Resolving Network Issues with FileWave Server or Boosters on macOS when using Carbon Black EDR Extension

What

FileWave has observed network issues when the Carbon Black EDR (Endpoint Detection and Response) extension is installed on a FileWave server or booster running on macOS. The issues can manifest as Boosters stopping to answer or respond, leading to disruption in device management workflows.

When/Why

The issue occurs when there is a high volume of network traffic and the Carbon Black EDR extension is inserted into the network stack. The extension's presence in the network stack seems to cause performance issues, which can result in network connectivity and communication problems.

How

If you experience network issues with FileWave when the Carbon Black EDR extension is installed, you can resolve the problem by removing the extension from the FileWave server or booster. This solution has been proven to resolve the issue in multiple cases. On a macOS system, you can use the following command in Terminal.app to list all kernel extensions:

```
systemextensionsctl list
```

The output will appear like this:

```
--- com.apple.system_extension.endpoint_security
enabled    active    teamID    bundleID (version)    name    [state]
*    *    7AGZNQ2S2T    com.vmware.carbonblack.cloud.se-agent.extension (3.7.2fc81/3.7.2fc81)
com.vmware.carbonblack.cloud.se-agent.extension    [activated enabled]
```

You should check the output of this command to determine if the Carbon Black EDR extension is present on your system. If you have concerns about the performance of the Carbon Black EDR extension in high-volume network traffic environments, it may be worth contacting Carbon Black's support team to discuss the issue further.

Related Content

- General Troubleshooting and Errors
- FileWave Log File Locations
- Booster Installation

Digging Deeper

Kernel extensions (KEXTs) are software modules that can be inserted into the macOS kernel to extend its functionality. They can be used to add new features, support new hardware, or modify the behavior of existing drivers. KEXTs run in kernel mode, which means they have the highest level of privilege and can access system resources directly.

However, KEXTs can also introduce stability and performance issues. Since they run in kernel mode, they can crash the system or cause conflicts with other KEXTs. In addition, they can potentially introduce security vulnerabilities if they're not properly designed or implemented.

The Carbon Black EDR extension is an example of a kernel extension that inserts itself into the macOS network stack. By doing so, it's able to monitor network traffic and detect security threats. However, in high-volume network traffic environments, the extension can cause performance issues, which can lead to disruptions in FileWave's device management workflows.

To manage kernel extensions on macOS, Apple provides the systemextensionsctl command. This command allows you to list, enable, disable, and uninstall extensions. If you're experiencing issues with a KEXT, you can use this command to disable or uninstall it to see if that resolves the issue.

In general, it's important to use kernel extensions with caution and only install those from trusted sources. If you're unsure whether a particular KEXT is necessary or safe to use, you should consult with the vendor or seek advice from a subject matter expert.

Revision #2
Created 13 June 2023 02:54:43 by Josh Levitsky
Updated 16 July 2023 23:38:35 by Josh Levitsky