Common Encountered Issues

- Log Collector - Network Connection
- Log Collector - Check OS Version
- Log Collector - File Access Permissions

Log Collector - Network Connection

Windows Network Connection Issues

On Windows, network problems frequently involve firewall rules, service refusals, or integration degradations that prevent agents from connecting to remote services like Fleet Server or Elasticsearch.

Common Problems

- Fleet Server unreachable during agent enrollment, often due to Windows Firewall blocking ports.
- Agents become unhealthy due to degraded integrations (e.g., elastic-defend-endpoints), caused by connection failures to Elasticsearch.
- Connection refused by target machine, especially when standalone agents can't reach Elasticsearch or Kibana.
- VM or host connectivity issues after agent installation, where services fail to load intermittently.
- Logs not sent from endpoints outside the network, despite agent health reports being received. **(Often due to, Outbound firewall blocks, Proxy Misconfigurations, TLS Certificate trust issues)**
- Upgrade failures (e.g., exit status 0xc0000142) that indirectly cause persistent connection drops.

Symptoms

- Errors like "No connection could be made because the target machine actively refused it."
- Agent status shows "unhealthy" or "degraded" in Fleet, with no logs ingested.
- Intermittent loss of network/Internet connectivity post-installation.
- Filebeat logs show connection attempts to localhost:9200 despite custom configs.
- No data received in Elasticsearch, but agent metadata (e.g., status) is visible.

Fixes

- Open required ports (e.g., 8220/TCP for Fleet, 9200/TCP for Elasticsearch) in Windows Firewall.
- Run agent as administrator or check service account privileges, restart after config changes.
- Verify connectivity with tools like ping, curl, or telnet to the target URLs/ports.
- Re-enroll agents or reset policies in Fleet if integrations are degraded.

- For upgrade issues, reboot the system or terminate conflicting services.
- Use --insecure flags for testing certificate issues or configure proper SSL verification.

Sources:

Not able to start standalone Elastic Agent in my windows machine - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Elastic-agent.exe not running on target - Elastic Security - Discuss the Elastic Stack

Elastic Agents Unhealthy Elasticsearch connection failure · Security-Onion-Solutions/securityonion · Discussion #13416 · GitHub

Elastic Agent causing VM connectivity issues - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Elastic Agent Not Sending Logs from Endpoint Outside the Network (AWS Cloud deployemnt on VM) : r/elasticsearch

Common problems with Fleet and Elastic Agent | Elastic Docs

Elastic Agent causing VM connectivity issues - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

External NIC Blocked by Elastic Agent - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Elastic Agent - Filebeat still tries to connect to localhost:9200 despite different host being configured : r/elasticsearch

Elastic Agent not sending Data - Elastic Security - Discuss the Elastic Stack

Common problems with Fleet and Elastic Agent | Elastic Docs

Unable to Connect Filebeat to Elasticsearch - Elastic Stack / Beats - Discuss the Elastic Stack

Linux Network Connection Issues

Linux issues often stem from system-level security (e.g., SELinux) or firewalls blocking outbound/inbound traffic, especially in containerized environments like Kubernetes.

Common Problems

- Agents unable to connect to Fleet Server or Elasticsearch due to firewall blocks (e.g., firewalld/iptables).
- Localhost TCP connection failures in Elastic Endpoint, broken by third-party security tools. **(Localhost TCP connection failures in Elastic Endpoint” are usually caused by kernel hardening or 3rd-party security tools interfering with the eBPF/detection pipelines)**

- Network disruption on Kubernetes nodes after installing Elastic Security integration.
- SELinux does not block *system network discovery* but often blocks: **(Outbound connections, Binding to low ports, eBPF driver loading)**
- Filebeat connection resets to Logstash, often due to protocol mismatches or timeouts.
- Agents go offline intermittently if check-ins fail every 5 minutes.

Symptoms

- Errors like "connection reset by peer" in Filebeat logs.
- Agent status toggles between "offline" and "healthy" in Fleet.
- No data sent to Elasticsearch despite agent running (e.g., system module fails).
- High CPU or stalled operations due to repeated connection attempts.
- "Unhealthy" status from firewall or SSL config errors.

Fixes

- Open ports in firewall (e.g., firewall-cmd --add-port=8220/tcp) and verify with netstat.
- Run agent as root (sudo elastic-agent run) for foreground testing.
- Set SELinux to permissive mode (setenforce 0) or create custom policies.
- Test connectivity with curl to Fleet/Elasticsearch URLs; check for proxy needs.
- Restart services or server if network establishment issues persist.
- Disable third-party security temporarily to isolate localhost connection breaks.

Sources

Elastic agent unhealthy because of elastic defend integration - Elastic Security - Discuss the Elastic Stack

Elastic-agent.exe not running on target - Elastic Security - Discuss the Elastic Stack

Elastic Endpoint cannot connect to agent - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Network Disruption on Kubernetes Node with Elastic Security Integration on Debian - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Connection issues between Elastic Agent (Filebeat) and Logstash: connection reset by peer - Elastic Stack / Beats - Discuss the Elastic Stack

Elastic agent goes offline & healthy every 5 minutes - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

Elastic-agent with system module does not send any data to elasticsearch - Elastic Stack / Kibana - Discuss the Elastic Stack

elasticsearch - elastic-agent is not collecting data - Stack Overflow

Elastic agent unhealthy because of elastic defend integration - Elastic Security - Discuss the Elastic Stack

macOS Network Connection Issues

macOS issues are less common but often involve network extensions or privacy controls that disrupt connections, especially with security integrations like Elastic Defend.

Common Problems

- External NIC blocked by agent, leading to total network/Internet loss post-install.
- Rarely network resets when loading third-party extensions (e.g., in Elastic Defend kernel extensions).
- Agents not sending data due to connectivity failures to Kibana or Fleet.
- Degraded Elastic Endpoint state from connection issues.
- Osquery integration failures in new installations, indirectly affecting network-based data collection.
- Intermittent offline status if check-ins fail.

Symptoms

- Complete loss of network connectivity after agent install/uninstall cycles. **(Typically happens on, Ventura, Monterey, Sequoia)**
- Agent appears in Fleet, but no logs or data ingested.
- "Degraded" status in integrations like Endpoint.
- Errors in logs related to extension loading or connection refusals.
- Service termination or failures that disrupt ongoing connections.

Fixes

- Approve network extensions in System Settings > Privacy & Security.
- Run agent as root (sudo) for troubleshooting.
- Verify connectivity with ping/curl; ensure no firewall/proxy blocks.
- Modify exception lists in policies to resolve degraded states.
- Restart agent and check status (elastic-agent status); update to latest version for known fixes.
- Test enrollment tokens and URLs; re-enroll if needed

Sources:

External NIC Blocked by Elastic Agent - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Elastic Agent not sending Data - Elastic Security - Discuss the Elastic Stack

Elastic Endpoint in a degraded state - Elastic Security - Discuss the Elastic Stack

Elastic Agent known issues | Elastic Agent

External NIC Blocked by Elastic Agent - Elastic Security / Endpoint Security - Discuss the Elastic

Stack

Elastic Endpoint in a degraded state - Elastic Security - Discuss the Elastic Stack

Guide for Using the Elastic Agent

Log Collector - Check OS Version

Windows OS Version Compatibility Issues

Elastic Agent supports Windows Server versions (e.g., 2016+), Windows 10/11, but drops support for EOL versions like Windows 8 and Server 2012 from 7.17.19 onwards. It does not support 32-bit systems or ARM processors. Common issues arise from attempting installations on unsupported or EOL versions, leading to failures in enrollment, data collection, or security integrations like Elastic Defend (which requires Windows Security Center, absent on Servers).

Common Problems

- Installation or upgrades fail on EOL versions (e.g., Windows Server 2012R2), causing BSOD or rollback due to incompatibility checks.
- Elastic Defend not recognized or installable on Windows Server editions, as they lack Windows Security Center.
- Agent starts loops or stuck in updating state on Windows 10 with specific versions (e.g., 8.5.3 or during failed upgrades).
- No support for ARM processors, leading to installation errors on ARM-based Windows devices.
- Uninstall failures on Windows Server with newer versions (e.g., 9.1.4), leaving corrupted installations.
- Integration issues (e.g., Windows security events not processed) in certain agent versions like 9.1.4 or 8.19.4.

Symptoms

- BSOD or automatic rollback during upgrades on unsupported versions. (Rare case, happened on unsupported OS)
- Agent status stuck in "updating" or "unhealthy," with no data ingested.
- Errors like "unsupported OS" or "compatibility check failed" in installation logs.
- Service start loops or agent not running properly on older Windows 10 builds.
- Defend integration shows as unavailable or degraded on Servers.
- Uninstall errors leaving broken symlinks or processes.

Fixes

- Upgrade to a supported Windows version (e.g., Server 2016+ or Windows 10/11 non-ARM).

- For Defend, use non-Server editions or alternative integrations; avoid upgrades that trigger BSOD.
- Manually uninstall via command line (e.g., elastic-agent uninstall) and reinstall a compatible version.
- Update to latest agent versions (e.g., 9.1.4+ fixes for security events) and verify in Fleet.
- Check support matrix before install; use x86_64 hardware only.
- For start loops, restart service or downgrade/upgrade agent version.

***Sources**:*

Elastic Defend not recognized from Windows Server operating system - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Elastic Defend on windows 2012R2 - Elastic Security - Discuss the Elastic Stack

Can't uninstall agent 9.1.4 on Windows server · Issue #10546 · elastic/elastic-agent

OSquery fails to run after upgrade from versions before v8.15.4 due to stricter extension permission checks · Issue #6792 · elastic/elastic-agent

Elastic Agent known issues | Elastic Agent

[Fleet] Agent gets stuck in the updating state if the upgrade action fails · Issue #2508 · elastic/elastic-agent

Elastic agent start loop - Security - Spiceworks Community

Upgrades that fail and are rolled back can break the elastic-agent command symlink · Issue #2264 · elastic/elastic-agent

Linux OS Version Compatibility Issues

Elastic Agent requires native Linux installs (no WSL), supports x86_64 and aarch64 (from 7.16+), but not 32-bit. Minimum distro versions include RHEL/CentOS 7+, Ubuntu 18.04+, with drops for EOL like CentOS 8, Debian 9/10 from 7.17.19/23. Issues often occur on unsupported distros or kernels, affecting installation, data collection, or integrations.

Common Problems

- No support for older distros like RHEL 5/6, CentOS 8, Debian 9/10, leading to install failures.
- WSL (Windows Subsystem for Linux) unsupported, causing agent to fail enrollment or run.
- Compatibility issues on EOL distros (e.g., CentOS/RHEL 7 dropped from 7.17.23, Users can still install older agent version), resulting in no updates or stability problems.
- OSquery or other integrations fail after upgrades on unsupported kernels/versions (e.g., post-8.15.4).
- Agent stuck in updating or unenrolled state on certain distros during version mismatches.
- No data collected on specific versions like 8.15.0 due to compatibility checks.

Symptoms

- Installation errors like "unsupported distribution" or "GO lang incompatibility."
- Agent shows "unhealthy" or "updating" indefinitely, with rollback logs.
- No metrics/logs ingested despite agent running.
- Unenrollment or duplicate processes after policy updates on mismatched versions.
- Stability issues post-EOL, like failed check-ins.

Fixes

- Migrate to supported distros (e.g., RHEL 7+ for older, or 8+ for full support).
- Use native Linux instead of WSL; install via package managers like yum/apt.
- Upgrade agent to versions that align with your distro (e.g., avoid post-7.17.23 on RHEL 7).
- Remove conflicting integrations (e.g., OSquery) before upgrade, then reinstall.
- Force unenroll/re-enroll in Fleet for stuck states.
- Check GO support for your distro; upgrade OS if near EOL.

Sources:

Agent support for OS windows server and red hat - Elastic Stack / Beats - Discuss the Elastic Stack

Elastic Agent support RHEL 6 - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

8.7.0 and 8.6.2 agents get stuck in the updating state if the osquery.db file cannot be copied to the next version · Issue #2433 · elastic/elastic-agent

Elastic-Agents unexpectedly unenrolled after update to 8.16.x · Issue #6213 · elastic/elastic-agent

Some policy updates can cause duplicate Endpoint processes · Issue #2008 · elastic/elastic-agent

macOS OS Version Compatibility Issues

Elastic Agent supports macOS 11+ (Big Sur+), with x86_64 and aarch64 (M1/M2) from 8.2+. Drops support for EOL like 10.14/10.15 from 7.17.19. Issues are common on newer versions like Sequoia (support in progress) or Ventura, often involving SIP, extensions, or version-specific errors.

Common Problems

- Support for macOS Sequoia (15.x) in progress, but Elastic Defend installation may not be fully supported yet.
- Errors initializing version info or running on Ventura (13.x+), especially M1 chips.
- Dropped support for older macOS (10.14/10.15), causing install/upgrade failures.
- Network issues like external NIC blocked by agent in Monterey (12.x+).
- OSquery fails post-upgrade on versions before 8.15.4 due to checks.
- Agent stuck updating or unenrolled on version mismatches.

Symptoms

- Installation errors like "failed to fix permissions" on Ventura/M1.

- Agent degrades or shows unhealthy due to unsupported extensions on Sequoia.
- No data or logs ingested post-upgrade.
- Network connectivity loss after install on older macOS versions.
- Rollback logs or stuck "updating" status.
- Unenrollment after updates.

Fixes

- Upgrade to supported macOS (11+ for Intel, 8.2+ for M1/M2).
- For Sequoia, wait for official support or test Defend manually.
- Run as root (sudo elastic-agent run) for troubleshooting on Ventura+.
- Approve network extensions in System Settings for NIC issues.
- Uninstall OSquery before upgrade, then reinstall.
- Force policy reset or re-enroll for stuck states.

Sources:

macOS Sequoia (15.x) Support - Elastic Security - Discuss the Elastic Stack

Error initializing version information: reading package version from file....package.version: no such file or directory · Issue #3285 · elastic/elastic-agent

External NIC Blocked by Elastic Agent - Elastic Security / Endpoint Security - Discuss the Elastic Stack

[Fleet] Agent gets stuck in the updating state if the upgrade action fails · Issue #2508 · elastic/elastic-agent

Compatibility

Support Matrix | Elastic

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