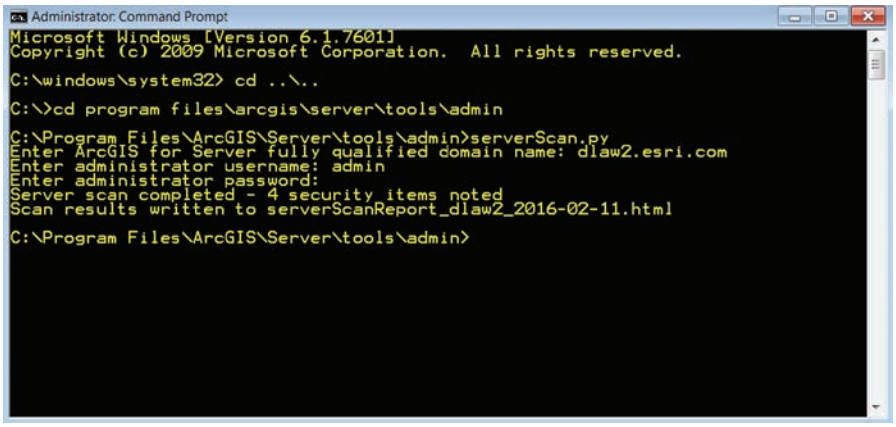
Apply Security Best Practices to an ArcGIS Server Site

By Derek Law, Product Manager, ArcGIS for Server

The new command line tool called serverScan.py is one of the many enhancements in ArcGIS 10.4 for Server. It scans your ArcGIS Server site and checks to see whether it has been configured following the security best practices recommended by Esri. After the tool executes, it returns a report that lists all the recommended actions that you can apply to make your ArcGIS Server site more secure so that it will better protect your data and GIS web services. This tip shows you how to run the serverScan.py tool and interpret the results in the report it generates.

This tool is written in Python and can be found in the ArcGIS Server installation directory (<installation location>\arcgis\server\tools\admin). In a default ArcGIS Server installation, it is located at C:\Program Files\ArcGIS\Server\tools\admin. (Note: ArcGIS for Server is the product name. This tip only applies to the GIS server [ArcGIS Server] component of ArcGIS for Server. Although it is meant to work with ArcGIS 10.4 for Server, it can be applied to server sites for ArcGIS 10.3 for Server. Portal for ArcGIS 10.4 also includes a new command line tool called portalScan.py that performs a similar best practices security check on your Portal.)



↑ A new tool called serverScan.py runs from the command line and helps you follow Esri best practices for enabling security.

Step 1

Open a new command prompt window on your server computer. Ensure that you have the appropriate administrator privileges on the computer.

Step 2

In the command prompt window, navigate to the ArcGIS Server installation directory. Then navigate to the admin folder in the Tools directory. For example, in a default ArcGIS Server installation, the tool is located in C:\Program Files\ArcGIS\Server\tools\admin.

Step 3

Run the serverScan.py tool. Before it executes, it will prompt you for three input parameters: the ArcGIS server machine fully qualified name, the GIS server site admin login, and the GIS server site admin login password.

For Example

```
<Server_machine_name>.<domain>.com
<Admin login name>
<password>
```

Step 4

After you enter the last parameter, hit Enter, and the serverScan.py tool will run. The serverScan.py tool generates a report written in HTML format. By default, the report will be named verrScanReport_<machine name>_<dategenerated> and will be stored at the same location where the tool executed—in this case, in the admin folder.

Step 5

Open Windows Explorer and navigate to the report's location. In this example, the location is C:\Program Files\ArcGIS\Server\tools\admin.

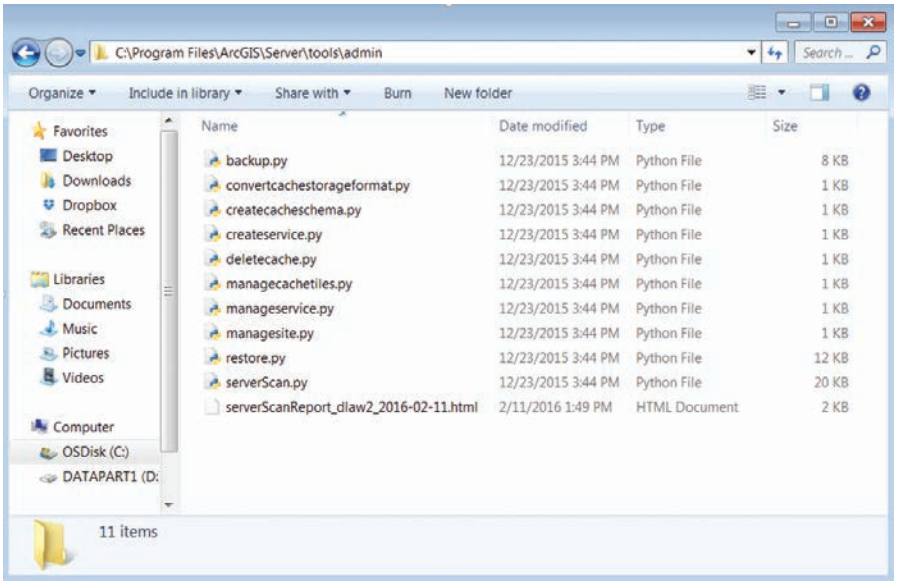
Step 6

Double-click to open the report in a web browser and view its contents. Notice that each reported item has a unique ID, is categorized based on the severity of the issue, and includes a name and description. The report recommends parameter settings you can set and/or adjust in your ArcGIS Server site so that you can make it more secure.

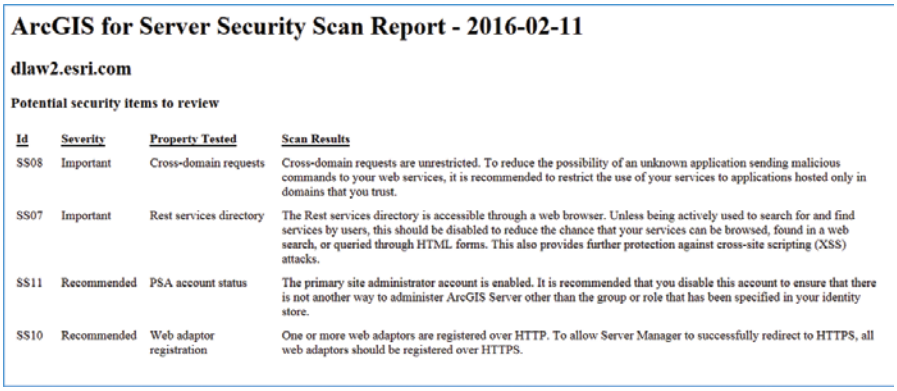
Step 7

Review the report results and check them against the ArcGIS for Server online help topic "Scan ArcGIS Server for security best practices." This help topic describes each of the 12 Esri security best practices for an ArcGIS Server site. You have the option to apply all, some, or none of these to your site. The more best practices you apply, the more secure your ArcGIS Server site will be.

See how easy it was to check that your ArcGIS Server site was properly configured following the Esri best practices for enabling security? For more information on securing your ArcGIS Server site, see the help topics "Configuring a secure environment for ArcGIS Server" and "Best practices for configuring a secure environment."



← The output from serverScan.py will be stored in the same location where the tool executed. In a default installation, that will be the admin folder.



ArcGIS for Server Security Scan Report - 2016-02-11

dlaw2.esri.com

Potential security items to review

Id	Severity	Property Tested	Scan Results
SS08	Important	Cross-domain requests	Cross-domain requests are unrestricted. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust.
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks.
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your identity store.
SS10	Recommended	Web adaptor registration	One or more web adaptors are registered over HTTP. To allow Server Manager to successfully redirect to HTTPS, all web adaptors should be registered over HTTPS.

↙ Open the report in a web browser to view descriptions of issues and suggestions for improving security.