Securing ArcGIS Server Services
An Introduction

David Cordes & Derek Law
Esri - Redlands, CA
Agenda

- Security in the context of ArcGIS for Server
- Background concepts
- Access
- Authentication
- Securing web services
- Encryption
- 10.2: Understanding standardized queries
- Summary
ArcGIS for Server Security

- Protecting your ArcGIS Server site and its web services
- Control who has access
  - Integrate with your organization’s IT infrastructure
- Define what valid users can do
  - Permissions
ArcGIS for Server 10.1 Architecture

ArcGIS Account (OS level)

GIS Server
- Service directories
- Manager
- Server Administrator API

http://6080

ArcGIS Server site
- Primary Site Administrator (PSA)
- Configuration store
- Server directories
- Data

Securing ArcGIS Server Services - An Introduction
ArcGIS for Server Access

- **User** – Valid login to access Server site
- **Role** – Grouping of users
  - 3 types
    1. Administrators – Full admin control
    2. Publishers – Publish web services
    3. Users – View web services

- **Identity store** – Defines your users and roles
ArcGIS for Server: User considerations

- Where are you users coming from?
  - Determines which type of identity store you should use
- Intranet = Windows Active Directory or LDAP
- Internet = Built-in or custom
ArcGIS for Server: Role considerations

• How much control do I have on my ArcGIS Server site?
  - Managed by me, within my Dept, or
  - Managed by my organization’s IT Dept

• May affect where you define your roles
ArcGIS for Server: Identity store

- **Identity store** – Defines your users and roles

- 3 different options
  1. **Built-in** (default)
  2. **Register with an enterprise identity store**
     - Windows Active Directory
     - LDAP
  3. **Mixed mode**
     - Users from enterprise identity store
     - Roles from built-in store
Demo

ArcGIS Server Manager
Show users and roles
Authentication Tier / Method

- **Authentication**
  - Check and verify user identity

- 2 options
  1. **GIS Tier**
     - Uses tokens to authenticate
  2. **Web Tier**
     - Uses HTTP Authentication
       - Basic, Digest, Integrated Windows, Client certificates, Custom
Server Architecture - Security

- ArcGIS Server site
  - + Identity store
  - + 3rd party web server
  - + Web Adaptor
ArcGIS for Server – Web Adaptor

- Enables Server to work with 3rd party web server
- Leverage web server features
- Provides more flexibility to control site access
- Conceptually like a reverse proxy
GIS Tier Authentication

- GIS Server checks credentials

- **Token**
  - Unique identifier sent from Server to client to identify an interaction session

1. Credentials sent to GIS server
2. Checked with ID store
3. Esri token sent back to client
Web Tier Authentication

- Must use Web Adaptor
- HTTP authentication
# GIS Tier vs. Web Tier Authentication

<table>
<thead>
<tr>
<th></th>
<th>GIS Tier / Token</th>
<th>Web Tier / HTTP Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Public / anonymous possible</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Clients Supporting</strong></td>
<td>Esri</td>
<td>All, including OGC</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>Enable SSL</td>
<td>Web Adaptor(s) required Basic – require SSL Digest – special setup IWA – Windows only</td>
</tr>
</tbody>
</table>
Demo

ArcGIS Server Manager
Show how to set-up authentication in wizard

Show IIS configuration of Web Adaptor
Securing GIS Web Services

- Set permissions for roles on folders and services
  - Administrators / Publishers grant permissions
- All new services are public by default
  - Anonymous access
- Can specify whether folders require HTTPs
Demo

ArcGIS Server Manager

Show how to secure a service
Show Flex App accessing a secure service
Supporting Public and Private Services

• How do I access public (anonymous) services?
• Web Server blocks me
Supporting Public and Private Services

- Use Web tier authentication
- Configure 2 Web Adaptors for the Server site

1. Configured for public services
2. Configured for private services
Demo

Contrast public and private services
Considerations for Server Publishers

- Publisher considerations
  - Limit web service capabilities
  - Ownership-based access control for web editing
  - Dynamic workspaces
Encryption / HTTPS

- HTTPS encrypts content sent/received
- HTTPS requires certificates
  - Statement of identity, statement of trust, public key
Encryption / HTTPS

- HTTPS not enabled by default in ArcGIS Server
  - Recommend enabling it
- ArcGIS Server comes with a self-signed certificate
  - Means that no trusted authority vouches for the server
  - In many organizations – not a problem, users don’t directly access ArcGIS Server
  - Can replace with a certificate trusted by a certifying authority (CA)
Using a CA-signed certificate

Log into Admin Directory

Click on machines
Using a CA-signed certificate

- Click on the machine you are interested in
- Click on sslcertificates
Using a CA-signed certificate

• Can see the automatically generated certificate
• Operations
  - `generate` creates a new one
  - `importRootOrIntermediate` to trust CA’s
  - `importExistingServerCertificate` brings in an existing certificate and the private key (advanced)
• We’ll pick generate
Using a CA-signed certificate

Before

After
Using a CA-signed certificate

- I now see my new certificate
- Click on it
- Click on `generateCSR`
Using a CA-signed certificate

- Send the CSR to your CA
- They will send you a server cert and their root/intermediate certs
- Import your CA’s root and intermediate certificates first
Using a CA-signed certificate

ArcGIS Server Administrator Directory

Home > machines > YINYANG.ESRI.COM > ssldirectories

SSL Certificates

- yinyang.esri.com
- selfsignedcertificate

Supported Operations: generate importRootOrIntermediate importExisting
Supported Interfaces: REST

Certificate - yinyang.esri.com

Certificate Information
- Alias name: yinyang.esri.com
- Creation date: Jul 8, 2013
- Entry type: PrivateKeyEntry
- Certificate chain length: 1
- Certificate[1]:
  - Owner: O=Esri, CN=YINYANG.ESRI.COM, OU=Development, L=Redlands, ST=California, C=US
  - Issuer: O=Esri, CN=YINYANG.ESRI.COM, OU=Development, L=Redlands, ST=California, C=US
  - Serial number: 229c8658
- Certificate fingerprints:
- Signature algorithm name: SHA1withRSA
- Version: 3
- Extensions:
  - #1: ObjectId: 2.5.29.14 Criticality=false
  - SubjectKeyIdentifier [ ]
  - KeyIdentifier [ ]
  - SubjectPublicKeyInfo [ ]

Supported Operations: generateCSReq export delete ImportSignedCertificate
Supported Interfaces: REST
Using a CA-signed certificate

### Machine - YINYANG.ESRI.COM

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>YINYANG.ESRI.COM</td>
</tr>
<tr>
<td>Admin URL</td>
<td><a href="http://yinyang.esri.com:6080/arcgis/admin">http://yinyang.esri.com:6080/arcgis/admin</a></td>
</tr>
<tr>
<td>Platform</td>
<td>Linux-amd64-2.6.32.12-0.7-default</td>
</tr>
<tr>
<td>Server Start Time</td>
<td>2013-06-16T01:25:14,96</td>
</tr>
<tr>
<td>Web server maximum heap size</td>
<td>256 MB</td>
</tr>
<tr>
<td>Web server SSL Enabled</td>
<td>false</td>
</tr>
<tr>
<td>Web server SSL Certificate</td>
<td>SelfSignedCertificate</td>
</tr>
</tbody>
</table>

### Operation - edit

**Warning**
A change in the web server's heap size will cause the web server to be restarted.

#### Server Machine Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>YINYANG.ESRI.COM</td>
</tr>
<tr>
<td>Admin URL</td>
<td><a href="http://yinyang.esri.com:6080/arcgis/admin">http://yinyang.esri.com:6080/arcgis/admin</a></td>
</tr>
<tr>
<td>Web server maximum heap size</td>
<td>-1 MB</td>
</tr>
<tr>
<td>Web server SSL Certificate</td>
<td>yinyang.esri.com</td>
</tr>
<tr>
<td>App server maximum heap size</td>
<td>256 MB</td>
</tr>
<tr>
<td>SOC maximum heap size</td>
<td>64 MB</td>
</tr>
<tr>
<td>Synchronize</td>
<td>false</td>
</tr>
</tbody>
</table>

### Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMXPort</td>
<td>4000</td>
</tr>
<tr>
<td>OpenEJBPot</td>
<td>4001</td>
</tr>
<tr>
<td>NamingPort</td>
<td>4002</td>
</tr>
<tr>
<td>DerbyPort</td>
<td>4003</td>
</tr>
</tbody>
</table>

**Resources:** status, sslcertificates

**Supported Operations:** edit, start, stop, unregister

**Supported Interfaces:** REST
Demo

Enabling HTTPS
Standardized queries

• Prior to 10.2, query syntax unique for each database

• Led to two problems
  1. Software passes through queries directly to database scanning for malicious attacks; hard to prevent many creative SQL injection attacks
  2. Hard for developers to write query code
Standardized queries

- 10.2 introduces standardized queries
  - Same syntax against all databases (FGDB syntax)
  - Each query parsed and prepared before sending to the database
  - Stronger defense against SQL injection attacks
  - Easier to write queries
Standardized queries

• This could be a breaking change for custom applications

• Things likely to break:
  - Date queries
  - Using non-SQL standard functions specific to a database
  - Putting non-where-clause syntax into where clause (such as `group by`)
Standardized queries

- What can you do if things break?
  - Recommended: update your applications to use new syntax
  - Disable standardized queries. Not recommended for security reasons. Puts your Server at risk.
Summary

• Security in the context of ArcGIS for Server
• Background concepts
• Access
• Authentication
• Securing web services
• Encryption
• 10.2: Understanding standardized queries
• Summary

How to configure
Security presentations at UC

ArcGIS Online
- Security and ArcGIS Online
- Building Secure Applications

ArcGIS for Server
- Securing ArcGIS Server Services Introduction
- Securing ArcGIS Server Services Advanced
- Best Practices in Setting Up Secured Services in ArcGIS for Server

ArcGIS Platform
- Designing an Enterprise GIS Security Strategy
<table>
<thead>
<tr>
<th>Name</th>
<th>Date / Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Secure Applications</td>
<td>Wed @ 10:15</td>
<td>07 A/B</td>
</tr>
<tr>
<td></td>
<td>Thurs @ 1:30</td>
<td>07 A/B</td>
</tr>
<tr>
<td>Securing ArcGIS Server Services – Introduction</td>
<td>Tues @ 1:30</td>
<td>Ball06 D</td>
</tr>
<tr>
<td></td>
<td>Fri @ 9:00</td>
<td>07 A/B</td>
</tr>
<tr>
<td>Securing ArcGIS Server Services – Advanced</td>
<td>Wed @ 3:15</td>
<td>Ball06 F</td>
</tr>
<tr>
<td></td>
<td>Thurs @ 3:15</td>
<td>Ball 06 F</td>
</tr>
<tr>
<td>Security and ArcGIS Online</td>
<td>Wed @ 10</td>
<td>Hall G: 2</td>
</tr>
<tr>
<td></td>
<td>Thurs @ 11</td>
<td>Hall F: 1</td>
</tr>
<tr>
<td>ArcGIS Online and Cloud Computing Security Best Practices</td>
<td>Thurs @ 8:30</td>
<td>Hall H – GIS Discussion Lounge</td>
</tr>
<tr>
<td>Designing an Enterprise GIS Security Strategy</td>
<td>Wed @ 3:15</td>
<td>31C</td>
</tr>
</tbody>
</table>
Thank you…

Please fill out the session evaluation

First Offering ID: 1212
Second Offering ID: 1412

Online – www.esri.com/ucsessionsurveys
Paper – pick up and put in drop box