

Accept

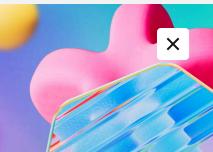
Reject

Manage cookies

Microsoft Ignite

Nov 19-22, 2024

Register now >





Learn

Discover ∨

Product documentation ∨

Development languages ~

Topics \

Sign in

Azure

Products ∨ Architecture ∨

Develop ∨

Learn Azure ∨

More ∨

Portal

Free account

Learn / Azure / Defender for Cloud /



File Integrity Monitoring in Microsoft Defender for Cloud

Article • 08/28/2024 • 5 contributors

Feedback

In this article

Which files should I monitor?

Next steps

File Integrity Monitoring (FIM) examines operating system files, Windows registries, application software, and Linux system files for changes that might indicate an attack.

Defender for Cloud recommends entities to monitor with FIM, and you can also define your own FIM policies or entities to monitor. FIM informs you about suspicious activity such as:

- File and registry key creation or removal
- File modifications (changes in file size, access control lists, and hash of the content)
- Registry modifications (changes in size, access control lists, type, and content)

Many regulatory compliance standards require implementing FIM controls, such as PCI-DSS and ISO 17799.

Which files should I monitor?

When choosing which files to monitor, consider the files that are critical for your system and applications. Monitor files that you don't expect to change without planning. If you choose files that are frequently changed by applications or operating system (such as log files and text files) it will create noise, making it difficult to identify an attack.

Defender for Cloud provides the following list of recommended items to monitor based on known attack patterns:

① Note

This table applies to <u>File Integrity Monitoring using Microsoft</u>

<u>Defender for Endpoint</u>. For the recommended items to monitor in FIM over Log Analytics, see <u>Recommended items to monitor</u>.

Expand table



>

File Integrity Monitoring over AMA (Deprecated) File Integrity Monitoring over Log Analytics

- > Just-in-time access
- Endpoint detection and response
- > Review server protection

- > Common questions (FAQ)
- > Defender for Containers
- > Database protection
- > Defender for App Service
- > Defender for Storage
- > Defender for Key Vault
- Defender for ResourceManager
- > Defender for DNS
- > DevOns security
- Download PDF

Linux Files	Windows files	Windows registry ke
/bin	C:\config.sys	SOFTWARE\Microsoft\
/bin/passwd	C:\Windows\regedit.exe	SOFTWARE\WOW643
/boot	C:\Windows\System32\userinit.exe	HKLM\SOFTWARE\Mic
/etc/*.conf	C:\Windows\explorer.exe	HKLM\SOFTWARE\Mic
/etc/cron.daily	C:\autoexec.bat	HKLM\SOFTWARE\Mic Folders
/etc/cron.hourly	C:\boot.ini	HKLM\SOFTWARE\Mic
/etc/cron.monthly	C:\Windows\system.ini	HKLM\SOFTWARE\Mic
/etc/cron.weekly	C:\Windows\win.ini	SOFTWARE\Microsoft\
/etc/crontab		SOFTWARE\WOW643
/etc/init.d		SOFTWARE\WOW643
/opt/sbin		SOFTWARE\WOW643
/sbin		SOFTWARE\WOW643
/usr/bin		SOFTWARE\WOW643
/usr/local/bin		SECURITY\POLICY\SE(
/usr/local/sbin		
/usr/sbin		
/bin/login		
/opt/bin		

Next steps

In this article, you learned about File Integrity Monitoring (FIM) in Defender for Cloud.

Next, you can:

 Enable File Integrity Monitoring using Microsoft Defender for Endpoint

Feedback

Was this page helpful?

☐ Yes ☐ No

Provide product feedback ☑ | Ask the community ☑

Additional resources

M Training

Module

Implement change tracking and file integrity monitoring for Windows IaaS VMs - Training

Implement change tracking and file integrity monitoring for Windows IaaS VMs

Certification

Microsoft Certified: Security Operations Analyst Associate - Certifications

Investigate, search for, and mitigate threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender.

S English (United States)

✓ Your Privacy Choices

☆ Theme ∨

Manage cookies Previous Versions Blog ☑ Contribute Privacy ☑ Terms of Use Trademarks ☑

© Microsoft 2024