

Actions for Communications Server Socket Directory Permissions

July 14, 2026

This PTF updates the AF_UNIX socket directories used by z/OS Communications Server. The AF_UNIX socket files within these directories enable communication between z/OS Communications Server components and Network Management Interface (NMI) applications.

- /var/pagent – new directory for Policy Agent AF_UNIX socket file
- /var/dm - used by the Defense Manager Daemon (DMD)
- /var/ike - used by the IKE daemon (IKED) and the z/OS UNIX ipsec command
- /var/sock - NMI sockets directory used by TCP/IP stack (real-time TCP/IP NMI), IKED (Local IPsec NMI) and NSSD (NSS NMI)

REQUIREMENTS:

The directories listed above must meet the following requirements

- must not be a symbolic link
- must have the sticky bit set - except for /var/ike directory
- write access must be restricted to the owning UID or group only (no write permission for others) - except for /var/sock directory

If these requirements are not met after applying this PTF:

- Policy Agent, DMD, IKED, NSSD will issue error messages and fail initialization
- The TCP/IP stack will remain active, but the real-time NMI function will not be available

USER ACTION:

The system programmer must verify that the directories meet the requirements and take corrective action where necessary. Use a superuser ID to issue the z/OS UNIX commands.

Step 1: Determine whether IP Security is used

Issue: `Netstat CONFIG/-f`

- If IpSecurity is set to No in the "IP Configuration Table", then IP security and IP Packet filtering are not in use. Proceed to Step 2.
- Otherwise, IP packet filtering is in use. IPsec protection might also be in use. Perform the following checks to determine if an action needs to be taken.

1a. Determine if Defensive Filtering and the Defense Manager Daemon is used:

- Issue: `ps -A`
- If DMD is not used, no action is required for the Defense Manager Daemon (DMD). Proceed to step 1b.
- If DMD is used, check the directory permissions for the DMD home directory /var/dm:
Issue: `ls -la /var/dm`
 - If /var/dm is not a symbolic link, has write access restricted to owner and group and has the sticky bit set, no action is required for /var/dm directory. Proceed to step 1b.
 - Otherwise, take the following actions:
 - Stop the DMD
 - If /var/dm is a symbolic link:
 - Note the target directory for the /var/dm symbolic link. It might be needed in later steps

Actions for Communications Server Socket Directory Permissions

July 14, 2026

- Remove the link: `unlink /var/dm`
- Create the `/var/dm` directory with the required permissions (write access is restricted to the owning UID and the sticky bit is set):
`mkdir /var/dm`
`chmod 755 /var/dm`
`chmod +t /var/dm`
- Permit the DMD user ID access to create, delete, read and write files to this directory:
`chown DMD /var/dm`
- Preserve any files in the DMD filters directory
 - If the `DefensiveFilterDirectory` statement in the DMD configuration file specifies a filters directory path that does not use the `/var/dm` symbolic link, no action is needed to preserve the files
 - Otherwise, either the `DefensiveFilterDirectory` parameter uses the `/var/dm` symbolic link or the default defensive filter directory `/var/dm/filters`. Any files in the filters directory should be preserved. There are 2 options. Either:
 - Update the `DefensiveFilterDirectory` parameter to specify the target of the `/var/dm` symbolic link OR
 - Create `/var/dm/filters` directory and copy the files from the previous filters sub-directory to `/var/dm/filters`.
- If `/var/dm` is not a symbolic link:
 - Ensure write access to the directory is restricted to the owning UID or group:
`chmod o-w /var/dm`
 - Set the sticky bit on `/var/dm`:
`chmod +t /var/dm`
- Check the DMD PID file:
 - If `/var/dm/dmd.pid` (or the path specified via the `DMD_PIDFILE` environment variable) is a symbolic link, then ensure the owning UID or GID matches the EUID or EGID that is assigned to the DMD.
- Start the DMD

1b. Determine if the IKE Daemon (IKED) is used:

- Issue: `ps -A`
- If IKED is not used, no action is required for IKED. Proceed to step 1c.
- If IKED is used, check the directory permissions for the IKED home directory `/var/ike`:
Issue: `ls -la /var/ike`
 - If `/var/ike` is not a symbolic link and has write access restricted to owner and group, no action is required for `/var/ike` directory. Proceed to step 1c.
 - Otherwise, take the following actions:
 - Stop the IKE daemon
 - If `/var/ike` is a symbolic link
 - Remove the link: `unlink /var/ike`
 - If the linked directory contains a file in the format `stackname.default`, recreate the file with the following command
`ipsec -f default -p stackname`

Actions for Communications Server Socket Directory Permissions

July 14, 2026

- If /var/ike is not a symbolic link:
 - Ensure write access to the directory is restricted to the owning UID or group
`chmod 775 /var/ike`
 - Permit the IKED user ID and any users with access to the EZB.IPSECCMD.sysname.stackname.CONTROL to create, delete, read, and write files in the /var/ike directory. See 'ipsec command security' in the z/OS Communications Server: IP System Administrator's Commands for more information.
- Start the IKE daemon
- Proceed to step 2.

1c. If IP Packet Filtering is used without IPsec (no IKED):

- If IP Packet Filtering is used but IKED is not running, check the directory permissions for the /var/ike directory:
Issue: `ls -la /var/ike`
- If /var/ike is not a symbolic link and has write access restricted to owner and group, no action is required for /var/ike directory. Proceed to step 2.
- Otherwise take the following actions:
- If /var/ike is a symbolic link:
 - Remove the link
`unlink /var/ike`
 - If the linked directory contains a file in the format *stackname.default*, recreate the file with the following command
`ipsec -f default -p stackname`
- If /var/ike is not a symbolic link:
 - Ensure write access to the directory is restricted to the owning UID or group
`chmod 775 /var/ike`
 - Permit the any users with access to the EZB.IPSECCMD.sysname.stackname.CONTROL to create, delete, read, and write files in the /var/ike directory. See 'ipsec command security' in the z/OS Communications Server: IP System Administrator's Commands for more information.

Step 2: Determine if Policy Agent is used

- Issue: `ps -A`
- If PAGENT is not in use, no action is required. Proceed to Step 3.
- If PAGENT is used, take the following actions:
- Stop the Policy Agent
- If /var/pagent directory exists, and it is a symbolic link:
 - Remove the link
`unlink /var/pagent`
- If /var/pagent directory exists, and it is not a symbolic link
 - Modify the /var/pagent directory using the following commands to ensure write access is restricted to the owning UID and the sticky bit is set

Actions for Communications Server Socket Directory Permissions

July 14, 2026

- ```
chmod 755 /var/pagent
chmod +t /var/pagent
```
- Permit the Policy Agent user ID access to create, delete, read, and write files to this directory
  - If /var/pagent does not exist and the Policy Agent user ID is not UID(0):
    - Create the directory with the required permissions (ensure write access is restricted to the owning UID and the sticky bit is set)

```
mkdir /var/pagent
chmod 755 /var/pagent
chmod +t /var/pagent
```
    - Permit the Policy Agent user ID access to create, delete, read, and write files to this directory

```
chown PAGENT /var/pagent
```
  - Start the Policy Agent
  - (Optional) If /tmp/unix.str socket file exists, delete it after this PTF is applied to the system using `rm /tmp/unix.str`.

---

### Step 3: Determine if the NMI sockets directory /var/sock is used

---

The Real-time TCP/IP network monitoring NMI provided by the TCP/IP stack, Local IPsec NMI provided by IKED and Network Security Services (NSS) NMI provided by NSSD create their socket files in the /var/sock directory. Check the directory permissions for the NMI sockets directory /var/sock.

- Issue: `ls -la /var/sock`
- If /var/sock is not a symbolic link and has the sticky bit set, no action is required for the /var/sock directory.
- Otherwise, take the following actions
- If /var/sock is a symbolic link:
  - Remove the link

```
unlink /var/sock
```
- If /var/sock is not a symbolic link:
  - Set the sticky bit on /var/sock

```
chmod +t /var/sock
```
- Issue: `ps -A`
  - If the NSS daemon is running, stop and start the NSS daemon
  - If the IKE daemon is running, stop and start the IKE daemon
- Issue the Netstat CONFIG/-f command to check if the NETMONITOR statement is configured in the TCP/IP profile
  - If all the parameters in the "Network Monitor Configuration Information" section are set to *No*, the network monitoring function is disabled and no action is required
  - Otherwise:
    - Turn off all active real time TCP/IP NMI services using a VARY OBEYFILE with NETMONITOR OFF.
    - Re-enable required services with a second VARY OBEYFILE. See 'Steps for modifying the NETMONITOR statement' in the TCP/IP profile.