Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

Securing ArcGIS Services

James Cardona

Agenda

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

How to configure

ArcGIS for Server Security

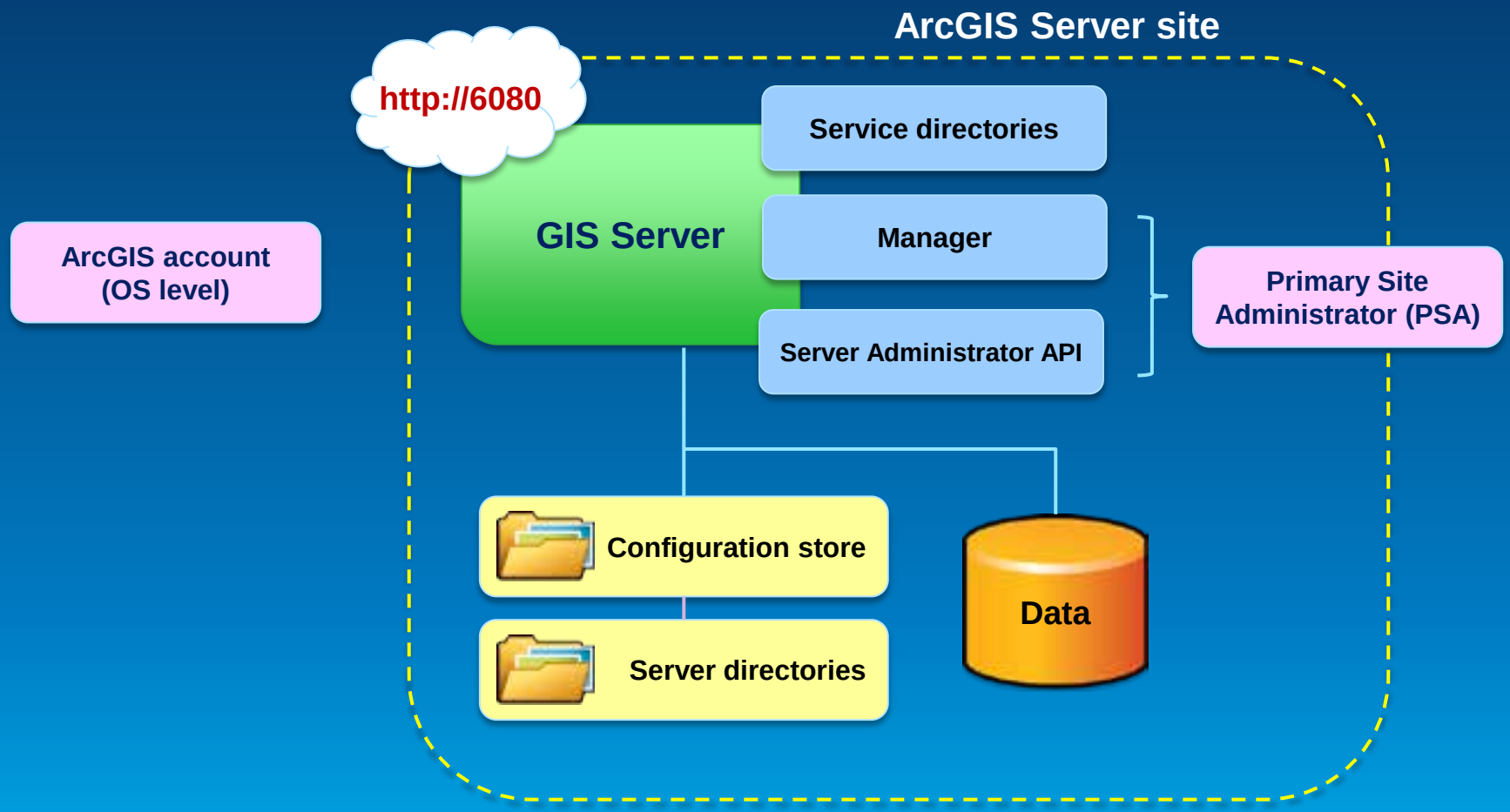
- Protecting your ArcGIS Server site and its web services
- Control who has access
  - Integrate with your organization’s IT infrastructure
- Define what valid users can do
  - Permissions

ArcGIS Server Help Documantation Security Links

Server for Linux Security Help

Server for Windows Security Help

ArcGIS for Server 10.2 Architecture



Limit “Run As” account to minimal privileges

Windows

- Access to data / software
- Run as service
- No administrative privileges
- Does not need “Allow log on locally”

Linux

- Upgrade to 10.1+, root not needed
- Access to data / software
- No administrative access.

Limit ArcGIS Server file access

- **Lock down ArcGIS Server directories.**

Config-store	Directories	Install Directory
• Run As • GIS Admins	• Run As	• Run As • GIS Admins

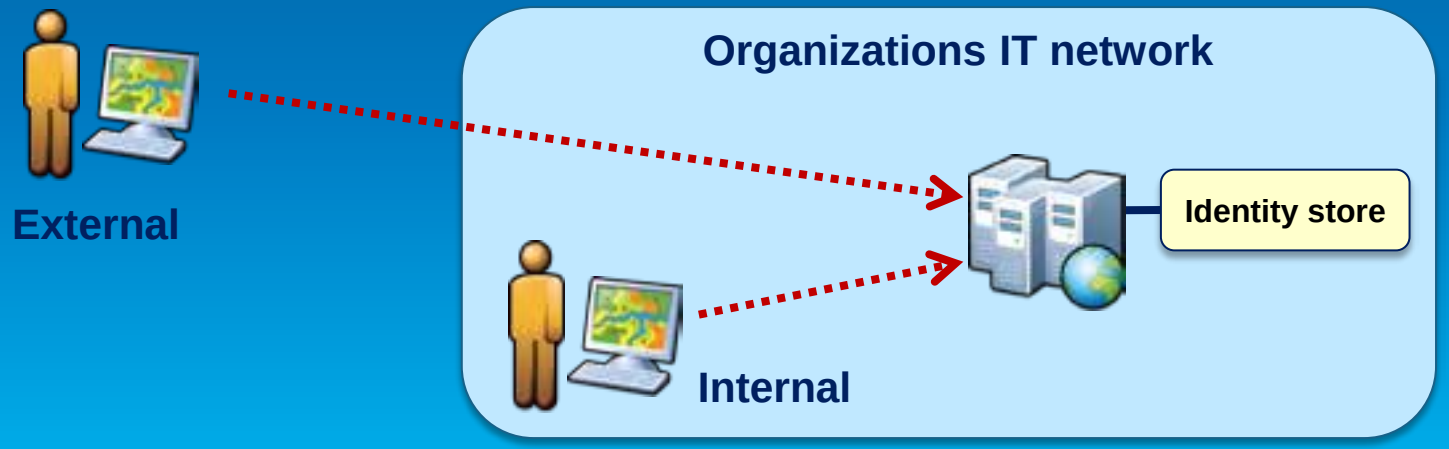
ArcGIS for Server Access

- **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

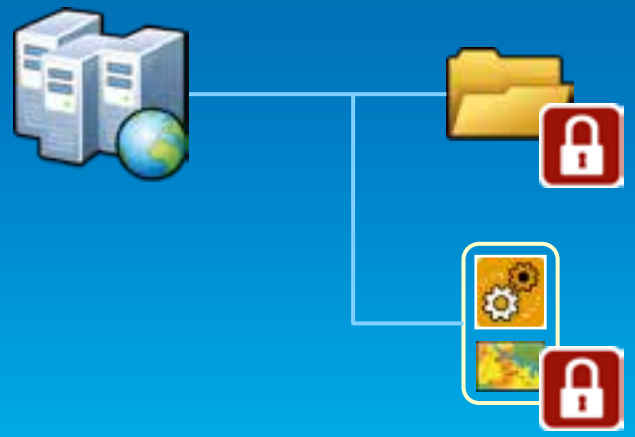
- **Identity store** – Defines your users and roles
- 3 different options
  1. **Built-in** (default)
  2. **Register with an enterprise identity store**
     - Windows Active Directory
     - LDAP
  3. **Mixed mode**
     - Users from enterprise identity store
     - Roles from built-in store

Demo

ArcGIS Server Manager
Show users and roles

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



Considerations for Server Publishers

- **Publisher considerations**
  - **Limit web service capabilities**
  - **Ownership-based access control for web editing**
  - **Dynamic workspaces**

Documentation links

- Configuring services help
- Ownership based access control help
- Dynamic layers and workspaces help

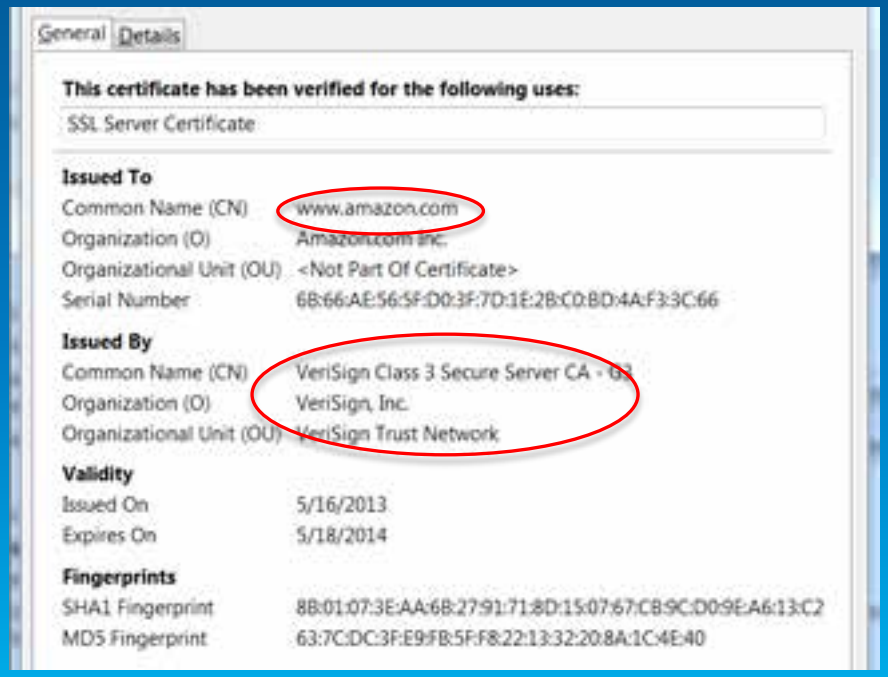
Demo

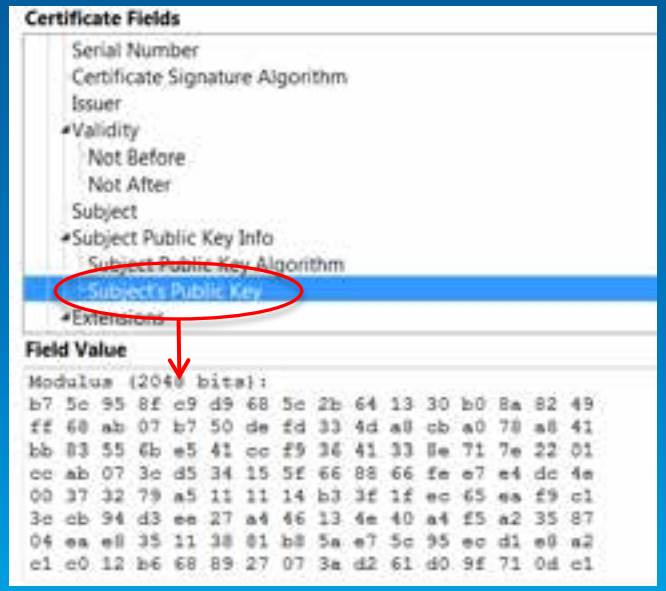
ArcGIS Server Manager
Show how to secure a service

Show how to set capabilities on a service

Encryption / HTTPS

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



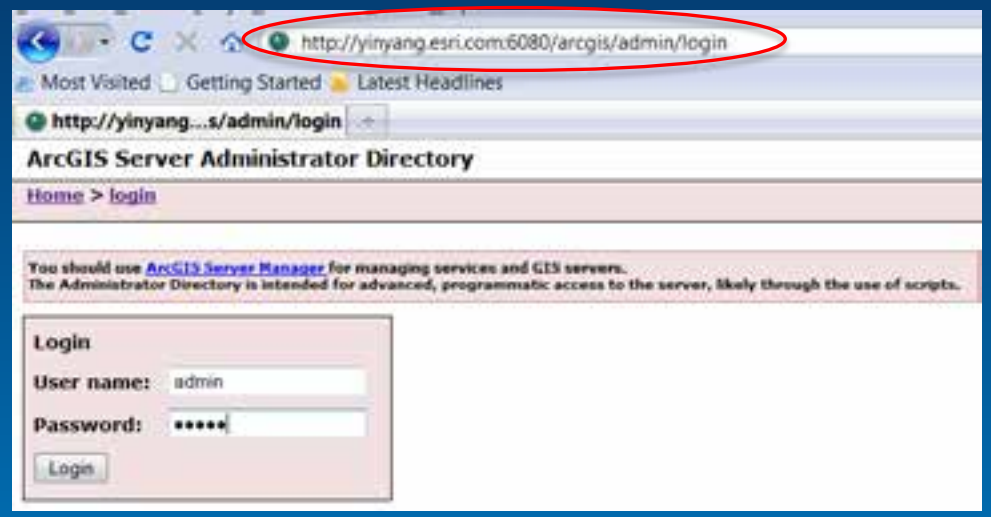


Encryption / HTTPS

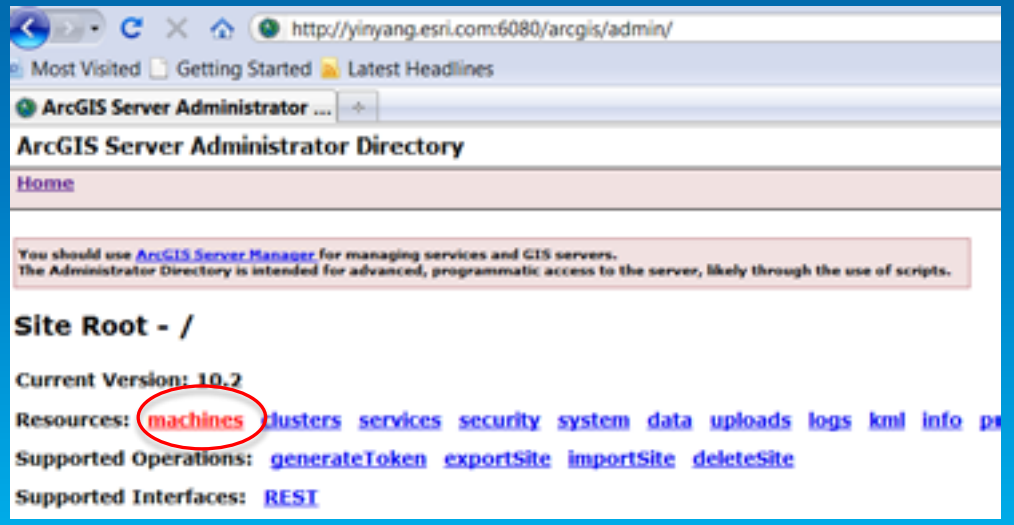
- HTTPS not enabled by default in ArcGIS Server.
  - Recommend enabling it.
- ArcGIS Server comes with a self-signed certificate.
  - Self-signed means that no trusted authority vouches for the server.
  - In many organizations – not a problem, users don’t directly access ArcGIS Server.
  - Can replace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

Using a CA-signed certificate

Log into Admin Directory



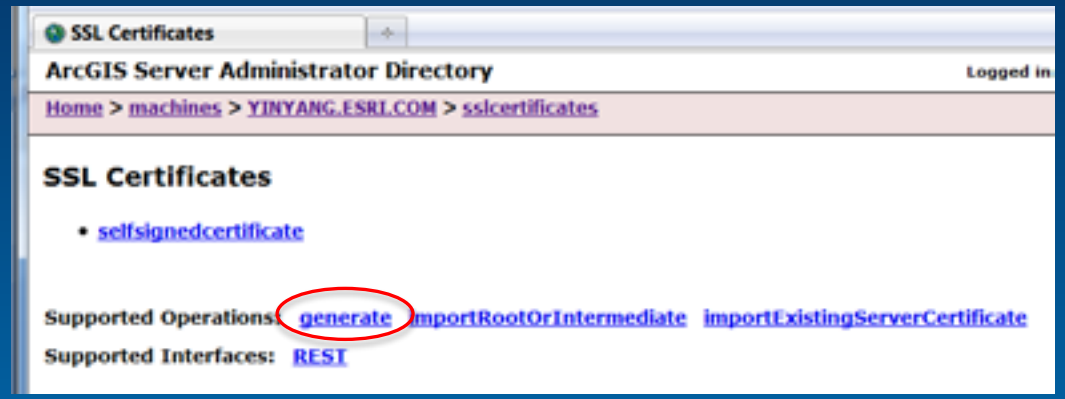
Click on machines



Using a CA-signed certificate

- Click on the machine you are interested in.
- Click on sslcertificates.

Using a CA-signed certificate



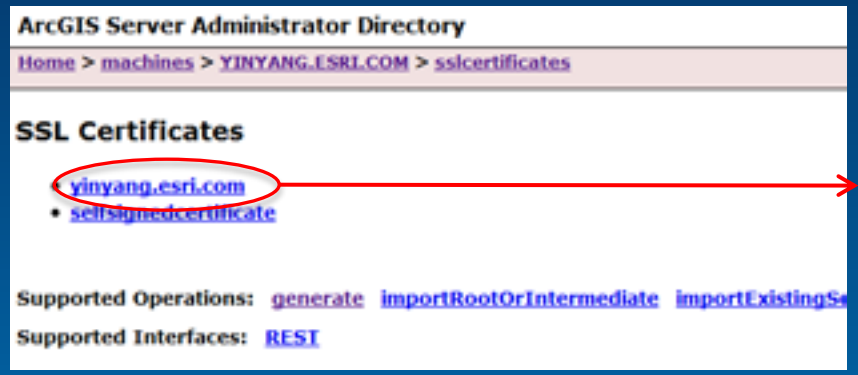
- Can see the automatically generated certificate.
- Operations
  - generate creates a new one
  - importRootOrIntermediate to trust CA's
  - importExistingServerCertificate brings in an existing certificate and the private key (advanced)
- We'll pick generate.

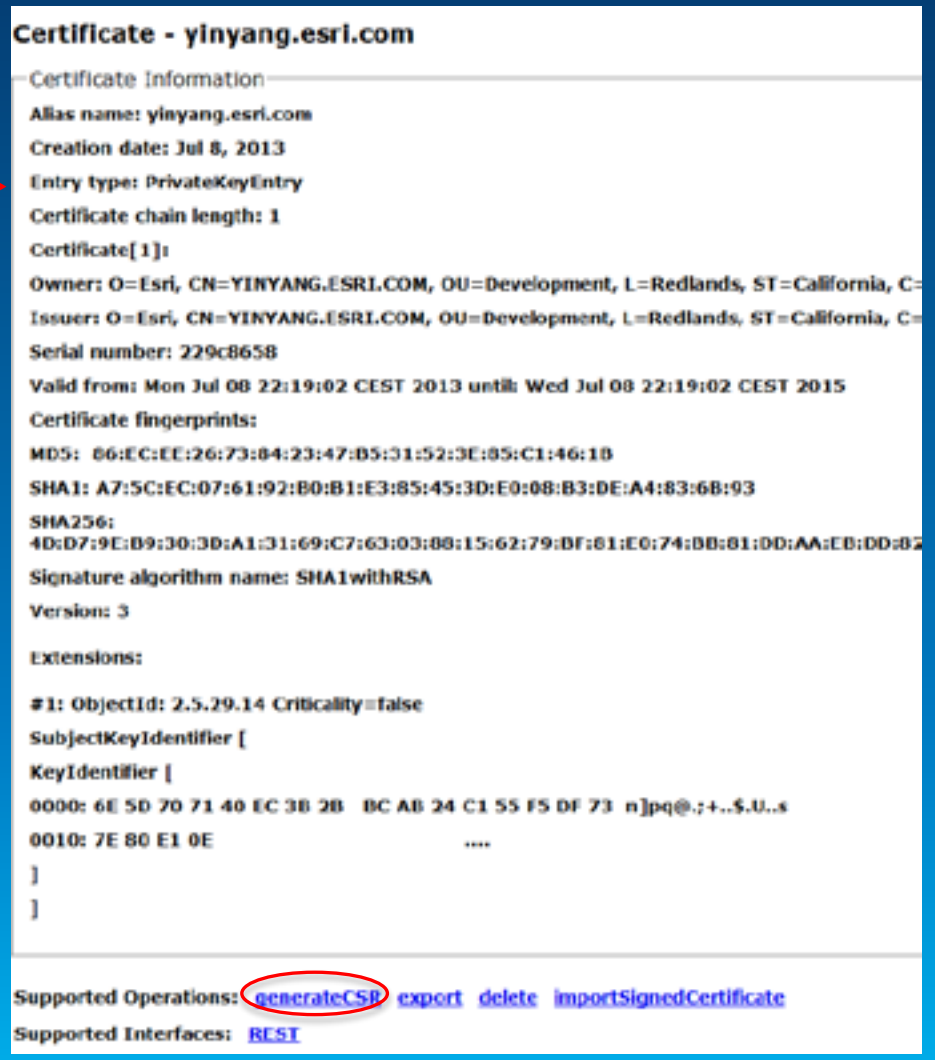
Using a CA-signed certificate

Before

After

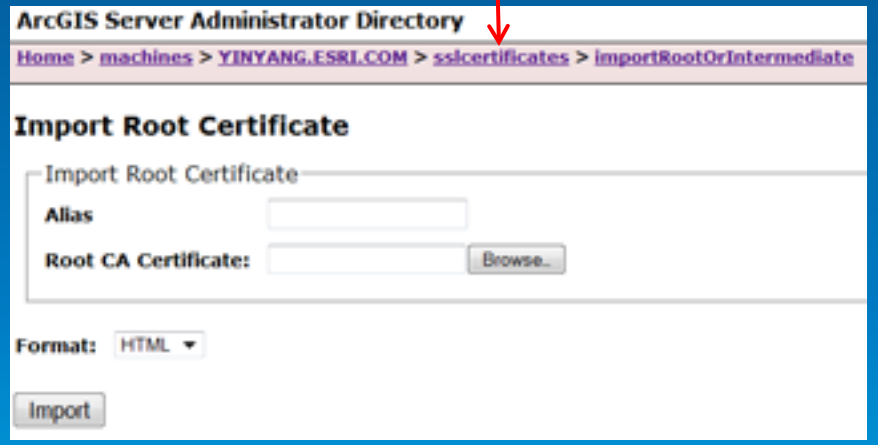
Using a CA-signed certificate





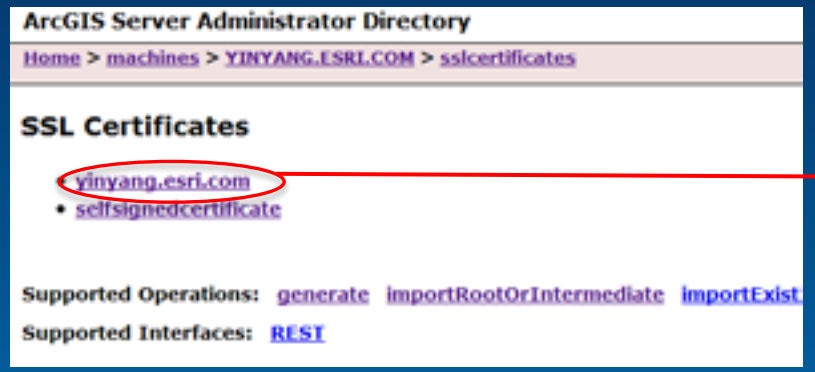
- I now see my new certificate.
- Click on it.
- Click on generateCSR

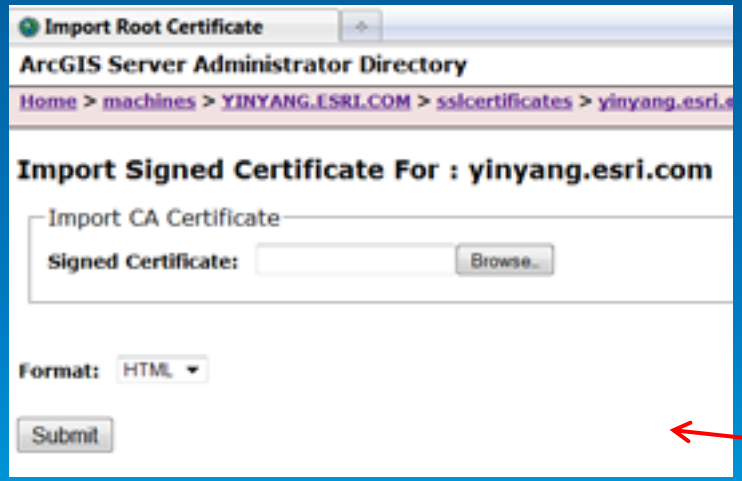
Using a CA-signed certificate



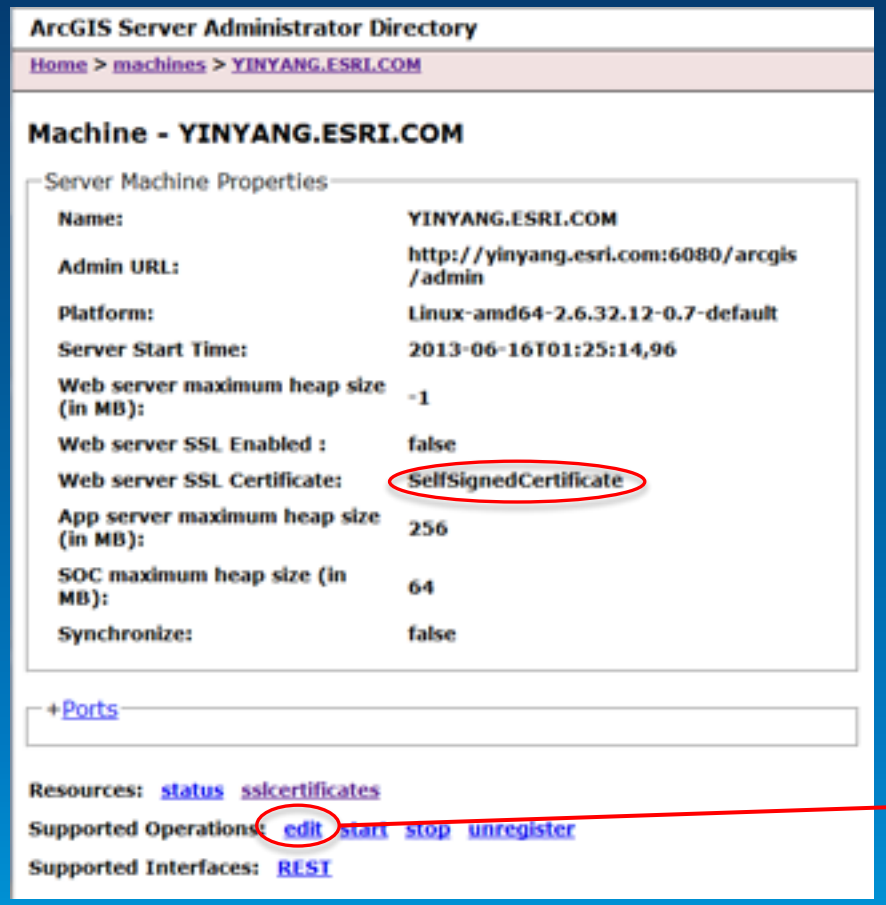
- Send the CSR to your CA.
- They will send you a server cert and their root/intermediate certs.
- Import your CA's root and intermediate certificates first.

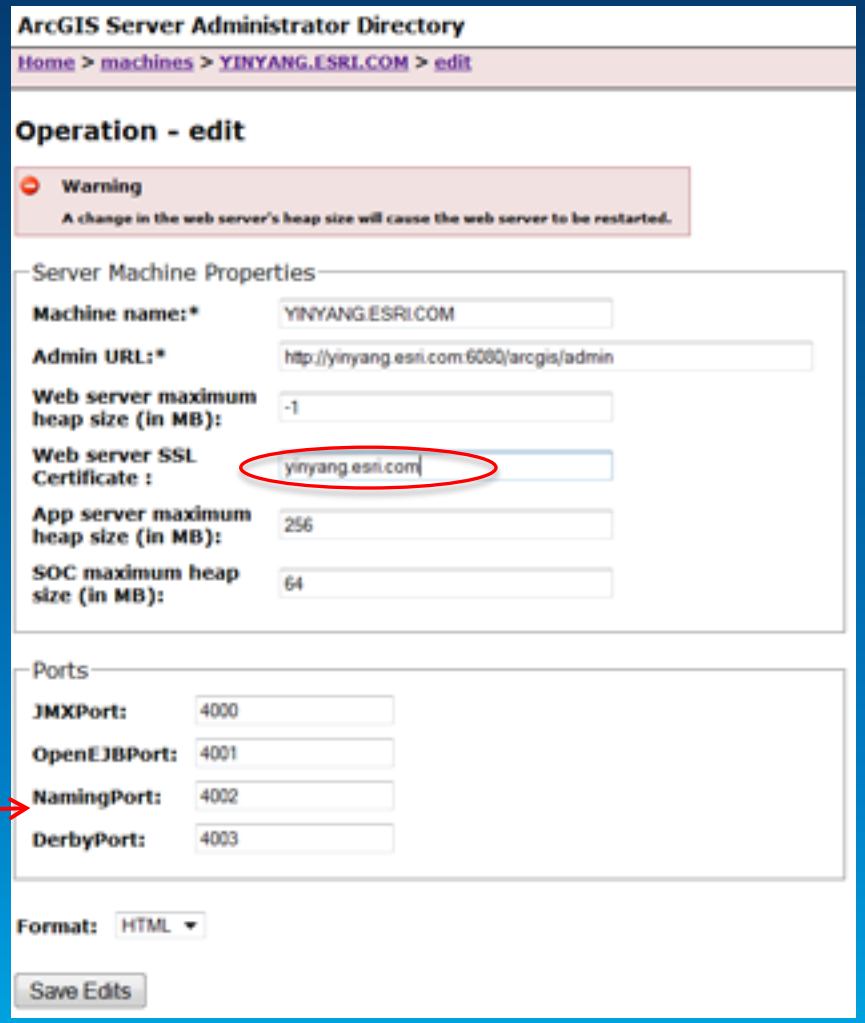
Using a CA-signed certificate





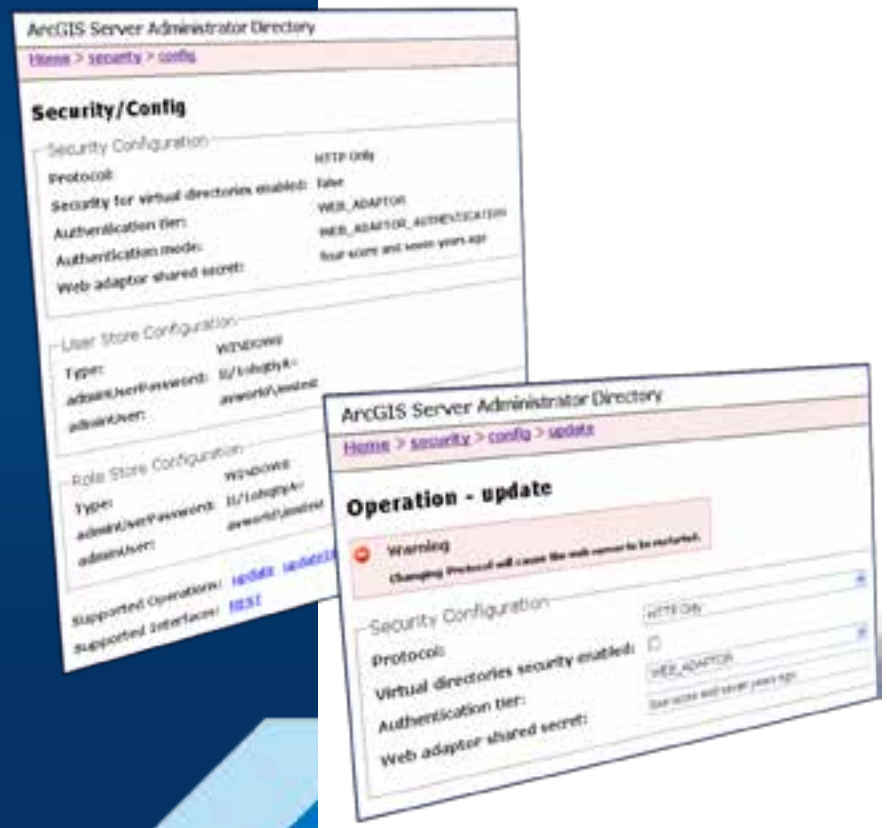
Using a CA-signed certificate





Demo

Enabling HTTPS

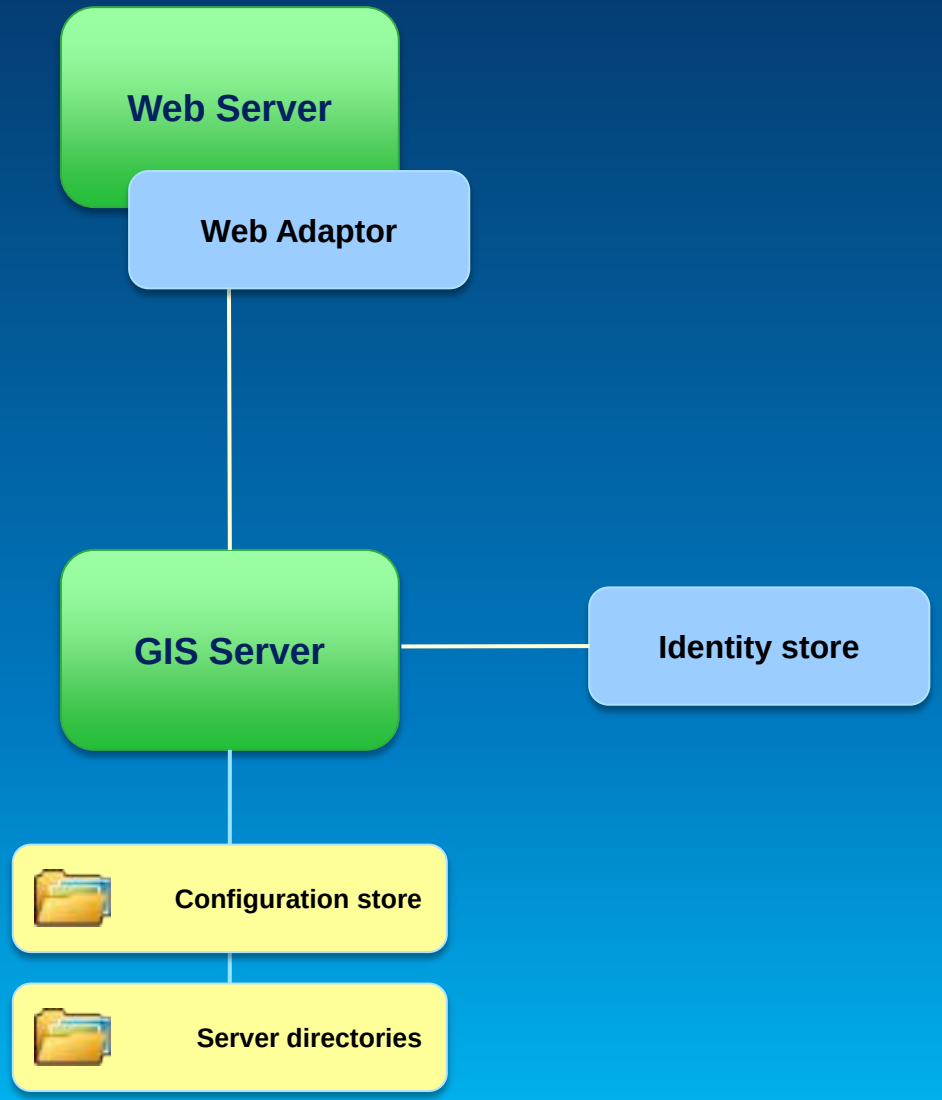


Authentication Tier / Method

- **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

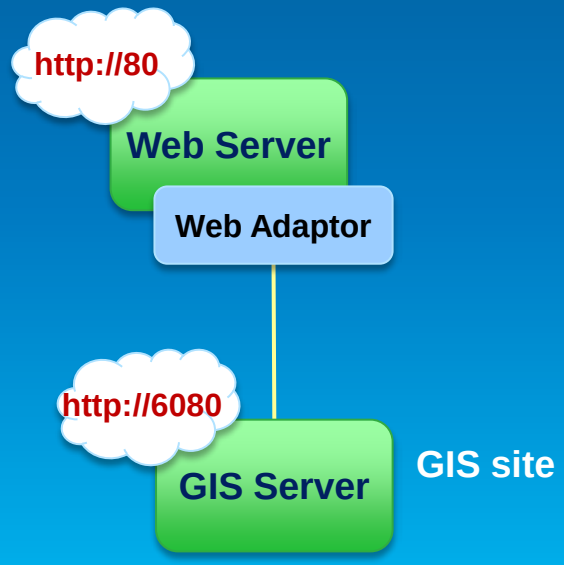
Server Architecture - Security

- 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



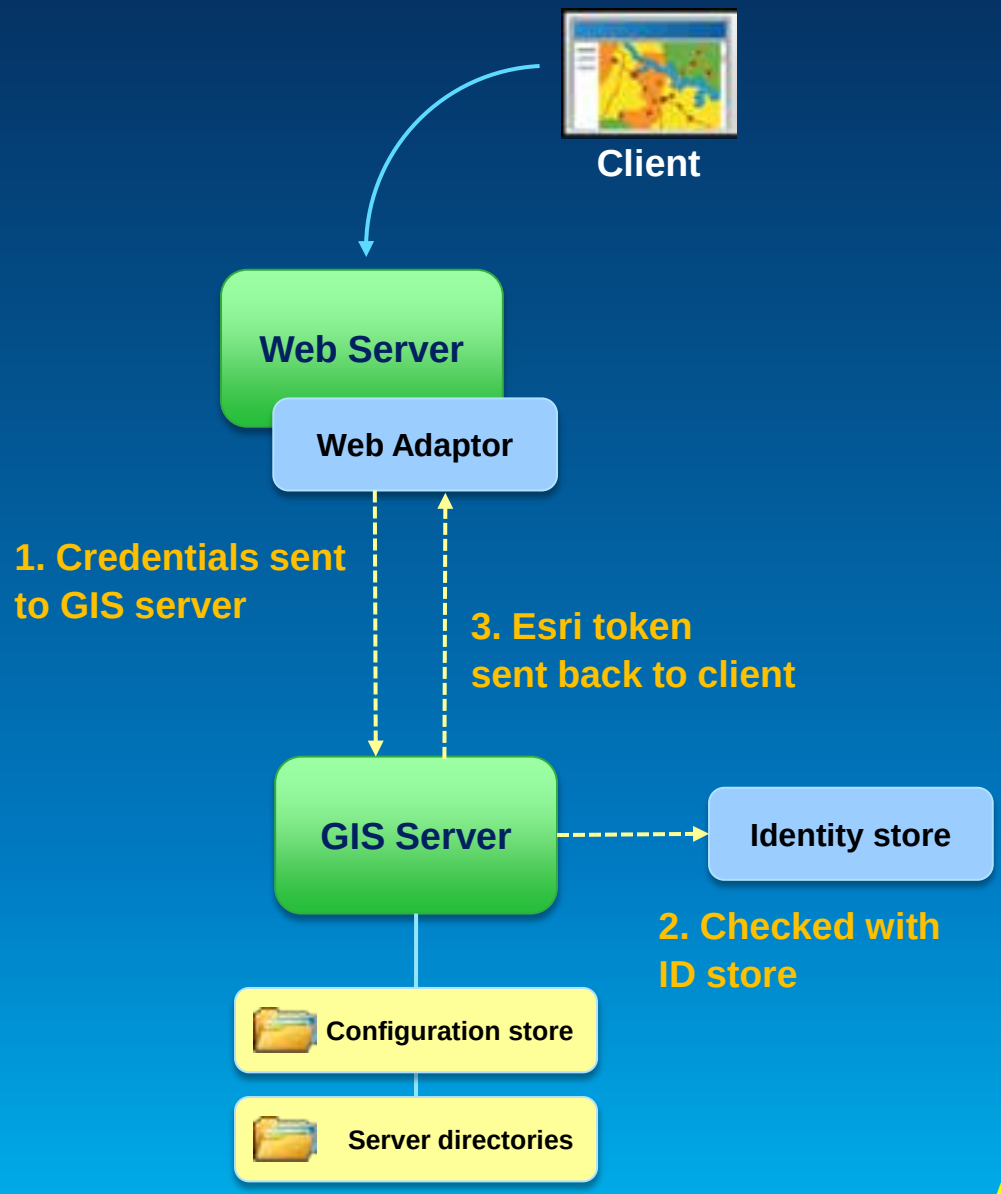
Documentation links

- About ArcGIS Web Adaptor

GIS Tier Authentication

- GIS Server checks credentials

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

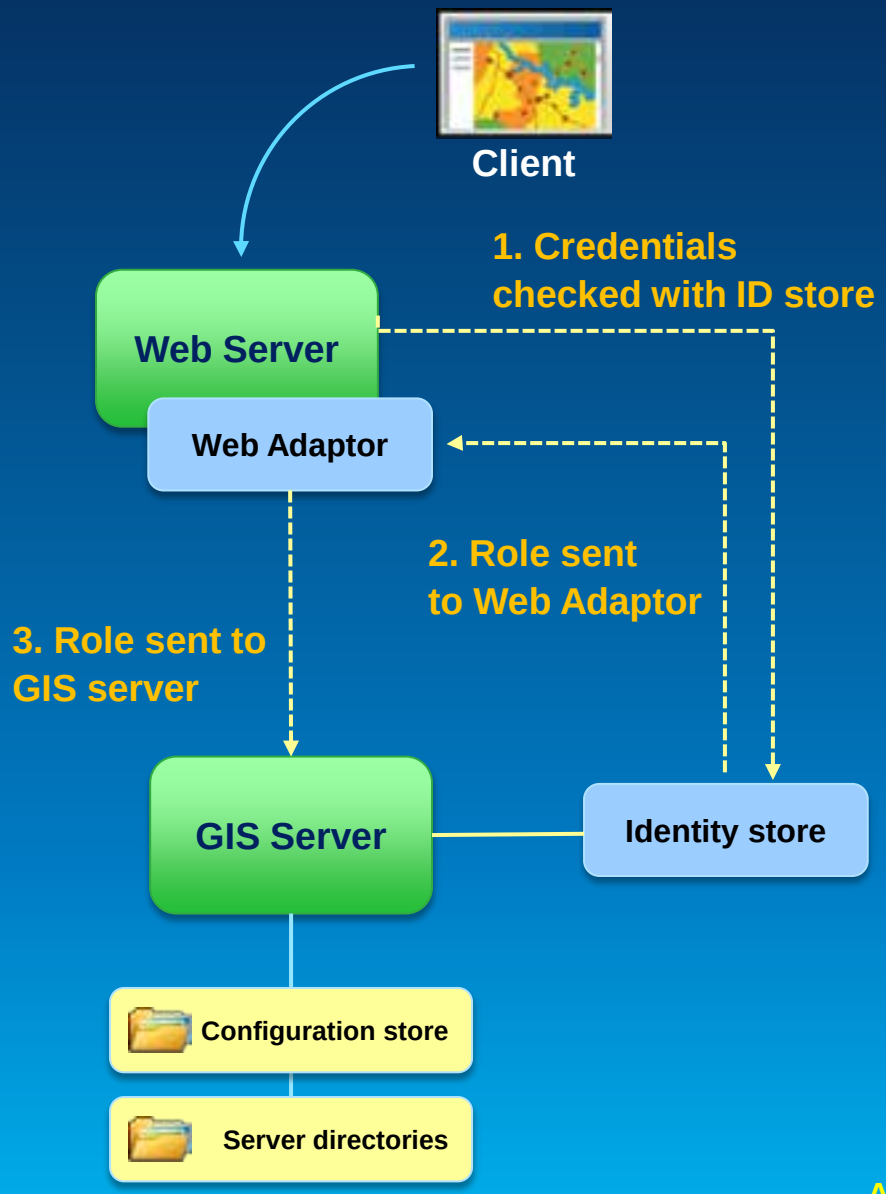


Documentation links

- About ArcGIS Server Tokens

Web Tier Authentication

- Must use Web Adaptor
- HTTP authentication



GIS Tier vs. Web Tier Authentication

	GIS Tier / Token	Web Tier / HTTP Auth
Default	Yes	No
Public / anonymous possible	Yes	No
Clients Supporting	Esri	All, including OGC
Requirements	Enable SSL	Web Adaptor(s) required Basic – require SSL Digest – special setup IWA – Windows only

Demo

ArcGIS Server Manager
Set up authentication in wizard

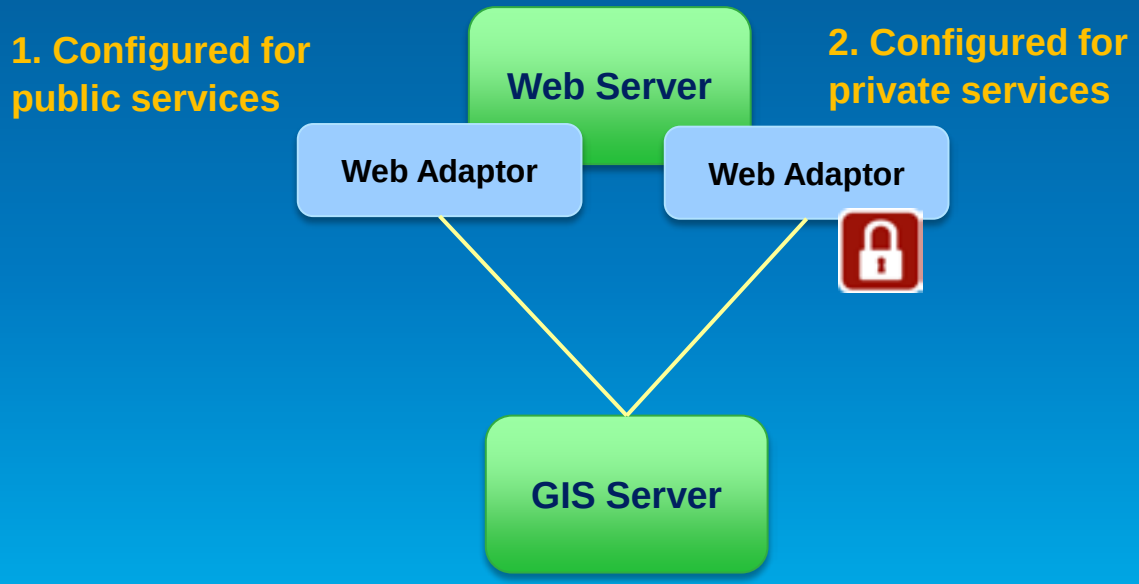
Show IIS configuration of
Web Adaptor

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



Standardized queries

- Prior to 10.2, query syntax unique for each database
- Led to two problems
  - Software passes through queries directly to database scanning for malicious attacks. Hard to prevent many creative SQL injection attacks.
  - 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.

Further Recommendations

Disable the primary site administrator	• Prevents backdoor attacks
Disable services directory	• Prevents XSS attacks
Block Admin Calls on web adaptor	• Limits attack vectors

Questions


esri
Understanding our world.