Windows Server 2012 Domain Controllers GPO Settings

https://campus.barracuda.com/doc/84313500/

The following GPO settings assume the Server 2012 Domain has a Domain Functional level and Forest Functional level of a Windows 2012 Server. The procedure below shows how to create a new Group Policy Object.

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.

Note: You do not have to create a new Group Policy Object. Editing any current object will have the same effect, providing there are no conflicts between multiple active Group Policy Objects.

Configuring the Workstation and Member Server Firewall

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Network > Network Connections > Windows Firewall > Domain Profile.
3. Configure the following:
    1. Windows Firewall: Allow local program exceptions
       Select Not configured
    2. Windows Firewall: Define inbound program exceptions
       Select Not configured
    3. Windows Firewall: Protect all network connections
       Select Enabled.
    4. Windows Firewall: Do not allow exceptions
       Select Not Configured
    5. Windows Firewall: Allow inbound 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 logging

Select Not Configured

8. Windows Firewall: Prohibit notifications
   Select Not Configured
9. Windows Firewall: Allow local port exceptions
   Select Not Configured
10. Windows Firewall: Define inbound port exceptions
    Select Enabled
    Click Show. In the Show Contents dialog, type in the following:
    `5985:TCP:<OM IP Address>:enabled:WinRM`
11. Windows Firewall: Allow inbound 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.
12. lWindows Firewall: Allow inbound Remote Desktop exceptions
    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.
13. Windows Firewall: Prohibit unicast response to multicast or broadcast requests
    Select Not Configured
14. Windows Firewall: Allow inbound UPnP framework exceptions
    Select Not Configured

Enabling Remote Desktop Services on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections.
3. Configure the following:
   1. Allow users to connect remotely by using Remote Desktop Services.Select Enabled

Enabling Remote Assistance on Clients

1. Right-click LPI MW Default Group and select Edit.

2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > System >Remote Assistance.
3. Configure the following:
    1. Allow only Windows Vista or later connections
       Select Disabled
    2. Turn on session logging
       Select Not Configured
    3. Turn on bandwidth optimization
       Select Not Configured
    4. Customize warning messages
       Select Not Configured
    5. Configure 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 email invitations

Enabling Remote Event Log Management on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Windows Settings > Security settings > Windows Firewall with Advanced Security > Inbound Rules.
3. Right-click Inbound Rules and select New Rule.
4. Select the Predefined option button, and from the list select Remote Event Log Management.
5. Click Next.
6. Ensure that all rules are selected.
7. Select the Allow the connection option.
8. Click Finish.

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

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Windows Settings> Security Settings > System Services.
3. Configure the following:
    1. Windows Management Instrumentation (WMI)
       Check: Define this policy setting
       Startup Type: Automatic
    2. Remote Registry
       Check: Define this policy setting
       Startup Type: Automatic
    3. Remote Procedure Call (RPC)
       Check: Define this policy setting
       Startup Type: Automatic
    4. Background Intelligent Transfer Service
       Check: Define this policy setting
       Startup Type: Automatic
    5. Windows Update
       Check: Define this policy setting
       Startup Type: Automatic
       Only required by Barracuda Managed Workplace if the site uses Patch Management.
    6. Windows Remote Management (WS-Management) Properties
       Check: Define this policy setting
       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: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Windows Update
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: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Windows Remote Management (WinRM) > WinRM Service
3. Configure Allow remote server management through WinRM by doing the following:
    - Select Enabled.
    - In the IPv4 filter field, type *.
4. Navigate to Computer Configuration > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Windows Remote Management (WinRM) > WinRM Client
5. Configure Trusted Hosts by doing the following:
    - Select Enabled.
    - In the TrustedHostsLists field, type *.

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.

IWindows Server 2008 Domain Controllers GPO Settings

The following GPO settings assume the Windows 2008 Domain has a Domain Functional level and Forest Functional level of a Windows 2008 Server. The procedure below shows how to create a new Group Policy Object.

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.

Note: You do not have to create a new Group Policy Object. Editing any current object will have the same effect, providing there are no conflicts between multiple active Group Policy Objects.

Configuring the Workstation and Member Server Firewall

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Network > Network Connections > Windows Firewall > Domain Profile.
3. Configure the following:
    1. Windows Firewall: Allow local program exceptions
       Select Not configured
    2. Windows Firewall: Define inbound program exceptions
       Select Not configured
    3. Windows Firewall: Do not allow exceptions
       Select Not Configured
    4. Windows Firewall: Allow inbound 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.
    5. Windows Firewall: Allow ICMP exceptions
       Select Enabled
       Enable the Allow inbound echo request check box.
    6. Windows Firewall: Allow logging
       Select Not Configured

7. Windows Firewall: Prohibit notifications
   Select Not Configured
8. Windows Firewall: Allow local port exceptions
   Select Not Configured
9. Windows Firewall: Define inbound port exceptions
   Select Enabled
   Click Show. In the Show Contents dialog, type in the following:

   ```
   5985:TCP:<OM IP Address>:enabled:WinRM
   ```

10. Windows Firewall: Allow inbound 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.
11. Windows Firewall: Allow inbound Remote Desktop exceptions
    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.
12. Windows Firewall: Prohibit unicast response to multicast or broadcast requests
    Select Not Configured
13. Windows Firewall: Allow inbound UPnP framework exceptions
    Select Not Configured

Enabling Remote Desktop Services on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections.
3. Configure the following:
   1. Allow users to connect remotely by using Remote Desktop Services.
      Select Enabled
      Note: For Windows Server 2008 R2, this option is called Remote Desktop Services. For Windows Server 2008, this option is called Terminal Services.

Enabling Remote Assistance on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > System >Remote Assistance.
3. Configure the following:
    1. Allow only Vista or later connections
       Select Disabled
    2. Turn on session logging
       Select Not Configured
    3. Turn on bandwidth optimization
       Select Not Configured
    4. Customize Warning Messages
       Select Not Configured
    5. 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
    6. Offer Remote Assistance
       Select Not Configured

Enabling Remote Event Log Management on Clients

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Windows Settings > Security settings > Windows Firewall with Advanced Security > Inbound Rules.
3. Right-click Inbound Rules and select New Rule.
4. Select the Predefined option button, and from the list select Remote Event Log Management.
5. Click Next.
6. Ensure that all rules are selected.
7. Select the Allow the connection option.
8. Click Finish.

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

1. Right-click LPI MW Default Group and select Edit.
2. Navigate to Computer Configuration > Policies > Windows Settings> Security Settings > System Services.
3. Configure the following:
   1. Windows Management Instrumentation (WMI)
      Check: Define this policy setting
      Startup Type: Automatic
   2. Remote Registry
      Check: Define this policy setting
      Startup Type: Automatic
   3. Remote Procedure Call (RPC)
      Check: Define this policy setting
      Startup Type: Automatic
   4. Background Intelligent Transfer Service (BITS)
      Check: Define this policy setting
      Startup Type: Automatic
   5. Windows Update
      Check: Define this policy setting
      Startup Type: Automatic
      Only required by Barracuda Managed Workplace if the site uses Patch Management.
   6. Windows Remote Management (WS-Management) Properties
      Check: Define this policy setting
      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: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Windows Update
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: Policy definitions (ADMX files) retrieved from the local machine > 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: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Windows Remote Management (WinRM) > WinRM Client
5. Configure Trusted Hosts by doing the following:
   - Select Enabled.
   - In the TrustedHostsLists field, type *.

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.