WEBSHEPRE SÉCURITÉ

WAS et DB2

présentation

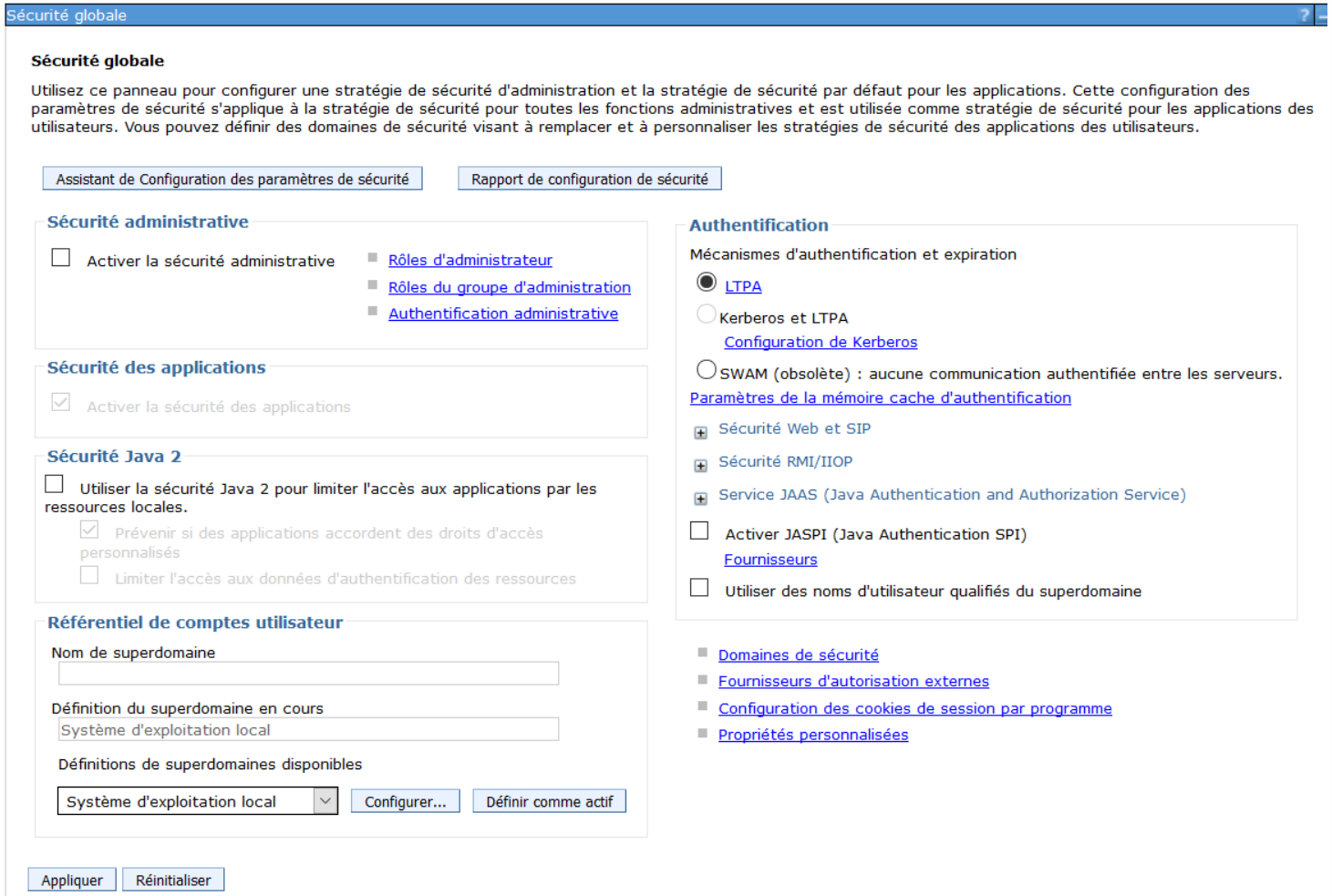
- Sécurité Java EE
- Sécurité globale
- Référentiel
  - Basé sur un fichier
  - Référentiel local au SE
  - LDAP autonome
  - Référentiel fédérés
- Les rôles d'administration
- Sécurité des domaines
- LTPA
- SSL

Référentiels de sécurité globale

- Un référentiel de sécurité contient des informations sur les utilisateurs et les groupes
- Il existe 4 types de référentiels
  - Système d'exploitation local: référentiel de sécurité du système local.
  - Registre LDAP autonome:
  - Registre personnalisé autonome: autorise un référentiel personnalisé basé essentiellement sur une implémentation Java
  - Référentiels fédérés

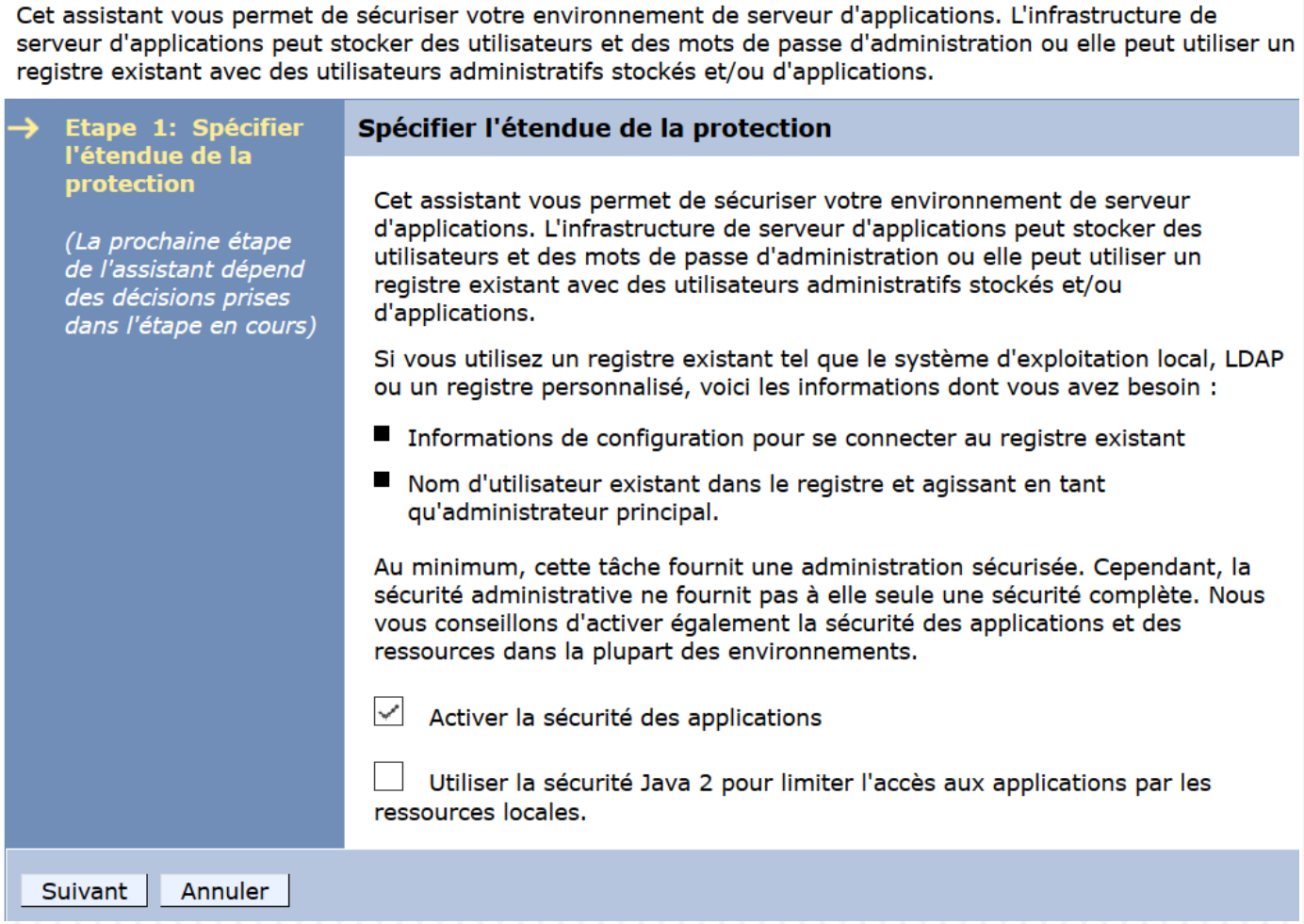
Activer la sécurité

- Sécurité/sécurité globale/Assistant de configuration des paramètres de sécurité



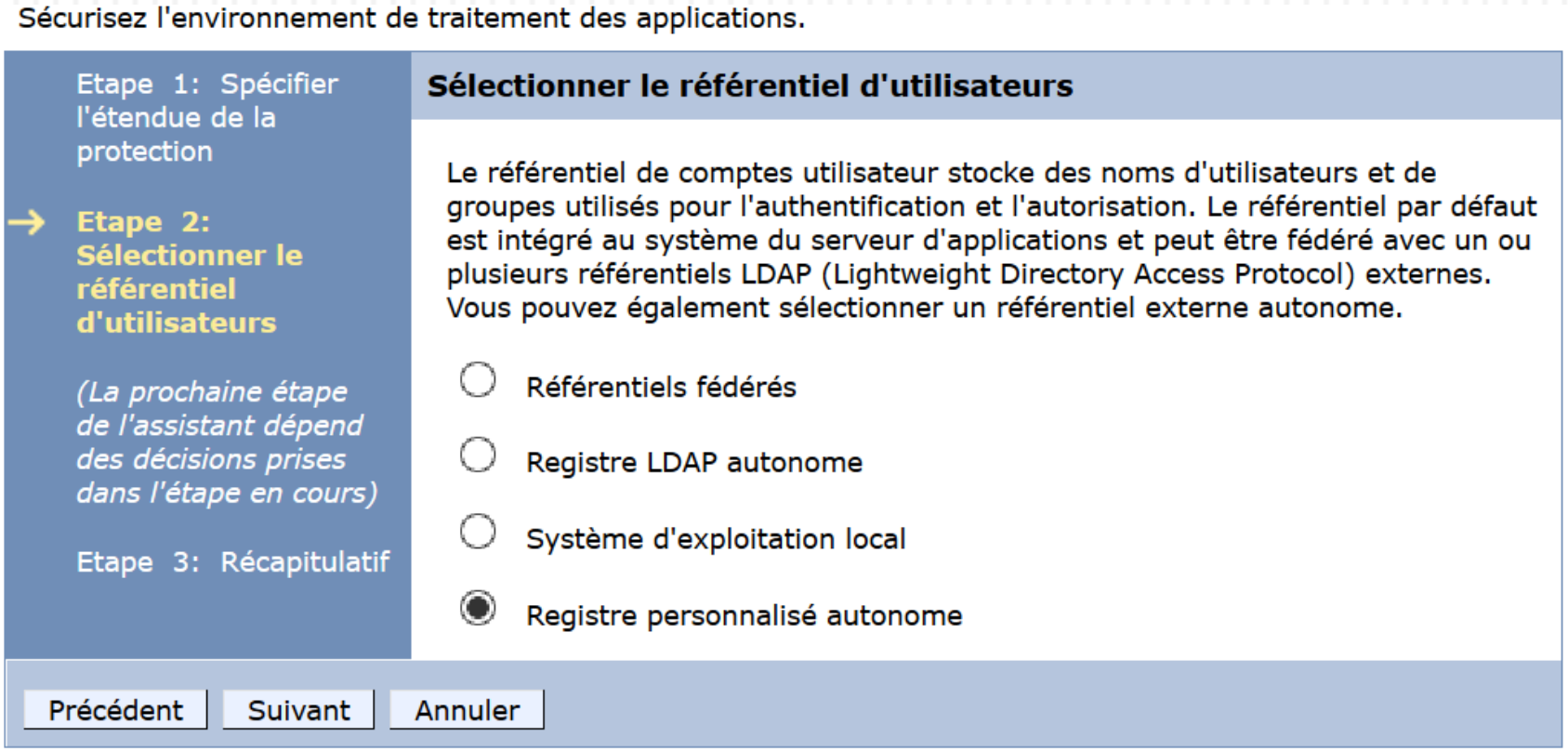
Configuration de la sécurité

- Garder l'option sélectionnée par défaut et cliquer sur suivant



Choix du référentiel

- Sélectionner l'option « registre personnalisé autonome »



Configuration du référentiel personnalisé

- Avant de poursuivre les étapes de l'assistant il faut créer deux fichiers de propriétés l'un pour les utilisateurs et l'autre pour les groupes.
  1. Créer un dossier nommé « emsiUsers » dans le dossier racine de WebShpere
  2. Créer dans le dossier emsiUsers un fichier nommé group.prop

  Format du fichier group.prop

  Une ligne précédée par # est un commentaire

  Pour créer un nouveau groupe, il faut ajouter une ligne ayant le format suivant:

  #nom:id du groupe :utilisateurs:nom d'affichage

  3. Créer le groupe suivant:

  Nom: admins

  Id du groupe: 101

  utilisateurs: 101

  Nom d'affichage: Administrateurs

Configuration du référentiel personnalisé

4. Créer dans le dossier emsiUsers un fichier nommé user.prop

Les informations d'un utilisateur sont représentées dans une ligne qui comme suit:

nom:pass:uid:gids:nom d'affichage

nom: nom utilisateur

uid= id unique de l'utilisateur

gids: liste des groupes auxquels appartient l'utilisateur.

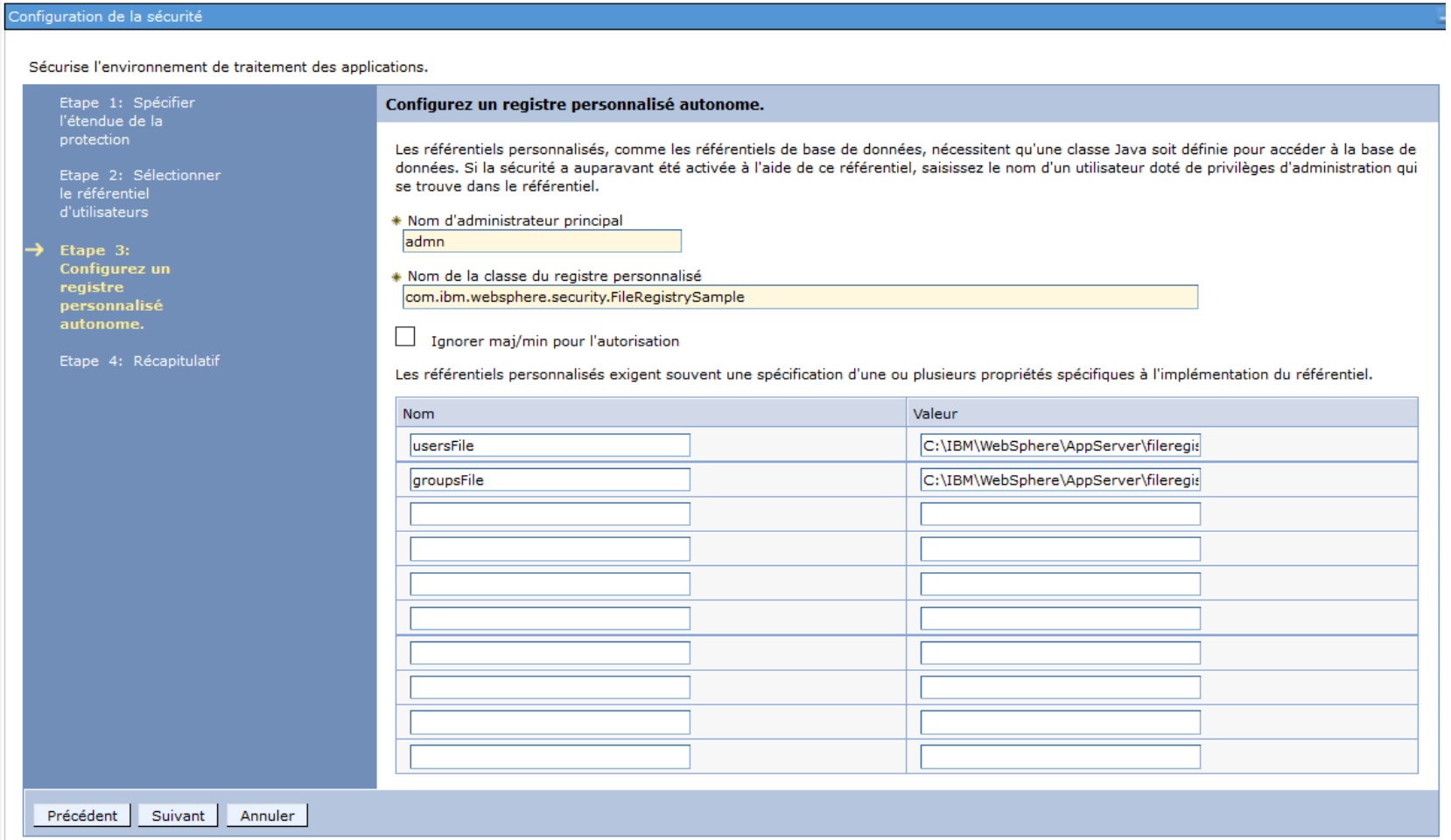
Nom d'affichage: nom qui sera affiché dans la console d'administration

5. Ajouter un utilisateur avec les informations suivantes:

nom:admn, pass:admn, id:101, id Groupe:101,Nom d'affichage:Administrateur WebSphere

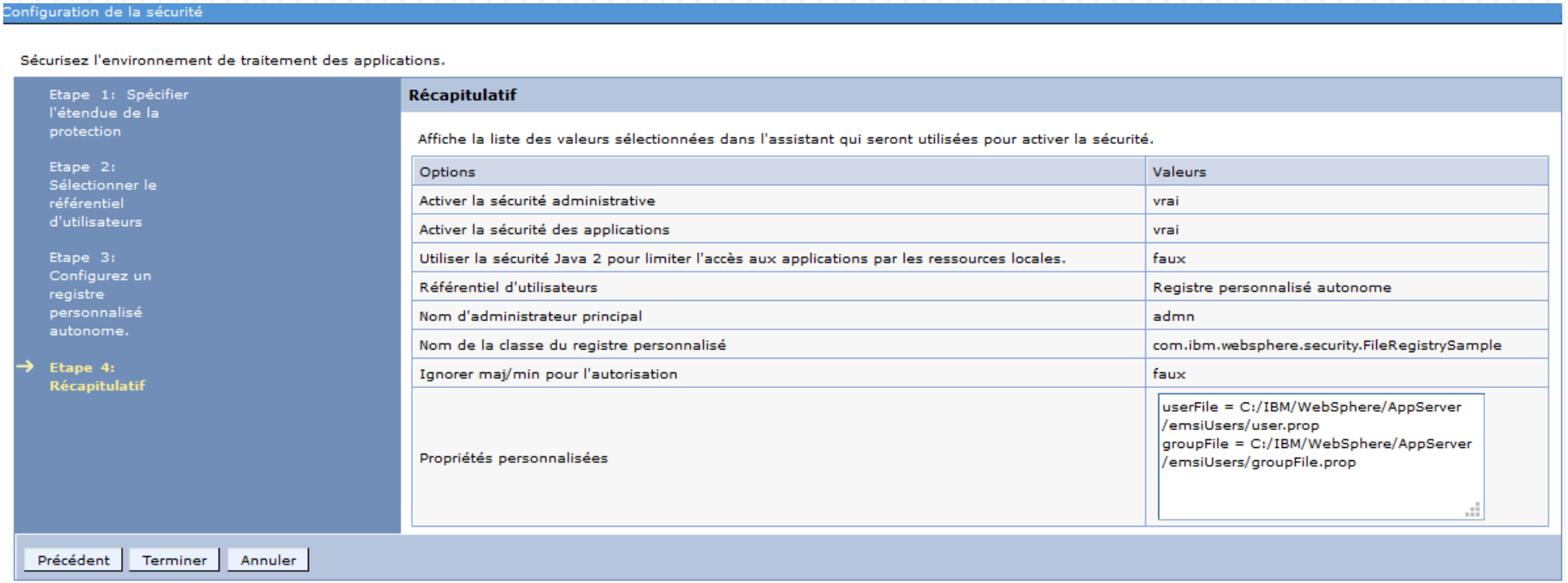
Configuration du référentiel personnalisé

- Dans l'assistant, saisir le nom de l'administrateur principal: admn
- renseigner les deux propriétés usersFile et groupsFile.



Récapitulatif

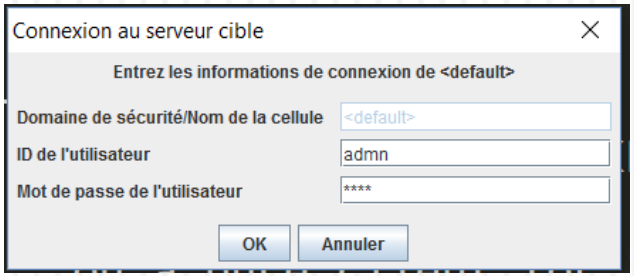
- Cliquer sur « Terminer » et sauvegarder la configuration.
- Pour que les modifications prennent effet, il faut redémarrer le serveur WAS, (StopServer server1, puis startServer server1).
- Se connecter à nouveau dans la console d'administration.



Enregistrer les informations d'authentification.

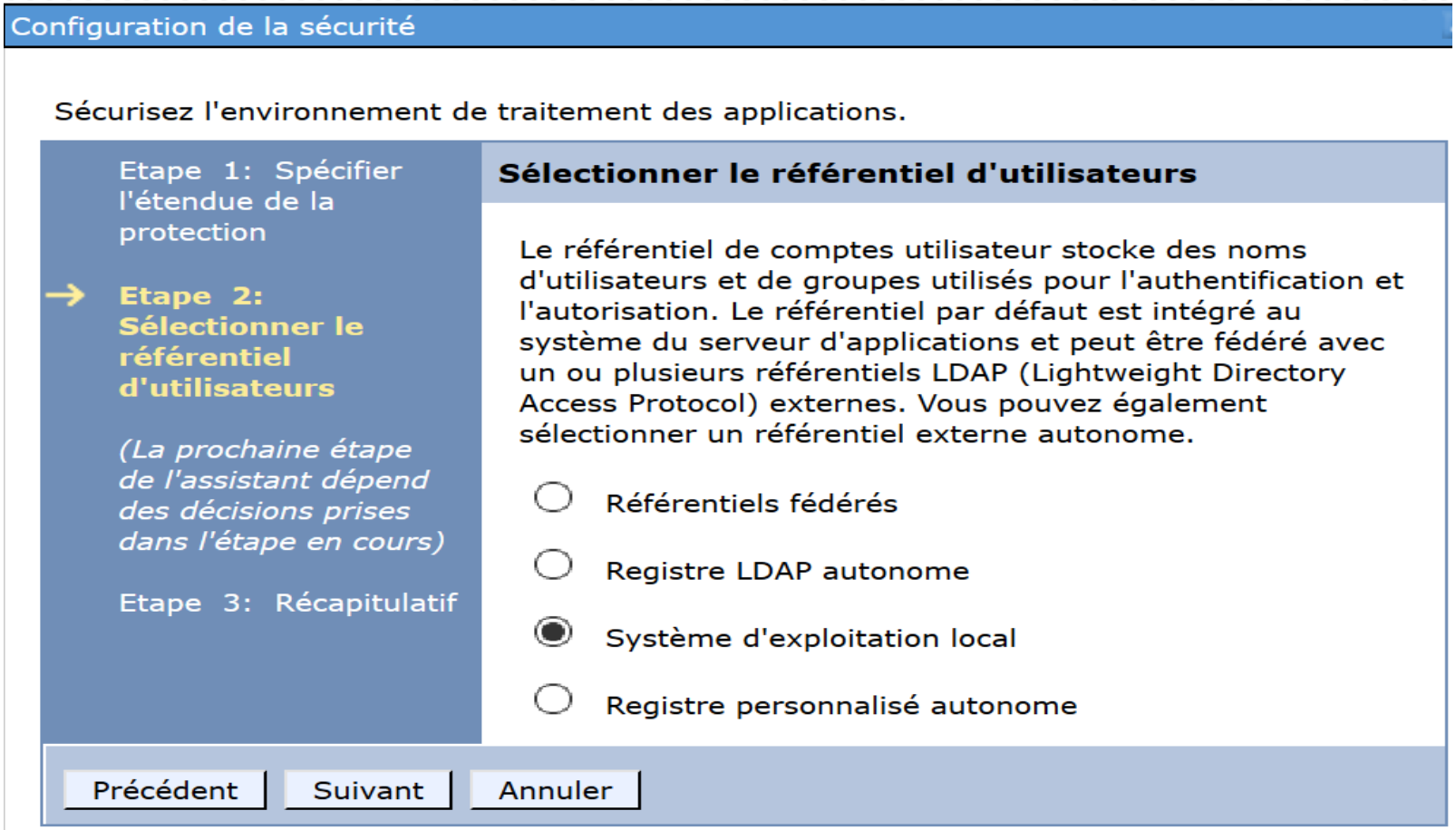
- Ouvrir le fichier WAS_PROFIL/properties/soap.client.props.
- Modifier les propriétés suivantes, comme suit:
  - com.ibm.SOAP.securityEnabled=true
  - com.ibm.SOAP.authenticationTarget=BasicAuth
  - com.ibm.SOAP.loginUserid=admn
  - com.ibm.SOAP.loginPassword=admn
- Redémarrer WAS, puis se reconnecter à la console d'administration.

  La commande stopserver, demandera de saisir les informations d'authentification

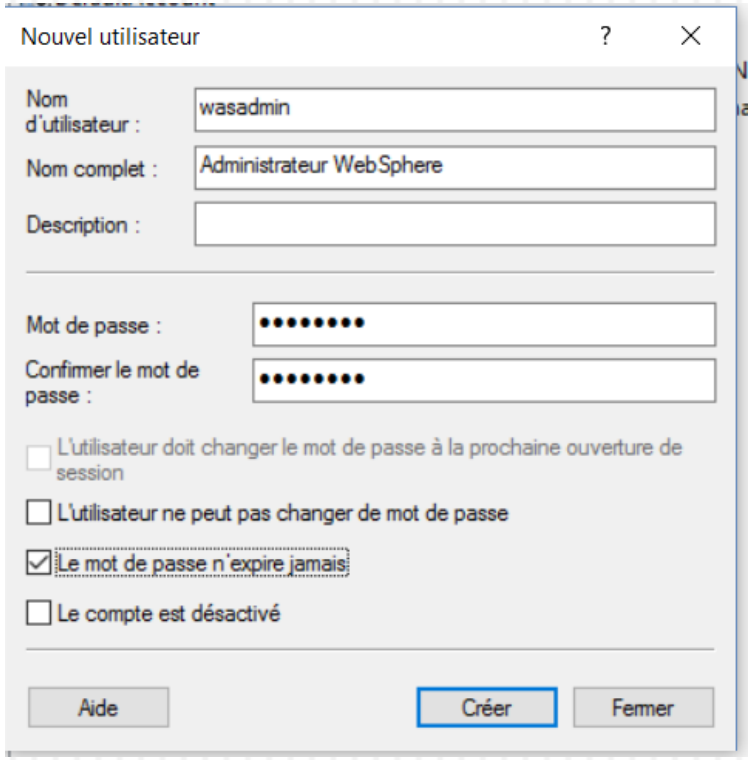


Le référentiel du système d'exploitation

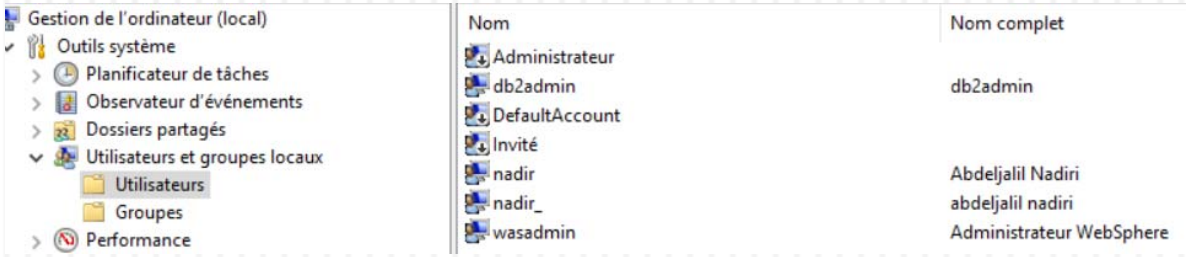
- Créer un nouveau profil.
- Se connecter à la console d'administration de ce nouveau profil (AppSrv02)
- Lancer l'assistant de sécurité et sélectionner le référentiel « Système d'exploitation local »



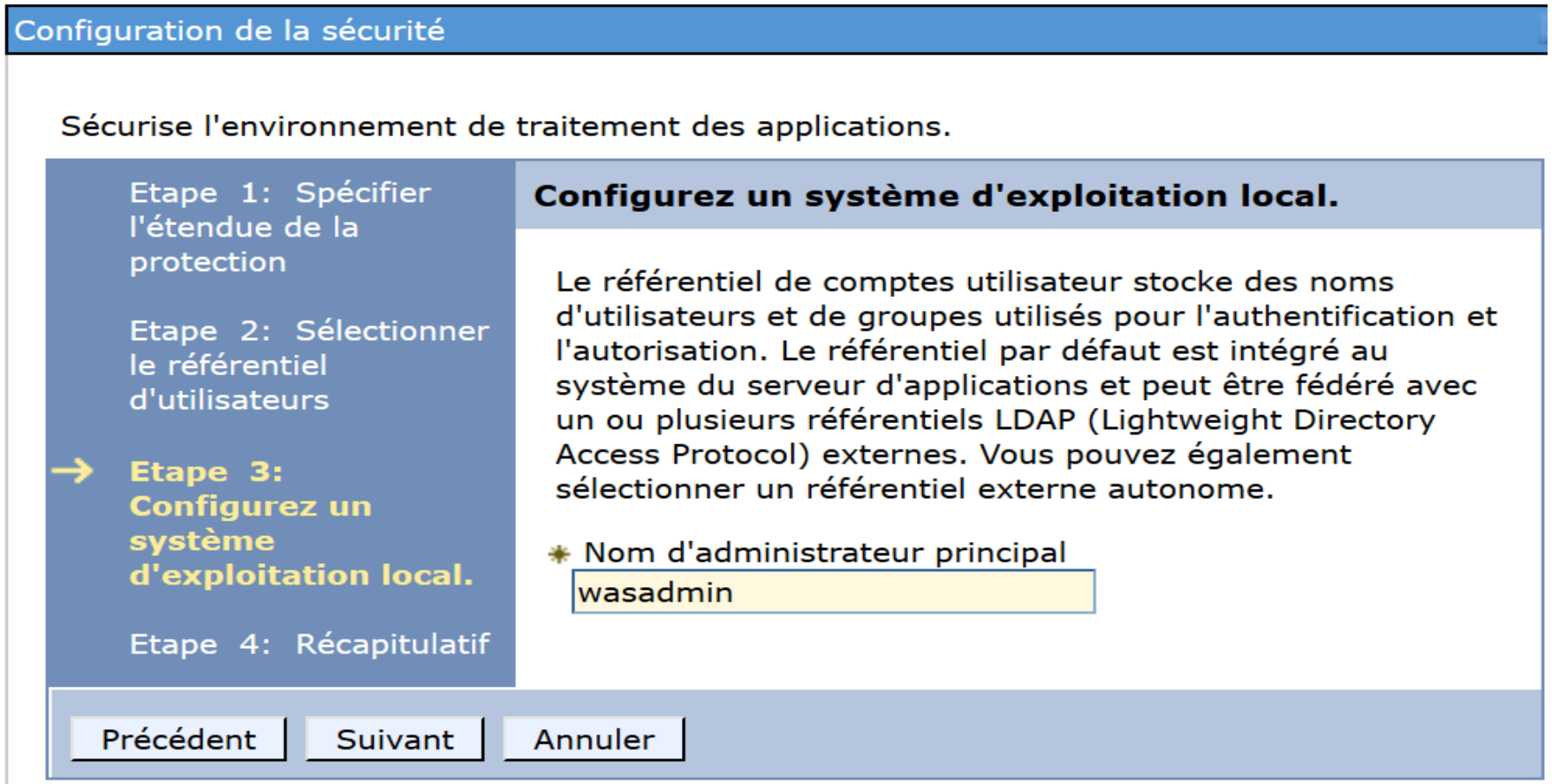
Ajout d'un utilisateur Windows



- Dans le panneau Gestion de l'ordinateur/Utilisateurs, Ajouter un nouvel utilisateur :
  - Nom: wasadmin
  - Nom complet: Administrateur WebSphere
  - Mot de passe: wasadmin
  - Cocher « le mot de passe n'expire jamais »

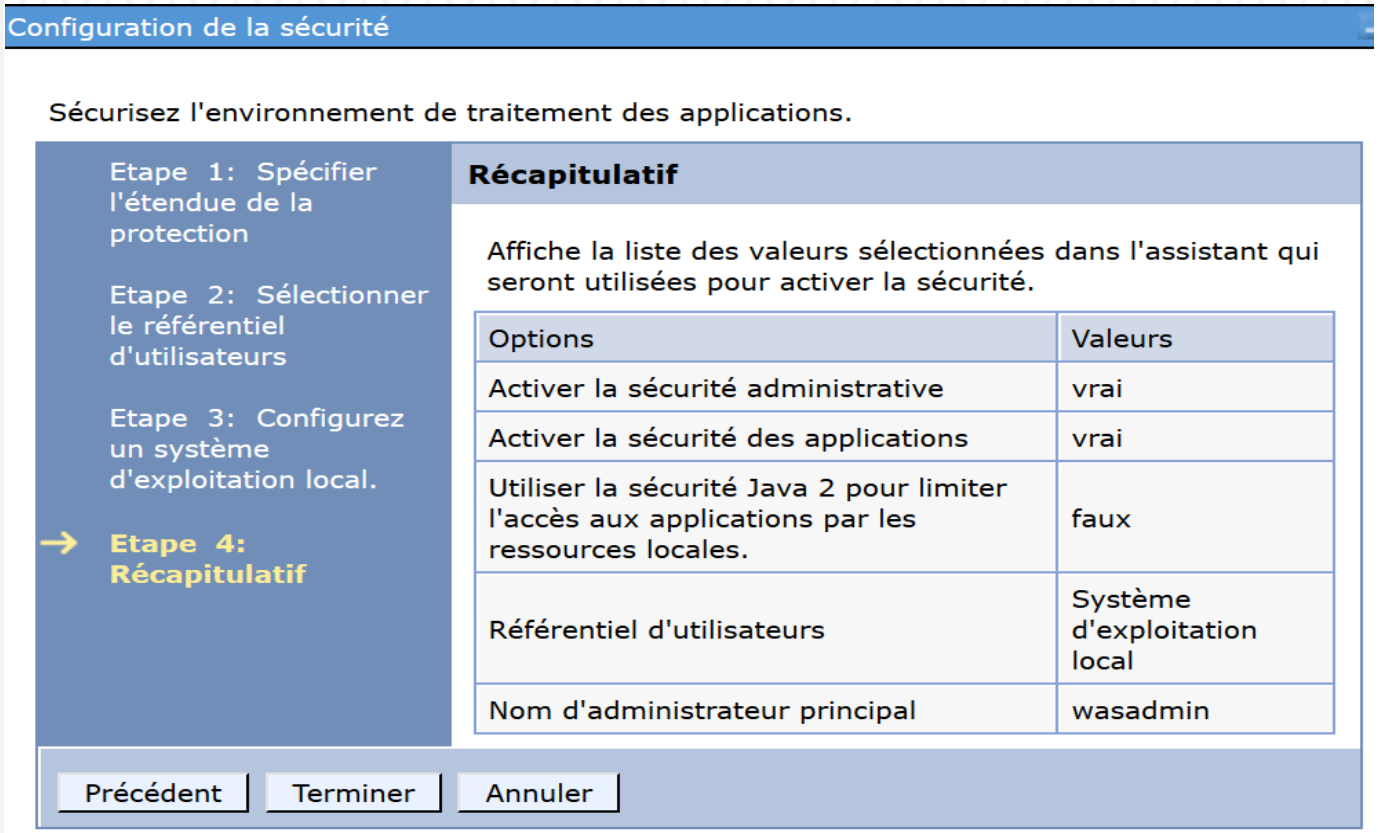


Saisir le nom d'utilisateur Windows « wasadmin »

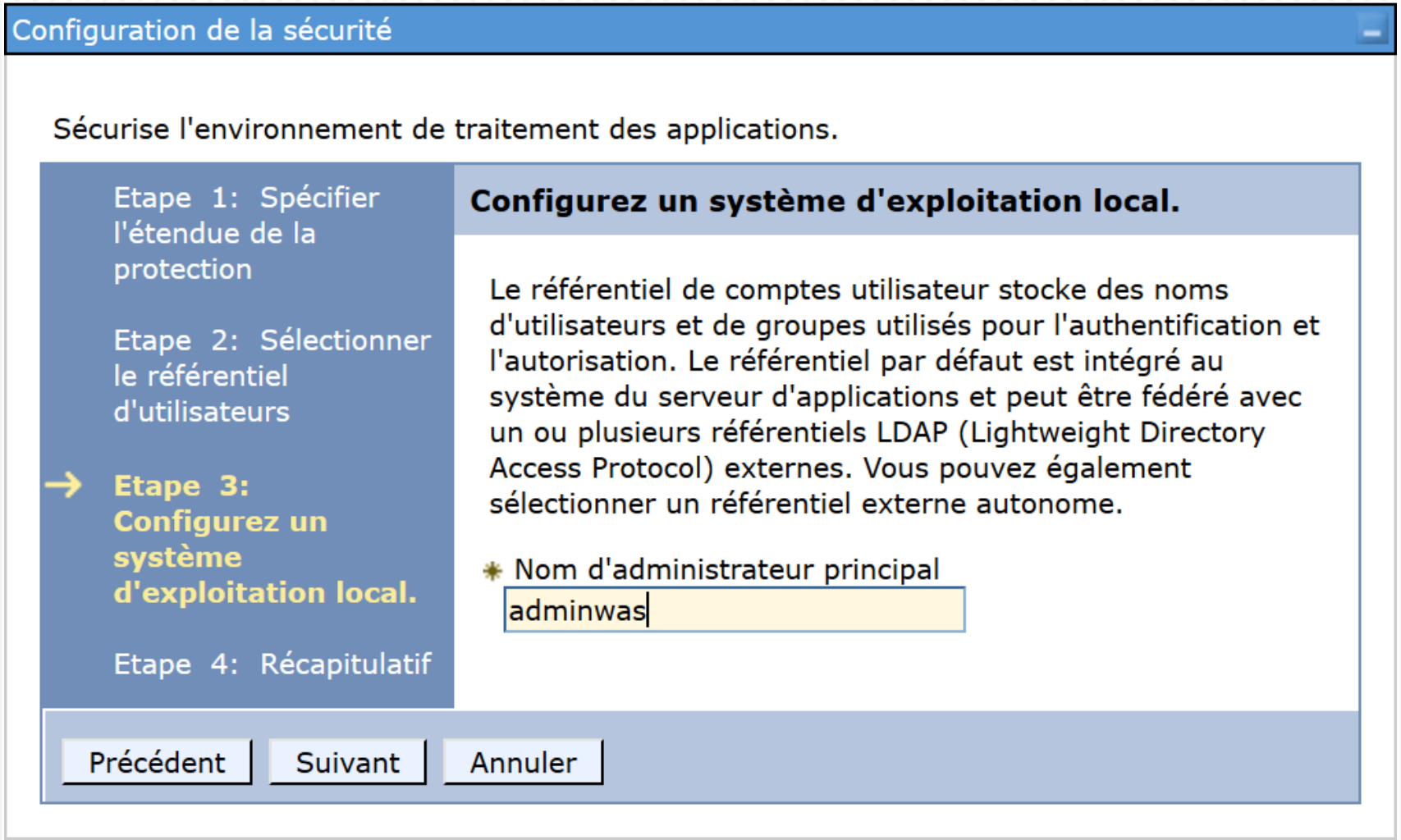


Configuration de la sécurité

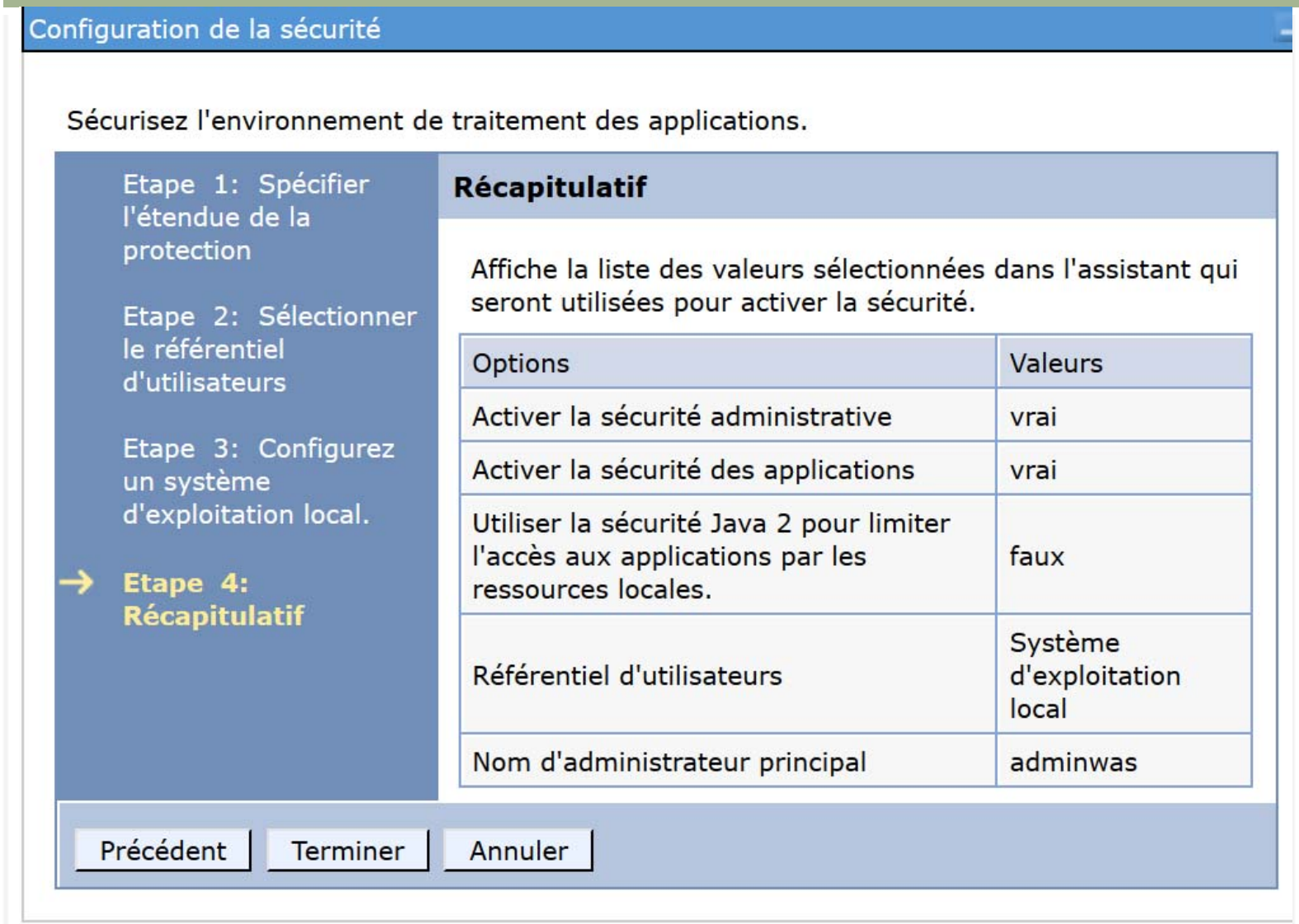
- Cliquer sur « Terminer » et sauvegarder la configuration.
- Redémarrer le serveur WAS
  - stopserver server1 –profileName AppSrv02
  - startServer Server1 –profileName AppSrv02
- Se connecter à nouveau dans la console d'administration



Configuration d'un système d'exploitation local



Récapitulatif



Référentiel LDAP autonome

- Implémentations
  - IBM Tivoli Directory Server
  - ADAM (Active Directory Application Mode): service d'annuaire LDAP qui possède les mêmes fonctionnalités que Active Directory sans imposer le déploiement de domaines et de contrôleurs de domaines.
    ADAM est exécuté comme un service utilisateur et non pas comme un service système.
  - Produits open source (non supportés officiellement par WAS): ApacheDS LDAP, OpenLDAP
- Les informations de configurations de la sécurité, sont enregistrés dans le fichier xml <RACINE_PROFILE>/config/cells/<nom_cellule>/security.xml

Les rôles utilisateurs

- WAS différencie 3 catégories d'utilisateurs:
  - Les utilisateurs du système d'exploitation (SE):

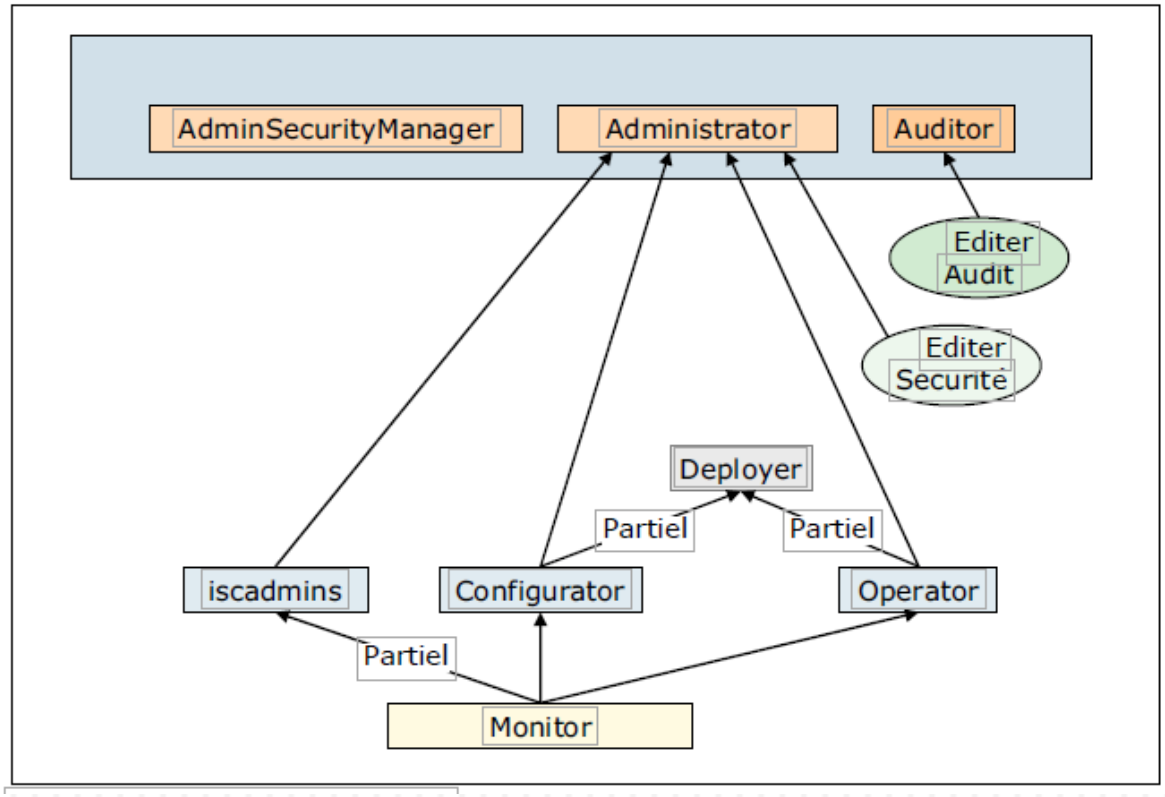
    Les comptes de ces utilisateurs sont gérés par le SE et ils peuvent exécuter les commandes en ligne.
  - Les administrateurs

    ils gèrent le serveur d'application, uniquement les administrateurs peuvent avoir accès à la console d'administration, les administrateurs doivent s'authentifier pour exécuter les commandes en ligne
  - Les utilisateurs d'application

  Ces utilisateurs peuvent uniquement accéder aux applications.
- Les comptes administrateurs et utilisateurs d'applications sont stockés dans un référentiel.
- Les autorisations sont basées sur deux types de rôles d'utilisateurs
  - Les rôles de sécurité administrative
  - Les rôles de sécurité des applications

Les rôles de sécurité administrative

- WAS définit 8 rôles de sécurité administrative



Monteur:

Visualiser la configuration WAS

Visualiser l'état courant du serveur d'application

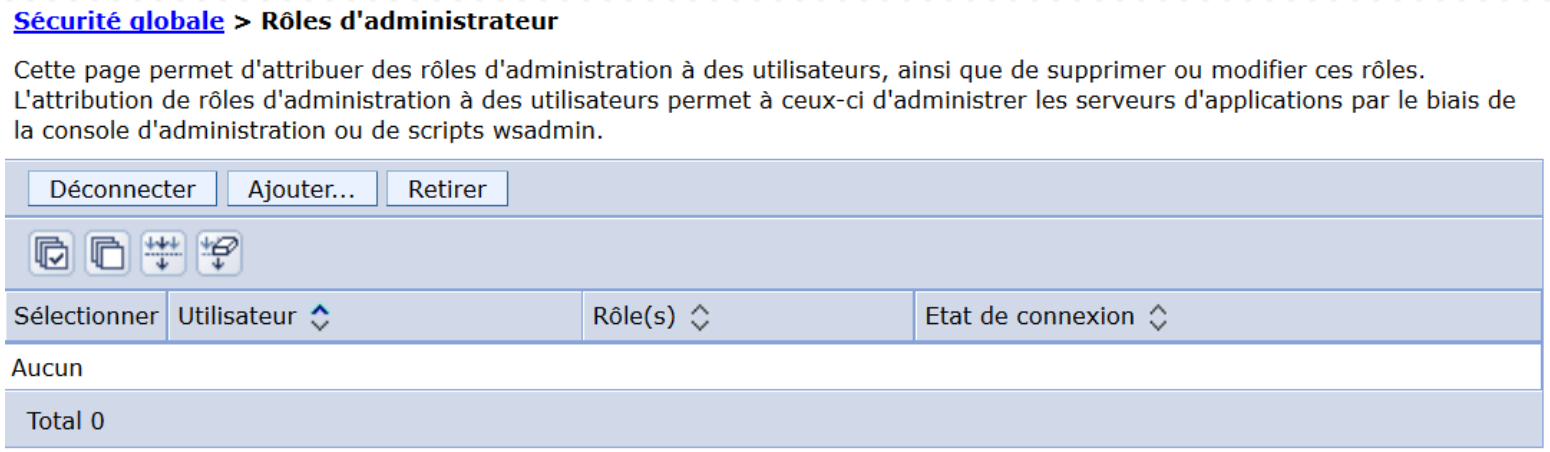
- Configurateur:
  - Possède les privilèges Monitor
  - Créer des ressources
  - Installer/Désinstaller une application
  - Déployer une application
  - Mapper un serveur d'applications
  - Assigner des utilisateurs et des groupes aux rôles pour des applications applications.
  - Configurer les permissions de sécurité Java 2 pour les applications.

Rôles de sécurité administrative

- Opérateur
  - Possède les privilège du rôle Monitor
  - Arrêter/Démarrer le serveur
  - Superviser l'état du serveur dans la console d'administration
- Administrator
  - Possède les privilèges Opérateur et Configurateur en plus d'autres privilèges comme la modification de l'environnement d'exécution .
- Iscadmins: disponible pour les utilisateurs de la console, ce rôle possèdent des privilèges administrateur pour la gestion des utilisateurs et des groupes dans les référentiels fédérés d'administration
- Déployeur: opérations de configuration et d'exécution sur une application.
- Gestionnaire de sécurité Administrateur: assigner à des utilisateurs et des groupes le rôle d'administrateur
- Auditeur: voir et modifier les paramètres de configuration du sous-système d'audit de sécurité.

Affecter des groupes et des utilisateurs à des rôles

- Dans la section sécurité/Sécurité globale/Sécurité administrative cliquer sur « Rôles d'administrateur »



Affectation des utilisateurs à des rôles