

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 \(AWS Cloud deployment on VM\)](#)

[: 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., firewall/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](#)

Revision #6

Created 27 November 2025 09:08:56 by Richmond Abella

Updated 4 December 2025 02:08:17