

Installation d'AX Serveur avec PostgreSQL (multi-serveurs)

Version : 14

Publié : dimanche 21 avril 2019

Table des matières

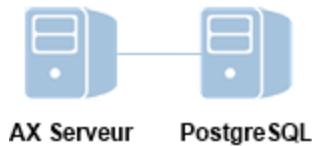
Table des matières	3
Introduction	5
Tâches de pré-installation	7
Recueillir des ressources d'installation	8
Ports d'AX Serveur	10
Télécharger les programmes d'installation d'Analytics Exchange	13
Installation	15
Installer le serveur de base de données PostgreSQL	16
Installer AX Serveur autonome pour PostgreSQL	20
Tâches de post-installation	27
Vérifier qu'AX Serveur est en cours d'exécution	29
Activer AX Serveur	31
Ajouter un administrateur AX Serveur	33
Configurer le répertoire d'archivage et de restauration des données	34
Vérifier les connexions des applications clientes	35
Configuration de Python pour être utilisé avec AX Serveur	37
Installation du nœud moteur d'AX (facultatif)	41
Installer le nœud moteur d'AX pour PostgreSQL	42
Configurer un dossier de données partagé	46
Configurer des nœuds moteur d'AX	47
Certificats de sécurité	51
Installer des certificats de sécurité pour le serveur AX	54
Installer les certificats de sécurité pour le connecteur ACL pour Analytics Exchange	59
Annexe	63
Conditions requises pour AX Serveur	64
Conditions requises pour Nœud moteur d'AX	70
Configuration du compte de service	74
Authentification d'Analytics Exchange	77
Attribuer des droits au service du Connecteur AX	78

Table des matières

Configurer l'authentification Windows intégrée	80
aclAuditExchange.xml	84
Désactiver AX Serveur	90

Introduction

L'objectif de ce guide est de vous accompagner tout au long du processus d'installation d'AX Serveur avec un serveur de base de données PostgreSQL. Le contenu de ce guide se limite à l'installation et la configuration initiale.



Pour obtenir plus d'informations sur la maintenance d'AX Serveur et l'utilisation d'Analytics Exchange, visitez les pages [Documentation d'aide d'ACL en ligne](#).

Public visé

Ce guide s'adresse aux administrateurs d'AX Serveur en charge de l'installation et de la configuration d'Analytics Exchange pour leurs organisations.

Tâches de pré-installation

Recueillir des ressources d'installation

Avant de commencer à installer ou à mettre à niveau AX Serveur, identifiez les principaux interlocuteurs prêts à vous aider et à vous communiquer des informations concernant le processus d'installation.

Assistance ACL

Contactez l'Assistance ACL si vous rencontrez des problèmes que vous ne parvenez pas à résoudre pendant l'installation ou la mise à niveau. Avant de contacter l'Assistance ACL, veuillez vous assurer d'être en possession des informations suivantes :

- La version précise d'AX Serveur que vous installez ou mettez à niveau
- Les détails sur la base de données (PostgreSQL ou Oracle) que vous utilisez avec AX Serveur
- Tous les messages d'erreur ou d'avertissement que vous rencontrez

Vous pouvez contacter l'Assistance ACL de plusieurs façons différentes :

- [en soumettant un ticket de support en ligne](#) (méthode conseillée)
- [chat en direct](#)
- e-mail (support@acl.com)
- [téléphone](#)

Contact primaire ACL

Pour télécharger le package d'installation d'AX Serveur à partir de la Barre de lancement, vous devez disposer d'un compte Barre de lancement valide.

- Si vous êtes le contact primaire dans votre organisation, vous devez avoir reçu un e-mail de bienvenue d'ACL avec des instructions pour la connexion à votre compte. Si vous n'avez pas reçu l'e-mail de bienvenue ou si avez besoin d'aide supplémentaire, contactez l'Assistance ACL.
- Si vous n'êtes pas le contact primaire, vous devriez avoir reçu des instructions par e-mail lorsque le contact primaire vous a ajouté à la Barre de lancement. Si vous n'avez pas reçu d'instructions, contactez le contact primaire de votre organisation ou l'administrateur de votre compte Analytics Exchange.

Administrateur de base de données

Si votre organisation dispose d'un administrateur de base de données, celui-ci disposera d'importantes informations dont vous avez besoin pour installer et configurer AX Serveur.

Personnel informatique

Si votre organisation dispose d'un personnel informatique qui administre des services comme l'accès au réseau, le stockage des fichiers et les politiques de sécurité, ce personnel peut disposer d'informations nécessaires à l'installation. Il se peut que ce personnel doive également effectuer des tâches comme créer des comptes utilisateur Active Directory et modifier les règles de pare-feu.

Ports d'AX Serveur

Pour que le service Analytics Exchange démarre correctement sur le serveur AX Serveur ou sur le nœud moteur d'AX, assurez-vous que les ports requis par le serveur d'applications TomEE ne sont pas utilisés par d'autres services ou applications.

Vérifier les ports utilisés

À partir d'une invite de commande, utilisez la commande NETSTAT pour afficher les ports en cours d'utilisation :

```
NETSTAT -a
```

Si les ports requis sont en cours d'utilisation par un autre service, vous devez effectuer l'une des opérations suivantes :

- reconfigurer le service pour utiliser un autre port
- désactiver temporairement le service dans les services Windows pendant que vous installez AX Serveur

Si nécessaire, modifiez certains ports utilisés par AX Serveur une fois l'installation terminée.

Remarque

Si vous installez AX Serveur ou le nœud moteur d'AX pour la première fois sur un serveur, vous devez vérifier que les ports utilisés par le serveur d'applications TomEE ne sont pas utilisés avant de lancer le programme d'installation.

Ports requis par AX Serveur

AX Serveur et le nœud moteur d'AX sont installés avec les paramètres de port par défaut utilisés par le service Analytics Exchange.

Port	Composant	Cryptage	Description
80	Tomcat Connector HTTP	Non SSL	Port utilisé pour la communication HTTP non cryptée avec le serveur. Il s'agit d'un port unidirectionnel. Il doit être ouvert pour les communications extérieures sur AX Serveur et sur le nœud moteur d'AX.
443	Tomcat Connector HTTPS	SSL	Port utilisé pour la communication HTTP (HTTPS) cryptée avec le serveur. Il s'agit d'un port bidirectionnel. Il doit être ouvert sur AX Serveur pour les communications avec AX Client.

Port	Composant	Cryptage	Description
			<p>Si vous mettez à niveau une version antérieure d'AX Serveur, le port par défaut est 8443.</p>
5432	PostgreSQL	Prise en charge	<p>Vous pouvez spécifier un autre port qui n'est pas utilisé dans le programme d'installation d'AX Serveur.</p> <p>Remarque</p> <p>Si vous configurez une installation sur deux serveurs, vérifiez que PostgreSQL, AX Serveur et le nœud moteur d'AX peuvent communiquer sur ce port.</p>
10000	Connecteur AX	TwoFish 128 bit	<p>Si ce port est utilisé, vous pouvez spécifier un autre port qui n'est pas utilisé dans le programme d'installation d'AX Serveur.</p> <p>Ce service est utilisé principalement pour accéder aux tables AX Serveur qui ont été exportées vers des projets ACL Analytics. Il doit être ouvert sur AX Serveur pour les communications entrantes.</p>
4201	Nœud moteur d'AX	Non SSL	<p>Permet de connecter le nœud moteur d'AX à l'AX Serveur maître. Si le nœud moteur d'AX et AX Serveur communiquent via un pare-feu, vous devez ouvrir ce port.</p>
1521	Base de données Oracle	Non SSL	<p>Port utilisé pour communication à la base de données Oracle non cryptée Il doit être ouvert sur AX Serveur et sur le nœud moteur d'AX pour la communication avec la base de données Oracle.</p> <p>Remarque</p> <p>Votre équipe informatique indiquera le port requis lorsqu'Oracle est utilisé comme serveur de base de données d'AX Serveur. Le port peut, au besoin, être modifié à la fin de l'installation.</p>
5432	Base de données Oracle	SSL	<p>Port utilisé pour communication à la base de données Oracle cryptée Il doit être ouvert sur AX Serveur et sur le nœud moteur d'AX pour la communication avec la base de données Oracle si vous chiffrerez la connexion.</p> <p>Remarque</p> <p>Votre équipe informatique indiquera le port requis lorsqu'Oracle est utilisé comme serveur de base de données d'AX Serveur. Le port peut, au besoin, être modifié à la fin de l'installation.</p>
1543	Connecteur ACL pour Analytics Exchange	SSL	<p>Port utilisé pour établir une connexion ODBC avec les résultats des outils d'analyse. Ce port est uniquement requis si vous installez le service facultatif Connecteur ACL pour Analytics Exchange.</p> <p>Il doit être ouvert sur AX Serveur pour les communications entrantes.</p>

Configuration du pare-feu

Pour vous connecter à AX Serveur depuis l'extérieur du pare-feu, vous devez autoriser les connexions entrantes sur les ports suivants :

Port	Composant	Description
443	Tomcat Connector HTTPS	<p>Permet d'activer les connexions HTTPS au serveur Web pour les applications Web Client Web d'AX et Configuration d'AX Serveur ainsi que pour les transferts de fichiers sécurisés depuis et vers AX Serveur.</p> <p>Ce port est également requis pour utiliser aclscript.exe afin de communiquer avec les modules ACL GRC tels que Résultats ou Projets.</p> <p>Remarque</p> <p>La valeur par défaut pour les serveurs mis à niveau à partir de versions antérieures sur 5.0.0 est 8443.</p>
10000	Connecteur AX	Permet d'activer l'accès aux tables d'AX Serveur à partir des ordinateurs clients par le biais d'ACL Analytics.
4201	Nœud moteur d'AX	Permet de connecter le nœud moteur d'AX à l'AX Serveur maître. Si le nœud moteur d'AX et AX Serveur communiquent via un pare-feu, vous devez ouvrir ce port.

Les ports correspondants de chaque ordinateur client qui se connecte à AX Serveur doivent également être ouverts pour les communications sortantes.

Connexion à ACL GRC

Si vous prévoyez de transférer des données entre AX Serveur et des modules ACL GRC tels que Résultats ou Projets, vous devez autoriser la connexion suivante :

- **Exécutable** : aclscript.exe
- **Port** : 443
- **Domaine sur liste blanche** : *.aclgrc.com

Télécharger les programmes d'installation d'Analytics Exchange

Téléchargez les programmes d'installation à partir de la Barre de lancement pour que vous puissiez installer Analytics Exchange.

Remarque

Vous devez pouvoir vous connecter à un compte Barre de lancement (www.aclgrc.com) afin de télécharger les programmes d'installation d'Analytics Exchange et d'activer AX Serveur.

Programmes d'installation disponibles

Les programmes d'installation pour les applications Analytics Exchange suivantes sont disponibles sur la Barre de lancement :

- AX Serveur (contient les programmes d'installation d'AX Serveur et de PostgreSQL)
- Nœud moteur d'AX
- Mise à niveau de comptabilité ACL Analytics pour AX Serveur (si applicable actuellement)
- Client AX
- Direct Link

Étapes de téléchargement

Remarque

La page de téléchargement de l'installateur offre la version la plus récente d'Analytics Exchange. Si vous avez besoin d'un installateur pour une version précédente, vous devez contacter l'Assistance ACL pour obtenir une copie de l'installateur de cette version.

1. Connectez-vous à la Barre de lancement (www.aclgrc.com) et cliquez sur **Analytics Exchange**.

Un e-mail contenant les instructions de connexion est envoyé depuis l'adresse notifications@aclgrc.com à l'administrateur du compte Analytics Exchange de votre société. Si vous n'êtes pas en mesure de vous connecter à votre compte de la Barre de lancement, contactez l'administrateur du compte Analytics Exchange de votre société ou l'Assistance ACL pour obtenir de l'aide.

2. Dans la liste **Sélectionnez le package de logiciels à télécharger**, choisissez le programme d'installation que vous souhaitez télécharger.

Remarque

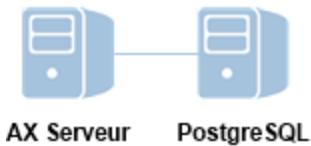
Assurez-vous d'avoir téléchargé l'édition correcte (non-Unicode ou Unicode) puisque toutes les applications installées doivent utiliser la même édition.

3. Cliquez sur **Télécharger <Version>** et enregistrez l'installateur dans l'ordinateur sur lequel vous prévoyez d'installer l'application.

Installation

Installer le serveur de base de données PostgreSQL

Exécutez le programme d'installation d'AX Serveur sur l'ordinateur du serveur de base de données pour installer PostgreSQL sur une machine physique distincte. Une fois la base de données installée, annulez le programme d'installation, puis exécutez la partie de l'installation d'AX Serveur sur la machine du serveur d'applications.



Remarque

Vous devez installer PostgreSQL avant d'installer AX Serveur.

Installer PostgreSQL

Exécuter le programme d'installation et sélectionner la configuration de votre base de données

1. Double-cliquez sur le package d'installation ; si une boîte de dialogue d'avertissement de sécurité s'affiche, vérifiez les informations indiquées et cliquez sur **Oui**.
2. Sélectionnez la langue d'installation, puis cliquez sur **OK**.
3. Sur la page **Configurer l'emplacement d'extraction**, spécifiez le dossier dans lequel les fichiers d'installation seront extraits, puis cliquez sur **Installer**.

Astuce

Cliquez sur **Parcourir** pour choisir un dossier ou accepter l'emplacement par défaut : `C:\Program Files (x86)\ACL Software\Installers\ACLAX<version>_Server_<édition>`.

4. Cliquez sur **Oui** dans la boîte de dialogue contenant le message à propos du moteur de base de données.
5. Sur la page **Options de configuration d'Analytics Exchange Serveur**, sélectionnez **PostgreSQL** et cliquez sur **Installer**.
6. Pour exécuter l'assistant d'installation PostgreSQL, cliquez sur **Oui**.
7. Si vous êtes invité à installer les logiciels prérequis, cliquez sur **Installer** et patientez pendant que les logiciels prérequis s'installent.

Suivez les instructions à l'écran pour effectuer la configuration prérequise.

Configurer la connexion à la base de données et la sécurité

- Sur la page **Bienvenue**, cliquez sur **Suivant**, puis sur la page **Accord de licence**, sélectionnez **J'accepte les conditions du présent accord de licence** et cliquez sur **Suivant**.
- Sur la page **Dossier de destination**, acceptez l'emplacement d'installation par défaut de PostgreSQL, ou cliquez sur **Modifier** pour modifier l'emplacement et cliquez sur **Suivant**.
Si vous modifiez l'emplacement de l'installation, le chemin d'accès que vous spécifiez ne doit pas inclure d'espace.
- Sur la page **Configurer votre serveur de base de données PostgreSQL Analytics Exchange**, sélectionnez **Nouvelle installation**, puis cliquez sur **Suivant**.

Le serveur de base de données PostgreSQL est installé ; pendant le processus d'installation d'AX Serveur qui suit, une nouvelle base de données Analytics Exchange est créée.

- Dans la page **Configuration du service** entrez les informations suivantes pour configurer le service de la base de données PostgreSQL, puis cliquez sur **Suivant** :

Champ	Description
Nom du compte	<p>Le nom du compte utilisateur Windows qui exécutera le service.</p> <p>Conservez le nom du compte par défaut « postgres », à moins que vous n'ayez une raison de le modifier. Si le compte n'existe pas déjà, il sera créé en tant que compte utilisateur local. Vous ne pouvez pas utiliser de comptes appartenant au groupe Administrateurs sur le serveur. Si vous utilisez un compte existant, les autorisations requises pour le système de fichiers et le droit « Se connecter en tant que service » sont attribués au compte.</p>
Domaine du compte	<p>Le nom du domaine Active Directory auquel le compte utilisateur appartient.</p> <p>Si vous utilisez un compte utilisateur local, conservez la valeur par défaut du nom de l'ordinateur.</p>
Mot de passe du compte	<p>Le mot de passe du compte utilisateur.</p> <p>Si le compte utilisateur existe déjà, vous devez entrer le mot de passe correspondant. Si le programme d'installation est en train de créer un nouveau compte, entrez le mot de passe à utiliser. Le mot de passe doit remplir l'ensemble des conditions exigées relatives à la complexité des mots de passe qui sont respectées par le système d'exploitation Windows. En outre, le mot de passe ne doit pas inclure de barres obliques inverses (\) ni d'apostrophes (').</p>
Vérifier le mot de passe	Entrez à nouveau le mot de passe pour le vérifier.

- Si le compte utilisateur n'existe pas, cliquez sur **Oui** pour créer le compte.
- Dans la page **Configuration de la base de données**, entrez les informations suivantes, puis cliquez sur **Suivant** :

Champ	Description
Numéro de port	Le port utilisé pour les communications avec PostgreSQL. Le port par défaut est 5432.
Nom du super-utilisateur	Le nom du compte superutilisateur PostgreSQL. La valeur par défaut est postgres et elle ne peut pas être modifiée.
Mot de passe	Le mot de passe du compte Superutilisateur PostgreSQL. Votre mot de passe ne doit pas inclure de barres obliques inverses (\) ni d'apostrophes (').
	<p>Remarque</p> <p>Pour des raisons de sécurité, n'utilisez pas le même mot de passe que vous avez utilisé pour le compte utilisateur Windows qui exécute le service de base de données PostgreSQL.</p>
Mot de passe (à nouveau)	Entrez à nouveau le mot de passe pour le confirmer.

Remarque

Prenez note du nom du compte superutilisateur PostgreSQL et du mot de passe.

Vous devrez les saisir lorsque vous crerez la base de données Analytics Exchange pendant la partie AX Serveur de l'installation.

Pour plus d'informations sur la configuration des comptes de service, consultez la rubrique "Configuration du compte de service" Page 74.

7. Dans la page **Informations sur le certificat SSL**, entrez les informations suivantes pour créer un certificat de sécurité auto-signé pour sécuriser les connexions HTTPS entre PostgreSQL et AX Serveur (et AX Exception s'il est installé), puis cliquez sur **Suivant** :

Champ	Description
Nom du serveur	Le nom d'hôte du serveur de bases de données. Par exemple : ax.abc.com .
Nom du service ou de la division	La division ou l'unité commerciale pour laquelle le certificat est émis. Par exemple : Développement .
Nom de l'organisation	Le nom de votre entreprise ou organisation. Par exemple : ABC Corporation .
Nom de la ville	La ville ou la localité où se trouve votre entreprise ou organisation. Par exemple : Vancouver .
Nom du Département/Région	Le département ou la région où se trouve votre entreprise ou organisation. Par exemple : BC .
Code du pays	Le code du pays à deux caractères correspondant au pays dans lequel votre entreprise ou votre organisation est située. Par exemple : CA .

Champ	Description
Mot de passe	Entrez un mot de passe d'au moins 6 caractères.
Vérifier le mot de passe	Entrez à nouveau le même mot de passe pour le confirmer.

Pour plus d'informations sur l'utilisation de ce certificat et pour connaître les options de configuration, consultez la rubrique "Certificats de sécurité" Page 51.

8. Cliquez sur **Installer**, puis une fois l'installation terminée, cliquez sur **Terminer**.

Le processus d'installtion d'AX Serveur démarre automatiquement lorsque l'installation de PostgreSQL est terminée.

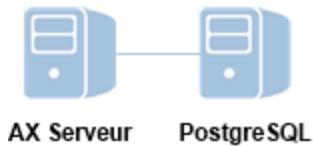
9. Annulez le programme d'installation en cliquant sur le bouton **Annuler** dès que le bouton **Annuler** apparaît.

Postrequis

Maintenant que PostgreSQL est installé, copiez le programme d'installation sur l'ordinateur du serveur d'applications, puis installez AX Serveur. Pour plus d'informations, consultez la section "Installer AX Serveur autonome pour PostgreSQL" Page suivante.

Installer AX Serveur autonome pour PostgreSQL

Installez AX Serveur sans PostgreSQL si votre serveur de base de données se trouve sur une machine physique distincte.



Conditions préalables

La base de données PostgreSQL doit être déjà installée sur un serveur distinct avant que vous installiez AX Serveur. Pour plus d'informations, consultez la section "Installer le serveur de base de données PostgreSQL" Page 16.

Installer AX Serveur

Attention

Vous devez installer les mises à niveau Windows [KB2919355](#) avant de démarrer l'installation d'Analytics Exchange sur Windows Server 2012 R2. En cas de non installation de cette mise à niveau, l'installation d'Analytics Exchange sera défaillante.

Exécuter le programme d'installation et sélectionner la configuration de votre base de données

1. Double-cliquez sur le package d'installation ; si une boîte de dialogue d'avertissement de sécurité s'affiche, vérifiez les informations indiquées et cliquez sur **Oui**.
2. Sélectionnez la langue d'installation, puis cliquez sur **OK**.
3. Sur la page **Configurer l'emplacement d'extraction**, spécifiez le dossier dans lequel les fichiers d'installation seront extraits, puis cliquez sur **Installer**.

Astuce

Cliquez sur **Parcourir** pour choisir un dossier ou accepter l'emplacement par défaut : `C:\Program Files (x86)\ACL Software\Installers\ACLAX<version>_Server _edition>`.

4. Cliquez sur **Oui** dans la boîte de dialogue contenant le message à propos du moteur de base de données.

5. Sur la page **Options de configuration d'Analytics Exchange Serveur**, sélectionnez **PostgreSQL** et cliquez sur **Installer**.
6. Pour annuler l'assistant d'installation PostgreSQL, cliquez sur **Non**.
7. Si vous êtes invité à installer les logiciels prérequis, cliquez sur **Installer** et patientez pendant que les logiciels prérequis s'installent.

Suivez les instructions à l'écran pour effectuer la configuration prérequise. Il peut vous être demandé de redémarrer votre ordinateur après l'installation des prérequis.

Configurer vos services Analytics Exchange

1. Si vous êtes invité à installer les logiciels prérequis, cliquez sur **Installer** et patientez pendant que les logiciels prérequis s'installent.

Suivez les instructions à l'écran pour effectuer la configuration prérequise. Il peut vous être demandé de redémarrer votre ordinateur après l'installation des prérequis. Si vous devez redémarrer l'ordinateur, poursuivez l'installation en double-cliquant sur le programme d'installation puis en sélectionnant la langue, l'emplacement d'installation et le serveur de base de données appropriés.

Remarque

Vous pouvez être invité(e) à accepter les termes et conditions de .NET Framework lors de l'installation des prérequis. Dans ce cas, une boîte de dialogue peut être cachée derrière la boîte de dialogue du programme d'installation d'Analytics Exchange. Lors de l'installation de .NET Framework, assurez-vous que le programme d'installation n'attend pas votre saisie.

2. Sur la page **Bienvenue**, cliquez sur **Suivant**, puis sur la page **Accord de licence**, sélectionnez **J'accepte les conditions du présent accord de licence** et cliquez sur **Suivant**.
3. Sur la page **Dossiers et paramètres de destination**, définissez l'emplacement d'installation des fichiers d'application d'AX Serveur et l'emplacement de stockage des données d'AX Serveur.

Si nécessaire, cliquez sur **Modifier** pour changer un des emplacements par défaut ou les deux. Les chemins d'accès spécifiés ne doivent pas inclure d'espaces et l'espace disque disponible à l'emplacement que vous spécifiez pour les données d'AX Serveur doit être suffisant.

Remarque

Si vous souhaitez stocker des données d'AX Serveur sur un serveur de fichiers dédié ou à un autre emplacement du réseau, vous devez configurer le dossier partagé après l'installation. Le dossier partagé ne peut pas être spécifié dans l'assistant d'installation d'AX Serveur.

4. Dans le panneau **Numéro de port du connecteur d'Analytics Exchange**, saisissez le numéro de port que le connecteur AX doit utiliser ou acceptez la valeur par défaut de 10000.

Le service Connecteur AX sert avant tout à accéder aux tables ACL sur AX Serveur à partir d'ACL Analytics.

5. Dans le panneau **Compte de service Tomcat ACL Analytics Exchange**, effectuez les opérations suivantes :

- a. Entrez le nom de domaine et le nom d'utilisateur du compte au format **domaine\nom_utilisateur**, ou cliquez sur **Parcourir** pour localiser le domaine et le nom d'utilisateur requis.

Si vous recherchez le nom de compte en cliquant sur Parcourir, vous devez tout d'abord entrer ou sélectionner le nom du domaine ou du serveur dans la boîte de dialogue **Rechercher un compte utilisateur** afin que le programme d'installation présente la liste appropriée des comptes utilisateur disponibles.

Remarque

L'utilisation d'un compte local n'est pas prise en charge pour l'exécution du service TomEE. Ces comptes ne disposent pas des priviléges appropriés pour exécuter certaines commandes ACL.

- b. Entrez le **mot de passe** du compte.
- c. Cliquez sur **Suivant**.
- d. Si vous êtes invité à accorder le droit « Log on as a service » sur le compte de service Tomcat, cliquez sur **Oui**, puis sur **OK**.

Pour plus d'informations sur les options de configuration des comptes de service, consultez la rubrique "Configuration du compte de service" Page 74.

Configurer vos paramètres de connexion à la base de données

1. Sur la page **Configurez votre base de données Analytics Exchange**, assurez-vous que **PostgreSQL** est sélectionné, puis effectuez l'une des opérations suivantes :
 - Si vous installez AX Serveur et PostgreSQL sur le même serveur physique, décochez **Crypter les communications de la base de données**.
 - Si vous installez AX Serveur et PostgreSQL sur des serveurs physiques différents, sélectionnez **Crypter les communications de la base de données** pour crypter la connexion.

Astuce

Le cryptage ralentit un peu les performances, c'est pourquoi vous devez l'activer uniquement si les données sont transférées entre le serveur de bases de données et le serveur d'applications sur un réseau non sécurisé.

2. Dans la page **Paramètres de connexion à la base de données Analytics Exchange**, saisissez les informations suivantes pour configurer la chaîne de connexion :

Champ	Description
Serveur de bases de données	L'adresse IP ou le nom du serveur sur lequel est située la base de données. Si vous installez AX Serveur sur le même serveur physique que PostgreSQL, conservez la valeur par défaut localhost à moins que vous n'ayez une raison de la modifier.

Champ	Description
Port	Le port à utiliser pour se connecter à la base de données PostgreSQL. Le port par défaut est 5432.
Superutilisateur	Le nom du compte superutilisateur PostgreSQL. Conservez la valeur par défaut postgres à moins que vous n'ayez une raison de la modifier.
Mot de passe	Le mot de passe du compte Superutilisateur.

3. Sur la page **Nouvel utilisateur PostgreSQL pour la base de données Analytics Exchange**, saisissez les informations suivantes, puis cliquez sur **Suivant** :

- **Nom d'utilisateur** : le nom du compte utilisateur de la base de données PostgreSQL à utiliser pour accéder à la base de données Analytics Exchange. Le programme d'installation crée ce compte utilisateur lorsqu'il crée la base de données.
- **Mot de passe** : le mot de passe du compte utilisateur de la base de données PostgreSQL.
- **Mot de passe (à nouveau)** : entrez à nouveau le mot de passe du compte utilisateur de la base de données PostgreSQL pour le confirmer.

Configurer la sécurité et l'authentification

1. Sur la page **Informations de connexion à Microsoft Active Directory**, vérifiez que la valeur indiquée dans la zone de texte **Domaine par défaut** est correcte, ou saisissez-la, puis cliquez sur **Suivant**.

Remarque

La valeur du domaine par défaut correspond au domaine pour lequel les utilisateurs sont authentifiés s'ils ne précisent pas de domaine lorsqu'ils se connectent à l'aide de l'authentification par formulaire. Par exemple, si un utilisateur saisit **jsmith** comme nom d'utilisateur et que le domaine par défaut est ABC, cela équivaut à saisir **abc\jsmith**.

2. Sur la page **Authentification d'Analytics Exchange**, choisissez la méthode d'authentification qui convient :
- **Authentification par formulaire** : sélectionnez cette option si vous souhaitez que les utilisateurs soient invités à entrer leur nom d'utilisateur et leur mot de passe à chaque fois qu'ils démarrent une nouvelle session avec Analytics Exchange. Une session est créée à l'ouverture d'une nouvelle fenêtre de navigateur Web ou au démarrage d'AX Client.
 - **Authentification Windows intégrée** : sélectionnez cette option si vous souhaitez que les utilisateurs soient authentifiés en mode silencieux par les applications Analytics Exchange basées sur le compte utilisateur servant à se connecter à Windows. Les comptes utilisateurs qui appartiennent au domaine Active Directory configuré ne devront pas nécessairement entrer les informations relatives à leur nom d'utilisateur et à leur mot de passe lorsqu'ils accéderont aux applications Analytics Exchange.

Pour obtenir plus d'informations sur les options d'authentification et sur la configuration requise, consultez la rubrique "Authentification d'Analytics Exchange" Page 77.

3. Spécifiez les détails de la configuration de l'authentification d'AX Serveur en effectuant l'une des actions suivantes, puis cliquez sur **Suivant**:
 - Si vous avez sélectionné **Authentification par formulaire**, spécifiez le nom d'hôte du serveur où AX Serveur est installé. Par exemple : **AX . ABC . COM**.
 - Si vous avez sélectionné **Authentification Windows intégrée**, saisissez les informations suivantes :
 - **Nom d'hôte d'ACL Analytics Exchange Serveur** : indiquez le nom d'hôte du serveur d'installation d'AX Serveur. Par exemple : **AX . ABC . COM**
 - **Domaine Active Directory** : spécifiez le domaine Active Directory à utiliser pour authentifier les utilisateurs
 - **Adresse IP du contrôleur de domaine Kerberos** : l'adresse IP à laquelle le contrôleur de domaine Active Directory de votre organisation est situé
 - **Mot de passe du service Kerberos** : le mot de passe du compte au nom principal de service créé dans Active Directory
4. Si vous avez un certificat de sécurité SSL existant, effectuez les opérations suivantes dans la page **Informations sur le certificat SSL** :
 - a. Sélectionnez **Utiliser le fichier de magasin de clés existant** et accédez au fichier de magasin de clés sur votre ordinateur.
 - b. Saisissez le **mot de passe du magasin de clés** existant.
5. Dans la page **Informations sur le certificat SSL**, entrez les informations suivantes, puis cliquez sur **Suivant**:

Champ	Description
Nom du serveur	Le nom de domaine qualifié du serveur du nœud moteur d'AX. Par exemple : ax . abc . com .
Nom du service ou de la division	La division ou l'unité commerciale pour laquelle le certificat est émis. Par exemple : Développement .
Nom de l'organisation	Le nom de votre entreprise ou organisation. Par exemple : ABC Corporation .
Nom de la ville	La ville ou la localité où se trouve votre entreprise ou organisation. Par exemple : Vancouver .
Nom du Département/Région	Le département ou la région où se trouve votre entreprise ou organisation. Par exemple : BC .
Code du pays	Le code du pays à deux caractères correspondant au pays dans lequel votre entreprise ou votre organisation est située. Par exemple : CA .
Mot de passe du magasin de clés	Entrez un mot de passe d'au moins 6 caractères.

Champ	Description
	<p>Remarque Si vous utilisez un fichier de magasins de clés existant, cette instance de la zone de texte Mot de passe du magasins de clés est désactivée.</p>
Mot de passe de clé privée	Entrez à nouveau le même mot de passe. Le mot de passe du magasin de clés et le mot de passe de clé privée doivent être identiques.

Pour plus d'informations sur l'utilisation de ce certificat et pour connaître les options de configuration, consultez la rubrique "Certificats de sécurité" Page 51.

- Sur la page **Saisir le nom d'utilisateur et le mot de passe de la console Tomcat**, saisissez les informations suivantes, puis cliquez sur **Suivant** :
 - Nom d'utilisateur** : saisissez le nom d'utilisateur que vous souhaitez utiliser pour accéder au Gestionnaire d'applications Web Tomcat et à l'application Configuration d'AX Serveur ainsi que pour les administrer
 - Mot de passe** : saisissez un mot de passe pour le nom d'utilisateur
 - Confirmer le mot de passe** : entrez à nouveau le mot de passe pour le confirmer

Terminer l'installation

- Cliquez sur **Installer**.

Remarque

Avant la fin du processus d'installation, vous devez attendre environ une minute avant que le serveur d'application TomEE ne devienne entièrement fonctionnel. La fenêtre de commande peut apparaître par intermittence pendant cette période.

N'annulez pas l'installation.

- Une fois le processus d'installation achevé, cliquez sur **Terminer** pour quitter le programme d'installation.

L'application Web Configuration d'AX Serveur s'ouvre dans le navigateur Web par défaut après la fin du programme d'installation. Vous devez terminer les tâches qui suivent l'installation dans l'application Web afin qu'AX Serveur puisse fonctionner parfaitement. Pour plus d'informations, consultez la section "Tâches de post-installation" Page 27.

Remarque

Si l'application Web Configuration d'AX Serveur affiche une erreur dans le navigateur Web, attendez 2 ou 3 minutes avant de recharger la page. En fonction du matériel de votre serveur, cela peut prendre quelques minutes aux services requis avant qu'ils soient fonctionnels.

Si vous fermez l'application Web Configuration d'AX Serveur avant de terminer toutes les tâches qui suivent l'installation, vous pouvez y accéder de nouveau dans un navigateur Web. L'emplacement par

défaut est <https://<nomserveur>/aclconfig>, où <nomserveur> est le nom d'hôte ou l'adresse IP de votre AX Serveur. Par exemple : <https://axserver.acl.com/aclconfig>.

Tâches de post-installation

Effectuez les tâches suivantes pour achever l'installation d'AX Serveur.

Remarque

En fonction de votre configuration d'AX Serveur, certaines de ces tâches peuvent être facultatives. Si vous avez des composants sur plusieurs serveurs physiques, il se peut que vous deviez effectuer ces tâches sur chaque machine.

Tâches d'AX Serveur

1. Vérifiez qu'AX Serveur est en cours d'exécution.

Pour plus d'informations, consultez la section "Vérifier qu'AX Serveur est en cours d'exécution" Page 29.

2. Activez AX Serveur.

Pour plus d'informations, consultez la section "Activer AX Serveur" Page 31.

3. Ajoutez un administrateur AX Serveur.

Pour plus d'informations, consultez la section "Ajouter un administrateur AX Serveur" Page 33.

4. Configurez le répertoire d'archivage et de restauration des données.

Pour plus d'informations, consultez la section "Configurer le répertoire d'archivage et de restauration des données" Page 34.

5. Facultatif. Installez et configurez Python sur AX Serveur et sur les instances du nœud moteur d'AX si vous avez l'intention d'utiliser l'intégration Python dans des scripts d'outils d'analyse.

Pour plus d'informations, consultez la section "Configuration de Python pour être utilisé avec AX Serveur" Page 37.

Tâches d'AX Client

1. Vérifiez les connexions des applications clientes.

Pour plus d'informations, consultez la section "Vérifier les connexions des applications clientes" Page 35.

2. Facultatif. Sur la machine AX Serveur, configurez le paramètre du délai d'expiration de l'application pour AX Client.

Par défaut, l'application expire après 30 minutes d'inactivité. Vous pouvez modifier le paramètre de durée d'inactivité maximale dans le fichier de configuration [aclAuditExchange.xml](#). Pour plus d'informations, consultez la rubrique "aclAuditExchange.xml" Page 84.

Vérifier qu'AX Serveur est en cours d'exécution

Vérifiez qu'AX Serveur est en cours d'exécution en vérifiant la trace du service, les services et le Gestionnaire d'applications Web Tomcat.

Consulter la trace du service Analytics Exchange

Pour vérifier que le service Analytics Exchange est en cours d'exécution, dans le sous-répertoire **TomCat/logs** d'AX Serveur, ouvrez le fichier **TomEE.date.log**, puis examinez les entrées de la trace.

Un nouveau fichier trace est créé à chaque fois que le service est démarré/redémarré ou lorsque le fichier dépasse la taille de fichier maximale.

Vérifier les services AX Serveur

L'état de chaque service AX Serveur Windows doit être défini sur « Démarré » ou « En cours d'exécution ». Si vous avez installé des composants AX Serveur sur plusieurs serveurs, assurez-vous de vérifier les services sur tous les serveurs.

1. Sur le serveur sur lequel les services sont exécutés, accédez au **Panneau de configuration de Windows**, sélectionnez **Outils d'administration**, puis ouvrez **Services**.
2. Dans la fenêtre **Services**, vérifiez que la colonne **Statut** des services suivants indique bien le statut « Démarré » ou «En cours d'exécution» :
 - **Service Analytics Exchange**: s'exécute sur AX Serveur et sur chaque instance du nœud moteur d'AX
 - **Connecteur AX**: s'exécute uniquement sur AX Serveur
 - **Base de données Analytics Exchange <numéro de version>** : s'exécute sur le serveur où PostgreSQL est installé

Ce service peut s'exécuter sur le même serveur qu'AX Serveur ou sur un serveur distinct. Le service est uniquement présent si PostgreSQL est le serveur de bases de données pour AX Serveur

Si certains services n'ont pas démarré, vous pouvez tenter de les lancer en cliquant dessus à l'aide du bouton droit de la souris et en sélectionnant **Démarrer**. Si le service ne démarre toujours pas, consultez le fichier trace pour déterminer la cause du problème ou contactez l'Assistance ACL.

Vérifier les applications AX Serveur

Vérifiez l'état du déploiement des applications AX Serveur dans le Gestionnaire d'applications Web Tomcat.

1. À partir d'un navigateur Web, accédez à http://nom_serveur/manager et connectez-vous au Gestionnaire d'applications Web Tomcat.

Remplacez *nom_serveur* par le nom d'hôte ou l'adresse IP du serveur hébergeant l'instance du Nœud moteur d'AX ou AX Serveur.

Remarque

Vos informations d'identification au Gestionnaire d'applications Web Tomcat sont spécifiées lors de l'installation d'AX Serveur. Si vous ne vous rappelez plus de vos informations d'identification, réinitialisez-les.

2. Confirmez que les applications suivantes affichent l'état **Exécution en cours** sur **true** dans AX Serveur :

- Analytics Exchange (AX) Serveur <numéro de version>
- Client Web AX <numéro de version>
- Admin système d'AX <numéro de version>
- Serveur AX Core <numéro de version>
- AX Central Authentication System (CAS) <numéro de version>
- AX Gateway Mapper <numéro de version>
- Client léger d'AX <numéro de version>
- Application Tomcat Host Manager
- Application Tomcat Manager
- Interface REST AX Core <numéro de version>
- Apache TomEE

Si certaines applications n'ont pas démarré, dans la colonne **Commandes**, cliquez sur **Démarrer**.

3. Quittez le Gestionnaire d'applications Web Tomcat.

Activer AX Serveur

Vous pouvez activer votre AX Serveur en ligne via la Configuration d'AX Serveur ou hors ligne via la Barre de lancement.

Remarque

Vous devez avoir un compte Barre de lancement valide avec les autorisations appropriées pour activer AX Serveur. Si vous n'avez pas de compte Barre de lancement, contactez votre administrateur de compte Analytics Exchange.

Renouvellement d'un abonnement ?

Si vous renouvez un abonnement expiré, vous devez désactiver, puis réactiver votre instance d'AX Serveur pour terminer le processus de renouvellement. Pour plus d'informations sur la désactivation du serveur, consultez la rubrique "Désactiver AX Serveur" Page 90.

Activation en ligne

1. Connectez-vous à l'application Web Configuration d'AX serveur (<https://<nomserveur>/aclconfig>) et localisez le panneau **Activation**.
2. Dans la liste **Type de serveur**, sélectionnez l'une des options suivantes :
 - **Production** : le serveur de production principal
 - **Non-Production** : le serveur utilisé à des fins de non-production comme les tests et l'élaboration de versions intermédiaires
 - **Reprise sur sinistre** : le serveur désigné pour la reprise sur sinistre ou le basculement
3. Dans **Activation**, saisissez vos informations d'identification de la Barre de lancement et cliquez sur **Sélectionner Org**.
4. Dans la liste **Organisations**, sélectionnez l'organisation à laquelle appartient le serveur, puis cliquez sur **Activer le serveur**.

Résultats : après l'importation du fichier d'identification, le message **Le serveur a été activé** s'affiche.

Activation hors ligne

1. Connectez-vous à l'application Web Configuration d'AX serveur (<https://<nomserveur>/aclconfig>) et localisez le panneau **Activation**.
2. Dans la liste **Type de serveur**, sélectionnez l'une des options suivantes :
 - **Production** : le serveur de production principal
 - **Non-Production** : le serveur utilisé à des fins de non-production comme les tests et

l'élaboration de versions intermédiaires

- **Reprise sur sinistre** : le serveur désigné pour la reprise sur sinistre ou le basculement

3. Dans **Activation hors ligne**, cliquez sur **Générer** et enregistrez le fichier d'identification de la machine **AXOfflineActivation.mif** sur votre poste de travail.

Votre poste de travail local doit disposer d'une connexion Internet pour accéder à la Barre de lancement et effectuer le reste de la procédure d'activation.

4. Connectez-vous à la Barre de lancement (www.aclgrc.com), puis sélectionnez votre organisation.

5. Sélectionnez **Options > Activations** et dans le côté gauche, cliquez sur **Activation hors connexion**.

6. Chargez votre fichier d'activation :

- a. Cliquez sur **Choisir un fichier**, accédez au fichier d'identification de l'ordinateur du serveur **AXOfflineActivation.mif**, puis cliquez sur **Ouvrir**.

- b. Dans la liste déroulante Application, sélectionnez le type d'installation AX Serveur.

- c. Dans la liste déroulante **Utilisateur**, sélectionnez votre nom puis cliquez sur **Charger**.

Résultat : une fois le fichier d'identification de l'ordinateur chargé, le nom de l'ordinateur du serveur apparaît dans la liste Activations.

7. En regard du nom du serveur activé, cliquez sur **Télécharger un fichier d'activation** et enregistrez le fichier d'activation (**analytics_exchange_server.oaf**) sur votre poste de travail local.

8. À partir de l'application Web Configuration d'AX Serveur, dans la section Activation hors connexion, naviguez jusqu'au fichier d'activation que vous avez téléchargé depuis la Barre de lancement et cliquez sur **Importer**.

Résultats : après l'importation du fichier d'identification, le message **Le serveur a été activé** s'affiche.

Ajouter un administrateur AX Serveur

Utilisez l'application Web Configuration d'AX Serveur pour ajouter un utilisateur administratif. Le rôle d'Administrateur est accordé à l'utilisateur.

Remarque

Vous devez ajouter au moins un compte d'administration après l'installation d'AX Serveur pour utiliser AX Client. Une fois que vous avez ajouté le premier utilisateur, vous pouvez en ajouter d'autres à l'aide d'AX Client.

1. Dans un navigateur Web, accédez à <https://<nomserveur>/aclconfig> et connectez-vous à l'application Web Configuration d'AX Serveur.

Utilisez les mêmes informations d'identification que pour vous connecter au Gestionnaire d'applications Web Tomcat.

2. Localisez le panneau **Ajouter un administrateur AX**, puis entrez le nom du compte utilisateur Windows à ajouter :

- Si le compte utilisateur fait partie du domaine Active Directory par défaut lié à votre mise en œuvre Analytics Exchange, saisissez le nom d'utilisateur sans indiquer le domaine.

Le domaine par défaut pour AX Serveur est spécifié dans la section **Paramètres** du panneau **Serveur**.

- Si le compte utilisateur ne fait pas partie du domaine Active Directory par défaut, spécifiez le domaine et le nom d'utilisateur au format suivant : **Domaine\NomUtilisateur**
- Si le compte utilisateur est un compte utilisateur Windows local sur le serveur où AX Serveur est installé, spécifiez le nom de l'ordinateur et le nom d'utilisateur dans le format suivant : **NomOrdinateur\NomUtilisateur**

3. Cliquez sur **Ajouter un administrateur**.

Configurer le répertoire d'archivage et de restauration des données

Configurez le répertoire d'archivage et de restauration des données pour que les utilisateurs finaux ayant des droits d'administrateurs pour l'application dans AX Client puissent avoir accès aux commandes d'archivage et de restauration.

Remarque

Si le répertoire n'est pas configuré, les commandes d'archivage et de restauration sont désactivées dans AX Client.

1. Dans un navigateur Web, accédez à <https://<nomserveur>/aclconfig> et connectez-vous à l'application Web Configuration d'AX Serveur.
Utilisez les mêmes informations d'identification que pour vous connecter au Gestionnaire d'applications Web Tomcat.
2. Dans la section **Serveur**, dans le champ **Répertoire d'archivage et de restauration des données**, saisissez le chemin du fichier ou le chemin UNC du répertoire où vous souhaitez enregistrer les collections archivées.

Vous devez spécifier un dossier qui existe déjà. Un chemin UNC est un dossier partagé spécifié sous le format suivant : `\<nom_serveur>\<dossier_partagé>`.

Le compte utilisateur utilisé pour exécuter le service Analytics Exchange doit avoir les Autorisations complètes pour le dossier que vous configurez comme répertoire d'archivage et de restauration des données. Vous devez affecter manuellement les droits de sécurité requis dans Active Directory.

Remarque

Le répertoire de données peut être situé localement sur AX Serveur, ou sur un serveur de fichiers distant ou un réseau de stockage (SAN). Vous devez vous assurer que l'emplacement spécifié dispose de suffisamment d'espace disque dédié au stockage de vos collections archivées en fonction de la taille des collections stockées dans AX Serveur, y compris les résultats des tâches d'analyse ainsi que les politiques d'archivage au sein de votre organisation.

3. Pour enregistrer vos modifications, cliquez sur **Actualiser** en bas de la section **Serveur**.

Vérifier les connexions des applications clientes

Vérifiez que les utilisateurs en local et à distance peuvent se connecter à AX Serveur à l'aide d'AX Client, d'ACL Analytics et du Client Web d'AX après l'installation d'AX Serveur et des instances du nœud moteur d'AX.

Conditions préalables

Aux emplacements depuis lesquels les utilisateurs se connecteront :

- installez AX Client
- installez ACL Analytics

Vérifications des connexions des applications

Vérifier	Détails
Démarrez AX Client et connectez-vous à AX Serveur.	<p>Si vous ne parvenez pas à vous connecter, confirmez les paramètres suivants :</p> <ul style="list-style-type: none"> ◦ Si le compte utilisateur avec lequel vous vous connectez n'appartient pas au domaine Active Directory par défaut spécifié pour AX Serveur, spécifiez le domaine à la connexion. Par exemple : NomDomaine\NomUtilisateur ◦ Les paramètres Serveur spécifiés dans la boîte de dialogue Options doivent correspondre aux paramètres requis par AX Serveur. ◦ Si un pare-feu est présent sur l'ordinateur client sur lequel AX Client est en cours d'exécution, assurez-vous que les ports requis sont inutilisés pour les communications sortantes. <p>Par défaut, c'est le port 443 (Connecteur Tomcat HTTPS). Le port 10000 (Connecteur AX) doit également être libre si ACL Analytics est en cours d'utilisation.</p>
Exportez une table à partir d'AX Serveur pour laquelle un fichier de données source est stocké sur AX Serveur.	<ol style="list-style-type: none"> a. Quand vous sélectionnez la table, vérifiez que la propriété Source de données indique : « La source de données est administrée par AX Serveur ». b. Dans la boîte de dialogue Exporter, vérifiez que Travailler avec le(s) fichier(s) exporté(s) est sélectionné et que Exporter les fichiers de données avec les définitions sélectionnées est désélectionné (paramètres par défaut). c. Si vous pouvez ouvrir la table dans ACL Analytics après avoir entré le mot de passe du profil de serveur, c'est que le Connecteur AX est configuré correctement. d. Si vous ne parvenez pas à ouvrir la table du serveur, consultez la rubrique "Attribuer des droits au service du Connecteur AX" Page 78 pour obtenir des instructions en vue d'effectuer la configuration de sécurité complémentaire pouvant s'avérer nécessaire. <p>Lorsque vous importez un projet ACL ou un outil d'analyse dans AX Serveur et que vous sélectionnez Importer des fichiers de données source (fichiers .fil), les tables du projet sont converties en tables de serveur et les fichiers de données ACL associés (.fil) sont copiés dans AX Serveur.</p>

Vérifier	Détails
	<p>Vous pouvez avoir accès aux tables de serveur à l'aide du Connecteur AX.</p>
Lancez le système d'aide en sélectionnant Aide > Contenu .	<p>Si les requêtes HTTP à partir de l'ordinateur client sont redirigées vers un serveur proxy, il est possible que les tentatives d'accès au système d'aide échouent. Vous pouvez spécifier l'adresse IP et le port corrects pour le serveur proxy en ajoutant les deux lignes suivantes au fichier ACLA-nalyticsExchange.ini dans le répertoire d'installation d'AX Client. L'emplacement par défaut est C:\Program Files\ACL Software\ACL Analytics Exchange Client.</p> <p>-Dhttp.proxyHost=<proxy_serveur_nom_hôte_ou_ip> -Dhttp.proxyPort=<proxy_serveur_port></p> <p>Par exemple :</p> <p>-Dhttp.proxyHost=192.168.5.190 -Dhttp.proxyPort=3128</p>

Configuration de Python pour être utilisé avec AX Serveur

Pour configurer Python afin de l'utiliser avec AX Serveur, vous devez installer la bonne version de Python et ajouter l'exécutable Python à la variable d'environnement PATH de votre système. Après avoir installé PYTHON, définissez les variables d'environnement système ACLPYTHONDLL et PYTHONPATH sur chaque machine qui héberge une instance d'AX Serveur ou du Nœud moteur d'AX.

Fonctionnement

Pour exécuter des scripts Python, ACL Exchange doit pouvoir appeler l'exécutable Python et trouver les scripts qu'on lui ordonne d'exécuter. AX Serveur utilise la variable d'environnement PATH pour localiser Python et la variable d'environnement PYTHONPATH pour localiser les scripts.

Installez Python version 3.5.x (32-bit)

Remarque

Vous devez effectuez ces étapes sur toutes les machines qui hébergent une instance d'AX Serveur ou du Nœud moteur d'AX.

1. À partir de la [page des téléchargements Python](#), téléchargez la dernière version de Python 3.5 sur votre poste.
2. Sur votre poste, double-cliquez sur le programme d'installation.
3. Dans le programme d'installation, sélectionnez **Ajouter Python *versionNumber* à PATH**.
4. Cliquez sur **Installer** et suivez les instructions à l'écran.
5. Redémarrez la machine avant d'exécuter des scripts Python depuis ACL.

Définir les variables d'environnement ACLPYTHONDLL et PYTHONPATH

Remarque

Vous devez effectuez ces étapes sur toutes les machines qui hébergent une instance d'AX Serveur ou du Nœud moteur d'AX. Le compte utilisateur qui exécute le service Analytics Exchange doit avoir l'autorisation d'accéder au(x) dossier(s) dans votre variable d'environnement PYTHONPATH.

1. Dans votre système d'exploitation Windows, créez un ou plusieurs dossiers qui hébergeront vos scripts Python.

Exemple : `C:\python_scripts`.

2. Dans le système d'exploitation Windows, ouvrez la boîte de dialogue **Propriétés système**, puis cliquez sur **Variables d'environnement**.
3. Dans la section **Variables système**, cliquez sur **Nouveau**, puis saisissez les variables suivantes :

Nom de la variable	Valeur de la variable	Exemple
PYTHONPATH	Le chemin d'accès complet au(x) dossier(s) que vous avez créé(s) pour héberger les scripts Python. Séparez plusieurs chemins d'accès au dossier par un point-virgule.	<code>C:\python_scripts;C:\dev;C:\tmp</code>
ACLPYTHONDLL	<p>Nom du chemin d'accès complet et nom du fichier Python DLL dans le dossier d'installation Python à utiliser avec ACL.</p> <p>Si vous utilisez Python 3.3.x, les restrictions suivantes s'appliquent :</p> <ul style="list-style-type: none"> ○ Les caractères Unicode ne sont pas pris en charge dans le chemin d'accès pour les plateformes européennes ○ Les caractères étendus ne sont pas pris en charge dans le chemin d'accès pour les plateformes asiatiques 	<code>c:\python_install\python33.dll</code>

Nom de la variable	Valeur de la variable	Exemple
	<p>Remarque</p> <p>Python ajoute la DLL au dossier système (<code>c:\Windows\System32\python33.dll</code>) plutôt qu'au dossier d'installation. Vous devez copier le fichier DLL du dossier système vers le dossier d'installation et l'utiliser comme valeur de variable afin qu'ACL puisse accéder à la DLL.</p> <p>Il se peut que vous deviez aussi supprimer les paramètres de lecture seule du dossier d'installation.</p> <p>Si vous ne définissez pas cette valeur, ACL tente d'utiliser la DLL version 3.5.x prise en charge par défaut <code>python35.dll</code>.</p>	

- Pour enregistrer la variable, cliquez sur **OK**, puis, dans la boîte de dialogue **Propriétés système**, cliquez à nouveau sur **OK**.

Installation du nœud moteur d'AX (facultatif)

Installer le nœud moteur d'AX pour PostgreSQL

Installez le nœud moteur d'AX pour augmenter la capacité de traitement analytique d'Analytics Exchange. Le nœud moteur d'AX est hébergé sur un serveur distinct d'AX Serveur.

Installer le nœud moteur d'AX

Attention

Vous devez installer les mises à niveau Windows [KB2919355](#) avant de démarrer l'installation d'Analytics Exchange sur Windows Server 2012 R2. En cas de non installation de cette mise à niveau, l'installation d'Analytics Exchange sera défaillante.

Exécuter le programme d'installation et sélectionner la configuration de votre base de données

1. Double-cliquez sur le package d'installation ; si une boîte de dialogue d'avertissement de sécurité s'affiche, vérifiez les informations indiquées et cliquez sur **Oui**.
2. Sélectionnez la langue d'installation, puis cliquez sur **OK**.
3. Sur la page **Configurer l'emplacement d'extraction**, spécifiez le dossier dans lequel les fichiers d'installation seront extraits, puis cliquez sur **Installer**.

Astuce

Cliquez sur **Parcourir** pour choisir un dossier ou pour accepter l'emplacement par défaut : `C:\Program Files (x86)\ACL Software\Installers\ACLAx<version>_EngineNode_<édition>`.

4. Sur la page **Options de configuration d'Analytics Exchange Serveur**, sélectionnez **PostgreSQL** et cliquez sur **Suivant**.
5. Si vous êtes invité à installer les logiciels prérequis, cliquez sur **Installer** et patientez pendant que les logiciels prérequis s'installent.

Suivez les instructions à l'écran pour effectuer la configuration prérequise.

Configurer votre service de base de données

1. Sur la page **Bienvenue**, cliquez sur **Suivant**, puis sur la page **Accord de licence**, sélectionnez **J'accepte les conditions du présent accord de licence** et cliquez sur **Suivant**.
2. Sur la page **Dossiers de destination**, définissez l'emplacement d'installation des fichiers d'application du nœud moteur d'AX ainsi que le répertoire de travail pour le traitement des outils d'analyse, puis cliquez sur **Suivant**.

Si nécessaire, cliquez sur **Modifier** pour changer un des emplacements par défaut ou les deux. Les chemins spécifiés ne doivent pas inclure d'espaces.

3. Sur la page **Informations du serveur ACL Analytics Exchange**, saisissez l'adresse IP du serveur sur lequel AX Serveur est installé et cliquez sur **Suivant**.
4. Sur la première page **Informations de connexion à la base de données Analytics Exchange Serveur**, sélectionnez **PostgreSQL** dans les options **Plateforme de bases de données**.
5. Pour crypter la communication de la base de données, sélectionnez **Crypter les communications de la base de données**, puis cliquez sur **Suivant**.

Pour crypter la connexion, votre serveur de base de données doit être configuré pour les connexions SSL.

Astuce

Le cryptage ralentit un peu les performances, c'est pourquoi vous devez l'activer uniquement si les données sont transférées entre le serveur de bases de données et le serveur d'applications sur un réseau non sécurisé.

6. Dans la deuxième page **Paramètres de connexion à la base de données Analytics Exchange**, saisissez les informations suivantes :

Champ	Description
Serveur de bases de données	L'adresse IP ou le nom du serveur sur lequel est située la base de données. Si vous installez AX Serveur sur le même serveur physique que PostgreSQL, conservez la valeur par défaut localhost à moins que vous n'ayez une raison de la modifier.
Port	Le port à utiliser pour se connecter à la base de données PostgreSQL. Le port par défaut est 5432.
Superutilisateur	Le nom du compte superutilisateur PostgreSQL. Conservez la valeur par défaut postgres à moins que vous n'ayez une raison de la modifier.
Mot de passe	Le mot de passe du compte Superutilisateur.

Configurer le compte et la sécurité du service d'application

1. Dans le panneau **Compte de service Tomcat ACL Analytics Exchange**, effectuez les opérations suivantes, puis cliquez sur **Suivant** :
 - a. Entrez le nom de domaine et le nom d'utilisateur du compte au format **domaine\nom_utilisateur**, ou cliquez sur **Parcourir** pour localiser le domaine et le nom d'utilisateur requis. Si vous recherchez le nom de compte en cliquant sur Parcourir, vous devez tout d'abord entrer ou sélectionner le nom du domaine ou du serveur dans la boîte de dialogue **Rechercher un compte utilisateur** afin que le programme d'installation présente la liste appropriée des comptes utilisateur disponibles.

Remarque

L'utilisation d'un compte local n'est pas prise en charge pour l'exécution du service TomEE. Ces comptes ne disposent pas des priviléges appropriés pour exécuter certaines commandes ACL.

- b. Entrez le **mot de passe** du compte.
- c. Cliquez sur **Suivant**.
- d. Si vous êtes invité à accorder le droit « Log on as a service » sur le compte de service Tomcat, cliquez sur **Oui**, puis sur **OK**.

Pour plus d'informations sur les options de configuration des comptes de service, consultez la rubrique "Configuration du compte de service" Page 74.

2. Dans la page **Informations sur le certificat SSL**, entrez les informations suivantes pour créer un certificat de sécurité auto-signé pour sécuriser les connexions HTTPS vers le nœud moteur d'AX, puis cliquez sur **Suivant**:

Champ	Description
Nom du serveur	Le nom de domaine qualifié du serveur du nœud moteur d'AX. Par exemple : ax.abc.com .
Nom du service ou de la division	La division ou l'unité commerciale pour laquelle le certificat est émis. Par exemple : Développement .
Nom de l'organisation	Le nom de votre entreprise ou organisation. Par exemple : ABC Corporation .
Nom de la ville	La ville ou la localité où se trouve votre entreprise ou organisation. Par exemple : Vancouver .
Nom du Département/Région	Le département ou la région où se trouve votre entreprise ou organisation. Par exemple : BC .
Code du pays	Le code du pays à deux caractères correspondant au pays dans lequel votre entreprise ou votre organisation est située. Par exemple : CA .
Mot de passe du magasin de clés	<p>Entrez un mot de passe d'au moins 6 caractères.</p> <p>Remarque</p> <p>Si vous utilisez un fichier de magasins de clés existant, cette instance de la zone de texte Mot de passe du magasin de clés est désactivée.</p>
Mot de passe de clé privée	Entrez à nouveau le même mot de passe. Le mot de passe du magasin de clés et le mot de passe de clé privée doivent être identiques.

Pour plus d'informations sur l'utilisation de ce certificat et pour connaître les options de configuration, consultez la rubrique "Certificats de sécurité" Page 51.

Terminer l'installation

1. Cliquez sur **Installer**.

Remarque

Avant la fin du processus d'installation, vous devez attendre environ une minute avant que le serveur d'application TomEE ne devienne entièrement fonctionnel. La fenêtre de commande peut apparaître par intermittence pendant cette période.

N'annulez pas l'installation.

2. Une fois le processus d'installation achevé, cliquez sur **Terminer** pour quitter le programme d'installation.

Postrequis

- "Configurer un dossier de données partagé" Page suivante
- "Configurer des nœuds moteur d'AX" Page 47

Configurer un dossier de données partagé

Pour stocker des fichiers de données dans un serveur autre qu'AX Serveur ou pour prendre en charge un Nœud moteur AX dans un ou plusieurs serveurs, vous devez fournir un accès aux fichiers de données d'AX Serveur via un dossier partagé.

Utilisation des dossiers de données

Il existe deux cas d'utilisation courants pour les dossiers de données partagés :

- **Stockage de données externe** : vous pouvez stocker les fichiers de données dans un serveur qui dispose d'un espace disque disponible plus important ou dans un serveur de fichiers en réseau.
- **Nœud moteur d'AX** : les installations exigent un dossier partagé afin que les serveurs d'outils d'analyse et AX Serveur puissent avoir accès aux fichiers de données.

Emplacement de dossier partagé

L'accès au dossier partagé doit s'effectuer via un chemin Windows UNC dont le format se présente sous la forme : \\NomOrdinateur\DossierPartagé et être localisé soit dans un dossier Windows partagé ou dans un réseau de stockage (SAN).

Autorisations de dossier nécessaires

Le compte utilisateur Windows servant à exécuter le service sur le serveur du serveur d'application TomEE sur AX Serveur et sur chaque Nœud moteur d'AX doit posséder des autorisations en lecture et en écriture pour le dossier.

Les utilisateurs ayant accès aux tables d'AX Serveur à l'aide d'ACL Analytics doivent posséder des autorisations d'accès en lecture pour le dossier.

Configurer un dossier partagé sur Windows 2008

1. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier que vous voulez partager et sélectionnez **Partager**.
2. Dans la boîte de dialogue **Partage du fichier**, sélectionnez les utilisateurs ou les groupes avec lesquels vous souhaitez partager le dossier.
3. Vérifiez les autorisations attribuées à chaque utilisateur ou groupe et cliquez sur la liste déroulante en regard de chaque entrée dont vous souhaitez modifier les autorisations, puis sélectionnez les autorisations appropriées.
4. Cliquez sur **Partager** puis sur **Exécuté**.

Configurer des nœuds moteur d'AX

Utilisez une ou plusieurs instances de Nœud moteur d'AX pour exécuter un outil d'analyse dans plusieurs serveurs et augmenter la puissance de traitement.

Fonctionnement

Augmentation de la puissance de traitement

Par défaut, les outils d'analyse sont traités directement sur AX Serveur. Bien que cette solution fonctionne dans la plupart des cas, il est possible que vous ayez besoin de puissance de traitement supplémentaire lorsque :

- vous voulez exécuter des outils d'analyse qui exigent une puissance de traitement élevée ;
- vous voulez exécuter un nombre d'outils d'analyse dans un laps de temps court.

Pour augmenter la puissance de traitement, vous pouvez configurer une ou plusieurs instances de Nœud moteur d'AX et exécuter vos outils d'analyse sur ces serveurs séparés.

Remarque

Lorsque le Nœud moteur d'AX est activé, les tâches d'outils d'analyse ne s'exécutent pas sur AX Serveur. Toutes les tâches s'exécutent sur une instance du Nœud moteur d'AX.

Équilibrage de plusieurs nœuds

Lorsqu'un nœud a de la place dans sa file d'attente, il informe AX Serveur de sa capacité à traiter des tâches et le serveur assigne alors des tâches à ce nœud. Ainsi, l'exécution de plusieurs nœuds moteur d'AX capables de gérer plusieurs tâches simultanément peut induire qu'un seul nœud gère plusieurs tâches pendant que d'autres restent vides.

Pour garantir un équilibrage des tâches entre les nœuds, indiquez le nombre maximum de tâches pouvant être traitées en tant que **1** et planifiez en conséquence les tâches des outils d'analyse.

Configuration des nœuds moteur d'AX

Conditions préalables

Avant d'ajouter et de configurer un nœud moteur d'AX dans l'application Web Configuration d'AX Serveur, vous devez :

- Configurer votre système afin que les fichiers de données AX Serveur soient stockés dans un dossier partagé accessible via un chemin UNC (par exemple `\nom_serveur\dossier_`

partagé). Pour plus d'informations, consultez la section "Configurer un dossier de données partagé" Page 46

- Installer physiquement et configurer chaque instance du nœud moteur d'AX dans un serveur.

Ajouter un Nœud moteur d'AX

1. Connectez-vous à l'application Web Configuration d'AX Serveur et localisez le panneau **Nœuds moteur**.
2. Dans le panneau **Ajouter un nœud moteur**, entrez les informations suivantes :
 - **Adresse IP ou nom de l'ordinateur du nouveau Nœud moteur** : le nom d'hôte ou l'adresse IP du serveur où le Nœud moteur d'AX est installé
 - **Tâches (max.)**: nombre maximum de tâches analytiques que le nœud moteur peut traiter en une fois

Remarque

Les tâches sont placées dans une file d'attente jusqu'à ce que le nombre de tâches exécutées simultanément tombent en-dessous du maximum.

3. Cliquez sur **Ajouter un nœud moteur**.
4. Cliquez sur **Mettez à jour les paramètres de Nœud moteur**.

Résultat : le nœud moteur d'AX permet de traiter les outils d'analyse. S'il s'agit du premier nœud moteur d'AX, le transfert s'effectue d'AX Serveur vers le nouveau nœud. Si vous avez ajouté plusieurs nœuds moteur d'AX, les tâches planifiées se répartissent entre eux.

Configurer des nœuds moteur d'AX

Depuis le panneau **Nœuds moteur** de l'application Web Configuration d'AX Serveur, vous pouvez éditer les paramètres de configuration de n'importe quel nœud moteur d'AX que vous avez ajouté.

Lorsque vous modifiez une valeur, cliquez sur **Mettre à jour** afin de sauvegarder la modification.

Paramètres individuels du nœud moteur AX

- Activer/Désactiver un nœud moteur
- Modifier le nom d'hôte ou l'adresse IP
- Modifier les tâches max
- Supprimer un nœud moteur

Paramètres globaux du nœud moteur AX

Remarque

Ces paramètres s'appliquent à toutes les instances du nœud moteur d'AX et à tous les outils d'analyse qui s'exécutent sur le(s) serveur(s).

Vous pouvez copier des fichiers de données vers chaque instance de nœud moteur d'AX avant le traitement des outils d'analyse via le paramètre **Copier les données analytiques vers le nœud moteur** :

- Oui** : les fichiers de données provenant du dossier de l'outil d'analyse d'AX Serveur sont copiés vers le répertoire de la tâche analytique du nœud moteur d'AX avant le début du traitement.
- Non** : les fichiers de données restent dans le dossier de l'outil d'analyse du noeud moteur d'AX et ne sont pas copiés vers le répertoire de la tâche nœud moteur d'AX avant le début du traitement.

Copier les fichiers de données	Ne pas copier les fichiers de données
Améliore les performances en cas d'accès répété aux fichiers de données dans le réseau	Améliore les performances en cas d'exécution simultanée d'un petit nombre d'outils d'analyse
Améliore les performances en cas d'exécution simultanée de plusieurs outils d'analyse ou si un seul outil d'analyse exécute plusieurs commandes dans des fichiers de données volumineux.	<p>Améliore les performances lorsque la durée nécessaire pour copier les fichiers de données dépasse le temps gagné lors de l'écriture de vos analyses de données afin de permettre le plus rapidement possible l'exécution en local des commandes de l'outil d'analyse dans le nœud moteur d'AX.</p> <p>Par exemple :</p> <ol style="list-style-type: none"> Rédigez une commande pour ne sélectionner que les enregistrements requis dans la table que le script a ouvert à distance. Utilisez la commande EXTRACT avec le paramètre LOCAL indiqué pour extraire les enregistrements dans la nouvelle table de l'instance du nœud moteur d'AX. Exécutez d'autres commandes dans la table locale.

Certificats de sécurité

Toute installation d'Analytics Exchange exige des certificats de sécurité SSL. Un certificat de sécurité auto-signé s'installe par défaut. Cependant, vous devez remplacer ce certificat par défaut par un certificat émis par une *autorité de certification tierce* (AC).

Fonctionnement

Les certificats SSL permettent d'établir une connexion cryptées, sécurisée, fiable entre des applications clientes et AX Serveur.

Les certificats auto-signés et ceux émis par CA permettent de garantir la difficulté pour un tiers d'accéder aux données transférées entre le serveur AX et les applications client. Cependant lorsque vous achetez un certificat CA, vous bénéficiez d'une confiance supplémentaire puisqu'une autorité de certification indépendante et fiable valide l'authenticité du serveur.

Utilisation de certificats auto-signés pour AX Serveur

Si vous choisissez d'utiliser le certificat auto-signé, chaque utilisateur ayant accès au serveur accède à une page d'avertissement indiquant que le certificat de sécurité n'a pas été émis par une autorité de certification fiable. Pour arrêter cet avertissement, chaque utilisateur client doit vérifier que le certificat est émis par une source fiable en suivant la procédure suivante :

- Installez le certificat auto-signé dans l'explorateur au moment de la connexion avec Client Web d'AX.
- Sélectionnez **Faire confiance aux certificats auto-signés** pendant l'installation ou dans le menu **Outils** dans AX Client.

Astuce

L'installation du certificat n'est généralement pas requise si vous remplacez le certificat auto-signé par un certificat acheté auprès d'une AC, car Internet Explorer prend automatiquement en charge les certificats émis par la plupart des AC. L'utilisation d'un certificat AC peut donc optimiser l'interaction de l'utilisateur final avec le serveur.

Remplacement du certificat

Pour remplacer le certificat auto-signé, vous devez créer un magasin de clés, importer le certificat puis configurer le serveur d'applications TomEE pour utiliser le certificat. Pour plus d'informations, consultez la section "Installer des certificats de sécurité pour le serveur AX" Page 54.

Remarque

Si la valeur *Nom Commun* (CN) indiquée dans les certificats de sécurité change lorsque vous remplacez le certificat auto-signé, vous devez modifier la propriété `cas.-securityContext.casserverHost` dans le fichier de configuration `ac1CasClient.xml` afin que la valeur CN mise à jour corresponde dans chaque serveur où les composants du serveur Analytics Exchange sont installés.

Si vous avez utilisé l'authentification Windows intégrée et que la valeur CN change, vous devez également mettre à jour les paramètres Internet Explorer sur chaque ordinateur client. Pour plus d'informations, consultez la section "Configurer l'authentification Windows intégrée" Page 80.

Certificats du Nœud moteur d'AX

Le certificat configuré dans chaque Nœud moteur d'AX permet de crypter les communications entre le Nœud moteur d'AX et la base de données Analytics Exchange.

Le certificat auto-signé peut être remplacé par un certificat acheté auprès d'une AC, mais étant donné que les utilisateurs finaux n'ont pas accès au Nœud moteur d'AX, le remplacement du certificat n'est généralement pas nécessaire.

Connexions PostgreSQL

Le certificat configuré pour PostgreSQL permet de crypter les communications entre le serveur de bases de données et les serveurs Analytics Exchange qui se connectent à la base de données :

- Serveur AX
- Nœud moteur d'AX
- AX Exception

Quand utiliser SSL pour les connexions aux bases de données

Le certificat est seulement utilisé si les applications se connectant à la base de données ont activé SSL. En raison du coût en termes de performance qui est associé à SSL, ce dernier doit être désactivé s'il n'est pas nécessaire. Par exemple, si AX Serveur et PostgreSQL sont installés sur le même ordinateur, SSL doit être désactivé pour les composants installés sur AX Serveur.

Remplacement du certificat

Le certificat de sécurité créé par l'assistant d'installation PostgreSQL au cours de l'installation est un certificat auto-signé. Le certificat serveur doit être en place pour que les connexions SSL fonctionnent, mais les informations spécifiques du certificat, comme le nom du serveur, ne sont pas validées. C'est

pourquoi il n'est généralement pas nécessaire de remplacer le certificat auto-signé installé par un certificat émis par une AC.

Connexions du Connecteur ACL pour Analytics Exchange

Le Connecteur ACL pour Analytics Exchange ne demande pas de connexion SSL, cependant il prend en charge le chiffrement SSL si vous décidez de l'activer.

Le connecteur repose sur une technologie et des protocoles différents de ceux d'AX Serveur, il n'utilise donc pas la même configuration de certificat de sécurité ou le même set d'outils que celui requis au moment du chiffrage de l'autre communication d'AX serveur.

Pour prendre en charge le chiffrement SSL, vous devez générer et installer un ensemble de certificats de sécurité sur la machine AX Serveur via OpenSSL. Si SSL est activé, le connecteur utilise OpenSSL pour chiffrer toutes les données qui se déplacent dans les connexions réseau.

Pour plus d'informations, consultez la section "Installer les certificats de sécurité pour le connecteur ACL pour Analytics Exchange" Page 59.

Installer des certificats de sécurité pour le serveur AX

Installez un certificat provenant d'une *autorité de certification* (AC) pour remplacer le certificat auto-signé par défaut utilisé pour sécurisé la connexion SSL entre AX Serveur et les applications clientes.

Outils et connaissances pré-requises

Cette tâche exige que vous utilisez l'utilitaire keytool d'Oracle pour gérer les clés et les certificats. Pour plus d'informations sur l'utilitaire keytool d'Oracle, consultez la [documentation dur keytool d'Oracle](#).

Pour exécuter cette tâche correctement, vous devez maîtriser l'utilisation des *certificats de sécurité* et de la technologie de *magasin de clés Java* :

- **Certificat de sécurité** : document électronique qui permet de prouver la propriété d'une clé publique. Le certificat comprend des informations sur la clé, des informations sur l'identité du propriétaire ainsi que la signature numérique d'une entité qui a vérifié l'exactitude des contenus du certificat. Pour plus d'informations, consultez la section "Certificats de sécurité" Page 51
- **Magasin de clés Java** : un répertoire contenant les certificats de sécurité et les clés privés correspondantes utilisées pour le chiffrement SSL. Pour plus d'informations, voir la section [Oracle : création d'un magasin de clés](#)

Sauvegardez la configuration du serveur d'application TomEE avant de commencer

1. Dans l'Explorateur Windows, ouvrez le sous-répertoire `TomCat\conf` situé dans le répertoire où vous avez installé le serveur d'application Analytics Exchange dont vous mettez la configuration du magasin de clés à jour.
2. Copiez les fichiers `conf\tomee.xml`, `conf\server.xml`, et `conf\system.properties` vers un emplacement de sauvegarde sécurisé.

Si vous rencontrez des problèmes lors de la configuration du certificat de sécurité, vous pouvez restaurer la configuration d'origine en arrêtant le service d'Analytics Exchange, en restaurant ces fichiers, puis en relançant le service.

Processus côté serveur

Astuce

Ajoutez le sous-répertoire Java `bin` à la variable d'environnement PATH de votre système d'exploitation pour pouvoir utiliser la commande keytool sans indiquer le chemin complet. Pour ajouter le sous-répertoire au chemin dans votre session, exécutez Set PATH=<chemin_java_bin>;%PATH%.

Si vous utilisez un fichier de certificat PFX, vous pouvez le convertir en magasin de clés avec une clé privée à l'aide d'une commande keytool :

```
keytool -importkeystore -srckeystore yourpfxfile.pfx -srcstoretype pkcs12 -destkeystore
cientcert.jks -deststoretype JKS
```

Créez un nouveau magasin de clés.

- Ouvrez une invite de commande sur le serveur.
- Utilisez la syntaxe suivante pour créer le nouveau magasin de clés :

```
keytool -genkeypair -alias <alias> -keyalg RSA -keystore <nomfichier_magasinclés>
```

Exemple : keytool -genkeypair -alias AX_store -keyalg RSA -keystore myAxKeystore

- Répondez à chacune des questions lorsque vous y êtes invité :

Champ	Exemple
Quel est votre nom et prénom ?	axserver.ax.com
Remarque Vous devez entrer le nom d'hôte de votre instance AX Serveur pour cette question.	
Quel est le nom de votre unité organisationnelle ?	Achats
Quel est le nom de votre organisation ?	ExempleSociété
Quel est le nom de votre ville ou localité ?	Cupertino
Quel est le nom de votre état ou de votre région ?	CA
Quel est le code pays à deux lettres de cette unité ?	US
Est-ce que <CN=axserver.ax.com, OU=Purchasing, O=ExampleCompany, L=Cupertino, ST=CA, C=US> est correct ?	y

Appuyez sur Entrée pour utiliser le même mot de passe que le magasin de clés ou indiquez-en un nouveau et appuyez sur Entrée.

Générez une demande de signature de certificat (CSR) dans le nouveau magasin de clés

Remarque

Ignorez cette section si vous utilisez un certificat existant.

Si vous avez acheté votre certificat de sécurité à une AC commerciale, telles que VeriSign, consultez la documentation fournie pour obtenir des informations sur la configuration de votre magasin de clés. Créez un CSR en appliquant la syntaxe suivante :

```
keytool -certreq -alias <alias> -keyalg RSA -file <fichier_sortie_csr> -keystore <nom_fichier_magasin_clés>
```

Résultat : Vous disposez désormais d'un fichier que vous pouvez utiliser pour demander un certificat auprès d'une autorité de certification.

Importez votre certificat CA dans le magasin de clés

Si votre certificat est dans un format de type PKCS12 qui ne peut pas être importé dans un magasin de clés et que vous ne pouvez pas le convertir au format PEM, contactez l'Assistance ACL pour obtenir de l'aide sur la configuration du certificat dans Tomcat.

1. En fonction de l'autorité de certification que vous utilisez, vous devrez peut-être importer un certificat intermédiaire ou un certificat racine dans votre magasin de clés. Utilisez la syntaxe suivante pour importer un ou l'ensemble de ces certificats :

```
keytool -import -alias <alias> -keystore <nom_fichier_magasin_clés> -trustcacerts -file <nom_fichier_certificat>
```

Si vous importez les deux certificats, l'*alias* indiqué pour chaque certificat doit être unique. Vous devez d'abord importer le certificat racine, puis relancer la commande keytool pour importer le certificat intermédiaire.

2. Utilisez la syntaxe suivante pour importer votre certificat de sécurité :

```
keytool -import -alias <alias> -keystore <nom_fichier_magasin_clés> -trustcacerts -file <nom_fichier_certificat>
```

L'*alias* indiqué doit avoir la même valeur que celle indiquée lorsque vous avez généré le magasin de clés. Le certificat importé remplacera le certificat auto-signé par défaut créé dans le magasin de clés.

3. Copiez le fichier du magasin de clés dans le sous-dossier [App\keystores](#).

Configurer le serveur d'application TomEE à utiliser pour le certificat

1. Localisez `server.xml` dans le sous-dossier `TomCat\conf` et ouvrez-le dans un éditeur de texte.
2. Mettez à jour les paramètres suivants, puis enregistrez et fermez `server.xml` :
 - `keystoreFile` : le nom et le chemin d'accès du fichier de magasin de clés que vous avez créé au format suivant : `C:\ACL\App\keystores\<votre_nom_magasin_clés>`
 - `keystorePass` : le mot de passe que vous avez spécifié pour le magasin de clés à sa création. Le mot de passe doit être entouré de guillemets doubles (" ") .
3. Localisez `system.properties` dans le sous-dossier `TomCat\conf` et ouvrez-le dans un éditeur de texte.
4. Mettez à jour les paramètres suivants, puis enregistrez et fermez `system.properties` :
 - `javax.net.ssl.trustStore` : le nom et le chemin d'accès du fichier de magasin de clés que vous avez créé au format suivant : `C:/ACL/App/keystores/<votre_nom_magasin_clés>`

Remarque

Vous devez utiliser le caractère barre oblique « / » dans le chemin du magasin de clés. Si vous utilisez le caractère barre oblique inverse « \ » comme on le trouve fréquemment dans les environnements Windows, vous rencontrerez des erreurs de serveur à la connexion.

- `javax.net.ssl.trustStorePassword` : le mot de passe que vous avez spécifié pour le magasin de clés à sa création
5. Redémarrez le service Analytics Exchange.

Processus côté client

Importer des certificats dans le fichier Java cacerts de la machine d'AX Client

Vous devez effectuer cette configuration dans chaque ordinateur d'utilisateur final sur lequel AX Client est installé si vous utilisez un certificat sans certificat racine dans le fichier `cacerts` par défaut.

1. Ouvrez l'explorateur Windows et naviguez jusqu'au fichier `cacerts` dans le sous-dossier `jre\lib\security` où AX Client est installé.

L'emplacement par défaut est `C:\Program Files (x86)\ACL Software\ACL Analytics Exchange\jre\lib\security`

2. Créez une copie du fichier avant de faire des modifications.
3. En fonction des certificats reçus par les autorités de certification que vous utilisez, vous aurez peut-être besoin d'importer un certificat intermédiaire ou un certificat racine dans le fichier `cacerts`. Utilisez la syntaxe suivante pour importer un ou l'ensemble de ces certificats :

```
keytool -import -alias <alias> -keystore <fichier_cacerts> -trustcacerts -file <nom_fichier_certificat>
```

Si vous importez les deux certificats, l'`alias` indiqué pour chaque certificat doit être unique.

4. Lorsque l'invite **Mot de passe** s'affiche, saisissez le mot de passe du magasin de clés et appuyez sur **Entrée**.

Le mot de passe Java par défaut pour le fichier `cacerts` est `changeit`.

5. À l'invite **Faites-vous confiance à ce certificat ?**, saisissez **o** et appuyez sur **Entrée**.

Si nécessaire, installez le certificat dans le navigateur Web de chaque ordinateur ayant accès aux applications Web d'Analytics Exchange.

Remarque

Cela n'est pas nécessaire si le certificat est fourni par une AC figurant dans la liste des autorités de certification racines fiables dans Internet Explorer. Les grandes AC commerciales, comme VeriSign, font partie de cette liste.

Installer les certificats de sécurité pour le connecteur ACL pour Analytics Exchange

Le connecteur ACL pour Analytics Exchange prend en charge le chiffrement SSL (Secure Sockets Layer) au niveau des connexions entre les machines client et le serveur AX. Si SSL est activé, le connecteur utilise OpenSSL pour chiffrer toutes les données qui se déplacent dans les connexions réseau entre les machines client et le serveur.

Pour configurer SSL via des certificats, vous devez générer un ensemble de certificats SSL sur la machine du serveur. Vous pouvez générer un des types de certificat suivant pour la connexion SSL :

- Certificat auto-signé
- Certificat d'une autorité de certification (CA)

Avant de commencer

Téléchargez et installez OpenSSL puis ajoutez le chemin d'accès de l'exécutable `openssl.exe` à votre environnement d'environnement PATH.

Remarque

Comme de nombreux projets de logiciel source, le projet OpenSSL ne distribue pas de code sous une forme binaire. Au contraire, vous devez télécharger le code source du projet et créer le binaire ou localiser un binaire qui est distribué dans votre système d'exploitation depuis une source tierce.

Pour plus d'informations, consultez la [documentation OpenSSL](#).

Générer un certificat SSL pour l'auto-signature

OpenSSL permet de générer un fichier clé et un fichier de certificat dans la machine serveur. Les certificats auto-signés s'avèrent utiles pendant la phase de développement ou de test, lorsque vous n'avez pas à acheter de certificat commercial.

En savoir plus

1. Ouvrez une invite de commande puis créez le répertoire `C:\newcerts`.

```
md C:\newcerts
```

2. Passez au nouveau répertoire et générez un fichier clé de serveur et un fichier de certificat du serveur.

```
cd C:\newcerts  
openssl req -x509 -newkey rsa:4096 -keyout server-key.pem -out server-cert.pem -days 365 -nodes
```

Le système vous invite à saisir des informations qui figurent dans le certificat comme le pays, la ville, le nom de la société, etc. Relevez les informations que vous saisissez car le système peut vous demander de les saisir à nouveau ultérieurement.

Remarque

L'argument `-nodes` supprime la protection de mot de passe pour la clé privée afin que vous n'ayez pas à saisir un mot de passe lorsque vous redémarrez le serveur.

Résultat : le certificat auto-signé est créé. Vous avez besoin de `server-key.pem` et `server-cert.pem` pendant l'installation du connecteur ACL pour Analytics Exchange sur la machine d'AX serveur. Les utilisateurs du client n'ont pas besoin d'un fichier de certificat lorsque vous utilisez cette option.

Génération d'un certificat SSL avec une autorité de certification (CA)

Comme les certificats auto-signés, les certificats d'une autorité de certification (CA) garantissent qu'aucun tiers ne peut accéder facilement à la connexion. Cependant, les certificats CA offrent une confiance supplémentaire car une autorité de certification indépendante et fiable valide l'authenticité du serveur.

En savoir plus

Créez la clé privée du serveur

1. Ouvrez une invite de commande puis créez le répertoire `C:\newcerts`.

```
md C:\newcerts
```

2. Modifiez le nouveau répertoire et générez une nouvelle clé.

```
cd C:\newcerts  
openssl genrsa -out server-key-withPass.pem
```

3. Générez une demande de signature de certificat.

```
openssl req -new -key server-key-withPass.pem -out signingReq.csr
```

Le système vous invite à saisir des informations qui sont intégrées au certificat, comme le pays, la ville, le nom de l'entreprise, etc. Relevez les informations que vous saisissez car le système peut vous demander de les saisir à nouveau ultérieurement. Lorsque vous devez saisir une adresse e-mail, fournissez une adresse valide afin que l'autorité de certification puisse envoyer le certificat via cette adresse.

- Vérifiez les informations dans le fichier `signingReq.csr` puis envoyez le fichier à l'autorité de certification sous forme de demande.

Résultat : Si la demande est correcte, l'autorité de certification vous envoie un certificat via l'adresse e-mail que vous avez indiqué dans la demande de signature. L'e-mail que vous recevez comprend un certificat CA chiffré et un lien vers un certificat intermédiaire CA chiffré.

Copiez les deux certificats vers un fichier texte, avec un certificat non-intermédiaire suivi d'un certificat intermédiaire puis enregistrez le fichier en tant que `CA-cert.pem`. Ce fichier est nécessaire pour la section suivante.

Créez et signez le certificat de serveur

- Regroupez les fichiers qui ont été générés dans la section précédente et copiez les trois fichiers dans `C:\newcerts` :
 - `server-key-withPass.pem`
 - `signingReq.csr`
 - `CA-cert.pem`
- Ouvrez une invite de commande et modifiez `C:\newcerts`:

```
cd C:\newcerts
```

- Créez le certificat de serveur :

```
openssl CA -in signingReq.csr -out server-cert.pem -keyfile server-key-withPass.pem -days 365  
-cert CA-cert.pem
```

- Supprimez le mot de passe de `server-key-withPass.pem` afin de ne pas avoir à saisir un mot de passe lorsque vous redémarrez le serveur, et générez le fichier clé de serveur final (`server-key.pem`).

```
openssl rsa -in server-key-withPass.pem -out server-key.pem
```

Avertissement

Une fois que vous avez supprimé l'obligation de mot de passe, vous pouvez copier et utiliser le certificat ailleurs. Cependant, lorsque vous supprimez le mot de passe, vous devez prendre les mesures correspondantes lorsque vous stockez le fichier. Assurez-vous que les autorisations sont définies afin de n'autoriser l'accès qu'aux personnes qui en ont besoin.

Résultat : Le certificat de serveur est créé et signé.

Répartition des certificats SSL

Une fois que vous avez généré un certificat CA ou auto-signé, vous avez un ensemble complet de certificats SSL que vous pouvez distribuez :

- **le fichier CA-cert.pem** : demandé par un client pour se connecter au Connecteur ACL pour Analytics Exchange sur SSL via un certificat d'autorité de certification ;
- **le fichier clé de serveur (server-key.pem) et le fichier de certificat de serveur (server-cert.pem)** : nécessaire lorsque vous exécutez l'installateur Connecteur ACL pour Analytics Exchange sur AX Server si vous voulez activer SSL.

Annexe

Cette annexe contient des rubriques supplémentaires pouvant être utiles pour réaliser les procédures de ce document.

Conditions requises pour AX Serveur

Pour bénéficier des performances optimales d'AX Serveur, assurez-vous que le matériel et le logiciel sont conformes à la configuration minimale requise. Il est possible que des ressources supérieures à la configuration minimale soient nécessaires afin de fournir des performances satisfaisantes pour l'environnement de production.

Matériel

Les exigences en matière de processeur, de mémoire et de disque dur pour les systèmes de production dépendent des facteurs suivants :

- le nombre d'utilisateurs simultanés et leurs profils d'utilisation
- la taille de la charge utile des données
- le temps de réponse désiré

Composant	Minimum	Recommandation
Processeur	2,5 gigahertz (GHz)	Processeur quad-core (ou 2 processeurs dual-core) de 3,5 GHz ou supérieur.
Mémoire (RAM)	8 Go	16 Go ou plus
Disque dur	100 Go Il s'agit de l'espace disque disponible approximativement requis pour télécharger, extraire et installer les logiciels prérequis. (AX Serveur fait 4,5 Go)	200 - 500 Go Les exigences concernant le stockage des données varient selon le nombre de types de tests d'audit réalisés et le volume des transactions. Les mises en œuvre de petite ampleur requièrent généralement 50 Go par an alors que les mises en œuvre de plus grande envergure peuvent exiger un maximum de 500 Go par an. Pour une utilisation en production, il est recommandé de disposer d'un accès au disque et d'une capacité à vitesse élevée.
Autre	Connectivité TCP/IP. Il est nécessaire de pouvoir se connecter à la Barre de lancement pendant l'activation du serveur en ligne.	

Logiciel

Attention

Vous devez installer les mises à niveau Windows [KB2919355](#) avant de démarrer l'installation d'Analytics Exchange sur Windows Server 2012 R2. En cas de non installation de cette mise à niveau, l'installation d'Analytics Exchange sera défaillante.

Configuration logicielle requise	Minimum	Recommandation
Système d'exploitation		
<ul style="list-style-type: none"> ○ Windows Server 2016 ○ Windows Server 2012 R2 ○ Windows Server 2008 R2 Enterprise Edition (64 bits) <p>Remarque Appliquez toutes les mises à jour Windows critiques avant d'installer AX Serveur. L'exécution de Windows Server à l'aide de l'option Server Core (et non GUI) n'est pas prise en charge.</p>	Windows Server 2008 R2 Enterprise Edition (64 bits)	Windows Server 2016
Navigateur Web		
<ul style="list-style-type: none"> ○ Chrome ○ Firefox ○ Internet Explorer 	Internet Explorer version 11	Dernière version de Chrome
Langages de programmation intégrés disponibles en option		
Langage de programmation Python Lors de l'installation de Python, vous devez également le configurer pour l'exécuter sur votre système. <p>Remarque Vous devez installer les logiciels préalables requis pour utiliser les fonctions Python intégrées dans vos outils d'analyse. Si vous n'avez pas l'intention d'utiliser ce langage, vous n'avez pas besoin de les installer.</p>	Python 3.3.x (32 bits)	Python 3.5.x (32-bits) La version 3.5.x est entièrement testée et prise en charge. Vous pouvez utiliser une version différente comme 3.3.x ou 3.6.x, toutefois, ces versions n'offrent pas la même garantie de test et de prise en charge que la version 3.5.x.

Configuration logicielle requise	Minimum	Recommandation
<p>Langage de rédaction de scripts R En fonction des packages R CRAN que vous avez l'intention d'utiliser, vous pouvez avoir besoin d'ajouter le répertoire binaire R 1386 32-bits dans votre variable d'environnement PATH.</p> <p>Remarque Vous devez installer les logiciels préalables requis pour utiliser les fonctions R intégrées dans vos outils d'analyse. Si vous n'avez pas l'intention d'utiliser ce langage, vous n'avez pas besoin de les installer.</p>	R 3.3.1 (32 ou 64 bits en fonction du système d'exploitation)	R 3.2.3 ou 3.2.5 (32 ou 64 bits en fonction du système d'exploitation)
<p>Pour utiliser le connecteur ACL pour Oracle, vous devez installer :</p> <ul style="list-style-type: none"> ◦ Oracle Instant Client 11g ou 12c 	<ul style="list-style-type: none"> ◦ Vous n'avez pas besoin d'installer Oracle Instant Client si vous n'avez pas l'intention d'utiliser le Connecteur ACL pour Oracle ◦ Le nombre de bits d'Oracle Instant Client doit correspondre au nombre de bits de votre système d'exploitation. Si Oracle Instant Client 32 bits est installé sur une machine de 64 bits, la connexion échoue ◦ Si vous installez Oracle Instant Client après AX Serveur, vous devez relancer le service Analytics Exchange avant de pouvoir utiliser le connecteur ◦ Si vous utilisez Oracle comme serveur de base de données pour AX Serveur, vous devez aussi installer Instant Client sur la machine hébergeant le serveur de base de données, consultez la rubrique "Serveur de bases de données" Page 68 	SO

Logiciels prérequis automatiquement installés

Les logiciels prérequis suivants sont installés automatiquement par l'assistant d'installation d'AX Serveur si le logiciel requis n'est pas détecté :

- Environnement d'exécution Oracle Java 8 (JRE 8u181)
- Apache TomEE 7.0.5 (Tomcat version 8.5.32)
- Java Cryptography Extension pour Java 8
- Moteur de base de données Microsoft Access 2016
- Microsoft .NET Framework 4.6.2

Remarque

Si votre ordinateur a déjà .NET 4.6.0 ou NET 4.6.1, l'application utilise la version installée de .NET et n'installe pas la version 4.6.2.

- Redistribuable Microsoft Visual C++ 2005 (x64 et x86)
- MSXML SDK 2.5

Connecteurs de données ACL

Les pilotes ODBC répertoriés ci-après sont installés afin d'être utilisés en tant que connecteurs de données ACL :

Nom du pilote			
Connecteur ACL pour Active Directory	Connecteur ACL pour Spark	Connecteur ACL pour Jira	Connecteur ACL pour Open Exchange Rates
Connecteur ACL pour DynamoDB	Connecteur ACL pour Impala	Connecteur ACL pour JSON	Connecteur ACL pour Oracle
Connecteur ACL pour Amazon Redshift	Connecteur ACL pour Concur	Connecteur ACL pour LDAP	Connecteur ACL pour Salesforce
Connecteur ACL pour Cassandra	Connecteur ACL pour Couchbase	Connecteur ACL pour Marketo	Connecteur ACL pour SAP
Connecteur ACL pour Drill	Connecteur ACL pour Email	Connecteur ACL pour SQL Server	Connecteur ACL pour ServiceNow
Connecteur ACL pour HBase	Connecteur ACL pour Exchange	Connecteur ACL pour MongoDB	Connecteur ACL pour TeraData
Connecteur ACL pour Hive	Connecteur ACL pour Google BigQuery	Connecteur ACL pour MySQL	Connecteur ACL pour Twitter

Logiciels pré-requis inclus dans Windows server

Les logiciels prérequis suivants sont inclus dans une installation de serveur Windows par défaut : Les versions indiquées sont les versions minimales requises et la plupart des installations de systèmes d'exploitation incluent des versions ultérieures :

- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Jet 4.0

Serveur de bases de données

AX Serveur prend en charge deux plates-formes de bases de données, Oracle et PostgreSQL.

Si votre organisation implémente AX Serveur et AX Exception, les configurations prises en charge sont :

- les deux applications de base de données qui utilisent Oracle ;
- la configuration d'AX Serveur pour utiliser PostgreSQL comme base de données et Microsoft SQL Server comme la base de données AX Exception

Configuration logicielle requise	Minimum	Recommandation
<p>Une de ces versions d'Oracle si Oracle est choisi comme plate-forme de base de données Analytics Exchange :</p> <ul style="list-style-type: none"> ◦ Oracle 12c ◦ Oracle 11gR2 ◦ Oracle 18c <p>Remarque</p> <p>Le serveur Oracle sur lequel le logiciel est installé doit répondre aux exigences matérielles requises spécifiées par le fournisseur de bases de données. Vous devez également installer Oracle Instant Client correspondant à la version de votre base de données si vous prévoyez d'utiliser un accès direct à la base de données du connecteur AX.</p> <p>Les bases de données Oracle s'exécutant sur Amazon RDS sont prises en charge.</p>	Oracle 11gR2	Oracle 18c
PostgreSQL 9.6 si PostgreSQL est choisi comme plate-forme de bases de données Analytics Exchange.	PostgreSQL 9.6	PostgreSQL 9.6

Configuration logicielle requise	Minimum	Recommandation
<p>Remarque</p> <p>Si PostgreSQL est installé sur le même serveur qu'AX Serveur, il suffit de respecter les exigences matérielles requises pour AX Serveur.</p> <p>Si PostgreSQL est installé sur un serveur distinct, il est recommandé de disposer d'un processeur dual 64 bits, d'un système d'exploitation 64 bits et 2 Go de mémoire pour une utilisation en production.</p>		

Conditions requises pour Nœud moteur d'AX

Pour bénéficier des performances optimales du moteur AX, assurez-vous que le matériel et le logiciel sont conformes à la configuration minimale requise. Il est possible que des ressources supérieures à la configuration minimale soient nécessaires afin de fournir des performances satisfaisantes pour l'environnement de production.

Matériel

Les exigences en matière de processeur, de mémoire et de disque dur pour les systèmes de production dépendent des facteurs suivants :

- le nombre d'utilisateurs simultanés et leurs profils d'utilisation
- la taille de la charge utile des données
- le temps de réponse désiré

Composant	Minimum	Recommandation
Mémoire (RAM)	8 Go	16 Go ou plus
Disque dur	3,5 gigaoctets (Go) Il s'agit d'une estimation de l'espace disque disponible requis pour télécharger, extraire et installer les logiciels prérequis et Nœud moteur d'AX.	10 Go ou plus Pour une utilisation en production, il est recommandé de disposer d'un accès au disque et d'une capacité à vitesse élevée.
Autre	Connectivité réseau à AX Serveur.	

Logiciel

Configuration logicielle requise	Minimum	Recommandation
<ul style="list-style-type: none"> ◦ Windows Server 2016 ◦ Windows Server 2012 R2 ◦ Windows Server 2008 R2 Enterprise Edition (64 bits) 	Windows Server 2008 Enterprise Edition R2 (64 bits)	Windows Server 2016

Configuration logicielle requise	Minimum	Recommandation
<p>Remarque</p> <p>Vous devez installer la mise à jour Windows Server 2012 R2 (KB2919355) comme prérequis à l'installation du Framework .NET.</p> <p>Appliquez toutes les mises à jour Windows critiques avant d'installer AX Serveur. L'exécution de Windows Server 2012 à l'aide de l'option Server Core (et non GUI) n'est pas prise en charge.</p>		
Langages de programmation intégrés disponibles en option		
<ul style="list-style-type: none"> ◦ Langage de programmation Python ◦ Langage de rédaction de scripts R <p>Lors de l'installation de Python, vous devez également le configurer pour l'exécuter sur votre système. Pour plus d'informations, consultez la section "Configuration de Python pour être utilisé avec AX Serveur" Page 37.</p> <p>En fonction des packages R CRAN que vous avez l'intention d'utiliser, vous pouvez avoir besoin d'ajouter le répertoire binaire R i386 32-bits dans votre variable d'environnement PATH.</p> <p>Remarque</p> <p>Vous devez respecter les recommandations d'installation pour utiliser les fonctions de Python ou de R dans vos outils d'analyse. Si vous n'avez pas l'intention d'utiliser ces langages, vous n'avez pas besoin de les installer.</p>	<ul style="list-style-type: none"> ◦ Python 3.5.x (32-bits) ◦ R 3.3.1 (32-bits) 	<ul style="list-style-type: none"> ◦ Python 3.5.x (32-bits) ◦ R 3.2.3 ou 3.2.5 (32-bits)
Pour utiliser le connecteur ACL pour Oracle, vous devez installer :	<ul style="list-style-type: none"> ◦ Oracle Instant Client 11g 12c 	<ul style="list-style-type: none"> ◦ Vous n'avez pas besoin d'installer Oracle Instant Client si vous n'avez pas l'intention d'utiliser le Connecteur ACL pour Oracle ◦ Le nombre de bits d'Oracle Instant Client doit correspondre au nombre de bits de votre système d'exploitation. Si Oracle Instant Client 32 bits est installé sur une machine de 64 bits, la connexion échoue ◦ Si vous installez Oracle Instant Client après le Nœud moteur d'AX, vous devez relancer le service Analytics Exchange avant de pouvoir
		SO

Configuration logicielle requise	Minimum	Recommandation
	<ul style="list-style-type: none"> utiliser le connecteur o Si vous utilisez Oracle comme serveur de base de données pour AX Serveur, vous devez aussi installer Instant Client sur la machine hébergeant le serveur de base de données, consultez la rubrique "Serveur de bases de données" Page 68 	

Logiciels prérequis automatiquement installés

Les logiciels prérequis suivants sont installés automatiquement par l'assistant d'installation d'AX Serveur si le logiciel requis n'est pas détecté :

- Environnement d'exécution Oracle Java 8 (JRE 8u181)
- Apache TomEE 7.0.5 (Tomcat version 8.5.32)
- Java Cryptography Extension pour Java 8
- Moteur de base de données Microsoft Access 2016
- Microsoft .NET Framework 4.6.2

Remarque

Si votre ordinateur a déjà .NET 4.6.0 ou .NET 4.6.1, l'application utilise la version installée de .NET et n'installe pas la version 4.6.2.

- Redistribuable Microsoft Visual C++ 2005 (x64 et x86)
- MSXML SDK 2.5

Connecteurs de données ACL

Les pilotes ODBC répertoriés ci-après sont installés afin d'être utilisés en tant que connecteurs de données ACL :

Nom du pilote			
Connecteur ACL pour Active Directory	Connecteur ACL pour Spark	Connecteur ACL pour Jira	Connecteur ACL pour Open Exchange Rates
Connecteur ACL pour DynamoDB	Connecteur ACL pour Impala	Connecteur ACL pour JSON	Connecteur ACL pour Oracle
Connecteur ACL pour Amazon Redshift	Connecteur ACL pour Concur	Connecteur ACL pour LDAP	Connecteur ACL pour Salesforce
Connecteur ACL pour Cassandra	Connecteur ACL pour Couchbase	Connecteur ACL pour Marketo	Connecteur ACL pour SAP

Nom du pilote			
Connecteur ACL pour Drill	Connecteur ACL pour Email	Connecteur ACL pour SQL Server	Connecteur ACL pour ServiceNow
Connecteur ACL pour HBase	Connecteur ACL pour Exchange	Connecteur ACL pour MongoDB	Connecteur ACL pour Tera-data
Connecteur ACL pour Hive	Connecteur ACL pour Google BigQuery	Connecteur ACL pour MySQL	Connecteur ACL pour Twitter

Logiciels pré-requis inclus dans Windows server

Les logiciels prérequis suivants sont inclus dans une installation de serveur Windows par défaut : Les versions indiquées sont les versions minimales requises et la plupart des installations de systèmes d'exploitation incluent des versions ultérieures :

- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Jet 4.0

Configuration du compte de service

AX Serveur utilise trois services Windows pour effectuer la plupart des fonctions de l'application sur le serveur : service Analytics Exchange, connecteur Analytics Exchange et base de données Analytics Exchange.

Noms de service

Afficher le nom du service	Nom du service
Service Analytics Exchange	TomEE
Connecteur Analytics Exchange	AXConnector
Base de données Analytics Exchange (Installations AX Serveur qui utilisent uniquement une base de données PostgreSQL)	ACL_AXDatabase

Service Analytics Exchange

Le service Analytics Exchange est installé sur AX Serveur et sur chaque Nœud moteur d'AX que vous configurez.

Compte utilisateur du service Analytics Exchange

Pour affecter un compte utilisateur afin d'exécuter le service Analytics Exchange, vous devez effectuer l'une des actions suivantes :

- sélectionner un compte de domaine existant
- créer un nouveau compte de domaine

Remarque

L'utilisation d'un compte local n'est pas prise en charge pour l'exécution du service TomEE. Ces comptes ne disposent pas des privilèges appropriés pour exécuter certaines commandes ACL.

Autorisations de répertoire pour le compte du service

Le compte utilisateur que vous choisissez doit disposer d'un accès complet au répertoire [ACL](#).

Si vous indiquez un **Répertoire de données** ou un **Répertoire d'archivage et de restauration des données** en dehors du répertoire **ACL**, vous devez également leur octroyer des autorisations complètes.

Remarque

Le programme d'installation d'AX Serveur attribue les autorisations locales requises sur le serveur pour l'exécution du service. Toutefois, les autorisations doivent être configurées manuellement si le dossier se trouve sur un serveur différent ou si le compte utilisateur ne possède pas les droits pour le dossier spécifié par défaut.

Comptes utilisateur pour plusieurs instances du service Analytics Exchange

Si votre installation contient plusieurs instances du service Analytics Exchange s'exécutant sur différents serveurs, vous devez créer un compte de domaine ayant les droits requis pour l'exécution du service et l'accès aux données d'AX Serveur avant de procéder à toute installation.

Au cours de chaque installation, indiquez ce compte pour exécuter le service Analytics Exchange.

Comptes utilisateur pour le servicer Analytics Exchange avec Direct Link

Si l'ordinateur hébergeant AX Serveur ou une instance du Nœud moteur AX a aussi une installation Direct Link, le compte utilisateur doit avoir l'autorisation d'exécuter les exécutables suivants :

- **saplogon.exe**
- **sapgui.exe**

Remarque

Sans l'autorisation d'exécuter ces fichiers exécutables, les outils d'analyse incluant les commandes Direct Link échouent. Vous pouvez affecter des autorisations de contrôle total vers le dossier contenant les exécutables. Par défaut, les exécutables se trouvent à cet emplacement : **C:\Program Files\SAP\FrontEnd\SAPgui**.

Connecteur Analytics Exchange

Le programme d'installation d'AX Serveur configure le service Connecteur Analytics Exchange pour utiliser le compte Système local. Il est recommandé d'utiliser cette configuration par défaut.

Base de données Analytics Exchange

L'Assistant d'installation de PostgreSQL configure le service de base de données Analytics Exchange avec les autorisations locales sur le serveur requis pour exécuter le service.

Pendant l'installation, vous pouvez :

- utiliser un compte utilisateur local existant sur le serveur
- faire créer un nouveau compte utilisateur local par le programme d'installation

- spécifier un compte de domaine

Par défaut, le groupe dont le compte utilisateur PostgreSQL fait partie reçoit un accès au programme qui contrôle la base de données ([pg_ctl.exe](#)). Vous pouvez toutefois limiter l'accès à ce programme au compte spécifique exécutant le service de la base de données uniquement.

Remarque

Vous ne pouvez pas utiliser le compte Système local intégré pour exécuter le service car le serveur de bases de données doit avoir accès aux ressources du réseau, ce que le Système local n'autorise pas.

Le service de base de données Analytics Exchange est installé sur le serveur où PostgreSQL est installé et il n'est présent que si vous utilisez PostgreSQL comme votre serveur de base de données.

Authentification d'Analytics Exchange

L'authentification par formulaire ou l'authentification Windows intégrée permet de valider l'identité de l'utilisateur lorsqu'il se connecte à des applications d'Analytics Exchange.

Types d'authentification

Authentification par formulaire

Pour chaque nouvelle session dans les applications Analytics Exchange Client, les utilisateurs doivent saisir le nom d'utilisateur et le mot de passe dans un formulaire de connexion :

- Client AX
- Client Web d'AX
- AX Exception

Remarque

Une nouvelle session est établie à chaque démarrage d'AX Client ou à chaque accès du Client Web d'AX depuis une nouvelle fenêtre de l'explorateur.

Authentification Windows intégrée

L'authentification de l'application d'Analytics Exchange Client s'effectue de manière silencieuse par le système d'exploitation Windows sans que les utilisateurs aient besoin de saisir des informations d'identification. Au lancement d'une application, il utilise les informations d'identification du compte que l'utilisateur a déjà entrées lorsqu'il s'est connecté au système d'exploitation. Si l'authentification échoue, l'utilisateur est invité à entrer les informations d'identification dans un formulaire de connexion.

Astuce

L'authentification intégrée exige plus de travail de configuration mais elle s'avère au final plus pratique pour les utilisateurs de l'application cliente.

Choisir une méthode d'authentification

Choisissez le type d'authentification que vous utiliserez pendant l'installation d'AX Serveur. Vous pouvez basculer entre les deux options d'authentification à tout moment.

Attribuer des droits au service du Connecteur AX

Si vous ne parvenez pas à ouvrir la table dans ACL Analytics après avoir entré le mot de passe du profil de serveur et avoir confirmé que le profil de serveur est correctement configuré, attribuez des droits pour le service du Connecteur AX sur la machine où AX Serveur est installé :

Ces droits doivent être attribués à chaque utilisateur d'Analytics Exchange. Vous avez la possibilité d'attribuer des droits à des comptes ou des groupes d'utilisateurs individuels.

Affectez un accès en lecture et en écriture au dossier d'installation du Connecteur AX.

1. Ouvrez l'explorateur Windows et accédez au dossier d'installation du Connecteur AX.
L'emplacement par défaut est `C:\ACL\App\analytic_engine\aclse`.
2. Cliquez avec le bouton droit de la souris sur le dossier et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Sécurité**.
4. Ajoutez les comptes utilisateur ou les groupes qui accéderont à AX Serveur et attribuez-leur des autorisations en **lecture** et **écriture** en cochant la case correspondante dans la colonne **Autoriser**.
5. Cliquez sur **OK**.

Attribuez des droits de contrôle complet à l'exécutable du Connecteur AX (`aclse.exe`).

1. Ouvrez l'explorateur Windows et accédez au dossier d'installation du Connecteur AX.
L'emplacement par défaut est `C:\ACL\App\analytic_engine\aclse`.
2. Cliquez avec le bouton droit de la souris sur le fichier `aclse.exe` et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Sécurité**.
4. Ajoutez les comptes ou les groupes utilisateur qui accéderont à AX Serveur et attribuez-leur l'autorisation **Contrôle total** en cochant la case dans la colonne **Autoriser**.
5. Cliquez sur **OK**.

Autorisez les droits de connexion locale

1. Pour ouvrir les paramètres de stratégie de sécurité, effectuez l'une des actions suivantes :
 - Si le serveur ne correspond pas au contrôleur de domaine, sélectionnez **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale.**
 - Si le serveur correspond au contrôleur de domaine, sélectionnez **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité du domaine.**
2. Dans **Paramètres de sécurité**, double-cliquez sur **Stratégies locales > Attribution de droits utilisateur > Autoriser la connexion locale.**
3. Si le serveur est un contrôleur de domaine, assurez-vous que la case **Définir ces paramètres de sécurité** est cochée.
4. Ajoutez les comptes utilisateur ou les groupes qui accèderont à AX Serveur.

Configurer l'authentification Windows intégrée

Configurez le serveur du contrôleur de domaine Active Directory, AX Serveur et l'environnement bureau pour chaque utilisateur final de l'application cliente pour configurer l'authentification Windows intégrée. L'authentification Windows intégrée permet un contrôle d'accès SSO pour les utilisateurs du client AX.

Remarque

L'authentification Windows intégrée n'est pas prise en charge pour les instances du client AX qui s'exécutent sur le système d'exploitation du serveur. Vous devez vous connecter depuis un système d'exploitation client sinon l'application utilise par défaut une authentification par formulaire.

Fonctionnement

L'authentification Windows intégrée utilise les fonctions de sécurité des clients et serveurs Windows. Elle n'invite pas les utilisateurs à saisir un nom d'utilisateur et un mot de passe, et les informations sur l'utilisateur Windows actuel disponibles sur l'ordinateur client sont fournies par l'explorateur Web via un échange de chiffrement. Les protocoles suivants permettent de gérer l'authentification :

- **SPNEGO** : connexions client AX
- **Kerberos** : connexions du profil de serveur à ACL Analytics

Si l'échange d'authentification ne parvient pas au départ à identifier l'utilisateur, l'explorateur Web invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe pour le compte utilisateur Windows.

Créer un compte SPN

Créez un nouveau compte Windows *Nom de service principal (SPN)* dans Active Directory pour mapper le service d'authentification d'AX Serveur à un compte Active Directory.

En savoir plus

1. Dans le serveur de contrôleur du domaine Active Directory, cliquez sur **Démarrer > Tous les programmes > Outils d'administration > Ordinateurs et utilisateurs Active Directory**.
2. Cliquez avec le bouton droit sur l'entrée dans l'arborescence où vous souhaitez créer le nouveau compte SPN et sélectionnez **Nouveau > Utilisateur**.
3. Entrez les informations demandées et cliquez sur **Suivant**.
4. Configurez le mot de passe utilisateur et cliquez sur **Suivant** :
 - a. Entrez le mot de passe du compte.
 - b. Décochez **L'utilisateur doit modifier son mot de passe à la prochaine connexion**.
 - c. Sélectionnez **Le mot de passe n'expire jamais**.
5. Cliquez sur **Terminer**.

Mapper le service d'authentification au compte SPN

Mappez le service d'authentification d'AX Serveur au compte SPN Active Directory à l'aide de la commande **ktpass**.

En savoir plus

1. Dans le serveur de contrôleur de domaine Active Directory, ouvrez une invite de commande et modifiez les répertoires selon l'emplacement de **ktpass.exe**.
L'emplacement par défaut est **c:\Program Files\Support Tools**.
2. Pour mapper le service d'authentification au compte SPN, saisissez la commande **keypass** suivante :

```
ktpass /out nomfichier/princ nom/pass motdepasse/mapuser nomutilisateur_local/ptype type_principal/crypto type_cryptage
```

Pour connaître la syntaxe **ktpass**, consultez [Référence Ktpass Microsoft](#).

Exemple

L'exemple suivant mappe le service d'authentification au compte SPN à l'aide de la commande **ktpass** :

```
ktpass /out 'C:\ax.keytab' /princ HTTP/axserver.ax.com@AX.COM /pass pass1234 /mapuser AXSSO /ptype KRB5_NT_PRINCIPAL /crypto RC4-HMAC-NT
```

Enregistrer un compte SPN pour le service Connecteur AX

Enregistrez un compte SPN pour le service Connecteur AX à l'aide de la commande **setspn**.

En savoir plus

1. Dans le serveur de contrôleur de domaine Active Directory, ouvrez une invite de commande et modifiez les répertoires selon l'emplacement de **setspn.exe**.
L'emplacement par défaut est **c:\Program Files\Support Tools**.
2. Pour enregistrer le compte SPN, saisissez la commande **setspn** suivante :

```
setspn -A ACLSE/domaine_complet_et_nomserveur nom_ordinateur
```

Remarque

ACLSE est la valeur requise pour identifier le Connecteur AX et elle doit être saisie tout en majuscules. La valeur *nom_ordinateur* peut se saisir comme *nom* ou *domaine\nom*.

3. Facultatif. Pour vérifier le mappage du compte SPN, utilisez la commande setspn suivante :

```
setspn -L nom_ordinateur
```

Exemple

L'exemple suivant utilise la commande setspn pour enregistrer le compte SPN :

```
setspn -A ACLSE/axserver.acl.com axserver
```

Tester le mappage de compte SPN

Si vous le souhaitez, copiez le fichier keytab vers l'instance AX Serveur et testez votre mappage de compte SPN à l'aide de la commande **kinit**.

En savoir plus

Conditions préalable : ajoutez le sous-dossier Java **bin** à votre variable d'environnement *path* pour utiliser la commande **klist** sans indiquer le chemin d'accès complet.

```
set PATH=java_bin_path;%PATH%
```

1. Dans le serveur du contrôleur de domaine Active Directory, copiez le fichier **.keytab** que vous avez créé avec la commande **ktpass** et collez-la dans le répertoire **Windows** d'AX Serveur.
2. Dans le répertoire **Windows** d'AX Serveur, créez un fichier intitulé **krb5.ini**.
3. Depuis l'invite de commande, utilisez la commande suivante pour vérifier que le fichier keytab peut se lire :

```
klist -k
```

4. Pour tenter l'authentification, utilisez la commande suivante :

```
kinit nomutilisateur@REALM.COM
```

5. Entrez le mot de passe utilisateur et appuyez sur **Entrée**.

Exemple

Voici un exemple de fichier krb5.ini :

```
[libdefaults]
ticket_lifetime = 24000
default_realm = votre_domaine
default_keytab_name = chemin_vers_fichier_keytab
dns_lookup_realm = false
dns_lookup_kdc = false
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac

[realms]
votre_domaine = {
    kdc = votre_serveur_active_directory.domaine.com:88
}

[domain_realm]
.votre_domaine = YOUR_DOMAIN
votre_domaine = YOUR_DOMAIN
```

Activer l'authentification Windows intégrée depuis Internet Explorer

Activez l'authentification Windows intégrée depuis Internet Explorer dans chaque environnement bureau de l'utilisateur final. Les utilisateurs doivent se connecter depuis un système d'exploitation client. L'authentification Windows intégrée n'est pas prise en charge pour les instances du client AX qui s'exécutent sur le système d'exploitation du serveur.

En savoir plus

1. Dans Microsoft Internet Explorer, cliquez sur **Outils > Options Internet > Avancé**.
2. Sous le groupe **Sécurité**, sélectionnez **Activer l'authentification Windows intégrée** et cliquez sur **Appliquer**.
3. Cliquez sur l'onglet **Sécurité**.
4. Sélectionnez l'icône **Intranet local**, puis cliquez sur **Sites**.
5. Dans la boîte de dialogue **Intranet local**, cliquez sur **Avancé** et saisissez l'URL HTTPS pour votre instance AX Serveur et cliquez sur **Ajouter**.

Exemple : <https://axserver.ax.com>.

6. Cliquez sur **Fermer**, cliquez sur **OK** dans chaque boîte de dialogue ouverte jusqu'à ce que la boîte de dialogue **Options Internet** se ferme puis redémarrez Internet Explorer.

Les paramètres mis à jours s'appliqueront la prochaine fois que vous lancerez Internet Explorer.

aclAuditExchange.xml

Stocke les paramètres généraux du serveur AX.

L'application Web Configuration du serveur AX permet de modifier les paramètres.

Remarque

Vous pouvez modifier la plupart de ces valeurs à partir de l'application Web Configuration du serveur AX. Vous devez utiliser l'application Web à chaque fois que cela est possible pour modifier les paramètres de serveur AX, car la validation des valeurs intervient avant que le réenregistrement du fichier `aclAuditExchange.xml`.

Paramètres fichier

Clé	Description	Champ cor-respondant dans l'application Web Configuration du serveur AX
allowExecCommand	<p>Spécifie comment le moteur de script traite la commande EXECUTE lorsqu'elle se trouve dans un outil d'analyse :</p> <ul style="list-style-type: none"> ◦ oui : la commande EXECUTE est traitée quand elle est rencontrée ◦ non (par défaut) : la commande EXECUTE est ignorée lorsqu'elle est rencontrée, un message est écrit dans la trace, mais l'outil d'analyse n'échoue pas <p>Remarque</p> <p>La commande EXECUTE est disponible dans la version 10 ou supérieure d'ACL Analytics.</p>	Autoriser la com-mande EXECUTE ?
aclsePortNumber	Le numéro de port utilisé pour se connecter au service Connecteur AX.	Numéro de port
allowExportData	<p>Spécifie si les utilisateurs d'AX Client peuvent ou non télécharger les fichiers de données depuis le serveur AX vers leur poste de travail :</p> <ul style="list-style-type: none"> ◦ oui : les options d'exportation de données dans AX Client sont activées ◦ non : les options d'exportation de données dans AX Client sont désactivées 	

Clé	Description	Champ correspondant dans l'application Web Configuration du serveur AX
	<p>Remarque Cette propriété est définie par défaut sur « oui » et ne doit pas être changée.</p>	
AXHttpsPort	Spécifie le port servant aux communications cryptées avec le serveur AX. La valeur par défaut est de 8443.	
aclsePrefixPath	Le chemin de fichier où les fichiers temporaires créés par le service Connecteur AX sont stockés.	Répertoire de travail du connecteur
AXHostname	Spécifie le nom d'hôte du serveur AX. La valeur doit être entrée en majuscules. Exemple : SERVEURAX.ABC.COM	Adresse IP ou nom de l'ordinateur du serveur
aclseProfileName	Le nom du profil de serveur utilisé pour se connecter aux tables de serveur AX Server.	<p>Remarque Utilisez la valeur par défaut de ce champ sauf si vous avez une raison spécifique de la modifier. Par défaut, la version 4.0.2 ou supérieure utilise Analytics Exchange. La version 4.0.0 utilise AuditExchange.</p>
EmDataLoadUrlRoot	L'adresse Web utilisée pour se connecter à AX Exception.	URL d'envoi des données
useWhiteList	Indique si la liste blanche des extensions de fichiers est activée : <ul style="list-style-type: none">○ oui : seuls les fichiers portant les extensions de fichiers spécifiées dans la liste blanche peuvent être chargés ou importés dans le serveur AX○ non (paramètre par défaut) : les fichiers portant n'importe quelle extension peuvent être chargés ou importés dans le serveur AX	Activer la liste blanche
mailHostServer	L'adresse IP du serveur de messagerie à utiliser pour relayer les messages vers les utilisateurs spécifiés en cas d'échec d'une chaîne analytique.	Adresse du serveur SMTP
copyDataFiles	Indique si les fichiers de données seront copiés avant le démarrage du traitement de l'outil d'analyse :	Copier les données d'analyse

Clé	Description	Champ cor-respondant dans l'application Web Configuration du serveur AX
	<ul style="list-style-type: none"> ○ oui : les fichiers de données du dossier situés à l'emplacement de l'outil d'analyse seront copiés dans le sous-répertoire de la tâche analytique avant le début du traitement de l'outil d'analyse ○ non : la tâche analytique sera traitée sans copier les fichiers de données <p>Remarque Ce paramètre ne s'applique que si vous utilisez un ou plusieurs nœuds moteur dans votre environnement se Serveur AX.</p>	
databaseLoadJobsPath	Spécifie l'emplacement de création des fichiers temporaires avant leur envoi dans la base de données.	
dataFilePath	Le dossier où les fichiers de données du serveur AX sont stockés sur le serveur. L'emplacement par défaut est C:\ACL\Data\repository\datafiles .	Répertoire de données
mailHostPassword	Le mot de passe du compte utilisateur pouvant servir à l'envoi des messages.	Mot de passe SMTP
doesLinkSecurityUseMasterLocation	<p>Indique le type des autorisations de l'application dont les utilisateurs du Client Web d'AX et du Client AX ont besoin pour accéder aux tables liées, aux formats liés et aux outils d'analyse liés.</p> <p>Les utilisateurs ont toujours besoin de l'autorisation d'accès au dossier contenant l'élément lié et à la collection parente. Ce paramètre spécifie la condition préalable d'autorisation pour l'élément maître :</p> <ul style="list-style-type: none"> ○ oui : les utilisateurs ont besoin d'autorisations vers l'élément maître et sa ou ses collections parentes ○ non : les utilisateurs n'ont pas besoin d'autorisations vers l'élément maître et ses collections parentes 	
mailHostUsername	<p>Facultatif. Le nom d'utilisateur d'un utilisateur disposant des droits appropriés sur le serveur de messagerie pour envoyer des messages électroniques.</p> <p>Remarque Selon la configuration du serveur, il se peut que ce compte ne soit pas forcément spécifié.</p>	Nom d'utilisateur SMTP

Clé	Description	Champ cor-respondant dans l'application Web Configuration du serveur AX
fileTransferPath	Le dossier où les fichiers de données sont stockés pendant les transferts de fichiers.	Répertoire de transfert des fichiers du serveur
archiveRestorePath	Spécifie l'emplacement de stockage des collections archivées.	Répertoire d'archivage et de restauration des données
emailOnFailureAddress	L'adresse électronique à utiliser comme adresse d'expéditeur dans les courriers électroniques envoyés aux utilisateurs.	adresse e-mail de l'expéditeur
trustETLserver	Cette propriété n'est pas utilisée dans cette version.	
resultsCleanupStartDate	Indique une date limite pour la fonctionnalité de nettoyage des résultats. Aucune tâche analytique ou résultat associé n'est supprimé avant la date indiquée, quels que soient les paramètres de Nettoyage des résultats d'un outil d'analyse. Cette propriété est définie par défaut sur 01/01/1900.	Date de démarrage pour le nettoyage des résultats
useResultsCleanup	Indique si le paramètre Nettoyage des résultats est activé dans l'onglet Configuration du Client AX : <ul style="list-style-type: none"> ○ oui : les utilisateurs ayant des « autorisations complètes » pour un outil d'analyse peuvent configurer la suppression automatique des tâches analytiques et des résultats associés ○ non (par défaut) : le paramètre Nettoyage des résultats est désactivé 	Activer le nettoyage des résultats
DefaultDomain	Le domaine Active Directory utilisé par défaut si un utilisateur ne spécifie pas de domaine quand il se connecte.	Domaine Active Directory par défaut
ServerType	Indique le type d'activation du serveur.	Type de serveur
fileExtensionWhiteList	La liste des types de fichiers acceptés pour le chargement ou l'importation vers le Serveur AX si la liste blanche des extensions de fichiers est activée.	Liste blanche des extensions de fichiers
mailHostPort	Le port requis pour communiquer avec le serveur de messagerie.	Port SMTP

Clé	Description	Champ cor-respondant dans l'application Web Configuration du serveur AX
	<p>Remarque Si vous utilisez le port par défaut 25, vous pouvez laisser ce champ non défini.</p>	
attachLogFile	<p>Le fait de joindre ou non les fichiers traces à la notification d'échec de l'outil d'analyse par e-mail :</p> <ul style="list-style-type: none"> ○ oui : les fichiers traces de l'outil d'analyse sont joints aux notifications par e-mail de l'échec de l'outil d'analyse ○ non (par défaut) : les fichiers traces de l'outil d'analyse ne sont pas joints aux notifications par e-mail de l'échec de l'outil d'analyse <p>Remarque Dans le cas d'un échec de la chaîne d'outils d'analyse, la trace correspondant à l'outil d'analyse ayant échoué est jointe à l'e-mail.</p>	Joindre les fichiers traces à la notification par e-mail
attachmentSizeLimitInMB	<p>La taille totale maximale des pièces jointes dans les notifications d'échec d'outil d'analyse envoyées par e-mail. Par défaut, cette valeur est définie sur 10 Mo.</p> <p>Remarque Si la taille totale maximale des pièces jointes dépasse la limite spécifiée, aucun fichier trace n'est joint à l'e-mail et la notification par e-mail indique que le système a omis les fichiers traces en raison d'une contrainte de taille.</p>	Taille totale maximale des pièces jointes (en Mo)
axClientIdleLogoutInMinutes	<p>Le nombre maximum de minutes pendant lequel AX Client peut rester inactif avant que la session soit fermée et que l'utilisateur soit déconnecté. Par défaut, cette valeur est définie sur 30.</p> <p>La valeur doit être un nombre entier ou une valeur nulle. Lorsque la valeur est définie sur nulle ou 0, l'application n'expire pas lorsqu'elle est inactive.</p>	

Clé	Description	Champ cor-respondant dans l'application Web Configuration du serveur AX
	<p>Remarque</p> <p>Si l'application effectue une importation ou exportation volumineuse et que la durée de traitement dépasse le délai d'expiration, le compteur du délai d'expiration démarrera après le traitement. L'importation ou l'exportation n'échoue pas suite au paramètre de durée d'inactivité maximale.</p> <p>Si une boîte de dialogue n'ayant aucun lien avec l'importation et l'exportation de fichiers est ouverte lorsque le délai arrive à expiration, l'application et toutes les boîtes de dialogue qui lui sont associées se ferment.</p>	
csvDataExportDisabled	<p>Indique si les utilisateurs du Client Web d'AX peuvent exporter les données de table au format CSV :</p> <ul style="list-style-type: none"> ◦ oui : l'option est désactivée ◦ non : l'option est activée <p>Le paramètre par défaut est non. Si vous modifiez le paramètre, vous devez aussi redémarrer le serveur.</p>	
addinsDataExportDisabled	<p>Indique si les utilisateurs de l'Add-in pour Excel peuvent ouvrir une table provenant d'AX Serveur dans MS Excel :</p> <ul style="list-style-type: none"> ◦ oui : l'option est désactivée ◦ non : l'option est activée <p>Le paramètre par défaut est non. Si vous modifiez le paramètre, vous devez aussi redémarrer le serveur.</p>	

Désactiver AX Serveur

Vous pouvez désactiver votre serveur à partir de l'application Web Configuration d'AX Serveur. Vous devez désactiver, puis réactiver votre serveur lors du renouvellement de votre abonnement.

Étapes

Remarque

Bien que vous puissiez désactiver le serveur, vous devez contacter l'Assistance ACL pour faire retirer le serveur de la liste des installations actives d'AX Serveur affichées dans la Barre de lancement.

1. Connectez-vous à l'application Web Configuration d'AX Serveur et localisez le panneau **Activation**.
2. Cliquez sur **Sélectionner org.**
3. Dans la liste déroulante **Organisations**, sélectionnez l'organisation à laquelle appartient le serveur, puis cliquez sur **Désactiver le serveur**.

Dépannage

Si le compte de l'utilisateur ACL GRC ayant activé AX Serveur à l'origine a été supprimé de la Barre de lancement, la désactivation échoue. Lorsque cela se produit, vous devez supprimer l'enregistrement lié à l'activation dans la base de données et réactiver l'instance de votre serveur à l'aide d'un compte ACL GRC existant.

Pour obtenir de l'aide afin de désactiver manuellement le serveur dans la base de données, contactez l'Assistance ACL.