2019 Esri Canada

User Conferences

GIS-The Intelligent Nervous System
ENTREPRISE? FEDERATION?
BASE DEPLOYMENT? PORTAL?
Getting Started with ArcGIS Enterprise: Base Deployment Patterns Highlighting Security Best Practices

Nathan Enge, Senior Technical Solutions Specialist
nenge@esri.ca
@nza_enge
TO PORTAL, OR NOT TO PORTAL
THAT IS THE QUESTION
GAME OVER, MAN!

GAME OVER!
Software Components

ArcGIS Enterprise = ArcGIS Web Adaptor + Portal for ArcGIS + ArcGIS Server + ArcGIS Data Store + Notebook Server + Other Server Roles
ArcGIS Server Licensing Roles

ArcGIS Server

GIS Server
Image Server
GeoAnalytics Server
GeoEvent Server*
Notebook Server**

One software component, multiple server roles

* GeoEvent Server requires installing the ArcGIS Server software + overlaying the GeoEvent Server setup
** Notebook Server is a separate download and install that does not require the main ArcGIS Server setup
Coming from ArcGIS Server to ArcGIS Enterprise

Typical deployment of ArcGIS Server

- Web Adaptor
- ArcGIS Server
- Geodatabase

Base deployment of ArcGIS Enterprise

- Portal for ArcGIS
- ArcGIS Server (GIS Server role as hosting server)
- ArcGIS Data Store (relational + tile cache)
- Enterprise Geodatabase (SQL Server, Oracle, PostgreSQL, etc.)
- ArcGIS Web Adaptor
- ArcGIS Web Adaptor
- ArcGIS Web Adaptor
Integrates with your organization’s existing web server to provide a single endpoint that distributes incoming requests and enables you to use web-tier authentication.
Portal for ArcGIS
The software component that enables the ArcGIS Enterprise portal. Portal for ArcGIS is the web frontend and API backend that supports a user’s interaction and overall experience with your Web GIS.
In a base deployment ArcGIS Server should be configured with a GIS Server licensing role and as the hosting server. In this capacity it gives you the ability to publish and share maps and layers from ArcGIS Pro using your own business databases and by copying data to the server.
The ArcGIS managed data repository that stores the Enterprise portal’s hosted content. It is not a replacement for your enterprise geodatabases.

ArcGIS Data Store

The ArcGIS managed data repository that stores the Enterprise portal’s hosted content. It is not a replacement for your enterprise geodatabases.

- Relational
- Tile Cache
- Spatiotemporal
Enterprise Geodatabase
The user-managed data repository that stores organizational datasets
Base ArcGIS Enterprise deployment

ArcGIS Enterprise comprises four software components. The minimum setup of ArcGIS Enterprise is called a base ArcGIS Enterprise deployment, and consists of the following:

- **ArcGIS Server**, licensed as ArcGIS GIS Server Standard or ArcGIS GIS Server Advanced and configured as the hosting server for your portal.
- **Portal for ArcGIS.**
- **ArcGIS Data Store**, configured as a relational and tile cache data store.
- Two installations of ArcGIS Web Adaptor, one installation for traffic to your ArcGIS Enterprise portal and another for traffic to your hosting server.

You can install the base deployment across one or more machines, any of which can be physical, virtual, or cloud machines. For details about the required machine specifications for the ArcGIS Enterprise components, see the **system requirements**.
Functionality of Base Deployment

Everything from traditional ArcGIS Server + Self Service
Functionality of Base Deployment

- Esri Story Maps
- Configurable App Templates
- ArcGIS Sites
- Web AppBuilder for ArcGIS
- Crowdsource Apps
- AppStudio for ArcGIS
Choosing a base deployment pattern
- **Software Tiers**
  - Portal for ArcGIS + Web Adaptors (web tier)
  - ArcGIS Server (app tier)
  - ArcGIS Data Store/EGDB (data tier)
- **All-in-one single machine deployment**
  - Great, simple approach for small and medium sized organizations
  - For Development systems

**Multi-machine deployment**
- Web Adaptor
- Portal for ArcGIS
- ArcGIS Server
- ArcGIS Data Store
Choosing a base deployment pattern

- Software Tiers
  - Portal for ArcGIS + Web Adaptors (web tier)
  - ArcGIS Server (app tier)
  - ArcGIS Data Store/EGDB (data tier)

- All-in-one single machine deployment
  - Great, simple approach for small and medium sized organizations
  - For Development systems
Base Deployment
DID YOU
ORDER THE INSTALL?
<table>
<thead>
<tr>
<th></th>
<th>Install Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install &amp; authorize Portal component. Create new site</td>
</tr>
<tr>
<td>2</td>
<td>Install &amp; configure Portal Web Adaptor</td>
</tr>
<tr>
<td>3</td>
<td>Install &amp; authorize Server component. Create new site</td>
</tr>
<tr>
<td>4</td>
<td>Install &amp; configure Server Web Adaptor</td>
</tr>
<tr>
<td>5</td>
<td>Install &amp; configure Data store component to Server</td>
</tr>
<tr>
<td>6</td>
<td>Federate Server to Portal</td>
</tr>
<tr>
<td>7</td>
<td>Designate Server as hosting</td>
</tr>
</tbody>
</table>
PREREQUISITES???

WE'LL DO IT LIVE, JUST DO IT LIVE
WHY DON’T YOU TAKE A PICTURE

IT’LL LAST LONGER
Prerequisites

• Setups for ArcGIS Server, Portal for ArcGIS, ArcGIS Data Store, and ArcGIS Web Adaptor.

• License files for authorizing your software. This will include an authorization file for ArcGIS Server and a .JSON file for authorizing portal members and app bundles.

• Ensure that port 80/443 is enabled for HTTP/S communication aka, IIS installed

• 6080,6443,7080,7443…

• A trusted CA-signed certificate for enabling HTTPS. (domain-signed OK)

• Domain Name System (DNS) resolves the FQDN to the hostname of the ArcGIS Enterprise (e.g. maps.yourville.com → servername.domain.local) for access from both internal and public networks and on the ArcGIS Enterprise server itself.

Sufficient disk space and memory. >16GB RAM and at least >20GB HDD
Base Deployment Configuration Quick Steps

1 Configure Web Adaptors

- ArcGIS Web Adaptor (Portal)
- Portal for ArcGIS
- ArcGIS Server (hosting server)
- ArcGIS Data Store (relational + tile cache)

To configure the Web Adaptor, specify the URL and an administrator account for your Portal.

Portal URL:
Example: https://machine.domain.com:7443

Administrator Username:
portaladmin

To configure the Web Adaptor, specify the URL and an administrator account for your ArcGIS Server.

ArcGIS Server URL:
https://serverhost.domain.com:6443

Administrator Username:
portaladmin

Enable administrative access to your site through the Web Adaptor.

The following servers are configured with your Web Adaptor:
- PACIFIC-AGS-SER.ESRIPACIFIC.CA

Last updated on 4/29/2019 7:02:43 AM

Use the following URL to access the Services Directory:
https://esripacific.ca/server/rest/services
Base Deployment Configuration Quick Steps

2 Configure the data store and register with server

- Portal for ArcGIS
- ArcGIS Server (hosting server)
- ArcGIS Data Store (relational + tile cache)

ArcGIS Data Store Type

Select an ArcGIS Data Store type to configure:

- **Relational**
  - Required data store type for ArcGIS Enterprise, used by hosted feature layers, spatial analysis tools, and Insights for ArcGIS

- **Tile Cache**
  - Stores tile caches for hosted scene layers

- **Spatiotemporal**
  - Archives real-time data for GeoEvent Server, and stores output from GeoAnalytics Server tools

[Back] [Next] [Help]
Base Deployment Configuration Quick Steps

3 Federate server with the portal and designate as hosting server

- ArcGIS Web Adaptor (Portal)
- ArcGIS Web Adaptor (Server)
- Portal for ArcGIS
- ArcGIS Server (hosting server)
- ArcGIS Data Store (relational + tile cache)

Add one or more servers to your portal:

- https://esriapacifica.ca/image
- https://esriapacifica.ca/server

Hosting Server

- Optionally choose one of your servers to act as your portal's hosting server. Your portal members will be able to publish hosted services to this server. A relational ArcGIS Data Store must be configured with the GIS Server site before it can be designated as the portal's hosting server.

Feature Analysis - Standard Tools

- The analysis service in your portal is enabled by default when a hosted server is configured. Click Disable to remove the analysis service from your portal configuration.
Tutorial: Set up a base ArcGIS Enterprise deployment

ArcGIS 10.7 (Windows) | Other versions

This tutorial provides an overview of setting up a single machine base ArcGIS Enterprise deployment. This configuration is commonly used for testing and prototyping purposes. It enables self-service mapping and can be used with ArcGIS Pro, ArcMap, and other client applications. Although this configuration can be used in a production system, your performance, system architecture, and other requirements will dictate the deployment pattern your production deployment follows.

The resulting deployment will include the following:

- An ArcGIS Server machine licensed as ArcGIS GIS Server and used as a hosting server
- Portal for ArcGIS
- ArcGIS Data Store configured as a relational and tile cache data stores
- Two ArcGIS Web Adaptors
How to deploy

• It’s not all about deploying components by hand anymore!

For GIS professionals and developers

ArcGIS Enterprise Builder
A wizard that installs and configures ArcGIS Enterprise on a single machine.

For those who want to deploy in the cloud

Machine Images and Cloud Builders
Easily deploy and configure ArcGIS Enterprise in the two most popular public cloud environments.

For those with DevOps experience

Chef
PowerShell DSC
Automate installation and configuration in your infrastructure.
SCALE OUT, THEY SAID
IT'S EASY, THEY SAID
Expanding out from the base deployment – new Server Roles

A couple of starting points:

• You can have any number of federated ArcGIS Server sites within your ArcGIS Enterprise deployment
  - Just because you can, doesn’t always mean you should
  - Don’t overcomplicate past a single machine if you don’t need to

• Different server roles have different recommendations and restrictions
Expanding out from the base deployment

- Multiple reasons and ways to add to the base deployment

1. Adding additional GIS Server sites
   - Add capacity, separate workloads

2. Adding additional capabilities
   - Image Server
   - GeoEvent Server
   - GeoAnalytics Server
   - Notebook Server – since 10.7
Adding Image Server to your deployment

- Image Server provides four key capabilities
  - Dynamic image services from your own mosaic datasets
    - Serve large collections of imagery, LiDAR and rasters with dynamic mosaicking and on-the-fly processing
  - Raster Analytics Site (designate in the portal)
    - Extracting information from imagery- distributed processing and analysis of imagery and rasters creating new persisted output at full source resolution, enable deep learning raster analysis
  - Raster Hosting Site (designate in the portal)
    - Upload and publish an image collection from raster data store
    - Hosts results from raster analytics
  - Ortho mapping
    - Server-side processing of satellite, aerial, or drone imagery into digital terrain models and orthomosaics

Adding Image Server to your deployment

- One Image Server site for both capabilities
Adding Image Server to your deployment

- Separate Image Server sites for each capability

Base deployment

- Image Server Site (dynamic image services)
- Image Server Site (raster analytics)
- Image Server Site (raster hosting)

Optional choice:
- Raster Analysis Server: esripacific.ca/server
- Image Hosting Server: esripacific.ca/image
Security Best Practices
Defense in Depth Paradigm

- Security Plans have many "layers" multiple levels of security
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a "layer"
"LAYERS"
Agenda

• **ArcGIS Server**
  - Enable and use HTTPS
  - Disable services directory
  - Restrict cross domain requests
  - Restrict System folder permissions
  - Disable PSA account
  - Scan Server script

• **Portal for ArcGIS**
Review: ArcGIS Server Administrator Directory

https://localhost:6443/arcgis/admin

- Web App, provides interface into an ArcGIS Server site
- Many security settings enabled via this interface

ArcGIS Server Administrator Directory

Home

You should use ArcGIS Server Manager for managing services and GIS servers. The Administrator directory is intended for advanced, programmatic access to the server, likely through the use of scripts.

Site Root - /

Current Version: 10.7.1

Resources: machines services security system data uploads logs kml info mode usagereports publicKey

Supported Operations: generateToken exportSite importSite deleteSite

Supported Interfaces: REST
HE'S PROBABLY THINKING ABOUT HER

I NEED TO ENABLE SSL
Enable and Use HTTPS

• **HTTPS** – *Hypertext Transfer Protocol Secure*
• Initial step in creating a secure environment should always be to encrypt traffic
• Protects against a simple network sniffer
• Enabled by default in 10.4+
• Recommended to restrict to HTTPS only if possible
• **ArcGIS Server Admin Directory**
  - Security > config > update

ArcGIS Server Administrator Directory

Update Security Configuration

- **Warning**
  Once this operation completes, ArcGIS Server may be restarted. During this time, your ArcGIS Server resources will be temporarily unavailable.

Security Configuration

- **Protocol:** HTTPS Only
- **SSL Protocols:** TLSv1.2
- **SSL Cipher Suites:**

HTTP Strict Transport Security (HSTS) enabled: 

Disable the Services Directory

- ArcGIS REST Services Directory exposes web services api in HTML format
  - https://server.mydomain.com/arcgis/rest
- Recommended NOT to expose REST services directory on Production Servers

Before

ArcGIS REST Services Directory
Home > services

Folder: /
Current Version: 10.71
View Footprints In: ArcGIS Online Map Viewer
Folders:
- Hosted
- System
- Utilities

Services:
- SampleWorldCities (MapServer)

After

ArcGIS REST Framework
Home

Error: Services Directory has been disabled.
Code: 403
How to Disable the Services Directory

- **Server Administrator Directory**
  - System > Handlers > Rest > Servicesdirectory > edit
  - Uncheck **Services Directory Enabled** option

- **Help topic**: Disable the Services Directory
Restrict Cross-Domain (CORS) Requests

- For JavaScript applications, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing)
- Required when making POST requests to Feature or GP services on a different server

enterprise.arcgis.com > Search “cross-domain requests”
How to Restrict Cross-Domain Requests

• By default, ArcGIS Server allows all cross-domain requests
• These can be restricted in the Server Administrator Directory
  - system > handlers > rest > servicesdirectory > edit
  - AllowedOrigins - specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services
• Does NOT restrict overall access to the web services
Restrict System Folder Permissions in Manager

- Verify System folder permissions are limited to Administrators and Publishers only
  - Prevents potential Denial of Service due to resource consumption, service deletion, etc.
  - Usually changed from default when troubleshooting
Disable Primary Site Administrator (PSA) Account

- Recommend disable the PSA account to remove an alternate method of administering ArcGIS Server outside of your enterprise users
- Access the Server Administrator Directory
  - Security > PSA > disable

ArcGIS Server Administrator Directory

Primary Site Administrator Account
Manage the primary site administrator account.
Disabled: false
Supported Operations: update, enable, disable
Supported Interfaces: REST
Scan GIS Server for Security Checks

- serverScan.py is a script in the Server installation directory
  - Located: <install directory>/ArcGIS/Server/tools/admin
- Script checks for security settings → generates a report that makes recommendations to improve security

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS02</td>
<td>Critical</td>
<td>Standardized queries</td>
<td>Enforcing standardized queries is disabled. To provide protection against SQL injection attacks, it is critical that this option be enabled. More information</td>
</tr>
<tr>
<td>SS09</td>
<td>Important</td>
<td>Dynamic workspace</td>
<td>Map service: SampleWorldCities One or more dynamic workspaces are registered with this map service. To prevent a malicious party from obtaining the workspace ID and potentially gaining access, these dynamic workspaces should be removed. More information</td>
</tr>
<tr>
<td>SS07</td>
<td>Important</td>
<td>Rest services directory</td>
<td>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. More information</td>
</tr>
<tr>
<td>SS12</td>
<td>Recommended</td>
<td>Feature service operations</td>
<td>Feature service: HostedAirports This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication.</td>
</tr>
<tr>
<td>SS11</td>
<td>Recommended</td>
<td>PSA account status</td>
<td>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 configuration. More information</td>
</tr>
</tbody>
</table>
Agenda

- ArcGIS Server
  - Portal for ArcGIS
    - Enforce HTTPS Communication only
    - Disable ArcGIS Portal Directory (aka Sharing API)
    - Restrict proxies
    - Disable the ‘Create An Account’ button on the sign-in page
    - Restrict cross-domain (CORS) requests
    - Trusted servers list
    - Scan Portal script
Enable HTTPS Communication

- Enforce HTTPS so that all communication in your portal is sent using HTTPS
- Configure your portal and the web server hosting ArcGIS Web Adaptor to only allow communication through HTTPS
Disable ArcGIS Portal Directory (Production Servers)

- Provides an HTML-based representation of all of Portal items
  - services, web maps, and content
- Recommend disable this to reduce the chance that your items can be browsed, found in a web search, or queried through HTML forms

Before

ArcGIS Portal Directory | Home
Root

Current Version: 7.1
Child Resources: Search Community Content Portals OAuth2
Supported Operations: Generate Token

After

ArcGIS Portal Directory

API Reference
How to Disable ArcGIS Portal Directory

• Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - Set “disableServicesDirectory” = true
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
  - Storing credentials (Single Sign On)
  - OGC Services
  - Non-CORS Systems

![Diagram showing restriction of machines accessible by Portal](image-url)
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines.
- By default the portal's proxy is open.
  - Your Portal can be used to launch attacks against internal and external targets.
How to Restrict Proxies

- Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
- Add “allowedProxyHosts” property and specify the list of approved hostnames
Disable ‘Create An Account’ on Sign In Page

- Disable the ability to create a new built-in Portal account
- My Organization > Edit settings > Security
Restrict Cross-Domain (CORS) Requests

- Limits external JavaScript applications making CORS requests to Portal items
- Does NOT restrict overall access to Portal items
Trusted Servers

- A list of servers to where web-tier credentials will be included when a web map or app makes a CORS request to a secured resource.
Allow Portal Access

• Needed to access layer from other Portals that use SAML authentication
SAML Access to any ArcGIS Enterprise

• Bring secured services together from anywhere!
Scan Portal for Security Checks

- `portalScan.py` is a script in the Portal installation directory
  - Location: `<install_directory>\ArcGIS\Portal\tools\security`
- When you run the script, it checks for security settings → generates a report that makes recommendations to improve security

<table>
<thead>
<tr>
<th>Potential security items to review</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Id</strong></td>
</tr>
<tr>
<td>PS01</td>
</tr>
<tr>
<td>PS03</td>
</tr>
<tr>
<td>PS04</td>
</tr>
<tr>
<td>PS06</td>
</tr>
<tr>
<td>PS05</td>
</tr>
<tr>
<td>PS09</td>
</tr>
</tbody>
</table>
I WANT ENTERPRISE GIS

ESRI GEONET, TECH SUPPORT, TSS, PROFESSIONAL SERVICES, EAP, AM
THAT'S WHAT I DO
I DRINK AND I KNOW THINGS
ARCGIS ENTERPRISE

MAKE IT SO
Session Rating