Windows Imaging in FileWave 15.5+: Secure NFS Tunneling and Fallback Options

What

In FileWave version 15.5.0, significant changes have been made to the Windows Imaging process using the Imaging Virtual Server (IVS). Previously, when imaging or capturing a Windows system, the device would mount NFS (Network File System) volumes directly over TCP/UDP port 2049. Starting with FileWave 15.5, the imaging process has been enhanced for security and reliability by establishing a VPN tunnel over TCP/UDP port 20490. Over this secure VPN tunnel, the system accesses the NFS mounts, providing a more secure and efficient imaging environment.

However, if issues arise with the new VPN tunneling method, there is a fallback mechanism that allows you to revert to the previous method of direct NFS mounting over port 2049. This ensures that imaging tasks can continue without interruption, even if the VPN tunnel encounters problems in certain network environments.

When/Why

When to Use

- Default Behavior: By default, FileWave 15.5 uses a VPN tunnel on port 20490 for all Windows imaging tasks.
- Fallback Scenario: If you experience issues with imaging or capturing images due to VPN tunneling problems, you may need to revert to the direct NFS mounting method.

Why This Change Matters

- Enhanced Security: Using a VPN tunnel adds an extra layer of security by encapsulating NFS traffic within a secure tunnel, protecting data during the imaging process.
- Improved Compatibility: The VPN tunnel can help navigate network restrictions or firewall rules that might block direct NFS traffic over port 2049.
- Operational Flexibility: Providing a fallback option ensures that imaging can continue smoothly, even if the new method encounters issues in certain network configurations.

How

Switching to the Fallback Mechanism: Direct NFS Mounting over Port 2049

If you encounter issues with the default VPN tunneling method during Windows imaging, you can switch back to the previous method of direct NFS mounting. Follow these steps on the Debian IVS server:

Create the Fallback Flag File

Open a terminal on the IVS server and create a flag file to signal that secure tunneling should be disabled:

```
sudo touch /etc/fw_insecure_nfs_mount
```

This file tells the system to use direct NFS mounting instead of the VPN tunnel.

Update UFW Firewall Rules

Allow traffic on port 2049, which is used by NFS:

```
sudo ufw allow 2049/tcp
sudo ufw allow 2049/udp
```

This updates the firewall to permit NFS communication over port 2049.

Restart Network Services

To apply the changes, restart all network-related services. The simplest method is to reboot the IVS server:

```
sudo reboot
```

Note: Rebooting ensures all services are restarted properly and the new settings take effect.

Reverting Back to Secure VPN Tunneling

Once any issues with VPN tunneling are resolved, you can switch back to the default secure method:

Remove the Fallback Flag File

Delete the flag file to re-enable secure tunneling:

```
sudo rm /etc/fw_insecure_nfs_mount
```

Remove UFW Firewall Rules for Port 2049

Close the ports that were opened for direct NFS access:

```
sudo ufw delete allow 2049/tcp
sudo ufw delete allow 2049/udp
```

This ensures that NFS traffic cannot bypass the VPN tunnel, maintaining a secure configuration.

Restart the IVS Server

Reboot the IVS server to apply the changes:

```
sudo reboot
```

This will restore the VPN tunneling over port 20490 for imaging tasks.

Important Considerations

- Security Implications: Reverting to direct NFS mounting over port 2049 is less secure than using the VPN tunnel. Use this fallback option only when necessary and ensure that your network is secure.
- Firewall Configuration: Make sure that your network's firewalls allow traffic over the necessary ports:
- Port 20490 for VPN tunneling (default method).
- Port 2049 for NFS if using the fallback method.
- Testing: After making changes, perform a test imaging task to confirm that everything is functioning as expected.
- Documentation: Keep a record of any changes made to the IVS server configuration for future reference and troubleshooting.

Related Content

- Setting up the IVS (Imaging Virtual Server)

Revision #3
★Created 18 October 2024 16:03:37 by Josh Levitsky
Updated 4 November 2024 13:40:09 by Josh Levitsky