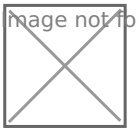
How to find the source of failed logon attempts

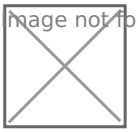
- ## Step 1: Enable 'Audit Logon Events' policy

- Open 'Server Manager' on your Windows server
- Under 'Manage', select 'Group Policy Management' to view the 'Group Policy Management Console'.
- Navigate to forest>Domain>Your Domain>Domain Controllers
- Either create a new group policy object or you can edit an existing GPO.
- In the group policy editor, navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy.
- In Audit policies, select 'Audit logon events' and enable it for 'failure'.



- ## Step 2: Use Event Viewer to find the source of failed logon events

The Event Viewer will now record an event every time there is a failed logon attempt in the domain. Look for event ID 4625 which is triggered when a failed logon is registered.



Open Event Viewer in Active Directory and navigate to Windows Logs> Security. The pane in the center lists all the events that have been setup for auditing. You will have to go through events registered to look for failed logon attempts. Once you find them, you can right click on the event and select Event Properties for more details. In the window that opens, you can find the IP address of the device from which the logon was attempted.

Revision #1
Created 5 January 2024 05:41:14 by ColtM
Updated 7 August 2024 23:24:38 by ColtM