Guide for Configuring NTP Time Synchronization on a Windows Domain Controller

Introduction
This guide provides step-by-step instructions to configure a Windows Server domain controller to use NTP for time synchronization. It includes configuring Group Policy settings and necessary firewall rules to ensure proper synchronization with NTP servers.

Steps to Configure NTP Time Synchronization

Step 1: Open Group Policy Management Console (GPMC)

1. Log in to the Domain Controller.
2. Open Group Policy Management Console:
   - Press `Win + R`, type `gpmc.msc`, and press Enter.

Step 2: Edit the Default Domain Controllers Policy

1. Navigate to the Appropriate Policy:
   - In the left pane, expand `Forest: YourDomain` > `Domains` > `YourDomain`.
   - Select `Default Domain Controllers Policy`.

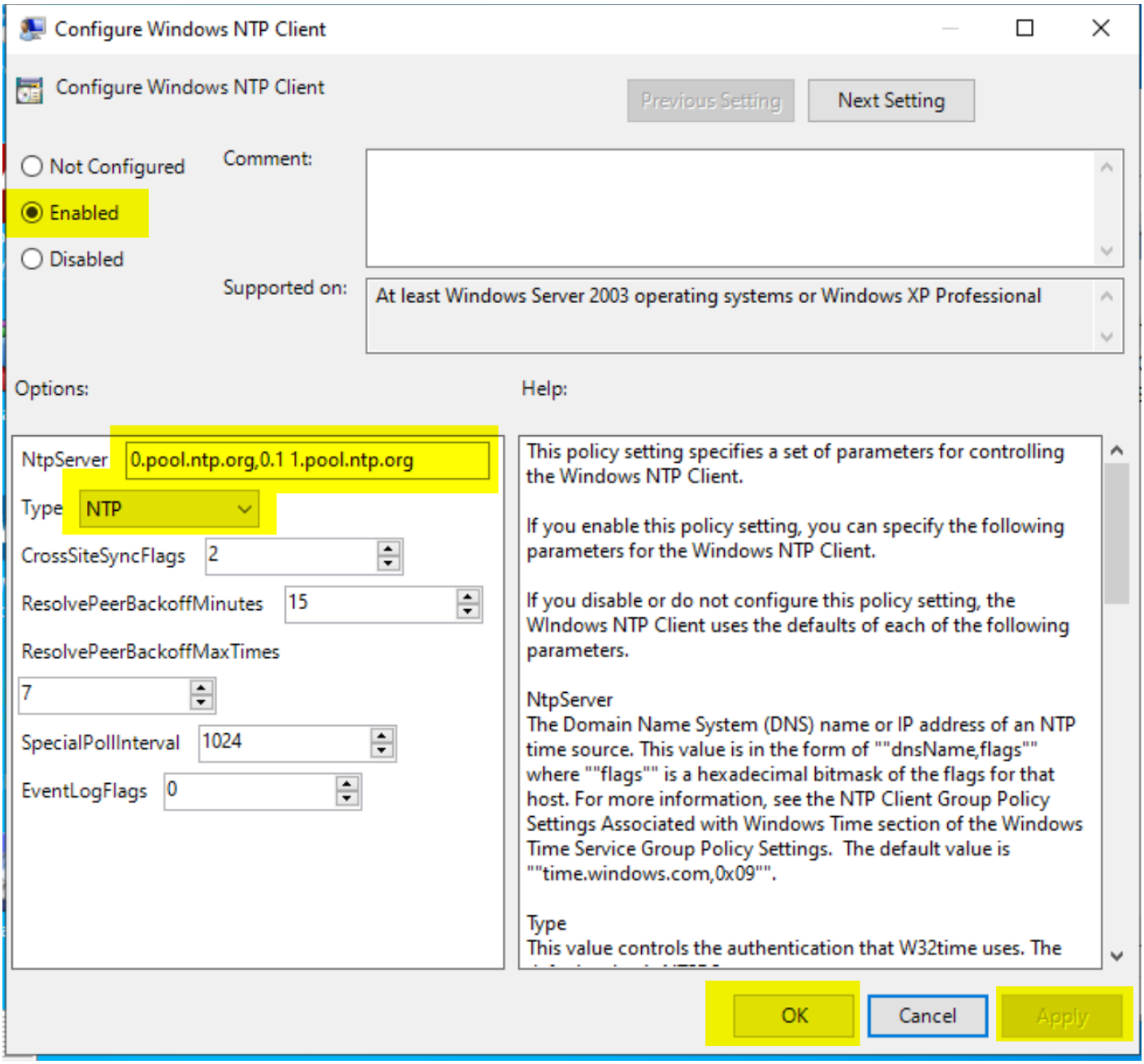
2. Edit the Policy:
   - Right-click on `Default Domain Controllers Policy` and select `Edit`.

Step 3: Configure Windows NTP Client in Group Policy

1. Navigate to the Time Service Settings:
   - Go to `Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers`.
1. Configure Windows NTP Client:
   - Double-click on `Configure Windows NTP Client`.
   - Set it to `Enabled`.
   - In the `NtpServer` field, enter the following NTP servers:

```
0.pool.ntp.org,0x1 1.pool.ntp.org,0x1 2.pool.ntp.org,0x1 3.pool.ntp.org,0x1 time.google.com,0x1
time.windows.com,0x1 time.nist.gov,0x1
```

- Ensure the `Type` is set to `NTP`.
- Click `Apply` and `OK`.



Step 4: Force Group Policy Update and Resynchronize

1. Open Command Prompt or PowerShell as Administrator:
   - Press `Win + X`, then select `Windows PowerShell (Admin)` or `Command Prompt (Admin)`.

2. Force Group Policy Update:

```
gpupdate /force
```

3. Restart the Windows Time Service:

```
Restart-Service w32time
```

4. Force Resynchronization:

```
w32tm /resync
```

Step 5: Verify the Configuration and Synchronization Status

1. Query the Current Configuration:

```
w32tm /query /configuration
```

2. Check the Synchronization Status:

```
w32tm /query /status
```

Step 6: Configure Firewall Rules (if necessary)

1. Open Windows Defender Firewall with Advanced Security:
   - Press `Win + R`, type `wf.msc`, and press Enter.

2. Create a New Inbound Rule for NTP:
   - Click on `Inbound Rules` in the left pane.
   - Click `New Rule...` in the right pane.
   - Select `Port` and click `Next`.
   - Select `UDP` and enter `123` in the `Specific local ports` field. Click `Next`.
   - Select `Allow the connection` and click `Next`.
   - Select the profiles this rule applies to (Domain, Private, Public). Click `Next`.
   - Name the rule (e.g., `Allow NTP`) and click `Finish`.

3. Create a New Outbound Rule for NTP:
   - Click on `Outbound Rules` in the left pane.
   - Repeat the steps above to create a rule that allows outbound UDP traffic on port 123

Summary

By following these steps, you can configure a Windows Server domain controller to synchronize time using NTP servers. This configuration ensures accurate timekeeping across your domain, which is essential for security, logging, and system coordination.

Feel free to adjust the NTP server list based on your organization's preferences and requirements.

Example Commands for Reference

```
# Force Group Policy update
gpupdate /force

# Restart the Windows Time service
Restart-Service w32time

# Force resynchronization
w32tm /resync

# Query the configuration to verify settings
w32tm /query /configuration

# Check the synchronization status
w32tm /query /status
```

This guide ensures that your domain controllers maintain accurate time synchronization, eliminating the need for manual time setting and improving overall system reliability.

Revision #2
Created 31 May 2024 01:29:40 by Nate Nash
Updated 31 May 2024 01:36:55 by Nate Nash