Windows Server 2003 Domain Controllers GPO Settings

https://campus.barracuda.com/doc/84313539/

The following GPO settings assume the Windows 2003 Domain has a Domain Functional level and Forest Functional level of Windows Server 2003.

1. Click Start and navigate to Administrative Tools > Group Policy Management.
2. Expand Forest.
3. Expand Domains.
4. Expand the Domain in which the Onsite Manager is located.
5. Right-click Group Policy Objects and select New.
6. In the Name field, type LPI MW Default Group Policy.
7. Click OK.

Configuring the Workstation and Member Server Firewall

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile.
3. Configure the following:
    1. Windows Firewall: Do not allow exceptions
       Select Not Configured
    2. Windows Firewall: Define program exceptions
       Select Not configured
    3. Windows Firewall: Allow local program exceptions
       Select Not configured
    4. Windows Firewall: Allow remote administration exception
       Select Enabled
       In the Allow Unsolicited Incoming Messages From field, enter the local subnet. For greater security, you can specify the IP address of the Onsite Manager server. However, make sure that by introducing this limitation you are not impacting actions of users who are not using Barracuda Managed Workplace.
    5. Windows Firewall: Allow file and printer sharing exception
       Select Enabled
       In the Allow Unsolicited Incoming Messages From field, enter the local subnet. For greater security, you can specify the IP address of the Onsite Manager server. However, make sure that by introducing this limitation you are not impacting actions of users who are not using Barracuda Managed Workplace.
    6. Windows Firewall: Allow ICMP exceptions
       Select Enabled
       Enable the Allow Inbound Echo Request check box.
    7. Windows Firewall: Allow remote desktop exception
       Select Enabled

In the Allow Unsolicited Incoming Messages From field, enter the local subnet. For greater security, you can specify the IP address of the Onsite Manager server. However, make sure that by introducing this limitation you are not impacting actions of users who are not using Barracuda Managed Workplace.
Caution: The LocalSubnet setting does not allow computers from networks other than the same subnet to connect to all devices to which the GPO is applied. Care should be taken when setting this. If additional networks need to connect to devices, adjust the setting accordingly.

8. Windows Firewall: Allow UPnP framework exception
   Select Not Configured
9. Windows Firewall: Prohibit notifications
   Select Not Configured
10. Windows Firewall: Allow logging
    Select Not Configured
11. Windows Firewall: Prohibit unicast response to multicast or broadcast requests
    Select Not Configured
12. Windows Firewall: Define port exceptions
    Select Enabled.
    Click the Show button, and in the Show Contents dialog box, type
    `5985:TCP:<OM IP address>:enabled:WinRM`
13. Windows Firewall: Allow local port exceptions
    Select Not Configured

Enabling Terminal Service (RDP) on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Administrative Templates > Windows Components > Terminal Services.
3. Configure the following:
   - Allow users to connect remotely using Terminal Services
     Select Enabled

Enabling Remote Assistance on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Administrative Templates > System >Remote Assistance.
3. Configure the following:
   1. Solicited Remote Assistance
      Select Enabled
      Choose Allow helpers to remotely control the computer
      Set Maximum ticket time (value) to 1

Set maximum ticket time (units) to Hours
Choose Mailto as the Method for sending e-mail invitations

Enabling MBSA Scans

To successfully run MBSA scans, you must enable the Log on as a batch job policy.

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Windows Settings > Security settings >Local Policies> User Rights Assignment.
3. Configure the following:

   Log on as batch job

   Check: Define these policy settings

   Click Add User or Group

   Type the user and group name, and click OK.

Configuring Windows Services for Domain Members

The Policy being updated will not start the Windows services because a policy update may be received while the device is up and logged into the Domain. The services will not be started until either manually started by a user or during the boot process.

These changes will only affect the startup for services when the device is joined to the Domain.

Configure the Window Services for Domain members using the Group Policy Management Tool on the Domain Controller.

1. Right-click LPI MW Default Group and select Edit.
2. In the Group Policy Object Editor window, navigate to Computer Configuration > Windows Settings > Security Settings > System Services
3. Configure the following:
   1. Windows Management Instrumentation (WMI)
      Select Startup Type: Automatic
   2. Remote Registry
      Select Startup Type: Automatic
   3. Remote Procedure Call (RPC)
      Select Startup Type: Automatic

4. Background Intelligent Transfer Service (BITS)
   Select Startup Type: Automatic
5. Windows Update
   Select Startup Type: Automatic
   Windows Update is only required by Barracuda Managed Workplace if the site uses Patch Management.

Note: If you have no updated the domain policy templates, the "Windows Update" service may be displayed as "Automatic Updates".

1. Windows remote Management (WS-Management)
   Select service startup mode: Automatic

Note: When you apply a system service startup policy to Windows XP machine, additional steps may need to be performed so that the service account handling the monitoring can connect to Windows Management Instrumentation. Follow the procedure below to configure the security appropriately.

1. Open the group policy, go to Computer configuration > Windows Settings > Security Settings > System Services.
2. Open the property page for Windows Management Instrumentation service from the list.
3. Click Edit Security.
4. Add the following permission:
   Authenticated Users > Read
   Note: When you add Authenticated Users, the default permission box selected will be Start, Stop and Pause which you need to change to only “Read”.
5. Apply the group policy to the Windows XP workstations and restart the affected machines.

Configuring Microsoft Updates for Domain Members

Barracuda Managed Workplace does not use GPO settings to define the update server to managed clients, so any WSUS policies that are in place on the Domain will interfere with normal operations of Patch Management.

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Administrative Templates> Windows Components > Windows Update (2008 and later) or Automatic Updates (2003).
3. Set all policies to Not Configured.

Enabling Windows Remote Management Settings

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service
3. Configure Allow automatic configuration of listeners by doing the following:
   - Select Enabled.

    - In the IPv4 filter field, type *.
4. Navigate to Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client
5. Configure Trusted Hosts by doing the following:
    - Select Enabled.
    - In the TrustedHosts_List field, type *.

Note: If you cannot locate the Windows Remote Management (WinRM) policies under Computer Configuration > Administrative Templates > Windows components in the Group Policy Editor, you may be required to follow these additional steps:

1. Download and install Microsoft update KB936059 from the following URL: http://support.microsoft.com/kb/936059
2. After you have installed the Microsoft update, in the Group Policy Editor, go to Compouter Configuration > Administrative Templates.
3. Select Add/Remove Templates.
4. In the Add/Remove Templates window, click Add.
5. Import the following templates:
    - C:\Windows\Inf\Windowsremoteshell.adm
    - C:\Windows\Inf\Windowsremotemanagement.adm
6. Click Close.

Linking GPO to Forest/Domain

1. Select the Forest to which you want to link the LPI MW Default Group GPO.
2. From the drop-down menu, select Action.
3. Click Link an Existing GPO.
4. Select LPI MW Default Group.
5. Click OK.