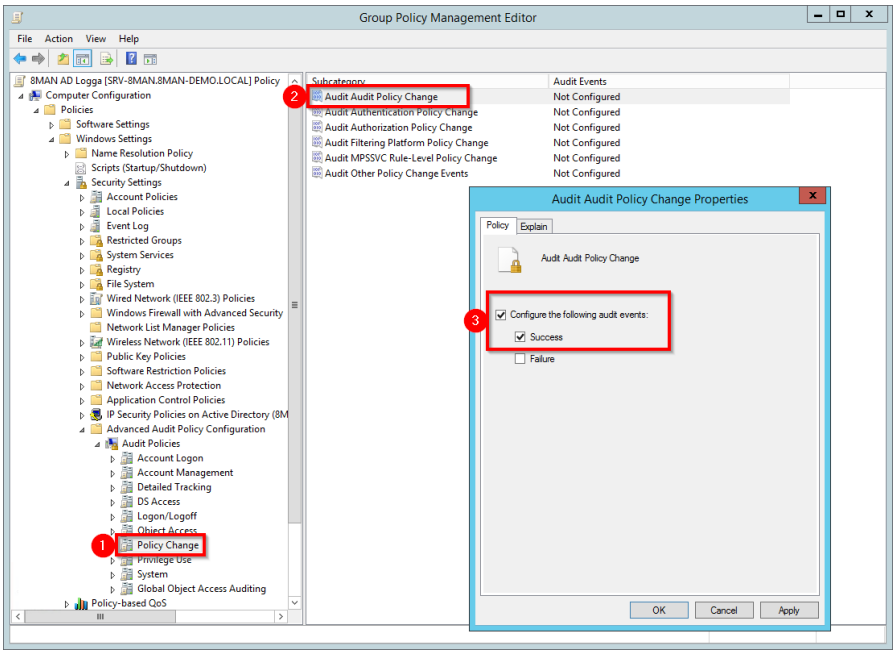
a. Select DS Access.

b. Under Subcategory, double-click Audit Directory Service Access.

c. In the Audit Directory Service Access Properties window, select the options as shown above.

d. Click Apply, and then click OK.

10. Configure the Audit Audit Policy Change properties.



a. Select Policy Change.

b. Under Subcategory, double-click Audit Audit Policy Change.

c. In the Audit Audit Policy Change Properties window, activate the audit as show above.

d. Click Apply, and then click OK.

11. Manually update the policy.

a. Open a Run window.

b. Run the following command:

```
gpupdate /force
```

Configure the AD Logga disk space

The database requires approximately .57 MB of storage space for every 1000 events, By default, AD Logg stores all events for 30 days.

You can determine how long scan and AD Logga data are stored. This affects the size of your data base and required disk storage.

Set the size of the Windows event log

To ensure that events are not lost, configure the maximum size for the security event logs. For audit policy settings, the storage requirements are approximately 1KB per event.

Example: Collector server selected for AD Logga

A collector server outage or maintenance time of one hour with approximately 1000 events per hour, the absolute minimum security event log size would be 1MB. Considering the low storage space requirements for 1000 events and the uncertainty of outage times as well as the potential relevance of individual security events, SolarWinds recommends that you ensure adequate storage space is available.

Verify the audit policy settings

You can verify the effectiveness of audit policies by starting the command prompt with administrator rights and entering one of the commands listed below.

English servers

```
auditpol /get /category:"policy change,account management,ds access"
```

All languages

```
auditpol /get /category:*
```

The marked subcategories must be set to Success or Failure, as shown below.