Considerations for configuring antivirus software for ArcGIS Enterprise hosts

Version 1.3

Esri Software Security and Privacy

December 2020

Summary

This document contains general guidelines to help choose and configure antivirus software for hosts running ArcGIS Enterprise.

More Information

We strongly recommend that you individually assess the security risk for each host that runs ArcGIS Enterprise in your environment and that you select the tools that are appropriate for the security risk level of each.

We also recommend that before you roll out any virus-protection project, you test the entire system, including desktop and web clients under a full load and measure any changes in stability and performance.

Virus protection software requires system resources to execute and in some cases may interfere with software performance. You must perform testing before and after you install your antivirus software to determine whether there is any performance effect on your ArcGIS Enterprise hosts, and you must balance your desired security level against any performance impacts.

Security risk factors

Risk factors that help quantify your organization’s risk tolerance include:

- The value to your business of the information that is stored in ArcGIS
- The value to your business of other information stored on the host
- The required security level protecting that information
- The cost of losing access to that information
- The risk of a virus, malware or bad information propagating from that that host to other resources in your environment

High-risk servers

Any interconnected server is at some risk of infection. The highest-risk servers generally meet one or more of the following criteria:

- The servers are accessible from the public Internet.
- The servers have open ports that are not governed by a firewall.
- The servers read or execute files hosted on other servers.
- The servers provide content over http/https, such as ArcGIS Enterprise.
- The servers also host file shares.

Virus tool types

Real-Time/Active virus scanning: These applications continuously check client and server machines and devices for incoming, outgoing and newly created files for viruses and malware.

Endpoint protection will typically include anti-malware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems

Active virus scanning or Endpoint protection software may cause the following issues in ArcGIS Enterprise components:

- May slow or interfere with the installation or configuration of ArcGIS Software or a major software update
- May slow or interfere with the creation or restoration of backup files
- May slow or interfere with map or scene service tile creation

In these situations, you may choose to temporarily relax active virus scanning and endpoint protection processes. Relaxing these processes introduces risk. You must balance your performance expectations against your security needs.

Virus Scan and Removal Software: Virus Scan software scans existing files for file infection. It detects files after they are infected by a virus. Virus scans (or sweeps) typically run on a set schedule and complement active virus scanning and endpoint protection.

Virus Scanning may cause the following issues in ArcGIS Enterprise components:

- If the virus scanner has opened a database file and still has it open when ArcGIS Enterprise tries to open the database (such as when ArcGIS Enterprise components start), the database to which the file belongs might be marked as suspect.

- Virus scanning may potentially result in false positives if software components or temporary files created by software resemble heuristics of known malware variants.

Web Application Firewall (WAF): A WAF or Web Application Firewall helps protect web applications and application servers by filtering and monitoring HTTP traffic between a server and the Internet. A WAF inspects HTTP traffic before it reaches your server and protects it by filtering out threats that could damage your site functionality or compromise data. By deploying a WAF in front of a web application server, a shield is placed between the web application and the Internet. Many WAFs can protect against attacks like Malicious file execution – a harmful technique which allows a person to execute code remotely after a user accepts a malicious file. Esri recommends leveraging a WAF with ArcGIS Enterprise as a component in a defense in depth posture.

When should ArcGIS Enterprise files and directories be excluded from virus scanning?

Backup or Restore Operations

You can create backups of your ArcGIS Enterprise deployment and restore the most recent backup in the event of a failure or corruption. This allows you to recover the portal items, services, and data that existed at the time you created the backup.

Use the webgisdr utility to export backup files of the following components of your ArcGIS Enterprise deployment:

- Your portal items and settings
- GIS services and settings
- The relational data store and tile cache data store

When a backup or restore is started, Active Virus scanners may scan each file as it is created on disk. These files are created in a %temp% location or in the target directory the backup or restore operation writes to. This scanning can cause write delays and increase the time it takes for a backup or restore process to complete.

Product installation, upgrade, or removal

Similarly, product installation, upgrade, and uninstall processes write to disk. Active Virus scan may increase the time required to install, upgrade or remove a product.

Map, Image or Scene tile or tile package creation or copy

The creation or map or scene tiles is a resource intensive operation that typically involves thousands of write operations as tile bundles are created. The time it takes to complete a caching operation may be impacted. You will see a greater impact on cache creation time if the option to create an exploded cache is used. In an exploded cache each tile is stored as a single file. With a compact format cache, larger files called bundles that store multiple tiles are created. Tiles are written into the ArcGIS Account's %temp% directories before being aggregated into .bundle files. The compact cache option usually is a better option as:

- Caches are easier to copy because the number of files is reduced.
- The total size on disk of the cache is reduced.
- Tiles are generally created more quickly because disk I/O is reduced during tile creation.
- Scalability is improved when creating tiles with multiple-machine deployments, because of reduced network traffic.

Anti-Virus software should be re-enabled after these activities are completed.

Directories and processes to exclude from virus scanning

When you configure your antivirus software settings, you may choose to exclude the following files or directories (as applicable) from real-time virus scanning. This improves the performance of the software and helps make sure that the files are not locked when the ArcGIS Server, ArcGIS Enterprise Portal, or ArcGIS Datastore services must use them.

If these files in these directories become infected, your antivirus software cannot detect the infection. Schedules for scanning these directories and processes can be relaxed but should still be periodically scanned during times of low use. You must balance your performance expectations against your security needs.

ArcGIS Server directories:

- \arcgisserver\directories\arcgiscache\
- \arcgisserver\directories\arcgisjobs\
- \arcgisserver\directories\arcgisoutput\
- \arcgisserver\directories\arcgissystem \

- \arcgisserver\config-store\

ArcGIS DataStore directories

- \arcgisdatastore\pgdata\
- \arcgisdatastore\nosqldata\

ArcGIS Enterprise Portal directories:

- \arcgisportal\temp\
- \arcgisportal\dsdata\
- \portalforarcgis\content\arcgisportal\db\
- \ portalforarcgis\content\arcgisportal\index\

Service account temp directories

These directories are owned by the process owner. In Windows, these are referred to as runAs accounts or service accounts. In Linux, these are process owners.

- \%ArcGIS Account%\appData\Local\temp\

Processes (Windows Hosts)

- %ProgramFiles%\ArcGIS\Server\framework\etc\service\bin\ArcGISServer.exe
- %ProgramFiles%\ArcGIS\Server\framework\runtime\ArcGIS\bin\ArcSOC.exe
- %ProgramFiles%\ArcGIS\Server\bin\ArcSOC.exe
- %ProgramFiles%\ArcGIS\Server\framework\runtime\jre\bin\rmid.exe
- %ProgramFiles%\ArcGIS\Server\framework\runtime\jre\bin\javaw.exe
- %ProgramFiles%\ArcGIS\Portal\framework\service\bin\ArcGISPortal.exe
- %ProgramFiles%\ArcGIS\Portal\framework\runtime\jre\bin\javaw.exe
- %ProgramFiles%\ArcGIS\Portal\framework\runtime\jre\bin\java.exe
- %ProgramFiles%\ArcGIS\Portal\framework\runtime\pgsql\bin\postgres.exe
- %ProgramFiles%\ArcGIS\DataStore\framework\etc\service\bin\ArcGISDataStore.exe
- %ProgramFiles%\ArcGIS\DataStore\framework\runtime\jre\bin\javaw.exe
- %ProgramFiles%\ArcGIS\DataStore\framework\runtime\jre\bin\java.exe

- %ProgramFiles%\ArcGIS\DataStore\framework\runtime\pgsql\bin\postgres.exe
- %ProgramFiles%\NotebookServer\framework\etc\service\bin\ArcGISNBServer.exe

Which ArcGIS Enterprise files and directories should NOT be excluded from virus scanning?

These directories should not be excluded from virus scan activities. When users upload content into ArcGIS Enterprise, the content is placed into these directories. It is important that the content created in these folders be scanned upon creation to prevent potentially malicious files from being introduced into the system.

- \ arcgisserver\config-store\uploads
- \arcgisserver\directories\arcgissystem\arcgisuploads
- \portalforarcgis\content\arcgisportal\content\items