



# WEBSHEPRE SÉCURITÉ



WAS et DB2

# présentation

2

- 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

3

- 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

4

## □ Sécurité/sécurité globale/Assistant de configuration des paramètres de sécurité

Sécurité globale

### Sécurité globale

Utilisez ce panneau pour configurer une stratégie de sécurité d'administration et la stratégie de sécurité par défaut pour les applications. Cette configuration des paramètres de sécurité s'applique à la stratégie de sécurité pour toutes les fonctions administratives et est utilisée comme stratégie de sécurité pour les applications des utilisateurs. Vous pouvez définir des domaines de sécurité visant à remplacer et à personnaliser les stratégies de sécurité des applications des utilisateurs.

Assistant de Configuration des paramètres de sécurité    Rapport de configuration de sécurité

#### Sécurité administrative

Activer la sécurité administrative

- [Rôles d'administrateur](#)
- [Rôles du groupe d'administration](#)
- [Authentification administrative](#)

#### Sécurité des applications

Activer la sécurité des applications

#### Sécurité Java 2

Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales.

Prévenir si des applications accordent des droits d'accès personnalisés

Limiter l'accès aux données d'authentification des ressources

#### Référentiel de comptes utilisateur

Nom de superdomaine

Définition du superdomaine en cours

Définitions de superdomaines disponibles

Configurer... Définir comme actif

#### Authentification

Mécanismes d'authentification et expiration

LTPA

Kerberos et LTPA  
[Configuration de Kerberos](#)

SWAM (obsolète) : aucune communication authentifiée entre les serveurs.  
[Paramètres de la mémoire cache d'authentification](#)

+ Sécurité Web et SIP

+ Sécurité RMI/IIOP

+ Service JAAS (Java Authentication and Authorization Service)

Activer JASPI (Java Authentication SPI)  
[Fournisseurs](#)

Utiliser des noms d'utilisateur qualifiés du superdomaine

- [Domaines de sécurité](#)
- [Fournisseurs d'autorisation externes](#)
- [Configuration des cookies de session par programme](#)
- [Propriétés personnalisées](#)

Appliquer   Réinitialiser

# Configuration de la sécurité

5

## □ Garder l'option sélectionnée par défaut et cliquer sur suivant

Cet assistant vous permet de sécuriser votre environnement de serveur d'applications. L'infrastructure de serveur d'applications peut stocker des utilisateurs et des mots de passe d'administration ou elle peut utiliser un registre existant avec des utilisateurs administratifs stockés et/ou d'applications.

### → Etape 1: Spécifier l'étendue de la protection

*(La prochaine étape de l'assistant dépend des décisions prises dans l'étape en cours)*

### Spécifier l'étendue de la protection

Cet assistant vous permet de sécuriser votre environnement de serveur d'applications. L'infrastructure de serveur d'applications peut stocker des utilisateurs et des mots de passe d'administration ou elle peut utiliser un registre existant avec des utilisateurs administratifs stockés et/ou d'applications.

Si vous utilisez un registre existant tel que le système d'exploitation local, LDAP ou un registre personnalisé, voici les informations dont vous avez besoin :

- Informations de configuration pour se connecter au registre existant
- Nom d'utilisateur existant dans le registre et agissant en tant qu'administrateur principal.

Au minimum, cette tâche fournit une administration sécurisée. Cependant, la sécurité administrative ne fournit pas à elle seule une sécurité complète. Nous vous conseillons d'activer également la sécurité des applications et des ressources dans la plupart des environnements.

Activer la sécurité des applications

Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales.

Suivant

Annuler

# Choix du référentiel

6

## □ Sélectionner l'option « registre personnalisé autonome »

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

→ **Etape 2:  
Sélectionner le référentiel d'utilisateurs**

*(La prochaine étape de l'assistant dépend des décisions prises dans l'étape en cours)*

Etape 3: Récapitulatif

### Sélectionner le référentiel d'utilisateurs

Le référentiel de comptes utilisateur stocke des noms d'utilisateurs et de groupes utilisés pour l'authentification et l'autorisation. Le référentiel par défaut est intégré au système du serveur d'applications et peut être fédéré avec un ou plusieurs référentiels LDAP (Lightweight Directory Access Protocol) externes. Vous pouvez également sélectionner un référentiel externe autonome.

- Référentiels fédérés
- Registre LDAP autonome
- Système d'exploitation local
- Registre personnalisé autonome

Précédent

Suivant

Annuler

# Configuration du référentiel personnalisé

7

- 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

8

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

# Configuration du référentiel personnalisé

9

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

Configuration de la sécurité

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

Etape 2: Sélectionner le référentiel d'utilisateurs

→ **Etape 3: Configurez un registre personnalisé autonome.**

Etape 4: Récapitulatif

### Configurez un registre personnalisé autonome.

Les référentiels personnalisés, comme les référentiels de base de données, nécessitent qu'une classe Java soit définie pour accéder à la base de données. Si la sécurité a auparavant été activée à l'aide de ce référentiel, saisissez le nom d'un utilisateur doté de privilèges d'administration qui se trouve dans le référentiel.

\* Nom d'administrateur principal  
adm

\* Nom de la classe du registre personnalisé  
com.ibm.websphere.security.FileRegistrySample

Ignorer maj/min pour l'autorisation

Les référentiels personnalisés exigent souvent une spécification d'une ou plusieurs propriétés spécifiques à l'implémentation du référentiel.

Nom	Valeur
usersFile	C:\IBM\WebSphere\AppServer\fileregis
groupsFile	C:\IBM\WebSphere\AppServer\fileregis

Précédent Suivant Annuler

# Récapitulatif

10

- 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.

Configuration de la sécurité

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

Etape 2: Sélectionner le référentiel d'utilisateurs

Etape 3: Configurez un registre personnalisé autonome.

→ Etape 4: Récapitulatif

## Récapitulatif

Affiche la liste des valeurs sélectionnées dans l'assistant qui seront utilisées pour activer la sécurité.

Options	Valeurs
Activer la sécurité administrative	vrai
Activer la sécurité des applications	vrai
Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales.	faux
Référentiel d'utilisateurs	Registre personnalisé autonome
Nom d'administrateur principal	adm
Nom de la classe du registre personnalisé	com.ibm.websphere.security.FileRegistrySample
Ignorer maj/min pour l'autorisation	faux

Propriétés personnalisées

```
userFile = C:/IBM/WebSphere/AppServer
/emsiUsers/user.prop
groupFile = C:/IBM/WebSphere/AppServer
/emsiUsers/groupFile.prop
```

Précédent

Terminer

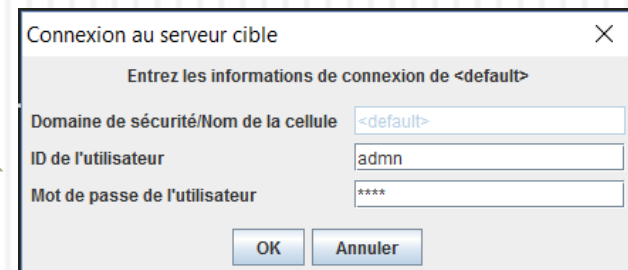
Annuler

# Enregistrer les informations d'authentification.

11

- 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=**adm**n
  - com.ibm.SOAP.loginPassword=**adm**n
- Redémarrer WAS, puis se reconnecter à la console d'administration.

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



Connexion au serveur cible

Entrez les informations de connexion de <default>

Domaine de sécurité/Nom de la cellule <default>

ID de l'utilisateur adm

Mot de passe de l'utilisateur \*\*\*\*

OK Annuler

# Le référentiel du système d'exploitation

12

- 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 »

## Configuration de la sécurité

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

→ **Etape 2: Sélectionner le référentiel d'utilisateurs**

*(La prochaine étape de l'assistant dépend des décisions prises dans l'étape en cours)*

Etape 3: Récapitulatif

### Sélectionner le référentiel d'utilisateurs

Le référentiel de comptes utilisateur stocke des noms d'utilisateurs et de groupes utilisés pour l'authentification et l'autorisation. Le référentiel par défaut est intégré au système du serveur d'applications et peut être fédéré avec un ou plusieurs référentiels LDAP (Lightweight Directory Access Protocol) externes. Vous pouvez également sélectionner un référentiel externe autonome.

- Référentiels fédérés
- Registre LDAP autonome
- Système d'exploitation local
- Registre personnalisé autonome

Précédent

Suivant

Annuler

# Ajout d'un utilisateur Windows

13

Nouvel utilisateur

Nom d'utilisateur : wasadmin

Nom complet : Administrateur WebSphere

Description :

Mot de passe : .....

Confirmer le mot de passe : .....

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

Aide Créer Fermer

□ 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 »

	Nom	Nom complet
✓ Gestion de l'ordinateur (local)		
✓ Outils système		
> Planificateur de tâches		
> Observateur d'événements		
> Dossiers partagés		
✓ Utilisateurs et groupes locaux		
Utilisateurs	Administrateur	
Groupes	db2admin	db2admin
> Performance	DefaultAccount	
	Invité	
	nadir	Abdeljalil Nadiri
	nadir_	abdeljalil nadiri
	wasadmin	Administrateur WebSphere

## □ Saisir le nom d'utilisateur Windows « wasadmin »

### Configuration de la sécurité

Sécurise l'environnement de traitement des applications.

Etape 1: Spécifier  
l'étendue de la  
protection

Etape 2: Sélectionner  
le référentiel  
d'utilisateurs

→ **Etape 3:  
Configurez un  
système  
d'exploitation local.**

Etape 4: Récapitulatif

#### **Configurez un système d'exploitation local.**

Le référentiel de comptes utilisateur stocke des noms d'utilisateurs et de groupes utilisés pour l'authentification et l'autorisation. Le référentiel par défaut est intégré au système du serveur d'applications et peut être fédéré avec un ou plusieurs référentiels LDAP (Lightweight Directory Access Protocol) externes. Vous pouvez également sélectionner un référentiel externe autonome.

\* Nom d'administrateur principal

Précédent

Suivant

Annuler

# Configuration de la sécurité

15

- 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 de la sécurité

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

Etape 2: Sélectionner le référentiel d'utilisateurs

Etape 3: Configurez un système d'exploitation local.

→ **Etape 4: Récapitulatif**

### Récapitulatif

Affiche la liste des valeurs sélectionnées dans l'assistant qui seront utilisées pour activer la sécurité.

Options	Valeurs
Activer la sécurité administrative	vrai
Activer la sécurité des applications	vrai
Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales.	faux
Référentiel d'utilisateurs	Système d'exploitation local
Nom d'administrateur principal	wasadmin

Précédent

Terminer

Annuler

# Configuration d'un système d'exploitation local

16

## Configuration de la sécurité

Sécurise l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

Etape 2: Sélectionner le référentiel d'utilisateurs

→ **Etape 3: Configurez un système d'exploitation local.**

Etape 4: Récapitulatif

### Configurez un système d'exploitation local.

Le référentiel de comptes utilisateur stocke des noms d'utilisateurs et de groupes utilisés pour l'authentification et l'autorisation. Le référentiel par défaut est intégré au système du serveur d'applications et peut être fédéré avec un ou plusieurs référentiels LDAP (Lightweight Directory Access Protocol) externes. Vous pouvez également sélectionner un référentiel externe autonome.

\* Nom d'administrateur principal

Précédent

Suivant

Annuler

# Récapitulatif

17

## Configuration de la sécurité

Sécurisez l'environnement de traitement des applications.

Etape 1: Spécifier l'étendue de la protection

Etape 2: Sélectionner le référentiel d'utilisateurs

Etape 3: Configurez un système d'exploitation local.

→ **Etape 4: Récapitulatif**

### Récapitulatif

Affiche la liste des valeurs sélectionnées dans l'assistant qui seront utilisées pour activer la sécurité.

Options	Valeurs
Activer la sécurité administrative	vrai
Activer la sécurité des applications	vrai
Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales.	faux
Référentiel d'utilisateurs	Système d'exploitation local
Nom d'administrateur principal	adminwas

Précédent

Terminer

Annuler

# Référentiel LDAP autonome

18

- 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

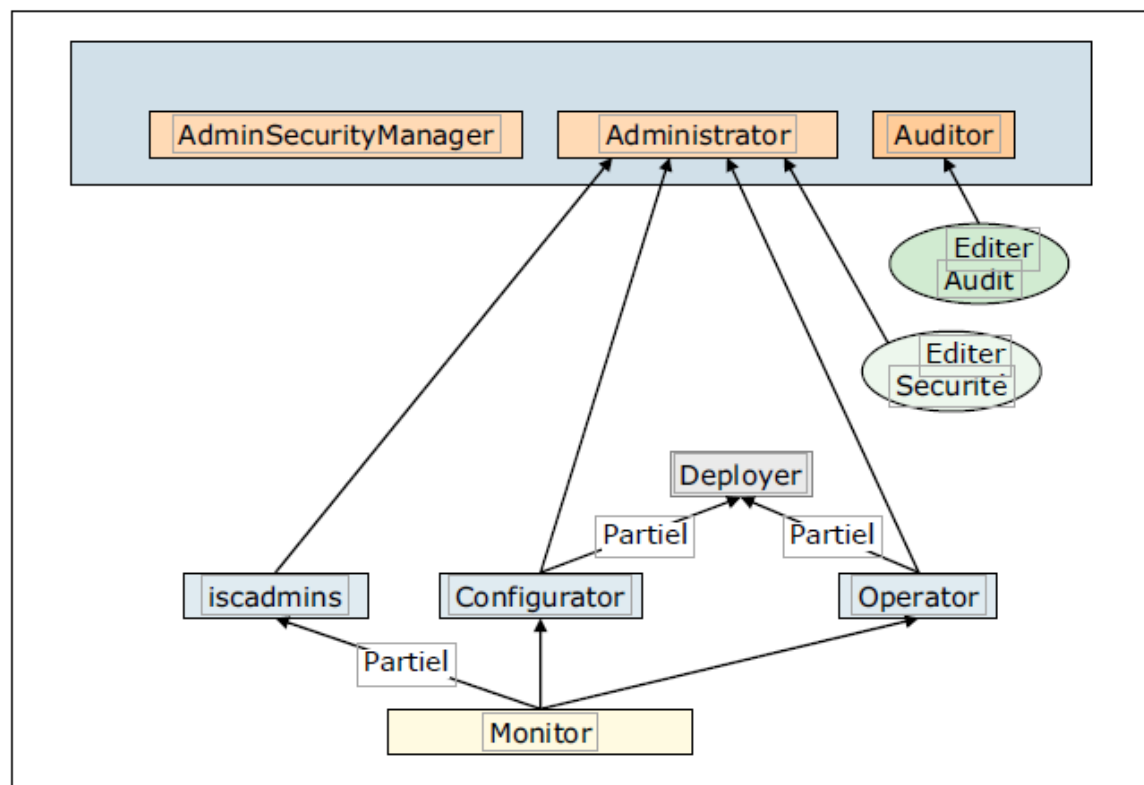
19

- 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

20

- 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

22

- Opérateur
  - Possède les privilèges 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 .
- Isadmins: disponible pour les utilisateurs de la console, ce rôle possède 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

23

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

## [Sécurité globale](#) > Rôles d'administrateur

Cette page permet d'attribuer des rôles d'administration à des utilisateurs, ainsi que de supprimer ou modifier ces rôles. L'attribution de rôles d'administration à des utilisateurs permet à ceux-ci d'administrer les serveurs d'applications par le biais de la console d'administration ou de scripts wsadmin.

<input type="button" value="Déconnecter"/> <input type="button" value="Ajouter..."/> <input type="button" value="Retirer"/>			
			
Sélectionner	Utilisateur 	Rôle(s) 	Etat de connexion 
Aucun			
Total 0			

# Affectation des utilisateurs à des rôles

24

## [Sécurité globale](#) > [Rôles d'administrateur](#) > [Utilisateur](#)

Cette page permet d'attribuer des rôles d'administration à des utilisateurs, ainsi que de supprimer ou modifier ces rôles. L'attribution de rôles d'administration à des utilisateurs permet à ceux-ci d'administrer les serveurs d'applications par le biais de la console d'administration ou de scripts wsadmin.

### \* Rôle(s)

Auditeur  
Configurateur  
Moniteur  
Opérateur

### Recherche et sélection des utilisateurs

Déterminez le nombre de résultats à afficher et entrez une chaîne de recherche (vous pouvez utiliser \* comme caractère générique), puis cliquez sur Rechercher. Dans la liste Disponible, sélectionnez des utilisateurs et ajoutez-les à la liste Mappé au rôle. Les utilisateurs ayant déjà été mappés à un rôle n'apparaîtront pas les résultats de la recherche.

Chaîne à rechercher

\*

Nombre maxi de résultats à afficher

Disponible

adm  
user2  
user3



Mappé au rôle

user1