High-Availability Pi-hole Synchronization & Docker Networking

Last Updated: March 2026 | **Target Hardware:** Micro PC Cluster (Intel i5 7th-gen)

Overview: This article documents the validated procedure for deploying a high-availability DNS sinkhole architecture using two micro PCs running CasaOS. [cite: 1, 3, 7] By leveraging **Gravity Sync**, the Secondary Pi-hole (192.168.x.x) mirrors the DNS payload of the Primary Pi-hole (192.168.x.x).

Prerequisites

- **Primary Server (LinuxServer):** 192.168.x.x
- **Secondary Server (LinuxServer2):** 192.168.x.x
- Pi-hole installed via Docker (CasaOS) on both nodes.
- Active SSH credentials for both servers.

Step 1: Install Gravity Sync on Both Servers

The synchronization tool must be installed on the host OS of **both** micro PCs. [cite: 16] To bypass retired domain links, execute the following command on both nodes:

```
curl -sSL https://raw.githubusercontent.com/vmstan/gs-install/main/gs-install.sh | bash
```

Step 2: Configure the Secondary Node

Because the Secondary Server "pulls" data from the Primary, execute the configuration wizard from **LinuxServer2 (192.168.0.152)**: [cite: 21]

1. **Initiate Wizard:** Run `gravity-sync config`.
2. **Define Remote Host:** Enter the IP of the Primary Server (192.168.x.x
3. **Authenticate:** Enter the Primary Server's SSH username and password to register RSA keys.

4. **Define Container Names:** Manually confirm the container names `pihole` for both Local and Remote prompts.

Step 3: Perform Initial Manual Sync

On the **Secondary Server (192.168.x.x)**, run the following to establish the baseline mirror:

```
gravity-sync pull
```

Step 4: Automate the Synchronization

To ensure future changes to blocklists or local DNS are synced automatically, enable the background service on the Secondary Server:

```
gravity-sync auto
```

Note: This registers a systemd timer that compares database hashes every 5 minutes with zero noticeable overhead on NVMe drives. [cite: 38, 39]

Step 5: Resolve Docker Network Restrictions (Pi-hole v6 Fix)

By default, CasaOS Docker deployments may cause Pi-hole to drop incoming LAN requests. [cite: 42] You must manually configure the secondary node to trust LAN traffic:.

- Log into the Secondary Web UI: `http://192.168.x.x:81/admin`
- Navigate to **Settings > DNS.**
- Toggle the top-right corner from **Basic** to **Advanced**.
- In **Interface settings**, select **Permit all origins**.
- Click **Save & Apply**.

Step 6: Validate Failover

Perform a direct query test from a Windows client on the same network: [cite: 51]

```
nslookup google.com 192.168.x.x
```

Expected Result: The terminal should return a list of IP addresses. [cite: 54] If it returns "Timeout," re-verify the settings in Step 5.

Revision #2
Created 2026-03-16 03:00:07 UTC by Francis
Updated 2026-03-26 13:00:20 UTC by Francis