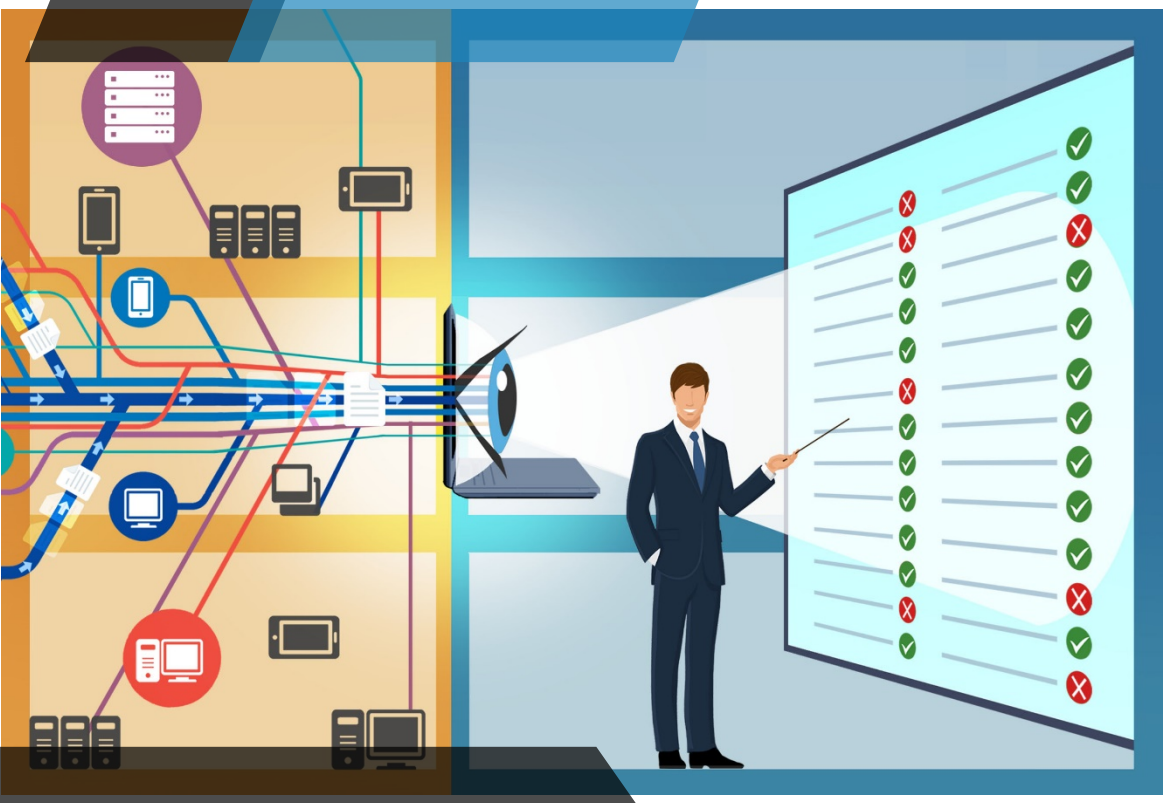
CSAT



Preparing Active Directory environment using GPO

Preparing Active Directory environment using GPO

CSAT requires adequate Microsoft Active Directory domain credentials to properly perform its authenticated scans. The following steps outline how to properly setup Group Policy Objects for CSAT. These processes only apply to domains with Windows Server 2008 R2, 2012 R2 and 2016 domain controllers. **The following procedures should be performed on the server that administers all domain Group Policies.**

Step 1: Creating Group Policy Object

Create a Windows Group Policy Object (GPO) called "CSAT Scan GPO"

- Open "Group Policy Management Console"
- Right-click on **Group Policy Objects** and select **New**
- Name the policy "CSAT Scan GPO"

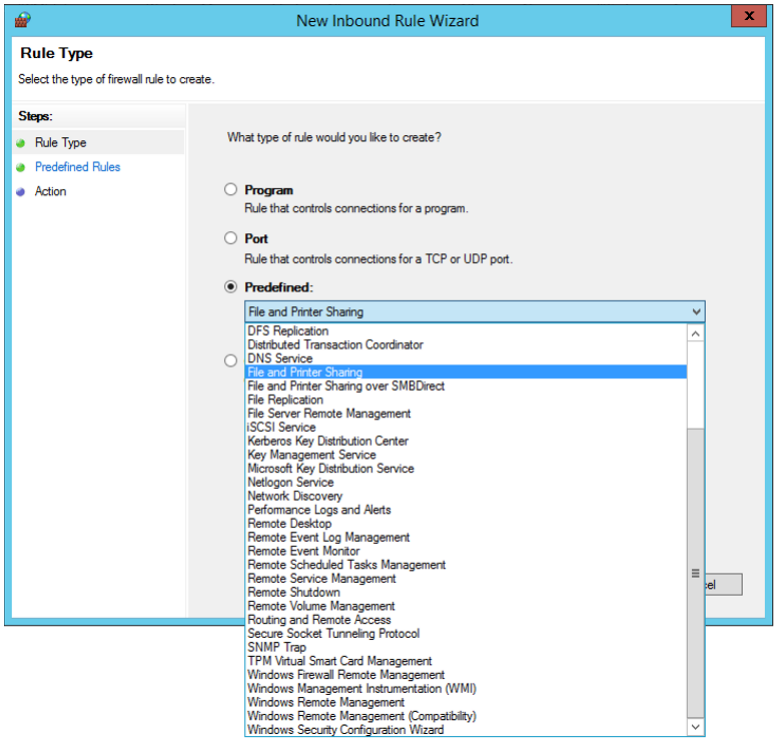
Step 2: Firewall configuration via GPO

CSAT requires the use of the **NetBIOS (NB)**, **Server Message Block (SMB)**, **Remote Procedure Call (RPC)** and **Windows Management Instrumentation (WMI)** protocols to scan a target network. Firewall rules will need to be set in the "CSAT Scan GPO" to allow proper communication

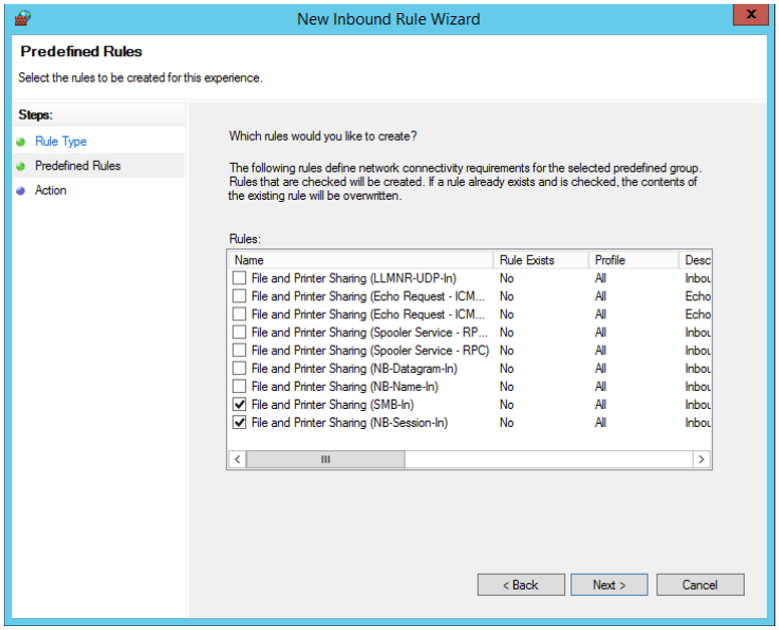
- Right-click on "CSAT Scan GPO" and select **Edit**

- Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules**

- Right-click in the right pane and choose **New Rule…**

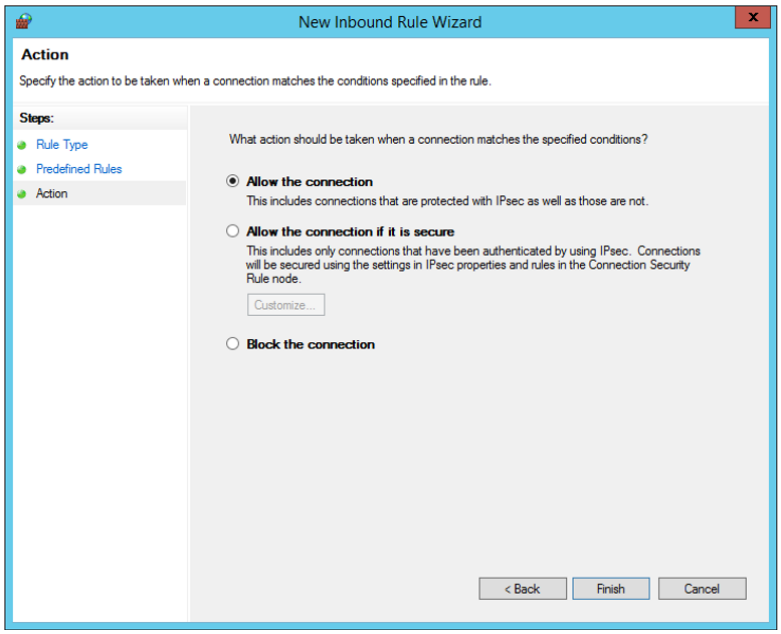


- Choose **Predefined** and select **"File and Printer Sharing"**
  - Make sure that two rules are check-marked:
    - **File and Printer Sharing (NB-Session-In)**
    - **File and Printer Sharing (SMB-In)**

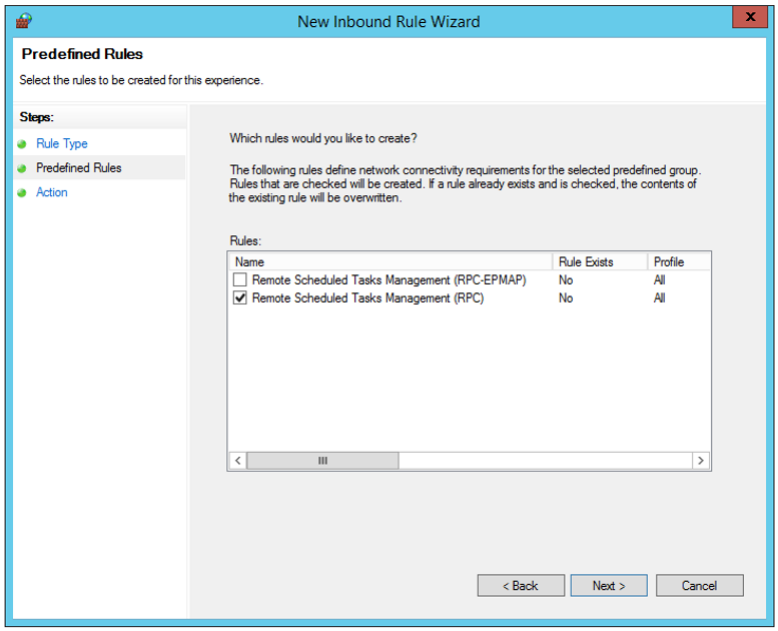


  - Click **Next**

- Choose **“Allow the connection”** option and click **Finish**

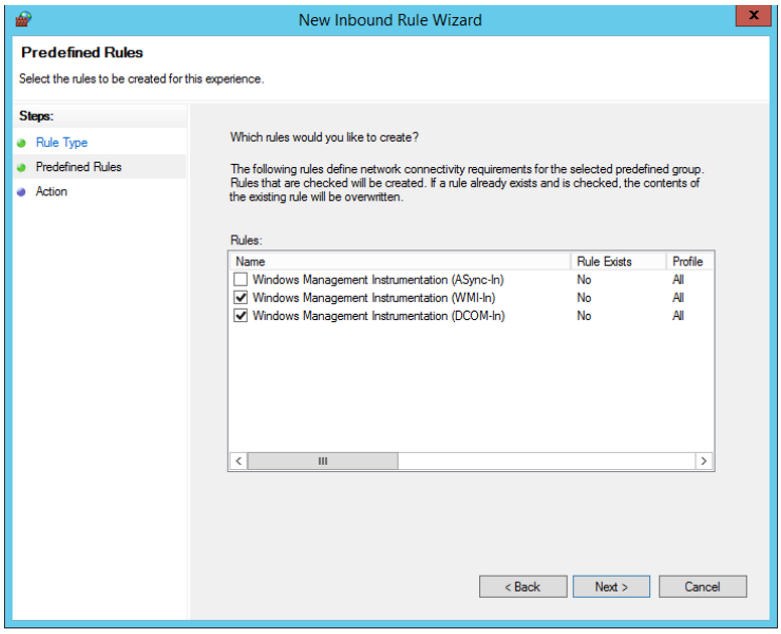


- Right-click in the right pane and choose **New Rule…**
- Choose **Predefined** and select **“Remote Schedule Tasks Management”**
  - Make sure that the rule is check-marked:
    - **“Remote Schedule Tasks Management (RPC)”**



  - Click **Next**
  - Choose **“Allow the connection”** option and click **Finish**

- Right-click in the right pane and choose **New Rule…**
- Choose **Predefined** and select **"Windows Management Instrumentation (WMI)"**
    - Make sure that two rules are check-marked:
        - **Windows Management Instrumentation (WMI-In)**
        - **Windows Management Instrumentation (DCOM-In)**



    - Click **Next**
    - Choose **"Allow the connection"** option and click **Finish**

Step 3: Configure Firewall exceptions (Optional if Windows XP is present in the system)

Most environments have a mix of different Windows operating systems. We recommend that the following step is added to your GPO for backward compatibility and to ensure that ALL systems are accessible to CSAT.

- Right-click on "CSAT Scan GPO" and select **Edit**
- Expand **Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**
- Right-click on **"Windows Firewall: Allow inbound file and printer sharing exceptions"** and click **Edit**
    - Click **Enable**
    - Click **OK**
- Right-click on **"Windows Firewall: Allow inbound remote administration exception"** and click **Edit**

- Click **Enable**
- Click **OK**

Recommended step: an abundant amount of information about a target system can be gleaned using WMI. We recommend that an administrator modify firewall rules for WMI to restrict only specific IP addresses or specific security groups/users to use this protocol.

Step 4: GPO Linking

Once the GPO is created, the GPO must be enabled and linked to a specific domain

- In "Group Policy Management Console", right-click on the target domain or organizational unit (OU) and select **Link an Existing GPO**
  (*) "**CSAT Scan GPO**" contains only **Computer** settings. These policies affect all users who log onto specific **computers.** However, **Computer Configuration** will only affect **computer accounts** that reside in the OU(s) that are in the scope of where that GPO is linked. Therefore, please link "**CSAT Scan GPO**" to the **Computers OU** (or any OUs which store **computer account objects**), not **Users OU** (or any OUs which store **only user account objects**).
  (*) Group Policy for the computer is always updated when the system starts or a user logs in. By default, computer Group Policy is updated in the background (while the computer is in use) every 90 minutes, with a random offset (a random time added to the refresh interval to prevent all clients from requesting Group Policy at the same time) of 0 to 30 minutes.

- Select "**CSAT Scan GPO**"