esri Canada

THE SCIENCE OF WHERE™

Meilleures pratiques en sécurité : ArcGIS Enterprise

Jonathan Gaudreau

Plan

- Mécanismes clés de sécurité
- L’authentification dans ArcGIS Enterprise
- Considérations architecturales
- Implémenter la sécurité
- Checklist de sécurité – ArcGIS Enterprise
- Démo: Quelques utilitaires/outils pour sécuriser son déploiement Enterprise

Mécanismes clés de sécurité

- **Authentification**
- **Autorisation**
- **Encryptage**
- **Filtrage**
- **Journalisation et audit**

Mécanismes clés de sécurité

Géré par vous (ou solution *third-party)*

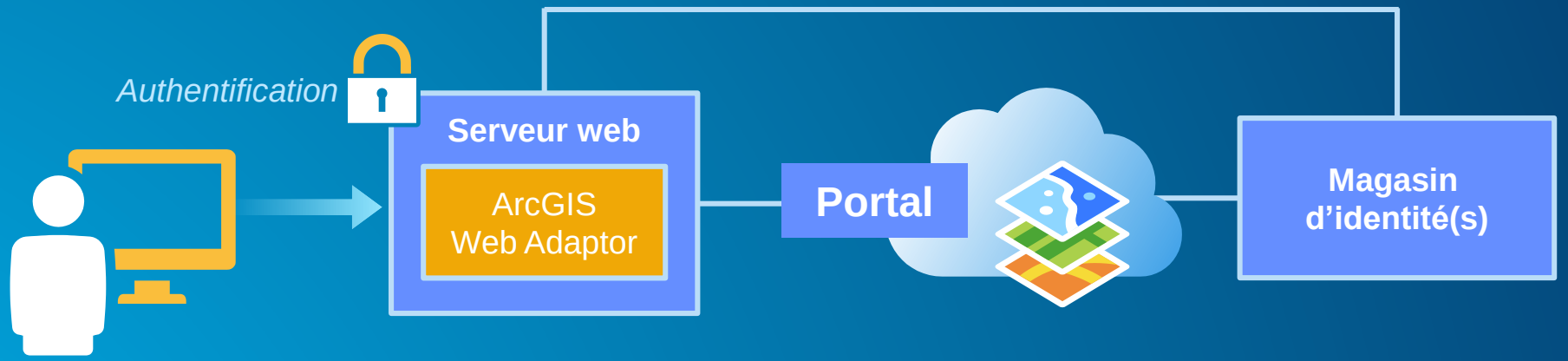
- **Authentification:** L'utilisateur est-il celui qu'il prétend être? Validation de l'identité.
- **Autorisation:** L'utilisateur authentifié a-t-il accès à la ressource (role, groupe, privilèges)
- **Encryptage:** La donnée peut-être être récupérée en transit? Quel est le protocole/algorithme utilisé? (HTTPS, Secure Hash Algorithms (SHA))
- **Filtrage:** Filtrage des requêtes malicieuses, règles de pare-feu, detection d'anomalies, etc.
- **Journalisation et audit:** Historique, journaux. Quel est l'état du système? Monitoring, etc.

L’authentification et les magasins d’identifiants | Authentification avec jetons

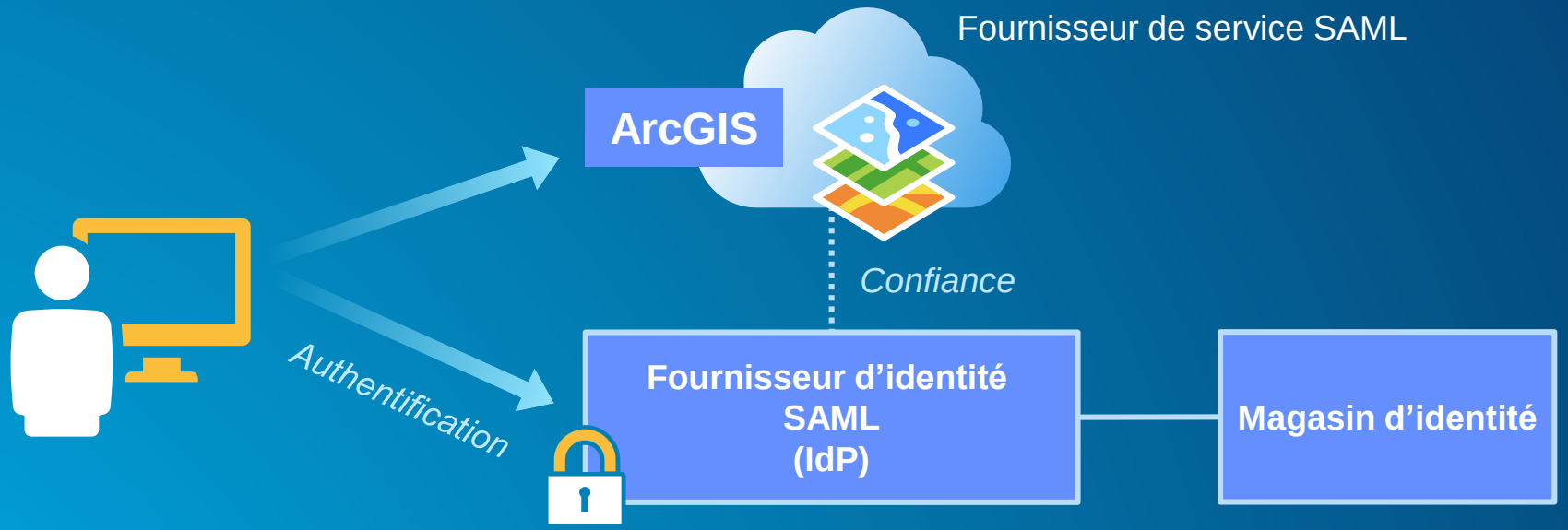
Authentification avec jetons ArcGIS

- Magasin inclus (*built-in*)
- Active Directory
- LDAP

L’authentification et les magasins d’identifiants | L’authentification web



L’authentification et les magasins d’identifiants | SAML 2.0



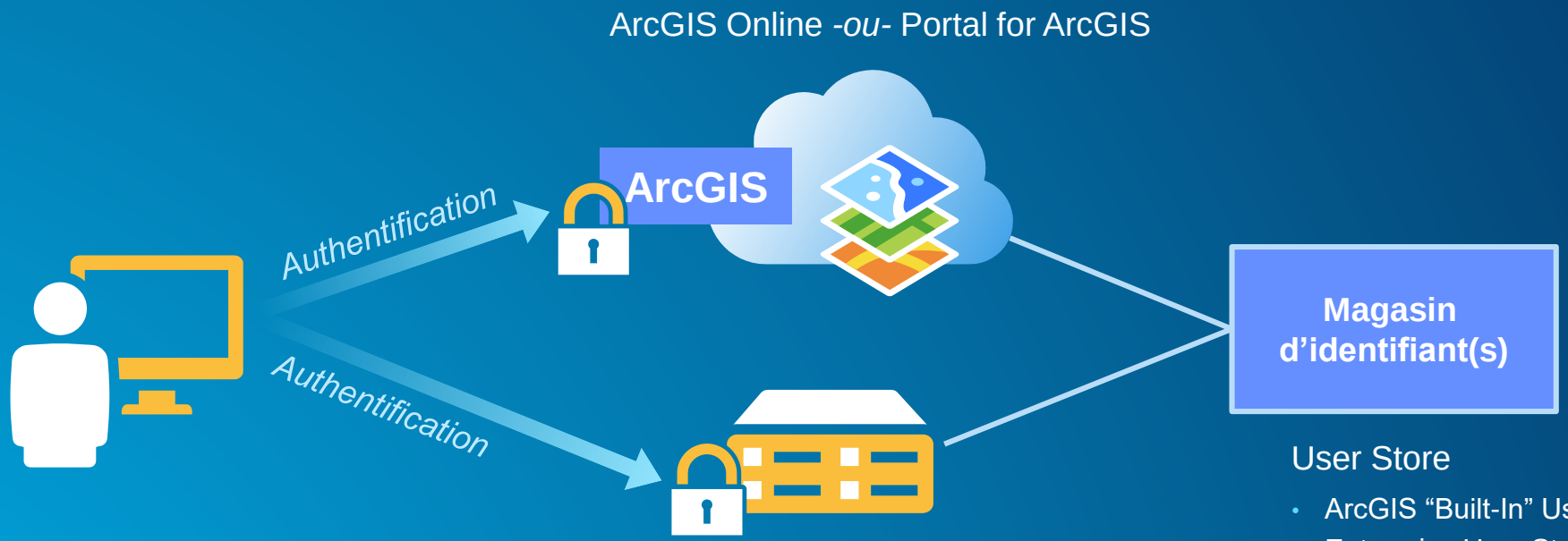
Plusieurs options …

- Authentification simple ou multi-facteur.
- Authentification spécifique
- Integrated Windows Authentication (IWA)
- …

Plusieurs options…

- Magasin(s) d’utilisateurs d’Entreprise
- Un ou plusieurs magasins
- Utilisateurs internes et externes
- …

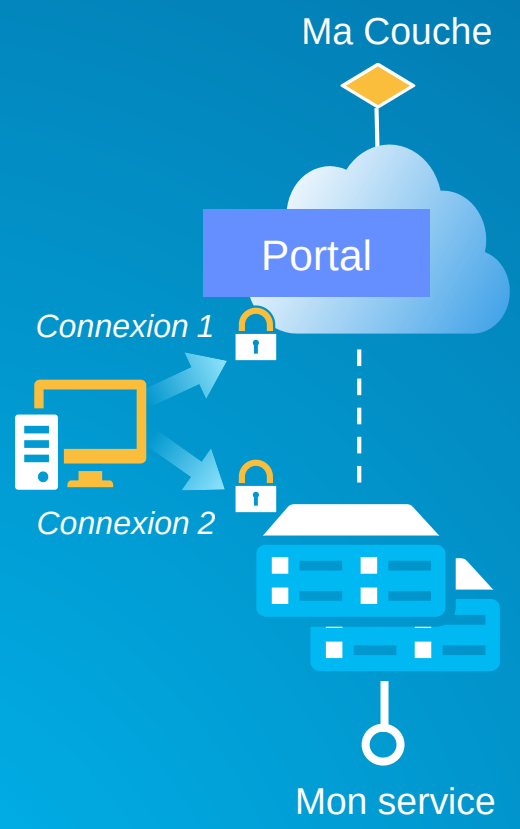
Authentification | Et pour ArcGIS Server?



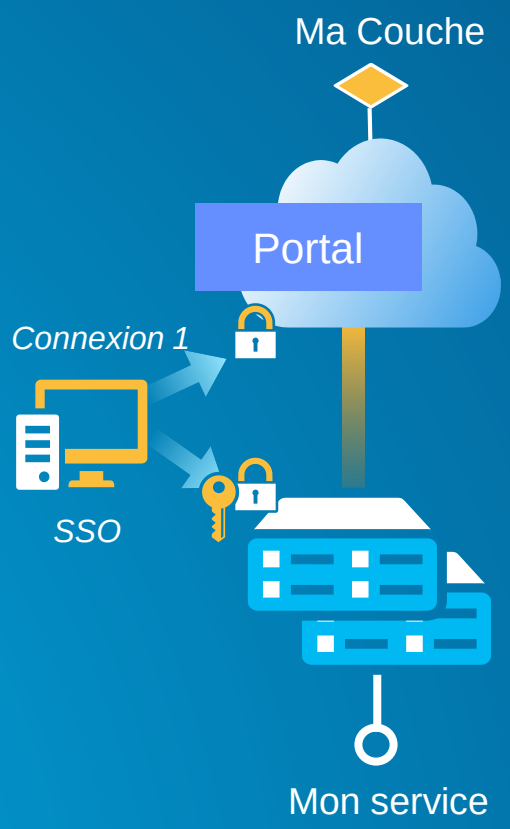
- À considérer…
  - Double authentification
  - Partage *Cross-Origin Resource Sharing* (CORS)
  - ArcGIS "Trusted Servers"
  - ArcGIS Server Federation

Authentification | Fédération ArcGIS Server

Référencé



Fédéré



- Bénéfices
  - Sécurité
    - Identité partagée, SSO
    - Permet SAML sur le serveur GIS
    - Groupes du portail
    - Rôles partagés et publication restreinte
  - Gestion par *Items* du Portail
- Considérations
  - Environnements hautement distribués
  - Consistance de versions (M-à-j)
  - Complexité de redondance/haute disponibilité

Autorisation | Aperçu

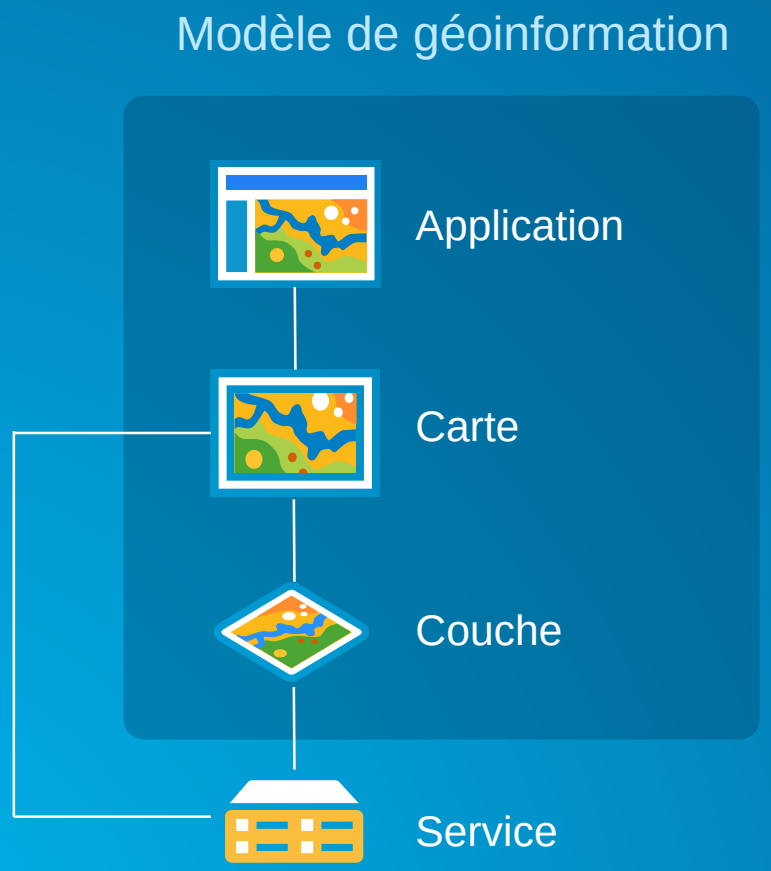
Rôles

- Donne accès à des fonctionnalités *(privilèges)*
- Options
  - Viewer, User, Publisher, Admin
  - Rôles personnalisés
- Considérations
  - Supportent les rôles “built-in” seulement
  - Utiliser le modèle “least-privilege”

Groupes / Partage

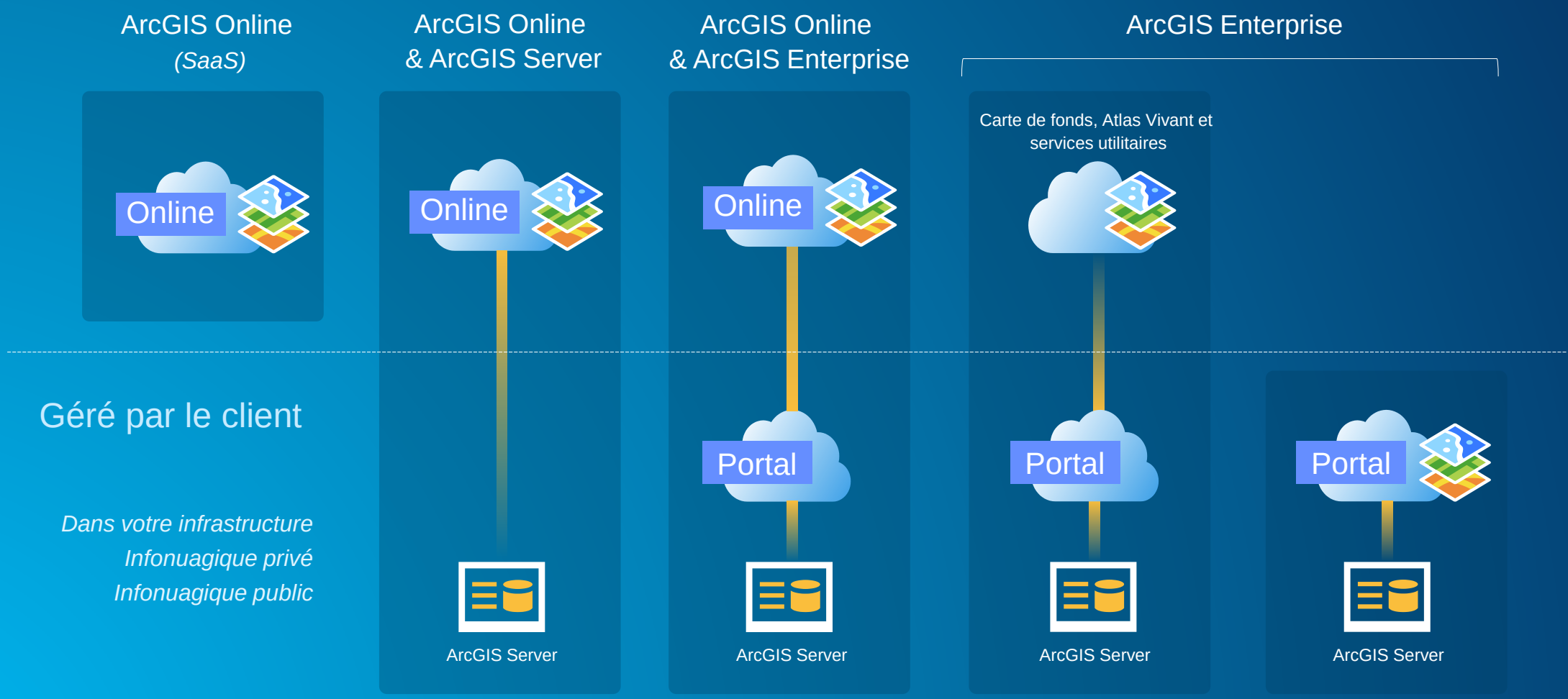
- Gèrent l’accès au Contenu *(items/services)*
- Options
  - Partage de groupe
  - Partage à l’Organisation
  - Tout le monde / public
- Considérations
  - Supportent les groupes “built-in”
  - Portal supporte les groupes d’Entreprise
  - Accès aux groupes
  - Rôles des Groupes
  - Groupes avec mise à jour

Autorisation | Appliquée au modèle de Géoinformation



- App et Carte autorisées séparément
- Carte et couche autorisée séparément
  - Portal vous indiquera quand vous utiliserez des couches non partagées à partir d'Items
  - Portal ne vous indiquera rien quand vous utiliserez à partir des Services URL
- Quand on n'est pas fédéré, l'autorisation des services se fait séparément (deux logins)

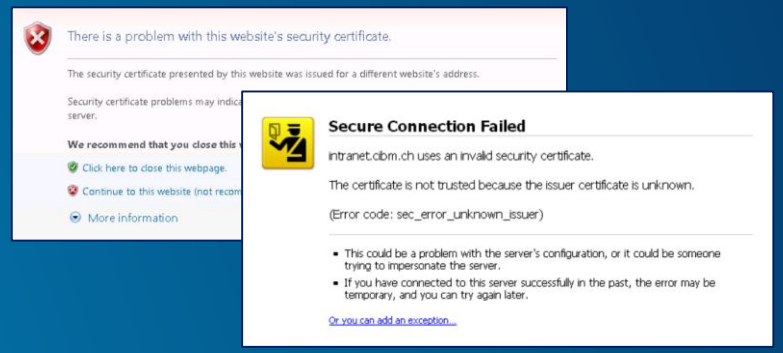
Authentification & Autorisation | Patrons de déploiement valides



Encryptage | HTTPS, SSL, et les Certificats

- Devriez-vous utiliser HTTPS? … **OUI!**
- HTTP et HTTPS
  - Portal a les deux par défaut
  - Server a maintenant les deux par défaut
  - Considérez aller vers 100% HTTPS
- Utilisez des certificats signés par un CA
  - Au moins en production
  - Considérez les pour les autres niveaux aussi
  - Considérez les tant pour le public qu'à l'interne

Want to avoid:



Ne sous-estimez pas les certificats de sécurité!

Implémenter la sécurité

- **La sécurité débute au niveau de la planification et de l’architecture**
- **Mettez sur pied la sécurité même dans vos environnements de développement**
- **Testez vos déploiements avec la sécurité active!**
- **Peu importe le stade de votre développement géomatique, il n’est jamais trop tard pour commencer à appliquer des bonnes pratiques de sécurité**

N’attendez pas un incident pour penser à la sécurité.

Tester la sécurité de son déploiement ArcGIS Enterprise | ArcGIS Server

- **Utilitaire serverScan.py**
  - **Analyse de nombre critère et les divise en trois niveaux de gravité:**
    - **Critical**
    - **Important**
    - **Recommended**

  - **Vous le trouverez dans [dossier d'installation]/tools/admin/serverScan.py**
  - **L'output est un rapport HTML**
  - **Exemple:**

python serverScan.py -n gisserver.domain.com -u admin -p my.password -o C:\Temp

Tester la sécurité de son déploiement ArcGIS Enterprise | Portal for ArcGIS

- **Utilitaire portalScan.py**
  - **Analyse de nombreux critères et les divise en trois niveaux de gravité:**
    - **Critical**
    - **Important**
    - **Recommended**

  - **Vous le trouverez dans [dossier d'installation]/tools/security/portalScan.py**
  - **L'output est un rapport HTML**
  - **Exemple:**

python portalScan.py -n portal.domain.com -u admin -p my.password -o C:\Temp

ArcGIS Enterprise | Guide d'implémentation

- Nécessiter HTTPS
- Empêcher l'accès anonyme
- Requêtes SQL standardisées
- Restreindre le partage public
- Utiliser des Logins d'entreprise *(SAML)*
- Utiliser un modèle du *least-privilege* pour les rôles et permissions *(rôles personnalisés)*
- Ne pas stocker les informations de connexion dans les items
- Masquer les métadonnées sensibles des propriétés des items *(utiliser des domaines, pas des adresses IP)*
- **SURTOUT**: Exécuter serverScan.py et portalScan.py périodiquement
  (intégrez les à vos routines/maintenance sous forme de tâche planifiée)

Démonstrations

Configuration Server, Portal et tests de sécurité