Log Collector - File Access Permissions

Windows File Access Permission Issues

Common issues on Windows stem from strict file locking, UAC (User Account Control), and service account privileges. Elastic Agent/Filebeat often needs admin rights to read system logs or event logs, and problems arise when running without elevation or when files are locked by other processes.

Common Problems

- Access denied when reading directories or log files (e.g., C:\DIR1\DIR2\LOG_DIR), even if paths are correctly configured.
- Installation fails with "access is denied" due to symlinks in Program Files.
- Errors integrating Windows modules (e.g., event logs), where Filebeat can't access logs despite healthy status.
- Filebeat locks files, preventing access or permission views even as admin, often with rotated logs.
- Insufficient cluster privileges for Filebeat service, especially on remote servers without direct access.
- Microsoft module (e.g., Defender ATP) fails due to missing API permissions like Alert.Read.All.

Symptoms

- "Access denied" errors in Filebeat logs when opening files.
- No logs ingested despite agent showing healthy.
- File properties (permissions/ownership) inaccessible while Filebeat runs.
- Integration errors like incomplete documents or API permission failures.

Fixes

- Run commands/install as administrator (elevated console).
- Grant Filebeat service account (e.g., SYSTEM) read access to logs via icacls or Properties > Security.
- Add required API permissions for modules (e.g., Alert.ReadWrite.All for Defender).
- Restart Filebeat after fixing permissions to release locks.
- Use config options like ignore_older for problematic files.

Sources:

Problem with filestream access denied on windows - Beats - Discuss the Elastic Stack

Access is denied in case of elastic agent in Windows installation - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Errors with filebeat when trying to integrate any windows integration logs with the agent - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Windows filebeat cluster privileges - Elastic Stack / Beats - Discuss the Elastic Stack

Filebeat Microsoft Module - Documents Incomplete - Elastic Stack / Beats - Discuss the Elastic Stack

Common problems with Fleet and Elastic Agent | Elastic Docs

Filebeat locking files (Access Denied) - Elastic Stack / Beats - Discuss the Elastic Stack

Config file ownership and permissions | Beats

Linux File Access Permission Issues

On Linux, issues often involve POSIX permissions, user/group ownership, SELinux/AppArmor, and Docker/container restrictions. Elastic Agent/Filebeat typically requires root or specific group access to read /var/log/* files owned by syslog or adm.

Common Problems

- Permission denied when reading log files (e.g., /var/log/auth.log) due to ownership by syslog:adm.
- Nginx module fails with access errors on /var/log/nginx/* if Filebeat lacks permissions.
- Config file (filebeat.yml) permission denied, especially in Docker with strict.perms.
- Running as non-root user blocks access to sensitive logs or directories.
- SELinux blocking file system monitoring or modifications.
- Ownership changes needed but not propagating correctly in installs.

Symptoms

- "Permission denied" on opening files in logs.
- Exiting with config load errors like "open filebeat.yml: permission denied."
- No data ingested from modules despite running.
- High CPU or stalled harvesting due to access loops.

Fixes

- Run as root or add Filebeat user to groups (e.g., adm, syslog) with usermod -aG.
- Set --strict.perms=false in Docker and chown root:root on config.
- Use chmod 0640 or umask 0027 on configs; ensure owner is beat user or root.
- Adjust SELinux with setenforce 0 (permissive) or custom policies.
- Configure fanotify for file system events in advanced settings.

Sources:

Filebeat: permission denied - Elastic Stack / Beats - Discuss the Elastic Stack

Filebeat/module nginx ; problem with permissions - Elastic Stack / Beats - Discuss the Elastic Stack

Exiting: error loading config file: open filebeat.yml: permission denied - Elastic Stack / Beats - Discuss the Elastic Stack

Filebeat as a non-root user - Elastic Stack / Beats - Discuss the Elastic Stack

Configure Linux file system monitoring | Elastic Docs

File and Directory Permissions Modification | Elastic Security [8.19] | Elastic

Changing ownership of filebeat installtion from root - Elastic Stack / Beats - Discuss the Elastic Stack

So seriously, what permissions do beats need? - Elastic Stack / Beats - Discuss the Elastic Stack

Config file ownership and permissions | Beats

macOS File Access Permission Issues

macOS issues frequently involve System Integrity Protection (SIP), Full Disk Access requirements, and privacy settings, especially for Endpoint Security or Defend integrations. Problems are common on newer versions like Ventura or M1 chips.

Common Problems

- Full Disk Access not granted for ElasticEndpoint or agent, blocking log reads.
- Installation fails with "failed to fix permissions" on M1 Ventura.
- Permission issues on macOS 12.x+ for agent processes.
- Unhealthy agents due to Defend Endpoint lacking access.
- Plist or directory permissions denied (e.g., 0xd error).
- Config/registry files permission denied, like mkdir /var/log/elastic-agent.

Symptoms

- Install/upgrade errors like "permission denied" on directories.
- Agents degrade or show unhealthy status in Fleet.
- No threat monitoring or log collection due to privacy blocks.
- Errors loading state/registry: "open /filebeat/data/registry: permission denied."

Fixes

- Enable Full Disk Access in System Settings > Privacy & Security for ElasticEndpoint and elastic-agent.
- Set plist permissions to 644 and directory to 755.
- Run as root/sudo for install and operations.

- Check and fix ownership on configs (beat user or root).
- Restart agent after granting access; verify in logs.

Sources:

Enable Elastic Defend access on macOS | Elastic Docs

Enable access for macOS Ventura and higher | Elastic Security [8.19] | Elastic

Macos M1 Ventura 13.0.1 Elastic agent install fail - Elastic Security - Discuss the Elastic Stack

Elastic Agent 8.0.0 on macOS 12.x - Elastic Security / SIEM - Discuss the Elastic Stack

MacOS agents are unhealthy due to Defend Endpoint - Elastic Security - Discuss the Elastic Stack

Elastic Agent 7.13.1 keeps degrading endpoint security for macOS - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Deploying Filebeat on MacOS X - Elastic Stack / Beats - Discuss the Elastic Stack

Config file ownership and permissions | Beats

Exiting: Could not start registrar: Error loading state: open /filebeat/data/registry: permission denied - Elastic Stack / Beats - Discuss the Elastic Stack

[Elastic Agent] Issue when running the snapshot on macOS · Issue #17950 · elastic/beats

---

Revision #4
Created 27 November 2025 09:09:30 by Richmond Abella
Updated 4 December 2025 02:08:43